

RESEARCH

Open Access



# BlueFMCW: random frequency hopping radar for mitigation of interference and spoofing

Thomas Moon<sup>1\*</sup> , Jounsup Park<sup>2</sup> and Seungmo Kim<sup>3</sup>

\*Correspondence:  
tmoon@illinois.edu

<sup>1</sup> Department of Electrical  
and Computer Engineering,  
University of Illinois at Urbana  
and Champaign, Urbana, USA  
Full list of author information  
is available at the end of the  
article

## Abstract

Radars form a central piece in a variety of emerging applications requiring higher degrees of localization. However, two problems are anticipated as more radars are deployed: viz., (i) inter-radar interference and (ii) security attacks. While many prior proposals have addressed the problems, no work in the radar literature addressed them simultaneously. In this context, we introduce a novel frequency-modulated continuous-wave (FMCW) radar scheme (namely, BlueFMCW) that aims to alleviate the damage from interference and active attacks (e.g., spoofing). The technique designs that the waveform randomly hops across multiple frequencies to dilute the damage at a certain frequency. Moreover, we propose a phase alignment algorithm to remove the phase discontinuity while combining the beat signals from the randomly-hopped chirps. The simulation results show that the proposed technique can efficiently mitigate the interference and spoofing signals in various scenarios without costing its resolution.

**Keywords:** FMCW, Frequency hopping, Inter-radar interference

## 1 Introduction

As the advancement of cyberphysical systems takes the direction of improving contextualization, the significance of knowing the position of a participant in a network has become more important than ever. In fact, a wide variety of emerging applications require precise localization. Examples include simultaneous localization and mapping (SLAM), indoor localization, automotive vehicles, and virtual reality (VR)/augmented reality (AR). Radars are attracting particular interest as a key technology enabling the localization, based on advantages in terms of stability and versatility over other sensor techniques such as camera and lidar.

However, the wide deployment of radars does not come at no cost. One can easily anticipate that the higher density of radars may degrade the detection accuracy mainly due to *inter-radar interference* [1, 2]. In addition, radars may be exposed to a higher chance of getting attacked, which raises a concern on *security*. *Spoofing attack* is known as one of the most likely types of attack [3] owing to its simplicity of execution. An attacker only needs to listen to a signal to spoof and re-generate after any intended

modification [4, 5]. Several prior attempts have appeared to address the issues of interference and spoofing attack. Distinguished from them, this paper proposes a technique resolving the two issues simultaneously.

### 1.1 Related work

There are several prior works on mitigation techniques against mutual interference or attacks on the automotive radars. *Communication-based* techniques such as dual function radar-communication [6, 7] proved effectiveness only against interference signals. Meanwhile, our proposed work provides a countermeasure against intended attack signals as well.

As efforts to combat the radar interference or attacks, techniques such as *beamforming* [8, 9] and *polarization* [10, 11] are also found in the literature.

Further enhancements on the FMCW are found in the latest work such as *adaptive noise cancellation* techniques [12, 13], which improves the signal-to-noise ratio by canceling the noise from the radar interference. However, they did not specify how to distinguish false objects created by the interference or attack, which is the main problem that our work focuses on.

In [14, 15], frequency hopping is utilized to mitigate the FMCW interference. [15] proposes bats-inspired frequency hopping that alters the frequency randomly if the interference is detected. [14] predicts the interfering chirp parameters and alters the chirp hopping sequence to avoid the interference. However, both papers focus on the scenarios when the victim's and aggressor's chips have different signs of slope (one has a positive slope and the other one has a negative slope). When the interfering signal has the opposite slope sign, it causes a less severe consequence, such as degrading the victim's SNR. BlueFMCW mitigates more severe interference that shares the same slope with the victim, which will create a false object on the victim's radar. Furthermore, [14, 15] only assume a single interference signal and optimize the chirp parameters based on the assumption. In contrast, BlueFMCW is robust against the presence of multiple interferences or attacks.

*Multiband chirp synthesis (MCS)* is a technique to stitch together the returns from several disjoint frequency bands to combine the bandwidths [16, 17]. While MCS offers increasing range resolution, it extrapolates the signal by fitting the chosen models. BlueFMCW does not use extrapolation, and therefore, it does not increase the range resolution more than its total bandwidth. However, BlueFMCW stitches the sub-chirps by aligning the phases and does not lose the resolution by random frequency hopping.

*Phase-coded FMCW (PC-FMCW)* [18] is proposed to mitigate interference and enable joint sensing and communication. While the phase coding enables carrying information and mitigating the interference simultaneously, it causes phase discontinuity on the waveforms. The realization of such waveforms in hardware is challenging due to the instantaneous phase change needing costly equipment; thus, it does not apply to the automotive radar domain straightforward.

#### 1.1.1 Contributions

To address the limitations of the abovementioned techniques, we introduce "BlueFMCW," a novel FMCW mechanism that features robustness against interference

and spoofing attacks simultaneously. BlueFMCW utilizes random hopping chirp signals in the physical layer. The randomness minimizes the impact from collisions in the first place, whether they are intended (security attacks) or not (interferences). The technique is named after Bluetooth [19] for the frequency hopping to avoid interfering signals. Bluetooth randomly switches the frequency over 79 channels between 2400 and 2483.5 MHz at a rate of 1600 hops per second. We adopt the frequency hopping to a radar system, in which way multiple radars can share a same band without interference thanks to the random hopping pattern. It also makes the BlueFMCW robust against spoofing attacks by making attackers not easily able to decrypt key parameters such as a random hopping pattern.

The idea of using a random waveform to mitigate the interference has been proposed before this paper. A recent work proposed an amplitude-modulated chirp waveform for a transmitted signal [20]. It exploits a hash function for the amplitude modulation and the pulse repetition period to avoid the interfering signal. Nonetheless, due to reliance on a precise control of the amplitude, its performance under noise cannot be guaranteed. Another recent proposal introduced a FMCW mechanism based on a random chirp signal [21]. It divides the pulse into  $N$  smaller chirp chips while randomly switching the starting frequencies of each chip. The limitation is that the resolution is sacrificed by the number of sub-chirps, focusing on confusing attackers by hopping the frequency and using the information from a single chirp chip.

To this end, we use a frequency hopping method where all the best signals from the sub-chirps are aggregated. It enables us to achieve  $N$  times higher resolution than using a single chirp chip. Our work also effectively suppresses the in-band spoofing or interference signal by spreading out their energy.

We summarize the contributions of BlueFMCW as follows:

- Avoids inter-radar interference and spoofing attacks;
- Avoids degradation of the resolution by using a random frequency hopping;
- Resolves the phase discontinuity caused by random frequency hopping using phase alignment algorithm;
- Keeps compatibility with conventional FMCW radars.

