Cover Chirp Jamming: Hybrid Jamming–Deception Attack on FMCW Radar and Its Countermeasure

Shoei Nashimoto
Nashimoto.Shoei@bx.MitsubishiElectric.co.jp
Mitsubishi Electric
Kamakura, Kanagawa, Japan

Tomoyuki Nagatsuka
Mitsubishi Electric Engineering
Kamakura, Kanagawa, Japan

ABSTRACT

The reliability of measurements is crucial for ensuring the safety of control systems that depend on such measurements. Frequency-modulated continuous-wave (FMCW) radar is an active sensor used to measure distance and speed. Security evaluations of commercial FMCW radars have focused primarily on deception attacks, assuming that jamming attacks are easier to address. In this study, we propose a novel and efficient jamming attack called *cover chirp jamming*. This attack utilizes deception techniques and concentrates energy near the target, resulting in higher efficiency compared to conventional jamming methods. Furthermore, it can bypass existing countermeasures against noise, interference, and jamming. We demonstrate the effectiveness and feasibility of the attack through field and simulation experiments using a modern 77-GHz multi-input multi-output FMCW radar. Moreover, we propose a software-based countermeasure that detects and mitigates the attack. Our quantitative evaluation shows that the power of cover chirp jamming is 17.4 dB higher than conventional jamming. In addition, the countermeasure effectively mitigates the attack if the jamming-to-signal ratio (JSR) is below 0.6 dB, whereas the cover chirp jamming cannot be mitigated when the JSR exceeds 0.6 dB.

CCS CONCEPTS

• **Security and privacy → Hardware attacks and countermeasures**.

KEYWORDS

FMCW Radar, Jamming Attack, Deception Attack, Countermeasure

ACM Reference Format:
Shoei Nashimoto and Tomoyuki Nagatsuka. 2023. Cover Chirp Jamming: Hybrid Jamming–Deception Attack on FMCW Radar and Its Countermeasure. In *Proceedings of the 2023 Workshop on Attacks and Solutions in Hardware Security (ASHES '23), November 30, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3605769.3623990

1 INTRODUCTION

A radar is an active sensor that uses radio waves to measure the distance, velocity, and direction of an object. Millimeter-wave frequency-modulated continuous-wave (FMCW) radar can miniaturize circuits and antennas and has good accuracy. Thus, FMCW radar systems are expected to be used in autonomous control, healthcare, and for detecting abnormal objects [1, 28]. The reliability of these systems is based on the premise that corresponding sensor measurements are reliable. Heterogeneous sensor measurements (i.e., sensor fusion) are used in many systems, and attacks on individual radars cannot be discussed in terms of their impact on the system. However, attacks on individual sensors are building blocks for attacks on sensor fusion. The security evaluations of commercial FMCW radars have been conducted from this perspective.

Table 1: Attack method, attack equipment, its cost, and operating frequency. D and J signify deception and jamming attacks, respectively.

Year	Paper	Attack	Equipment	Cost *1	Frequency
Ours		J by D	Radar board	low	77 GHz
2022	[15]	D	Self-assembled	low	24 GHz
2021	[33]	D with J	SDR	high	60 GHz
2021	[24]	D	Radar board	low	24 GHz
2020	[36]	D	Radar board	low	77 GHz
2016	[42]	D, J	Instrumentation	high	77 GHz
2022	[23]	D	Self-assembled	-	10 GHz <
2021	[22]	D	Self-assembled		
2021	[14]	D	SDR		
2014	[4]	D	SDR		
2022	[20]	D		-	24 GHz
2022	[3]	D			77 GHz
2018	[34]	D, J	Simulation		77 GHz
2018	[12]	D			77 GHz
2017	[7]	D			77 GHz

*1: Costs are estimates based on equipment; low and high costs mean less than $1,000 and over $100,000, respectively.

Radar attacks are divided into two types [4, 14, 20, 23, 38]: jamming attacks, which cause targets to become undetectable, and deception attacks, which cause non-existent targets to become detectable. Table 1 summarizes previous studies on attacks and countermeasures against commercial FMCW radars. These studies can be divided into three categories: demonstrations using millimeter-wave band FMCW radars with actual equipment [15, 24, 33, 36, 42], evaluations using low-frequency FMCW radars (or only waveforms) with actual equipment [4, 14, 22, 23], and only simulations [3, 7, 12, 20, 34].

The aforementioned studies have mainly focused on deception attacks because jamming attacks are considered easier to detect and prevent [12, 14, 15, 20, 22, 23]. This is because noise suppression through signal processing and interference countermeasures, which are based on a *detect and repair* approach, have become standard in commercial radar systems today [40]. However, the threat of jamming attacks bypassing such countermeasures has to be considered. Jamming is superior to deception in certain situations (e.g., jamming the emergency brake of autonomous vehicles, as shown in Fig. 1) because only jamming can render a target undetectable.

ASHES '23, November 30, 2023, Copenhagen, Denmark.

ACM ISBN 979-8-4007-0262-4/23/11.
https://doi.org/10.1145/3605769.3623990

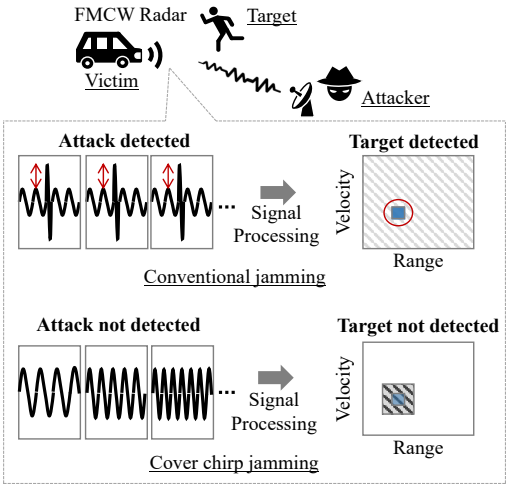


Figure 1: Overview of cover chirp jamming which makes target undetectable without attack detection.

In this study, we propose *cover chirp jamming*, a novel jamming attack that bypasses fundamental countermeasures. As illustrated in Fig. 1, the basic idea is to perform a deception attack by gradually shifting the frequency to concentrate the jamming noise in a targeted narrow band. As cover chirp jamming appears as a false target on a per-waveform basis, existing interference and jamming countermeasures cannot detect the attack. In addition, the concentrated noise is difficult to suppress. We also propose a countermeasure for detecting the proposed attack and extracting the target signal from jammed measurement data. We demonstrate the effectiveness of the proposed attack and countermeasures through field experiments using a radar board and simulations. As an ideal cover chirp jamming requires high-resolution waveform control capability, we also propose a low-cost attack equipment implementation.

Related works. Some studies have demonstrated jamming attacks. Sun et al. proposed a deception attack combined with a conventional jamming attack (i.e., *deception with jamming*) to make only false targets detectable while making real objects undetectable [33]. Therefore, this approach differs from ours, which uses deception techniques for jamming (i.e., *jamming by deception*). At the user level, detection of a jamming attack also differs in addition to object visibility. Yan et al. and Tanis demonstrated a classical jamming attack that intentionally created interference conditions [34, 42]. Thus, the attack can be detected and mitigated using existing interference and jamming countermeasures.

Attack equipment that is effective against millimeter-wave FMCW radar involves a tradeoff between cost and performance. Software-defined radio (SDR)-based equipment with a transmitter/receiver [33] and instrumentation-based equipment with a signal analyzer and a signal generator [42] are expensive but can generate FMCW waveforms with high resolution. In contrast, radar board-based equipment and self-assembled equipment are low-cost but have limited capabilities. Lazaro et al. and Nashimoto et al. overcame

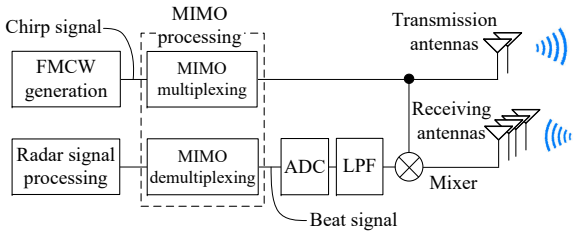


Figure 2: Frequency-modulated continuous-wave (FMCW) multi-input multi-output (MIMO) radar system including analog-to-digital converter (ADC) and low-pass filter (LPF).

such drawbacks by devising attack algorithms [15, 24]. We employed radar-board-based equipment with no circuit design and a simple configuration.

Contributions. The contributions of this study can be summarized as follows.

(1) To the best of our knowledge, this is the first demonstration of a novel jamming attack on commercial FMCW radars that can bypass detection by interference (and jamming) countermeasures.
(2) A software-based countermeasure is developed for detecting and mitigating the proposed attack.
(3) Field experiments using a radar board demonstrated the cover chirp jamming.
(4) We provide quantitative evaluations of the effectiveness of the proposed attack and countermeasures through simulation experiments.

