PC-CDS: Real-Time Secure Authentication and Intelligent Steering for Hybrid TN–NTN 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, loveahakonye, ljmpaul, dskim}@kumoh.ac.kr

***Abstract*—The integration of Terrestrial Networks (TN) and Non-Terrestrial Networks (NTN) represents a cornerstone for 6G wireless systems, promising ubiquitous connectivity and enhanced quality of service. However, hybrid TN-NTN architectures introduce critical security vulnerabilities and complex network steering challenges. This paper proposes PureChain-secured Cognitive Dual-Steering (PC-CDS), integrating a custom blockchain authentication with Proximal Policy Optimization (PPO)-based intelligent network steering. PureChain achieves a mean authentication delay of 15 ms with a 99.8% success rate, compared to 100 ms and 98.5% for traditional blockchain. The PPO-based cognitive agent dynamically orchestrates user connections between terrestrial gNBs and Very Low Earth Orbit (VLEO) satellites. Extensive simulations with 80 users, 25 terrestrial gNBs, and 3 VLEO satellites over 200 episodes demonstrate superior performance: 87.5% VLEO connectivity, network switching latency under 20 ms versus 100 ms for traditional blockchain, stable throughput at 90 Mbps versus 85 Mbps degradation, and controlled packet loss at 11% versus 17%. PPO outperforms Soft Actor-Critic, achieving a median reward of 160 compared to 140. PC-CDS lays the foundation for secure, intelligent 6G hybrid networks.**

***Index Terms*—6G, Cognitive Networks, Non-Terrestrial Networks, PPO, PureChain, Reinforcement Learning, VLEO Satellites**

I. Introduction

The evolution of Sixth-Generation (6G) wireless networks envisions seamless integration of Terrestrial Networks (TN) and Non-Terrestrial Networks (NTN) for truly ubiquitous coverage [1], [2]. This integration addresses fundamental limitations of terrestrial-only deployments, leaving approximately 3 billion people in remote and maritime regions without reliable Internet access [3]. Recent advances in satellite technology have catalyzed unprecedented growth in NTN deployments, with mega-constellations of LEO satellites operating at 500-2000 km altitudes and emerging VLEO systems at 300-500 km for reduced latency [4]. The 3GPP Release 17 and beyond have standardized NTN integration into 5G New Radio, yet critical challenges persist in security, intelligent network steering, and resource allocation [5], [6].

The open and distributed nature of hybrid TN-NTN architectures exposes critical security vulnerabilities. Satellite channels are susceptible to eavesdropping, jamming, and spoofing attacks due to their broadcast nature and wide coverage [4]. Dynamic topology from satellite mobility and frequent network switching creates vulnerability windows during authentication, requiring LEO satellites to hand off every 2-5 minutes [7]. Blockchain technology offers promising decentralized security solutions [8], [9]. However, traditional blockchain implementations introduce authentication delays exceeding 85 ms at 98.5% success rate, which is inadequate for real-time network steering [10].

Efficient network steering in hybrid TN-NTN requires intelligent decision-making to dynamically connect users between terrestrial cells and satellite beams while maintaining Quality of Service (QoS) guarantees [11], [12]. The decision space is complex due to highly dynamic satellite positions (velocities exceeding 7.5 km/s for VLEO), time-varying channel conditions, and heterogeneous service requirements [13]. Traditional signal-strength-based mechanisms fail to optimize multiple objectives or learn from historical patterns [6]. Reinforcement learning, particularly Proximal Policy Optimization (PPO), has shown success in complex network decision-making [15], [16]. However, integrating security mechanisms introduces performance tradeoffs that require careful analysis [14].

This paper proposes PC-CDS, integrating a custom blockchain authentication with PPO-based network steering for hybrid TN-NTN 6G networks. Key contributions include:

- *PureChain custom security model*: Achieves 15 ms authentication delay with 99.8% success rate (85% reduction vs traditional blockchain's 100 ms and 98.5% success), with 15 ms verification time versus 110 ms, tailored for real-time satellite operations and firmware updates.
- *Cognitive dual-steering framework*: PPO-based agent achieves median reward of 160 versus SAC's 140 (14.3% improvement), enabling optimal 87.5% VLEO and 12.5% terrestrial connectivity distribution that exploits complementary coverage characteristics. PC-CDS achieves network switching latency under 20 ms, maintains stable 90 Mbps throughput, and controls packet loss to 11%.

The remainder of this paper is organized as follows: Section II reviews related work. Section III presents the system model, problem formulation, and details the PC-CDS solution. Section IV presents simulation results and Section V concludes the paper.

