Hindawi
Security and Communication Networks
Volume 2018, Article ID 3580536, 13 pages
https://doi.org/10.1155/2018/3580536

Research Article

Modeling and Simulation for the Investigation of Radar Responses to Electronic Attacks in Electronic Warfare Environments

So Ryoung Park,[1] **Ilku Nam**,[2] **and Sanguk Noh**[3]

[1]*School of Information, Communications, and Electronics Engineering, The Catholic University of Korea, Bucheon, Republic of Korea*
[2]*Department of Electrical Engineering, Pusan National University, Busan, Republic of Korea*
[3]*School of Computer Science and Information Engineering, The Catholic University of Korea, Bucheon, Republic of Korea*

Correspondence should be addressed to So Ryoung Park; srpark@catholic.ac.kr

Received 18 November 2017; Accepted 5 March 2018; Published 5 April 2018

Academic Editor: Prem Mahalik

An electronic warfare (EW) simulator is presented to investigate and evaluate the tracking performance of radar system under the electronic attack situations. The EW simulator has the input section in which the characteristic parameters of radar threat, radar warning receiver, jammer, electromagnetic wave propagation, and simulation scenario can be set up. During the process of simulation, the simulator displays the situations of simulation such as the received signal and its spectrum, radar scope, and angle tracking scope and also calculates the transient and root-mean-squared tracking errors of the range and angle tracking system of radar. Using the proposed EW simulator, we analyze the effect of concealment according to the noise and signal powers under the noise jamming and also analyze the effect of deception by calculating errors between the desired value and the estimated one under the deceptive jamming. Furthermore, the proposed EW simulator can be used to figure out the feature of radar threats based on the information collected from the EW receiver and also used to carry out the electronic attacks efficiently in electronic warfare.

1. Introduction

The collection and analysis of electronic intelligence have been regarded as one of the most important factors for improving the survival rate of friendly forces in modern electronic warfare (EW). The radar warning receiver (RWR) receives radio frequency (RF) signals radiated from radar threats and extracts the characteristic parameters from the RF signals in which the features of radar threats can be included. The characteristic parameters have been used to identify the detecting or tracking type of radar threats and then to attack the electronic circuit of radar tracking system effectively in the integrated EW environments with multiple and complex threats of the enemy forces [1–4].

Recently, intelligent decision-making problems in integrated EW environments have been actively studied [5–7]. Among these studies, the system in [7] performs reverse extrapolation in order to identify and classify threats by using profiles compiled through a series of machine learning algorithms, that is, naive Bayesian classifier, decision tree, neural network, and k-means clustering algorithms. In other words, the system in [7] has focused on improving the performance of learning algorithms to enhance the accuracy of reverse modeling. However, to examine and verify the performance of various learning algorithms in a realistic and detailed EW situation, we need an effective simulator which has the essential elements of EW, such as detecting and tracking radar threats, jamming for electronic countermeasures or attacks, propagation of electromagnetic waves, and simulation of battle scenarios.

There have been a lot of researches on the modeling and simulation for particular parts of radar system, recognition methods of the characteristics of RF threats, specific jamming technologies, or propagation characteristics including [8–11]. In addition, some researches on the discrete event simulation in EW environments have been carried out with the purpose

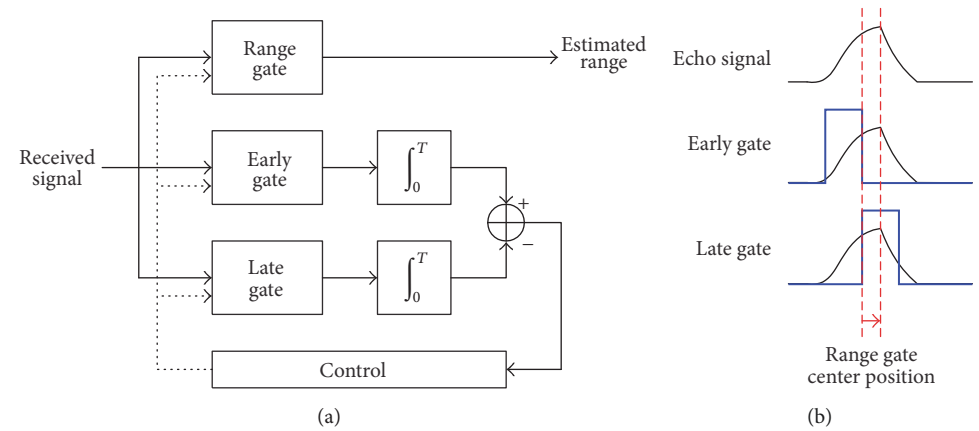

Figure 1: The range tracking scheme: (a) the block diagram of tracking circuit and (b) the operation principle.

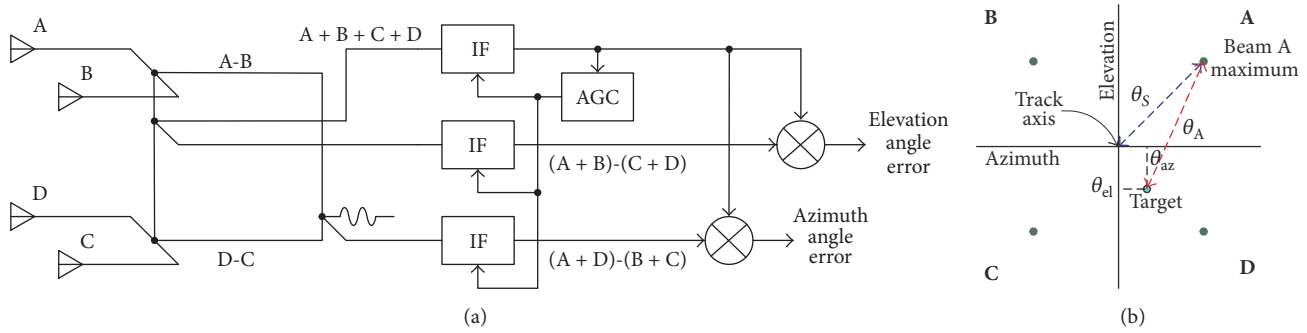

Figure 2: The angle tracking scheme: (a) the block diagram of tracking circuit and (b) the operation principle.

of handing a lot of variables and multiagents [12–14]. However the research on the modeling and simulation considering all the essential functions of EW from a signal processing point of view is rare. In order to achieve the simulation results that are very similar to the actual reality, each function module in simulator have to be modeled precisely. For example, the module for constant false alarm rate (CFAR) radar has to operate in accordance with the detection theory, and the module for propagation of electromagnetic wave has to consider the free space loss and Doppler effects. In passing, let us note that the theme of signal detection, the basis of radar detection, has been extensively studied in the literature including [15–19].

In this research, we present an EW simulator that includes the modules of antenna, intermediate frequency (IF) conversion, automatic gain control (AGC), CFAR detection, range tracking, angle tracking, and velocity estimation for radar threat; the module of noise jamming, range deceptive jamming, velocity deceptive jamming, and range-velocity complex jamming for electronic attack; the motion control module for aircraft with RWR and jammer; the module of signal attenuation, frequency shifting, and multipath spreading for the propagation of electromagnetic wave. We have designed the modules of proposed EW simulator in compliance with the theoretical model or the principles of circuit operation.

The following three sections describe the radar modeling, the electronic attack modeling, and the propagation modeling of the proposed EW simulator. Section 5 shows and analyzes the simulation results. In conclusion, we summarize our result and discuss further research issues.

2. Radar Modeling

Among the various function modules in radar threat, we describe the modeling methods of three important modules related to detecting and tracking which are the most basic functions of the surveillance radar. The three important modules are the range tracking, angle tracking, and CFAR.

2.1. The Range Tracking Module. We adopt the circuit of early-late gate as shown in Figure 1 to the operation principles of the range tracking scheme in radar threat of the proposed EW simulator. The received signal is integrated through the early gate when the amplitude of the signal begins to rise above a certain threshold. The early gate is closed after holding the half of pulse width and the received signal is integrated through the late gate during the half of pulse width. The range can be calculated using the pulse location obtained from the difference of two integrated values.

