

Article

# Theory and Design of Blink Jamming

Kyle Davidson \* and Joey Bray

Royal Military College of Canada, Kingston, ON K7K 7B4, Canada; joey.bray@rmc.ca

\* Correspondence: kyle.davidson@rmc.ca

Received: 2 January 2020; Accepted: 30 January 2020; Published: 11 March 2020



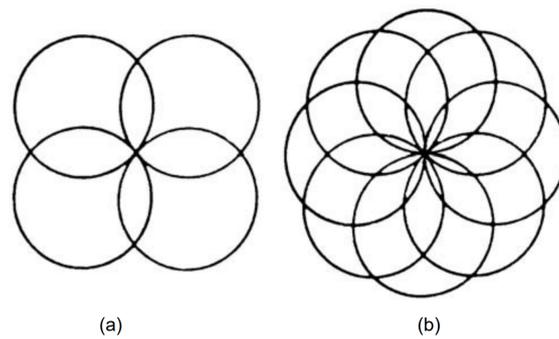
**Abstract:** Establishing an error in the angle estimates of a monopulse radar is critical to creating miss distance during the terminal stage of missile engagements. However, the tools for creating angle deception are limited, with blink jamming offering significant potential. This paper fills in the conceptual gaps in understanding of blink jamming, through a theoretical analysis, which is validated using modelling and simulation, including hardware-in-the-loop with a Field Programmable Gate Array (FPGA). Additionally, a novel version of blink jamming is proposed, using a synchronized amplitude modulation, and its performance compared to traditional, unmodulated blink jamming. The complete results are discussed, with design guidance provided for implementing blink jamming in operational scenarios.

**Keywords:** radar; electronic warfare; FPGA; electronic attack; digital radio frequency memory; electronic support

## 1. Introduction

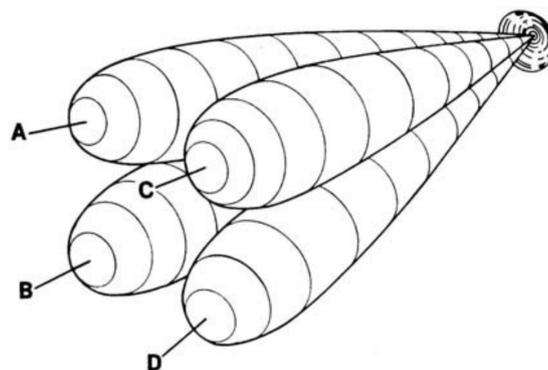
Blink jamming is a technique which has been documented as far back as the 1970s for inducing angle errors in tracking radars [1]. However, its understanding has remained limited since that time, as researchers have pursued other mechanisms for countering monopulse radars. Despite this, it offers tantalizing benefits to the Electronic Warfare (EW) engineer in creating a miss distance during missile engagements. Specifically, prior research has not established a theoretical understanding of blink jamming's operation, and its influence on a monopulse seeker, or validated the study of blink jamming in any way. This paper seeks to provide a theoretical understanding of blink jamming, incorporating effects such as skin return and jammer power, the model was then implemented using Field Programmable Gate Arrays (FPGA) and hardware-in-the-loop simulation to validate this framework against a modern threat. This modelling architecture is then used to explore a novel method of blink jamming, and understanding their the factors affecting their design.

Monopulse antenna systems have seen wide spread use since the 1970s in tracking radars for air defence systems and airborne missiles [2]. Prior to the advent of monopulse, variants of lobe-on-receive only (LORO) and conical-scan-receive-only (CSRO) were the principle forms of angle tracking in radar systems. LORO and CSRO used a moving receive beam around a fixed transmit antenna to track the angle to a target [3], shown in Figure 1, comparing the received signal amplitude from the beam positions to determine the pointing error. Unfortunately these systems have several downsides, particularly from an electronic warfare (EW) perspective, due to the fact they require multiple pulses from different positions to measure the angle to a target. This leaves them vulnerable to a highly effective form of angle deception using an amplitude modulated signal to replicate the return from a target at an incorrect angle [4,5].



**Figure 1.** The lobe positions of (a) lobe-on-receive-only, and (b) conical-scan-receive-only antenna systems [6].

Monopulse systems were a significant improvement over LORO and CSRO, by using four or more receivers to create multiple simultaneous antenna beams, shown in Figure 2. These beams were typically created with a parabolic dish by off-setting the feedhorns from the focal point, doing so forced the beams slightly off bore-sight, known as beam squint. The resulting antenna patterns could then be used in multiple ways, summing them to create a beam at boresight for transmitting, and using the relative difference in the azimuth and elevation planes to determine the angle to target with as little as one pulse, hence the name monopulse.



**Figure 2.** The lobe positions of the individual beams of a monopulse antenna [6].

From a military perspective monopulse antennas were adopted for tracking radars due to their accuracy and protection against angle deception attacks [1]. Unfortunately for EW engineers, it is difficult to create errors in the estimated angle for monopulse systems, which are critical to affecting large miss distances in missile engagements. The existing solutions include cross-eye and cross-polarization jamming, both of which require complex jammer architectures and high jammer-to-signal ratios to be effective [7].

In the case of cross-polarization jamming, the orthogonal polarization of the incident signal must be generated, and it must be done with a high level of polarization purity to distort the monopulse response curve. Cross-eye jamming creates a distortion in the phase-front, through the use of an antenna array that retransmits the incident signal with a  $180^\circ$  phase reversal. This change in phase is difficult to create precisely over a large bandwidth. In both cases the use of these techniques is often restricted to naval platforms against anti-ship missiles, where the engagement geometry is often limited to a narrow plane.

An alternative to the problem of deceiving monopulse systems is to utilize two jammers simultaneously, referred to here as formation jamming, combining their signals in the monopulse receiver in a manner that creates either increased measurement error or jamming controlled indicated angles. Formation jamming allows for the creation of these effects while also using existing

jamming systems on modern military platforms. This combination of characteristics makes a detailed understanding of formation jamming and how to design effective attacks using it highly desirable. Unfortunately, there is little open literature on the subject of formation jamming outside brief mentions in a few text books, [6] and [8], that the technique exists and several conference papers that are limited to high-level modelling of the technique [9–14].

In order to advance the scientific understanding of formation jamming this paper provides a theoretical analysis of formation jamming in a two source configuration against an amplitude comparison monopulse radar. This engagement scenario is then modelled and the results explored using continuous jamming sources, a blink attack, and an amplitude modulated blink attack. The results were validated using a Field Programmable Gate Array (FPGA) implementation of the monopulse receiver in a testbed that emulates the desired jamming signals. The validated results were then used to develop guidance on effective use of these countermeasures.

## 2. Analysis of Formation Jamming

Monopulse radar systems have been in use for decades, using four or more antennas to measure the angle to a target. This procedure is performed in amplitude comparison monopulse by adding together the received signal from each beam to create a sum channel, and subtracting the relevant beams to create difference channels for azimuth and elevation. In a four antenna configuration, the sum signal is

$$s = \frac{1}{2} (A + B + C + D) \quad (1)$$

where  $A$ ,  $B$ ,  $C$ , and  $D$  are the signals from the four antennas, shown in Figure 2. Similarly, the azimuth and elevation difference signals are:

$$d_{az} = \frac{1}{2} [(C + D) - (A + B)] \quad (2)$$

$$d_{el} = \frac{1}{2} [(A + C) - (B + D)]. \quad (3)$$

The difference signals are then divided by the sum creating an error signal that is proportional to the target's angle off boresight in each plane:

$$\varepsilon = \frac{d}{s} = k_m \theta \quad (4)$$

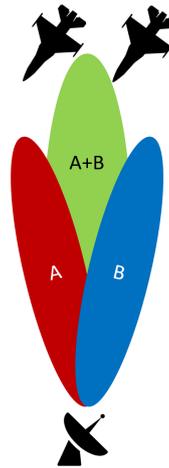
where the constant  $k_m$  is a function of the beamwidth and squint angle, and  $d$  is a generic difference signal for either axis [6]. This equation is then used to calculate the indicated angle:

$$\theta_i = \frac{1}{k_m} \frac{d}{s}. \quad (5)$$

However, the error signal is usually the preferred metric, allowing it to be used in a tracking loop to correct for any angle deviation while tracking a target.

### 2.1. The Two Target Problem

In the context of a monopulse radar conducting an angle measurement, targets are "unresolved if an angle measurement cannot be made on each target without significant error due to the presence of others" [6]. To resolve two or more targets they must be sufficiently separated in coordinates including: angle, range, or Doppler, to make interference with each other negligible. The intent of this section is to study what occurs when a monopulse radar encounters two unresolved target and its effect on angle tracking as shown in Figure 3.



**Figure 3.** The formation jamming scenario, with two jammers indicated by the aircraft icons, and a monopulse tracking radars beams shown in a single plane. The *A* and *B* beams are used for amplitude comparison, and the sum beam location is indicated by *A + B*.

