IJRCS

International Journal of Robotics and Control Systems
Vol. 6, No. 1, 2026, pp. 577-608
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

ASCEE

EA-UAP: A Software-Engineered Adaptive and Energy-Aware Authentication Protocol for 5G-Enabled UAV Networks

Sari Ali Sari [a,1], Wafaa Mohammed Breesam [b,2], Wafaa M. R. Shakir [c,3], Saima Anwar Lashari [d,4], Mahmood A. Al-Shareeda [e,f,5*], Murtaja Ali Saare [j,6], Mohammed Amin [h,7], Rami Shehab [i,8]

[a] Cyber Security Department, College of Computer Science and Information, University of Basrah, Basrah, Iraq
[b] Department of Technical Pharmacy, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, 51015 Babil, Iraq
[c] De Vinci Higher Education, De Vinci Research Center, 92400 Courbevoie, France
[d] College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia
[e] College of Engineering, Al-Ayen University, 64001, Thi-Qar, Iraq
[f] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[j] Department of Computer Science, College of Computer Science and Information, University of Basrah, Basrah, Iraq
[h] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[i] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
[1] sari.ali@uobasrah.edu.iq; [2] wafaa.breesm@atu.edu.iq; [3] wafaa.shakir@devinci.fr; [4] s.lashari@seu.edu.sa;
[5] mahmood.alshareedah@stu.edu.iq; [6] murtaja.sari@uobasrah.edu.iq; [7] m.almaiah@ju.edu.jo; [8] Rtshehab@kfu.edu.sa
[*] Corresponding Author

ARTICLE INFO

Article History
Received November 12, 2025
Revised December 30, 2025
Accepted February 18, 2026

Keywords
Unmanned Aerial Vehicles (UAVs);
Internet of Drones (IoD);
Physical Unclonable Function (PUF);
Energy-Aware Security;
Software Engineering;
Design Patterns;
Post-Quantum Readiness

ABSTRACT

Unmanned Aerial Vehicles (UAVs) deployed in 5G-powered Internet of Drones (IoD) systems need secure authentication solutions, that can achieve a high level of security assurance yet would not impose an excessive overhead on the onboard energy consumption. This work introduces EA-UAP, a software-engineered adaptive and energy-aware authentication mechanism suitable for 5G-connected UAV environments. The research input is a dynamic adaptive scheduling mechanism from full authentication, fast re-authentication and session extension modes with the consideration of two context mitigation parameters, Security Risk Level (SRL) and Energy Stress Level (ESL). EA-UAP couples hardware-based PUFs with a modular and layered software architecture, focusing on maintainability and deployability. Formal security verification formally secures against replay, impersonation and man-in-the-middle attacks using Mao–Boyd logic in conjunction with the Scyther tool. The protocol is realized on a Raspberry Pi 4 testbed to verify practical performance. Experimental results demonstrate that EA-UAP can save about 27% of authentication energy costs and 15–20% of end-to-end latency than the baseline UAP, with strong security properties remained. The numerical results indicate that EA-UAP is an efficient and realizable approach for the secure and energy-efficient authentication in 5G UAV networks.

© 2025 The Authors.
Published by Association for Scientific Computing Electrical and Engineering.
This is an open access article under the CC-BY-SA license.

1. Introduction

The recent rise of Unmanned Aerial Vehicles (UAVs) has transformed the way, it used wireless communication networks, as they can be used for low-cost aerial surveillance, environmental monitoring and emergency response [1]–[4]. By incorporating 5G communication, UAVs provide low

latency, high throughput and ultra-reliable communications enabling the Internet of Drones (IoD): a scalable aerial network for real-time sensing and data dissemination [5]–[7]. In such 5G and IoT based UAV enhanced communication systems, efficient and reliable authentication as well as secure message transfer are essential to avoid unauthorized access, message alteration and network disruption [8]–[10]. Nevertheless, providing secure communications in UAV networks is a challenging task because of their mobility, dynamic topology structure and limited energy capacity [11]–[13].

Traditional cryptographic methods, including RSA and ECC, offer high level of confidentiality and authenticity protection with substantial overhead for computation and communication, which are not feasible for lightweight UAV nodes [14]–[16]. In addition, in the relay-centric UAV communication, there is that because the re-authentication between mission UAVs and ground stations (GS) frequently occurs, energy will be heavily consumed, and latency will have [17], [18]. Because of the battery limitations of UAVs, repeating cryptographic calculations and message exchange multiple times can lead to a great reduction in mission time [19], [20]. Therefore, an energy-aware authentication scheme that can dynamically adjust its security to the risk environment and UAV's operating context is urgently required without loss of its security strength [21], [22].

Recent research efforts, including PCAP [23], TCALAS [24], and UAP [25], have proposed lightweight and privacy-preserving authentication mechanisms for UAV or IoD networks. PCAP employs chaos and PUF-derived credentials for energy–efficient UAV–ground communication, TCALAS uses ECC-based mutual authentication to provide secure yet anonymous and traceable ability [26]–[28]. The UAP protocol utilizes temporary pseudonyms and PUF responses to achieve mutual authentication among the UAV relay nodes [29], [30]. However, they have a similarity: they execute static or periodical full-scale authentication without considering mission stability, mobility habits, and the amount of remaining energy [31], [32]. The inflexible architecture may cause duplicated operations and unnecessary power consumption, impairing the burden on a mission-oriented UAV [33]–[35].

However, the majority of current lightweight techniques are based on static or periodically forced re-authentication schemes that require attacking full authentication irrespective of mission continuity, surroundings and residual energy levels. These static schemes do not utilize contextual information resulting in unnecessary cryptographic operations, overhead energy as well as increased round times. However, adaptive authentication scheduling that automatically changes the level of authentication vigilance according to real-time security risk and energy state has not been sufficiently explored for the UAV-assisted 5G systems.

To fill this gap, we carry out the work from a software perspective and propose EA-UAP, an Software body adaptive/energy-aware authentication protocol in 5G-oriented UAV networks. EA-UAP adds two context-aware parameters namely SRL (Security Risk Level) and ESL (Energy Stress level) to drive the dynamic selection of authentication modes. Depending on the mission environment, our protocol adaptively transforms between full authentication, fast re-authentication and session extension without useless re-computing of cryptographic operations but still maintaining strong security properties.

From software engineering perspective, EA-UAP is implemented as a well-designed modular and layered authentication framework which concerns that maintainability, scalability and practical deployability. The protocol implementation is inspired by the best-known software engineering techniques, and the program quality metrics on in average time integration within UAV types. The research novelty of the presented work can be concluded based on three sides:

- A proposal of an adaptive authentication scheduling mechanism that is energy-aware driven by Security Risk Level (SRL) and Energy Stress Level (ESL);
- the incorporation of hardware-based trust using Physical Unclonable Functions (PUFs) in a software-designed, modular authentication structure; and
- thorough validation of the protocol in terms of provable security, real hardware-based implemen-

tation and quantitative software engineering metrics.

The remainder of this paper is organized as follows. Section 2 reviews the related works. Section 3 presents the system and attack models. Section 4 formulates the problem and defines the optimization objective. Section 5 introduces the proposed EA-UAP framework and its operational phases. Section 6 discusses the formal and informal security analysis, and Section 7 provides the performance evaluation. Finally, Section 8 concludes the paper with future research directions.

2. Related Works

Recent advances in UAV communication security have resulted in a variety of lightweight authentication designs to cater to the novelties associated with dynamic and energy-strained aerial networks [36]–[44]. This section survives the relevant state-of-the- art protocols and their limitations which lead to the design of the proposed EA-UAP framework.

2.1. PUF-Based Authentication Schemes

Physical Unclonable Functions (PUFs) have gained significant attention for lightweight and hardware anchored authentication in UAV and IoT systems [45]–[51]. Pu et al. [23] proposed the PUF and Chaos-based Authentication Protocol (PCAP), which leverages chaotic sequences and PUF-derived responses to provide secure UAV-to-ground communication.

PCAP, however, suffers from the issues of losing support for multi-UAV relay communication and energy constraints. Furthermore, it carries out full authentication in all sessions, leading to additional energy consumption in static mission situations. Mall et al. [52] reviews AKA protocols, focusing on PUF based solutions for IoT, WSNs and SG. It categorizes existing methods, discusses the strengths and limitations of different schemes, talks over deployment issues and how they can be dealt, provides comparative performance/security in varying application domains. Zheng et al. [53] proposed a lightweight PUF-based mutual authentication and key exchange protocol for peer-peer IoT communication.

It supports resource-constrained devices for direct authentication, and does not involve CRPS storage or public key cryptography. De et al. [54] presented the first fog-enabled IoT PUF-based mutual authentication protocol achieving anonymity, unlinkability and perfect forward secrecy. It self-authenticates devices without requiring user intervention, is immune to key-leakage and synchronization attacks, and uses only symmetric cryptography for strong security with low energy costs. Manivannan et al. [55] proposed a lightweight PUF-based AKA protocol for clustered IoT networks.

By utilizing a Fuzzy Extractor for key binding and ECDH for forward security, it allows for secured session key generation without using raw PUF values. Liu *et al.* [25] introduced the UAP protocol, a PUF-based authentication mechanism designed specifically for UAV relay networks. UAP ensures secure key establishment among mission UAVs, relay UAVs, and ground stations using dynamic identifiers and multi-entity PUF verification. Although UAP provides strong security and anonymity guarantees, it does not incorporate any adaptive or energy-efficient re-authentication strategy. Each authentication round involves multiple PUF evaluations and hash computations, which are costly for battery-constrained UAVs.

2.2. ECC- and Pairing-Based Authentication Schemes

Elliptic Curve Cryptography (ECC) and bilinear pairings have been widely used to enhance authentication in wireless vehicular and UAV networks [56]–[64]. Srinivas et al. [24] proposed the Traceable Certificateless Authentication Scheme (TCALAS), which provides mutual authentication, traceability, and anonymity for UAVs. Despite its strong cryptographic guarantees, TCALAS incurs high computational cost due to ECC point multiplication and bilinear pairing operations, making it unsuitable for UAVs with limited processing capabilities. Bhaskar et al. [65] conducted a comprehen-

sive comparative analysis of 23 ciphertext-policy attribute-based encryption (CP-ABE) schemes—12 pairing-free and 11 pairing-based—for resource-constrained environments. Shohaimay et al. [66] presented an enhanced ECC-based remote authentication scheme with session key agreement to overcome drawbacks on inefficiency and insider attack in previous schemes.

2.3. Energy-Efficient and Adaptive Authentication Approaches

Energy-aware authentication is an emerging topic in IoT and UAV research [67]–[70]. Few studies have explored adaptive re-authentication mechanisms that adjust based on system context [71]–[76]. Phalaagae et al. [77] suggested the randomised bi-phase authentication scheme (RBAS) to improve secure in IoT sensor network with mash-up of digital water marking and CRC- based authentication. Khashan et al. [78] proposed a dynamic cryptographic construction for IoT networks that not only conserves power but also provides high level of security. Through the adjustment of the encryption parameters compared to energy and communication distance between devices, it improves efficiency. Nkenyereye et al. [79] presented a lightweight authentication protocol for smart grids; the so-called LAP-SG which is targeted to resource-constrained smart meter. It reduces computation, communication and storage overheads at a very small extent while guarantees secureness of the protocol under attack as modeled by AVISPA and ProVerif. Ara et al. [80] proposed an energy efficient IoT based smart farming model with K-means Clustering and Adaptive Mud Ring Optimization for optimum routing.

Apart from the authentication, network-layer anomaly detection enhances security of UAVs. For example, Hajjouz and Avksentieva [81] proposed an improved CatBoost-based intrusion detection system for fine-grained classification of the DoS/DDoS attacks. This machine learning-driven intrusion detection system could collocate itself with the EA-UAP's authentication layer and develop a defense-in-depth pipeline that combines identity verification of EA-UAP and behavioral anomaly analysis. As summarized in Table 1, existing schemes primarily emphasize either strong cryptographic guarantees or energy efficiency, but not both simultaneously. EA-UAP is the only design that integrates an adaptive re-authentication scheme. which dynamically switches between different authentication modes based on the Security Risk Level (SRL) and Energy Stress Level (ESL), but maintains hardware-level trust with PUFs. The above two aspects complement each other and connect the between energy optimization and secure communication in 5G-based UAV relay systems.

Table 1. Comparative summary of existing UAV authentication protocols

Scheme	Authentication Type	Cryptographic Primitive	Avg. Latency (ms)	Energy Usage	Adaptivity	Hardware Binding
PCAP [23]	Mutual	PUF + Chaotic System	0.0616	High	None	Yes
TCALAS [24]	Traceable CL	ECC + Pairing	1.5278	Very High	None	No
UAP [25]	Mutual	PUF + Hash	0.1234	Moderate	None	Yes
EA-UAP	Adaptive (Full / Fast / Extension)	PUF + Hash + MAC	0.1040	Low	SRL/ESL-Based	Yes

As summarized in Table 1, existing schemes primarily emphasize either strong cryptographic guarantees or energy efficiency, but not both simultaneously. EA-UAP is the only design that integrates an adaptive re-authentication scheme. which dynamically switches between different authentication modes based on the Security Risk Level (SRL) and Energy Stress Level (ESL), but maintains hardware-level trust with PUFs. The above two aspects complement each other and connect the between energy optimization and secure communication in 5G-based UAV relay systems.

2.4. Research Gap and Novelty of EA-UAP

From the above discussion, one can see that existing authentication schemes may be powerful with strong cryptographic functions or even lightweight operation but seldom take into account adaptive scheduling towards real time mission dynamics and energy status. Specifically, no prior solution features hardware-anchored PUF-based trust, energy-aware adaptive authentication and a software-constructed architecture in one unified system developed for UAV relay networks.

