An Opportunistic Key Exchange Scheme for Location Information Sharing on UAV Networks Resilient to MiM Attacks

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

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

[2]Depto. de Ciência da Computação (DCC) – UFMG

asbatista@inf.ufpr.br, {vinicius.trindade, aldri}@dcc.ufmg.br

Abstract. *As unmanned aerial vehicles (UAVs) demand wireless technologies for their communication, they become prone to serious security threats that aim to compromise the integrity and confidentiality of the exchanged control data, standing out man-in-the-middle (MiM) attacks as one of the most damaging. Besides, UAV networks require essential critical services for their regular operation, like the UAV location service. Key exchange is one way to protect UAV communications against MiM attacks. This paper proposes KEYSUAV, a key exchange scheme to enable a resilient location information sharing on UAV networks against MiM attacks. KEYSUAV relies on opportunistic approaches and on the lightweight cryptographic standard ASCON, an algorithm designed for resource-constrained devices like UAVs. Simulation results show that KEYSUAV over the FlySafe system detected 100% of compromised messages sent by a MiM attacker with a slight reduction in UAVs' spatial awareness, around 4.5%, thus fostering the resilience of the location service for UAV networks.*

1. Introduction

The adoption of unmanned aerial vehicles (UAVs) in commercial sectors like agriculture, construction, and logistics has driven the expansion of the UAVs market. It has been expected a growth around 9.6% per year in the Americas from 2025, reaching $79 billion in 2033 [Grand View Research 2025]. While UAV mobility benefits the execution of several services by those sectors, UAVs still face many challenges to carry out a safe operation, such as energy limitation, location coordination [Anagnostis et al. 2025], and even communication vulnerabilities [Xia et al. 2023] that demand secure control information.

The UAV communication infrastructure exposes messages exchanged between UAVs to malicious actions such as man-in-the-middle (MiM), replay, and denial-of-service (DoS) attacks [Anagnostis et al. 2025]. Among such attacks, MiM attacks are regarded as a harmful threat to mobile networks due to their ability to delay or drop critical network information [Al-Shareeda and Manickam 2022]. A MiM attacker can intercept and secretly modify control data exchanged between two devices in order to gain unauthorized access to confidential data. The attacker compromises properties such as availability and integrity of control information exchanged, and impairs the functioning of basic network services like routing and location. Thus, UAVs require resilient message exchanges, which can take place by key exchange between UAVs to provide mutual

authentication, thus avoiding disturbances in decision-making to achieve a secure operation. 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].

UAV networks specially differ from other mobile ad-hoc networks (MANETs) particularly due to the high mobility of the devices and the variety of threats to which they are exposed. Therefore, such networks require security strategies appropriate for communication UAVs - base stations (BS), and UAV-UAV [Alladi et al. 2020]. In general, approaches seen in the literature against MiM attacks on integrity of control information in UAV networks focus on vehicle authentication to guarantee a secure UAV-BS. Strategies like Advanced Encryption Standard (AES) [Dogan 2023] and the Physical Unclonable Function (PUF) [Alladi et al. 2020] stand out. In UAV-UAV communications, despite the investigation of using PUFs takes place [Zhang et al. 2023], they are subject to vulnerabilities arising from variations in temperature, voltage levels, and characteristics of the electronic circuits [Kumar et al. 2025], rendering their use unfeasible. Further, several existing schemes disregard the application of encryption mechanisms suitable for UAV networks, and rely on solutions designed for other mobile network environments.

This paper proposes an opportunistic key exchange scheme, called KEYSUAV, for supporting FlySafe [Batista and Santos 2025], a specific location information sharing system, in order to make critical systems resilient to MiM attacks. The novelty of KEYSUAV encompasses enabling mutual authentication of UAVs by leveraging their moments of interaction. Unlike other schemes for UAV networks, KEYSUAV is an adaptive scheme for basic UAV network services based on the lightweight cryptographic standard ASCON-128 protocol [Turan et al. 2025] – an algorithm designed for resource-constrained devices like UAVs [Patel and Cherukuri 2025] – and employs Elliptic Curve Cryptography (ECC) to provide public key security. We evaluated KEYSUAV through the FlySafe location service. Analysis of the simulation results shows that KEYSUAV over the FlySafe system detected 100% of compromised messages sent by a MiM attacker due to opportunistic approaches with a slight reduction in UAVs' spatial awareness, around 4.5%, thus significantly enhancing the resilience of the location service for UAV networks.

This paper is organized as follows: Section 2 presents the related work. Section 3 presents the system and threat models investigated. Section 4 describes the KEYSUAV scheme and its operation. Section 5 details a performance evaluation against MiM attacks and the achieved results. Section 6 presents the conclusion.

2. Related work

The literature on lightweight authentication schemes for UAV networks has been increasing to ensure exchanged data security and privacy, particularly to meet UAV constrained resources. Regarding works focused on UAV-GS secure communication, [Dogan 2023] proposed a lightweight authentication and key agreement scheme. It relies on elliptic curve encryption (ECC) to support mutual authentication between UAV and GS devices against threats like impersonation, replay, and MiM attacks. Whenever a UAV connects to the UAV network, the scheme employs a session key for data exchange. The scheme regularly renews the dynamic secret key, current timestamps, and random nonces to provide a unique key pair (public and private) and temporary identification to each entity in the network face the attacks. Although UAVs exchange messages directly with each other,

their authentication occurs only through GS.

