Analyzing The FlySafe System Face to Malicious UAVs Playing Black Hole Attacks

Agnaldo Batista[1], **Aldri Santos**[1,2]

Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR

Depto. de Ciência da Computação (DCC) – UFMG

asbatista@inf.ufpr.br, aldri@dcc.ufmg.br

Abstract. *Many of UAV networks demand dynamic structural topological services, such as sharing UAV location information, to provide UAV-coordinated and safe flight. More than just fault-tolerant, this basic service must be resilient to black hole attacks that aim corrupt and damage the UAV network topology by ignoring the neighborhood information. This work analyzes the resilience of the FlySafe system for protecting UAV networks against malicious UAV performing black hole attacks when they disregard sharing location information about its neighbors in a swarm environment. The FlySafe system relies on opportunistic approaches like epidemic and direct delivery, and enhancing neighbor discovery process. A simulation evaluation with NS3 showed the security of the location service, particularly in detecting and segregating black hole attacks from network operation with an average accuracy of 96%. Further, FlySafe exhibited an improvement in overall neighborhood perception in about 49.9%.*

1. Introduction

Unmanned aerial vehicles (UAV), a.k.a drones, have been gaining popularity worldwide with applications in domains such as agriculture [Delavarpour et al. 2021], health emergency services [Kramar 2020], and communication during natural disasters [Tian et al. 2023]. The global UAV market size is projected to surpass USD 182 million by 2033. Such increase is driven by advancements in UAV technology, like battery efficiency, AI-powered autonomous systems, and enhanced imaging sensors [GVR 2026]. Characteristics like high maneuverability, efficient communication, and portable carrying equipment enables the application of UAVs in green buildings, fault detection and diagnosis, city infrastructure deployment, public traffic dispatching, smart transportation, emergency delivery and so on. Further, there are initiatives around UAV designs, various application scenarios, lifecycle carbon footprint quantifications, standardization and regulations for LAE [Huang et al. 2024, Zhou 2025].

UAV networks still have a long way to go in supporting reliable basic services, mainly due to their particular mobility and maneuverability behavior. Because a safe air operation requires each UAV knows others around during flight, keeping such space awareness calls for a resilient exchange of information. *Unlike fault-tolerant systems, resilient systems aim to provide greater adaptation to threats to their operation* [Batista and Dos Santos 2024, Farooq and Zhu 2025]. Since UAV network-based services rely on safe flights, obstacles in urban environments and other vehicles flying in the same area put in danger a reliable air operation. The collection of UAVs must keep

their spatial awareness to accomplish a coordinated flight. The absence of such conditions leads them to disregard a safe distance from each other, potentially causing collisions during air maneuvers [Zhang et al. 2018]. UAVs usually get their global localization from Global Positioning System (GPS) signals or a known landmark [Lima and Pereira 2021] and they must share such information to attain spatial awareness. Hence, location information emerges as crucial to provide successful services. In this way, UAVs refusing to share its neighbor's location jeopardizes others' spatial awareness, hampering resilient information sharing.

At the same time, the range of threats to the security of UAV communications has also increased [Wang et al. 2021]. As these UAVs have limited computational resources, there is a constant demand for technological advances to enhance the security of high-mobility UAV networks, like FANETs [Tsao et al. 2022]. The current initiatives of standardization on UAV operation by government agencies and other institutions still fail to protect these vehicles from several threats. Further, the malicious use of UAVs brings up a severe risk to air operations. They perform passive attacks like eavesdropping to get information from a system or active attacks like impersonation and false data injection (FDI) to alter system behavior and hence jeopardize UAV operations [Hernandez et al. 2023].

It is imperative to adopt measures to prevent and mitigate potential threats that could jeopardize UAV operations due to the sensitive and valuable data transmitted to support UAV network operations, particularly those that disregard the location information received from neighboring UAVs. Whenever a malicious UAV omits its neighborhood information when interacts with others, it performs a Black hole (BH) attack, giving that it indicates to its neighbors the absence of UAVs in its coverage area. Therefore, such a false void space around it jeopardizes message forwarding. The works usually focus on security issues of BH attacks by applying intrusion detection systems (IDS) based on machine learning [Tlili et al. 2024, Hadi et al. 2024], rule-based IDS [Sedjelmaci et al. 2017] trust assessment [Ren et al. 2022, Yang et al. 2023], and authentication through blockchain technology [Yang et al. 2023, Qureshi et al. 2024]. Although the proposed approaches face threats like black hole attacks, they commonly target attack detection and mitigation, but disregard resilience issues to adapt their operation to threats.

This work aims to analyze the resilience of the FlySafe system, an UAV location service against black hole attacks. Unlike GPS spoofing attacks that create incorrect signals causing UAV to change its position [Tsao et al. 2022], we consider a BH attacker that discards the information received from honest UAVs. Therefore, whenever the attacker interacts with others, it shares no neighborhood information, thus jeopardizing their spatial awareness. FlySafe [Batista and Santos 2025] explores an active collaboration among UAVs by applying jointly opportunistic approaches (OPPAPPS) epidemic and direct delivery in order to identify such attackers and improve UAV spatial awareness. The integration of individual spatial awareness brings resilience to network operations, overcoming the lack of neighborhood information due to such threat. We have evaluated the FlySafe performance in the NS3 simulator under three simulation settings. Results showed the security of the location service, particularly in detecting and isolating black hole attacks from network operation with an average accuracy of 96%. Further, FlySafe achieved an improvement in overall neighborhood perception in about 49.9%.

This paper is organized as follows: Section 2 presents related work. Section 3

describes the FlySafe system and details its operation. Section 4 presents a security evaluation against BH attacks. Section 5 concludes the work and presents future direction.

2. Related Work

A range of scientific efforts have addressed to ensure UAVs information sharing due to network attacks by applying intrusion detection systems (IDS) based on machine learning, such as in [Tlili et al. 2024, Hadi et al. 2024], rule-based IDS like in [Sedjelmaci et al. 2017], trust assessment as in [Ren et al. 2022, Yang et al. 2023], and authentication through blockchain technology like in[Yang et al. 2023, Qureshi et al. 2024].

