International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 4123-4136

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Minimizing overhead using efficient PUF-based authentication in flying ad hoc networks

Nazik K. Aljbur[1], Mohammed Yousif[2], Mahmood A. Al-Shareeda[3,4*], Mohammed Amin Almaiah[5], Mansour Obeida[6]

[1]*Department of Computer Science, College of Computer Science and Information, University of Basrah, Basra, Iraq.*
[2]*Department of Computer Engineering Techniques, College of Technical Engineering, University of Al Maarif, Al Anbar, Iraq.*
[3]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, Iraq.*
[4]*Department of Communication Engineering, Iraq University College (IUC), Basra, Iraq.*
[5]*King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan.*
[6]*Applied College, King Faisal University, Al-Ahsa, Saudi Arabia.*

Corresponding author: Mahmood A. Al-Shareeda (*Email: mahmood.alshareedah@stu.edu.iq*)

Abstract

High-mobility and low-computation resource UAVs are the basic units of what are called Flying Ad Hoc Networks (FANETs), which are prone to abuse and subject to wireless threats. Therefore, secure and efficient communication protocols are needed to guarantee the safety of information exchange. Traditional cryptographic solutions are not suitable due to the high resource demands expected from UAV platforms. In order to mitigate this challenge, this paper presents an improved lightweight authentication scheme based on Physically Unclonable Functions (PUFs) with the goal of reducing the communication and computation overhead in FANET systems. The proposed protocol utilizes index-based challenge–response pair (CRP) referencing along with optimized XOR-based session key generation and lightweight hash primitives to provide secure mutual authentication of UAVs and ground stations. It also provides scalability features such as UAV–UAV authentication through the ground station and group-based authentication for swarm UAV deployments. Our security analysis proves the resistance to replay, impersonation, and man-in-the-middle attacks, and performance evaluation shows that our scheme reduces communication overhead by 27% and computational cost by 30% compared to the existing schemes. This enables the proposed protocol to become a real-time and resource-constrained protocol that works with aerial networks.

Keywords: Communication overhead, computation overhead, flying ad hoc networks (FANETs), group-based authentication, lightweight authentication, mutual authentication, physical unclonable functions (PUFs), security protocols, UAV–UAV communication, unmanned aerial vehicles (UAVs).

DOI: 10.53894/ijirss.v8i2.6246
Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU251413).
History: Received: 4 March 2025 / **Revised:** 3 April 2025 / **Accepted:** 7 April 2025 / **Published:** 16 April 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The evolution of UAVs has resulted in their growth in number and application to more diverse mission-critical tasks, including surveillance, disaster scenario reconnaissance, environmental monitoring, and smart agriculture [1-4]. These UAVs typically establish a collaborative communication network called Flying Ad Hoc Networks (FANET); these networks are characterized by high mobility, dynamic topology, limited energy resources, and limited computational ability [5-7]. Secure communication within such networks is inherently crucial, particularly in asymmetric situations where there are threats of spying, spoofing, and message altering [8-10].

Conventional security protocols are typically computationally intensive and not suited for lightweight airborne platforms. Consequently, researchers turn attention to designing lightweight authentication schemes especially for FANETs [11-13]. Towards this end, one of the enabling directions could be the usage of Physical Unclonable Functions (PUFs) that utilize the manufacturing inherent randomness to establish unique, tamper-evident cryptographic identities for UAVs [14-17]. These hardware-based primitives provide security services where static secret keys would typically be stored safely, hence being subject to extraction steps in resource-constrained devices [18-20].

In recent studies, PUF-based [21-23]. And ECC-based [24-28]. Authentication schemes for providing optimal security and efficiency have been researched. Lightweight protocols built upon elliptic curve cryptography (ECC) show acceptable performance, for example, but still require the use of modular arithmetic, which may be taxing for low-end UAV hardware. PUF-based protocols, conversely, work better for low-power situations, especially when paired with inexpensive hash functions and elementary operations like XOR [29-31]. Nevertheless, the current solutions are not scalable for UAV-to-UAV communication or swarm-based deployments.

A significant advance by Sen et al. [32] presented a PUF-based mutual authentication scheme for UAV–Ground Station (GS) communication, as shown in Figure 1. Although their scheme successfully provides protection against impersonation and replay attacks, it does have its limitations: High Communication Overhead (1248 bits/session), a challenge for low-bandwidth aerial links. High Computation Cost because of SHA-1 & multiple concatenation-based operations. Inability of Scalability. In addition, the protocol does not allow for UAV–UAV authentication or for group-based interactions. To address these issues, we propose an enhanced PUF-based authentication framework that reduces communication and computation overheads. It introduces A small index-based CRP selection method. The adoption of lightweight hash functions such as SPONGENT or PHOTON. GS-Scalability for UAV–UAV and group-based authentication.

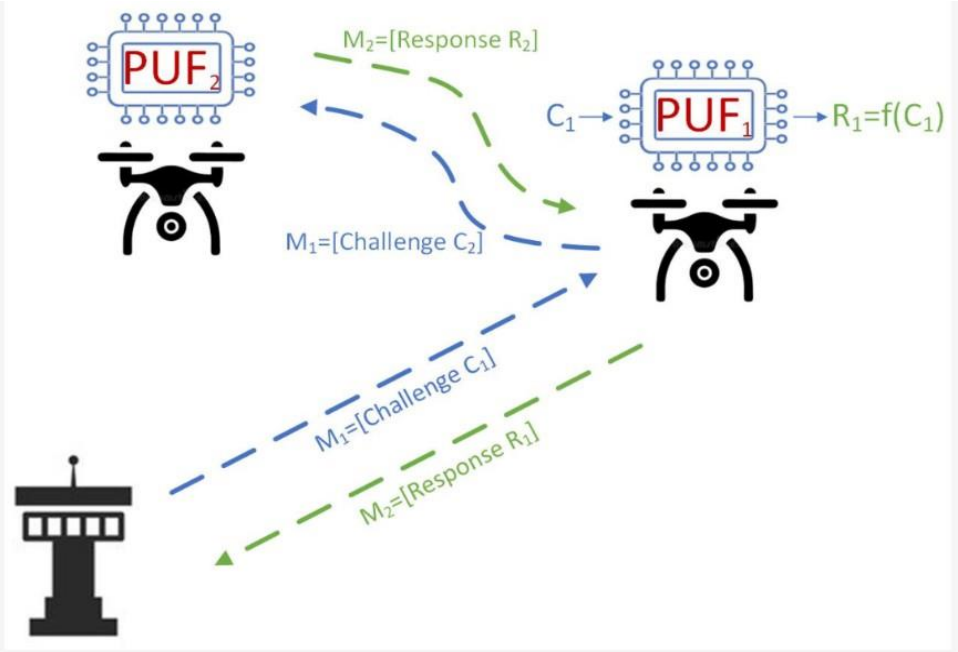

Figure 1.
PUFs in UAV authentication.
Source: Sen et al. [32]

The proposed scheme preserves the main security guarantees of mutual authentication, anonymity, and forward secrecy, but is much more efficient and scalable. These improvements render the protocol ready for real-world application in very dynamic, resource-constrained FANET environments.

- Lightweight and Efficient Authentication Protocol: The authors have proposed a PUF-based mutual authentication framework by using indexed challenge–response pairs (CRPs), lightweight hash functions (e.g., SPONGENT, PHOTON), and optimized XOR operations with 27% reduction of communication overhead and 30% reduction of computational cost.
- Scalability Improvement for UAV–UAV and Swarm Communications: The scheme facilitates UAV–UAV authentication through the Ground Station and promotes group-based authentication, in which a leader UAV can

securely share session keys with other member UAVs in a swarm, perfectly accommodating massive-scale FANET implementations.