2 FREQUENCY-MODULATED CONTINOUS WAVE (FMCW) RADAR

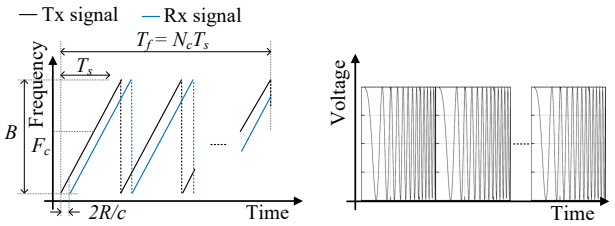
In this section, we provide an overview of the measurement principle and signal processing of FMCW radar using fast chirp modulation, which is commonly used in various applications [1, 18, 30].

2.1 Measurement Principle

Fig. 2 shows a typical configuration of an FMCW multi-input multi-output (MIMO) radar systems. It consists of modules for FMCW signal generation, MIMO signal processing, radio wave propagation between the transmitting (Tx) and receiving (Rx) antennas, conversion to an intermediate frequency by a mixer, digitization by an analog-to-digital converter (ADC), frequency extraction by a low-pass filter (LPF), and radar signal processing.

The FMCW radar performs frequency modulation with a linear time variation in the frequency, as shown in Fig. 3. The signal that determines the frequency change pattern is called the ramp signal (Fig. 3(a)), and the modulated signal is called the chirp signal (Fig. 3(b)). The sweep time T_s, center frequency F_c, bandwidth B, and the number of chirps in one frame N_c are the basic parameters determining the radar performance. The transmitted and received waves are mixed using a mixer as follows:

$$\cos f_T t \cos f_R t = \frac{\cos(f_T - f_R)t + \cos(f_T + f_R)t}{2}, \quad (1)$$



(a) Ramp signal. (b) Chirp signal.

Figure 3: FMCW waveform.

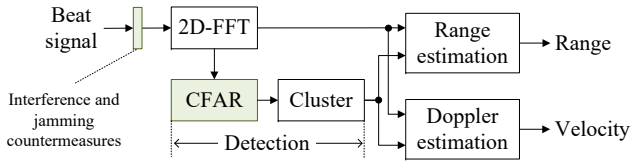


Figure 4: Radar signal processing including fast Fourier transform (FFT) and constant false alarm rate (CFAR). Colored processes represent obstacles to jamming attacks.

where f_T and f_R are the frequencies of the transmitted and received waves, respectively. In addition, only the component of $\cos(f_T - f_R)t$ is obtained by the LPF. The obtained signal and its frequency are called the beat signal and beat frequency, respectively.

The distance to the target and relative velocity were obtained from the frequency change of the beat signal. When the distance to the measurement target is R, the round-trip time of the wave is $2R/c$, where c is the speed of light. As the chirp signal changes at B/T_s, the frequency shift due to distance is given as follows:

$$f_r = \frac{2R}{c}\frac{B}{T_s}, \tag{2}$$

where f_r is the *range frequency*. In addition, the velocity is extracted as the phase change of the multiple beat signals (N_c). The phase change ϕ derived from the round-trip time $T = 2R/c$ is as follows:

$$\phi = 2\pi F_c T = \frac{4\pi R}{\lambda}, \tag{3}$$

where $\lambda = c/F_c$ is the radar wavelength. From $\Delta\phi/\Delta t = \omega$ and $\omega = 2\pi f$, (3) can be differentiated to obtain the frequency caused by the velocity v_d as follows:

$$f_d = \frac{2v_d}{\lambda}, \tag{4}$$

where f_d is the *Doppler frequency*.

2.2 Radar Signal Processing

Fig. 4 shows the flow of radar signal processing. Here, we focus on the two-dimensional fast Fourier transform (2D-FFT) and the constant false alarm rate (CFAR). Interference and jamming countermeasures are described later in Section 3.4.

First, we perform a 2D-FFT on the beat signal, as shown in Fig. 5. The 2D-FFT applies FFT once on multiple beat signals (range FFT), and a further FFT on the obtained results (Doppler FFT). It forms a two-dimensional array of range and Doppler frequencies, which is called a range–Doppler (RD) map.

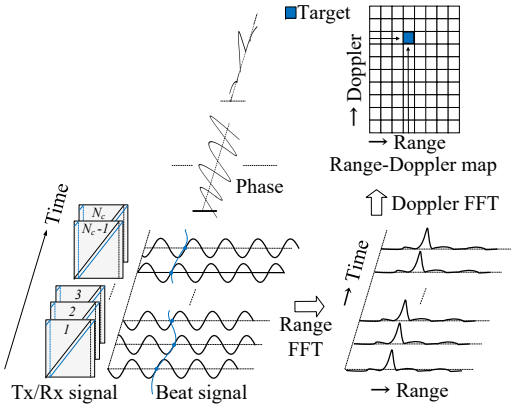


Figure 5: Computation of range–Doppler (RD) map by 2D-FFT.

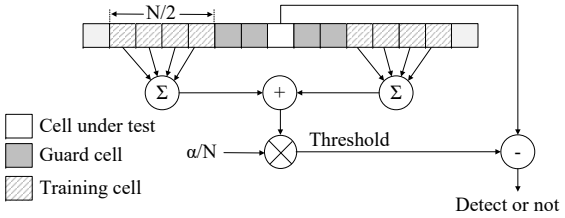


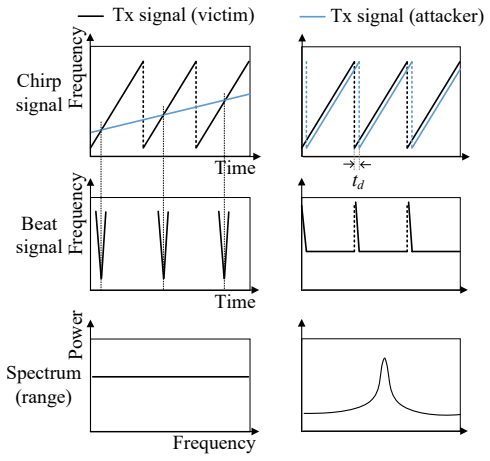
Figure 6: One-dimensional cell-averaging (CA)-CFAR. α represents a scaling factor based on the probability of false alarm (i.e., false positive rate).

Next, the target is detected using an RD map. The CFAR method detects targets with a constant false-alarm rate, even in the presence of noise derived from interference or clutter [11, 31]. A one-dimensional cell-averaging (CA)-CFAR is shown in Fig. 6. The CA-CFAR compares the value of the cell under test (CUT) with a threshold based on the average value of its surrounding cells (training cells) and determines whether an object exists. Considering that the CUT has a frequency spread, the cells to be excluded from averaging (guard cells) can be set. In the RD map, these cells are extended in two dimensions. See [31] for the specific threshold calculations, including those for α.

Subsequently, the CA-CFAR results are clustered. For instance, density-based spatial clustering of applications with noise (DBSCAN), a major clustering algorithm for radar processing [9, 16, 19], clusters based on the number of points within a circle of certain size. Finally, the RD map is referenced to obtain f_r and f_d, and the distance and velocity are calculated using (2) and (4), respectively.

3 CONVENTIONAL ATTACKS AND COUNTERMEASURES

Fig. 7 shows the concepts of jamming and deception attacks through chirp signals, beat signals, and their spectra. First, jamming and deception attacks are explained based on Fig. 7. Next, interference and jamming countermeasures based on a *detect and repair* approach [40] are described. Countermeasures against deception attacks are discussed in Section 6.1.



(a) Denial jamming attack. **(b) Deception attack.**

Figure 7: Concepts of jamming and deception attacks.

3.1 Jamming Attacks

Jamming attacks aim to make the target undetectable. Denial jamming, as described in [34, 42], uses a slow chirp (or a continuous wave), as shown in Fig. 7(a). Beat signals are observed at the intersections of the transmitted and attack waves, resulting in the application of noise over a wide bandwidth within a short period of time.

3.2 Deception Attacks

Deception attacks aim to cause non-existent targets to become detectable. They can be performed by controlling the transmission timing and phases of the attack waves [14, 33].

Distance deception imitates the reflected waves, as shown in Fig. 7(b). To achieve this, the attacker adjusts a delay t_d to change the transmission timing of the chirp signal. When the relative distance of the attacker from the victim is R_{rel} and the distance he/she wants to deceive is R_{atk}, the delay t_d is as follows:

$$t_d = \begin{cases} \frac{R_{atk}-R_{rel}/2}{c} & (R_{atk} \geq R_{rel}/2) \\ T_s + \frac{R_{atk}-R_{rel}/2}{c} & (R_{atk} < R_{rel}/2) \end{cases}. \tag{5}$$

The term $R_{rel}/2$ incorporates a correction for the actual one-way distance between the attacker and victim.