In [Tlili et al. 2024], an exhaustive distributed intrusion detection systems (E-DIDS) based on artificial intelligence (AI) operates to enforce UAVs security against attacks like GPS spoofing, GPS jamming, flooding, replay and man-in-the-middle (MiM) by distributing the workload across interconnected IDSs deployed on a UAV. E-DIDS employs an LSTM trained with labeled data to tolerate the presence of abnormal data during training instead of normal data. The proposed methodology deploys IDS on various edges within the UAV systems and network to achieve an accurate detection and security, where each IDS segment monitors and analyzes a particular subsystem or network or the communication protocol within the network. Therefore, these segments collaborate and share knowledge to identify and detect potential intrusions or malicious behavior according to the datasets employed for system training. The distributed segments of E-DIDS within a UAV improves vehicle security and operation. However, IDSs accuracy requires tailored labeled data that fits the protected UAV sensor.

In [Hadi et al. 2024], an autonomous collaborative IDS for UAV networks (UAV-CIDS) employs a feedforward convolutional neural network (FFCNN) to identify zero-day and known attacks. Further, UAV-CIDS training relies on UAVIDS [Alipour-Fanid et al. 2019], a dataset that contains real world encoded Wi-Fi traffic logs of three popular UAVs: DBPower UDI, parrot Bebop, and DJI spark. The FFCNN architecture comprises a hybrid activation function combining rectified linear unit (ReLU) and tanh linear unit (TaLU) to capture positive and negative feature values. The distributed operation allows CIDS to face incomplete detection of coordinated attacks, thus protecting the entire UAV networks, i.e, it prevents a compromised UAV from spreading to the entire network or affecting other nodes. Although UAV-CIDS detects zero-day attacks, it depends on a traffic data exchanged by specific UAV devices.

In [Sedjelmaci et al. 2017], an hierarchical intrusion detection and response scheme operates at the UAV and ground station levels to detect malicious anomalies like false information dissemination, GPS spoofing, jamming, and black hole and gray hole attacks. The intrusion detection runs on UAVs level by adopting rules-based detection and anomaly detection techniques, while intrusion response mechanism runs at the ground station level. A set of detection and response techniques allows UAV to monitor other behaviors and classify them according to the detected cyber-attack in an appropriate list as normal, abnormal, suspect, and malicious. Each UAV operates in a promiscuous monitoring mode to hear all packets within its radio range and observe the behavior of UAVs that traverse its neighboring area. Further, each UAV monitors its neighbors performing a mutual monitoring. In the face of a malicious or abnormal classification, the UAV deliv-

ers the decision making to the ground station, which assess false positives and negatives. Isolating malicious UAVs from network ensure a secure aerial environment. However, the scheme disregards additional procedures to enhance UAV spatial awareness due to lacking of neighborhood information.

In [Ren et al. 2022], an optimized link state routing (OLSR) protocol called Secure-OLSR (S-OLSR) runs to detect black hole attacks. S-OLSR evaluates node trust value through fuzzy logic, optimizes the multipoint relay node (MPR) selection algorithm in OLSR in order to improve the security of the protocol. Thus, each node holds a trust table of all its neighboring nodes and whenever a newly added neighbor successfully establishes link communication with the node, it sets neighbor trust value to zero in a range of extremely dangerous (-1) to absolutely safe (1). Throughout operation, nodes monitor the amount of exchanged messages of their neighbors. When it remains unchanged compared with the previous period, the neighbor is perceived as honest. At the time that the ratio of forwarding and receiving packets of a neighboring node is less than a security level, it suggests the neighbor node may discard packets, i.e., it behaves as a Bh attacker. While trust helps to know UAVs behavior when exchanging messages, sparse environments and vehicles mobility may inhibit interactions, compromising thus trust evaluation.

In [Yang et al. 2023], a blockchain-based UAV trusted self-organizing networking mechanism (BC-UTSON) runs to enhance internal security of UAV swarms. BC-UTSON relies on a practical Byzantine fault tolerance (U-PBFT) to provide a lightweight consensus and real-time full-node trustworthiness evaluation. The consensus takes place through the cluster leaders to reduce message overhead. A blockchain-based multiweighted subjective logic (BMWSL) scheme executes to identify malicious UAV nodes based on the trustworthiness evaluation. BMWSL employs blockchain technology to detect malicious UAVs accurately and sensitively by classifying UAVs behaviors in verifiable or unverifiable. Only verifiable behaviors are uploaded to blockchain by a smart contract and are available for other UAVs. Also, BMWSL supports the trusted path quality-aware dynamic routing (TPDR) mechanism to prevent data from routing through malicious nodes. In this way, as a distributed routing protocol, each node in TPDR determines only the next hop of data forwarding in order to achieve a secure transmission path. Dynamic path changes in time avoid malicious nodes, thus keeping a low routing overhead. Emulation results show a high performance for the BMWSL. Though, heterogeneous and dense networks environments may lead to a network overhead, compromising UAVs regular operation.

In [Qureshi et al. 2024], UAVs run a trust establishment mechanism for flying ad hoc network (FANET) and authentication system through Blockchain to face security threats like black hole attacks. The model assesses UAVs trust through direct, indirect (reputation), cumulative trust values. Each UAV keeps a packet profiler to check UAVs behavior by evaluating the packet traffic based on data received and drop rate, direct and indirect trust evaluation. Devices authentication takes place through blockchain to leverage the immutability and decentralization features to establish and manage UAV identities securely. Each UAV is assigned with a public-private key pair, whose the public key is employed to generate a public address, which identifies it over the blockchain, while the private key is used to sign transactions. The integration of this model with ground stations enable record keeping and decision-making processes. The mechanism ensure FANET operates with authenticated and trusted UAVs, but sparse network environments

may jeopardize trust evaluation.

In nutshell, most of UAVs studies disregard the potential failures due to an authenticated and trusted UAV whenever it omits its neighborhood information to others, i.e., plays as a black hole attacker. Thus, attack detection and mitigation in UAV networks is essential to support UAV regular operation. Table 1 summarizes by comparing the related work limitations. To address these constraints, we argue that opportunistic approaches allow leveraging the freshness of UAV location, and assisting in accurate and effective decision-making. Thus, it is required to assess the performance of a UAV location service to verify its effectiveness in achieving and holding spatial awareness under threats like black hole attacks.