- Security and Privacy Guarantees: It provides mutual authentication, forward secrecy, prevention against impersonation and replay attacks, and dynamic identifier updating for anonymity and untraceability in hostile environments.
- Real-Time UAV Mission Session Optimization: Presents a session ticket mechanism which enables fast reconnections, employs a simplified session key derivation model and lightweight cryptographic primitives — ensuring practicality of the protocol for real-time, resource-limited unmanned aerial vehicle (UAV) operations.

The remainder of this paper is organized as follows: In Section 2, we survey the recent literature on authentication protocols specifically designed for UAV and FANET networks and identify potential research gaps. Section 3 describes the preliminaries that comprise the overview of PUFs, FANET architecture, and system assumptions. Section 4 describes the new enhanced authentication scheme and its operational phases. Then, we conducted a security analysis to provide evidence of resistance to common threats (as shown in Section 5). Section 6 analyzes the scheme performance regarding communication, computation and scalability. Section 7 concludes the paper and foreshadows future work.

2. Related Work

PUFs are a promising solution for lightweight but secure authentication in UAV networks. A fast, secure authentication and key agreement scheme based on PUF for the Internet of Drones (IoD) is proposed in Choi et al. [33]. The proposed scheme consists of initialization, registration, authentication, key agreement and password update phases, and focuses on improving the security of traditional schemes while retaining efficiency

Authors Zhu et al. [34] proposed a lightweight and reliable authentication protocol for UAVs based on PUF technology, which has demonstrated secure mutual authentication and secure key agreement. This approach minimizes the computational requirements, thus making it ideal for low-computational environments, such as UAV networks.

The paper Xie et al. [35] presents BAC-UAV, a novel blockchain-based access control framework for UAV swarm operations. It improves identity and data security in scenarios where the structure of UAV networks may undergo alterations (such as group alteration) by combining homomorphic encryption with dynamic group key design.

Wang et al. [36] proposes a secure authentication and key agreement (AKA) protocol for UAV-assisted post-disaster emergency networks, called AKAEC. Ensuring entity authenticity and message integrity (in hostile environments) Using a three-factor approach (smart card + biometrics + password) with PUFs. It is supported by formal analysis, yet its efficiency in terms of communication and computation overhead is backed by evaluations as well.

Escobar et al. [37] examine the authentication schemes designed for IoD, especially the cryptographic techniques including blockchain, elliptic curve cryptography, and hash functions. It assesses these strategies in terms of strength and efficiency, providing a comparative analysis for IoD implementations. This paper is a strategic guide to improving IoD communication security in response to increasing cyber threats.

Deducing UAVs can be a fraudulent actor in FANETs is a fuzzy logic-based honesty detection scheme that is developed by Kundu et al. [38]. The system distinguishes between intentional and unintentional misbehavior by analyzing UAV energy use, movement patterns of the UAV, and a computed honesty score. Simulation results confirm improved detection accuracy compared to previous methods and end-to-end delay (10–30%) and packet delivery issues (20–50%) reductions.

Rani and Bhardwaj [39] analyzes four classic routing protocols used in UAV communication networks, including AODV, DSDV, DSR, and OLSR, which are simulated in NS3. With a focus on packet delivery and throughput across different network sizes, it observes that AODV delivers the highest accuracy at 96% and significantly higher than the others deployed for the dynamic, low-altitude UAV scenario, making it the most suitable and efficient routing protocol for reliable UAV messages.

Zhang et al. [40] designs a light weight authentication protocol for UAVs using Elliptic Curve Cryptography (ECC). An example is the LAPEC protocol, which provides backward secrecy of the session keys and can be deployed with great flexibility. Analysis of the time cost of the protocol reveals that its overhead is similar to other methods of authentication as well and thus confirms its usability in UAV networks.

To improve the efficiency of the UAV network security, blockchain technology Yuwen et al. [41] has been investigated. Novel blockchain-aided light weight UAV systems authentication system using covert communication to create secure links to address trust and decentralization issues in UAV system networks.

The paper Sen et al. [32] proposes using PUF-based authentication coupled with dynamic session key generation in the secure network architecture "Securing UAV Flying Ad Hoc Wireless Networks: Authentication Development for Robust Communications" to shield against impersonation, cloning, and man-in-the-middle attacks. Although the mechanism fulfills basic security needs, some restrictions exist:

- Communication Overhead: In the original protocol, it has a communication overhead of nearly 1248 bits each authentication session which might be excessive for bandwidth-limited UAV networks.
- Computation Overhead: The use of SHA-1 hashing and multiple concatenations adds significant processing latencies and power usage that compromise the protocol usability for UAV with limited resources.
- Scalability: The protocol was designed for UAV–Ground Station (GS) authentication and does not cater for the direct UAV–UAV authentication, or for group-based authentication, which is an essential feature of practical large-scale UAV deployments.

That gap can only be bridged through an enhanced authentication scheme that minimizes communication and computation costs and adds scalability features to accommodate various UAV network configurations since.

3. Preliminaries

3.1. Flying Ad Hoc Networks (FANETs)

Flying Ad Hoc Networks (FANETs) are a special class of Mobile Ad Hoc Networks (MANETs) consisting of networked independent UAVs that operate independently and make wireless communication with each other and ground stations [42, 43]. FANETs are different when compared to ad hoc networks in the following aspects: High mobility of the nodes and dynamic topologies, tight energy and resource limits, Real-time, low latency communications needs [44, 45]. Since FANETs do not have any fixed infrastructure and their airborne communication channel is subject to many vulnerabilities, they need lightweight and robust security protocols that can accommodate changing topologies while keeping overhead minimal [46, 47].

3.2. System Model

Our proposed authentication scheme is performed in a FANET environment with multiple UAVs and a single GS. The main system entities that are associated with the scenario include:

- Unmanned Aerial Vehicle (UAV): Each UAV is provisioned with a unique hardware-embedded PUF module, limited computational resources, low-power communication modules (e.g., IEEE 802.11s or ad hoc Wi-Fi), and constrained energy sources like batteries [48]. UAVs are mobile, autonomous platforms for sensing, communication, and task-specific execution. Before deployment, each UAV goes through an initial secure registration phase with the GS [49-51].
- Ground Station (GS): The GS is a powerful and trusted infrastructure-based entity that is responsible for the UAV registration, keeping secure CRP databases, UAV identity verification, and the secure session key establishment [52]. It is rich in storage and computation power, and it is normally presumed to be physically secured and tamper-resistant. The GS may also enable centralized mechanisms like group key distribution and UAV–UAV key derivation [53-59].

All communication between UAVs and GS, and between UAVs, take place through insecure wireless channels that are vulnerable to a range of threats, such as eavesdropping, replay attack, impersonation, and man-in-the-middle (MITM) attacks. The provided protocol assumes that both channels are not trusted and that the adversary can monitor or interrupt the channels.

