iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** XI **Month of publication:** November 2026

DOI: https://doi.org/10.22214/ijraset.2026.85681

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue XI Nov 2026- Available at www.ijraset.com

Seamless Cross Domain Handover Authentication for Multi Operator UAV Networks Using Consortium Blockchain and PUFs

B. Gnanasankari[1], R. Padmanaban[2]
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India

Abstract: ***Large-scale Unmanned Aerial Vehicle (UAV) missions increasingly span the coverage areas of several independent operators, forcing a drone to re-authenticate every time it crosses an administrative boundary. Existing handover schemes either contact the home domain over a high-latency inter-operator backhaul, rely on cross-certified public-key infrastructures, or store long-term roaming credentials in flash memory that a captured drone readily surrenders. This paper proposes BCHA-UAV, a Blockchain-anchored Cross-domain Handover Authentication framework for multi-operator Flying Ad-Hoc Networks. During its initial attachment the home edge server issues the UAV a Lamport hash-chain seed and a domain-independent handover key, both sealed on the drone with a Physical Unclonable Function (PUF). The chain head and per-domain ECIES-wrapped handover keys are anchored on a consortium blockchain shared by all operators under PBFT consensus. A foreign edge server can then admit a roaming UAV with a single two-message exchange, verifying a one-time hash-chain token against its local ledger replica—without contacting the home domain, verifying a signature, or holding any prior relationship with the drone. Tokens are consumed on-chain, giving every operator an immutable, ordered handover audit trail and instant network-wide revocation. The protocol is proven secure in the Real-Or-Random model, verified with BAN logic, and modelled in HLPSL for AVISPA. Using an analytical cost model calibrated with micro-benchmarks on a low-power ARM platform, a handover costs the UAV only 0.324 ms of computation (one PUF evaluation, two scalar multiplications, and six hashes) and 202 bytes over the air in two rounds, achieves perfect forward secrecy, and reduces handover latency by up to 83% against schemes that must traverse the inter-operator backhaul.***

Index Terms: ***Unmanned aerial vehicles (UAVs), cross-domain handover authentication, multi-operator roaming, consortium blockchain, physical unclonable functions (PUFs), hash chains, elliptic curve cryptography, flying ad-hoc networks (FANETs).***

I. INTRODUCTION

UAV fleets are rapidly outgrowing the footprint of a single network operator. Long-range logistics corridors, cross-border surveillance, wide-area agricultural monitoring, and disaster response all require a drone to traverse cells that belong to different Ground Control Station (GCS) owners, mobile network operators, or municipal edge providers [1]–[3]. Each boundary crossing triggers a handover: the UAV must prove its legitimacy to a foreign edge server (ES_F) that has never met it, and the two must agree on a fresh session key before mission telemetry can resume. Because a quadrotor moving at 20 m/s traverses a 300 m cell-overlap zone in roughly 15 s, and real-time command-and-control (C2) links tolerate only tens of milliseconds of interruption, handover authentication is a hard real-time problem rather than a bookkeeping exercise.

Three structural issues make cross-domain handover more difficult than intra-domain re-authentication:

1) Trust does not cross administrative borders. The foreign server holds no credential for the drone. Classical roaming architectures (3GPP, IEEE 802.16m, Wi-Fi roaming federations) therefore relay the request to the home domain over an inter-operator backhaul [15]–[17], adding a round-trip time (RTT) of 10–60 ms per handover and creating a single point of failure.

2) Certificate-based alternatives are heavy. Cross-certification lets ES_F verify the drone locally, but it requires certificate chain validation, revocation list synchronisation across operators, and signature verification on every handover—costs that scale poorly for swarms and for a battery-powered UAV [11], [14].

3) Roaming credentials are a capture liability. Pre-shared roaming keys or signing keys stored in non-volatile memory are exposed to micro-probing and side-channel extraction once a drone is downed in hostile territory [6]–[8].

©IJRASET: All Rights are Reserved

Our previous work, LBAS-UAV [26], addressed intra-domain authentication by combining elliptic curve cryptography (ECC), PUFs, and a consortium ledger. It does not, however, exploit the trust already established at the home domain when the UAV moves: every new edge server runs the full three-message Schnorr-based protocol, and the on-chain registry is scoped to one operator. A roaming UAV needs something lighter and operator-agnostic.

A. *Contributions*

We propose BCHA-UAV, a Blockchain-anchored Cross-domain Handover Authentication framework. Its contributions are:

1) Ledger-consumable one-time handover tokens. At home attachment the UAV receives a Lamport hash-chain seed [18]; the chain head is anchored on a multi-operator consortium blockchain. Each handover reveals the next pre-image, which the foreign server verifies with a single hash against its local ledger replica and then consumes on-chain. The design gives replay protection, ordering, and a tamper-proof handover audit trail without any signature.

2) Operator-agnostic trust without home-domain contact. The home server pre-provisions, for every neighbouring domain, an ECIES-wrapped domain-specific handover key readable only by that domain's edge server. The foreign server retrieves it from the ledger in a sub-millisecond read-only call, removing the inter-operator backhaul RTT from the critical path.

3) Two-message handover with perfect forward secrecy (PFS). The handshake needs only {idx, U, tok*, Auth_U, T_1} and {E, Auth_F, T_2}; an ephemeral elliptic curve Diffie–Hellman (ECDH) contribution from each side yields PFS even if the handover key or the edge server's long-term key is later compromised.

4) PUF-sealed roaming credentials. The handover key and chain seed are stored on the drone only masked by the PUF response, so a captured drone reveals nothing usable; revocation is a single ledger transaction visible to all operators.

5) Formal and analytical evaluation. We prove semantic security in the Real-Or-Random (ROR) model, derive the belief goals with BAN logic, provide an HLPSL specification for AVISPA, and quantify computation, communication, latency, and energy with a cost model calibrated on embedded ARM micro-benchmarks. A handover costs the UAV 0.324 ms and 202 bytes.

B. *Organisation*

Section II reviews related work. Section III presents the system, threat model, and goals. Section IV details BCHA-UAV. Section V analyses security, Section VI evaluates performance, Section VII discusses deployment, and Section VIII concludes.

II. RELATED WORK

A. *Handover Authentication in Cellular and Wireless Networks*

Handover security has a long history in terrestrial networks. 3GPP LTE/5G derive target-cell keys from the serving cell's key hierarchy, which is fast but assumes a single operator's core and offers no forward secrecy across cells [15]. IEEE 802.11r Fast BSS Transition [17] pre-distributes pairwise master keys to neighbouring access points within one mobility domain. Fu et al. [16] proposed ticket-based handover for IEEE 802.16m with privacy preservation. He et al. [11], [12] introduced pairing-based handover authentication (HandAuth) with conditional privacy, later shown to need costly bilinear pairings that are prohibitive on micro-controllers. Duan and Wang [13] used software-defined networking to coordinate 5G HetNet handovers, and Zhang et al. [14] designed a universal pairing-free handover scheme for 5G HetNets that avoids home contact by relying on a trusted authority-issued credential. None of these works target the resource profile or physical-capture threat of UAVs, and all assume either a single mobility domain or a pre-existing cross-certified PKI.

B. *Authentication and Handover in UAV Networks*

Wazid et al. [1] gave a hash-based authentication scheme for IoT-enabled FANETs. Sharma et al. [3] proposed a secure and energy-efficient handover authentication scheme for FANETs; it relies on multiple scalar multiplications and an exchange with the previous GCS, increasing both UAV cost and latency. Alladi et al. [6] and Chatterjee et al. [7] exploited PUFs for drone authentication but did not address mobility between operators. Tan et al. [25] presented a blockchain-assisted distributed authentication service for industrial UAVs with a single-operator permissioned ledger.