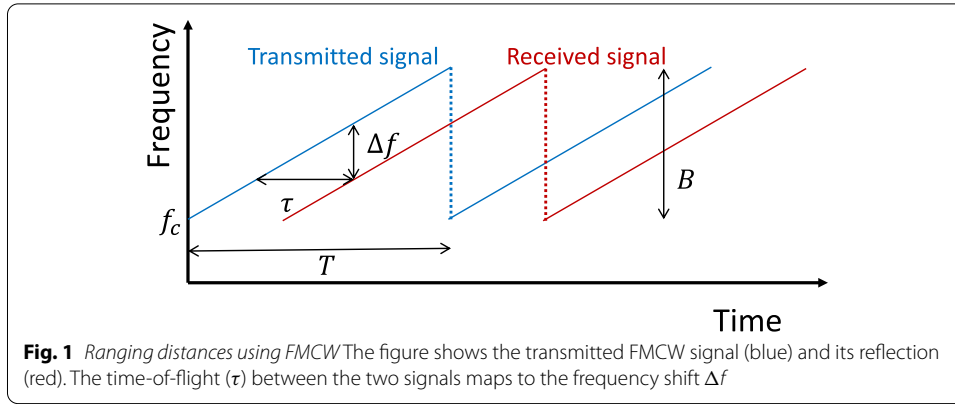
This paper is organized as follows. Section 2 covers the background of FMCW radar and adversary model. Details of BlueFMCW radar are discussed in Sect. 3. Section 4 presents performance evaluation of BlueFMCW radar compared with baseline methods. Conclusions are made in Sect. 5.

## 2 Background

### 2.1 FMCW radar

FMCW radar continuously transmits periodic pulses whose frequency sweeps linearly in time, as shown by the blue line in Fig. 1. Mathematically, the transmitted signal is

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



where  $f_c$  and  $\alpha$  are the starting frequency and slope of the FMCW chirp, respectively. The reflected signal is a time-delayed version of the transmitted signal, which arrives after bouncing off a reflector, as illustrated by the red line shown in Fig. 1. The time-of-flight (TOF,  $\tau$ ) is an elapsed time for the transmitted signal, traveling the round-trip distance  $2d$  from the radar to the reflector and back to the radar. In the presence of multiple reflectors, the received signal is written as  $s_r(t) = \sum A_i s_t(t - \tau_i)$ , where  $A_i$  and  $\tau_i$  are the attenuation factor and TOF of the  $i$ th reflector. The receiver mixes the transmitted signal with the received signal to produce a beat signal  $x(t) = s_r(t) \cdot s_t(t)^*$ . The beat signal becomes

$$x(t) = \sum_i A_i \exp \left( j2\pi \left( \alpha \tau_i t + f_c \tau - \frac{\alpha}{2} \tau_i^2 \right) \right). \quad (2)$$

This enables us to extract a distance profile of multiple reflectors because the frequency of the beat signal is  $\alpha \tau$  where  $\alpha$  is a known parameter. Hence, we can perform the FFT on the beat signal and measure the distance by  $d = \frac{\tau}{2} = \frac{f}{2\alpha}$ .

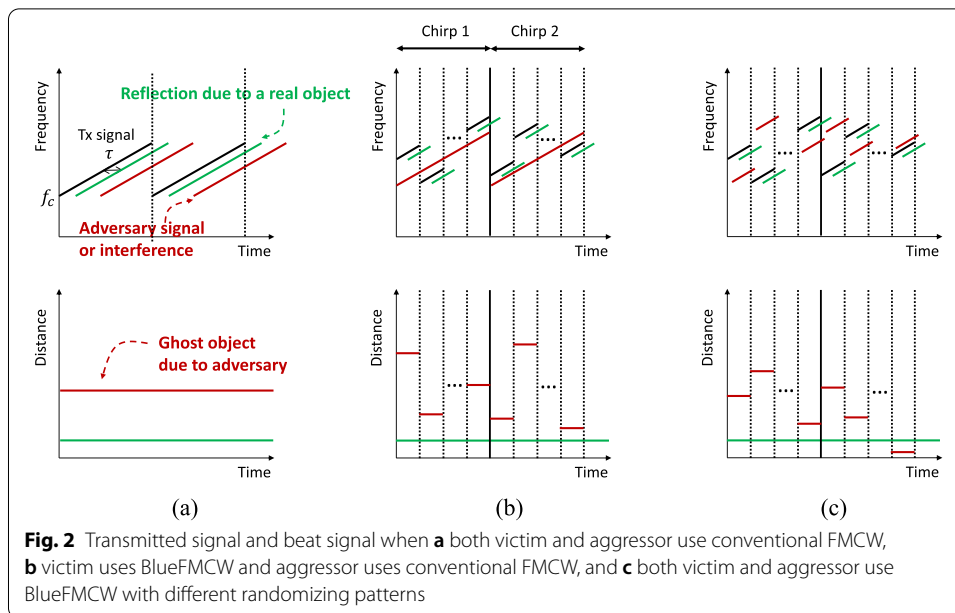
The resolution of FMCW is defined by the ability to distinguish two objects close to each other. The distance is proportional to the TOF, which is linearly mapped to the frequency. Hence, the distance resolution depends on the ability to resolve two frequencies. The resolution of resolving two frequencies  $\Delta f_{min}$  is equal to the size of a single FFT bin. When the FFT is taken over a chirp-duration  $T$ , the size of one FFT bin is equal to  $1/T$ . Hence, the distance resolution is

$$\Delta d = \frac{C \cdot \Delta TOF}{2} = \frac{C \cdot \Delta f_{min}}{2\alpha} = \frac{C}{2\alpha T} = \frac{C}{2B} \quad (3)$$

where  $B$  is the frequency bandwidth equal to  $\alpha T$  and  $C$  is the speed of light. It is important to note that the resolution of FMCW is a function of the bandwidth of the transmitted signal.

## 2.2 Adversary models

We assume two adversary models: (1) a victim radar can be attacked by a spoofing signal intentionally generated by a malicious radar, (2) two or more radars with identical



parameters interfere with each other. In both scenarios, the victim radar would falsely detect an object, i.e., a ghost object.

Figure 2a shows an example of the ghost object when both victim and aggressor (or attacker) use the conventional FMCW configuration. The attacker can easily figure out the adversary signal by a few known parameters (frequency range and slope) or by listening to the victim's signal, learning the characteristics, and reproducing the replica. When it comes to the interference scenario, the victim would detect a ghost object if any aggressor shares the same frequency slope.

We propose BlueFMCW that divides a chirp into multiple sub-chirps and randomizes their order every chirp period as shown in Fig. 2b, c. BlueFMCW effectively avoids detecting the ghost object by hashing the beat frequencies from the adversary signals. This includes the scenarios when the victim uses BlueFMCW but the aggressor (or attacker) still uses the conventional FMCW shown in Fig. 2b, or when both victim and aggressor (or attacker) use BlueFMCW shown in Fig. 2c. In the latter case, the victim can avoid the ghost object only if the adversary signal has a different randomizing pattern from the victim. This condition may not be true when the attacker is agile enough to listen and replicate the adversary signal within a short time window. However, it is not a practical scenario for two reasons. First, the physical distance between the attacker and victim is an unavoidable latency of the attack. The attacker has to be close to the victim. Alternatively, the attacker timely generates the adversary signal to arrive at the next chirp. It is impossible when the victim uses FMCW configuration because the attacker cannot predict the starting frequency of the next chirp. Second, the attacker needs to synchronize with the victim's signal to minimize its frequency offset, which typically requires listening to a series of the same chirps [4]. This is also impossible in BlueFMCW because the next chirp jumps to a random frequency.

In this paper, we will use the notation *adversary signals* to represent both spoofing and interference signals that create a ghost object at the victim radar.

### 3 Methods

To address the above adversary scenarios, we introduce BlueFMCW, a radar system that mitigates the adversary signals. Specifically, instead of transmitting a full chirping signal from the lower to upper frequency, BlueFMCW makes a *random-frequency-jump* in the middle of the chirp signal as shown in Fig. 2 (b) and (c). While the TOF of the reflected signals remains the same, the frequency gap with the adversary signal will be randomized. As a result, the false beat frequency does not stay at the same FFT bin. In other words, the energy of the adversary signal will be *randomly* dispersed over various FFT bins, which results in significantly smaller peaks in the spectrum.