2.2. The Angle Tracking Module. To the operation principles of the angle tracking scheme in radar threat, we also adopt the circuit of amplitude-compared monopulse as shown in Figure 2 [20]. The monopulse radar measures a target return on four sides of the tracking axis simultaneously as shown

in Figure 2(b). For a beam with its maximum in quadrant 1, displacement from the beam maximum can be written as

$$\left(\frac{\theta_s}{\sqrt{2}} - \theta_{\text{el}}\right)^2 + \left(\frac{\theta_s}{\sqrt{2}} - \theta_{\text{az}}\right)^2 = \theta_{\text{A}}^2, \quad (1)$$

where θ_s is the squint angle of the monopulse beam, θ_{el} and θ_{az} are the differences of elevation angles and azimuth angles between the tracking axis and target, respectively, and θ_{A} is the angle difference between the beam maximum of quadrant 1 and target. Assuming that the antenna pattern be modeled as a Gaussian and the differences of elevation angles and azimuth angles are small enough, that is, $\theta_{\text{el}}^2 + \theta_{\text{az}}^2 \approx 0$, the quadrant 1 voltage gain is

$$g(\theta_{\text{A}}) = g_0 \left\{1 + \frac{k}{\theta_3}(\theta_{\text{az}} + \theta_{\text{el}})\right\}, \quad (2)$$

where $g_0 = g(\theta_s)$, θ_3 is the 3 dB beamwidth and $k = 2\sqrt{2}\ln 2\theta_s/\theta_3$. In the same way as (2), the voltage gains of quadrant 2, 3, and 4 can be obtained as

$$g(\theta_{\text{B}}) = g_0 \left\{1 - \frac{k}{\theta_3}(\theta_{\text{az}} - \theta_{\text{el}})\right\}, \quad (3)$$

$$g(\theta_{\text{C}}) = g_0 \left\{1 - \frac{k}{\theta_3}(\theta_{\text{az}} + \theta_{\text{el}})\right\}, \quad (4)$$

$$g(\theta_{\text{D}}) = g_0 \left\{1 + \frac{k}{\theta_3}(\theta_{\text{az}} - \theta_{\text{el}})\right\}, \quad (5)$$

respectively. Let the errors of elevation angle and azimuth angle in Figure 2(a) be shown in equations as $\epsilon_{\text{el}} = 4g_0k\theta_{\text{el}}/\theta_3$ and $\epsilon_{\text{az}} = 4g_0k\theta_{\text{az}}/\theta_3$, respectively; then we can obtain $\theta_{\text{el}} = \theta_3\epsilon_{\text{el}}/4g_0k$ and $\theta_{\text{az}} = \theta_3\epsilon_{\text{az}}/4g_0k$ [20].

2.3. The CFAR Module. The threshold of CFAR for detecting target is determined by

$$V_{\text{th}} = \sqrt{2N \ln \frac{1}{P_{\text{fa}}}}, \quad (6)$$

where N is the noise power obtained as

$$\text{SNR} = \left(\sqrt{-\ln P_{\text{fa}}} - \text{erfc}^{-1}(2P_d)\right)^2 - \frac{1}{2},$$
$$\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} dt \quad (7)$$

with the false alarm rate P_{fa} and the detection rate P_d. The signal power in the signal-to-noise power ratio (SNR) is the power of reflecting signal to the target at the maximum range of radar [16].

3. Electronic Attack Modeling

In EW environment, the radar threat detects or tracks the targets by receiving and analyzing the electromagnetic waves that are reflected in targets. The radar jamming means the electronic countermeasure (ECM) or electronic attack (EA) technology and is the intentional radiation or reradiation of RF signals to interfere with the operation of radar. The primary purpose of radar jamming is to create confusion and deny the target information such as position and velocity for negating the effectiveness of enemy radar systems.

One of the fundamental measures of jamming effectiveness is the jamming-to-signal power ratio (JSR):

$$\text{JSR} = \frac{P_J G_J}{P_T G_T} \frac{4\pi R^2}{\sigma}, \quad (8)$$

where P_J is the jamming power, G_J is the antenna gain of jammer, P_T is the peak power transmitted by radar, G_T is the antenna gain of radar, R is the range from jammer to radar, and σ is the radar cross section (RCS) of aircraft with jammer [21]. For a jamming signal to be effective, the JSR must be greater than one. At long ranges, a low power jamming system can generate a JSR much greater than one. At closer ranges, the jamming pulse is no longer masking the aircraft, and the aircraft can be detected in reduced JSR less than one. The point where the radar can see through the jamming is called burn-through range. The proposed EW simulator is designed considering the JSR and burn-through range.

There are generally two types of radar jamming: noise and deception. The noise jamming conceals the target signal with the intentionally radiated noise-like signal and the deception jamming deceives the tracking system of radar with the false information about the critical intelligence such as range, angle, or velocity of target. In the proposed EW simulator, the noise jamming, range deceptive jamming, velocity deceptive jamming, and range-velocity complex jamming are considered under the self-protection scenario [22, 23].

3.1. Noise Jamming. Noise jamming is classed as the barrage and spot noise jamming according to the spectral coverage. The jamming signal of barrage noise is spread over a wide frequency range as shown in Figure 3(b), which lowers the effective radiated power (ERP) at any one frequency and conceals the return signal with random noise as shown in Figure 3(a). Advantages of barrage jamming are its simplicity and ability to cover a wide portion of the electromagnetic spectrum. The primary disadvantage is the low power density, especially when a high JSR is needed against modern radars. One way to take advantage of the noise jammer's simplicity, but raise the jamming signal power, is to use a spot jammer. The jamming signal of spot noise can be a narrow-band signal covering a bandwidth of a radar signal or less as shown in Figure 4(b).

3.2. Deception Jamming. A deception jammer receives the signal from the radar threat and modifies the signal to provide false range, angle, or velocity information. The modified signal is then retransmitted by jammer. In this deceptive jamming process, a digital radio frequency memory (DRFM) system plays an important role [24]. DRFM system is designed to digitize an incoming RF input signal and reconstruct the RF signal coherently when required as shown in Figure 5.

The range deception jammer memorizes the radar signal using DRFM and then amplifies and retransmits the signal

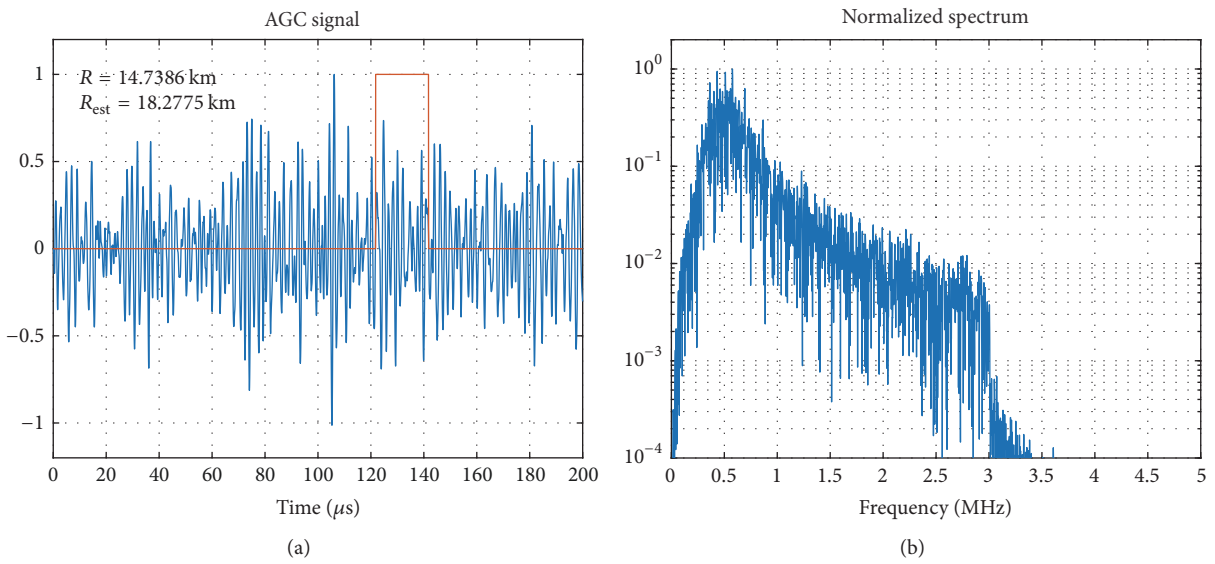

Figure 3: An example of barrage noise jamming: (a) received signal and (b) normalized spectrum.