Velocity deception changes the phase of transmitted waves. When the relative velocity of the attacker from the victim is V_{rel} and the velocity that the attacker wants to deceive with is V_{atk}, the attacker must incrementally rotate the phase by the following unit ϕ_{atk} for each chirp, as follows:

$$\phi_{atk} = \frac{V_{atk} - V_{rel}/2}{V_{max}}\pi = \frac{4T_{sweep}}{\lambda}(V_{atk} - V_{rel}/2)\pi, \tag{6}$$

where V_{max} is the maximum velocity as determined by the radar parameters.

3.3 Jamming Power

In addition to the measurement limit, the maximum possible attack distance is determined by the relationship between the jamming and noise power [11, 31]. The jamming power must be higher than the noise power. Depending on the one-way radio propagation and jammer system, the jamming power can be expressed as

$$P_j = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2 L}, \tag{7}$$

where P_t is the attacker's transmitted power, G_t and G_r are the gains of the Tx and Rx antennas, respectively, λ is the wavelength, R is the distance, and L is the jammer system loss. This means that jamming power depends only on the distance if the attacker's radar system and attack method are fixed.

3.4 Interference and Jamming Countermeasures

Interference countermeasures are applied to each beat signal and detect the features shown in Fig. 7(a). An approach to detect drastic amplitude changes in the time domain by threshold comparison was proposed [27, 29, 32, 37]. Another approach detects the V-shaped frequency transitions in the frequency domain based on filtering [21, 26, 32] or short time Fourier transform (STFT) [8, 25, 41]. Similar methods have been proposed as jamming countermeasures [34, 42] because conventional jamming attacks only intentionally cause interference.

This paper focuses on the following two typical countermeasures. One compares the amplitude of the beat signal to the following threshold [27]: $m_{threshold} = k/N \sum_{i=1}^{N} |m(i)|$, where $m(i)$, N, and k are the beat signal at the i-th sample point, the number of sample points, and a threshold parameter, respectively. The other applies STFT to the beat signal to obtain a spectrogram. Then, peaks are detected by one-dimensional CA-CFAR for each frequency in the spectrogram [41]. Hereinafter, these interference countermeasures are also assumed to be jamming countermeasures and are abbreviated as *AMP* and *STFT*, respectively.

4 COVER CHIRP JAMMING

In this section, we propose cover chirp jamming. Considering the limitations of low-cost attack devices, we also propose a low-cost implementation.

4.1 Attacker Model

The goal of an attacker is to cause the *target* to become undetectable by the *victim*'s radar. The attacker employs cover chirp jamming to circumvent interference countermeasures and to maximize the impact at a constant radio strength. The capabilities of an attacker can be described as follows: The attacker can 1) measure the distances and velocities of the target and victim, 2) obtain the victim's radar parameters, such as F_c, T_s, and B (e.g., via signal analysis [42] or public information [14]), and 3) modify his/her own radar parameters to conduct the deception attack.

4.2 Concept

To successfully jam a modern radar, it is essential to overcome noise suppression achieved by CFAR while avoiding detection by interference countermeasures. Therefore, cover chirp jamming leverages the 2D-FFT algorithm and employs deception attacks to concentrate noise specifically around the target.

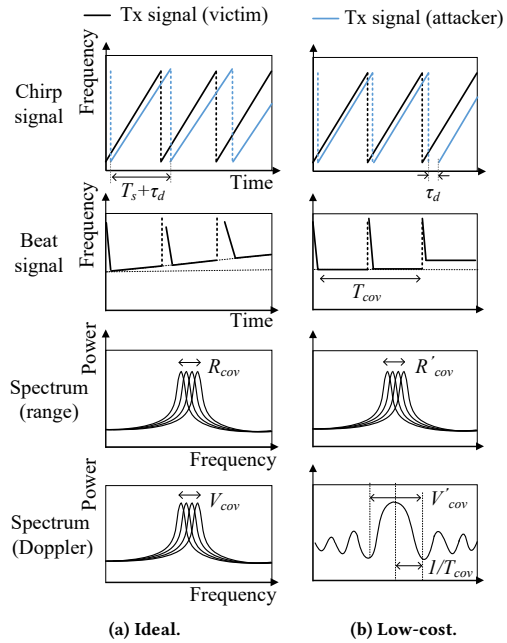


Figure 8: Concepts of cover chirp jamming.

The concept of cover chirp jamming is illustrated in Fig. 8(a), based on chirp signals, beat signals, and spectra. In the proposed attack, the sweep time is set to a value slightly higher than the victim's sweep time ($T_s + \tau_d$). Hence, the beat frequency is time-varying, as shown in the beat signal and spectra in Fig. 8(a). Finally, it is observed as a square noise on the RD map obtained by applying the 2D-FFT to the beat signals.

Cover chirp jamming is more efficient than denial jamming. In cover chirp jamming, beat signals are observed over a long time and in a narrow frequency range, as shown in the beat signal and spectra in Fig. 8(a). However, in denial jamming, the opposite is true. Furthermore, because cover chirp jamming has the same characteristics as deception attacks, it cannot be detected or mitigated by conventional interference and jamming countermeasures as described in Section 3.4. CFAR effectively detects targets in noisy environments and mitigates conventional jamming to some extent [5, 17]. However, targets jammed by cover chirp jamming are difficult to detect because the jamming noise is strong and the energy spread is not recognized by CFAR.

4.3 Ideal Cover Chirp Jamming

Cover chirp jamming is most effective when the center of the noise is aligned with that of the target. To do so, we derive the spectral spread of the range and velocity (R_{cov} and V_{cov}) for a delay of τ_d per chirp, as shown in Fig. 8(a). As the change in range through one frame corresponds to the accumulation of that delay ($\tau = N_c\tau_d$), the following calculation holds:

$$R_{cov} = \frac{c\tau}{2}. \tag{8}$$

Velocity can be calculated from the phase change caused by the delay. The change in frequency due to the delay per chirp can be derived as follows: $f_d = (B/T_s)\tau_d$. Therefore, from (4), the velocity can be derived as follows:

$$V_{cov} = \frac{B}{T_s}\frac{\tau_d\lambda}{2}. \tag{9}$$

Ideal cover chirp jamming requires delay control of the order of 0.1–1 ns for common FMCW radars. Although it is possible to achieve this with an attacker using high-cost equipment, it may not be feasible for radar board-based equipment.

4.4 Low-Cost Cover Chirp Jamming

Common radar boards can only insert delays of the order of 10 ns [6, 35]. The approach to relaxing the delay insertion constraint is to insert a delay only once every multiple iteration so that the same amount of delay is inserted in a total of one frame. The low-cost cover chirp jamming concept is shown in Fig. 8(b). The beat signal in Fig. 8(b) indicates that multiple targets with the frame time T_{cov} appear. Such a beat signal can be regarded as a pulse and appears as a sinc function when the FFT is applied. The frequency at which the n-th valley of the sinc function depends on the pulse width (T_{cov}) and can be calculated as $f(n) = \pm n/T_{cov}$.

Based on the above observations, we can derive the spectral spread. Given that one delay is inserted for every N_{step} chirp, the total delay and pulse widths are $\tau = \lfloor N_f/N_{step} \rfloor \tau_d$ and $T_{cov} = N_{step}T_s$, respectively, where $\lfloor\rfloor$ is the floor function. The range coverage is the same as in the ideal and can be derived as follows:

$$R'_{cov} = \frac{c\tau}{2}. \tag{10}$$

The velocity coverage depends on the pulse width and can be derived as follows:

$$V'_{cov} = \frac{\lambda}{T_{cov}} = \frac{\lambda}{N_{step}T_s}. \tag{11}$$

4.5 Attack Flow

The overall attack flow of cover chirp jamming can be divided into three steps, as shown in Fig. 9. 1) In the intelligence-gathering step, the attacker determines the area to be covered by measuring the distances and velocities of objects in the surrounding environment, including the victim and target. 2) Synchronization involves only receiving and changing the transmission timing until the victim's transmission signal is observed in ADC data. 3) In the attack, the attacker applies cover chirp jamming and spreads noise around the target in the victim's RD map. If the victim's signal is no longer observable in the ADC data, the attacker begins to resynchronize.

The specific deception distance and velocity (R_{atk} and V_{atk}) required to achieve cover chirp jamming can be calculated as follows:

$$R_{atk} = R_{tgt} - R_{cov}/2, \tag{12}$$
$$V_{atk} = V_{tgt} - V_{cov}/2, \tag{13}$$

where R_{tgt} and V_{tgt} are the range and velocity of the target to the victim, respectively. Namely, in the deception attack of R_{atk} and V_{atk}, the cover chirp jamming around R_{tgt} and V_{tgt} is realized by accumulating the time shifts caused by the slight delay τ_d for one frame.

