Investigando a Resiliência de Serviços de Localização Para Redes de UAVs Diante de Ataques de Injeção de Dados Falsos

Lucas de Oliveira Araújo
Depto. de Ciência da Computação
Univ. Federal de Minas Gerais (UFMG)
Belo Horizonte, Brasil
araujolucas@dcc.ufmg.br

Agnaldo de Souza Batista
Depto. de Informática
Univ. Federal do Paraná (UFPR)
Curitiba, Brasil
asbatista@inf.ufpr.br

Aldri Luiz dos Santos
Depto. de Ciência da Computação
Univ. Federal de Minas Gerais (UFMG)
Belo Horizonte, Brasil
aldri@dcc.ufmg.br

***Resumo*—Veículos aéreos não tripulados (UAVs) dependem de serviços de compartilhamento de localização para garantir a consciência espacial e evitar colisões. No entanto, a comunicação sem fio e a topologia altamente dinâmica tornam as redes FANETs vulneráveis a ataques de injeção de dados falsos (FDIA), que comprometem a integridade das informações de localização trocadas. Este trabalho investiga a resiliência do FlySafe, um serviço de localização para redes de UAVs, diante de oito modos de FDIAs. Para tanto, o FlySafe foi estendido com o instante de geração e um identificador único das mensagens trocadas, dando origem ao FlySafeTI, capaz de detectar FDIAs repetitivos. Os resultados de simulação revelam comportamentos complementares: diante de FDIAs repetitivos, o FlySafeTI detectou e descartou mais de 95% dos pacotes falsificados, enquanto o FlySafe descartou apenas cerca de 50%. Em contrapartida, diante de FDIAs únicos com erro de localização aleatório, o FlySafe apresentou taxa de descarte de 89,93%, ao passo que o FlySafeTI atingiu 48,58%. Em todos os cenários avaliados, ambos os sistemas mantiveram consciência espacial por pelo menos 93,1% do tempo de operação, confirmando que a extensão proposta não compromete a disponibilidade do serviço de localização.**

***Index Terms*—UAV, FANET, Segurança, Ataque de injeção de dados falsos, FlySafe**

I. Introdução

Os veículos aéreos não tripulados (do inglês, *Unmanned Aerial Vehicle* — UAV), comumente conhecidos como Drones, têm apresentado um aumento expressivo na sua popularidade devido a sua versatilidade e mobilidade. Eles têm sido empregados em diversas atividades da sociedade, como em busca e salvamento, onde eles ajudam a detectar e acompanhar as vítimas, além de auxiliar no transporte de pequenas cargas [1]. Em operações militares, eles apoiam a vigilância e o reconhecimento, a aquisição e confirmação de alvos, a caracterização de áreas hostis e ataques [2]. Nesse cenário de expansão, a Gartner [3] estima que mais de um milhão de UAVs estarão realizando entregas no varejo até 2026, o que significa um aumento substancial em comparação aos 20.000 dispositivos que desempenhavam essa função em 2020.

Para atender a essas diferentes aplicações, em muitos cenários esses veículos precisam trocar informações entre si, o que caracteriza uma rede *ad hoc* aérea, (do inglês, *Flying Ad hoc Network* — FANET). Nesse tipo de rede, os UAVs estabelecem enlaces ponto-a-ponto e podem atuar como dispositivos terminais e roteadores em uma topologia com alta dinamicidade. Além disso, sempre que disponível, podem também utilizar a infraestrutura terrestre para ampliar o alcance da comunicação. Em geral, em uma FANET trafegam (i) dados de localização e estado — posição/altitude, velocidade e direção —, para consciência situacional, manutenção de formação e prevenção de colisões; (ii) dados de missão e de sensores, como imagens e vídeo; e (iii) informações operacionais, como a disponibilidade atual de recursos e a qualidade do enlace. [4], [5] A Figura 1 ilustra o cenário em que múltiplos UAVs trocam informações entre si e também com a infraestrutura terrestre.

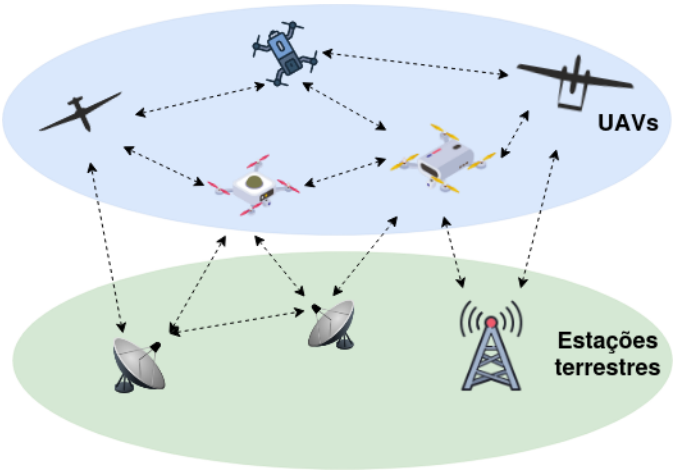

Figura 1: Rede de UAVs com enlaces ar-ar e ar-terra

A troca de informações entre os UAVs é fundamental para a operação correta destes dispositivos. No entanto, por dependerem predominantemente de canais sem fio abertos para essa comunicação, as FANETs estão expostas a diversas ameaças cibernéticas. Essa exposição agrava-se pelas vulnerabilidades inerentes aos protocolos que operam nas camadas física, de rede e de transporte, os quais deixam os enlaces

suscetíveis à interceptação, à manipulação e à repetição de mensagens, comprometendo a confidencialidade, a integridade e a disponibilidade da rede [6]. Além da topologia altamente dinâmica das FANETs, o uso de protocolos leves que frequentemente carecem de criptografia e autenticação robustas contribui para esse cenário de insegurança. Na prática, observam-se na camada física, ataques de interferência (*jamming*); na camada de rede, ataques de homem-do-meio (*man-in-the-middle*), negação de serviço (DoS), repetição (*replay*), buraco negro (*blackhole*), buraco de minhoca (*wormhole*), ataque *Sybil* e transbordamento da tabela de roteamento (*routing table overflow*); e na camada de transporte ocorre a exploração de vulnerabilidades de protocolo que habilita o sequestro e resultante tomada de controle dos UAVs, e ataques de injeção de pacotes, a fim de interromper a transmissão de dados.

Diante desse cenário de ameaças e da importância da comunicação entre os UAVs, destacam-se os ataques de injeção de dados falsos (do inglês, *False Data Injection Attack* — FDIA). Nesse modelo de ataque, agentes maliciosos inserem ou compartilham informações forjadas na rede com o objetivo de comprometer o seu funcionamento regular [7]. Em redes de UAVs, os FDIAs são particularmente críticos, pois podem modificar o comportamento dos veículos, induzindo trajetórias incorretas, interrompendo operações ou permitindo o acesso não autorizado a dados. Em virtude da criticidade de tais cenários, as operações de UAVs demandam a existência de um serviço de localização que seja resiliente a FDIA, de maneira a mitigar os efeitos dessa ameaça no funcionamento da rede.

