RAHMAN, K.U., FOUGH, N., MCDERMOTT, C.D., SUNDAS, R., BAIG, N. and KANNAN, S. 2024. Securing underwater wireless communication with frequency-hopping spread spectrum. In *Proceedings of the 2024 IEEE (Institute of Electrical and Electronics Engineers) International workshop on Metrology for the sea; learning to measure sea health parameters (IEEE MetroSea 2024), 14-16 October 2024, Portorose, Slovenia*. Piscataway: IEEE [online], pages 266-271. Available from: https://doi.org/10.1109/metrosea62823.2024.10765656

Securing underwater wireless communication with frequency-hopping spread spectrum.

RAHMAN, K.U., FOUGH, N., MCDERMOTT, C.D., SUNDAS, R., BAIG, N. and KANNAN, S.

2024

Securing Underwater Wireless Communication with Frequency-Hopping Spread Spectrum

Khaliq Ur Rahman , Nazila Fough, Christopher D. McDermott, Rida Sundas , Nauman Baig, Somasandar Kannan

School of Computing, Engineering and Technology, Robert Gordon University,Aberdeen, Scotland , UK

Abstract— **The significance of subsea communication has increased substantially, with growing interest in replacing wired communication with wireless alternatives. However, subsea communication faces several challenges due to the harsh environment, including high noise, significant multipath propagation, signal attenuation, salinity, and temperature variations. Additionally, it is vulnerable to cyber-attacks. Ensuring secure and reliable communication for authorized users remains a significant challenge, requiring an integrated approach that balances efficiency, stability, and security considerations. Current efforts primarily focus on designing multimodal wireless communication systems, but integrating robust security measures into subsea wireless infrastructure is challenging due to its inherently open nature and susceptibility to external interference. Technical advancements are necessary to strengthen the security of subsea wireless communication while managing power loss effectively. To address these challenges, we propose a mechanism that implements a pre-determined frequency hopping schedule, enhancing security and improving reliability through periodic changes in transmission frequency. The hopping sequence is shared in advance among authorized parties. While the current system does not adapt to real-time threats, future work could explore dynamic adjustments in response to detected threats or unauthorized access attempts.**

Keywords— Data Integrity, Confidentiality, Underwater Acoustic Communication, Frequency-Hopping Spread Spectrum (FHSS)

I. INTRODUCTION

The importance of subsea communication has grown significantly, driven by the need for efficient data transfer in underwater environments. There is increasing interest in transitioning from wired to wireless communication to enhance flexibility and reduce infrastructure costs. However, subsea communication systems face numerous challenges due to the harsh underwater environment, which includes high noise levels, limited bandwidth, high pressure, significant multipath propagation, signal attenuation, and variations in salinity and temperature. some of the major factors affecting the ability to transmit signal effectively in underwater environment, include multipath propagation, Doppler spread, and time varying channel conditions [1]. Multipath propagation does cause signal distortion due to the path differences and interferences that the signals encounter from the transmitter to the receiver. Relative motion between the transmitter and the receiver interferes with frequencies, referred to as Doppler spread, which distorts the transmitted signal. Time-varying channel conditions also poses another challenge as such issues like random fluctuations, scattering, and shifting of frequency directly influence the channel dynamics of communication as well as the actual stability of the link. Additionally, these systems are vulnerable to various cyber-attacks, making it crucial to ensure secure and reliable communication for authorized users while maintaining an optimised power usage. Possible cyber threats to subsea communication include:

- Eavesdropping: Unauthorized interception of data transmitted through underwater communication channels.
- Jamming: Deliberate interference with acoustic signals to disrupt communication.
- Spoofing: Sending false data or commands to mislead the communication system.
- Malware Insertion: Introducing malicious software into the control systems of subsea communication infrastructure.
- Replay Attacks: Repeating or delaying valid data transmissions to deceive the system.

Subsea wireless communication can be used for transmission of data related to sensitive operations like oil and gas exploration, environmental surveys and monitoring, or military applications. Therefore, it must be secure to avoid unauthorized access, tampering, and to protect sensitive information. The confidentiality, integrity, and availability of this data must be protected to maintain operational efficiency, prevent environmental hazards, and preserve national security. Addressing this complex issue requires an integrated approach that balances efficiency, stability, and security considerations. While current efforts primarily focus on designing multimodal wireless communication systems [2], integrating robust security measures into subsea wireless infrastructure is challenging due to its inherently open nature and susceptibility to external interference. Technical advancements are necessary to enhance the security of subsea wireless communication, but these improvements must be balanced with power management considerations. To tackle these challenges, we propose a mechanism that implements a pre-defined frequency hopping schedule. This approach enhances security and improves communication reliability by periodically changing transmission frequencies according to a predetermined pattern.

