Algoritmo Distribuído para Enxame de Drones Defensivos de Pequeno Porte Baseado em Planejamento

Lucas Silva Lima[1], João Paulo de Andrade Dantas[2] e Paulo Marcelo Tasinaffo[1]
[1]Instituto Tecnológico de Aeronáutica, São José dos Campos/SP - Brasil
[2]Instituto de Estudos Avançados, São José dos Campos/SP - Brasil

***Resumo*— Este trabalho propõe um algoritmo distribuído para defesa de pontos críticos por enxames de drones de pequeno porte, operando em rede *ad hoc* sem comando central. A abordagem utiliza planejamento clássico para coordenação defensiva, permitindo reação autônoma às ameaças. O sistema baseia-se na troca de mensagens entre drones para mesclar informações parciais, compondo representações atualizadas do ambiente e aumentando robustez e eficácia. Foi desenvolvido o simulador *DroneSwarm2D* para avaliar o desempenho em cenários com perda de mensagens, falhas sensoriais e variações no número de agentes. Os resultados experimentais demonstram capacidade de manter a integridade do ponto de interesse sob condições adversas, evidenciando o potencial de algoritmos distribuídos em aplicações defensivas. Comparações entre arquiteturas distribuída e centralizada sugerem superioridade da primeira em todos os cenários testados. O estudo discute limitações do modelo e sugere integração com aprendizado de máquina para trabalhos futuros.**

***Palavras-Chave*— Simulação de Defesa, Algoritmo Distribuído, Enxame de Drones.**

I. Introdução

O uso de Sistemas Aéreos Não Tripulados (*Uncrewed Aerial Systems* – UAS) tem se intensificado significativamente em operações militares nas últimas décadas [1]. Esse crescimento é impulsionado pela redução de custos, miniaturização de sensores e acessibilidade de algoritmos de navegação autônoma [2]. A proliferação global dos UAS, empregados por mais de oitenta países [3], tem sido particularmente associada aos drones leves, ágeis e de baixo custo [4].

Paralelamente, grupos armados não-estatais têm adaptado plataformas comerciais para fins militares, incluindo missões de reconhecimento e ataques com artefatos improvisados [5]. Essa tendência representa um desafio crescente para sistemas de defesa tradicionais, que não foram originalmente concebidos para enfrentar múltiplos alvos pequenos e lentos.

Segundo [6], sistemas de detecção convencionais apresentam limitações significativas ao lidar com alvos caracterizados por baixa Seção Reta Radar (*Radar Cross Section* – RCS). Essa vulnerabilidade é explorada por estratégias de saturação deliberada de sistemas de alerta. Em conflitos recentes, observaram-se relatos do uso de drones caseiros adaptados com baterias de maior capacidade e cargas explosivas improvisadas, demonstrando a facilidade de conversão de plataformas artesanais em armas para destruir aeronaves estacionadas ou sobrecarregar defesas terrestres, conforme ilustrado na Fig. 1.

Fig. 1: Drone caseiro adaptado com bateria de maior capacidade e carga explosiva improvisada fixada com fita adesiva.

Fonte: [7]

A defesa convencional permanece estruturada sobre arquiteturas hierárquicas de Comando e Controle (C2), cuja eficácia depende da integridade de sensores fixos e conectividade em tempo real [8]. Essa dependência de infraestrutura centralizada revela-se vulnerável diante de ataques dinâmicos, *jamming* e *spoofing*, capazes de comprometer comunicações e paralisar centros de decisão [3].

Os métodos tradicionais enfrentam limitações críticas: assimetria de custo-efetividade entre mísseis caros e UAS comerciais adaptados; exaustão logística por alto volume de incursões; versatilidade dos UAS ofensivos em manobras de baixa altitude; rigidez estrutural de sistemas centralizados; e baixa adaptabilidade a alvos móveis múltiplos com padrões não-balísticos.

Diante desse cenário, este trabalho propõe uma arquitetura de defesa aérea distribuída baseada em UAS autônomos operando em redes *ad hoc* descentralizadas. A solução elimina pontos únicos de falha, favorece escalabilidade e permite maior adaptabilidade diante de falhas sensoriais e interrupções comunicacionais. Desenvolvida inteiramente em ambiente simulado bidimensional na camada de aplicação do modelo OSI (*Open Systems Interconnection*) [9], a comunicação é modelada por trocas de mensagens ponto-a-ponto [10].

