International Journal of Microwave and Wireless Technologies, 2017, 9(9), 1853–1861.
doi:10.1017/S1759078717000708

TUTORIAL AND REVIEW PAPER

A review of self-protection deceptive jamming against chirp radars

SAMER BAHER SAFA HANBALI AND RADWAN KASTANTIN

The well-known range-Doppler coupling property of the chirp radar makes it more vulnerable to different types of deceptive repeater jammers that benefit from the pulse compression processing gain of the radar-matched filter. These jammers generate many false targets that appear before and after the true target. Therefore, the radar cannot distinguish the true target from the false ones. This paper reviews different self-protection repeater jammers and presents their pros and cons, in order to provide a reference for the study of jamming/anti-jamming methods.

Keywords: Frequency-shifting jamming, Interrupted-sampling, Repeater jamming, Echo suppression, ECCM

Received 2 March 2017; Revised 2 June 2017; Accepted 10 June 2017; first published online 17 July 2017

I. INTRODUCTION

Chirp waveform is one of the most used signals in radars due to its high Doppler tolerance [1], but chirp radars are vulnerable to active jamming, which is the process of transmitting interfering signals toward the victim radar with the objective of degrading its ability to detect targets or to make it obtain wrong information about them. According to the jamming topology, we can distinguish between self-protection and stand-off jammers. In self-protection topology, the jammer is carried by the same vehicle or airplane to be protected from detection by a hostile radar. While, in stand-off jammers, the target is protected by a jammer carried by other friendly platform (vehicle or airplane) or located at some distance far from the hostile radar [2]. Another difference between these two jamming modes is the gain of the radar's transmit antenna in the direction of the jamming system, which is the side lobe antenna gain for the stand-off jamming and the main lobe antenna gain for the self-protection jamming, respectively [2, 3].

The active jammers can be classified as cover jammers and deceptive jammers. Cover jammers mask the friendly targets by continuous transmission of high-power noise signal concentrated around the radar frequency, but deceptive jammers transmit modified versions of the radar signal, which distorts the matched filter output and generates false targets. An important parameter in these jamming systems is the jammer-to-signal ratio (JSR), which is often greater than unity [2].

Since the signal of deceptive jammer looks like the reflected signal from the target, it benefits from the pulse compression processing gain of the radar. Therefore, the jammer does not need high-power transmission in order to be effective. In contrast, when countering radars by transmitting noise signal, the jamming signal does not benefit from the gain of the matched filter. Therefore, the jammer needs high-power transmission in order to disable the radar's capability for detecting the true target. However, high jamming power could lead to the hostile anti-radiation missile attack [3].

Since digital radio frequency memory (DRFM) jammers retransmit the jamming pulses behind the true target echo, they can be recognized by radar systems easily [4]. Therefore, different repeater jammers are proposed in literatures for avoiding the limitations of DRFM jammer; for instance, frequency-shifting jammer, interrupted sampling repeater jammer (ISRJ), and the spectrum-dividing jammer [5–7].

Frequency-shifting jammers benefit from the well-known range-Doppler coupling property of chirp waveform, where a copy of the radar signal shifted in frequency can be transmitted as an echo to the radar to confuse it, because the jammer signal in this case looks like the radar return [5].

ISRJ is an effective method to jam chirp radars. ISRJ is based on sampling and storing segments of the radar signal and retransmitting them toward the victim radar. By this way, the ISRJ generates many false targets at the output of radar-matched filter [6].

The spectrum-dividing jammer divides a received radar signal into several equal parts to form a whole jamming signal before being retransmitted back to the radar in a different order. By this way, many false targets are generated at the output of radar-matched filter [7].

This paper presents a review of deceptive repeater jammers against chirp radar, including frequency-shifting jammer, ISRJ, and spectrum-dividing jammer in Sections II, III, and IV respectively, where a basic theoretical analysis and Matlab® simulation results of jamming systems are described. Finally, the comparison between different jamming types, and the practical guidance to the target detection in the jamming environment are given in Section V.

Department of Communication Engineering, Higher Institute of Applied Sciences and Technology, Damascus, Syria
Corresponding author:
S.B.S. Hanbali
Email: hanbali.samer@gmail.com

II. FREQUENCY-SHIFTING JAMMING

Frequency-shifting jammer can generate false targets at the output of radar-matched filter by instantly shifting the frequency of radar signal. The jamming retransmission may take different modes, such as single-false target jamming, multiple-false targets jamming, and multiple-cover jamming [5].

The main advantage of frequency-shifting jamming is its ability to generate many false targets before and after the true target. However, the amplitudes of these false targets are lower than the amplitude of the true one, first because of the frequency mismatch between the jamming signals and the matched filter, and second because the jamming signals could be only parts of the radar pulse. Therefore, the jammer has to increase its power in order to compensate for these losses. Another disadvantage of this jammer is the need of a high isolation of two receive–transmit antennas, which might be difficult to implement.

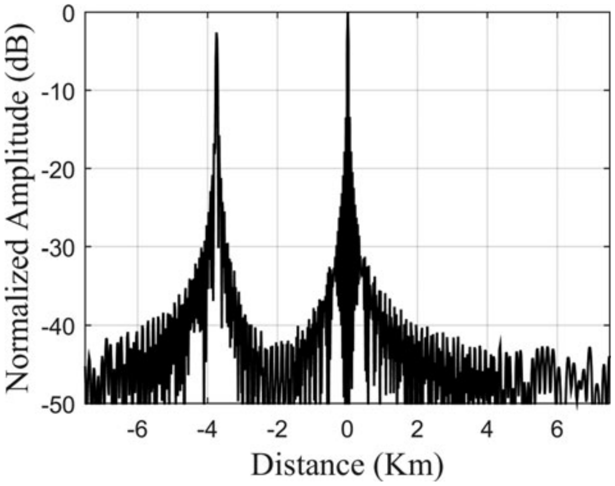

Fig. 1. The simulation result of single-false target jamming.

