Publisher
Vandana Publications
www.vandanapublications.com

International Journal of Engineering and Management Research

2026 Volume 16 Number 3 June

E-ISSN:2250-0758
P-ISSN:2394-6962

Research Article

UAV Security

LightSecurePUF: A Lightweight PUF-Based Mutual Authentication and Session Key Establishment Protocol for Secure UAV-Ground Station Communications

Singh A[1*]

DOI:10.31033/IJEMR/16.3.2026.1930

[1*] Anjali Singh, Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka, New Delhi, India.

The rapid deployment of Unmanned Aerial Vehicles (UAVs) in military, surveillance, disaster management, precision agriculture, and intelligent transportation systems has significantly increased the demand for secure and lightweight authentication mechanisms. Due to the limited computational capability and energy constraints of UAV platforms, conventional public-key cryptographic protocols often impose excessive computational and communication overhead. Furthermore, wireless UAV-Ground Station (GS) communication is vulnerable to replay, impersonation, man-in-the-middle, and session hijacking attacks. To address these challenges, this paper proposes LightSecurePUF, a lightweight mutual authentication and session key establishment protocol based on Physically Unclonable Functions (PUFs), cryptographic hash functions, and Hash-based Message Authentication Codes (HMACs). The proposed protocol employs a challenge-response PUF mechanism to uniquely authenticate UAV devices while deriving a fresh session key from the long-term shared secret, PUF response, random nonces, and session identifier. Consequently, each communication session establishes an independent session key without increasing computational complexity. The security of the proposed protocol is formally verified using the Scyther protocol verification tool under the Dolev-Yao adversarial model. The verification results demonstrate that the protocol satisfies secrecy, mutual authentication, non-injective agreement, synchronization, and key confirmation properties, with no attacks detected within the verification bounds. Furthermore, the protocol achieves lower computational and communication overhead than existing authentication schemes, making it suitable for resource-constrained UAV-assisted Internet of Things (IoT) and cyber-physical systems.

Keywords: UAV Security, Physically Unclonable Function, Session Key Establishment, Lightweight Cryptography, HMAC, Scyther Verification, Internet of Things

Corresponding Author

Anjali Singh, Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka, New Delhi, India.
Email: sianjali18@gmail.com

How to Cite this Article

Singh A, LightSecurePUF: A Lightweight PUF-Based Mutual Authentication and Session Key Establishment Protocol for Secure UAV-Ground Station Communications. Int J Engg Mgmt Res. 2026;16(3):101-112.
Available From
https://ijemr.vandanapublications.com/index.php/j/article/view/1930

To Browse

Manuscript Received	Review Round 1	Review Round 2	Review Round 3	Accepted
2026-05-09	2026-05-24			2026-06-11

Conflict of Interest	Funding	Ethical Approval	Plagiarism X-checker	Note
None	Nil	Yes	4.82	

1. Introduction

1.1 Background

Unmanned Aerial Vehicles (UAVs) have emerged as an essential component of modern intelligent systems due to their flexibility, mobility, and cost-effectiveness. UAVs are extensively deployed in applications including environmental monitoring, military reconnaissance, border surveillance, disaster response, precision agriculture, smart cities, package delivery, and Internet of Things (IoT) networks **[1,2]**. In most of these applications, UAVs continuously exchange sensitive information with Ground Stations (GSs) through wireless communication channels, making communication security a critical requirement **[1,3]**.

Despite their increasing adoption, UAV platforms typically possess limited computational resources, memory capacity, and battery power. These resource constraints make the implementation of computationally intensive public-key cryptographic mechanisms challenging, particularly in real-time applications requiring low latency and high energy efficiency. Consequently, lightweight authentication protocols have become an active research area for securing UAV communications while maintaining acceptable computational and communication costs **[1,4,5]**.

1.2 Motivation

Wireless communication between UAVs and Ground Stations is inherently exposed to various security threats because transmissions occur over open and potentially hostile communication channels. An adversary operating under the Dolev-Yao threat model may intercept, modify, replay, or fabricate protocol messages, enabling attacks such as replay attacks, impersonation attacks, man-in-the-middle attacks, session hijacking, and unauthorized device access **[1,2,4]**. Existing lightweight authentication schemes often rely solely on pre-shared symmetric keys or static credentials, which may become vulnerable if long-term secrets are compromised **[4,6,7]**.

Physically Unclonable Functions (PUFs) have recently emerged as a promising hardware-based security primitive capable of generating unique and unclonable device identities without permanently storing secret keys in non-volatile memory. Since the response generated by a PUF depends on intrinsic manufacturing variations, duplicating the same hardware behavior becomes computationally infeasible. Integrating PUF technology into lightweight authentication protocols therefore enhances device authentication while preserving computational efficiency **[8,9]**.

