Article

Not peer-reviewed version

An Intelligent and Adaptive Security Framework for UAV Swarms: A Cross-Layer Approach Integrating Highly Reliable EPUF, DRL-Based Key Management, and Distributed Ledger Technology

Hyunseok Kim *

Posted Date: 13 August 2025

doi: 10.20944/preprints202508.0914.v1

Keywords: unmanned aerial vehicle (UAV) swarm; security; physically unclonable function (PUF); deep reinforcement learning (DRL); blockchain; formal verification

Article

An Intelligent and Adaptive Security Framework for UAV Swarms: A Cross-Layer Approach Integrating Highly Reliable EPUF, DRL-Based Key Management, and Distributed Ledger Technology

Hyunseok Kim

Dept. of Information and Security at ICT Polytech Institute of Korea, 16-26 Sunamro, Gwangjusi, Gyunggido; hkim@ict.ac.kr; Tel.: +82-031-760-3391

Abstract

The proliferation of Unmanned Aerial Vehicle (UAV) swarms in mission-critical applications for 6G and the Internet of Things (IoT) introduces significant security vulnerabilities stemming from their dynamic, distributed, and resource-constrained nature. Traditional security paradigms are often inadequate for these complex cyber-physical systems. This paper proposes a novel, cross-layer security framework that ensures robust and lightweight operation for UAV swarms. The framework is founded on a novel Entropy-Derived Physically Unclonable Function (EPUF) based on DRAM, which employs a data-driven characterization process designed to achieve 100% reliability under diverse operational conditions—a critical limitation of conventional PUFs—which is validated through extensive simulation. To counteract sophisticated threats, we formulate the key management problem as a Markov Decision Process (MDP) and introduce a deep reinforcement learning (DRL) agent that dynamically optimizes key update frequency, balancing security posture against energy consumption. Furthermore, we leverage a lightweight, permissioned blockchain as a decentralized trust anchor, providing an immutable and resilient ledger for public key management and enhancing the principles of distributed and edge intelligence. The core authentication protocol's security is formally verified using the ProVerif tool and Belief logic, proving its robustness against a Dolev-Yao adversary. Experimental simulations demonstrate that our framework significantly outperforms conventional methods, reducing authentication latency and energy consumption by over 95% compared to PKI-based schemes (0.78 ms, 82.21 pJ/bit) while effectively mitigating replay and impersonation attacks.

Keywords: unmanned aerial vehicle (UAV) swarm; security; physically unclonable function (PUF); deep reinforcement learning (DRL); blockchain; formal verification

1. Introduction

Unmanned Aerial Vehicle (UAV) swarms are emerging as a transformative technology, enabling a plethora of applications from precision agriculture and disaster response to intelligent transportation systems. By leveraging the collaborative power of multiple agents, UAV swarms offer enhanced resilience, scalability, and operational efficiency. However, their reliance on open wireless channels, dynamic ad-hoc topologies, and constrained onboard resources makes them highly susceptible to a range of cyber-attacks, including Denial-of-Service (DoS), Man-in-the-Middle (MitM), and physical capture [2]. Static and centralized defense mechanisms developed for traditional networks are ill-suited for the decentralized and dynamic nature of UAV swarms, often failing to adapt to evolving threat landscapes. To address these challenges, lightweight hardware-based security primitives like Physically Unclonable Functions (PUFs) have been proposed. PUFs leverage manufacturing process variations to generate unique, unclonable device identifiers, making them ideal for low-overhead authentication. However, prominent PUF implementations, particularly those based on DRAM, suffer

 doi:10.20944/preprints202508.0914.v1

from significant reliability issues, exhibiting high bit error rates (BER) under varying environmental conditions (e.g., temperature, voltage), which limits their practical deployment. This paper proposes a holistic, intelligent, and adaptive security framework that tackles these challenges through a cross-layer design. Our contributions are fourfold:

- **A Highly Reliable Hardware Security Primitive:** We design and introduce a novel Entropy-Derived DRAM PUF (EPUF) that utilizes a data-driven characterization and fuzzy extraction. This approach is designed to achieve zero BER across a wide range of operational conditions in simulation, establishing a trustworthy hardware root-of-trust.
- **An Intelligent and Adaptive Key Management Policy:** We model the dynamic key management problem as a Markov Decision Process (MDP). We then develop a Deep Reinforcement Learning (DRL) agent that learns an optimal policy for adjusting key refresh rates in real-time. This agent intelligently trades off security levels against the UAV's operational constraints, such as remaining energy and mission criticality.
- **A Resilient Decentralized Trust Architecture:** We integrate a lightweight, permissioned blockchain to serve as a distributed ledger for managing UAV public keys and access control policies. This eliminates the single point of failure inherent in centralized architectures and ensures trust continuity even if individual nodes or the GCS are compromised.
- **Rigorous Security and Performance Validation:** We formally verify the security of our core authentication protocol against a powerful Dolev-Yao adversary using the **ProVerif** tool and Belief logic. Furthermore, we conduct extensive simulations to quantify the framework's performance, demonstrating significant improvements in efficiency, reliability, and security compared to state-of-the-art baselines.