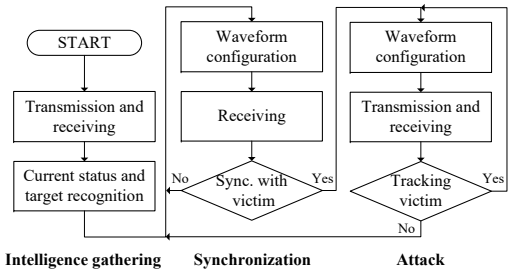
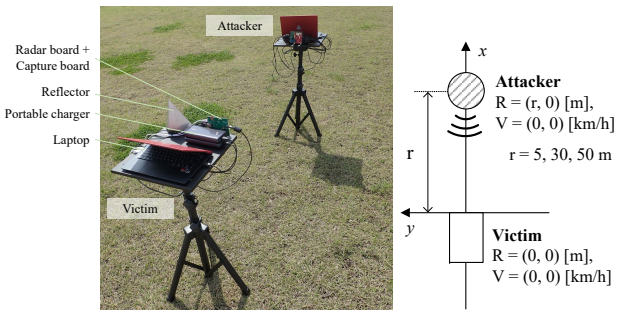
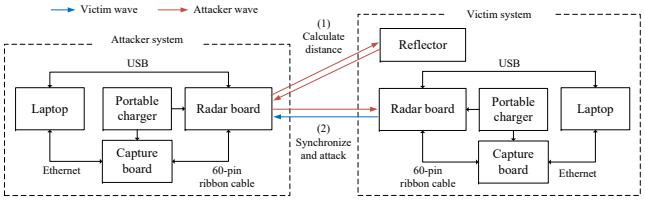


Figure 9: Overall attack flow of cover chirp jamming.

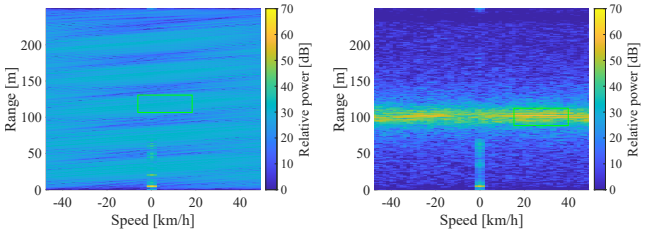


(a) Overview. **(b) Conditions.**



(c) Hardware configuration.

Figure 10: Field experimental setup.



(a) Denial jamming. **(b) Low-cost cover chirp jamming.**

Figure 11: RD map calculated under jamming attack when $r = 5$. The green frame indicates the jamming area calculated from (10) and (11). The same jamming area size is set for denial jamming.

5 ATTACK EXPERIMENTS

This section describes two experiments: 1) field experiments using radar boards and 2) simulation experiments using field experiment data. Field experiments demonstrated the feasibility and effectiveness of the proposed attack. Simulation experiments relaxed the constraints of the field environment and the radar board to qualitatively evaluate the attacks under a variety of conditions. For example, the signal-to-noise ratio (SNR) of a target can be kept constant, or a long-distance attack on a moving object can be simulated. The theoretical verification is presented in Appendix A.

5.1 Field Experiments

These experiments demonstrated that cover chirp jamming is feasible with radar board-based equipment, can bypass typical interference countermeasures (i.e., AMP and STFT), and is more efficient than denial jamming.

5.1.1 Setup.

Figs. 10(a), (b), and (c) show the overview, conditions, and hardware configuration of the field experiments, respectively. The radar system consisted of a radar board (TI AWR1843BOOST), data capture board (TI DCA1000EVM), laptop, and portable charger. The radar board operates with 2Tx–4Rx time-division multiplexing (TDM)-MIMO (See Appendix B for TDM-MIMO). A reflector exists in the victim system to enable the attacker to measure the distance between them.

The distance of the attacker varies from 5 to 50 m as shown in Fig. 10(b). Here, both the victim and the attacker were stationary. The attacker set the deception distance as $R_{tgt} = 100$ m. No velocity deception was performed due to the controllability constraints of the radar board.

The radar parameters and interference countermeasure parameters are shown in Tables 2 and 3 in Appendix C, respectively. Denial jamming used a continuous wave with the center frequency of the target FMCW radar. As low-cost cover chirp jamming, the tiny delay was set to $\tau_d = 10$ ns owing to the specification of the radar board. The delay insertion step was experimentally set to $N_{step} = 8$.

5.1.2 Result.

Feasibility demonstration. Fig. 11 shows the RD map observed on the victim radar board under denial jamming and low-cost cover-chirp jamming. It represents the jamming power relative to the noise floor without attack, i.e., jamming-to-noise ratio (JNR). Fig. 11(a) shows that denial jamming caused a weak spread of noise. Fig. 11(b) shows that low-cost cover chirp jamming can adaptively concentrate jamming noise on R_{tgt}.The diffusion in the velocity direction can be caused by the shape of the sinc function (cf. Figs. 8(b)) and the variation in the phase of the attacking wave.

Stealth evaluation. Fig. 12 presents the results of interference detection with five attacks conducted at each distance. The results show that denial jamming was detected by both countermeasures, whereas cover chirp jamming was not detected at all. The results also show that 1) STFT had better detection performance than AMP, 2) the number of detections dropped with attack distance, i.e., jamming power.

To provide a more detailed analysis, Figs. 13 and 14 illustrate the behavior of AMP and STFT, respectively, at r=5. Fig. 13 shows that only the interfered waveform (#1 under denial jamming) exceeded the threshold. Fig. 13(b) shows that the high thresholds were set because cover chirp jamming was always sinusoidal. Figs. 14(a) and (b) show that energy across frequencies caused by denial jamming was detected by CFAR. Figs. 14(c) and (d) show that cover chirp jamming was not detected because a single waveform could not distinguished an attack from a true target.

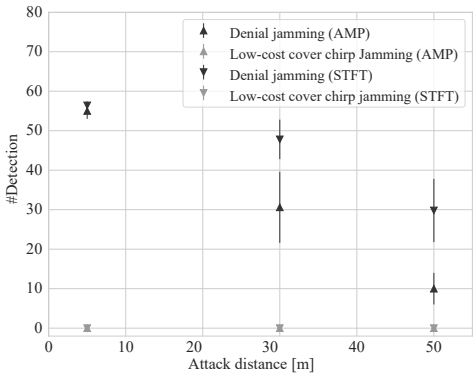
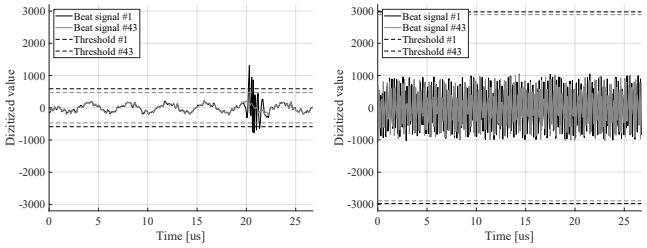


Figure 12: Interference detection result. The number of interfered waveforms detected from the 64 waveforms after MIMO demodulation is shown with error bars.



(a) Denial jamming. **(b) Low-cost cover chirp jamming.**

Figure 13: Beat signal based on field experiments when the attacker is 5 m away from the victim. The 1st and 43rd waveforms and detection thresholds are shown.

In order to compare the fundamental performance with conventional jamming attacks, we excluded the detection (and mitigation) by countermeasures in the subsequent analysis.

Efficiency evaluation. Fig. 15 shows the JNR for jamming attacks at distances of 5, 30, and 50 m. The average of 5 trials (frames) was used for the JNR calculation. Fig. 15 shows that the power of the low-cost cover chirp jamming was 17.4 dB higher than that of denial jamming.

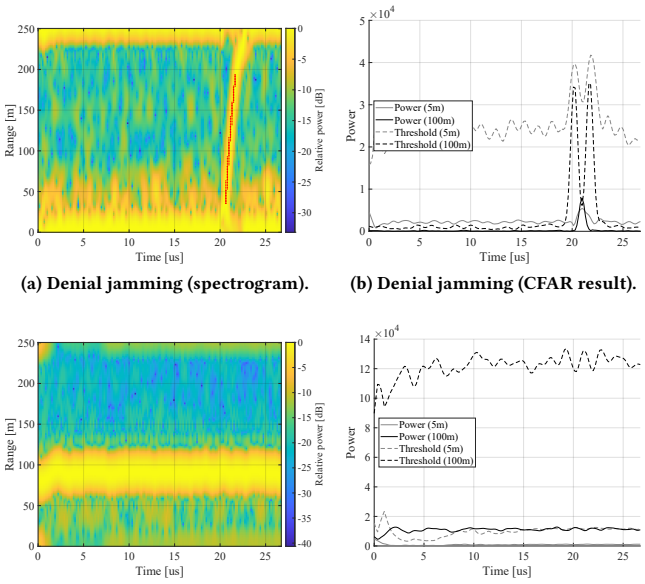
5.2 Simulation

The effect of the attacker's distance on object detection was investigated in this experiment.

