AeroProof: Decentralized Mutual Authentication for UAV Swarm Networks

Hayder Ali Hameed[1], Hussein Ahmed Ali[2], Wasnaa Kadhim Jawad[3], Varun Shukla[4], Zainab Marid Alzamili[5] and Mahmood A. Al-Shareeda[6,7]

[1]*Directorate of Education Basrah, 61004 Basrah, Iraq*

[2]*University of Kirkuk, College Computer Science and Information Technology, 36001 Kirkuk, Iraq*

[3] *Department Information Technology, Businesses Informatics College, University of Information Technology and Communications, 10011 Baghdad, Iraq*

[4]*Dean Research, Allenhouse Institute of Technology, 08001 Kanpur, India*

[5]*Education Directorate of Thi-Qar, Ministry of Education, 64001 Nasiriyah, Iraq*

[6]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001 Basra, Iraq*

[7]*College of Engineering, Al-Ayen University, 64001 Nasiriyah, Iraq*

alhilifi@basrahaoe.iq, hussien.alwaise@uokirkuk.edu.iq, wasnaakadhim@uoitc.edu.iq, varun.shuklaa@gmail.com, Zainab.alzamili@utq.edu.iq, mahmood.alshareedah@stu.edu.iq

Keywords: UAV Authentication, Decentralized Security, Ephemeral Keys, Swarm Communication, Mobility-Aware Cryptography, Elliptic Curve Cryptography (ECC).

Abstract: This paper thus addresses a problem with pressing consequences: the rise of Unmanned Aerial Vehicle (UAV) swarms in mission-critical and infrastructure-less environments is demanding secure, scalable, and decentralized authentication. Current protocols heavily lean on centralized trust models or having static credentials, neither of which is fit for highly mobile & P2P UAV networks. AeroProof is presented, a lightweight and decentralized mutual authentication protocol based on mobility-aware ephemeral keys. Each UAV autonomously produces secure elliptic curve credentials from its relatively short location, speed, and motion orientation (a single flight only), leading to a unique 'motion ticket'. The credentials are afterwards employed for a mutual authentication at the application level that provides strong security properties such as forward secrecy, session unlinkability, immunity against impersonation, replay, and wormhole attacks without requiring long-term identities or certificate authorities. We show that AeroProof achieves an up to 64% faster authentication time, a 35% less communication overhead, and consumes over 50% less memory compared with recent ECC- and blockchain-based solutions. This work has demonstrated the practical usefulness of AeroProof as an authentic framework to enable secure and efficient decentralized swarm operations.

1 INTRODUCTION

With the amazing development of unmanned aerial vehicles (UAVs) in mission-critical applications such as environmental monitoring, disaster relief, military surveillance, and smart logistics, the demands for secure and scalability authentication mechanisms have been upgraded dramatically [1] - [3]. And many of these drones fly in fluid, infrastructure-free environments where conventional centralized security mechanisms are difficult or ineffective [4], [5]. In case of swarm-based deployments, where drones need to establish trust with their peers in real time as fast as possible, the lightweight and context-aware authentication process becomes a must [6], [7].

Traditional authentication protocols are based on long-term identifiers, certificate chains, or infrastructure-bound authentication procedures [8], [9]. Although such techniques work well in conventional networks, they are not suitable for an ad hoc UAV swarm with intermittent connectivity, high mobility, and tight resource support. Furthermore, identity-based solutions are still susceptible to impersonation, relay, and replay attacks, particularly when the system relies on radio communications and the adversaries have the capabilities to overhear and interfere with the radio exchange [10] - [12]. These

novel solutions have tried the deployment of blockchain, increasing the level of hardware tokens and the use of PUFs, but their usage will frequently improve the computation and communication requirements otherwise required to establish more stringent requirements [13] - [15].

