IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 30, 2019, accepted June 26, 2019, date of publication July 10, 2019, date of current version July 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2928000

Application of Hash Function on FMCW Based Millimeter-Wave Radar Against DRFM Jamming

ZHENYU GUAN[1], (Member, IEEE), YONGJIANG CHEN[1], PENG LEI[2], DAWEI LI[2], AND YING ZHAO[2]

[1]School of Cyber Science and Technology, Beihang University, Beijing 100191, China
[2]School of Electronic and Information Engineering, Beihang University, Beijing 100191, China

Corresponding author: Peng Lei (peng.lei@buaa.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Project 2017YFB0802502, in part by the Aeronautical Science Foundation of China under Project 2017ZC51038, in part by the National Cryptography Development Fund under Project MMJJ20170106, in part by the Foundation of Science and Technology on Information Assurance Laboratory under Project 6142112030516211 2006, and in part by the National Natural Science Foundation of China under Project 61672083, Project 61532021, Project 61472429, Project 61402029, Project 61702028, and Project 61571024.

ABSTRACT Transport innovations and technological improvements have increased attention to specific techniques of communications, such as millimeter-wave radars used in autonomous vehicles (AVs). In order to improve the performance of antijamming capability of a millimeter-wave radar, the suppression of interference using random functions is widely used in current applications. However, the main limitation of this method is that it lack a mechanism to withstand message replaying attack, forgery attack, Masquerade attack, and guessing and stolen verifier attack. In this paper, we propose an antijamming method based on a hash function to provide a secure antijamming solution with a stronger ability to suppress the interference echoes and flexible controls. The associated techniques include digital radio frequency memory (DRFM), millimeter-wave radar, and hash value processing. Three types of experiments are performed to achieve 32.87%∼38.34% improvement in terms of the peak difference between the true and false targets, and the results are reported and analyzed in this paper. In each of the experiments, different variables are tested by the controlled variable method, and the experimental results are compared. On this occasion, it is concluded that the modulation signal based on the hash function has a stronger ability to suppress the interference echoes than that based on the pseudorandom function.

INDEX TERMS Millimeter-wave radar, electronic counter-countermeasures, digital radio frequency memory, hash function.

I. INTRODUCTION

Since Connected and Autonomous Vehicles (CAVs) have promised to be one of the most predominant modes in the next generation mobility, a range of challenges and opportunities necessitate paying more attention to, such as the implementation of prospective data from CAVs into the existing traffic management systems. The concept of Internet of Vehicles (IoV), as one of the most efficient methodologies with wireless sensor networks used by CAVs, is increasingly widespread in traffic management and has been implemented in the construction of future smart mobility infrastructures. During this deployment of IoV with CAVs, communication security concerns are becoming increasingly prominent.

The RSA conference in 2018 [1] discussed the relevant communication security of the IoV. As indicated from the conference discussion, the most important component in the application of the IoV to address the security issues is radar positioning, which is a support technology based on radar application foundations. Many functions of the Internet of vehicles have been proposed based on vehicle-mounted radar positioning. The security and availability of the acquired data play important roles in scenarios involving the Internet of vehicles. Because of autonomous control in CAVs, vehicles can be dominated by adversaries to gain access to damage systems, and thus, the potential for malicious attacks deserves special attention.

The associate editor coordinating the review of this manuscript and approving it for publication was Ning Zhang.

Because of the wide frequency range (30 $GHz \sim 300\ GHz$), the large bandwidth and high-accurate multidimensional detection rate, millimeter-waves are widely used in the communication of CAVs. In summary, the development and application of communications in CAVs benefits from the performance of the existing millimeter-wave technologies, but necessitate attention regarding safety aspects in practice.

Potential interferences on radar include passive jamming and active jamming. The interference of vehicle-mounted radar can involve mutual interference between vehicles or malicious interference. Discussed here is a kind of active jamming of digital radio frequency memory (DRFM) interference: the special equipment generates interference after intercepting the radar transmission signal. The attacker needs to apply false signal modulation to the intercepted radar wave and then forward the interference.

Interference is the main threat to radar because it changes the position of the target scattering to deceive the radar, and this application of interference can cause irreparable damage. Both distance deception and speed deception can arise from disturbances. With the application of millimeter-wave radar, the development of a millimeter-wave jammer is imperative [2], so solutions also need to be developed.

In this scenario, the most significant threat is to inject false information into vehicles, deceive vehicle radars, or even force vehicles to execute (or fail to execute) emergency braking, resulting in casualties. A radar jamming technology can generate severe interference, which is the key component of DRFM jamming technology exploiting the digital use of storage technology. This technology will be introduced in section II. DRFM performs exact copying of the radar signal and incorporates the ability to disrupt the radar system, making it difficult to identify true and false targets.

In this case, we apply the method of cryptographic authentication to enhance discrimination so that even receiving the opponent's highly realistic spoofing echo can reduce the probability of being deceived. In general, spoofing signals can reasonably simulate the real target echo, but the distances are different from those of the real target echo.

Regarding electronic countermeasures (ECM) and electronic counter-countermeasures (ECCM), [2] carried out related research. The research [2] discussed active deception jamming, which usually refers to an interference pulse generated by a jammer by simulating the target echo to deceive radar systems so that the true and false targets are difficult to distinguish, with false target identification being the key goal. The general active spoofing methods include angle spoofing, distance spoofing and speed spoofing.

The literature [3] describes potential means of attack in autonomous vehicles and points out the social problems brought by automated vehicles, including those associated with road safety, privacy, traffic flow, energy and environmental impacts, the automobile industry, the economy and network security. With the increase in the popularity of such attacks in the vehicle automation stage, it is necessary to evaluate this threat through debating and discussion.

Vehicle attacks may damage some information sources used for position determination and trajectory planning. An attack implies the presence of global positioning system (GPS) jammers, a DRFM attack, or an electromagnetic pulse (EMP); in the context of the DRFM technique, the received signal is quantified and stored in the digital memory as a copy of the exchange.

According to the needs of the attacker, the signal needs to be copied and retransmitted.

To date, there have been many attempts to subvert DRFM jamming technology, and increasing the robustness against this interference is achieved mainly through waveform design and the adjustment of the polarization characteristics, which constitute the initial phase in related research on antijamming.

The antijamming strategy of [4] uses the beat-frequency nonoverlapping properties of the signal in the frequency domain and filters out the interference signal, and this proposed scheme has been the subject of a brief analysis using simulations.

However, the anti-interference method in [5] uses a random initial phase when sending signals, which makes the DRFM jammer unable to adapt to the randomness of the initial phase. This polarization radar is mentioned in the article [6]. The anti-interference technology mentioned in another article [7] introduces the influence of the phase noise difference in the received signal to distinguish the target. Reference [8] describes using the orthogonal block coding ECCM scheme for repeated radar jamming.

A chirp-chip-based linear frequency modulated (LFM) random radar waveform is proposed in [9]. The instantaneous frequency of each chirp chip is a random value, and linear interpolation is performed. The result of distance ambiguity can be suppressed by random noise waveform was presented and analyzed by [10].

DRFM jamming technology is a very effective active attack jamming technology among many relevant antijamming solutions. Noise radar, developed in the 1950s, is a radar type that can achieve pulse agility and resist DRFM repeated jamming.