#### 3.1 Random frequency hopping

Consider a conventional FMCW chirp signal, i.e., linear frequency modulation signal from a starting frequency  $f_c$  for  $T$  duration. BlueFMCW creates a series of frequency-hopping chirps by (1) dividing the conventional FMCW signal into  $N$  equal sub-intervals, and then (2) randomly permuting the sub-chirps. Suppose the victim radar receives a reflected signal from a real object and an adversary signal that spawns a ghost target. The bottom figures in Fig. 2a, b compare the victim's spectrograms of the conventional FMCW and BlueFMCW. The beat frequency from the adversary signal remains constant through  $T$  in the conventional FMCW. In contrast, BlueFMCW can *hash* the beat frequency thanks to its *randomized* starting frequencies of the sub-chirps. However, the beat frequency from the real object is not hashed and remains constant through  $T$ . This is because the beat frequency of a true object only depends on the TOF regardless of the starting frequency. BlueFMCW leverages this to mitigate the adversary signal while achieving the same detection capability on the real objects.

To formalize this, we first denote the starting frequency of the  $k$ th sub-chirp to be  $f_k$ . For the random frequency hopping, we can define a random permutation  $\sigma : F \rightarrow F$ , where  $F$  is a finite set of the index  $1, 2, \dots, N$ . The two-line notation of  $\sigma$  can be written as:

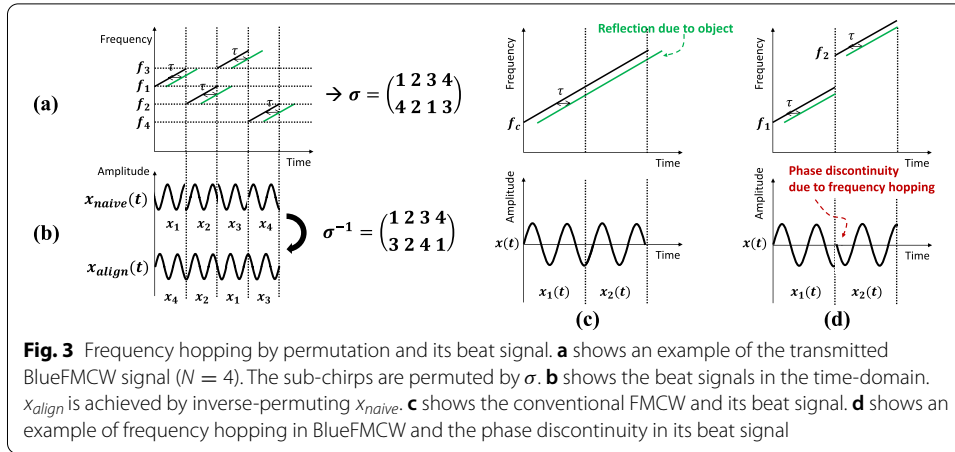
$$\begin{pmatrix} 1 & 2 & \dots & N \\ \sigma(1) & \sigma(2) & \dots & \sigma(N) \end{pmatrix} \quad (4)$$

Figure 3a illustrates an example of BlueFMCW sub-chirps with  $N = 4$ . In this example, the first sub-chirp of the conventional FMCW 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 fourth slot. In the next section, we will discuss the impact of the phase discontinuity of the beat signal and how we can reconstruct the original beat signal using the inverse permutation.

#### 3.2 Reconstruction

##### 3.2.1 Challenges: resolution and discontinuities

By observing the pattern of the BlueFMCW spectrogram, one can speculate which one is the true object or adversary signal. The true object tends to have a consistent peak frequency while the adversary signal jumps from one to another frequency. Using this observation, one can estimate a rough distance profile from the single sub-chirp's beat signal.



However, the distance resolution of a sub-chirp is degraded by  $N$  because its bandwidth is reduced by  $B/N$ . As discussed in Sect. 2, the distance resolution achieved by a single sub-chirp becomes  $\frac{cN}{2B}$ .

A naive attempt to solve the resolution problem is simply concatenating the beat signals of all sub-chirps in time-order such as

$$x_{naive}(t) = [x_1(t), x_2(t), \dots, x_N(t)] \quad (5)$$

where  $x_k(t)$  is the beat signal by  $k$ -th sub-chirp. By concatenating all  $N$  beat signals as illustrated in Fig. 3b, the resolution will remain the same with the conventional FMCW,  $\frac{c}{2B}$ . It will create, however, spurious frequency components in the frequency domain. To understand why, we need to examine the phase of the beat signal. Recall the beat signal from Eq. 2. For simplicity, we can rewrite the beat signal of the  $k$ -th sub-chirp with a single reflection:

$$x_k(t) = \exp(j2\pi(\alpha\tau t + f_k\tau - \alpha\tau^2/2)) \quad , t \in [0, T/N] \quad (6)$$

The phase in frequency is written as:

$$\phi = 2\pi(f_k\tau - \alpha\tau^2/2) \quad (7)$$

Figure 3c shows an example of the conventional FMCW. As can be seen, the conventional FMCW signal is a special case of BlueFMCW where  $f_k$ 's are sorted in ascending order. Hence, we can represent  $x_2(t)$  in two ways; one with Eq. 6 and the other with the  $T/N$  advanced version of Eq. 2.

$$x_2(t) = \begin{cases} \exp(j2\pi(\alpha\tau t + f_2\tau - \alpha\tau^2/2)) & \text{by Eq. 6} \\ \exp(j2\pi(\alpha\tau(t + T/N) + f_1\tau - \alpha\tau^2/2)) & \text{by Eq. 2} \end{cases} \quad (8)$$

For the conventional FMCW, the phases of the two equation are always the same.

$$2\pi(f_2\tau - \alpha\tau^2/2) = 2\pi(\alpha\tau T/N + f_1\tau - \alpha\tau^2/2) \quad (9)$$

The two phases are always identical in the conventional FMCW because  $f_2$  is equal to  $f_1 + \alpha T/N$ . However, if the sub-chirps are randomly permuted, it is not guaranteed that



$f_{k+1}$  is equal to  $f_k + \alpha T/N$ . This will cause phase discontinuities as shown in Fig. 3d. We will address this issue in the following section.

### 3.2.2 Phase alignment

To eliminate the phase discontinuity due to the frequency hopping, BlueFMCW rearranges the beat signals by inverting the permutation used in the frequency hopping. For example in Fig. 3a, the first sub-chirp of the conventional FMCW (starting frequency  $f_1$ ) was permuted to the fourth time-slot. If we concatenate the beat signals in time-order, the beat signal starting at  $f_1$  comes at the last place, causing the phase discontinuity. As we know how the sub-chirp was permuted ( $\sigma$ ), we can invert the permutation to bring the beat signal back to the correct time-slot so that the phase becomes continuous. By the inverse permutation  $\sigma^{-1}$ , the fourth beat signal is permuted to the first time-slot, and so the others (Fig. 3 b).