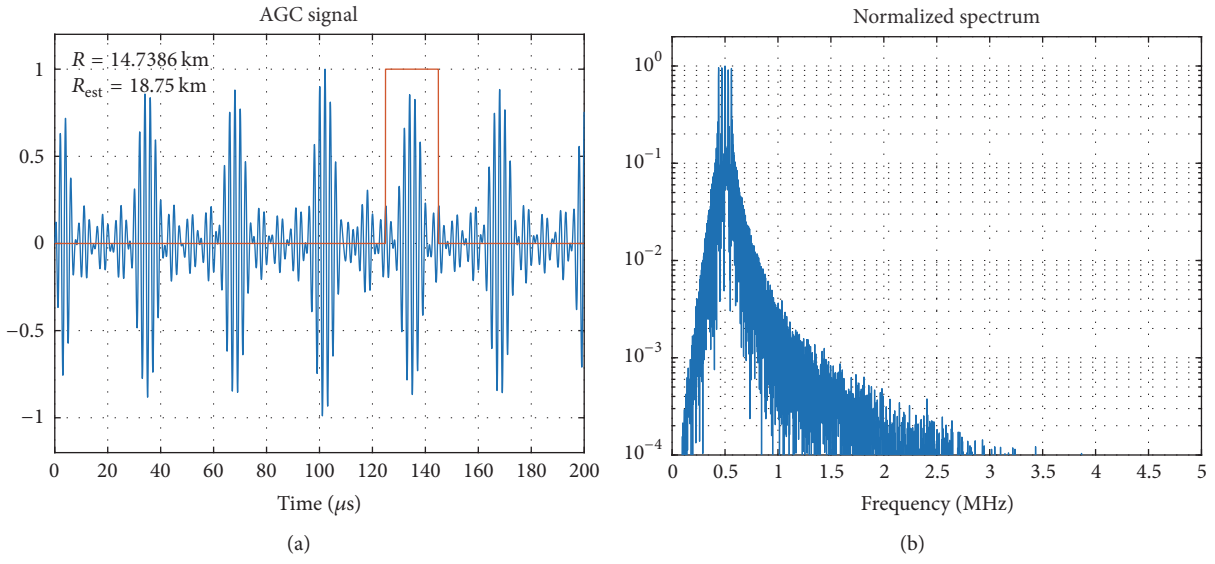

Figure 4: An example of spot noise jamming: (a) received signal and (b) normalized spectrum.

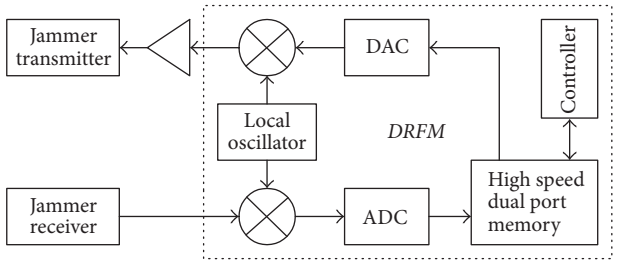

Figure 5: The block diagram of DRFM.

much stronger than the return signal with a certain amount of time delay [25]. By increasing these time delays, the range gate will detect an increase in range and automatically move off to a false range. This range deception method is called a range gate pull-off (RGPO) and we show an example of RGPO signal in Figure 6(a). On the contrary, the range deception method that the range gate will detect an decrease in range and move in to a false range is called a range gate pull-in (RGPI) method, and an example of RGPI signal is shown in Figure 6(b).

Using the same deception method in frequency domain, we can implement the velocity deceptive jamming such as velocity gate pull-off (VGPO) and velocity gate pull-in (VGPI) [26]. We also show examples of VGPO and VGPI spectra in Figures 7(a) and 7(b), respectively. Furthermore, we can implement the range-velocity deceptive complex jamming by transmitting the frequency shifted signal with a corresponding time delay.

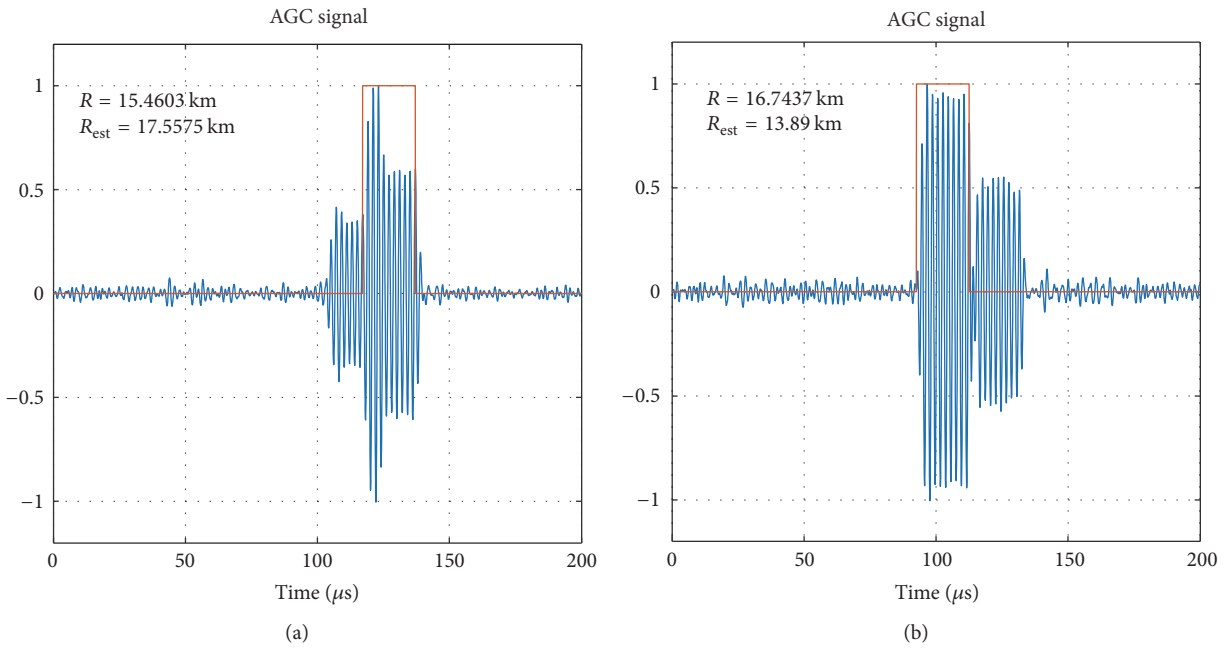

Figure 6: An example of range deceptive jamming: (a) RGPO; (b) RGPI.

