Journal of Telecommunication, Electronic and Computer Engineering
ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. 15 No. 1
jtec.utem.edu.my

Application of Tuneable Notch Filters for Improved Signal Jamming Protection

P. Elechi, E.U. Okowa and U.B. Cornelius
Department of Electrical/Electronic Engineering, Rivers State University, Port Harcourt, Nigeria
elechi.promise@ust.edu.ng

Article Info

Article history:
Received Oct 5th, 2022
Revised Dec 15th, 2022
Accepted Jan 17th, 2023

Index Terms:
Filters
Signal Jamming
Signal-to-Noise Ratio
Interference

Abstract

Adjacent channel interference is an inevitable consequence of the increasing number of radio signals and their widespread accessibility. In addition to this interference, information can be distorted by jamming techniques used by hackers and, in some cases, security services like the military. This research concentrated on enhancing jamming protection using a tunable notch filter, considering the growing need to ensure that accurate information reception. The necessary signal was provided through a signal source, and a barrage jammer was used to introduce the jamming signal that would interfere with the original signal. The circuit also featured an adjustable notch filter designed to mitigate the impact of the jamming signal. A spectrum analyzer was used to examine the circuit's performance. The effectiveness of the notch filter in counteracting the effects of the jammer was examined through simulations using MatLab. Based on the distortion measurement, the signal-to-noise ratio (SNR) of the filtered signal, which was 4.92 dB, which was higher than the original signal's 1.92 dB. This finding indicates that the jamming effect was substantially reduced or eliminated. Additionally, it was discovered that without a notch filter, an increase in the jammer-to-signal noise ratio significantly decreased the signal-to-noise ratio value. However, the implementation of the notch filter prevented a drastic decline in performance, demonstrating that as the jammer-to-signal noise ratio increased, the depth of the notch also increased.

I. INTRODUCTION

A. Background of the Study

Over the past few decades, there has been a remarkable surge in the use of cellular systems, leading to an increasingly congested radio radio spectrum. As the number of subscribers and cellular technologies continues to grow, the radio spectrum becomes more crowded, particularly in densely populated areas. This congestion often results in increased interference, which negatively impacts the optimal performance of communication systems. However, the degree of interference varies depending on the location. For example, on naval vessels, numerous high-powered systems are co-located on a single mast, making it impossible to use spatial antenna separation techniques to mitigate interference due to the high level of interference [1].

In addition to the interference caused by closely co-located masts, another increasing and worsening type of interference arises from the actions of hackers and even military authorities that use jammers to disrupt legitimate radio frequency communications. Such interference can lead to disastrous and catastrophic consequences. Additionally, the widespread availability of software-defined radio (SDR) enables the easy generation of continuous wave signals that jam communication systems. Unfortunately, the challenges posed by jammers show no sign of abating in the foresaable future.

During times of war, opposing forces employ various tactics to deceive, or weaken their adversaries in an attempt to gain an upper hand. One such tactic involves the intentional transmission of radio signals that operate at the same frequency as the receiver used by the enemy. If the intentionally transmitted radio signal is powerful enough, it can override any signals present at the receiving equipment, disrupting the opponent's communication and potentially providing a strategic advantage.

According to [2], communication disruption occurs when the signal-to-noise ratio (SNR) is decreased due to such intentional radio signal transmissions.With the ongoing global expansion of wireless technology, jamming has become a significant area of research, given the potential to obstruct communication. Researchers aim to understand jamming attacks fully and explore how malicious nodes introduce interference in wireless networks, hindering seamless communication.

Although many countries have declared the use of jamming devices illegal, these devices can still be easily acquired online, as governments have not been entirely successful in preventing their availability. As a result, the challenge remains to improve protection against jamming and ensure the integrity and reliability of wireless communication systems.

Now, more than ever, devices capable of broadcasting or transmitting signals designed to disrupt normal digital communication are proliferating. Despite many countries declaring the use of devices that intentionally transmit jamming signals illegal, their use continues unabated. In fact, jammers or devices that broadcast signals to disrupt electronic communication can be easily obtained online. The rapid spread of these jammers, despite being banned in many countries, is becoming a growing concern for communication experts.

If relevant authorities worldwide cannot stop the production, sale and use of these disruptive jammers, telecommunication experts must develop methods to mitigate jamming in communication systems. Without such jamming protection or mitigation measures, there is a considerable risk that communication could be blocked, distorted or disrupted. However, with improved jamming protection, we can ensure reliable communication with minimal disruption, even in the face of the widespread availability of portable jamming devices across many countries.