Os ataques de injeção de dados falsos abrangem diversas categorias, destacando-se, como uma vertente específica e crítica, o ataque de repetição (do inglês, *Replay Attack*). Nesse caso, em vez de gerar dados inteiramente novos, um UAV malicioso captura mensagens válidas transmitidas por outro veículo e as reencaminha como se tivessem sido originadas por ele próprio, falsificando a fonte e o contexto temporal das informações [5], [6]. Tal comportamento ataca diretamente o frescor dos dados de rede, métrica que quantifica o quão atual é o dado recebido em relação à sua origem [8]. Essa perda de atualidade das informações afeta serviços críticos, como roteamento e localização, induzindo os dispositivos a tomarem decisões incorretas, por exemplo, na navegação e coordenação de voo. Consequentemente, há um aumento do risco operacional decorrente da redução da consciência espacial, visto que os UAVs passam a ter dificuldade para determinar de forma fidedigna a posição de seus vizinhos adjacentes dentro do seu alcance de comunicação. Assim, torna-se necessário implementar mecanismos de resiliência nas operações de rede para mitigar o impacto de nós maliciosos.

O restante deste trabalho está organizado da seguinte forma: A Seção II apresenta o referencial teórico e os trabalhos relacionados. A Seção III descreve a metodologia e as atividades de implementação conduzidas. A Seção IV apresenta os resultados obtidos por meio de simulações e a respectiva análise de desempenho e segurança. Por fim, a Seção V traz as conclusões e as perspectivas de trabalhos futuros.

II. Referencial Teórico

Esta seção apresenta os fundamentos teóricos necessários para a compreensão da proposta de mitigação. Inicialmente, descreve-se o funcionamento de serviços de compartilhamento de localização em redes de UAVs, seguido pela definição e caracterização dos FDIAs e seus impactos no funcionamento de rede. Na sequência, detalha-se o sistema FlySafe, serviço de compartilhamento de localização escolhido como base para investigar o impacto de diferentes modos de FDIAs em redes de UAVs. Por fim, discutem-se os trabalhos relacionados que abordam a segurança e a autenticação nesse contexto, destacando as lacunas que motivam esta pesquisa.

A. Serviço de Localização para Redes de UAVs

Um serviço de compartilhamento de localização em redes de UAVs consiste no mecanismo responsável por disseminar informações de posição atualizadas entre os veículos. Assim, cada UAV mantém consciência espacial sobre os demais que operam em sua área de cobertura [9]. Esse serviço deve garantir que as posições recebidas sejam suficientemente recentes para apoiar decisões de navegação e evitar colisões. A Figura 2 exemplifica esse fluxo de informações entre UAVs. O UAV_1 estima sua posição e a transmite para o UAV_2, que recebe a mensagem e atualiza sua consciência espacial com base na localização informada. Esse mecanismo possibilita que todos os UAVs mantenham conhecimento atualizado sobre seus vizinhos, requisito fundamental para navegação segura, coordenação de trajetórias e manutenção de formação.

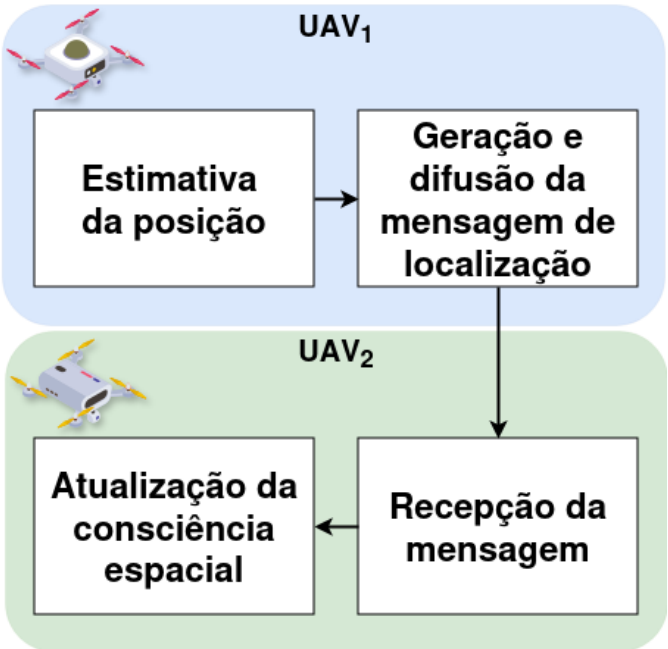

Figura 2: Fluxo de operação de um serviço de compartilhamento de localização em redes de UAVs

A disseminação das informações de localização pode seguir diferentes estratégias, que se distinguem principalmente

quanto ao momento e ao alcance da transmissão. Nas abordagens proativas, cada UAV anuncia periodicamente sua posição por meio de mensagens de difusão (*beacons*), mantendo a vizinhança continuamente informada ao custo de tráfego constante na rede. Já nas abordagens reativas, ou orientadas a eventos, a posição é transmitida apenas quando ocorre uma mudança significativa de localização, reduzindo o volume de mensagens em troca de atualizações menos frequentes [4]. Quanto ao alcance, a disseminação pode restringir-se aos vizinhos a um salto (*single-hop*) ou propagar-se por múltiplos saltos (*multi-hop*) para alcançar UAVs fora do raio de comunicação direta. Independentemente da estratégia adotada, cada UAV organiza as posições recebidas em uma estrutura de vizinhança, frequentemente denominada lista ou tabela de vizinhos, a partir da qual constrói e atualiza sua consciência espacial.

B. FDIA em Redes de UAVs

Os FDIAs ocorrem quando um dispositivo não autorizado manipula mensagens para enganar o destinatário ou inundar a rede com mensagens falsas. Em redes de UAVs podem ocorrer diferentes modelos de FDIAs, os quais dependem da localização do atacante e dos métodos de ataque empregados. Alguns modelos injetam informações falsas de maneira constante ou senoidal [10], [11], caracterizando padrões previsíveis de ataque. Entretanto, esses modelos podem ser ineficazes em cenários reais devido à simplicidade ou à regularidade dos métodos utilizados [12], [13]. Apesar dessas diferenças, uma característica comum entre os FDIAs é a capacidade de induzir o alvo, i.e., dispositivo, usuário ou aplicação, a aceitar entradas provenientes de fontes externas ou não autenticadas [14].

Em redes de UAVs, um veículo malicioso pode explorar essa característica ao interceptar o conteúdo das mensagens trocadas entre dois UAVs, alterar a sua localização e enviar a mensagem para o UAV final, levando esse UAV a tomar decisões com base em dados incorretos. No contexto dos FDIAs repetitivos, o atacante retransmite múltiplas mensagens falsificadas de forma persistente, comprometendo a integridade temporal e a confiabilidade da rede. Em contrapartida, os FDIAs únicos consistem no envio de uma mensagem fraudulenta isolada, o que pode dificultar a detecção por mecanismo estatísticos. Tais ataques podem degradar serviços de localização, induzir estimativas espaciais incorretas e comprometer a coordenação e prevenção de colisões ao tornar a topologia da rede de UAVs indisponível [15]. A Figura 3 ilustra um FDIA repetitivo em uma rede de UAVs em missão de detecção de focos de incêndio. Inicialmente, no instante t_1, o UAV malicioso intercepta as mensagens de localização emitidas pelo UAV_2 para o UAV_1. Posteriormente, em t_2, o atacante retransmite múltiplas mensagens falsas na rede, falsificando a identidade do UAV_2 e comprometendo o funcionamento do UAV_1 com informações de localização desatualizadas, afetando a sua tomada de decisão.