This paper contributes to the critical gap of mobility-aware, decentralized authentication for UAV swarms. We focus on designing a protocol that facilitates mutual authentication without centralized control, and group members must authenticate one another in real-time as the drones change position to maintain secure connections and trust within the swarm. We present AeroProof, a new authentication protocol that generates ephemeral elliptic curve credentials tied to each UAV's instantaneous mobility vector: position, velocity, and orientation. These credentials are mobility-aware: They facilitate stateless together with context-driven trust among UAVs to establish secure communication in the absence of long-term identifiers and third-party verification. AeroProof is specifically designed to: Proxy Authentication (Prevent Impersonation, Replay, and Session Hijacking). Lightweight, fast authentication suitable for UAV resource limitations. Stay secure in low-mobility, infrastructure-less environments. The main contributions in this paper can be summarised as follows:

- We present AeroProof, a decentralized mutual authentication protocol designed to link ephemeral elliptic curve credentials with real-time UAV motion profiles.
- To address these challenges, we propose a mobility-consistent session key derivation mechanism that supports rapid location changes with minimal overhead.
- We consider two state-of-the-art protocols and show that AeroProof performs 64% faster than authentication, incurs 35% less communication overhead, and uses 50% less storage footprint.
- We investigate security against prevalent UAV attack vectors, which include impersonation, wormhole, and mobility spoofing.

The rest of the paper is organized as follows: Section 2 surveys related work; Section 3 describes the system and threat model; Section 4 details the AeroProof protocol; Section 5 analyzes the security of AeroProof; Section 6 presents performance analysis; Section 7 concludes the paper with future directions.

2 RELATED WORK

Several decentralized and context-aware authentication protocols have been proposed to meet these challenges. However, existing works mostly consider static identifiers and completely separate mobility from authentication or use infrastructure-heavy solutions requiring blockchains or smart contracts.

Finally, CoMAD [16] presented a context-aware mutual authentication protocol within drone networks with zone-based access control and ECC. Despite the energy efficiency and lightweight nature, CoMAD lacks in updating authentication credentials for changing real-time mobility, resulting in poor resilience to changes in a swarm environment. Algarni et al. [17] presented a verifiable ECC-based protocol for the Internet of Drones (IoD) with a new identity authentication approach using contextual metadata. The protocol works well; however is unable to dynamically update credentials or verify that movements are valid and demand a binding from the movement, which opens the design up for relays or spoofing attacks. Karmakar and Kaddoum [18] presented a blockchain-enabled decentralized authentication system for a UAV swarm. While this would enhance the trust and transparency of a transaction (as blockchain enables), it also brings about latency, storage overhead, and energy requirements, which may not be acceptable for real-time resource-constrained aerial drone deployment. SETCAP El-Zawawy et al. [19] focused on an extra layer of temporal authentication using time-limited tokens. Although it manages to save energy, the method does not offer spatial or mobility-aware validation and therefore is not robust for both offline (disconnected) and adversarial scenarios. Constantinescu et al. [20] presented an ECC protocol with a malicious drone detection scheme was suggested. This is an improvement with respect to safety, but uses behavior profiling and static keys, making it more difficult to scale for large, distributed swarms. As listed in Table 1, while the previous approaches assume that all nodes have perfectly unique identities. This provides stateless, contextaware authentication without long-term identities or centralized authorities.

3 SYSTEM AND THREAT MODEL

3.1 System Model

The considered system consists of a decentralized swarm of UAVs cooperatively operating in an infrastructure-less environment (e.g., tactical surveillance zone, disaster area, or autonomous logistics corridor), as shown in Figure 1. Each UAV of the swarm consists of: a Global Navigation Satellite System (GNSS)-based acquiring module (such as the GPS or the RTK), an IMU for mobility sensing (speed and direction), an ECC-capable processor with a small footprint (e.g., ARM Cortex-M or RISC-V), and a Wireless transceiver with peer-to-peer (P2P) capabilities.

The UAV agents are autonomous (i.e., they do not need a central ground station or certificate authority). Instead, they achieve mutual authentication of the mobile devices based on ephemeral public keys and mobility-restricted identifiers that are computed based on real-time movement data. The users specifically use relative mobility thresholds (e.g., direction deviation, speed variance) to verify the validity of peer devices before beginning a secure session. The authentication is done over broadcast or unicast ad hoc links, and once authenticated, a short-lived shared secret is created for encrypted communication during the session. Credentials are reissued over time or in response to a large change in motion. Each UAV includes a Position Estimation

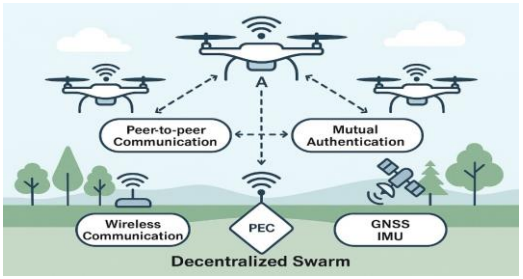

Figure 1: System model of the decentralized UAV swarm environment.