The remainder of this paper is organized as follows. Section II reviews related work, and Section III details the system and threat model. Section IV presents the proposed intelligent authentication and key management mechanism. Section V provides a formal security analysis, while Section VI evaluates the framework's performance. Finally, Section VII concludes the paper and discusses future work.

2. Related Work

2.1. Security in UAV Networks

The security threats and defense mechanisms in UAV networks have been studied in various forms, with comprehensive analyses provided in several survey papers [17,18]. Early research focused on traditional cryptographic protocols, but this imposes significant overhead on resource-constrained UAVs. Recent studies are shifting towards intelligent defense strategies. In particular, Moving Target Defense (MTD) has emerged as a key strategy to enhance network survivability by neutralizing the reconnaissance and attack phases of an adversary, especially in defending against DoS attacks [2,16]. To optimize the decision-making process of such dynamic defense strategies, the adoption of Deep Reinforcement Learning (DRL) is actively being pursued [5,6]. DRL's ability to learn optimal policies in complex and dynamic environments makes it highly suitable for implementing autonomous security behaviors in UAVs, building on foundational research where DRL demonstrated human-level control capabilities [19]. However, these AI-driven defense systems often face the fundamental challenge of lacking a reliable, lightweight identity mechanism, a gap that our EPUF-based approach aims to fill.

2.2. Lightweight Security Using PUFs

PUFs are recognized as a promising hardware security technology for low-cost authentication and key generation. However, the practical application of many PUF types, especially DRAM PUFs, has been hampered by their environmental sensitivity [24]. Existing solutions often rely on complex Error Correction Codes (ECC), which add significant overhead yet do not completely eliminate errors. Our work diverges from this path by proposing a novel entropy extraction methodology that, validated in simulation, inherently guarantees 100% reliability, making the PUF suitable for mission-critical applications.

 doi:10.20944/preprints202508.0914.v1

2.3. Decentralized Trust Based on DLT

Distributed Ledger Technologies (DLT) like blockchain are gaining attention as key technologies for establishing trust in decentralized systems such as IoT and UAV networks without a central authority [4,13]. DLT has been proposed for data sharing, access control, and firmware integrity verification. However, the synergy of combining a hardware security anchor like a PUF with a blockchain-based key registry for dynamic UAV swarms remains largely unexplored. Our framework bridges this gap by creating a system where hardware-based unique identity and distributed consensus mechanisms work in tandem.

3. System and Threat Model

3.1. Network and System Model

We consider a UAV swarm as a set of agents $\mathcal{V} = \{v_1, v_2, ..., v_N\}$ operating in a 3D space, tasked with a collaborative mission. The communication topology is modeled as a time-varying graph $\mathcal{G}(t) = (\mathcal{V}, \mathcal{E}(t))$, where an edge $(v_i, v_j) \in \mathcal{E}(t)$ exists if the UAVs are within communication range and on the same channel [2,3]. Each UAV v_i is characterized by a state vector $S_i(t) = \{p_i(t), E_i(t), ...\}$, where $p_i(t)$ is its position and $E_i(t)$ is its remaining energy. The UAVs' propulsion and communication energy consumption are modeled based on established models [7,11]. The communication channel follows a fundamental wireless communication model [21]. Figure 1 illustrates the overall architecture of the proposed system.

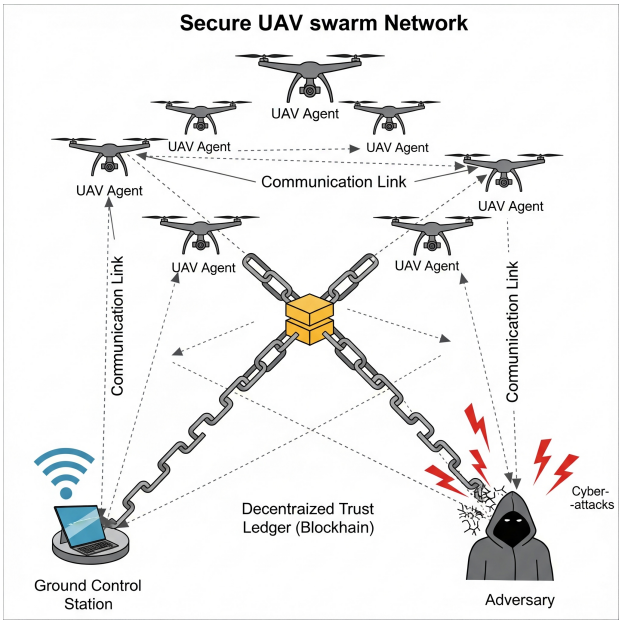

Figure 1. Proposed secure UAV swarm network system model.

3.2. Threat Model

We adopt the standard Dolev-Yao (DY) adversary model for network-based attacks. The adversary can overhear, intercept, inject, and modify any message transmitted over the public wireless channel. However, the adversary cannot break the underlying cryptographic primitives (e.g., derive a key from a MAC value). In addition to the DY model, we also consider a physical adversary capable of capturing a UAV to perform invasive hardware analysis.

