KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS

Electrical Engineering Department

EE573 – DIGITAL COMMUNICATIONS II

Term Paper

Modified BlueFMCW: Frequency Hopping Spread Spectrum for joint Communication and Sensing Radar for Mitigation of Interference and Spoofing

Name

Name: Mahmoud Yassin Mahmoud

ID: g202113650

Submitted to

Dr. Wessam Mesbah

Table of Contents

Motivation

By detecting surrounding obstacles, automotive sensor systems are regarded as a key technology in autonomous driving. Radars, as an important component of the sensing system, detect obstacles in the long range, as opposed to cameras and ultrasonic sensors, which detect obstacles in the short range. Radar techniques that use radio frequency (RF) have gained popularity, owing to their ability to detect objects in a variety of weather conditions. Among these, frequency-modulated continuous-wave (FMCW) radar detects both the range and speed of objects, which piques the radar's interest.

The growing popularity of automotive radar creates an opportunity for joint radar and communication systems, which are expected to supplement legacy vehicular communication systems like dedicated short-range communication (DSRC) to support rapidly increasing traffic demands due to the upcoming deployment of connected vehicles.

While a joint automotive radar and communication system could be implemented using either time-sharing between both functions or a joint waveform for dual use of radar and communication, the current work focuses on the latter, which ensures continuous radar functionality.

In this paper, we present Modified Blue FMWC, a joint radar and communication spread spectrum system. The system is based on FSK modulating the widely used FMCW waveform by varying the starting frequency of each component chirp and hopping between various frequency ranges.

Problem Statement

Security is an important factor to consider when designing an automotive radar. There are two types of automotive radar attacks.

First, future jamming attacks have the potential to cause major collisions. Attackers who use jamming intentionally send out a high-power radio signal to confuse or overwhelm the radar receiver. By saturating the radar with noise, jamming attacks render it inoperable. However, in a highly mobile environment, the damage from a jamming attack can be reduced, making it difficult for an aggressor to target vehicles [6].

Second, automotive radars are known to be vulnerable to spoofing, replicating, and retransmitting radar transmit signals to provide false information to the radar and corrupt received data.

Related Work

Wild Thorsten, Volker Braun, and Harish Viswanathan[1] showed in their work the key drivers for embedded sensing capabilities into cellular mobile networks, which are illustrated in Figure 1.

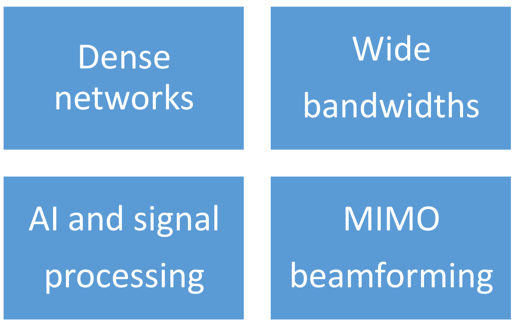

Figure 1. The main drivers for joint communications and sensing in mobile networks.

Wang, Chang-Heng, and Onur Altintas[2] demonstrated a cooperative radar and communication system based on commercially available FMCW radar in their study. The authors offer a hybrid automobile radar and communication system that uses FSK modulation on the FMCW waveform, which is often used in automotive radars. The concept is easily implementable on most commercial off-the-shelf automobile radars, and a prototype based on the TI AWR1642BOOST vehicle radar has been developed.

Alloulah Mohammed, and Howard Huang[3], proposed a design for a future mm-wave network that will provide sensing capabilities in addition to standard data communications. they show that spatial multiplexing will be possible due to the intrinsic beamformed nature of mm-wave systems. they also show that incorporating robust radar-sensing techniques into a communication protocol is feasible and that the accompanying issues, including radio resource management, processing complexity, and inference, are within the capabilities of existing technology.

Sinha, Priyanka, Ismail Güvenç, and M. Cenk Gürsoy's work utilizes existing terrestrial radio frequency (RF) networks for drone passive sensing[4]. They construct an analytical framework that establishes basic limitations on the network-wide probability for drone detection.

Moon, Thomas, Jounsup Park, and Seungmo Kim work presents BlueFMCW, a novel frequency-modulated continuous-wave (FMCW) radar scheme that mitigates both interference and spoofing signals. BlueFMCW hops frequencies at random to avoid interference and spoofing signals. their phase alignment algorithm can remove the phase discontinuity while combining the beat signals from the randomly-hopped chirps, ensuring that radar resolution is not compromised. The simulation results show that BlueFMCW can effectively mitigate interference and spoofing signals in a variety of scenarios without sacrificing resolution.