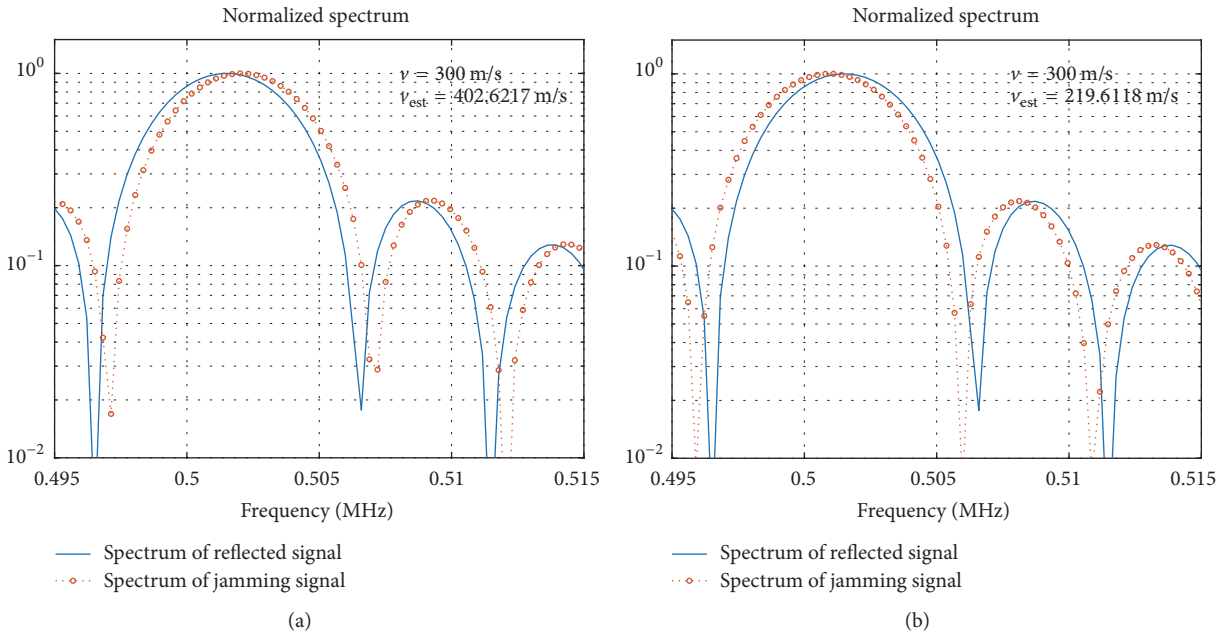

Figure 7: An example of velocity deceptive jamming: (a) VGPO; (b) VGPI.

Lastly, there are several angle deception methods for monopulse radar such as cross-eye jamming that generates angular errors by radiating phase-controlled repeated pulses using separate antennas mounted on an aircraft or other platform [27], but the angle deceptive jamming has not yet been (and is expected to be) reflected in the proposed EW simulator.

4. Propagation Modeling

The electromagnetic signal radiated from the transmission antenna of radar threat basically suffers the free space loss according to the radar frequency and target distance. In addition, the transmission signal is attenuated by atmospheric absorption or rainfall, which is related to the radar wavelength, temperature, atmospheric pressure, water vapor, and target distance. In the proposed EW simulator, we use the model of the loss and attenuation of the transmission signal in [7, 28–30].

On the other hand, when the radar or target is moving, a change in frequency of electromagnetic waves, namely, Doppler shift, can occur. And also, under the multipath fading environment, the pulses from multipath do not arrive at the same time since the path lengths are different from each

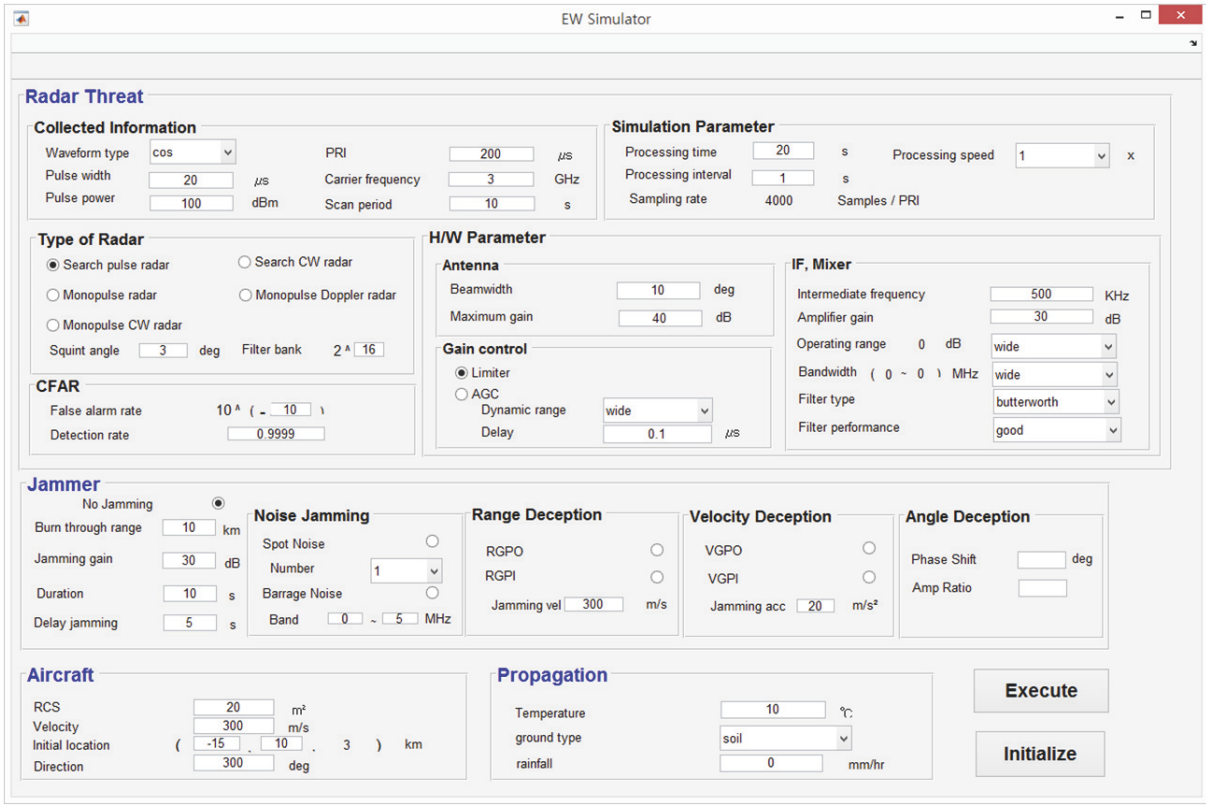

Figure 8: The input screen of the proposed EW simulator.

other. Then, a pulse will spread and consequently the pulse width will widen. In the proposed EW simulator, we consider the Doppler and multipath fading effects as the same way in [7].

5. Simulation Results

Figure 8 shows the input screen of the EW simulator developed using MATLAB®. We can investigate the responses of radars to electronic attacks in various EW environments. A radar threat can be select among five types, pulse type search radar, continuous wave (CW) type search radar, monopulse radar with range and angle tracking, monopulse Doppler radar with range, angle, and velocity tracking, and monopulse CW radar with angle and velocity tracking, and an electronic attack can be selected among seven types: barrage and spot noise jamming, RGPO and RGPI range deceptive jamming, VGPO and VGPI velocity deceptive jamming, and no jamming. After selecting the types of radar and jamming, we can adjust the collected information and some hardware parameters accordingly.

When a simulation starts, the output screen such as shown in Figure 9 is turned up. As the simulation progresses, the results of the output screen are updated according to the processing interval and speed. Figures 9(a) and 9(b) graphs display the radar scope and monopulse angle scope, respectively; those provide the range and angle tracking status. Figures 9(c) and 9(d) graphs show the received signal and its spectrum, respectively. The text boxes in Figure 9(e) report the selected radar and jamming types, instantaneous tracking results, and root-mean-squared (rms) errors estimated in the whole simulation. The tracking results and rms estimation errors are stored separately in files. They can be used to investigate or analyze the effectiveness of jamming.

We show the block diagram of the proposed EW simulator in Figure 10. The simulator accepts input variables and parameters from the UI screen as shown in Figure 8 for the modeling of radar threat, aircraft, jammer, and propagation in EW environments. After the "Execute" button is pressed, the simulator has generated the appropriate radar signal and received signals at both sides of aircraft and radar threat by applying the input variables and parameters, and then, has analyzed the target (aircraft) information during the processing time. Simultaneously, the output screen has presented the target information analyzed by radar threat as shown in Figure 9.