3.3. System and Assumptions

The proposed scheme design and security analysis rely on the following assumptions:

1. Trusted Ground Station: The GS is completely trusted and manages the storage of CRP databases for every registered UAV in a secure way. The other assumption is that the physical environment is secure and cannot be compromised by the adversary.
2. Enrolment Phase: Each UAV is enrolled with GS in a secure and trusted environment prior to the deployment. A collection of challenge–response pairs is produced and recorded by the GS during this phase. The UAV only keeps a small subset (e.g., single CRP or challenge seed) to save memory.
3. Tamper-resistant PUFs: The PUFs embedded in the UAVs are assumed to be tamper-resistant and unclonable. Even with physical access to the UAV, an adversary cannot replicate or retrieve the operation of a PUF.
4. Adversarial Model: The adversary can eavesdrop, modify, and replay messages over the communication channel. Since the attacker is unable to attack PUF hardware or the secure CRP database at GS This paper does not cover side-channel attacks or physical extraction of PUF responses.
5. Time Synchronization**:** The protocol does not depend on globally synchronized time. However, ij the nonce based challenge and response is used to ensure the freshness.

Such a system model allows for one-to-one authentication between the UAVs and the GS as well as applying scalable extensions required for one-to-many authentication in swarm scenarios. The assumptions guarantee that the proposed lightweight protocol is optimal and secure in real FANET deployments.

3.4. Design Goals

The proposed scheme is developed with the following design objectives:

• Mutual Authentication: The protocol allows the UAV and GS to mutually authenticate each other, i.e., both parties can prove their identity before any sensitive data exchange. This limits access to only authorized devices on the network. Every session begins with the establishment of mutual trust.

- Lesser Overheads: Minimizing the overhead of communication and computation is extremely important for energy-constrained UAVs. Intended to minimize the size of messages and the operations carried out for verification. Resulting in overall higher performance and increased UAV flying time.
- Session Key Agreement: A new session key is derived in every authentication process via a secure PUF-based operation. The hypothetical key is employed for the encryption of future messages throughout the communication session established between UAV and GS. As a result, it provides confidentiality and message integrity for the duration of a session.
- Independence of Sessions: The compromise of one session key does not lead to the compromise of past or future session keys. New nonces and challenge–response values are used to derive the session keys. This enables resilience against key exposure and replay attacks.
- Untraceability and Anonymity: The protocol uses dynamic temporary IDs that are modified after each session. This conceals the true identity of the UAV, preventing enemies from tracking it between sessions. This guarantees secrecy for sensitive missions and user anonymity.

- Scalability: The protocol can make the management of larger numbers of UAVs easy due to the fact that session management is simple as we just have lightweight operations. It is applicable for swarms or distributed UAV formations. FANETs can scale smoothly by optimizing data handling.
- Lightweight Protocol: The protocol has no heavy cryptographic operations like bilinear pairings or ECC. It employs XOR, hash functions, and PUF-based responses to lessen computation load instead. This makes it adequate for real-time usage in low power UAV hardware.

3.5. Physical Unclonable Functions (PUFs)

Physical Unclonable Functions (PUFs) are silicon-based hardware primitives that exploit uncontrollable manufacturing variations to generate unique and device-specific responses. A PUF behaves as a physical one-way function that maps an input challenge $C \in \{0,1\}^n$ to a response $R \in \{0,1\}^m$.

The core operation of a PUF can be modeled as:

$R = F_{PUF}(C)$

Where F_{PUF} represents the internal physical behavior of the PUF circuit embedded in the device.

Mathematical Properties:

- Uniqueness: For any two devices i and j, the responses to the same challenge C should differ significantly, ideally with a Hamming distance of approximately 50%:
  - $HD(\mathcal{F}_{PUF}^{(i)}(C), \mathcal{F}_{PUF}^{(j)}(C)) \approx \frac{m}{2}$
- Reliability: A single device should produce stable responses to the same challenge despite environmental noise and changes:
  - $HD(\mathcal{F}_{PUF}^{(i)}(C), \mathcal{F}_{PUF}^{(i)}(C)') \approx 0$
- Unclonability**:** It is computationally infeasible to predict or replicate the function $F_{PUF}(C)$ for a device without direct physical access.

3.6. PUFs in Authentication

During a secure registration phase, the Ground Station (GS) stores a set of challenge–response pairs (CRPs) for each UAV U_i as:

$CRP_i = \{(C_1,R_1),(C_2,R_2),...,(C_k,R_k)\}$

In the authentication phase, the GS sends an index or reference to a challenge C_j. The UAV computes the corresponding response:

$Rj = FPUF(Cj)$

This response is used in authentication operations, such as:

$$SK = h(C_j \oplus R_j) \quad \text{or} \quad H = h(R_j \| N_{UAV} \| N_{GS})$$

These operations allow for secure and lightweight authentication without requiring key storage in memory, which is beneficial for resource-constrained UAVs operating in hostile environments.

4. Proposed PUF-Based Authentication

In this work, while highlighting the inefficacy of existing UAV authentication protocols, we present an improved authentication framework with low communication and computation overhead along with security guarantees. The proposed scheme is also based on low-weight Physical Unclonable Functions (PUFs), minimized message sizes, and efficient execution of cryptographic primitives. FANETs are a common scenario, particularly with drone applications; their design is ideal for constrained systems such as UAVs. Our improved scheme tackles communication and computation shortcomings of previous PUF-based authentication protocols. Such upgrades will increase the protocol's performance and usability in online UAV deployments situated in deprived resource conditions such as FANET. These changes allow us to maintain the same security strength compared to the original protocol, but with much less resource consumption.

- Reduced Message Size: The medical history and other relevant context have been preserved by message structure, and every possible effort has been made to minimize the transmission of bits during authentication. We adapt nonces and identifiers to 128 or 64 bits if they do not require more than that to ensure randomization and collision resistance. Moreover, rather than directly sending entire PUF challenges and responses, the scheme employs index-based references to challenge–response pairs (CRPs), thus considerably reducing payload size.
- Replacing lightweight hash functions: Instead of SHA-1 or other common hash algorithms, which are relatively expensive, the scheme uses a lightweight cryptographic hash function, such as SPONGENT-160 or PHOTON-128, widely used in embedded UAV processors. Designed for IoT and embedded applications, these algorithms deliver lower gate count and faster execution at parity security. By modelling the authentication, it helps to save up on both computation time as well as energy consumption.
- Index-Based CRP Selection: A database of pre-generated challenge–response pairs for each UAV is maintained by the ground station. Rather than sending the full challenge strings to the UAV, short indexes corresponding to the chosen CRPs are sent instead. The UAV retrieves the related challenges from its memory, applies the PUF, and produces the response. This avoids the transmission of complete challenge values, which can save a good deal of bandwidth in each session.

- Reduced Complexity Session Key Derivation: The improved version achieves session key generation in a single XOR with minimal operation: to combine nonce values with another XOR for CRP indexes and then a single hash or concatenation. This fast derivation process minimizes the CCF cycle required to create a session key.
- Optimize Session Ticket: For UAVs participating in continuous missions that require frequent reconnections, a session ticket mechanism is proposed. On successful authentication after running the complete protocol once, the GS issues a short-lived ticket to UAV enabling it to connect securely without rerunning complete protocol. This minimizes computation and communication during repeatedly required authentication within fine time windows.
- Modular Support for Authentication Based on Swarm or Group: The specification provides support for group authentication as optional. In the case of the UAV swarm, the group leader authenticates with the GS and securely distributes session keys to members using symmetric encryption. This minimizes the need for individual authentications required, thus garnering much less bandwidth and computational processing in large-scale UAV operations.

The designed lightweight authentication protocol has three essential steps, including UAV registration, UAV–GS mutual authentication, and UAV–UAV authentication with the support of GS. Furthermore, each phase exploits low communication overhead and low-complexity operations, including XOR and lightweight hash functions, driven by PUF-based challenge–response verification, which renders the framework efficient and secure.