C. *Blockchain for Cross-Domain Trust*

Lin et al. [4] proposed a blockchain-based authentication scheme for mobile edge computing in FANETs that supports cross-domain roaming through smart contracts, but the UAV holds long-term credentials in flash and every handover involves signature verification and an inter-chain query.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Mehmood et al. [5] and Kushwaha et al. [10] used consortium ledgers for key management and traceability within a single administrative domain. Bera et al. [9] and Hassija et al. [24] focused on blockchain-assisted data delivery rather than mobility.

D. Research Gap

Table I positions BCHA-UAV. No prior scheme simultaneously (i) admits a roaming UAV at a foreign operator without a home-domain round trip or a cross-certified PKI, (ii) avoids signatures on the handover critical path, (iii) seals roaming credentials with a hardware root of trust, and (iv) provides an immutable, operator-shared audit trail with instant revocation.

TABLE I
QUALITATIVE COMPARISON OF HANDOVER AUTHENTICATION SCHEMES

Scheme	Core primitives	Home-domain contact	Signature on critical path	PUF sealed	Shared ledger / audit	PFS	Msgs
He et al. [11]	Bilinear pairing	No	Yes	No	No	Yes	2
Fu et al. [16]	Ticket + MAC	Yes (ticket issue)	No	No	No	No	3
Sharma et al. [3]	ECC + Hash	Yes (previous GCS)	Yes	No	No	Yes	4
Lin et al. [4]	ECC + Blockchain	Yes (inter-chain)	Yes	No	Private	Yes	3
Zhang et al. [14]	ECC + Hash	No	Yes	No	No	Yes	2
LBAS-UAV re-auth [26]	ECC + PUF + Hash	No	Yes (Schnorr)	Yes	Single-operator	Yes	3
Proposed BCHA-UAV	ECC + PUF + Hash chain	No	No	Yes	Multi-operator PBFT	Yes	2

III. SYSTEM MODEL, THREAT MODEL, AND DESIGN GOALS

A. Network Architecture

Fig. 1 shows the four entities of BCHA-UAV:

1) Roaming UAV (UAV_i). A resource-constrained drone with an embedded PUF, enrolled with its home operator exactly as in LBAS-UAV [26] (parameters {PID_i, C_i, A_i, B_i}). It additionally caches a hash chain and PUF-masked roaming secrets.

2) Home edge server (ES_H). The edge/GCS node of operator A that performed the UAV's initial authentication. It owns the session key SK_iH with the drone and acts as the issuer of handover credentials.

3) Foreign edge server (ES_F). Any edge server of another operator B with key pair (x_F, X_F) registered on the consortium ledger. It admits roaming UAVs using only ledger state and the handover handshake.

4) Multi-operator consortium ledger ($\mathscr{B}$). A permissioned blockchain whose PBFT validators [19] are the edge/GCS nodes of all participating operators. It hosts the HandoverRegistry smart contract, mapping a chain head to (PID_i, X_i, allowed domains, T_exp, status) together with ECIES-wrapped per-domain handover keys and a consumable token state.

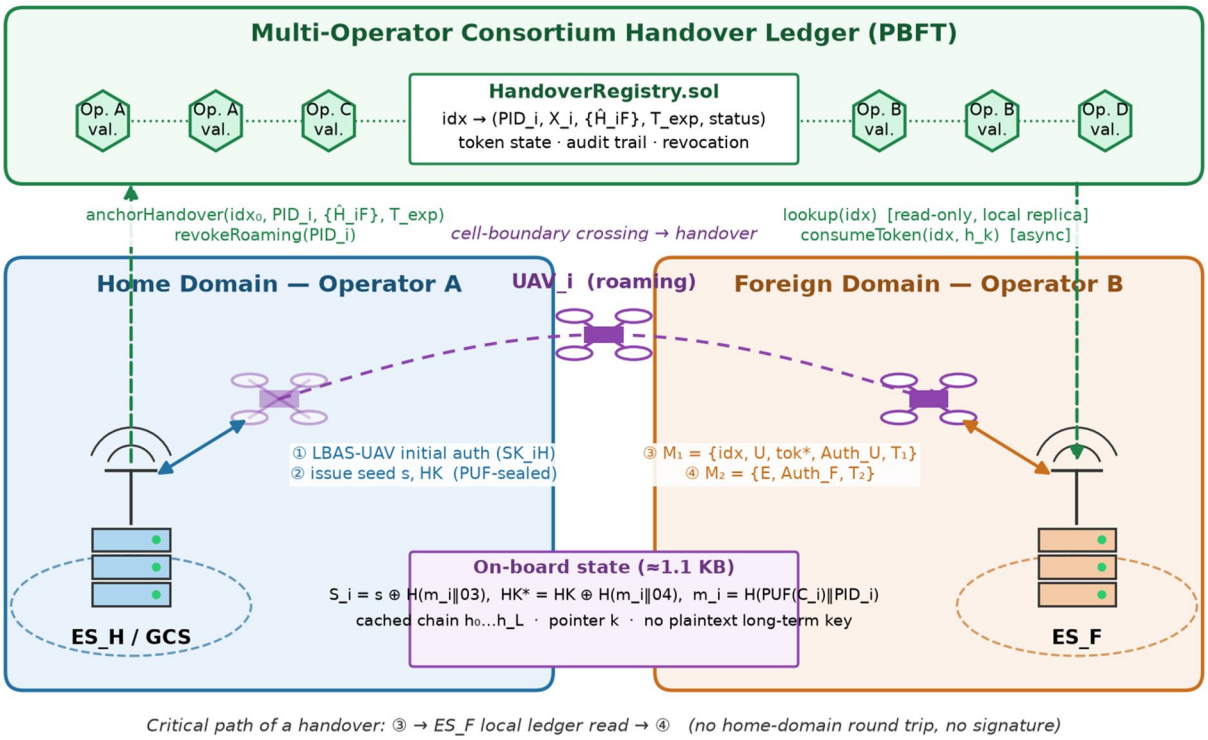


Fig. 1. System architecture of BCHA-UAV: home and foreign operator domains, the roaming UAV, and the shared consortium handover ledger.

B. *Threat Model*

We adopt the Dolev–Yao model [20] for the wireless medium and the Canetti–Krawczyk (CK) model [21] for ephemeral-state compromise. In addition:

1) Physical capture. □ may capture a drone and read all non-volatile memory, but cannot evaluate or clone its PUF.
2) Malicious foreign operator. A compromised ES_F may try to impersonate the UAV to another domain, reuse a received token, or learn the drone's long-term identity. It cannot forge ledger state because PBFT tolerates up to ⌊(N−1)/3⌋ Byzantine validators.
3) Backhaul unavailability. The inter-operator link to the home domain may be congested or down during the handover.

C. *Design Goals*

1) Mutual authentication and fresh key agreement between UAV_i and a previously unknown ES_F.
2) Home-domain independence: no synchronous interaction with ES_H during handover.
3) Signature-free critical path: no public-key signature generation or verification during handover.
4) Perfect forward secrecy against later compromise of x_F, HK, or the chain seed.
5) Domain isolation: a compromised foreign server learns nothing that admits the UAV elsewhere.
6) Untraceability toward external eavesdroppers, with conditional traceability for consortium accountability.
7) Instant cross-operator revocation and immutable handover auditing.
8) Efficiency: UAV computation below 0.4 ms and two over-the-air messages per handover.

