Simulação e Análise dos Efeitos da Técnica de Interferência *Range Gate Pull-Off* em Detectores CFAR

Derek Nogueira, Leandro Geraldo da Costa, Dimas Irion Alves, Olympio Coutinho, André Martins Kruger e Renato Machado

***Resumo*— Radares de rastreamento são sistemas de detecção de alvos de alta resolução bastante usados em artilharias antiaéreas. Com o intuito de contrapor esses radares, aeronaves de combate são equipadas com sistemas eletrônicos interferidores embarcados, que empregam diversas técnicas de interferência. Dentre elas, destaca-se a técnica RGPO (*Range Gate Pull-Off*), que consiste em transmitir réplicas dos pulsos radar com um atraso em relação ao eco radar refletido. A técnica RGPO induz efeitos diretamente no processador CFAR do receptor radar, elevando o nível de *threshold* do processador a tal ponto de mascarar o alvo real e causar a detecção do eco de despistamento. Por meio de simulação computacional, foram desenvolvidos cenários para testar e analisar os efeitos dessa técnica de interferência em um radar de rastreamento utilizando-se diferentes detectores CFAR. Os resultados mostram diferenças de eficiência entre os detectores CA-CFAR e GOCA-CFAR, de acordo com a relação interferência-sinal, e a não efetividade da RGPO em detectores SOCA-CFAR e OS-CFAR. Este artigo demonstrou que a escolha do tipo de filtro CFAR deve ser adequada levando em consideração as funções do sistema radar e o ambiente em que este está submetido.**

***Palavras-Chave*— Interferência, CFAR, RGPO, radar, rastreamento.**

***Abstract*— Tracking radars are high-resolution target detection systems widely used in anti-aircraft artillery. In order to counter these radars, combat aircraft are equipped with on-board electronic jamming systems, which employ various jamming techniques. These include the RGPO (Range Gate Pull-Off) technique, which consists of transmitting radar pulse replicas with a delay in relation to the reflected radar echo. The RGPO technique induces effects directly on the radar receiver's CFAR processor, raising the processor's threshold level to such an extent as to mask the real target and cause the detection of the stray echo. Using computer simulation, scenarios were developed to test and analyze the effects of this interference technique on a tracking radar using different CFAR detectors. The results show differences in efficiency between CA-CFAR and GOCA-CFAR detectors, according to the interference-signal ratio, and the non-effectiveness of RGPO in SOCA-CFAR and OS-CFAR detectors. This article has shown that suitable CFAR detectors should be used according to the functions of the respective radar.**

***Keywords*— Jamming, CFAR, RGPO, radar, tracking.**

Derek Nogueira, André Martins Kruger, Instituto de Aplicações Operacionais, São José dos Campos, e-mail: [derekdesn, krugeramk]@fab.mil.br; Leandro Geraldo da Costa, Olympio Coutinho, Dimas Irion Alves, Renato Machado, Laboratório de Guerra Eletrônica, Instituto Tecnológico de Aeronáutica, São José dos Campos-SP, e-mail: [geraldolgc, olympio, dimasirion, renatomachado]@ita.br

I. INTRODUÇÃO

O radar de rastreamento é um recurso utilizado por sistemas de artilharia antiaérea para acompanhar alvos oponentes com o fim de os neutralizar [1]. Seu principal objetivo é fornecer informações precisas de alcance, azimute, elevação e velocidade do alvo [2]. Diversos tipos de processadores de sinal são empregados em sistemas radares para otimizar a relação sinal-ruido como o filtro casado, processamento Doppler e processador CFAR (*Constant of False Alarm Rate*) [2]. O processador foco desse artigo é o CFAR. Ele compara o nível de sinal recebido com um limiar de detecção, chamado *threshold*. O nível de *threshold* se ajusta para maximizar a detecção de alvos mantendo a probabilidade de falso alarme constante [2].