Alladi et. al [Alladi et al. 2020] proposed an authentication scheme based on physical unclonable function (PUF) for UAV-GS and UAV-UAV communication against many security attacks such as masquerade, replay, node tampering, and cloning attacks. The scheme generates secret information on the fly based on the response generated from the inbuilt PUFs to ensure UAV-GS authentication. Such a process took place in three phases, i.e., UAV registration, UAV-GS authentication, and UAV-UAV authentication. However, UAV-UAV communication occurs through GS operation, disregarding opportunities of direct interactions between UAVs to enable message exchanges. [Xia et al. 2023] proposed an identity authentication scheme based on ECC. The scheme allows the mutual authentication and session key agreement configuration between the UAV and GS, and also UAV-UAV authentication, which occurs through the GS. The scheme employs the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol to allow the establishment of a shared key over an insecure communication channel. Based on Diffie-Hellman key exchange, it employs ECC to generate and exchange keys to ensure data security and privacy. However, the key configuration depends on the GS, being challenging to deal with the authentication and encrypted UAV-UAV communication in a large-scale environment.

With relation to UAV-UAV communication, [Chen et al. 2026] proposed a lightweight intra/inter-domain authentication scheme for UAV networks based on fractional-order Chebyshev chaotic maps, PUFs with error-correcting code, and hash functions against security and privacy threats like key leakage, identity forgery, and physical tampering attacks. To access a network domain, UAVs exchange keys with GS. Inside the domain, they can communicate securely with other UAVs, but the interaction with GS is required to start the key exchange process. Therefore, although the scheme provides secure communication for UAVs, it occurs through GS. [Zhang et al. 2023] presented a lightweight authentication scheme based on PUF and ECC to provide UAV-UAV mutual authentication against threats on their communication. As the PUF is embedded in the UAV, the scheme can also defend against physical capture attack. The scheme counts a GS to register each UAV and generate authentication parameters. It works on four phases, i.e., setup, UAV registration, UAV-UAV authentication, and dynamic UAV addition. The last phase allows to connect other UAVs to the established network. However, since PUF is prone to vulnerabilities arising from variations in temperature, voltage levels, and the characteristics of the electronic circuits [Kumar et al. 2025], inputting the same challenge may not always produce the same response.

Despite the existence of several key exchange schemes for UAV networks, the security of UAV communication remains a challenging task due to threats like MiM attacks, since many of the schemes provide UAVs authentication based on GS. The demand for a ground station to enable UAV-UAV communication commonly jeopardizes key exchanges in the face of network scalability and UAV mobility. Moreover, these schemes often adapt the strategies applied to get a secure communication in other mobile environments to UAV networks, disregarding UAV constrained-resources. Thus, this work proposes an opportunistic key exchange scheme suitable to limited resources of UAVs based on the lightweight cryptographic standard ASCON to get a secure UAV-UAV communication.

3. System, authentication and threat models

The system model required for the KEYSUAV scheme considers a set of UAVs, denoted by $\mathcal{U} = \{u_1, u_2, u_3, ..., u_j\}$, where $u_j \in \mathcal{U}$, interconnected by a wireless communication network to exchange messages. Equipped with sensors and communication facilities, UAVs can perform missions in urban, rural, or mountainous locations. Before start operating, we suppose that each UAV u is previously configured with private ($PrivK$) and public ($PubK$) keys, which are assumed to be secure, and an adversary cannot obtain them. During operation, each $u_j \in \mathcal{U}$ monitors the flight environment to identify others in its coverage area through a discovery function and updates such information to perform a safe flight. Then, nearby UAVs exchange keys to communicate securely, enabling both devices to share information resiliently and complete assigned tasks.

The main threat encompasses MiM attacks targeting a UAV-UAV communication to compromise the integrity and confidentiality of the exchanged data. We suppose a malicious UAV (MalUAV) m carries out a MiM attack, i.e., it steals exchanged messages by eavesdropping on the communication channel. Then, it modifies and replays them to legitimate entities by spoofing the IP and MAC addresses of the source UAV. We denote the set of deployed MalUAVs, denoted by $\mathscr{U} = \{m_1, m_2, m_3, ..., m_k\}$, where $m_k \in \mathscr{U}$, such that $\mathscr{U} \not\subset \mathcal{U}$, i.e., m_k is out of the network. Figure 1 shows a MiM attack over UAV communication, UAV_1 and UAV_2. As they connect over a wireless channel, which is naturally insecure, MalUAV in the coverage area can eavesdrop on their communication channel and steal exchanged messages.