The two target problem assumes the tracking radar is using either a passive monopulse receiver which is being guided by an off-board illuminator, providing only angular information, or in the monostatic case the targets are in the same range and Doppler cells. Assuming the returns from the two sources are superimposed we can explore this mathematically at true angular displacements  $\theta_a$  and  $\theta_b$ . The true difference signals for the two targets are:

$$d_a = k_m \theta_a s_a \tag{6}$$

$$d_b = k_m \theta_b s_b \tag{7}$$

with an indicated angle of:

$$\theta_i = \frac{1}{k_m} \frac{d}{s} = \frac{1}{k_m} \frac{d_a + d_b}{s_a + s_b} \tag{8}$$

Substituting in (6) and (7), we then get a more useful solution:

$$\theta_i = \frac{\theta_a s_a + \theta_b s_b}{s_a + s_b} \tag{9}$$

The new equation effectively describes the relation of the indicated angle to the weighted sum of the two sources.

### 2.2. Formation Jamming Techniques

In any individual situation, (9) is related to the weighted sum of the two targets. This should allow a pair of jammers to control the angle in the receiver, by using the relative power of the two sources to “pull” the tracking system towards the more powerful source.

This presents several options for attacking the monopulse receiver; first, a constant power signal from both sources could be transmitted to the monopulse system. Weighted by their received power and angle of arrival, the indicated angle would be calculated at some point between the two sources. In the second case, commonly known as blink jamming, the monopulse system would be deceived by switching the jammers on and off at opposing times, causing the tracking point to oscillate between the two target locations. Blink jamming, like most electronic attacks, would be expected to perform optimally when operating at the frequency of the tracking system [4].

In the final scenario, a new technique proposed in this chapter, uses a set jamming signals would operate similar to that in conventional blink jamming, but a sinusoidal amplitude modulation would be applied to each source. With the amplitude modulation from the two sources 180° out of

synchronization with each other, they should cause the same reaction as blink jamming, oscillating the tracking antenna between the two sources, with an additional benefit as the two signals approached zero power. As the power of both signals drops to zero, the noise in the receiver and tracking system can cause spurious high indicated angles. Taking (9), the point where both jammer sources approach zero power can be expressed mathematically as a limit

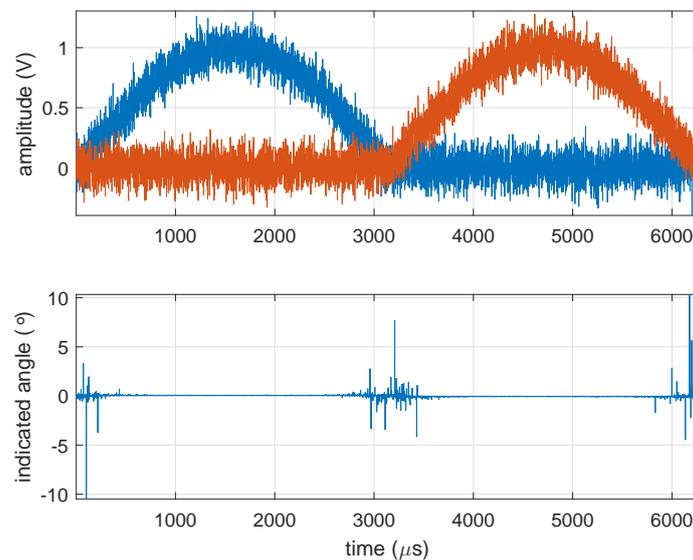
$$\theta_i = \lim_{s_a, s_b \rightarrow 0} \frac{\theta_a s_a + \theta_b s_b}{s_a + s_b} \tag{10}$$

while (10) can be understood strictly as a conventional limit, that analysis is practically irrelevant as the tracking radar is not performing that operation in the strict sense. Instead the two variable  $s_a$  and  $s_b$  are approaching zero from the positive and negative directions, in combination with various sources of noise, and the result is solved for using an analogue beamforming network or digitally with fixed or floating point math. As the two signals taper off to almost zero power the thermal noise in the receiver becomes the dominant signal. While random, in some cases  $s_a \approx -s_b$ , as described by

$$\theta_i = \lim_{s_a \rightarrow -s_b} \frac{\theta_a s_a}{s_a + s_b} + \frac{\theta_b s_b}{s_a + s_b} \tag{11}$$

This has the potential to create an extremely small denominator relative to the numerator. The resulting division, while not creating a true divide by zero situation, does create abnormally large errors in the indicated angle.

These concepts are validated using the FPGA model later in this paper, but the results from (11) are shown in Figure 4. The two jammer sources are shown with thermal noise at a SNR of 20 dB in Figure 4, as the powers approach zero every half-period of the jammer signal spikes in the indicated angle can be seen in the lower graph.



**Figure 4.** Two amplitude modulated blink jamming signals with a signal-to-noise ratio of 20 dB are simulated using (11), demonstrating the noise effects in the indicated angle as the two signals approach zero amplitude.

### 2.3. Jammer-to-Signal Ratio Effects

Angle electronic attacks are typically applied in scenarios where a range-gate or velocity-gate attack has been used first to pull the tracking gate off the actual target. This is done to create the very high jammer-to-signal ratio (JSR) required for most angle deception techniques to be effective, such as cross-eye or cross-polarization jamming. To understand formation jamming in the context of JSR, the analysis discussed so far needs to be expanded.

Extending the analysis in (9), each sum signal can be expressed as superposition of the jammer and skin return:

$$s_n = p_n + j_n \tag{12}$$

where  $p_n$  is the power of the skin return and,  $j_n$  is the power of the jammer.

Substituting (12) into (9) results in:

$$\theta_i = \frac{\theta_a(p_a + j_a) + \theta_b(p_b + j_b)}{p_a + j_a + p_b + j_b} \tag{13}$$

which can be framed in terms of the JSR. Where the JSR is:

$$\chi_n = \frac{j_n}{p_n}. \tag{14}$$

Combining the Equations (13) and (14), we arrive at an expression for the indicated angle given the power of two jammers, and two radar targets, framed in terms of the JSR:

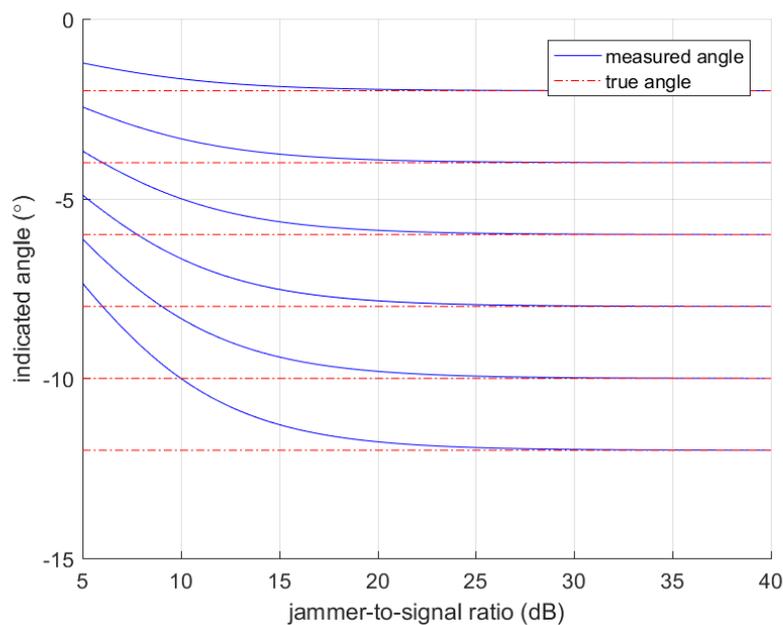
$$\theta_i = \frac{\theta_a p_a (\chi_a + 1) + \theta_b p_b (\chi_b + 1)}{p_a (\chi_a + 1) + p_b (\chi_b + 1)} \tag{15}$$

where  $\chi_a$  is the JSR from target  $a$  and  $\chi_b$  is the JSR from target  $b$ .