Now, let us investigate the responses of radar under the various electronic attacks. Table 1 shows the parameters for the basic simulation scenario to be called s_A in this paper and the trace of aircraft in s_A is shown in Figure 11. The aircraft reconnoiters the enemy territory heading toward a radar threat and is locked on at about 26 km away from the radar threat. And then, the simulation will be terminated after the aircraft reaches within the burn-through range. Figure 12 presents the range tracking results in the scenario s_A under no jamming. It is shown that the range estimation errors occur

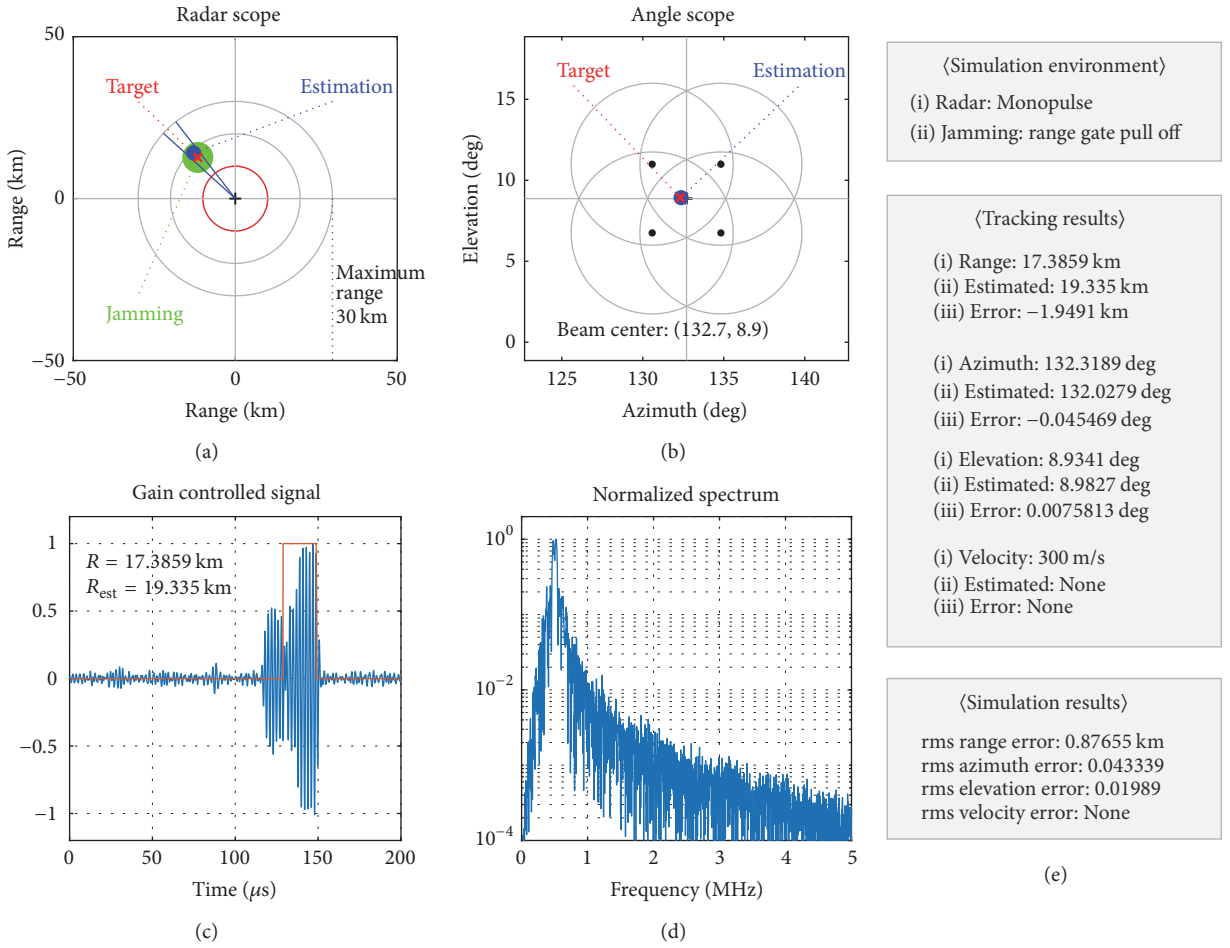

Figure 9: The output screen of the proposed EW simulator under RGPO jamming.

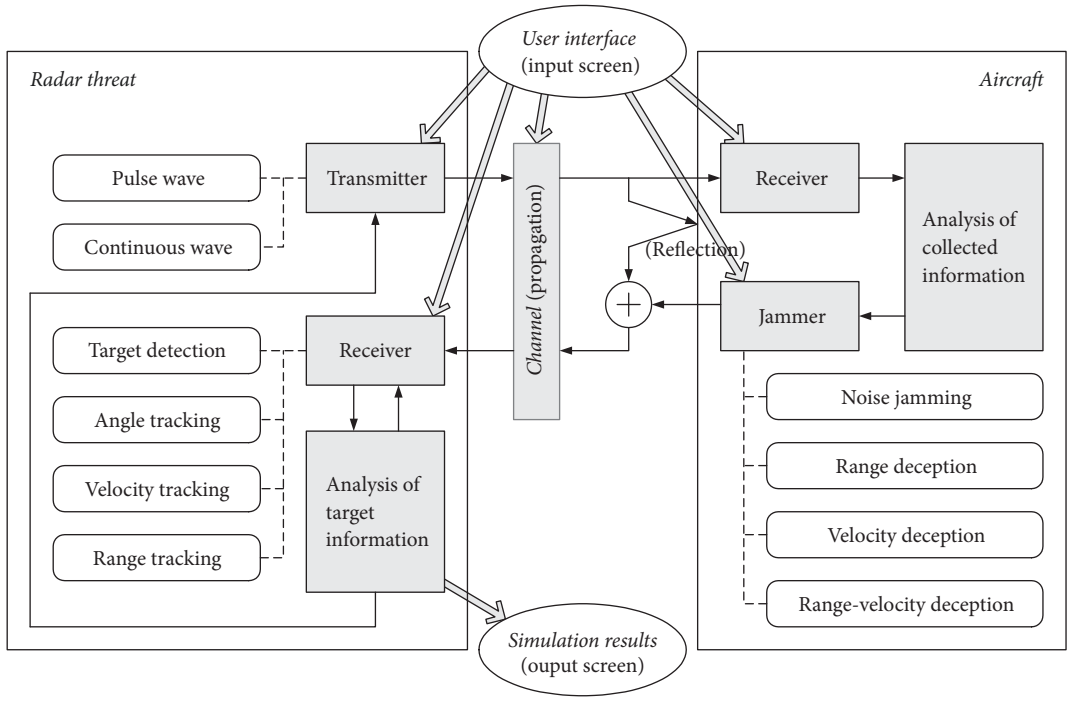

Figure 10: The block diagram of the proposed EW simulator.

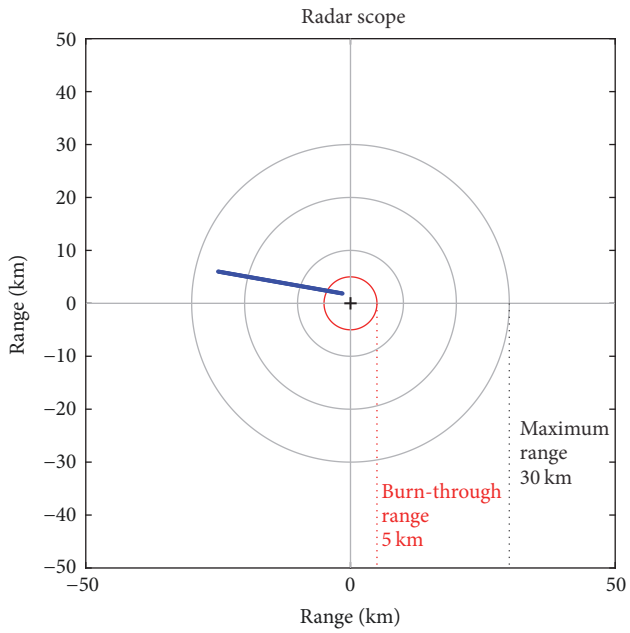

Figure 11: The trace of aircraft in the basic simulation scenario.

Table 1: The parameters for the basic simulation scenario.

Radar Threat	Monopulse Doppler Radar
Collected Information	(i) Waveform type: cos wave (ii) Pulse width: 20 μs (iii) Pulse power: 70 dBm (iv) PRI: 200 μs (v) Carrier frequency: 1 GHz (vi) Scan period: none
Type of Radar	(i) Squint angle: 5° (ii) False alarm rate: 10^{-3} (iii) Filter bank size: 2^{16} (iv) Detection rate: 0.999
H/W Parameter	(i) Antenna beamwidth: 10° (ii) Antenna gain: 40 dB (iii) Gain control: AGC mode (iv) IF frequency: 500 MHz (v) IF gain: 30 dB (vi) IF performance: good
Aircraft	(i) RCS: 20 m^2 (ii) Velocity: 300 m/s (iii) Initial location: (−25, 6, 3) km (iv) Moving direction: 350°
Propagation	(i) Temperature: 10°C (ii) Ground type: soil (iii) Rainfall: 0 mm/hour
Simulation Parameters	(i) Processing time: 40 s (ii) Processing speed: 5 times (iii) Processing interval: 1 s (iv) Sampling rate: 400 samples/PRI
Jamming	(i) Burn-through range: 5 km (ii) Jamming gain: 30 dB

within 4 m and the range tracking is being performed very accurately when there is no electronics attack.

