DroneSwarm2D: Um Simulador de Enxame de Drones Autônomos para o Estudo de Táticas Defensivas Distribuídas

Lucas Silva Lima[1], Rafael Duarte Rocha[1], Rafael Hoffmann Giannico[1], Denys Derlian Carvalho Brito[1], João Paulo De Andrade Dantas[1]
[1]Instituto Tecnológico de Aeronáutica, São José dos Campos/SP

***Resumo*— A crescente acessibilidade a drones de baixo custo, frequentemente de produção simplificada, vem transformando significativamente o cenário dos conflitos modernos, ao serem empregados como armamentos em operações assimétricas e ataques improvisados. Essa nova realidade impõe desafios às defesas convencionais e demanda soluções que sejam, além de eficazes, economicamente viáveis e sustentáveis do ponto de vista logístico. Neste contexto, o simulador 2D para drones autônomos configura-se como uma ferramenta útil de experimentação, permitindo o estudo detalhado dos comportamentos colaborativos e adversariais em enxames de drones. O sistema atualiza continuamente a percepção do ambiente por meio do registro dinâmico de mudanças e direções das detecções. A comunicação entre os drones ocorre de forma direta e colaborativa, sem depender de um comando central, o que confere ao sistema maior resiliência, escalabilidade e flexibilidade operacional. Ao longo deste trabalho, serão discutidos os desafios inerentes à implementação de soluções distribuídas, os ganhos operacionais decorrentes da eliminação de pontos únicos de falha e os benefícios logísticos de estratégias que possibilitem uma resposta mais dinâmica e sustentável. A análise busca demonstrar que a adoção de abordagens distribuídas é uma alternativa promissora para o futuro dos sistemas autônomos de vigilância e proteção, oferecendo respostas proporcionais e economicamente viáveis frente às ameaças emergentes.**

***Palavras-Chave*— Drones autônomos, Simulação de Defesa, Computação Distribuída, Rede *ad hoc*.**

I. INTRODUÇÃO

O uso crescente de drones de baixo custo, frequentemente construídos com materiais acessíveis, tem transformado os cenários de conflito modernos, ampliando a assimetria entre capacidades ofensivas e defensivas (Zegart 2020). Estudos recentes indicam que, enquanto os drones empregados em operações de ataque podem ser fabricados com investimentos relativamente baixos, utilizando tecnologias improvisadas e adaptações criativas (Karner 2024), os sistemas de defesa tradicionais, tais como interceptadores, caças de alta tecnologia e radares avançados, demandam investimentos substanciais e, frequentemente, não conseguem acompanhar a frequência e o volume dos ataques em enxame (Myre 2024).

De modo a exemplificar as potenciais aplicações, a Fig. 1 apresenta um drone quadricóptero modificado para fins ofensivos, evidenciando a capacidade de adaptação dessas aeronaves. Tais modificações podem incluir a incorporação de explosivos, sistemas de mira aprimorados e algoritmos de navegação autônoma, tornando esses dispositivos acessíveis e altamente eficazes em operações assimétricas (Botasot 2024). Esse tipo de adaptação demonstra como tecnologias originalmente desenvolvidas para uso civil podem ser convertidas em armamentos de baixo custo, contrapondo as defesas convencionais.

Fig. 1: Exemplo de drone quadricóptero adaptado para uso ofensivo. (Ventura 2024)

Nesse contexto, observa-se, ainda, a incorporação de recursos de inteligência artificial, que ampliam a precisão e a efetividade das aeronaves, especialmente em missões de vigilância e ataque (Lendon et al. 2024). Um exemplo de adaptação criativa inclui o desenvolvimento de drones de papelão, como os projetados na Austrália, explicitados na Fig. 2, cujo baixo custo de produção contrasta com sua capacidade de realizar missões em profundidade (Whittaker 2023). Ao mesmo tempo, a produção caseira de drones – por meio de componentes comerciais ou mesmo materiais não convencionais – tem possibilitado uma resposta ágil a demandas específicas do campo de batalha (A Referência 2022).

Em paralelo, análises demonstram que a utilização de drones improvisados – seja por meio dos "drones kamikazes", que utilizam explosivos acoplados e apresentam um custo de substituição relativamente baixo, ou dos sistemas de ataque caseiros – pode proporcionar vantagens táticas significativas, ampliando o alcance das operações ofensivas e forçando o adversário a repensar suas estratégias defensivas (Lendon et al. 2024). Além disso, iniciativas de engenharia adaptativa, como a construção de drones por entusiastas na Ucrânia e o uso de modelos artesanais, evidenciam a capacidade de adaptação em cenários com recursos limitados (A Referência 2022; Whittaker 2023). Relatos de diferentes regiões, inclusive de grupos irregulares, como os dissidentes das Forças Armadas Revolucioná-

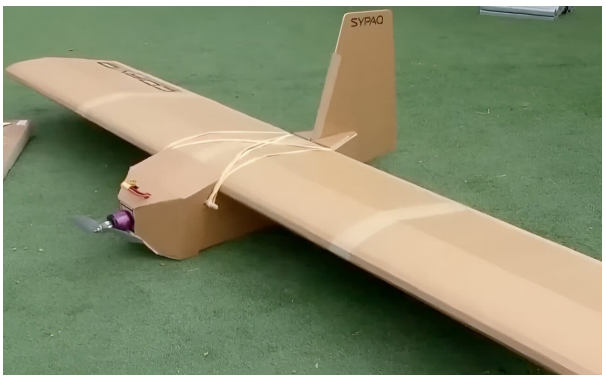


Fig. 2: Exemplo de aeronave produzida em papelão. (Botasot 2024)

rias da Colômbia (FARC) na Colômbia, evidenciam que a adoção de tecnologias semelhantes transcende barreiras geopolíticas (SWI swissinfo.ch 2024).

A análise dos casos apresentados evidencia uma transição significativa no emprego das tecnologias de drones: passa-se do uso isolado e centralizado para a operação em enxames, onde a distribuição dos agentes e a ausência de uma infraestrutura fixa impõem novos desafios operacionais e estratégicos. Essa mudança de paradigma ressalta a importância de integrar as vantagens operacionais dos enxames com sistemas que possam funcionar de forma distribuída, possibilitando maior flexibilidade e adaptabilidade no campo de batalha.

Diante desse contexto, como concepção a enfrentar os desafios supramencionados, este trabalho propõe um sistema de defesa baseado em enxames de drones autônomos, que operam de forma distribuída em redes *ad hoc*, eliminando a dependência de uma infraestrutura fixa e centralizada. Essa abordagem elimina a dependência de um comando central, permitindo que cada agente se comunique e se adapte dinamicamente às condições do ambiente, mantendo uma visão integrada mesmo a partir de informações parciais (Padilha 2024). O simulador *DroneSwarm2D* desenvolvido neste estudo configura-se como uma ferramenta para investigar os comportamentos colaborativos e adversariais em enxames, contribuindo para o avanço das estratégias de defesa aérea em cenários de conflito moderno (Stepanenko 2023).

Isto posto, este trabalho está estruturado da seguinte forma: na Seção II, abordam-se os fundamentos teóricos da modelagem, controle e simulação de enxames de drones, destacando redes *ad hoc*, algoritmos distribuídos e técnicas de atualização de informações. Na Seção III, discutem-se os trabalhos correlacionados, os quais posicionam a proposta no contexto das pesquisas recentes sobre táticas defensivas e o uso de drones em conflitos assimétricos. Na Seção IV, descreve-se a metodologia de implementação do simulador *DroneSwarm2D*, com atenção à sua interface e aos conceitos de informação parcial que fundamentam a coordenação dos drones. Na Seção V, é apresentado um exemplo de cenário possível. Na Seção VI, expõe-se a visão dos autores acerca das potencialidades do simulador, bem como sugestões para futuras investigações. Por fim, na Seção VII são detalhadas as contribuições de cada autor.