C. O Sistema FlySafe

A operação segura de UAVs em FANETs depende de consciência espacial contínua entre vizinhos, isto é, cada aeronave precisa conhecer quem está ao seu redor, com informação de posição suficientemente atualizada. O sistema FlySafe [9] aborda essa necessidade ao prover um serviço de compartilhamento de localização que leva em conta a idade da informação (do inglês, *Age of Information* — AoI) da localização compartilhada, ou seja, o tempo decorrido desde a geração da informação até a sua aplicação [8]. O sistema organiza-se em duas etapas: descoberta de vizinhos e manutenção de vizinhos. Na fase de descoberta, os UAVs enviam periodicamente mensagens de anúncio (do inglês, *Hello Messages* — HM) para avisar a vizinhança sobre sua presença; ao receber uma HM, um vizinho responde com mensagens de identificação (do inglês, *Identification Message* — IM), possibilitando que ambos atualizem suas listas de vizinhança. Já na fase de manutenção, quando ocorre a mudança de posição, o UAV envia mensagens de localização (do inglês, *Trap Message* — TM) diretamente aos vizinhos conhecidos, indicando sua nova posição. Esse ciclo de mensagens de controle e gerenciamento garante que cada UAV mantenha consciência espacial atualizada sobre quem está em sua vizinhança, mesmo em cenários de alta mobilidade.

A estratégia de detecção de mensagens com localização falsa empregada pelo FlySafe é baseada na plausibilidade espacial, i.e., verificar se a localização informada corresponde a de um UAV dentro do raio de cobertura do UAV receptor [9], como mostra o Algoritmo 1. A partir dessa análise, o FlySafe emprega uma estratégia de classificação do UAV malicioso, inicialmente como suspeito, e caso esse comportamento seja recorrente, o UAV malicioso é bloqueado. Essa ação leva a segregação do UAV da rede, e as próximas mensagens provenientes desse UAV serão descartadas. Além disso, os UAVs vizinhos serão notificados acerca da presença de um UAV malicioso na rede, estendendo para os demais participantes na rede a mitigação dos efeitos das informações de localização falsas enviadas pelo UAV malicioso. Apesar de comprovar a eficiência do mecanismo de plausibilidade em detectar FDIA únicos, não há, contudo, experimentos que levam em conta os diferentes modos desse tipo de ataque, em especial o FDIA repetitivo. Essa limitação decorre do fato de que o módulo de detecção de FDIA do FlySafe analisa exclusivamente o valor da localização recebido, sem considerar frescor temporal ou a unicidade da mensagem. Assim, pacotes capturados e retransmitidos por um atacante externo, que preservam a identidade do UAV legítimo, não são distinguíveis de mensagens genuínas pelo mecanismo de plausibilidade espacial. Dessa maneira, há a oportunidade de investigar a performance do FlySafe em diferentes modos de FDIAs e aumentar a capacidade do sistema em identificar e mitigar tais ataques.

D. Trabalhos Relacionados

Serviços de compartilhamento de localização para redes de UAVs têm sido propostos com diferentes estratégias de disseminação de mensagens. Em [16], os autores propõem um serviço para UAVs em enxame (do inglês, *swarm*) que, além de compartilhar posições entre vizinhos, estima localizações

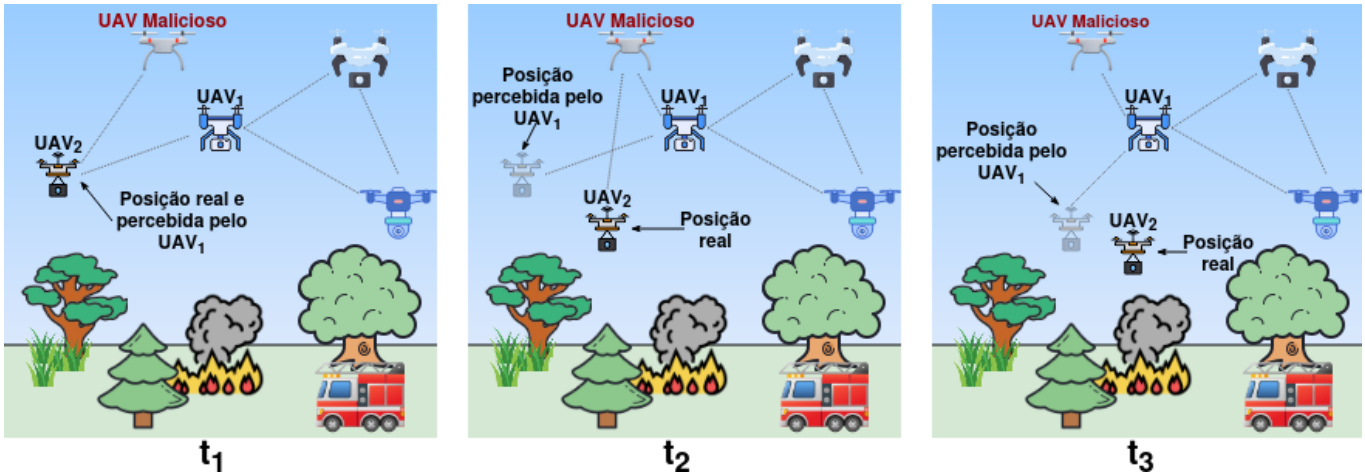

Figura 3: FDIA repetitivo em missão de detecção de incêndio. Em t_1, o UAV malicioso intercepta a mensagem transmitida pelo UAV_2 para o UAV_1. Em t_2, a mensagem capturada em t_1 é injetada ao UAV_1; nesse mesmo instante, o UAV_2 muda de posição e emite nova mensagem, também interceptada. Em t_3, essa segunda mensagem capturada é injetada ao UAV_1. Assim, em t_2 e t_3, o UAV_1 recebe informações de localização desatualizadas do UAV_2.

Algoritmo 1: FlySafe: Detecção de FDIA

```
Data: u (UAV), n (UAV vizinho), NL (Lista de vizinhos), L
      (Localização), s (Estado do UAV)
while u = ON do
    u ← L(n) + NL(n)
    if Bloqueado(n) = True then
        Descarta (L(n) + NL(n))
    else
        if L(n) = False then
            Envia s_n ∀ n ∈ NL(u)
            if Honesto(n) = True then
                Processa (L(n) + NL(n))
            else
                Descarta (L(n) + NL(n))
            end
        else
            if Suspeito(n) = True then
                Envia s_n ∀ n ∈ NL(u)
            end
            Processa (L(n) + NL(n))
        end
    end
end
```

não recebidas por meio de ajuste de curvas [17], mitigando os efeitos da alta mobilidade e de falhas de comunicação. Em [18], o compartilhamento de localização é apoiado por Blockchain, garantindo privacidade das comunicações e consenso distribuído sobre as posições dos veículos. Entretanto, ambos os serviços assumem que os UAVs da rede são confiáveis, desconsiderando a possibilidade de dispositivos maliciosos injetarem informações de localização falsas para comprometer a operação do enxame.

Os FDIAs repetitivos são amplamente tratados no nível de autenticação de aplicação, onde protocolos recentes incorporam provas formais contra a reintrodução de mensagens antigas [5]. Em [19], os autores apresentam o PRLAP-IoD (*A PUF-based Robust and Lightweight Authentication Protocol for Drone-Gateway and Drone-Drone Communication*), um protocolo leve baseado em PUF (*Physical Unclonable Function*) para autenticação e acordo de chaves em internet dos drones (do inglês, *Internet of Drones* — IoD), que combate FDIA repetitivos via checagem de frescor. Nele, cada sessão usa carimbos de tempo e valores aleatórios de desafio-resposta PUF exclusivos, assegurando que mensagens antigas não sejam aceitas. Apesar disso, essa proteção só foi atestada para mensagens do protocolo de autenticação, não necessariamente para mensagens de controle de serviços de compartilhamento de localização.