II. BACKGROUND

The use of spread spectrum modulation techniques for securing underwater wireless communication is comprehensive research field that target data transmission stability and cyber-attacks prevention [3].

Spread spectrum modulation techniques significantly contribute to securing underwater wireless communication systems as the signal is spread over a wide bandwidth thus making it difficult to interfere with the signal or intercept the data being transmitted [3]. This approach is especially useful in underwater environments where typical communication methods are limited by issues such as multipath fading, turbulence, and signal attenuation. Using methods such as frequency hopping and direct sequence spreading, spread spectrum modulation improves the privacy of communication in underwater environments [3]. These methods serve to ensure the confidentiality, integrity and availability of information, key to reliability of underwater communication systems.

The two primary spreading techniques that are vital in increasing the effectiveness and security of underwater wireless communication are: (i) Direct Sequence Spread Spectrum (DSSS) and (ii) Frequency Hopping Spread Spectrum (FHSS).

i) Direct Sequence Spread Spectrum (DSSS)

DSSS is done by spreading the spectrum of the transmitted signal using a pseudo-random spreading code sequence; this assists in narrowing down interference power within the signal band, thus enhancing signal-to-noise ratio at the receiver end [4]. While DSSS has been compared with other spread spectrum techniques for channel distortions in underwater acoustic communication [5][6][14], we will explore this comparison in future work.

ii) Frequency Hopping Spread Spectrum (FHSS)

In contrast, FHSS consist of hopping through frequencies within a specific range at a very high speed. This technique targets at enhancing the reliability of underwater communication systems by hopping the signal at different frequencies; thereby making it difficult for the attackers to jam the signal. Using encrypted spreading codes and switching between two or more frequencies, FHSS systems should be able to improve the level of security and ensure the integrity of the communication even in the case of partial band noise jamming [7].

Due to their anti-interference capabilities and ability to ensure secure data transmission, FHSS and DSSS techniques have been widely researched and used in terrestrial wireless communication systems [8], however, lacks its implementation in underwater wireless communication systems. These spreading techniques are crucial in addressing many challenges faced in underwater environment for instance, multipath propagation conditions and channel distortions. By integrating spread spectrum techniques like DSSS and FHSS, underwater communication systems can achieve robust and secure data transmission [9], which are advantageous in numerous underwater applications such as underwater exploration, environmental monitoring, and underwater surveillance. In this paper, we have utilised and implemented a novel technique based on FHSS with 4-FSK modulation, while we will be using DSSS in our future research.

A. Frequency Hopping Spread Spectrum (FHSS)

Frequency hopping spread spectrum (FHSS) is a method applied in communication systems to improve the signal security or resistance against interference and jamming. In underwater acoustic communication, FHSS involves rapidly switching frequencies within a predefined sequence. It means that the transmitter and the receiver hop from one frequency to another within a given frequency band within a short period. The given method proves useful in expanding the signal over a wide bandwidth, making it more resilient to noise and interference and hence, enhance the signal to noise ratio [10]. This sequence of frequency changes plays a big role in expanding the signal energy over a wide bandwidth, which in turn enhances the link's resistance to interferences, jamming, and fading.

The mathematical representation of FHSS involves defining a set of frequencies and a hopping pattern that determines how the transmitter and the receiver switch between the set frequencies [11]. The hopping pattern can be deterministic or pseudo-random, and this must be very well arranged to get the synchronization between the transmitter and the receiver. FHSS makes it possible for the frequency hops to be coordinated based on the hopping pattern so as help in the transmission of the data over a wide frequency band thus improving on the security and reliability of the communication network. Using FHSS in the underwater acoustic communication, the system can guarantee enhanced reliability and performance under challenging underwater environments [12].

Let's assume that the set of available frequencies for hopping is denoted by $F = \{f_1, f_2, f_3, \dots, f_n\}$ (1)

where n is the total number of frequencies.

The hopping pattern is represented by a sequence

$$H = \{h_1, h_2, h_3, \dots, h_n\} \qquad (2)$$

where each element $h_i \in \{1, 2, 3, \dots, n\}$ represents the index of the frequency f_{hi} to be used during the i^{th} hop.