Para contrapor à ameaça da artilharia antiaérea que usa radar de rastreamento, são utilizadas técnicas de interferência eletrônica pelas aeronaves [1]. Essas técnicas têm o objetivo de impedir com que o radar tenha sucesso em detectar ou rastrear o alvo. Uma delas é a interferência por despistamento que visa enganar o radar adversário injetando sinais com informações falsas. O objetivo é que esse sinal interferente seja processado pelo sistema radar como se fosse um sinal legítimo, ocasionando o acompanhamento de um alvo falso [3]. A técnica *range gate pull-off* (RGPO) é um exemplo de interferência de despistamento, a qual gera informações falsas de distância da aeronave ao gerar alvos semelhantes ao eco, mas com atrasos progressivos e potência mais alta. Ao afastar o rastreio do radar distante o suficiente do alvo real para quebrar o acompanhamento, a interferência é interrompida e o radar perde o rastreamento do alvo [4]. Os efeitos da RGPO já foram analisados em radar de rastreamento, sem variação da JSR (*jamming to signal ratio*) [5]. Analisou-se o efeito de diferentes quantizações de fase e taxas de atrasos do sinal da RGPO e as diferenças de cada variação de parâmetro [6].

Muito em função da natureza reservada desta temática relacionada com a área de Guerra Eletrônica (GE), não se tem disponível em literatura científica aberta muito material de consulta, com uma consequente lacuna de conhecimento público. Neste contexto, este trabalho aborda os efeitos da técnica em diferentes detectores CFAR.

Sendo assim, neste artigo são simulados e analisados cenários de aplicação da técnica de interferência RGPO em radar de rastreamento com o uso de diferentes tipos de detectores CFAR variando a JSR. As contribuições desse trabalho são:

apresentar os efeitos da RGPO em detectores CFAR distintos sob diferentes JSR e analisar os seus impactos na efetividade da técnica de interferência utilizada como ataque eletrônico.

O restante deste artigo é organizado da seguinte forma: na Seção II são apresentados os princípios básicos de um detector CFAR e alguns tipos de detectores. Na Seção III é apresentado o simulador radar, a descrição do cenário e a metodologia aplicada para as simulações. Na Seção IV os resultados são apresentados e discutidos. Por fim, na Seção V são feitas as conclusões.

II. Detector CFAR

O processo de detecção de radar compara o sinal recebido com um limite chamado de *threshold*. Ele é ajustado para maximizar a detecção de alvos, mantendo constante a probabilidade de falso alarme (PFA). Alarmes falsos acontecem quando ruído ou interferência são erroneamente detectados como alvos. Para lidar com isso, o *threshold* pode ser ajustado conforme a variação intensidade das interferências, usando detectores CFAR [2].

A arquitetura de um detector CFAR genérico é apresentada na Figura 1, a qual foi adaptada de [2]. A célula sob teste (CUT) é o centro da janela CFAR onde o nível do sinal será avaliado em relação ao valor do *threshold*. As células de guarda (G) têm a função de reduzir a influência de partes do sinal que extrapolem a CUT e poderiam enviesar a estimada do *threshold*. As janelas de referência, *lagging* e *leading*, são as células onde são calculadas a potência do ruído para estimar o nível do *threshold* [2]. O *threshold* é determinado conforme [7]:

$$T_h = {\sigma_w}^2 \alpha, \tag{1}$$

em que ${\sigma_w}^2$ é a variância da somatória das amostras de ruído de cada janela de referência e α é a constante CFAR do detector.

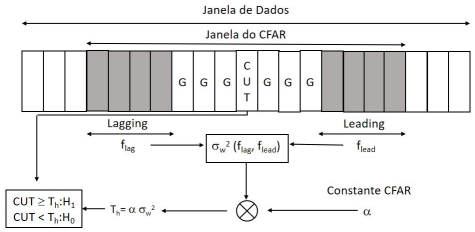

Fig. 1. Janela de sequência de dados de um detector CFAR 1D.

O modelo mais comum de detector é o CA-CFAR (*cell averaging*-CFAR). Ele calcula o *threshold* baseado na estimativa da média da potência das interferências nas janelas de referência. Esse tipo de detector é considerado adequado para ambientes homogêneos, ou seja, com interferências, ruídos e *clutters* regulares. Em cenários mais complexos, em que há a presença de *clutter* heterogêneo ou múltiplos alvos, por exemplo, este tipo de detector mostra-se não adequado, de modo que torna-se necessário o uso de algoritmos mais robustos para se adaptar melhor a essas características [2].