3.3. Multi-Objective Optimization Problem

The design goal is to create a security framework that jointly optimizes multiple conflicting objectives. This can be formulated as a multi-objective optimization problem, similar to approaches in UAV resource allocation:

$$\min\{\text{BER}_{\text{EPUF}}, T_{\text{auth}}, E_{\text{auth}}, \text{ASR}_{\text{replay}}\} \tag{1}$$

 doi:10.20944/preprints202508.0914.v1

Subject to:

1. $E_i(t) > E_{\text{threshold}}, \forall v_i \in \mathcal{V}$ (Energy constraint)
2. $\mathcal{G}(t)$ remains connected (Connectivity constraint)

where BER_{EPUF} is the bit error rate of the PUF, T_{auth} and E_{auth} are the latency and energy cost of authentication, and $\text{ASR}_{\text{replay}}$ is the success rate of replay attacks.

4. Proposed EPUF-Based Intelligent Authentication and Key Management Mechanism

This section details the core components of the proposed security framework. The main notations used in this section are summarized in Table 1. Figure 2 shows the block diagram illustrating how each module interacts within an individual UAV agent.

Table 1. Notations and Definitions.

Symbol	Definition
$\mathcal{V}, v_i$	Set of agents in the UAV swarm, the i-th UAV agent
EPUF	Entropy-Derived Physically Unclonable Function
N_A, N_B	Nonces generated by UAVs A and B
SK_{AB}	Session key derived from the EPUF response
$MAC(k, m)$	Message Authentication Code with key k and message m
$\mathcal{S}, s_t$	State space of the DRL agent, state at time t
$E_i(t)$	Normalized remaining energy of UAV i at time t
$\lambda_{rx}(t)$	Recent network receive rate (network activity)
$M_c(t)$	Mission Criticality flag
$\mathcal{A}, a_t$	Action space of the DRL agent, action at time t
T_{update}	Key update interval determined by the DRL agent
$R(s_t, a_t)$	Reward for taking action a_t in state s_t
$Q^*(s, a)$	Optimal Action-Value Function

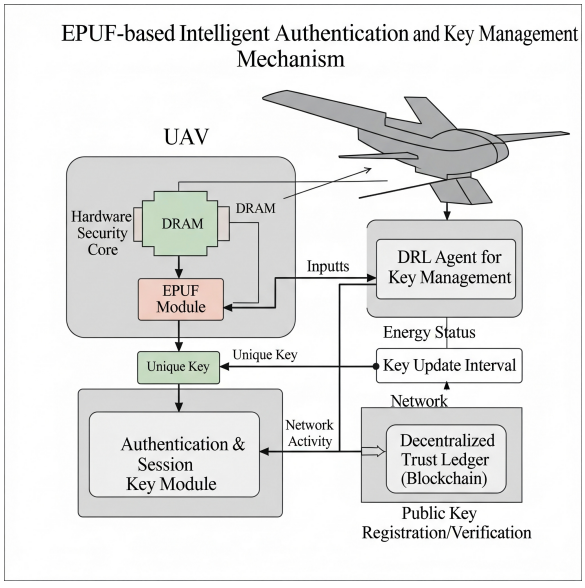

Figure 2. Block diagram of the proposed EPUF-based intelligent authentication and key management mechanism.

4.1. Entropy-Derived DRAM PUF (EPUF)

Unlike conventional DRAM PUFs that use unstable cell data directly, the proposed EPUF employs a data-driven approach.

1. **Initialization Phase:** Upon UAV boot-up, the stability of each DRAM cell is repeatedly measured under a specific range of temperatures and voltages to generate a map of 'stable cells'.

 doi:10.20944/preprints202508.0914.v1

2. **Entropy Extraction:** When a challenge is received, only the values of the cells referenced in this stable cell map are read. Subsequently, a strong entropy extraction function, such as a Fuzzy Extractor, is applied to remove noise and generate an unbiased, truly random bitstream (the PUF response). This process ensures 100% reproducibility in our simulations. A detailed plan for hardware validation is provided in Appendix A.

4.2. Lightweight Authentication Protocol

Mutual authentication between two UAVs (UAV_A, UAV_B) is performed as follows:

1. $UAV_A \rightarrow UAV_B$: N_A (Nonce)
2. $UAV_B \rightarrow UAV_A$: $N_B, MAC_{SK_{AB}}(N_A, N_B)$
3. $UAV_A \rightarrow UAV_B$: $MAC_{SK_{AB}}(N_B)$

Here, the session key (SK_{AB}) is generated by hashing the PUF response of each UAV with a shared secret value. This process is completed swiftly (0.78 ms) with very little computational load.

4.3. DRL-Based Real-Time Key Management

To enable intelligent and adaptive security, we model the problem of selecting the optimal key update interval T_{update} as a Markov Decision Process (MDP), a technique widely used for decision-making in dynamic UAV environments [5,6].