The transmitted signal $s(t)$ using FHSS can be mathematically represented as:

$$s(t) = A_k(t)\, cos(2\pi f_{hk}(t - kT_h) + \theta_k) \qquad (3)$$

where:

- $A_k(t)$ is the amplitude of the k-th hop, which can be a constant or a time-varying function.
- f_{hk} is the frequency used during the k^{th} hop, selected from the set F based on the hopping pattern H.
- T_h is the hop duration, which is the time interval during which a specific frequency is used.
- θ_k is the initial phase of the k^{th} hop.

The hopping pattern H is typically generated using a pseudorandom sequence known to both the transmitter and receiver. This sequence can be mathematically represented as:

$$H = \{h_1, h_2, h_3, \dots, h_n\} = \{PN(1), PN(2), PN(3), \dots, PN(n)\} \qquad (4)$$

where $PN(i)$ is the i-th element of a pseudorandom sequence generated using a specific algorithm or function.

At the receiver end, the demodulation process involves synchronizing with the hopping pattern and de-hopping the received signal to recover the original transmitted signal.

The received signal r(t) can be represented as:

$$r(t) = A_k(t - \tau)\, cos(2\pi f_{hk}(t - \tau - kT_h) + \theta_k) + n(t) \qquad (5)$$

where:

- τ is the propagation delay
- $n(t)$ is the additive noise present in the channel

The de-hopping process involves multiplying the received signal r(t) with a locally generated replica of the hopping sequence, which can be mathematically expressed as:

$$r(t)\, cos(2\pi f_{hk}(t - kT_h)) \qquad (6)$$

This process effectively removes the frequency hopping and recovers the original transmitted signal, assuming perfect synchronization and knowledge of the hopping pattern.

These mathematical representations provide a formal description of the FHSS technique, including the definition of the frequency set, hopping pattern, transmitted and received signals, and the de-hopping process at the receiver.

B. *Implementation of Frequency Hopping Spread Spectrum (FHSS)*

The whole FHSS process utilized in this paper from binary data to demodulation can be expressed as:

A sequence of 20 random binary digits (0 or 1) are generated. These binary digits represent the information to be transmitted. Each pair of bits in the sequence is encoded into a specific frequency shift keying (FSK) signal.

Let $b[i]$ denote the i-th binary digit. The binary input sequence is represented as:

$$b(t) = \{b1, b2, \dots, bN\}, bi \in \{0,1\} \qquad (7)$$

A sampling frequency F_s is set to 100 kHz, the duration of each frequency hop T to 0.01 seconds which generates a time vector t for one hop. This vector is used to create the signal in the time domain. Here we used the following:

$$F_s = 90{,}000 \text{ Hz}$$

$$T = 0.01s$$

$$t = \left\{\{0, \frac{1}{F_s}, \frac{2}{F_s}, \dots, T - \frac{1}{F_s}\}\right. \qquad (8)$$

A pool of six frequencies is used in the frequency hopping spread spectrum (FHSS) scheme which specifies a pseudorandom sequence for frequency hopping.

$$freq_{pool} = \{20kHz, 24kHz, 28kHz, 32kHz, 36kHz, 40kHz\}$$

And $hop_{sequence} = \{2,4,1,3,6,5\}$ (9)

Then the 4-FSK Frequency Offsets sets the frequency offsets for the 4-FSK modulation. These offsets determine the exact frequencies used to encode the four possible 2-bit combinations. In 4-FSK modulation, we use four distinct frequencies to represent the four possible combinations of two bits: 00, 01, 10, and 11. These frequency offsets are calculated based on a central frequency and a frequency deviation value Δf. Here we set the frequency deviation Δf to 2 kHz. The frequency deviation is the step size between the different frequency levels used in the 4-FSK scheme. For each 2-bit combination, a specific frequency offset is defined as per following details:

f_{low}: Offset for the bit pair 00

f_{midlow}: Offset for the bit pair 01

$f_{midhigh}$: Offset for the bit pair 10

f_{high}: Offset for the bit pair 11

This can be mathematically represented as:

f_{low}: $-1.5\Delta f = -1.5 \times 2000 = -3000Hz$

f_{midlow}: $-0.5\Delta f = -0.5 \times 2000 = -1000Hz$

$f_{midhigh}$: $0.5\Delta f = 0.5 \times 2000 = 1000Hz$

f_{high}: $1.5\Delta f = 1.5 \times 250 = 3000Hz$

In 4-FSK, each pair of bits $(b1, b2)$ is mapped to one of these four frequency offsets. The mapping can be described as:

(00) → $f_{low} = -3000Hz$

(01) → $f_{midlow} = -1000Hz$

(10) → $f_{midhigh} = 1000Hz$

(11) → $f_{high} = 3000Hz$

These frequency offsets are added to the central hopping frequency to generate the actual frequencies used for transmitting each 2-bit pair. The central hopping frequency changes according to the pseudorandom hop sequence, and the offsets ensure that the four unique frequencies corresponding to the 4-FSK modulation are used.