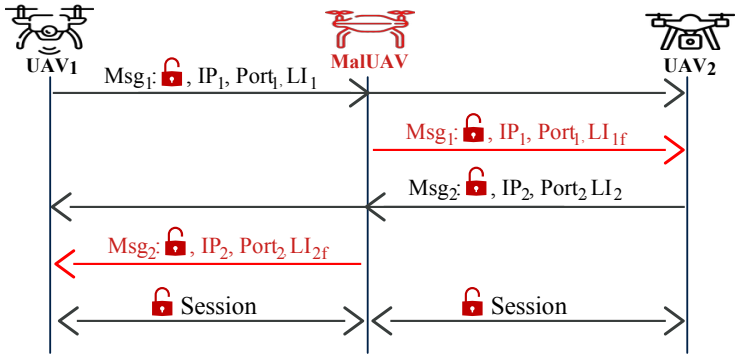

Figure 1. MiM attack on UAV communication

As shown in Figure 1, UAV_1 sends a message (Msg_1) to UAV_2. A MalUAV performs a MiM attack by eavesdropping on their communication channel and get Msg_1. Then, it modifies UAV_1 location information (LI_1) carried by Msg_1 and sends a new Msg_1 to UAV_2 with a false location information (LI_{1f}). Thus, UAV_2 receives two messages from UAV_1 with different location information. In the same way, when UAV_2 sends a message (Msg_2) to UAV_1, the MalUAV gets Msg_2, modifies L_2 and sends a new Msg_2 to UAV_1 with a false location information (LI_{2f}).

4. The key exchange scheme for location information sharing on UAVs

This section presents KEYSUAV, an opportunistic key exchange scheme for supporting location information sharing on UAV networks. KEYSUAV is adapted to carry out with the FlySafe location service [Batista and Santos 2025] against MiM attacks. Next, we

detail both KEYSUAV communication model and its architecture. Unlike TLS protocol, which relies on a secure communication protocol like TCP, KEYSUAV runs over UDP protocol. Its goal is to enable a set of UAVs securely exchange location information to support flight coordination, then preventing collisions.

4.1. Communication model

The KEYSUAV scheme exploits both epidemic and direct delivery opportunistic approaches to exchange keys between UAVs. For that, it operates in two main steps, called ***Symmetric key generation*** and ***Symmetric key application***, as depicted in Figure 2.

Symmetric key generation: In the scheme, each UAV sends a broadcast request to authenticate other UAVs in its coverage area. Upon receiving this request message, the receiver UAV establishes and stores a symmetric key to securely exchange messages with the requester UAV. Then, the receiver sends its public key to the requester, which also creates and stores a symmetric key for securely message exchanges. As illustrated in Figure 2(a), a UAV_1 broadcasts a request (Req) with its public key. From the received request, UAV_2 chooses an elliptic curve $Eq(a, b)$ over a finite field $GF(q)$ and a base point U over $Eq(a, b)$. Next, it generates and stores a symmetric key from $Eq(a, b)$. Then, it responds (resp) to UAV_1 sending its public key. Based on the received public key, UAV_1 creates and stores a symmetric key, so that both UAVs can securely exchange messages.

Symmetric key application: It supposes the existence of two adjacent UAVs, UAV_1 and UAV_2, as depicted in Figure 2(b), and each one owns a symmetric key to exchange messages with the other. UAV_1 encrypts a message and sends to UAV_2, which employs their symmetric key to decrypt the message. In the same way, UAV_2 encrypts a message and sends to UAV_1, which employs the symmetric key to decrypt the message.

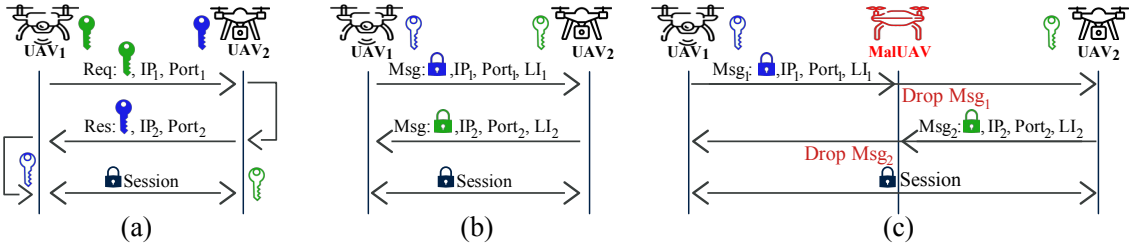

Figure 2. (a) Two UAVs exchanging keys. (b) Two secure UAVs exchanging messages. (c) A MiM attacker exploiting UAV communication.

The scheme provides resilience against a MiM attacker hijacking UAV communication, as shown in Figure 2(c), where an attacker eavesdrops on the exchanged messages between UAV_1 and UAV_2. As UAVs securely exchange messages by applying their symmetric keys, it becomes a challenging task to the MalUAV to understand and modify the stolen message. Therefore, the MalUAV drops the message.

4.2. Architecture

The KEYSUAV architecture comprises three modules installed on a UAV and adapted to FlySafe, as shown in Figure 3. The ***Information sharing controlling*** module analyzes the FlySafe shared messages to ensure a secure communication with a neighbor UAV. The ***Handshake controlling*** module controls the key exchanges with other devices and

answers their requests for authentication. The ***Message monitoring*** module monitors the received messages to identify and keep the UAV updated about MalUAVs within its coverage area performing MiM attacks.