A) Single-false target jamming

Let $x(t)$ be the complex representation of the transmitted radar chirp [5]:

$$x(t) = \frac{1}{\sqrt{T}} rect\left(\frac{t}{T}\right) e^{j\mu\pi t^2}, \quad |t| < \frac{T}{2}, \tag{1}$$

where T is the chirp duration, $\mu = B/T$ is the frequency modulation slope, and B is the sweep bandwidth. Then, the complex representation of the jamming signal is given by [5]:

$$x_J(t) = x(t) e^{j2\pi f_J t} = e^{j2\pi f_J t + j\pi\mu t^2}, \quad |t| < \frac{T}{2}, \tag{2}$$

where f_J is the frequency shift of the jammer. When $f_J \ll B$, then the output of the matched filter is given by [5]:

$$s_J(t) = \sqrt{BT}\left(1 - \frac{f_J}{B}\right) \cdot sinc\left[\pi(B - f_J)\left(t - t_o + \frac{f_J}{\mu}\right)\right] \cdot e^{j\pi f_J (t - t_o)}, \tag{3}$$

where $t_o = 2R/c$ is the time delay of the true target echo, c is the speed of light, and R is the true target range. Equation (3) shows that the amplitude of the false target is less than the amplitude of the true target by a factor of $(1 - f_J/B)$, also it shows that the false target lags behind the true target when $f_J < 0$ and leads it when $f_J > 0$ by a distance of $d = cf_J/2\mu$.

Figure 1 shows the simulation result of single-false target jamming when $B = 4$ MHz, $T = 100$ µs, $f_J = 1$ MHz, and JSR = 0 dB. In this case, $d = 3.750$ km.

B) Multiple-false targets jamming

In order to make it difficult for the radar to recognize the true target, several false targets could be generated simultaneously at the output of the matched filter. The jammer divides radar pulse into N parts, and then modulates them by different frequencies. The first part is modulated by f_{Jo}, and the modulated frequency of each part is [5]:

$$f_{Jn} = f_{Jo} + (n - 1)\Delta f_J, \quad n = 1, 2, 3, \ldots, N, \tag{4}$$

where Δf_J is the difference between the modulation frequencies of every two adjacent parts. The jamming signal is given by [5]:

$$x_{Jn}(t) = e^{j2\pi f_{Jn} t + j\pi\mu t^2}, \quad t \in \left(-\frac{T}{2} + \frac{n-1}{N}T, -\frac{T}{2} + \frac{n}{N}T\right). \tag{5}$$

In this case, all the false targets have the same amplitude, which is less than the amplitude of the true target by a factor of $1/N$, and the number of false target equals [5]:

$$N_{ft} = \frac{B - f_{Jo}}{\mu.\Delta T + \Delta f_J}, \tag{6}$$

where $\Delta T = T/N$. When $f_{Jn} \in [0, (N - n/N)B]$, the matched filter output is given by [5]:

$$S_{Jn}(t) = \frac{\sqrt{BT}}{N}\ sinc\left[\frac{\pi B}{N}\left(t - t_o + \frac{f_{Jn}}{\mu}\right)\right] \cdot e^{j[2\pi(t - t_o + (f_{Jn}/\mu))(f_{Jn} + (2n - N - 1/2N)B) - \pi f_{Jn}^2/\mu]}. \tag{7}$$

The relative distance between each false target and the true one is $d_n = cf_{Jn}/2\mu$.

Figure 2 shows the simulation result of multiple-false targets jamming when $B = 4$ MHz, $T = 100$ µs, $N = 8$, $f_{Jo} = 0.5$ MHz, $\Delta f_J = 0.4$ MHz, and JSR = 0 dB. In this case, $N_{ft} = 4$, according to equation (6), and the corresponding forward-shifting distance equals 1.875, 3.375, 4.875, 6.375 km, respectively.

C) Multiple-cover jamming

The multiple-cover jamming is better than the single-false target and multiple-false targets jamming [5], because it has an effect of blanket jamming. In this case, the jammer divides radar pulse into N parts at first, and then frequency modulate each part linearly. This gives false targets each of which covers some range in the frequency domain that is more efficient in jamming.

The jamming signal is given by [5]:

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press

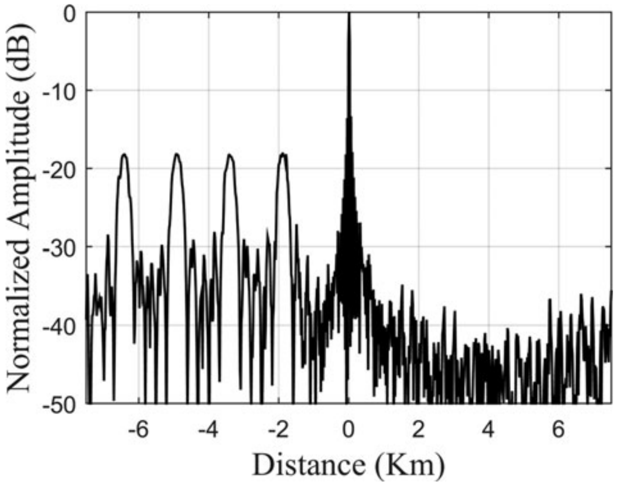

Fig. 2. The simulation result of multiple-false targets jamming.

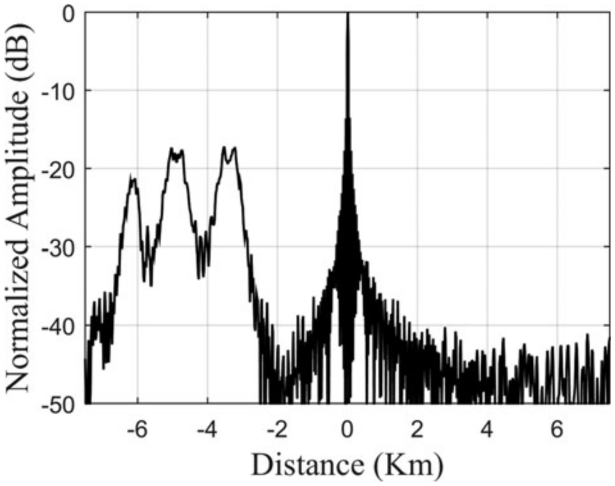

Fig. 3. The simulation result of multiple-cover jamming.

$$x_{Jn}(t) = e^{j2\pi f_{Jn}t + j\pi(\mu+\mu_J)t^2}, \quad t \in \left(-\frac{T}{2} + \frac{n-1}{N}T, -\frac{T}{2} + \frac{n}{N}T\right), \tag{8}$$

where μ_J is the frequency modulation slope of the jamming signal.