B. Review of Related Work

[3] used a Stackelberg Game approach to investigate anti-jamming hierarchical optimization in the relay communication system. The researchers examined the selection of joint relays in conjunction with the power control optimization problem specific to an anti-jamming relay communication system. They assumed that the system consists of four entities: the user, the base station, the relay groups, and the jammer. Due to channel fading inherent in wireless communication, the user does not transmit directly to the base station; instead, they sends the signal to the group of relays that already possessing their information. The transfer of information or message to the relay group constitutes phase 1. Upon receiving the message from the user, the relay group retransmits the received information to the base station, which constitutes phase 2. To adversely impact communication quality, the jammer introduces signals as noise, as shown in figure 1.

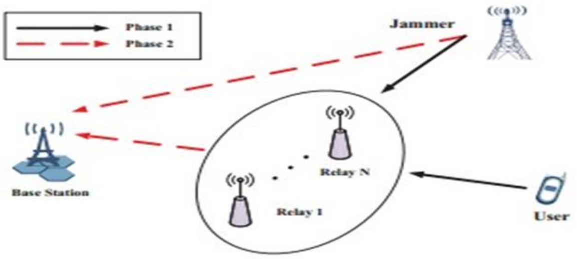

Figure 1: Anti-jamming Communication System [20].

The anti-jamming joint optimization problem was formulated as a Stackelberg game by the authors, where the user as the leader and the jammer as the follower. They proposed an algorithm to achieve the user's strategic optimization based on the Q-learning algorithm and the multi-armed bandit method. The results showed the superiority of the proposed algorithm over the random selection algorithm.

In their study,[4] utilized the bit error rate to detect jamming. By relying on the received signal strength level (RSS) of a communication network when transmitted bits are received, the authors proposed a novel network, as a solution to the jamming problem in wireless networks.

[5] proposed a scheme to detect and counter-jamming attacks in wireless sensor networks, utilizing an evolutionary algorithm. In the work, an agent iteratively navigates the network, allowing Ant system to collect information on different routes to a given destination. This information is saved for redirection purposes. The authors employed various types of gammers, including single-tone jammers, pulsed-noise jammers, multiple-tone jammers, and electronic intelligent jammers. Metrics used in their study included packet loss (PL), hops, distance, and packet delivery ratio (PDR). According to the authors, carefully examining these metrics activates a decision model that determines if jamming detection is false or true. The system then iteratively calculates transition probabilities, and if such probability falls within a particular range of threshold, jamming is confirmed. To counteract the effects of detected jamming, the affected link is excluded from the route, and an alternative route is used.

In a research work carried out by [6], a jamming detection based on location checks and PDR (packet delivery ratio) was proposed. The authors justified the use of these two measurement methods, arguing that relying on a a single method would not efficiently detect the presence of jammers. A low PDR value indicates jamming, but other factors can also cause a low PDR. Therefore, consistency checks must be adopted to ascertain whether a low PDR value is due to jamming. A high signal strength corresponds to a high PDR, while a low signal strength results in a low PDR. However, a low PDR does not always imply low signal strength. Consequently, whenever the PDR is high and the signal strength is low, a check must be performed on the neighbouring nodes' PDR values .

[7] introduced a centralized jamming detection scheme based on the computation of a jamming index using signal-to-noise ratio (SNR) and packets dropped per terminal PDPT values. PDPT measures the number of packets dropped in a single terminal. Calculating the jamming index is followed by a check to confirm the presence of jamming. The base station collects data such as the number of dropped packets, the number of received packets by the node, and signal strength through a detection algorithm. After these data are collected, the base station calculates the PDPT and SNR to determine the presence of a jammer.

A fuzzy interference system uses PDPT and SNR values to detect jammers. As [8] pointed out, the jammer detection method involves a three-step method: (1) regardless of the PDPT level, if the SNR is low, the probability of jamming is high; (2) the probability of jamming depends on PDPT when the SNR has medium values; (3) when the SNR has high values, probability of jamming will be one level lower than the PDPT.

[9] proposed various techniques for detecting and classifying jamming, especially in 802.11b cellular networks. These techniques relied on packet delivery ratio (PDR), camer sensing time (CST), and signal strength (SS) to detect jamming signal. They investigated the correlation between SS variance, PDR, and the received signal's pulse width. The proposed model successfully differentiated between the jammed regions caused by various jamming attacks.