Table 1. Comparison of related work limitations

Reference	Based on	Addressed attack(s)	Detection capabilities	Centralized operation	Device Mobility	Resilience
[Tlili et al. 2024]	LSTM	GPS spoofing and jamming, flooding replay, and MiM	Anomaly-based IDS	×	✓	×
[Hadi et al. 2024]	FFCNN	Zero-day	Anomaly-based IDS	×	✓	×
[Sedjelmaci et al. 2017]	Intrusion detection	FDI, GPS spoofing, jamming, BH and gray hole	Rule-based IDS	✓	✓	×
[Ren et al. 2022]	Trust	BH	Fuzzy logic	✓	×	×
[Yang et al. 2023]	Authentication and consensus	BH	Subjective logic	×	✓	Next hop path
[Qureshi et al. 2024]	Authentication and trust	Bad mouth, Denial of Service, and on-off	Trust evaluation	✓	×	×
Our proposal	OPPAPPS and Individual spatial awareness	BH	Deny neighbor information	×	✓	OPPAPPS

3. The UAV Location-Sharing Service

This section briefly presents the FlySafe system for UAV location-sharing proposed by [Batista and Santos 2025], describing its main characteristics and operation under black hole attacks. Further, it details attack detection and mitigation applied strategies.

The FlySafe system operates between network and application layers to allow UAVs to share their location information. UAVs make distributed and autonomous decisions to announce their presence and mobility behavior, which takes place in two phases: *Neighbor discovery* and *Neighbor maintenance*. A network discovery protocol jointly with opportunistic approaches like crowdsourcing and direct delivery enables UAVs to identify close devices and update such information. All exchanged messages carry UAV location and neighborhood information, being subject to prior analysis by each UAV to identify missing neighborhood information. The joined approaches operation enables resilient location information service against BH attacks, enabling UAVs to achieve and keep spatial awareness.

We explore the scenario shown in Figure 1, where FlySafe performs over UAVs interconnected by wireless communication and denoted by $\mathcal{U} = \{u_1, u_2, u_3, ..., u_j\}$, such

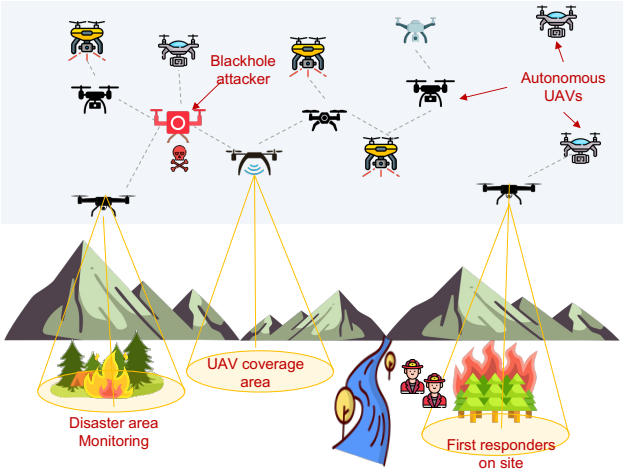

Figure 1. UAVs operation environment with black hole attacker

that $u_j \in \mathcal{U}$. All UAVs hold communication and processing resources to disseminate data, and each one owns a unique and exclusive address (*Id*) to identify it in all time slots t. Further, each UAV gets its location information from GPS, and the wireless channels connecting them run by a LoS wireless link. A UAV neighborhood $\mathcal{W}$ encloses a set of distinct tuples $\langle Id_u, t, L_t^u, q_u, h_u, a_u, d_u, s_u \rangle$, so that each one retains the information about a close vehicle in a slot t, such that

$$\mathcal{W} = \{\langle Id_1, t_1, L_{t_1}^{u_1}, q_1, h_1, d_1, s_1 \rangle, \langle Id_2, t_1, L_{t_1}^{u_2}, q_2, h_2, d_2, s_2 \rangle, ..., \langle Id_j, t_1, L_{t_1}^{u_j}, q_j, h_j, d_j, s_j \rangle\}.$$

The location information L_t^u consists of a tuple $\langle x_t^u, y_t^u, z_t^u \rangle$ indicating the position of a UAV in a 3D space. The *quality flag* q_u denotes the freshness of the collected neighbor location information. The *hop flag* h_u indicates the existence of a neighbor in a UAV coverage area. The *distance* d_u is the Euclidean distance of the neighbor UAV. The state s_u holds a neighbor condition - regular or malicious. By simplicity, we consider a turned-off or stationary UAV on the ground out of the network. Further, any UAV can eventually carry out a black hole attack by omitting neighborhood information, thus jeopardizing system operation. The UAV mobility pattern leads vehicles to simultaneously be a neighbor of one or more UAVs according to location. After discovering its neighborhood, UAVs update such information by establishing network connections with known neighbors to exchange messages. For instance, as shown in Figure 1, UAV u_3 establishes connections with UAVs u_2, u_6, u_7, u_8, which also belong to others neighborhoods.

Since in mobile networks, identifying devices connected to the network generally relies on frequently sending hello messages [Lakew et al. 2020], FlySafe targets dynamic scenarios, as depicted in Figure 1, and thus it employs a *Hello message* (HM) and a *Identification message* (IM) to make neighbor discovery. In this way, when a UAV with FlySafe starts operating it announces its presence by broadcasting an HM, which carries its identification *Id*, location L, and neighborhood *NL*. The system adopts the duration λ_t of time slots t to 1.5 seconds, i.e., three times the message report time employed by ADS-B systems [ICAO 2018] with crewed aircraft. Upon receiving an HM, a neighbor UAV responds with an IM, a unicast message carrying its *Id*, L, and *NL*, and updates its *NL* with the announcer UAV information. Thus, when receiving an IM, the announcer

UAV registers the neighbor in *NL*, hence improving its spatial awareness.