O primeiro exemplo de detector CFAR robusto é o GOCA-CFAR (*greatest of cell averaging*-CFAR). Considerado adequado para ambientes com baixa probabilidade de se encontrar alvos próximos em região de *clutter* altamente homogêneo. Nesse cenário, portanto, ocorre mais mascaramento de alvos próximos [7]. Nesse tipo de detector, as janelas *lagging* e *leading* são calculadas separadamente para criar duas estimativas independentes, baseads em $\frac{N}{2}$ células de referência. O *threshold* é calculado a partir da maior das duas estimativas [7]:

$$T_h = \alpha_{GO} \max({\sigma_{w1}}^2, {\sigma_{w2}}^2), \tag{2}$$

em que α_{GO} é a constante CFAR ajustada para o modelo GOCA-CFAR, ${\sigma_{w1}}^2$ a média das janelas *lagging* e ${\sigma_{w2}}^2$ a média das janelas *leading*.

Outro detector CFAR robusto é o SOCA-CFAR (*smallest of cell averaging*-CFAR), que tem por objetivo a redução do efeito de mascaramento de alvos próximos mais fracos. O ponto negativo é o aumento da ocorrência de falsos alarmes [7]. Como no GOCA-CFAR, as janelas *lagging* e *leading* são calculadas separadamente, mas o *threshold* é calculado a partir da menor das duas estimativas [7]:

$$T_h = \alpha_{SO} \min({\sigma_{w1}}^2, {\sigma_{w2}}^2), \tag{3}$$

sendo α_{SO} a constante CFAR ajustada para o modelo SOCA-CFAR.

Uma alternativa aos modelos anteriores é o OS-CFAR (*order statistic*-CFAR), classe de CFAR baseada em estatística de ordem. Para reduzir o efeito de mascaramento, substitui-se a média do conteúdo das janelas de referência da estrutura padrão do CA-CFAR pelo ordenamento dos dados determinando o *k*-ésimo elemento da lista [7]. No OS-CFAR, a estatística de ordem k mais adequada para determinado cenário é selecionada como representativa do nível de interferência e um *threshold* apropriado é definido como um múltiplo desse valor [7]:

$$T_h = \alpha_{OS} z_k, \tag{4}$$

sendo α_{OS} a constante OS-CFAR e z_k a janela de referência k.

III. Metodologia das simulações

Para as simulações, foi utilizado um simulador radar desenvolvido com o *software* MATLAB. Este simulador foi desenvolvido no ITA e está sob processo de registro de software. Um exemplo de sua interface é apresentado na Figura 2.

Na avaliação experimental, considera-se um radar de rastreamento com características conforme a Tabela I. A aeronave a ser rastreada está a 2 mil metros de distância do radar. Sua velocidade é de 100 m/s se aproximando do radar na mesma radial. A sua seção reta radar (RCS) é de 3 m^2. A forma de onda do radar é do tipo linear modulada em frequência. Os pulsos são integrados a cada 10 pulsos. A simulação tem 4 mil integrações de pulsos. Esses parâmetros foram determinados para representar fidedignamente um cenário real de guerra eletrônica [4]. A interferência inicia a partir da integração de pulso 1 mil. Este cenário pode ser caracterizado como uma situação de uma aeronave estar se aproximando de um alvo de

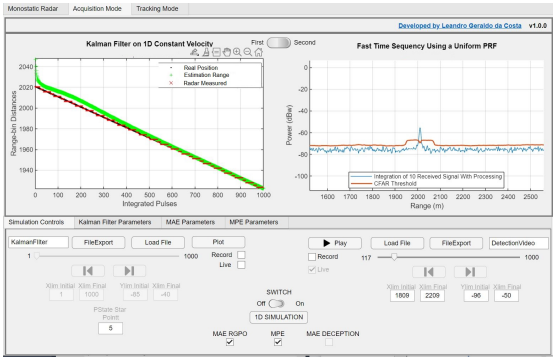

Fig. 2. Interface do simulador desenvolvido pelos autores.

interesse, o qual é protegido por uma artilharia antiaérea. Esse sistema de proteção aérea utiliza um radar de rastreamento como ferramenta de controle e orientação do seu armamento.