Background:

A. Basic FMCW Waveform:

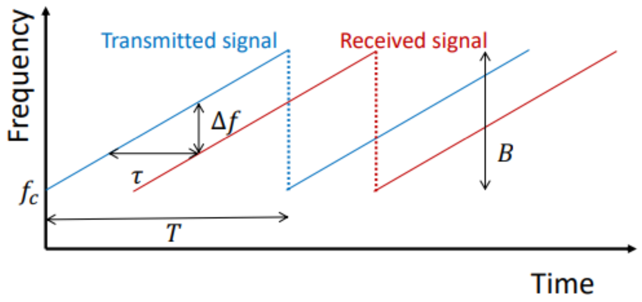

Figure 2. Using FMCW to measure distances. The illustration depicts the transmitted FMCW signal (blue) and its reflection (red).

The blue line in Figure 2 depicts FMCW radar continuously transmitting periodic pulses whose frequency sweeps linearly in time. The transmitted signal is defined mathematically as:

$$s_t(t) = \exp(j2\pi(f_c t + \frac{\alpha}{2}t^2)) \qquad (1)$$

where fc and α are the FMCW chirp's starting frequency and slope, respectively. The reflected signal is a time-delayed version of the transmitted signal that arrives after bouncing off a reflector, as shown in Figure 2.

The time-of-flight (TOF, τ) is the amount of time it takes for the transmitted signal to travel the round-trip distance 2d from the radar to the reflector and back to the radar. When there are multiple reflectors, the received signal is written as:

$$x(t) = \breve{s}_r(t) \cdot s_t(t)^* \; = \sum_i A_i \exp(j2\pi(\alpha\tau_i t + f_c\tau - \frac{\alpha}{2}\tau_i^2)).$$

Because the frequency ατ of the beat signal is where α is a known parameter, we can extract a distance profile of multiple reflectors. As a result, we can apply FFT to the beat signal and detect objects by locating the peaks.

B. Basic BlueFMCW:[5]

Instead of sending the entire chirping signal from low to high frequency, BlueFMCW performs a random frequency hop in the middle of the chirp signal, as seen in Figure 3. (b). The frequency gap with the aggressor signal will be randomized while the TOF of the reflected signals stays constant. As a result, the false beat frequency does not remain in the same FFT bin as seen in Figure 3. (d). In other words, the energy of the enemy signal will be distributed at random over several FFT bins, resulting in substantially smaller peaks in the spectrum.

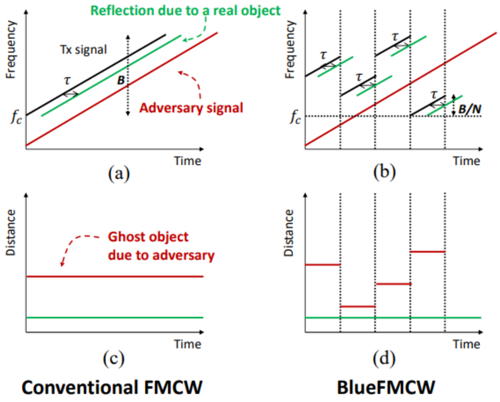

Figure 3. Tx signal and beat signal of (a)(c) conventional FMCW vs (b)(d) BlueFMCW .

In next part, we will first go over how to achieve random frequency hopping in FMCW. The difficulties in reconstructing the beat signal are then addressed.

Consider a standard FMCW chirp signal, which is a linear frequency modulation signal with a beginning frequency of fc and a duration of T. BlueFMCW generates a sequence of frequency-hopping chirps by first splitting the standard FMCW signal into N equal sub-intervals and then randomly permuting the sub-chirps.

The beat frequency of the real object, on the other hand, is not hashed and remains constant during T. This is due to the fact that the beat frequency of a genuine object is determined only by the TOF, independent of the initial frequency. BlueFMCW takes use of this to reduce the enemy signal while maintaining the same detection capacity on actual objects.