1.3 Problem Statement

Although numerous authentication protocols have been proposed for UAV-assisted networks, several limitations remain. Many existing schemes require expensive elliptic curve cryptography or bilinear pairing operations that are unsuitable for lightweight UAV platforms **[2,7]**. Other protocols employ static authentication credentials that are susceptible to replay and impersonation attacks. Furthermore, several PUF-based schemes utilize the PUF only for device identification rather than incorporating it into the session key establishment process, thereby limiting the contribution of the PUF to overall communication security **[6,10].**

1.4 Contributions

This paper proposes LightSecurePUF, a lightweight mutual authentication protocol specifically designed for secure UAV-Ground Station communications. The main contributions of this work are summarized as follows:

1. A lightweight three-message mutual authentication protocol is proposed for secure communication between UAVs and Ground Stations.
2. A challenge-response PUF mechanism is integrated into the authentication phase to provide hardware-based device authentication.
3. A fresh session key is derived from the long-term shared secret, challenge-dependent PUF response, random nonces, and session identifier, ensuring unique session keys for every communication session.
4. The protocol employs only lightweight cryptographic primitives, including hash functions, HMAC operations, and PUF evaluations, making it suitable for resource-constrained UAV platforms.
5. The proposed protocol is formally verified using the Scyther protocol verification tool under the Dolev-Yao adversarial model. Verification results confirm secrecy, mutual authentication, synchronization, agreement, and resistance against replay, impersonation, and man-in-the-middle attacks within the symbolic model.

6. Performance analysis demonstrates that the proposed protocol achieves lower computational and communication overhead compared with existing authentication protocols while maintaining a high level of security.

1.5 Organization of the Paper

The remainder of this paper is organized as follows. Section 2 reviews related work on UAV authentication and PUF-based security mechanisms. Section 3 presents the system model, threat model, and design assumptions. Section 4 describes the proposed LightSecurePUF authentication protocol in detail. Section 5 provides the formal and informal security analysis, including Scyther-based verification. Section 6 evaluates the computational and communication performance of the proposed protocol and compares it with existing approaches. Finally, Section 7 concludes the paper and discusses future research directions.

2. Related Work

Secure authentication and key establishment have become fundamental requirements for Unmanned Aerial Vehicle (UAV) networks because wireless communication between UAVs and Ground Stations (GSs) is vulnerable to replay, impersonation, man-in-the-middle (MITM), and device capture attacks. At the same time, UAVs are constrained by limited computational capability, battery capacity, and storage resources. Consequently, recent research has focused on lightweight authentication protocols that provide strong security while minimizing computational and communication overhead **[1,2]**.

Early lightweight authentication protocols for UAV networks primarily relied on symmetric cryptographic primitives such as hash functions, XOR operations, and message authentication codes (MACs). These schemes significantly reduced computational complexity compared with public-key cryptography; however, many depended on static credentials or long-term shared secrets. As a result, compromise of stored credentials could enable replay attacks, impersonation attacks, or session key disclosure. Moreover, several early protocols lacked formal verification or were subsequently shown to contain security weaknesses **[1,2,4]**.

To improve security, researchers introduced Physically Unclonable Functions (PUFs) as hardware roots of trust for UAV authentication. Because PUF responses originate uncontrollable manufacturing variations, they provide device-unique identities that are extremely difficult to duplicate or predict. Alkatheiri *et al.* proposed a lightweight PUF-based authentication scheme for UAV networks using hardware-assisted security primitives **[5]**. Subsequently, Zhang *et al.* developed a lightweight PUF-based authentication and key agreement protocol for smart UAV networks that combines PUF technology with lightweight cryptographic operations to resist physical capture attacks while maintaining low computational overhead **[6]**.

Subsequent research extended PUF-based authentication to Internet of Drones (IoD) and UAV-assisted Internet of Vehicles (IoV) environments. PRLAP-IoD introduced a robust and lightweight authentication protocol that combines PUFs with efficient authentication techniques for Internet of Drones applications **[3]**. Similarly, Choi *et al.* proposed a lightweight authentication protocol for UAV-assisted IoV environments and demonstrated improved resistance against man-in-the-middle and ephemeral secret leakage attacks while avoiding computationally expensive elliptic curve operations. Their protocol was formally analyzed using BAN logic, the Real-or-Random (RoR) model, and AVISPA **[7]**.

Anonymous authentication has also received considerable attention in recent years. Xie and Wang proposed a PUF-based anonymous authentication protocol for cross-domain UAV environments that preserves UAV identity privacy while supporting authenticated key establishment across multiple administrative domains **[8]**. Furthermore, blockchain-assisted authentication has recently emerged as a promising research direction. Yu *et al.* introduced RLBA-UAV, which integrates blockchain technology with PUF-enabled authentication to enhance trust management and secure key agreement in UAV networks **[9]**.

Another active research direction focuses on reducing the overall computational and communication cost of authentication protocols. Recent lightweight PUF-enabled authentication schemes avoid computationally expensive operations such as elliptic curve scalar multiplication, bilinear pairings, and modular exponentiation, replacing them with hash functions, XOR operations, and PUF evaluations **[2],[3],[5], [6]**.

For example, Kumar *et al.* proposed LiteWTAKA, a lightweight authentication and key agreement,

mechanism for both UAV-to-Ground Station and UAV-to-UAV communications using PUF technology together with lightweight hash operations. The protocol was formally analyzed using Scyther, BAN logic, and the RoR model while demonstrating improved computational efficiency **[10]**.