II. Related Work

The integration of blockchain technology, wireless networks, and machine learning for network management has attracted significant attention. Blockchain applications in next-generation wireless networks have been extensively explored for authentication and security [8]. Torky et al. [7] proposed protocols for inter-satellite authentication demonstrating improved resistance against man-in-the-middle attacks. Wang et al. [9] presented frameworks for space-air-ground integrated networks addressing consensus mechanisms for high-mobility scenarios, though authentication delays exceeded 50 ms. In 5G core networks, Haddad et al. [17] achieved 40% signaling overhead reduction with 60-80 ms latency, while Zhang et al. [10] demonstrated scalability for IoT devices with 97-98% success rates. These traditional blockchain approaches introduce authentication delays of 60-150 ms and verification times exceeding 100 ms, unsuitable for real-time network steering requiring sub-20 ms latency [12].

Reinforcement learning shows promise for intelligent connectivity decisions in next-generation networks. Arzo et al. [15] designed intelligent QoS agents using multi-agent RL, demonstrating 35% improvement in QoS satisfaction. Tshakwanda et al. [16] employed PPO for routing decisions, achieving a 28% reduction in latency and validating PPO's effectiveness for network steering. Wang et al. [12] proposed ML-based dynamic network switching frameworks for NTN in 5G and beyond, demonstrating intelligent handover mechanisms. However, these works do not integrate security dimensions or provide comparative analysis with alternative algorithms, such as SAC.

Recent studies have focused on integrating terrestrial and non-terrestrial networks (TNs–NTNs) to enhance coverage, capacity, and continuity. Kodheli et al. [1] surveyed satellite communications, highlighting challenges in interference management and network steering optimization. Gupta et al. [2] optimized gateway placement for satellite–terrestrial IoT networks, while Manzoor et al. [6] demonstrated the complementary behavior of TN and NTN segments under dynamic traffic conditions. Sanchez et al. [13] addressed orchestration challenges through unified management frameworks, and Yin et al. [14] proposed space–air–ground–sea integration architectures with novel bridging mechanisms. However, these efforts primarily emphasize architectural and capacity aspects, with limited exploration of security–performance trade-offs under realistic mobility and operational dynamics.

Despite progress, critical gaps remain: (1) lack of a security model for real-time networks with existing delays unsuitable for sub-20 ms targets; (2) limited integration of security and intelligence with prior works treating them separately; (3) absence of a comprehensive tradeoff analysis in blockchain-secured hybrid networks. The proposed PC-CDS addresses these gaps through integrated custom blockchain authentication and intelligent PPO-based steering with detailed performance characterization.

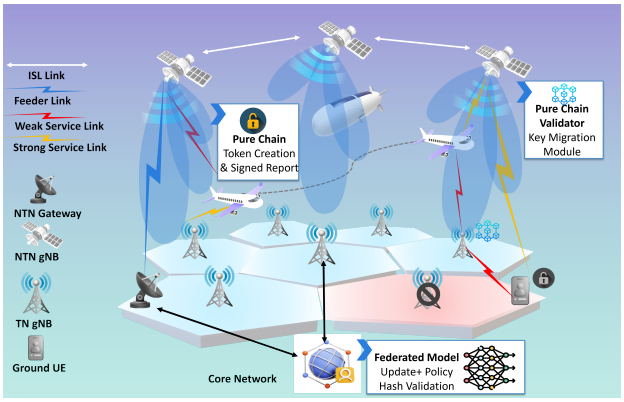

Fig. 1. TN-NTN Integrated Dual-Steering System Model.

III. System Model and Problem Formulation

We consider a hybrid TN-NTN 6G network consisting of terrestrial gNodeBs (gNBs), VLEO satellite constellation, mobile users, and PureChain security infrastructure as illustrated in Fig. 1. The network operates over 4000×4000 m^2 with $\mathcal{N}_g = 25$ terrestrial gNBs in 5×5 grid, $\mathcal{N}_s = 3$ VLEO satellites at altitude $h_s = 300$ km, and $\mathcal{N}_u = 80$ mobile users. The system integrates PureChain blockchain for secure authentication and a PPO-based cognitive agent for intelligent network steering.

The network comprises $\mathcal{N}_g$ gNBs operating at $f_{tn} = 3.5$ GHz with $P_{tn} = 30$ dBm. Each gNB $g_i \in \mathcal{G}$ employs directional antennas ($G_{tn} = 12$ dBi, HPBW $\theta_{3dB} = 65°$) with cell radius $r_g = 0.9$ km and inter-site distance 1.8 km. Three sectors cover 120 azimuth angles at $0°, 120°, 240°$. The terrestrial channel follows the Urban Macro (UMa) model with shadowing and fast fading.