Simplifying this expression to the common blink jamming scenario, where only one target is jamming but the skin returns are present from both, the assumption is made that the skin returns are equal ( $p = p_a = p_b$ ). This changes (15) to

$$\theta_i = \frac{\theta_a (\chi_a + 1) + \theta_b}{\chi_a + 2} \tag{16}$$

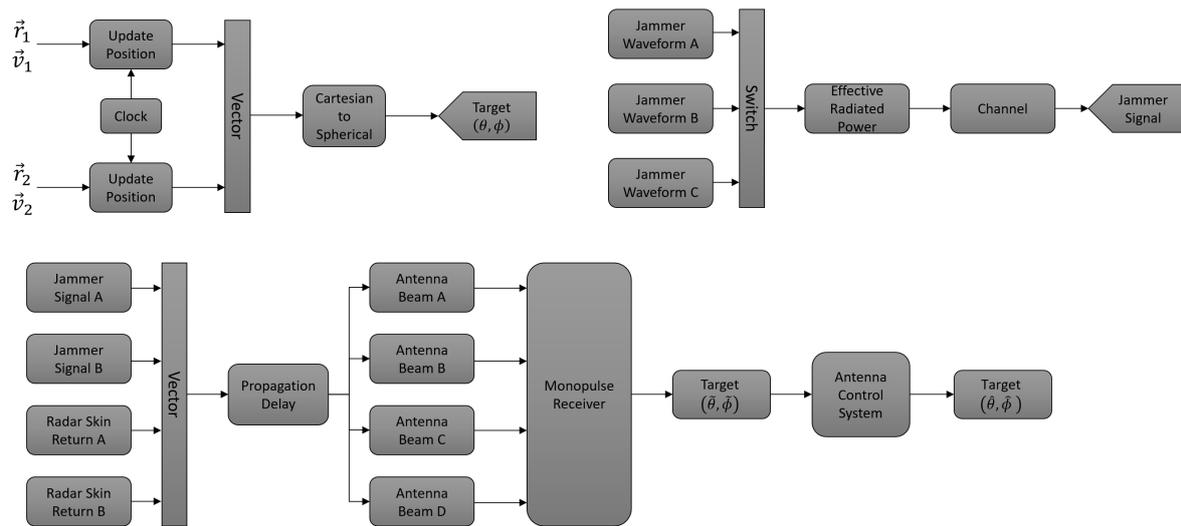
The critical question from (16) is at what JSR level does the jammer induced error become negligible? To evaluate this problem several MATLAB simulations were conducted, comparing the indicated versus true angle to the JSR for several different target separations. The results, shown in Figure 5, consistently demonstrate convergence at a JSR of 20 dB, and negligible effects of the skin return at 25 dB



**Figure 5.** The measured and true angles for target separations of 2, 4, 6, 8, 10, and 12 degrees, plotted against the jammer-to-signal-ratio.

### 3. Modelling Formation Jamming

In order to validate the theoretical understanding of formation jamming the blink jamming engagement was modelled in MATLAB and Simulink, with the radar receiver implemented on an FPGA in a hardware co-simulation. This model, shown in Figure 6, created a 3-D engagement between two jamming sources travelling independently and an amplitude comparison monopulse receiver with an antenna tracking system. The scenario accurately replicates a common electronic warfare problem of deceiving a semi-active guided missile.



**Figure 6.** The monopulse tracking radar model Field Programmable Gate Array (FPGA) implementation and tested in Simulink.

The Field Programmable Gate Array (FPGA) sub-systems were implemented in System Generator, then run using hardware-in-the-loop mode on a Xilinx Kintex-7 KC705 FPGA development board. This method served to validate the proposed electronic attacks using an actual radar receiver, as opposed to a software model. The remainder of this section details the model, test-bed, and FPGA implementation. The radar was modelled at baseband with a sampling frequency of 50 MHz.

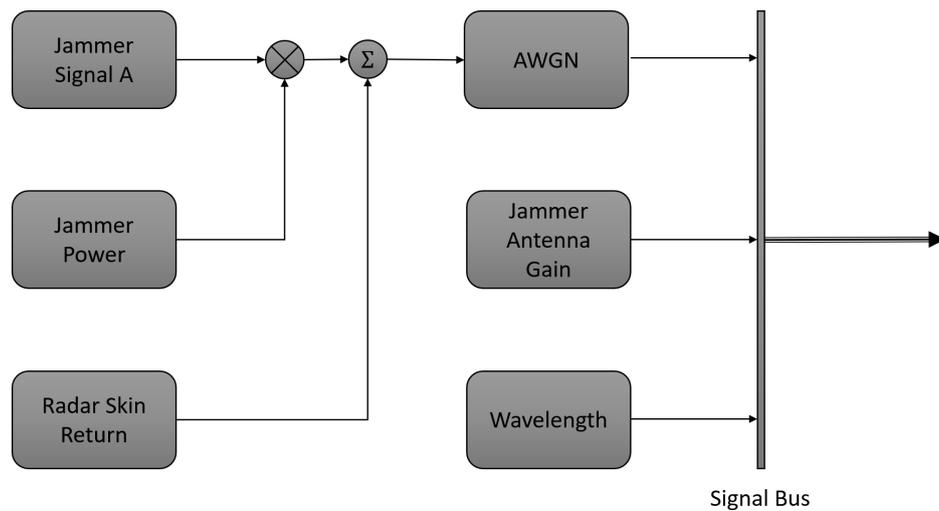
#### 3.1. Jammers and Target RF Models

Both jammer sources were modelled as point targets travelling from their initial position at a constant velocity. During the course of the Electronic Attack (EA) development and optimization process this was confined to a separation that put the two jammers within a formation of several hundred meters, inside the main lobe of the monopulse antenna. The distance of less than a kilometer replicates several possible formation jamming configurations including active and towed decoys, as well as chaff illumination jamming.

The jammers were developed to allow for several techniques to be evaluated: continuous illumination, blink jamming, and an amplitude modulated blink jamming attack, all with an adjustable jammer-to-signal ratio (this allowed for the skin return’s impact to be evaluated).

The jammer system, shown in Figure 7, is separated on the left and right into the two jammers with adjustable frequencies for the blink jamming attacks. The standard blink jamming attack’s envelope is created using a square wave of adjustable duty cycle. Similarly, the sinusoidal blink jamming attack uses the standard blink waveform, multiplied by a sinusoid of the same frequency.

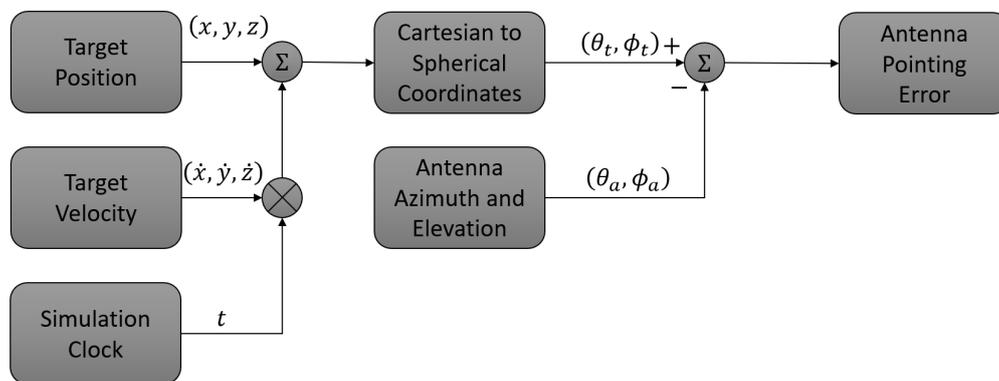
The selected formation jamming technique was then combined with the skin return and White Gaussian Noise (WGN) to reflect the signal-to-noise ratio of the monopulse receiver. The transmitter RF parameters were then embedded in a vector signal with the waveform, to allow the receiver to calculate the RF power received for each signal.



**Figure 7.** The system model for the formation jamming system, replicated for each of the two jammers. A set of user operated switches, embedded in the jammer signal subsystem, allowed for selection of the three possible jamming techniques.

### 3.2. Target Kinematics Model

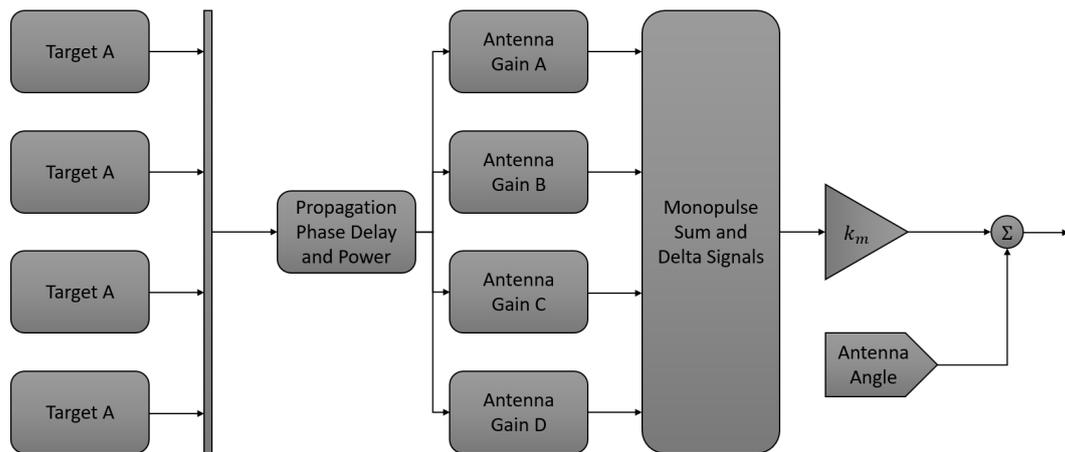
The jammer platforms were restricted to constant velocity with a fixed location tracking antenna, in order to isolate the formation jamming effects on the antenna from any other issues. The resulting model is shown in Figure 8, with identical models for the two targets on the top and bottom of the figure. Initial information on the target position and velocity vectors was provided via a MATLAB script, and the resulting target kinematics were updated at every simulation sample time. This data was then converted to spherical coordinates referenced the the antenna position for use in calculating the received power from each target.