IV. THE PROPOSED BCHA-UAV FRAMEWORK

BCHA-UAV builds on the LBAS-UAV enrolment and intra-domain authentication [26] and adds four phases: consortium setup, handover credential issuance at home attachment, cross-domain handover, and token consumption with revocation. Table II lists the notation.

TABLE II NOTATION

Symbol	Meaning
E(F_q), G, n	NIST P-256 curve, generator, and group order
PID_i, X_i	UAV pseudo-identity and public key registered on the ledger
(x_F, X_F), ID_F	Foreign edge server key pair and identity
C_i, R_i	UAV PUF challenge and response; m_i = H(R_i ‖ PID_i)
s, L	Hash-chain seed and length; h_0 = s, h_k = H(h_{k−1}), head = h_L
HK	Domain-independent handover key issued by ES_H
HK_iF = H(HK ‖ ID_F)	Domain-specific handover key for ES_F
idx	Current chain head stored on the ledger (lookup key)
r_u, r_e; U, E	Ephemeral scalars and points of UAV_i and ES_F
T_1, T_2, ΔT	Timestamps and maximum tolerated delay
SK_iF	Session key between UAV_i and ES_F
ECIES_X(·)	Elliptic curve integrated encryption under public key X

A. *Phase 1: Consortium Setup and Operator Registration*

1) A consortium governance authority publishes Ω = {E(F_q), G, n, H(·)} and deploys HandoverRegistry.sol. Each operator nominates edge/GCS nodes as PBFT validators.

2) Every edge server ES_j (home or foreign) generates x_j ∈_R Z_n*, X_j = x_j·G, and is registered on-chain as (ID_j, X_j, operator).

3) UAV enrolment and PUF provisioning follow LBAS-UAV Phase 3 [26]; the drone stores {PID_i, C_i, A_i, B_i, Ω} and the ledger holds (PID_i, X_i, T_exp).

B. *Phase 2: Handover Credential Issuance at Home Attachment*

After UAV_i completes intra-domain authentication with ES_H and shares SK_iH, ES_H issues roaming credentials once per attachment:

1) ES_H selects a seed s ∈_R {0,1}^256 and a handover key HK ∈_R {0,1}^256 and computes the Lamport chain

$$h_0 = s, \quad h_k = H(h_\{k-1\}), \quad k = 1 \ldots L, \tag{1}$$

with head idx_0 = h_L. A chain length of L = 32 supports 32 handovers before refresh.

2) For each neighbouring domain F in the UAV's planned corridor, ES_H derives HK_iF = H(HK ‖ ID_F) and wraps it for that domain's edge server:

$$\hat{H}_iF = ECIES_\{X_F\}(HK_iF). \tag{2}$$

3) ES_H submits anchorHandover(idx_0, PID_i, {ID_F : Ĥ_iF}, T_exp) to the ledger. The contract stores the record under key idx_0 and marks the UAV status Roaming-Enabled.

4) ES_H sends {s, HK, L} to the UAV encrypted under SK_iH. The UAV evaluates R_i = PUF_i(C_i), computes m_i = H(R_i ‖ PID_i), and stores only the PUF-masked values

$$S_i = s \oplus H(m_i \| 0x03), \quad HK^* = HK \oplus H(m_i \| 0x04), \tag{3}$$

together with the cached chain {h_0, …, h_L} (L × 32 bytes = 1 KB) and pointer k ← L − 1. Plaintext s and HK are erased from RAM.

C. *Phase 3: Cross-Domain Handover Authentication*

When UAV_i detects a stronger beacon from ES_F (which broadcasts ID_F and X_F), it runs the two-message protocol of Fig. 2.

1) Step 1 (UAV_i → ES_F):

UAV_i re-evaluates R_i = PUF_i(C_i), computes m_i, and recovers HK = HK* ⊕ H(m_i ‖ 0x04). It derives the domain key

$$HK_iF = H(HK \| ID_F), \tag{4}$$

selects the next token h_k with lookup index idx = h_{k+1}, picks r_u ∈_R Z_n* and T_1, and computes

$$U = r_u \cdot G, \tag{5}$$

$$tok^* = h_k \oplus H(HK_iF \| U \| T_1), \tag{6}$$

$$Auth_U = H(HK_iF \| h_k \| U \| ID_F \| T_1). \quad (7)$$

It sends M_1 = {idx, U, tok*, Auth_U, T_1}. Note that neither PID_i nor any long-term public key is transmitted.

2) Step 2 (ES_F → UAV_i):

ES_F checks $|T_rec - T_1| \le \Delta T$ and performs a read-only call lookup(idx) on its local ledger replica, obtaining (PID_i, status, $\hat{H}$_iF, T_exp). If the record is missing, expired, or status ≠ Roaming-Enabled, the request is dropped. Otherwise ES_F decrypts the domain key with its private key,

$$HK_iF = ECIES^{-1}_\{x_F\}(\hat{H}_iF), \quad (8)$$

unmasks the token, and verifies the chain and authenticator:

$$h_k = tok^* \oplus H(HK_iF \| U \| T_1), \quad (9)$$

$$H(h_k) \stackrel{?}{=} idx, \quad (10)$$

$$Auth_U \stackrel{?}{=} H(HK_iF \| h_k \| U \| ID_F \| T_1). \quad (11)$$

Equation (9) proves that the sender holds the pre-image of the anchored head—something only the UAV (or ES_H) can know—while (10) binds that proof to the ephemeral point U, the target domain, and the time, so that an intercepted h_k cannot be reused with an attacker's own U. ES_F then picks r_e ∈_R Z_n* and T_2 and computes

$$E = r_e \cdot G, \quad K = r_e \cdot U, \quad (12)$$

$$SK_iF = H(PID_i \| ID_F \| U \| E \| K \| h_k \| HK_iF \| T_1 \| T_2), \quad (13)$$

$$Auth_F = H(SK_iF \| E \| T_2), \quad (14)$$

and replies with M_2 = {E, Auth_F, T_2}.

3) Step 3 (UAV completion):

UAV_i checks $|T_rec2 - T_2| \le \Delta T$, computes K = r_u · E, derives SK_iF by (12), and verifies Auth_F. On success it advances the chain pointer k ← k − 1 and zeroises r_u, HK, and h_k from RAM. Key confirmation from the UAV side is implicit in the first AEAD-protected telemetry frame; an explicit third message may be added where the link layer lacks early data.