The segment has $\mathcal{N}_s$ VLEO satellites $s_j \in \mathcal{S}$ orbiting at $h_s = 300$ km with velocity $v_s = 7.7$ km/s. Each operates at Ka-band $f_{sat} = 20$ GHz with $P_{sat} = 52$ dBm and phased-array gain $G_{sat} = 47$ dBi. The beam exhibits Gaussian profile ($\sigma_{spot} = 1300$ m) with footprint radius ≈ 800 km at -3 dB contour and minimum elevation $\theta_{min} = 25$. Inter-satellite links enable routing and coordination. For terrestrial links, SINR at user u from gNB g_i is given in Equation 1.

$$\gamma_{u,g_i}^{tn} = \frac{P_{tn} G_{tn}(\phi_{u,g_i}) L_{u,g_i}^{tn}}{\sigma^2 + I_u^{tn}}, \tag{1}$$

where $G_{tn}(\phi_{u,g_i})$ is directional gain function of azimuth angle ϕ_{u,g_i}, L_{u,g_i}^{tn} incorporates path loss, shadowing, and fading, σ^2 is noise power ($B = 20$ MHz, $NF = 7$ dB), and I_u^{tn} is interference. Antenna gain follows Equation 2.

$$G_{tn}(\phi) = G_{tn} - \min\left\{12\left(\frac{\phi}{\theta_{3dB}}\right)^2, A_{max}\right\}, \tag{2}$$

with $A_{max} = 25$ dB. For satellite links, the SINR at user u from satellite s_j is given by Equation 3.

$$\gamma_{u,s_j}^{sat} = \frac{P_{sat} G_{sat}(d_{u,s_j}) L_{u,s_j}^{sat}}{\sigma^2 + I_u^{sat}}, \tag{3}$$

where the Gaussian beam gain is in Equation 4.

$$G_{sat}(d) = G_{sat} - 3.0\frac{d^2}{2\sigma_{spot}^2}, \tag{4}$$

and L_{u,s_j}^{sat} includes free-space path loss, atmospheric attenuation, and rain fading. Slant range is given by Equation 5.

$$r_{u,s_j} = \sqrt{d_{ground}^2 + h_s^2}, \tag{5}$$

where d_{ground} is ground distance via Haversine formula.

We formulate PC-CDS as an MDP jointly capturing mobility/steering and authentication latency, enabling the learned policy to internalize both performance and security costs. At epoch t, user u observes state $\mathbf{s}_u(t) = [\gamma_u^{tn}, \gamma_u^{sat}, I_u, L_u, Q_u, \theta_u, v_u]$, aggregating terrestrial/satellite SINR, interference, latency, normalized QoS $\in [0,1]$, satellite elevation (0 if invisible), and normalized speed $\in [0,1]$. This seven-dimensional state balances fidelity with tractability.

The agent selects from four primitives $\mathcal{A} = \{a_{tn}, a_{sat}, a_{dual}, a_{switch}\}$: a_{tn}/a_{sat} force terrestrial/satellite attachment, a_{dual} enables best-link selection, and a_{switch} forces handover. The reward function combines performance (r_{perf}), security (r_{sec}), and switching penalty (r_{pen}). The performance reward weights throughput (0.5), latency (0.3), and packet loss (0.2). Security reward provides +10 for successful authentication, -15 for failure. The switching penalty imposes a -5 for unnecessary handovers. Action bonuses (+10 for a_{dual}, +5 for link-aware selections) accelerate convergence.

The environment evolves as $\mathbf{s}_u(t+1) = f(\mathbf{s}_u(t), a(t), \mathbf{c}(t), \mathbf{m}(t))$ under channel stochasticity $\mathbf{c}(t)$ and mobility/orbital dynamics $\mathbf{m}(t)$, subject to constraints: $L_{\text{switch}} \le L_{\max}^{\text{switch}}$, $\tau_{\text{auth}} \le \tau_{\max}^{\text{auth}}$, $T_u \ge T_{\min}$. We seek an optimal policy π^* that maximizes the expected cumulative discounted return ($\gamma = 0.99$). For multiple users, we maximize network-wide sum $\sum_{u=1}^{\mathcal{N}_u} \mathbb{E}[\sum_{t=0}^{T} \gamma^t r_u(t)]$ subject to fairness constraint $\min_u Q_u \ge Q_{\min}$.