II. Revisão Teórica

Esta seção apresenta os fundamentos teóricos essenciais para a modelagem, o controle e a simulação de enxames de drones autônomos. Em especial, discutem-se os desafios associados à comunicação distribuída, à coordenação autônoma e às estratégias de defesa aérea baseadas em drones. O entendimento desses conceitos é fundamental para o desenvolvimento do simulador *DroneSwarm2D*, que visa investigar a eficácia de táticas defensivas baseadas em redes *ad hoc* e algoritmos distribuídos.

A. Redes Ad Hoc e Flying Ad Hoc Networks (FANETs)

Redes *ad hoc* são caracterizadas pela formação dinâmica e descentralizada de conexões entre nós, dispensando uma infraestrutura fixa (Ramanathan e Redi 2002). No contexto dos drones, as *Flying Ad Hoc Networks* (FANETs) são o canal para a comunicação entre drones, permitindo o compartilhamento de informações em tempo real, mesmo em ambientes com alta mobilidade (Bekmezci, Sahingoz e Temel 2013). Tais redes oferecem a base para a implementação de estratégias de coordenação e defesa, possibilitando que cada agente contribua com dados locais limitados para uma visão global do ambiente (Kundu et al. 2024). Essa abordagem descentralizada é essencial para a resiliência e a escalabilidade dos sistemas autônomos de vigilância.

B. Algoritmos Distribuídos e Controle Colaborativo

A robustez dos sistemas autônomos depende, em grande parte, da capacidade dos agentes de tomar decisões de forma distribuída. Modelos de controle colaborativo aplicam algoritmos distribuídos onde cada drone processa suas informações locais e as integra por meio de comunicação direta com seus vizinhos (Rimawi et al. 2024). Essa estratégia elimina o ponto único de falha e permite a formação de uma visão compartilhada do ambiente.

a) Exemplo de Algoritmo Distribuído - Eleição de Líder entre Agentes (Vasudevan et al. 2003): Considere um grupo de agentes, cada um com um identificador único (ID). O objetivo é eleger um líder entre os agentes, seguindo o critério clássico: o agente com o maior ID disponível deve assumir a liderança.

Implementação Centralizada

1) **Coleta de Dados:** Cada agente envia seu ID e status (disponível ou não) para um nó central.
2) **Processamento Central:** O nó central recebe todas as informações, analisa os IDs e seleciona aquele com o maior valor dentre os agentes disponíveis.
3) **Anúncio do Líder:** O nó central comunica a decisão a todos os agentes.

A figura 3 ilustra a dinâmica típica de troca de mensagens nesse tipo de solução.

Características da Abordagem Centralizada:

- **Simplicidade:** A lógica de decisão está concentrada em um único ponto.
- **Ponto Único de Falha:** Se o nó central falhar, todo o processo de eleição é comprometido.
- **Comunicação Centralizada:** Todos os agentes dependem de um único canal para enviar suas informações.

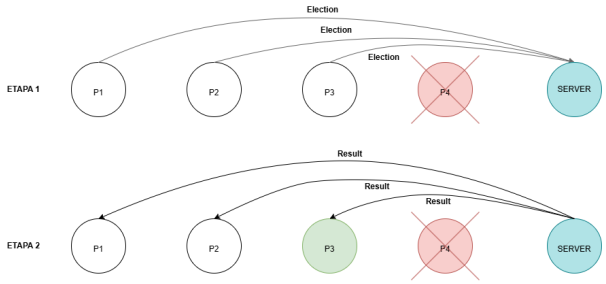


Fig. 3: Diagrama com exemplo de eleição segundo algoritmo centralizado. O agente 4, até então lider, falha. Os demais agentes, percebendo sua falha, convocam eleição ao nó central.

Implementação Distribuída (Algoritmo Bully)

Em sistemas distribuídos aplicados a enxames de drones, a coordenação é fundamental para garantir respostas eficientes a ameaças. Métodos de eleição de líder, como o algoritmo *Bully*, permitem que um drone assuma um papel de comando temporário quando necessário (Vasudevan et al. 2003). No entanto, para cenários de alta mobilidade, abordagens descentralizadas baseadas em consenso são mais robustas, evitando pontos únicos de falha. Alternativas como algoritmos de consenso distribuído, incluindo o *Consensus-Based Bundle Algorithm* (CBBA), têm sido investigadas para permitir uma tomada de decisão colaborativa em tempo real (Choi, Brunet e How 2009).

Assim sendo, nesta abordagem, cada agente é capaz de iniciar o processo de eleição sem depender de um nó central. O algoritmo *Bully* é um exemplo clássico (Lianjiong 2004):

1) **Detecção de Falha:** Quando um agente percebe que o líder atual não responde, ele inicia uma eleição.
2) **Envio de Mensagens de Eleição:** O agente que inicia o processo envia uma mensagem a todos os agentes com IDs maiores, solicitando confirmação de que estão ativos.
3) **Resposta dos Agentes:** Se algum agente com ID maior estiver ativo, ele responde e assume a responsabilidade de conduzir a eleição.
4) **Decisão:** Se o agente que iniciou a eleição não receber nenhuma resposta de agentes com IDs superiores, ele se declara líder e notifica todos os demais.

A figura 4 ilustra a dinâmica típica de troca de mensagens nesse tipo de solução.

Características da Abordagem Distribuída:

- **Autonomia Local:** Cada agente toma decisões com base em sua própria visão e na comunicação com seus pares.
- **Resiliência:** A ausência ou falha de um agente não compromete a eleição, pois os demais continuam o processo.
- **Complexidade de Coordenação:** A comunicação entre os agentes e o uso de algoritmos de consenso aumentam a complexidade da implementação.

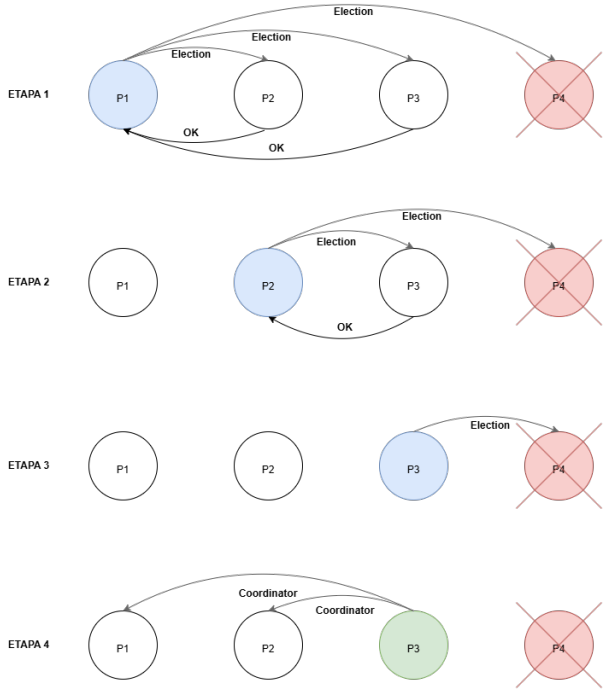


Fig. 4: Diagrama com exemplo de eleição segundo algoritmo descentralizado. O agente 4, até então lider, falha. O agente 1 é o primeiro a perceber a falha do lider e dá início à eleição.

Comparação Resumida

- **Centralizado:** Simples e fácil de controlar, porém vulnerável a falhas no ponto único.
- **Distribuído:** Mais robusto e escalável, eliminando o ponto único de falha, mas exigindo maior complexidade na comunicação e coordenação.

Este exemplo evidencia, de forma prática, as diferenças conceituais entre uma abordagem centralizada e uma distribuída para a eleição de um líder em um grupo de agentes. Enquanto a implementação centralizada depende de um único ponto de controle, a abordagem distribuída promove a autonomia dos agentes e a resiliência do sistema, aspectos fundamentais para a robustez e a confiabilidade em sistemas autônomos.

C. Mecanismos de Interceptação e Estratégias de Holding

A interceptação eficiente de alvos por drones defensivos pode ser modelada por equações de perseguição, como a trajetória de Dubins para minimização de curvas em cenários com restrição de raio de giro (Dubins 1957). Além disso, o uso de Guiamento Proporcional (PN – Proportional Navigation) permite que os drones ajustem dinamicamente suas trajetórias com base na variação angular do alvo (Guelman 1971).