A random permutation is defined as $\sigma : F \to F$, where F is a finite set having the indexes 1, 2,..., N. The two-line notation of σ is as follows:

$$\begin{pmatrix} 1 & 2 & \dots & N \\ \sigma(1) & \sigma(2) & \dots & \sigma(N) \end{pmatrix}$$

Figure 4 (a) shows an example of N = 4 BlueFMCW sub chirps. In this example, the typical FMCW's first sub-chirp is permuted to the third slot, the second sub-chirp to the second slot, the third sub-chirp to the first slot, and the fourth sub-chirp to the third slot.

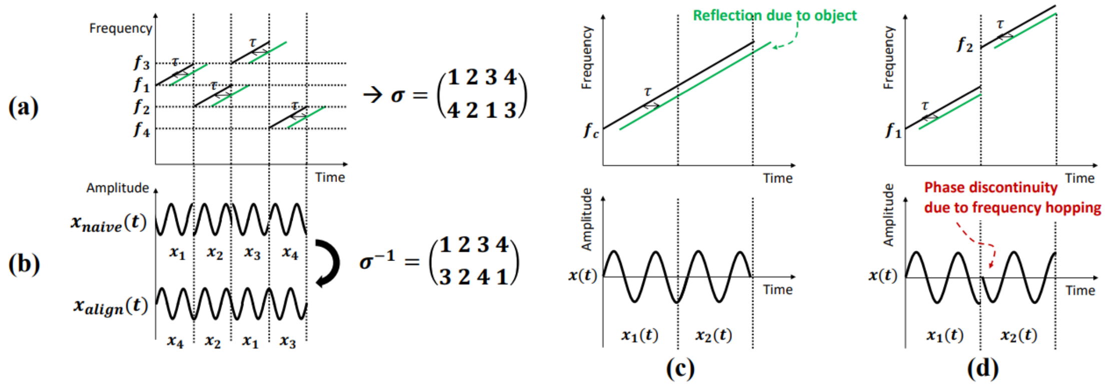

Figure 4. example of N = 4 BlueFMCW

A sub-distance chirp's resolution, on the other hand, is deteriorated by N since its bandwidth is lowered by B/N. the distance resolution achieved by a single sub-chirp is (cN/2B).

Concatenating the beat signals of all sub-chirps in time-order is a naïve effort to tackle the resolution problem. However, this will result in phase discontinuity. The fourth beat signal is permuted to the first time-slot by the inverse permutation σ^{-1}, and so on (Figure 4 (b)).

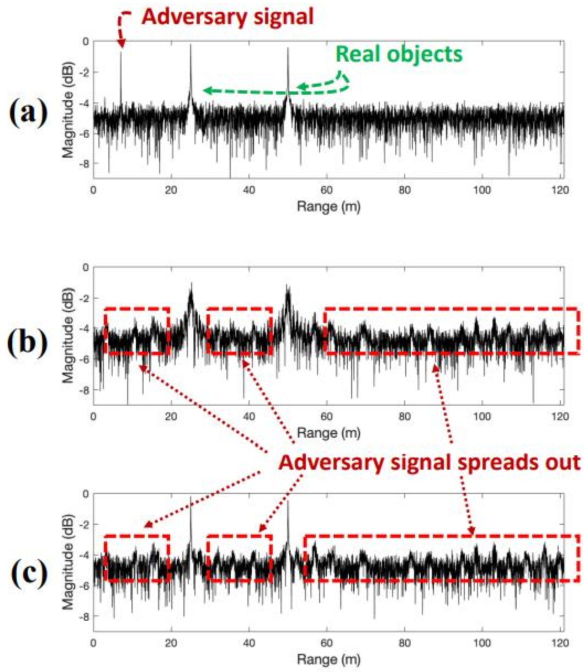

Figure 5. Beat spectrum (distance profile) of (a) conventional FMCW, (b) BlueFMCW without phase alignment, and (c) BlueFMCW with phase alignment.

Proposed Scheme for Modified BlueFMCW:

In the modified Blue FMWC, we apply two types of frequency-hopped (FH) spread spectrum:

(1) Blue FMWC within Ts duration for the radar system.

(2) frequency-hopped spread spectrum communication system (FH-CS)

It's noteworthy that the code that is being used for hoping for the two types are different from each other, where in the blue FMWC the code randomly permuting the sub-chirps and in the SFH-CS the other code is being made pseudo randomly according to the output from a PN generator. That was made because the need for the phase continuity in the chirp. Figure 6 shows the main idea of the proposed system.