For instance, if the current hopping frequency (f_{hop}) is 20,000 Hz, the actual frequencies used for each 2-bit combination would be:

(00): $f_{hop} + f_{low} = 20{,}000\ Hz + (-3000Hz) = 17\ kHz$

(01): $f_{hop} + f_{midlow} = 20{,}000\ Hz + (-1000Hz) = 19kHz$

(10): $f_{hop} + f_{midhugh} = 20{,}000\ Hz + (1000Hz) = 20\ kHz$

(11): $f_{hop} + f_{high} = 20{,}000\ Hz + (3000Hz) = 23\ kHz$

By using these frequency offsets, the code ensures that each pair of bits is uniquely represented by a specific frequency, facilitating accurate data transmission and reception using 4-FSK modulation within an FHSS system.

After that a seed is generated for synchronization purposes. This seed is used to initialize the pseudorandom number generator, ensuring that both the transmitter and the receiver can produce the same sequence of numbers if they share the same seed. Currently we are using fixed seed.The seed ensures that the transmitter and receiver are synchronized, using the same sequence of frequencies for hopping. After that signals are generated by initializing empty arrays to store the generated FHSS 4-FSK signal, FSK signal, and non-return-to-zero (NRZ) signal. Initializing these arrays prepares the program for signal generation and processing.

The. Hopping of entire FHSS signal is the concatenation of these modulated signals:

$$s(t) = \sum_{i=1}^{N} s_i\,(t) = \sum_{i=1}^{N} cos\,(2\pi f_i t + \phi_i) \qquad (10)$$

At the receiver end, the synchronization signal is correlated with the received signal to determine the timing offset. This synchronization step ensures accurate alignment of received data with the transmitter's timing, crucial for subsequent demodulation and decoding processes which can represented as:

$$correlation\ (k) = \int_{-\infty}^{\infty} r(t)s(t-k)dt \qquad (11)$$

Where $s(t)$ is the synchronized signal and $r(t)$ is the received signal.

For the timing offset τ:

$$\tau = \arg max_k \mid \text{correlation(k)} \mid \qquad (12)$$

Here, τ represents the timing offset where the synchronization signal aligns best with the received signal.

Once τ is determined, using the synchronized timing information, the data portion of the received signal is extracted. $r_{data} = r(t - \tau - T_{sync})$ (13)

Frequency domain analysis FFT is performed on $r_{data}\ (t)$ segments to estimate the frequency components.

$$R(f) = \mathrm{F}\{r_{data}(t)\} \qquad (14)$$

Then the frequency offset identification determine the frequency offset Δf applied to each 2-bit pair by analyzing the frequency spectrum $R(f)$.

$$\Delta f = f_{estimated} - f_{carrier} \qquad (15)$$

The binary symbol recovery map Δf back to the corresponding 2-bit binary symbol to reconstruct the transmitted binary sequence.

$$\begin{cases} [00], & if\ \Delta f = \Delta f_{low} \\ [01], & if\ \Delta f = \Delta f_{midlow} \\ [10], & if\ \Delta f = \Delta f_{midhigh} \\ [11], & if\ \Delta f = \Delta f_{high} \end{cases} \qquad (16)$$

These steps collectively outline the process of FHSS with 4-FSK modulation for underwater acoustic communication, highlighting essential techniques and considerations for robust, secure, and reliable data transmission in challenging subsea environments.

III. PROPOSED METHOD AND SIMULATION DESIGN

In this section, we explain the methodology and simulation model to assess the performance of Frequency Hopping Spread Spectrum combined with Frequency Shift Keying (FHSS-4 FSK) for underwater acoustic communication. This includes several key stages: signal generation, its modulation technique, signal to be transmitted through underwater channel, reception/de-modulation and analysis of performance. Each stage is made purposefully to model the actual conditions of underwater acoustic channel, which includes, high attenuation, noise, and variability of underwater environment.

