Analysis and Investigation of Disturbance in Radar Systems using New Techniques of Electronic Attack

Pouriya Etezadifar[1*], Saeed Talati[2]
1- Department of Electrical Engineering, Imam Hussein University (IHU), Tehran, Iran.
Email: petezadifar@ihu.ac.ir (Corressponding Author)
2- Department of Electrical Engineering, Imam Hussein University (IHU), Tehran, Iran.
Email: saeed.talati@yahoo.com

Received: January 2021 Revised: March 2021 Accepted: April 2021

ABSTRACT:
With the end of World War II and the rapid advent of war technology, wars have shifted to electronic warfare, and today a nation can win wars that are more powerful in the field of telecommunications and electronic warfare. The purpose of this article is to promote new content in the field of electronic warfare and we try to introduce and introduce new techniques of electronic attacks on victim radar systems. With the exception of false targets created by point or sweep jams, most false targets are created with automatic responders or repeaters. An automatic response generator for producing false targets includes a receiver, a variable delay circuit, a signal generator, a power amplifier, and an antenna. Upon receiving a pulse from the threatening radar, the transponder waits for the time corresponding to the target man's distance to the false target, and then sends a similar echo signal to the radar. . As soon as the pulse is received from the threatening radar, the transponder delays it sufficiently to cause the difference in distance to create a false target. Then, a pulse similar to the RF echo pulse of the radar is returned to it.

KEYWORDS: Electronic Attack, Electronic Warfare, Information, Electronic Support.

1. INTRODUCTION

A blind man steadily walks his way on the sidewalk, finding his way onto a crowded street, and with his right hand he maintains a fixed range from the wall of a building, to his right, and thus a safe range from the edge of the sidewalk creates traffic jams on its left. As the bunch of sharp insects come out, the bat is skillfully informed of their presence and avoids some of them and sets out on the path of others who are preying on them. Also, the pilot of a "Super Sonic" fighter can certainly detect the approach of an enemy aircraft hiding behind a cloud mass 150 miles away. Since the end of World War II there have been many advances in the areas of science, especially radar[1], Low Probability of Intercept Radar, [2], electronic defense[3], telecommunications systems[4], genetic algorithms[5], hardware[6], software[7], phase lock loops[8], distributed production resources[9], Neural networks [10], cryptography and watermarking[11]. One of the issues that is very important in the field of electronic warfare and especially electronic attack is the issue of false targets.

2. FALSE TARGETS

Usually a repeater that produces false targets contains a memory and has a system capable of producing several apparently realistic targets. The repeating memory stores the actual pulses received from the radar. after an appropriate delay, the pulse is amplified to be called and transmitted to the radar.

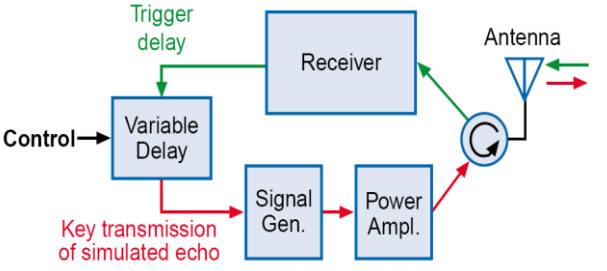

Fig. 1. Automatic responder for producing false targets.

A repeater produces several seemingly real false targets. When a pulse is received from a threatening radar, it is stored in iterative memory. After the

Paper type: Research paper
DOI: https://doi.org/10.52547/mjtd.10.2.55
How to cite this paper: P. Etezadifar, S. Talati "**Analysis and Investigation of Disturbance in Radar Systems using New Techniques of Electronic Attack**", Majlesi Journal of Telecommunication Devices, Vol. 10, No. 2, pp. 55-59, 2021.

appropriate time delay, the pulse is recalled from the memory, amplified and returned to the radar.

Although a shared antenna for both transmitter and receiver can be divided by time, with regard to isolation issues it is preferable to use two separate antennas for transmitter and receiver.