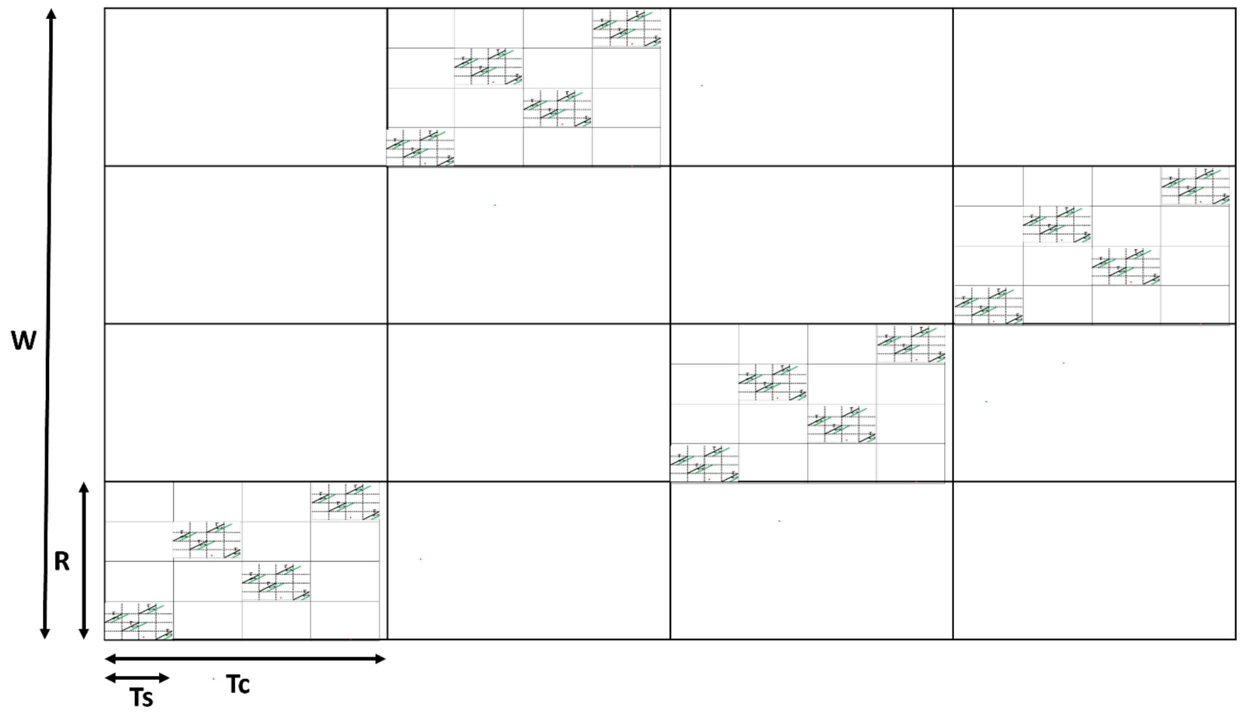

Figure 6. 4-Ary Modified Blue FMWC for joint communication and sensing

Mathematical Analysis Results:

Following the same procedure of Proakis, John G., and Masoud Salehi in their book[7] we can excute our analysis as following:

If we supposed that our data will be encoded using binary linear coding (n_1, k), and to simplify the analysis we will suppose our modulation is BFSK and wideband jamming.

The n_2 hops per coded bit can be considered as a repetition code where also n_2 equals N which is the number of sub-chirps in the FMWC. Then the new code will be (n_1*N, k).

$\therefore R_c$ (code rate) = $\left(\frac{k}{n1*N}\right)$, $\therefore$w (weight distribution) = $N*w_m$

Where w_m is the weight distribution for binary linear code (n_1, k).

$\therefore R_c*w=\left(\frac{k}{n1*N}\right)*N*w_m=\frac{k}{n1}*w_m=R_{c1}*w_m$

From here we can make an observation that the number of hops per chirp(number of sub-chirps in Ts) would not effect the coding gain, but it will have an effect in the distance resolution that can be achieved by a single sub-chirp which will be $\frac{c.N}{2B}$.