A. Underwater Acoustic Channel Model:

To accurately simulate the underwater acoustic channel, several critical parameters are considered. These include the transmission distance d, carrier frequency f_c, ambient noise power spectral density (PSD), and the speed of sound c in water. Path loss, a key metric influenced by these parameters, is estimated using Thorp's empirical model, which accounts for frequency-dependent absorption and scattering effects over distance d.

$$\alpha(f_c, d) = 0.11 \times 10^{-3} + \frac{f_{c^2}}{1+f_{c^2}} + 44 \times 10^{-3} \frac{f_{c^2}}{4100+f_{c^2}} + 2.75 \times 10^{-4} f_{c^2} + 0.003 \qquad (17)$$

where $\alpha(f_c, d)$ denotes the path loss coefficient in dB, $f_c$is the carrier frequency in Hz, and d is the transmission distance in meters. The resulting path loss L_{path} is then calculated as:

$$L_{path} = \alpha(f_c, d) \times d \qquad (18)$$

Ambient noise, another critical factor, is characterized by its PSD N_o in dB re $\mu Pa^2/Hz$, primarily influenced by environmental noise sources such as shipping activity. The noise power P_n across a bandwidth B is determined using:

$$N_o\ (f_c) = 17 - 30log_{10}(f_c) \qquad (19)$$

$$P_n = (10^{\frac{N_0+10log_{10}B}{10}}) \qquad (20)$$

The speed of sound c in water is calculated using the formula:

$$c = 1449.2 + 4.6.\mathrm{T} - 0.055\ .T^2 + 0.00029 \cdot T^3 + (1.34 - 0.01 \cdot \mathrm{T}) \cdot (\mathrm{S} - 35) + 0.016 \qquad (21)$$

where T is the water temperature in degrees Celsius, S is the salinity in parts per thousand (ppt), and D is the depth in meters. These parameters collectively define the underwater acoustic channel, enabling realistic simulation of signal propagation and reception in challenging underwater environments.

B. Simulation Deisgn:

The design of the simulation for the FHSS together with 4-FSK modulation is to examine the efficiency of the same for the purpose of using it in underwater acoustic communication. This section details the comprehensive methodology employed to model and simulate the FHSS-4-FSK system using MATLAB_R2023b. This simulation is intended to simulate the performance of an underwater acoustics communication system using Frequency Hopping Spread Spectrum FHSS with 4-FSK modulation. The simulation starts with the generation of 10 random 2-bit input sequences in binary format. Every two bits ‘00,’ ‘01,’ ‘10,’ ‘11’ is represented using using specific frequency offsets within a 4-FSK modulation scheme. The modulation process assigns each binary pair a unique frequency shift from the predetermined set of frequencies; -3 kHz: f_{low} ; -1 kHz: f_{midlow}; 1 kHz: $f_{midhigh}$; 3 kHz: f_{high}.

Performance analysis of this simulation process is done through calculating Bit Error Rate (BER) by comparing the recovered binary sequence to the original transmitted sequence. BER measures the accuracy of the communication system with respect to simulated underwater conditions, considering noise, path loss, and synchronization accuracy. The table I provides details for different parameters used in this simulation. The parameters in Table 1 are designed based on the specifications of high-speed underwater acoustic modems for short-range transmissions [15] in shallow waters to ensure optimal performance and reliability. The table II gives detail about how different frequencies are used from the pre-determined hopping frequencies. It is clear that a distant frequency is used for each of the transmitted bits.