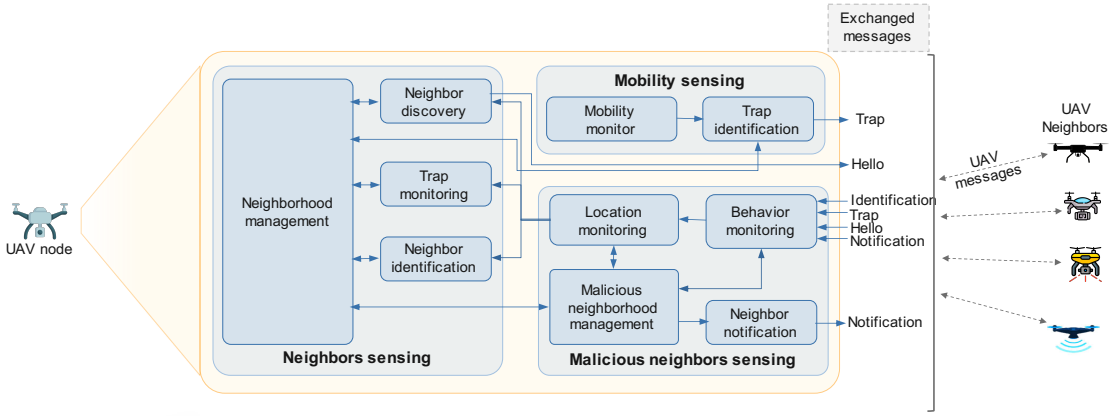

Figure 2. The Flysafe architecture for resilient sharing information

FlySafe relies on UAVs' mobility as a trigger to UAVs keep their spatial awareness. Thus, UAVs update neighbors' information when they move to a new position. Further, a *quality flag* q compels neighbor list updates. Hence, whenever a UAV moves to a new location, it notifies one-hop neighbors by a *Trap message* (TM), a unicast message carrying UAV new L, *Id*, and *NL*. Upon receiving a TM, a UAV updates its *NL* with the received information.

For providing resilient information sharing, we employ the FlySafe architecture [Batista and Santos 2025], which comprises three modules, as depicted in Figure 2, where the *Neighborhood Sensing* module makes neighbor discovery and maintains UAV awareness about others in its coverage area; the *Mobility Sensing* module warns UAV neighbors about its location changes; the *Malicious Neighborhood Sensing* module checks received messages to identify UAVs that disregard sharing location information about its neighbors, thus performing black hole attacks, i.e., although the attacker receives neighbor location information, it omits its neighborhood information while interacting with others. As presented in [Batista and Santos 2025], when a malicious UAV shares neighborhood manipulated yet plausible location information, it performs an FDI attack, and can affect the accuracy of the proposed mechanism.

The *Malicious neighborhood sensing* module (MS) inspects the received messages for a UAV disregarding its neighborhood information. Algorithm 1 describes its operation, where initially UAVs create a Suspect List (SL) to hold malicious neighboring UAVs (*l*.1). While operating, whenever a UAV u receives a message different an announcement, and with an empty NL (*l*.2-4), it then suspects the message sender (n_s) and alerts its neighbors about UAV n_s by a suspicion message (SM) and adds it in NL (*l*.6-8). When UAV n_s is already a suspect neighbor, UAV u selects close neighbors from a sliding window (SW) and asks them about the suspect UAV by a check message (SC) (*l*.11-12). Case UAV n_s is a known neighbor from others, UAV u blocks it and warns them by a BN (*l*.13-17). Similarly, when the message initially received carries a non-empty NL and comes from a suspect UAV n_s, UAV u turns UAV n_s honest by removing it from SL. It then warns others by a regular operation message (RM) (*l*.21-26).

UAVs build the sliding window to enhance their spatial awareness whenever they interact with a suspicious node sharing no neighbor information. As seen in Figure 3(a),

Algoritmo 1: Black hole attacks analysis

Data: u (UAV), n (Neighbor UAV), NL (Neighbors List), L (Location Information), SL (Suspects List), SM (Suspicion Message), CM (Check Message), BM (Blocking Message), RM (Regular Message)

```
1  SL(u) ← 0                                                    // Create a suspect list (SL)
2  while (u = ON) do
3      u ← L(n) + NL(n)
4      if (NL(n) = ∅) AND (!Announce_u(L(n) + NL(n))) then
5          n_s ← n
6          if (IsHonest(n_s) = True) then
7              Send SM(n_s) ∀ n ∈ NL(u) − n_s                    // Notify neighbors about a suspect UAV
8              SL(u) ← n_s                                      // Make neighbor suspicious
9          else
10             if (IsSuspect(n_s) = True) then
11                 nl(u) ← slidingWindow(n_s,u)                 // Get neighbors inside a sliding window
12                 for ∀ n ∈ NL(u) − n_s do
13                     Send CM(n_s)                             // Request neighbors from UAVs inside window
14                 end
15                 if (n_s ∈ NL(NL(u))) then
16                     Block(n_s)                               // Block a suspect node
17                     n_b ← n_s
18                     Send BM(n_b) ∀ n ∈ NL(u) − n_b           // Notify neighbors about a blocked node
19                 end
20             end
21         end
22     else
23         if (IsSuspect(n) = True) then
24             n_s ← n
25             Remove n_s from SL(u)                            // Remove a suspect node from SL
26             if (NL(u) ≠ ∅) then
27                 Send RM(n_s) ∀ n ∈ NL(u) − n_s               // Notify nodes about a status change
28             end
29         end
30     end
31 end
```

an honest UAV u interacts with a suspicious UAV s playing a black hole attack. Given that s disregard neighbor information when sharing its location, u rules a sliding window encompassing the area resulting from the intersection of their coverage areas. Then, UAV u identifies its neighbors into the SW area and query them about their neighborhood. Therefore, UAV u can infer the disregarded neighborhood by the suspicious UAV s. Such strategy raises neighbor discovery of UAV u, thus improving location service resilience.