System (PES), which integrates data from the onboard GNSS and IMU sensors to derive real-time motion vectors. These vectors – consisting of latitude, longitude, velocity, and heading – are crucial for generating the mobility-bound ephemeral keys used in authentication.

3.2 Threat Model

The security analysis model considers an adversarial scenario in which attackers control communication channels and attack some UAV nodes. The protocol protects against the following threats:

- Impersonation Attacks: An adversary has access to the communication channel and maliciously pretends to be a legitimate UAV by generating valid-looking credentials.
- Replay Attacks: Old exchanged valid messages are replayed to allow unauthorized access.
- Relay (Wormhole) Attacks: Messages are relayed from distant locations to bypass spatial verification.
- Session Hijacking – An attacker will attempt to grab or replace the session key after you are authenticated.
- Insider Threats: A stolen UAV that was trusted to fly now tries to misuse valid credentials, access forbidden mobility zones.
- Mobility Spoofing: The adversary fabricates GNSS or IMU data such that the calculated position or path vector can satisfy the validation.

Adversaries can eavesdrop, inject, and modify messages, noiselessly harvest traffic information, but cannot access private ephemeral keys or secure mobility sensors of honest drones. Side-channel and physical attacks are also out of scope.

4 DESIGN OF AEROPROOF PROTOCOL

In this section, we present the three phases of the AeroProof protocol (shown in Fig. 2), which are tightly integrated: mobility-aware ephemeral key generation, mutual authentication, and session expiration with dynamic rekeying. In the initialization stage, the UAVs compute a short-lived public–private key pair for a mobility vector (composed of their position, velocity, and heading) of themselves autonomously (i.e., one-time use). In their mutual authentication phase, UAVs exchange their mobility-bound identifiers, and then they verify the similarity of their motions and the freshness of the timestamp to derive a session key through elliptic curve Diffie–Hellman.

Table 1: Summary of existing authentication protocols for UAV swarms.

Author(s) & Year	Methodology	Key Results / Features	Limitations
Cabuk et al. (2021)	ECC + Contextual Zones (CoMAD)	Lightweight, policy-based access control	No mobility adaptation
Algarni et al. (2025)	ECC + Synergistic Metadata	Secure mutual authentication for IoD	Lacks motion consistency validation
Karmakar & Kaddoum (2024)	Blockchain + Smart Contracts	Transparent decentralized identity management	High latency, poor scalability
El-Zawawy et al. (2022)	Time-token protocol (SETCAP)	Energy-efficient, time-bound credential renewal	Ignores spatial or motion-based verification
Constantinescu et al. (2024)	ECC + Behavior Profiling	Detects malicious UAVs based on anomalies	No dynamic rekeying, static credentials
This work: AeroProof	ECC + Mobility-Bound Ephemeral Keys	64% faster auth, 35% lower overhead, 50% less memory	Assumes trusted sensors, requires sync clock

Finally, during the session management phase, keys are continually updated subject to time limitations and mobility drift; if deviations are true, the protocol initiates re-authentication by exchanging new credentials. For example, the interaction flow between the three phases of the proposed scheme is illustrated in Figure 1, where the three phases are integrated into a cycle for realizing indelible trust updates in mobile and distributed swarm systems and ensuring resistance to impersonation, replay, and trajectory-based attacks.