Pensando-se em aplicações de defesa e vigilância, torna-se necessária a definição de estratégias que permitam aos drones interceptar alvos ou se manter em vigilância em posições estratégicas. Modelos matemáticos para a interceptação consideram a posição, a velocidade e a direção dos agentes, utilizando equações quadráticas para estimar o tempo de interceptação ideal. De forma complementar, estratégias de espera (*holding*) são empregadas

para manter os drones em posições defensivas estratégicas até que uma ameaça seja detectada, utilizando cálculos de projeção e definição de pontos de interesse.

D. Protocolos de Comunicação e Disseminação de Informação

A comunicação eficiente entre drones autônomos depende da escolha de protocolos que minimizem a sobrecarga de rede sem comprometer a confiabilidade dos dados. Estratégias baseadas em protocolos de disseminação, como *Gossip Protocols*, permitem que a informação seja distribuída de maneira eficiente, mesmo em condições adversas (Jelasity, Montresor e Babaoglu 2005). Além disso, técnicas de atualização baseadas em tempo (*Time-Stamped Updates*) evitam que drones tomem decisões baseadas em informações obsoletas, garantindo respostas adaptativas e coordenadas (Hassija, Saxena e Chamola 2020).

Nesse sentido, a eficácia dos algoritmos de controle está intrinsecamente ligada à capacidade de disseminar informações entre os drones. Os protocolos de comunicação são empregados para reduzir a sobrecarga de mensagens e garantir a entrega rápida e confiável dos dados, mesmo em cenários emergenciais. A integração desses protocolos com mecanismos de atualização contínua – que substituem dados antigos por dados mais recentes – é fundamental para manter uma visão integrada do ambiente, permitindo respostas coordenadas e adaptativas.

E. Integração dos Conceitos para Simulação de Enxames

A combinação dos fundamentos teóricos descritos anteriormente permite a construção de simuladores que reproduzem de forma realista o comportamento de enxames de drones. O simulador *DroneSwarm2D* se apoia na modelagem de redes FANET, na implementação de algoritmos distribuídos e no uso de modelos matemáticos para a otimização de trajetórias e estratégias de interceptação. Essa integração possibilita a avaliação de táticas defensivas distribuídas, oferecendo uma plataforma útil para o estudo de comportamentos colaborativos e a análise de desempenho em cenários de defesa.

Em síntese, os conceitos discutidos nesta seção fornecem a base para a modelagem e implementação do simulador *DroneSwarm2D*. A adoção de FANETs possibilita a comunicação autônoma entre drones, enquanto os algoritmos distribuídos garantem coordenação descentralizada e resiliência do sistema. Além disso, a modelagem de interceptação e os protocolos de comunicação otimizados permitem avaliar estratégias defensivas em tempo real. Essa integração de técnicas viabiliza a simulação realista de enxames de drones autônomos, permitindo a análise e otimização de táticas defensivas distribuídas.

III. Trabalhos Correlacionados

O estudo e a simulação de enxames de drones têm ganhado destaque na literatura, não apenas pelo emprego individual de drones, mas principalmente pela complexidade inerente à coordenação, comunicação e tomada de decisões em sistemas distribuídos. Diversas abordagens investigam desde algoritmos de otimização para a gestão de redes FANET até modelos de simulação que reproduzem o comportamento coletivo e as táticas de defesa distribuída.

A. Otimização Energética e Gerenciamento de Redes FANET

Em contextos onde a autonomia dos drones é crítica, pesquisas têm explorado estratégias para prolongar o tempo de operação das redes formadas por múltiplos drones. Por exemplo, Catarro, Pinto e Oliveira 2024 apresentam um algoritmo baseado em *Particle Swarm Optimization* (PSO) que promove a troca estratégica de posições entre os drones, de modo a equilibrar o consumo energético e aumentar a robustez da rede. Essa abordagem é especialmente relevante em simulações que avaliam o desempenho de enxames em ambientes dinâmicos.

B. Simulação de Comunicação e Coordenação em Enxames

A simulação de redes *ad hoc* e de FANETs é uma ferramenta fundamental para analisar a eficiência dos sistemas distribuídos. Estudos como o de Andrade Martins, Garren e Robertson 2022 investigam métodos para ranging e identificação em enxames, utilizando técnicas inspiradas no 5G (por exemplo, sequências Zadoff-Chu) que melhoram a precisão na determinação de distâncias e a sincronização entre os agentes. Tais avanços possibilitam a construção de modelos simulados onde os drones interagem de forma colaborativa, compartilhando informações locais e mantendo uma visão integrada do ambiente.

C. Aspectos Regulatórios e Implicações Éticas em Sistemas Autônomos

Embora o foco principal deste trabalho seja a simulação de comportamentos coletivos, é importante notar que o aumento da autonomia e a implementação de sistemas distribuídos levantam questões regulatórias e éticas. Trabalhos como o de Issmael Júnior 2024 e Aquino Cabral 2020 discutem os desafios da regulação do uso de drones autônomos e a transformação dos conflitos modernos por meio do emprego de robôs automatizados. Esses estudos oferecem um contraponto teórico que, embora não seja o foco da simulação propriamente dita, fornece o contexto para o desenvolvimento de táticas de defesa distribuída.

D. Aplicações em Segurança Pública e Monitoramento por Simulação

Além das aplicações militares, a simulação de enxames de drones tem sido explorada para estratégias de monitoramento e vigilância urbana. Santos Lima e Ribaski 2019 demonstram, por meio de estudos de caso, como o emprego de Aeronaves Remotamente Pilotadas (*Remotely Piloted Aircraft* - RPA) em simulações pode auxiliar no enfrentamento à criminalidade, ressaltando a importância de redes descentralizadas e a troca de informações em tempo real. Essas investigações reforçam a viabilidade de sistemas simulados que avaliam a comunicação direta e a coordenação entre agentes.

E. Modelos de Otimização de Trajetórias e Controle Distribuído

No âmbito da Internet das Coisas (IoT), a otimização de trajetórias dos drones é determinante para garantir a máxima cobertura e eficiência energética. Rodrigues et al. 2019 propõe modelos que combinam programação linear e algoritmos inspirados em colônias de formigas para otimizar as rotas dos drones que atuam como *gateways* de comunicação. Ademais, abordagens de controle distribuído e de auto-organização, como as apresentadas em Oliveira, Speranzini e Florentino 2021 e Santos Lima e Nayara Guetten Ribaski 2015, enfatizam a importância de mecanismos que permitam a coordenação autônoma dos enxames, eliminando pontos únicos de falha e aumentando a resiliência do sistema simulado.

F. Disseminação de Informações em Redes Simuladas

Por fim, a disseminação eficiente de informações é um tópico recorrente em simulações de redes de drones. Protocolos *geocast*, como o proposto em Bine et al. 2020, demonstram, em ambiente simulado, a capacidade de reduzir o número de transmissões e aumentar a taxa de entrega das mensagens em cenários emergenciais, o que é essencial para a coordenação de enxames em tempo real.

Em conjunto, essas abordagens demonstram que a simulação de enxames de drones é uma ferramenta poderosa para testar e aprimorar estratégias de defesa aérea distribuída. A diversidade de métodos – que vai desde a otimização energética e o controle de trajetórias até a coordenação autônoma e a disseminação de informações – fornece uma base robusta para o desenvolvimento de sistemas resilientes, escaláveis e economicamente viáveis.

IV. DroneSwarm2D: O Simulador

O simulador *DroneSwarm2D* para drones autônomos foi desenvolvido para fornecer uma plataforma experimental que permita a investigação dos mecanismos de defesa aérea baseados em táticas distribuídas contra enxame de drones. Inicialmente, o uso do simulador é destinado a analistas com expertise em programação, especialmente na linguagem *Python*, o que possibilita a customização e a extensão dos módulos existentes. A seguir, são apresentados os principais componentes e funcionalidades do simulador.