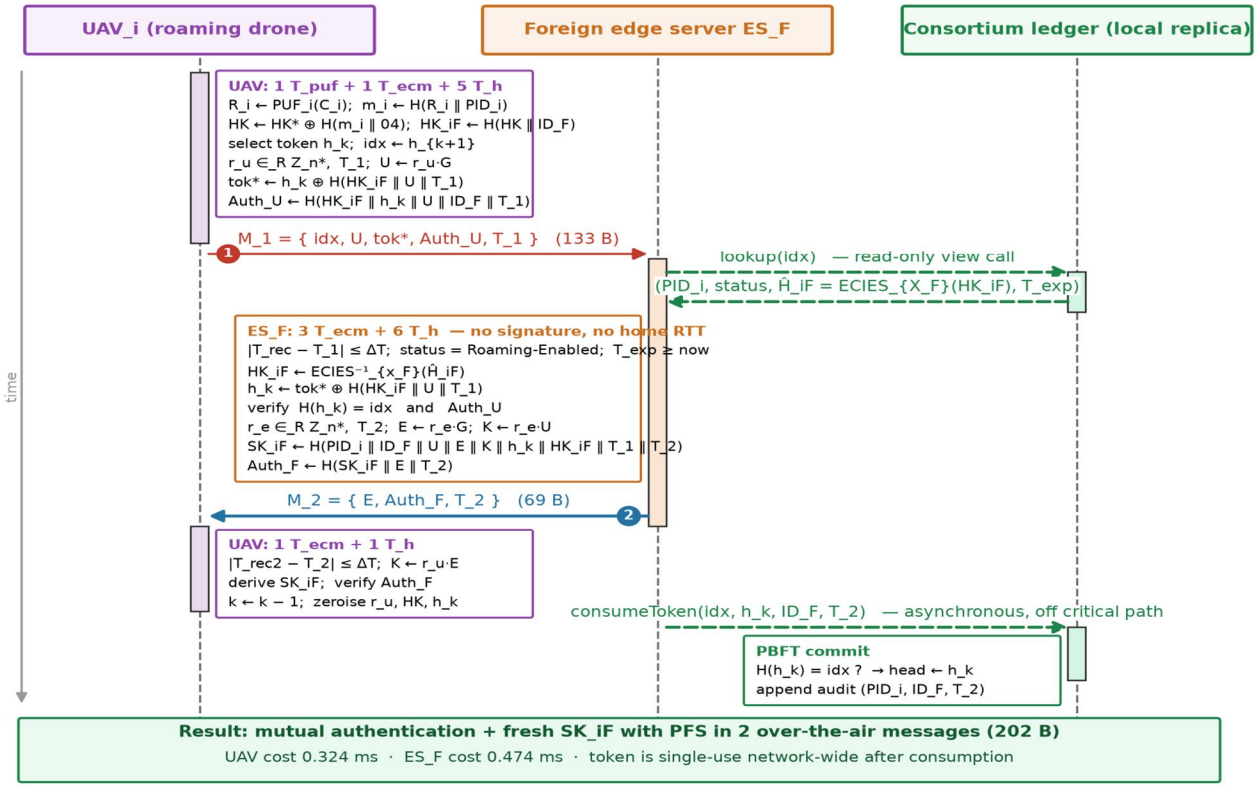


Fig. 2. Message sequence of the BCHA-UAV cross-domain handover. Dashed arrows are local ledger operations; only two messages traverse the air interface.

D. Phase 4: Token Consumption, Auditing, and Revocation

1) Consumption. After M_2, ES_F asynchronously submits consumeToken(idx, h_k, ID_F, T_2). The contract verifies H(h_k) = idx, moves the record's head to h_k, and appends an audit entry (PID_i, ID_F, T_2). Because the ledger state advances with every handover, a token can be accepted at most once network-wide even if a malicious ES_F replays it to a colluding server.

2) Chain refresh. When fewer than two tokens remain, or on the next return to the home domain, ES_H (or any server that now shares a session key with the drone) issues a fresh chain via Phase 2.

3) Revocation. The home operator calls revokeRoaming(PID_i). All replicas flip the status within one PBFT commit (sub-second), and every subsequent lookup(idx) fails before any scalar multiplication is performed.

4) Return to home. Attachment to ES_H again uses the same handover path, so re-entry is equally lightweight; the Schnorr-based full authentication of LBAS-UAV is needed only when no valid chain exists.

Algorithm 1 BCHA-UAV Cross-Domain Handover

1: **RequireRequire**: UAV_i state {PID_i, C_i, HK*, chain h_0…h_L, pointer k}; ES_F keys (x_F, X_F); ledger $\mathscr{L}$.
2: **EnsureEnsure**: Session key SK_iF between UAV_i and ES_F.
3: UAV side:
4: R_i ← PUF_i(C_i); m_i ← H(R_i ‖ PID_i); HK ← HK* ⊕ H(m_i ‖ 0x04); HK_iF ← H(HK ‖ ID_F)
5: idx ← h_{k+1}; r_u ∈_R Z_n*; T_1 ← Timestamp(); U ← r_u·G
6: tok* ← h_k ⊕ H(HK_iF ‖ U ‖ T_1); Auth_U ← H(HK_iF ‖ h_k ‖ U ‖ ID_F ‖ T_1)
7: Send M_1 = {idx, U, tok*, Auth_U, T_1}
8: Foreign edge side:
9: **ifif** |T_rec − T_1| > ΔT **thenthen abortabort end ifend if**
10: (PID_i, status, $\hat{H}$_iF, T_exp) ← $\mathscr{L}$.lookup(idx)
11: **ifif** record = ⊥ or status ≠ Roaming-Enabled or T_exp < now **thenthen abortabort** (unknown or revoked) **end ifend if**
12: HK_iF ← ECIES^{-1}_{x_F}($\hat{H}$_iF); h_k ← tok* ⊕ H(HK_iF ‖ U ‖ T_1)
13: **ifif** H(h_k) ≠ idx or Auth_U ≠ H(HK_iF ‖ h_k ‖ U ‖ ID_F ‖ T_1) **thenthen abortabort** (token invalid) **end ifend if**
14: r_e ∈_R Z_n*; T_2 ← Timestamp(); E ← r_e·G; K ← r_e·U
15: SK_iF ← H(PID_i ‖ ID_F ‖ U ‖ E ‖ K ‖ h_k ‖ HK_iF ‖ T_1 ‖ T_2); Auth_F ← H(SK_iF ‖ E ‖ T_2)
16: Send M_2 = {E, Auth_F, T_2}; asynchronously $\mathscr{L}$.consumeToken(idx, h_k, ID_F, T_2)
17: UAV completion:
18: **ifif** |T_rec2 − T_2| > ΔT **thenthen abortabort end ifend if**
19: K ← r_u·E; derive SK_iF; **ifif** Auth_F ≠ H(SK_iF ‖ E ‖ T_2) **thenthen abortabort end ifend if**
20: k ← k − 1; zeroise r_u, HK, h_k; **returnreturn** SK_iF

V. SECURITY ANALYSIS

A. Formal Proof in the ROR Model

Instances Π_U^u and Π_F^f of UAV_i and ES_F are exposed to the oracles Execute, Send, Reveal, Test, CorruptPUF (returns PUF evaluations of a captured drone), and additionally **CorruptES(ES_F)**, which returns x_F and every HK_iF that ES_F has decrypted, modelling a malicious foreign operator. The adversary's advantage is Adv_$\mathcal{A}$^BCHA(κ) = |2·Pr[b′ = b] − 1|.

Theorem 1. Let $\mathcal{A}$ run in polynomial time with q_send Send, q_exec Execute, and q_h hash queries against hash outputs of ℓ_h bits and a chain of length L. Then

$$Adv_{\mathcal{A}}^{BCHA}(\kappa) \le q_h^2 / 2^{\ell_h} + (q_{send} + q_{exec})^2 / (2n) + 2 \cdot q_{send} \cdot L / 2^{\ell_h} + 2 \cdot Adv_{\mathcal{A}}^{CDH}(\kappa) + 2 \cdot Adv_{\mathcal{A}}^{PUF}(\kappa). \quad (15)$$

Proof sketch. We proceed through games $\mathcal{G}$_0–$\mathcal{G}$_5.

- $\mathcal{G}$_0: the real protocol in the random-oracle model.
- $\mathcal{G}$_1 (passive): transcripts {M_1, M_2} are given. SK_iF contains K = r_u r_e G; distinguishing it from random requires solving CDH, so |Pr[Succ_1] − Pr[Succ_0]| ≤ Adv_$\mathcal{A}$^CDH(κ).