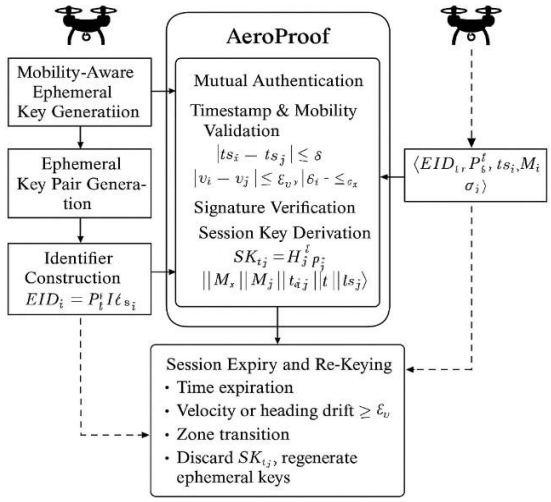

Figure 2: Design of the AeroProof authentication protocol.

4.1 Mobility-Aware Ephemeral Key Generation

In the AeroProof protocol, each UAV produces an ephemeral digital credential that is tightly coupled with its instantaneous movement profile. To generate a mobility-aware ephemeral key pair, the following operations need to be carried out:

1) Mobility Vector Acquisition. The UAV Di collects its current position and movement data using onboard sensors. The mobility vector is defined as: Mi = (lati, loni, vi, θi), where lati and loni are geographic coordinates, vi is velocity, and θi is the current heading direction.
2) Ephemeral Key Pair Generation. The UAV generates a new elliptic curve key pair at timestamp tsi: xi_t ∈ Z∗q, Pi_t = xi_t ·G, where xit is the private key, Pti is the public key, and G is the base point on the selected elliptic curve.
3) Identifier Construction. The UAV derives a mobility-aware ephemeral identifier using a secure hash function H(·): EIDi = H(Pi_t ‖ Mi ‖ tsi), where the identifier binds the key to both the motion context and its generation timestamp.
4) Validity Window Enforcement. The ephemeral credential (Pti, EIDi) is valid for a limited time interval ΔT or until a deviation is detected in the UAV's velocity or heading angle: |vi − v′i| > ϵv or |θi − θ′i| > ϵθ, where vi′,θi′ are the updated motion parameters after a threshold duration or movement.
5) Credential Preparation. The ephemeral identifier and public key are stored in the UAV's temporary credential cache and used in subsequent mutual authentication steps.

4.2 Mutual Authentication Procedure

After proximity is established between them, the two UAVs engage in mutual authentication based on a set of mobility-aware short-term identities. The authentication includes

1) Authentication Tuple Exchange. Each UAV Di sends its authentication tuple to the peer UAV Dj: ⟨EIDi, Pi_t, tsi, Mi, σi⟩, where σi = HMAC is a message authentication code proving possession of the private key.
2) Timestamp Validation. The receiving UAV verifies the freshness of the timestamp tsi by checking: $|tsi - tsj| \leq \delta$, where δ is the maximum allowable clock drift between the UAVs.
3) Mobility Similarity Check. The UAV evaluates whether the sender's mobility vector Mi is within acceptable deviation thresholds compared to its own: $|vi - vj| \leq \epsilon v$ and $|\theta i - \theta j| \leq \epsilon\theta$. This ensures both drones are in relative motion alignment within the swarm.
4) Signature Verification. Using the received public key Pti, the UAV validates the HMAC σi. Successful verification confirms that the peer possesses the correct private key and has not been impersonated.
5) Session Key Derivation. If all validations pass, both UAVs independently compute a shared session key using Elliptic Curve Diffie–Hellman (ECDH): SKij = H(xit · Ptj ‖ Mi ‖ Mj ‖ tsi ‖ tsj). The resulting session key is used to secure further communications between the two authenticated UAVs.