Although recent studies have significantly advanced lightweight UAV authentication, several challenges remain. First, many protocols employ the PUF only as a device authentication primitive, whereas the session key is derived primarily from long-term shared secrets and random nonces **[5], [6], [10]**. Consequently, the PUF contributes little to the actual key establishment process. Second, some schemes introduce additional mechanisms such as fuzzy extractors, blockchain, biometric authentication, chaotic maps, or multi-factor authentication to strengthen security; however, these techniques increase implementation complexity, storage requirements, or computational overhead, making them less attractive for highly resource-constrained UAV platforms **[3], [7], [8], [9]**.

Furthermore, although several protocols provide comprehensive formal security analysis using BAN logic, AVISPA, the Real-or-Random (RoR) model, or blockchain-based trust analysis, comparatively fewer lightweight UAV authentication schemes have been modeled using Scyther with explicit verification of secrecy, authentication, synchronization, and agreement properties in a concise three-message protocol **[4], [10]**. Formal symbolic verification remains valuable because it enables automated analysis against an active Dolev-Yao adversary model, in which an attacker can intercept, modify, replay, and fabricate protocol messages without breaking the underlying cryptographic primitives **[11]**.

Table 1: Summary of Related Work

Reference	Main Technique	Formal Verification	Limitation
Zhang et al. (2022)	PUF + Hash/XOR	Informal analysis	PUF mainly used for authentication
CoMSeC++ (2021)	PUF + Lightweight Mutual Authentication	Scyther	Drone-enabled WSN focus rather than UAV-GS authentication
Choi et al. (2025)	PUF + Fuzzy Extractor + Hash	AVISPA, BAN, RoR	IoV-oriented architecture
LiteWTAKA (2026)	PUF + Hash + XOR	Scyther, BAN, RoR	Includes session update but targets both UAV-UAV and UAV-GS communication

3. System Model, Threat Model, and Design Goals

3.1 System Model

The proposed LightSecurePUF protocol considers a UAV communication architecture consisting of three primary entities: the Unmanned Aerial Vehicle (UAV), the Ground Station (GS), and a trusted registration authority (RA) responsible for the initial enrollment of legitimate UAVs. Figure 1 illustrates the overall system architecture.

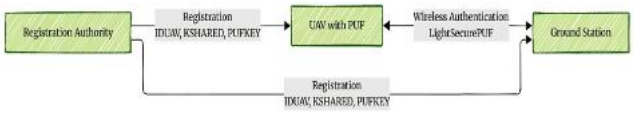

Figure 1: System Architecture

During the registration phase, the RA securely registers each UAV by assigning a unique identity $1D_{UAV}$, provisioning a long-term shared secret key K_{SHARED}, and enrolling the device-specific Physically Unclonable Function (PUF). The enrollment process stores the required challenge-response information for subsequent authentication while ensuring that the intrinsic hardware characteristics of the UAV remain unique and unclonable.

During normal operation, the UAV communicates directly with the Ground Station through an open wireless communication channel. Since wireless transmissions are susceptible to eavesdropping and active manipulation, the proposed protocol performs mutual authentication before establishing a secure communication session. Upon successful authentication, both entities independently derive an identical session key using the long-term shared secret, the challenge-dependent PUF response, fresh random nonces, and a session identifier.

The protocol employs only lightweight cryptographic primitives, namely hash functions, HMAC operations, and PUF evaluations, making it suitable for UAV platforms with limited computational capability and energy resources.

The assumptions of the proposed system are summarized as follows:

1. The Registration Authority is fully trusted and performs secure offline enrollment.
2. Each UAV possesses a unique hardware PUF that cannot be physically cloned.
3. The Ground Station securely stores the registered credentials associated with each legitimate UAV.
4. The long-term shared secret remains confidential after the registration phase.
5. Hash functions and HMAC are assumed to be cryptographically secure.
6. The communication channel between the UAV and GS is insecure and completely controlled by an adversary.

3.2 Threat Model

The security analysis of the proposed protocol follows the widely adopted Dolev-Yao **[11]** adversary model, which assumes that an attacker has complete control over the public communication channel.

Specifically, the adversary is capable of:

a) intercepting transmitted messages
b) modifying protocol messages
c) replaying previously captured messages
d) fabricating new protocol messages
e) deleting or delaying transmitted packets
f) initiating concurrent protocol sessions
g) impersonating legitimate communication entities whenever protocol weaknesses permit.

However, the adversary is not capable of:

a) breaking secure cryptographic hash functions
b) forging valid HMAC values without knowledge of the corresponding secret key
c) predicting fresh random nonces generated during protocol execution
d) cloning the intrinsic physical characteristics of a legitimate PUF
e) deriving the challenge-response behavior of the enrolled PUF within practical computational limits.

In addition, it is assumed that the Registration Authority and the Ground Station remain uncompromised throughout protocol execution. Although an attacker may physically capture a UAV, extracting the exact hardware characteristics of its PUF is considered computationally infeasible because the response is determined by uncontrollable manufacturing variations.

Under these assumptions, the proposed protocol aims to maintain secure mutual authentication and session key establishment despite the presence of an active network adversary.