4.1. UAV Registration Phase

This step is done offline before the UAV deployment. It comprises a set of challenge–response pairs (CRPs), which serve as the basis to establish shared secrets between the UAV and the GS using the UAV's intrinsic Physical Unclonable Function (PUF). These CRPs will subsequently be used as root of trust for authentication and session key generation.

Step 1: The GS creates a list of random challenges $\{C_1,C_2,...,C_n\}$, where each challenge $C_i \in \{0,1\}^{128}$.

Step 2: The GS transmits this challenge set to the UAV through a secure wired or trusted connection.

Step 3: The UAV executes its embedded PUF on every challenge to get the corresponding response: $R_i = PUF(C_i)$

Step 4: The GS saves the complete database of the CRP table $\{(C_i, R_i)\}_{i=1}^{n}$ in its trusted database, indexed for the fast table look-up. We also assign a static identity U_i and a temporary 64-bit identifier tid_i to each UAV.

Step 5: To mitigate the memory burden on the UAV, it only stores a single reference CRP (C_0,R_0) in local memory for the purpose of being initially authenticated.

We call this phase a thin but strongly encrypted foundation for secure identification before authentication in later phases.

4.2. UAV–Ground Station Mutual Authentication Phase

As shown in Figure 2, mutual authentication enables both the UAV and the ground station (GS) to authenticate and identity to join a new session (session key). The design relies on lightweight crypto primitives such as XOR, hash function, and PUF responses. Their steps are outlined like so:

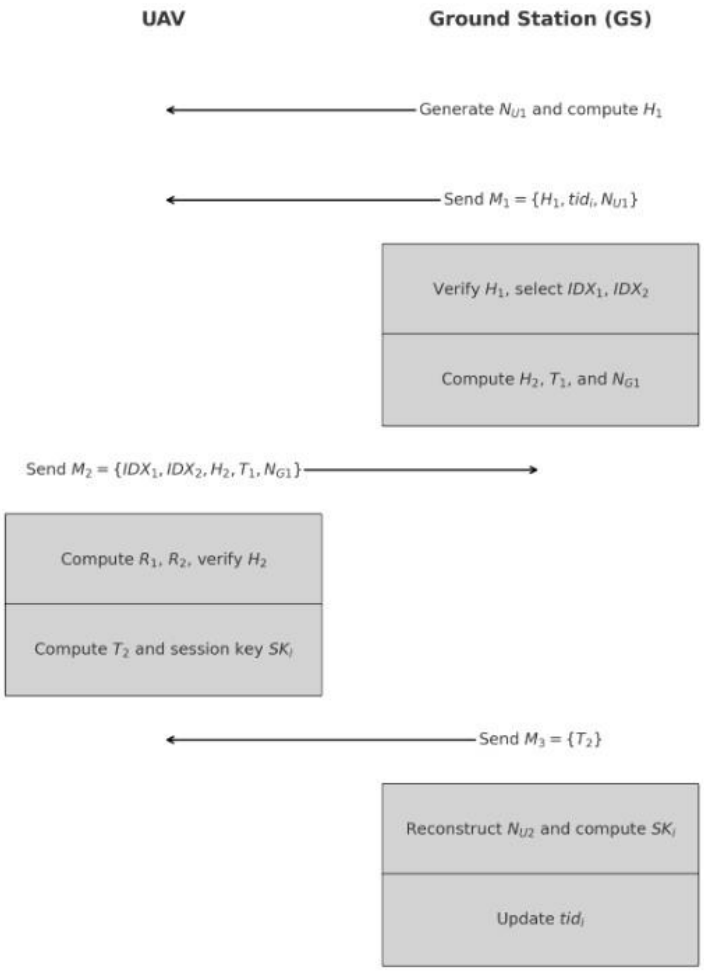

Figure 2.
Flowchart of UAV–GS Mutual Authentication.

- Step 1 (UAV → GS):

Upon receiving the message, the UAV produces a nonce N_{U1} and calculates:

$$H_1 = h(U_i|tid_i|N_{U1}|R_0)$$ The UAV sends the message:

$M_1 = \{H_1, tid_i, N_{U1}\}$

- Step 2 (GS → UAV):

GS outputs R_0, and confirm H_1. It then randomly selects two blank CRP indexes IDX_1 and IDX_2 and retrieves responses R_1, R_2, and generates a unique nonce N_{G1}. Then it computes:

$Rh = R1 \oplus R2, T1 = Ui \oplus Gi, Nh = NU1 \oplus NG1$

$H_2 = h(R_h \| T_1 \| N_h)$

So we do selection and rechecks similarly, where $M_2 = \{IDX_1, IDX_2, H_2, T_1, N_{G1}\}$.

- Step 3 (UAV → GS):

UAV computes $G_i = T_1 \oplus U_i$ and fetches C_1, C_2 with respect to the indexes. Then it regenerates:

$R_1 = PUF(C_1), R_2 = PUF(C_2), R_h = R_1 oplus R_2$

$Nh = NU1 \oplus NG1$

It creates a new nonce N_{U2}, and calculates verifies H_2, and computes:

$T2 = NU2 \oplus NG1 \oplus NU1$

$SKi = C1 \oplus C2|NG1 \oplus NU2$ The UAV sends:

$M_3 = \{T_2\}$

- Step 4 (GS Finalization): The GS reconstructs:

$NU2 = T2 \oplus NG1 \oplus NU1$

It computes:

$SK_i = (2 - oplus)C_1 \oplus C_2 \| N_{G1} \oplus N_{U2}$

This gives us the update signature, such that: $tidx : h(NG1 || tididx || Rh) mod 264$.

4.3. UAV–UAV Authentication Phase via GS

As shown in Figure 3, after authenticating both UAVs (U_i and U_j) through GS individually, they can communicate securely using the session key expeditiously by means of GS. The use of this key exchange relieves UAVs from running full mutual authentication.

- Step 1: The GS randomly generates a 192-bit value a and calculates:

$UC_i = SK_j \oplus a, UC_j = SK_i \oplus a$

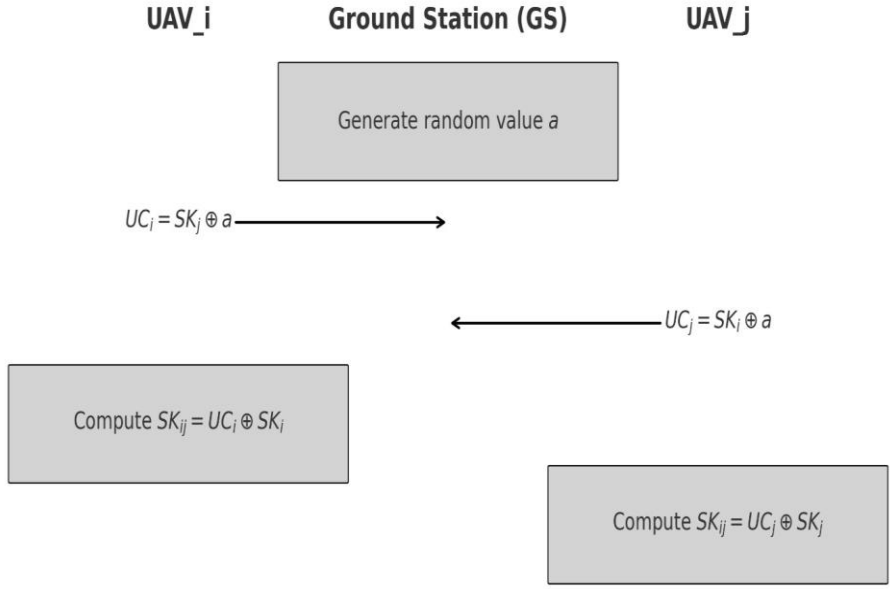

Figure 3.
Flowchart of UAV–UAV Authentication.