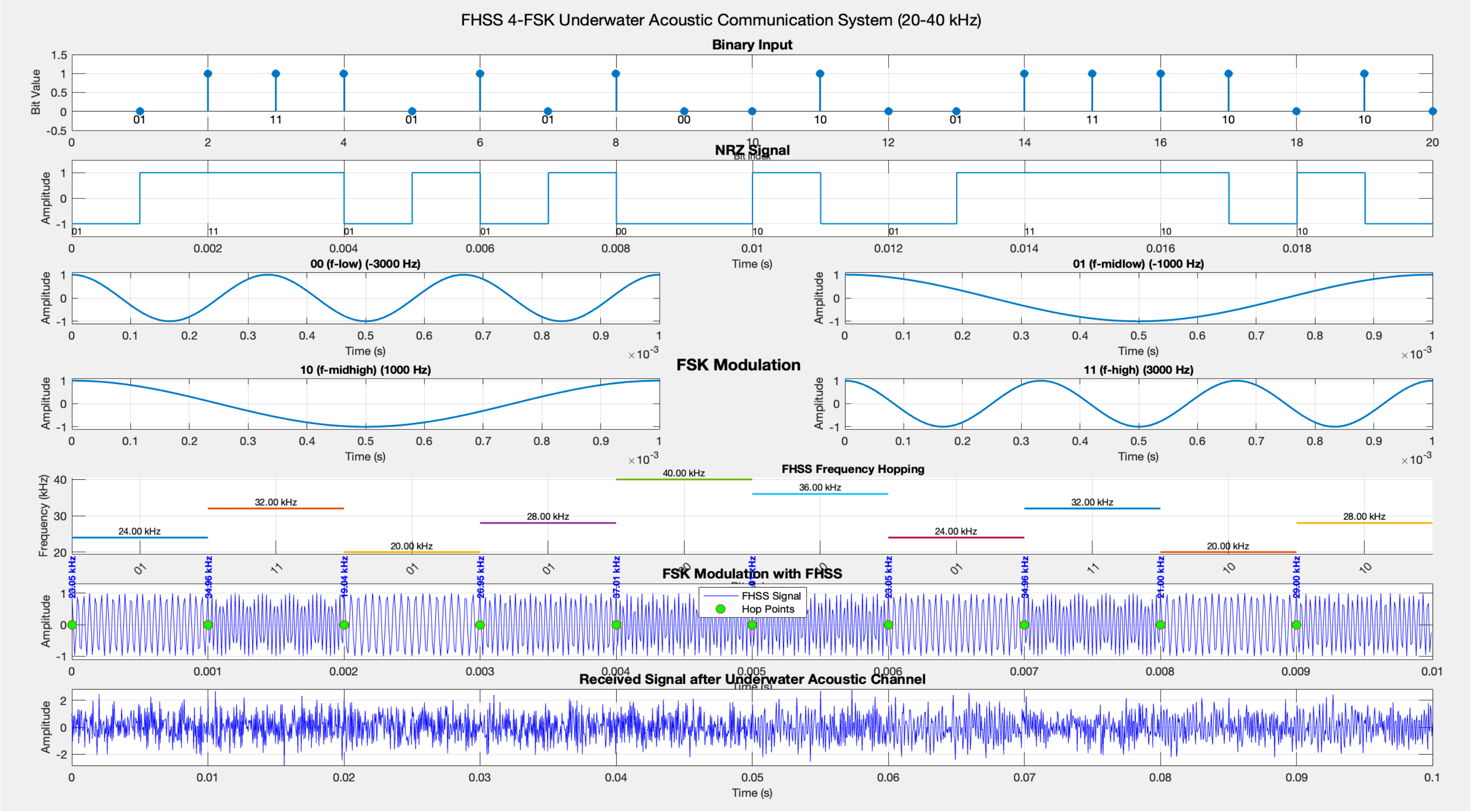

Figure 1 Simulation results of (i) Binary information, (ii) NRZ Signal of (i), (iii) 4-FSK modulated signals, (iv) FHSS Frequency Hopping (v) FSK Modulated signal with FHSS, (vi) Recieved Signal through Underwater Acoustic Channel

IV. RESULTS AND DISCUSSION

The FHSS 4-FSK Underwater Acoustic Communication System operating in the 20-40 kHz range was implemented and analyzed to evaluate its performance in challenging underwater environments.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Binary Input Sequence Length	20 bits (10 pairs of 2-bit combinations)
Sampling Frequency F_s	90,000 Hz (90 kHz)
Transmission Distance	300 meters
Frequency Pool for Hopping	[20 kHz, 24 kHz, 28 kHz, 32 kHz, 36 kHz, 40 kHz]
Pseudorandom Hopping Sequence	[2, 4, 1, 3, 6, 5]
Synchronization Preamble Duration	100 ms
Path Loss	Calculated based on fc and distance
Ambient Noise PSD	Modeled based on underwater noise characteristics
Carrier Frequencies Mean	Mean of frequency pool (e.g., 20 kHz)
Water Temperature	20°C
Salinity	35 parts per thousand (ppt)
PRNG Seed for Synchronization	Predefined and fixed
Speed of Sound in Water	Calculated based on temperature, salinity, and depth

Figure 1 presents a comprehensive visualization of the system's signal processing stages, from binary input to received signal after transmission through simulated underwater acoustic channel. This multi-faceted approach, combining Frequency Hopping Spread Spectrum (FHSS) with 4-ary Frequency Shift Keying (4-FSK) modulation, aims to enhance communication reliability and security in underwater applications. The following discussion examines the key components of the system, their interactions, and the implications for underwater acoustic communication performance.