II. MATERIALS AND METHOD

A. Materials

The materials utilized in this research work included a personal computer (PC) installed with Matlab used in running simulations and a mobile station.

B. Mitigating Jamming Using Tunable Notch Filter

Figure 2 presents a block diagram used for jamming mitigation. It comprises of five different blocks; the chirp block, the barrage jammer block, the sum or adder block, the variable bandwidth IIR notch band stop (notch) filter block, and the spectrum analyzer block.

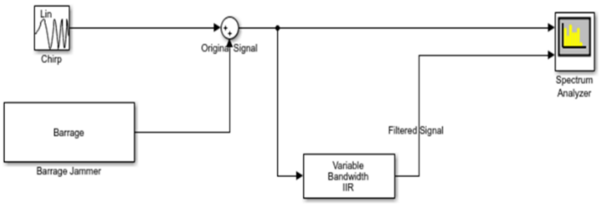

Figure 2: A Block Diagram for Mitigating Jamming Effect

C. Jammed Area Mapping (JAM) Protocol

Jammed area mapping is a method used to detect and mitigate jamming in wireless communication. It works by mapping the specific area of the network affected by jamming, allowing packets to be routed within the affected area.

The jammed area mapping protocol can complete the mapping process within one to five seconds [10]. This technique involves setting a threshold, below which jamming is considered detected, if a node's channel utility falls below the specified value. For example, if the threshold is set at 15, and the node's channel utility is less than 15, then jamming is detected. At this point, a JAMMED message is sent to the neighbouring nodes, which initiate a countermeasure by creating a group that has its identity (ID) and direction vector pointing toward the direction of the jammed nodes. However, this technique did not achieve optimal convergence in sparse networks compared with moderately connected networks. The mapping service area is illustrated in figure 3 [11].

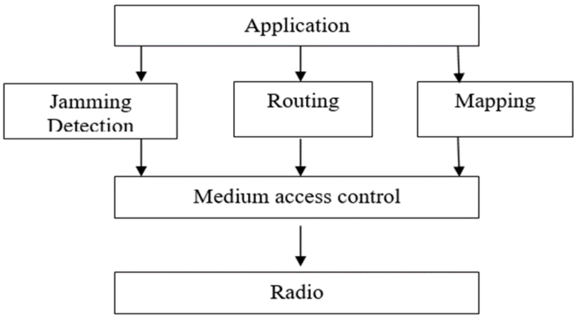

Figure. 3: Mapping Service Architectural Diagram

D. Notch Filter

In this section, a tunable notch IIR filter is described. A notch filter is a special kind of bandstop filter designed to be highly selective and with a high Q-factor, capable of rejecting undesirable frequencies. This is often the case when inductive loads, such as ballast lighting or motors induce electrical noise into a circuit. A well-designed notch filter can reduce or eliminate this type of noise or interference. Usually, a notch filter has a deep and narrow stopband around its centre frequency. The selectivity of the Q describes the notch filter's width.

The most common type of notch filter is the twin T-design, which consists of three capacitors and three resistors arranged in two sections (upper and lower sections) that resemble the letter T. The upper T configuration includes two resistors and one capacitor, forming the lowpass section of the notch filter. The lower T arrangement, on the other hand, consists of two capacitors and a single resistor, which together creating the highpass section of the notch filter. The basic notch filter is depicted in figure 4. If the frequency of the notch filter is denoted by f_n, and R and C represent the resistor and capacitor, the relationship between the resistor, the capacitor and the notch frequency is given by:

$$f_n = \frac{1}{4\pi CR} \tag{1}$$

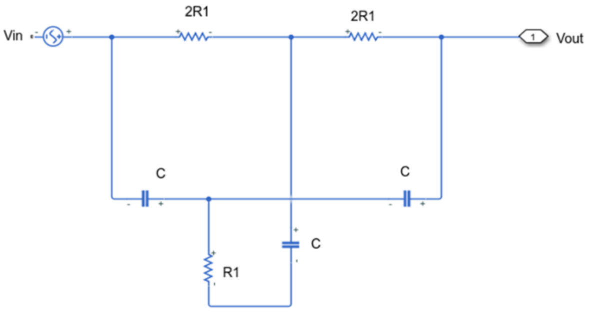

Figure. 4: Basic Notch Filter Circuit

However, this basic notch filter has some significant drawbacks. First, the peak value of the output voltage below the frequency of the notch is less than the peak value of the output voltage above the frequency. This occurs because the two resistors forming the low pass section of the notch filter circuit have losses greater than the capacitive reactances of the capacitors in the high pass section of the notch filter. Second, the Q value is fixed at 0.25 for this type of notch filter circuit. This is due to the reactances and resistances of the two-series capacitors and two-series resistors are equal at the frequency of the notch.