In this paper, we have developed a new technique regarding the anti-interference method of receiving a spoofing echo and carried out simulation experiments. The premise of anti-interference here is the interference technology of DRFM, and the key point is the access to identify whether the received echo is emitted by ourselves or by the opponent. In addition, a cryptographic hash function is used. Considering the anticollision properties of the hash function itself, the use of the hash function instead of the pseudorandom function will achieve better results in some condition because the pulse compression graph has larger peak differences when using hash functions.

Furthermore, we have carried out a comparative simulation experiment and selected three comparison samples: waveforms without modulation, waveforms modulated by pseudorandom functions, and waveforms modulated by hash functions. The three types of waveforms were compared

under specific identical interference scenarios, and the conclusions were drawn. In the end, an analysis experiment of the expanded sample was carried out to verify the conclusion with reasonable probability.

II. PRELIMINARY WORK

A. DRFM

The most important aspect of DRFM is the digital replication of the received signal in a form related to that signal. DRFM can modify the signal before retransmission, change the target characteristics, and adjust the radar cross section (RCS), range, speed and angle. DRFM poses a serious obstacle to radar sensors.

The waveforms are intercepted by the jammer from that emitted by radar, the principle of DRFM is to modulate the waveforms stored in the jammer.

What can DRFM do? First, it can provide a coherent time delay of RF signals and produce coherent spoofing to the radar system. Radar pulses captured by DRFM can be replayed with very little delay. By playing back the waveform with DRFM, a false target can be generated from the normal radar, and the delayed change of the false target makes the target appear to be moving [11]. Second, the pulse data captured by DRFM can be modulated in amplitude, frequency and/or phase and can be used to produce other effects [11], [12]. DRFM can increase the Doppler frequency shift so that the range and range rate tracker will be correlated in the interfered radar [11], [12]. Finally, the pulses captured by DRFM can be replayed many times, so the interfered radar can detect many targets, and in certain cases, DRFM can generate arbitrary interference waveforms.

DRFM technology includes three types of coding: phase coding, amplitude coding and I-Q coding.

The working principle of DRFM is theoretically analyzed as follows: if a radio frequency signal with a carrier frequency f_c is received by DRFM at time t, the signal can be expressed as

$$\mathcal{S}_{drfm_{in}}(t) = x(t)\cos(2\pi f_c t + \varphi_0) \quad 0 \le t \le \mathcal{T}_P \tag{1}$$

where $x(t)$ represents the envelope of the signal and φ_0 represents the initial phase of the signal.

The DRFM also includes the capability of signal processing. In receiving systems, if the incoming signal $\mathcal{S}(t) = x(t)\cos(2\pi f_c t + \varphi(t))$ $(2\pi f_c = \omega_c)$ is mixed with the local oscillator frequency f_{lo}, the resulting frequency output is $f_{out} = |f_c \pm f_{lo}|$.

$\mathcal{S}(t)$ and its quadrature components $\mathcal{S}_2(t)$ are expressed as follows:

$$\mathcal{S}(t) = x(t)\cos(\omega_c t + \varphi(t)) \tag{2}$$
$$\mathcal{S}_2(t) = x(t)\sin(\omega_c t + \varphi(t)) \tag{3}$$

The complex analytical signal representation is

$$\mathcal{S}_c(t) = x(t)e^{j[\omega_c t + \varphi(t)]} = x(t)e^{j\varphi(t)} \cdot e^{j\omega_c t} \tag{4}$$

The baseband signal $\mathcal{S}_B$ is expressed as

$$\begin{aligned}\mathcal{S}_B(t) &= \mathcal{S}_c(t) \cdot e^{-j\omega_c t} = x(t)e^{j\varphi(t)} \cdot e^{j\omega_c t} \cdot e^{-j\omega_c t} \\ &= x(t)\cos(\varphi(t)) + jx(t)\sin(\varphi(t)) \\ &= I(t) + jQ(t)\end{aligned} \tag{5}$$

Then, the signal can be expressed as

$$I(t) = x(t)\cos(\varphi(t)) \tag{6}$$
$$Q(t) = x(t)\sin(\varphi(t)) \tag{7}$$

The amplitude of the signal can be obtained from the following formula:

$$x(t) = \sqrt{I^2(t) + Q^2(t)} \tag{8}$$

The parameter $\varphi(t)$ in the formula contains the carrier phase offset and modulation frequency phase slope. The phase information of the signal can be obtained from the following formula:

$$\begin{aligned}\varphi(t) &= \arctan[\frac{Q(t)}{I(t)}] \\ &= \arctan[\frac{x(t)\sin(\varphi(t))}{x(t)\cos(\varphi(t))}]\end{aligned} \tag{9}$$

The radar wave intercepted by the DRFM jammer is represented by Equation (1). After receiving the wave, $\mathcal{S}_{drfm_{in}}(t)$ is mixed with the local oscillator signal and low-pass filtered. Then, according to the interference demand of the attacker, the wave undergoes modulation of its amplitude, frequency and phase.

The obtained quadrature signal is represented by the following formula:

$$\mathcal{S}_{drfm_I}(t) = A_{drfm}(t)\cos(2\pi f_{drfm}t + \varphi_{drfm}) \tag{10}$$
$$\mathcal{S}_{drfm_Q}(t) = A_{drfm}(t)\sin(2\pi f_{drfm}t + \varphi_{drfm}) \tag{11}$$

where $A_{drfm}(t)$ is the amplitude of the interfering signal, f_{drfm} is the frequency of the interfering signal, and φ_{drfm} is the phase of the interfering signal.

B. LFM

The LFM is a signal with a large time-width bandwidth product. The frequency of this signal increases or decreases over time and is widely used in radar, sonar and other aspects. A typical LFM signal can be expressed as

$$\mathcal{S}_{lfm}(t) = rect(\frac{t}{\mathcal{T}_p})e^{j2\pi(f_c t + \mu\frac{t^2}{2})} \tag{12}$$

where f_c denotes the carrier frequency, μ denotes the frequency modulation rate, $\mathcal{T}_p$ is the pulse width, and $rect(\frac{t}{\mathcal{T}_p})$ denotes a rectangular pulse of width $\mathcal{T}_p$:

$$rect(\frac{t}{\mathcal{T}_p}) = \begin{cases} 1, & |t| \le \frac{\mathcal{T}_p}{2} \\ 0, & \text{others} \end{cases} \tag{13}$$

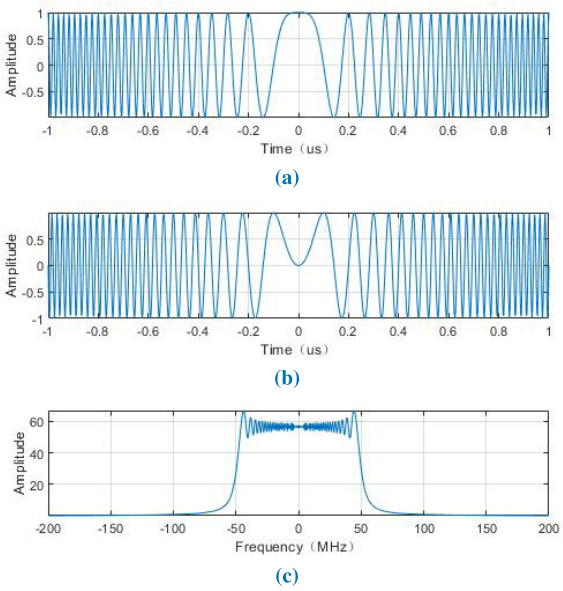


FIGURE 1. Typical chirp signal. (a) The real part of the chirp signal. (b) The imaginary part of the chirp signal. (c) Spectrum magnitude of the chirp signal.