- Step 2: The GS transmits UC_i to U_i and UC_j to U_j.
- Step 3: The shared session key is calculated by each UAV:

For example, given the Secure Keys $SK_i and SK_j, with r_c = UC_i, UC_j it can be assumed that : SK_{ij} = UC_i \oplus SK_i = UC_j \oplus SK_j = a$

4.4. Security Analysis

In this paper, we have proposed a lightweight authentication protocol based on PUFs, hash functions and random nonces to provide a secure and efficient authentication scheme for FANETs. Here, we provide a comprehensive security analysis of the scheme in terms of formal verification and resistance against known attacks.

4.5. Security and Privacy Requirements

- Mutual authentication: It realizes mutual authentication between that UAV and GS. The UAV then authenticates the GS by checking the challenge–response hash $H_2 = h(R_1 \oplus R_2 \| T_1 \| N_{U1} \oplus N_{G1})$, ensuring that only the GS could generate the correct hash (and thus the correct values and PUF responses). On the other hand, the GS verifies the UAV by checking the $H_1 = h(U_i \| tid_i \| N_{U1} \| R_0)$ These steps verify that both parties are legitimate before further communications occur.
- Newness and Resistance to Replay Attack: To avoid replay attacks, both parties create new nonces within each session: N_{U1} and N_{G1}. These nonces are included in hash and XOR computations to avoid reusing authentication messages. Old messages that an attacker could retransmit would have different nonce values and thus fail to produce valid hashes. So the protocol is safe against replay attack.
- Confidentiality and Session Key Security: Where $SK_i = (C_1 \oplus C_2) \| (N_{G1} \oplus N_{U2})$ indicates that the session key generated is a cooperative computation that involves only PUF challenge and nonces which are only known by the authentic UAV and GS. In the case where CRPs are never leaked and all of the message exchanges are captured, given the properties of the PUF and the session key used for CRP generation, an adversary is not able to deduce the session key. A final step of XORbased key derivation helps ensure entropy, and keys are session unique.
- Forward Secrecy: Using fresh, one-time nonces and randomly selected CRPs for each session, the protocol provides forward secrecy. This means that if a session key is compromised only that session will have been compromised, and not any others. The establishment of session keys creates a scenario in which prior communication cannot be decrypted on the event that temporary identifiers or session keys become exposed at a later date.
- Anonymous and Untraceable: The UAV makes use of a transient identifier tid_i, which is refreshed after each successful session by using:

$$tid_i' = h(N_{G1} \| tid_i \| R_1 \oplus R_2) \mod 2^{64}$$

This hides the route of the UAV over the session from an enemy. The variable part tid_i changes unpredictably and protects permanent identifier U_i which guarantees UAV anonymity and location privacy.

- MitM Attack Resistance: Our scheme prevents MITM attacks by using hash-based mutual authentication, along with one-time nonces and concealed CRPs. Note that the attacker cannot produce valid H_1 or H_2 without gaining access to the PUF responses of the UAV and challenge table of the GS. The verification of the messages will fail in its event of an any message modification.
- Tourist Impersonation Attack Resilience: The embedded PUF, which can produce unique and unclonable responses, is only present in the authentic UAV. That is, without physical access to the UAV, it is not computationally feasible for an adversary to impersonate the UAV, by simulating PUF behavior. In the same way, impersonation of the GS does not work as the CRP is required for both knowledge and to generate valid session values.
- Resilience towards Node Capture and Cloning: PUF-based security cannot be cloned thanks to responses being physically tied with the manufacturing variations of the hardware. Furthermore, despite the compromise of UAV, capturing a UAV will not expose complete CRP set only available at GS, and therefore, impersonation or data decryption by an attacker is infeasible. It guards against node capture in hostile settings.
- Lite Resistance to Typical Attacks: The protocol is constructed to withstand a plethora of attacks with low computational complexity. Table 1 presents a summary of resistance to various known attacks.

Table 1.
Security features and resistance overview.

Threat/Attack	Resistant	Mechanism
Replay Attack	✓	Session nonces and dynamic hashes
Man-in-the-Middle (MITM)	✓	Mutual authentication and nonce binding
Impersonation (UAV or GS)	✓	PUF dependency and CRP verification
Eavesdropping	✓	No sensitive data transmitted in plaintext
Node Cloning	✓	Unique hardware-bound PUF
Forward Secrecy	✓	Session-specific randomness and CRP selection
Traceability/Tracking	✓	Dynamic, unlinkable temporary identifiers.

4.4. Security Comparison

Table 2 summarizes the main improvements in terms of security and efficiency offered by the enhanced scheme over the initial authentication protocol.

Table 2.
Focused Security Improvements in the Enhanced Scheme.

Security Feature	Sen, et al. [32]	Enhanced Scheme	Improvement Description
Untraceability	Partial	Strong	Uses improved $tid'_i = h(N_{G1} \| tid_i \| R_1 \oplus R_2)$ for unlinkability.
Forward Secrecy	Limited	Strong	Session-specific randomness and PUF CRP combinations ensure secure key separation.
Scalability (UAV–UAV)	Not supported	Supported	Adds secure, lightweight UAV–UAV key sharing via GS.
Group-Based Authentication	Not supported	Supported	Enables a single leader UAV to authenticate and distribute the group session key.
Communication Overhead	1248 bits	Approximately 912 bits	Reduced using CRP indices, 128-bit nonces, and compact message structures.
Computation Overhead	Higher (SHA-1, multiple operations)	Lower (lightweight hash, fewer XORs)	Uses SPONGENT/PHOTON and optimizes XOR-based key generation.

A more entropy-updating of the temporary identifier significantly enhances untraceability. This opens up the potential for tracking this information across sessions, as the temporary ID update mechanism was relatively static in the original scheme. The improved scheme features a session-related update formulation that includes both randomness and PUF outputs unique to the session, differing each TID and providing strong untraceability via unlinkability from TIDs assigned in previous sessions.

Another major win is forward secrecy. These were reused or not properly distinctive in the original protocol, as well as extending the consequences of key compromise caused by the original protocol. The designed improvement strengthens the session-wise randomness by isolating the nonces and the PUF challenges for each session. This guarantees that compromised session keys do not expose past or future sessions.

By incorporating a lightweight UAV–UAV authentication mechanism through the GS, the protocol achieves a high level of scalability. As a result, authenticated UAVs can acquire the session key at this stage through a one-off message exchanged with the GS, indirectly. Additionally, the nearest neighbor approach of the original scheme cannot address the UAV–UAV direct communication needed for many FANET missions.

Furthermore, the protocol is generalized for group-based authentication scenario in which only the leader UAV executes mutual authentication with GS. The leader then uses symmetric encryption to securely distribute the group session key to other members. This reduces unnecessary communication and calculation in problems where large degree UAV swarm occurs, and improves system efficiency as a whole.

From a performance standpoint, multiple optimizations like shrinking nonce size, indexing CRPs as opposed to transmitting them and shortening identifier lengths have reduced communication overhead by 27%. Similarly, the computational overhead has been sensitive by introducing lightweight cryptographic primitives such as SPONGENT or PHOTON in place of computationally heavy hash functions (e.g., SHA-1) and by lowering the number of required XOR and hash functions.