To overcome these limitations, positive feedback is introduced. In this arrangement, the junction of R and C in the highpass section is connected to a voltage-divider network. The voltage divider ratio sets the amount of the feedback signal, which in turn determines the value of the Q, and consequently, the depth of the notch. The feedback fraction, denoted by the letter q is given by [12]-[14]:

$$q = 1 - \left(\frac{1}{4Q}\right) \tag{2}$$

Also,

$$q = \frac{R_2}{R_2 + R_3} \tag{3}$$

Suppose a notch filter is a centre frequency of 1 $k\Omega$ and a bandwidth of 100 Hertz. Using a capacitor value of 0.1 μF, this notch filter can be designed as follows:
Using equation (1),

$$R = \frac{1}{4\pi \times 1000 \times 0.1 \times 10^{-6}} = 397 \cong 400\Omega$$

The q value is given by [13]:

$$Q = \frac{f_n}{B_w} \tag{4}$$

$$Q = \frac{1000}{100} = 10$$

From equation (2),

$$q = 1 - \frac{1}{4 \times 10} = 0.975$$

To determine the values of the resistors forming the voltage divider network, let R₂ be 10 k Ω. Then, from equation (3):

$$0.975 = \frac{10 \times 10^3}{10 \times 10^3 + R_3}$$
$$R_3 = 130\Omega$$

The notch depth in decibels is given by [15]:

$$fn = 20\log(\frac{1}{Q}) \qquad (5)$$

Therefore, $fn(dB) = 20\log(0.1) = -20dB$

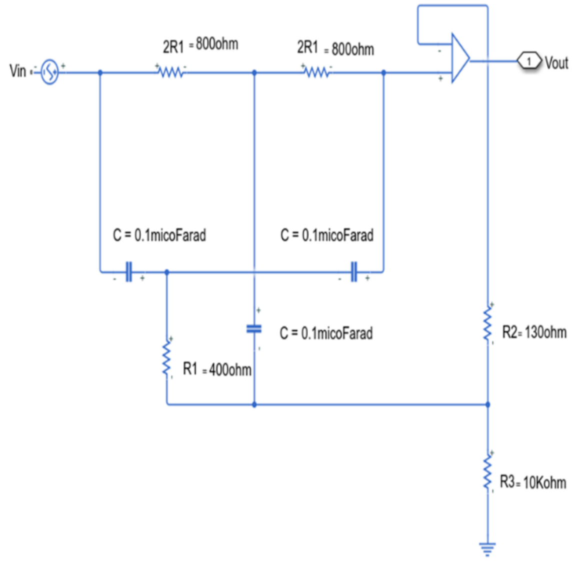

Figure. 5: A Notch Filter Op-Amp and Voltage Divider Network

E. Effect of Jamming on Signal

When a signal is jammed, data or information becomes distorted. The extent of this distortion can be analyzed using the signal-to-noise ratio (SNR) and signal-to-jamming noise ratio (SJNR). If the variance of the jammer, which acts as a deliberate noise source, is denoted by δ^2, then the signal-to-noise ratio can be given by [16]. Figure 6 shows the effects of jamming on the SNR and SJNR of the system. The SJNR is expressed using equation (6). Figure 6 shows the effect of jamming on the signal.