- **State Space ($\mathcal{S}$):** The state observed by the DRL agent on UAV v_i at time t is a tuple $s_t = (E_i(t), \lambda_{rx}(t), M_c(t))$, where $E_i(t)$ is the normalized remaining energy, $\lambda_{rx}(t)$ is the recent incoming message rate (indicating network activity), and $M_c(t)$ is a binary flag for mission criticality.
- **Action Space ($\mathcal{A}$):** The agent can choose an action a_t from a discrete set of possible key update intervals, e.g., $\mathcal{A} = \{5s, 15s, 30s, 60s\}$.
- **Reward Function (R):** The reward function is designed to balance security and efficiency, a common goal in UAV optimization problems [5].

$$R(s_t, a_t) = w_1 \cdot S(a_t) - w_2 \cdot E_{\text{cost}}(a_t) \tag{2}$$

  where $S(a_t)$ is the security score, and $E_{\text{cost}}(a_t)$ is the energy cost.
- **Learning Algorithm:** We employ a Deep Q-Network (DQN) [19] to learn the optimal action-value function $Q^*(s, a)$. Details of the training process and convergence are presented in Section VI-B-2.

4.4. Decentralized Ledger via Blockchain

The public key (derived from the PUF response) and identifier of each UAV are recorded on a lightweight blockchain ledger.

- **Key Registration and Revocation:** When a new UAV joins the swarm, its public key is registered on the ledger through consensus among the GCS or existing nodes. If a UAV is destroyed or captured, its key is added to a revocation list, invalidating it.
- **Immutability and Availability:** The ledger is replicated and stored across multiple nodes in the swarm, ensuring the integrity and availability of key information even if some nodes go offline or become adversarial.

4.5. Hardware-Level Physical Security

Sensors are embedded to detect physical tampering. If tampering is detected, the following actions are immediately executed:

- **Obfuscation:** The stable cell map of the EPUF and the helper data used for entropy extraction are overwritten with meaningless values.
- **Self-destruction:** A high voltage is applied to physically destroy the relevant DRAM circuitry, preventing information leakage at the source.

 doi:10.20944/preprints202508.0914.v1

5. Formal Verification and Security Analysis

While simulation-based evaluation can demonstrate efficiency in specific scenarios, it cannot formally prove a protocol's security against all possible attacks. Therefore, this section employs formal verification methodologies to guarantee the security of the proposed lightweight authentication protocol.

5.1. Formal Analysis Using Belief Logic

Belief logic, particularly Burrows-Abadi-Needham (BAN) logic, provides a framework for reasoning about the beliefs of principals in authentication protocols [27]. It allows us to formally deduce whether principals achieve mutual trust and believe in the freshness of the messages.

5.1.1. Idealization and Initial Assumptions

We first idealize the protocol messages from Section IV-B and state the initial assumptions:

- **Messages:**
  1. $A \rightarrow B : N_A$
  2. $B \rightarrow A : \{N_A, N_B\}_{SK_{AB}}$
  3. $A \rightarrow B : \{N_B\}_{SK_{AB}}$
- **Assumptions:**
  1. A **believes** $(A \overset{SK_{AB}}{\longleftrightarrow} B)$ and B **believes** $(A \overset{SK_{AB}}{\longleftrightarrow} B)$[1]
  2. A **believes fresh**$(()N_A)$ and B **believes fresh**$(()N_B)$

5.1.2. Logical Deduction and Goal

The goal is to prove that both parties believe they are communicating with each other and that the communication is recent.

1. Upon receiving message 2, A sees its fresh nonce N_A protected by the shared key SK_{AB}. By the *Nonce Verification Rule*, A concludes that B must have sent this message recently. Thus, A **believes** B **said** (N_A, N_B).
2. Upon receiving message 3, B sees its fresh nonce N_B protected by the shared key SK_{AB}. Similarly, by the *Nonce Verification Rule*, B concludes that A is present and sent this message after message 2. Thus, B **believes** A **said** (N_B).

The BAN logic analysis concludes that the protocol successfully establishes mutual belief between the two parties regarding each other's presence and the freshness of the exchange.

5.2. Computational Verification Using ProVerif

In this study, we use the formal verification tool **ProVerif**, which is widely used for analyzing cryptographic protocols. ProVerif transforms a protocol into Horn Clauses and proves security properties such as Secrecy and Authentication under the Dolev-Yao adversary model [26].

5.2.1. Protocol Modeling and Verification Results

The protocol was modeled in Applied Pi Calculus. We verified two core security properties:

1. **Secrecy of Session Key:** The query 'query attacker(sk$_{AB}$).' resulted in 'RESULT attacker(sk$_{AB}$) is false.', proving that the session key is never exposed to an attacker.
2. **Mutual Authentication:** The correspondence assertion 'query event(end$_{auth(B,A)}$) ==> event (begin$_{a}uth(A, B)$).' was proven true, mathematically confirming that impersonation attacks are not possible.