The modulated frequency on each part is:

$$f_{Jn} = f_{J0} + (n-1)\Delta f_J, \; n = 1, \; 2, \; 3, \; \ldots, N, \tag{9}$$

where f_{J0} is the initial modulated frequency of the first part of jamming signal.

The number of the cover jamming is given by [5]:

$$N_{ft} = \frac{B - f_{J0}}{(\mu + \mu_J) \cdot \Delta T + \Delta f_J}. \tag{10}$$

The nearest distance of each jamming covered is given by [5]:

$$\frac{c(f_{Jnc} - (\mu_J T/2) - (\Delta f_J/2))}{2\mu}, \tag{11}$$

where f_{Jnc} is the center frequency of each jamming signal.

The distance range each jamming covered is given by [5]:

$$\frac{c}{2} \cdot \frac{\mu_J((B + B_J/N) + \Delta f)}{\mu(\mu + \mu_J)}. \tag{12}$$

Figure 3 shows the simulation result of multiple-cover jamming when $B = 4$ MHz, $T = 100$ µs, $N = 4$, $f_{J0} = 0.8$ MHz, $\Delta f_J = 0.2$ MHz, $\mu_J = 4$ MHz/ms, and JSR = 0 dB. In this case, $N_{ft} = 3$, according to equation (10), the nearest cover distance of the jamming is 3 km, and each jamming covers 443 m, according to equations (11) and (12), respectively.

III. INTERRUPTED SAMPLING REPEATER JAMMER

It is an effective method to deceive chirp radars. This method is based on sampling and storing segments of the radar signal and retransmitting them toward the victim radar. By this way, the ISRJ generates main false target that always lags behind the true target by jammer's delay τ_d, and several other false targets that are located symmetrically around the main false target, at the output of radar-matched filter [6].

A) The advantages and shortcomings of ISRJ

ISRJ has some advantages such as [6, 8]:

- A jammer used one receive and transmit time-sharing antenna, so there is no need for high isolation of two receive–transmit antennas.
- A receive and transmit time-sharing antenna can be carried by a missile, because it has easier implementation than the two receive–transmit antennas.
- The spatial distribution of the false targets can be adjusted by controlling the repeated time delay of jammer. Therefore, there is no need to do complex frequency modulation.

ISRJ has two main shortcomings [6, 8]:

- Power amplification is required due to interrupted sampling.
- The effective false targets of ISRJ lag behind the true target. Therefore, they could be recognized by radar.

B) The principle of ISRJ

The sampling function $p(t)$ is a rectangular pulse train with pulse duration τ and pulse repeat interval $T_s = 1/f_s$, as shown in Fig. 4. The jammer receives the radar chirp and samples it in the interrupted mode, where a single antenna is used for receive and transmit alternately [6].

The output of the matched filter is given by [6]:

$$y(t) = \sum_{n=-\infty}^{\infty} a_n u_n(t), \tag{13}$$

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press

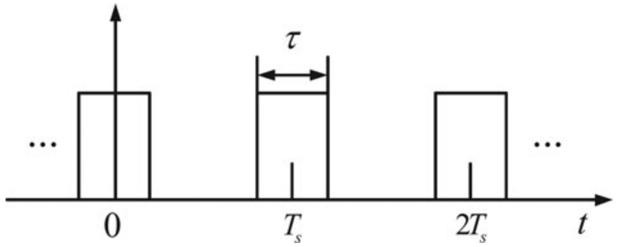

Fig. 4. Interrupted sampling function.

where

$$a_n = \tau f_s\, sinc(\pi n f_s \tau), \tag{14}$$

and $u_n(t)$ is given by [6]:

$$u_n(t) = sinc\left[\pi(nf_s + \mu t)(T - |t|)\right]\left(1 - \frac{|t|}{T}\right)e^{j\pi n f_s t}. \tag{15}$$

On the basis of equations (13) and (15), it is clear that matched filter output consists of many false targets $\{u_n(t)\}$, each one has a frequency shift nf_s and a scale factor a_n. With increasing values of n, the amplitudes of false targets decrease rapidly according to the *sinc* function. In practice, this ISRJ technique usually generates 3–5 effective false targets [6].

Figure 5 shows the simulation result of ISRJ when $B =$ 4 MHz, $T =$ 100 μs, $\tau = 2$ μs, $\tau_d = 10$ μs, $f_s = 200$ KHz, and JSR = 0 dB. In this case, the main false target lags behind the true target by 1.5 km, and the other false targets are located symmetrically around it.

C) Improved ISRJ

Some researchers proposed modified versions of ISRJ to make it more effective as shown in the following examples [8–10]:

1) GENERATION A TRAIN OF FALSE TARGETS THAT PRECEDE THE TRUE ONE

The effective false targets of ISRJ lag behind the true target because of the jammer's delay τ_d; they could be recognized by radar easily. Therefore, a frequency shift or DRFM can be applied to put them before the true target.

DRFM is applied as follows [8]:

- The radar signal is received and stored to digital memory.
- The sampled signal is multiplied with its delay signal that can obtain false targets that lead the true one.
- The amplitude can be amplified before retransmitting to overcome the amplitude decrease.