O simulador *DroneSwarm2D* permite avaliar táticas defensivas distribuídas, explorando autonomia dos agen-

L. S. Lima, limalsl@ita.br; João P. A. Dantas, jpdantas@ita.br; Paulo M. Tasinaffo, tasinaffo@ita.br.

tes, robustez comunicacional e eficiência de coordenação descentralizada para proteção de pontos críticos contra ataques coordenados de múltiplos UAS inimigos [11].

O restante do trabalho está organizado em cinco seções principais: a Seção II apresenta revisão bibliográfica sobre simulação militar, coordenação distribuída e aspectos éticos de sistemas autônomos; a Seção III aborda o desenvolvimento teórico cobrindo processamento distribuído, redes *ad hoc* aéreas e planejamento automatizado multiagente; a Seção IV descreve a metodologia apresentando o simulador *DroneSwarm2D* e as táticas experimentais para avaliação comparativa; a Seção V apresenta os resultados e discussões com análises de desempenho e robustez dos algoritmos propostos; e a Seção VI sintetiza as conclusões, contribuições e limitações identificadas.

II. Revisão Bibliográfica

A literatura contemporânea evidencia o avanço das pesquisas voltadas à aplicação de UAS autônomos em cenários de defesa, com ênfase em coordenação distribuída e estratégias colaborativas de interceptação [12].

No campo da simulação militar aplicada, [13] apresentam o Ambiente de Simulação Aeroespacial (ASA), um *framework* desenvolvido pelo Instituto de Estudos Avançados da Força Aérea Brasileira (IEAv/FAB). O ASA constitui uma solução de infraestrutura distribuída para modelagem de cenários operacionais militares, integrando três módulos: *AsaSimulation* (núcleo de simulação), *AsaUserInterfaces* (interfaces de usuário) e *AsaDataScience* (análise de dados). A arquitetura distribuída permite processamento em múltiplas máquinas e execução em lote, demonstrando a viabilidade prática de simulações de defesa e fornecendo base conceitual para avaliação de cenários operacionais militares.

No contexto de simulação de múltiplos agentes, [14] desenvolveram uma plataforma de cossimulação acoplada ao *Ptolemy II* e ao *ArduPilot/SITL*, permitindo a avaliação realista de estratégias de voo autônomo com múltiplos drones. A ferramenta considera colisões, consumo energético, falhas de sensores e restrições aerodinâmicas, reforçando a importância da integração entre níveis de simulação física e lógica para modelagem de sistemas complexos.

Entre os trabalhos voltados à coordenação distribuída, [15] propõem uma abordagem baseada em *Particle Swarm Optimization* (PSO) para prolongar a longevidade de redes FANET (*Flying Ad Hoc Networks*) por meio da troca estratégica de posições entre drones. A proposta visa mitigar o consumo energético desigual entre os nós da rede, balanceando o esforço computacional e de comunicação de cada agente. Embora focado em aplicações civis de busca e resgate, seus conceitos de conservação energética e manutenção de cobertura são pertinentes para a sustentação de malhas defensivas em ambientes operacionais de longa duração.

Complementarmente, [16] apresentam um estudo de otimização de rotas para drones *gateways* em redes *Internet of Things* (IoT), utilizando heurísticas como programação linear e o Algoritmo da Colônia de Formigas (*Ant Colony Optimization* – ACO). Embora voltado ao contexto civil, o trabalho fornece bases metodológicas valiosas para problemas de roteamento e balanceamento de carga em ambientes com restrições energéticas, aplicáveis também em cenários de defesa descentralizada.

No plano ético e jurídico, [17] analisa as implicações da adoção de sistemas autônomos letais sob a ótica do Direito Internacional Humanitário (DIH). O autor destaca a ausência de regulamentações claras para robôs autônomos em combate, levantando preocupações quanto à responsabilização por danos e aderência aos princípios de distinção e proporcionalidade. Mesmo sistemas exclusivamente defensivos devem ser concebidos com restrições explícitas de controlabilidade e auditabilidade.