3.3 Design Goals

The proposed LightSecurePUF protocol is designed to satisfy the following security and performance objectives.

G1. Mutual Authentication

The UAV and Ground Station must authenticate each other before exchanging sensitive information. Successful authentication ensures that both communicating entities are legitimate participants in the protocol.

G2. Replay Attack Resistance

Previously transmitted authentication messages should not enable an attacker to establish a valid communication session. The incorporation of fresh random nonces and a session identifier guarantees message freshness for every protocol execution.

G3. Man-in-the-Middle Attack Resistance

An adversary intercepting communication between the UAV and GS should be unable to modify authentication messages or establish independent secure sessions with either entity. The HMAC-based authentication mechanism prevents unauthorized message manipulation.

G4. UAV Impersonation Resistance

An attacker should not be able to impersonate a legitimate UAV without possessing both the long-term shared secret and the corresponding PUF response associated with the enrolled hardware.

G5. Ground Station Impersonation Resistance

Similarly, unauthorized entities should be unable to masquerade as the legitimate Ground Station because generation of valid authentication messages requires knowledge of the shared secret and the derived session key.

G6. Session Key Freshness

Every successful authentication session should establish a unique session key. In the proposed protocol, the session key is derived as

$$SK = h(K_{SHARED} \parallel PUF(PUFKEY, R_1) \parallel R_1 \parallel R_2 \parallel SID)$$

where R_1, R_2, and SID are freshly generated during each protocol execution. Consequently, every authentication session produces an independent session key.

G7. Secrecy of Long-Term Credentials

The long-term shared secret *K* and the enrolled PUF key must remain confidential throughout protocol execution, even in the presence of an active adversary controlling the communication channel.

G8. Lightweight Computation

The protocol should avoid computationally expensive public-key operations such as modular exponentiation, elliptic curve scalar multiplication, and bilinear pairings. Instead, authentication is achieved using only lightweight hash computations, HMAC operations, and PUF evaluations, thereby minimizing computational overhead for resource-constrained UAV platforms.

G9. Formal Verifiability

The protocol should be amenable to formal verification under the symbolic Dolev-Yao model. Accordingly, the proposed protocol is modeled in the Security Protocol Description Language (SPDL) and formally verified using the Scyther protocol verification tool, demonstrating secrecy, mutual authentication, agreement, synchronization, and key confirmation properties.

4. Proposed LightSecurePUF Authentication Protocol

4.1 Overview

This section presents LightSecurePUF, a lightweight mutual authentication and session key establishment protocol designed for secure communication between a UAV and a Ground Station (GS). The protocol integrates a challenge-response Physically Unclonable Function (PUF) with lightweight cryptographic primitives, including cryptographic hash functions and HMAC, to achieve secure authentication while maintaining low computational overhead.

Unlike many existing PUF-based authentication protocols, the proposed scheme incorporates the challenge-dependent PUF response directly into the session key derivation process. Consequently, the PUF contributes not only to device authentication but also to establishing a fresh session key for every communication session.

The protocol consists of two phases:

1. Registration Phase

2. Mutual Authentication and Session Key Establishment Phase

4.2 Notation

The notations used in this work are shown in Table 2.

Table 2: Notation used in the proposed protocol

Symbol	Description
UAV	Unmanned Aerial Vehicle
GS	Ground Station
RA	Registration Authority
ID_{UAV}	UAV identity
ID_{GS}	Ground Station identity
K_{SHARED}	Long-term shared secret key
$PUFKEY$	Device-specific PUF enrollment key
$PUF(\cdot)$	Physically Unclonable Function
R_1	UAV-generated random nonce
R_2	GS-generated random nonce
SID	Session identifier
$h(\cdot)$	One-way cryptographic hash function
$HMAC(\cdot)$	Hash-based Message Authentication Code
SK	Session key

4.3 Registration Phase

The registration phase is executed only once before the UAV joins the network. It is assumed that the Registration Authority (RA) communicates securely with both the UAV and the Ground Station.

During registration, the following steps are performed:

Step 1. UAV Enrollment

The Registration Authority assigns a unique identity $1D_{UAV}$ to each UAV.

Step 2. Secret Initialization

A long-term secret key

K_{SHARED}

is securely stored in both the UAV and the corresponding Ground Station.

Step 3. PUF Enrollment

The intrinsic hardware PUF of the UAV is enrolled.

The Registration Authority stores the required challenge-response information associated with the UAV while securely provisioning the PUF enrollment parameter *PUFKEY*.

Step 4. Completion

After registration, both the UAV and GS possess

- $1D_{UAV}$
- K_{SHARED}
- *PUFKEY*

The Registration Authority is not involved during subsequent authentication sessions.

4.4 Mutual Authentication Phase

The authentication protocol consists of three lightweight message exchanges.

Message 1:

UAV → GS

$$(ID_{UAV}, R_1, SID, PUF(PUFKEY, R_1))$$

where

- R_1 is a fresh random nonce,
- SID is a fresh session identifier,
- $PUF(PUFKEY, R_1)$ is the challenge-response generated using the UAV's hardware PUF.

Upon receiving Message 1, the Ground Station verifies the received PUF response against the enrolled PUF information.