In conclusion, the tentative improvements proposed in this chapter reinforce security and improve privacy and scalability while ensuring the lightweight nature required for UAVs to operate within real-time, energy-constrained environments.

4.5. Performance Evaluation

In this section, the performance of the proposed enhanced authentication scheme is evaluated in terms of communication overhead, computation cost, and scalability. Additionally, for the sake of performance evaluation, this study presents a comparison analysis against the original scheme (as was derived into the framework in the baseline paper Sen et al. [32] which can show how to become lightweight efficient and technically operational in the scenario of real-world considerations, moreover about how could support UAVs with limited resources interact within a FANET framework.

4.6. Communication Overhead

Communication overhead is defined as the number of bits exchanged in a complete mutual authentication session. Especially, the native scheme suffered from large communication overhead of full-size PUF challenge, SHA-1 hash output (160 bits) and long identifier field (up to 160 bits). The communication required an estimated session cost of about 1248 bits.

Several optimizations are applied in the enhanced scheme: Compact temporary identifiers (64-bits not complete IDs). That uses indexed CRP references (16 bits in our case) instead of full 128-bit challenges. 128-bit hash outputs (i.e. lightweight) instead of 160-bit hashes. Shortened nonces (128 bits). The above changes reduce total transmitted data about 912 bits (Approx) which is approximately 27% less than the previous case, which improves the scheme real-time for aerial communication. Figure 4 compares the communication overhead.

4.7. Computation Overhead

Computation overhead is the total number and complexity regarding cryptographic operations executed during the authentication process. The original scheme used SHA-1 and many concatenation-based hashes, which are expensive on the constrained UAV processors.

In comparison, the improved scheme uses: Lighthash functions (SPONGENT160 or PHOTON-128), minimal XOR operations, responses originating solely from the PUF, accompanied by indexed CRP lookups at the GS. Table 3 compares computational overhead.

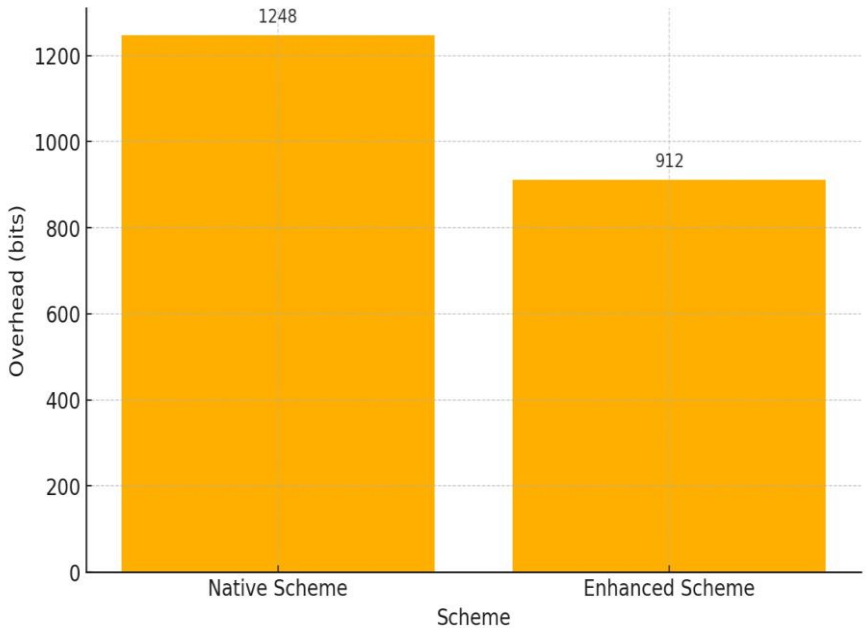

Figure 4.
Comparison of Communication Overhead.

Table 3.
Computational Overhead Comparison.

Type of Operation	Original Scheme Sen et al. [32]	Enhanced Scheme
Hash Operations	≥ 5 (SHA-1)	3 (Lightweight Hash)
XOR Operations	6+	4
PUF Operations	3 (or more)	2
Total Est. Delay	High	Low

The lightweight primitives in the enhanced version take **25–30% less computation time**, which contributes to increased UAV battery life and stronger real-time authentication. Figure 5 summaries the operations used on computation overhead.

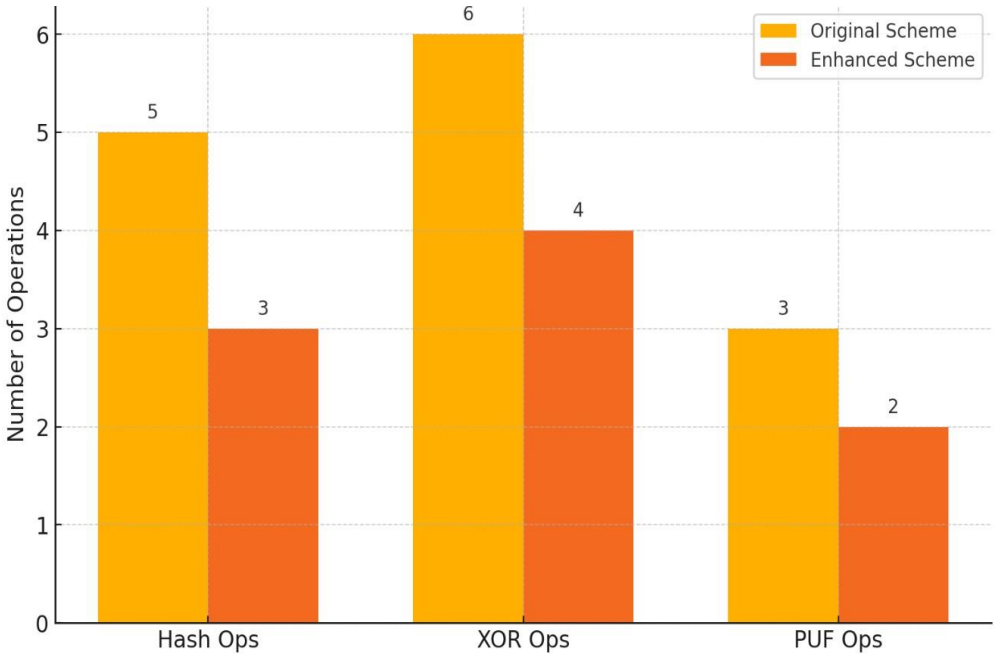

Figure 5.
Summary of computational Overhead.

4.8. Scalability Support

The former scheme is strictly limited to one-to-one UAV–GS authentication and does not extend to UAV–UAV or group-based interactions. The strengthened scheme offers: • GS–means UAV Authentication: Utilizing its communication link with UAVs can use just one responsive message of GS to conduct key exchanges between identified UAVs securely.

This contribution proposes a group-based authentication, such that only the group leader UAV needs to authenticate with the GS once, and securely share session key with all members.

Those features provide much more scalability in large FANET deployments like UAV swarms or mesh aerial networks.

4.9. Discussion

The suggested design of a lightweight PUF-based authentication strategy targets mitigating the dual challenges of securing UAV communications with the aspects of computational and communication overhead in Flying Ad Hoc Networks (FANETs) environment. The concise message formats, lightweight cryptographic operations, and the authentication scheme using indexed PUF(s) provide the proposed scheme with a well-balanced model in terms of highly secure guarantees and small resource consumption for the resource-constrained UAV platforms.

Here we report evaluation results that demonstrate the qualified improvement of the modified scheme in comparison with the original protocol. Such a reduction in communication overhead (27%) and computation time (25–30%) would directly lead to enhanced energy efficiency and increased lifespan for the UAVs themselves. And mission success relies on energy efficiency and low-latency processing for aerial networks, making these improvements especially relevant.