A. Interface de Visualização

A interface do simulador é composta por duas áreas inter-relacionadas:

1) **Área de Simulação:** Nesta área, são exibidos os drones ofensivos e defensivos, a área de interesse e eventuais elementos de solo que complementam a simulação. Os drones ofensivos, que emergem das bordas do ambiente, seguem trajetórias diversas (como movimentos diretos, zigzag ou espirais) em direção à área alvo. Em contrapartida, os drones defensivos são posicionados estrategicamente ao redor do ponto de interesse e baseiam suas ações na análise das informações parciais que eles obtem do ambiente.

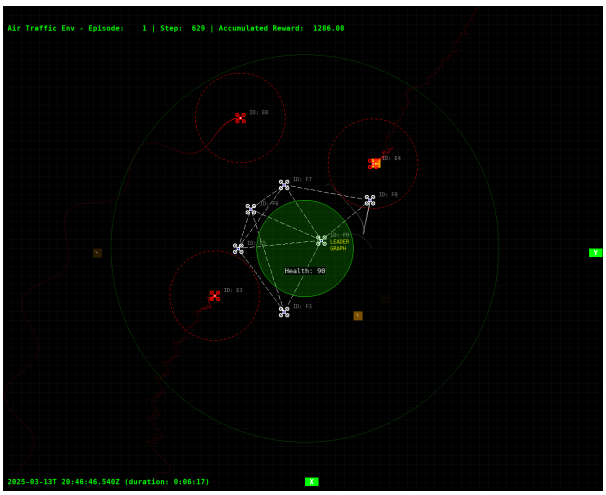


Fig. 5: Exemplo da área de simulação, demonstrando a interação entre drones ofensivos e defensivos, bem como a delimitação da área de interesse.
(Produção do Autor)

2) **Área de Visualização de Estados:** Esta seção apresenta a representação interna do estado do ambiente do drone defensivo que estiver selecionado (marcador *GRAPH*), destacando as matrizes de recência e de direção, que registram a atualidade e a orientação das detecções. Essa visualização permite que o analista compreenda como cada drone processa as informações do ambiente, contribuindo para a concepção de um algoritmo de defesa.

B. Conceitos de Informação Parcial

A principal inovação do simulador reside na modelagem de informações parciais. Os drones defensivos não dispõem de uma visão completa do ambiente, mas sim de dados obtidos por meio de suas detecções locais e da troca de informações com seus pares. Essa abordagem é estruturada em três componentes:

- **Matriz de Recência:** A área de simulação é discretizada em uma grade, onde cada célula armazena um valor entre 0 e 1, representando a atualidade da detecção naquela região. Valores próximos a 1 indicam detecções recentes, enquanto valores próximos a 0 refletem informações desatualizadas ou ausência de detecção quando o valor é exatamente nulo. Esta gradação permite que a representação do ambiente evolua de forma vitualmente contínua.
- **Matriz de Direção:** Discretização da área de simulação, onde cada célula da grade também contém um vetor de mesmo sentido que o observado na detecção naquela porção de área, permitindo que o drone estime a trajetória dos alvos.
- **Posição do Próprio Drone:** A posição do drone é constantemente monitorada e utilizada como referência para comparar e integrar as informações parciais captadas.

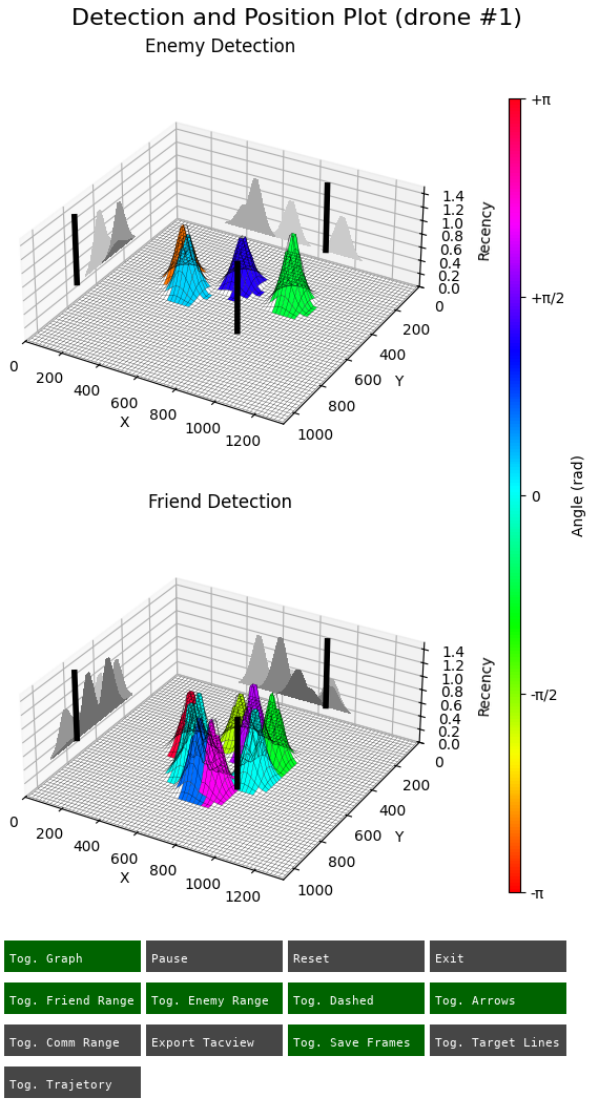


Fig. 6: Visualização do estado interno de um drone, evidenciando a matriz de recência e de direção bem como a posição atual.

C. Mecanismo de Comunicação e Compartilhamento de Informação

Cada drone defensivo mantém matrizes de detecção – tanto de recência quanto de direções – que são compartilhadas com drones vizinhos dentro do seu raio de comunicação R_c. A rotina responsável por comunicação realiza a junção (*merge*) dessas matrizes, de forma que informações mais recentes provenientes dos demais pares substituam dados desatualizados. Este procedimento permite que, mesmo na ausência temporária de um agente, os demais mantenham uma visão do ambiente, ainda que parcial.

Além da comunicação, o sistema implementa processos contínuos de atualização das matrizes de detecção, que utilizam um mecanismo de decaimento exponencial para tornar detecções passadas em dados obsoletos.

Em síntese, os mecanismos de comunicação e atualização asseguram que a rede de defesa opere de forma resiliente, mantendo a operacionalidade mesmo sob condições adversas, tal como bipartição de rede e eventuais falhas de comunicação, ainda que sequenciais.

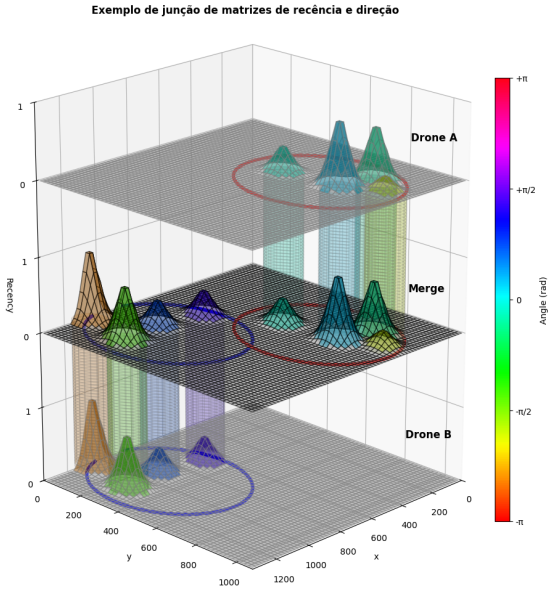


Fig. 7: Exemplo de junção da matriz de recência onde os drones, isoladamente, atingem um estado de conhecimento do ambiente além do raio de detecção graças a troca de informações pela rede.