(5)

$$SJNR = \frac{P_S}{P_J} = \frac{1}{\delta^2} \qquad (6)$$

where Ps is the transmitted signal power and P_J is the jammer power

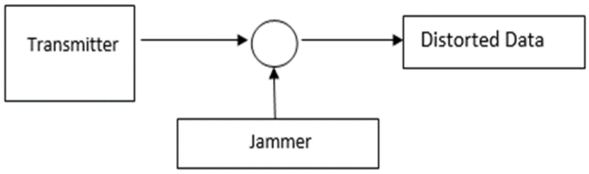

Figure. 6: Effect of Jamming on Signal

The signal-to-jammer-noise ratio can be calculated using equation (7) [15]-[20].

$$SJNR = log\left(\frac{1}{SNR} + \alpha^2\right) \qquad (7)$$

Where α^2 is the interference power and it is equal to the inverse of signal to jammer ratio.

$$\alpha^2 = \frac{1}{SJR} \qquad (8)$$

Substituting equation (8) into equation (9).

$$SJNR = log\left(\frac{1}{SNR} + \frac{1}{SJR}\right) \qquad (9)$$

A plot of SJNR against SJR for different values of SNR reveals the effects of jamming on the system.

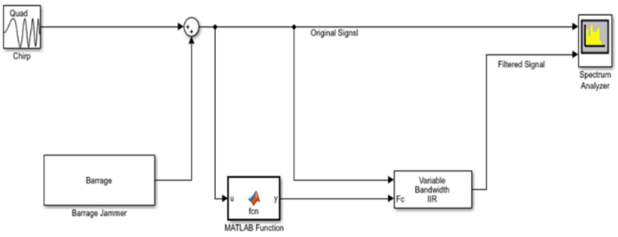

Figure. 7: Simulation Arrangement for Filtering Jamming Signal

Figure 7 shows the block diagram of the notch filtering. In the block diagram, a Matlab function block is included. By allowing the bandstop filter to have a center frequency that can be specified by an input port, as shown in figure 7, it becomes tunable, enabling easy parameter adjustments during simulation.

III. RESULTS AND DISCUSSION

Figure 8 shows the plot of Signal to Jammer Noise Ratio against Signal to Jammer Ratio for different values of Signal toNoise Ratio. The signal to jammer noise ratio nearly approached the value of the signal-to-noise ratio of 20dB as the value of the signal-to-jammer ratio increased. The same was true when the signal-to-noise ratio was 10dB. In other words, as the signal-to-jammer ratio grew bigger, the signal to jammer plus noise ratio almost approached the value of signal to noise ratio 10dB. Evidently, jamming adversely affects communication systems.

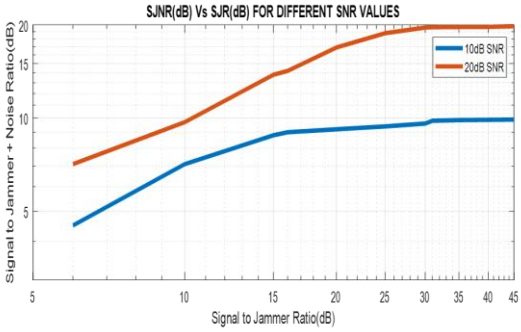

Figure 8: A Plot of Signal to Jammer Noise Ratio against Signal to Jammer Ratio for Different Values of Signal to Noise Ratio

Figure 9 reveals the performance of the system when the signal-to-noise ratio is plotted against jammer to signal-noise ratio, both with and without a notch filter. Without a notch filter, an increase in the value of jammer to signal-noise ratio significantly affected the value of the signal-to-noise ratio. For example, when an increase from a jammer-to-signal-noise ratio of -20dB to 0dB, the signal-to-noise ratio decreased significantly from about 20dB to approximately 0.1dB. However, when a notch filter was used, this decrease was mitigated, indicating that as the jammer-to-signal noise ratio increased, the depth of the notch deepened.

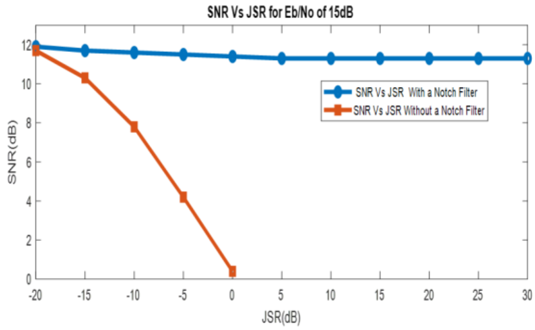

Figure 9: A Graph of Signal-to-Noise Ratio against Jammer-to-Signal Ratio when Eb/No is 15dB with and without a Notch Filter.