Ainda no contexto de segurança em IoD, em [20] os autores propõem o BSD2C-IoD (*Blockchain-based secure data delivery and collection scheme in the 5G-envisioned IoT-enabled IoD environment*), um esquema de entrega de dados e controle de acesso voltado para ambientes IoD habilitados por 5G. Embora o protocolo utilize números pseudoaleatórios para o estabelecimento de chaves de sessão, a detecção de FDIA repetitivos delega-se estritamente à verificação de etiquetas de tempo (do inglês, *timestamps*) e janelas de tolerância. Essa dependência cria uma vulnerabilidade residual: o mecanismo não garante a unicidade estrita do pacote dentro da janela de tempo válida. Logo, as mensagens de controle de serviços de consciência situacional, como as empregadas no FlySafe, permanecem suscetíveis à reintrodução maliciosa caso sejam retransmitidas rapidamente dentro desse intervalo de aceitação, comprometendo a operação em cenários de alta mobilidade.

Em síntese, os trabalhos discutidos demonstram que os protocolos que incorporam técnicas de avaliação de frescor e deduplicação de mensagens [19], [20] restringem-se ao nível de autenticação, sem cobrir as mensagens de controle de serviços de localização. Da mesma forma, serviços de localização para redes de UAVs [16], [18] desconsideram ações maliciosas de dispositivos pertencentes à própria rede.

Dessa forma, permanece a lacuna no nível do serviço de localização e consciência situacional, evidenciando a oportunidade de avaliar e projetar defesas específicas para mensagens de controle de serviços de compartilhamento de localização em redes de UAVs.

III. Metodologia e Desenvolvimento

Esta seção detalha a metodologia adotada para avaliar o impacto dos FDIAs repetitivos no serviço de localização de UAVs. Inicialmente, apresenta-se a variação do sistema FlySafe que conta com a estratégia de detecção e mitigação de FDIAs repetitivos chamado FlySafeTI. Em sequência, descreve-se o ambiente de simulação configurado no simulador de redes ns-3, incluindo os modelos de mobilidade e os parâmetros de comunicação utilizados. Posteriormente, apresenta-se o modelo de ameaça desenvolvido, especificando a implementação do comportamento malicioso e a mecânica de injeção de pacotes falsificados nos cenários experimentais. Por fim, são apresentadas as métricas utilizadas para avaliar o impacto do ataque na performance da rede.

A. O sistema FlySafeTI

Diante do cenário em que diferentes modos de FDIAs podem se manifestar, os impactos à operação do FlySafe tendem a se amplificar. Como descrito na Seção II, o módulo de detecção do FlySafe analisa apenas a plausibilidade espacial da posição declarada, sem verificar frescor ou unicidade da mensagem. Isso torna o sistema incapaz de detectar FDIAs repetitivos, nos quais o atacante reenvia mensagens com identificação legítima de um vizinho e que podem passar pelo teste de plausibilidade por terem sido geradas em contexto válido.

Para aumentar a resiliência do FlySafe a esse tipo de ataque, propõe-se incorporar ao módulo de detecção duas informações adicionais: o instante de geração da mensagem (do inglês, *timestamp* ϕ) e um número de uso único (do inglês, *nonce* η). A combinação dessas técnicas é necessária porque cada uma, isoladamente, apresenta limitações: o uso exclusivo de *timestamps* é vulnerável a repetições rápidas dentro da janela de aceitação Δt_{max}, enquanto o uso isolado de *nonces* exigiria armazenamento indefinido de histórico, inviável para sistemas embarcados com memória limitada. Na abordagem híbrida proposta, o *timestamp* delimita a validação temporal da mensagem, permitindo o descarte eficiente de registros antigos, enquanto o *nonce* garante a unicidade estrita dentro dessa janela sem consumo excessivo de memória. O sistema resultante, denominado FlySafeTI, mantém toda a arquitetura original do FlySafe, modificando apenas a estrutura da mensagem e o módulo de detecção de FDIA. Dessa forma, à mensagem originalmente composta pelo identificador do dispositivo emissor (id), informação de localização (L) e lista de vizinhos (NL), são adicionados o *timestamp* ϕ e o número de uso único η, utilizados para identificar mensagens atrasadas ou repetidas, indicando a presença de um UAV malicioso realizando FDIAs na rede de UAVs. Assim, sempre que um UAV recebe uma mensagem, o FlySafeTI valida se sua idade está dentro da janela de tempo permitida para processamento e se aquela é a primeira recepção da mensagem. Caso a mensagem não seja aceita nas etapas de validação, o sistema identifica a existência de um vizinho realizando FDIA repetitivo e a descarta, conforme exposto no Algoritmo 2.

Algoritmo 2: FlySafeTI: Adaptação para detecção de FDIA baseada na temporalidade da mensagem

Data: u (UAV), n (UAV vizinho), ϕ (Instante de geração da mensagem), η (Número de uso único da mensagem), L (Localização), NL (Lista de vizinhos), t_a (Instante atual), Δt_{max} (Limiar temporal de aceitação de mensagens), LN_n (Lista de η do UAV n), T_{max} (Tamanho máximo de LN_n)

```
1  while u = ON do
2      u ← φ, η, L(n), NL(n)
3      if |φ − t_a| < Δt_max then
4          if η ∉ LN_n then
5              Processa (φ, η, L(n), NL(n))
6              if (Tamanho (LN_n) +1) = T_max then
7                  Remove (LN_n(0))
8              LN_n ← η
9          else
10             Descarta (φ, η, L(n), NL(n))
11         end
12     else
13         Descarta (φ, η, L(n), NL(n))
14     end
15 end
```

O emprego do *timestamp* ϕ como critério de frescor pressupõe que os UAVs compartilham uma referência temporal comum. Essa premissa é razoável em FANETs, uma vez que os UAVs podem dispor de receptores GPS, que fornecem, além do posicionamento, uma base de tempo sincronizada entre os dispositivos. Assim, ao receber uma mensagem, o UAV calcula a idade da informação como a diferença entre o instante de recepção e o *timestamp* ϕ contido na mensagem, aceitando-a apenas se essa idade for inferior à janela de aceitação Δt_{max}, fixada em 2 s nas simulações. Mensagens cuja idade excede Δt_{max} são consideradas desatualizadas e descartadas, o que limita a janela temporal disponível para o atacante reintroduzir pacotes capturados.

A verificação de unicidade, por sua vez, baseia-se em um registro dos *nonces* η já recebidos dentro da janela Δt_{max}. Como somente as mensagens cujo *timestamp* ainda se encontra dentro dessa janela precisam ser verificadas, os *nonces* associados a mensagens já expiradas podem ser removidos do registro, de modo que o histórico não cresce com o tempo total de operação. Para assegurar um limite superior de memória independente das condições da rede, cada UAV mantém, para cada vizinho, um registro de capacidade fixa, configurado em 500 mensagens nas simulações. Esse valor atua apenas como um teto conservador: como a remoção dos *nonces* expirados é regida pela janela Δt_{max}, o registro não é preenchido por completo em operação normal e a detecção independe do valor exato adotado, bastando que ele seja suficientemente grande. Dessa forma, o consumo de memória por UAV permanece

limitado e previsível, tornando o mecanismo adequado para dispositivos embarcados com memória restrita.

