PureChain-Enabled Privacy-Preserving Handover Authentication for LEO Networks

Abdul Samim [1], Love Allen Chijioke Ahakonye [2], Jae Min Lee [1], Dong-Seong Kim [1] *
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
* NSLab Co. Ltd. *Kumoh National Institute of Technology*, Gumi, South Korea
samimbaloch1@gmail.com, (loveahakonye, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Frequent handovers in Low-Earth-Orbit (LEO) networks increase latency when authentication relies on off-path authorities. We present PureChain, a privacy-preserving handover authentication scheme that separates identity from mobility using transferable anonymous tokens and a proof-of-authority and association (PoA^2) consensus. Simulations indicate that reducing protocol latency from 1.3s to 0.9s improves handover success by 2-3dB. Under Byzantine conditions, PoA^2 achieves sub-second finality (150–325ms at 0–30% adversaries), outperforming PBFT by 35-55% and classic proof-of-authority by 10%. On-chain load scales efficiently at 0.02 KB/user per minute, 89% lower than write-every-handover baselines. These results demonstrate PureChain's potential for anonymity, auditability, and scalability in large-scale Non-Terrestrial Networks.**

***Index Terms*—Blockchain, Handover authentication, Non-Terrestrial Networks (NTN), PoA^2, PureChain.**

I. Introduction

Low Earth Orbit (LEO) mega-constellations deliver low round-trip latency but force frequent beam/satellite handovers; recent studies show that high Handover (HO) rates inflate signaling overhead and tail delays, jeopardizing session continuity [1]. Although 3GPP Releases 17–18 formally integrate non-terrestrial networks (NTN), mobility and security across discontinuous coverage remain in active evolution [2], making it critical to avoid off-path round-trip delays during HO [3]. Classical Authentication and Key Agreement (AKA)/Elliptic Curve Cryptography (ECC)-style authentication can repeatedly expose identifiers leaking mobility patterns and add delay when validation depends on distant authorities, as documented in recent satellite/Non-terrestrial Network (NTN) security surveys and demonstrated by location-privacy attacks [4].

Blockchain enhances auditability and anonymity in access control [5]; however, recording every handover HO on-chain incurs delays and overhead. Recent satellite-network prototypes therefore favor lightweight, selective on-chain use [6]. Energy-intensive schemes like PoW are unsuitable for time-critical NTN, whereas permissioned proof-of-authority variants offer rapid finality with modest compute and are evolving to counter validator risks [6]. Building on this, we employ PureChain with proof-of-authority and association (PoA^2) [7], which preserves anonymity via transferable, unlinkable transactions, maintains "hot" HO paths through edge-local verification, and limits on-chain activity to refresh, revocation, and rotation, an approach aligned with orbital edge-computing that pushes trust and computation to the network edge.

II. Methodology

Figure 1 presents the proposed system of the HO authentication framework for non-terrestrial LEO networks, which couples an edge-first control plane with the permissioned PureChain ledger. At initial attachment, the ledger issues a batch of one-time, transferable, unlinkable tokens (TUTs) to each User Equipment (UE); every token carries its scope, a short expiry time T_{exp}, a rotation counter, and a nonce. It is signed under the current PoA^2 epoch key. Gateways/Handover Controllers (HCs) cache a revocation bitmap, a token Bloom filter, and the PoA^2 checkpoint so that, upon an HO trigger, the HC verifies the presented token locally (signature vs. checkpoint, not-revoked/not-spent, and within-expiry) and completes the HO without contacting the chain in the typical case.

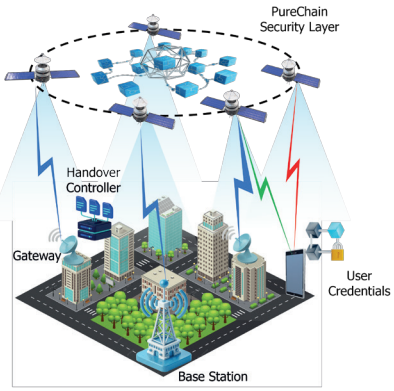

Fig. 1. PureChain backed LEO handover

On-chain writes are limited to three cases: Refresh (token top-up), Revocation (misuse), and Rotation (epoch changes), all secured by PoA^2 fast finality with periodic checkpoints. Edge nodes validate tokens within a safe staleness window W_s, fetching updated checkpoints only after W_s expires. By tuning batch size B, expiry T_{exp}, and W_s, the system achieves 90–95% cache-only handovers, significantly lowering p90/p99 latency and radio pause while maintaining privacy, replay/clone resistance, and auditable revocation. Evaluation covers latency distributions (p50/p90/p99), handover success,

cache-hit and exception ratios, and revocation responsiveness under mobility and Byzantine delays, benchmarked against per-handover AKA/ECC and naïve ledger-write baselines. Figure 2 illustrates the workflow.