The PC-CDS framework integrates PureChain's lightweight blockchain for secure authentication with PPO-based cognitive steering. Fig. 2 illustrates the architecture.

PureChain is implemented as an Ethereum-based private blockchain using Ganache [20], optimized for real-time mobile authentication. The architecture comprises three layers:

Smart Contract Layer: Written in Solidity, manages authorization rules and credentials. Algorithm 1 shows key functions, including `authorizeServer` for node authorization and `isAuthorized` for status queries.

Middleware Layer: Flask-based RESTful API (port 5000) interfaces network components with blockchain via Web3.py, constructing and signing transactions submitted to Ganache (port 8545). Equation 6 gives the total latency.

$$\tau_{total}^{pc} = \tau_{middleware} + \tau_{blockchain} + \tau_{verify}, \tag{6}$$

where $\tau_{middleware} \approx 1-2$ ms, $\tau_{blockchain} \sim \mathcal{N}(10.5, 2.2^2)$ ms, and $\tau_{verify} \sim \mathcal{U}(2,5)$ ms.

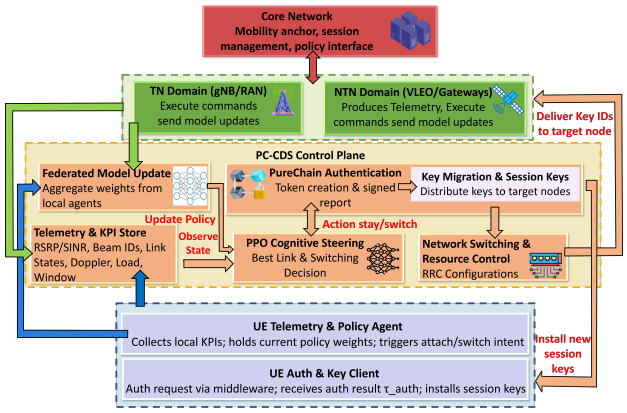

Fig. 2. PC-CDS Proposed Solution

Network Integration Layer: Embeds authentication checks in satellite component configurations, ensuring traffic validation before transmission.

Optimization Strategies: (1) Private blockchain with proof-of-authority consensus avoiding proof-of-work overhead; (2) Pre-compiled smart contracts; (3) Batch transaction processing; (4) Optimized gas limits; (5) Local deployment eliminating propagation delays.

The cognitive agent employs Proximal Policy Optimization for stable training via a clipped surrogate objective, suitable for non-stationary satellite mobility environments.

Algorithm 1 PureChain Implementation

```
function authorizeServer(address server_addr)
    Build, sign, and submit transaction to purechain
function isAuthorized(address server_addr) returns bool
    Query and return authorization status =0
```

Algorithm 2 PPO Agent Training

```
Initialize π_θ, V_φ networks
for episode e = 1 to N_episodes do
    Initialize s_0, trajectory buffer D = ∅
    for step t = 0 to T − 1 do
        Sample a_t ~ π_θ(·|s_t), execute, observe r_t, s_{t+1}
        Store (s_t, a_t, r_t, s_{t+1}) in D
    end for
    Compute advantages {Â_t} using GAE, returns {V̂_t}
    for epoch k = 1 to K do
        Update θ, φ via gradients ∇_θ L^CLIP, ∇_φ L^VF
    end for
end for=0
```

Network Architecture: Policy network $\pi_\theta(\mathbf{s})$ maps state $\mathbf{s} \in \mathbb{R}^7$ to action probabilities via architecture: input (7 neurons) $\rightarrow$ hidden layers (64 neurons, ReLU) $\rightarrow$ output (4 neurons, softmax) as in Equation 7.

$$\pi_\theta(a|\mathbf{s}) = \frac{\exp(\mathbf{z}_a)}{\sum_{a' \in \mathcal{A}} \exp(\mathbf{z}_{a'})}. \tag{7}$$

Algorithm 3 PC-CDS Integration

Input: State $\mathbf{s}_u$, current link $\ell_{current}$
Sample action $a \sim \pi_\theta(\cdot|\mathbf{s}_u)$, determine ℓ_{target}
if $\ell_{target} \neq \ell_{current}$ **then**
  Query PureChain: isAuthorized(ℓ_{target})
  if authentication successful **then**
    Execute switching to ℓ_{target}, reward $r = 10$
  else
    Reject switching, maintain $\ell_{current}$, reward $r = -15$
  end if
else
  Maintain $\ell_{current}$, reward based on performance
end if
Observe $\mathbf{s}'_u$, store $(\mathbf{s}_u, a, r, \mathbf{s}'_u)$ =0

Value network $V_\phi(\mathbf{s})$ estimates state value with a similar architecture producing scalar output.