TABLE II. FREQUENCY HOPPING PATTERN

Pair Index	Binary Pair	Frequency Hopping Sequence	Hopping Frequency (kHz)	Frequency Offset (Hz)	Final Frequency (kHz)
1	**11**	**2**	**24 kHz**	**+3 kHz**	**27 kHz**
2	**10**	**4**	**32 kHz**	**+1 kHz**	**33 kHz**
3	**01**	**1**	**20 kHz**	**-1 kHz**	**19 kHz**
4	**11**	**3**	**28 kHz**	**+3 kHz**	**31 kHz**
5	**01**	**6**	**40 kHz**	**-1 kHz**	**39 kHz**
6	**00**	**5**	**36 kHz**	**-3 kHz**	**33 kHz**

Figure 1 presents the sSimulation results of FHSS-FSK Communication. (i) Binary Input: The top plot shows the binary input sequence, representing the digital data to be transmitted. (ii) NRZ Signal:. This plot demonstrates the Non-Return-to-Zero (NRZ) encoding of the binary input, which is a common transmission technique. (iii) 4 FSK modulated signal: The next four sub plots illustrate the Frequency Shift Keying (FSK) modulation process. They show the carrier signals for each of the four frequency states (00, 01, 10, 11) used in 4-FSK modulation. (iv) FHSS Frequency Hopping: This plot shows the hopping pattern used in the FHSS technique. It illustrates how the carrier frequency changes at regular intervals, enhancing the system's resistance to interference and improving security (v) 4- FSK Modulation with FHSS: This plot combines the FSK modulated signal with Frequency Hopping Spread Spectrum (FHSS) technique. The varying amplitudes and frequencies demonstrate how the signal hops between different frequency channels over time..(vi) Received Signal through Underwater Acoustic Channel: The bottom plot represents the received signal after passing through the underwater acoustic channel. The noise and distortion evident in this plot highlight the challenges of underwater communication. This figure not only confirms the effectiveness and successful implementation of the FHSS 4-FSK system but also provides a visual understanding of how it generates its performance in underwater conditions.

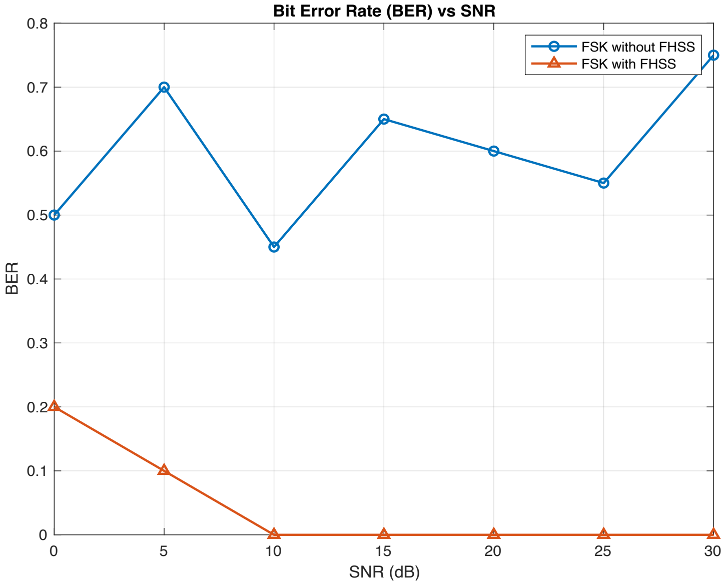

Figure 2 BER Comparison with FHSS and without FHSS

In the context of our system, the frequency deviation Δf directly impacts the system's performance by determining how easily the receiver can distinguish between the four frequency states in 4-FSK modulation. A larger Δf improves BER by increasing the separation between frequency states, making the signal more resilient to noise and multipath effects in underwater environments. However, an overly large Δf reduces spectral efficiency by occupying more bandwidth, while a smaller Δf increases BER due to overlapping frequency bands. Therefore, Δf is selected to balance spectral efficiency and BER performance, ensuring reliable communication in short-range underwater transmissions.