The tracking results of azimuth angle and elevation angle are shown in Figures 13 and 14, respectively. In addition to the scenario s_A, we perform the simulation in scenarios s_B and s_C with slight change in aircraft velocity and radar beamwidth. The parameters in scenario s_B are the same as Table 1 except that the aircraft velocity is 600 m/s and those in scenario s_C are the same as in scenario s_B except that the antenna beamwidth of radar threat is 5°. It is shown that the estimation errors of azimuth and elevation angles increase as the aircraft gets closer to the radar threat, as the velocity of aircraft increases, and as the antenna beamwidth of radar decreases. Particularly, in scenario s_C; that is, when the aircraft is fast and the antenna beamwidth is not large enough to track the aircraft, the estimation errors of azimuth and elevation angles are larger than the antenna beamwidth of radar, and it means that the radar misses the aircraft.

Figures 15–18 are the simulation results obtained under various electronic attacks in scenario s_A. In these figures, we exhibit when the jamming starts using blue lines and when the aircraft enters in the burn-through range using red lines. In Figure 15, it is shown that the range tracking carries out wrongly under barrage noise jamming, but the range error decreases as aircraft gets closer to burn-through range, and, then, the aircraft is locked on again within the burn-through range in spite of barrage noise jamming.

The similar aspects appear under other kinds of jamming. Figure 16 shows the range tracking result under RGPO jamming which pulls off the range gate of radar to 40 m per second. We can see that the range error is up to about 2.2 km at 60 s (the time since the jamming started and 55 seconds later), and, consequently, the proposed simulator operates as intended. The radar tracks the false target under RGPO jamming, but the true aircraft is locked on again after a few seconds within the burn-through range despite range deceptive jamming.

Figure 17 shows the velocity estimation results in scenario s_B under VGPI jamming which pulls in the spectrum of the received signal and makes the aircraft seem slower as 4 m/s per second. The solid line, dashed line, and dotted line indicate the true velocity of aircraft, the desired velocity under VGPI, and the estimated velocity by radar under VGPI, respectively. Although the estimated velocity is not the same as the desired one in VGPI, it tends to recognize small velocity gradually in radar as intended. The difference between the desired velocity and the estimated one occurs because the size of fast Fourier transform (FFT) used for estimating the Doppler shift is smaller than the sample size of received signal, but the FFT size cannot be larger enough considering the simulation speed.

Lastly, Figure 18 shows the range tracking result in scenario s_B under velocity deceptive jamming which makes the aircraft seem slower as 4 m/s per second and range deceptive jamming which pulls off the range gate of radar corresponding to the false velocity of the velocity deceptive jamming. It

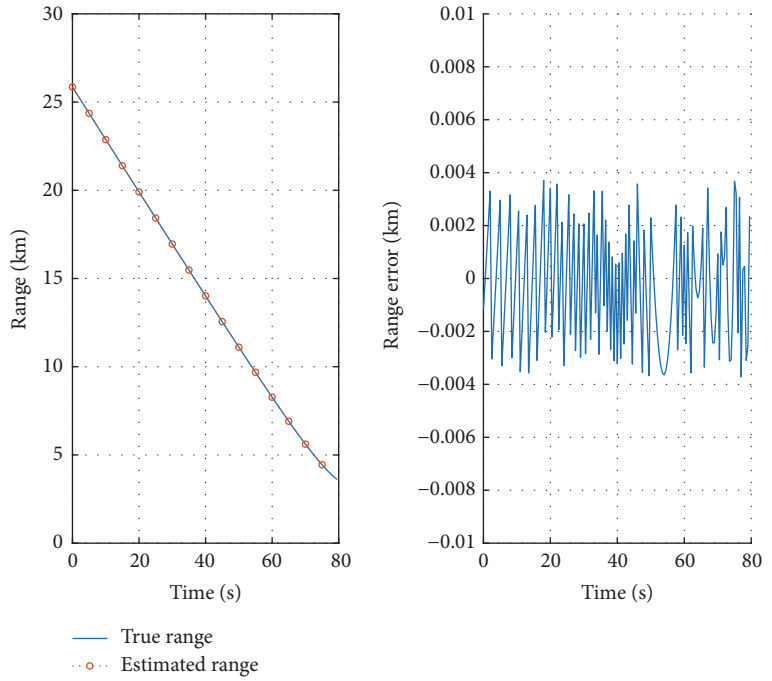

Figure 12: Range tracking results under no jamming.

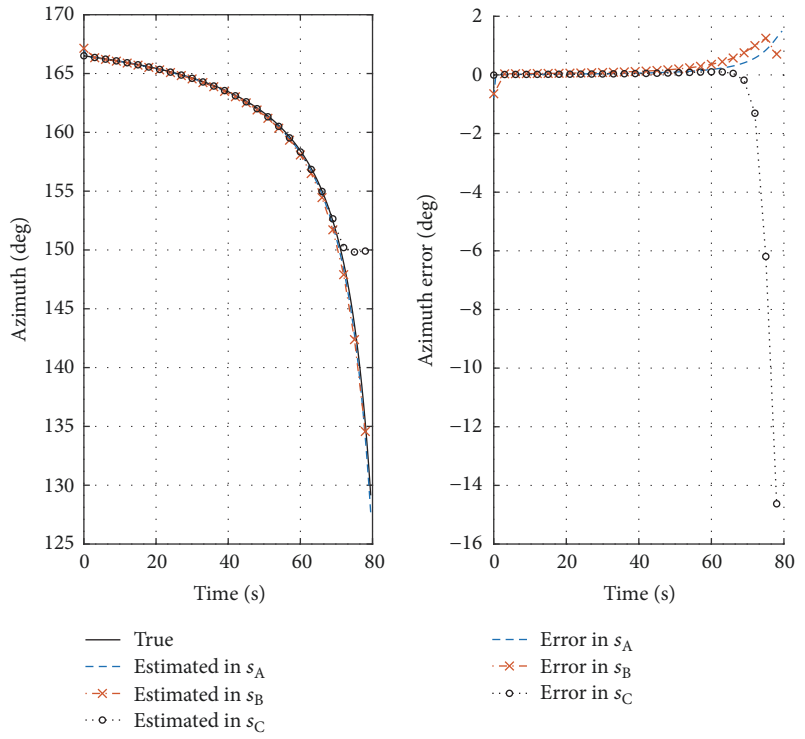

Figure 13: Azimuth angle tracking result under no jamming.

is shown that the desired range in this complex jamming is formed as a curve of secondary degree because the desired velocity decreases linearly. The true aircraft is also locked on again after a few seconds within the burn-through range in spite of the complex deceptive jamming.