TABELA I

PARÂMETROS GERAIS DO RADAR DE RASTREAMENTO NAS SIMULAÇÕES

Parâmetro	Valor
Potência de Pico	1.000 kW
Frequência da Portadora	10 GHz
Frequência de Repetição de Pulsos	10 kHz
Largura de Pulso	500 ns
Largura de Banda	29,98 MHz
Taxa de Amostragem	65 MHz
Duty Cycle	0,01
Relação Sinal Ruído	10
Probabilidade de Falso Alarme	10^{-4}
Resolução de Distância	5 m

Para cada simulação, a JSR foi variada em 6, 8, 10 e 12 dB para cada detector CFAR. Foram usados os detectores CA, GOCA, SOCA e OS-CFAR com 100 janelas de referência e 4 células de guarda.

IV. SIMULAÇÕES E RESULTADOS

No primeiro cenário de simulação foram avaliados os efeitos da variação da JSR em um cenário de RGPO aplicado à um detector CA-CFAR. A Figura 3 apresenta os resultados dos sinais recebidos pelo radar contendo a interferência, sinal real e comportamento do *threshold* de cada variação de JSR.

Pode-se observar nos resultados apresentados na Figura 3 que com JSR de 6 e 8 dB o sinal real do alvo não é mascarado pela interferência. Por outro lado, para as condições de JSR de 10 e 12 dB, as interferências conseguem sobrepor o alvo suficientemente para serem efetivas. Dessa forma, a técnica de interferência foi efetiva em detector CA-CFAR para JSR de 10 e 12 dB, provocando a elevação do *threshold* acima da amplitude do sinal real do alvo, atingindo o objetivo do ataque eletrônico que é despistar em distância.

No segundo cenário de simulação foram avaliados os efeitos da variação da JSR, considerando a aplicação de RGPO à um detector GOCA-CFAR. A Figura 4 apresenta os resultados dos sinais recebidos pelo radar contendo a interferência, sinal real e comportamento do *threshold* de cada variação de JSR.

Pode-se observar que com 6 dB de JSR o sinal real do alvo não é mascarado pela interferência. Por outro lado para

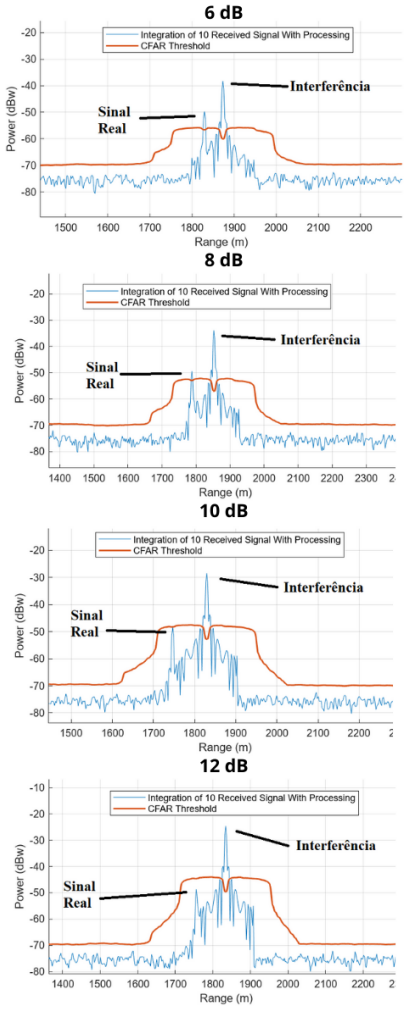

Fig. 3. Simulações de RGPO com variação de JSR em detector CA-CFAR.

as interferências com JSR de 8, 10 e 12 dB o efeito de interferência sobre o sinal é suficiente para enganar o receptor. Dessa forma, a técnica de interferência foi efetiva em detector GOCA-CFAR com 8, 10 e 12 dB de JSR, elevando o *threshold* acima da amplitude do sinal real do alvo, atingindo o objetivo do ataque eletrônico que é despistar em distância.