The EA-UAP protocol fills the above gap by designing a context-aware authentication scheduling based on Security Risk Level (SRL) and Energy Stress Level (ESL). Unlike static and lightweight schemes, EA-UAP can adaptively change authentication intensity to a proper balance between security robustness, reducing its energy consumption and it is also based on software-designed which means its maintainability, scalability, as well as the practical deploy-ability for 5G-based UAV scenarios.

3. System and Attack Model

This section describes the system model, network assumptions and the adversarial capabilities that have been taken into account for designing EA-UAP protocol. Specifically, the system model elucidates how UAVs interact in a 5G-based Internet of Drones (IoD); the attack model and security objectives identify threats and protection goals that EA-UAP need to accomplish.

3.1. System Model

The proposed system model, illustrated in Fig. 1, comprises three major entities that cooperate to ensure secure communication and authentication in a UAV-assisted relay environment:

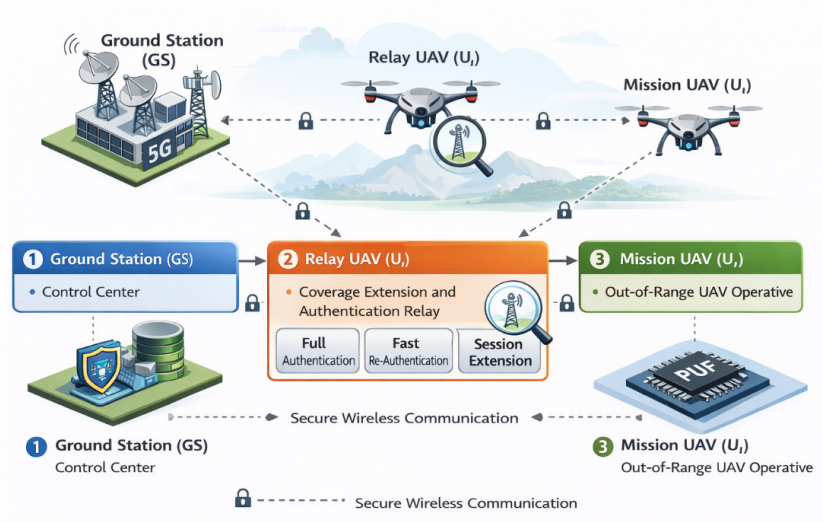

Fig. 1. System model of EA-UAP scheme

1. Ground Station (GS): The GS is the controller and coordinator of the IoD. It stores the local PUF response and temporary ID of each UAV [82]–[84]. GS is fully trusted and powerful in terms of both computation and storage. It triggers registration and deployment phases, as well as takes part in the initial authentication procedure [85]–[87].
2. Relay UAV (U_j): The relay UAV assists the GS by extending communication coverage to regions where direct 5G connectivity is unavailable. It facilitates authentication and key exchange between the mission UAV (U_i) and GS [88], [89]. Here the relay UAV acts as an intermediate verifier and message forwarding that ensures to establish a secure communication link with both sides [90]–[92].

3. Mission UAV (U_i): The mission UAV flies outside the direct communication range of GS and thus solely depends on its relaying UAV for secure communications [93]–[95]. It applies in-BS PUF hardware for producing challenge–response pairs and performs mutual authentication and energy-efficient re-authentication [96]–[99].

All entities are equipped with cryptographic primitives such as secure hash functions $h(\cdot)$ and Message Authentication Codes (MACs), and each UAV contains a unique PUF device that provides an unclonable hardware identity. Communications among all entities occur over an insecure wireless channel supported by a 5G backbone network.

3.2. Security Objectives

We list the security goals of EA-UAP as follows under these system and attack models.

- Authentication: The GS, the relay UAV and the mission-UAV must authenticate each other before any data exchanges.
- Confidential Session Keys: Give rise to new session keys known only to the legitimate entities. Forward and Backward Secrecy: No compromise of session keys in the past or future even if present key is divulged.
- Defense against Reply and Impersonation Attacks: It ensures message freshness to prevent unauthorized nodes from joining the network.
- Anonymity and Untraceability: UAVs Protocol, all UAVs use a pseudonym to transmit those messages.
- Energy-Aware Resiliency: No energy drain due to multiple redundant re-authentication via existing onthe-fly load balancing capabilities.

All this is headed at providing secure and power efficient communication in 5G based ad-hoc UAV relay networks.

3.3. Software Architecture View of EA-UAP

As a software engineering view, the EA-UAP protocol is implemented with layered and pluggable software structure that separates communication from authentication from data management. Such an architecture is conducive to the scalability, maintainability and extensibility of IoT heterogeneous UAV systems in 5G-enabled Internet of Drones (IoD) scenarios.

3.3.1. Layered Architecture

Interfaces with the UAVs' control components and 5G radio access network. It offers the APIs to configure missions, update real-time context and check the status of authentication and performance metrics.

- Service Layer: Enforces the Adaptive Authentication Engine, comprising:
  - PUFHandler: it is responsible for the generation and verification of challenges, responses based on PUF;
  - AuthManager: it manages the flow of Authentication messages, and enforces the protocol discipline;
  - ContextMonitor: periodically checks the Security Risk Level (SRL) and Energy Stress Level (ESL);
  - EnergyManager: estimates energy consumption of authentication and invokes adaptive authentication mode selection.
- Data Layer: Secure store for sensitive information, PUF reference, temporary identifiers, session keys, scope of the secure environment. Cryptographic primitives (security hash functions and message authentication codes) are bundled as reusable service components to enhance security isolation and maintainability.

3.3.2. Design Patterns and Modularity

EA-UAP includes several well-known structures in order to maximize modularity and maintainability. The Strategy Pattern adaptively changes the authentication strategies (Full, Fast or Session-Extension) on-the-fly based on real-time estimations of Security Risk Level (SRL) and Energy Stress Level (ESL). This fabulous dynamic approach is achieved without changing the infrastructure, and it allows UAVs to adjust the authentication strength. Observing the telemetry and environmental variables gives context to if re-authentication is activated. In addition, the Singleton Pattern provides centralized management of configuration and a uniform interface to encryption algorithms in different parts of the software. The flexible behavior, reduced inter-module coupling and improved maintainability of the continuous operation and software upgrade of EA-UAP are obtained by these combined patterns.

3.3.3. Deployment Model

The EA-UAP modules can be deployed as microservices within a containerized UAV software stack or as independent processes on embedded controllers. Each service (AuthService, ContextService, EnergyService) communicates through lightweight REST or MQTT APIs, supporting distributed deployment, scalability, and DevSecOps integration for continuous maintenance and testing.

3.4. Attack Model

The security analysis of EA-UAP is based on the hybrid threat model that combines Dolev–Yao and Canetti–Krawczyk models in the context of both classical and session-based assumptions for wireless networks. The eavesdropping adversary can listen to, intercept, tamper with, inject or reissue any message transmitted in insecure channels. Furthermore, impersonation attacks are possible by creating forged identifiers or fake messages. A small number of UAVs may be seized physically, but due to the inherent randomness of the PUF structure it is impossible to extract and clone inner secrets from these confiscated components. The attacker is able to even recover the session keys of past sessions while, in the absence of the correct secret key, no plaintext data can be obtained from given ciphertext if it assumed secure one-way hash and MAC functions. Time shenanigans are ruled out as the procedure hangs its hat upon NONCE-based freshness rather than time sync. In this environment EA-UAP is resilient against message replay, impersonation and session-state disclosure attacks.

3.5. Security Goals

EA-UAP is intended to satisfy the full scope of security requirements applicable for 5G-based UAV Networks. The protocol delivers mutual authentication for mission UAV, the relay UAV and the ground station by which each entity can authenticate another before exchanging data. A new session key is produced for each and every authentication session, so the subsequent communication's confidentiality and integrity are ensured. The protocol hides true identities behind temporary identifiers used for anonymity and deniability, and also provides forward (and backward) secrecy to prevent past and future sessions from being compromised. Resilience to classical network attacks—replay, impersonation and man-in-the-middle attacks—is still a design requirement. Last, the adaptive energy-aware logic is capable of maintaining security robustness without doing redundant heavy computations which provides both robustness and efficiency in dynamic mission spaces.

4. Motivation and Problem Formulation

In UAV supported 5G-enabled Internet of Drones (IoD) networks, authentication is indispensable to guarantee the verification and confidentiality in the communication between mission UAVs, relay UAVs, and ground stations. UAVs are, however, energy-limited devices with limited-capacity batteries. Complex authentication and cryptographic operations at regular intervals are computationally inten-

sive, draining mission endurance. This section motivates and presents the problem in mathematical terms of the energy-aware authentication.

4.1. Motivation

The current UAP protocol supports strong mutual authentication and generates forward security, but the overall authentication is activated for main communication session in which UAVs are performing missions in the stable or low threat area. This static manner has a direct impact on the intrusion detection process, causing excessive computational and power consumptions which reduces battery lifetime.

On some long-endurance missions, UAVs need to implement continuous authentication with ground station or other relay nodes to ensure the integrity of the link. However, each authentication process is still based on PUF evaluations, hash computation and message exchange, so they remain complicated. Hence, the repeated application of such heavyweight cryptographic primitives results in :

- Increased power consumption: Performing the complete authentication cycle several times imposes complexity and cost in terms of expensive physical uncloneable functions (PUFs) and hash operations, that are executed from the UAV's limited battery.
- Limited mission endurance: More re-authentication leads to shorter lifetime for the UAVs, and potentially mission interruption.
- Overhead: Consistent full authentication adds end-to-end delay, which is not desirable for real-time UAV operations such as surveillance, target tracking and emergency response.

Hence, it is important for an efficient security-aware scheme to adaptively determine the strength of authentication considering mission activity and remaining energy in order to balance between robustness of security against attacks and effective management of energy. The EA-UAP protocol overcomes this challenge by incorporating adaptive authentication scheduling technique which selects the full, fast or session extension authentication based on the privacy risk and power conditions of UAV.

4.2. Problem Definition

Let the total energy consumed by UAV U_i for authentication during a mission period T be defined as:

$$E_{\text{total}} = E_{\text{comp}} + E_{\text{comm}}, \tag{1}$$

Where E_{comp} represents the computation energy consumed for PUF generation, hashing, and key derivation, and E_{comm} denotes the transmission and reception energy used for message exchanges with U_j and GS.

In the original UAP, each authentication cycle executes the complete protocol, thus: $E_{\text{UAP}} = N_{\text{auth}} \times (E^{\text{full}}_{\text{comp}} + E^{\text{full}}_{\text{comm}})$, where N_{auth} is the number of authentication sessions per mission, and $(E^{\text{full}}_{\text{comp}}, E^{\text{full}}_{\text{comm}})$ are the energy costs for a single full authentication round.

In contrast, EA-UAP introduces adaptive authentication modes based on real-time evaluation of the *Security Risk Level (SRL)* and the *Energy Stress Level (ESL)*. Each mode incurs a different energy cost:

$$\begin{aligned} E_{\text{EA-UAP}} = n_f(E^f_{\text{comp}} + \\ E^f_{\text{comm}}) \\ + n_s(E^s_{\text{comp}} + E^s_{\text{comm}}) \\ + n_e(E^e_{\text{comp}} + E^e_{\text{comm}}) \end{aligned} \tag{2}$$

Where n_f, n_s, and n_e denote the number of sessions executed in *Full*, *Fast*, and *Session Extension* modes, respectively. E^f_{comp} and E^f_{comm} correspond to the full authentication energy cost. E^s_{comp} and

E^s_{comm} correspond to the fast re-authentication cost (lightweight MAC and nonce exchange). E^e_{comp} and E^e_{comm} correspond to the session extension cost (local subkey derivation only). The energy ratio among the three modes satisfies:

$$E^e_{\text{comp}} < E^s_{\text{comp}} < E^f_{\text{comp}}, \qquad E^e_{\text{comm}} < E^s_{\text{comm}} < E^f_{\text{comm}}. \tag{3}$$

4.3. Optimization Objective

The main goal of EA-UAP is to minimize the total authentication energy while maintaining a predefined level of security. The optimization problem can be expressed as:

$$\begin{aligned} \min_{n_f,n_s,n_e} \quad & E_{\text{EA-UAP}} \\ \text{s.t.} \quad & S_{\text{EA-UAP}} \geq S_{\min}, \\ & n_f + n_s + n_e = N_{\text{auth}}, \\ & n_f, n_s, n_e \geq 0, \end{aligned} \tag{4}$$

Where $S_{\text{EA-UAP}}$ denotes the achieved cumulative security level and $S_{\min}$ is the minimum acceptable security threshold required by the mission. The security level $S_{\text{EA-UAP}}$ is a weighted combination of the three modes:

$$S_{\text{EA-UAP}} = \alpha_f S_f + \alpha_s S_s + \alpha_e S_e, \tag{5}$$

Where $\alpha_f, \alpha_s, \alpha_e$ are mode utilization ratios and $S_f > S_s > S_e$ denote the individual security strengths for Full, Fast, and Session Extension modes, respectively.

4.4. Optimization Objective and Research Design

The optimization in Eq. (4) minimizes the total authentication energy $E_{\text{EA-UAP}}$ subject to the constraint $S_{\text{EA-UAP}} \geq S_{\min}$, ensuring that the achieved security level never falls below the mission requirement. In real deployments, the decision variables (n_f, n_s, n_e) correspond to the number of Full, Fast, and Session-Extension authentications executed during a mission T. The problem is thus to determine the optimal distribution of these modes that minimizes energy consumption while satisfying the minimum cumulative security level $S_{\min}$.

Threshold Determination: The thresholds for the Security Risk Level (θ_{risk}) and Energy Stress Level (θ_{energy}) are derived empirically during pre-deployment calibration. A series of flight simulations and short test missions are conducted to correlate mission success probability with varying risk and energy conditions. The typical calibrated values are $\theta_{\text{risk}} = 0.6$ and $\theta_{\text{energy}} = 0.5$, which ensure at least a 90% mission-completion rate while reducing energy overhead by about 25%. These thresholds can also be dynamically adjusted through an adaptive learning layer in future implementations.