For the case of fast hopping for radar chirps we can use an appropriate combing technique for the radar signal which be the output of the matched filter for N sub-chirps, the error rate performance of FH signal is:

$P_2 = \frac{1}{2^{2NWm-1}} * \exp(-[\gamma_b \cdot Rc_1 \cdot \omega_m]) * \sum_{i=0}^{(N\cdot\omega_m-1)} k_i \cdot \left[\frac{1}{2}\gamma_b \cdot R_{C_I} \cdot \omega_m\right]^i$

Where $\gamma_b = \frac{\varepsilon_b}{J_o} = L \cdot \gamma_C$, γ_C is the SNR per sub-chirp.

$$k_i = \frac{1}{i!} \cdot \sum_{r=0}^{[N\cdot w_m-1-i]} \binom{2N\omega_m - 1}{r}$$

For the case of soft-decision decoding of the square-law demodulation FSK signal, the probability of a codeword error is upper-bounded as:

$$P_e \leq \sum_{m=2}^{n} P_2(m)$$

It is noteworthy to mention that $P_2(m)$ is the probability error in deciding between the m^th codeword and all-zero codeword when the all-zero codeword has been transmitted.

For the case of hard-decision decoding:

$P_2 = \frac{1}{2^{2N-1}} * \exp(-[\gamma_b \cdot Rc_1 \cdot \omega_m]) * \sum_{i=0}^{(N-1)} k_i \cdot \left[\frac{1}{2}\gamma_b \cdot R_{C_I} \cdot \omega_m\right]^i$

$$k_i = \frac{1}{i!} \cdot \sum_{r=0}^{[N-1-i]} \binom{2N - 1}{r}$$

We can easily upper-bounded the probability of error using the Chernov bound as:

$$p_e \leq \sum_{m=2}^{M} [4p(1-p)]^{\omega_{m/2}}$$

It is important also to mention that the performance of the fast FH system in broadband interference is degraded compared to the slow FH by an amount equals to the noncoherent combining loss of the signals received from the N hops.

So from the previous analysis we can conclude the effect of N number of sub-chirps on our system as the following:

- increasing N will increase the number of hops per chirp signal which will increase the immunity of the system to jamming and spoofing.
- On the other hand, that will decrease the distance resolution per sub-chirp.
- Not only the radar system will be affected from that, but also that would affect the communication system as follows:
    (1) We showed that increasing the N would not affect the coding gain as we interpret it as repetition code.
    (2) But it would degrade the system performance due to the combination loss.

Simulation Results

The first simulation employs an FHSS communication system with FSK and noncoherent detecting receivers. We can demonstrate the impact of FHSS against partial band jamming signals by supplying input values of 1 (with jamming) and 0 (without jamming).

Number of users	m = 1
Spreading factor (number of FSK bands)	L = 8
Number of hops per symbol per bit	Lh= l
Modulation	BFSK
Detection	Noncoherent
Partial band jamming	1 fixed FSK band

Table2. Simulation Parameters for FH.

Table 2 shows the FHSS system parameters used in this simulation. When partial band jamming is enabled, jamming blanks out a fixed but randomly chosen FSK channel.

Figure 7 depicts the effect of partial band jamming on the FHSS user under additive white Gaussian channel noise. Without jamming, we can clearly observe that the FHSS performance matches that of the AWGN FSK. Performance visibly increases when partial jamming and L are increased from 4 to 8, and then to 16.