B. Ambiente de Simulação

Os experimentos foram conduzidos utilizando o simulador de redes discretas ns-3 (versão 3.34) [21]. O cenário simula uma FANET composta por 40 UAVs voando a 20 m/s em uma área quadrada com 1,5 km de lado a um nível de voo de 300 pés, que se trata de um nível de voo permitido para UAVs [22]. A mobilidade dos nós segue o modelo *2D Random Walk* e a velocidade constante de 20 m/s foram adotados com o objetivo de replicar o ambiente de simulação do FlySafe [9] para permitir comparação direta entre os sistemas. Embora esse modelo não represente plenamente o comportamento aerodinâmico real dos UAVs, ele foi adotado como prova de conceito, seguindo a mesma abordagem do trabalho base. A comunicação utiliza o padrão IEEE 802.11n no modo ad-hoc, operando na frequência de 2.4 GHz. Os UAVs compartilham suas localizações colaborativamente para auxiliar na construção de consciência espacial individual e atualizam seu posicionamento a cada 1,5 s. Os principais parâmetros da simulação estão sumarizados na Tabela I.

Tabela I: Parâmetros da simulação

Parâmetro	**Valor(es)**
Tempo da simulação	1200 s
# UAVs	40
Velocidade de voo	20 m/s
Nível de voo	300 ft
Modelo de mobilidade	2D Random Walk
Área do mapa	1,5 km $\times$ 1,5 km
Protocolo de comunicação	802.11n
Protocolo de transporte	UDP
Raio de comunicação	115 m
# simulações	35

C. Vetores de FDIAs

A análise da resiliência do FlySafe considerou somente um modelo de FDIA único, no qual um UAV pertencente à rede opera de maneira maliciosa e compartilha com os outros UAVs informações de localização falsas. Dessa maneira, para avaliar sua resistência, foram implementados diversos modos de FDIAs modificando-se características como intensidade (ι), frequência (f), duração (δ) e erro da informação de localização (ϵ). A implementação desses modos baseou-se em [12], no qual o erro-alvo, $\varepsilon(\phi, L_u)$, corresponde a um valor correto da informação de localização do UAV u, L_u, no instante de tempo ϕ, conforme a Equação 1. Diante da mudança de posição de u em função do tempo, cada $\varepsilon(\phi, L_u)$ sofre uma perturbação específica, $\rho(\phi, L_u)$, que representa o valor do tamanho da L_u falsa definido por uma distribuição uniforme dentro de um intervalo $[a, b]$, que varia de acordo com L_u. Assim, o erro-alvo perturbado, $\xi(\phi, L_u)$, equivale ao valor de L_u falsa injetada na rede após a aplicação de $\rho(\phi, L_u)$, tornando a detecção do ataque essencial para mitigar seus efeitos no funcionamento da rede [18].

$$\xi(\phi, L_u) = \varepsilon(\phi, L_u) + \rho(\phi, L_u) \tag{1}$$

Um conjunto de novos modelos de FDIAs foram implementados considerando que o UAV malicioso não pertence à rede. Nesse caso, o atacante intercepta as mensagens transmitidas no meio sem fio entre os UAVs legítimos. Em vez de criar uma nova mensagem, o atacante preserva as informações originais da mensagem capturada, como a identificação do UAV transmissor. Quando se deseja que o erro de posição seja fixo, o atacante altera a coordenada indicada na mensagem antes do envio para que o UAV receptor processe a localização com o erro almejado. Dessa forma, o emprego das informações de identificação originais dos UAVs pertencentes à rede nas mensagens repetidas inviabiliza a identificação do atacante por checagem de identidade. Adicionalmente, o recebimento dessas mensagens modificadas e retransmitidas pode indicar que uma determinada mensagem foi enviada com atraso ou mesmo caracterizá-la como uma mensagem antiga [23]. Logo, o objetivo principal desses ataques por repetição é injetar informações falsas na rede repetidamente, enganando os UAVs vizinhos, a fim de prejudicar o funcionamento do serviço de localização e tornar a operação dos UAVs insegura.

Para melhor análise e comparação do FlySafe com o FlySafeTI, as simulações de ambos os sistemas ocorreram em três configurações de cenários: BASELINE, com apenas UAVs honestos (NO-ATK); BASEATTK, com um UAV malicioso (MalUAV), mas sem as medidas de proteção do serviço de localização; e ATTKPROT, com um MalUAV e as medidas de proteção do serviço de localização ativadas. As configurações BASEATTK e ATTKPROT foram simuladas em cada sistema e individualmente com cada modelo de FDIA descrito na Tabela II. As métricas aplicadas são calculadas como a média de 35 simulações para atingir um intervalo de confiança de 95%.

D. Métricas de avaliação

Em apoio à avaliação, foram empregadas métricas de resiliência e desempenho para analisar e comparar a resistência do FlySafe e FlySafeTI para proverem e manterem o serviço de localização diante de vários modos de FDIAs. As métricas de resiliência permitem destacar o comportamento dos sistemas contra perturbações causadas por um MalUAV que executa um FDIA. Portanto, foram computadas Idade da Informação Incorreta (AoII), o Tempo de Consciência Espacial (ψ) e a Idade da Informação (AoI). As métricas de desempenho visam determinar a capacidade de cada UAV de alcançar e manter uma consciência espacial empregando um serviço de localização. Assim, foram computados a Taxa de sucesso do ataque (SAT), Taxa de descarte de pacotes (DPT), o Erro de localização (Ω), Número de mensagens para convergência (φ) e Atraso no reconhecimento de mudanças de localização (Υ). A Tabela III detalha cada métrica.

A adoção conjunta de métricas de resiliência e de desempenho permite uma avaliação abrangente e complementar dos

Tabela II: Configurações dos FDIAs

Modo do ataque	**Identificação**	**Parâmetros dos ataques** $(\rho(\phi, L))$				Operação regular
		Frequência (f)	Intensidade (ι)	Duração (δ)	Erro loc. (ϵ)	
Único	U1MC	Todas msg U	1 msg	Contínuo	Aleatório	0s
	U1M10	Todas msg U	1 msg	10 s	10 m	10 s
	U1M20	Todas msg U	1 msg	10 s	20 m	20 s
	U1M30	Todas msg U	1 msg	10 s	30 m	30 s
Repetitivo	R3MC	Cada msg RX	3 msg	Contínuo	Aleatório	0s
	R5M10	Cada msg RX	5 msg	10 s	10 m	10 s
	R10M20	Cada msg RX	10 msg	10 s	20 m	20 s
	R15M30	Cada msg RX	15 msg	10 s	30 m	30 s

Tabela III: Métricas de avaliação

Descrição	**Equação**
Tempo de Consciência Espacial (ψ) corresponde ao período total em que um UAV reconhece com sucesso todos os outros em sua área de cobertura.	$\psi = \sum_{t=0} \int_0 \Delta_{\lambda_{\{\Gamma=0\}}}(t)dt$
Idade da Informação (AoI) indica a atualização das informações de vizinhança dos UAVs, sendo adaptada de [8].	$AoI = \int_0 \Delta(t)dt$
Idade da Informação Incorreta (AoII) computa o período em que um UAV detém informações incorretas sobre outros, sendo uma adaptação de [24].	$AoII = \int_0 \Delta_{\lambda_{\{\Gamma>0\}}}(t)dt.$
Taxa de descarte de pacotes (DPT) representa a quantidade de pacotes descartados pelo mecanismo de segurança (PD) em relação ao total de pacotes repetidos pelo atacante (PR).	$DPT = \frac{PD}{PR}$
Taxa de sucesso do ataque (SAT) determina o sucesso do ataque a partir da relação entre a quantidade de pacotes repetidos aceitos (PRA) por um UAV e o total de pacotes repetidos pelo atacante (PR).	$SAT = \frac{PRA}{PR}$
Erro de localização (Ω) avalia a precisão na percepção da localização de um UAV vizinho no intervalo de tempo t.	$\Omega^t = \lvert d^r - d^m \rvert$
Mensagens para convergência (φ) representam a quantidade de mensagens trocadas por um UAV para alcançar a consciência espacial em cada período.	$\varphi = \sum_{\substack{t=0 \\ \Gamma>0}}^{t \leq T} (HM + IM + TM)$
Atraso no reconhecimento de mudanças de localização (Υ) equivale ao período entre a detecção de uma mudança de localização (t_i^d) por um UAV i e o momento em que um vizinho j tem ciência da nova posição do UAV (t_j^r).	$\Upsilon = t_j^r - t_i^d$