In addition, μ in Equation (12) is expressed as $\mu = \frac{B}{\mathcal{T}_p}$, where B is the signal bandwidth.

The instantaneous phase of the signal is

$$\Psi(t) = 2\pi(f_c t + \mu\frac{t^2}{2}) \tag{14}$$

The instantaneous frequency of this signal is

$$f_{lfm_i}(t) = \frac{1}{2\pi}\frac{d(2\pi(f_c t + \mu\frac{t^2}{2}))}{dt} = f_c + \mu t \tag{15}$$

If $\mu < 0$, then the instantaneous frequency is linearly reduced; if $\mu > 0$, then the instantaneous frequency increases linearly.

Equation 12 could be rewritten as

$$\mathcal{S}_{lfm}(t) = \mathcal{S}_{com}(t)e^{j2\pi f_c t} \tag{16}$$

where

$$\mathcal{S}_{com}(t) = rect(\frac{t}{\mathcal{T}_p})e^{j\pi\mu t^2} \tag{17}$$

According to the Euler formula, Equation (17) can also be expressed as

$$\begin{aligned}\mathcal{S}_{com}(t) &= rect(\frac{t}{\mathcal{T}_p})e^{j\pi\mu t^2} \\ &= \mathcal{S}_{com_I}(t) + j\mathcal{S}_{com_Q}(t) \\ &= \cos(\pi\mu t^2) + j\sin(\pi\mu t^2)\end{aligned} \tag{18}$$

where $0 \le t \le \mathcal{T}_p$.

The spectrum of the signal can be obtained by Fourier transformation, so when $B = 100\ MHz$ and $\mathcal{T}_p = 2\ \mu s$, the real part, imaginary part and spectrum of the chirp signal are expressed as shown in Figure 1.

C. HASH FUNCTION

The hash function $\mathcal{H}(x)$ is a basic tool for cryptography and has applications in many areas, such as digital signatures and message integrity verification. The hash function is a one-way function [13]. The basic properties of the hash function can be expressed by the following formula:

$$\mathcal{H} : \{0, 1\}^* \rightarrow \{0, 1\}^n \tag{19}$$

where $*$ indicates the input length of the hash function, which is arbitrary, and n indicates the output length of the hash function, which is fixed.

The properties of the hash function include the following:

- The length of the output is fixed while that of the input is arbitrary: the variable x can be of arbitrary length, and the result of $\mathcal{H}(x)$ has a fixed length of n bits (such as 64 b, 80 b, or 160 b), as expressed by Equation (19).
- Preimage attack resistance: finding an input x with a known hash value $y = \mathcal{H}(x)$ is computationally infeasible.
- Collision attack resistance: finding two different inputs x_1 and x_2 ($x_1 \neq x_2$) with $\mathcal{H}(x_1) = \mathcal{H}(x_2)$ is computationally infeasible.

Typical hash functions include MD5, SHA1, SHA256, SHA384, and SHA512 [13]. The HASH256 used in Bitcoin [14] executes SHA256 twice consecutively on the input string. The output of SHA256 can be truncated, and the SHA224 hash function works in the same way, resulting in a shorter hash at the expense of reduced security.

III. ANALYSIS OF THE ANTI-INTERFERENCE SCHEME

When a target exists in a certain space, the signal transmitted by the radar is affected by the target distance, angle, velocity, and other parameters and then reflected back in the form of an echo. In the radar receiver, by analyzing the received signal, information such as the distance, angle, and speed of the target can be obtained. Radar detects the presence of a target and measures its parameter information by detecting and analyzing the echo signal, however, the purpose of the interference is to disrupt or hinder the radar from finding the target and measuring the target parameters.

Active deception jamming based on DRFM technology is highly harmful due to its high efficiency, deception, and flexibility, and the interference effect, which is remarkable, is part of active radar interference. Automobile millimeter-wave radar is vulnerable to spoofing attacks. The replication and retransmission of radar transmission signals introduce false information to destroy the received data, causing the radar to report erroneous information, which greatly increases the risk of collision.

A. PRINCIPLE OF DECEPTION JAMMING

The jammer provides false information to the radar by replicating and retransmitting the radar-transmitted signal and destroying the received data, thus confusing and disrupting the system. Spoofing, on the other hand, creates false signals

by imitating the real signal and adding appropriate modulation to forge a signal and inject it into the system to be disrupted.

Obviously, the distance R between the radar and the target can be expressed as the time delay τ between the radar-transmitted signal $\mathcal{S}_{tran}$ and the received signal $\mathcal{S}_{rec}$, where the time delay τ is expressed as

$$\tau = \frac{2R}{c} \tag{20}$$

where c is the propagation speed of the speed of light.

Let $\mathbb{SPACE}$ denote the observation space of radar for various types of targets (also called the range of power observation for various types of targets). For radars with four-dimensional (distance, azimuth, elevation and speed) observation capabilities, the typical $\mathbb{SPACE}$ is

$$\mathbb{SPACE} = \{[R_{min}, R_{max}], [\alpha_{min}, \alpha_{max}], [\beta_{min}, \beta_{max}], [f_{d_{min}}, f_{d_{max}}], [S_{i_{min}}, S_{i_{max}}]\} \tag{21}$$

where R_{min} and R_{max} represent the minimum and maximum observation distances, respectively; α_{min} and α_{max} indicate the minimum and maximum observation orientations, respectively; β_{min} and β_{max} indicate the minimum and maximum detected elevation angles, respectively; $f_{d_{min}}$ and $f_{d_{max}}$ indicate the minimum and maximum detected Doppler frequencies, respectively; and $S_{i_{min}}$ and $S_{i_{max}}$ represent the minimum detected signal power and saturated input signal power (echo power), respectively.

The ideal point target $\mathbf{T}$ is just one of a number of points in space $\mathbb{SPACE}$:

$$\mathbf{T} = \{R, \alpha, \beta, f_d, S_i\} \in \mathbb{SPACE} \tag{22}$$

where R represents the distance to the target, α represents the orientation of the target, β represents the elevation angle to the target location, f_d represents the Doppler frequency of the target, and S_i represents the echo power of the target.

According to the definition of $\mathbb{SPACE}$, $\triangle\mathbb{SPACE}$ can be denoted as

$$\triangle\mathbb{SPACE} = \{\triangle R, \triangle\alpha, \triangle\beta, \triangle f_d, [S_{i_{min}}, S_{i_{max}}]\} \tag{23}$$

where $\triangle R$ is the radar's range resolution, $\triangle\alpha$ is the azimuth resolution, $\triangle\beta$ is the elevation resolution, and $\triangle f_d$ is the speed resolution, whose energy is the same as that of the observation range.

Under general conditions, the false target $\mathbf{T}_f$ formed by deceptive jamming is also a set of one or a group of certain fixed points in $\mathbb{SPACE}$ that are different from the true target $\mathbf{T}$, so the false target can also be detected by radar to achieve the jamming purpose of treating the false target as the true target or disrupting the observation of the true target with the false target.