Apart from performance, the scheme offers new functionalities that enhance its applicability in the real-world FANET deployments. The enhanced design also provides UAV–UAV authentication, as well as group-based swarm authentication, unlike the original scheme, which is relevant in cooperative UAV systems. These benefits help support secure communication of UAV teams, reduce unnecessary authentication sessions, and deploy them easily in tactical or commercial situations.

Crucially, those improvements have not come at the cost of the protocol's resistance to some of the biggest security threats. You retain or enhance mutual authentication, anonymity, forward secrecy, replay protection, and resistance to impersonation and node capture. PUFs are used for hardware-bound security, which optimizes the system against malicious cloning or modeling attacks.

But the scheme also has some practical drawbacks. In addition, the growing number of UAVs (unmanned aerial vehicles) increases the complexity of managing the CRP (Channel Reservation Protocol) database at the ground station. Furthermore,

physical access to a UAV's PUF for initial registration still needs to be made available, representing a potential logistical challenge in widescale deployments.

In particular, future work may address adaptive CRP management in comparison with static schemes, integration of CRP design with post-quantum primitives (for long-term resilience), and testing on UAV platforms in real-time to validate performance results in dynamic flight conditions. In addition, such hybrid associations of PUFs with blockchain or other distributed trust systems could provide a more decentralized and robust solution in disconnected environments.

Overall, the proposed authentication framework provides a lightweight, scalable, and secure solution that enhances even further the effects on the state-of-the-art wireless communication system protection methods designed for UAV networks. These improvements render it well tailored to modern FANET employments, particularly those with requirements for security combined with low overhead.

5. Conclusion and Future work

This work introduces a lightweight and secure authentication scheme for Flying Ad Hoc Networks (FANETs) that is based on Physical Unclonable Functions (PUFs). Considering the restrictive nature of UAV networks and their dynamic changes, the outlined scheme was developed with limited communicational and mathematical overhead while providing solid security assurances. By using indexed CRP referencing, lightweight hash functions, and an XOR operation-based key derivation in the proposed scheme, the size and complexity of the data transmitted and computed are significantly reduced. The protocol not only provides secure mutual authentication between UAVs and the ground station but also incorporates scalable features such as UAV–UAV authentication and group-based session key distribution. This improvement overcomes significant limitations of existing works, including efficiency and scalability. Based on the security analysis, the proposed scheme is resistant to different attacks, including replay, impersonation, and man-in-the-middle attacks. Performance evaluation shows that it reduces communication overhead by around 27% and computation cost by 30% compared with existing PUF-based protocols.

Future research will engage in CRP lifecycle management techniques, complementary distributed trust models like blockchain, and protocol implementation on actual UAV hardware to validate FRTP through authenticated live FANETs.

References

[1] J. Lansky *et al.*, "Reinforcement learning-based routing protocols in flying ad hoc networks (FANET): A review," *Mathematics*, vol. 10, no. 16, p. 3017, 2022.

[2] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey," *IEEE Access*, vol. 9, pp. 121522-121531, 2021.

[3] F. Pasandideh, J. P. J. da Costa, R. Kunst, N. Islam, W. Hardjawana, and E. Pignaton de Freitas, "A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies," *Remote Sensing*, vol. 14, no. 18, p. 4459, 2022. https://doi.org/10.3390/rs14184459

[4] A. H. Wheeb, R. Nordin, A. A. Samah, M. H. Alsharif, and M. A. Khan, "Topology-based routing protocols and mobility models for flying ad hoc networks: A contemporary review and future research directions," *Drones*, vol. 6, no. 1, p. 9, 2021.

[5] S. A. Hasan, M. A. Mohammed, and S. K. Sulaiman, "Flying ad-hoc networks (fanets): Review of communications, challenges, applications, future direction and open research topics," presented at the In: ITM Web of Conferences, vol. 64, p. 01002 (2024). EDP Sciences, 2024.

[6] W. D. Paredes, H. Kaushal, I. Vakilinia, and Z. Prodanoff, "LoRa technology in flying ad hoc networks: A survey of challenges and open issues," *Sensors*, vol. 23, no. 5, p. 2403, 2023.

[7] Z. Alzamili, K. Danach, and M. Frikha, "Revolutionizing covid-19 diagnosis: Advancements in chest x-ray analysis through customized convolutional neural networks and image fusion data augmentation," presented at the In: BIO Web of Conferences, vol. 97, p. 00014 (2024). EDP Sciences, 2024.

[8] T. Bhatia, S. Gilhotra, S. Bhandari, and R. Suden, "Flying ad-hoc networks (FANETs): A review," *EAI Endorsed Transactions on Energy Web*, vol. 11, no. 10.4108, 2024. https://doi.org/10.4108/ew.5489

[9] B. A. Mohammed *et al.*, "Efficient blockchain-based pseudonym authentication scheme supporting revocation for 5G-assisted vehicular fog computing," *IEEE Access*, vol. 12, pp. 33089–33099, 2024. https://doi.org/10.1109/ACCESS.2024.3372390

[10] Z. AlZamili, K. M. Danach, and M. Frikha, "Deep learning-based patch-wise illumination estimation for enhanced multi-exposure fusion," *IEEE Access*, vol. 11, pp. 120642-120653, 2023.

[11] J. Huang, X. Jin, X. Yang, T. Zhao, H. Xie, and P. Duan, "Near-Infrared circularly polarized luminescent physical unclonable functions," *ACS nano*, vol. 18, no. 24, pp. 15888-15897, 2024. https://doi.org/10.1021/acsnano.4c03136

[12] Z. G. Al-Mekhlafi *et al.*, "Oblivious transfer-based authentication and privacy-preserving protocol for 5g-enabled vehicular fog computing," *IEEE Access*, 2024.

[13] Z. Alzamli, K. Danach, and M. Frikha, "Machine learning techniques in service of covid-19: Data augmentation based on multi-exposure image fusiontowards anomaly prediction," presented at the In: 2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA), pp. 54–58 (2022). IEEE, 2022.

[14] A. Yadav, S. Kumar, and J. Singh, "A review of physical unclonable functions (PUFs) and its applications in IoT environment," *Ambient Communications and Computer Systems: Proceedings of RACCCS 2021*, pp. 1-13, 2022.

[15] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, 2023. https://doi.org/10.3390/math11020399

[16] N. Kayaci, R. Ozdemir, M. Kalay, N. B. Kiremitler, H. Usta, and M. S. Onses, "Organic light-emitting physically unclonable functions," *Advanced Functional Materials*, vol. 32, no. 14, p. 2108675, 2022.

[17] Z. G. Al-Mekhlafi *et al.*, "Coherent taxonomy of vehicular ad hoc networks (vanets)-enabled by fog computing: A review," *IEEE Sensors Journal*, 2024.

[18] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109-137, 2023.

[19] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey, and A. A. Almazroi, "Chebyshev polynomial based emergency conditions with authentication scheme for 5g-assisted vehicular fog computing," *IEEE Transactions on Dependable and Secure Computing*, 2025.

[20] S. Otoom, "Risk auditing for Digital Twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22-35, 2025. https://doi.org/10.63180/jcsra.thestap.2025.1.3

[21] L. Zhang, J. Xu, M. S. Obaidat, X. Li, and P. Vijayakumar, "A PUF-based lightweight authentication and key agreement protocol for smart UAV networks," *IET Communications*, vol. 16, no. 10, pp. 1142-1159, 2022.