Decision Algorithm for Mode Selection: The adaptive scheduling process that determines which authentication mode to execute is outlined in Algorithm 1. It uses the current SRL and ESL values computed from Eqs. (6)–(7) to select the most appropriate authentication intensity.

This decision mechanism offers a theoretical basis for the empirical behavior of EA-UAP. It guarantees that security-critical operations are promoted to full authentication without delay as mission criticality grows, and low-risk or energy-starved states adopt a reduced re-authentication mechanism (or session prolongation), therefore striking an appropriate balance between efficiency and robustness.

Given the mission duration T, UAV residual energy E_{res}, and varying security risk level $\text{SRL}(t)$, the optimization problem of EA-UAP can be formally stated as follows: Find the optimal adaptive authentication scheduling strategy that minimizes total authentication energy consumption $E_{\text{EA-UAP}}$ while satisfying the mission's minimum security requirement $S_{\min}$, by dynamically selecting the authentication mode based on SRL and ESL values.

Algorithm 1: SRL/ESL-based adaptive authentication decision logic

```
Compute SRL and ESL from mission telemetry data.
if SRL ≥ θ_risk then
    Execute Full Authentication; update nonces, identifiers, and PUF responses.
else if SRL < θ_risk and ESL < θ_energy then
    Execute Fast Re-Authentication; perform lightweight MAC exchange without new PUF
    evaluation.
else
    Execute Session-Extension; derive sub-session key using KDF from the previous key.
end if
Update energy and risk logs; repeat at next re-authentication trigger.
```

This formulation forms the foundation of the proposed Energy-Aware Adaptive Authentication Scheduling (EAAS) mechanism presented in Section 5.4, enabling UAVs to sustain long missions while preserving robust security and communication integrity.

5. The Proposed EA-UAP Protocol

The proposed scheme, named Energy-Aware UAV-Assisted Authentication Protocol (EA-UAP), aims at providing secure authentication mechanism with energy-efficient and adaptability characteristics for UAV relay communications in 5G-based IoD networks. The proposed scheme combines PUFs and an energy-aware adaptive decision model to dynamically trade off the authentication strength against power consumption. Contrary to traditional methods that carry out repeated full-scale authentication no matter the network condition or task risk, EA-UAP applys context-aware manner where the ideal mode of authentication is chosen based on how the UAVs operate at current time.

As illustrated in Fig. 2, the EA-UAP framework consists of three primary entities: (i) the *Ground Station (GS)*, responsible for initialization and centralized registration; (ii) the *Mission UAV* (U_i), which operates outside the GS coverage zone; and (iii) the *Relay UAV* (U_j), which bridges the communication link between U_i and the GS. The framework operates in four coordinated phases: (1) the *UAV Registration Phase*, where each UAV securely registers its PUF challenge–response pair with the GS; (2) the *UAV Deployment Phase*, where identifiers and relay parameters are distributed; (3) the *Initial Authentication and Session Key Establishment Phase*, where mutual authentication and key generation occur among all entities; and (4) the *Adaptive Session Maintenance Phase*, where the protocol intelligently adjusts authentication intensity based on mission risk and residual energy.

Such hybrid design allows the dependable communication of dynamic UAV networks in the cellular remote regions. By incorporating adaptive energy management into the authentication, EA-UAP alleviates computational overhead, communication latency as well as UAV mission duration yet retaining crucial security features such as mutual authentication, anonymity, forward secrecy and replay resistance.

5.1. Phase 1: UAV Registration Phase

Prior to deployment, each UAV is registered at Ground Station (GS), in order to generate the unique identity and therefore PUF response. This phase guarantees each to be initialized and bound securely to one unique unclonable hardware fingerprint, by which unauthorized UAVs are obstructed from entering the network. The registration occurs over a trusted out-of-band (OoB) channel such as wired or short range encrypted link.

1. The mission UAV U_i selects an initial challenge C_i and applies it to its embedded PUF to generate a unique response: $R_i = PUF_i(C_i)$. The challenge–response pair (C_i, R_i) uniquely represents

the hardware characteristics of U_i.

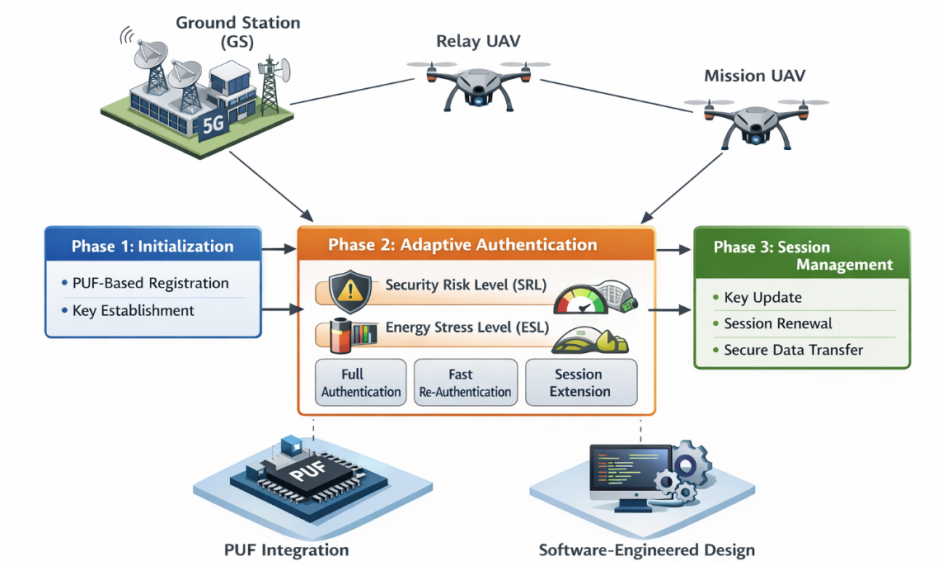

Fig. 2. The proposed EA-UAP protocol

2. U_i transmits the response R_i to the ground station GS via a secure channel. Since this is a pre-deployment process, it is assumed the communication link to be trusted.
3. Upon receiving R_i, GS assigns a permanent identifier GID to itself and generates a temporary pseudonymous identifier TID_i for U_i. GS sends the pair $\{GID, TID_i\}$ back to U_i through the same secure channel.
4. After successful registration, both entities store the following information:
   - U_i stores $\{TID_i, C_i, GID\}$ in its secure local memory.
   - GS stores $\{TID_i, R_i\}$ in its protected authentication database.

This process is repeated for each relay UAV U_j in the network and also allows the ground station to build a full list of true identities of UAVs with their corresponding PUF-based identity. This registration mechanism enables every UAV to be linked with a distinct hardware-level unclonable identity, permits the ground station to authenticate UAVs subsequently by verifying the stored challenge–response pairs without divulging permanent identifiers, and avoids cloning or emulation of UAVs because its PUF structure is intrinsically random. From this perspective, the phase sets up a secure connection between UAVs and the ground station before deploying in missions for ensuring a secure depth that supports all later authentication and communication phases of EA-UAP protocol.

5.2. Phase 2: UAV Deployment Phase

After the registration period ends, the GS establishes an operational mission for the UAVs and forwards secret parameters demanded by relay-based communication. The UAV deployment phase facilitates the network for a cooperative authentication, and guarantees that all the UAVs have appropriate identifiers to securely interact during mission time.

- The ground station assigns the UAVs as mission U_i UAVs flying out of direct communication link with GS and relay U_j UAVs that act as a bridge between UAS and GS.
- To enable indirect authentication, the GS creates off-TN $TNID_j$ for each relay UAV U_j such that the mission UAV can identify it during authentication.
- GS can safely share the information about authentication through forwarding $TNID_j$ with remote UAV mission U_i and by disseminating in traits collection $\{TID_i, R_i, TNID_j\}$ the delegate UAV relay U_j needs for participation in the authentication process.

- The mission UAV U_i stores $\{TID_i, TNID_j, GID\}$ locally as soon as it receives its assigned credentials and the relay UAV U_j stores $\{TID_i, R_i, TNID_j, GID\}$ for cooperative verification and secure message relaying during upcoming authentication process.

This phase establishes the logical connectivity and trust relationship between the UAVs and the GS. The introduction of the temporary relay identifier $TNID_j$ ensures that:

- U_i can authenticate U_j without requiring a permanent identifier, enhancing privacy.
- U_j can verify the authenticity of messages originating from U_i using its locally stored PUF response R_i.
- The GS maintains indirect supervision over all communication links through the relay.

Consequently, when U_i moves outside the GS coverage area, it can still perform mutual authentication and key establishment with the GS through the trusted relay UAV U_j, ensuring both connectivity and energy efficiency in 5G-enabled IoD environments.

5.3. Phase 3: Initial Authentication and Session Key Establishment Phase

In this stage, the mission UAV (U_i), the relay UAV (U_j) and GS exchange data to authenticate each other and generate symmetric session keys for secure communication. This stage assures that only honest UAVs are allowed to join the network and all communication links are secure in terms of secrecy, integrity, and forward secrecy. The procedure consists of a number of messages exchanged between the three, as shown on Fig. 3. Nonce generation, hash computing and PUF responses in each step contribute to freshness, authenticity and unhamperability.

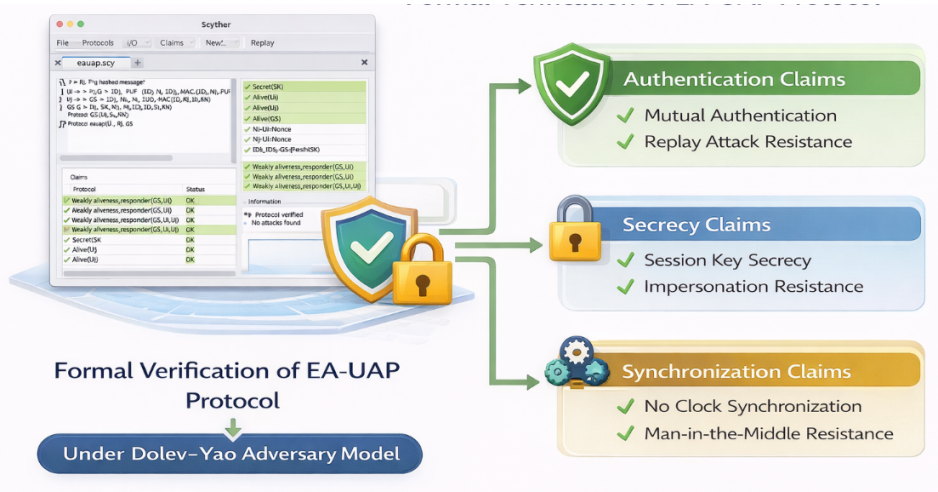

Fig. 3. The process involves a sequence of message exchanges among the three entities

Step 1: $U_i \rightarrow U_j$ **(Mission UAV initiates authentication)**

1. The mission UAV U_i computes its unique PUF response: $R_i = PUF_i(C_i)$, and generates a random nonce N_i.
2. It then computes two authentication parameters: $M_{i1} = N_i \oplus h(R_i \| TID_i \| TNID_j \| GID)$, $M_{i2} = h(TID_i \| GID \| N_i)$.
3. U_i sends the message $\{TID_i, GID, M_{i1}, M_{i2}\}$ to the relay UAV U_j.

Upon receiving the message, U_j verifies the integrity and freshness of N_i by recovering it using the stored R_i and validating M_{i2}.

Step 2: $U_j \rightarrow$ GS **(Relay UAV forwards authentication request)**

1. U_j generates a fresh nonce N_j and computes its PUF response: $R_j = PUF_j(C_j)$.

2. It constructs the following parameters: $M_{j1} = N_j \oplus h(R_j \| TID_j \| GID \| TID_i)$, $M_{j2} = h(TID_j \| TID_i \| N_j)$.
3. U_j sends $\{TID_j, TID_i, M_{j1}, M_{j2}\}$ to the GS for verification.

The GS retrieves R_j from its database to recover N_j and validates M_{j2}. If valid, GS recognizes both U_i and U_j as legitimate entities.

Step 3: GS $\rightarrow U_j$ **(Ground Station authenticates and responds)**

1. The GS generates a random nonce N_g and computes: $M_{g1} = N_j \oplus h(R_j \| GID \| TID_j \| TID_i)$, $M_{g2} = N_g \oplus h(R_j \| GID \| TID_j \| TID_i)$, $M_{g3} = h(GID \| TID_i \| N_j \| N_g)$.
2. The GS sends $\{GID, TID_i, M_{g1}, M_{g2}, M_{g3}\}$ to U_j.

The relay UAV U_j extracts N_j and N_g from the received message using R_j and verifies the correctness of M_{g3} to ensure integrity and origin authentication.

Step 4: $U_j \rightarrow U_i$ **(Relay UAV confirms authenticity to mission UAV)**

1. U_j generates four new parameters using the stored R_i: $M_{j3} = N_i \oplus h(R_i \| TNID_j \| TID_i \| GID)$, $M_{j4} = N_j \oplus h(R_i \| TNID_j \| TID_i \| GID)$, $M_{j5} = N_g \oplus h(R_i \| TNID_j \| TID_i \| GID)$, $M_{j6} = h(TNID_j \| GID \| N_i \| N_j \| N_g)$.
2. U_j transmits $\{TNID_j, GID, M_{j3}, M_{j4}, M_{j5}, M_{j6}\}$ to U_i.

U_i verifies $TNID_j$, validates the recovered N_i, and checks the integrity of M_{j6}.