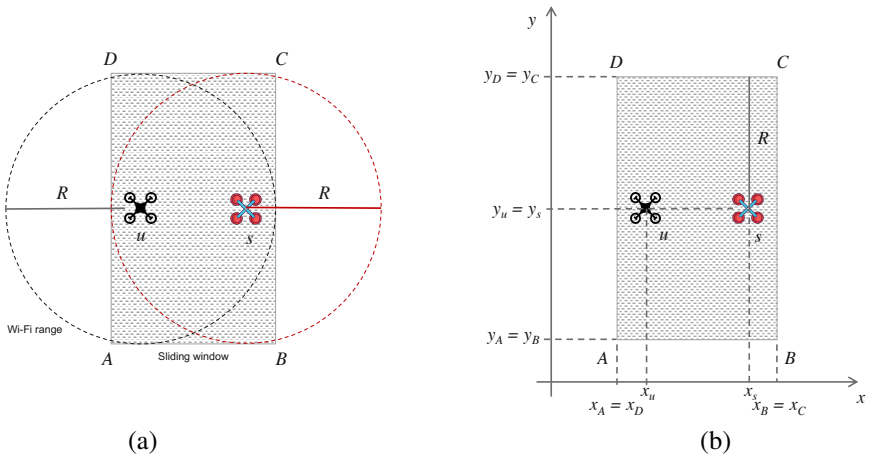

Figure 3. SW for neighbor discovery better. (a) Overview. (b) Construction

A UAV u establishes the sliding window coordinates based on its transmission range R and the location of both UAVs, u and s, denoted by $L_u = [x_u, y_u, z_u]$ and $L_s = [x_s, y_s, z_s]$, respectively. It disregards z-axis coordinates, giving that lower and higher values are limited by R. As shown in Figure 3(b), the coordinates of the SW correspond to the coordinates of its vertices A, B, C and D. Therefore, coordinates of A = ($x_s - R$, $y_u - R$), B = ($x_u + R$, $y_u - R$), C = ($x_u + R$, $y_u + R$), and D = ($x_s - R$, $y_u + R$). Figure 4 shows sliding windows positioning according to the UAV location. In Figures 4(a) and (b), UAVs are vertical and horizontal aligned, respectively. On the other hand, UAVs are misaligned in Figures 4(c) and (d), thus reducing window size.

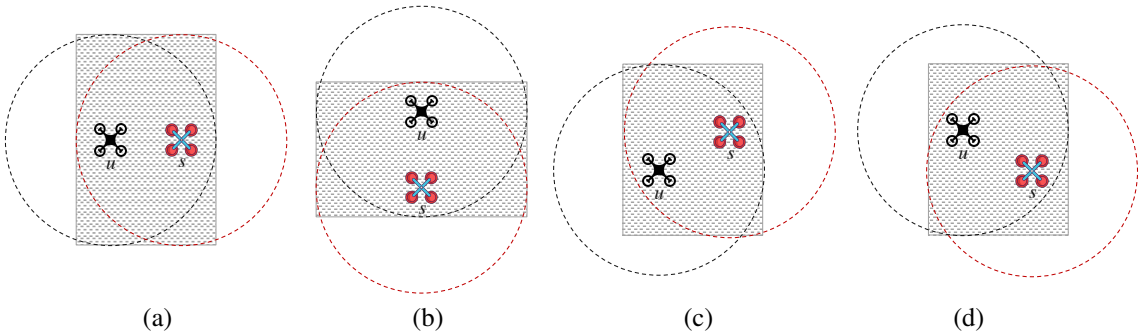

Figure 4. SW according to the UAVs positioning. (a) Vertical aligned. (b) Horizontal aligned. (c) suspicious above right. (d) Suspicious below right

An example of the location service adaption under a BH attacker sharing no neighborhood information is shown in Figure 5. UAV u_1 interacts with BH attacker s, which sent its own location information only. The neighborhood of u_1 is $\mathcal{W}_1 = \{u_2, u_6, u_7, u_8, s\}$, while $\mathcal{W}_s = \{u_1, u_2, u_3, u_4, u_5, u_6\}$ encompasses neighbors of BH attacker. Given that s disregard $\mathcal{W}_s$ whenever it shares its location, u_1 builds a sliding window over the intersection of its coverage area with that of s. Next, it looks for its neighbors inside the sliding window area and finds u_2, u_6, and s. Then, u_1 direct requests the neighborhood for u_2 and u_6. Upon receiving messages from these UAVs, $\mathcal{W}_1$ increases of u_3 and u_5, both are two hop neighbors, and becomes $\mathcal{W}_1 = \{u_2, u_3, u_5, u_6, u_7, u_8, s\}$. Since u_4 is only to $\mathcal{W}_s$, other UAVs remain unaware of it.

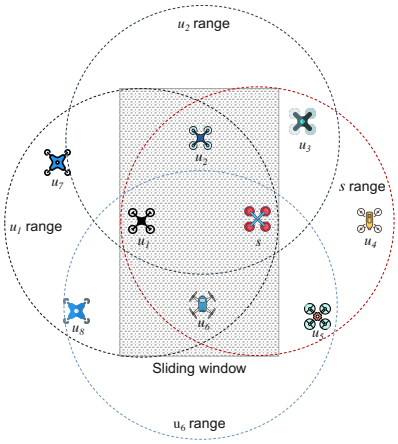

Figure 5. SW application

4. Evaluation methodology

This section presents the methodology applied for evaluating FlySafe security, performance and resilience against BH attacks in a simulated environment. We employed the FlySafe system developed in the NS-3 network simulator version 3.34 [NS-3 2022], made given adaptation and developed the black hole attacks. We applied the setting parameters shown in Table 2. The exploited scenario resembles a rescue application supported by

UAVs swarm, in which the applied parameters seek to envision real operating conditions. A disaster-hit area of 1.5 km $\times$ 1.5 km is under the surveillance of a swarm of 40 UAVs. They own WiFi technology IEEE 802.11n with a communication range of nearly 115 m. Further, all UAVs fly at flight level 300 ft, which means a realistic flying height for UAVs [Administration 2021], and move at a constant speed of 20 m/s. Each UAV follows a 2D Random walk mobility model, updating its positioning every 1.5 s to collect environmental data and cooperatively sharing its location information to support building individual spatial awareness. Although mobility models are not best suited for evaluating the service performance in FANETs since they do not represent the natural behavior of UAVs, we adopted such a model as a proof of concept.

Table 2. Simulation Setup

Parameter	**Value(s)**	**Parameter**	**Value(s)**
Simulation time	1200 s	PHY/MAC Protocol	802.11n
Map area	1.5 km $\times$ 1.5 km	Communication range	115 m
Flight level	300 ft	Propagation Model	Free-space
Number of UAVs	40	Antenna Type	Omni-directional
Mobility Model	2D Random Walk	# malicious node	0, 1
Flight speed	20 m/s		

Based on [Hesford et al. 2024], we have established a three-step methodology for evaluating FlySafe. During each simulation, we randomly set up one UAV to exchange messages disregarding neighborhood information to deny network information to others, thus hindering them from achieving spatial awareness. Therefore, that selected malicious UAV (MalUAV) mimics a black hole attack to jeopardize others' operations, as also shown in Figure 1. Lastly, we checked for the absence of neighborhood information in all received messages as a trigger to detect a BH attacker. When information is missing, the transmitter UAV becomes suspect and may be blocked in the case of a repeating behavior.