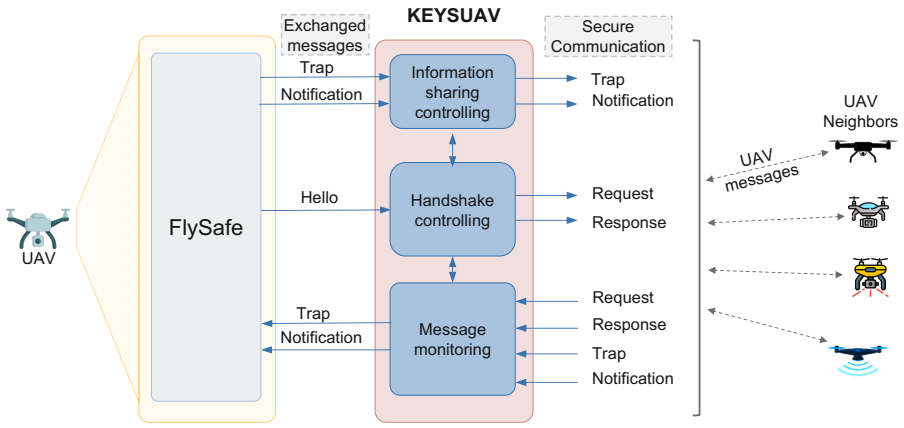

Figure 3. KEYSUAV architecture integrated with location service

(a) Information sharing controlling module (ISC): It ensures that FlySafe shares messages – Trap messages (TM) and notifications – only with an authenticated UAV. In this way, it verifies whether the UAV has already exchanged keys with the neighbor UAV by checking the Symmetric key list (SL) available in the Handshake controlling module. If so, this module encrypts the message, TM or notification, employing the symmetric key from the neighbor UAV and sends the message to it.

(b) Handshake controlling module (HC): It manages the key exchanges between UAVs by storing the symmetric keys from the neighbor UAVs in the SL. HC also keeps control of ongoing exchanges through a Handshake list (HL). From a Hello message (HM) created by FlySafe to start neighbor discovery, this module drops the HM and creates a request message to authenticate other devices in the UAV coverage area. The request, $\langle Id_r, PubK_r \rangle$, carries UAV identification (Id) and public key ($PubK$). Further, based on received requests from neighbor UAVs, HC answers with a response message, $\langle Id_r, PubK_r \rangle$. Then, it creates a symmetric key and stores in the SL. As described in Algorithm 1, before starts key exchange, each UAV establishes an HL to keep track of which neighbors the key exchange process has started (*l.1*). Next, whenever UAV u has no neighbors in its neighbor list, it broadcasts a request message carrying its public key ($PubK_u$) to authenticate UAVs inside its coverage area and waits for a response of neighbors UAVs (*l.2-5*). Upon receiving a request, UAV u holds the requester UAV n in its HL, creates a symmetric key from $PubK_n$ and its private key $PrivK_n$. Next, it sends its public key $PubK_u$ to n (*l.6-10*). Whenever UAV u receives $PubK_n$, it holds n in its HL, creates a symmetric key from $PubK_n$ and its private key $PrivK_u$ (*l.11-14*). Therefore, as both UAVs have each other's symmetric key, they can exchange messages securely.

(c) Message monitoring module (MM): It monitors all received messages in order to identify MalUAVs making MiM attacks or even bad formed messages. Upon receiving a message, it decrypts it and checks the information contained. When messages from no authenticated UAVs or bad formed, MM drops them, otherwise it delivers TM and notification to FlySafe, while the HC module handles requests and responses.

Algorithm 1: Key exchange management

Data: *u* (UAV device), *n* (UAV neighbor device), *HL* (Handshake List), *NL* (Neighbor List), *PubK* (Public Key), *PrivK* (Private Key), *SimK* (Symmetric Key)

```
HL(u) ← 0
while u = ON do
    if (NL(u) = 0) then
        Request-u(PubK(u))
    end
    if (u ← Request-n(PubK(n))) then
        HL(u) ← n
        SimK(n) ← CreateSharedKey(PubK(n), PrivK(u))
        Send (n, PubK(u))
    end
    if u ← Recv(PubK(n)) then
        HL(u) ← n
        SimK(n) ← CreateSharedKey(PubK(n), PrivK(u))
    end
end
```

KEYSUAV relies on the lightweight cryptographic standard ASCON-128 [Turan et al. 2025], an algorithm designed for resource-constrained devices like UAVs in order to encrypt data before transmission [Dobraunig et al. 2021]. ASCON requires a single secret key for encryption and decryption, thus reducing system complexity and enhancing the efficiency of data transmission. Its authenticated encryption mode ensures security, data authenticity and integrity.