The signal processing of improved ISRJ with DRFM causes a frequency shift that moves the position of false targets forward [8]. Several false targets are generated after matched filter as shown in equation (16).

$$y_j(t) = \tau f_s\left(1 - \frac{|t|}{T}\right)\sum_{n=-\infty}^{+\infty} sinc(\pi f_s \tau)$$
$$.\ sinc\{(\mu t + \Delta f + nf_s)(T - |t|)\} \cdot e^{\{j\pi[(\Delta f + nf_s)t - nf_s(\tau_o + \tau_d)\}}, \tag{16}$$

where τ_o is the DRFM delay, and $\Delta f = \mu(\tau - 2\tau_o)$ is the frequency shifting that is caused by signal processing of improved ISRJ.

Figure 6 shows the simulation result of ISRJ with frequency shift when $B = 4$ MHz, $T = 100$ μs, $\tau = 2$ μs, $\tau_d = 10$ μs, $\tau =$ 2 μs, $f_s = 200$ KHz, $f_J = 1$ MHz, and JSR = 0 dB. Figure 7 shows the simulation result of ISRJ with DRFM when $f_s =$ 250 KHz, $\tau_d = 10$ μs, $\tau_o = 2.5$ μs, and JSR = 0 dB. In both previous figures, the effective false targets of ISRJ lead the true target.

2) ACTIVE ECHO CANCELLATION

When $\tau_d = f_s/\mu$, then the first false target adjacent to and preceding the main false target (−1st false target) will coincide with the true target, a property proposed in [9] for partial echo cancellation if the false target phase is exactly opposing the true target phase and the amplitudes of these two targets are equal.

The phase of the radar target echo consists of two components: the propagation phase and the signature of the radar target itself. In self-protection jamming, the target and jammer echoes travel the same distance to the radar, and therefore the propagation phase difference is zero. On the other hand, it is assumed, for simplicity, that the target cross-section amplitude equals 1 and the phase equals 0 [9]. The −1st false

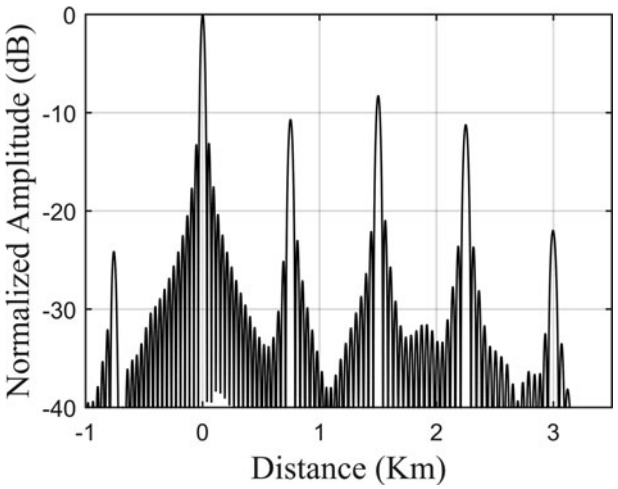

Fig. 5. The simulation result of ISRJ.

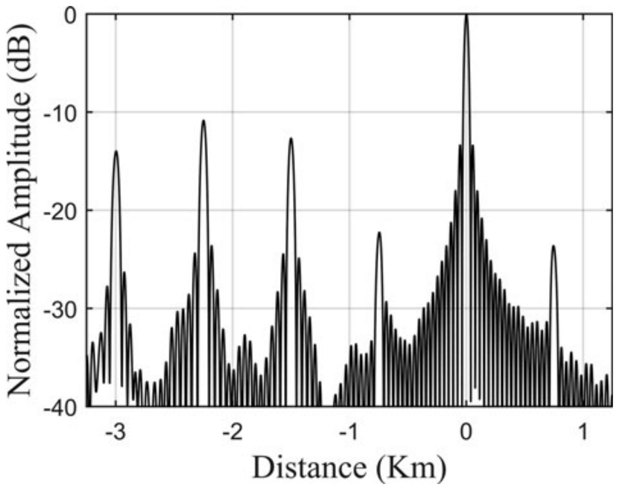

Fig. 6. The simulation result of ISRJ with frequency shift.

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press

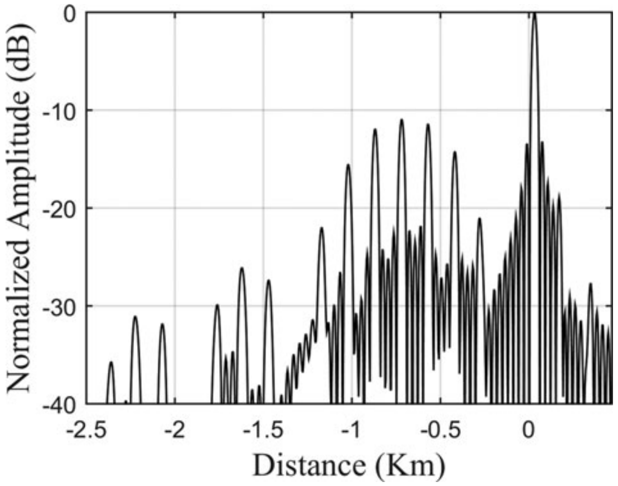

Fig. 7. The simulation result of ISRJ with DRFM.

target will cancel the target echo when τ_d, f_s, and the jammer gain A_j satisfy [9]:

$$\tau_d = f_s/\mu \tag{17}$$

to bring the -1st false target to the location of the true target,

$$f_s = \sqrt{\mu} \tag{18}$$

to make the phase of the -1st false target opposite to the phase of the true target, and

$$A_j = \frac{1}{a_{-1}} = \frac{1}{\tau f_s\, sinc(-\pi f_s \tau)} \tag{19}$$

for the amplitudes of the two echoes to be equal.

Figure 8 shows the simulation results of active echo cancellation jamming when $T = 100$ μs, $B = 5$ MHz, and $\tau = 1.34$ μs, then $f_s = 224$ KHz, $\tau_d = 4.47$ μs, and $A_j = 3.8$, according to equations (17), (18), and (19), respectively. In this case, the true target is suppressed in front of the main false target to about -16 dB, because of the coherent cancellation with -1st false target.