We made three simulation settings of such a scenario enable analysis and comparisons: **BASELINE:** FlySafe with only honest UAVs; **ATTKSIM:** FlySafe with one MalUAV, but without protection measures; and **ATTDKEF:** ATTKSIM with protection measures activated. Each simulation time corresponds to the operation of 1200 s and the exhibited results mean to the average over 35 simulation runs, which offers a confidence interval of 95%.

We analyzed the system behavior through a set of **security**, **performance** and **resilience metrics** in order to assess its ability to provide and keep a location service in the face of MalUAVs performing black hole attacks. As detailed in Table 3, For security assessment against black hole attacks, we measure *Recognition Convergence Rounds* (RCD), *UAV Blocking Time* (UBT), and also True Negative (TN), True Positive (TP), False Negative (FN), and False Positive (FP) rates to verify the precision on attacks detection; for performance assessment, we measure *Convergence Rounds* (CRD) and *Neighbor discovery error* (NDE); and for system resilience assessment, we measure the *Age of Incorrect Information* (AoII), the *Spatial Awareness Time* (SAT), and the *Rounds to Improve Spatial Awareness* (RIA).

Table 3. Applied metrics for FlySafe resilience and security assessment

Goal	Metric	Description	Equation
Security	**RCD**	Computes the amount of transmitted messages – suspicion messages (SM) and check messages (CM) – to recognize a suspicious UAV.	$RCD = SM + CM$
	UBT	Assesses the blocking time of a malicious UAV, i.e., the period between the suspicion of a UAV (t_s) until the confirmation of its malicious behavior (t_s).	$UBT = t_s - t_c$
Performance	**CRD**	Computes the amount of sent messages – Hello messages (SM), Identification messages (IM), and trap messages (TM) – to allow a node to achieve spatial awareness.	$CRD = HM + IM + TM$
	NDE	Determines the erroneous neighborhood estimates over a time interval t.	$NDE^t = W_j^t - W_{\mathcal{S}}^t$
Resilience	**SAT**	Indicates a UAV spatial awareness condition by the period a UAV is aware of its neighbors.	$SAT = \int_0^{\mathcal{T}} \Delta_{\lambda_{\{NDE=0\}}}(t)dt$
	AoII	Adapted from [Maatouk et al. 2020], it measures the period a UAV holds incorrect neighborhood information.	$AoII = \int_0^{\mathcal{T}} \Delta_{\lambda_{\{NDE>0\}}}(t)dt$
	RIA	Computes the amount of sent messages – neighbor request (NR) and neighbor delivery (ND) – to improve spatial awareness due to the presence of a blocked UAV in the neighborhood.	$RIA = NR + ND$

4.1. Results and Analysis

In this section, we show and discuss the achieved results during simulations. For some metrics, we computed the average, the maximum, and the minimum values for all simulations. For the other metrics, computed only the average value.

We started by analyzing FlySafe security through TP, TN, FP, and FN in the ATTKDEF configuration. As shown in Figure 6, in average, FlySafe correctly classified 96% of benign UAVs (TN), which corresponds to more than 38 nodes in each simulation, while the Black hole attacker was always correctly identified by honest nodes (TP = 2.5%). Given that detection of BH attackers relies on no shared neighborhood, eventually benign UAVs flying out of range of others may be mistaken for attackers due to the absence of neighbor information. In this sense, FlySafe incorrectly classified 1.5% of benign UAVs as malicious (FP). Further, all nodes assigned as suspicious were subsequently classified as malicious and blocked. Therefore, such results indicate that the location service operate regularly even under Black hole attacks.

A BH attacker in the network disregarding neighbor information when exchange messages with others UAVs jeopardizes their spatial awareness. Therefore, in real environments, an improvement in the neighbor discovery process becomes crucial to keep a secure UAVs operation. However, such a behavior augments energy consumption and reduces operating time. Thence, there is a need to study and consider a balance between spatial awareness maintenance and energy consumption to improve FlySafe operation in these conditions. Furthermore, detection of BH attackers in dynamic network environments is far from a trivial operation. In this work, we rely on the absence of neighborhood information as an indication of a BH malicious activity. Nevertheless, such strategy can be improved by adopting spatiotemporal validation mechanisms based on trajectory

consistency verification and Lamport logical clocks [Lamport 2019]. Therefore, the acceptance of a location update could occur only if it is temporally consistent with previous positions, received messages, and the UAV's physical mobility constraints.

The security results shown in Table 4 evidence FlySafe resilience in the face of black hole attacks. Although a couple of UAVs exchanged up to six messages before segregating the MalUAV from the network, UAVs commonly exchanged at least one message (RCD = 1.35) to block a MalUAV. Such behavior highlights the relevance of information sharing between honest UAVs for network security. In these cases, the blocking occurred as a result of the interaction of other UAVs with the MalUAV, i.e., the UAV blocked the MalUAV without having direct contact with it, but with its neighbors. Therefore, the adoption of opportunistic approaches epidemic and direct delivery to information sharing allows UAVs improve their spatial awareness even in the face of a black hole attacker denying neighborhood information.

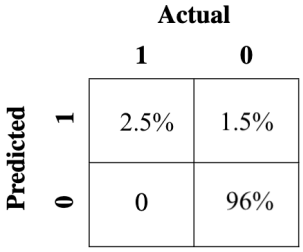

Figure 6. Confusion matrix for FlySafe operation

Table 4. Security evaluation results

Metric	**RCD** (# messages)			**UBT** (s)		
Scenario	**min**	**max**	**avg**	**min**	**max**	**avg**
ATTKDEF	0	6	1.35	0	296.99	33.79

Generally, blocking a MalUAV making a black hole attack in the network takes place after 33.79 s from when it sends a message omitting its neighborhood information. From now on, the others disregard MalUAV when sharing location information. But, there are cases whose MalUAV interaction with other UAVs and the exchange of messages between honest UAVs about the MalUAV led to a much shorter blocking time, UBT = 0 s. Since blocking a malicious UAV depends on message exchange in sparse environments, for instance, where vehicles rarely interact, blocking a MalUAV to segregate it from the network makes a more time-consuming task. In these cases, FlySafe took up to 296.99 s to block the malicious UAV.