Modelagem da Ameaça

No presente estudo, a modelagem da ameaça é realizada a partir do enxame dos drones inimigos e de seus comportamentos quando confrontados com a presença de drones defensivos.

a) Padrões de Aproximação: A Fig. 8 ilustra diferentes trajetórias executadas pelos drones inimigos, demonstrando a variedade de padrões disponíveis no sistema. Cada cor representa um comportamento distinto, como aproximação direta, manobras em ziguezague, espirais, aproximações com recuo (*bounce approach*) ou movimentos oscilatórios. Note que o ponto de interesse (destacado em azul ao centro) é o alvo comum de todos os drones.

b) Detecção de Drones Amigos e Agressividade: Quando um drone inimigo detecta a presença de um drone amigo dentro de seu alcance de detecção, ele adota um comportamento dual que oscila entre a continuidade de sua aproximação ao ponto de interesse e a evasão temporária para minimizar o risco de neutralização. Este comportamento é determinado através de uma avaliação probabilística baseada em um parâmetro de agressividade, o qual modula a decisão de atacar ou recuar.

Seja d a distância entre o drone inimigo e o ponto de interesse, e R o raio externo que delimita a área de atuação dos drones defensivos. O parâmetro de agressividade, denotado por α, quantifica a predisposição inicial do drone inimigo para realizar um ataque direto. A probabilidade de ataque, p_{attack}, é calculada por (1):

$$p_{\text{attack}} = \max\left(1 - \frac{d}{2R}, \alpha\right), \tag{1}$$

onde:

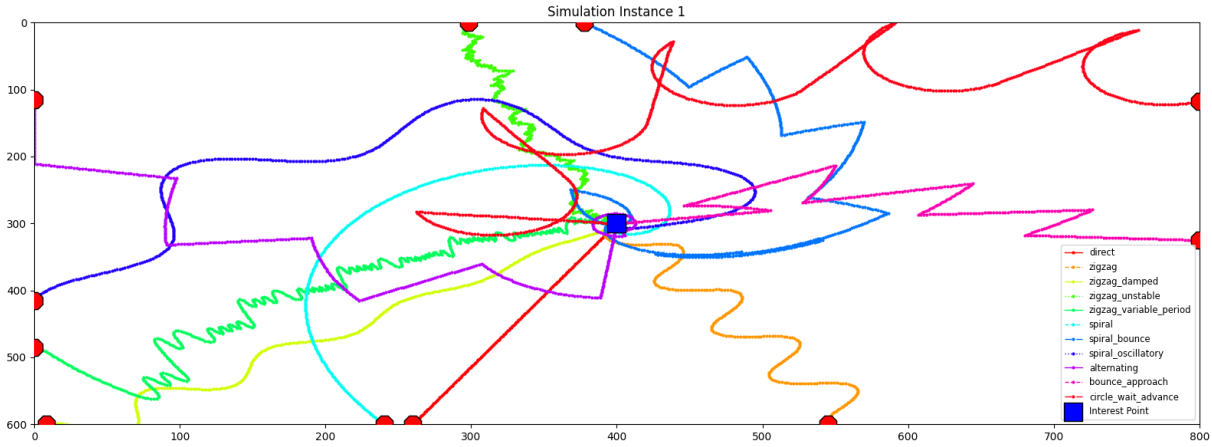


Fig. 8: Exemplo de trajetórias de drones inimigos, cada um exibindo um padrão de aproximação distinto em direção ao ponto de interesse (em azul).

- d representa a distância atual do drone inimigo até o ponto de interesse;
- R é o raio externo de atuação dos drones amigos;
- α é o parâmetro de agressividade inicial, normalmente configurado com um valor entre 0 e 1.

Ao detectar um drone defensivo, o drone ofensivo gera um número aleatório r, uniformemente distribuído em $[0, 1]$. Se $r < p_{\text{attack}}$, o drone mantém sua trajetória em direção ao ponto de interesse, ativando o modo de ataque desesperado (*desperate attack*), caracterizado por uma abordagem direta e agressiva sem levar em consideração novas detecções. Caso contrário, o drone ativa um comportamento de evasão, desviando-se temporariamente, na direção oposta ao drone defensivo, para evitar o confronto direto, durante um número fixo de passos definido por S_{escape}.
Esta modelagem, que se baseia no exame dos drones inimigos, permite a simulação de ameaças dinâmicas e pseudo-aleatórias em que a decisão do drone se adapta às condições locais e à proximidade com o ponto de interesse, equilibrando o risco de um ataque agressivo com a necessidade de evasão diante da presença dos drones defensivos.

D. Dinâmica da Comunicação Ad Hoc

A comunicação entre os drones é estabelecida de forma direta e descentralizada, utilizando redes *ad hoc*. Cada drone compartilha periodicamente suas matrizes de recência e de direção com os drones que se encontram dentro de um determinado raio. Esse mecanismo assegura que, mesmo que um drone não detecte diretamente uma ameaça, ele receba informações complementares dos seus vizinhos, promovendo uma visão mais integrada, atualizada e ampla do ambiente. Além disso, a atualização inteligente – que consiste em substituir informações obsoletas pelas mais recentes – garante que a rede mantenha a operacionalidade, mesmo diante de eventuais falhas pontuais.

E. Mecanismo de Perseguição e Interceptação

Para que um drone, denominado *chaser*, intercepte um drone ofensivo, é necessário determinar a trajetória e a direção de movimento ideais que considerem tanto a posição atual do alvo quanto sua velocidade. Esta subseção apresenta, de forma detalhada, todos os passos do procedimento matemático utilizado para calcular o tempo de interceptação e a direção a ser seguida pelo *chaser*.

Sejam:

- $\mathbf{p}_c$ a posição atual do drone perseguidor;
- $\mathbf{p}_t$ a posição atual do alvo;
- $\mathbf{v}_t$ o vetor velocidade do alvo (assumido módulo constante durante o período de interesse);
- v_c a velocidade escalar constante do perseguidor.

Inicialmente, define-se o vetor de diferença de posição entre o alvo e o perseguidor:

$$\mathbf{r} = \mathbf{p}_t - \mathbf{p}_c. \tag{2}$$

O objetivo é determinar o tempo t necessário para que o perseguidor alcance um ponto de interseção com o alvo, considerando que o alvo continua se movendo com velocidade $\mathbf{v}_t$. Assim, após um tempo t, a posição do alvo pode ser expressa por:

$$\mathbf{p}_t(t) = \mathbf{p}_t + \mathbf{v}_t\, t. \tag{3}$$

Simultaneamente, o perseguidor, que se move com velocidade v_c na direção de interceptação $\mathbf{d}$, percorrerá uma distância igual a $v_c\, t$ ao longo de um vetor unitário. Para que o perseguidor atinja o alvo, a distância entre sua posição atual e a posição futura do alvo deve ser igual à distância que ele percorrerá em t segundos. Assim, a condição de interceptação pode ser modelada como:

$$\|\mathbf{p}_t + \mathbf{v}_t\, t - \mathbf{p}_c\| = v_c\, t. \tag{4}$$

Utilizando a definição de $\mathbf{r}$, a equação pode ser reescrita como:

$$\|\mathbf{r} + \mathbf{v}_t\, t\| = v_c\, t. \tag{5}$$

A partir daí, é possível rearranjar (5) de modo a agrupar os termos que envolvem t^2 da seguinte forma:

$$t^2 \left[(\mathbf{v}_t \cdot \mathbf{v}_t) - v_c^2\right] + 2t\,(\mathbf{r} \cdot \mathbf{v}_t) + \mathbf{r} \cdot \mathbf{r} = 0. \tag{6}$$