5.2.1 Setup.

Fig. 16 shows the simulation configuration including a radar system, measurement objects, noise, and two attack channels. The simulation experiments used attack channel 2, whereas the theoretical verification used attack channel 1 (see Appendix A). White Gaussian noise (WGN) maintained the SNR at 30 dB.

The JNR was adjusted to 5–200 m based on the experimental fitting results shown in Fig. 15. A detection target was generated at the center of the jamming area of the jammed data to imitate the condition in which the impact of the attack was maximized. See Appendix D for examples of received signals simulating attacks based on field experiment data.



(a) Denial jamming (spectrogram). **(b) Denial jamming (CFAR result).**

(c) Low-cost cover chirp jamming (spectrogram). **(d) Low-cost cover chirp jamming (CFAR result).**

Figure 14: Spectrogram for the 1st waveform and interference detection results when the attacker is 5 m away from the victim. Red dots in the spectrogram indicate CFAR detection areas. CFAR results for the frequencies of 5 and 100 m of the spectrogram are shown.

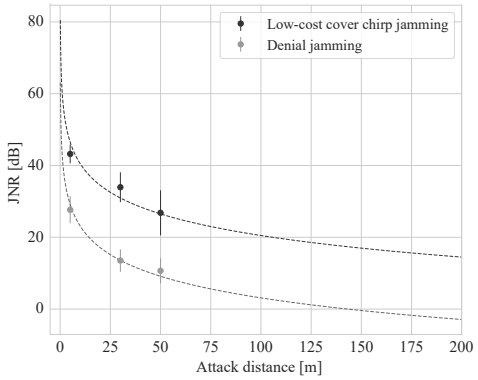


Figure 15: Jamming-to-noise ratio (JNR) vs. attack distance in the field experiment. Dots represent measured value on the radar board, and dotted lines are theoretical values fitted to (7).

5.2.2 Result.

Impact on object detection. Fig. 17 shows the measurement errors from the true values of the target, as detected using CFAR and DBSCAN. The results show that object detection is effective at 20 m (JNR: 17.1 dB) and 175 m (JNR: 14.5 dB) under denial jamming and low-cost cover-chirp jamming, respectively. The results also show that 1) if an object is detectable, the measurement error is small and 2) detectability is not determined by the JNR alone. The noise density could be the reason that the cover chirp jamming succeeded in making the target undetectable at a lower JNR.

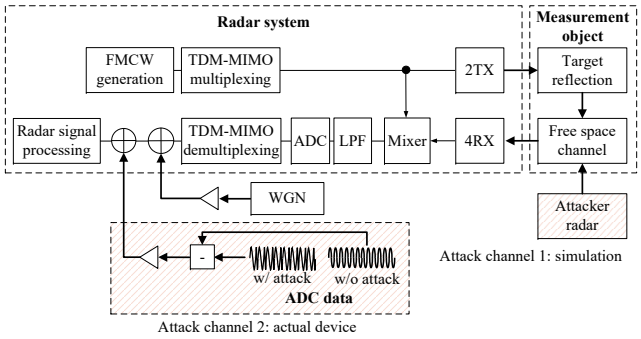


Figure 16: Simulation configuration including two attack channels: attack channel 1 implemented in MATLAB and attack channel 2 used real ADC data measured in the field experiment.

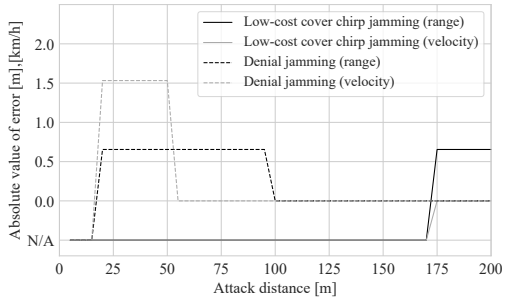


Figure 17: Measurement error of detected target under 30-dB SNR vs. attack distance. The detection result at no attack is set as the true value. In case of no detection, the value is set to N/A (not applicable).

6 COUNTERMEASURES

This section proposes a countermeasure against cover chirp jamming.

6.1 Concept and Related Work

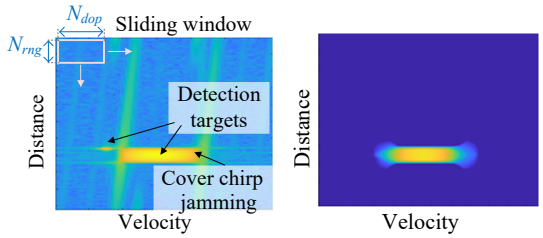
There are two types of countermeasures against cover chirp jamming: One aims to prevent deception attacks, and the other aims to detect and mitigate jamming attacks. Because cover chirp jamming utilizes deception techniques, countermeasures against deception attacks are effective.

The existing deception countermeasures have certain limitations. Randomizing waveforms, i.e., the FMCW parameters, prevents attack signals from mixing [4, 7, 12, 15, 20, 22, 24, 33, 34, 36]. This approach only applies to some types of FMCW radars due to hardware requirements and degrades measurement performance [38]. Another approach uses waveform fingerprinting to detect anomalous beat signals [33]. However, no mitigation method is indicated, and naively discarding deception data would accomplish the goal of jamming.

Based on the above observations, this study proposes a countermeasure focused on the attack features of cover chirp jamming. Our countermeasure detects and mitigates attacks from the jammed ADC data. It has the advantage that it can be implemented for signal processing, regardless of the radar specifications. Our method

Algorithm 1 Detect cover chirp jamming.

Input: $\boldsymbol{s_b}, N_{rng}, N_{dop}, th_{pow}, N_{th}$
Output: $detect$
1: $\boldsymbol{RD} = pow(2DFFT(\boldsymbol{s_b}, N_{rFFT}, N_{dFFT}))$; $N_{rFFT} \times N_{dFFT}$
2: **for** $0 \leq i < N_{rFFT} - N_{rng}$ **do**
3: **for** $0 \leq j < N_{dFFT} - N_{dop}$ **do**
4: $\boldsymbol{M}[i][j] \leftarrow median(\boldsymbol{RD}[i : i + N_{rng}][j : j + N_{dop}])$
5: **end for**
6: **end for**
7: **if** $(sum(\boldsymbol{M} > th_{pow}) > N_{th})$ **then**
8: $detect \leftarrow true$
9: **else**
10: $detect \leftarrow false$
11: **end if**



(a) RD map under attack. **(b) Median processing result.**

Figure 18: Detect cover chirp jamming.

is also threshold-based detection, but it compares the RD map to a threshold value rather than a single beat signal as in existing interference countermeasures. In mitigation, the attack signal is filtered by focusing on the frequency change of the false target with the time transition.

6.2 Proposed Method

6.2.1 *Attack Detection.*

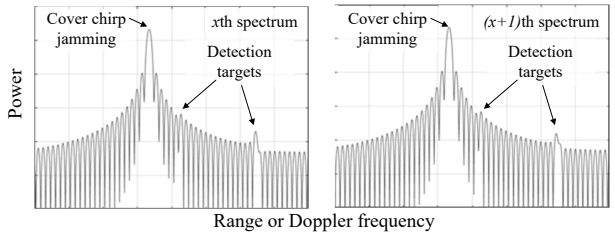
The attack detection algorithm is explained in Algorithm 1, and the concept is shown in Fig. 18. In the algorithm, bold and normal values represent arrays and variables, respectively (e.g., $\boldsymbol{s_b}$ and N_{rng}). First, a 2D-FFT is applied to the beat signal of one frame $\boldsymbol{s_b}$ and is converted into a power spectrum (Line 1). Then, the RD map is scanned with a window of size defined by N_{rng} and N_{dop}, and the median value is recorded (Lines 2–6). As the target energy has a much smaller spread than that of the cover chirp jamming (Fig. 18(a)), false positives can be prevented by setting the appropriate window size. Finally, we count the number of extracted median values exceeding the threshold th_{pow} (Fig. 18(b)). If this number exceeds the threshold N_{th}, an attack is detected (Lines 7–11).

6.2.2 *Target Signal Extraction.*

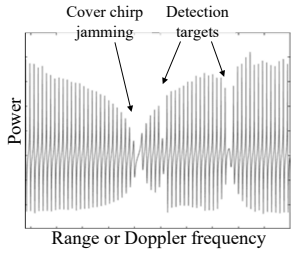
The signal extraction algorithm is described in Algorithm 2, and the concept is illustrated in Fig. 19. This process is separately applied to the range and Doppler frequencies. First, the range- or Doppler-FFT is applied to the beat signal in one frame unit $\boldsymbol{s_b}$ and is converted to a power spectrum of N_{FFT} points (Line 1). Then, we record the differences between adjacent power spectra for *span* waveforms (Lines 2–4 and Figs. 19(a) and (b), where N_{sample} represents the sample points of the beat signal). This operation is repeated for

Algorithm 2 Extract target signal.