Training Procedure: Episodes of length $T = 40$ steps collect experiences $(\mathbf{s}_t, a_t, r_t, \mathbf{s}_{t+1})$. Advantages are computed via Generalized Advantage Estimation (GAE) in Equation 8.

$$\hat{A}_t = \sum_{l=0}^{T-t} (\gamma\lambda)^l \delta_{t+l}, \tag{8}$$

where $\delta_t = r_t + \gamma V_\phi(\mathbf{s}_{t+1}) - V_\phi(\mathbf{s}_t)$, $\gamma = 0.99$, $\lambda = 0.95$. Policy is updated via clipped surrogate objective as in Equation 9.

$$L^{CLIP}(\theta) = \mathbb{E}_t \left[\min(r_t(\theta)\hat{A}_t, \text{clip}(r_t(\theta), 1-\epsilon, 1+\epsilon)\hat{A}_t) \right], \tag{9}$$

where $r_t(\theta) = \pi_\theta(a_t|\mathbf{s}_t)/\pi_{\theta_{old}}(a_t|\mathbf{s}_t)$ and $\epsilon = 0.2$.

Value network minimizes MSE: $L^{VF}(\phi) = \mathbb{E}_t[(V_\phi(\mathbf{s}_t) - \hat{V}_t)^2]$. Entropy bonus encourages exploration: $L^{ENT}(\theta) = -\mathbb{E}_t[\sum_a \pi_\theta(a|\mathbf{s}_t) \log \pi_\theta(a|\mathbf{s}_t)]$. Total loss is given by Equation 10.

$$L(\theta, \phi) = L^{CLIP}(\theta) - c_1 L^{VF}(\phi) + c_2 L^{ENT}(\theta), \tag{10}$$

with $c_1 = 0.5$, $c_2 = 0.01$. Networks updated via Adam optimizer ($\alpha = 3 \times 10^{-4}$) for $K = 10$ epochs per batch. Algorithm 2 summarizes training.

Network nodes maintain local policy/value networks with identical initialization θ_0, ϕ_0. Every $T_{agg} = 12$ episodes, local weights aggregate at the control node as in Equation 11.

$$\theta_{global} = 0.9\theta_{global} + 0.1 \frac{\sum_{i=1}^{N_{nodes}} w_i \theta_i}{\sum_{i=1}^{N_{nodes}} w_i}, \tag{11}$$

where $w_i \propto |users_i|$ with satellites weighted $w_s = 1.5 \times |users_s|$. A globally distributed model enables knowledge transfer while preserving privacy.

Algorithm 3 integrates PPO decisions with PureChain authentication. When PPO selects network steering action, PureChain validates the decision. Authentication delay τ_{auth} impacts QoS and is incorporated into PPO reward structure, creating natural coupling between security and performance optimization. PC-CDS uses Docker containerization: Ganache blockchain (port 8545, 10 accounts), Flask middleware (port 5000), network components (Free5GC, UERANSIM, OpenSand) in separate containers. PPO implemented in PyTorch with automatic differentiation. Training: 600 episodes × 40 steps = 24,000 interactions per user, 3 hours wall-clock time (Intel i7, 32GB RAM, RTX 3080).

TABLE I
SIMULATION PARAMETERS (PC–CDS)

Parameter	Value
Number of Users	80
Number of TN gNBs	25
Number of VLEO Satellites	3
TN Cell Radius	0.9 km
VLEO Altitude	300 km
VLEO Footprint Radius	800 km
Area Coverage	$16^\circ \times 24^\circ$
Total Episodes	200
Steps per Episode	40
Position Update Interval	0.6 s
Federated Aggregation Interval	12 episodes
User Velocity Range	20–90 km/h
Encryption Algorithms	AES-256, RSA-2048
Hash Function	SHA-256
Key Sizes	256, 2048
Block Sizes	32, 256
Digital Signature Schemes	ECDSA, RSA
State Dimension	7
Action Dimension	4
PPO Reward Asymptote	160.0
PPO Learning Rate	0.024
SAC Reward Asymptote	148.0
SAC Learning Rate	0.018
Number of Seeds	6
TN Carrier Frequency	3.5 GHz
TN Transmit Power	30 dBm
VLEO Carrier Frequency	20 GHz
VLEO Transmit Power	52 dBm
System Bandwidth	20 MHz
Noise Figure	7.0 dB