Em perspectiva estratégica, [18] discute o impacto das tecnologias disruptivas sobre o futuro das operações militares, projetando uma transformação doutrinária até 2050 baseada em inteligência artificial, robótica e redes inteligentes. O autor defende que a evolução do combate envolverá a integração de plataformas autônomas em ambientes complexos e altamente conectados.

Dessa forma, o presente trabalho se insere nesse panorama propondo uma arquitetura distribuída de defesa aérea baseada em UAS autônomos e algoritmos de planejamento clássico, enfatizando resiliência através da eliminação de pontos únicos de falha e escalabilidade via algoritmos distribuídos de coordenação.

III. Desenvolvimento Teórico

O paradigma do processamento distribuído oferece maior tolerância a falhas, escalabilidade e resistência a ataques comparado a sistemas centralizados, sendo adequado para defesa autônoma baseada em enxames de UAS [19, 20].

As FANETs caracterizam-se por alta mobilidade e topologias dinâmicas, exigindo mecanismos robustos como técnicas de *Store-and-Forward* e fusão de informações parciais para manter coordenação sob condições adversas de comunicação [21, 22].

O controle baseado em planejamento distribuído elimina pontos únicos de falha através de decisões locais baseadas em condições predefinidas (critérios de priorização, engajamento e coordenação), permitindo operação coordenada sem supervisão centralizada contínua [23, 24].

A arquitetura proposta integra esses elementos, utilizando algoritmos de coordenação descentralizada para múltiplos UAS autônomos operarem colaborativamente via protocolos *ad hoc* e decisões baseadas em percepção local compartilhada.

IV. Desenvolvimento Metodológico

Esta seção apresenta a metodologia experimental desenvolvida para validação da arquitetura distribuída proposta. O *framework* metodológico compreende o desenvolvimento do simulador *DroneSwarm2D*, a modelagem de informações parciais, os sistemas de detecção e comunicação, e as táticas experimentais definidas para análise comparativa. A abordagem visa estabelecer um ambiente controlado de teste que permita a avaliação quantitativa das estratégias de coordenação defensiva, considerando variáveis operacionais relevantes como taxa de perda de mensagens, falhas de sensores e diferentes proporções numéricas entre agentes defensivos e atacantes.

A. Arquitetura do Simulador

O simulador *DroneSwarm2D* [11] foi desenvolvido para investigar algoritmos distribuídos aplicados à defesa aérea baseada em enxames de drones autônomos, fornecendo uma plataforma experimental para análise comparativa de diferentes abordagens de coordenação defensiva.

A interface compreende duas áreas principais: a área de simulação, onde são exibidos drones ofensivos e defensivos, área de interesse e elementos complementares; e a área de visualização de estados, que apresenta a representação interna do drone defensivo selecionado, destacando as matrizes de recência e direção que registram a atualidade e orientação das detecções.

B. Modelagem de Informações Parciais

A principal inovação reside na modelagem de informações parciais, onde drones defensivos operam com dados obtidos por detecções locais e troca de informações com pares. A estrutura inclui:

- **Matriz de recência:** discretiza a área em grade com valores entre 0 e 1 representando atualidade das detecções;
- **Matriz de direção:** armazena vetores de movimento observados;
- **Posição própria:** referência espacial do drone para cálculos de trajetória.

A Área de Interesse é definida por círculos concêntricos com raio interno delimitando a região protegida e raio externo estabelecendo o limite de atuação defensiva. A Zona Desmilitarizada proíbe engajamento em regiões sensíveis, simulando áreas civis que devem ser evitadas durante confrontos militares. A Fig. 2 ilustra a dinâmica operacional do simulador, demonstrando a interação entre todos esses elementos em um cenário de defesa ativa.

C. Sistemas de Detecção e Comunicação

O sistema opera em dois modos de detecção complementares:

- **Detecção direta:** obtém posição exata dentro do alcance;
- **Detecção por triangulação:** utiliza direção angular compartilhada entre múltiplos drones.

Quando múltiplas linhas de visada se cruzam, a posição do inimigo é triangulada se o número de cruzamentos excede o limiar predefinido. A comunicação utiliza redes *ad hoc* descentralizadas, onde cada drone compartilha periodicamente informações de percepção com vizinhos dentro do raio de comunicação. O processo de fusão substitui dados obsoletos por informações mais recentes, incorporando decaimento exponencial para manter relevância dinâmica.