The key points of the deceptive interference technique for true and false targets are explained by the following formula:

$$\{\mathbf{T}_{f_i}\}_{i=1}^{n} \quad \mathbf{T}_{f_i} \in \mathbb{SPACE} \quad \mathbf{T}_{f_i} \neq \mathbf{T} \quad i = 1, \ldots, n \tag{24}$$

where $\mathbf{T}_{f_i}$ represents the i-th false target scattering point and $\mathbf{T}$ represents the true target.

If the false target interference is to be successful, the following formula must be satisfied:

$$|\mathbf{T}_f - \mathbf{T}| > \triangle\mathbb{SPACE} \tag{25}$$

In other words, the parameter difference of the true and false targets is greater than the spatial resolution of the radar. The radar can distinguish $\mathbf{T}_f$ and $\mathbf{T}$ as two different targets, but it is possible to detect and track false targets as real targets, resulting in a false alarm, or it may not find the true target, resulting in an alarm failure.

There are many different types of spoofing interference; a brief introduction to three types of spoofing interference is as follows:

- Distance deception interference:

$$R_f \neq R, \quad \alpha_f \approx \alpha, \beta_f \approx \beta, f_{d_f} \approx f_d, S_f > S \tag{26}$$

  With distance deception interference, the distance to the false target is different from that of the true target, the energy is often stronger than that of the true target, and the remaining parameters are approximately equal to those of the true target.
- Angle deception interference:

$$\alpha_f \neq \alpha \text{ or } \beta_f \neq \beta, \quad R_f \approx R, f_{d_f} \approx f_d, S_f > S \tag{27}$$

  With angle deception interference, the azimuth or elevation angle of the false target is different from that of the true target, the energy is stronger than that of the true target, and the remaining parameters are approximately equal to those of the true target.
- Speed deception interference:

$$f_{d_f} \neq f_d, \quad R_f \approx R, \alpha_f \approx \alpha, \beta_f \approx \beta, S_f > S \tag{28}$$

  With speed deception jamming, the Doppler frequency of the false target is different from that of the true target, the energy is stronger than that of the true target, and the remaining parameters are approximately equal to those of the true target's parameters.

Radar can distinguish different targets in the distance, which mainly depends on the distance resolution $\triangle R$:

$$\triangle R = \frac{c}{2B} \tag{29}$$

Spoofing attacks are designed to confuse the target victim and focus on the signal reception. If there are no means to detect the signal, the receiver cannot filter the spoofing signal; a spoofing attack that disrupts the target radar for a short period of time can have a serious impact on the behavior of the target vehicle, possibly causing it to stop, change direction, or crash.

B. ANTI-INTERFERENCE SCHEME

As mentioned in the first part of this work, there are many relevant anti-interference schemes. Here, it is proposed to combine the hash function to obtain a scheme that is more

advantageous than a pure random function, and relevant simulation experiments are carried out in the following part.

For convenience of description, Equation (12) is expressed as Equation (30).

$$\mathcal{S}_{tran}(\hat{t}, t_\kappa) = \sum_{i=0}^{N-1} A_n rect(\frac{\hat{t} - i\mathcal{T}_{PRI}}{\mathcal{T}_p}) e^{j2\pi(f_c t + \mu \frac{(\hat{t} - i\mathcal{T}_{PRI})^2}{2})} \tag{30}$$

The relationship between $\mathcal{T}_{PRI}$ (the pulse repetition interval), $\hat{t}$, t_κ, and t is as follows: $t = \hat{t} + t_\kappa, t_\kappa = \kappa\mathcal{T}_{PRI}$.

Similar to Equation (13), $rect(\frac{\hat{t}}{\mathcal{T}_p})$ denotes a rectangular pulse of width $\mathcal{T}_p$.

From the above, we can know that the true target echo can be expressed as

$$\begin{aligned} \mathrm{y}_{true}(t) &= \sum_{i=1}^{N} \sigma_i A_i \mathcal{S}_{tran}(\hat{t} - \frac{2R_{i\kappa}}{c}, t_\kappa) \\ &= \sum_{i=1}^{N} \sigma_i A_i rect(\frac{\hat{t} - \frac{2R_{i\kappa}}{c}}{\mathcal{T}_p}) e^{j2\pi(f_c(t - \frac{2R_{i\kappa}}{c}) + \mu \frac{(\hat{t} - \frac{2R_{i\kappa}}{c})^2}{2})} \end{aligned} \tag{31}$$

where N is the number of scattering of the true target and σ_i is the scattering coefficient of the i-th scattering center. $R_{i\kappa}$ is the distance from the radar for the i-th target at $t_\kappa = \kappa\mathcal{T}_{PRI}$.

The false target echo can be expressed as

$$\begin{aligned} \mathrm{y}_{jam}(t) &= \sum_{l=1}^{L} \sigma_l A_l \mathcal{S}_{tran}(\hat{t} - \frac{2R_{l\kappa}}{c}, t_\kappa) \\ &= \sum_{l=1}^{L} \sigma_l A_l rect(\frac{\hat{t} - \frac{2R_{l\kappa}}{c}}{\mathcal{T}_p}) e^{j2\pi(f_c(t - \frac{2R_{l\kappa}}{c}) + \mu \frac{(\hat{t} - \frac{2R_{l\kappa}}{c})^2}{2})} \end{aligned} \tag{32}$$

where L is the number of scattering of the false targets and σ_l is the scattering coefficient of the i-th scattering center. $R_{l\kappa}$ is the distance from the radar for the i-th target at $t_\kappa = \kappa\mathcal{T}_{PRI}$.

The signal received by the radar contains the target echo and the interference signal and is expressed as

$$\begin{aligned} &\mathrm{y}_{echo}(t) \\ &= \mathrm{y}_{true}(t) + \mathrm{y}_{jam}(t) \\ &= \sum_{i=1}^{N} \sigma_i A_i rect(\frac{\hat{t} - \frac{2R_{i\kappa}}{c}}{\mathcal{T}_p}) e^{j2\pi(f_c(t - \frac{2R_{i\kappa}}{c}) + \mu \frac{(\hat{t} - \frac{2R_{i\kappa}}{c})^2}{2})} \\ &\quad + \sum_{l=1}^{L} \sigma_l A_l rect(\frac{\hat{t} - \frac{2R_{l\kappa}}{c}}{\mathcal{T}_p}) e^{j2\pi(f_c(t - \frac{2R_{l\kappa}}{c}) + \mu \frac{(\hat{t} - \frac{2R_{l\kappa}}{c})^2}{2})} \end{aligned} \tag{33}$$

There are three different cases used for comparison here: the standard LFM signal, the signal with the rand function based on amplitude modulation, and with the hash function based on amplitude modulation. The principle used here is to conduct correlation processing between the echo and the reference signal, and the matching filter is based on the transmitted signal. After receiving the echo, the output of the filter is obtained by convolution.