These figures collectively provide insights into the effectiveness of FHSS-4 FSK modulation in enhancing security, reliability, and performance in underwater acoustic communication systems. The simulations are conducted using MATLAB_R2023b, incorporating realistic environmental parameters and signal processing techniques to evaluate system behavior under challenging underwater conditions.

V. CONCLUSION

The combination of Frequency Hopping Spread Spectrum (FHSS) and Frequency Shift Keying (4-FSK) modulation has demonstrated great potential in improving the security and reliability of underwater acoustic communication by reducing noise and multipath effects. In comparison to non-hopped systems, the simulation results demonstrated how well FHSS-FSK performs in enhancing signal integrity, lowering Bit Error Rates (BER), and increasing overall system reliability. Going forward, the emphasis should be on refining adaptive approaches and hopping patterns to further improve system security, performance, and resilience against cyber threats. Investigating novel FHSS combinations with various spreading strategies may improve spectral efficiency, reliability, and cyber security.

References

[1] C. Stewart, Nazila Fough, and R. Prabhu, "A simulation into the physical and network layers of optical communication network for the subsea video surveillance of illicit activity," *OpenAIR@RGU (Robert Gordon University)*, Oct. 2022.

[2] C. Stewart, N. Fough and R. Prabhu, "Multimodal, Software Defined Networking for Subsea Sensing and Monitoring," *OCEANS 2023 - Limerick*, Limerick, Ireland, 2023, pp. 1-6.

[3] A. Badrudduza, M. Ibrahim, S. Islam, M. Hossen, I. Ansari, & H. Yu, "Security at the physical layer over gg fading and megg turbulence induced rf-uowc mixed system", IEEE Access, vol. 9, p. 18123-18136, 2021.

[4] Y. Zhang, Z. Zhao, X. Feng, T. Zhao, & Q. Hu, "Implementation of underwater electric field communication based on direct sequence spread spectrum (dsss) and binary phase shift keying (bpsk) modulation", Biomimetics, vol. 9, no. 2, p. 103, 2024.

[5] J. An, H. Ra, C. Youn, & K. Kim, "Experimental results of underwater acoustic communication with nonlinear frequency modulation waveform", Sensors, vol. 21, no. 21, p. 7194, 2021.

[6] F. Zhou, B. Liu, D. Nie, G. Yang, W. Zhang, & D. Ma, "M-ary cyclic shift keying spread spectrum underwater acoustic communications based on virtual time-reversal mirror", Sensors, vol. 19, no. 16, p. 3577, 2019.

[7] A. Ebrahimzadeh and A. Falahati, "Frequency hopping spread spectrum security improvement with encrypted spreading codes in a partial band noise jamming environment", Journal of Information Security, vol. 04, no. 01, p. 1-6, 2013.

[8] M. ElSharkawy, "A new scheme for spreading &amp; de-spreading in the direct sequence spread spectrum mechanism", International Journal of Communication Networks and Information Security (IJCNIS), vol. 10, no. 1, 2022.

[9] M W. Shen, P. Ning, X. He, & H. Dai, "Ally friendly jamming: how to jam your enemy and maintain your own wireless connectivity at the same time", 2013 IEEE Symposium on Security and Privacy, 2013.

[10] L. Segers, J. Tiete, A. Braeken, & A. Touhafi, "Ultrasonic multiple-access ranging system using spread spectrum and mems technology for indoor localization", Sensors, vol. 14, no. 2, p. 3172-3187, 2014.

[11] B. Wen, "Construction of optimal sets of frequency hopping sequences", ISRN Combinatorics, vol. 2013, p. 1-4, 2013.

[12] G. Lee, W. Park, T. Kang, K. Kim, & W. Kim, "Chirp-based fhss receiver with recursive symbol synchronization for underwater acoustic communication", Sensors, vol. 18, no. 12, p. 4498, 2018.

[13] C. Zhan, F. Xu, & X. Hu, "Parallel combinatory multicarrier frequency-hopped spread spectrum for long range and shallow underwater acoustic communications", Proceedings of the Eighth ACM International Conference on Underwater Networks and Systems - WUWNet '13.

[14] L. Freitag, M. Stojanovic, S. Singh and M. Johnson, "Analysis of channel effects on direct-sequence and frequency-hopped spread-spectrum acoustic communication," in IEEE Journal of Oceanic Engineering, vol. 26, no. 4, pp. 586-593, Oct. 2001.

[15] EvoLogics Home Page. Available online https://www.evologics.com/acoustic-modem/hs (accessed on 06 September 2024).