sistemas investigados. As métricas de resiliência — AoII, ψ e AoI — quantificam o impacto dos FDIAs no estado operacional da rede, evidenciando por quanto tempo os UAVs mantêm consciência espacial e com que qualidade as informações de localização chegam a cada dispositivo. Já as métricas de desempenho — SAT, DPT, Ω, φ e Υ — avaliam a eficácia dos mecanismos de detecção e mitigação, mensurando tanto a capacidade de identificar e descartar pacotes maliciosos quanto a precisão e a eficiência de comunicação mantidas sob ataque. Essa distinção permite diferenciar cenários em que o sistema detecta o ataque mas sofre degradação de desempenho daqueles em que o ataque não é detectado, mas causa impacto mínimo na consciência espacial. Dessa maneira, a análise conjunta dessas dimensões possibilita identificar os pontos fortes e as limitações de cada sistema diante dos diferentes modos de FDIAs avaliados.

IV. Análise dos Resultados

Esta seção apresenta e discute os resultados das simulações que comparam o FlySafe e o FlySafeTI diante dos oito modos de FDIAs descritos na Tabela II, além do cenário de referência sem ataques (NO-ATK). Para cada modo de FDIA, são analisadas as métricas de segurança (DPT e SAT), de consciência espacial (ψ e AoI) e de percepção de vizinhança (Ω e Υ). Todos os resultados representam a média de 35 simulações com intervalo de confiança de 95%.

A. Detecção e Mitigação de FDIAs

A Tabela IV apresenta a taxa de descarte de pacotes (DPT) e a taxa de sucesso do ataque (SAT) para todos os cenários avaliados. Diante de FDIAs únicos com erro aleatório (U1MC), o FlySafe alcançou DPT de 89,93%, enquanto o FlySafeTI atingiu apenas 48,58%. Essa diferença reflete o fato de que o mecanismo de plausibilidade espacial do FlySafe é eficaz quando os erros injetados são grandes e aleatórios, pois

frequentemente colocam a posição declarada fora do raio de cobertura do receptor. O mecanismo do FlySafeTI, baseado em *timestamp* e *nonce*, não distingue FDIAs únicos de mensagens legítimas: uma mensagem com erro aleatório mas *timestamp* válido e *nonce* inédito é aceita pelo FlySafeTI, resultando em maior taxa de sucesso do ataque. Nos demais FDIAs únicos (U1M10, U1M20 e U1M30), com erros constantes de 10, 20 e 30 m, respectivamente, ambos os sistemas falharam em detectar os ataques (DPT $\approx$ 0%), pois as posições injetadas, embora incorretas, permanecem dentro da faixa de plausibilidade espacial utilizada pelo FlySafe e são temporalmente válidas e únicas para o FlySafeTI.

Tabela IV: Análise da resistência aos FDIAs

Modo	**Cenário**	**FlySafe**		**FlySafeTI**	
		DPT (%)	SAT (%)	DPT (%)	SAT (%)
Único	U1MC	89,93	10,07	48,58	51,42
	U1M10	0,00	100,00	0,00	100,00
	U1M20	0,00	100,00	0,00	100,00
	U1M30	0,12	99,88	0,02	99,98
Repetitivo	R3MC	49,24	50,76	95,98	4,02
	R5M10	49,67	50,33	98,52	1,48
	R10M20	49,88	50,12	98,95	1,05
	R15M30	49,79	50,21	99,34	0,66

Diante dos FDIAs repetitivos, o comportamento é oposto e a diferença entre os sistemas é expressiva. O FlySafe descartou aproximadamente 49–50% dos pacotes repetidos em todos os modos. Esse valor reflete a atuação parcial do mecanismo de plausibilidade espacial: à medida que o UAV receptor e o UAV legítimo se movem, a posição contida nos pacotes repetidos (desatualizados ou com erro fixo) eventualmente se torna implausível e é descartada. No entanto, como o FlySafe não verifica o frescor das mensagens, aproximadamente metade das repetições passa pelo filtro. Em contraste, o FlySafeTI detectou e descartou mais de 95% dos pacotes repetidos em todos os modos avaliados, atingindo 99,34% no cenário R15M30. A tendência de crescimento do DPT com o aumento da intensidade do ataque indica que, quanto mais cópias do mesmo pacote são injetadas na rede, mais eficaz se torna o mecanismo de deduplicação baseado em *nonce*.

B. Consciência Espacial

A Tabela V exibe o tempo de consciência espacial (ψ) e a Idade da Informação (AoI) médios para todos os cenários. Em termos de ψ, ambos os sistemas demonstraram alta resiliência: o menor valor registrado foi de 1117,66 s, equivalente a 93,1% do tempo de operação de 1200 s. Em todos os demais cenários, ψ superou 1133 s. Esses resultados indicam que tanto o FlySafe quanto o FlySafeTI são capazes de manter a consciência espacial dos UAVs durante quase todo o tempo de missão, mesmo sob FDIAs. As medianas de ψ dos dois sistemas são estatisticamente similares na maioria dos cenários, o que é esperado: o FlySafe, apesar de não detectar FDIAs repetitivos, ainda beneficia-se do fato de que os UAVs honestos continuam trocando mensagens de localização válidas, compensando parcialmente a injeção de mensagens falsas.

A AoI apresentou comportamento similar entre os sistemas na maior parte dos cenários, com valores médios de 51 e 57 s. A exceção mais relevante ocorre no cenário U1MC com o FlySafe, cujo AoI médio sobe para 65,44 s — valor 11 s acima do BASELINE do mesmo sistema (54,99 s). Esse aumento indica que as mensagens com localização falsa e erro aleatório, quando aceitas, degradam o frescor médio das informações de vizinhança do FlySafe. O FlySafeTI, por aceitar apenas mensagens com *timestamp* válido e *nonce* inédito, manteve a AoI próxima ao BASELINE mesmo no cenário U1MC (57,12 s). Nos cenários repetitivos, ambos os sistemas apresentaram AoI similares, sem diferença estatisticamente significativa entre si.