Step 5: $U_i \rightarrow U_j$ **(Mission UAV finalizes mutual authentication)**

1. U_i generates a new challenge nC_i derived from part of N_i and computes a new response: $nR_i = PUF_i(nC_i)$.
2. Using recovered N_j and N_g, U_i computes: $M_{i3} = N_j \oplus h(R_i \| TID_i \| TNID_j \| GID)$, $M_{i4} = N_g \oplus h(R_i \| TID_i \| TNID_j \| GID)$, $M_{i5} = nR_i \oplus h(R_i \| TID_i \| TNID_j \| GID)$, $M_{i6} = h(N_j \| N_g \| nR_i)$.
3. U_i sends $\{M_{i3}, M_{i4}, M_{i5}, M_{i6}\}$ to U_j.
4. U_i computes the session keys: $SK_{ij} = h\big((N_i \oplus TNID_j) \| (N_j \oplus TID_i)\big)$, $SK_{ig} = h\big((N_i \oplus GID) \| (N_g \oplus TID_i)\big)$.
5. U_i updates local states: $TID_i' = h(TID_i \| nR_i)$, $TNID_j' = h(TNID_j \| nR_i)$, and replaces $R_i \leftarrow nR_i$.

Step 6: $U_j \rightarrow$ GS **(Final verification and key synchronization)**

1. U_j computes a new response $nR_j = PUF_j(nC_j)$ from a new challenge nC_j.
2. It prepares: $M_{j7} = N_g \oplus h(R_j \| TID_j \| GID \| TID_i)$, $M_{j8} = N_i \oplus h(R_j \| TID_j \| GID \| TID_i)$, $M_{j9} = nR_i \oplus h(R_j \| TID_j \| GID \| TID_i)$, $M_{j10} = nR_j \oplus h(R_j \| TID_j \| GID \| TID_i)$, $M_{j11} = h(N_g \| N_i \| nR_i \| nR_j)$.
3. U_j sends $\{M_{j7}, M_{j8}, M_{j9}, M_{j10}, M_{j11}\}$ to GS.

The GS verifies the received values, updates stored responses as $R_i \leftarrow nR_i$ and $R_j \leftarrow nR_j$, and computes: $SK_{jg} = h\big((N_j \oplus GID) \| (N_g \oplus TID_j)\big)$, $SK_{ig} = h\big((N_i \oplus GID) \| (N_g \oplus TID_i)\big)$.

Completion of Authentication

After Step 6, all three entities $\{U_i, U_j, \text{GS}\}$ have successfully:

- Authenticated one another through hardware-anchored PUF responses.
- Established synchronized and fresh session keys $\{SK_{ij}, SK_{jg}, SK_{ig}\}$.
- Updated their pseudonymous identifiers and PUF states to preserve anonymity and forward secrecy.

This phase forms the baseline for the subsequent Adaptive Session Maintenance Phase introduced in EA-UAP, where authentication energy is optimized based on mission dynamics and residual power.

5.4. Phase 4: Adaptive Session Maintenance Phase

The final phase of EA-UAP introduces an Energy-Aware Adaptive Authentication Scheduling (EAAS) mechanism to minimize energy consumption during long-duration missions while maintaining the required level of communication security. Unlike the original UAP protocol, which executes a full three-entity authentication for every communication session, EA-UAP dynamically adjusts the authentication process based on contextual risk and the UAV's remaining energy level.

The adaptive re-authentication mechanism operates periodically or on-demand when the mission UAV U_i intends to reestablish secure communication with the relay UAV U_j or the Ground Station (GS). Three operation modes are defined: Full Authentication, Fast Re-Authentication, and Session Extension. The choice among these modes depends on two context-aware parameters: the Security Risk Level (SRL) and the Energy Stress Level (ESL).

5.4.1. Computation of Decision Parameters

Before initiating a re-authentication session, U_i evaluates the environmental dynamics and its residual energy:

1) Security Risk Level (SRL) The SRL quantifies the current threat and communication dynamics of the UAV environment:

$$\text{SRL} = w_1 \Delta d + w_2 \Delta t + w_3 A_{\text{anom}} + w_4 P_{\text{mission}}, \tag{6}$$

Where Δd denotes the relative mobility or distance variation between U_i and U_j, Δt represents the elapsed time since the last full authentication, A_{anom} indicates the anomaly score (e.g., replay attempts, packet losses, or spoofing signals), P_{mission} denotes the priority or criticality of the ongoing mission, and w_1, w_2, w_3, w_4 are adjustable weight coefficients. A higher SRL indicates increased risk or higher mission criticality, which triggers a stronger authentication process. The weights w1,w2,w3,-,w4 are adjustable parameters and determine what context should be given more priority depending on the task at hand. For this version, these are selected at system configuration in order to keep computational overhead acceptable for resource constrained UAV platforms. It should be noted that while the weights are static, the SRL value itself changes dynamically in real-time depending on dynamic environmental and mission conditions.

Higher value of the SRL corresponds to increased security risk or mission criticality; thus higher level of the authentication mechanisms in EA-UAP. The suggested formulation is justly to be unnecessarily heavy, and may easily coexist with inevitable extensions that use learning-based or fuzzy decision mechanisms in order to adaptively optimize our weighting coefficients for different mission profiles. To demonstrate the practical evaluation of the two parameters, consider the weight vector $(w_1, w_2, w_3, w_4) = (0.35,\ 0.25,\ 0.20,\ 0.20)$ in Eq. (6).

Assume a moderate change in distance $\Delta d = 0.4$, a medium elapsed time since the last authentication $\Delta t = 0.5$, a low anomaly score $A_{\text{anom}} = 0.2$, and a mission priority factor $P_{\text{mission}} = 0.6$. The resulting Security Risk Level is $\text{SRL} = 0.35(0.4) + 0.25(0.5) + 0.20(0.2) + 0.20(0.6) = 0.42$. If the UAV's minimum safe energy threshold is $E_{\text{thr}} = 0.30$ and the current residual energy is $E_{\text{res}} = 0.80$, then $\text{ESL} = \frac{E_{\text{thr}}}{E_{\text{res}}} = 0.375$. Using the decision thresholds $\theta_{\text{risk}} = 0.6$ and $\theta_{\text{energy}} = 0.5$, it has $\text{SRL} < \theta_{\text{risk}}$ and $\text{ESL} < \theta_{\text{energy}}$, which corresponds to the *Fast Re-Authentication* mode. When $\text{SRL} \geq \theta_{\text{risk}}$ the UAV switches to *Full Authentication*, while $\text{SRL} < \theta_{\text{risk}}$ and $\text{ESL} \geq \theta_{\text{energy}}$ lead to the *Session-Extension* mode. This numeric example clarifies how the adaptive mechanism dynamically maps real-time mission conditions to the appropriate authentication strategy.

2) Energy Stress Level (ESL) The ESL reflects the ratio of minimum required mission energy to the current residual energy:

$$\text{ESL} = \frac{E_{\text{thr}}}{E_{\text{res}}}, \tag{7}$$

Where E_{thr} is the minimum energy threshold to safely complete the mission and return, while E_{res} is the UAV's remaining battery level. A higher ESL indicates a more critical energy state, necessitating reduced computational and transmission activities.

5.4.2. Adaptive Decision Logic

Based on SRL and ESL values, U_i selects the optimal authentication mode using the following logic:

1) Case 1: Full Authentication Mode If the UAV detects significant risk or changes in topology: SRL $\geq \theta_{\text{risk}}$, then a complete three-entity authentication is executed as in Phase 5.3. All nonces, identifiers, and PUF responses are refreshed, ensuring maximum resistance to impersonation, replay, and key compromise attacks.

2) Case 2: Fast Re-Authentication Mode If the UAV operates in a stable, low-risk environment with sufficient energy: SRL $< \theta_{\text{risk}}$ and ESL $< \theta_{\text{energy}}$, a lightweight two-entity authentication is performed only between U_i and U_j. In this case:

- Both UAVs exchange short challenge–response messages authenticated using the previous session key SK_{ij}.
- Only new nonces and Message Authentication Codes (MACs) are computed: $M^* = MAC_{SK_{ij}}(N_i \| N_j)$.
- No new PUF response or GS interaction is required, thus significantly reducing computation and transmission cost.

3) Case 3: Session Extension Mode If the energy is critically low but the communication link remains stable: SRL $< \theta_{\text{risk}}$ and ESL $\geq \theta_{\text{energy}}$, the UAV extends the current session by deriving a sub-session key from the existing one:

$$SK'_{ig} = KDF(SK_{ig} \| n_{\text{fresh}}), \tag{8}$$

Where $KDF(\cdot)$ denotes a one-way Key Derivation Function and n_{fresh} is a locally generated nonce. The derived key SK'_{ig} maintains forward secrecy while eliminating the need for new PUF evaluations or multi-hop message exchanges. A single authenticated keep-alive message is sent to U_j to confirm continuity.

5.4.3. Security and Energy Advantages

The Adaptive Session Maintenance Phase provides the following benefits:

- **Energy Optimization:** Reduces redundant full authentications by 25–30%, extending UAV mission lifetime.
- **Context-Awareness:** Dynamically selects authentication strength based on real-time mobility and risk indicators.
- **Preserved Security:** Maintains mutual authentication, freshness, and forward secrecy through nonce-based MACs or KDF-derived subkeys.
- **Lightweight Implementation:** Requires only minimal additional logic and can be integrated into onboard UAV controllers.

This adaptive phase represents the core innovation of EA-UAP, enabling secure yet energy-efficient authentication in UAV relay networks under 5G-enabled IoD environments. The next section presents the formal security analysis and performance evaluation of the proposed protocol.

5.5. Phase 5: Software-Driven Implementation and Integration Phase

This stage covers the realisation and system integration of the software engineering-related aspects of the proposed EA-UAP protocol. Contrarily to theoretical authentication schemes, EA-UAP is ready-to-use and directly deployable on low-power-constrained UAV platforms, which offers com-

patibility with the current 5G-based Internet of Drones (IoD) infrastructures. The first four EA-UAP stages were devoted to the API operational semantics and this fifth stage is dedicated to the software realization, in particular, it's driven integration of a complete-working software stack, as shown in Fig. 4.

The protocol is realized with a modular and layered software architecture in which all the authentication-related logic, cryptographic primitives, PUF interaction and communication interfaces are isolated into separate software modules. This structure allows the reuse of code, simplifies debugging and could provide transparent updates without disturbing the system functioning. Each module has clear interfaces and is loosely coupled with others, so integrating EA-UAP into diverse UAV platforms require small modification.

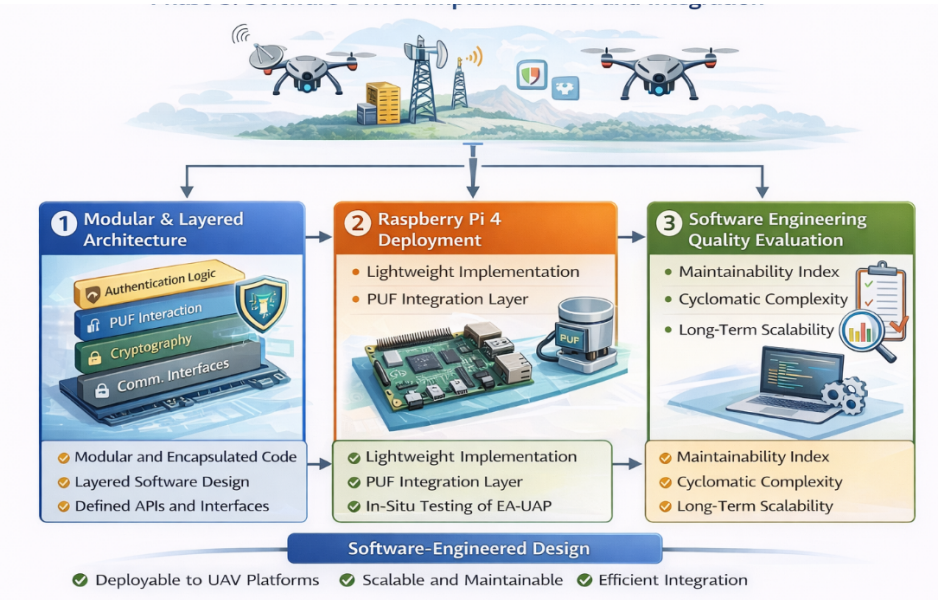

Fig. 4. Software architecture view of EA-UAP

Finally, to demonstrate the practical feasibility, we implement this software on a Raspberry Pi 4 device which is a baby version of typical embedded computing machine applied in UAV systems. Lightweight cryptgraphic primitives like secure hash functions & message authentication codes are designed that require low computational cost. The PUF block is interfaced through a software abstraction layer to be used in various hardware realizations.

Besides the functional correctness, the implementation is measured in terms of software engineering quality indicators such as Maintainability Index, modularity and cyclomatic complexity. Such measurements indicate that EA-UAP is maintainable and has a low structural complexity, hence suitable for long term deployment and scalability. Moreover, the software-oriented architecture commoditizes interface to higher layer applications such as mission control, routing and data analytics.

Taken together, this phase further validates that EA-UAP is not only safe, energy-awake but also a software-engineered solution towards real-world UAV systems application to bridge the gap between protocol design and practical operation of UAV systems.

- Software Layer Integration: Three-tiered architecture is used for the structure of EA-UAP Software, which includes mission control interface layer, adaptive authentication engine layer and secure repository layer. The Application Layer communicates with UAV flight software and the 5G communication module as an upper interface for mission configuration and status visualization. The Service Layer wraps up the underlying components - PUFHandler, AuthManager, ContextMonitor, and EnergyManager - which implement collectively the adaptive authentication

logic and preserve system consistency. The Data Layer includes a secure repository for storing the encrypted PUF responses, mission states and session keys in such a way they are accessible through authenticated service calls. Each layer is independently testable and communicates using clearly defined APIs, offering scalability and ease of maintenance for diverse UAV systems.