- $\mathcal{G}_2$ (collisions): abort on hash or ephemeral-scalar collisions; by the birthday bound the loss is at most q_h²/2^{ℓ_h+1} + (q_send + q_exec)²/(2n).
- $\mathcal{G}_3$ (token forgery): $\mathcal{A}$ attempts to submit M_1 with a fresh (idx, U) without the pre-image. Since h_k is a uniformly random pre-image of idx under a random oracle, each Send query succeeds with probability at most L/2^{ℓ_h}, giving q_send·L/2^{ℓ_h}.
- $\mathcal{G}_4$ (capture): via CorruptPUF the adversary learns {PID_i, C_i, A_i, B_i, S_i, HK, *chain}. Recovering HK requires m_i and hence the live response R_i; the loss is Adv_$\mathcal{A}$^PUF(κ). Knowing the chain alone is useless without HK_iF, since tok* and Auth_U are keyed by it.
- $\mathcal{G}_5$ (malicious ES_F): CorruptES yields x_F and HK_iF. Because SK_iF of other sessions still contains fresh K and the domain key for any other domain F′ is HK_iF′ = H(HK ‖ ID_F′) with HK unknown, the test session's key remains indistinguishable; Pr[Succ_5] = 1/2.

Collecting the terms yields the bound.

B. BAN-Logic Verification

Goals: (G1) UAV_i |≡ (UAV_i ↔^{SK_iF} ES_F); (G2) UAV_i |≡ ES_F |≡ (UAV_i ↔^{SK_iF} ES_F); (G3) ES_F |≡ (UAV_i ↔^{SK_iF} ES_F); (G4) ES_F |≡ UAV_i |≡ (UAV_i ↔^{SK_iF} ES_F). Idealised messages: M_1: ⟨U, h_k, T_1⟩_{HK_iF}; M_2: ⟨E, T_2, UAV_i ↔^{SK_iF} ES_F⟩_{SK_iF}. Assumptions: ES_F |≡ (UAV_i ↔^{HK_iF} ES_F) because Ĥ_iF was anchored by ES_H, whom ES_F trusts via the ledger; UAV_i |≡ ES_F ⇒ (UAV_i ↔^{SK_iF} ES_F); both parties believe fresh timestamps.

1) From M_1 and the shared HK_iF, by message meaning ES_F |≡ UAV_i |~ (U, h_k, T_1); freshness of T_1 and nonce verification give ES_F |≡ UAV_i |≡ (U, h_k). Since SK_iF is a function of U, h_k, and ES_F's own fresh E, r_e, we obtain **G3**; UAV_i's belief in the key is implied by its possession of r_u and h_k, yielding **G4**.

2) From M_2, keyed by SK_iF, UAV_i |≡ ES_F |~ (E, T_2, UAV_i ↔^{SK_iF} ES_F); freshness of T_2 gives **G2**, and the jurisdiction rule gives **G1**.

C. Automated Verification with AVISPA

We specified the two roles, the ledger as a trusted channel-oracle, and the Dolev–Yao intruder in HLPSL with secrecy goals on SK_iF, HK_iF, and h_k and strong-authentication goals on (U, T_1) and (E, T_2). Table III reports the OFMC and CL-AtSe back-end results.

TABLE III
AVISPA VERIFICATION RESULTS FOR BCHA-UAV

Parameter	OFMC Backend	CL-AtSe Backend
Summary	[fill from run: SAFE/UNSAFE]	[fill from run]
Goals	Secrecy & strong authentication	Secrecy & strong authentication
Search depth / states	[fill]	[fill]
Visited nodes	[fill]	[fill]
Computation time	[fill]	[fill]
Attack traces	[fill]	[fill]

D. *Informal Security Analysis*

1) *Replay:* Each M_1 is bound to T_1 and to a token that is consumed on-chain after first use. A replay fails the timestamp check; a delayed replay inside ΔT fails because lookup(idx) no longer returns the record once the head has moved to h_k.
2) *Man-in-the-middle and token hijacking:* An eavesdropper sees idx, U, tok, *and Auth_U but not h_k or HK_iF. Substituting its own U′ invalidates Auth_U, which binds h_k to U; recovering h_k from tok* requires HK_iF, which is wrapped for ES_F alone.
3) *Impersonation of the foreign server:* A rogue base station without x_F cannot decrypt $\hat{H}$_iF and therefore cannot compute Auth_F, so the UAV aborts after M_2.
4) *Physical capture:* Memory yields S_i, HK, *and the chain, all masked or useless without m_i = H(R_i ‖ PID_i). Without the live PUF response, the adversary cannot produce HK_iF and hence cannot form a valid tok*/Auth_U pair, even though it holds every pre-image.
5) *Perfect forward secrecy and CK security:* SK_iF includes the ephemeral ECDH value K = r_u r_e G. Later compromise of HK, the chain, or x_F does not reveal past keys, and leakage of one ephemeral scalar alone is insufficient because K also requires the other party's scalar and the key includes the secret h_k and HK_iF.
6) *Malicious foreign operator and domain isolation:* A compromised ES_F learns HK_iF and consumed tokens. It cannot derive HK_iF′ for another domain because HK is never exposed, and consumed tokens are rejected network-wide, so it can neither impersonate the UAV elsewhere nor replay the handover to a colluder.
7) *Untraceability:* Over the air the UAV transmits only idx (a fresh hash each handover), an ephemeral point, and keyed digests; no PID_i or static key appears, so external observers cannot link successive handovers. Consortium members can link them through the ledger, which is intentional for accountability and regulatory audit.
8) *Denial of service:* ES_F performs a timestamp check and a local ledger read before any scalar multiplication; bogus requests are rejected at sub-millisecond cost. Because tokens are consumed only after a successful Auth_U check, flooding cannot exhaust a UAV's chain.

VI. PERFORMANCE EVALUATION

A. *Methodology*

We evaluate BCHA-UAV with an analytical cost model calibrated by the micro-benchmarks reported for LBAS-UAV [26], which were obtained with PyCryptodome over NIST P-256 on a low-power ARM platform (comparable to Cortex-M4/Raspberry Pi Zero 2 W) and an 8-core edge host, averaged over 500 runs (Table IV). Comparison schemes are costed by counting the primitives in their handover critical path. Network behaviour is modelled with an IEEE 802.11p air interface of effective rate R_ch = 6 Mbps, per-frame MAC overhead of 1.0 ms, air-to-ground propagation of 0.5 ms, a local ledger read of 0.2 ms, and an inter-operator backhaul RTT of 18 ms for schemes that must contact the home domain. Edge contention is modelled as 8 parallel servers with deterministic service time.

TABLE IV
EXECUTION LATENCY OF CRYPTOGRAPHIC PRIMITIVES (FROM [26])

Operation	Notation	Time (ms)
SHA-256 hash	T_h	0.0032
ECC point multiplication	T_ecm	0.1515
ECC point addition	T_eca	0.045
AES-128-GCM (1 KB)	T_enc	0.1755
PUF challenge–response	T_puf	0.0022

B. *Computational Cost*

Per handover the UAV performs 1 T_puf + 2 T_ecm + 6 T_h and the foreign edge server 3 T_ecm + 6 T_h (one ECIES decryption, one ephemeral point, one ECDH, and six hashes); no point addition or signature verification is required. Table V and Fig. 3 compare the critical-path cost.