D. Comportamento dos Agentes

Drones inimigos executam diferentes padrões de aproximação incluindo movimentos diretos, zigzag, espirais, *bounce* e oscilatórios. Ao detectar drones defensivos, adotam comportamento dual baseado no parâmetro de agressividade e distância ao ponto de interesse, oscilando entre ataque direto e evasão temporária.

O mecanismo de interceptação determina trajetórias ideais considerando posição atual e velocidade do alvo. Se não há solução temporal válida, o drone move-se diretamente ao alvo; caso contrário, calcula o ponto de interseção estimado para interceptação antecipada.

Drones não envolvidos em perseguição utilizam estratégia de *holding*, avaliando ameaças em ordem crescente de distância e identificando alvos com proa agressiva. Verificam distância até a trajetória esperada ou ponto de interesse, posicionando-se estrategicamente para interceptação quando abaixo do limiar estabelecido.

Os drones operam através de máquina de estados finitos com transições dinâmicas baseadas em detecções e informações da rede, incluindo estados de perseguição ativa, retorno ao ponto de interesse, espera por detecções, comunicação insuficiente, movimento para interceptação e posicionamento para engajamento.

E. Modelo de Engajamento

O engajamento ocorre quando a distância entre drones torna-se inferior a um raio predefinido, resultando em três possíveis desfechos: neutralização mútua (30%), sucesso defensivo (50%) ou falha defensiva (20%). O sistema incorpora resiliência contra propagação de informações errôneas através de verificação de compatibilidade na área de interseção entre drones vizinhos, garantindo que apenas dados consistentes sejam incorporados ao estado global da rede.

F. Táticas Experimentais Propostas

Para análise comparativa das abordagens de coordenação defensiva, foram definidas duas táticas principais:

- **Tática Centralizada:** sistema com controle centralizado onde um elemento central coordena todas as ações dos drones defensivos, mantendo comunicação direta com cada agente e tomando decisões táticas baseadas em informações consolidadas (vídeo demonstrativo [25]);
- **Tática Distribuída:** arquitetura descentralizada onde cada drone opera autonomamente através de algoritmos de coordenação local, utilizando comunicação *ad hoc* para compartilhamento de informações parciais e tomada de decisões distribuída sem dependência de comando central (vídeo demonstrativo [26]).

G. Metodologia Experimental

Para validar a eficácia das estratégias propostas, foram realizados experimentos padronizados com 200 amostras por cenário/tática. A métrica principal avaliada foi a **Saúde da Área de Interesse** (porcentagem de saúde remanescente da área de interesse), que quantifica o sucesso defensivo do sistema através da preservação da integridade da região protegida.

Foram analisados três cenários operacionais distintos, variando a razão numérica entre drones defensivos (amigos) e atacantes (inimigos):

- **Cenário de Desvantagem Numérica (0,7:1):** 28 drones defensivos contra 40 atacantes;