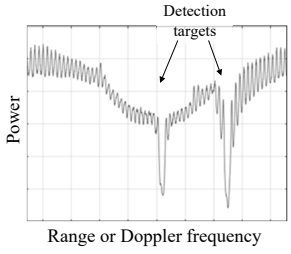
Input: $s_b, N_{FFT}, span, pt_{av}$
Output: f
1: $S_b = pow(FFT(s_b, N_{FFT}))$; $N_{FFT} \times N_c$ (or N_{sample})
2: **for** $0 \leq i < N_{trace} - span$ **do**
3: $X[i] \leftarrow S_b[:][i] - S_b[:][i + span]$; [:] means all data
4: **end for**
5: $M \leftarrow move\_average(std(X), pt_{av})$
6: $f \leftarrow peak\_detection(M)$



(a) Two adjacent power spectra ($span = 1$).



(b) Difference between the two power spectra shown in Fig. 19(a).



(c) Standard deviation and moving average of Fig. 19(b).

Figure 19: Extract target signal.

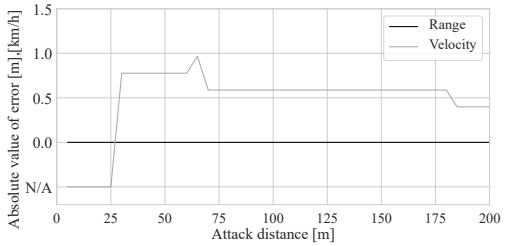


Figure 20: Measurement error of detected target under 30-dB SNR vs. attack distance with the countermeasure. In case of no detection, the value is set to N/A.

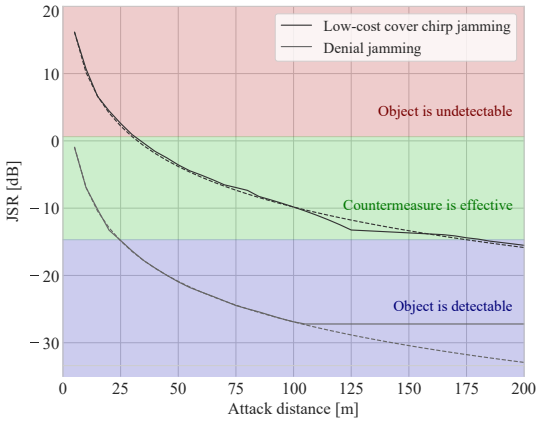


Figure 21: Jamming-to-signal ratio (JSR) vs. attack distance under 30-dB SNR. The solid line represents simulated data and dotted line represents theoretical values fitted to (7).

all spectra. Next, we calculate the standard deviation of the obtained power spectral differences and apply a moving average with a width of pt_{av} (Line 5). This enables the extraction of only the target signal, with less time variance (Fig. 19(c)). Finally, the peak points corresponding to the target's range or Doppler frequency are extracted (Line 6). Notably, peak detection also has parameters, but they are omitted here.

6.3 Experiment

Countermeasures were applied to the jammed data used in Section 5.2.2. Table 4 in Appendix C lists the experimentally obtained countermeasure parameters.

Fig. 20 shows the measurement errors of the target extracted by applying this countermeasure. The results indicate that the target can be detected with a small error from 30 m onward. The small velocity error comes from the difference in the number of FFT points between normal radar signal processing ($N_{dFFT} = 64$) and the countermeasure ($N_{FFT} = 512$). In addition, it was confirmed that cover chirp jamming was not falsely detected for the data of no attack and under denial jamming. See Appendix D for a demonstration of target signal extraction.

Based on the results of Sections 5.2.2 and 6.3, the effective ranges of the attacks and countermeasures are summarized in Fig. 21 in terms of the attacker capability over the victim, that is, the jamming-to-signal ratio (JSR). The impact of an attack decreases with increasing distance from the attacker in a 30-dB SNR environment. Above 110 m, the ambient noise becomes dominant over the denial jamming and saturates at around -30 dB, which is the inverse of the 30-dB SNR.

Fig. 21 shows the following: 1) up to 30 m (JSR: 0.6 dB), cover chirp jamming cannot be prevented; 2) from 30 to 175 m (JSR: 0.6 to -14.7 dB), the object is detectable with a small error owing to the proposed countermeasure; 3) from 175 m (JSR: -14.7 dB) and beyond, the attacks have no effect even without a countermeasure.

Fig. 21 can generally be used to predict the impact of an attack. The JSR is offset according to the SNR of the target and the ability of the attacker (cf. (7)). For example, a positive offset is applied to Fig. 21 if the attacker's transmit power is high or the SNR is low. In other words, the distance until the target is detectable increases.

7 CONCLUSION

In this study, we proposed a novel jamming attack against a commercial millimeter-wave FMCW radar. The feasibility, stealth, and efficiency of the proposed attack were demonstrated through field experiments and simulations. Experimental results showed that cover chirp jamming is 17.4 dB more efficient than denial jamming and can bypass the CFAR and conventional interference and

jamming countermeasures. Moreover, we proposed a countermeasure to detect the proposed attack and extract the signal from the jammed data. We showed that the countermeasure works when JSR is less than 0.6 dB and has no false positives when no attack occurs.

Future work will include 1) evaluation under sensor fusion, 2) evaluation in more complex scenarios, 3) discussion of feasibility in terms of attack time (cf. Fig 9) and attack scenarios, 4) discussion of attacks that bypass the proposed countermeasures, 5) and verification of the effectiveness of the proposed attacks on advanced interference countermeasures such as threshold-free [39]. In this study, attacks on a single radar were assumed to provide a basic evaluation of cover chirp jamming. It is necessary to evaluate the impact on the system when measurements from multiple radars or different sensors are combined. We also need to demonstrate the effectiveness of the countermeasure in scenarios such as the emergency braking of autonomous vehicles under jamming attacks.

ACKNOWLEDGMENTS

This work is partially based on results obtained from the project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

REFERENCES

[1] Mostafa Alizadeh, George Shaker, João Carlos Martins De Almeida, Plinio Pelegrini Morita, and Safeddin Safavi-Naeini. 2019. Remote Monitoring of Human Vital Signs Using mm-Wave FMCW Radar. *IEEE Access* 7 (2019), 54958–54968.

[2] Francesco Belfiori, Wim van Rossum, and Peter Hoogeboom. 2012. Random transmission scheme approach for a FMCW TDMA coherent MIMO radar. In *2012 IEEE Radar Conference*. IEEE, 0178–0183.

[3] Alper Cemil and Mehmet Ünlü. 2022. Analysis of ADAS Radars with Electronic Warfare Perspective. *Sensors* 22, 16 (2022), 6142.

[4] Ruchir Chauhan. 2014. *A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar.* Master's thesis. Utah State University.

[5] Det8, ACC TRSS. 2000. ELECTRONIC WARFARE FUNDAMENTALS.

[6] ANALOG DEVICES. 2023. EVAL-DEMORAD Evaluation Board. https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/eval-demorad.html. Access 8 June 2023.

[7] Raj Gautam Dutta, Xiaolong Guo, Teng Zhang, Kevin Kwiat, Charles Kamhoua, Laurent Njilla, and Yier Jin. 2017. Estimation of Safe Sensor Measurements of Autonomous System Under Attack. In *Proceedings of the 54th Annual Design Automation Conference 2017*. 1–6.

[8] Christoph Fischer, Hans Ludwig Blöcher, Jürgen Dickmann, and Wolfgang Menzel. 2015. Robust Detection and Mitigation of Mutual Interference in Automotive Radar. In *2015 16th International Radar Symposium (IRS)*. IEEE, 143–148.

[9] Soori Im, Donghoon Kim, Hoiyoung Cheon, and Jaekwan Ryu. 2021. Object Detection and Tracking System with Improved DBSCAN Clustering using Radar on Unmanned Surface Vehicle. In *2021 21st International Conference on Control, Automation and Systems (ICCAS)*. IEEE, 868–872.

[10] ITU-T. 2018. *Recommendation ITU-R M.2057-1: Systems characteristics of automotive radars operating in the frequency band 76-81 GHz for intelligent transport systems applications.* Technical Report. International Telecommunication Union.

[11] Mohinder Jankiraman. 2018. *FMCW Radar Design.* Artech House.

[12] Prateek Kapoor, Ankur Vora, and Kyoung-Don Kang. 2018. Detecting and Mitigating Spoofing Attack Against an Automotive Radar. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 1–6.

[13] Eun Hee Kim and Ki Hyun Kim. 2018. Random phase code for automotive MIMO radars using combined frequency shift keying-linear FMCW waveform. *IET Radar, Sonar & Navigation* 12, 10 (2018), 1090–1095.

[14] Rony Komissarov and Avishai Wool. 2021. Spoofing Attacks Against Vehicular FMCW Radar. In *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*. 91–97.