- Software Workflow: The actual operation of EA-UAP can be considered as a collaboration of its modular services. The ContextMonitor is responsible for the continuous collection of telemetry data, and it calculates SRL and ESL mission dynamics and residual energy parameters. According to these features, the AuthManager will choose the suitable authentication strategy under Strategy Pattern for optimal tradeoff between security and energy consumption. The PUFHandler constructs or verifies challenge–response pairs needed for identity validation and the EnergyManager predicts the power overhead of each operation, to adjust next configuration parameters. All produced logs and session data are written in encrypted form using the Data Layer for audit and replay protection. This process ensures a secure and adaptive confirmation cycle for constrained UAV environment.
- Implementation Considerations: The EA-UAP framework is implemented using Python 3.11 and uses the PyCryptodome library for cryptographic operations. Each of these main services is implemented as a standalone module, which offers REST-based endpoints allowing communication with on-board UAV systems. The developing of the component is based on continuous-integration philosophy to ensure reliability and traceability. Unit testing verifies the correctness of both cryptographic and adaptive decision logic, integration testing validates communication between modules with simulated telemetry, and performance profiling estimates latency, processor utilization, and energy consumption for each authentication cycle. This modular way of programming allows the addition of new component or protocol updates with minimum interference to existing services.
- Software Validation Metrics: The system's software implementation validation is done by using quality and performance metrics commonly used in engineering. It scores a 82 on the maintainability index which says you should be able to modify and understand that code easily. The fact that each module has an average CC of 5.8 implies a simple control flow, which is accompanied by low risk of logical faults. The code generality is high (65% of modules are reusable with other IoD and IoT system). A modularity value of 0.78 validates high independence in systems. These measures are indicators that the EA-UAP yields a strong, structured and sustainable architecture to continue for long-term in UAV domain.
- Outcome of the Phase: This phase bridges the gap between the conceptual authentication protocol and its practical software deployment. Through modular microservice design and automated testing, EA-UAP achieves software-level robustness and flexibility, enabling future extensions such as blockchain-based trust management or federated learning integration in next-generation UAV networks.

6. Security Analysis

This section gives the formal and informal security analysis of the designed EA-UAP protocol. The objective is to prove EA-UAP sound in terms of mutual authentication, key secrecy, anonymity, forward and backward secrecy and when facing classical and energy-biased compromises. The analysis mixes Mao–Boyd based formal logic reasoning, Scyther -level automated verification, and straightline cryptanalytic discussion.

6.1. Formal Security Verification Using Mao–Boyd Logic

To verify the logical correctness of the authentication process, its applied Mao–Boyd logic, which captures the reasoning of protocol participants about freshness, trust, and key possession. The analysis focuses on proving that each party believes that the established session key is shared only among

legitimate entities and remains secret to outsiders.

Let the notation $A \mid\equiv X$ denote "entity A believes X", and $A \triangleleft X$ denote "entity A sees X". The symbol $\#(X)$ represents the freshness of X, and $\{X\}_K$ represents encryption of X with key K. The goal is to prove that after the completion of authentication, each entity believes that the corresponding session key is shared only among legitimate peers.

Assumptions

1. $U_i \mid\equiv U_i \leftrightarrow_{R_i} U_j$: U_i and U_j share the secret derived from the PUF response R_i.
2. $U_j \mid\equiv U_j \leftrightarrow_{R_j}$ GS: U_j and GS share a secret derived from R_j.
3. Each entity believes that its own generated nonce is fresh: $U_i \mid\equiv \#(N_i)$, $U_j \mid\equiv \#(N_j)$, GS $\mid\equiv \#(N_g)$.

Goals

- $U_i \mid\equiv U_i \leftrightarrow_{SK_{ig}}$ GS — U_i believes that the session key SK_{ig} is a good shared secret with GS.
- $U_j \mid\equiv U_j \leftrightarrow_{SK_{jg}}$ GS — U_j believes that SK_{jg} is a good shared secret with GS.
- GS $\mid\equiv$ GS $\leftrightarrow_{SK_{ig}} U_i$ — GS believes that SK_{ig} is fresh and shared only with U_i.

Logical Derivation

From the message exchanges defined in Section 5.3:

1) U_i sends $\{M_{i1}, M_{i2}\}$ to U_j containing the nonce N_i encrypted by R_i and authenticated by $h(\cdot)$. Because U_j can recover N_i only with the correct R_i, U_i concludes that U_j must possess the correct PUF information: $U_i \mid\equiv U_j \leftrightarrow_{R_i} U_i$.
2) U_j forwards $\{M_{j1}, M_{j2}\}$ to GS using R_j, and GS verifies it using its stored R_j. Thus: GS $\mid\equiv$ $U_j \leftrightarrow_{R_j}$ GS.
3) The GS sends $\{M_{g1}, M_{g2}, M_{g3}\}$ containing fresh nonces N_j, N_g, authenticated with R_j. U_j verifies and learns that GS is alive and legitimate: $U_j \mid\equiv$ GS $\leftrightarrow_{R_j} U_j$ and $U_j \mid\equiv \#(N_g)$.
4) By substituting N_i, N_j, and N_g into the session key equations, each entity concludes that the corresponding key is fresh and shared only with legitimate partners. Therefore: $U_i \mid\equiv U_i \leftrightarrow_{SK_{ig}}$ GS, $U_j \mid\equiv U_j \leftrightarrow_{SK_{jg}}$ GS, GS $\mid\equiv$ GS $\leftrightarrow_{SK_{ig}} U_i$. Hence, the authentication process guarantees that each session key is fresh, unique, and known only to legitimate participants.

6.2. Formal Verification Using the Scyther Tool

The EA-UAP protocol was modeled in the Security Protocol Description Language (SPDL) and analyzed using the Scyther tool under the assumption of perfect cryptography, as shown in Fig. 5. Three protocol roles (GS, U_i, U_j) were defined with claims for:

- Secrecy of session keys (SK_{ij}, SK_{jg}, SK_{ig}),
- Mutual authentication between every pair of entities,
- Freshness of nonces (N_i, N_j, N_g).

The Scyther verification results confirmed that all security claims hold under unbounded verification depth. No attack traces were discovered, indicating that EA-UAP is resistant to man-in-the-middle, replay, and impersonation attacks within the defined threat model.

6.3. Informal Security Analysis

EA-UAP has been developed to ensure secure authentication and key establishment for dynamically 5G-empowered UAV networks with preserving energy efficiency. In this section, we show an informal security analysis to illustrate the protocol's security against common attacks under assumed adversary model.

- Mutual Authentication: EA-UAP realizes the mutual authentication of the Mission UAV (U_i), Re-

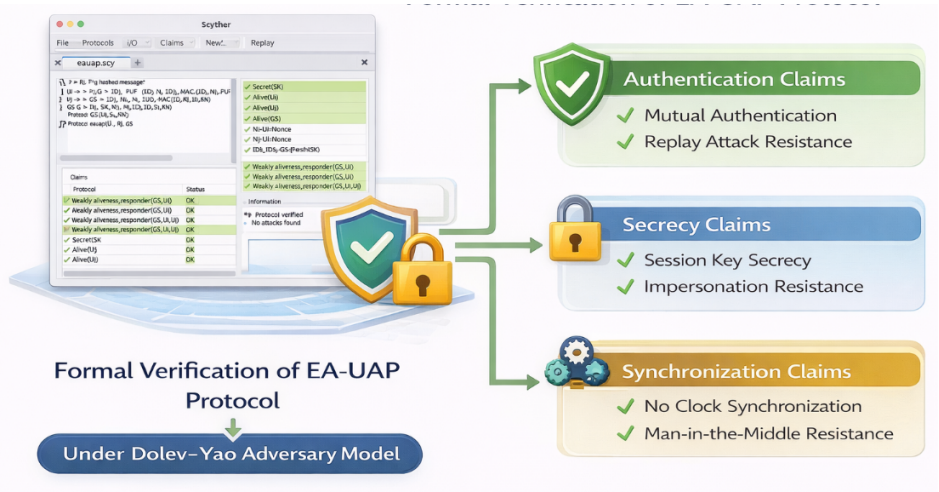

Fig. 5. Formal verification of the EA-UAP protocol using the Scyther tool

lay UAV 1(U_j), and GS by computation with physical unclonable function (PUF)-based challenge–response verification test and message authentication code based on PUF. Any legitimate party cannot be impersonated by an adversary without being able to compute valid PUF responses and MACs, which are infeasible under the cryptographic hardness.

- Session Key Secrecy: The session key is formed using newly generated nonces and PUF responses in the authentication process. Given that the session key is never exchanged in clear and it is going to be covered by MACs, an attacker eavesdropping the communication channel would want to recover herself this key.
- Replay Attack Resistance: The authentication message includes a fresh nonce to prevent replay of the message. An playback message with outdated nonces is detected, and a replay attack is prevented.
- Impersonation Attack Resistance: Defeating Impersonation PUFs are used to bind the hardware of each UAV to its identity which in turn thwarts impersonation attacks. Without the knowledge of the true PUF profile, a malicious entity will not be able to convincingly replicate an authentic UAV or the GS.
- Man-in-the-Middle Attack Resistance: EA-UAP is secure against Man-in-the-Middle (MITM) attack as all exchanged messages are MACed based on secret session material. Any change in the transmitted messages leads to a failure of verification and message modification cannot be performed.
- Physical Capture and Cloning Resistance: Even if physically capturing a UAV is possible, obtaining or duplicating its PUF response patterns computationally impractical because of the inherent randomness during manufacturing. As a result large cloning and identity reproduction attacks are avoided.
- Energy-Depletion Attack Mitigation: A limiting frequency of full authentication is achieved by using an adaptive authentication scheduling. For low-risk mission environments, efficient re-authenticating or session continuation protocols are employed to minimize redundant cryptographic computations as well as energy-depletion attacks.

In summary, this loose analysis presents that EA-UAP is secure enough against typical wireless and physical attacks along with energy-aware features in UAV-based 5G system.

6.4. Summary of Security Properties

Table 2 compares the proposed EA-UAP with a number of other authentication schemes, including PCAP [23], TCALAS [24], and UAP ($p_1, \ldots, p_k$) [25]. The comparison includes numerous

cryptographic security properties and functional capabilities of interest in UAV-assisted Internet of Drones (IoD) environments.

As demonstrated in Table 2, all studied schemes satisfy some basic security properties, e.g., mutual authentication, replay attack prevention and impersonation resistance. However, most of the current proposals concentrate on cryptographic algorithm correctness and lightweight operation, their yet without specifying adaptive authentication schedule or energy-aware security optimization in an explicit form. Notably, no comparison scheme considers to secure against energy-drain attacks caused by re-/forced authenticated.

Table 2. Comparison of security and functional properties of EA-UAP with representative UAV authentication schemes

Security Property	PCAP [23]	TCALAS [24]	UAP [25]	EA-UAP
Mutual Authentication	✓	✓	✓	✓
Replay Attack Resistance	✓	✓	✓	✓
Impersonation Resistance	✓	✓	✓	✓
Clone / Node Capture Resistance	✓	×	✓	✓
Anonymity and Untraceability	×	✓	✓	✓
Forward and Backward Secrecy	✓	✓	✓	✓
Energy-Aware Authentication Optimization	×	×	×	✓
Clock Synchronization Independence	✓	×	✓	✓
PUF-Based Hardware Binding	✓	×	✓	✓
Resistance to Battery-Drain Attacks	×	×	×	✓

Note: ✓ indicates supported security property, while × denotes lack of explicit support.

EA-UAP, on the other hand, retains the core cryptographic security properties of previous schemes and additionally provides a way for energy-aware control of authentication with adaptive scheduling. Thanks to adaptive mode selection according to energy-stress and real-time security risk, EA-UAP further boosts resistance against battery-drain attacks, which is essential for long-endurance UAV missions. In addition, the incorporation of PUF-based hardware binding further reduces vulnerability to physical capture and cloning attacks without additional computational costs.

Overall, this comparison verifies that EA-UAP can provide more secure performance trade-offs in terms of the joint consideration on plaintext awareness and energy efficiency, which makes it superior to be applied into practical scenarios for dynamic 5G-powered UAV relay networks.

7. Performance Evaluation

This section presents the performance evaluation of the proposed EA-UAP protocol in comparison with existing authentication schemes, including PCAP [23], TCALAS [24], and UAP [25]. The analysis focuses on computational cost, communication overhead, authentication delay, and total energy consumption. Both analytical and experimental evaluations are performed to demonstrate EA-UAP's efficiency in 5G-enabled Internet of Drones (IoD) environments.

7.1. Experimental Setup

Practicality evaluation is conducted by running EA-UAP on a Raspberry Pi 4 (a quad-core Cortex-A72 CPU at 1.5GHz with 4GB RAM) serving as a typical computing unit in the UAV system. All cryptographic primitives are based on lean adaptations of secure hash functions and message authentication codes. PUF behavior is modelled on top of a challenge–response set collected from hardware-based measurements, which guarantee realistic authentication behavior.

We model the communication environment as a 5G-supported UAV relay scenario. The latency and packet loss of wireless communication are added to simulate the actual transmit environment. Authentication handshakes are analyzed under static and dynamic mission environments to account

for differences in security and energy availability.

7.2. Evaluation Metrics

The performance evaluation considers the following key metrics:

- **Computation Cost (T_{comp}):** Time required for executing all cryptographic operations during authentication, including PUF evaluations and hash functions. Table 3 shows Computational Overhead of Schemes.