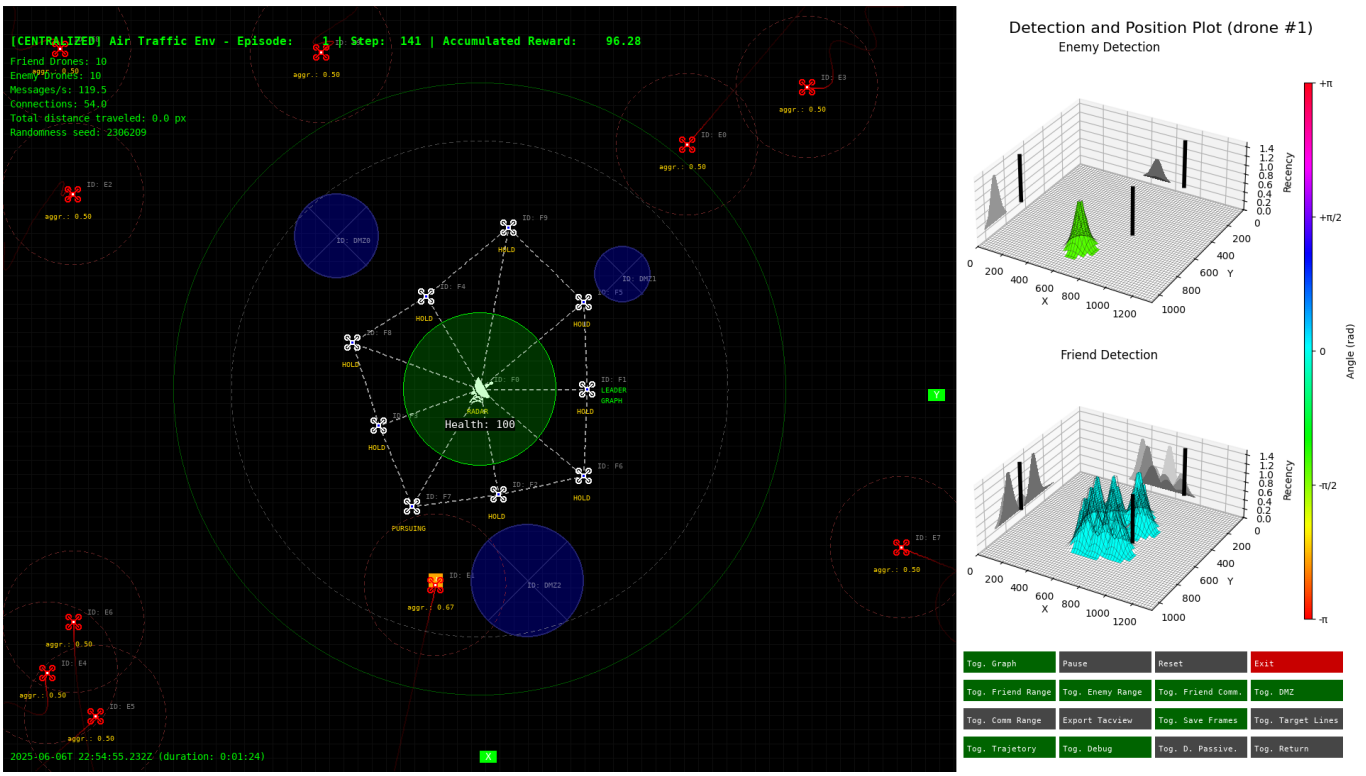

Fig. 2: Captura de tela de uma simulação, ilustrando a dinâmica de proteção do ponto de interesse (círculo verde central) por drones defensivos (em branco) e a aproximação de drones inimigos (em vermelho), evidenciando as interações de detecção e perseguição.

- **Cenário de Paridade Numérica (1:1):** 40 drones defensivos contra 40 atacantes;
- **Cenário de Vantagem Numérica (1:0,7):** 40 drones defensivos contra 28 atacantes.

Todos os cenários foram submetidos, par a par, a **testes *bootstrap* [27] não paramétricos** com 10.000 iterações, os quais confirmaram a significância estatística das diferenças observadas (valor-$p < 0,05$, onde p representa a probabilidade de se observar um resultado tão extremo sob a hipótese nula). Os testes rejeitaram consistentemente a hipótese nula ($H_0 : \mu_1 = \mu_2$, sendo μ_1 e μ_2 as médias das distribuições comparadas), indicando que as melhorias de desempenho não são atribuíveis a variações aleatórias.

V. Resultados e Discussões

Esta seção apresenta a análise quantitativa do desempenho dos algoritmos propostos, comparando a eficácia da arquitetura distribuída desenvolvida com abordagens centralizadas tradicionais.

A. *Apresentação dos Resultados*

Os resultados demonstram superioridade consistente da arquitetura distribuída proposta em relação aos sistemas centralizados tradicionais. A Fig. 3 apresenta a comparação das distribuições de saúde da área de interesse para todos os cenários testados, enquanto a Tabela I sumariza os valores médios de preservação e respectivos desvios padrão para cada cenário e tática avaliados.

B. *Interpretação dos Resultados*

A análise revela que a arquitetura distribuída apresenta:

- **Melhoria de 18,0%** na capacidade defensiva em cenário de desvantagem numérica;
- **Melhoria de 11,0%** em cenário de paridade numérica;
- **Melhoria de 5,1%** em cenário de vantagem numérica.

A arquitetura distribuída demonstra maior **robustez operacional**, especialmente em cenários de desvantagem numérica. No cenário 0,7:1, onde o sistema defensivo opera com 30% menos drones, a proposta distribuída mantém alta eficácia defensiva, enquanto o sistema centralizado sofre degradação significativa de performance.