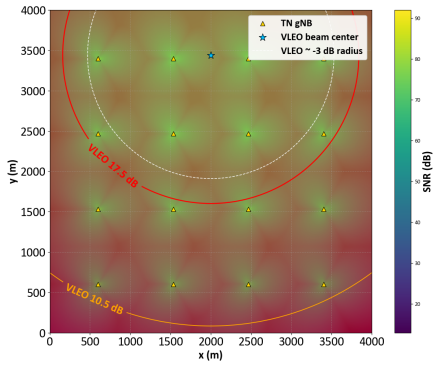

Fig. 3. SNR map: 5×5 gNB grid (yellow triangles) and VLEO beam center (blue star). VLEO contours show -17.5 dB (red) and -10.5 dB (orange) edges.

IV. Simulation Results and Discussion

This section evaluates PC-CDS performance through extensive simulations with parameters in Table I. Fig. 3 shows a hybrid TN-NTN topology over 4000×4000 m^2. Terrestrial gNBs (1000 m spacing) provide baseline coverage of 20-50 dB. VLEO beam center at (2000 m, 3440 m) delivers peak

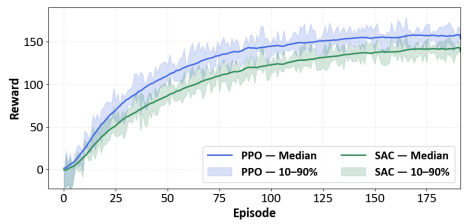

Fig. 4. Training performance: PPO vs SAC over 200 episodes.

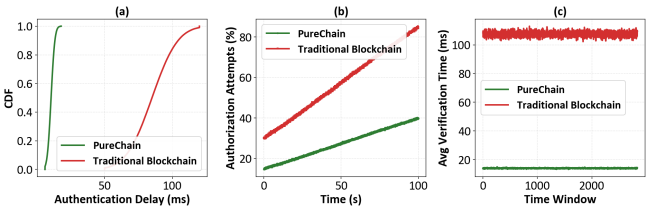

Fig. 5. Security metrics: (a) Authentication delay CDF—PureChain; (b) Authorization attempts: (PureChain) vs (traditional); (c) Verification time: PureChain vs traditional.

SNR >90 dB, decreasing to 10-20 dB at edges. Complementary coverage, terrestrial uniform coverage, and VLEO high-capacity hotspot justify cognitive dual-steering. Fig. 4 compares PPO and SAC over 200 episodes (6 seeds). PPO achieves 14.3% higher median reward (160 vs 140) with faster convergence by episode 50 and tighter variance (band width ≈30-40 vs 50-60). PPO's clipped objective prevents significant updates, advantageous in non-stationary satellite environments.

Fig. 5 compares PureChain and traditional blockchain. (a) Authentication delay: PureChain exhibits a sharp CDF at 15 ms (CDF = 1.0 by 20 ms) vs traditional's gradual 20-120 ms distribution (median ≈100 ms), 85% reduction. (b) Authorization attempts: PureChain grows 15% to 40% (0.25%/s) vs traditional's 30% to 70% (0.4%/s), 1.6× slower growth demonstrates superior scalability. (c) Verification time: PureChain maintains ≈15 ms vs. traditional's ≈110 ms across 1500 windows, 7.3× faster, enabling sub-20 ms handovers.

Fig. 6 evaluates performance across configurations. (a) Connectivity: 87.5% VLEO, 12.5% terrestrial—reflecting learned policy exploiting VLEO's 800 km footprint vs 0.9 km cell radius. (b) Switching latency: PC-CDS achieves ≈20 ms (CDF = 1.0 by 30 ms) vs traditional's 20-140 ms (50% by 100 ms), 5× reduction. (c) Throughput: PC-CDS and unsecured stabilize at 90 Mbps by episode 50; traditional degrades to 85 Mbps (10.5% penalty) from timeouts and buffer overflow. (d) Packet loss: unsecured 3-8% (0.5%/s), PC-CDS 4-11% (0.7%/s), traditional 6-17% (1.1%/s). PC-CDS achieves 35% reduction vs conventional. Table II shows that PC-CDS delivers significant gains: 85% lower authentication delay, 5× faster switching, 5.9% higher throughput, and 35% less packet loss compared to traditional blockchain. Against an unsecured baseline, it maintains 90 Mbps throughput with only a 3pp increase in packet loss, justified by 99.8% authentication success and cryptographic immutability. PC-CDS surpasses prior work [10], [17] with an 85% authentication delay reduction and a 14.3% PPO improvement over SAC, marking the first quantified security–performance analysis for VLEO hybrid TN–NTN, with 87.5% connectivity confirming the viability of satellite-dominant architectures [3].