3) Blanket jamming

The blanket jamming effect will be formed when modulating radar echo using pseudo-random noise sequence (PRN). A different covering distances and jamming effects will be achieved by flexible controlling the parameters of ISRJ and PRN [10].

PRN is commonly generated using linear feedback shift register (LFSR). The maximum length of the sequence created by n bit shift register equals to $P = 2^n - 1$. The power spectral density of pseudo-random sequence that has a chip width T_c and a period T is given by [10]:

$$G(f) = \frac{P+1}{P^2} sinc^2(\pi f T_c) \sum_{\substack{l=-\infty \\ l \neq 0}}^{l=\infty} \delta\left(f - \frac{l}{PT_c}\right) + \frac{1}{P^2}\delta(f). \tag{20}$$

The shape of this power spectral density follows $sinc^2$ function. Furthermore, its width controlled by T_c; the shorter T_c, the wider frequency spreading but its amplitude level will be down. In fact, binary phase modulation of the chirp waveform, using PRN, is equivalent to shifting chirp waveform simultaneously by a series of frequencies.

The ISRJ modulates the phases of sampled radar signal according to the values of PRN, and then it sends the jamming signal to victim radar. This method will form a large amount of noise around the pulse compression output of target echo, because the spectrum of radar signal is expanded by modulating it by PRN. However, in this case, $a_n \ll 1$. Therefore, the jammer has to increase JSR to a high degree in order to disable the radar's capability for detecting the true target [10].

Figure 9 shows the simulation results of the blanket jamming when $T = 100$ μs, $B = 5$ MHz, and $P = 127$, $T_c = 800$ ns, $f_s = 200$ KHz, and JSR $= 0$ dB. In this case, more JSR is required to cover the true target by noise jamming.

IV. THE SPECTRUM-DIVIDING JAMMER

The spectrum-dividing jammer divides a received radar signal into several equal parts to form a whole jamming signal before being retransmitted back to the radar in a different order. A train of false targets will be achieved at the output of

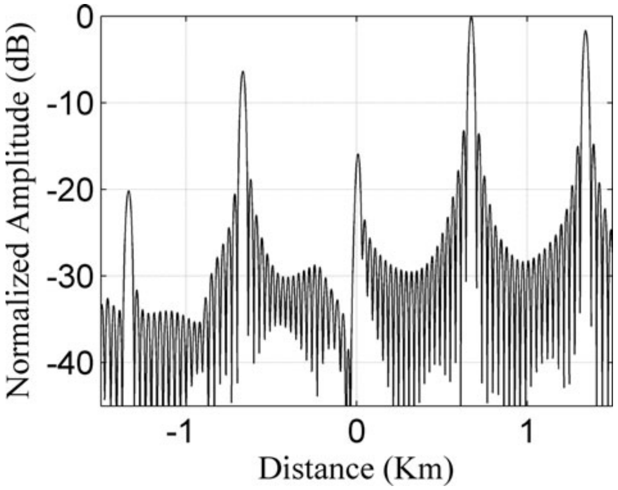

Fig. 8. The simulation results of active echo cancellation.

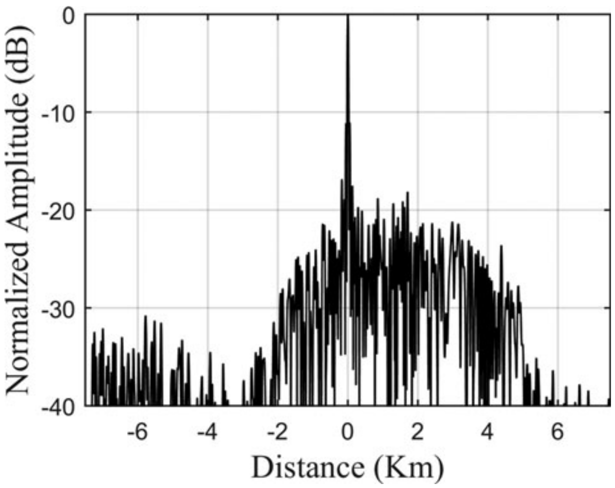

Fig. 9. The simulation results of the blanket jamming.

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press

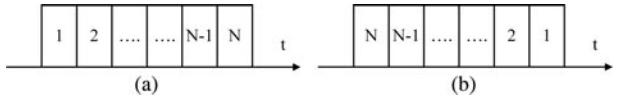

Fig. 10. The schematic diagram of the spectrum-divided repeat jamming. (a) Radar signal; (b) jamming signal.

radar-matched filter. The spectrum changed in the jamming signal contrast to the original radar signal will induce different time delay due to the group delay [7]. Figure 10 shows the schematic diagram of this jammer, the chirp is divided into N equal pulses in frequency spectrum and arranged in a different order to form the jamming signal.

The ith pulse in the radar signal (called signal order) is retransmitted as kth part in the jamming signal (called jamming order or retransmitted order), and the k_ith jamming pulse is derived [7]:

$$p_{k_i}(t) = rect\left[\frac{t-(-(T/2)+(k/N)T+(T/2N))}{T/N}\right] e^{j\pi\mu[t-(k-i)T/N]^2}, \tag{21}$$

where $k, i = 0, 1, \ldots, N-1$. From equation (21), it can be seen that the retransmitted jamming pulse is a chirp signal with T/N in duration and B/N in bandwidth [7]. Figure 11(a) shows the amplitude spectrum of the transmitted signal, and Fig. 11(b) shows the amplitude spectrum of the spectrum-divided repeat jamming pulses in four equal parts.

The matched filter output is given by [7]:

$$y_{k_i}(t) = \frac{\sqrt{BT}}{N} sinc\left(\frac{\pi B(t-(k-i)T/N)}{N}\right) e^{-j2\pi(B/2-KB/N-B/2N)(t-(k-i)T/N)}. \tag{22}$$

On the basis of equation (22), the amplitude of the false targets equal $|y_{k_{i\,max}}(t)| = \sqrt{BT}/N$. The false targets are located at $(N-1/N)T$, $(N-3/N)T$, $(N-5/N)T, \ldots, (1-N/N)T$, respectively [7]. The space between the false targets equals $(2/N)T$.