C. *Validação das Hipóteses*

Os resultados experimentais forneceram evidências que corroboram as hipóteses iniciais. A análise estatística demonstrou superioridade consistente da proposta distribuída em todos os cenários testados, com melhorias médias variando de 5,1% a 18,0% na preservação da área de interesse. A robustez da arquitetura destacou-se especialmente em cenários de desvantagem numérica (0,7:1), nos quais a abordagem distribuída manteve 88,5% de preservação, em contraste com os 70,5% da abordagem centralizada — evidenciando sua capacidade de compensar inferioridade quantitativa por meio de uma coordenação tática mais eficiente.

VI. Conclusão

Este trabalho apresentou o desenvolvimento e validação de uma arquitetura de defesa aérea distribuída baseada

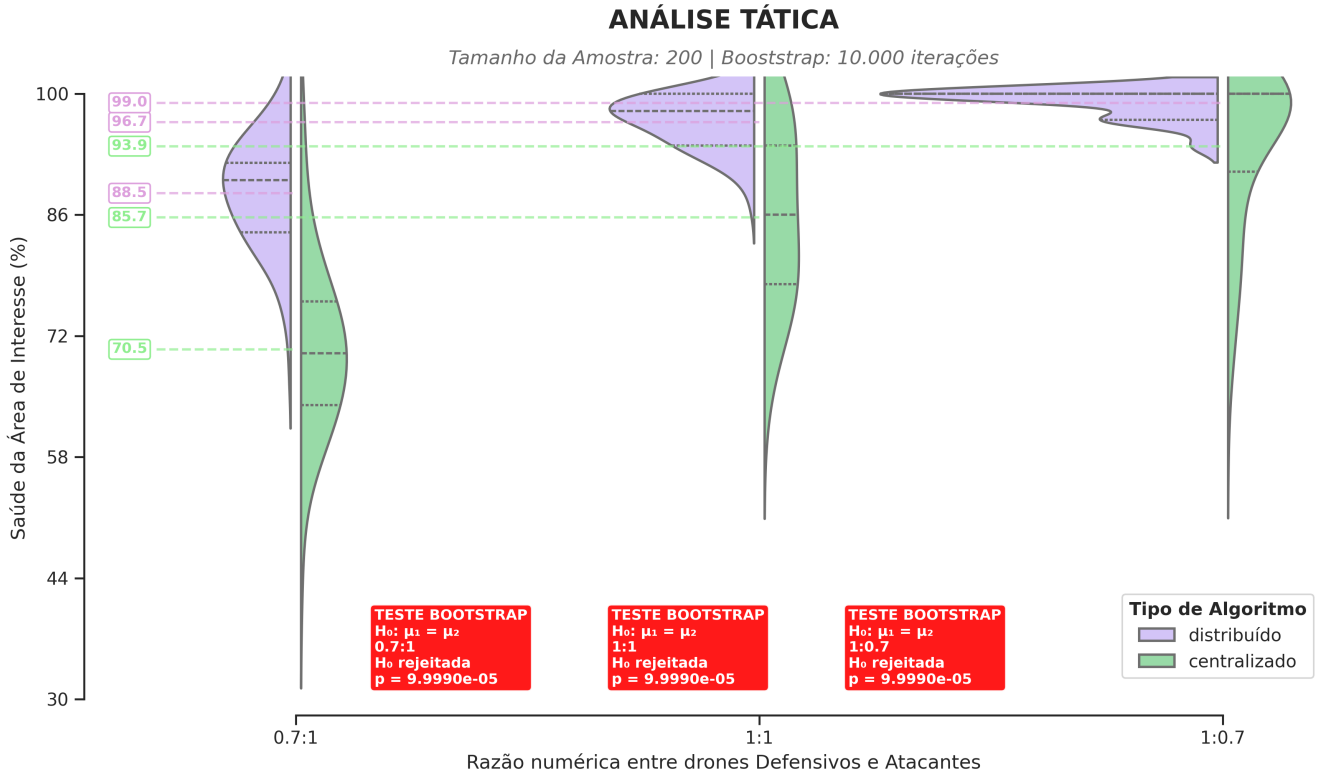

Fig. 3: Análise comparativa de estratégias defensivas mostrando distribuições de saúde da área de interesse para diferentes razões quantitativas entre drones defensivos e atacantes.