For handling encryption, authentication, and decryption, we employ a symmetric key as a pre-shared key to meet ASCON requirements. In this way, each UAV establishes a symmetric key from the public key received from other UAVs. This happens during mutual authentication through a standard Key Derivation Function (KDF) from an elliptic curve (ECC). We adopted an ECC over a finite field $GF(q)$, where q is a large prime number and represents the number of elements in $GF(q)$. The equation $y^2 = x^3 + ax + b$ (mod q) $\mid a, b \in GF(q)$ and $\Delta = 4a^3 + 27b^2 \neq 0$ (mod q) [Cilardo et al. 2006] defines the elliptic curve $Eq(a, b)$. A point O at infinity on $Eq(a, b)$ together with all the other points on $Eq(a, b)$ form a set $G = \{(x, y) : x, y \in GF(q) \mid y^2 - x^3 - ax - b = 0\} \cup \{O\}$. Therefore, we can compute the point $Q = s \cdot U$ by setting the base point U on $Eq(a, b)$ and an integer s, which means adding multiple points U, as shown in $Q = s \cdot U = U + U + ... + U$ (s times). However, it is computationally difficult to find s from Q and U [Mehrabi et al. 2020]. Initially, KDF generates a symmetric key from $Eq(a, b)$ with 256 bits. Nevertheless, as ASCON carries out with 128-bit keys, we have configured KDF to deliver the first 128 bits as the symmetric key.

5. Evaluation and analysis

This section presents the performance evaluation of KEYSUAV established through simulation to analyze the behavior of the UAV location service during Man-in-the-Middle

attacks in a UAV network. First, we detail the scenario and configurations applied in the simulations. Then, we present the metrics employed to measure and analyze the service against MiM attacks. Lastly, we show and discuss the results obtained in the evaluation.

5.1. Simulation scenario

We have employed the NS-3 [NS-3 2025] simulator to develop and evaluate the performance and resilience of KEYSUAV against MiM attacks over the FlySafe [Batista and Santos 2025] location service. Table 1 presents the setup parameters employed in the simulation. We suppose a scenario in which a swarm of 40 UAVs monitors and surveys an inaccessible region with an area of 1.5 $\times$ 1.5 km, where fixed communication infrastructure is unavailable. Due to the lack of standardization among various organizations regarding the space between UAVs during flight, we have defined this amount of vehicles as representative of the scenario. The UAVs own IEEE 802.11n Wi-Fi technology and have a communication range of approximately 115 m. They fly at an altitude of 300 feet, which is a permitted flight level for UAVs [Administration 2021], at a constant speed of 20 m/s. All UAVs follow a 2D random walk mobility model to collect environmental data. They collaboratively share their locations to assist in building individual spatial awareness and update their positioning every 1.5 s. We adopted the 2D random walk model as a proof of concept.

Table 1. Simulation settings

Parameter	Value(s)
Simulation time	1200 s
Map area	1.5 km $\times$ 1.5 km
Flight level	300 ft
# UAVs	40
Mobility model	2D Random Walk
Flight speed	20 m/s
PHY/MAC Protocol	802.11n
Communication range	115 m
# malicious UAVs	0, 1

For better analysis and comparison, we simulated the established scenario with three distinct configurations: BASELINE: FlySafe with one MalUAV; BASESCHM: FlySafe without MalUAVs and with KEYSUAV; and ATTKPROT: BASESCHM with one MalUAV. Further, we present the simulation results for FlySafe with only honest UAVs. Table 2 presents the security parameters employed in the simulation. Each simulation lasts 1200 seconds, and we calculated the applied metrics as the average of 35 simulations to achieve a 95% confidence interval, except where otherwise specified.

5.2. Metrics

We evaluate the performance and resilience of KEYSUAV through specific metrics and by those applied on FlySafe, as shown in Table 3. For performance, we compute True Negative (**TN**), True Positive (**TP**), False Negative (**FN**), and False Positive (**FP**) rates to verify the precision on attacks detection. We monitor the Compromised Message Rate (**CMR**) and Compromised Message Delay (**CMD**) to determine the mitigation of false information injected into the network. We analyze the Delay on Location Changes Recognition

Table 2. Security settings

Parameter	Value(s)
Elliptic Curve	NIST P-256
Curve Form	Short Weierstrass
Field Type	Prime finite field ($\mathbb{F}_p$)
Curve Equation	$y^2 \equiv x^3 - 3x + b \pmod{p}$
Key Library	OpenSSL
Entropy Source	OS-based entropy
KDF Algorithm	Truncated SHA-256
KDF Output	First 16 bytes of SHA256 (secret)

(Υ) to determine network responsiveness and the Neighbor Discovery Error (Γ) to identify inconsistencies in neighborhood perception. Finally, we measure the Convergence Rounds (φ) to quantify the total communication overhead required to reach a stable state of awareness. For resilience, we monitor the Age of Information (**AoI**) to evaluate the freshness of neighborhood data and the Age of Incorrect Information (**AoII**) to quantify the time a UAV stores incorrect information about others. We track the Spatial Awareness Time (ψ) to measure how long nodes maintain a correct view of their surroundings and the Localization Error (Ω) to assess the precision of perceived coordinates.