6. Conclusion

In this paper, we have presented an electronic warfare (EW) simulator to investigate and evaluate the tracking performance of monopulse radar system under various electronic

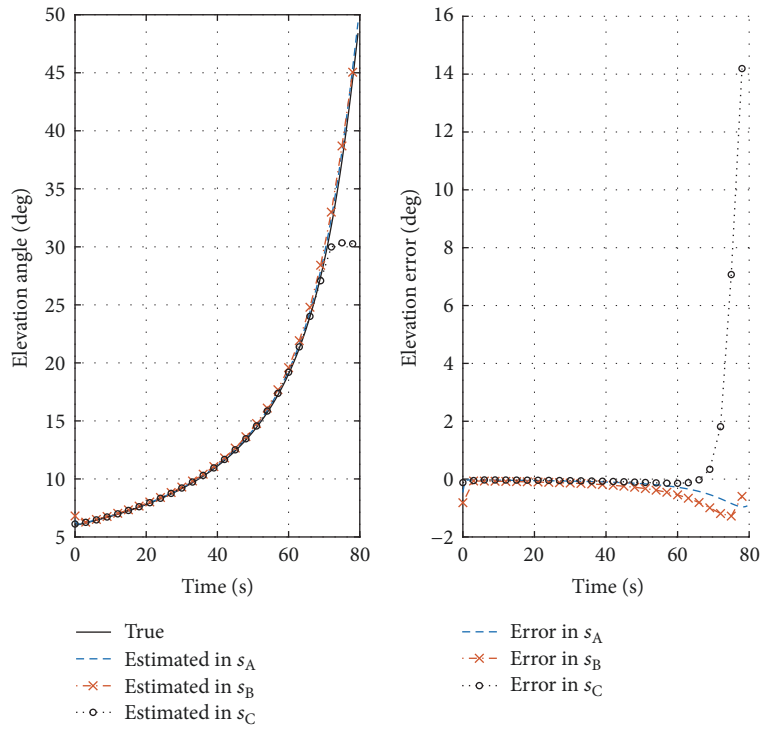

Figure 14: Elevation angle tracking result under no jamming.

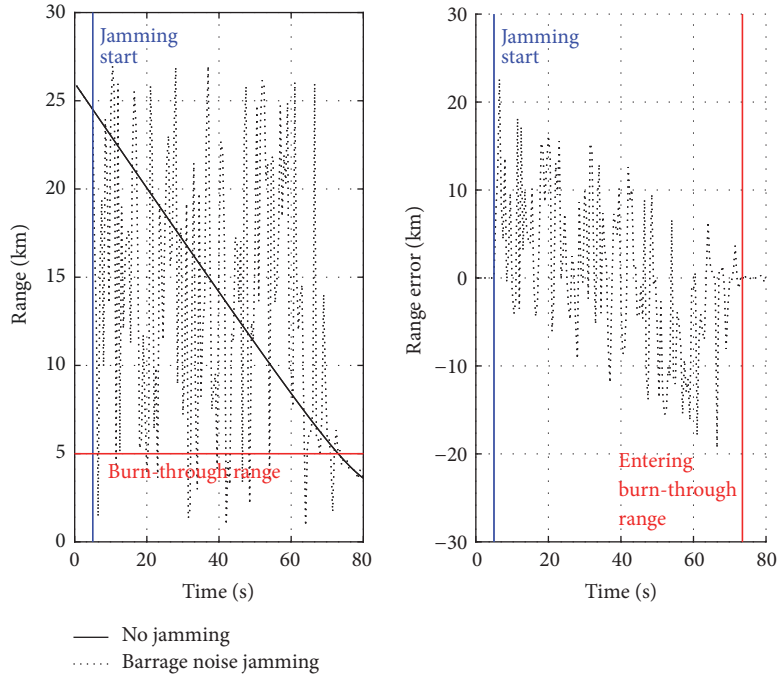

Figure 15: Range tracking results under barrage noise jamming.

attack environments. The EW simulator was developed using MATLAB® in compliance with the theoretical model or the principles of circuit operation and included the modules for radar threat such as antenna, intermediate frequency (IF) conversion, automatic gain control (AGC), CFAR detection, range tracking, angle tracking, velocity estimation, the modules for electronic attack such as noise jamming, range deceptive jamming, velocity deceptive jamming, and range-velocity complex, the modules for aircraft with RWR and jammer, and the modules for the propagation of electromagnetic wave such as signal attenuation, frequency shifting, and multipath spreading.

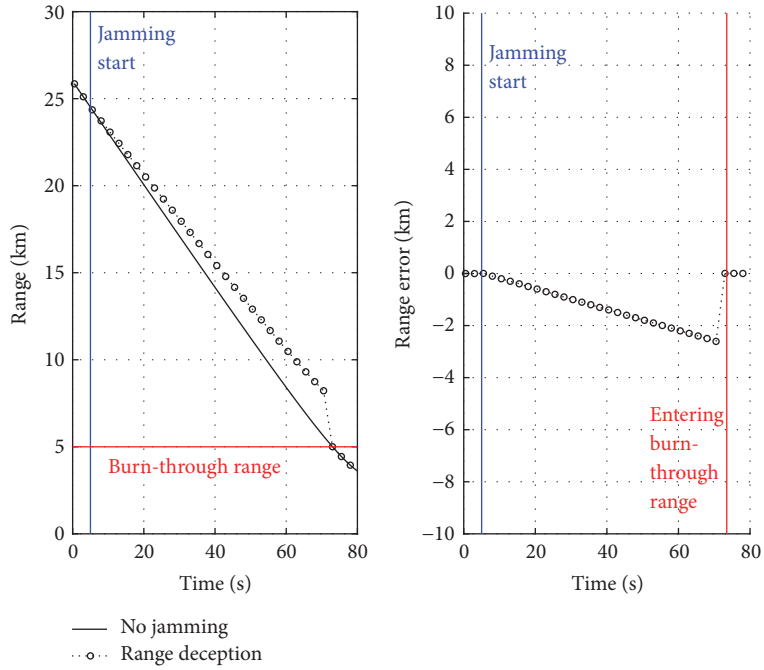

FIGURE 16: Range tracking results under RGPO jamming.

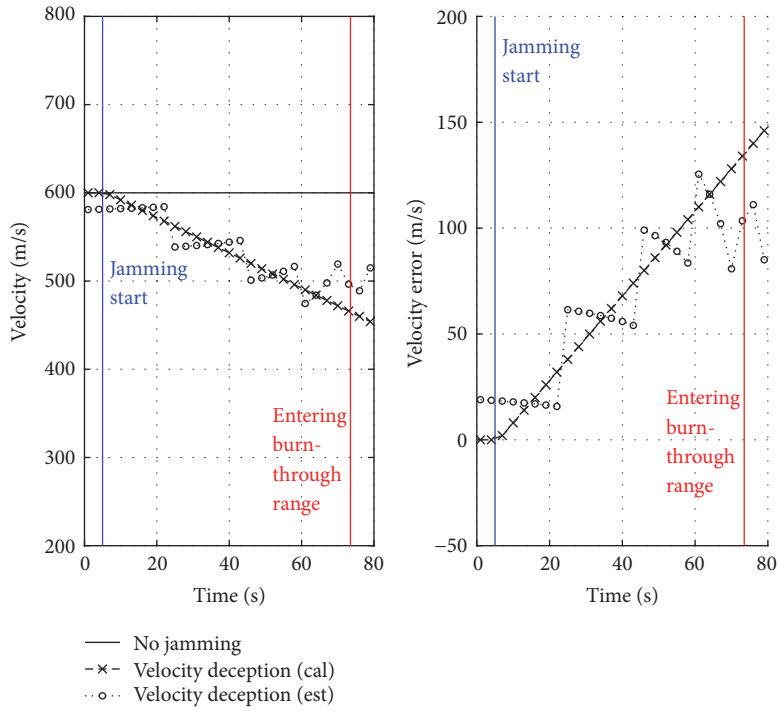

FIGURE 17: Frequency estimation results under VGPI jamming.

The proposed EW simulator has the input section in which the characteristic parameters of radar threat, radar warning receiver, jammer, electromagnetic wave propagation, and simulation scenario can be set up. During the process of simulation, the simulator displays the situations of simulation such as the received signal and its spectrum, radar scope, and angle tracking scope and also calculates the transient and rms tracking errors of the range and angle tracking system of radar. The tracking results and rms estimation errors are stored separately in files. They can be used to investigate or analyze the effectiveness of jamming.