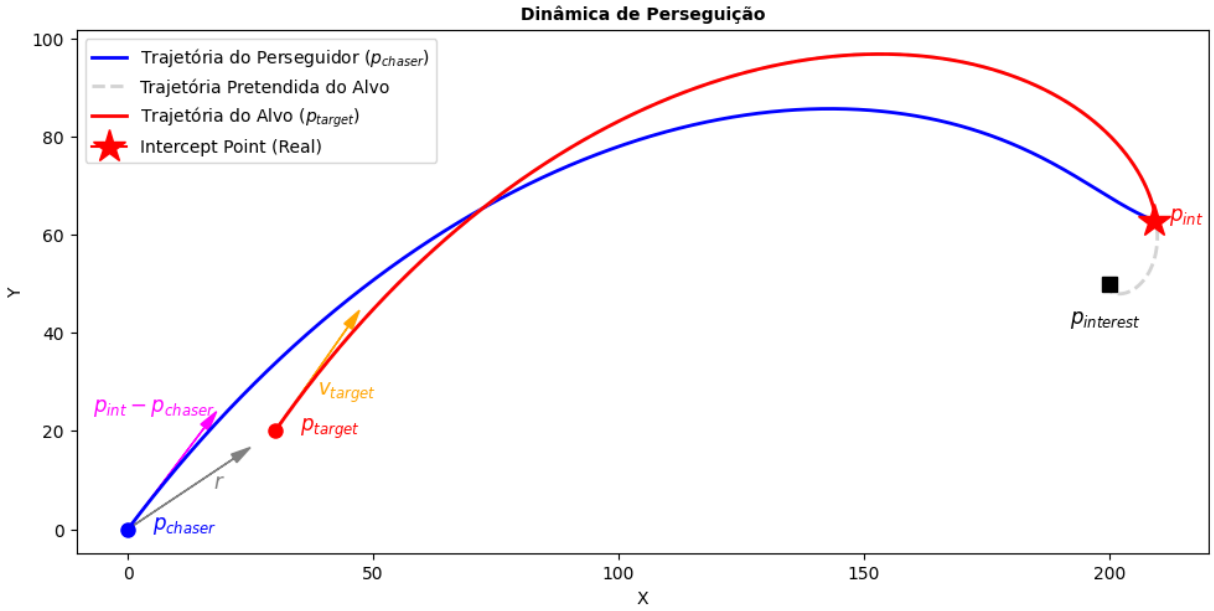


Fig. 9: Exemplo de dinâmica de perseguição com interceptação.

Para simplificar a notação, definem-se as constantes:

$$a = (\mathbf{v}_t \cdot \mathbf{v}_t) - v_c^2,$$
$$b = 2\,(\mathbf{r} \cdot \mathbf{v}_t),$$
$$c = \mathbf{r} \cdot \mathbf{r}.$$

A equação passa a ser escrita na forma padrão de uma equação quadrática:

$$a\,t^2 + b\,t + c = 0. \tag{7}$$

Se, mesmo após o cálculo, nenhum $t > 0$ for encontrado, a estratégia adotada é utilizar a direção diretamente do perseguidor ao alvo. Nesse caso, define-se:

$$\mathbf{d} = \frac{\mathbf{p}_t - \mathbf{p}_c}{\|\mathbf{p}_t - \mathbf{p}_c\|}, \tag{8}$$

o que implica em mover o drone na direção do alvo conforme sua posição atual, sem antecipar seu movimento.

Por outro lado, se uma solução $t > 0$ for obtida, calcula-se o ponto de interseção ($\mathbf{p}_i$) estimado por (3) e a direção de interceptação é, então, determinada como:

$$\mathbf{d} = \frac{\mathbf{p}_i - \mathbf{p}_c}{\|\mathbf{p}_i - \mathbf{p}_c\|}. \tag{9}$$

Esta direção orienta o drone perseguidor para interceptar o alvo, considerando tanto a posição atual quanto a tendência de movimento do mesmo.

Esta abordagem, fornece um modelo matemático detalhado para a interceptação, permitindo que o drone perseguidor ajuste sua trajetória de maneira a antecipar o movimento do alvo.

F. Estratégia de Holding para Posições Defensivas

O modo *holding* representa o estado em que um drone se encontra quando não está diretamente envolvido em uma perseguição. Estar em *holding* não significa, necessariamente, que o drone permaneça parado. Pelo contrário: assume-se que exista um conjunto de regras de movimentação específicas para esse estado que seja capaz de maximizar a eficiência defensiva.

Na estratégia exemplificada na Seção V, primeiramente avalia-se, em ordem crescente de distância do drone inimigo até o ponto de interesse, qual o primeiro drone ofensivo que apresenta uma proa agressiva, isto é, cuja direção é contínua e direta para a área de interesse. Em seguida, todos os drones defensivos que não estão envolvidos em perseguição verificam a distância até a reta correspondente à trajetória esperada para o drone ofensivo ou até o próprio ponto de interesse, considerando o que for mais próximo. Se essa distância estiver abaixo de um limiar pré-estabelecido, o drone defensivo em modo *holding* desloca-se para se posicionar entre o drone ofensivo e a área de interesse, ou mesmo diretamente na área de interesse.

1) Seja $\mathbf{p}$ a posição atual do drone e $\mathbf{p}_c$ o centro da célula candidata, cujo vetor de direção associado é $\mathbf{d}_e$. A projeção da posição $\mathbf{p}$ sobre a reta que passa por $\mathbf{p}_c$ com direção $\mathbf{d}_e$ é obtida computando

$$s = (\mathbf{p} - \mathbf{p}_c) \cdot \mathbf{d}_e,$$

onde $\cdot$ denota o produto interno. O ponto de projeção, que chamaremos de P, é então definido por

$$P = \mathbf{p}_c + s\,\mathbf{d}_e.$$

2) Define-se um limiar T (denotado por `THRESHOLD_PROJECTION`) para a distância máxima permitida entre a posição do drone e seu ponto de projeção. Se

$$\|\mathbf{p} - P\| > T,$$

o drone permanece em *holding* e não se desloca.

3) Caso contrário, o ponto defensivo D é determinado de forma a garantir que o agente se posicione de maneira estratégica para interceptar a ameaça. Em

termos práticos, D é definido como:

$$D = \begin{cases} P, & \text{se } \|\mathbf{p} - P\| \leq \|\mathbf{p}_{IP} - P\|, \\ \mathbf{p}_{IP}, & \text{caso contrário,} \end{cases}$$

onde $\mathbf{p}_{IP}$ representa o ponto de interesse central da defesa.

A Fig. 10 ilustra um exemplo em que ocorre a dinâmica descrita.

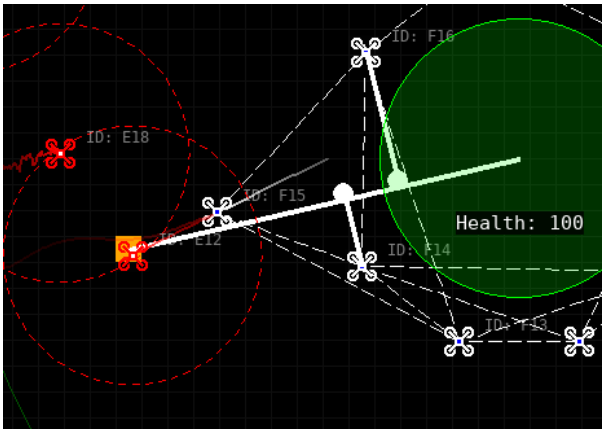


Fig. 10: Dois drones em estado de *holding* se deslocam para se colocarem entre drone inimigo, que tem proa agressiva, e o ponto de interesse.

G. Resiliência à propagação de informações erradas devido à falha de Drones Amigos

Uma característica fundamental do simulador *DroneSwarm2D* é a robustez do mecanismo de comunicação e integração de informações entre os drones amigos, que contribui para a resiliência a falhas não intencionais.

Nesse procedimento, cada drone realiza uma junção seletivo dos dados de detecção provenientes de um vizinho, mas somente se, na área de interseção dos seus respectivos círculos de detecção, uma fração mínima das células (definida pelo parâmetro `TOLERANCE_RATIO`) apresentar significativas semelhanças. As diferenças são avaliadas célula a célula com base em dois critérios:

- **Intensidade de Detecção:** A diferença absoluta entre as intensidades registradas pelo drone e pelo vizinho não pode exceder um limiar preestabelecido (`POSITION_INTENSITY_THRESHOLD`).
- **Vetores de Direção:** A norma da diferença entre os vetores de direção correspondentes a cada célula deve ser inferior a um limite definido (`POSITION_DIRECTION_THRESHOLD`).