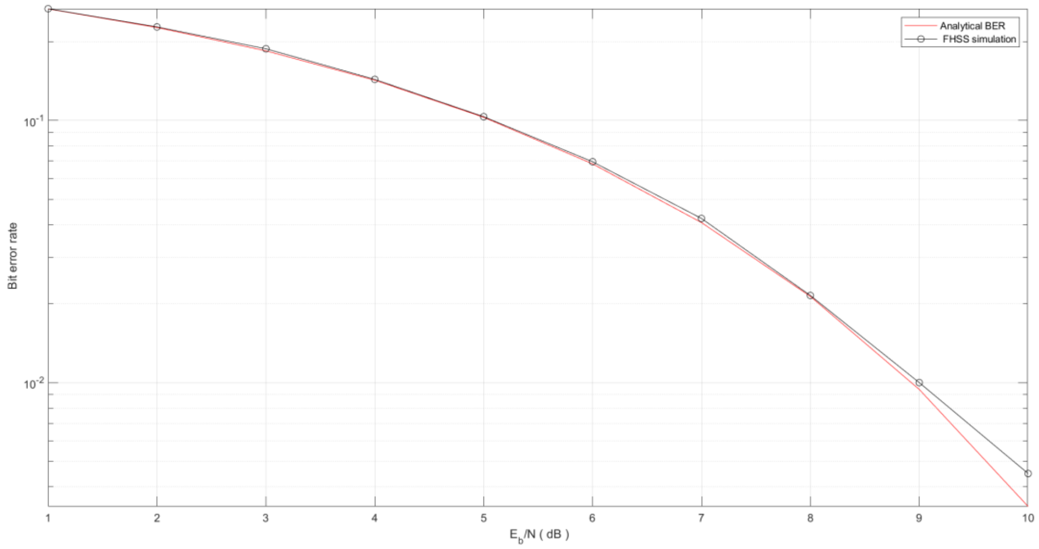

Figure 7.a Performance of FHSS noncoherent detection with no jamming.

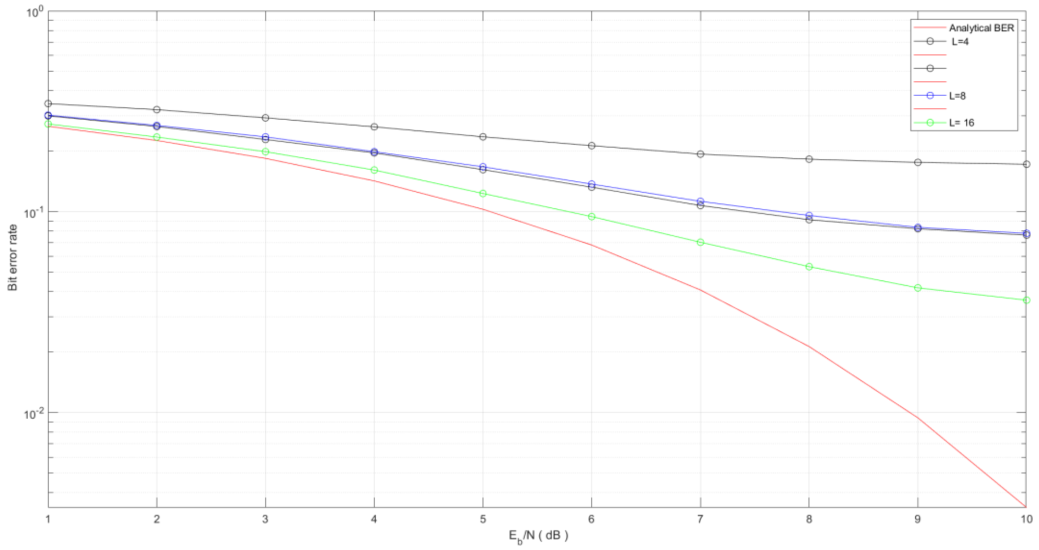

Figure 7.b Performance of FHSS noncoherent detection with partial band jamming.

The second simulation is an FMCW radar that estimates range and Doppler on a moving vehicle using an automotive long-range radar (LRR) model that is utilized for adaptive cruise control (ACC). This type of radar typically operates in the 77 GHz band. The radar system constantly calculates the distance between the vehicle on which it is mounted and the vehicle in front of it, alerting the driver when the two grow too close. Figure 8 depicts the working idea of ACC and table 2 summarize the system parameters.

Figure 8. ACC working idea.

System parameters	Value
Operating frequency (GHz)	77
Maximum target range (m)	200
Range resolution (m)	1
Maximum target speed (km/h)	230
Sweep time (microseconds)	7.33
Sweep bandwidth (MHz)	150
Maximum beat frequency (MHz)	27.3
Sample rate (MHz)	150

Table3. Simulation Parameters for FMCW radar.

A car in front of it is normally the target of an ACC radar. This simulation assumes the target car is 50 meters ahead of the car with the radar, traveling at 96 kilometers per hour along the x-axis. Figure 9 shows the used FMCW signal.