Table 3. Performance metrics

Description	Equation
Location Error (Ω) evaluates FlySafe's accuracy in maintaining a correct perception about a neighbor location over the time interval t.	$\Omega^t = \lvert d^r - d^m \rvert$
Convergence Rounds (φ) represent the number of messages exchanged for a UAV achieve spatial awareness in a time interval t.	$\varphi = \sum_{\substack{t=0 \\ \Gamma>0}}^{t \leq T} (HM + IM + TM)$
Neighbor discovery error (Γ) determines the erroneous neighborhood estimates over a time interval t.	$\Gamma_j^t = W_j^t - W_{\mathcal{S}}^t$
Delay on Location Changes Recognition (Υ) equals the period between the detection of a location change (t_i^d) by a UAV i and the moment a neighbor j becomes aware of the UAV's new position (t_j^r).	$\Upsilon = t_j^r - t_i^d$
Compromised messages rate (CMR) evaluates the rate of messages falsified by a MiM attacker and equals the number of compromised messages (CM) divided by the total of exchanged messages (TEM).	$CMR = \frac{CM}{TEM} \cdot 100$
Compromised messages delay (CMD) computes the delay on receiving a falsified message from a MiM attacker and equals the interval between the instant of receiving the legitimate message (t_l) and the instant of receiving the correspondent falsified message (t_f)	$CMD = t_f - t_l.$
Age of Information (AoI) indicates the updating of neighborhood information for UAVs. Adapted from [Yates et al. 2021].	$AoI = \int_0^{\mathcal{T}} \Delta(t) dt$
Age of Incorrect Information (AoII) means the period a UAV holds incorrect information about others. Adapted from [Maatouk et al. 2020].	$AoII = \int_0^{\mathcal{T}} \Delta_{\lambda_{\{\Gamma > 0\}}}(t) dt.$
Spatial Awareness Time (ψ) corresponds to the total period in which a UAV successfully recognizes all others in its coverage area.	$\psi = \sum_{t=0}^{\mathcal{T}} \int_0^{\mathcal{T}} \Delta_{\lambda_{\{\Gamma = 0\}}}(t) dt$

5.3. Performance and resilience results

We started by analyzing KEYSUAV performance through TP, TN, FP, and FN in the ATTKPROT configuration. As shown in Figure 4, KEYSUAV successfully classified all the exchanged messages. While most of the messages were legitimate, 0.2% were false information injected by a MiM attacker to compromise UAVs operation. Therefore, the confusion matrix shows that KEYSUAV detected and mitigated all the false information, TP = 0.2%, injected intothe network in the ATTKPROT configuration. In the same way, KEYSUAV correctly classified the benign traffic, TN = 99.8%, thus allowing the location service operate regularly even in the face of MiM attacks.

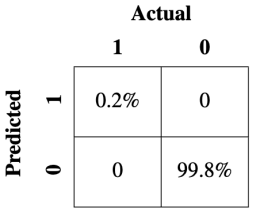

Figure 4. Confusion matrix for KEYSUAV operation

Table 4. Compromised messages

Config.	CMR (%)	CMD (ms)
FlySafe	0.00	0.00
BASELINE	2.65	3.15
BASESCHM	0.00	0.00
ATTKPROT	1.52	2.12

The adoption of KEYSUAV to provide a secure communication against MiM attacks benefited the UAVs location service, as shown in Table 4. We evaluated two configuration scenarios, BASELINE and ATTKPROT, with a MiM attack, but KEYSUAV operated only in ATTKPROT. Without KEYSUAV protection (BASELINE), the attacker successfully compromised (CMR) 2.65% of the exchanged messages in the location service. However, such malicious behavior strongly changed due to KEYSUAV operation (ATTKPROT), so that the location service experienced a reduction of approximately 42.64% in the amount of compromised messages by the attacker. In the same way, the delay caused by the MiM attacker when sending a false message decreased from 3.15 ms to 2.12 ms with the KEYSUAV operation, i.e., a reduction of 32.7%. Such results indicate that KEYSUAV improves the resilience of the location service against MiM attacks due to the secure communication achieved by the opportunistic key exchanges, given that it diminishes the amount of false information injected into the network. Further, as discussed below, the compromised messages changed the location service behavior to get and keep spatial awareness, particularly increasing the convergence rounds (φ) and the time to recognize location changes (Υ).

Table 5. Convergence rounds to achieve spatial awareness

	Configuration scenario			
	FlySafe	BASELINE	BASESCHM	ATTKPROT
φ	139.1	152.63	296.16	274.03

As expected, the amount of exchanged messages by a UAV to achieve spatial awareness naturally increased to get a secure communication, since KEYSUAV leverages HM and IM for key exchange. Therefore, neighbor discovery and maintenance processes rely only on TM, i.e., location updates. Although such behavior brings a cost to the location service operation, increasing φ from BASELINE to ATTKPROT by 79.3%, UAVs

keep spatial awareness above 90.68% of their operating time, as shown in Table 7. When the location service carried out only with honest UAVs (FlySafe), it demanded around 139 messages (φ) to get spatial awareness, as shown in Table 5. The presence of a MiM attacker injecting false information into the network (BASELINE) required the UAVs increasing the numberof messages to be aware of others in its coverage area, about 9.72%.

The increase in the number of exchanged messages by UAVs due to KEYSUAV operation with the location service is evidenced in the BASESCHM configuration. φ achieved 296.16 messages, an increase of approximately 94%, particularly due to location updates, TM, which almost tripled compared to BASELINE. The graphs in Figure 5 show the averaged values achieved for IM, TM and HM. When KEYSUAV runs with protection measures (ATTKPROT), φ experienced a reduction of 7.47%, given that the secure communication provided by KEYSUAV inhibits MiM attacker from compromising the location updates.