Formally, the phase aligned beat signal,  $x_{align}$ , is achieved by performing the inverse permutation  $\sigma^{-1}$  on the time-order beat signals,  $x_{naive}$ .

$$x_{naive}(t) = [x_1, x_2, \dots, x_N] \quad (10)$$

$$x_{align}(t) = [x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \dots, x_{\sigma^{-1}(N)}] \quad (11)$$

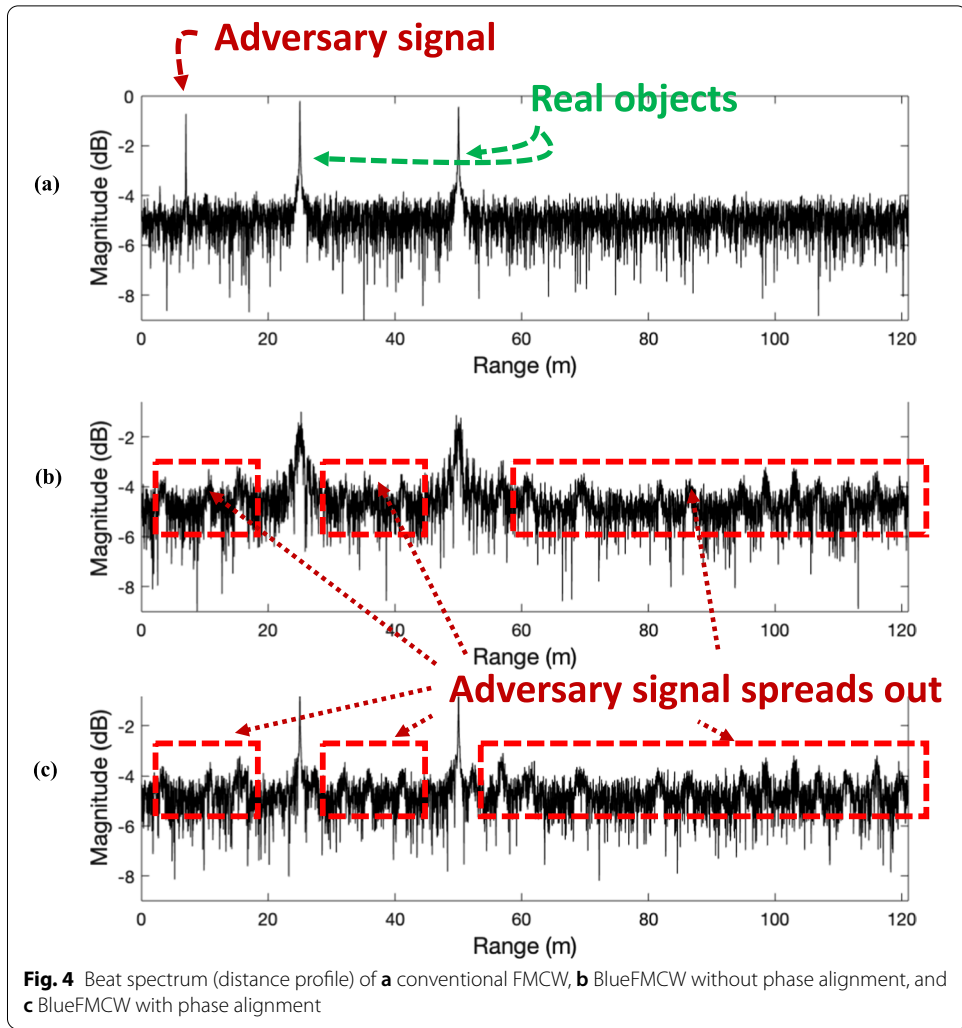
Figure 4 shows the impact of the phase alignment in the beat spectrum. In this example, two true objects and one adversary signal are simulated. The conventional FMCW in Fig. 4 (a) images all three components in the spectrum. In Fig. 4b, the spectrum of  $x_{naive}$  is shown. Due to the phase discontinuity, we can observe many spurious signals around the objects and the smaller and unclear peaks for the true objects. After the phase alignment, Fig. 4c shows two clear peaks of the objects. Note that both BlueFMCWs with and without phase alignment can alleviate the adversary signal. This is because random frequency hopping makes random frequency gaps against the adversary, and thus, the result beat frequencies also become randomized whether phase-aligned or not. The mitigated adversary signal, however, did not disappear. Instead of persisting at one frequency, the adversary signal is randomly dispersed over the various frequencies.

### 3.3 Designing BlueFMCW

In the previous section, we showed that BlueFMCW can spread out the adversary signal while holding the phase continuity of the reflected signals from the real objects. We assume the sub-chirps share the same slope ( $\alpha$ ) and duration ( $T_b$ ) for the simplicity. In addition, the frequency support of each sub-chirp must be mutual exclusive in order to align the phase by the permutation. For example, if a frequency support overlaps with another, the phase cannot be aligned without dropping the overlapping samples. For the opposite case, if there are empty gaps among the frequency supports, the phase alignment again cannot be achieved without interpolating the missing samples. Thus, having the frequency supports to be mutual exclusive each other and to cover the full bandwidth makes the problems easy.

The question remains *how diverse BlueFMCW can spread out the adversary signals*. To maximize the spread, we want to avoid the adversary signals falling in the same FFT bin. By properly choosing the sub-chirp parameters, the down-converted adversary signals





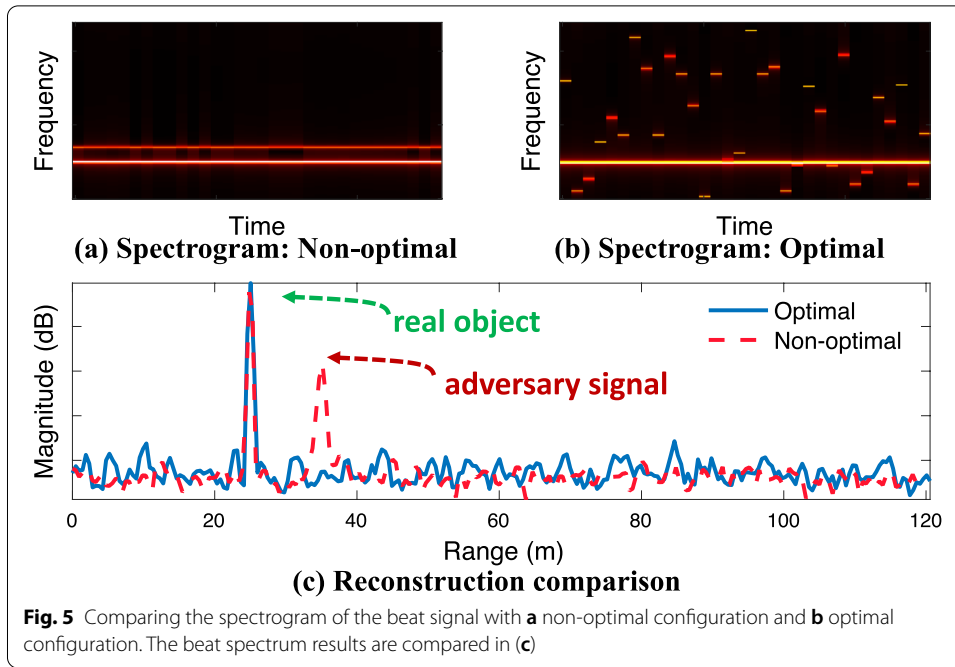
fall into many different FFT bins.<sup>1</sup> As a result, the energy of the adversary signal will be widely spread over the bandwidth. In the opposite case, when the adversary signals fall at a few identical FFT bins, they will end up with high-magnitude tones in FFT.