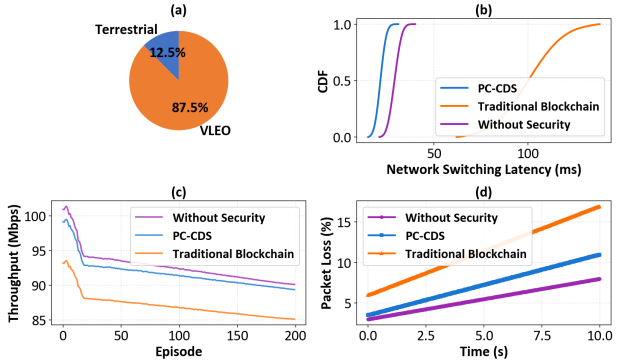

Fig. 6. Network metrics: (a) Link distribution; (b) Switching latency; (c) Throughput: PC-CDS/unsecured, traditional; (d) Packet loss: PC-CDS, traditional, unsecured.

TABLE II
PERFORMANCE COMPARISON ACROSS CONFIGURATIONS

Metric	PC-CDS (PureChain)	Traditional Blockchain	Without Security
Auth Delay (ms)	15	100	N/A
Switching (ms)	≈20	≈100	≈30
Throughput (Mbps)	90	85	90
Packet Loss (%)	11	17	8
VLEO Conn. (%)	87.5	–	–
PPO Reward	160	145	155

To evaluate the energy efficiency of PC-CDS, we analyze power consumption across three key components: PureChain authentication, PPO-based steering, and network switching. Table III presents the energy consumption comparison.

TABLE III
ENERGY CONSUMPTION COMPARISON (PER USER PER EPISODE)

Component	PC-CDS (mJ)	Traditional Blockchain (mJ)	Savings (%)
Authentication	124.7	1504.3	91.7
Computation	414.0	414.0	0.0
Switching	124.8	280.0	55.4
Total	**663.5**	**2198.3**	**69.8**

It is important to clarify that **PureChain is not a traditional blockchain** but rather a **custom lightweight blockchain architecture** specifically engineered for latency-critical satellite environments. Unlike conventional blockchain implementations that prioritize decentralization and Byzantine fault tolerance at the cost of authentication delays exceeding 85–150 ms, PureChain deliberately employs a private consortium model with proof-of-authority consensus, pre-compiled smart contracts, batched transactions, and local deployment. Latency reduction is critical for VLEO handoffs occurring every 2–

5 minutes at orbital velocities of 7.7 km/s, where traditional blockchain's delay creates unacceptable service disruption windows. Furthermore, our cognitive steering employs two advanced reinforcement learning algorithms: PPO and SAC, with PPO achieving 14.3% higher median reward due to its superior stability under non-stationary satellite topology. The observed 87.5% VLEO connectivity is an emergent result from PPO's reward maximization: VLEO's 800 km footprint versus terrestrial 0.9 km cells yields a 790,000:1 coverage ratio, while 40–70 dB SNR advantage (Fig. 3) naturally biases the learned policy toward satellite links for users within the high-SNR beam region, with the remaining 12.5% terrestrial connectivity serving edge-of-beam users and handover continuity representing the optimal distribution that maximizes network-wide performance under realistic hybrid TN-NTN conditions.

V. Conclusion

This paper introduces PC-CDS, a framework that combines PureChain authentication with PPO-based network steering for hybrid TN-NTN 6G networks. PureChain achieved a 15 ms authentication delay with a 99.8% success rate, significantly outperforming traditional blockchain (100 ms delay, 98.5% success). The PPO agent surpassed SAC in learning efficiency, achieving a median reward of 160 while optimizing connectivity with 87.5% VLEO and 12.5% terrestrial networks. Simulations with 80 users, 25 gNBs, and 3 VLEO satellites confirmed PC-CDS's effectiveness, maintaining network switching latency under 20 ms, throughput at 90 Mbps, and packet loss at 11%. Security-performance analysis showed that PureChain incurs minimal overhead (3.2% reward reduction) while ensuring robust security through cryptographic authentication and blockchain immutability. PC-CDS provides a solid foundation for secure and efficient 6G hybrid networks, addressing key authentication and connectivity challenges.