Regarding FlySafe performance assessment, the results seen in Table 5 indicate a stable behavior in all evaluated scenarios. The amount of exchanged messages to keep UAV spatial awareness (CRD) remained around 1370. Nonetheless, the quantity of individual messages sent by each UAV indicate that whenever the MalUAV disregards its neighborhood information when sending messages, it requires FlySafe to change its behavior. Particularly, we note an intensification in the neighbor discovery process, given the lack of neighborhood information from the attacker. Therefore, without protection (ATTKSIM), UAVs sent 8.5% more HM. With protections measures activated (ATTKDEF), UAVs sent even more HM, at about 3%. Although some UAVs detect and segregate the MalUAV from the network, it remains in its coverage area, but UAVs cannot count on it. On the other hand, location updates (TM messages) decreased in about 9.75% from BASELINE to ATTKDEF. Such behavior arises from the difficulty of UAVs to perform neighbor discovery due to the MalUAV, thus reducing their spatial awareness. In general,

the results point out FlySafe resilience under a MalUAV performing a BH attack, since it adapts its behavior in reason of a lack of location information and enhances neighbor discovery process to improve UAV spatial awareness.

Table 5. Rounds to keep UAV spatial awareness

	Scenario		
	BASELINE	**ATTKSIM**	**ATTKDEF**
HM	487.4	529.1	545.2
IM	45.7	41.1	45.7
TM	858.3	800.3	774.6
CRD (# rounds)	1391.4	1370.5	1365.5

Table 6. Neighbors perception analysis

	NDE (# nodes)		
Scenario	**min**	**max**	**avg**
BASELINE	0.1	4.0	1.4
ATTKSIM	0.25	4.55	1.25
ATTKDEF	0.44	2.28	1.44

The black hole attacker strongly jeopardizes the location service neighborhood perception, particularly leadint to an erroneous neighbor discovery (NDE). Although, in average, NDE remains stable, as shown in Table 6, the maximum achieved values show a distinct behavior. In an environment with the attacker (ATTKSIM), UAVs perceived its neighborhood with an error greater than four nodes. Nevertheless, when applied the detection and mitigation strategies (ATTKDEF), UAVs improved neighbor perception in about 49.9%. Such result is even better than without the attacker (BASELINE). The achieved behavior occurs due to the exchanged messages right after attack detection, which also improve the overall neighbor discovery process. Therefore, FlySafe benefits from this strategy to carry a resilient operation.

Regarding spatial awareness, as shown in Table 7, the results point out how the black hole attacker jeopardize UAVs spatial awareness periods. The results to SAT were severely reduced by about 67.73% from a scenario with only honest UAVs (BASELINE) to an environment with one MalUAV (ATTKSIM). Under attack, UAVs experienced shorter intervals of full spatial awareness alternating with periods of partial awareness about their neighbor nodes. Given that MalUAV denies sharing neighborhood information to other UAVs, they end up ignoring the presence of some neighbors nearby, lacking spatial awareness. In the face of defense measures (ATTKDEF), UAVs improved their spatial awareness in about 18.3%, highlighting FlySafe resilience to BH attacks. The network segregation of the MalUAV combined with neighbor UAVs opportunistic interactions to infer MalUAV neighborhood allowed UAVs to improve their spatial awareness.

Table 7. Spatial awareness assessment

Metric	**SAT** (s)			**AoII** (s)		
Scenario	**min**	**max**	**avg**	**min**	**max**	**avg**
BASELINE	0.0	310.5	53.68	0.0	15.84	1.57
ATTKSIM	0.4	188.06	17.32	0.0	28.94	2.01
ATTKDEF	0.4	200.87	20.49	0.0	30.68	2.1

Table 8. Rounds to improve UAV spatial awareness

	Sent messages		**RIA**
	NR	**RD**	
# rounds	8.2	8.1	16.53

SAT and AoII are complementary, i.e., by adding the average values of SAT and AoII for each scenario, we get the total operation time, 1200 s. Therefore, AoII results allow us to confirm the values attained by SAT. As shown in Table 7, AoII values indicate that UAVs know their neighborhood during almost all their operation time. Even under attack, UAVs are commonly aware of others during periods of at least 1.44% and 1.7% of their operation time to ATTKSIM and ATTKDEF scenarios, respectively. Further, although the MalUAV jeopardizes UAVs' spatial awareness, they operated unaware of their neighborhood typically during 2 s, at about 0.16% of their operation time, which evidence FlySafe resilience against black hole attacks.

The interactions with a black hole attacker that deny sharing neighborhood information demand from honest UAVs an improvement on neighbor discovery process. In this way, whenever honest UAVs receive a message from a MalUAV, they request their neighbors their neighborhood information. Thus, they can infer the neighborhood omitted by MalUAV, improving its own spatial perception. The achieved results, as presented in Table 8, show that UAVs sent in average 16.53 messages to improve their spatial awareness in the face of a black hole attacker.

The simulated environment enabled us to analyze the FlySafe security against UAVs performing Black hole attacks. Due to regulatory issues, the ingress of UAVs in Class-G airspace, i.e., the uncontrolled air space [Aviation 2024] requires preparedness concerning security, safety, and protection of human life, especially in urban scenarios. Thus, as real environments challenge system deployment and operation, the seamless coexistence of unmanned vehicles with crewed aircraft still has a long way to go.

5. Conclusion

This paper analyzed the resilience of the FlySafe system for protecting UAV networks against malicious UAV operating black hole attacks sharing no location information about its neighbors in a swarm environment. FlySafe applies opportunistic approaches like epidemic and direct delivery during UAVs interactions, and enhances neighbor discovery process in the face of attack detection. Simulations evaluated the security of the location service , particularly in identifying and segregating black hole attackers, and its resilience by adapting the operation due to the detected threat. FlySafe demonstrated reliability when detecting and segregating a black hole attacker from the network in average up to 33.79 s. It also improved its performance by increasing overall neighborhood perception.

Acknowledgment

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001 and by National Council for Scientific and Technological Development (CNPq/Brazil), grant #307752/2023-2, PQ #307752/2023-2, INCT ICoNIoT #405940/2022-0, and Universal #409275/2025-5.