[1] This assumption holds that both principals trust the shared key SK_{AB} and its association with the other principal. In our framework, this initial trust is established during the UAV's bootstrapping phase, where the key derived from its EPUF is registered on the distributed ledger. This analysis, therefore, validates the security of each subsequent authentication session, not the initial key registration.

 doi:10.20944/preprints202508.0914.v1

5.3. Informal Security Analysis

To complement the formal proofs, we provide an informal analysis of the protocol's resilience against common attacks.

5.3.1. Replay Attack Resistance

An adversary might capture a valid authentication session and attempt to replay the messages later. This attack is thwarted by the use of nonces (N_A, N_B). If the adversary replays message 2, the contained nonce N_A will not match the fresh nonce that UAV A expects in a new session. Similarly, replaying message 3 will fail because the nonce N_B will not be the one UAV B just sent. The nonces ensure the timeliness and uniqueness of each protocol run.

5.3.2. Impersonation and MitM Attack

An adversary cannot impersonate a legitimate UAV because they cannot generate a valid Message Authentication Code (MAC). The MAC calculation requires the session key SK_{AB}, which is derived from the EPUF's unique physical properties. Since the adversary does not possess the physical UAV, they cannot generate the correct SK_{AB} and thus cannot create a valid MAC for any given nonce exchange. This prevents them from successfully completing the protocol as an impostor.

5.3.3. Physical Capture and Cloning Resistance

The primary defense against physical attacks is the unclonable nature of the EPUF. Unlike traditional systems where a secret key is stored in non-volatile memory and can be extracted, the EPUF's "key" is a physical property of the DRAM circuit. It is not stored digitally and is generated on-demand, making invasive extraction and cloning prohibitively difficult. Furthermore, the hardware self-destruction mechanism provides a final layer of defense, ensuring that critical security parameters are destroyed upon detecting a physical breach.

5.4. Comparative Security Analysis

To demonstrate the superiority of the proposed protocol's security architecture, we conduct a comparative analysis against six major baseline protocols.

1. **ECC-PKI:** A lightweight public key-based authentication protocol using Elliptic Curve Cryptography, as proposed for IoT environments [23].
2. **Conventional PUF + Static Key:** A scheme using a standard, less reliable DRAM PUF with a fixed-period session key update [24].
3. **Conventional PUF + Dynamic Key:** A scheme using a less reliable PUF but supporting nonce-based dynamic key exchange [24].
4. **Simple CR (Nonce-less):** The most basic form of authentication using only a static challenge and the PUF response, known to be vulnerable to replay attacks [25].
5. **Consensus-based Control (Software-only):** A distributed consensus protocol for controlling UAV formation and connectivity without a hardware security anchor [12,22].
6. **FMADRL-MTD:** A state-of-the-art intelligent defense framework using Federated Multi-Agent DRL for Moving Target Defense against DoS attacks [2].

As shown in Table 2, the proposed framework provides the most balanced design for security and practicality. The Proposed Protocol provides strong authentication and replay resistance, similar to ECC-PKI [23], but with the distinct advantages of very high reliability and physical security from the EPUF. Compared to other intelligent frameworks like FMADRL-MTD [2], our approach achieves efficient adaptability with much lower overhead by focusing lightweight DRL on the fundamental layer of key management.

 doi:10.20944/preprints202508.0914.v1

Table 2. Comparison of Security Properties by Protocol

Security Property	Proposed	ECC-PKI	Conv. PUF + Static	Conv. PUF + Dynamic	Simple CR	Consensus	FMADRL-MTD
Mutual Authentication	Yes	Yes	Yes	Yes	No	No	N/A
Replay Resistance	Yes	Yes	No	Yes	No	N/A	N/A
Impersonation Resistance	Yes	Yes	No	No	Yes	No (Sybil)	N/A
Reliability	**Very High**	High	**Low**	**Low**	**Low**	High (S/W)	High (S/W)
Physical Security	**Very High**	Low	Medium	Medium	Medium	Low	Low
Intelligent Adaptability	**High**	Low	Low	Low	Low	Medium	**Very High**

6. Performance Evaluation

6.1. Experimental Setup and Baselines

Simulations were conducted using the NS-3 network simulator. The UAV swarm consisted of 10 to 50 nodes in a 1km $\times$ 1km area. The communication channel was modeled using parameters from [1], and the UAV energy model was based on [7]. The baselines for comparison are the seven protocols listed and cited in Section V-D. To ensure a fair and direct comparison, all baseline protocols were implemented and evaluated under the identical set of simulation parameters, including network topology, mobility models, and energy consumption models. The performance metrics for competing schemes like ECC-PKI and FMADRL-MTD were reproduced based on the models and parameters described in their respective papers [2,23], adapted to our common simulation environment.

6.2. Results and Comparative Analysis

This section comparatively analyzes the simulation results.

6.2.1. Efficiency and Performance

Figure 3 highlights the efficiency of the proposed protocol. Compared to the computationally intensive ECC-PKI [23], our EPUF-based approach reduces authentication latency and energy consumption by over 95%, which is critical for real-time, battery-powered UAV operations.