Em comparação com os resultados no detector CA-CFAR, utilizando o GOCA-CFAR, com apenas 8 dB de JSR é suficiente para elevar o *threshold* e mascarar o sinal real. Isso era esperado devido ao conceito do cálculo do *threshold* no detector GOCA-CFAR, em que as médias das janelas *lagging* e *leading* são calculadas separadamente e o valor maior é baseado para a média geral, como aplicado em (2). O detector CA-CFAR tem melhor performance em ambientes homogêneos em comparação ao GOCA-CFAR [8] - [10]. Como pode-se observar na Tabela II, a RGPO aplicada em radar com detector GOCA-CFAR eleva o *threshold* entre 5 e 6 dBW a mais em relação ao CA-CFAR. Pode-se afirmar que o detector CA-CFAR é mais efetivo que o GOCA-CFAR em cenários de interferência eletrônica com técnicas de alvos falsos, como é o caso da RGPO, pelo fato do primeiro ter melhor desempenho em diferenciar múltiplos alvos [11].

No terceiro cenário de simulação foram considerados os

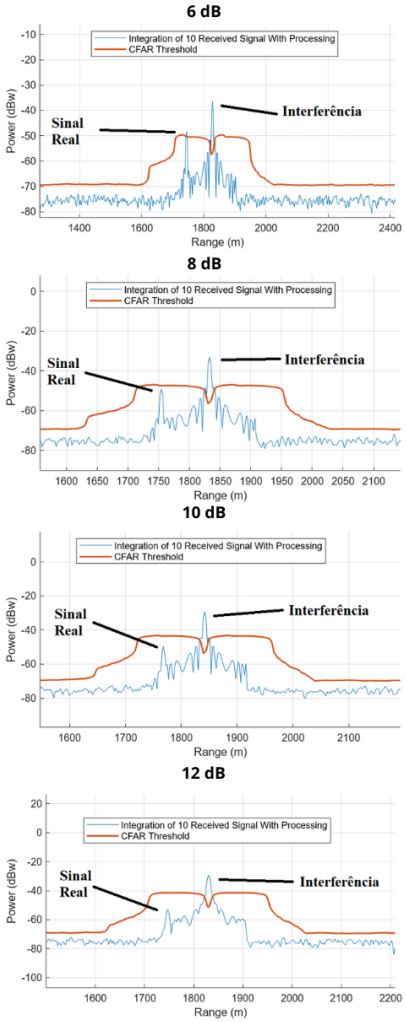

Fig. 4. Simulações de RGPO com variação de JSR em detector GOCA-CFAR

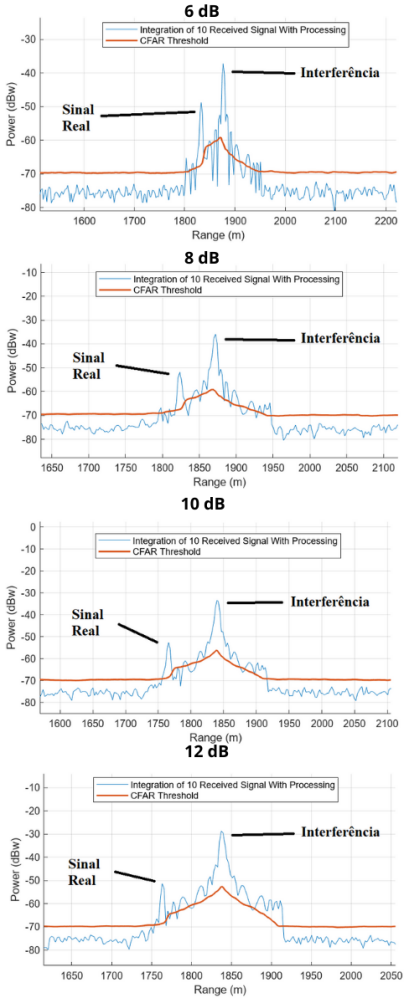

Fig. 5. Simulações de RGPO com variação de JSR em detector SOCA-CFAR

TABELA II

COMPARAÇÃO DA ELEVAÇÃO DO *THRESHOLD* NAS SIMULAÇÕES CA E GOCA-CFAR

JSR	*Threshold* CA	*Threshold* GOCA
6 dB	-56 dBW	-50 dBW
8 dB	-53 dBW	-47 dBW
10 dB	-48 dBW	-43 dBW
12 dB	-45 dBW	-40 dBW

efeitos da variação da JSR em um cenário de RGPO aplicado em um detector SOCA-CFAR. A Figura 5 apresenta os resultados dos sinais recebidos pelo radar contendo a interferência, sinal real e comportamento do *threshold* de cada variação de JSR.