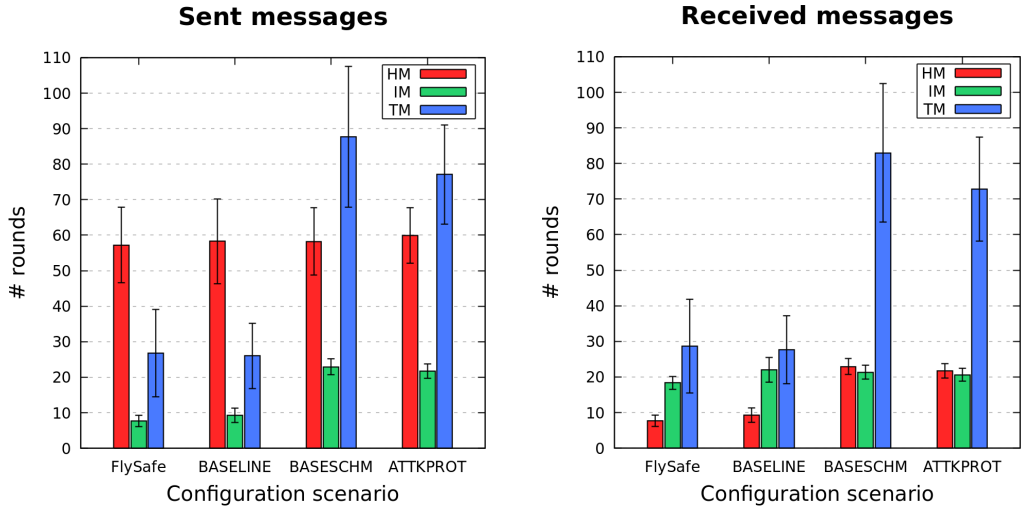

Figure 5. Convergence rounds to achieve spatial awareness

As KEYSUAV performance relies on UAVs opportunistic interactions to exchange keys, we analyzed the amount of key pairs created in each period of the simulation with the ATTKPROT configuration, as shown in the graph of Figure 6. We accumulated the average number of key pairs created by all UAVs from a set of simulation runs by summing such quantity successively throughout the simulations. Thus, we can represent UAVs behavior to exchange keys and establish a secure communication. It is worth noting that the key exchanges occur more frequently at the beginning of the simulation, when UAVs start moving. Up to 100 seconds of simulation, the UAVs created approximately 30 key pairs. From that point on, the interactions between the UAVs change due to their mobility, decreasing the number of key pairs created over time.

Finally, we evaluated the location service performance with KEYSUAV based on location precision (Ω), recognition delay (Υ), and neighbor discovery error (Γ). As shown in Table 6, a MiM attacker strongly jeopardizes the location service precision about the position of neighbor UAVs (BASELINE). As the attacker shares false location information with neighbor UAVs, their erroneous perception (Ω) about position of them increased by 403% when compared to an environment without attacks (FlySafe). However, the application of KEYSUAV with the location service reduced Ω to its lowest value, 0.62 m.

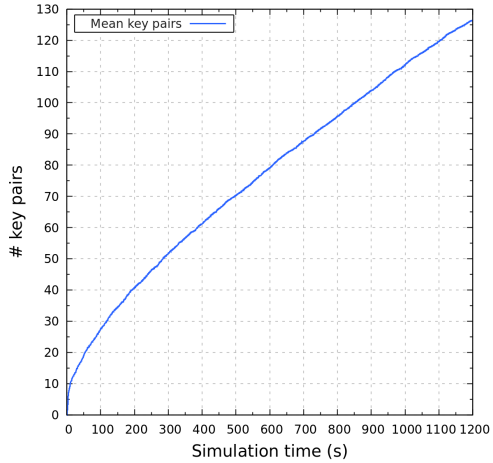

Figure 6. Key exchanges in ATTKPROT configuration

The delay in recognizing location changes (Υ) and the neighbor discovery error (Γ) kept stable throughout the simulations. We have observed a slight increase in Υ about 6.82%, from 2.93 ms (BASESCHM) to 3.13 ms (ATTKPROT). Those behaviors can be attributed to the compromised messages and the processes of encryption and decryption messages, and to the protection measures implemented by KEYSUAV.

Table 6. Neighborhood perception

Config.	Ω (m)	Υ (ms)	Γ (# nodes)
FlySafe	0.76	2.86	0.38
BASELINE	4.38	2.98	0.37
BASESCHM	0.67	2.93	0.34
ATTKPROT	0.62	3.13	0.31

Regarding KEYSUAV resilience, UAVs' spatial awareness condition remained stable during FlySafe operation with KEYSUAV, as shown in Table 7. As the scheme in BASESCHM operates with detection and mitigation measures deactivated, the MiM attacker freely jeopardizes UAV communication. Hence, AoI intervals reduced about 34.6%, while the duration of periods with incorrect neighborhood information (AoII) almost doubled reaching 2.63 s. However, the use of the scheme slightly decreased UAVs total spatial awareness (ψ) from 95.29% to 90.25% of their operation time from BASELINE to BASESCHM configurations, respectively.