Message 2:

After successful PUF verification, the Ground Station generates a fresh nonce R_2 and computes the session key as

$$SK = h(K_{SHARED} \parallel PUF(PUFKEY, R_1) \parallel R_1 \parallel R_2 \parallel SID)$$

The Ground Station computes

$$MAC_2 = HMAC(SK, ID_{UAV}, R_1, ID_{GS}, R_2, SID)$$

and transmits

$$(ID_{GS}, R_2, MAC_2)$$

to the UAV.

Message 3:

The UAV independently derives the same session key

$$SK = h(K_{SHARED} \parallel PUF(PUFKEY, R_1) \parallel R_1 \parallel R_2 \parallel SID)$$

The UAV verifies the received authentication code.

If verification succeeds,

$$MAC_3 = HMAC(SK, ID_{GS}, R_2, ID_{UAV}, R_1, SID)$$

is generated and transmitted to the Ground Station.

Authentication Completion:

The Ground Station verifies

MAC_3

If the verification succeeds,

- mutual authentication is completed;
- both parties share an identical session key;
- secure communication begins.

4.5 Session Key Establishment

Unlike conventional lightweight authentication protocols that derive the session key solely from long-term credentials and random numbers, the proposed protocol additionally incorporates the challenge-dependent PUF response.

The session key is computed as

$$\boxed{SK = h(K_{SHARED} \parallel PUF(PUFKEY, R_1) \parallel R_1 \parallel R_2 \parallel SID)}$$

This construction provides several security advantages:

- incorporation of a device-specific hardware secret;
- fresh session keys for every protocol execution;
- resistance to replay attacks;
- resistance to impersonation attacks;
- lightweight computation suitable for UAV platforms.

4.6 Protocol Algorithm

Algorithm.1: LightSecurePUF Authentication Procedure

Step-1. UAV generates R_1 and SID.
Step-2. UAV computes $PUF(PUFKEY, R_1)$.
Step-3. UAV sends Message 1.
Step-4. GS verifies the received PUF response.
Step-5. GS generates R_2.
Step-6. GS derives the session key SK.
Step-7. GS computes MAC_2 and sends Message 2.
Step-8. UAV derives the same session key.
Step-9. UAV verifies MAC_2.
Step-10. UAV computes MAC_3 and sends Message 3.
Step-11. GS verifies MAC_3.
Step-12. Secure communication is established.

4.7 Message Flow

Figure 2 shows the message transactions between UAV and GS.

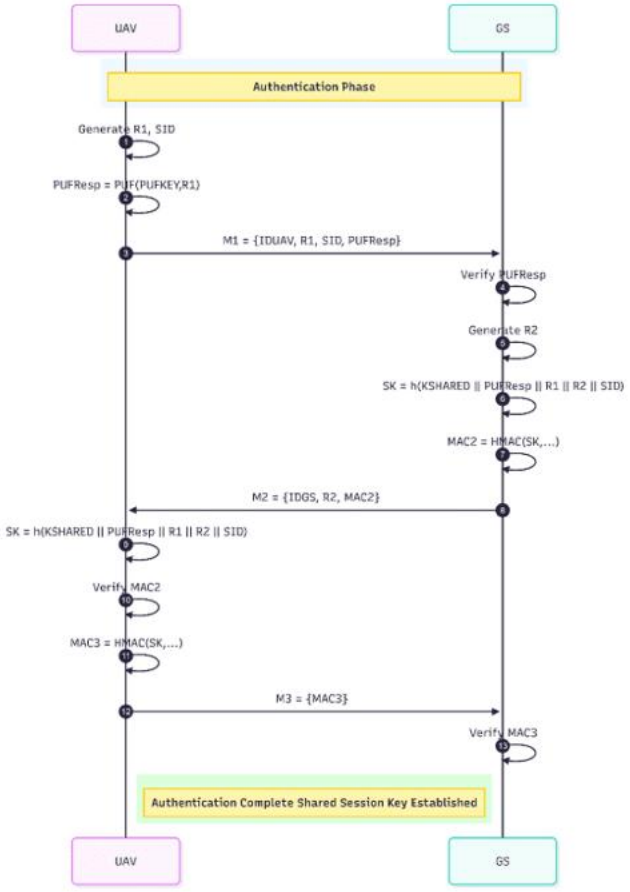

Figure 2: Proposed LightSecurePUF Authentication Protocol

5. Security Analysis

This section evaluates the security of the proposed LightSecurePUF protocol through both informal analysis and formal verification. The informal analysis demonstrates the protocol's resistance to common attacks under the assumed threat model, while the formal analysis uses the Scyther verification tool under the Dolev-Yao adversarial model to verify authentication and secrecy properties.

5.1 Informal Security Analysis

The proposed protocol employs fresh random nonces, a challenge-response Physically Unclonable Function (PUF), cryptographic hash functions, and Hash-based Message Authentication Codes (HMACs) to establish mutual authentication and derive a fresh session key. The session key is computed as

$$SK = h(K_{SHARED} \parallel PUF(PUFKEY, R_1) \parallel R_1 \parallel R_2 \parallel SID),$$

which binds the session to both communicating entities and incorporates both long-term and session-specific secrets.