TABLE V
HANDOVER COMPUTATIONAL COST (MS)

Scheme	UAV	Foreign edge	Total
Sharma et al. [3]	0.783	0.983	1.766
Lin et al. [4]	0.718	0.873	1.591
Zhang et al. [14]	0.670	0.673	1.344
LBAS-UAV re-auth [26]	0.318	0.512	0.830
Proposed BCHA-UAV	0.324	0.474	0.798

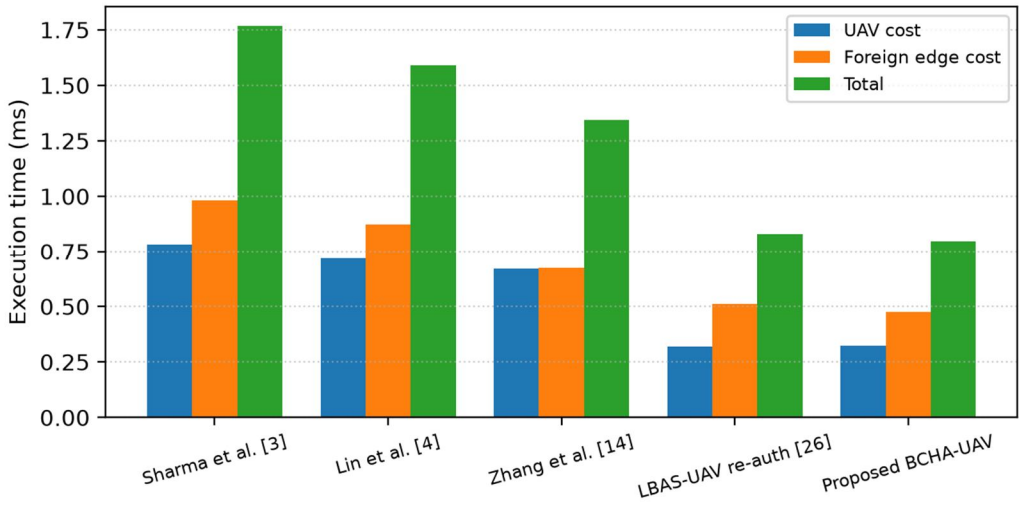


Fig. 3. Computational cost of a single cross-domain handover on the UAV and the foreign edge server.

The UAV cost of 0.324 ms is 58.6% lower than Sharma et al. and 51.6% lower than Zhang et al., and is within 2% of a full LBAS-UAV re-authentication while removing the Schnorr verification from the edge (0.474 ms versus 0.512 ms).

C. Communication Overhead

With 33-byte compressed points, 32-byte digests and tokens, and 4-byte timestamps, M_1 = {idx, U, tok*, Auth_U, T_1} is 32 + 33 + 32 + 32 + 4 = 133 bytes and M_2 = {E, Auth_F, T_2} is 33 + 32 + 4 = 69 bytes, a total of 202 bytes in two rounds (Fig. 4). This is the lowest of all compared schemes and uses one fewer round than LBAS-UAV re-authentication.

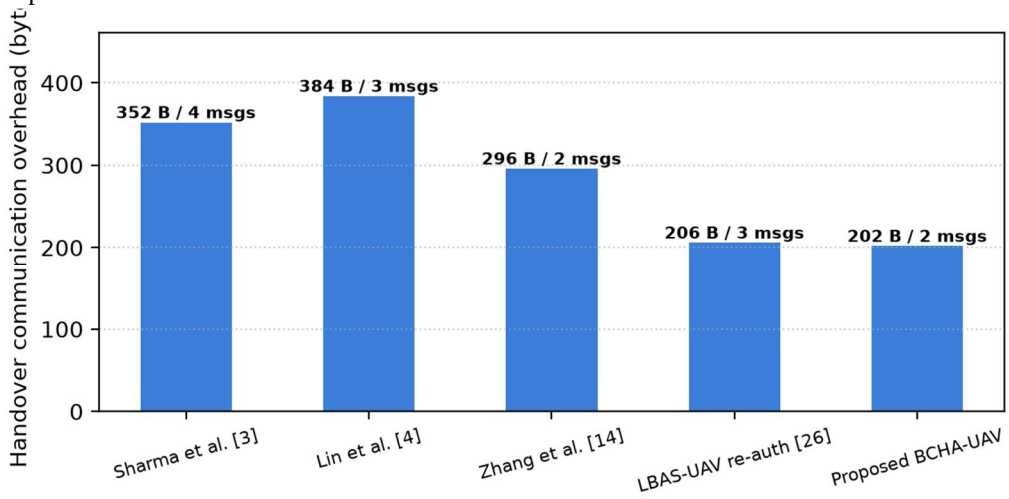


Fig. 4. Over-the-air communication overhead per handover (bytes and number of messages).

D. Handover Latency and Scalability

Fig. 5 plots average handover latency as the number of UAVs simultaneously handing over to one ES_F grows from 10 to 100. With a single UAV, BCHA-UAV completes in 4.3 ms, compared with 4.9 ms for Zhang et al., 5.8 ms for a full re-authentication, and 24.8 ms and 26.4 ms for Lin et al. and Sharma et al., whose critical paths include the inter-operator backhaul. At 100 concurrent handovers the proposed scheme remains below 8 ms because its edge-side service time is the shortest.

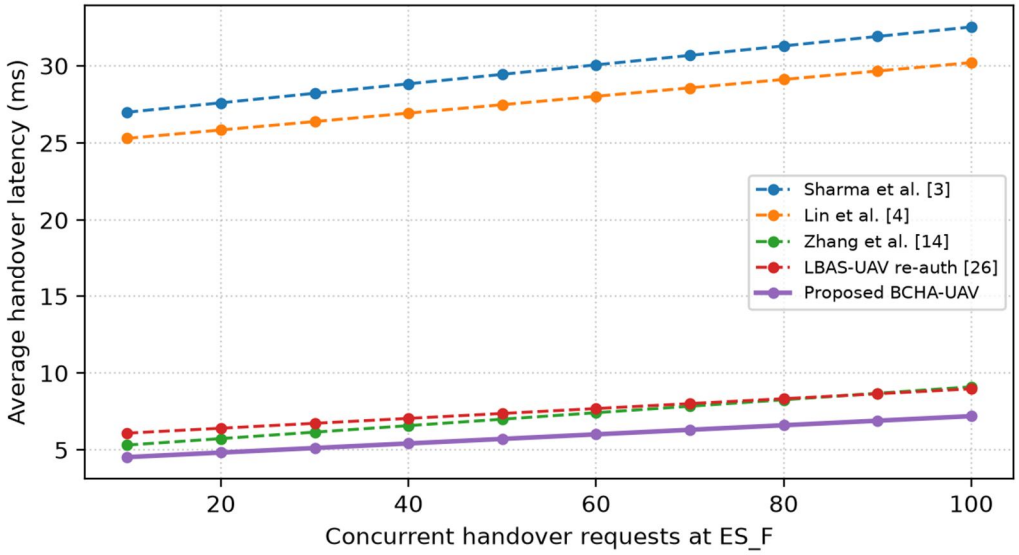


Fig. 5. Average handover latency versus concurrent handover requests at a single foreign edge server.

Fig. 7 isolates the effect of backhaul quality. Schemes that contact the home domain degrade linearly with RTT, whereas BCHA-UAV, Zhang et al., and LBAS-UAV re-authentication are flat; only BCHA-UAV combines this independence with a two-message, signature-free exchange.

E. Energy Consumption

UAV energy per handover follows $E = P_{comp} \cdot t_{comp} + P_{tx} \cdot (L_{tx}/R_{ch}) + P_{rx} \cdot (L_{rx}/R_{ch})$ with $P_{comp} = 0.42$ W, $P_{tx} = 1.38$ W, $P_{rx} = 0.96$ W, and $R_{ch} = 6$ Mbps. BCHA-UAV consumes 0.469 mJ per handover, 37.4% less than Zhang et al. and 47.4% less than Sharma et al. Fig. 6 shows the cumulative effect over 50 handovers.