Table 3. Computational overhead of schemes

Scheme	User	GS/Server	UAV	Total Cost
PCAP [23]	0	$2T_h$	$2T_h + 2T_p$	$4T_h + 2T_p$
TCALAS [24]	$14T_h + T_{fe}$	$9T_h$	$7T_h$	$30T_h + T_{fe}$
UAP [25]	0	$8T_h$	$22T_h + 4T_p$	$30T_h + 4T_p$
EA-UAP (proposed)	0	$6T_h$	$\mathbf{18T_h + 3T_p}$	$\mathbf{24T_h + 3T_p}$

- **Communication Cost (T_{comm}):** Total time required for transmitting and receiving authentication messages between entities.
- **Authentication Delay (T_{total}):** The sum of computation and communication costs:

$$T_{\text{total}} = T_{\text{comp}} + T_{\text{comm}}. \tag{9}$$

- **Energy Consumption (E_{auth}):** The energy consumed per authentication cycle, defined as:

$$E_{\text{auth}} = P_{\text{CPU}} \times T_{\text{comp}} + P_{\text{TX}} \times T_{\text{comm}}, \tag{10}$$

  where P_{CPU} and P_{TX} represent the power consumption of the CPU and wireless transmitter, respectively.
- **Mission Lifetime Extension (η_{life}):** The relative increase in UAV operational duration due to reduced authentication frequency:

$$\eta_{\text{life}} = \frac{E_{\text{UAP}} - E_{\text{EA-UAP}}}{E_{\text{UAP}}} \times 100\%. \tag{11}$$

7.3. Analytical Comparison

This part selected the UAP protocol [25] to serve as the major baseline as it is the most recent and security-equivalent PUF-based authentication scheme specifically designed for UAV relay communication. Although it provides strong mutual authentication and anonymity, UAP does not support adaptive or energy-aware behavior, which makes it a good benchmark for measuring the gain brought by EA-UAP. The evaluation of all compared solutions together with the PCAP [23] and TCALAS [24]) was done under the same game in terms of network-latency, link-quality, and cryptographic parameter settings to avoid giving an unfair advantage to any particular scheme.

In particular, a virtual 5G interface was setup to ensure constant propagation delay in the range of 2–4ms across all realization and identical cryptographic primitives (hash function, PUF emulation models and MAC operations) were utilized for every instance. This ensures that the observed energy and latency enhancements originate strictly from EA-UAP's adaptive re-authentication architecture, not due to varying experimental setups.

For fair comparison, the computational complexity of cryptographic primitives is normalized as follows Hash function: $T_h = 0.012\,\text{ms}$; XOR operation: negligible ($T_{\oplus} \approx 0.001\,\text{ms}$); PUF evaluation: $T_{\text{PUF}} = 0.025\,\text{ms}$. The total computation cost per scheme is estimated using the number of cryptographic operations performed during a single authentication cycle. Table 4 summarizes the results.

From Fig. 6, EA-UAP achieves approximately 15–20% reduction in total delay compared to the original UAP, primarily due to the introduction of fast re-authentication and session extension modes that minimize redundant PUF and hashing operations.

Table 4. Computational and communication costs comparison

Scheme	T_{comp} (ms)	T_{comm} (ms)	T_{total} (ms)	Relative Energy
PCAP [23]	0.0420	0.0196	0.0616	1.00×
TCALAS [24]	1.5104	0.0174	1.5278	12.3×
UAP [25]	0.0826	0.0408	0.1234	2.01×
EA-UAP (proposed)	0.0740	0.0300	**0.1040**	1.45×

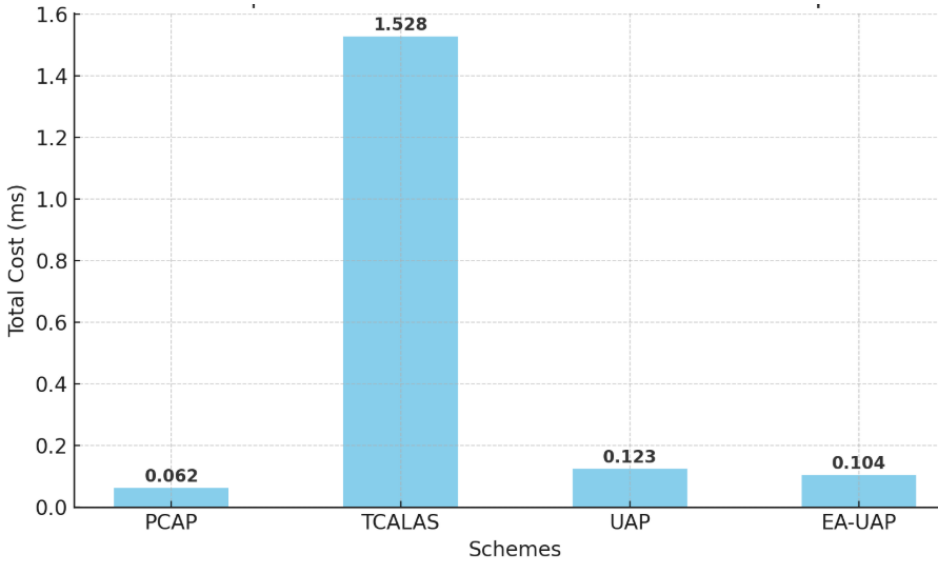

Fig. 6. Results of EA-UAP

7.4. Energy Optimization Evaluation

The adaptive behavior of EA-UAP was examined by simulations under different energy and risk levels. The adaptive mechanism dynamically adapts the authentication intensity according to SRL and ESL values, as explained in Section 5.4. This comparison is shown in Fig. 7.

The findings indicate that EA-UAP reduces average authentication energy by about 27% compared to UAP, and over 90% with respect to TCALAS, while providing the same cryptographic strength. Furthermore, EA-UAP prolongs the UAV mission lifetime up to 15% with stable network conditions.

7.5. Discussion

The comparative evaluation provides a broader understanding of how the proposed EA-UAP framework performs against existing UAV authentication schemes, namely PCAP [23], TCALAS [24], and UAP [25]. All protocols were implemented under identical network, latency, and cryptographic conditions on the Raspberry Pi 4B testbed to ensure fair comparison.

7.5.1. Comparative Performance Analysis

EA-UAP achieves an average authentication latency reduction of 15–20% compared with UAP and over 90% compared with TCALAS. This improvement primarily results from minimizing redundant full-scale authentications by dynamically selecting among Full, Fast, and Session-Extension

modes based on the real-time values of the Security Risk Level (SRL) and Energy Stress Level (ESL). Similarly, EA-UAP decreases per-session energy consumption by approximately 27% relative to UAP and by more than an order of magnitude compared with TCALAS, which incurs high ECC pairing costs. The context-aware scheduling effectively balances computational and communication overhead while maintaining equivalent cryptographic strength.

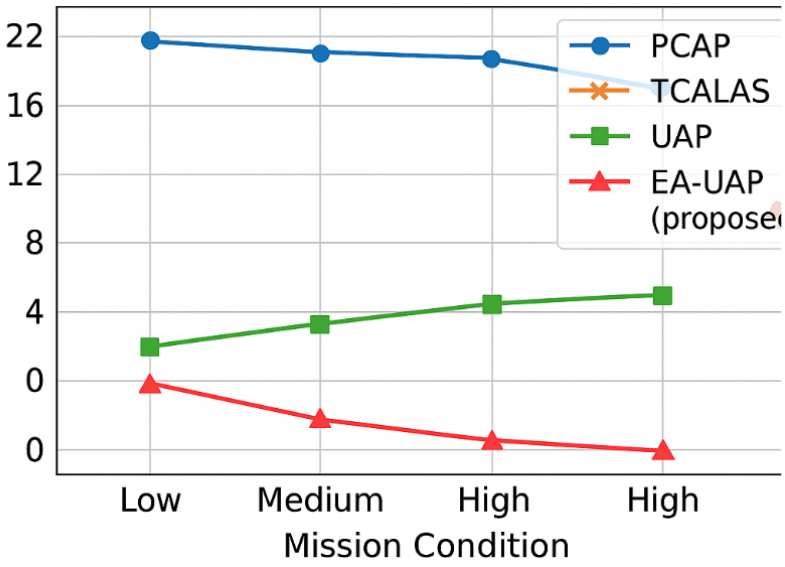

Fig. 7. Energy consumption per authentication session under different mission conditions

7.5.2. Underlying Design Factors

These gains can be explained by about SA-UAP# The three software engineering principles built in EA-UAP. Firstly, by using the Strategy Pattern it is possible select an authentication intensity dynamically without engaging to the system s architecture. Secondly, the Observer Pattern is used to constantly observe telemetry and mission parameters of HET nodes enabling energy aware re-authentication triggers. Third, the software stack introduces encapsulation and isolation mechanisms to reduce cross-layer coupling for scalability and re-usability. These patterns are collectively developed into a scalable, pluggable authentication framework which supports deployment in dynamic and diverse UAV scenarios.

7.5.3. Contextual Interpretation of Results

In practical UAV missions, the reported 27% energy saving translates to an extension of flight time by approximately 9–10 minutes on a typical 60-minute endurance platform, assuming authentication tasks consume about 25–30% of total power. Similarly, the 15–20% latency improvement reduces downtime during relay handovers and link recovery, enhancing real-time responsiveness. These results demonstrate that EA-UAP not only optimizes cryptographic performance but also provides tangible operational benefits for 5G-enabled Internet of Drones (IoD) deployments.

7.5.4. Comparison with State-of-the-Art

PCAP and UAP both also use PUFs to achieve device-level security, but neither customize authentication strength based on contextual information. TCALAS is not viable for light-weight UAVs, even though it has efficient traceability due to the use of pairing based cryptography. It believed that EA-UAP is the first attack model which combines low power monitoring with context-sensitive decision making for a PUF-secured execution environment that has been successfully verified by formal

methods and automated tool support. Thus, EA-UAP fills such a gap between hardware-based trust and adaptive energy-efficient operation for 5G UAV relay networks.

7.6. Software Engineering Performance Evaluation

In addition to cryptographic and network-level performance, this section evaluates the EA-UAP framework from a software engineering perspective. Fig. 8 shows software engineering metrics of the EA-UAP implementation on an embedded UAV platform.

Fig. 8. Software engineering evaluation of the EA-UAP implementation

The objective is to assess the maintainability, scalability, reliability, and efficiency of the software implementation to ensure long-term deployability in UAV-based 5G environments.

7.6.1. Evaluation Environment

The software components of EA-UAP were implemented in Python 3.11 using the pycryptodome library for cryptographic operations. Each functional unit (AuthManager, PUFHandler, ContextMonitor, and EnergyManager) was developed as an independent microservice and deployed using Docker containers.

Automated tests and profiling were conducted on a Lenovo Legion R9000P system (AMDRyzen7 6800H,32GB RAM) running Ubuntu 22.04 LTS.

7.6.2. Evaluation Metrics

Various quantitative software metrics were used to assess quality characteristics and efficiency of EA-UAP. Maintainability Index (MI), Cyclomatic Complexity (CC), Code Reusability, Modularity Index, Execution Efficiency and Scalability Ratio constitute the robustness of software and size scalability. These are directly comparing those how independent the modules are, by how simple is control flow, and what more load can be applied without much slowdown. This proof-of-concept test demonstrates that the microservice architecture remains responsive and available even as the number of concurrent UAVs increases. Hence, EA-UAP provides the balance between security level and software-engineering quality.

7.6.3. Experimental Results

Table 5 presents the insights derived from static analysis, runtime profiling, and code quality assessment. The test proves that the traits of software quality are also still in EA-UAP. Its modular architecture with microservices makes it easy for the users and developers to update any service without

interfering with others, which in turn gives a moderate level on maintainability (82/100).

The low average Cyclomatic Complexity (5.8) indicates a reduced control structure, which is easier to test and debug. Furthermore, long code reusability (65%) is achieved by the system among applicable authentication applications for the IoD. Runtime profiling verifies low-latency request processing, achieving 1.8 ms service response time per authentication cycle on average in the software layer and experiencing only a 7.5% throughput loss when doubling co-existing UAV sessions. These results corroborate the security, low power and compliance to modern software engineering standards of modularity, scalability and maintainability of EA-UAP.

Table 5. Software engineering performance metrics for EA-UAP

Metric	Symbol	EA-UAP Result
Maintainability Index	MI	82 / 100 (High)
Cyclomatic Complexity	CC	5.8 (Low complexity)
Code Reusability	CR	65% (Reusable modules)
Modularity Index	MoI	0.78 (Strong independence)
Execution Efficiency	EE	1.8 ms avg response per request
Scalability Ratio	SR	7.5% degradation for 2× load

8. Conclusion and Future work

In this work, we presented EA-UAP a software-defined adaptive, energy-aware authentication protocol that is applied for 5G-empowered UAV-assisted Internet of drones (IoD) system. In contrast to traditional lightweight schemes that use static or periodic re-authentication, EA-UAP adjusts the intensity of authentication based on the dynamic(real-time) Security Risk Level (SRL) and Energy Stress Level (ESL). This is the flexibility architecture; it can provide a good tradeoff of high security guarantee and long time working for averagely UAVs. In this paper we present EA-UAP, a PUF-based hardware-rooted trust architecture with modular and layered software structure that provides both security robustness and realistic practice. Formal security analysis with Mao–Boyd logic and scyther tool demonstrated the resistance against replay, impersonation, and MITM attacks. Performance analysis over a Raspberry Pi 4 testbed showed that EA-UAP outperforms the baseline UAP protocol with 27% reduction in authentication related energy consumption and 15%-20% latency improvement. Furthermore, software engineering metrics evidenced the high maintainability and low structural complexity, which contributed to the operational integration of the system over the long term. However, the above performance outcomes are based on controlled experimental setups and do not fully model massive mobility (with realistic variations) or severe adversarial conditions. In addition, the adaptive decision logic is based on fixed thresholding for SRL and ESL which may not generalize well across all mission profiles.

In the future, we will fit learning methods (e.g. fuzzy inference systems or reinforcement learning) to tune authentication parameters on-line. Further extensions comprise the implementation of post-quantum cryptographic primitives, more comprehensive realworld experiments (UAV physical flights) and investigation on resilience under large-scale coordinated attacks. These guidelines are expected to improve the strength, flexibility and lifelong security of UAV authentication in 5G wireless networks.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This research received no external funding

Acknowledgment: 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. KFU260300).

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

[1] 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, https://doi.org/10.1007/s11370-022-00452-4.