Suppose the impulse response of the matched filter in the time domain is

$$h(t) = \mathrm{y}^*_{tran}(t_\kappa - t) \tag{34}$$

Then, the output of the filter is expressed as

$$\mathrm{y}_{out}(t) = \int_{-\infty}^{\infty} \mathrm{y}_{tran}(s) h(t - s) ds \tag{35}$$

Since the DRFM jammer needs to store the intercepted radar signal and delay it for a certain period of time, the jammer cannot have the function of transmitting and receiving at the same time. Usually, the jammer needs a certain processing delay for the intercepted signal, and the delay of the forwarded interference signal is typically greater than a $\mathcal{T}_{PRI}$ [15]. By modulating the envelope of different pulse repetition period signals and embedding a certain number of random numbers, the pulse signals of different repetition periods can carry different encryption information that can be known only by the user.

IV. SIMULATION RESULTS AND DISCUSSION

The main anti-interference idea is to design a radar transmission signal with a certain relationship between the target echo signal and the interference return signal in the time domain or frequency domain and suppress the interference signal by a certain anti-interference method.

The two envelope modulation methods used here for comparison are the rand function and the hash function mentioned above. Using the difference of the information A_n, interference recognition is achieved by matching the echo signals.

According to the above, detailed descriptions are given here, including the basic parameter settings and specific scenarios.

A. SCENARIO SETTINGS

The radar transmission signal is set to the LFM signal; the bandwidth is 100 MHz, the time width is 2 μs, and the pulse repetition period is 8 μs. The equation used here is (30). In the scheme, a sequence of envelope addition A_n with a quantization number of 8 is added to the signal envelope in each pulse repetition period, and A_n is the information carried by the signal. For false target interference, in an echo pulse repetition period, a real target echo and an interference echo are included, and the interference is identified by matching the echo signal by using the difference of the information A_n.

For the LFM signal in the slow time domain, the transponder chirp signal is delayed by $k\mathcal{T}_{PRI}$ relative to the radar-transmitted signal, and the interference signal delay is set to a $\mathcal{T}_{PRI}$ for convenience. Then, the A_i signal added to the target echo in the same pulse repetition period is different from the

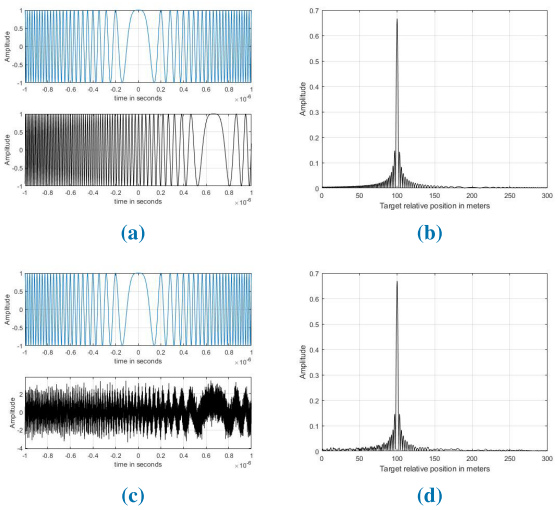


FIGURE 2. LFM simulation results for a target. (a) LFM and its echo at Range=100 m. (b) The result of pulse compression. (c) Adding SNR=0 dB noise to the echo compared to (a). (d) The result of pulse compression.

A_{i-1} signal of the false echo. When the interference signal delays the target echo signal by one or more pulses, the target echo signal does not overlap with the interference echo signal.

There are three situations in this scenario:

1) $A_n = 1$;
2) Using the rand function to generate A_n, with A_n quantized to 8 bits;
3) Using the SHA256 output hash value $H(x \parallel r)$ and processing the hash value to generate A_n, with A_n also quantized to 8 bits.

B. PERFORMANCE ANALYSIS

Simulation experiments were carried out on three kinds of modulation cases, including the assumption that there is only one true target and the assumption that there is a true target and a false target. The echo equation used here is Equation (33), and the radar cross section RCS is set to $\sigma = 1\ m^2$. The noise used here is white noise.

1) SIMULATION OF THE LFM

According to Equation (30), S_{tran} is modeled; when $An = 1$, the envelope is not modulated, and the complex envelope of the signal can be simply expressed as

$$\mathcal{S}_{lfm_{com}}(t) = rect(\frac{t}{\mathcal{T}_p})e^{j\pi\mu t^2} \tag{36}$$

In the case of $\mathcal{T}_{PRI} = 8\mu s$, the maximum unambiguous distance is

$$\mathcal{R}_{max} = \frac{C * \mathcal{T}_{PRI}}{2} \tag{37}$$

The results obtained from a simulation in conjunction with Equation (36) are shown in Figure 2.

As shown in Figure 2, the distance performance of the LFM signal is almost unchanged in the case of noise, and the performance is ideal.

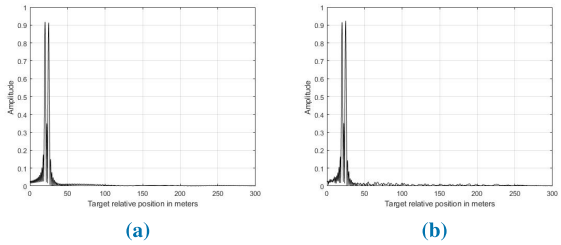


FIGURE 3. Matched filtering result. (a) The result of pulse compression (without noise). (b) The result of pulse compression (noise).

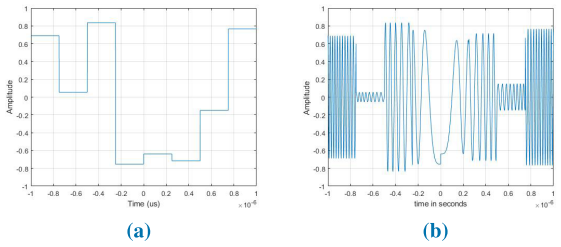


FIGURE 4. Random number modulation envelope simulation. (a) A_n. (b) Waveform after modulation.

Next, the echo containing the real signal and the interference signal is detected using the standard LFM signal. Here, the distance of the true target is set to 20 in meters, and the distance of the false target is set to 25 in meters. The results are presented in Figure 3.

As shown in Figure 3, the original LFM signal is also ideal for detecting false targets, but this is not what we want but what the attacker wants. The peaks in Figure 3 (a) at 20.09 is 0.9177 and at 24.87 is 0.9129, the peaks in Figure 3 (b) at 20.1 is 0.9163 and at 24.87 is 0.9237, so $\Delta Peak$ is 0.0014.

The focus of the discussion here is how to improve the anti-interference capability based on random numbers.

2) SIMULATION OF AMPLITUDE MODULATION BASED ON RANDOM NUMBERS WITH AN ENVELOPE

In this part of the experiment, the simulation is divided into two parts, both of which use a matching function for the envelope of the random number modulated signal. The first part contains the key goal, which is to correlate the signal with itself and then relate it to the echo of the target, as shown in Figure 4.

Obviously, the performance relative to that of the original LFM signal has decreased. Figure 5 shows the results for detecting a true target using the modulated signal.

Next, we simulate the transmission of two adjacent signals. The information of the modulation envelope is A_{n_1} and A_{n_2}, as shown in Figure 6.

Assuming that the interfering signal differs from the true signal by a pulse repetition interval (PRI), the echo is simulated with noise and without noise.

The simulated echo includes the echo of the true target and the echo of the false target; distance performance is then performed, as shown in Figure 7.