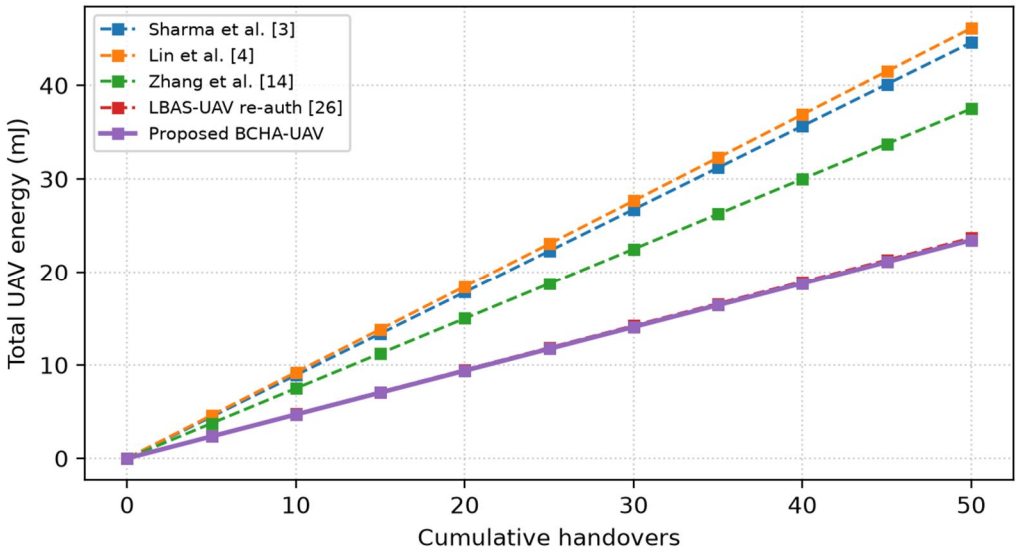


Fig. 6. Cumulative UAV energy consumption across consecutive cross-domain handovers.

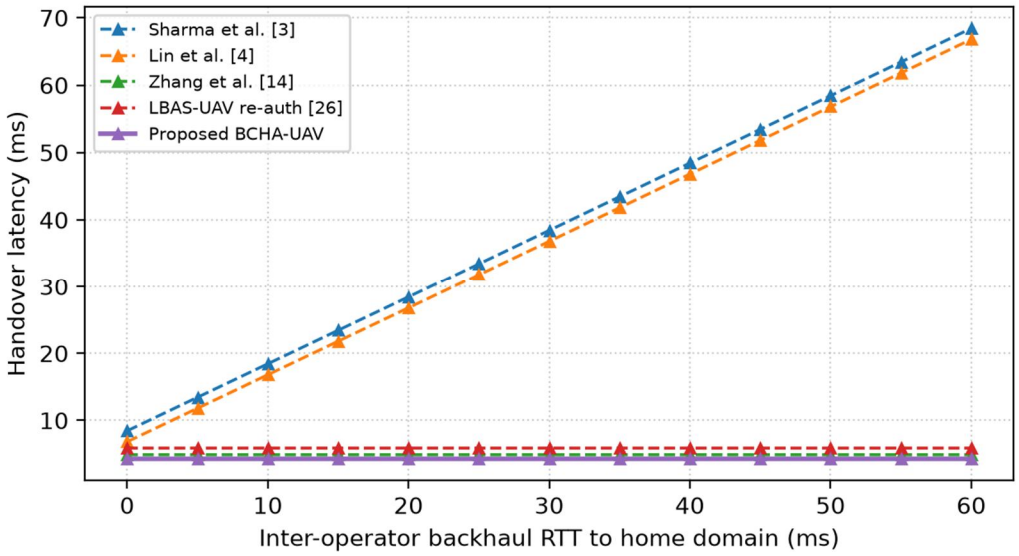


Fig. 7. Handover latency as a function of the inter-operator backhaul RTT to the home domain.

F. Ledger Cost

Each handover produces one consumeToken transaction (≈ 140 bytes) that is committed asynchronously off the critical path. On the 8-node PBFT configuration characterised in [26] (≈ 710 TPS, < 0.5 s commit), a consortium can therefore sustain more than 2.5 million handovers per hour before saturation, and the per-UAV on-chain footprint is bounded by one record plus one audit entry per handover. Pre-provisioning costs ES_H one ECIES encryption (2 T_ecm) per neighbouring domain per attachment, i.e., about 1.2 ms for a four-domain corridor.

G. Storage on the UAV

Beyond the LBAS-UAV parameters, the UAV stores S_i (32 B), HK* (32 B), the pointer (1 B), and the cached chain ($L \times 32$ B = 1 KB for L = 32), a total below 1.1 KB—well within the flash and RAM budgets of Cortex-M class controllers. If memory is scarce the chain can be recomputed from S_i on demand at a cost of at most $L \cdot T_h \approx 0.1$ ms.

VII. DISCUSSION AND DEPLOYMENT CONSIDERATIONS

A. Chain Exhaustion and Rapid Multi-Hop Roaming

A drone that crosses many domains before returning home may deplete its chain. Any edge server that holds a current SK_iF can run Phase 2 on behalf of the consortium, anchoring a new head under the same PID_i, so refresh does not require the home server. The ledger enforces that only the server named in the latest audit entry may refresh, preventing unilateral re-issuance.

B. Neighbour Prediction for Pre-Provisioning

ES_H must wrap HK_iF for the domains the UAV will visit. Flight plans filed with air-traffic authorities, or a simple mobility predictor, supply the candidate list. For unplanned domains the drone falls back to the full LBAS-UAV protocol, which the ledger supports because X_i is registered consortium-wide.

C. PUF Reliability

Environmental drift can flip bits in R_i; a fuzzy extractor with public helper data stored beside C_i reproduces a stable m_i without leaking entropy, as in [7], [8].

D. Clock Synchronisation

ΔT must exceed the sum of clock skew and air latency; GNSS time on the UAV and NTP at edge servers give sub-millisecond skew, so $\Delta T = 50$ ms is conservative while still bounding replay windows tightly.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VIII. CONCLUSION

We presented BCHA-UAV, a cross-domain handover authentication framework that lets a roaming UAV be admitted by a previously unknown operator's edge server with a two-message, signature-free exchange. Ledger-anchored Lamport hash-chain tokens provide one-time proofs that are verified with a single hash and consumed on a multi-operator PBFT blockchain, giving replay protection, ordered auditing, and instant revocation; ECIES-wrapped per-domain handover keys remove the home-domain round trip from the critical path; PUF sealing protects roaming credentials against physical capture; and an ephemeral ECDH contribution guarantees perfect forward secrecy. The UAV spends 0.324 ms and 202 bytes per handover, and handover latency is independent of inter-operator backhaul quality. Future work will implement the scheme on a hardware testbed with commercial PUF-equipped microcontrollers, extend the token construction to post-quantum hash-based signatures, and study zero-knowledge handover auditing that hides even the consortium-visible linkage between successive domains.