The beat frequency of an adversary signal in FFT can be represented by the starting frequencies of the victim and aggressor (interferer or attacker), the bandwidth of the sub-chirps ( $B_{sub} = \alpha T_b$ ), and the sampling rate ( $f_s$ ).

$$f_{beat} = \text{mod}(\Delta f + kB_{sub}, f_s) \quad , k = 0, 1, 2, \dots, N - 1 \quad (12)$$

where  $\Delta f$  is the frequency difference between the transmitted signal and the received adversary signal, and  $k$  is an integer dependent on the permutation. In the conventional FMCW,  $k$  is zero for the entire chirp duration which makes the beat frequency constant.  $\Delta f$  is dependent on the distance, the starting frequency of the aggressor, and the delay

<sup>1</sup> In order to highlight the impact of sub-chirp design, we assume a worst-case scenario that the out-of-band adversary signal after the receiver mixer can be leaked to ADC and cause aliasing spectrum in the FFT. In practice, the LPF can filter out most of the out-of-band signals.



of the adversary signal. Therefore, BlueFMCW does not have control over  $\Delta f$ . However, BlueFMCW can configure  $B_{sub}$  and  $f_s$ . Assume they are set to  $B_{sub} = \frac{n}{m}f_s$  where  $m$  and  $n$  are the integers. To calculate  $f_{beat}$ , consider the argument of the modulo operation in Eq. 12 as

$$\frac{\Delta f + kB_{sub}}{f_s} = \frac{\Delta f}{f_s} + \frac{kn}{m} \quad (13)$$

$$= \underbrace{Q}_{\text{Quotient}} + \underbrace{\delta f + \frac{p}{m}}_{\text{remainder}} \quad (14)$$

where  $Q$  is the quotient of the division, and  $\delta f + \frac{p}{m}$  is the remainder where  $p$  is an integer such that  $-m < p < m$ . We can use the above result to rewrite the beat frequency as

$$f_{beat} = \left( \delta f + \frac{p}{m} \right) f_s \quad (15)$$

Note that  $\delta f$  is the constant remainder from  $\frac{\Delta f}{f_s}$  that does not impact on the diversity. Therefore, there exists at most  $m$  different  $f_{beat}$ . For the worst case example ( $m = 1$ ), consider  $N = 4$ ,  $f_s = 100\text{MHz}$ ,  $B_{sub} = 2f_s = 200\text{MHz}$ , and  $\Delta f = 70\text{MHz}$ . No matter how we hop the frequency, the remainder is  $70/100$ , and thereby  $f_{beat}$  is always  $70\text{MHz}$ . For a better configuration ( $m = 3$ ), consider  $B_{sub} = \frac{7}{3}f_s$  with the same setup for the rest. For  $k = 0, 1, 2, 3$ , the remainders are  $70/100$ ,  $70/100 + 1/3$ ,  $70/100 + 2/3$ , and  $70/100$ , respectively. Therefore, we can achieve 3 different  $f_{beat}$  as  $m$  is set to 3.

Figure 5a shows the BlueFMCW spectrogram of the worst case. Clearly, the adversary is not spread even with the random frequency hopping. This is because  $f_s$  and  $B_{sub}$  have the integer relationship with  $m = 1$ . The red lines in Fig. 5c correspond to the reconstruction

**Table 1** Simulation setup

	Parameter	Value
FMCW	$f_c$	24 GHz
	Sampling rate	20 MHz
	Chirp duration	204.8 $\mu$ s
	# of total samples	4096
	Slope (optimal)	24.785 MHz/ $\mu$ s
	Slope (non-optimal)	26.562 MHz/ $\mu$ s
BlueFMCW	# of sub-chirps	32
	Sub-chirp duration	6.4 $\mu$ s
Aggressor	# of Aggressors	1–10
	Distance (m)	Unif (0.5, 200)
	SIR(dB)	Unif (2.5, 6)
Static object	Distance	25 m

result by the worst case. Figure 5b shows the BlueFMCW spectrogram of  $m = 131$ . Compared to the worst case, the adversary signal is spread on 131 different beat frequencies. As a result, the adversary signal is greatly reduced as shown in the blue lines in Fig. 5c.

## 4 Results and discussions

### 4.1 Simulation setup

We conducted a simulation on MATLAB to evaluate BlueFMCW's ability to mitigate the adversary signals. We choose two slope rates of the chirp; 24.785 MHz/us for the optimal configuration and 26.562 MHz/us for the non-optimal. BlueFMCW divides the chirp into 32 sub-chirps and randomly permutes them while sharing the common FMCW parameters. We simulated 10 different numbers of the aggressor radars, 1–10 aggressors. The distance to the aggressors is randomly chosen between 0.5–200 m. The power of the aggressor signal is also randomly generated to have SIR between 2.5–6 dB. Table 1 summarizes the experimental setup.

### 4.2 Evaluation metrics

We evaluate the performance of BlueFMCW along two axes. The first is how well it can mitigate the adversary. In this case, our metric is the *signal-to-interference ratio (SIR)* defined by the ratio between the signal power of the true object and the strongest interference signal seen in the beat frequency domain. The higher the SIR, the better BlueFMCW mitigates the adversary signals.

The second metric is the *signal-to-interference-plus-noise ratio (SINR)* loss. BlueFMCW spreads the adversary signals across the bandwidth. This will end up increasing noise floor, i.e., decreasing SINR. We first calculate the SINR of the conventional FMCW without any adversary signals,  $SINR_{base}$ . Then, we compare  $SINR_{base}$  with the SINR degraded by adversary signals.

$$SINR_{loss\_conv} = SINR_{base} - SINR_{conv} \quad (16)$$

$$SINR_{loss\_blue} = SINR_{base} - SINR_{blue} \quad (17)$$

### 4.3 Compare scenarios

We compare the following scenarios:

- *Conventional FMCW vs conventional FMCW's (CvC)* The victim radar and aggressor radars (interferers or attackers) use the conventional FMCW.
- *BlueFMCW vs conventional FMCW's (BvC)* The victim radar uses BlueFMCW, but the aggressor radars use the conventional FMCW.
- *BlueFMCW vs BlueFMCW's (BvB)* The victim radar and aggressor radars use BlueFMCW. However, they do not share the random permutation.