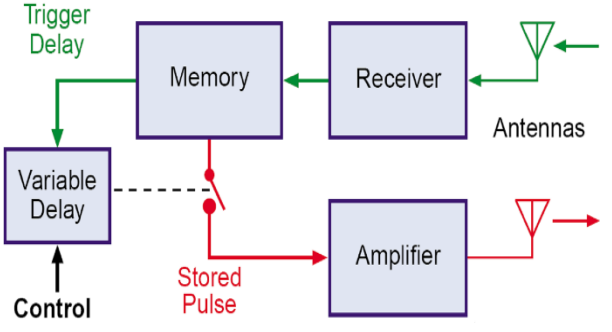

Fig. 2. Repeater for Producing False Targets.

A repeater can even work by delaying more than two consecutive radar transmissions that make the location of the false targets closer to the original target. The repeater can also show false targets with different Doppler frequencies.

Although a rotary delay line can be used as a replication memory, digital radio memory (DRFM) is more reliable and efficient for this purpose. This memory instantly stores the digital sample of each received pulse. After storing, the disruptor can transmit pulses very similar to the real state by delaying and varying the Doppler shift.

In a more advanced measure, the disruptor can measure the time taken by the victim's radar antenna. Then send the false pulses from the sub petals to the radar by making the delayed radar scan start. In this case, the angles of the targets observed on the radar would also be unrealistic.

Direct repeaters are used against continuous wave radars and high PRF radars that do not use pulse latency to measure target ranges.

3. GATE STEALING DECEPTION

If, despite noise disturbance, concealment, and false positives, the radar still performs well-managed management and can lock on to the original target, the use of deceptive gate techniques can effectively prevent the radar from properly tracking.

When the radar detects the target, the small sampling gate opens around the time the target echo is received, and only in that sampling gate. As such, the effect of Clutter and other disturbing signals is greatly reduced.

In contrast to all gate deception methods, the disruptor tries to control the radar tracking gate by sending the right signals at the right time. By capturing the radar gate, the cheat system will perform one of the following operations:

- Slow Motion: The Disruptive picks up her signal, moving slowly so that the radar can sense the target at a range other than the actual range.
- Breaking the lock: The trickster breaks the lock by pulling the gate out of the target range and dropping or moving it to the chaff or clutter returns.
- Angular Deception Facilitator: By increasing the ratio of the jammer power to the target signal, the radar will attempt to estimate the target angle.

Each time the tracker loop is broken, the victim 's radar can retrieve the target and lock it again with a limited search. But if the breaker breaks the tracking loop again and repeats this cycle repeatedly, the accuracy of the victim radar tracking will be greatly reduced. Gate deception is basically divided into two types of range gate stealer (RGS) and Velocity gate stealer (VGS).

4. RANGE GATE STEALER

This technique can be used against radars with low or medium PRFs. In contrast to non-coherent radars with low PRF, the Disruptive may simply operate as a transponder. In this case, the breaker system detects the front edge of each radar pulse and, after a delay, returns the RF pulse to the radar. Initially the delay is short enough and the false pulse falls within the range of the correct return pulse from the real target, but the deceptive pulse is much stronger than the target echo. As a result, the victim's radar responds to this pulse rather than the actual echo. From now on, the disruptor will gradually increase the sending time delay, and as a result, the range gate will be pulled out of the real target range. In front of a non-coherent radar, the range gate Disruptive may have a transponder-like mechanism. Upon receiving each pulse from the radar, the transponder sends an RF pulse to the radar automatically.