**Figure 8.** The Simulink model for the target movement using constant velocity targets. The target kinematic information is then converted to spherical coordinates and compared to the pointing location of the tracking antenna to provide range, azimuth, and elevation information for modelling the received signal power and delay.

### 3.3. Monopulse Receiver

At the highest level in the simulation, shown in Figure 9, the monopulse receiver calculates the antenna gains for each monopulse beam, the RF path-loss, propagation delay, and then creates the sum and difference signals to calculate the angular error signal.

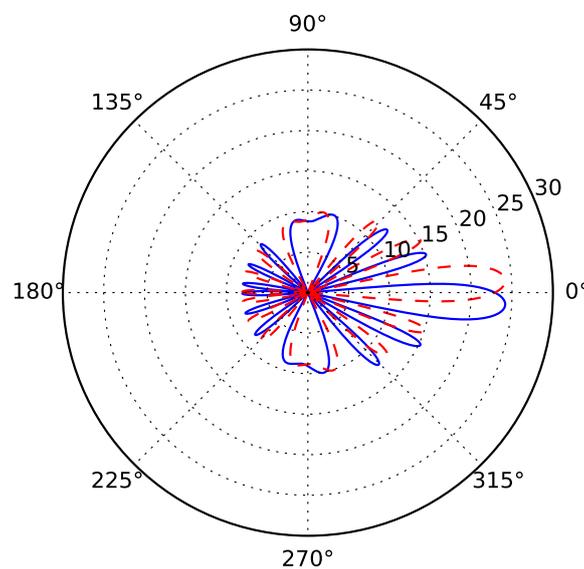


**Figure 9.** The Simulink model for the monopulse receiver, with the analog and testbed components implemented in Simulink and the digital systems on an FPGA.

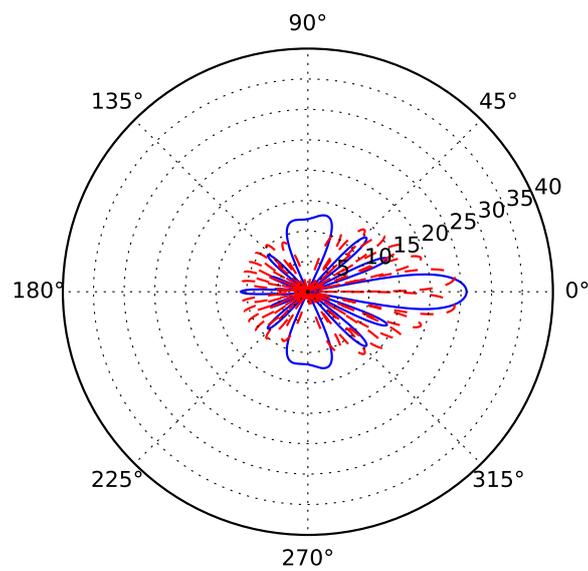
In this monopulse receiver, sinc antenna patterns were chosen to model the tracking radars [3]. These beam patterns are described by:

$$f(\theta) = \frac{\sin\left(\frac{\pi w}{\lambda} \sin \theta\right)}{\frac{\pi w}{\lambda} \sin \theta} \tag{17}$$

where  $\theta$  is the azimuth,  $w$  is the aperture width, and  $\lambda$  is the wavelength. A similar equation was applied for the elevation pattern, replacing the width with height. A typical radiation pattern is shown in Figure 10 for the left and right beams in a single plane, squinted by 0.468 beamwidths. The resulting sum and difference patterns of these two antennas are shown in Figure 11.

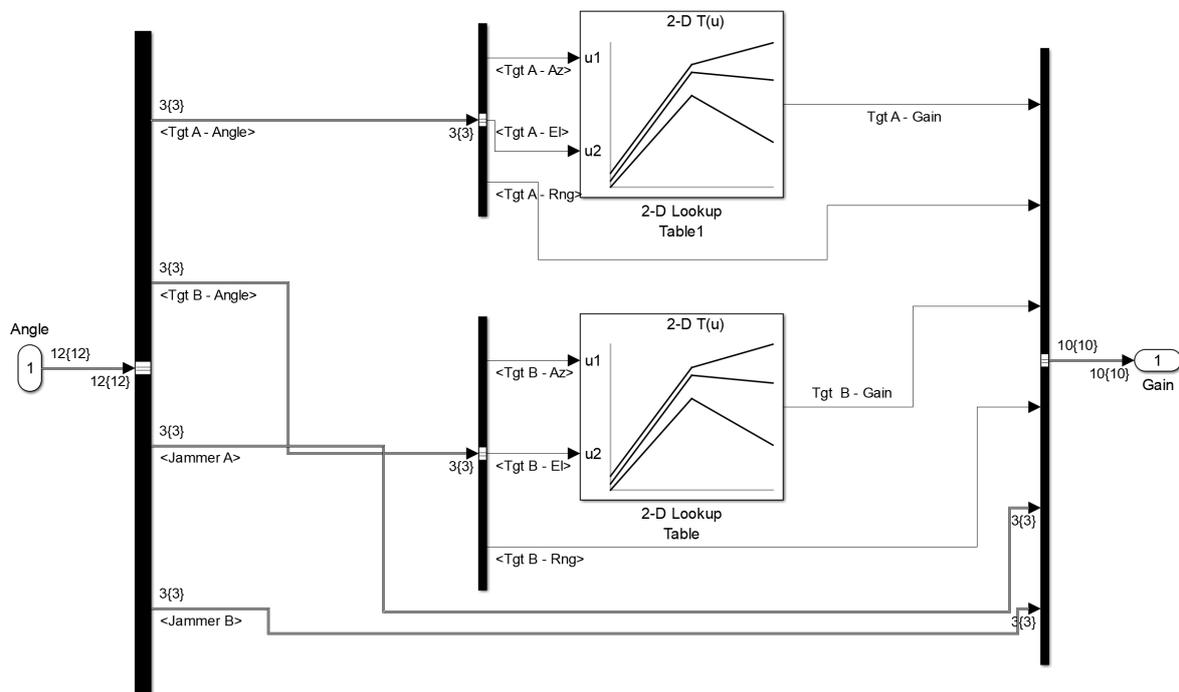


**Figure 10.** The left and right beam patterns for an amplitude comparison monopulse receiver squinted for angle measurement, units are in dBi.



**Figure 11.** The sum and difference beam patterns for an amplitude comparison monopulse receiver, units are in dBi.

The antenna gain values were stored in a 2-D look-up table for each beam, shown in Figure 12. After receiving the azimuth and elevation associated with a received signal the gain in that direction was calculated for use in determining the received power.

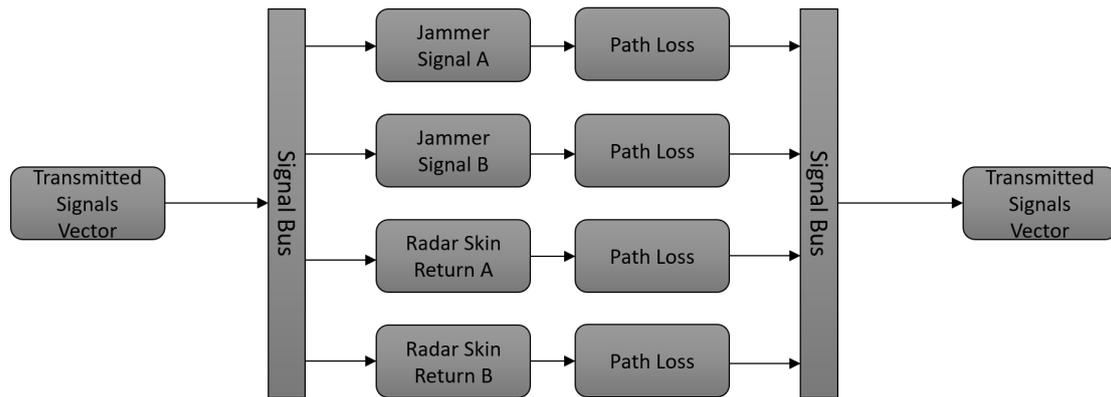


**Figure 12.** The antenna gain subsystem is implemented four times to replicate the four beams of the monopulse tracking system. In each case, as shown here, it takes the received azimuth and elevation for a signal and calculates the gain in that direction.