TABELA I: VALORES MÉDIOS DE PRESERVAÇÃO POR CENÁRIO E TÁTICA

Cenário	Tática	Média (%)	Desvio Padrão (%)
0,7:1	Distribuída	88,50	6,02
	Centralizada	70,45	9,67
1:1	Distribuída	96,71	2,96
	Centralizada	85,69	10,03
1:0,7	Distribuída	98,95	1,75
	Centralizada	93,94	9,07

em enxames de drones autônomos, constituindo uma alternativa resiliente e escalável aos sistemas centralizados tradicionais. As principais contribuições incluem: (i) uma solução completamente distribuída que elimina pontos únicos de falha; (ii) o simulador *DroneSwarm2D* para validação experimental; e (iii) algoritmos específicos de coordenação descentralizada com mecanismos de perseguição preditiva e estratégias de *holding* posicional.

A. Implicações e Limitações

Os resultados sugerem viabilidade prática da implementação em cenários reais, oferecendo melhor relação custo-benefício e flexibilidade doutrinária comparada a sistemas centralizados. No entanto, o estudo limitou-se a ambiente bidimensional simulado, não contemplando complexidades tridimensionais, interferências eletromagnéticas ou aspectos de segurança criptográfica.

B. Trabalhos Futuros

As direções prioritárias para pesquisas futuras incluem: (i) integração com técnicas de *Deep Reinforcement Learning* para adaptação automática dos algoritmos; (ii) expansão tridimensional do simulador considerando dinâmicas complexas; (iii) integração com protocolos de comunicação militares e medidas de segurança cibernética; e (iv) validação experimental em ambiente físico com UAS reais;

C. Considerações Finais

Este trabalho corrobora para um novo paradigma de defesa aérea distribuída, demonstrando que arquiteturas descentralizadas podem superar limitações de sistemas tradicionais centralizados. A crescente sofisticação das ameaças aéreas assimétricas demanda soluções defensivas adaptáveis e resilientes. Os resultados apresentados indicam que algoritmos distribuídos para coordenação de enxames defensivos representam uma direção promissora, com potencial para revolucionar a defesa de pontos críticos através de proteção eficaz, econômica e escalável contra ameaças aéreas modernas.

Apêndice

Artefatos: Os dados obtidos das simulações realizadas neste trabalho, bem como o código-fonte das análises e imagens geradas, encontram-se disponíveis no repositório: `https://anonymous.4open.science/r/sige_public_DroneSwarm2D-7C55`

Referências

[1] A. Calcara, A. Gilli, M. Gilli, R. Marchetti, and I. Zaccagnini, "Why drones have not revolutionized war: The enduring hider-finder competition in air warfare," *International Security*, vol. 46, no. 4,

pp. 130–171, 2022. [Online]. Available: https://direct.mit.edu/isec/article/46/4/130/111172/Why-Drones-Have-Not-Revolutionized-War-The

[2] S. A. H. Shah, K. Khursheed *et al.*, "Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109–137, 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11370-022-00452-4

[3] D. Barreiros, "Projeções sobre o futuro da guerra: Tecnologias disruptivas e mudanças paradigmáticas (2020–2060)," Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, Texto para Discussão 025, novembro 2019, iE-UFRJ Discussion Paper.

[4] Australian Army, "Swarm: UAS Swarming Technology and 'Future Ready' for the 20th Regiment," The Cove – Australian Army, Canberra, Australia, Tech. Rep., December 2021. [Online]. Available: https://cove.army.gov.au/article/swarm-uas-swarming-technology-and-future-ready-20th-regiment

[5] B. M. Figueiredo, "The Use of Uncrewed Aerial Systems by Non-State Armed Groups: Exploring Trends in Africa," United Nations Institute for Disarmament Research (UNIDIR), Geneva, Tech. Rep., 2024, uNIDIR Report. [Online]. Available: https://unidir.org/publication/the-use-of-uncrewed-aerial-systems-by-non-state-armed-groups-exploring-trends-in-africa

[6] J. Gong, J. Yan, D. Kong, and D. Li, "Introduction to drone detection radar with emphasis on automatic target recognition," *IEEE Transactions on Aerospace and Electronic Systems*, 2023.