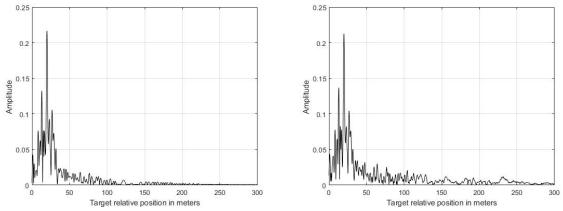


FIGURE 5. Performance of a true target with a modulated signal. (a) The distance performance (without noise). (b) The distance performance (noise).

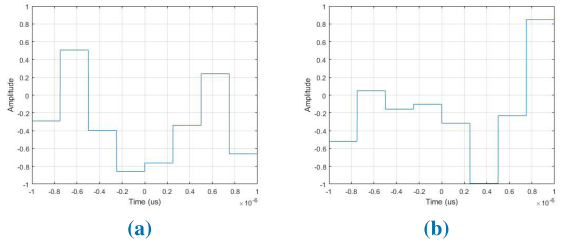


FIGURE 6. Simulation of two adjacent modulated signals. (a) Modulation information A_{n_1}. (b) Modulation information A_{n_2}.

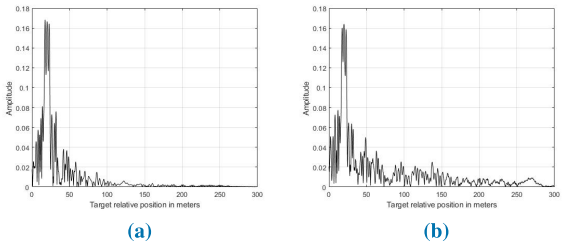


FIGURE 7. Performance of echoes containing true and false targets. (a) The distance performance (without noise). (b) The distance performance (noise).

As shown in Figure 7, the performance of the true target with Range=20 m is higher than that of the false target with Range=25 m, but there are many side lobes that have a strong influence. If random number modulation is generated multiple times, there may be a transmitted signal with a good performance effect. However, this condition is very difficult to control, which leads to the application of the hash function.

3) SIMULATION EXPERIMENT BASED ON A HASH FUNCTION

The hash function used here is SHA256, which is the most widely used hash function, and the security is relatively high. The basic properties are discussed in section II-C. The number processed here is the average grouping of the obtained hash values, which is then normalized to obtain the corresponding A_n. Because of the output nature of the hash function, A_n has a certain randomness. The experimental results here are compared with those in section IV-B.2.

In this part, matching filtering is performed on echoes containing the true target and the false target, indicating that performance is feasible in this case. Two experiments are performed, and the input to SHA256 is different in the two experiments. More detailed performance descriptions and comparisons are described in section IV-C.

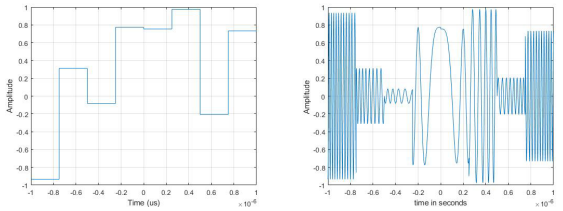


FIGURE 8. Modulation envelope simulation. (a) A_n generated by a hash value. (b) Waveform after modulation.

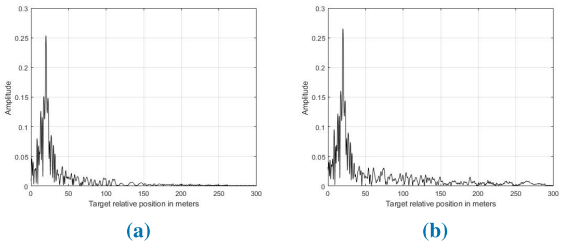


FIGURE 9. Performance of a true target with a modulated signal. (a) The distance performance (without noise). (b) The distance performance (noise).

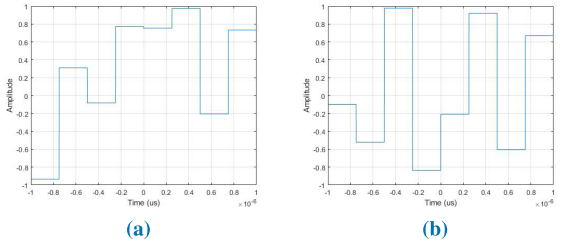


FIGURE 10. Simulation of adjacent transmitted signals. (a) A_{n_1} generated by a hash value. (b) A_{n_2} generated by a hash value.

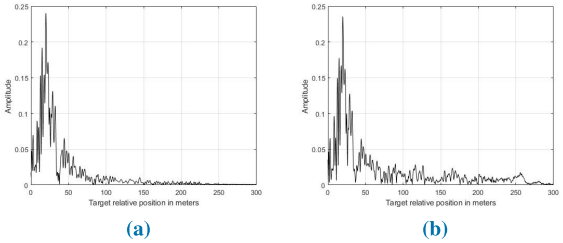


FIGURE 11. Performance of echoes containing the true and false targets (the false target is suppressed). (a) The distance performance (without noise). (b) The distance performance (noise).

This part reports the comparison with section IV-B.2, the simulation for the generated A_n, and simulates the transmitted signal, as shown in Figure 8.

Figure 9 shows the results obtained by the signal of the Figure 8 performance target.

Figure 8 and 9 show the performance of a true target using the transformed waveform. Figure 10 and 11 assume that there is both a true target and a false target. The modulated information of the false target is different from the modulated information of the true target, so the false target is suppressed.

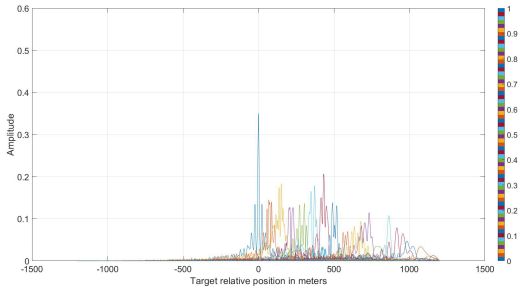


FIGURE 12. Randomly generated 64 groups of $\mathcal{S}_{rand}$ for the performance analysis (with a time delay).

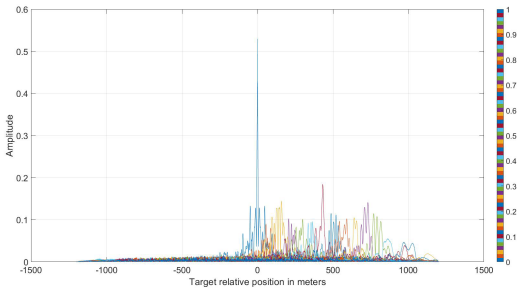


FIGURE 13. The performance of sixty-four consecutive inputs (with a time delay).

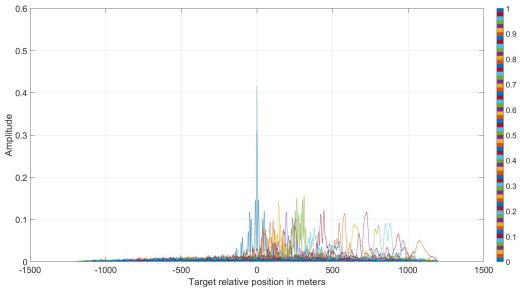


FIGURE 14. The performance of sixty-four consecutive inputs plus rand (with a time delay).