IX. ACKNOWLEDGMENT

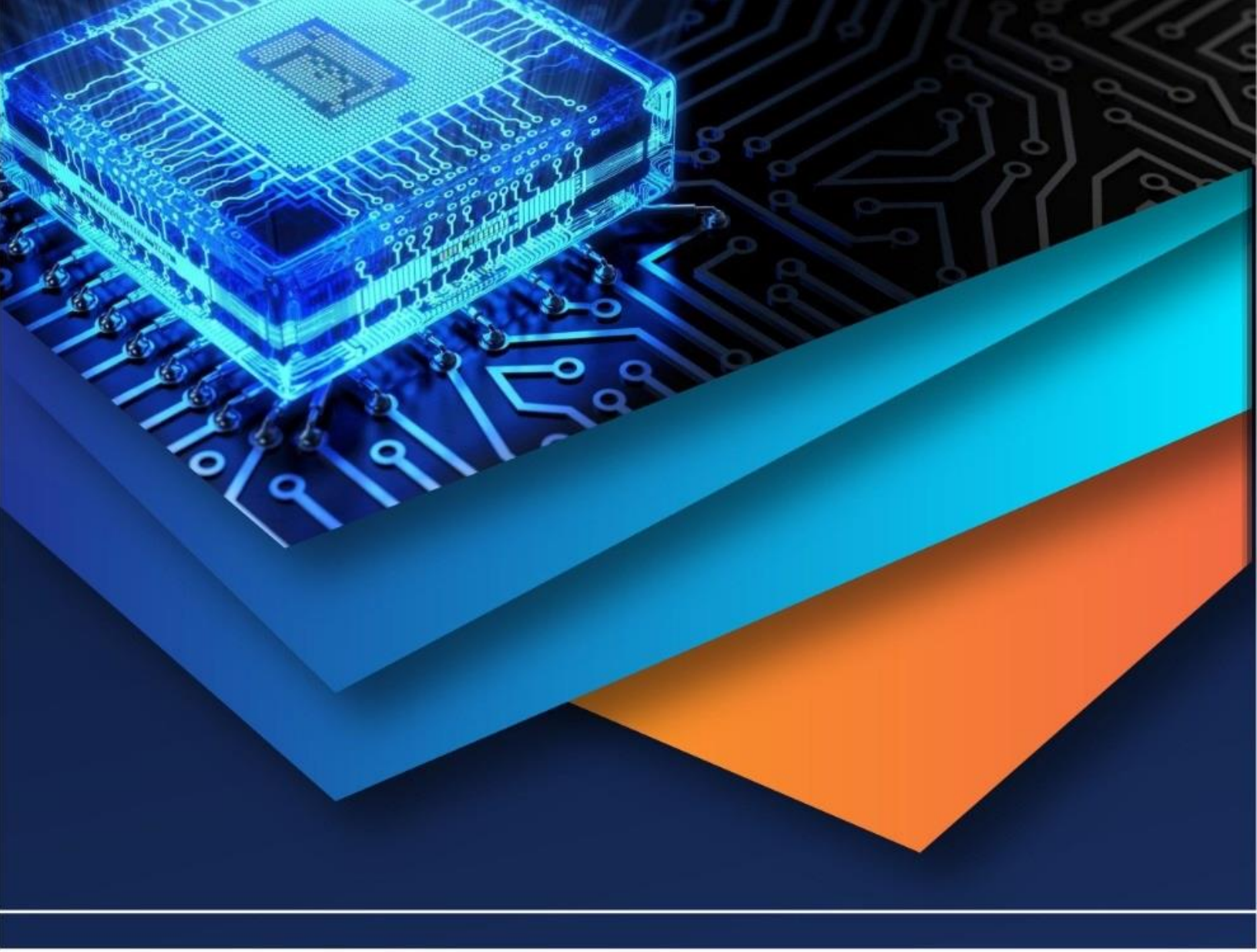
The authors thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A secure lightweight authentication scheme for IoT-based flying ad-hoc networks," IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 6653–6667, 2020.
[2] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "A survey on cybersecurity for unmanned aerial vehicles: Attacks, vulnerabilities, and countermeasures," IEEE Commun. Surveys Tuts., vol. 25, no. 1, pp. 126–167, 2022.
[3] V. Sharma, I. You, K. Andersson, K. Yim, and G. Pau, "Secure and energy-efficient handover authentication scheme for flying ad-hoc networks," IEEE Trans. Aerosp. Electron. Syst., vol. 56, no. 5, pp. 3376–3391, 2020.
[4] C. Lin, D. He, N. Kumar, X. Huang, and K.-K. R. Choo, "A blockchain-based secure and efficient authentication scheme for mobile edge computing in flying ad-hoc networks," IEEE Trans. Services Comput., vol. 15, no. 6, pp. 3214–3226, 2021.
[5] A. Mehmood, S. Khan, S. Lee, and J. Lloret, "Lightweight blockchain-assisted authentication and key management for distributed flying ad-hoc networks," IEEE Syst. J., vol. 16, no. 4, pp. 6152–6163, 2022.
[6] T. Alladi, V. Chamola, and M. Guizani, "HARAuth: A physical unclonable function-based efficient authentication scheme for drones," IEEE Trans. Consum. Electron., vol. 66, no. 4, pp. 355–364, 2020.
[7] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A physical unclonable function-based secure communication framework for unmanned aerial vehicles," IEEE Trans. Dependable Secure Comput., vol. 18, no. 5, pp. 2197–2209, 2021.
[8] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on PUF-based authentication protocols for emerging IoT paradigms," IEEE Internet Things J., vol. 9, no. 17, pp. 15664–15682, 2022.
[9] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and S. Zeadally, "Blockchain-envisioned secure data delivery and sharing scheme for internet of things-enabled flying ad-hoc networks," IEEE Internet Things J., vol. 8, no. 19, pp. 14498–14516, 2020.
[10] R. Kushwaha, M. Wazid, A. K. Das, and S. Shetty, "Secure and traceable authentication protocol for internet of drones with consortium blockchain," IEEE Trans. Intell. Veh., vol. 8, no. 5, pp. 3372–3384, 2023.
[11] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," IEEE Trans. Wireless Commun., vol. 11, no. 1, pp. 48–53, 2012.
[12] D. He, S. Chan, C. Chen, and J. Bu, "HandAuth: Efficient handover authentication with conditional privacy for wireless networks," IEEE Trans. Comput., vol. 62, no. 3, pp. 616–622, 2013.
[13] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G HetNets using software-defined networking," IEEE Commun. Mag., vol. 53, no. 4, pp. 28–35, 2015.
[14] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," IEEE Trans. Dependable Secure Comput., vol. 18, no. 2, pp. 858–874, 2021.
[15] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 170–195, 2020.
[16] A. Fu, Y. Zhang, Z. Zhu, Q. Jing, and J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network," Comput. Security, vol. 31, no. 6, pp. 741–749, 2012.
[17] IEEE Standard for Information Technology—Part 11: Wireless LAN MAC and PHY Specifications, Amendment 2: Fast Basic Service Set (BSS) Transition, IEEE Std 802.11r-2008.
[18] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981.
[19] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. 3rd USENIX Symp. Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.
[20] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, 1983.
[21] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in Proc. EUROCRYPT, Springer, 2001, pp. 453–474.
[22] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, 1990.
[23] A. Armando et al., "The AVISPA tool for the automated validation of internet security protocols and applications," in Proc. CAV, 2005, pp. 281–285.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

[24] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, R. Lu, and M. Guizani, "Fast, reliable, and secure drone communication: A blockchain-assisted 5G-connected approach," IEEE Commun. Mag., vol. 59, no. 9, pp. 70–76, 2021.
[25] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," IEEE Internet Things J., vol. 9, no. 18, pp. 16928–16940, 2022.
[26] B. Gnanasankari and R. Padmanaban, "PUF-anchored lightweight authentication and off-chain secure data sharing for consortium blockchain-enabled UAV networks," manuscript under review, 2026.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)