A. Mutual Authentication

The protocol achieves mutual authentication through a three-message challenge-response mechanism.

The Ground Station authenticates the UAV by verifying the received PUF response

$$PUF(PUFKEY, R_1),$$

which is generated from the UAV's unique hardware PUF using the fresh challenge R_1. Since the PUF response cannot be reproduced without the enrolled hardware, an adversary cannot successfully impersonate a legitimate UAV.

Conversely, the UAV authenticates the Ground Station by verifying the HMAC received in Message 2. Generation of a valid HMAC requires knowledge of both the long-term shared secret and the challenge-dependent PUF response incorporated into the derived session key. Therefore, only a legitimate Ground Station can generate a valid authentication message.

After successful verification of Message 3, both entities obtain explicit confirmation that mutual authentication has been completed.

B. Replay Attack Resistance

Replay attacks are prevented through the use of fresh random nonces and together with the session identifier . Every protocol execution generates new authentication parameters and a new session key. Consequently, replaying previously captured protocol messages produces authentication values that are inconsistent with the current session and are therefore rejected during HMAC verification.

C. Man-in-the-Middle Attack Resistance

Under the Dolev-Yao threat model, an adversary may intercept, modify, delay, or fabricate protocol messages. However, successful modification of Messages 2 or 3 requires the attacker to generate valid HMAC values computed using the derived session key. Since the session key depends on the confidential long-term shared secret and the challenge-dependent PUF response, the adversary cannot construct valid authentication messages. Therefore, the protocol resists man-in-the-middle attacks.

D. UAV Impersonation Attack Resistance

To impersonate a legitimate UAV, an attacker must generate a valid PUF response corresponding to the challenge . Because the PUF is derived from uncontrollable manufacturing variations and is assumed to be unclonable, reproducing the correct response without the legitimate hardware is computationally infeasible. Consequently, UAV impersonation attacks are prevented under the assumed threat model.

E. Ground Station Impersonation Attack Resistance

An attacker attempting to impersonate the Ground Station must generate a valid HMAC in Message 2. This requires knowledge of the derived session key, which depends on the long-term shared secret, the challenge-dependent PUF response, fresh nonces, and the session identifier. Without access to these confidential values, the attacker cannot generate a valid authentication message.

F. Session Key Freshness

The proposed protocol derives a unique session key for every successful authentication session. Since the session key incorporates the fresh nonces R_1 and R_2 together with the session identifier SID, identical session keys cannot be generated across different protocol executions. This property ensures session independence and prevents reuse of authentication material.

G. Key Confidentiality

The long-term shared secret K_{SHARED} is never transmitted over the public communication channel. Likewise, the session key is derived locally by both communicating entities and is never exchanged explicitly. Under the assumed security of the hash function and HMAC construction, an adversary observing protocol messages cannot recover either the long-term secret or the derived session key.

H. Device Authentication Using PUF

Unlike conventional lightweight authentication protocols that rely solely on stored cryptographic secrets, the proposed protocol integrates a challenge-dependent PUF response into both the authentication procedure and the session key derivation process. Consequently, successful authentication depends on the physical characteristics of the enrolled UAV hardware in addition to cryptographic credentials, providing an additional layer of protection against device cloning and hardware impersonation.

5.2 Formal Security Verification Using Scyther

To complement the informal analysis, the proposed protocol was formally verified using the **Scyther** protocol verification tool. Scyther performs symbolic protocol analysis under the Dolev-Yao adversarial model, where an attacker has complete control over the communication channel but cannot break the underlying cryptographic primitives.

The protocol was modeled using the Security Protocol Description Language (SPDL). The Scyther model includes the UAV and Ground Station roles together with authentication, agreement, synchronization, and secrecy claims as shown in Figure.3.

The following security properties were verified:

- Alive
- Weak Agreement
- Commit Authentication
- Non-injective Agreement (Niagree)
- Non-injective Synchronization (Nisynch)
- Secrecy of the long-term shared secret
- Secrecy of the PUF enrollment key
- Secrecy of the fresh nonces

Scyther reported **"No attacks within bounds"** for all specified claims, indicating that no attack violating the modeled security properties was discovered within the explored state space.

Table 3: Scyther Verification Results

Security Claim	UAV	GS	Verification Result
Alive	✓	✓	Pass
Weak Agreement	✓	✓	Pass
Commit	✓	✓	Pass
Non-injective Agreement (Niagree)	✓	✓	Pass
Non-injective Synchronization (Nisynch)	✓	✓	Pass
Secret (,)	✓	✓	Pass
Secret ()	✓	✓	Pass
Secret ()	✓	✓	Pass