Pode-se observar que nenhuma JSR foi capaz de mascarar o sinal real do alvo. Ao contrário do GOCA-CFAR, o detector SOCA-CFAR calcula o seu *threshold* considerando a média menor entre as médias das janelas *lagging* e *leading*, como aplicado em (3). Sendo assim, a elevação do *threshold* é baixa para que o sinal interferente afete na detecção do sinal real. Isso era esperado, pois o detector SOCA-CFAR tem a vantagem de distinguir melhor múltiplos alvos. Por outro lado, há considerável elevação da taxa de falso alarme, gerando outros problemas na detecção do alvo [8] - [10]. De fato, para cenário desse trabalho, o detector SOCA-CFAR é imune à técnica RGPO de acordo com os resultados obtidos.

No quarto cenário de simulação foram avaliados os efeitos da variação da JSR em um cenário de RGPO aplicado à um detector OS-CFAR. A Figura 6 apresenta os resultados dos sinais recebidos pelo radar contendo a interferência, sinal real e comportamento do *threshold* de cada variação de JSR.

Como pode ser observado, a interferência não tem influência significativa para elevar o *threshold* do CFAR o suficiente para mascarar o sinal do alvo. O uso da estatística de ordem, em vez de uma estimativa média, torna o detector pouco suscetível ao mascaramento por alvos próximos nos cenários avaliados neste artigo. Desse modo, para suprimir a capacidade de detecção e rastreio do radar utilizando esse tipo de detector CFAR é necessário o uso de técnicas de contramedida eletrônicas mais complexas. Por exemplo, algumas possíveis técnicas candidatas são as interferências por bloqueio [7].

Adicionalmente, devido ao grande número de cálculos estatísticos, esse tipo de detector exige uma alta capacidade de processamento do sistema onde está sendo utilizado [7]. O autor em [12] apresenta em seu trabalho simulações de

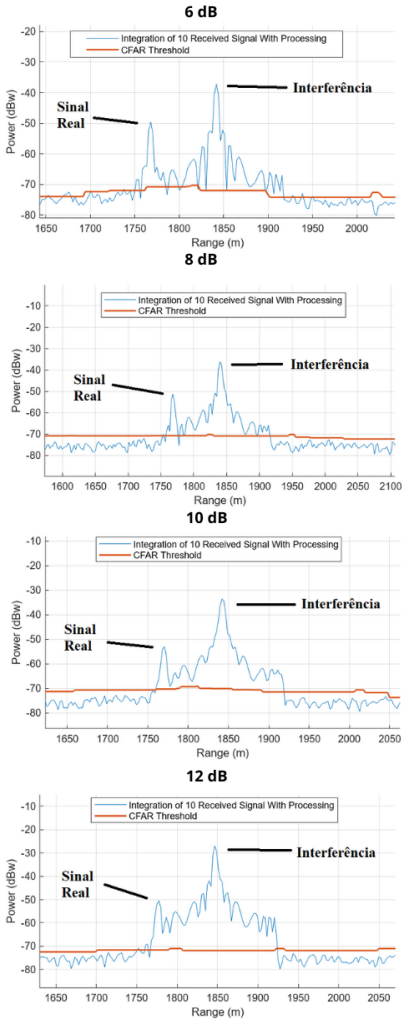

Fig. 6. Simulações de RGPO com variação de JSR em detector OS-CFAR

radar com diferentes detectores CFAR e apresenta resultados da diferença do custo de processamento de cada modelo. A comparação entre os custos evidencia que o OS-CFAR exige aproximadamente sete vezes mais processamento em relação aos demais detectores CFAR analisados [12].