The received signal power was calculated using effective radiated power of the transmitter, receiver antenna gain, wavelength of propagation, and target range. This model used Friss transmission equation to determine the received power:

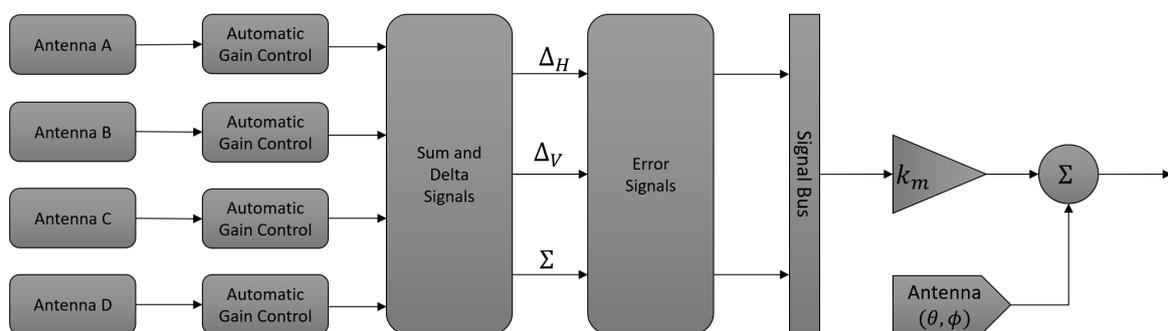
$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2} \tag{18}$$

where  $P_t$  is the transmitted power,  $G_t$  is the transmitter gain,  $G_r$  is the receiver gain, and  $R$  is the range [3]. The model implements (18) in Figure 13, along with the phase delay.



**Figure 13.** The received signal power subsystem takes the received signal vectors, and using the transmitted power and RF path-parameters, calculates the path loss and received power in each case.

The received signal power from each of the four antennas was processed through an amplitude comparison monopulse receiver to produce the sum and delta signals, convert those to error signals, and finally pointing error in degrees for azimuth and elevation, shown in Figure 14. The FPGA implementation was chosen to be done in floating point math, instead of fixed point. Floating point was chosen to effectively deal with the potential high dynamic ranges involved with specific techniques. The FPGA implementation itself was done on a Kintex-7 FPGA development board, operating at the sample frequency of the complete model. The total resource utilization of the FPGA was less than 10 % due to the relatively limited signal processing required (no finite impulse response filters, or similarly computationally intensive systems).



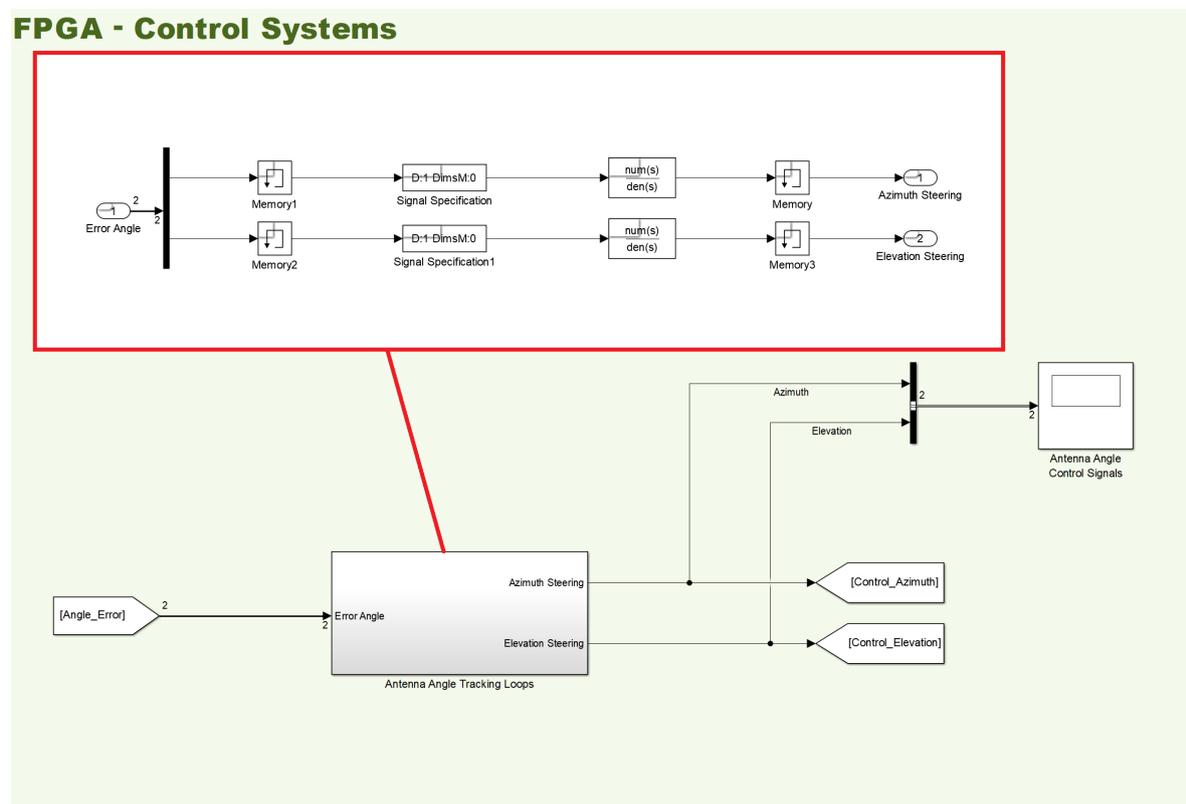
**Figure 14.** The monopulse receiver shown at the system level, calculates the error in the measured angle relative to the pointing angle of the antenna.

### 3.4. Antenna Tracking System

While the monopulse antenna system measures the error signal for the azimuth and elevation it performs no corrective action to reduce the error signals, that is the purpose of the antenna tracking system. First the antenna tracking loop, shown in Figure 15, takes the error signal for the azimuth and elevation positions and uses a second order tracking loop to estimate the target position based on the prior measurements and current indicated angle. The tracking loop was implemented as a second order transfer function of the form:

$$G(s) = \frac{\omega_n^2}{s^2 + 2\zeta\omega_n s + \omega_n^2} \tag{19}$$

where  $\zeta$  is the damping coefficient, and  $\omega_n$  is the natural frequency. The antenna tracking system is based on threat models known to be used in missile tracking radars [15,16]. The precise values were varied using a critically damped transfer function with a natural frequency in the 5 to 10 Hz range. It was implemented as an analogue model in (19), to reflect the analogue nature of the antenna movement and its servo motors.

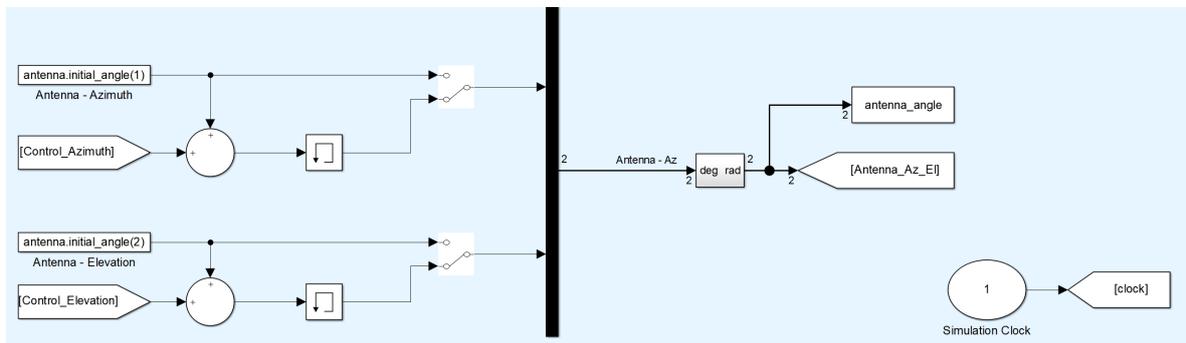


**Figure 15.** The Simulink model that takes the angle error signals in azimuth and elevation and, using a tracking loop, updates the estimate of the target position for the antenna.

The updated azimuth and elevation estimates were then used to move the antenna for the next Simulink model simulation step, shown in Figure 16. This follows the standard architecture of a radar control system where the parameter—azimuth or elevation—is measured, the measurement is compared to the estimate from the control system, the control system updates the estimate, and the antenna is pointed to the new estimate.

In this specific model of the antenna control system, see Figure 16, the initial pointing azimuth and elevation are provided at the simulation initialization. The sub-system then receives the change in pointing angle from the control system, and updates the memory block storing that value. The resulting

pointing angle is then fed back into the control system via a Simulink “Goto” block, while also stored to memory at every time step for later analysis.