Se a fração de células compatíveis na área de interseção for igual ou superior à fração mínima exigida, a junção é efetuado da forma esperada, ou seja, as células onde o *timestamp* do vizinho é mais recente são atualizadas com as informações desse agente. Essa estratégia garante que pequenas falhas ou erros sistemáticos de medição – que podem ocorrer de forma não intencional em um drone amigo – não se propaguem pelo sistema, pois apenas dados consistentes e verificados são incorporados ao estado global da rede.

Assim, o mecanismo de junção contribui para a resiliência do sistema, permitindo que o conjunto de drones mantenha uma visão integrada e atualizada do ambiente mesmo quando algum agente apresenta falhas temporárias em suas medições ou comunicação. Essa abordagem fortalece a robustez das propostas de soluções distribuídas, garantindo que a cooperação entre os drones amigos se mantenha efetiva mesmo sob condições adversas.

V. Exemplo de Cenário: Enxame com Detecção Local e Comunicação Distribuída

Neste cenário, cada drone defensivo utiliza sensores de curto alcance para realizar detecções locais. A troca de informações ocorre de forma distribuída entre drones próximos, permitindo que cada agente atualize seu estado com base em dados coletados coletivamente. Essa abordagem visa ampliar a cobertura e a precisão das detecções, superando as limitações de uma detecção local e limitada do ambiente.

Segue a Fig. 11 com dois momentos da simulação. O vídeo pode ser acessado através do *link* clicável ou da página fornecida nos Apêndices.

VI. Conclusão

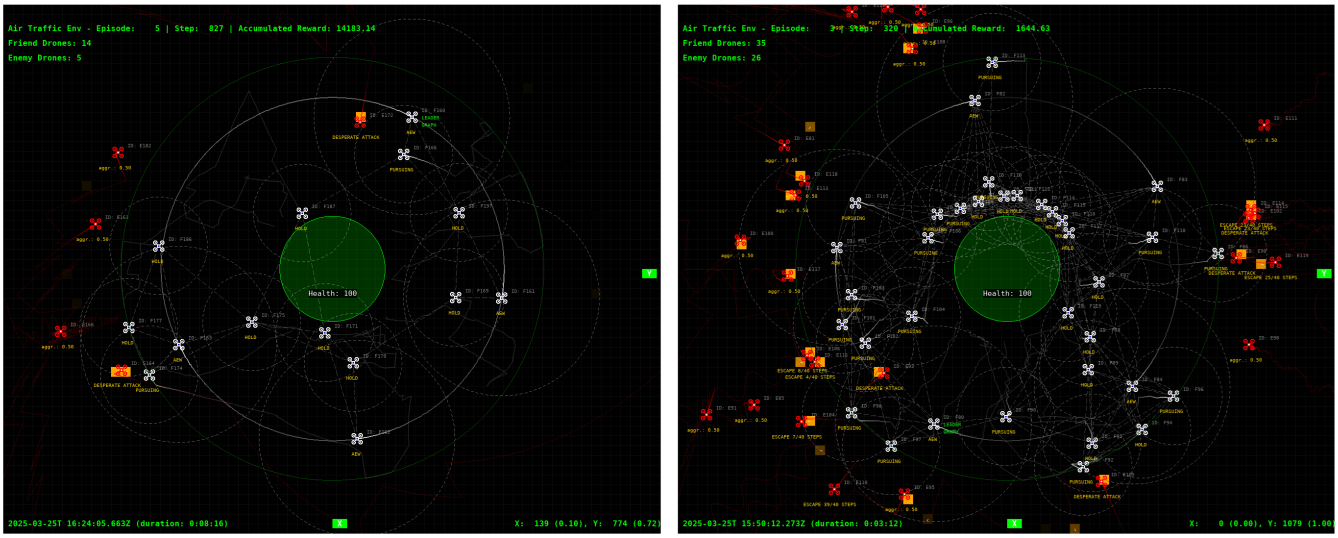
O trabalho apresentado demonstra que o simulador 2D, *DroneSwarm2D*, constitui uma ferramenta eficaz para o estudo e a validação de táticas defensivas distribuídas em ambientes com drones autônomos. A integração de redes *ad hoc*, algoritmos distribuídos e modelos matemáticos para interceptação e estratégias de holding evidencia a viabilidade de eliminar pontos únicos de falha, típicos em soluções centralizadas, promovendo uma resposta coordenada e resiliente a ameaças emergentes. Além disso, a plataforma permite a experimentação e a customização de estratégias de defesa, contribuindo significativamente para o avanço do conhecimento na área.

Adicionalmente, a crescente diversificação no emprego de drones – que abrange desde sistemas de ataque autônomos até a incorporação de tecnologias de inteligência artificial para aprimorar a precisão e a autonomia das operações – reflete uma tendência global (Lendon et al. 2024; Somos Notícia 2023). Tais inovações demonstram que a economia de recursos aliado à flexibilidade operacional, pode ser decisiva para o sucesso nesse tipo de cenário.

Em síntese, os resultados indicam que a adoção de abordagens distribuídas para a coordenação de drones autônomos representa uma alternativa promissora para a defesa aérea, contribuindo para o desenvolvimento de sistemas mais resilientes, escaláveis e economicamente viáveis.

Como direções para investigações futuras, sugerem-se as seguintes abordagens:

1) **Integração com Algoritmos de Aprendizado por Reforço:** Investigar a aplicação de técnicas de aprendizado por reforço para que os drones possam aprimorar de maneira autônoma suas táticas defensivas com base em *feedback* contínuo, ajustando dinamicamente suas estratégias conforme o ambiente e o comportamento das ameaças.



(a) (b)

Fig. 11: **(a)** Simulação do exemplo proposto, onde o ponto de interesse (centro do círculo de cor verde) é protegido por drones defensivos (brancos) enquanto drones inimigos (vermelhos) se aproximam; **(b)** Outro episódio da simulação do mesmo cenário num momento em que ocorrem as primeiras detecções, onde se observa um maior número de drones remanescentes.

2) **Estudos de Escalabilidade e Robustez:** Realizar investigações que explorem a escalabilidade do sistema em ambientes com um número significativamente maior de drones e ameaças simultâneas, bem como a análise da robustez do sistema diante de falhas parciais na comunicação e na detecção.

VII. CONTRIBUIÇÕES DOS AUTORES

Lucas S. Lima: Concepção e desenho da pesquisa; elaboração do manuscrito; e implementação do simulador.

Rafael Duarte Rocha: Revisão intelectual do manuscrito.

Rafael H. Giannico: Criação de exemplo de cenário.

Denys D. C. Brito: Revisão da literatura.

João P. A. Dantas: Aprovação final da versão submetida ao congresso.

Referências

A Referência. 2022. De 'geeks' a guerrilheiros: jovens ucranianos constroem drones para uso no front. A Referência. https://areferencia.com/europa/de-geeks-a-guerrilheiros-jovens-ucranianos-constroem-drones-para-uso-no-front/.

Andrade Martins, Madjer de, David Alan Garren e Ralph Clark Robertson. 2022. Método inspirado no 5G para a determinação de distância entre drones em composição de enxame. *Revista Pesquisa Naval* 34:50–55.

Aquino Cabral, Luiz Antônio Barros de. 2020. A Transformação da Guerra por Robôs Automatizados e sua Regulação pelo Direito Internacional Humanitário. Trabalho de Conclusão de Curso, Universidade Federal da Paraíba.

Bekmezci, Ilker, O. K. Sahingoz e S. Temel. 2013. Flying Ad-Hoc Networks (FANETs): A survey. *Ad Hoc Networks* 11:1254–1270. https://doi.org/10.1016/j.adhoc.2012.12.004.