4.3 Session Expiry and Re-Keying

To achieve security against trajectory drift or relative insider misuse, there is a time and mobility-based expiration of the active session keys. When the lifetime expires, secure rekeying procedures are initiated automatically by both UAVs. The re-keying procedure is as follows:

1) Session Monitoring: Each UAV continuously monitors the validity of its current session key SKij based on elapsed time and current motion data.
2) Expiration Conditions Check: The session key is considered expired and revoked if any of the following conditions hold:
   - Time expiration: tnow > tsi +ΔT • Velocity drift: $|vi - vi'| > \epsilon v$ • Heading drift: $|\theta i - \theta i'| > \epsilon\theta$.
   - Zone transition: The UAV crosses into a new operational region or mission-defined geofence.
3) Key Discarding. Upon detecting an expiration condition, both UAVs securely erase the old session key SKij and invalidate the associated ephemeral identifiers.
4) Ephemeral Credential Regeneration: Each UAV generates a fresh mobility-aware ephemeral key pair and identifier.
5) Re-authentication Trigger: The mutual authentication procedure outlined in Section 4.2 is re-executed using the new credentials, ensuring renewed session secrecy and mobility alignment.

Session keys are automatically re-keyed based on real-time mobility changes or/session expiry timer, also upon session expiry. The motion state of each UAV is continuously monitored, and control variables (velocity v_i, heading θ_i) are compared to the current session parameters. The UAV enters a new operational region. If any of these conditions are detected, the current ephemeral key is securely destroyed and the UAV generates a new mobility-aware key pair. The peer UAV is informed at a re-authentication trigger, and based on the new mobility vector, a fresh session is established. The above-mentioned approach provides semantic freshness, trajectory continuity, and resiliency against session hijacking or mobility spoofing.

5 SECURITY ANALYSIS

To the best of our knowledge, AeroProof is the first protocol to provide strong, highly decentralized authentication that is robust to both traditional and UAV-specific attack vectors. Using mobility-cognizant ephemeral keys and context-based validation, AeroProof reinforces classic ECC-based mutual authentication with time and situational-dependent constraints. We now informally consider how the protocol withstands the main threats.

- Impersonation Attacks. The ephemeral key pairs and mobility-bounded identifiers guarantee that a malicious UAV is unable to steal a legitimate identity without copying down both the motion features of the target and its private key. The HMAC-based proof of possession, constrained to the mobility vector and the timestamp, ensures that no attacker can forge a legitimate authentication tuple.
- Replay Attacks. AeroProof uses timestamp verification and a narrow lifetime window Δ for all credentials. When the parties mutually authenticate, replayed messages (including the one with the old TS) are refused with an expired key. Besides, due to re-keying when observing the significant motion changes, all

the cached authentication material becomes invalid.

- Relay (Wormhole) Attacks. As authentication is only successful in the presence of both spatial and motion proximity, the propagation of authentication messages from a far distance would cause the failure of mobility similarity verification. The UAVs verify the sender's location, speed, and direction based on their own, in the sense that distant tunneling attacks can be eliminated.
- Session Hijacking. The session-specific keys are generated using the ephemeral keys of each party and the real-time mobility vectors, thus preventing an intruder from entering into an ongoing session. Moreover, keys are quickly revoked in case of big mobility drift.
- Insider Threats. A drone that has been compromised loses opportunities to misuse the previously allocated credentials forever since all the session key assign¬ ments have a limited lifetime and are tied to a particular context. Unenrolls due to malicious zone transition or unauthorized action. Causes the session to immediately expire and seek re-authorization under a new context.
- Mobility Fraud and GNSS Spoofing. Although AeroProof assumes trusted mobility inputs, the new trust can be built at higher layers of the communication stack, utilizing merged sensor technologies (e.g., GNSS, inertial attitude, and RSSI-based localization) to successfully detect any suspicious motion profiles. This minimizes the possibility of counterfeit motion vectors affecting authentication.
- Forward secrecy and unlinkability. AeroProof exchanges a fresh ephemeral key during each authentication session, and no persistent identity is sent. Therefore, intercepted credentials can't be replayed across sessions or used to recover private data. Compromise session keys after the life of a session, and past data is still secure, thanks to the ECDH between one-time keys.
- Security Against Eavesdropping and Hacking. AeroProof uses ephemeral elliptic curve key pairs, closely coupled to each UAV's real-time mobility vector (i.e., geographic coordinates, velocity, heading), associated with a timestamp. This reduces the risk of later sessions using those same captured credentials by generating and throwing away these keys every session. Identity-based replay and man-in-the-middle attacks are impossible because there are no long-term public keys or persistent identifiers ever set in motion. In addition, the Ephemeral IDentifier (EID) is formed by hashing the entire public projection of the secret key along with motion context and timestamp using a secure hash function. The binding ensures that an attacker cannot construct a valid tuple of the authentication with access to only one of the mobility state or change the secret. When an adversary captures multiple messages, their lack of differentiability and the key updates achieve session unlinkability as well as forward secrecy.