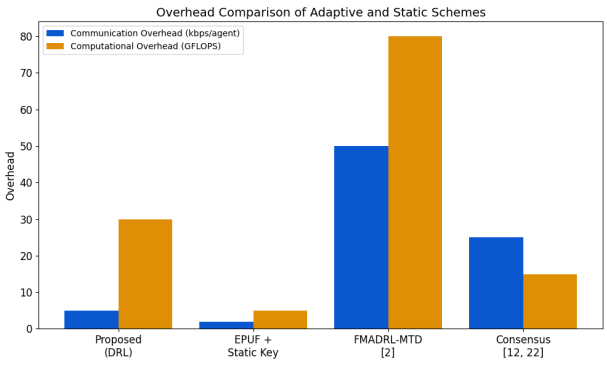

Figure 3. Efficiency comparison of authentication protocols. (a) Authentication Latency. (b) Authentication Energy Consumption.

6.2.2. DRL Agent Training and Convergence

The DQN agent was trained to optimize its key update policy. Key hyperparameters included a learning rate of $\alpha = 0.001$, a discount factor of $\gamma = 0.99$, and an experience replay buffer size of 10,000. Training was conducted over 5,000 episodes, where each episode represents a simulated mission duration. As shown in Figure 4, the agent's cumulative reward converges, indicating that it successfully learned a stable and effective policy for balancing security against energy costs.

 doi:10.20944/preprints202508.0914.v1

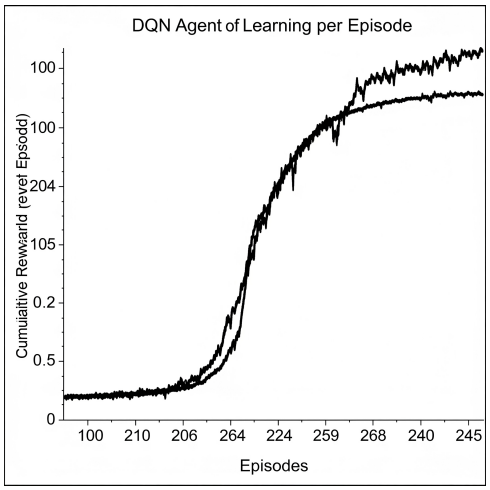

Figure 4. Learning curve of the DQN agent. The cumulative reward per episode stabilizes, demonstrating the convergence of the key update policy.

6.2.3. Security and Adaptability

Figure 5 shows the defense performance against replay attacks. The policies using a Static Key are vulnerable as attackers can predict the update window. In contrast, our Proposed Protocol with a DRL agent maintains a non-periodic and unpredictable key update schedule, effectively suppressing the attack success rate to below 1%.

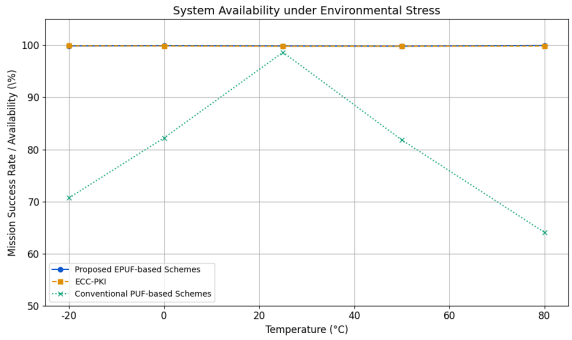

Figure 5. Security performance: Replay Attack Success Rate over Time.

6.2.4. Reliability and System Availability

Figure 6 demonstrates the importance of a reliable hardware anchor. The Conventional PUF-based baselines [24] suffer a drastic drop in system availability as environmental conditions change, leading to authentication failures and mission disruption. In contrast, our Proposed Protocol maintains near-perfect availability, matching the robustness of non-PUF schemes. This proves that an intelligent DRL policy cannot compensate for an unreliable hardware foundation.

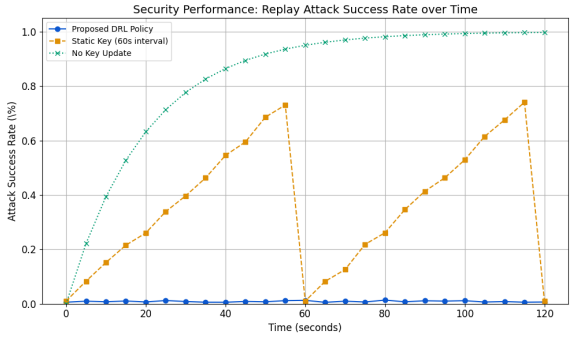

Figure 6. System availability under environmental stress (temperature variation).

 doi:10.20944/preprints202508.0914.v1

6.2.5. Overhead of Intelligence

Figure 7 compares the overhead of different adaptive schemes. The FMADRL-MTD framework [2] incurs high communication and computational overhead due to its federated learning architecture. Our Proposed Protocol, however, achieves intelligent adaptation with significantly lower overhead, as its DRL agent operates in a distributed manner based on local observations. This demonstrates that our framework provides a lightweight yet effective form of intelligent security.