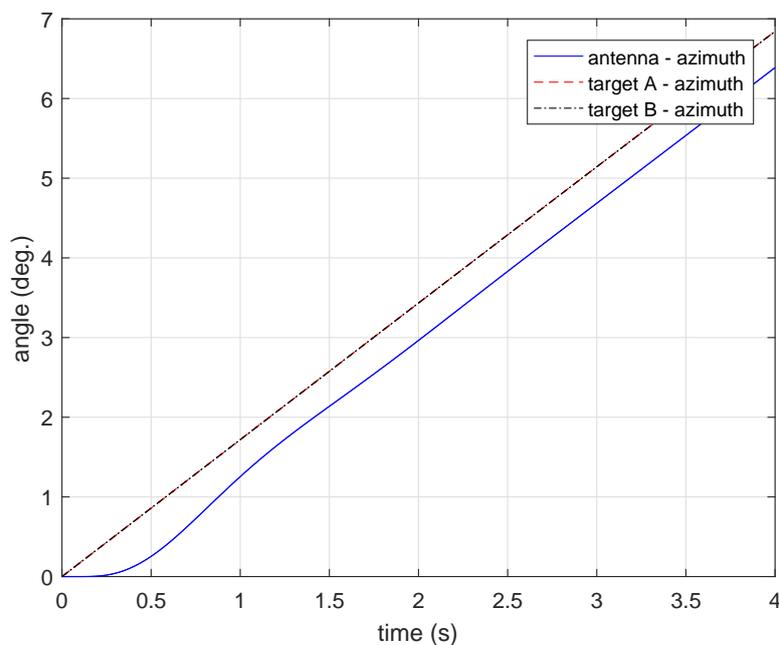


**Figure 16.** The Simulink model to adjust the pointing angle of the antenna using the existing angle and the output of the tracking system.

#### 4. Designing Formation Jamming Techniques

In order to isolate and understand the effects of different types of formation jamming on a monopulse radar, the engagement scenarios were limited to a single plane, in this case azimuth, during a cross-over engagement (a cross-over engagement is when an aircraft flies in a straight path, perpendicular to the radar, moving from a positive Doppler shift to a negative one). This geometry also allowed for understanding how the system performs as the sources move across the main-lobe.

Operating at a range of 10 km, the effectiveness of three types of formation jamming were explored: simultaneous continuous wave jamming, blink jamming, and amplitude modulated blink jamming. As a baseline the model was validated with only a single target active, the results for jammers A and B are shown in Figure 17, demonstrating the expected constant angle lag for a constant velocity target, in this case by approximately  $-0.5^\circ$  (the lag can be increased or decreased by adjusting the control loop’s natural frequency).



**Figure 17.** The azimuth response against a single target, run separately for targets A and B, in order to validate the system model.

#### 4.1. Continuous Jamming from Both Sources

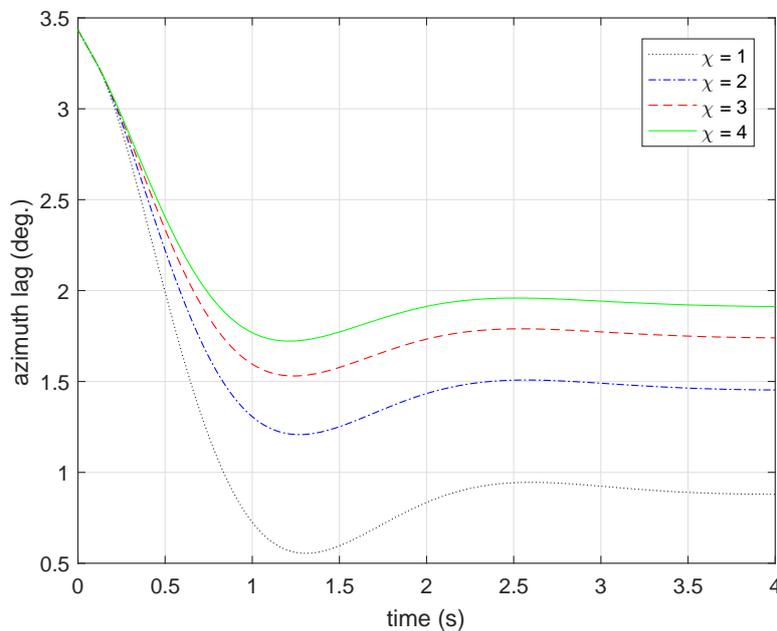
In the case of a continuous jamming signal from both sources, the jammers were positioned at boresight 10 km away from the radar, separated by a horizontal distance of 600 m in the  $y$ -plane. Travelling in the  $+y$  direction at a speed of 300 m/s, the targets followed the same path across the radar beam at a constant separation with the initial antenna pointing angle at 0 degrees in azimuth and elevation.

As expected from (9), the measured angle is a function of the power ratio of the two jammers

$$Y = \frac{P_{t_b}}{P_{t_a}} \tag{20}$$

where  $P_{t_a}$  is the transmitted power from jammer  $A$  and  $P_{t_b}$  is the transmitted power from jammer  $B$ .

The effects of this ratio change are shown in Figure 18, where the same scenario is used in all four simulations, with the only change being the ratio  $\chi$ . This changing power ratio causes the antenna to get “pulled” towards the stronger source.

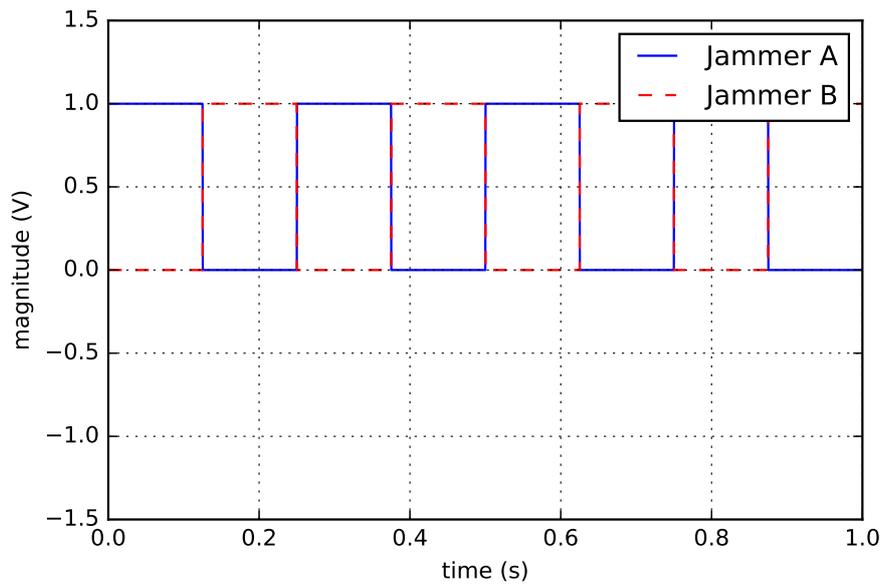


**Figure 18.** The azimuth lag for target A in a two target scenario with both sources providing a continuous wave jamming signal at different relative powers.

While not terribly useful in isolation this technique could be applied in a powerful way with an off-board decoy, by gradually shifting the tracking system from the target aircraft to the deceptive source. This could be accomplished by linearly increasing one source’s power while decreasing the other simultaneously causing the angle measured to shift towards the desired, higher power source, in a controlled fashion.

#### 4.2. Synchronous Blink Jamming

A more effective attack comes in the form of blink jamming, where the two sources “blink” on and off 180° out of phase. This is accomplished by using an amplitude modulated jammer signal, synchronized between the two platforms, as shown in Figure 19. The result is to isolate the two angle measurements from each other in time, while still operating a frequency low enough that the two platforms’ attacks can be synchronized in physical isolation.



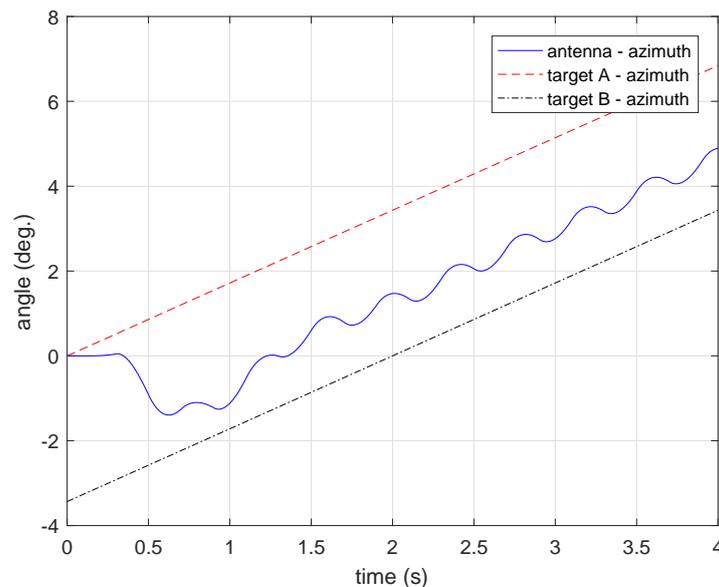
**Figure 19.** The jammer amplitude modulation waveforms from sources *A* and *B* operating at a 4 Hz blink and 180° out of phase.