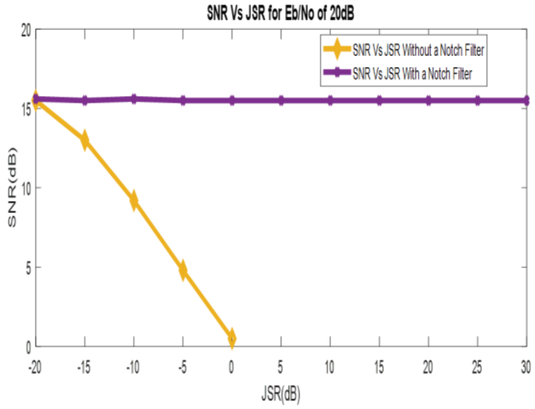

Figure 10: A Graph of Signal-to-Noise Ratio against Jammer-to-Signal Ratio when Eb/No is 20dB with and without a Notch Filter.

Figure 10 shows the system performance when the signal-to-noise ratio is plotted against the jammer to signal-noise ratio for an Eb/No of 20dB, both with and without a notch filter. Unlike Figure 9, where the value of the signal-to-noise ratio was about 12dB for a jammer-to-signal ratio of -20dB when Eb/No was 15dB, for the same value of jammer to signal ratio (-20dB) when Eb/No value of 20dB, the signal to noise ratio value exceeded 15dB. Again, without a notch filter, increasing the value of the jammer-to-signal-noise ratio significantly decreased the value of the signal-to-noise ratio. However, when a notch filter was used, this substantial decrease was mitigated, indicating that as the jammer-to-signal noise ratio increased, the depth of the notch deepened.

Figure 11 presents a bandstop filter used for filtering a signal. The lower and upper passband frequencies are 150Hz and 250Hz respectively with a bandwidth of 100Hz. As can be observed, the stopband of the filter has a large bandwidth and cannot effectively filter off signals. This is a characteristic of a pure bandstop filter, not a notch filter, which is expected to have a very narrow bandwidth. The top figure in Figure 11 clearly shows the filtered signal in the middle of the spectrum.

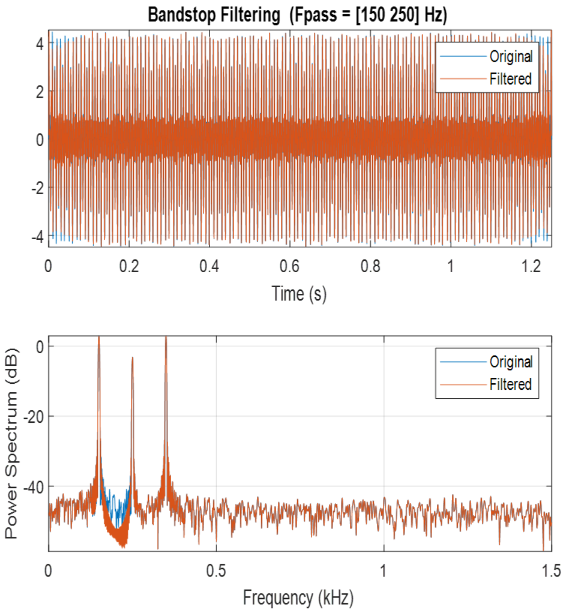

Figure 11: Filtering of Signal using Ordinary Bandstop Filter

As mentioned earlier, a notch filter is a specialized type of a bandstop filter designed to have a narrower bandwidth than a standard bandstop filter. As shown in Figure 12, the bandwidth of the filter is 20Hz, with lower and upper passband frequencies at 1.35kHz and 1.37kHz respectively. Using a sampling frequency of 2.8kHz, the notch filter effectively filtered out signals below and above 1.35kHz and 1.37kHz, including an unwanted jamming signal.

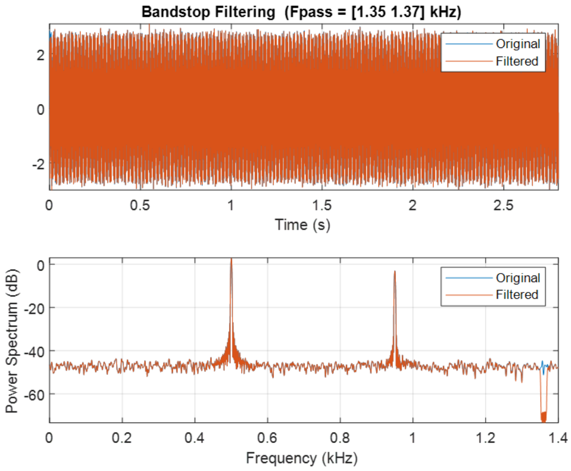

Figure 12: Filtering of Signal using a Notch Filter

In Figure 13, the bandwidth of the filter is 30Hz, with lower and upper passband frequencies at 800Hz and 830Hz respectively. Using a sampling frequency of 2.8kHz, the notch filter effectively filtered out signals below and above the lower and upper passband frequencies, including an undesirable jamming signal.