References

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

Alipour-Fanid, A., Dabaghchian, M., Wang, N., Wang, P., Zhao, L., and Zeng, K. (2019). Machine learning-based delay-aware UAV detection and operation mode identification over encrypted Wi-Fi traffic. *IEEE Transactions on Information Forensics and Security*, 15:2346–2360.

Aviation, F. A. (2024). Section 3. Class G Airspace. Available at: https://www.faa.gov/air_traffic/publications/atpubs/aim_html/chap3_section_3.html. [Online]. Accessed: Jul, 2026.

Batista, A. and Santos, A. (2025). Resilient UAVs location sharing service based on information freshness and opportunistic deliveries. *Pervasive and Mobile Computing*, 111:102066.

Batista, A. D. S. and Dos Santos, A. L. (2024). A survey on resilience in information sharing on networks: Taxonomy and applied techniques. *ACM Computing Surveys*, 56(12):1–36.

Delavarpour, N., Koparan, C., Nowatzki, J., Bajwa, S., and Sun, X. (2021). A Technical Study on UAV Characteristics for Precision Agriculture Applications and Associated Practical Challenges. *Remote Sensing*, 13(6):1204. doi: 10.3390/rs13061204.

Farooq, J. and Zhu, Q. (2025). Cyber Resilience in Next-Generation Networks: Threat Landscape, Theoretical Foundations, and Design Paradigms. *arXiv preprint arXiv:2512.22721*.

GVR, N. G. T. R. T. (2026). Drone Market (2026 - 2033). https://www.grandviewresearch.com/industry-analysis/drone-market-report. [Online]. Accessed: May, 2026.

Hadi, H. J., Cao, Y., Li, S., Hu, Y., Wang, J., and Wang, S. (2024). Real-time collaborative intrusion detection system in UAV networks using deep learning. *IEEE Internet of Things Journal*, 11(20):33371–33391.

Hernandez, M., Gur, G., Tangade, S., and Namuduri, K. (2023). Security for Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems. *Security for Vehicle-to-Vehicle Communications for Unmanned Aircraft Systems*, (10085742):1–24.

Hesford, J., Cheng, D., Wan, A., Huynh, L., Kim, S., Kim, H., and Hong, J. B. (2024). Expectations Versus Reality: Evaluating Intrusion Detection Systems in Practice. *arXiv preprint arXiv:2403.17458*. doi: 10.48550/arXiv.2403.17458.

Huang, H., Su, J., and Wang, F.-Y. (2024). The Potential of Low-Altitude Airspace: The Future of Urban Air Transportation. *IEEE Transactions on Intelligent Vehicles*, 9(8):5250–5254.

ICAO (2018). ADS-B Implementation and Operations Guidance Document - Edition 11. https://www.icao.int/sites/default/files/sp-files/APAC/Documents/AIGD%20Edition%2011.pdf. [Online]. Accessed: Jul, 2021.

Kramar, V. (2020). UAS (drone) in Response to Coronavirus. In *27th Conference of Open Innovations Association*, FRUCT, pages 90–100, New Jersey, USA. IEEE.

Lakew, D. S., Sa'ad, U., Dao, N.-N., Na, W., and Cho, S. (2020). Routing in Flying Ad Hoc Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, 22(2):1071–1120. doi: 10.1109/COMST.2020.2982452.

Lamport, L. (2019). Time, clocks, and the ordering of events in a distributed system. In *Concurrency: the Works of Leslie Lamport*, pages 179–196. ACM.

Lima, R. R. and Pereira, G. A. (2021). On the Development of a Tether-based Drone Localization System. In *International Conference on Unmanned Aircraft Systems*, ICUAS, pages 195–201. IEEE. doi: 10.1109/ICUAS51884.2021.9476778.

Maatouk, A., Kriouile, S., Assaad, M., and Ephremides, A. (2020). The Age of Incorrect Information: A New Performance Metric for Status Updates. *IEEE/ACM Transactions on Networking*, 28(5):2215–2228. doi: 10.1109/TNET.2020.3005549.

NS-3, C. (2022). NS-3 Discrete-event Network Simulator. https://www.nsnam.org. [Online]. Accessed: Feb, 2022.

Qureshi, K. N., Nafea, H., Javed, I. T., and Ghafoor, K. Z. (2024). Blockchain-based trust and authentication model for detecting and isolating malicious nodes in flying ad hoc networks. *IEEE Access*, 12:95390–95401.

Ren, S., Li, D., Hu, Q., Liu, Y., and Liu, J. (2022). An Improved Security OLSR Protocol against Black Hole Attack based on FANET. In *13th Asian Control Conference*, ASCC, pages 383–388, New Jersey, USA. IEEE.

Sedjelmaci, H., Senouci, S. M., and Ansari, N. (2017). A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9):1594–1606.

Tian, B., Wang, L., Xu, L., Pan, W., Wu, H., Li, L., and Han, Z. (2023). UAV-Assisted Wireless Cooperative Communication and Coded Caching: A Multiagent Two-Timescale DRL Approach. *IEEE Transactions on Mobile Computing*, 23(5).

Tlili, F., Ayed, S., and Fourati, L. C. (2024). Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). *Computers & Security*, 142:103878.

Tsao, K.-Y., Girdler, T., and Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, 133(102894):1–39. doi: 10.1016/j.adhoc.2022.102894.

Wang, L., Chen, Y., Wang, P., and Yan, Z. (2021). Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications. *IEEE Communications Standards Magazine*, 5(4):41–47. doi: 10.1109/MCOMSTD.0001.2000078.

Yang, J., Liu, X., Jiang, X., Zhang, Y., Chen, S., and He, H. (2023). Toward trusted unmanned aerial vehicle swarm networks: A blockchain-based approach. *IEEE Vehicular Technology Magazine*, 18(2):98–108.

Zhang, Y., Zhang, B., and Yi, X. (2018). Adaptive Data Sharing Algorithm for Aerial Swarm Coordination in Heterogeneous Network Environments (Short Paper). In *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, volume 268 of *CollaborateCom*, pages 202–210. Springer, Cham. doi: 10.1007/978-3-030-12981-1_14.

Zhou, Y. (2025). Unmanned aerial vehicles based low-altitude economy with lifecycle techno-economic-environmental analysis for sustainable and smart cities. *Journal of Cleaner Production*, 499:145050.