Figure 12 shows the simulation results of spectrum-dividing jammer when $T = 100$ µs, $B = 5$ MHz, and $N = 4$. In this case, the false targets are located at −11.25, −3.75, 3.75, and 11.25 km, respectively, and the relative distance between each adjacent false target equals 7.5 km.

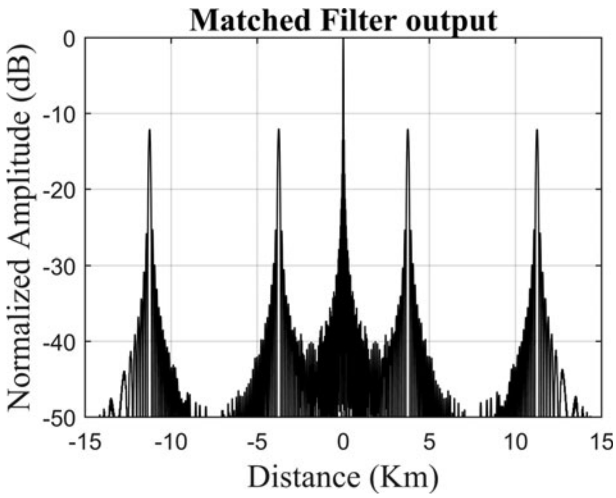

Fig. 12. The simulation results of spectrum-dividing repeater jammer.

The main advantage of spectrum-dividing jamming is its ability to generate false targets with different range while achieving a coherent processing gain. However, the jamming signals are parts of the radar pulse. Therefore, the jammer has to increase its power in order to compensate for this loss.

V. CONCLUSIVE REMARKS

The properties of each presented jammer are summarized in Table 1.

The jamming signal processing causes amplitude loss L_j, which should be compensated by the jammer amplifier gain $A_j \geq 1/L_j$ and jammer antenna gain G_j. Figures 13 and 14 show the loss (L_j) for different jamming types.

In self-protection jammer, the propagation loss is applied equally on both true target echo and jamming signals. However, the jamming signal has an advantage over the true target echo by a factor of $(A_j + G_j)$ dB. Therefore, jamming signal confuses the radar to a high degree, especially at far distances where the true target echo is weak.

The comparison between the presented jammers is summarized as follows:

(1) The main disadvantage of the frequency-shifting jammer is the need of a high isolation of two receive–transmit

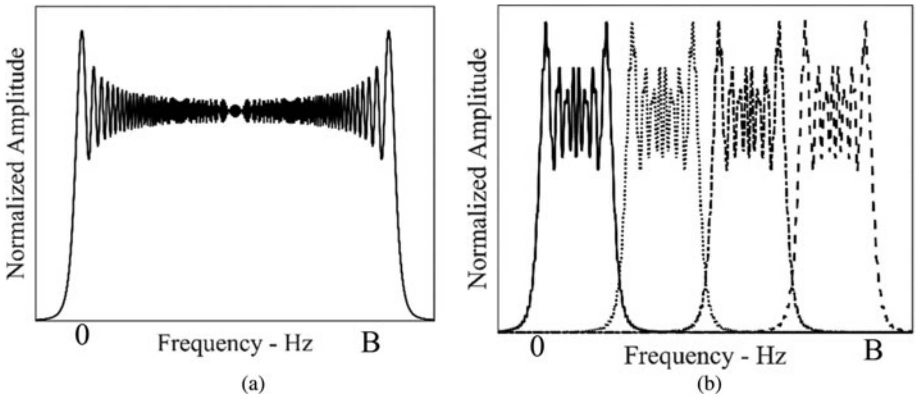

Fig. 11. Amplitude spectrum plots. (a) Transmitted signal; (b) retransmitted jamming pulses.

Table 1. The properties of different jammers.

Type	Repeater jammer type	Number of antennas	amplitude loss L_j	Based on DRFM
a	Frequency-shifting jamming, single false target	2	$1 - f_j/B$	No
b	Frequency-shifting jamming, multiple-false targets	2	$\frac{(1 - f_{jn}/B)}{N}$	No
c	Frequency-shifting jamming, multiple-cover targets	2	$\frac{(1 - f_{jn}/B)}{N}$	No
d	ISRJ	1	a_n	No
e	ISRJ-DRFM	1	a_n	Yes
f	ISRJ-active echo cancellation	1	a_n	No
g	ISRJ-blanket jamming	1	$a_n \ll 1$	No
h	Spectrum-dividing jammer	2	$\frac{1}{N}$	Yes

antennas, which might be difficult to implement. Therefore, ISRJ with a receive–transmit time-sharing antenna is preferred.

(2) When the deceptive jammer shifts the radar signal by a single frequency as shown in Table 1 (type a) and Fig. 13, the amplitude of false target is lower than the amplitude of true one, especially for high values of f_j, because of the frequency mismatch between jamming signal and matched filter [5]. However, more jamming power is required when the deceptive jammer divides radar pulse into N parts as shown in Table 1 (types b, c, and h) and Fig. 13, because the jamming signals are parts of the radar pulse [5, 7].

(3) When jamming types (d, e, and f) are used, the false targets are scaled by a_n (a_n is a function of $f_s\tau$) as shown in Fig. 14. On the other hand, when jamming type (g) is used, the jamming signal does not benefit from the gain of the matched filter ($a_n \ll 1$ as shown above). Therefore, the jammer has to increase its transmitted power to a high degree in order to disable the radar's capability for detecting the true target.

(4) Some presented jammers are based on DRFM, such as types (e and h) as shown in Table 1. Therefore, they can be countered by using traditional electronic counter-countermeasures (ECCM) techniques.

(5) ISRJ generates many false targets without sampling and storing the complete radar pulse, unlike spectrum-dividing jammer that samples and stores the complete radar pulse. Therefore, more memory is required in jamming system.