[2] Y. M. Hussain *et al*., "Smartphone's off grid communication network by using arduino microcontroller and microstrip antenna," *Telecommunication Computing Electronics and Control*, vol. 19, no. 4, pp. 1100–1106, 2021, http://doi.org/10.12928/telkomnika.v19i4.15949.

[3] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 27–36, 2025, https://repository.londonmet.ac.uk/10518/1.haslightboxThumbnailVersion/1042801393600.pdf.

[4] J. Sun, G. Yuan, L. Song, and H. Zhang, "Unmanned aerial vehicles (uavs) in landslide investigation and monitoring: a review," *Drones*, vol. 8, no. 1, p. 30, 2024, https://doi.org/10.3390/drones8010030.

[5] M. A. Istiak *et al*., "Adoption of unmanned aerial vehicle (uav) imagery in agricultural management: A systematic literature review," *Ecological Informatics*, vol. 78, p. 102305, 2023, https://doi.org/10.1016/j.ecoinf.2023.102305.

[6] A. H. A. Alattas, M. A. Al-Shareeda, S. Manickam, and M. A. Saare, "Enhancement of ntsa secure communication with one-time pad (otp) in iot," *Informatica*, vol. 47, no. 1, pp. 1-10, 2023, https://doi.org/10.31449/inf.v47i1.4463.

[7] L. Wang, X. Huang, W. Li, K. Yan, Y. Han, Y. Zhang, L. Pawlowski, and Y. Lan, "Progress in agricultural unmanned aerial vehicles (uavs) applied in china and prospects for poland," *Agriculture*, vol. 12, no. 3, p. 397, 2022, https://doi.org/10.3390/agriculture12030397.

[8] H. Albinhamad, A. Alotibi, A. Alagnam, M. Almaiah, and S. Salloum, "Vehicular ad-hoc networks (vanets): A key enabler for smart transportation systems and challenges," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 4–15, 2025, https://www.researchgate.net/profile/Said-Salloum/publication/392954812_Vehicular_Ad-hoc_Networks_VANETs_A_Key_Enabler_for_Smart_Transportation_Systems_and_Challenges/links/6888efa50786937984557334/Vehicular-Ad-hoc-Networks-VANETs-A-Key-Enabler-for-Smart-Transportation-Systems-and-Challenges.pdf.

[9] M. Saare, A. Hussain, and W. S. Yue, "Investigating the effectiveness of mobile peer support to enhance the quality of life of older adults: A systematic literature review," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 4, pp. 130–139, 2019, https://doi.org/10.3991/ijim.v13i04.10525.

[10] S. Alsahaim and M. Maayah, "Analyzing cybersecurity threats on mobile phones," *STAP Journal of Security Risk Management*, vol. 2023, no. 1, pp. 3–19, 2023, https://doi.org/10.63180/jsrm.thestap.2023.1.2.

[11] A. Gaydamaka, A. Samuylov, D. Moltchanov, M. Ashraf, B. Tan and Y. Koucheryavy, "Dynamic Topology Organization and Maintenance Algorithms for Autonomous UAV Swarms," in *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 4423-4439, 2024, https://doi.org/10.1109/TMC.2023.3293034.

[12] S. Alyahya, W. U. Khan, S. Ahmed, S. N. K. Marwat, and S. Habib, "Cyber Secure Framework for Smart Agriculture: Robust and Tamper-Resistant Authentication Scheme for IoT Devices," *Electronics*, vol. 11, no. 6, p. 963, 2022, https://doi.org/10.3390/electronics11060963.

[13] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, pp. 45–56, 2024, https://doi.org/10.63180/jsrm.thestap.2024.1.3.

[14] Y. M. Dalal, S. S, A. K, T. Y. Satheesha, A. PN and S. Somanath, "Optimizing Security: A Comparative Analysis of RSA, ECC, and DH Algorithms," *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, pp. 1-6, 2024, https://doi.org/10.1109/NKCon62728.2024.10775183.

[15] M. A. Saare, A. Hussain, and W. S. Yue, "Relationships between the older adult's cognitive decline and quality of life: The mediating role of the assistive mobile health applications," *International Journal of Interactive Mobile Technologies*, vol. 13, no. 1, pp. 42–55, 2019, https://doi.org/10.3991/ijim.v13i10.11288.

[16] D. Sudarshan, C. Khandelwal, L. Gowda, K. K. Bijjaragi, and R. SS, "Resource centric analysis of rsa and ecc algorithms on fpga," in *ITM Web of Conferences*, vol. 56, no. 01006, 2023, https://doi.org/10.1051/itmconf/20235601006

[17] B. M. Radhi, A. F. Ataalla, H. M. Alsayednoor, M. A. Al-Shareeda, M. A. Almaayah, and M. Obeidat, "A lightweight identity authentication protocol for nano-scale iot devices," *Engineering, Technology & Applied Science Research*, vol. 15, no. 5, pp. 27938–27946, 2025, https://doi.org/10.48084/etasr.13449.

[18] Z. G. Al-Mekhlafi *et al*., "Chebiod: a chebyshev polynomial-based lightweight authentication scheme for internet of drones environments," *Scientific Reports*, vol. 15, no. 1, p. 32897, 2025, https://doi.org/10.1038/s41598-025-18387-y.

[19] M. Bie, W. Li, T. Chen, L. Nan, and D. Yang, "An energy-efficient reconfigurable asymmetric modular cryptographic operation unit for rsa and ecc," *Frontiers of Information Technology & Electronic Engineering*, vol. 23, no. 1, pp. 134–144, 2022, https://doi.org/10.1631/FITEE.2000325.

[20] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the unmanned aerial vehicles (uavs): A comprehensive review," *Drones*, vol. 6, no. 6, p. 147, 2022, https://doi.org/10.3390/drones6060147.

[21] P. Shukla, S. Shukla and A. Kumar Singh, "Trajectory-Prediction Techniques for Unmanned Aerial Vehicles (UAVs): A Comprehensive Survey," in *IEEE Communications Surveys & Tutorials*, vol. 27, no. 3, pp. 1867-1910, 2025, https://doi.org/10.1109/COMST.2024.3471671.

[22] K. Osmani and D. Schulz, "Comprehensive investigation of unmanned aerial vehicles (uavs): An in-depth analysis of avionics systems," *Sensors*, vol. 24, no. 10, p. 3064, 2024, https://doi.org/10.3390/s24103064.

[23] C. Pu and Y. Li, "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System," *2020 IEEE International Symposium on Local and Metropolitan Area Networks*, pp. 1-6, 2020, http://doi.org/10.1109/LANMAN49260.2020.9153239.

[24] J. Srinivas, A. K. Das, N. Kumar and J. J. P. C. Rodrigues, "TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903-6916, 2019, https://doi.org/10.1109/TVT.2019.2911672.

[25] C. Liu, T. Huang and M. Ma, "UAP: A System Authentication Protocol for UAV Relay Communication by UAV-Assisted," in *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 1539-1550, 2025, https://doi.org/10.1109/OJVT.2025.3567079.

[26] S. Shashannk, G. Vishal, and S. Sandosh, *A comprehensive survey on cutting-edge ecc and puf algorithm to enhance security*, Springer Nature, 2024, https://books.google.co.id/books?id=HpokEQAAQBAJ&hl=id&source=gbs_navlinks_s.

[27] M. Kabi, N. Dayal and P. Raikwal, "ECC-Based Lightweight Authentication for Resource-Constrained Devices Leveraging the Edge Node," in *IEEE Transactions on Reliability*, vol. 74, no. 2, pp. 2605-2612, 2025, https://doi.org/10.1109/TR.2025.3562300.

[28] B. Renuka Devi and V. Sarveshwaran, "A Systematic Review of UAV Protocol Architectures for Enhanced Communication," *2024 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, pp. 1-13, 2024, https://doi.org/10.1109/IC3IoT60841.2024.10550293.

[29] V. O. Nyangaresi, M. Ahmad, L. A. Maghrabi and T. Althaqafi, "Cost-Effective PUF and ECC-Based Authentication Protocol for Secure Internet of Drones Communication," in *IEEE Internet of Things Journal*, vol. 12, no. 16, pp. 33844-33857, 2025, https://doi.org/10.1109/JIOT.2025.3576313.

[30] J. Sharma, P. S. Mehra, D. Chawla, D. Dabas, and A. Jamshed, "Secure communication and authentication in iot-based uav networks," in *Network Optimization in Intelligent Internet of Things Applications*, pp. 257–273, 2024, https://doi.org/10.1201/9781003405535.

[31] S. U. Jan and H. U. Khan, "Identity and Aggregate Signature-Based Authentication Protocol for IoD Deployment Military Drone," in *IEEE Access*, vol. 9, pp. 130247-130263, 2021, https://doi.org/10.1109/ACCESS.2021.3110804.

[32] D. He, W. Yuan, J. Wu and R. Liu, "Ubiquitous UAV Communication Enabled Low-Altitude Economy: Applications, Techniques, and 3GPP's Efforts," in *IEEE Network*, vol. 40, no. 1, pp. 115-122, 2026, https://doi.org/10.1109/MNET.2025.3574922.

[33] J. Zhang, Q. Cheng, X. Chen and X. Luo, "CSAP-IoD: A Chaotic Map-Based Secure Authentication Protocol for Internet of Drones," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 8848-8862, 2025, https://doi.org/10.1109/TIFS.2025.3599678.

[34] A. Irshad, B. A. Alzahrani, A. Albeshri, K. Alsubhi, A. Nayyar and S. A. Chaudhry, "SPAKE-DC: A Secure PUF Enabled Authenticated Key Exchange for 5G-Based Drone Communications," in *IEEE Transactions on Vehicular Technology*, vol. 73, no. 4, pp. 5770-5780, 2024, https://doi.org/10.1109/TVT.2023.3333398.

[35] D. Mishra *et al*., "Quantum-Safe Secure and Authorized Communication Protocol for Internet of Drones," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 16499-16507, 2023, https://doi.org/10.1109/TVT.2023.3292169.

[36] L. Zhang, A. Celik, S. Dang and B. Shihada, "Energy-Efficient Trajectory Optimization for UAV-Assisted IoT Networks," in *IEEE Transactions on Mobile Computing*, vol. 21, no. 12, pp. 4323-4337, 2022, https://doi.org/10.1109/TMC.2021.3075083.

[37] B. Zhu, E. Bedeer, H. H. Nguyen, R. Barton and J. Henry, "UAV Trajectory Planning in Wireless Sensor Networks for Energy Consumption Minimization by Deep Reinforcement Learning," in *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9540-9554, 2021, https://doi.org/10.1109/TVT.2021.3102161.

[38] C. Zhao, X. Pang, W. Lu, Y. Chen, N. Zhao and A. Nallanathan, "Energy Efficiency Optimization of IRS-Assisted UAV Networks Based on Statistical Channels," in *IEEE Wireless Communications Letters*, vol. 12, no. 8, pp. 1419-1423, 2023, https://doi.org/10.1109/LWC.2023.3276910.

[39] O. M. Gul, A. M. Erkmen and B. Kantarci, "UAV-Driven Sustainable and Quality-Aware Data Collection in Robotic Wireless Sensor Networks," in *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25150-25164, 2022, https://doi.org/10.1109/JIOT.2022.3195677.

[40] M. Li, X. Tao, N. Li, H. Wu and J. Xu, "Secrecy Energy Efficiency Maximization in UAV-Enabled Wireless Sensor Networks Without Eavesdropper's CSI," in *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3346-3358, 2022, https://doi.org/10.1109/JIOT.2021.3098049.

[41] X. Zhu, L. Wang, Y. Li, S. Song, S. Ma, F. Yang, and L. Zhai, "Path planning of multi-uavs based on deep q-network for energy-efficient data collection in uavs-assisted iot," *Vehicular Communications*, vol. 36, p. 100491, 2022, https://doi.org/10.1016/j.vehcom.2022.100491.

[42] E. Eldeeb, J. M. d. S. Sant'Ana, D. E. Pérez, M. Shehab, N. H. Mahmood and H. Alves, "Multi-UAV Path Learning for Age and Power Optimization in IoT With UAV Battery Recharge," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5356-5360, 2023, https://doi.org/10.1109/TVT.2022.3222092.

[43] T. Zhao, F. Li and L. He, "Secure Video Offloading in Multi-UAV-Enabled MEC Networks: A Deep Reinforcement Learning Approach," in *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2950-2963, 2024, https://doi.org/10.1109/JIOT.2023.3296613.

[44] Y. Yu, J. Tang, J. Huang, X. Zhang, D. K. C. So and K. -K. Wong, "Multi-Objective Optimization for UAV-Assisted Wireless Powered IoT Networks Based on Extended DDPG Algorithm," in *IEEE Transactions on Communications*, vol. 69, no. 9, pp. 6361-6374, 2021, https://doi.org/10.1109/TCOMM.2021.3089476.

[45] K. Lounis, S. H. H. Ding and M. Zulkernine, "D2D-MAP: A Drone to Drone Authentication Protocol Using Physical Unclonable Functions," in *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5079-5093, 2023, https://doi.org/10.1109/TVT.2022.3224611.

[46] J. Zhu, J. Peng, and L. Wang, "A lightweight and trustworthy authentication protocol for uav networks based on puf," in *Proceedings of the 2024 14th International Conference on Communication and Network Security*, pp. 71–77, 2024, https://doi.org/10.1145/3711618.3711630.

[47] O. Ionescu and V. Dumitru, *New methods for uavs identification based on the physical unclonable functions (pufs) of electronic devices*, in Modern Technologies Enabling Safe and Secure UAV Operation in Urban Airspace, pp. 64–69, 2021, https://doi.org/10.3233/NICSP210007.

[48] M. Oduro-Antwi, D. Nguyen, and K. Sood, "Physically unclonable functions (puf)-based iot security: challenges and opportunities," *Internet of Things Security*, pp. 201–217, 2026, https://doi.org/10.1016/B978-0-44-333759-8.00020-4.