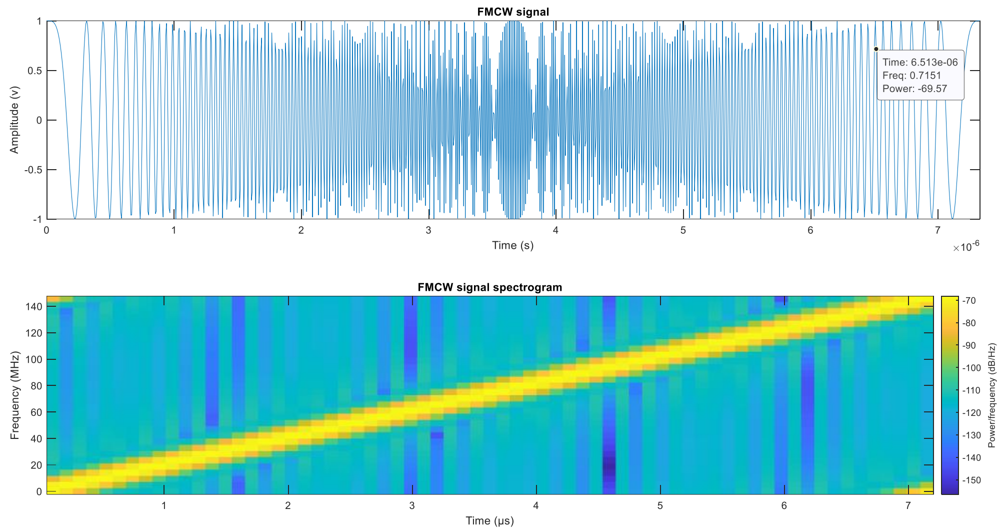

Figure 9. FMWC signal.

Figure 10 demonstrates that, despite the fact that the received signal is wideband (channel 1), sweeping across the whole bandwidth causes the dechirped signal to become narrowband (channel 2).

Figure 11 depicts the range Doppler response, which demonstrates that the automobile in front is somewhat more than 40 m distant and seems nearly motionless. This is predicted given that the car's radial speed relative to the radar is only 4 km/h, or 1.11 m/s.

There are several methods for calculating the target car's range and speed. The root MUSIC technique is used in this simulation to calculate both the beat frequency and the Doppler shift.

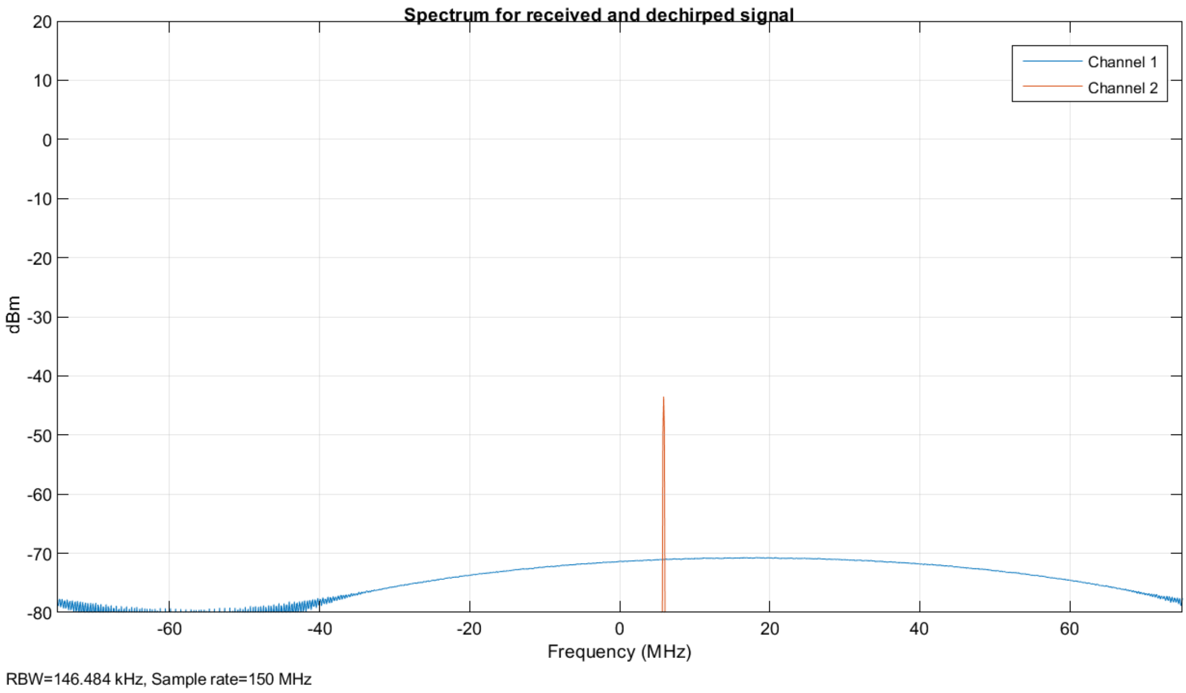

Figure 10. Spectrum for received and dechirped signal.