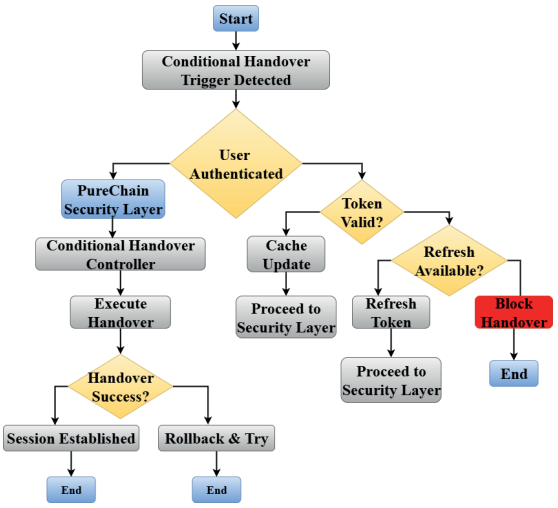

Fig. 2. PureChain backed LEO handover

III. Experimental Results and Discussion

Our results show that PureChain improves mobility by lowering the radio margin needed for reliable handovers. The handover–success curves follow the expected logistic rise with SINR but shift left as authentication latency decreases: at 5dB, success rates are ≈0.82 (0.9s), ≈0.75 (1.1s), and ≈0.60 (1.3s). At the 95% reliability target, the threshold moves from 10 dB (0.9s) to 12 dB (1.1s) and 13 dB (1.3s), confirming that faster authentication directly reduces the SINR required for seamless mobility.

Under adversarial conditions, PoA^2 sustains sub-second consensus finality while outperforming alternatives. Finality remains ≈150/250/325ms at 0/20/30% Byzantine validators, compared with ≈180/280/350ms for classic PoA and ≈250/510/730 ms for PBFT. Ledger overhead scales linearly with users but is an order of magnitude lighter than a write-every-handover baseline (≈0.02 KB user^{-1} min^{-1} vs. ≈0.18 KB). An off-chain plus periodic commit variant is lightest (≈0.004 KB user^{-1} min^{-1}), though at the cost of deferred confirmation. Taken together, these results highlight PoA^2 as an effective radio–security co-design point, balancing reliability, resilience, and scalability for large-scale LEO handover authentication.

IV. Conclusion

We presented PureChain-enabled privacy-preserving handover authentication for LEO networks, which unifies anonymous tokens with PoA^2 consensus mechanism. The approach achieves lower protocol latency, sub-second consensus finality, and 89% reduced on-chain load, outperforming PBFT and classic proof-of-authority while preserving radio reliability and scalability. These results establish PureChain as a practical foundation for large-scale NTN mobility with anonymity, auditability, and rapid admission. While our evaluation is simulation-based and does not capture all real-world dynamics, future work will validate the system on hardware-in-the-loop testbeds, extend to multi-orbit and extreme-mobility regimes, co-design radio/ledger scheduling with adaptive batching, and strengthen guarantees on energy, cost, privacy, and availability under more powerful adversaries.

TABLE I
Unified performance summary for PureChain. Values are read from plots; "∼" denotes approximate.

(A) Handover success probability			
SINR (dB)	0.9 s	1.1 s	1.3 s
0	∼0.45	∼0.36	∼0.28
3	∼0.64	∼0.54	∼0.44
5	∼0.82	∼0.75	∼0.60
10	∼0.95	∼0.92	∼0.90
(B) Consensus finality (ms) vs Byzantine validators			
Byz. %	PoA^2	PoA classic	PBFT
0	∼150	∼180	∼250
10	∼195	∼230	∼355
20	∼250	∼280	∼510
30	∼325	∼350	∼730
(C) On-chain overhead (KB/min)			
Users	PureChain	Baseline	Off-chain+periodic
100	∼2.0	∼18.0	∼0.5
500	∼10.0	∼88.0	∼2.0
1000	∼20.0	∼179.0	∼4.0

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] S. S. S. G. Seeram, L. Feltrin, M. Ozger, S. Zhang, and C. Cavdar, "Handover Challenges in Disaggregated Open RAN for LEO Satellites: Tradeoff Between Handover Delay and Onboard Processing," *Frontiers in Space Technologies*, vol. 6, p. 1580005, 2025.

[2] J. Krause, "Non-Terrestrial Networks (NTN)," 3GPP website, 3rd Generation Partnership Project (3GPP), May 2024, last updated 2025-07-04; Accessed 2025-09-25. [Online]. Available: https://www.3gpp.org/technologies/ntn-overview

[3] S. Yao, X. Zhang, and J. Xu, "A Blockchain-Based Lightweight Privacy-Preserving Authentication Protocol for Access and Handover in Space-Ground Integrated Networks," in *Proceedings of the 2025 5th International Conference on Computer Network Security and Software Engineering*, ser. CNSSE '25. New York, NY, USA: Association for Computing Machinery, 2025, p. 50–58.

[4] M. Kang, S. Park, and Y. Lee, "A Survey on Satellite Communication System Security," *Sensors*, vol. 24, no. 9, 2024.

[5] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[6] M. Arshad, L. Jianwei, M. Khalid, W. Khalid, Y. Cao, and F. A. Khan, "Access authentication via blockchain in space information network," *Plos one*, vol. 19, no. 3, p. e0291236, 2024.

[7] D.-S. Kim, I. S. Igboanusi, L. A. Chijioke Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*, 2025, pp. 1–6.