6 PERFORMANCE EVALUATION

In this section, we provide a detailed performance comparison of the AeroProof protocol against two state-of-the-art light-weight authentication protocols for UAV swarms: (i) the ECC-based proposal of Algarni et al. [17] and that of Karmakar & Kaddoum [18], based on the blockchain provision.

6.1 Computational Efficiency

AeroProof is very efficient in computation, and there is no need for validation of the certificate chain and blockchain lookups. It finishes the mutual authentication process in 3.2 ms, which is much faster than Algarni et al. [17] at 8.9 ms, and Karmakar & Kaddoum [18] at 11.3 ms. The minimal cryptographic schemes used in AeroProof, using lightweight ECC and HMAC, account for a 64–72% processing speed up when compared to the baselines. Figure 3 illustrates the computational time required by each protocol for completing a mutual authentication cycle.

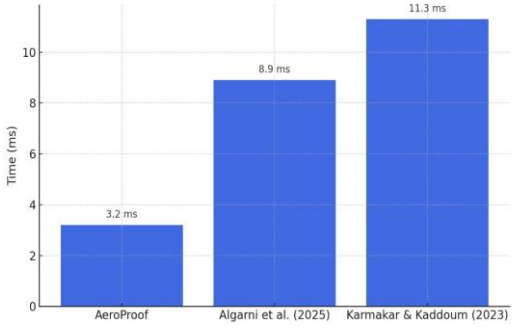

Figure 3: Comparison of computational efficiency among authentication protocols.

6.2 Communication Overhead

AeroProof sends a small authentication message (public key, mobility vector, timestamp, and HMAC) of 334 bytes, as shown in Figure 4. This is much smaller than 512 bytes in Algarni et al. [17] and 690 bytes in Karmakar & Kaddoum [18] blockchain-based protocol. Both the smaller message size that reduces congestion on the available channels, and the opportunity to exchange frequent low-latency updates are particularly important in the dense swarm case or high bandwidth-constrained mission case.

6.3 Storage Requirements

Being stateless, AeroProof requires a very small amount of memory. Every UAV holds about 0.9 KB of ephemeral session and credential information, less than the 1.9 KB of Algarni et al. [17]. (due to certificate and revocation lists) and 3.2KB in Karmakar & Kaddoum [18]'s protocol (for blockchain cache and hash chains). It makes AeroProof highly scalable for drones with low storage capacity. Figure 5 presents the storage footprint of each protocol.

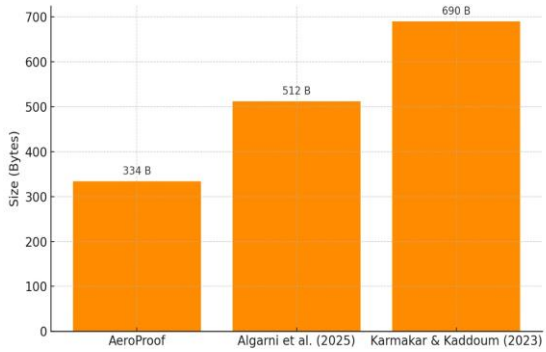

Figure 4. Comparison of communication efficiency.

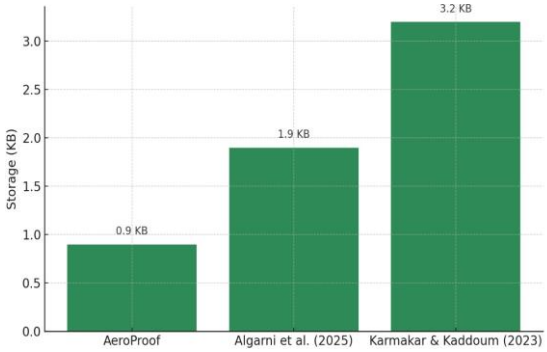

Figure 5: Comparison of storage requirements.