V. Conclusões

Foram feitas simulações com diferentes tipos de detectores CFAR variando a JSR. Com o detector CA-CFAR, a RGPO mostrou não efetiva para JSR igual ou abaixo de 8 dB. Já com o detector GOCA-CFAR, como era esperado, somente para a JSR de 6 dB a técnica RGPO não foi efetiva. Para os valores de JSR de 8, 10 e 12 dB a técnica foi capaz de atingir seu objetivo, pois esse tipo de detector apresenta uma maior elevação de *threshold* do que para o caso do CA-CFAR.

As simulações com o detector SOCA-CFAR apresentaram um tipo de detector que não é suscetível à técnica RGPO, pois a técnica não é capaz de elevar o *threshold* de maneira suficiente para mascarar o alvo real. O ponto negativo desse modelo reside no aumento indesejável de falsos alarmes. Outra variação CFAR em que a RGPO não se mostrou efetiva foi com o OS-CFAR. Devido à sua forma de processar os cálculos para estimar o *threshold*, essa técnica é capaz de reduzir o mascaramento do alvo real sem elevar o *threshold*, bem como não causar o aumento dos falsos alarmes como ocorre no SOCA. O único fator negativo desse detector é a necessidade de um sistema radar com maior complexidade e capacidade de processamento de dados.

Por fim, os experimentos mostraram que a escolha do detector CFAR de um radar deve ser adequado para as suas funções. No caso de um radar de rastreamento de um sistema de defesa antiaérea, o cenário esperado é um ambiente com diferentes fontes de interferência eletromagnética, utilizados, por exemplo, para a aparição de alvos falsos no sistema radar de rastreamento. Neste tipo de cenário, há alta possibilidade de múltiplos alvos, sejam alvos reais ou falsos, criados por alguma técnica de interferência. Logo, a escolha de um detector CFAR robusto com a capacidade de discriminação alvos próximos é necessária para esse tipo de radar.

Agradecimentos

Os autores desse artigo agradecem à Força Aérea Brasileira (FAB), ao Programa de Pós-Graduação em Aplicações Operacionais (PPGAO) e ao Laboratório de Guerra Eletrônica (LabGE-ITA), pelo apoio durante a realização deste trabalho. Este estudo foi financiado em parte pela Financiadora de Estudos e Projetos (FINEP) sob benefício 01.22.0581.00.

Referências

[1] R. Grant, *The Radar Game: Undertanding Stealth and Aircraft Survability*. Mitchell Institute Press, 2010.
[2] M. A. Richards, *Principles of Modern Radar: Basic Principles*. Citeseer, 2010.
[3] F. Neri, *Introduction to electronic defense systems*. SciTech Publishing, 2006.
[4] R. N. Lothes, *Radar Vulnerability to Jamming*. Norwood: Artech House, 1999.
[5] J. L. Luo, Z. S. Shi e X. N. Wang , “Research on the effect of range gate pull-off jamming on the tracking radar and the countermeasures" *Advanced Materials Research, Trans Tech Publ*, v. 433, pp. 5789–5793, 2012.
[6] M. Greco et al, “Effect of phase and range gate pull-off delay quantisation on jammer signal" *IEE Proceedings-Radar, Sonar and Navigation, IET*, v. 153, n. 5, pp. 454–459, 2006.
[7] M. A. Richards, *Fundamentals of radar signal processing*. McGraw-Hill Education, 2014.
[8] P. P. Gandhi e S. A. Kassam, “Analysis of CFAR processors in nonhomogeneous background" *IEEE Transactions on aerospace and electronic systems*, v. 24, n. 4, pp. 427–445, 1988.
[9] A. Jalil, H. Yousaf e M. I. Baig, “Analysis of CFAR techniques" *International Bhurban Conference on applied sciences and technology (IBCAST)*, 2016.
[10] M. Sahal et al, “Comparison of CFAR methods on multiple targets in sea clutter using spx-radar-simulator" *International seminar on intelligent technology and its applications (ISITIA)*, pp. 260-265, Julho 2020.
[11] D. Kumuda et al, “Multitarget detection and tracking by mitigating spot jammer attack in 77-GHz mm-wave radars: an experimental evaluation" *IEEE Sensors Hournal*, v. 23, n. 5, pp. 5345–5361, 2022.
[12] F. Yavuz, “Radar target detection with CNN" *29th European Signal Processing Conference (EUSIPCO*, pp. 1581–1585, 2021.