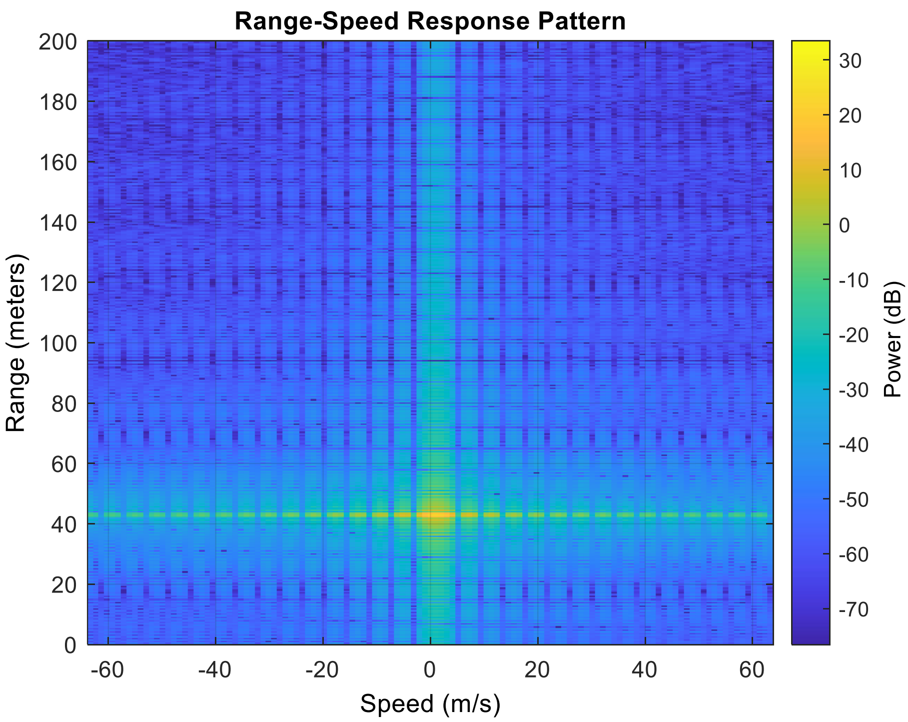

Figure 11. Range-Speed Response Pattern.

Conclusion

In this term paper, I present Modified Blue FMCW, a joint radar and communication spread spectrum system. The system is based on FSK modulating the widely used FMCW waveform by varying the starting frequency of each component chirp and hopping between various frequency ranges. Analysis have been done to show the effect of integrating the communication and radar systems together using spread spectrum on each other. Two simulations have been done, the first one for regular FHSS to show the effect of jamming on the system and how to enhance its performance. the second simulation was to show how FMCW radar works in an automotive adaptive cruise control.

References

1- Wild Thorsten, Volker Braun, and Harish Viswanathan. "Joint design of communication and sensing for beyond 5G and 6G systems." *IEEE Access* 9 (2021): 30845-30857.

2- Wang, Chang-Heng, and Onur Altintas. "A joint radar and communication system based on commercially available FMCW radar." 2018 IEEE Vehicular Networking Conference (VNC). IEEE, 2018.

3- Alloulah, Mohammed, and Howard Huang. "Future millimeter-wave indoor systems: A blueprint for joint communication and sensing." *Computer* 52.7 (2019): 16-24.

4- Sinha, Priyanka, Ismail Güvenç, and M. Cenk Gürsoy. "Fundamental Limits on Detection of UAVs by Existing Terrestrial RF Networks." *IEEE Open Journal of the Communications Society* 2 (2021): 2111-2130.

5- Moon, Thomas, Jounsup Park, and Seungmo Kim. "BlueFMCW: Random frequency hopping radar for mitigation of interference and spoofing." *EURASIP Journal on Advances in Signal Processing* 2022.1 (2022): 1-17.

6- E. Yeh, J. Choi, N. Prelcic, C. Bhat, and R. W. Heath Jr, "Security in automotive radar and vehicular networks," submitted to Microwave Journal, 2016

7- Proakis, John G., and Masoud Salehi. Digital communications. Vol. 4. New York: McGraw-hill, 2014.