Figure 10 shows the use of two different input values to obtain two different types of information. Figure 11 assumes that there is a true target echo with a false target echo. The currently used waveform suppresses the outdated waveform. The results obtained are shown in Figure 11.

Figure 11 shows the results of the processing of the echo signal. Since the interference signal differs from the transmission signal, the modulation information A_n of the two signals is different, so the interference signal can be suppressed. The distance to the true target in Figure 11 is showed as Range=20 m; the result is Range=20 m, as expected, and the performance of the false target is not obvious.

Compared with the results shown in Figure 11, the performance effect in Figure 7 is poor. However, the advantage of using the hash function is that the transmitted signal with good performance can be reproduced when the input is known. The hash function is a deterministic random function. One application that may be used is to select a signal with good performance to create a collection of transmission signals under a certain large base.

C. RANDOM NUMBER VS HASH VALUE: COMPARISON EXPERIMENT

Many experiments have been carried out in this research area, mainly to detect the correlation of signals modulated by two different modulation methods, which are divided into two parts: one part is the signal $\mathcal{S}_{rand}$ modulated based on the modulation of the pseudorandom rand function, and the other part is the signal $\mathcal{S}_{hash}$ modulated based on the modulation method of the hash function. The match performance of the signals are analyzed.

(1) $\mathcal{S}_{rand}$ correlation analysis

The determinacy of signals based on pseudorandom function modulation causes its different outputs every time, so the performance is unstable, and there is a lack of controllability. The simulation results for the randomly generated 64 groups of $\mathcal{S}_{rand}$ for the matching performance analysis are shown in Figure 12.

Because the signal generated based on the pseudorandom method is unstable, there is no relationship between the generated signals. As shown in Figure 12, the difference value between y coordinate of the first highest point and the second highest point is 0.1443.

(2) $\mathcal{S}_{hash}$ correlation analysis

For a hash function, the input can be direct or timestamped. When the input is direct, set the hash value to $H(x)$, and take x as the input. When the input has a timestamp, it sets the hash value to $H(x\|r)$, and takes $x\|r$ as the input.

1) The input of $H(x)$ only contains x.

A total of 64 correlation processes are performed here. S_{hash} is related to 64 consecutive inputs. Simulations with a time delay are performed.

$$string = [\text{'}ID01\text{'}, \text{'}ID02\text{'}, \cdots, \cdots, \text{'}ID64\text{'}] \tag{38}$$

The results are shown in Figure 13. The difference value between y coordinate of the first highest point and the second highest point is 0.345.

2) An additional assistant input r for H is added, which is denoted as $H(x||r)$.

The r can also be a timestamp. By simply adding changes to the continuous input, the changes here are generated with rand, i.e., r =rand. In practical applications, the timestamp can be used with timing to assign r. The experimental results are shown in Figure 14. The difference value between y coordinate of the first highest point and the second highest point is 0.2607.

(3) The relationships of the difference $\Delta peaks$ between the first and second peaks with the signal-to-noise ratio (SNR).

The SNR calculation methods are expressed as follows:

$$SNR = 10\lg(\frac{P_s}{P_n}) \tag{39}$$

where P_s represents the power of the signal, P_n is the power of the noise.

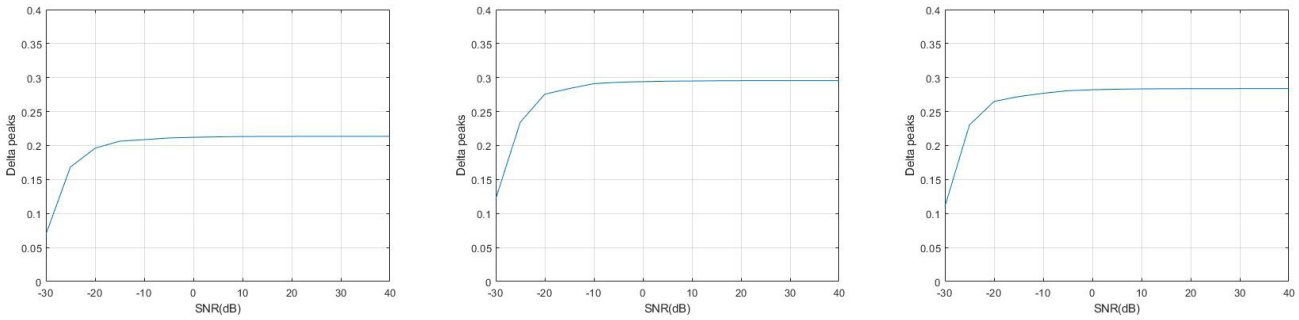


FIGURE 15. Experimental performance comparisons. (a) The relationship between SNR and the average of $\Delta peak$ ($\mathcal{S}_{rand}$). (b) The relationship between SNR and the average of $\Delta peak$ ($\mathcal{S}_{hash}$). (c) The relationship between SNR and the average of $\Delta peak$ ($\mathcal{S}_{hash+rand}$).

Taking a sample from the previous three experiments, take the SNR as the abscissa data and the difference between the first and second peaks as the ordinate data, because the added noise is random, the $\Delta peak$ calculation is performed 100 times and then averaged, and draw the plot as shown in Figure 15.

The three sets of results are shown as (a), (b) and (c) in Figure 15. The first group involves $\mathcal{S}_{hash}$, the second group involves $\mathcal{S}_{rand}$, and the third group involves $\mathcal{S}_{hash+rand}$. With the increase of SNR, it can be concluded from the Figure 15 (a), (b), (c) that there is a difference in the final value that tends to be stable under three different conditions. In the case of $\mathcal{S}_{rand}$, the stable value is 0.2136. In the case of $\mathcal{S}_{hash}$, the stable value is 0.2955. In the case of $\mathcal{S}_{hash+rand}$, the stable value is 0.2838. The larger the $\Delta peak$ value, the better the ability to suppress interference echoes. The increase is calculated as 32.87% and 38.34%. So the case of $\mathcal{S}_{hash}$ has the best ability to suppress interference.

As shown in Figure 15, the results of the first group are better than those of the second group. However, the results of the third group of experiments indicate that the third group constitutes a compromise. It can be seen that adding randomized hash function can significantly enhance the performance of the system against echo interference.

V. CONCLUSION

After theoretical analysis and experimental simulation, it can be concluded that the use of the hash function to replace the pseudorandom function is of great significance, both in terms of generating the transmitted signal and in terms of management strategy. After the hash function is introduced, the ability to suppress interference echoes can be enhanced by $32.87\% \sim 38.34\%$. On the one hand, the signal modulated based on the hash function has a certain randomness and can be controlled. For example, using a time stamp to make the modulated signal related to the order of time can be applied to many scenes; on the other hand, the use of hash function modulation signals can create a signal collection that is random but has good performance, but only if there are enough practice data.

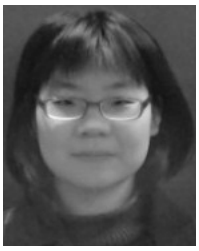
Moreover, the modulation signal modulated based on the hash function is not necessarily modulated on the envelope amplitude but may be modulated in terms of the frequency or phase and even combined with CW, OFDM or other complex waveforms. This result reveals to a certain extent that we are free to control the generation of a random signal.