The effect of this blink attack in the monopulse receiver is shown in Figure 20 in the form of an offset between the true target angles and the estimated angle. The frequency of the “blinking” is evident in the oscillations of the tracking signal which are related to the transfer function that governs the angle tracking system.

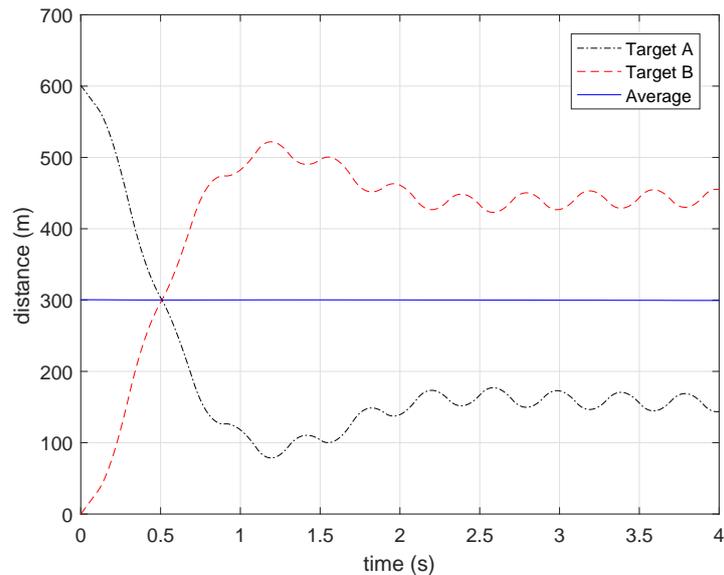
The metric generally associated with the effectiveness of an electronic attack while conducting self-defence jamming is miss distance. In this scenario the miss distance, shown in Figure 21, is defined as the distance between the tracking point at the target range and the actual target location. This is calculated as

$$d_m = R \tan (\theta_e) \tag{21}$$

where  $R$  is the target range, and  $\theta_e$  is the error in tracking angle.



**Figure 20.** The azimuth to targets *A* and *B* compared to the antenna’s pointing angle during the blink jamming scenario.

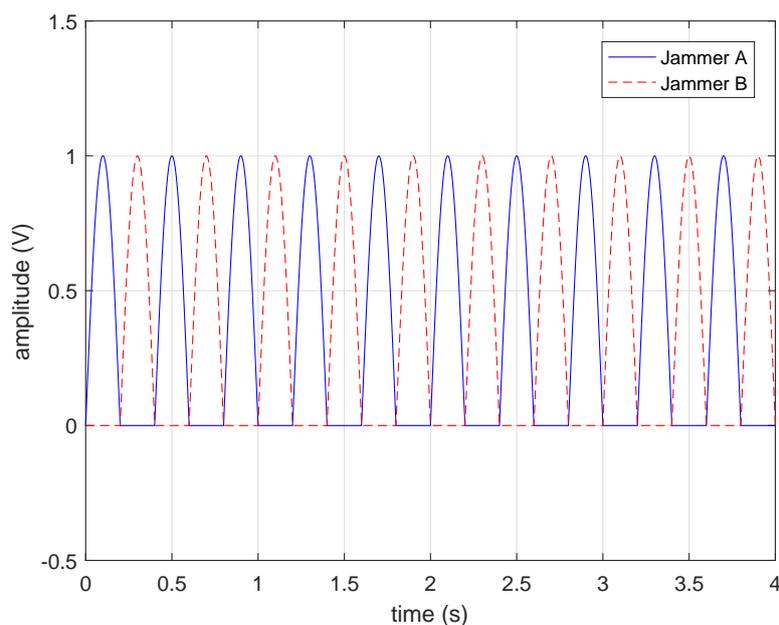


**Figure 21.** The miss distance, defined as the distance between the tracking point at the target range and its actual location, for targets *A* and *B*, as well as their average.

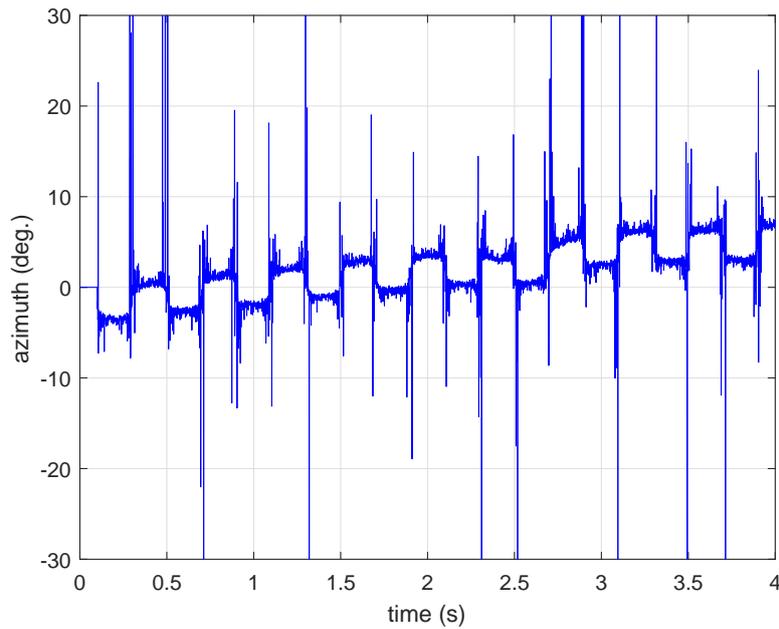
In a blink jamming scenario  $d_m$  oscillates between the two targets at the frequency of the blinking but depends primarily on the geometry of the two jammers relative to the antenna pattern of the monopulse antenna. In order to maximize this distance the two jammers should be separated by as large a range as possible, while staying within the main lobe of the radar.

#### 4.3. Sinusoid Modulated Blink Jamming

A variation of blink jamming was examined in order to evaluate a possible weakness in the monopulse system. This was the application of a sinusoidal amplitude modulation on the blink waveform, shown in Figure 22. The impact of this waveform is particularly evident in the error signal at the output of the monopulse receiver shown in Figure 23. As the two jammers hand-off and the power levels drop close to zero the angular error spikes, in some cases well above the  $\pm 30^\circ$  shown (the vertical axis were limited in the figure to capture the more detailed effects).

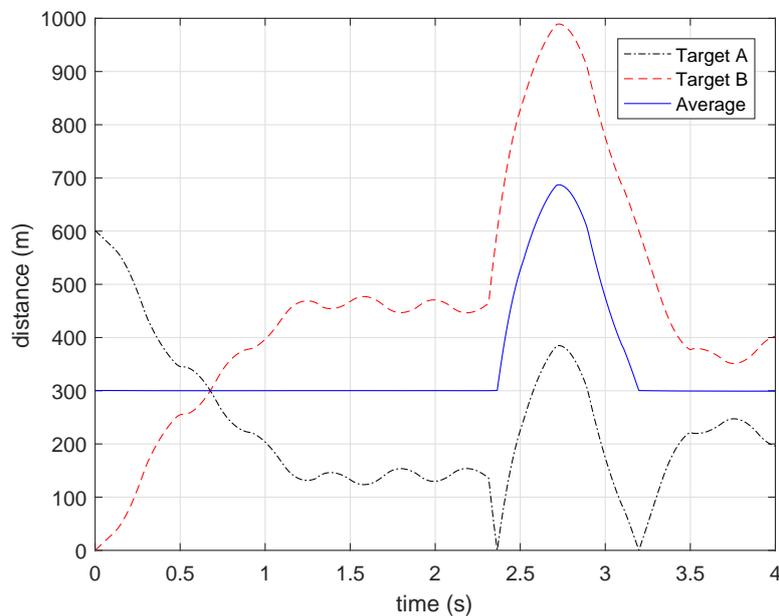


**Figure 22.** The jammer blink waveforms from sources *A* and *B* operating at a 4 Hz and  $180^\circ$  out of phase with a sinusoidal amplitude modulation applied.



**Figure 23.** The azimuth error signal from the monopulse receiver when a sinusoidal amplitude modulation is applied to the blink jamming signal.

The effect of this impulse in the tracking system is demonstrated in Figure 24 where, despite the filtering effects of the tracking system, the antenna is pulled off the targets at 2.4 s. While it locks back on to the centroid of the two sources over the next 1.5 s this kind of “break-lock” action is the goal of most electronic attacks against tracking radars.