[7] Botasot. (2024) "I was very afraid": the hunting of Russian drones against civilians in Ukraine, evidence from the field. [Online]. Available: https://botasot.co/kisha-shume-frike-gjuetia-e-droneve-ruse-ndaj-civileve-ne-ukraine-deshmi-nga-terreni/

[8] National Research Council, *Realizing the Potential of C4I: Fundamental Challenges*. Washington, DC: The National Academies Press, 1999. [Online]. Available: https://nap.nationalacademies.org/read/6457/chapter/3

[9] International Organization for Standardization, *Information processing systems — Open Systems Interconnection — Basic Reference Model*, International Organization for Standardization Std. ISO/IEC 7498-1:1994, 1994. [Online]. Available: https://www.iso.org/standard/20269.html

[10] M. Conti and S. Giordano, "A survey on mobile ad hoc networks," *Computer Communications*, vol. 27, no. 5, pp. 127–150, 2003.

[11] L. S. Lima, R. D. Rocha, R. H. Giannico, D. D. C. Brito, and J. P. D. A. Dantas, "Proposta de algoritmo distribuído para enxame de drones defensivos de pequeno porte baseado em planejamento," http://dx.doi.org/10.13140/RG.2.2.32495.96161, 2025, preprint, disponível no ResearchGate.

[12] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.

[13] J. P. A. Dantas, A. N. Costa, V. C. F. Gomes, A. R. Kuroswiski, F. L. L. Medeiros, and D. Geraldo, "ASA: A Simulation Environment for Evaluating Military Operational Scenarios," in *Proceedings of the 20th International Conference on Scientific Computing (CSC'22)*. Las Vegas, NV, USA: American Council on Science and Education, July 25–28 2022. [Online]. Available: https://arxiv.org/abs/2207.12084

[14] L. B. Silva, "Plataforma de cossimulação para sistemas autônomos com múltiplos drones," Ph.D. dissertation, Universidade Federal do Ceará, 2019.

[15] Catarro, T. et al., "Energy-aware pso-based topology control in fanets," *Ad Hoc Networks*, 2024, in press.

[16] K. R. Rodrigues, W. E. Speranzini, and I. S. Florentino, "Roteamento otimizado para uav gateways em redes IoT com energia limitada," in *Anais do X Workshop de Computação Aplicada à Gestão do Meio Ambiente e Recursos Naturais*. Belém, PA: Sociedade Brasileira de Computação (SBC), 2019.

[17] A. Cabral, *Robôs Autônomos e o Direito Internacional Humanitário*. São Paulo: Quartier Latin, 2020.

[18] G. Barreiros, "A nona fronteira: guerra, robôs e energia em 2050," *Revista da Escola de Guerra Naval*, vol. 25, no. 1, 2019.

[19] A. S. Tanenbaum and M. van Steen, *Distributed Systems: Principles and Paradigms*, 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2007.

[20] N. A. Lynch, *Distributed Algorithms*, 1st ed. Morgan Kaufmann, 1996. [Online]. Available: https://www.elsevier.com/books/distributed-algorithms/lynch/978-1-55860-348-6

[21] I. Bekmezci, O. K. Sahingoz, and Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, 2013.

[22] A. Chriki, H. Touati, H. Snoussi, and F. Kamoun, "FANET: Communication, mobility models and security issues," *Computer Networks*, vol. 163, p. 106877, 2019.

[23] M. Ghallab, D. Nau, and P. Traverso, *Automated Planning: Theory and Practice*. San Francisco, CA: Morgan Kaufmann, 2004.

[24] P. Stone and M. Veloso, "Multiagent systems: A survey from a machine learning perspective," *Autonomous Robots*, vol. 8, no. 3, pp. 345–383, 2000.

[25] L. S. Lima, "Exemplo de cenário: Tática centralizada [Atacantes desorganizados]," YouTube, [S.l.], jun 2025. [Online]. Available: https://youtu.be/L_cXyGGKOyA

[26] ——, "Exemplo de cenário: Tática distribuída [Atacantes desorganizados]," YouTube, [S.l.], jun 2025. [Online]. Available: https://youtu.be/FOD6VzWxXQU

[27] B. Efron and R. J. Tibshirani, *An Introduction to the Bootstrap*, ser. Chapman & Hall/CRC Monographs on Statistics and Applied Probability. New York: Chapman and Hall/CRC, 1994.