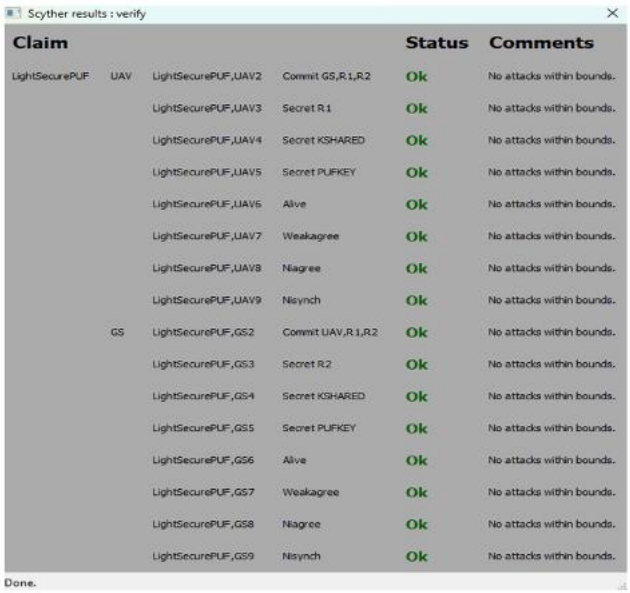

Figure 3: Scyther Output

The successful verification of these claims provides symbolic evidence that the proposed protocol satisfies the modeled secrecy and authentication properties under the Dolev-Yao adversary assumptions.

5.3 Discussion

The security analysis demonstrates that the proposed LightSecurePUF protocol provides lightweight mutual authentication while maintaining resistance against replay, impersonation, and man-in-the-middle attacks. By integrating the challenge-dependent PUF response into both authentication and session key derivation, the protocol strengthens device authentication without introducing computationally expensive public-key operations. Furthermore, formal verification using Scyther confirms that the protocol satisfies the specified secrecy, agreement, and synchronization properties, supporting its suitability for resource-constrained UAV-Ground Station communication environments.

6. Performance Evaluation

This section evaluates the efficiency of the proposed LightSecurePUF protocol in terms of computational cost, communication cost, and comparison with recent lightweight UAV authentication schemes.

Since UAVs operate under strict energy and processing constraints, reducing authentication overhead is essential for extending operational lifetime and supporting real-time communication.

6.1 Computational Cost Analysis

The computational complexity of an authentication protocol depends primarily on the cryptographic operations executed during one authentication session. The proposed protocol employs only lightweight operations, namely one-way hash functions, Hash-based Message Authentication Codes (HMACs), and Physically Unclonable Function (PUF) evaluations. It avoids computationally intensive public-key cryptographic operations such as elliptic curve scalar multiplication, modular exponentiation, and bilinear pairings.

Computational Cost of the Proposed Protocol

During one authentication session, the UAV performs:

- One PUF evaluation
- Two hash operations (one for session-key derivation and one within HMAC)
- Two HMAC computations

Similarly, the Ground Station performs:

- One PUF verification
- Two hash operations
- Two HMAC computations

Accordingly, the total computational complexity of the proposed protocol can be expressed as

$$C_{total} = 2T_{PUF} + 4T_H + 4T_{HMAC},$$

where

- T_{PUF} denotes the execution time of one PUF evaluation,
- T_H denotes the execution time of one hash computation, and
- T_{HMAC} denotes the execution time of one HMAC operation.

Because all employed cryptographic primitives are lightweight, the proposed protocol is suitable for resource-constrained UAV platforms.

6.2 Communication Cost Analysis

The proposed protocol consists of three authentication messages exchanged between the UAV and the Ground Station.

Message 1:

$$(ID_{UAV}, R_1, SID, PUF(R_1))$$

Message 2:

$$(ID_{GS}, R_2, MAC_2)$$

Message 3:

$$MAC_3$$

Assuming typical field sizes shown in Table 4, the total communication overhead can be estimated.

Table 4: Message Size Assumptions

Parameter	Size (bits)
UAV Identity	128
GS Identity	128
Nonce	128
Session Identifier	128
PUF Response	128
HMAC	256

Using these values,

Message 1:

$$128 + 128 + 128 + 128 = 512 \text{ bits}$$

Message 2:

$$128 + 128 + 256 = 512 \text{ bits}$$

Message 3:

$$256 \text{ bits}$$

Therefore,

$$\boxed{\text{Total Communication Cost} = 1280 \text{ bits}}$$

The communication complexity is independent of expensive public-key parameters, resulting in a compact authentication protocol suitable for bandwidth-constrained wireless UAV networks.

6.3 Comparison with Existing Schemes

Table 5 compares the proposed protocol with representative lightweight UAV authentication schemes published in recent years. Table 6 and 7 shows Computational Cost and Communication Cost Comparison respectively.

Table 5: Security Feature Comparison

Feature	Zhang (2022)	CoMSeC++	Choi (2025)	LiteWTAKA	Proposed
Mutual Authentication	✓	✓	✓	✓	✓
Replay Resistance	✓	✓	✓	✓	✓
MITM Resistance	✓	✓	✓	✓	✓
Impersonation Resistance	✓	✓	✓	✓	✓
Session Key Agreement	✓	✓	✓	✓	✓
PUF Authentication	✓	✓	✓	✓	✓
PUF in Session Key	X	X	X	X	✓
Scyther Verification	X	✓	X	✓	✓
HMAC-Based Authentication	X	X	X	X	✓