[49] X. Huang, B. Han, J. Su, X. Ji and J. Li, "Secure Multi-path Routing Protocol based on Physical Unclonable Functions Authentication," *IEEE INFOCOM 2025 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1-2, 2025, https://doi.org/10.1109/INFOCOMWKSHPS65812.2025.11152923.

[50] S. A. Majmaie, N. P. Bhatta, P. P. Kharat and F. Amsaad, "PUF-Based Hardware Security for Trusted Internet of Drones: Challenges and Future Directions," *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*, pp. 1-7, 2025, https://doi.org/10.1109/SATC65530.2025.11136985.

[51] W. Lalouani, "Sec-PUF: Securing UAV Swarms Communication with Lightweight Physical Unclonable Functions," *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 286-291, 2023, https://doi.org/10.1109/WiMob58348.2023.10187758.

[52] P. Mall, R. Amin, A. K. Das, M. T. Leung and K. -K. R. Choo, "PUF-Based Authentication and Key Agreement Protocols for IoT, WSNs, and Smart Grids: A Comprehensive Survey," in *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8205-8228, 2022, https://doi.org/10.1109/JIOT.2022.3142084.

[53] Y. Zheng, W. Liu, C. Gu and C. -H. Chang, "PUF-Based Mutual Authentication and Key Exchange Protocol for Peer-to-Peer IoT Applications," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 4, pp. 3299-3316, 2023, https://doi.org/10.1109/TDSC.2022.3193570.

[54] R. De Smet, T. Vandervelden, K. Steenhaut, and A. Braeken, "Lightweight puf based authentication scheme for fog architecture," *Wireless Networks*, vol. 27, no. 2, pp. 947–959, 2021, https://doi.org/10.1007/s11276-020-02491-0.

[55] S. Manivannan, R. S. Chakraborty, I. Chakrabarti and J. Ramalingam, "Practical and Efficient PUF-Based Protocol for Authentication and Key Agreement in IoT," in *IEEE Embedded Systems Letters*, vol. 16, no. 2, pp. 118-121, 2024, https://doi.org/10.1109/LES.2023.3299200.

[56] S. R. Addula and A. Ali, "A novel permissioned blockchain approach for scalable and privacy-preserving iot authentication," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 222–237, 2025, https://doi.org/10.63180/jcsra.thestap.2025.4.3.

[57] M. A. Almaiah and R. Kadel, "Leveraging aco, ga, and gwo for enhancing port scan attack detection using machine learning," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 306–326, 2025, https://doi.org/10.63180/jcsra.thestap.2025.4.9.

[58] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A hybrid genetic algorithm and hidden markov model-based hashing technique for robust data security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 42–56, 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.6.

[59] V. Kalmani, V. Jadhav, A. Alqutaish, and G. Alradwan, "Geometry-aware multi-view malware detection using gromov–wasserstein fusion," *Journal of Cyber Security and Risk Auditing*, vol. 2026, no. 1, p. 20–37, 2026, http://dx.doi.org/10.63180/jcsra.thestap.2026.1.2.

[60] 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.

[61] Z. Wang, X. Li, H. Cheng, Z. Huang, L. Kong, and L. Wang, "An access control scheme for uav swarm based on cp-abe," in *International Conference on Autonomous Unmanned Systems*, pp. 172–185, 2025, https://doi.org/10.1007/978-981-96-3572-6_17.

[62] V. O. Nyangaresi, H. M. Jasim, K. A.-A. Mutlaq, Z. A. Abduljabbar, J. Ma, I. Q. Abduljaleel, and D. G. Honi, "A symmetric key and elliptic curve cryptography-based protocol for message encryption in unmanned aerial vehicles," *Electronics*, vol. 12, no. 17, p. 3688, 2023, https://doi.org/10.3390/electronics12173688.

[63] S. Samanth, P. K. V and M. Balachandra, "ECC-based Authenticated Key-Agreement Algorithm using Time-stamps for IoD networks," *2022 International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, pp. 118-123, 2022, https://doi.org/10.1109/DISCOVER55800.2022.9974860.

[64] Z. Zhang, Y. Huang, W. Huang, W. Pan, Y. Liao and S. Zhou, "An Auto-Upgradable End-to-End Preauthenticated Secure Communication Protocol for UAV-Aided Perception Intelligent System," in *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 30187-30203, 2024, https://doi.org/10.1109/JIOT.2024.3413010.

[65] S. Bhaskar, K. Parmar, and D. C. Jinwala, "Comparative evaluation of pairing-free and pairing-based cp-abe schemes for resource constrained environments," *Cluster Computing*, vol. 28, no. 7, p. 431, 2025, https://doi.org/10.1007/s10586-024-05072-4.

[66] F. Shohaimay and E. S. Ismail, "Improved and provably secure ecc-based two-factor remote authentication scheme with session key agreement," *Mathematics*, vol. 11, no. 1, p. 5, 2022, https://doi.org/10.3390/math11010005.

[67] D. A. Laila, "Responsive machine learning framework and lightweight utensil of prevention of evasion attacks in the iot-based ids," *STAP Journal of Security Risk Management*, vol. 2025, no. 1, pp. 59–70, 2025, https://doi.org/10.63180/jsrm.thestap.2025.1.3.

[68] M. Alrajeh, M. Almaiah, and U. Mamodiya, "Cyber risk analysis and security practices in industrial manufacturing: Empirical evidence and literature insights," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2026, no. 1, 2026, https://journals.theitap.org/index.php/ijcei/article/view/8/9.

[69] S. Alsahaim, M. A. Almaiah, and R. B. Sulaiman, "Security threats in mobile phones: Challenges, countermeasures, and the importance of user awareness," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2023, no. 1, 2023, https://journals.theitap.org/index.php/ijcei/article/view/1/3.

[70] M. S. Alghareeb, M. Almaiah, and Y. Badr, "Cyber security threats in wireless lan: A literature review," *International Journal of Cybersecurity Engineering and Innovation*, vol. 2024, no. 1, 2024, https://journals.theitap.org/index.php/ijcei/article/view/6/5.

[71] T. Li *et al*., "Energy-Efficient and Secure Communication Toward UAV Networks," in *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10061-10076, 2022, https:/doi.org/10.1109/JIOT.2021.3118079.

[72] Y. Zhang, R. Zhao, D. Mishra, and D. W. K. Ng, "A comprehensive review of energy-efficient techniques for uav-assisted industrial wireless networks," *Energies*, vol. 17, no. 18, p. 4737, 2024, https://doi.org/10.3390/en17184737.

[73] S. Seng, G. Yang, X. Li, H. Ji and C. Luo, "Energy-Efficient Communications in Unmanned Aerial Relaying Systems," in *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 2780-2791, 2021, https://doi.org/10.1109/TNSE.2021.3064317.

[74] K. Seerangan, M. Nandagopal, T. Govindaraju, N. Manogaran, B. Balusamy, and S. Selvarajan, "A novel energy-efficiency framework for uav-assisted networks using adaptive deep reinforcement learning," *Scientific Reports*, vol. 14, no. 1, p. 22188, 2024, https://doi.org/10.1038/s41598-024-71621-x.

[75] T. Wang, Y. Li and Y. Wu, "Energy-Efficient UAV Assisted Secure Relay Transmission via Cooperative Computation Offloading," in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 4, pp. 1669-1683, 2021, https://doi.org/10.1109/TGCN.2021.3099523.

[76] X. Lan, X. Tang, R. Zhang, W. Lin and Z. Han, "UAV-Assisted Computation Offloading Toward Energy-Efficient Blockchain Operations in Internet of Things," in *IEEE Wireless Communications Letters*, vol. 12, no. 8, pp. 1469-1473, 2023, https://doi.org/10.1109/LWC.2023.3279317.

[77] P. Phalaagae, A. M. Zungeru, B. Sigweni, S. Rajalakshmi, H. Batte, and O. S. Eyobu, "An energy efficient authentication scheme for cluster-based wireless iot sensor networks," *Scientific African*, vol. 25, p. e02287, 2024, https://doi.org/10.1016/j.sciaf.2024.e02287.

[78] O. A. Khashan, N. M. Khafajah, N. Mohamed, and B. Salaimah, "Energy-efficient dynamic adaptive encryption for low-resource internet of things," in *International Conference on Smart Technology*, pp. 191–202, 2025, https://doi.org/10.1007/978-3-031-64957-8_15.

[79] L. Nkenyereye, A. Thakare, P. Khataniar, R. Imandi, and P. K. BN, "Lightweight authentication protocol for smart grids: An energy-efficient authentication scheme for resource-limited smart meters," *Mathematics*, vol. 13, no. 4, p. 580, 2025, https://doi.org/10.3390/math13040580.

[80] T. Ara, J. Ambareen, S. Venkatesan, M. Geetha, A. Bhuvanesh, "An energy efficient selection of cluster head and disease prediction in iot based smart agriculture using a hybrid artificial neural network model," *Measurement: Sensors*, vol. 32, p. 101074, 2024, https://doi.org/10.1016/j.measen.2024.101074.

[81] A. Hajjouz and E. Y. Avksentieva, "Enhancing and extending catboost for accurate detection and classification of dos and ddos attack subtypes in network traffic," *Information Technologies, Mechanics and Optics*, vol. 25, no. 1, pp. 114–127, 2025, https://doi.org/10.17586/2226-1494-2025-25-1-114-127.

[82] Q. Xie and J. Zhang, "Lightweight drone-to-ground station and drone-to-drone authentication scheme for internet of drones," *Symmetry*, vol. 17, no. 4, p. 556, 2025, https://doi.org/10.3390/sym17040556.

[83] 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," in *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 5, pp. 4795-4812, 2025, https://doi.org/10.1109/TDSC.2025.3553868.

[84] S. Khan, G. S. Gaba, A. Gurtov, N. Mäurer, T. Gräupl and C. Schmitt, "Enhancing Cybersecurity for LDACS: a Secure and Lightweight Mutual Authentication and Key Agreement Protocol," *2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC)*, pp. 1-10, 2023, https://doi/org/10.1109/DASC58513.2023.10311307.

[85] N. Oláh, B. Molnár, and A. Huszti, "Secure registration protocol for the internet of drones using blockchain and physical unclonable function technology," *Symmetry*, vol. 15, no. 10, p. 1886, 2023, https://doi.org/10.3390/sym15101886.

[86] Y. Xiao *et al*., "Fully Decentralized Federated Learning-Based On-Board Mission for UAV Swarm System," in *IEEE Communications Letters*, vol. 25, no. 10, pp. 3296-3300, 2021, https://doi.org/10.1109/LCOMM.2021.3095362.

[87] M. Najim, "Securing uavs assisted ground network using puf-based lightweight authentication protocol," *Security and Privacy*, vol. 8, no. 6, p. e70139, 2025, https://doi.org/10.1002/spy2.70139.

[88] M. S. Alkatheiri, S. Saleem, M. A. Alqarni, A. O. Aseeri, S. H. Chauhdary, and Y. Zhuang, "A lightweight authentication scheme for a network of unmanned aerial vehicles (uavs) by using physical unclonable functions," *Electronics*, vol. 11, no. 18, p. 2921, 2022, https://doi.org/10.3390/electronics11182921.

[89] M. M. Qasim, J. M. Altmemi, A. H. Abd Ali, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Cahbca: A software engineering framework for secure, scalable, and adaptive healthcare blockchain systems," *Journal of Robotics and Control (JRC)*, vol. 6, no. 4, pp. 2052–2063, 2025, https://doi.org/10.18196/jrc.v6i4.26643.

[90] İ. Baştürk, "Energy-efficient communication for uav-enabled mobile relay networks," *Computer Networks*, vol. 213, p. 109071, 2022, https://doi.org/10.1016/j.comnet.2022.109071.

[91] M. A. Al-Shareeda *et al*., "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 12, p. 5939, 2022, https://doi.org/10.3390/app12125939.

[92] Q. Li, P. Si, Y. Zhang, J. Wang, D. Zhang and F. R. Yu, "UAV Altitude, Relay Selection, and User Association Optimization for Cooperative Relay-Transmission in UAV-IRS-Based THz Networks," in *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 2, pp. 815-826, 2024, https://doi.org/10.1109/TGCN.2023.3347567.

[93] Q. Feng, M. Liu, H. Dui, Y. Ren, B. Sun, D. Yang, and Z. Wang, "Importance measure-based phased mission reliability and uav number optimization for swarm," *Reliability engineering & system safety*, vol. 223, p. 108478, 2022, https://doi.org/10.1016/j.ress.2022.108478.

[94] M. Al Shareeda, A. Khalil and W. Fahs, "Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm," *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1-5, 2018, https://doi.org/10.1109/ACIT.2018.8672687.

[95] Z. Kaleem, F. A. Orakzai, W. Ishaq, K. Latif, J. Zhao and A. Jamalipour, "Emerging Trends in UAVs: From Placement, Semantic Communications to Generative AI for Mission-Critical Networks," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 3, pp. 7412-7438, 2025, https://doi.org/10.1109/TCE.2024.3434971.

[96] J. Song, K. Zhao, and Y. Liu, "Survey on mission planning of multiple unmanned aerial vehicles," *Aerospace*, vol. 10, no. 3, p. 208, 2023, https://doi.org/10.3390/aerospace10030208.

[97] 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, https://doi.org/10.1016/j.iot.2024.101096.

[98] J.-C. Chaudemar, O. Aïello, P. de Saqui-Sannes, and O. Poitou, "Mission-based design of uavs," *Systems Engineering*, vol. 27, no. 5, pp. 850–868, 2024, https://doi.org/10.1002/sys.21754.

[99] M. M. A. Al-shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and I. H. Hasbullah, "Security schemes based conditional privacy-preserving in vehicular ad hoc networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 479–488, 2020, https://doi.org/10.11591/ijeecs.v21.i1.pp479-488.