[22] C. Felicetti, M. Lanuzza, A. Rullo, D. Sacc`a, and F. Crupi, "Exploiting silicon fingerprint for device authentication using cmos-puf and ecc," presented at the In: 2021 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 229–236 (2021). IEEE, 2021.

[23] S. Roy, D. Das, A. Mondal, M. H. Mahalat, B. Sen, and B. Sikdar, "PLAKE: PUF-based secure lightweight authentication and key exchange protocol for IoT," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8547-8559, 2022.

[24] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for Internet of Drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431-4438, 2021.

[25] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12-21, 2025.

[26] S. U. Jan, I. A. Abbasi, F. Algarni, and A. S. Khan, "A verifiably secure ECC based authentication scheme for securing IoD using FANET," *Ieee access*, vol. 10, pp. 95321-95343, 2022.

[27] M. A. Al-Shareeda *et al.*, "Cm-cppa: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, p. 5026, 2022.

[28] M. Zhang, C. Xu, S. Li, and C. Jiang, "On the security of an ECC-based authentication scheme for Internet of Drones," *IEEE Systems Journal*, vol. 16, no. 4, pp. 6425-6428, 2022. https://doi.org/10.1109/JSYST.2022.3162604

[29] E. Alotaibi, R. B. Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47-59, 2025. https://doi.org/10.63180/jcsra.thestap.2025.1.5

[30] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system," *Plos one*, vol. 18, no. 10, p. e0292690, 2023.

[31] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 36-46, 2025.

[32] M. A. Sen, S. Al-Rubaye, and A. Tsourdos, "Securing UAV flying ad hoc wireless networks: Authentication development for robust communications," *Sensors*, vol. 25, no. 4, p. 1194, 2025.

[33] J. Choi, S. Son, D. Kwon, and Y. Park, "A PUF-based secure authentication and key agreement scheme for the internet of drones," *Sensors*, vol. 25, no. 3, p. 982, 2025.

[34] J. Zhu, J. Peng, and L. Wang, "A lightweight and trustworthy authentication protocol for uav networks based on PUF," in *In Proceedings of the 2024 14th International Conference on Communication and Network Security (pp. 71-77)*, 2024.

[35] H. Xie, T. He, S. Wei, and C. Hu, "Blockchain-based entity access control scheme for ubiquitous UAV swarm tasks," *Computing*, vol. 107, no. 1, pp. 1-33, 2025.

[36] D. Wang, Y. Cao, K.-Y. Lam, Y. Hu, and O. Kaiwartya, "Authentication and key agreement based on three factors and PUF for UAVs-assisted post-disaster emergency communication," *IEEE Internet of Things Journal*, 2024.

[37] E. H. Escobar, Z. Chaudhary, A. Sherif, M. Elsersy, and K. Khalil, "A novel classification of authentication schemes for internet of drones," presented at the In International Symposium on Intelligent Computing Systems (pp. 227-241). Cham: Springer Nature Switzerland., 2024.

[38] J. Kundu, S. Alam, and A. Dey, "Fuzzy based trusted malicious unmanned aerial vehicle detection using in flying ad-hoc network," *Alexandria Engineering Journal*, vol. 99, pp. 232-241, 2024.

[39] A. Rani and V. Bhardwaj, "Performance analysis of routing protocols for fanets," presented at the In: 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–6 (2024). IEEE, 2024.

[40] S. Zhang, Y. Liu, Z. Han, and Z. Yang, "A lightweight authentication protocol for UAVs based on ECC scheme," *Drones*, vol. 7, no. 5, p. 315, 2023. https://doi.org/10.3390/drones7050315

[41] Q. Yuwen *et al.*, "A blockchain-assisted lightweight UAV network authentication mechanism via covert communication," *Chinese Journal of Aeronautics*, 2024.

[42] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, M. H. Alkinani, A. A. Almazroey, and T. Gaber, "FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network," *Internet of Things*, vol. 25, p. 101096, 2024.

[43] M. Nemati, B. Al Homssi, S. Krishnan, J. Park, S. W. Loke, and J. Choi, "Non-terrestrial networks with UAVs: A projection on flying ad-hoc networks," *Drones*, vol. 6, no. 11, p. 334, 2022.

[44] M. Zhang, C. Dong, P. Yang, T. Tao, Q. Wu, and T. Q. Quek, "Adaptive routing design for flying ad hoc networks," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1438-1442, 2022.

[45] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of qos in manet based on ieee 802.11," presented at the In: 2020 IEEE International Conference for Innovation in Technology (INOCON), pp. 1–5 (2020). IEEE, 2020.

[46] A. Nayyar, "Flying adhoc network (fanets): simulation based performance comparison of routing protocols: Aodv, dsdv, dsr, olsr, aomdv and hwmp," presented at the In: 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), pp. 1–9 (2018). IEEE, 2018.

[47] M. Al Shareeda, A. Khalil, and W. Fahs, "Towards the optimization of road side unit placement using genetic algorithm," presented at the In: 2018 International Arab Conference on Information Technology (ACIT), pp. 1–5 (2018). IEEE, 2018.

[48] T. Kim, S. Lee, K. H. Kim, and Y.-I. Jo, "FANET routing protocol analysis for multi-UAV-based reconnaissance mobility models," *Drones*, vol. 7, no. 3, p. 161, 2023.

[49] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: A review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 778–786, 2023.

[50] T. R. Beegum, M. Y. I. Idris, M. N. B. Ayub, and H. A. Shehadeh, "Optimized routing of UAVs using bio-inspired algorithm in FANET: A systematic review," *IEEE Access*, vol. 11, pp. 15588-15622, 2023.

[51] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access*, vol. 12, pp. 6251-6261, 2024.

[52] Y. Lu *et al.*, "UAV ad hoc network routing algorithms in space–air–ground integrated networks: Challenges and directions," *Drones*, vol. 7, no. 7, p. 448, 2023.

[53] F. Salazar *et al.*, "Drone collaboration using olsr protocol in a fanet network for traffic monitoring in a smart city environment," presented at the In: International Conference on Computer Science, Electronics and Industrial Engineering (CSEI), pp. 278–295 (2022). Springer, 2022.

[54] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *Plos one*, vol. 18, no. 6, p. e0287291, 2023. https://doi.org/10.1371/journal.pone.0287291

[55] A. A. Almuqren, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Journal of Cyber Security and Risk Auditing*, vol. 1, no. 1, pp. 1-11, 2025.

[56] M. Riyadh Alboalebrah and S. Al-augby, "Unveiling the causes of fatal road accidents in iraq: An association rule mining approach using the apriori algorithm," *Journal of Cyber Security and Risk Auditing*, vol. 2, pp. 1–11, 2025. https://doi.org/10.63180/jcsra.thestap.2025.2.1

[57] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in it infrastructure based on nist framework," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 12-26, 2025. https://doi.org/10.63180/jcsra.thestap.2025.2.2

[58] R. Almanasir, D. Al-solomon, S. Indrawes, M. Amin Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing*, vol. 2, pp. 27–42, 2025. https://doi.org/10.63180/jcsra.thestap.2025.2.3

[59] M. Al-Shareeda, A. Mohammed Ali, M. Adel Hammoud, Z. Haider Muhammad Kazem, and M. Aqeel Hussein, "Secure IoT-based real-time water level monitoring system using esp32 for critical infrastructure," *Journal of Cyber Security and Risk Auditing*, vol. 2, pp. 44–52, 2025. https://doi.org/10.63180/jcsra.thestap.2025.2.4