Tabela V: Análise do impacto dos FDIAs no tempo de consciência espacial e na Idade da Informação

Modo	**Cenário**	ψ médio (s)		AoI médio (s)	
		FlySafe	FlySafeTI	FlySafe	FlySafeTI
Sem ataque	NO-ATK	1150,15	1151,26	54,99	56,86
Único	U1MC	1117,66	1147,55	65,44	57,12
	U1M10	1146,13	1145,07	51,64	51,58
	U1M20	1145,09	1146,54	55,86	55,14
	U1M30	1151,02	1144,73	53,03	55,80
Repetitivo	R3MC	1155,31	1151,82	57,10	55,90
	R5M10	1149,17	1149,77	53,82	51,01
	R10M20	1153,18	1150,91	53,13	52,96
	R15M30	1148,29	1147,45	54,17	52,41

C. Percepção de Vizinhança

O erro de localização (Ω) em ambos os sistemas manteve-se menor que 1 m nos cenários de FDIAs únicos com erros constantes e nos FDIAs repetitivos, conforme apresentado na Tabela VI. A exceção é o cenário U1MC, no qual Ω sobe para 8,52 m no FlySafe e 6,99 m no FlySafeTI, refletindo a maior taxa de aceitação de mensagens com erro elevado nesses sistemas. A diferença mais marcante entre os sistemas aparece no atraso de reconhecimento (Υ). No cenário NO-ATK, ambos apresentam valores baixos (3,58 ms para o FlySafe e 1,85 ms para o FlySafeTI). Sob FDIAs repetitivos, o Υ do FlySafe cresce progressivamente com a intensidade do ataque: de 20,19 ms (R3MC) até 39,28 ms (R15M30). Esse crescimento ocorre porque os pacotes repetidos são processados pelo FlySafe e a informação de localização falsa é utilizada como legítima, aumentando a dificuldade do sistema em reconhecer a mudança de posição à medida que há uma maior quantidade de pacotes falsificados recebidos. Por outro lado, o FlySafeTI, ao descartar repetições pelo mecanismo de *timestamp* e *nonce*, manteve Υ próximo ao BASELINE em todos os cenários com FDIAs repetitivos, sem degradação perceptível com o aumento da intensidade do ataque.

Tabela VI: Análise do erro de localização e do atraso no reconhecimento de mudança de posição

Modo	Cenário	Ω médio (m)		ϒ médio (ms)	
		FlySafe	FlySafeTI	FlySafe	FlySafeTI
Sem ataque	NO-ATK	0,67	0,66	3,58	1,85
Único	U1MC	8,52	6,99	3,79	1,78
	U1M10	0,75	0,75	5,30	1,77
	U1M20	0,78	0,81	3,71	1,79
	U1M30	0,75	0,80	3,66	1,80
Repetitivo	R3MC	0,75	0,65	20,19	2,01
	R5M10	0,77	0,65	22,02	1,85
	R10M20	0,75	0,68	26,61	1,91
	R15M30	0,78	0,71	39,28	1,96

D. Eficiência de Comunicação

As Figuras 4 e 5 apresentam o número médio de mensagens trocadas para que os UAVs alcançassem consciência espacial completa (φ) nos cenários com FDIAs únicos e repetitivos, respectivamente. No cenário de referência (NO-ATK), os dois sistemas apresentam valores praticamente idênticos: 134,68 mensagens para o FlySafe e 131,82 mensagens para o FlySafeTI, diferença de apenas 2,1%. Sob FDIAs únicos, φ variou entre 130 e 147 mensagens para o FlySafe e entre 141 e 147 para o FlySafeTI. As diferenças entre os sistemas são inconsistentes em direção — em alguns cenários o FlySafe usa menos mensagens (U1M30: 130 vs. 145), enquanto em outros o FlySafeTI usa menos (U1M10: 143 vs. 141). Esse comportamento indica ausência de tendência sistemática, confirmada pelos intervalos de confiança sobrepostos.

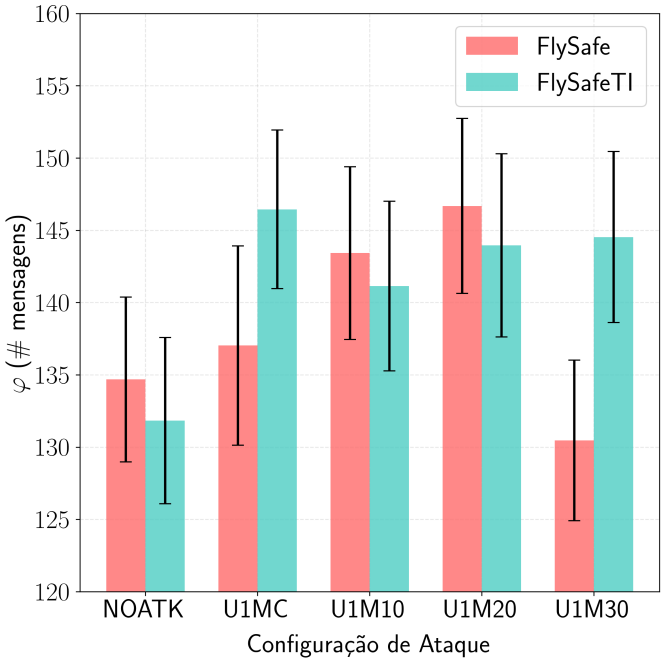

Figura 4: Convergência da consciência espacial sob FDIAs únicos.

Para FDIAs repetitivos, os valores foram igualmente próximos: 129–139 mensagens para o FlySafe e 130–143 mensagens para o FlySafeTI. Esse leve aumento de φ observado no FlySafeTI em alguns cenários repetitivos é esperado, uma vez que, ao descartar os pacotes repetidos aceitos pelo FlySafe como atualizações, o FlySafeTI precisa aguardar mensagens legítimas para reconstituir a consciência espacial, trocando quantidade de mensagens por qualidade da informação recebida. Apesar disso, em nenhum cenário a diferença absoluta entre os sistemas superou 15 mensagens, confirmando que a extensão proposta pelo FlySafeTI não introduz *overhead* de comunicação significativo em relação ao FlySafe.

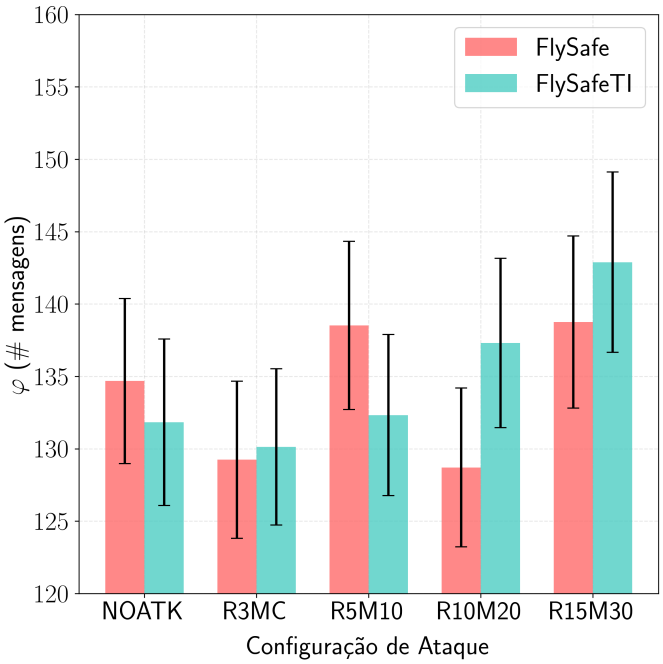

Figura 5: Convergência da consciência espacial sob FDIAs repetitivos.

V. Conclusão

Este trabalho investigou a resiliência dos serviços de localização FlySafe e FlySafeTI para redes de UAVs diante de oito modos de FDIAs — quatro únicos e quatro repetitivos — além de um cenário de referência sem ataques. A análise comparativa revelou que os dois sistemas têm comportamentos complementares e delimitados.

Diante de FDIAs únicos com erros de localização constantes, ambos os sistemas falharam em detectar os ataques (DPT $\approx 0\%$), pois as posições injetadas são espacialmente plausíveis e temporalmente válidas. No cenário de erro aleatório, o FlySafe apresentou desempenho superior (DPT = 89,93%), pois erros elevados e aleatórios frequentemente resultam em posições implausíveis, rejeitadas pelo mecanismo de plausibilidade espacial. Já o FlySafeTI mostrou DPT de apenas 48,58% nesse cenário, uma vez que o mecanismo de *timestamp* e *nonce* não distingue FDIAs únicos de mensagens legítimas.