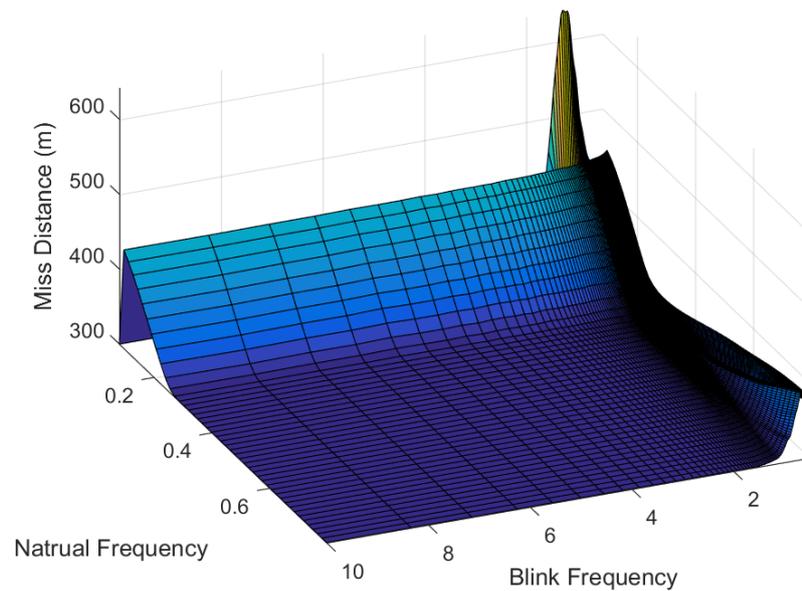
**Figure 24.** The miss distance, defined as the distance between the tracking point at the target range and its actual location, for targets A and B, as well as their average during a sinusoidal amplitude modulated blink jamming attack.

Understanding this effect and how it is created inside the radar receiver does not make it easy to predict due to the random behaviour of the noise. This differentiation in performance between blink jamming and its modulated version is best illustrated in Figures 25 and 26. In both figures the same jamming scenario is repeated with the two different waveforms while the natural frequency of the tracking loop and the blink frequency are swept over a range of values. In Figure 25 the unmodulated

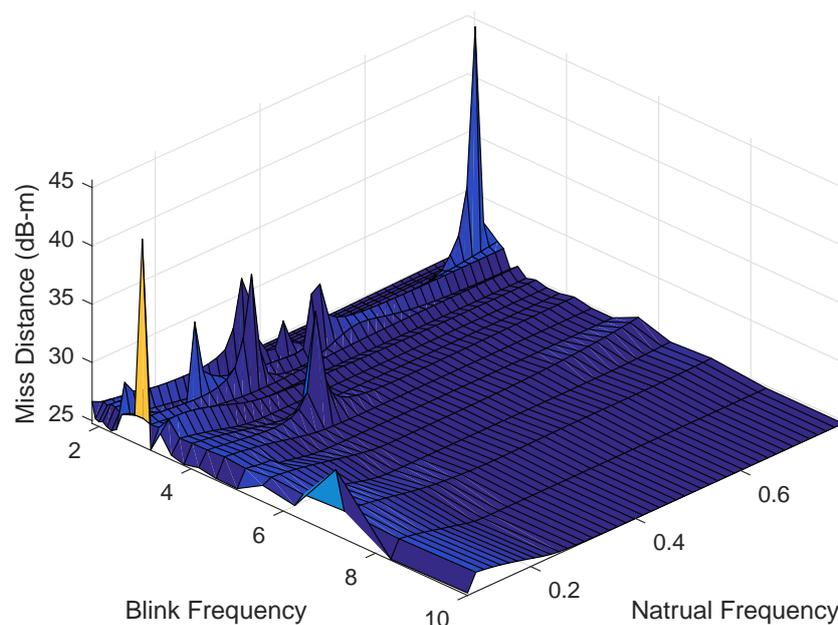
blink jamming attack shows a stable miss distance over a range of scenarios, tracking the mid-point of the two jammers except in cases of the natural frequency being too low, or the blink frequency simply not pulling the tracking system back-and-forth fast enough (the 600 m miss distance is indicating its actually tracking one of the targets that are separated by 600 m).

The effects seen in Figure 26 for the average miss distance of the amplitude modulated attack are very different, requiring a scale in dB-meters in stead of meters. Break-lock events can be seen occurring over a range of values causing large increases in miss distance compared to the more typical tracking point between the two aircraft.

Unfortunately the random nature of this break-lock event makes it a feature that cannot be designed to occur at specific times. However despite its random nature, even if it does not occur it still causes a miss distance equal to or greater than that of the unmodulated blink attack.



**Figure 25.** The average miss distance during a set of engagements with varied antenna angle tracking response frequencies and blinking frequencies using a square wave.



**Figure 26.** The average miss distance during a set of engagements with varied antenna angle tracking response frequencies and blinking frequencies using a sinusoidal wave.

## 5. Conclusions

This paper has developed a theoretical analysis of formation jamming against a monopulse radar, and validated that theory first using a model, and then an FPGA implementation of the receiver. These results were then built upon to analyze the performance of three methods of formation jamming: continuous wave, blink jamming, and amplitude modulated blink jamming. In all three cases, the system was validated on an FPGA and the potential application of each attack vector explored. Based on these experiments and analysis formation jamming attacks are clearly effective, and an amplitude modulated blink jamming attack is recommended for most scenarios, due to its ability to create break-lock events.

**Author Contributions:** Conceptualization, K.D.; methodology, K.D. and J.B.; software, K.D.; validation, K.D. and J.B.; formal analysis, K.D. and J.B.; investigation, K.D.; resources, K.D.; data curation, K.D.; writing—original draft preparation, K.D.; writing—review and editing, K.D. and J.B.; visualization, K.D.; supervision, J.B.; project administration, K.D. and J.B.; funding acquisition, K.D. and J.B. All authors have read and agree to the published version of the manuscript.

**Funding:** This research was funded by the Directorate of Technical Airworthiness and Engineering Support, Air Warfare project number 4102.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Maksimov, M. *Radar Anti-Jamming Techniques*; Artech House: Norwood, MA, USA, 1979.
2. O'Halloran, J.; Foss, C. *Jane's Land-Based Air Defence: 2008–2009*; Jane's Information Group: Coulsdon, UK, 2008.
3. Barton, D.K. *Radar System Analysis and Modeling*; Number v. 1; Artech House: Norwood, MA, USA, 2005.
4. Golden, A. *Radar Electronic Warfare*; American Institute of Aeronautics and Astronautics: Reston, VA, USA, 1987.
5. Lothes, R.; Szymanski, M.; Wiley, R. *Radar Vulnerability to Jamming*; Artech House: Norwood, MA, USA, 1990.
6. Sherman, S.; Barton, D. *Monopulse Principles and Techniques*; Artech House radar library, Artech House: Norwood, MA, USA, 2011.
7. Chrzanowski, E. *Active Radar Electronic Countermeasures*; Artech House: Norwood, MA, USA, 1990.
8. Leonov, A.; Fomichev, K. *Monopulse Radar*; Artech House radar library, Artech House: Norwood, MA, USA, 1986.
9. Yan, X.; Zhao, Y.; Yang, Q.; Li, P. Research on Synchronized non-coherent Blinking Jamming to Monopulse Radar Seeker. In Proceedings of the International Conference on Automatic Control and Artificial Intelligence (ACAI 2012), Xiamen, China, 24–26 March 2012; pp. 1753–1756. [[CrossRef](#)]
10. Li, P.; Geng, X.M.; Zhang, Y.; Zhai, Z.G. The Analysis on Angle Noise Produced by Blinking Jamming. In Proceedings of the 2009 International Asia Conference on Informatics in Control, Automation and Robotics, Bangkok, Thailand, 1–2 February 2009; pp. 441–444. [[CrossRef](#)]
11. Markin, E. Jamming Detection in Providing for Radar Jamming Immunity. In Proceedings of the IEEE EUROCON 2009, St. Petersburg, Russia, 18–23 May 2009; pp. 1565–1567. [[CrossRef](#)]
12. Hong, S.; Longbrake, M.; Saville, M.; Wu, Z. Non-Coherent Cooperative Jammer for Multi-Platform Applications. In Proceedings of the 2008 IEEE Radar Conference, Rome, Italy, 26–30 May 2008, pp. 1–6. [[CrossRef](#)]
13. Wang, J.; Geng, X.; Zhang, D. Analysis on Influence of Synchronous Blinking Jamming to Radar Seeker Antenna. In Proceedings of the 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, Dalian, China, 12–17 October 2008; pp. 1–4. [[CrossRef](#)]
14. Hoo, K.M.S. Adaptive Satcom Antenna Performance against Blinking Jammers. In Proceedings of the Antennas and Propagation Society Symposium 1991 Digest, London, ON, Canada, 24–28 June 1991; Volume 2, pp. 944–947. [[CrossRef](#)]

15. Hughes, R. *Analog Automatic Control Loops in Radar and EW*; Artech House: Norwood, MA, USA, 1988.
16. Bogler, P. *Radar Principles with Applications to Tracking Systems*; Wiley: Hoboken, NJ, USA, 1990.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).