[15] Antonio Lazaro, Arnau Porcel, Marc Lazaro, Ramon Villarino, and David Girbau. 2022. Spoofing Attacks on FMCW Radars with Low-Cost Backscatter Tags. *Sensors* 22, 6 (2022), 2145.

[16] Sohee Lim, Seongwook Lee, and Seong-Cheol Kim. 2018. Clustering of detected targets using DBSCAN in automotive radar systems. In *2018 19th international radar symposium (IRS)*. IEEE, 1–7.

[17] Wei Liu, Jin Meng, and Liang Zhou. 2019. Impact analysis of DRFM-based active jamming to radar detection efficiency. *The Journal of Engineering* 2019, 20 (2019), 6856–6858.

[18] Steffen Lutz, Daniel Ellenrieder, Thomas Walter, and Robert Weigel. 2014. On fast chirp modulations and compressed sensing for automotive radar applications. In *2014 15th International Radar Symposium (IRS)*. IEEE, 1–6.

[19] MathWorks. 2023. Radar Signal Simulation and Processing for Automated Driving. https://www.mathworks.com/help/driving/ug/radar-signal-simulation-and-processing-for-automated-driving.html. Access 5 June 2023.

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

[21] Sriram Murali, Karthik Subburaj, Brian Ginsburg, and Karthik Ramasubramanian. 2018. Interference Detection in FMCW Radar Using A Complex Baseband Oversampled Receiver. In *2018 IEEE Radar Conference (RadarConf18)*. IEEE, 1567–1572.

[22] Prateek Nallabolu and Changzhi Li. 2021. A Frequency-Domain Spoofing Attack on FMCW Radars and Its Mitigation Technique Based on a Hybrid-Chirp Waveform. *IEEE Transactions on Microwave Theory and Techniques* 69, 11 (2021), 5086–5098.

[23] Prateek Nallabolu, Daniel Rodriguez, and Changzhi Li. 2022. Emulation and Malicious Attacks to Doppler and FMCW Radars for Human Sensing Applications. *IEEE Transactions on Microwave Theory and Techniques* (2022).

[24] Shoei Nashimoto, Daisuke Suzuki, Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, and Makoto Nagata. 2021. Low-cost distance-spoofing attack on FMCW radar and its feasibility study on countermeasure. *Journal of Cryptographic Engineering* (2021), 1–10.

[25] Sharef Neemat, Oleg Krasnov, and Alexander Yarovoy. 2018. An Interference Mitigation Technique for FMCW Radar Using Beat-Frequencies Interpolation in the STFT Domain. *IEEE Transactions on Microwave Theory and Techniques* 67, 3 (2018), 1207–1220.

[26] Fatemeh Norouzian, Anum Pirkani, Edward Hoare, Mikhail Cherniakov, and Marina Gashinova. 2021. Phenomenology of automotive radar interference. *IET Radar, Sonar & Navigation* 15, 9 (2021), 1045–1060.

[27] Takuya Nozawa, Yuya Makino, Nobuyuki Takaya, Masahiro Umehira, Shigeki Takeda, Xiaoyan Wang, and Hiroshi Kuroda. 2017. An Anti-collision Automotive FMCW Radar Using Time-domain Interference Detection and Suppression. (2017), 1–5.

[28] Zhengyu Peng and Changzhi Li. 2019. Portable microwave radar systems for short-range localization and life tracking: A review. *Sensors* 19, 5 (2019), 1136.

[29] Muhammad Rameez, Mats I Pettersson, and Mattias Dahl. 2022. Interference Compression and Mitigation for Automotive FMCW Radar Systems. *IEEE Sensors Journal* 22, 20 (2022), 19739–19749.

[30] Sandeep Rao. 2017. Introduction to mmWave sensing: FMCW radars. *Texas Instruments (TI) mmWave Training Series* (2017), 1–11.

[31] Mark A Richards. 2014. *Fundamentals of radar signal processing.* McGraw-Hill Education.

[32] Sasanka Sanka. 2017. *RADAR to RADAR Interference for 77GHz Automotive RADARs.* Master's thesis. Delft University of Technology.

[33] Zhi Sun, Sarankumar Balakrishnan, Lu Su, Arupjyoti Bhuyan, Pu Wang, and Chunming Qiao. 2021. Who Is in Control? Practical Physical Layer Attack and Defense for mmWave-Based Sensing in Autonomous Vehicles. *IEEE Transactions on Information Forensics and Security* 16 (2021), 3199–3214.

[34] Sefa Tanis. 2019. Automotive Radar and Congested Spectrum: Potential Urban Electronic Battlefield. *MICROWAVE JOURNAL* 62, 1 (2019), 48–+.

[35] Texas Instruments. 2023. AWR1243. https://www.ti.com/product/AWR1243. Access 5 June 2023.

[36] Onur Toker and Suleiman Alsweiss. 2020. Design of a Cyberattack Resilient 77 GHz Automotive Radar Sensor. *Electronics* 9, 4 (2020), 573.

[37] Masahiro Umehira, Takuya nozawa, Yuya makiko, wang Xiaoyan, Shigeki takeda, and Hiroshi kuroda. 2018. A Novel Iterative Inter-Radar Interference Reduction Scheme for Densely Deployed Automotive FMCW Radars. In *2018 19th International Radar Symposium (IRS)*. IEEE, 1–10.

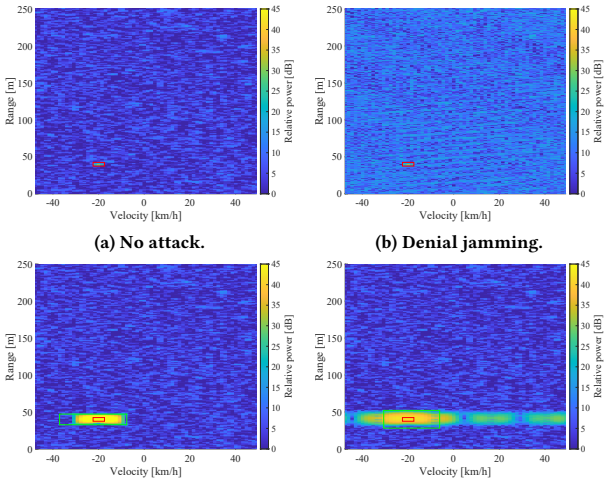
[38] Minh A Vu, William C Headley, and Kevin P Heaslip. 2022. A Comparative Overview of Automotive Radar Spoofing Countermeasures. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 245–252.

[39] Matthias Wagner, Fisnik Sulejmani, Alexander Melzer, Paul Meissner, and Mario Huemer. 2018. Threshold-Free Interference Cancellation Method for Automotive FMCW Radar Systems. In *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 1–4.

[40] Christian Waldschmidt, Juergen Hasch, and Wolfgang Menzel. 2021. Automotive Radar–From First Efforts to Future Systems. *IEEE Journal of Microwaves* 1, 1 (2021), 135–148.

[41] Jianping Wang. 2021. CFAR-Based Interference Mitigation for FMCW Automotive Radar Systems. *IEEE Transactions on Intelligent Transportation Systems* 23, 8 (2021), 12229–12238.

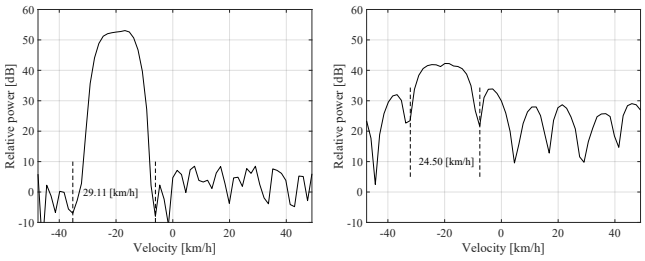
[42] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle. *DEF CON* 24 (2016).



(a) No attack. (b) Denial jamming.

(c) Ideal cover chirp jamming. (d) Low-cost cover chirp jamming.

Figure 22: RD map from the simulation experiment under 30-dB SNR. Red and green frames indicate target and jamming areas, respectively.



(a) Ideal cover chirp jamming. (b) Low-cost cover chirp jamming.

Figure 23: Doppler spectrum at $R = 40$ obtained from Fig. 22.

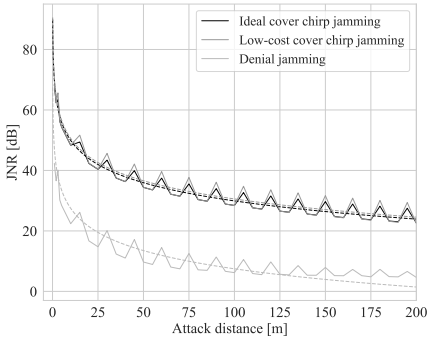


Figure 24: JNR vs. attack distance in the simulation experiment. The solid line represents simulated data and dotted line represents theoretical values fitted to (7).

A THEORETICAL VERIFICATION

This experiment verified the theory of noise spreading for cover chirp jamming according to (8)–(11).