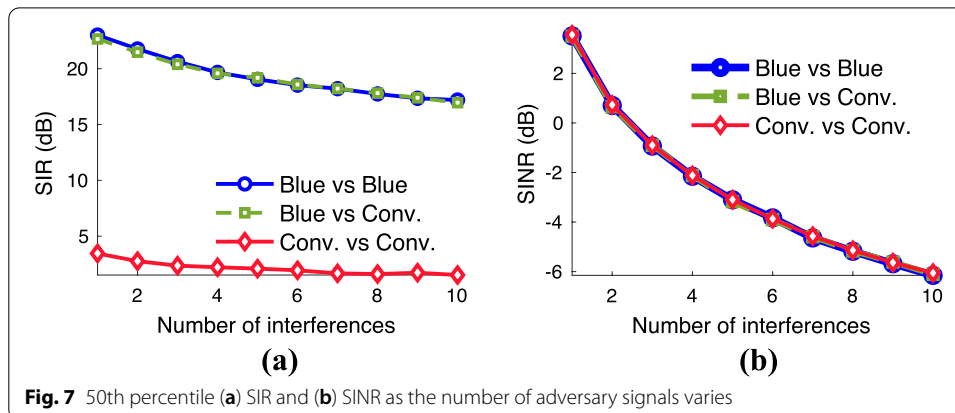
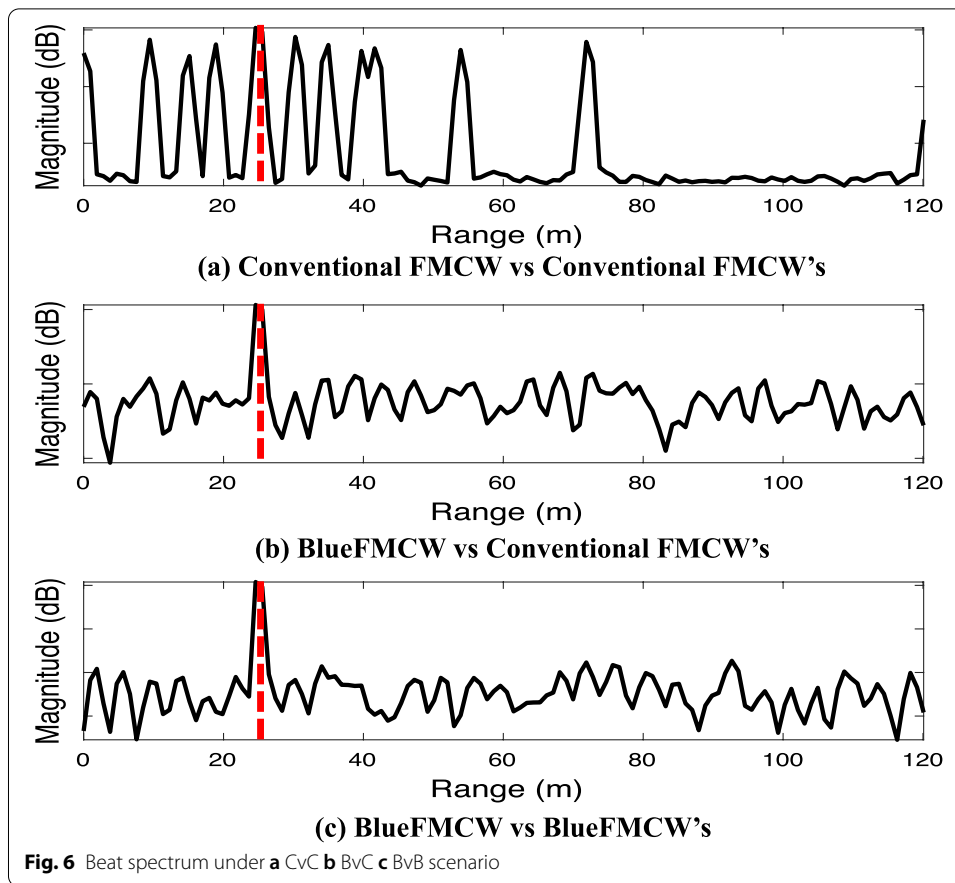
In addition, we evaluate the impact of the phase alignment and the BlueFMCW design on the performance.

### 4.4 Adversary mitigation performance

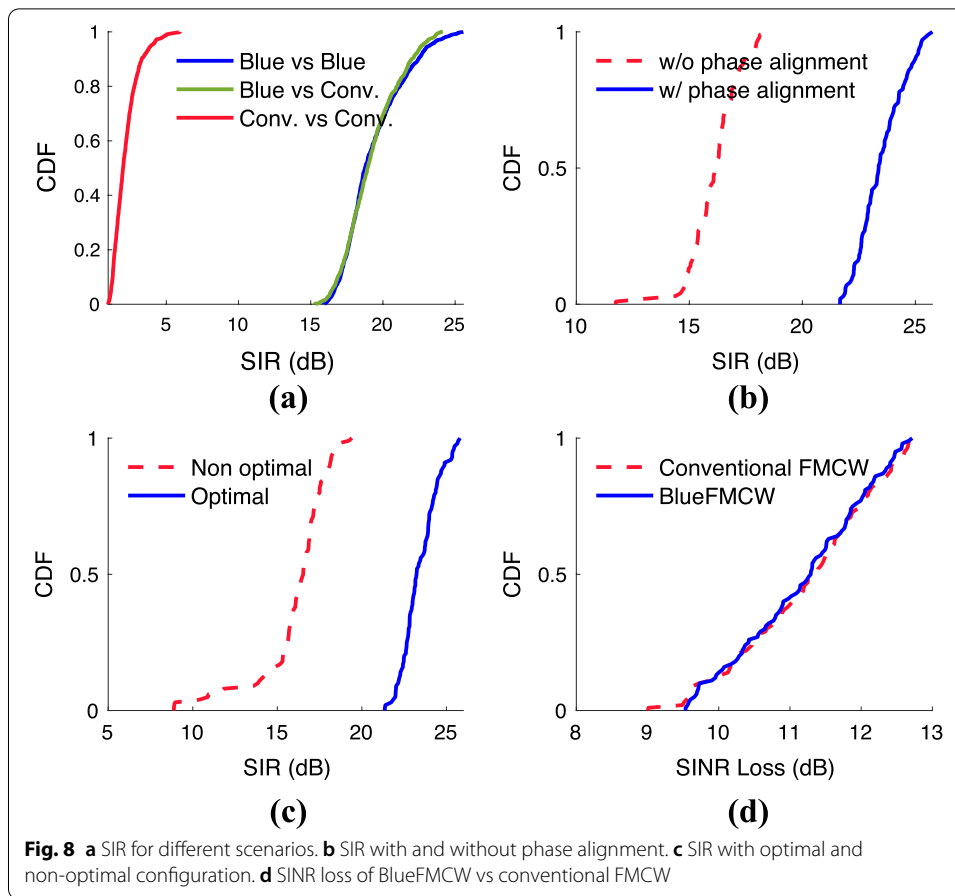
*Impact of the number of attackers* We first demonstrate the impact of the number of adversary signals on the performance of BlueFMCW. We compare the above three scenarios across the number of adversaries. The distance of the aggressor radars and the power of the adversary signals follow the uniform distribution in Table 1. Each case repeats 100 runs. One of the beat spectrum of the three scenarios with 10 adversary signals are compared in Fig. 6. The red dotted line represents the distance of the real object. As shown in Fig. 6a, the victim radar with the first scenario (all radars are conventional FMCW) has no capability of mitigating the adversary signals. However, when the victim radar uses BlueFMCW, it can suppress the adversary significantly regardless of the aggressor radar type as shown in Fig. 6b, c. Figure 7a shows the 50th percentile SIR as a function of the number of adversary signals. As the number of adversaries increases, BlueFMCW is able to uphold the high SIR in both BvC and BvB scenarios. On the other hand, the conventional FMCW is unable to mitigate a single adversary signal. Figure 8a plots the CDF of the SIRs of the three scenarios. BlueFMCW can achieve the 50th percentile SIR of 18.75 dB for BvB scenario and 18.93 dB for BvC scenario. Whereas in CvC scenario, the 50th percentile SIR is around 2 dB.

*Impact of the phase alignment* Next, we evaluate the impact of the phase alignment on the performance of BlueFMCW. In Sect. 3.2.2, we explain that the phase alignment reduces the discontinuities as combining the received signals to improve the distance resolution. Figure 8b plots the CDF of SIR gain with and without the phase alignment. The figure shows that the phase alignment can improve SIR more than 7dB. This is because the phase discontinuity is minimized by the alignment, and therefore, there are less spurs introduced by the true object signals.