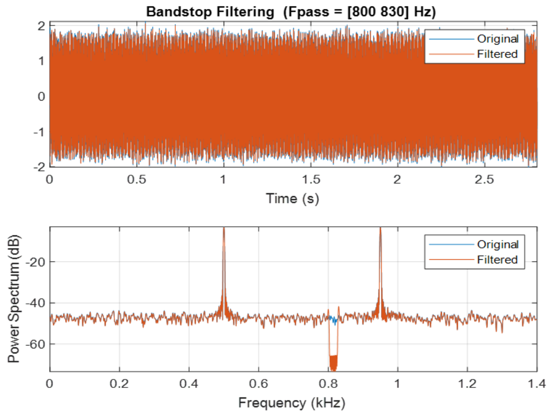

Figure 13: Filtering of Signal using a Notch Filter

Figures 14 and 15 show the plot of the magnitude and phase responses of the notch filter for filtering out the jamming signal that distorts the originally transmitted signal. Figure 14 presents the phase response before reaching the jamming frequency of 100 Hz, while Figure 15 shows the magnitude and phase responses as the frequency of the notch decreases.

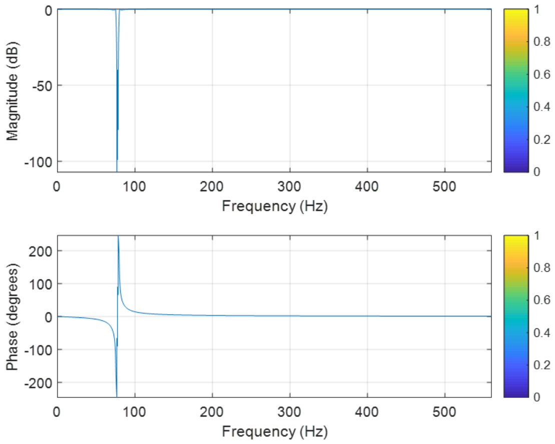

Figure 14: Magnitude and Phase Responses of the Notch Filter

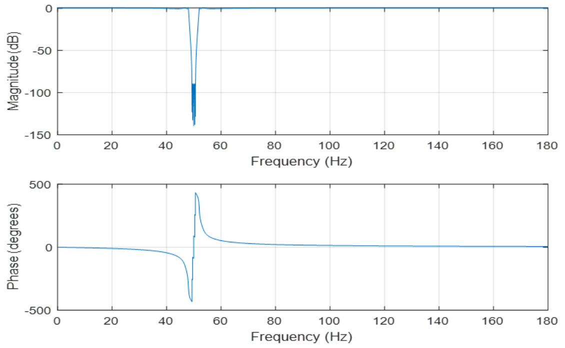

Figure 15: Magnitude and Phase Responses of the Notch Filter

IV. CONCLUSION AND RECOMMENDATION

A. Conclusion

The focus of this research was to enhance jamming protection using a tunable notch filter. A comprehensive evaluation of various jamming mitigation techniques was carried out, along with designing a notch filter for jamming mitigation and examining the effects of jamming on the signal in communication systems. The result showed that the use of notch a filter for jamming protection increased the signal-to-noise ratio, leading to the conclusion that a tunable notch filter can effectively improve jamming protection in communication systems.

Furthermore, the result revealed that a notch filter with narrower bandwidth more effectively filters out unwanted signals, including the jamming signals compared to a standard bandstop filter with a larger bandwidth. Therefore, it can be concluded that designing a notch filter with a narrower bandwidth for effective jamming protection improvement ensures that the jamming signal will be minimized. The notch filter places a deep null at the frequency of the jamming signal, thereby preventing the jamming signal from distorting communication.

B. Recommendation

In view of the results presented in Section 3, the following recommendations are made. First, since the notch filter eliminates a range of frequencies, a narrower bandwidth notch filter should always be used to effectively remove jamming signals and improve communication without adversely affecting useful information. Second, a cascaded number of individual notch filters should be adopted to track different notches embedded in a jamming signal and mitigate the effects.