Table 7. Spatial awareness condition

Config.	**AoI** (s)	**AoII** (s)	ψ (s)
FlySafe	55.73	1.58	1141.58
BASELINE	54.59	1.58	1143.49
BASESCHM	35.70	2.63	1083.58
ATTKPROT	37.01	2.56	1090.24

When KEYSUAV fully runs in ATTKPROT, i.e., with detection and mitigation measures activated, it enhanced AoI by 3.7%, thus increasing ψ to 90.83%. Such results

point out that under MiM attacks, the KEYSUAV operation has a minimal impact on the FlySafe functioning, while it enhances to the location service resilience.

6. Conclusion

This paper presented KEYSUAV, an opportunistic key exchange scheme for location information sharing on UAV networks resilient against Man-in-the-Middle attacks. It takes advantage of UAVs interactions to support key exchange and thus achieve UAV mutual authentication. Specifically KEYSUAV exploits jointly epidemic and direct delivery opportunistic approaches to leverage UAV interactions for key exchange. KEYSUAV runs over a location service to support secure communication between UAVs, thus fostering the resilience of location sharing. Simulation results pointed out that KEYSUAV supporting the FlySafe system have risen the reliability of the service facing MiM attacks sharing false location information in the network.

Acknowledgment

This study was financed by the Brazilian Federal Agency for Support and Evaluation of Graduate Education (CAPES) - Finance Code 001 and by the National Council for Scientific and Technological Development (CNPq/Brazil) through INCT ICoNIoT #405940/2022-0, PQ #307752/2023-2 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`. (accessed 8 august 2023).

Al-Shareeda, M. A. and Manickam, S. (2022). Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation. *Symmetry*, 14(8):1543.

Alladi, T., Bansal, G., Chamola, V., Guizani, M., et al. (2020). SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Transactions on Vehicular Technology*, 69(12):15068–15077. doi: 10.1109/TVT.2020.3033060.

Anagnostis, I., Kotzanikolaou, P., and Douligeris, C. (2025). Understanding and securing the risks of uncrewed aerial vehicle services. *IEEE Access*, 13:47955–47995.

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.

Batista, A. S. and Santos, A. L. (2025). Resilient UAVs location sharing service based on information freshness and opportunistic deliveries. *Pervasive and Mobile Computing*, 111:102066. doi: 10.1016/j.pmcj.2025.102066.

Chen, X., Hu, C., Xia, H., Hu, P., and Yu, J. (2026). Lightweight and Efficient Authentication Scheme for Secure Intra/Inter-Domain Communications in the Internet of Drones. *IEEE Transactions on Network Science and Engineering*, 13:3810–3827.

Cilardo, A., Coppolino, L., Mazzocca, N., and Romano, L. (2006). Elliptic curve cryptography engineering. *Proceedings of the IEEE*, 94(2):395–406.

Dobraunig, C., Eichlseder, M., Mendel, F., and Schläffer, M. (2021). ASCON v1.2 - Submission to NIST. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf. (Access: Jan 2026).

Dogan, H. (2023). Protecting UAV-networks: a secure lightweight authentication and key agreement scheme. In *7th International Conference on Cryptography, Security and Privacy*, CSP, pages 13–21, New Jersey, USA. IEEE. doi: https://doi.org/10.1109/CSP58884.2023.00010.

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

Grand View Research, I. (2025). Americas UAV Market (2025 - 2033). https://www.grandviewresearch.com/industry-analysis/americas-uav-market-report. (acesso em 22 dezembro 2025).

Kumar, N., Nehal, A., Singh, A. V., Kandpal, K., and Goswami, M. (2025). Efficient, reliable, and secure PUF architecture with temperature invariance and ML attack resilience. *Integration*, 106:102538. doi: https://doi.org/10.1016/j.vlsi.2025.102538.

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.

Mehrabi, M. A., Doche, C., and Jolfaei, A. (2020). Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module. *Transactions on Computers*, 69(11):1707–1718.

NS-3, C. (2025). NS-3 Discrete-event Network Simulator. https://www.nsnam.org. (accessed 10 december 2025).

Patel, A. and Cherukuri, A. K. (2025). Analysis of light-weight cryptography algorithms for uav-networks. *arXiv preprint arXiv:2504.04063*.

Turan, M. S., McKay, K. A., Chang, D., Kang, J., and Kelsey, J. (2025). Ascon-Based Lightweight Cryptography Standards for Constrained Devices. *NIST SP 800*, 232:1–41.

Xia, T., Wang, M., He, J., Lin, S., Shi, Y., and Guo, L. (2023). Research on Identity Authentication Scheme for UAV Communication Network. *Electronics*, 12(13):2917. doi: 10.3390/electronics12132917.

Yates, R. D., Sun, Y., Brown, D. R., Kaul, S. K., Modiano, E., and Ulukus, S. (2021). Age of Information: An Introduction and Survey. *Journal on Selected Areas in Communications*, 39(5):1183–1210. doi: 10.1109/JSAC.2021.3065072.

Zhang, Y., Meng, L., Gan, J., and Huang, Z. (2023). A Novel and Efficient Authentication Scheme Based on UAV-UAV Environment. *Wireless Communications and Mobile Computing*, 2023(1):7107015. doi: 10.1155/2023/7107015.