(6) ISRJ and spectrum-dividing jammer generate many false targets without the need to do complex frequency modulation used by frequency-shifting jammers.

(7) ISRJ with a receive–transmit time-sharing antenna can be carried by a missile easily, unlike two receive–transmit antennas used by frequency-shifting jammers.

The presented jammers in Table 1 degrade the performance of radar receiver as follows:

(1) Unfortunately, the optimum detection of chirp signals by a matched filter cannot distinguish the true target from the false one in the time domain, because they are interchangeable in time, i.e. the false target may come before or after the true one; also in the frequency domain, their spectra may be overlapping, which make them impossible to isolate.

(2) In jamming types (a, b, c, d, e, f, and h), the false targets look like the true targets at the output of radar-matched filter. When high JSR is used, a mutual target masking occurs; the strong false target that falls within the constant false alarm rate (CFAR) reference window will bias the threshold. Consequently, the conventional CFAR masks the weaker of the two closely spaced targets. Therefore, a modified CFAR is used such as trimmed mean or censored CFAR, and order statistics CFAR, which are designed to suppress mutual target masking. But these

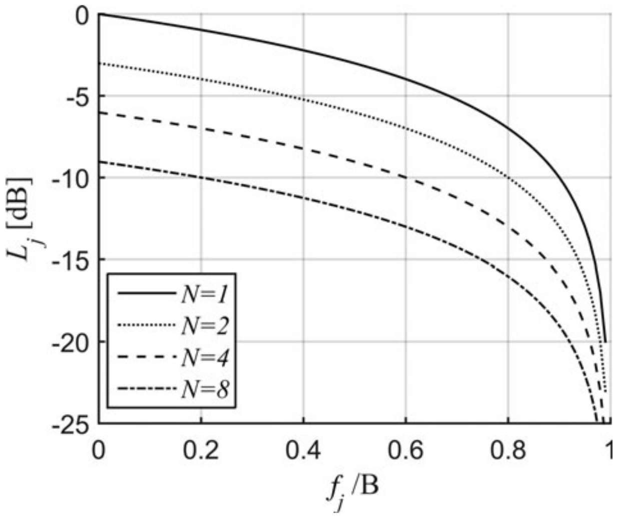

Fig. 13. Jammer loss in the case of frequency-shifting jamming and spectrum-dividing jammer (when $f_j/B = 0$).

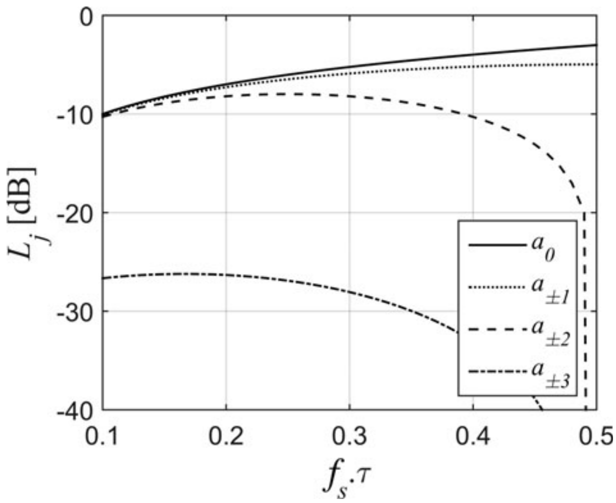

Fig. 14. Jammer loss in the case of ISRJ.

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press

methods are not enough alone to counter deceptive jammers and to recognize the true target. In addition, they exhibit additional complexity, higher computational cost, and a higher CFAR loss, in terms of signal-to-noise ratio (SNR), above the conventional CFAR due to the use of lower number of cells [11, 12].

(3) When high JSR is used in jamming type (g), the jamming signal increases the detection threshold. Therefore, the true target echo is beneath the threshold. The covering distance of noise should be equivalent or larger than the detection window of CFAR detection [10].

The commonly used (ECCM) techniques are effective against some types of deceptive jammers. Pulse repetition interval (PRI) jitter technique identifies the false targets returns if the deception jammer uses a delay that is greater than a PRI period to generate false targets return [13], but this technique is inefficient in the case of instantaneously retransmitting the radar pulse after frequency-shifting or interrupted sampling during the radar chirp itself. The frequency agility technique changes the radio frequency of radar to make it impossible to know what the radio frequency of the next pulse will be, but if the jammer has a digital instantaneous frequency measurement receiver that measures approximately the first 50 ns of a pulse, it can quickly set to that radio frequency because modern radars typically have pulses of several microseconds long [13]. Orthogonal waveforms technique transmits successive orthogonal waveforms that have low cross-correlation [14], and when the jammer pulse lags behind the true target pulse, it will not benefit from the pulse compression gain, a situation that is not applicable in the case of frequency-shifting jammer or ISRJ.

Recently, a method is proposed to remove the ISRJ-based false targets by using short-time Fourier transform [15], where it was found that the time–frequency characteristics of the ISRJ signal are discontinuous in the pulse duration, because the ISRJ jammer needs short durations to receive the radar signal. Based on the discontinuous characteristics, a particular band-pass filter can be generated to retain the true target signal and suppress the ISRJ signal, but this method needs a high SNR to counter ISRJ because it is done before the pulse compression process. In addition, this is only applicable to counter ISRJ in the case of de-chirping radar (stretch processing).