*Optimal vs non-optimal configuration* In this experiment, we evaluate the performance of BlueFMCW with different chirp parameters. As explained in Sect. 3.3, we can configure BlueFMCW chirp to spread the adversary signal on more or less distinctive beat frequencies, i.e., how well it can disperse the adversary on the noise floor. Spreading the adversary signal on more number of distinctive beat frequencies



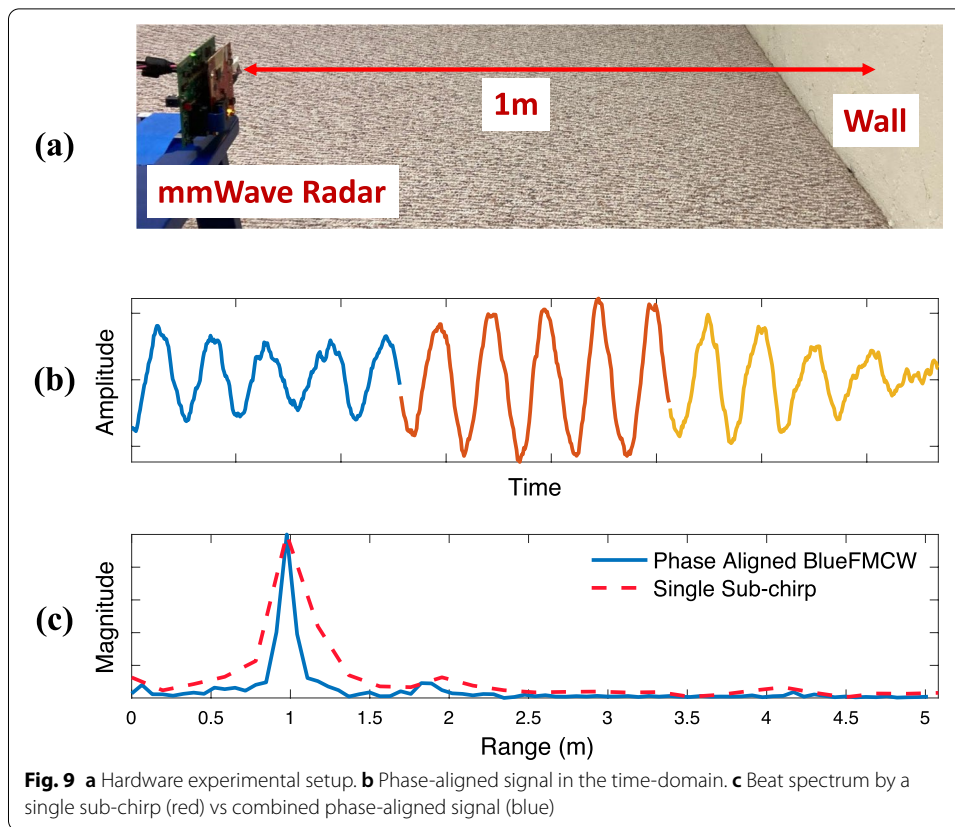
will increase SIR. Figure 8c compares the CDF of SIR when BlueFMCW spreads the adversary signal on (i) 131 possible beat frequencies (optimal configuration), and (ii) 2 possible beat frequencies (non-optimal configuration). We only changed the slope of the chirp while fixing the rest configuration as shown in Table 1. This will effectively change the bandwidth of the FMCW chirp. The non-optimal configuration degrades the median SIR by 7 dB and the 10th percentile SIR by 9 dB. This is due to the fact that there are only two possible beat frequencies where the adversary energy



falls onto. In contrast, the optimal configuration can create 131 possible beat frequencies and the adversary signals have more location to be spread out.

#### 4.5 SINR degradation

So far, we focus on the adversary mitigation performance of BlueFMCW by measuring SIR gain. In this experiment, we want to understand how the dispersed adversary signal will impact on the noise level. We first calculate the SINR over the number of interferences. Figure 7b shows the 50th percentile SINR as a function of the number of adversary signals. In all three scenarios (CvC, BvC, and BvB), the SINR drops as the number of interferences increases. However, the SINR between the scenarios is almost the same. This result is expected because BlueFMCW simply spreads the interference into different beat frequencies without creating or removing any signals. Next, we calculate the SINR of the conventional FMCW without any adversary, which serves as the base line. Then, we compare the base SINR with the SINR by the conventional FMCW and BlueFMCW interfered by an aggressor. Figure 8d compares the CDF of SINR loss of the conventional FMCW and BlueFMCW. The figure shows both cases have almost same amount of the SINR loss. Again, this suggests that the energy of the adversary is not either created nor removed. BlueFMCW spreads the energy of the interferences into different beat frequencies so that none of them creates a strong peak. The spreaded will effectively increase



the noise floor which is to pay in BlueFMCW. However, increasing the noise floor is a less critical problem than detecting a ghost object by a strong interference.

#### 4.6 Hardware measurement

We implement a proof-of-concept system on an off-the-shelf mmWave radar (TI IWR1843 evaluation board). In Fig. 9, we generate three sub-chirps starting at 77, 77.768, 78.535 GHz with 29.982 MHz/us slope for 256 number samples at 10Msps. We put the radar 1m from the wall as shown in Fig. 9a. The samples from the sub-chirps are captured in different time and post-processed for phase-alignment. Figure 9b shows the phase-aligned signal in the time-domain. The result verifies our observation in Eq. 9. Figure 9c compares the beat spectrum by a single sub-chirp (red) and the combined phase-aligned signal (blue). The range resolution is improved by three times.

Figure 10 shows more examples of phase-aligned signal and its beat spectrum generated by BlueFMCW. In the left figure, BlueFMCW measures the wall at a longer distance (3.9m). We use the same configuration with Fig. 9 experiment. The three sub-chirps are phase-aligned in Fig. 10a and its spectrum is compared with a single sub-chirp in Fig. 10b. In the right figure, BlueFMCW measures the same wall with a fire extinguisher at 2.1m. This setup uses eight sub-chirps starting at 77, 77.2, 77.4, 77.6, 77.8, 78, 78.2, 78.4 GHz with 4.731 MHz/us slope for 128 samples at 3Msps. The eight sub-chirps are phase-aligned in Fig. 10c and its spectrum is compared with a single sub-chirp in



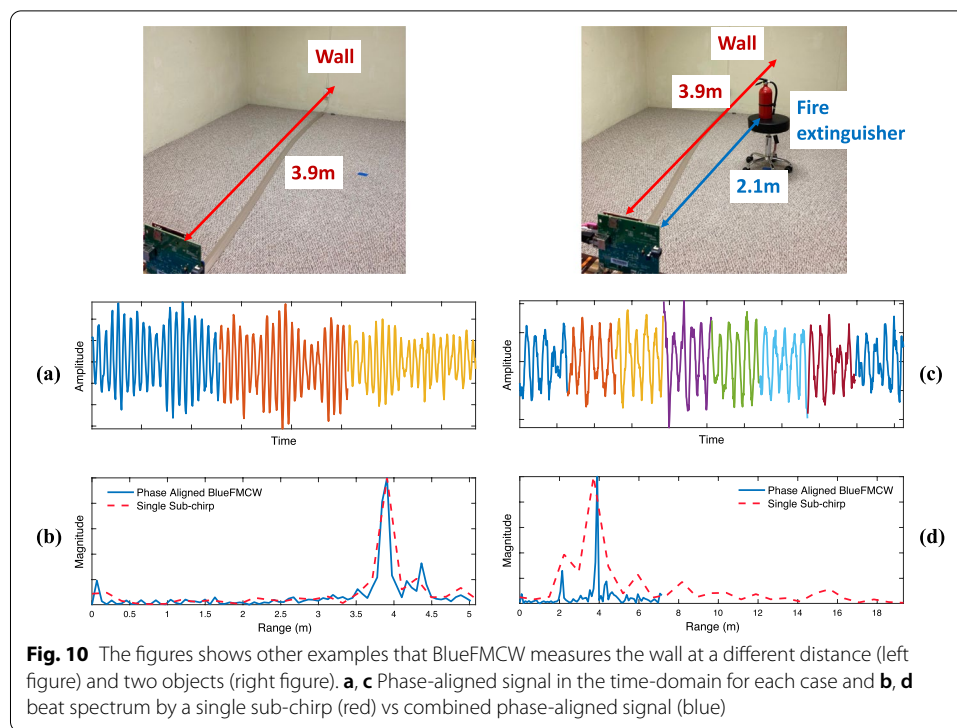


Fig. 10d. Note that the distance resolution is 8-times improved, and the two objects are sharply distinct.