Bine, Lailla M. S., Luiz Filipe M. Vieira, Linnyer B. Ruiz e Antonio A. F. Loureiro. 2020. GeoIoD: Um Protocolo de Disseminação de Informação Geocast para Internet dos Drones. *International Journal of Drone Applications.*

Botasot. 2024. "I was very afraid": the hunting of Russian drones against civilians in Ukraine, evidence from the field. Acesso em 28 de março de 2025. https://botasot.co/kisha-shume-frike-gjuetia-e-droneve-ruse-ndaj-civileve-ne-ukraine-deshmi-nga-terreni/.

Catarro, Miguel, Luis Ramos Pinto e Alan Oliveira. 2024. Aumento da Longevidade de FANET através da Troca Estratégica de Posições dos Drones. Em *Anais do INForum 2024.* Disponível em: [link ou DOI, se houver]. Lisboa, Portugal.

Choi, Han-Lim, L. Brunet e J. How. 2009. Consensus-Based Decentralized Auctions for Robust Task Allocation. *IEEE Transactions on Robotics* 25:912–926. https://doi.org/10.1109/TRO.2009.2022423.

Dubins, L. E. 1957. On Curves of Minimal Length with a Constraint on Average Curvature, and with Prescribed Initial and Terminal Positions and Tangents. *American Journal of Mathematics* 79 (3): 497–516. ISSN: 00029327, 10806377, acesso em 28 de março de 2025. http://www.jstor.org/stable/2372560.

Guelman, M. 1971. A qualitative study of proportional navigation. *IEEE Transactions on Aerospace and Electronic Systems* AES-7:637–643. https://doi.org/10.1109/TAES.1971.310406.

Hassija, Vikas, Vikas Saxena e V. Chamola. 2020. Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory. *Comput. Commun.* 149:51–61. https://doi.org/10.1016/j.comcom.2019.09.021.

Issmael Júnior, Ali Kamel. 2024. A Convenção de Genebra e as tecnologias disruptivas: Impactos e possíveis soluções. *Revista do Ministério Público Militar* 51 (43): 61–78. https://doi.org/10.5281/zenodo.13939740.

Jelasity, Márk, Alberto Montresor e Ozalp Babaoglu. 2005. Gossip-based aggregation in large dynamic networks. *ACM Trans. Comput. Syst.* (New York, NY, USA) 23, n. 3 (agosto): 219–252. ISSN: 0734-2071. https://doi.org/10.1145/1082469.1082470. https://doi.org/10.1145/1082469.1082470.

Karner, Natasha. 2024. Combatendo drones com drones: aprendendo com a Ucrânia sobre o futuro da guerra. Instituto Australiano de Assuntos Internacionais. https://www.internationalaffairs.org.au/australianoutlook/fighting-drones-with-drones-learning-from-ukraine-on-the-future-of-warfare/.

Kundu, Joydeep, Sahabul Alam, J. C. Das, Arindam Dey e Debasis De. 2024. Trust-Based Flying Ad Hoc Network: A Survey. *IEEE Access* 12:99258–99281. https://doi.org/10.1109/ACCESS.2024.3419904.

Lendon, Brad, Maria Kostenko, Darya Tarasova e Hande Atay Alam. 2024. Ucrânia diz ter destruído caça russo essencial à ação militar do Kremlin. CNN Brasil. https://www.cnnbrasil.com.br/internacional/ucrania-diz-ter-destruido-caca-russo-essencial-a-acao-militar-do-kremlin/.

Lian-jiong, Zhong. 2004. Bully algorithm and optimization in distributed systems. *Journal of Xi'an Institute of Technology.*

Myre, Greg. 2024. Para atingir profundamente a Rússia, a Ucrânia construiu seus próprios drones. NPR. https://www.npr.org/2024/11/20/nx-s1-5065480/ukraine-war-drones-russia.

Oliveira, Kaleb Rodrigues, William Speranzini e Israel S. Florentino. 2021. Controle de Drones por Swarm. Artigo exploratório sobre controle autônomo de enxames de drones, *Anais da Faculdade de Computação e Informática – Universidade Presbiteriana Mackenzie.*

Padilha, Luiz. 2024. O Uso de IEDs na Guerra Rússia-Ucrânia. Defesa Aérea & Naval. https://www.defesaaereanaval.com.br/analise/o-uso-de-ieds-na-guerra-russia-ucrania.

Ramanathan, R. e J. Redi. 2002. A brief overview of ad hoc networks: challenges and directions. *IEEE Communications Magazine* 40:20–22. https://doi.org/10.1109/MCOM.2002.1006968.

Rimawi, Diaeddin, Antonio Liotta, Marco Todescato e Barbara Russo. 2024. Modeling Resilience of Collaborative AI Systems. *2024 IEEE/ACM 3rd International Conference on AI Engineering – Software Engineering for AI (CAIN),* 24–29. https://doi.org/10.1145/3644815.3644955.

Rodrigues, Lucas Soares, Ciro José Almeida Macedo, Vinicius da Cunha Martins Borges, Leizer de Lima Pinto, Kleber Vieira Cardoso e Antonio Carlos de Oliveira Júnior. 2019. Otimização da trajetoria com adaptação à autonomia de Drones como gateway de comunicação para dispositivos IoT. *Revista de Sistemas de Informação da FSMA,* n. 23, 10–23.

Santos Lima, Jonas Felipe dos e Nayara Guetten Ribaski. 2019. Aeronaves Remotamente Pilotadas (RPAs): Uma alternativa de enfrentamento à criminalidade. *Brazilian Journal of Technology* 2 (1): 483–501.

Santos Lima e Nayara Guetten Ribaski, Jonas Felipe dos. 2015. Modelos de Controle de Enxame em Redes de Drones. Referência genérica para coordenação de enxames, *Revista RPN.*

Somos Notícia. 2023. Drones de ataque caseiros, baratos e letais são vitais para a Ucrânia. Somos Notícia. https://somosnoticia.com.br/drones-de-ataque-caseiros-baratos-e-letais-sao-vitais-para-a-ucrania/.

Stepanenko, Viktoriia. 2023. Zelensky's Year-End Press Conference: Kyiv Post Special Report. Kyiv Post. https://www.kyivpost.com/post/25768.

SWI swissinfo.ch. 2024. Drones com explosivos se tornam a nova arma de dissidentes das Farc. SWI swissinfo.ch. https://www.swissinfo.ch/por/drones-com-explosivos-se-tornam-a-nova-arma-de-dissidentes-das-farc/81265270.

Vasudevan, Sudarshan, B. DeCleene, N. Immerman, J. Kurose e D. Towsley. 2003. Leader election algorithms for wireless ad hoc networks. *Proceedings DARPA Information Survivability Conference and Exposition* 1:261–272 vol.1. https://doi.org/10.1109/DISCEX.2003.1194890.

Ventura, Bona Cipto. 2024. Rusia Sukses Uji Drone Kamikaze Piranha-10 FPV, Menghancurkan Tank M1 Abrams Milik Ukraina Pemberian Amerika Serikat. Indonesia jakarta daily. https://indonesia.jakartadaily.id/nasional/69312046852/rusia-sukses-uji-drone-kamikaze-piranha-10-fpv-menghancurkan-tank-m1-abrams-milik-ukraina-pemberian-amerika-serikat?page=2.

Whittaker, Mark. 2023. Drones de papelão da Austrália atingem a Rússia. Forbes. https://www.forbes.com.au/covers/innovation/the-aussie-cardboard-drones-hitting-russia-in-massed-attacks/.

Zegart, Amy. 2020. Cheap fights, credible threats: The future of armed drones and coercion. *Journal of Strategic Studies* 43:46–6. https://doi.org/10.1080/01402390.2018.1439747.

Apêndice

- **Repositório**: O código-fonte da aplicação de simulação, juntamente com os cenários e os resultados dos estudos, está disponível no repositório online: https://github.com/lucasll37/DroneSwarm2D

- **Simulação**: O vídeo demonstrativo da visualização da simulação pode ser acessado pelo seguinte link: https://youtu.be/KauXy_OLA7o