We addressed countering some types of frequency-shift jammers for the first time using sweep bandwidth agility [16]. In that paper, the sweep bandwidth of the transmitted chirp was changed slightly, then the relative distances between the true target and the false ones changed. Consequently, false targets appeared in different range bins, but the true target remained in the same range bin, because the jammer frequency shift is much bigger than the Doppler shift of the true target. By doing that the radar range resolution and the matched filter gain do not degrade too much. Recently, we proposed a new anti-jamming technique based on the fractional Fourier transform (FrFT) at the radar receiver to counter different types of frequency-shift jammers against surveillance radars [17]. In that paper, the FrFT compresses the received signal in such a manner that the true target echo and the jamming signal are resolved, so that they are separated. Then, after FrFT compression and separation, the resulting signals are returned to the frequency domain where their spectra are compensated for Doppler shift, and then compared with spectrum of the original radar chirp in terms of the center frequency and the bandwidth. The signal that has less differences of the center frequency and sweep bandwidth is considered as the true target. We also addressed countering active echo cancellation of self-protection ISRJ for the first time by introducing a linear phase shift of the transmitted radar signal [18]. By doing that, the true target and the jammer echo will be in phase. Consequently, the true target power is augmented by jammer echo, converting the jamming signal from being malicious to beneficial.

VI. CONCLUSION

This paper reviewed different types of deceptive jammers against chirp radars. These jammers generate many false targets that appear before and after the true target. Unfortunately, the radar cannot distinguish the true target from the false one, because the true target echo and jamming signals overlap in time and frequency domains. The presented simulation of jamming systems, jammers comparison, and ECCM techniques are helpful for researchers in electronic warfare field.

ACKNOWLEDGEMENT

The authors would like to thank Hatem Najdi for his helpful discussions and for reviewing the final version of this paper.

REFERENCES

[1] Curtis Schleher, D.: Electronic Warfare in the Information Age, chapter 4, Artech House, Boston–London, 1999.

[2] Stimson, G.W.; Griffiths, H.; Baker, C.; Adamy, D.: Introduction to Airborne Radar, 3rd ed., chapter 4, Copyright © 2014 by SciTech Publishing, Edison, NJ, 2014.

[3] Shi, C.; Wang, F.; Sellathurai, M.; Zhou, J.: Low probability of intercept based multicarrier radar jamming power allocation for joint radar and wireless communications systems. IET Radar Sonar Navig., **11** (5) (2017), 802–811.

[4] De Martino, A.: Introduction to Modern EW Systems, chapter 5, Copyright © 2012 by Artech House, Boston–London, 2012.

[5] Yong, Y.; Zhang, W.-M.; Yang, J.-H.: Study on frequency-shifting jamming to linear frequency modulation pulse compression radars, in Wireless Communications & Signal Processing, IEEE, Nanjing, China, 2009, 1–5.

[6] Wang, X.S.; Liu, J.C.; Zhang, W.M.; Fu, Q.X.; Liu, Z.; Xie, X.X.: Mathematic principles of interrupted-sampling repeater jamming (ISRJ). Sci. China Ser. F Inf. Sci., **50** (1) (2007), 113–123.

[7] Pan, X-Y.; Wang, W.; Feng, D-J.; Fu, Q.-X.; Wang, G.-Y.: Repeat jamming against LFM radars based on spectrum-divided, in Radar Conf. 2013: 0490-0490, IET Int, Xi'an, China.

[8] Li, C.Z.; Su, W.M.; Gu, H.; Ma, C.; Chen, J.L.: Improved interrupted sampling repeater jamming based on DRFM, in Signal Processing, Communications and Computing (ICSPCC), 2014 IEEE Int. Conf. on, IEEE, 2014, 254–257.

[9] Feng, D.; Xu, L.; Wang, W.; Yang, H.: Radar echo cancellation using interrupted-sampling repeater. IEICE Electronics Express, **11** (8) (2014), 1–6.

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press

[10] Tai, N.; Yuan, N.C.; Pan, Y.J.: Quasi-coherent noise jamming to LFM radar based on pseudo-random sequence phase-modulation. Radioengineering, **24** (4) (2015), 1013–1024.

[11] Richards, M.A.: Fundamentals of Radar Signal Processing, 2nd ed., chapter 4, 6, McGraw-Hill, New York, 2014, ISBN: 978-0-07-179833-4.

[12] Richards, M.A.; Scheer, J.A.; Holm, W.A.: Principles of Modern Radar, vol. **I**: Basic Principles, chapter 16, Copyright © 2010 by SciTech Publishing, Edison, NJ, 2010.

[13] Adamy, D.L.: EW 104, EW against a New Generation of Threats, chapter 4, Copyright © 2015 by Artech House, Boston–London, 2015, ISBN 13:978-1-60807-869-1.

[14] Deng, H.: Polyphase code design for orthogonal netted radar systems. IEEE Trans. Signal Process., **52** (11) (2004), 3126–3135.

[15] Gong, S.; Wei, X.; Li, X.: ECCM scheme against interrupted sampling repeater jammer based on time–frequency analysis. J. Syst. Eng. Electron., **25** (6) (2014), 996–1003.

[16] Hanbali, S.B.S.; Kastantin, R.: Countering a self-protection frequency shifting jamming against LFM pulse compression radars. Int. J. Electron. Telecommun., **63** (2) (2017), 145–150.

[17] Hanbali, S.B.S.; Kastantin, R.: Fractional Fourier transform-based chirp radars for countering self-protection frequency-shifting jammers. Int. J. Microw. Wireless Technol., (2017), 1–7. doi: 10.1017/S1759078717000289.

[18] Hanbali, S.B.S.; Kastantin, R.: Technique to counter active echo cancellation of self-protection ISRJ. Electron. Lett., **53** (10) (2017), 680–681.

Samer Baher Safa Hanbali received the B.Sc. degree in Electronic Engineering from Damascus University, Syria, in 2000, and the M.Sc. degree from FH Joanneum, Austria, in 2011. He is pursuing the Ph.D. degree, in the area of Radar Signal Processing, at the Department of Communication Engineering in the Higher Institute of Applied Sciences and Technology, Damascus, Syria.

Radwan Kastantin received the B.Sc. degree in Electronic Engineering from Damascus University, Syria, in 1986, and the Ph.D. degree from ICP-INPG, France, in 1996. He is a Professor of communication and signal processing at the Department of Communication Engineering in the Higher Institute of Applied Sciences and Technology, Damascus, Syria.

https://doi.org/10.1017/S1759078717000708 Published online by Cambridge University Press