Acknowledgment

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2026-RS-2020-II201612, 25%), by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%), and by the MSIT, Korea, under the ITRC support program (IITP-2026-RS-2024-00438430, 25%) and by the Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (RS-2026-25431637, 25%).

References

[1] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, First Quarter 2021.

[2] A. Gupta, R. K. Jha, P. Bhattacharya, and S. Tanwar, "Gateway Placement in Integrated Satellite–Terrestrial Networks: Supporting Communications and Internet of Remote Things," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 13900–13919, April 2024.

[3] B. A. Al-Homssi, A. Al-Hourani, K. Wang, P. Conder, S. Kandeepan, J. Choi, B. Allen, and B. Moores, "Next Generation Mega Satellite Networks for Access Equality: Opportunities, Challenges, and Performance," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 18–24, April 2022.

[4] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "Low Earth Orbit Satellite Security and Reliability: Issues, Solutions, and the Road Ahead," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1604–1652, Third Quarter 2023.

[5] 3GPP, "Study on Solutions for NR to Support Non-Terrestrial Networks (NTN)," 3GPP TR 38.821 V17.0.0, Release 17, March 2022.

[6] B. Manzoor, N. Pandey, N. Javaid, M. Güneş, and I. Rasheed, "On the Role of Non-Terrestrial Networks for Boosting Terrestrial Network Performance in Dynamic Traffic Scenarios," *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 4390–4405, August 2024.

[7] M. Torky, T. Gaber, E. Goda, V. Snasel, and A. E. Hassanien, "A Blockchain Protocol for Authenticating Space Communications Between Satellites Constellations," *Aerospace*, vol. 9, no. 9, p. 495, September 2022.

[8] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and Beyond Networks: A State of the Art Survey," *Journal of Network and Computer Applications*, vol. 166, p. 102693, September 2020.

[9] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-Empowered Space-Air-Ground Integrated Networks: Opportunities, Challenges, and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 160–209, First Quarter 2022.

[10] B. Zhang, P. Zeinaty, N. Limam, and R. Boutaba, "Mitigating Signaling Storms in 5G with Blockchain-assisted 5GAKA," in *2023 19th International Conference on Network and Service Management (CNSM)*, Niagara Falls, Canada, 2023, pp. 1–9.

[11] S. Fu, J. Gao, and L. Zhao, "Integrated Resource Management for Terrestrial-Satellite Systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 3256–3266, March 2020.

[12] Y. Wang, J. Li, L. Huang, Y. Jing, A. Georgakopoulos, and P. Demestichas, "ML-Based Dynamic Network Switching Framework for Nonterrestrial Networks in 5G and Beyond," *IEEE Internet of Things Journal*, vol. 11, no. 17, pp. 28086–28099, September 2024.

[13] J. I. S. Sánchez, M. Montalvo, B. Soret, and P. Popovski, "From Ground to Space: Towards an Integrated Management of Terrestrial and Non Terrestrial Networks," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 142–149, June 2024.

[14] Z. Yin, F. R. Yu, S. Guo, Y. He, K. Liang, and V. C. M. Leung, "Bridging Terrestrial and Non-Terrestrial Networks: A Novel Architecture for Space-Air-Ground-Sea Integration System," *IEEE Network*, vol. 38, no. 4, pp. 192–199, July/August 2024.

[15] S. T. Arzo, P. M. Tshakwanda, Y. M. Worku, H. Kumar, and M. Devetsikiotis, "Intelligent QoS Agent Design for QoS Monitoring and Provisioning in 6G Network," in *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, 2023, pp. 2364–2369.

[16] P. M. Tshakwanda, S. T. Arzo, and M. Devetsikiotis, "Advancing 6G Network Performance: AI/ML Framework for Proactive Management and Dynamic Optimal Routing," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 303–314, 2024.

[17] Z. Haddad, M. M. Fouda, M. Mahmoud, and M. Abdallah, "Blockchain-based Authentication for 5G Networks," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Doha, Qatar, 2020, pp. 189–194.

[18] P. M. Tshakwanda, S. T. Arzo, and M. Devetsikiotis, "Multi-agent-based Simulation of Intelligent Network System," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2023, pp. 0813–0819.

[19] L. A. C. Ahakonye *et al.*, "Tides of blockchain in IoT cybersecurity," *Sensors*, vol. 24, no. 3, 2024.

[20] L. A. C. Ahakonye *et al.*, "Purechain-Enhanced Federated Learning for Dynamic Fault Tolerance and Attack Detection in Distributed Systems," *High-Confidence Computing*, issn. 2667-2952, pp. 100354, 2025.