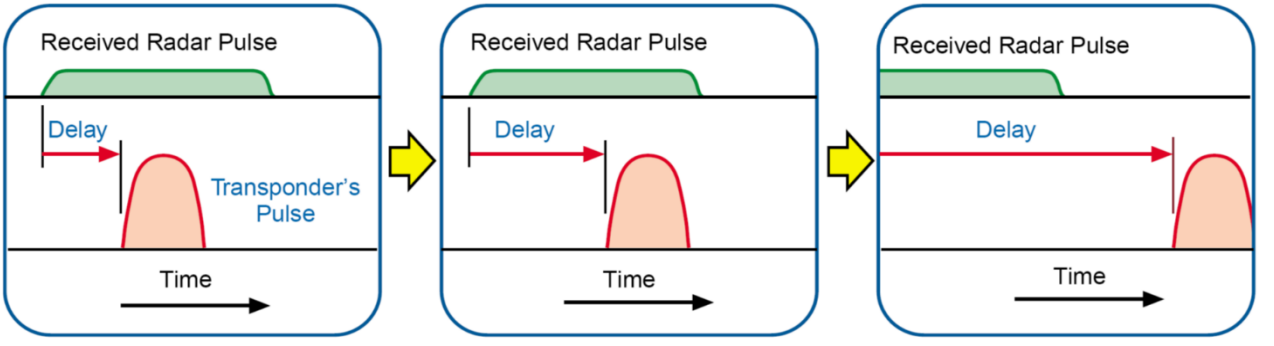

Fig. 3. The gate of the space bar. **A**: The delay is adjusted and covered by the return pulse of the true target radar, then the gate receives the radar range. **B**: The delay increases gradually, as the transponder pulse pulls the radar gate away from the actual range. **C**: The delay is increased enough for the interval gate to completely push the gate out of the target range.

If the PRF radar is known or measured by the deceptive logic circuit, it first generates a delay equal to the inter-pulse period and then gradually reduces it, in which case the delay is replaced in the radar gate and the gate is drawn in, thus radar. Sees its purpose at closer ranges.

In deceiving coherent radars it is also necessary to have a Doppler received frequency to match. Thus the range gate deception in this case is slightly different and somewhat more complex. In older designs using circular latencies, the mechanism of deception signal generation is as follows:

- Sampling the front edge of each pulse is reached.
- Sample delay for arbitrary duration.
- Amplify and radiate the sample toward the radar.

In these systems, because the edge of each pulse is stored, if the pulse of the radar is encoded, the disturber will not notice it and as a result the transmitting signal will be ineffective on the radar. To fix this problem in new designs, the code is repeated with a DRFM. In this way, DRFM will sample and store all the pulses, allowing the pulses to be generated with appropriate coding and frequency, and the antennas will be guided by the EA receiver on the victim radar.

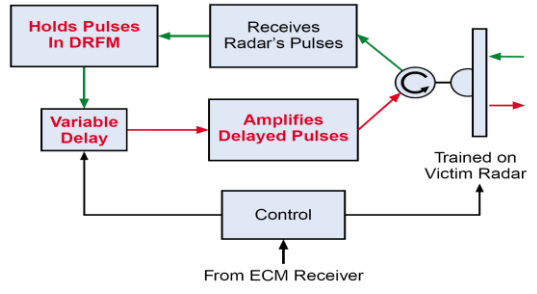

Fig. 4. A more effective system to deceive in the range gate.

5. VELOCITY GATE STEALER

This technique is used to counter radar with high PRF or continuous search radar and Missiles with search warheads. This technique is performed by a direct repeater. The velocity gate deception is essentially the same as the range gate stealer targeted at the frequency domain around the echo signal.

In this method, where the jammer carrier platform is on target, the radar signal is first received and amplified and transmitted to it without change. Therefore, the Doppler frequency of the deceptive signal will be equal to the real Doppler frequency, but the higher power of the deceptive signal causes the radar to respond to and follow this signal. The radar always generates a gate (filter) around the observed target frequency and uses this gate to detach the desired target signal from other reflections that have other Doppler frequencies. After the breaker takes control of the Doppler radar gate, the radio frequency shifts its signal up or down gradually, pushing the gate out of position.

In all deception methods, in order for Jamar to effectively affect the radar, it is necessary that its antenna be in line with the victim's radar line of sight. Usually, the task of orienting the disturbing antenna toward the radar is at the EA unit, but in a self-orienting system as described below, the radar signals are automatically transmitted to the radar direction. Unfortunately, their directional systems, unlike conventional antennas, often have large physical dimensions. This restricts their use in many cases.