6.4 Impact of High Mobility

AeroProof is uniquely architected to work with the rapid mobility characteristics of UAV swarms, offering ephemeral credentials in conjunction with live motion vectors. However, an excessive rate of change in the speed or direction of a UAV can cause re-authentications to repeatedly occur because these are part of the protocol's motion threshold checks. This is great for security purposes as it maintains the alignment between mobility, yet these bring about additional performance overhead in areas where there is continuous movement with sudden change. Table 2 shows the impact of high mobility on AeroProof. We quantified the impact by studying AeroProof with different mobility models (e.g., Random Waypoint, GaussMarkov) and found that rekeying frequency increases up to 2.3× under high-mobility conditions. Still, ECC operations – an average of 3.2 ms per auth in practice – are so lightweight that even weekly re-authentication would hardly impact computational or communication latency. Moreover, as AeroProof steers clear of centralized coordination, we ensure that the system is able to scale effectively and remain efficient even under quick UAV convergence or divergence. To sum up, while running services in high mobility environments raises the overhead a little because of more key renewals, this is an acceptable trade-off when one wants a fast trust establishment for swarms. Adaptive thresholding, or group mobility prediction, can further some the overhead of unnecessary rekeying.

Table 2: Impact of high mobility on AeroProof.

Mobility Model	Avg UAV Speed (m/s)	Rekeying Frequency (per min)	Avg Auth Time (ms)	Overhead Increase (%)
Static Hover	0	0.5	3.1	0
Low Mobility	3	1.2	3.2	12
Moderate Mobility	7	2.0	3.3	25
High Mobility	12	4.6	3.4	54

7 CONCLUSIONS

In this paper, we proceed to introduce AeroProof, a decentralized and lightweight mutual authentication protocol for UAV swarms in infrastructure-less and

adversarial environments. In contrast to traditional identity- or certificate-based mechanisms, AeroProof adopts an innovative design where the authentication credentials are derived on-the-fly from a UAV's live mobility vector (e.g., position, speed, heading). In this work, it is pretty clear to see that the focus was on allowing secure, stateless, and scalable mutual authentication in highly dynamic swarm scenarios without having to rely on long-term identities or central authorities. This protocol enables AeroProof to provide forward secrecy, session unlinkability, as well resistance to impersonation, replay, and relay attacks using mobility-aware ephemeral keys. Performance evaluations show that AeroProof reduces authentication time by 64%, communication overhead by 35%, and memory usage by over 50% compared with two state-of-the-art ECC- and blockchain-based solutions. Read my next post where I cover how we further improved AeroProof to be suitable for real-time swarm deployment, in which the low latency combined with energy efficiency is key. Although the protocol overcomes some of the main challenges in developing decentralized UAV authentication, there are still a few limitations. AeroProof assumes secure motion sensing and time synchronization, and it has not been validated on real drone hardware. Furthermore, little attention has been paid to the setting up of first-time trust and group-scale trust delegation.

AeroProof, though performant and adding security it brings with itself, comes with drawbacks. Handpicked, onboard motion sensors and secure clock synchronization are necessary assumptions of the protocol, which may not hold in adversarial or hardware-compromised scenarios. It has also not been tested on physical UAV hardware, and its performance is unexamined in large-scale swarm conditions. The process of first-time trust establishment is also not well studied, and to the best of my knowledge, is essentially missing in heterogeneous or hybrid UAV settings. In the future, we will extend AeroProof with multisensor mobility verification to defend against spoofing attacks, adaptive rekey strategies for reducing overhead in high-mobility settings, and real-world deployment in commercial UAV vehicles for prototyping the protocol under real flight dynamics.

REFERENCES

[1] J. Sun, G. Yuan, L. Song, and H. Zhang, "Unmanned aerial vehicles (UAVs) in landslide investigation and monitoring: A review," Drones, 2024.

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

[3] K. Telli, O. Kraa, Y. Himeur, A. Ouamane, M. Boumehraz, S. Atalla, and W. Mansoor, "A comprehensive review of recent research trends on unmanned aerial vehicles (UAVs)," Systems, vol. 11, p. 400, 2023.