In Sections 2, 3, and 4, we described the modeling of the important modules related to detecting and tracking which are the most basic functions of the surveillance radar, that

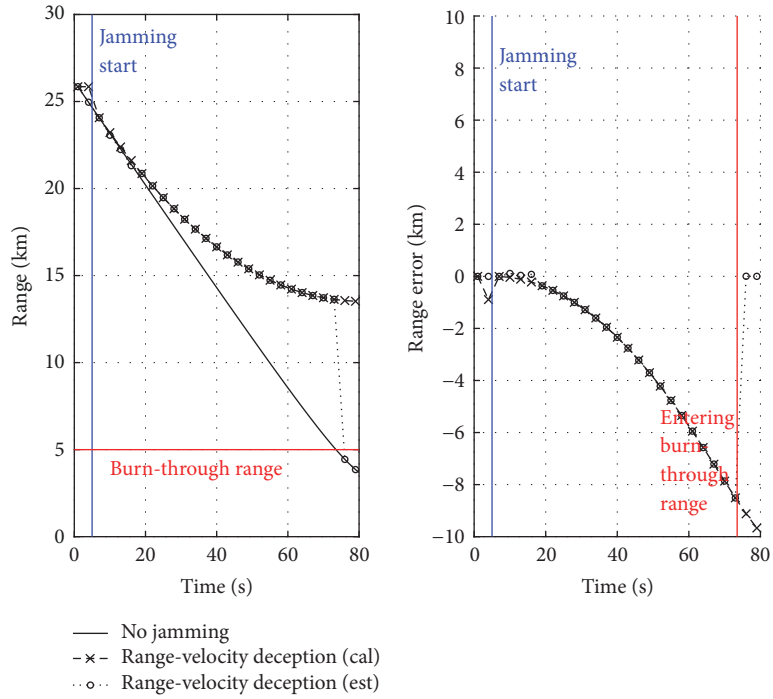

Figure 18: Range tracking results under range-velocity deceptive complex jamming.

of the various jamming module considering the JSR and burn-through range, and that of the propagation of electromagnetic wave, respectively. It was shown that the proposed EW simulator operated as intended in modeling in Section 5. The range tracking was performed very accurately when there is no electronic attack. The estimation errors of azimuth and elevation angles increased as the aircraft got closer to the radar threat, as the velocity of aircraft increased, and as the antenna beamwidth of radar decreased. The range tracking was carried out wrongly under noise and deceptive jamming, but the aircraft was locked on again within the burn-through range in spite of jamming.

Through the simulation result, it was also shown that we can analyze the effect of concealment under the noise jamming and also the effect of deception under the deceptive jamming using the proposed EW simulator. Furthermore, it is expected that the proposed EW simulator can be used to figure out the feature of radar threats based on the information collected from the EW receiver and also used to carry out the electronic attacks efficiently in electronic warfare environment.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors gratefully acknowledge the support from Electronic Warfare Research Center at Gwangju Institute of Science and Technology (GIST), originally funded by Defense Acquisition Program Administration (DAPA) and Agency for Defense Development (ADD).

References

[1] J. Matuszewski, "The radar signature in recognition system database," in *Proceedings of the 2012 19th International Conference on Microwaves, Radar and Wireless Communications, MIKON 2012*, pp. 617–622, Poland, May 2012.

[2] R. G. Wiley, *ELINT The Interception and Analysis of Radar Signals*, Artech House, 2006.

[3] A. Graham, *Communications, Radar and Electronic Warfare*, John Wiley and Sons, 2011.

[4] L. Neng-Jing and Z. Yi-Ting, "A Survey of Radar ECM and ECCM," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 31, no. 3, pp. 1110–1120, 1995.

[5] S. R. Park and S. Noh, "Optimal decision-making of countermeasures by estimating their expected utilities," *IEICE Transaction on Information and Systems*, vol. 93, no. 3, pp. 560–568, 2010.

[6] S. K. Das, "Modeling intelligent decision-making command and control agents: An application to air defense," *IEEE Intelligent Systems*, vol. 29, no. 5, pp. 22–29, 2014.

[7] S. Noh and S. R. Park, "Reverse modeling and autonomous extrapolation of RF threats," *International Journal on Advances in Computer Science*, vol. 4, no. 18, pp. 89–97, 2015.

[8] Y. Cao, Y. Li, G. Hu, Y. Liu, and X. Ma, "A modeling method of radar seeker in the presence of electronic warfare," in *Proceedings of the 2010 International Conference on Computer Application and System Modeling, ICCASM 2010*, vol. 11, pp. 456–460, China, October 2010.

[9] B. Barshan and B. Eravci, "Automatic radar antenna scan type recognition in electronic warfare," *IEEE Transactions on*

Aerospace and Electronic Systems, vol. 48, no. 4, pp. 2908–2931, 2012.

[10] M. McDonald and D. Cerutti-Maori, "Multi-phase centre coherent radar sea clutter modelling and simulation," *IET Radar, Sonar & Navigation*, vol. 11, no. 9, pp. 1359–1366, 2017.

[11] R. F. Mofrad and R. A. Sadeghzadeh, "Scenario modeling and simulation for performance prediction of a modern radar in electronics warfare environment," in *Proceedings of the International Radar Symposium*, pp. 1–5, Vilnius, Lithuania, June 2010.

[12] C. M. Macal and M. J. North, "Agent-based modeling and simulation," in *Proceedings of the 2009 Winter Simulation Conference, WSC 2009*, pp. 86–98, USA, December 2009.

[13] Z. Han, "Modeling method and application of multi-agents in armored force operation simulation," in *Proceedings of the 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 2046–2049, Chongqing, China, March 2017.

[14] A. E. Opcin, A. H. Buss, T. W. Lucas, and P. J. Sanchez, "Modeling anti-air warfare with discrete event simulation and analyzing naval convoy operations," in *Proceedings of the 2017 Winter Simulation Conference (WSC)*, pp. 4048–4057, Las Vegas, NV, USA, December 2017.

[15] I. Song, J. Bae, and S. Y. Kim, *Advanced Theory of Signal Detection*, Springer, 2002.

[16] H. L. Van Trees, *Detection, Estimation, and Modulation Theory: Part III - Radar-Sonar Signal Processing and Gaussian Signals in Noise*, John Wiley and Sons, 2014.

[17] I. J. Kim, S. R. Park, I. Song, J. Lee, H. Kwon, and S. Yoon, "Detection schemes for weak signals in First-Order moving average of impulsive noise," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 1, pp. 126–133, 2007.

[18] J. Lee, I. Song, H. Kwon, and H. . Kim, "Locally optimum detection of signals in multiplicative and first-order Markov additive noises," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 1, pp. 219–234, 2008.

[19] D. Tahmoush, "Review of micro-Doppler signatures," *IET Radar, Sonar & Navigation*, vol. 9, no. 9, pp. 1140–1146, 2015.

[20] A. Golden Jr., *Radar Electronic Warfare*, American Institute of Aeronautics and Astronautics Education Series, 1988.

[21] R. Poisel, *Mordern Communications Jamming Principles and Techniques*, Artech House, 2011.

[22] L. Surendra, S. Shameem, N. Susmitha, and T. S. Ram, "Analysis of self-screening jammer parameters with radar equation," *International Journal of Engineering Research and Applications*, vol. 4, no. 3, pp. 205–207, 2014.

[23] A. Mpitziopoulos and D. Gavalas, "An effective defensive node against jamming attacks in sensor networks," *Security and Communication Networks*, vol. 2, no. 2, pp. 145–163, 2009.

[24] P. C. J. Hill and V. Truffert, "Statistical processing techniques for detecting DRFM repeat-jam radar signals," in *Proceedings of the IEE Colloquium on Signal Processing Techniques for Electronic Warfare*, pp. 1–6, London, UK, 1992.

[25] W. D. Blair, G. A. Watson, T. Kirubarajan, and Y. Bar-Shalom, "Benchmark for radar allocation and tracking in ECM," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 4, pp. 1097–1114, 1998.

[26] J. D. Townsend, M. A. Saville, S. M. Hong, and R. K. Martin, "Simulator for velocity gate pull-off electronic countermeasure techniques," in *Proceedings of the 2008 IEEE Radar Conference, RADAR 2008*, pp. 1–6, Rome, Italy, May 2008.

[27] L. Falk, "Cross-eye jamming of monopulse radar," in *Proceedings of the 2007 International Conference on Waveform Diversity and Design, WDD'07*, pp. 209–213, Italy, June 2007.

[28] B. R. Mahafza, *Radar Systems Analysis and Design Using MATLAB*, CRC Press, 3rd edition, 2012.

[29] D. L. Adamy, *EW 101: A First Course in Electronic Warfare*, Artech House, 2015.

[30] M. Pätzold, *Mobile Fading Channels*, John Wiley & Sons, Ltd, Chichester, UK, 2002.