6. RETRODRECTIVE REPEATER

It is easier to understand the repetitive function of the oriented by considering a passive set. This system is shown in Figure 5. Here, the antenna consists of a linear array of radiating elements, interconnected in pairs with coaxial cables.

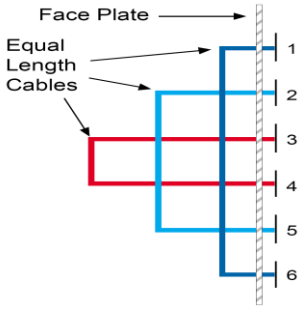

Fig. 5. A more effective system for repeater orientation.

The radiation emitted by each element is again radiated by the other element of its own pair. For example, radiation emitted by element 1 is emitted by element 6 and radiation emitted by element 6 is emitted by element 1.

Here the length of all the cables connecting the antennas to each other is equal. Thus, the delay to the signal is equal to all paths, so that the input signal phase due to the non-perpendicular angle to the array is reversed exactly in the reflected waves, and the wave is in the same direction. The transmitted waves will be propagated in the opposite direction.

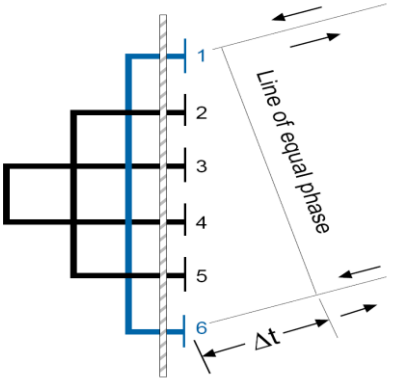

Fig. 6. Show the constant delay in your repeater.

By placing the DRFM segment and the amplifier in the communication loop of both pairs of elements, as in Figure7, an ideal self-directional repeater can be achieved.

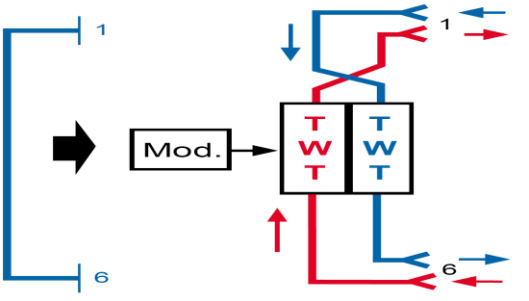

Fig. 7. Self-directional repeater with DRFM loop.

7. ANGLE DECEPTION

The purpose of this electronic attack is to prevent the enemy's weapon from reaching the desired target by making errors in the tracking angle of the fire control radar, or missile guidance radar.

In older tracking systems that use lobe to determine angles. Angle deception is easily achieved by sending pulses of timing and proper amplitude to the radar. But most mono-pulse tracking radars today measure angles, so the simple technique of transmitting pulses to the radar cannot make them difficult to measure.

Until now, several techniques have been designed to generate errors in advanced radar and single-pulse tracking systems. All of these techniques require accurate information from the victim's radar parameters, which cannot be easily obtained.

Techniques that can be effective in any type of tracking include: Causing disruption, including Terrain Bounce jamming and Cross-eye, which will be discussed below.

8. TERRAIN BOUNCE JAMMING

The ground-reflection technique is designed for use in low-altitude and short-range engagement modes. In this situation, this technique can be very effective against missiles with radar seeker heads. In this technique, there is a directional antenna equipped with a repeater threatening aircraft. This repeater receives and amplifies radar pulses and returns to the surface of the Earth. After the waves hit the Earth's surface, it will return to radar. These reflections from Earth will create a false radar target.