## 5 Conclusion

This paper introduced BlueFMCW, a novel radar system that can efficiently mitigate spoofing and interference signals without compromising radar resolution. Our simulation and hardware results demonstrate that BlueFMCW can significantly improve the SIR ratio compared to the conventional FMCW system while avoiding resolution degradation by the random sub-chirps. Moving forward, we are interested in conducting more hardware experiments in the presence of adversary signals.

### Abbreviations

FMCW:: Frequency-modulated continuous-wave; SLAM:: Simultaneous localization and mapping; VR:: Virtual reality; AR:: Augmented reality; PC-FMCW:: Phase-coded frequency-modulated continuous-wave; MHz:: Mega Hertz; TOF:: Time-of-flight; FFT:: Fast Fourier Transform; LPF:: Low-pass filter; SIR:: Signal-to-interference ratio; SINR:: Signal-to-interference-plus-noise ratio; dB:: Decibel; CDF:: Cumulative distribution function; mmWave:: Millimeter wave; Msps:: Mega sample per second.

### Acknowledgements

Not applicable.

### Authors' contributions

Thomas Moon contributed to methodology, formal analysis, and experiments. Jounsup Park and Seungmo Kim contributed to literature investigation. All authors read and approved the final manuscript.

### Funding

Not applicable.

### Availability of data and materials

Please contact author for data requests.

**Ethics declarations**

Not applicable.

**Competing interests**

The authors declare that they have no competing interests.

**Author details**

<sup>1</sup>Department of Electrical and Computer Engineering, University of Illinois at Urbana and Champaign, Urbana, USA.

<sup>2</sup>Department of Electrical Engineering, University of Texas at Tyler, Tyler, USA. <sup>3</sup>Department of Electrical and Computer Engineering, Georgia Southern University, Statesboro, USA.

Received: 23 June 2021 Accepted: 13 January 2022

Published online: 26 January 2022

**References**

1. J. Lien, N. Gillian, M.E. Karagozler, P. Amihoud, C. Schwesig, E. Olson, H. Raja, I. Poupyrev, Soli: ubiquitous gesture sensing with millimeter wave radar. *ACM Trans. Graphics* **35**(4), 1–19 (2016)
2. S. Praveen, O. Raoul, P. Bradley, A. David, L. Todd, S. Daniel, K. Jonathan, Miniature radar for mobile devices. In: 2013 IEEE High Performance Extreme Computing Conference (HPEC), pp. 1–8 (2013). IEEE
3. P. Kapoor, A. Vora, K. Kang Detecting and mitigating spoofing attack against an automotive radar. In: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), pp. 1–6 (2018)
4. N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, D. Suzuki A low-cost replica-based distance-spoofing attack on mmwave fmcw radar. In: Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop, pp. 95–100 (2019)
5. Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, M. Srivastava, Attack resilience and recovery using physical challenge response authentication for active sensors under integrity attacks. *arXiv preprint* [arXiv:1605.02062](https://arxiv.org/abs/1605.02062) (2016)
6. D. Ma, N. Shlezinger, T. Huang, Y. Liu, Y.C. Eldar, Joint radar-communications strategies for autonomous vehicles. *arXiv preprint* [arXiv:1909.01729](https://arxiv.org/abs/1909.01729) (2019)
7. T. Huang, N. Shlezinger, X. Xu, Y. Liu, Y.C. Eldar, Majorcom: A dual-function radar communication system using index modulation. *IEEE Trans. Signal Process.* (2020)
8. J. Bechter, K. Eid, F. Roos, C. Waldschmidt, Digital beamforming to mitigate automotive radar interference. In: 2016 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM), pp. 1–4 (2016). IEEE
9. J. Bechter, M. Rameez, C. Waldschmidt, Analytical and experimental investigations on mitigation of interference in a dbf mimo radar. *IEEE Trans. Microw. Theory Tech.* **65**(5), 1727–1734 (2017)
10. H. Dai, X. Wang, Y. Li, Y. Liu, S. Xiao, Main-lobe jamming suppression method of using spatial polarization characteristics of antennas. *IEEE Trans. Aerosp. Electron. Syst.* **48**(3), 2167–2179 (2012)
11. H. Dai, X. Wang, Y. Li, Novel discrimination method of digital deceptive jamming in mono-pulse radar. *J. Syst. Eng. Electron.* **22**(6), 910–916 (2011)
12. M. Gerstmaier, A. Melzer, A. Onic, M. Huemer, On the safe road toward autonomous driving: phase noise monitoring in radar sensors for functional safety compliance. *IEEE Signal Process. Mag.* **36**(5), 60–70 (2019)
13. F. Jin, S. Cao, Automotive radar interference mitigation using adaptive noise canceller. *IEEE Trans. Veh. Technol.* **68**(4), 3747–3754 (2019)
14. Y. Stettiner, N. Arkind, FMCW Automotive Radar Incorporating Nonlinear Frequency Hopping Sequence Of Fractional Bandwidth Multiband Chirps. Google Patents. US Patent App. 17/048,576 (2021)
15. J. Bechter, C. Sippel, C. Waldschmidt, Bats-inspired frequency hopping for mitigation of interference between automotive radars. In: 2016 IEEE MTT-S International Conference on Microwaves for Intelligent Mobility (ICMIM), pp. 1–4 (2016). IEEE
16. K.M. Cuomo, J.E. Pion, J.T. Mayhan, Ultrawide-band coherent processing. *IEEE Trans. Antennas Propag.* **47**(6), 1094–1107 (1999)
17. J. Yu, J. Krolik, Multiband chirp synthesis for frequency-hopped fmcw radar. In: 2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, pp. 1315–1319 (2009). IEEE
18. F. Uysal, Phase-coded fmcw automotive radar: system design and interference mitigation. *IEEE Trans. Veh. Technol.* **69**(1), 270–281 (2020)
19. J.C. Haartsen, The bluetooth radio system. *IEEE Pers. Commun.* **7**(1), 28–36 (2000)
20. Z. Guan, Y. Chen, P. Lei, D. Li, Y. Zhao, Application of hash function on fmcw based millimeter-wave radar against drfm jamming. *IEEE Access* **7**, 92285–92295 (2019)
21. J. Liu, Y. Zhang, X. Dong, High resolution moving train imaging using linear-fm random radar waveform. In: 2018 Asia-Pacific Microwave Conference (APMC), pp. 839–841 (2018). IEEE

**Publisher's Note**

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.