Diante de FDIAs repetitivos, a situação se inverte: o FlySafe descartou apenas ≈50% dos pacotes repetidos (atuação parcial do filtro de plausibilidade), enquanto o FlySafeTI descartou mais de 95% em todos os modos, atingindo 99,34% no cenário R15M30. Consequentemente, o FlySafeTI manteve o atraso de reconhecimento de mudanças de localização (Υ) próximo ao BASELINE (1,85–2,01 ms), enquanto o FlySafe acumulou atrasos crescentes com a intensidade do ataque, chegando a 39,28 ms no R15M30. Em contrapartida, ambos os sistemas mantiveram consciência espacial (ψ) acima de 93% do tempo de operação em todos os cenários, e o número de mensagens para convergência (φ) foi equivalente entre os sistemas (menos de 10% de diferença), confirmando que o FlySafeTI não introduz *overhead* de comunicação significativo.

Em síntese, os resultados evidenciam que os mecanismos de detecção do FlySafe e do FlySafeTI são complementares e apresentam limitações delimitadas. O FlySafe supera o FlySafeTI diante de FDIAs únicos com erros aleatórios elevados, enquanto o FlySafeTI é significativamente mais eficaz contra FDIAs repetitivos. Entretanto, ambos os sistemas falham na detecção de FDIAs únicos com erros de localização constantes, revelando uma lacuna que demanda investigação futura. Em todos os cenários, a consciência espacial e a eficiência da comunicação foram preservadas, confirmando que a extensão proposta não compromete a disponibilidade do serviço de localização.

REFERÊNCIAS

[1] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2624–2661, 2016, doi: 10.1109/COMST.2016.2560343.

[2] Z. Xiaoning, "Analysis of military application of UAV swarm technology," in *2020 3rd International Conference on Unmanned Systems (ICUS)*, 2020, pp. 1200–1204, doi: 10.1109/ICUS50048.2020.9274974.

[3] L. Goasduff, "Why Flying Drones Could Disrupt Mobility and Transportation Beyond COVID-19," Disponível em: https://www.gartner.com/smarterwithgartner/why-flying-drones-could-disrupt-mobility-and-transportation-beyond-covid-19, may 2020, acessado em: set. 2025.

[4] D. S. Lakew, U. Sa'ad, N.-N. Dao, W. Na, and S. Cho, "Routing in flying ad hoc networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, 2020. [Online]. Available: https://doi.org/10.1109/COMST.2020.2982452

[5] O. Ceviz, S. Sen, and P. Sadioglu, "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024, doi: 10.1109/COMST.2024.3515051.

[6] N. Bai, X. Hu, and S. Wang, "A survey on unmanned aerial systems cybersecurity," *Journal of Systems Architecture*, vol. 156, p. 103282, 2024, doi: 10.1016/j.sysarc.2024.103282.

[7] M. Ahmed and A.-S. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adaptive Systems Modeling*, vol. 8, no. 1, p. 4, 2020.

[8] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, and S. Ulukus, "Age of information: An introduction and survey," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 5, pp. 1183–1210, 2021, doi: 10.1109/JSAC.2021.3065072.

[9] A. d. S. Batista and A. L. dos Santos, "Resilient UAVs location sharing service based on information freshness and opportunistic deliveries," *Pervasive and Mobile Computing*, vol. 111, p. 102066, 2025, doi: 10.1016/j.pmcj.2025.102066.

[10] E. Mousavinejad, F. Yang, Q.-L. Han, Q. Qiu, and L. Vlacic, "Cyber Attack Detection in Platoon-Based Vehicular Networked Control Systems," in *27th International Symposium on Industrial Electronics*, ser. ISIE. New Jersey, USA: IEEE, 2018, pp. 603–608. [Online]. Available: https://doi.org/10.1109/ISIE.2018.8433814

[11] M. Jagielski, N. Jones, C.-W. Lin, C. Nita-Rotaru, and S. Shiraishi, "Threat Detection for Collaborative Adaptive Cruise Control in Connected Cars," in *11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec. New York, USA: Elsevier, 2018, pp. 184–189. [Online]. Available: https://doi.org/10.1145/3212480.3212492

[12] B. Ko and S. H. Son, "An Approach to Detecting Malicious Information Attacks for Platoon Safety," *IEEE Access*, vol. 9, pp. 101 289–101 299, 2021.

[13] E. Andrade, F. Matos, and A. Santos, "A virtual models-based CAVs platoon resilient to network and sensor attacks," *Ad Hoc Networks*, vol. 149, p. 103225, 2023.

[14] I. Anagnostis, P. Kotzanikolaou, and C. Douligeris, "Understanding and Securing the Risks of Uncrewed Aerial Vehicle Services," *IEEE Access*, vol. 13, pp. 47 955–47 995, 2025.

[15] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad hoc networks*, vol. 133, p. 102894, 2022.

[16] E. P. de Freitas, L. A. L. da Costa, C. F. E. de Melo, M. Basso, M. R. Vizzotto, M. S. C. Corrêa, and T. D. e Silva, "Design, Implementation and Validation of a Multipurpose Localization Service for Cooperative Multi-UAV Systems," in *International Conference on Unmanned Aircraft Systems*, ser. ICUAS. New Jersey, USA: IEEE, 2020, pp. 295–302. [Online]. Available: https://doi.org/10.1109/ICUAS48674.2020.9213898

[17] K. Molugaram and G. S. Rao, "Chapter 5 - Curve Fitting," in *Statistical Techniques for Transportation Engineering*, K. Molugaram and G. S. Rao, Eds. Butterworth-Heinemann, 2017, pp. 281–292. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128115558000052

[18] D. Kilinç and H. Çelik, "Blockchain-Based Data Sharing within Unmanned Aerial Vehicles Swarm," in *10th International Conference on Recent Advances in Air and Space Technologies*, ser. RAST. New Jersey, USA: IEEE, 2023, pp. 01–04. [Online]. Available: https://doi.org/10.1109/RAST57548.2023.10197989

[19] Z. Zhang, C. Hsu, M. H. Au, L. Harn, J. Cui, Z. Xia, and Z. Zhao, "PRLAP-IoD: A PUF-based Robust and Lightweight Authentication Protocol for Internet of Drones," *Computer Networks*, vol. 238, p. 110118, 2024, doi: 10.1016/j.comnet.2023.110118.

[20] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020, doi: 10.1109/TVT.2020.3000576.

[21] Consortium NS-3, "NS-3 Discrete-event Network Simulator," Disponível em: https://www.nsnam.org, nov 2025, acessado em: 17 de nov. de 2025.

[22] F. A. Administration, "Operation of Small Unmanned Aircraft Systems Over People," https://www.faa.gov/sites/faa.gov/files/2021-08/OOP_Final%20Rule.pdf, 2021, (accessed 8 august 2023).

[23] K. Soltani, F. Corò, P. Chatterjee, and S. K. Das, "DATAMUt: Deterministic Algorithms for Time-Delay Attack Detection in Multi-Hop UAV Networks," in *27th International Conference on Distributed Computing and Networking*, ser. ICDCN '26. New York, USA: ACM, 2026, pp. 113–122, doi: https://doi.org/10.1145/3772290.3772293.

[24] A. Maatouk, S. Kriouile, M. Assaad, and A. Ephremides, "The Age of Incorrect Information: A New Performance Metric for Status Updates," *IEEE/ACM Transactions on Networking*, vol. 28, no. 5, pp. 2215–2228, jul 2020, doi: 10.1109/TNET.2020.3005549.