REFERENCES

[1] RSA Conference. (2018). *Where the World Talks Security*. [Online]. Available: https://www.rsaconference.com/
[2] L. Neng-Jing and Z. Yi-Ting, "A survey of radar ECM and ECCM," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 3, pp. 1110–1120, Jul. 1995.
[3] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
[4] G. Lu, D. Zeng, and T. Bin, "Anti-jamming filtering for DRFM repeat jammer based on stretch processing," in *Proc. 2nd Int. Conf. Signal Process. Syst.*, vol. 1, Jul. 2010, pp. 78–82.
[5] Z. Liu, J. Sui, Z. Wei, and X. Li, "A sparse-driven anti-velocity deception jamming strategy based on pulse-Doppler radar with random pulse initial phases," *Sensors*, vol. 18, no. 4, p. 1249, 2018.
[6] C. Huang, Z. Chen, and R. Duan, "Novel discrimination algorithm for deceptive jamming in polarimetric radar," in *Proc. Int. Conf. Inf. Technol. Softw. Eng.*, vol. 210. Berlin, Germany: Springer, 2013, pp. 359–365. [Online]. Available: http://link.springer.com/10.1007/978-3-642-34528-9_38
[7] M. Nouri, M. Mivehchy, and M. F. Sabahi, "Novel anti-deception jamming method by measuring phase noise of oscillators in LFMCW tracking radar sensor networks," *IEEE Access*, vol. 5, pp. 11455–11467, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7827908/
[8] J. Akhtar, "Orthogonal block coded ECCM schemes against repeat radar jammers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 3, pp. 1218–1226, Jul. 2009.
[9] J. Liu, Y. Zhang, and X. Dong, "High resolution moving train imaging using linear-FM random radar waveform," in *Proc. Asia–Pacific Microw. Conf. (APMC)*, Nov. 2019, pp. 839–841. [Online]. Available: https://ieeexplore.ieee.org/document/8617646/
[10] S. R. J. Axelsson, "Noise radar using random phase and frequency modulation," *IEEE Trans. Geosci. Remote Sens.*, vol. 42, no. 11, pp. 2370–2384, Nov. 2004. [Online]. Available: http://ieeexplore.ieee.org/document/1356052/
[11] Mercury Systems. *DRFM Technology*. Accessed: Dec. 21, 2018. [Online]. Available: https://www.mrcy.com/drfm-technology/
[12] B. V. Nityananda, "Spurs in digital radio frequency memory and applications of DRFM," M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 1993.
[13] R. Sobti and G. Geetha, "Cryptographic hash functions: A review," *Int. J. Comput. Sci.*, vol. 9, no. 2, pp. 461–479, 2012. [Online]. Available: https://www.researchgate.net/profile/Geetha_Ganesan3/publication/267422045_Cryptographic_Hash_Functions_A_Review/links/549cf6d10cf2b8037138c35c.pdf

[14] S. Nakamoto and N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system," BitGive Found., Truckee, CA, USA, Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[15] F. Wang, S. Wei, D. Jiang, Z. Ma, and C. Zhang, "DRFM jamming suppression for radar exploiting linear frequency modulation transmission," in *Proc. CIE Int. Conf. Radar (RADAR)*, no. 8, Oct. 2016, pp. 1–4.
[16] C. Zhou, F. Liu, and Q. Liu, "An adaptive transmitting scheme for interrupted sampling repeater jamming suppression," *Sensors*, vol. 17, no. 11, p. 2480, 2017.
[17] S. J. Roome, "Digital radio frequency memory," *Electron. Commun. Eng. J.*, vol. 2, no. 4, pp. 147–153, 2009.
[18] A. Almslmany, "Spoofing technique based on digital radio frequency memory and chaotic algorithm," *WSEAS Trans. Commun.*, vol. 16, no. 30, pp. 281–287, 2017.
[19] G. Lu, S. Liao, S. Luo, and B. Tang, "Cancellation of complicated DRFM range false targets via temporal pulse diversity," *Prog. Electromagn. Res.*, vol. 16, pp. 69–84, Sep. 2010.
[20] A. Abdalla, Z. Yuan, M. Ramadan, and T. Bin, "An improved radar ECCM method based on orthogonal pulse block and parallel matching filter," *J. Commun.*, vol. 10, pp. 610–614, Aug. 2015.
[21] S. Jonathan and G. Dmitriy, "Performance of random OFDM radar signals in deception jamming scenarios," in *Proc. IEEE Radar Conf.*, May 2009, pp. 1–6.
[22] K. Tony. *Driving Toward Safety: Automotive Industry Struggles With Security in Rolling Out Connected Vehicles*. [Online]. Available: https://www.rsaconference.com/blogs
[23] M. Soumekh, "SAR-ECCM using phase-perturbed LFM chirp signals and DRFM repeat jammer penalization," in *Proc. IEEE Int. Radar Conf.*, May 2005, pp. 507–512.
[24] A. Abdalla, Z. Yuan, S. N. Longdon, J. C. Bore, and T. Bin, "A study of ECCM techniques and their performance," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput. (ICSPCC)*, Sep. 2015, pp. 1–6.
[25] B. Mahafza and A. Elsherbeni, *Radar Systems Analysis and Design Using MATLAB*. Boca Raton, FL, USA: CRC Press, 2003. [Online]. Available: https://www.taylorfrancis.com/books/9780203502556
[26] L. Wei, X. Yang, Z. Chao, S. Li, and L. Ning, "DRFM range false target cancellation method based on slope-varying LFM chirp signal," in *Proc. IEEE 13th Int. Conf. Signal Process. (ICSP)*, Nov. 2017, pp. 1629–1632.
[27] K. A. Lukin and R. M. Narayanan, "Historical overview and current research on noise radar," in *Proc. IEEE 3rd Int. Asia–Pacific Conf. Synthetic Aperture Radar (APSAR)*, Sep. 2011, pp. 1–2.
[28] L. Xu, H. Liu, S. Zhou, J. Liu, and J. Yan, "Colocated MIMO radar waveform design against repeat radar jammers," in *Proc. Int. Conf. Radar (RADAR)*, Aug. 2018, pp. 1–5.

ZHENYU GUAN (M'17) received the Ph.D. degree in electronic engineering from Imperial College London, U.K., in 2013. He then joined Beihang University (China) as a Lecturer. His current research interests include cryptography engineering, security of the IoT, and blockchain. He is a member of IEICE.



YONGJIANG CHEN received the bachelor's degree from the Beijing University of Chemical Technology, Beijing, China, in 2018. She is currently pursuing the master's degree with Beihang University, Beijing.

PENG LEI received the B.S. and Ph.D. degrees in electrical engineering from Beihang University, Beijing, China, in 2006 and 2012, respectively, where he is currently an Assistant Professor with the School of Electronic and Information Engineering. His research interests include signal processing, especially in time–frequency analysis and spectral estimation, image processing, and target recognition. He was a recipient of the 2011 IEEE IGARSS Student Travel Grant.

DAWEI LI was born in Shandong, China. He received the B.S. degree from Beihang University, Beijing, China, in 2015, where he is currently pursuing the Ph.D. degree in electronic and information engineering. His research interests include applied cryptography and blockchain.

YING ZHAO received the bachelor's degree from Northeastern University, Shenyang, China, in 2017. She is currently pursuing the master's degree with Beihang University, Beijing, China. Her research interests include blockchain and trusted computing.