A.1 Setup

This experiment used a simulation configuration with attack channel 1, as illustrated in Fig. 16. The basic conditions were the same as in the field experiment in Fig. 10(b); however, the distance and velocity of the attacker were changed as follows: $R = (40, 0), V = (20, 0)$.

Denial jamming used a FMCW waveform with a sweep time of 4 ms due to the limitations of the FMCW function in MATLAB. The low-cost cover chirp jamming waveform is the same as that used in Section 5.1. The tiny delay was set to $\tau = 0.75$ ns for ideal cover chirp jamming. This value was set to be close to the jamming area of the low-cost cover chirp jamming.

A.2 Result

Theoretical verification. The RD maps with and without jamming attacks are shown in Fig. 22. Cover chirp jamming applied noise such that the target, i.e., the attacker, was centered. The green frame for the cover chirp jamming was calculated using (8)–(11) and indicated the location in the RD map where the average power in the frame was the largest.

Fig. 22 shows the following: 1) denial jamming spreads energy over a wide area; 2) the noise of the cover chirp jamming spreads theoretically according to the position and size of the green frame representing the jamming area; and 3) low-cost cover chirp jamming diffuses energy in the velocity direction relative to the ideal one.

For the detailed verification of the velocity coverage, the Doppler spectra of Figs. 22(c) and (d) at $R = 40$ are shown in Figs. 23(a) and (b), respectively. The velocity coverages calculated from (9) and (11) are $V_{cov} = 29.42$ and $V'_{cov} = 24.51$ km/h, respectively, which are very close to those in Fig. 23.

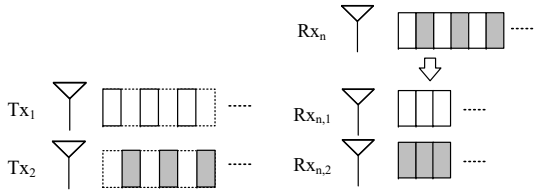
Efficiency evaluation. Fig. 24 shows the JNR of each jamming attack when varying the distance from 5 to 200 m. It shows the following: 1) there is little difference between the average powers of the two types of cover chirp jamming, 2) the JNR of cover chirp jamming is 22.5 dB higher than that of denial jamming, and 3) the attenuation follows the theory. The fluctuation of the JNR is considered to be an effect of the phase interference between the signals of the attacker and victim.

Similar results to the field experiment (cf. Fig 15) were obtained, but the JNR was higher in the simulation for both jamming attacks. This can be explained by differences in conditions, such as the strength of the attacker's radio signal.

B MULTI-INPUT MULTI-OUTPUT PROCESSING

MIMO processing enhances the angle-of-arrival resolution and is common in modern FMCW radars. In particular, TDM-MIMO is often used due to the ease of hardware configuration and processing [2, 13, 35]. Although the angle deception is out of the study focus, we briefly describe TDM processing.

Figs. 25(a) and (b) depict the transmission and receiving processes for TDM, respectively. The TDM switches the transmission antennas individually (Tx_1 and Tx_2). As the transmission waves are received alternately by each receiving antenna, demultiplexing processing is required to sort them chronologically. This means that the number of receiving antennas is virtually increased, thereby increasing the aperture length and improving the angular resolution.



(a) Transmission (multiplexing). (b) Receiving (demultiplexing).

Figure 25: Time-division multiplexing (TDM)-MIMO.

Table 2: Radar and signal processing parameters.

Parameter	Value
Performance	
Maximum range	250 m
Range resolution	0.75 m
Maximum velocity	49 km/h
Velocity resolution	0.77 km/h
Chirp	
Center frequency (F_c)	77.120 GHz
Bandwidth (B)	200 MHz
Sweep time (T_c)	30.74 us
Idle time	5.0 µs
#chirp in one frame (N_c)	128
Radar signal processing	
Sampling frequency	12.5 MHz
#range FFT (N_{rFFT})	512
#Doppler FFT (N_{dFFT})	64
CFAR guard cell (R, D)*	4, 4
CFAR training cell (R, D)	4, 4
Probability of false alarm	1^{-6}

*: (R, D) signify (range, Doppler).

Table 3: Interference countermeasure parameters.

Parameter	Value
Amplitude detection	
k	5
STFT and CA-CFAR	
N_{FFT}	128
#overlap	14
Window size	16
Guard cell	4
Training cell	8
Probability of false alarm	1^{-3}

Table 4: Proposed countermeasure parameters.

Parameter	Value
Attack detection	
N_{rng}	42
N_{dop}	20
th_{pow}	octiles
N_{th}	$N_{rng} \times N_{dop}/2$
Target signal extraction	
N_{FFT} (R, D)*	512, 512
$span$ (R, D)	36, 4
pt_{av} (R, D)	4, 2

*: (R, D) signify (range, Doppler).

C RADAR PARAMETER

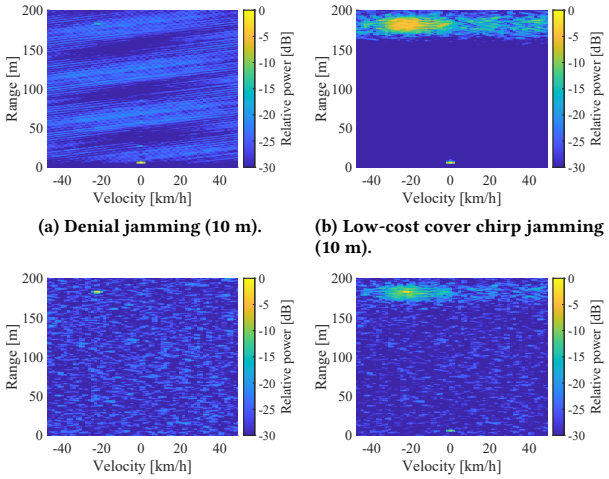
Table 2 lists the parameters of the radar and signal processing. The parameters refer to Radar A in [10]. Table 3 lists the parameters of conventional interference countermeasures used in Section 5. Table 4 lists the parameters of the proposed countermeasure used in Section 6.3.

D HYBRID SIMULATION

This section presents simulation data based on actual equipment data and the operation of the proposed countermeasures.

D.1 Hybrid Data

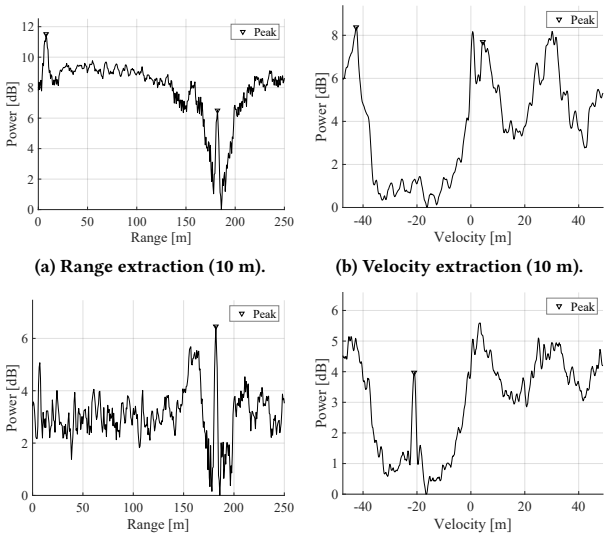
As shown in Fig. 16, the hybrid data was generated by simulating a SNR-tuned target and combining it with JNR-tuned ADC data obtained from field experiments. Fig. 26 shows the RD map calculated from the hybrid data at attacker distances R = 10 and 150 m under denial jamming and low-cost cover chirp jamming. As the cover chirp jamming data at R_{tgt} = 182 m and V_{tgt} = −22 km/h was adopted, a target was generated at this location. Figs. 26(b) and (d) indicate a slight change in the noise floor, i.e., noise outside the jamming region. Nevertheless, this change does not pose a concern as it does not alter the relation between the power of the target and the jamming noise.



(a) Denial jamming (10 m). (b) Low-cost cover chirp jamming (10 m).

(c) Denial jamming (150 m). (d) Low-cost cover chirp jamming (150m).

Figure 26: RD map calculated from simulation data based on field experiment data. Attacker distances are 10 and 150 m.



(a) Range extraction (10 m). (b) Velocity extraction (10 m).

(c) Range extraction (150 m). (d) Velocity extraction (150 m).

Figure 27: Target signal extraction results under attacker distances of 10 and 150 m.

D.2 Details of Signal Extraction

Fig. 27 shows the results of range and velocity signal extraction based on the proposed countermeasures for the hybrid data shown in Fig. 26. Note that Fig. 27 shows the same process as Fig. 19(c), but upside down for peak detection.

Figs. 27(a) and (c) demonstrate the successful extraction of the target distance (182 m) at all attack distances. Meanwhile, Figs. 27(b) and (d) demonstrate that the target velocity (-22 km/h) cannot be extracted at 10 m attacker distance.