Table 6: Computational Cost Comparison

Scheme	Computational Cost
Zhang et al. (2022)	$16T_{HASH} + 2T_{PUF}$
CoMSeC++ (2021)	Hash + PUF + Symmetric Encryption (protocol dependent)
Choi et al. (2025)	Hash + XOR + PUF + Fuzzy Extractor
LiteWTAKA (2026)	$15T_{HASH} + T_{PUF}$
Proposed	$4T_{HASH} + 4T_{HMAC} + 2T_{PUF}$

Table 7: Communication Cost Comparison

Scheme	Messages	Communication Cost
Zhang et al. (2022)	3	2688 bits
Choi et al. (2025)	3	Not directly comparable (different parameter sizes)
CoMSeC++ (2021)	Multiple	Higher than proposed (reported qualitatively)
LiteWTAKA (2026)	3	1536 bits
Proposed	3	1280 bits

6.4 Discussion

The performance evaluation demonstrates that the proposed protocol satisfies the requirements of lightweight UAV authentication. By relying exclusively on hash functions, HMACs, and PUF evaluations, the protocol avoids expensive public-key cryptographic operations that increase execution time and energy consumption. Furthermore, the three-message authentication exchange minimizes communication overhead while establishing a fresh session key and achieving mutual authentication. The integration of the PUF into session-key derivation distinguishes the proposed protocol from several existing lightweight schemes that use the PUF only for device authentication.

7. Conclusion

This paper proposed **LightSecurePUF**, a lightweight mutual authentication and session key establishment protocol for secure UAV-Ground Station communications. The protocol integrates a challenge-response Physically Unclonable Function with cryptographic hash functions and HMAC operations to provide hardware-assisted device authentication while maintaining low computational complexity. Unlike conventional lightweight authentication schemes that use the PUF only for identity verification, the proposed protocol incorporates the challenge-dependent PUF response into the session-key derivation process, thereby strengthening both authentication and key establishment.

The protocol requires only lightweight cryptographic primitives and a three-message authentication exchange, making it suitable for resource-constrained UAV platforms and wireless IoT environments.

Security analysis demonstrated that the protocol provides mutual authentication, replay attack resistance, man-in-the-middle attack resistance, impersonation resistance, session-key freshness, and protection of long-term credentials under the assumed threat model. Formal verification using the Scyther protocol verification tool further confirmed the secrecy, agreement, synchronization, and authentication properties of the protocol, with no attacks detected within the explored verification bounds.

Performance evaluation indicates that the proposed protocol achieves low computational and communication overhead while preserving a high level of security. These characteristics make LightSecurePUF an attractive candidate for practical deployment in UAV-assisted cyber-physical systems, intelligent transportation systems, smart agriculture, disaster response, and other resource-constrained wireless applications.

Future work will focus on extending the protocol to support multi-UAV collaborative networks, dynamic group authentication, UAV handover between multiple Ground Stations, and post-quantum lightweight authentication mechanisms. Additionally, implementing the protocol on embedded UAV hardware will enable experimental evaluation of execution time, energy consumption, and scalability under real-world operating conditions.

References

[1] Mekdad, Y., Aris, A., Acar, A., et al. (2024). *A comprehensive security and performance assessment of UAV authentication schemes*. *Security and Privacy, 7*(1), e338, 2024.

[2] Adil, M., Abulkasim, H., Farouk, A., & Song, H. (2024). *R3ACWU: A lightweight, trustworthy authentication scheme for UAV-assisted iot applications*. *IEEE Transactions on Intelligent Transportation Systems, 25*(6), pp. 6161-6172.

[3] Zhang, Z., Hsu, C., Au, & M. H., et al. (2024). *PRLAP-IoD: A PUF-based robust and lightweight authentication protocol for internet of drones*. *Computer Networks, 238*, 110118.

[4] Singh, M. *et al.* (2021). CoMSeC++: PUF-based secured light-weight mutual authentication protocol for Drone-enabled WSN. *Computer Networks*.

[5] Alkatheiri, M. S., Saleem, S., & Alqarni, M. A., et al. (2022). *A lightweight authentication scheme for a network of unmanned aerial vehicles using physical unclonable functions*. *Electronics, 11*(18), 2921.

[6] Zhang, X. *et al.* (2022). A PUF-based lightweight authentication and key agreement protocol for smart UAV networks. *IET Communications*.

[7] Choi, J., Kwon, D., Son, S., Park, Y., Das, A. K., & Park, Y. (2025). A PUF-based lightweight authentication scheme for UAV-assisted internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*.

[8] Xie, Q., & Wang, H. (2025). PUF-based secure and efficient anonymous authentication protocol for UAV towards cross-domain environments. *Drones*.

[9] Yu, S., Das, A. K., & Park, Y. (2024). *RLBA-UAV: A robust and lightweight blockchain-based authentication and key agreement scheme for PUF-enabled UAVs*.

[10] Kumar, N. *et al.* (2026). LiteWTAKA: Authenticating UAV-GCS and UAV-UAV communication using secure and lightweight mechanism based on PUF. *Journal of Network and Computer Applications*.

[11] D. Dolev, & A. Yao. (2003). On the security of public key protocols. *IEEE Transactions on Information Theory, 29*(2), 198-208.