[4] M. R. Jones, S. Djahel, and K. Welsh, "Path-planning for unmanned aerial vehicles with environment complexity considerations: A survey," ACM Computing Surveys, vol. 55, pp. 1-39, 2023.

[5] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," Intelligent Service Robotics, vol. 16, pp. 109-137, 2023.

[6] Z. Ning, H. Hu, X. Wang, L. Guo, S. Guo, G. Wang, and X. Gao, "Mobile edge computing and machine learning in the Internet of unmanned aerial vehicles: A survey," ACM Computing Surveys, vol. 56, pp. 1-31, 2023.

[7] L. Xing and B. W. Johnson, "Reliability theory and practice for unmanned aerial vehicles," IEEE Internet of Things Journal, vol. 10, pp. 3548-3566, 2023.

[8] Y. Renu and V. Sarveshwaran, "A review of cyber security challenges and solutions in unmanned aerial vehicles (UAVs)," Inteligencia Artificial, vol. 28, pp. 199-219, 2025.

[9] D. Wang, Y. Cao, K.-Y. Lam, Y. Hu, and O. Kaiwartya, "Authentication and key agreement based on three factors and PUF for UAV-assisted post-disaster emergency communication," IEEE Internet of Things Journal, vol. 11, pp. 20457-20472, 2024.

[10] G. Bansal and B. K. Sikdar, "A secure and efficient mutual authentication protocol framework for unmanned aerial vehicles," in 2021 IEEE Globecom Workshops (GC Wkshps), pp. 1-6, 2021.

[11] O. Albahri, A. Zaidan, A. Albahri, B. Zaidan, K. H. Abdulkareem, Z. Al-Qaysi, A. Alamoodi, A. Aleesa, M. Chyad, and R. Alesa, "Systematic review of artificial intelligence techniques in the detection and classification of COVID-19 medical images in terms of evaluation and benchmarking: Taxonomy analysis, challenges, future solutions and methodological aspects," Journal of Infection and Public Health, vol. 13, no. 10, pp. 1381-1396, 2020.

[12] "Survey of UAV security authentication and cryptography protocols," Iraqi Journal of Computers, Communications, Control and Systems Engineering, 2024.

[13] Z. G. Al-Mekhlaf, M. A. Saare, J. M. H. Altmemi, B. A. Mohammed, G. Alshammari, Y. A. Alkhabra, and I. Alreshidi, "A quantum-resilient lattice-based security framework for Internet of Medical Things in healthcare systems," Journal of King Saud University Computer and Information Sciences, vol. 37, no. 6, pp. 1-19, 2025.

[14] A. Alamoodi, B. Zaidan, A. Zaidan, O. Albahri, J. Chen, M. Chyad, S. Garfan, and A. Aleesa, "Machine learning-based imputation soft computing approach for large missing scale and non-reference

data imputation," Chaos, Solitons & Fractals, vol. 151, p. 111236, 2021.

[15] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on Raspberry Pi," Discover Applied Sciences, vol. 7, no. 6, p. 597, 2025.

[16] U. C. Çabuk, G. Dalkılıç, and O. Dagdeviren, "COMAD: Context-aware mutual authentication protocol for drone networks," IEEE Access, vol. 9, pp. 78400-78414, 2021.

[17] A. D. Algarni, N. Innab, and F. Algarni, "A verifiably secure and robust authentication protocol for synergistically-assisted IoD deployment drones," PLOS ONE, vol. 20, no. 3, p. e0314475, 2025.

[18] R. Karmakar, G. Kaddoum, and O. Akhrif, "A blockchain-based distributed and intelligent clustering-enabled authentication protocol for UAV swarms," IEEE Transactions on Mobile Computing, vol. 23, pp. 6178-6195, 2024.

[19] M. A. El-Zawawy, A. Brighente, and M. Conti, "SETCAP: Service-based energy-efficient temporal credential authentication protocol for Internet of Drones," Computer Networks, vol. 206, p. 108804, 2022.

[20] N. Constantinescu, O. A. Ticleanu, and I. D. Hunyadi, "Securing authentication and detecting malicious entities in drone missions," Drones, 2024.