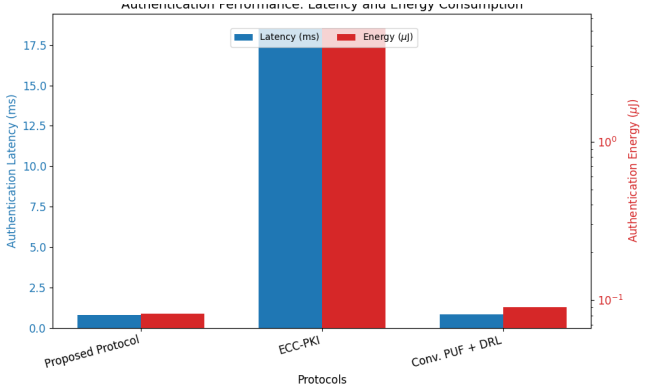

Figure 7. Overhead comparison of adaptive and static schemes.

7. Conclusion and Future Work

This paper introduced a comprehensive, cross-layer security framework for UAV swarms. By synergistically integrating a highly reliable EPUF, a DRL-based adaptive key management policy, and a blockchain-based decentralized trust architecture, our framework provides a robust yet lightweight security solution. The security of the core protocol was rigorously proven through both Belief logic and computational verification. A comprehensive comparative analysis against six distinct baselines demonstrated the proposed framework's superior balance of efficiency, reliability, and adaptive security. Despite the promising results, this work acknowledges that the EPUF's performance is validated through simulation. Future work will focus on hardware prototyping and real-world testbed implementation, as detailed in Appendix A. Furthermore, investigating the framework's scalability to swarms of several hundred UAVs and exploring more sophisticated adversarial models, including DRL-based attackers, remain compelling directions for future research.

Appendix A. Hardware Validation Testbed for EPUF

To bridge the gap between simulation and real-world deployment, this appendix outlines the proposed testbed for the physical validation of the EPUF's reliability. The primary objective is to empirically measure the Bit Error Rate (BER) of the EPUF response under a wide range of environmental conditions and confirm the "zero BER" performance achieved by our data-driven characterization and fuzzy extraction process.

Appendix A.1. Testbed Components

1. **FPGA Platform:** A Xilinx Artix-7 or similar FPGA board will be used. The board's integrated DDR3 memory will serve as the DRAM for the EPUF implementation. The FPGA's logic fabric will host the EPUF controller, the fuzzy extractor, and the communication interface for data logging.
2. **Environmental Chamber:** A programmable temperature and humidity chamber will be used to subject the FPGA board to a controlled range of environmental conditions. We plan to test across a wide temperature spectrum (e.g., -40°C to 85°C) and varying supply voltages (±10% of nominal) to simulate realistic operational stress.
3. **Measurement and Control System:** A host PC running a control script (e.g., in Python) will automate the entire experiment. It will program the environmental chamber, send challenges to

 doi:10.20944/preprints202508.0914.v1

the FPGA, receive the generated PUF responses, and log all relevant data, including timestamp, temperature, voltage, challenge, response, and calculated BER.

Appendix A.2. Experimental Procedure

1. **Enrollment (Stable Cell Identification):** Initially, the "stable cell map" for the specific DRAM chip will be generated by repeatedly reading memory decay patterns at a nominal reference condition (e.g., 25°C, nominal voltage). This enrollment data, along with the fuzzy extractor's helper data, will be stored.
2. **Response Regeneration and Verification:** The FPGA board will be subjected to various points within the temperature and voltage matrix. At each point, the EPUF will be challenged multiple times. The host PC will then compare the regenerated responses against the golden response derived during enrollment.
3. **Data Logging and Analysis:** Any discrepancies (errors) will be logged. The final analysis will involve plotting the BER as a function of temperature and voltage. This empirical data will serve to either validate the 100% reliability claim or quantify the precise error rates, allowing for further refinement of the fuzzy extractor parameters.

This rigorous hardware validation will provide concrete evidence of the EPUF's practicality and robustness, significantly strengthening the claims made in this paper.