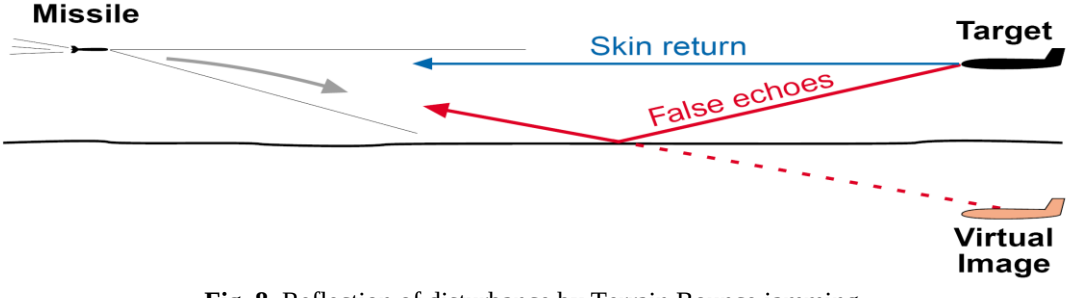

Fig. 8. Reflection of disturbance by Terrain Bounce jamming.

In this type of deception, the aircraft uses high-gain repeaters to protect itself and two sets of receiver and transmitter antennas mounted at the two wings end. The repeater has a mechanism as follows:

If the repeating signal is sufficient, the reflection signals from the ground overwhelm the actual signal and cause the missile to divert to the false target, which is the image of the original target.

The phase difference generated by the phase shifter on the signal transmitted from one wing is approximately 180 degrees relative to the signal transmitted from the other wing.

9. CONCLUSION

This paper examines the latest electronic warfare techniques using electronic attack methods on radar systems, as well as methods of tracking window tracking, deception in the distance window, speed window deception, iterator, autocorrect, deception in two speed and distance windows, Deception in Angle, Earth Reflection (TBJ), We examined the reverse view and examined the advantages and disadvantages of each.

REFERENCES

[1] Merrill I. Skolnik, "**Introduction to Radar Systems**", *Third Edition, McGraw-Hill Higher Education*, 2001.

[2] GuoSui Liu, Hong Gu, WeiMin Su, HongBO Sun, "**The Analysis and Design of Modern Low Probability of Intercept Radar**", 2001 CIE *International Conference*, pp. 120-124, 2001.

[3] Filippo Neri, "**Introduction to Electronic Defense Systems**", *Second Edition, Artech House Publishers*, 2001.

[4] Wayne Tomasi, "**Electronic Communications Systems**", *Forth Edition, Prentice Hall*, Inc., 2001.

[5] Hashemi, Seyed Mohammad, Shahrokh Barati, Saeed Talati and Heshmat Noori. "**A GENETIC ALGORITHM APPROACH TO OPTIMAL PLACEMENT OF SWITCHING AND PROTECTIVE EQUIPMENT ON A DISTRIBUTION NETWORK.**" Vol. 11, No. 3, 2016.

[6] O. Sharifi-Tehrani and S. Talati, "**PPU Adaptive LMS Algorithm, a Hardware-Efficient Approach; a Review on**", *Majlesi Journal of Mechatronic Systems*, Vol. 6, No. 1, 2017.

[7] Hashemi. Seyed Mohammad, Abyari. Mohammad, Barati. Shahrokh, Tahmasebi Sanaz, Talati, Saeed. "**A PROPOSED METHOD TO CONTROLLER PARAMETER SOFT TUNING AS ACCOMMODATION FTC AFTER UNKNOWN INPUT OBSERVER**." *ARPN Journal of Engineering and Applied Science*s Vol. 11, No. 5, 2016.

[8] S. Talati, A. Rahmati, and H. Heidari, "**Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops**", *MJTD*, Vol. 8, No. 2, pp. 57-61, 2019.

[9] Saeed. Talati, Behzad. Ebadi, Houman. Akbarzade "**Determining pf the fault location in distribution systems in presence of distributed generation resources using the original post phasors**", *QUID 2017*, pp. 1806-1812, Special Issue No.1- ISSN: 1692-343X, Medellín-Colombia. April 2017

[10] Saeed Talati, Mohamadreza HasaniAhangar, "**Analysis, Simulation and Optimization of LVQ Neural Network Algorithm and Comparison with SOM**", *MJTD*, Vol. 10, No. 1, 2020.

[11] Saeed Talati, Pouriya Etezadifar, "**Providing an Optimal Way to Increase the Security of Data Transfer Using Watermarking in Digital Audio Signals**", *MJTD*, Vol. 10, No. 1, 2020.