REFERENCES

[1] B. Danide, O. Cillian, and F.G Joaquim "Fast and Flexible: Tracking and Mitigating a Jamming Signal with an Adaptive Notch Filter 2014.

[2] S. Gollakota, and D. Katabi "Jamming Oneself for Secure Wireless Communication". Tech. Rep. Massachusetts Institute of Technology, 2010.

[3] K. Grover, A. Lim, and Q. Yang, "Jamming and Anti-jamming Techniques in Wireless Network: A Survey", International Journal of Adhoc and Ubiquitous Computing, vol. 17, no. 4, pp. 197 – 215, 2014.

[4] S. Hussian and N.A. Saqib, "Protocol-aware Shot-noise Based Radio Frequency Jamming Method in 802.11 Networks, in Proceedings of the 8th International Conference on Wireless and Optical communications Networks, Paris, France, pp. 1 – 6, 2010.

[5] F. Jack, "Tunable and Non-tunable Filters, Video examples Files". Retrieved from https://github.com/mathworks/filter-tunability-examples/releases/tag/v1.0 Retrieved on January 5, 2022.

[6] S.B. Jerome, "Broadcasting on the Short Waves, 1945 to Today". Mc Farland. ISBN 978-0-7864-5198-2. (46). 2008.

[7] Q. Lv, and A.H. Qin, "A novel Algorithm for Adaptive Notch Filter to Detect and Mitigate the CWI for GNSS Receivers". In Proceedings of the IEEF 3rd International Conference on Signal and Image processing (ICSIP), Shenzhen, China, 444 – 451, 2018.

[8] S. Misra, R. Singh, and S.V.R. Mohan, "Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy Interference System. Pp. 3444 – 3479, 2010.

[9] R. Muraleedharan and L.A. Osadeiw, "Jamming Attach Detection and Counter-measures in Wireless Sensor Network Using Ant System". International Society for Optical Engineering, vol. 6248 no. 4, 6240G 2016.

[10] S. Nadeem, N.A. Saqib and Z. Muhammed "Detection of Jamming Attaches in 802.11b Wireless Networks. EURASIP Journal on Wireless Communication and Networking, pp. 1 – 18, 2013.

[11] D. Nick, An Introduction to Filters. 2017. Retrieved from https://www.allaboutcircuits.com/technical-articles/an-introduction-to-filters/.

[12] O. Opeyemi, S.A. Attahiru, and P.H. Gerhard "A Statistical Approach to Detect Jamming Attaches in Wireless Sensor Networks". Doi:10.3390/518061691. 2018.

[13] J. Raasakka, and M. Orejas, "Analysis of Notch Filtering Methods for Narrow-band Interference Mitigation. In proceeProceedingse 2014 IEEE/ION Position, Location and Navigation Symposium Monterey, CA, USA, pp. 1282 – 1292, 2014.

[14] N. Song, R.C. De Lamare, M. Haardt, and M. Wolf "Adaptively Widely Linear Reduced – Rank Interference Suppression Based on the Multistage Wiener Filter. IEEE Trans. Signal Process, 60, 4003 – 4016, 2012.

[15] M. Strasser, B. Danev and S. Capkun, "Detection of Reactive Jamming in Sensor Networks". ACM Transactions on Sensor Networks vol. 7, no. 2, pp. 1 – 29, 2010.

[16] R.K. Tony "Lessons in Electric Circuits" 6th ed, 2007.

[17] US Department of Defence "Tunable Band-stop Filters for Suppression of Co-site Interference and Jamming Sources". Retrieved from https//sbir.gov/node/374025-on-14th-Dec.-2021.

[18] A.D. Wood, A. Stankovic and S.H. Son, "A Jammed-Area Mapping service for Sensor Networks", 2016. Retrieved from cupdf.com/document/jam-a-jammed-area-mapping-service-for-sensor-networks.

[19] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks". In Proceedings of the 6th ACM International Symposium on Mobile Adhoc Networking and Computing, pp. 46 – 57, 2015.

[20] F. Zhibin, R. Guochun, C. Jin, C. Chaohui, Y. Xiaoqin, L. Yijie and X. Kun, "An Anti-Jamming Hierarchical Optimization Approach in relay Communication System via Stackelberg Game". Applied Science. doi:10.3390/9pp9163348, 2019.