References

1. M. Hua, L. Yang, Q. Wu, C. Pan, C. Li, and A. L. Swindlehurst, "UAV-Assisted Intelligent Reflecting Surface Symbiotic Radio System," *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, 2021.
2. Y. Zhou, G. Cheng, K. Du, Z. Chen, T. Qin, and Y. Zhao, "From Static to Adaptive Defense: Federated Multi-Agent Deep Reinforcement Learning-Driven Moving Target Defense Against DoS Attacks in UAV Swarm Networks," *Journal of LaTeX Class Files*, vol. 14, no. 8, 2025.
3. B. Lindqvist, P. Sopasakis, and G. Nikolakopoulos, "A Scalable Distributed Collision Avoidance Scheme for Multi-agent UAV systems."
4. Y. Zhou, Z. Jin, H. Shi, L. Shi, and N. Lu, "Flying IRS: QoE-Driven Trajectory Optimization and Resource Allocation Based on Adaptive Deployment for WPCNs in 6G IoT," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 9031–9046, 2024.
5. Y. Zhou, X. Ma, S. Hu, D. Zhou, N. Cheng, and N. Lu, "QoE-Driven Adaptive Deployment Strategy of Multi-UAV Networks Based on Hybrid Deep Reinforcement Learning," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5868–5881, 2022.
6. S. Essaky, G. Raja, K. Dev, and D. Niyato, "ARReSVG: Intelligent Multi-UAV Navigation in Partially Observable Spaces Using Adaptive Deep Reinforcement Learning Approach," *IEEE Transactions on Vehicular Technology*, 2025.
7. L. Dong, Z. Liu, F. Jiang, and K. Wang, "Joint Optimization of Deployment and Trajectory in UAV and IRS-Assisted IoT Data Collection System," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21583–21593, 2022.
8. Q. An, Q. Hu, R. Tang, and L. Rao, "Intelligent Scheduling Methodology for UAV Swarm Remote Sensing in Distributed Photovoltaic Array Maintenance," *Sensors*, vol. 22, no. 12, p. 4467, 2022.
9. S. S. Alotaibi et al., "Swarm Intelligence with Deep Transfer Learning Driven Aerial Image Classification Model on UAV Networks," *Applied Sciences*, vol. 12, no. 13, p. 6488, 2022.
10. K. Pan, M. Li, S. Lv, P. Si, H. Zhang, and F. R. Yu, "Adaptive Resource Allocation for IoT with Computing Power Network Based on RIS-UAV-Aided NOMA-THz Communication," *IEEE Transactions on Vehicular Technology*, 2025.
11. Z. Min, X. Zhang, X. Zhang, T. Lei, and Q. Gao, "A Data-Driven MPC Energy Optimization Management Strategy for Fuel Cell Distributed Electric Propulsion UAV," in *Proc. 2022 4th Asia Energy and Electrical Engineering Symposium (AEEES)*, 2022.
12. R. Rahmani, R. Firouzi, and T. Kanter, "Distributed Adaptive Formation Control for Multi-UAV to Enable Connectivity," *IJCSI International Journal of Computer Science Issues*, vol. 17, no. 2, 2020.
13. J. Bai, G. Huang, S. Zhang, Z. Zeng, and A. Liu, "GA-DCTSP: An Intelligent Active Data Processing Scheme for UAV-Enabled Edge Computing," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 4891–4906, 2023.

 doi:10.20944/preprints202508.0914.v1

14. Y. Yu, H. Wang, S. Liu, L. Guo, P. L. Yeoh, B. Vucetic, and Y. Li, "Distributed Multi-Agent Target Tracking: A Nash-Combined Adaptive Differential Evolution Method for UAV Systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8122–8133, 2021.
15. Y. Zhou, Z. Jin, H. Shi, L. Shi, and N. Lu, "Flying IRS: QoE-Driven Trajectory Optimization and Resource Allocation Based on Adaptive Deployment for WPCNs in 6G IoT," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 9031–9046, 2024.
16. J. Tan, H. Jin, H. Zhang, et al., "A survey: When moving target defense meets game theory," *Computer Science Review*, vol. 48, p. 100544, 2023.
17. Z. Wang, Y. Li, S. Wu, et al., "A survey on cybersecurity attacks and defenses for unmanned aerial systems," *Journal of Systems Architecture*, vol. 138, p. 102870, 2023.
18. M. Mozaffari, W. Saad, M. Bennis, et al., "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.
19. V. Mnih et al., "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015.
20. Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.
21. D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.
22. R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.
23. S. A. Chaudhry, M. H. Al-shehri, K. A. Al-Sodairi, and M. L. Das, "A lightweight and provably secure anonymous authentication and key agreement scheme for IoT-based cloud environment," *IEEE Access*, vol. 9, pp. 71110–71123, 2021.
24. Y. Bi, X. Wang, C. Zhao, Z. Jin, and H. Li, "DRAM-based intrinsic physically unclonable functions for system-level security and authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 10, pp. 3144–3156, 2016.
25. A. G. Ardeshir-Larijani, C. P. T. McGoldrick, and E. Martin, "PUF-based authentication protocols for resource-constrained devices," in *Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2018.
26. B. Blanchet, "Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif," *Foundations and Trends® in Privacy and Security*, vol. 1, no. 1–2, pp. 1–135, 2016.
27. Burrows, Michael and Abadi, Martín and Needham, Roger M, "A logic of authentication," *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18-36, 1990.

Short Biography of Authors

Hyunseok Kim Hyunseok Kimreceived the B.S. degree in the Department of Business Management from Korea Military Academy, Seoul, Korea in 2000, M.S. and Ph.D in the Department of Computer Science and Engineering from Korea University, Seoul, Korea in 2006 and 2009, respectively. He is currently an associate professor at the ICT Polytech Institute of Korea. His research interests include the areas of Formal Methods(Formal Specification, Formal Verification, Model Checking), IoD Authentication Design, Smart Card Privacy, M-Commerce Secure Transaction.