Position-Aware Adaptive Turbine: Leveraging Leader Rotation as an Intrinsic Entropy Source for Secure and Efficient Block Propagation

Seokmin Kim, Hwangnam Kim*

Korea Univ.

{slartler17, hnkim}@korea.ac.kr

위치 인식 적응형 터빈: 안전하고 효율적인 블록 전파를 위한 리더 회전의 내재적 엔트로피 활용

김석민, 김황남*
고려대학교

Abstract

In high-throughput blockchain systems, randomly constructed topologies ensure security but degrade propagation efficiency. We propose the Position-aware Adaptive Turbine (PAT) protocol, which optimizes scalability by incorporating physical location awareness. PAT employs a two-pass balanced assignment strategy to mitigate local monopoly effects and leverages leader rotation as an intrinsic entropy source to prevent Eclipse attacks without external randomness. Simulation results demonstrate that PAT reduces block propagation time by a factor of 3.2 and achieves a near-zero stale rate compared to the baseline Turbine, proving that performance and security can coexist in dynamic consensus environments.

Ⅰ. Introduction

High-throughput blockchains, such as Solana [1], aim to process thousands of transactions per second by minimizing block time. However, the rapid propagation of large blocks remains a critical bottleneck. Existing protocols like Turbine utilize randomized tree topologies to prevent censorship and Eclipse attacks [3, 4]. While secure, this randomization causes a "topology mismatch," connecting physically distant nodes and increasing tail latency. Previous hybrid approaches [5, 6, 7] attempt to balance locality and randomness but often suffer from complexity or local resource exhaustion.

In this letter, we propose the Position-aware Adaptive Turbine (PAT), a deterministic propagation protocol that maximizes efficiency using location awareness while ensuring security through consensus dynamics. Our key insight is that the leader rotation mechanism inherent in modern blockchains acts as a sufficient source of topological uncertainty. We mathematically prove that this intrinsic entropy maximizes the difficulty of path prediction, rendering artificial randomness unnecessary. Experimental results confirm that PAT achieves a 3.2x speedup in propagation and a 98% reduction in stale rates relative to the standard Turbine.

Ⅱ. Proposed Protocol: PAT

1. Optimization Goal

We model the validator network as a complete graph $G = (V, E)$. Given a leader r, the objective is to construct a propagation tree T that minimizes the maximum propagation delay (tail latency) under a strict fanout constraint k:

$$\min_{T} \max_{v \in V} D_T(v) \quad \text{s.t. } \deg_{out}(u) \le k, \forall u \in V \qquad (1)$$

This formulation aligns with the Minimum Broadcast Time problem [8], a known NP-Hard variation of the Degree-Constrained Minimum Spanning Tree (DCMST).

2. Two-Pass Balanced Assignment

Naive greedy approaches rapidly exhaust the fanout of nearby nodes, forcing adjacent stragglers to connect to distant parents. To resolve this local monopoly problem, PAT employs a Two-Pass Balanced Assignment strategy. Each node u splits its fanout budget k into two components using a tunable parameter α (empirically set to 0.5):

$$k_{priority} = \lfloor \alpha \cdot k \rfloor, \quad k_{balanced} = k - k_{priority} \qquad (2)$$

- Phase 1 (Priority Selection): Node u assigns $k_{priority}$ slots to its nearest unassigned neighbors. This guarantees essential locality and fast cluster entry.

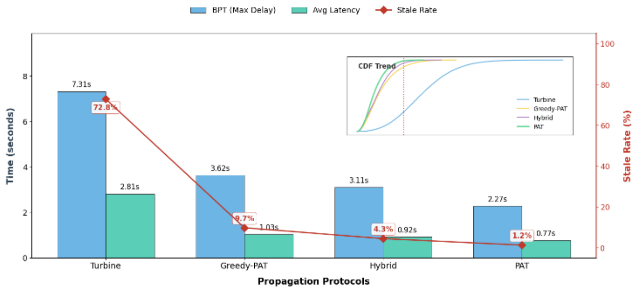

Fig. 1. Performance comparison of block propagation efficiency and stale rate across different protocols.

- Phase 2 (Balanced Filling): Node u uses the remaining $k_{balanced}$ slots to connect to the next nearest available nodes. This phase accommodates stragglers, ensuring topological balance and preventing coverage holes.

Ⅲ. Security Analysis and Evaluation

1. Security Model: Intrinsic Entropy

A primary concern with position-aware topology is predictability. We challenge this by modeling Leader Rotation as an entropy source. The topological entropy is defined as $H(X) = -\sum P(x_i)\log_2 P(x_i)$, where X is the parent node selected by a validator. In a static setting, a deterministic algorithm yields $H(X) = 0$. However, leader rotation shifts the geographic root every slot, fundamentally reshaping the shortest-path tree. This dynamic decorrelates parent selection across rounds. According to information theory [9], the probability of sustaining an Eclipse attack for T consecutive rounds is bounded by:

$$P_{success} \le 2^{-T \cdot H(X)} \qquad (3)$$

This model aligns with the Moving Target Defense (MTD) principle [10], where a continuously shifting attack surface exponentially increases attacker cost.

2. Experimental Results

We evaluated PAT using a discrete-event simulator with $N = 1{,}000$ validators distributed in a $100 \times 100km^2$ area ($k = 6$).

- Propagation Efficiency: As shown in Fig. 1, PAT achieved a Block Propagation Time (BPT) of 2.27s, a 3.2x speedup over Turbine (7.31s). The average latency was reduced by 72% (0.77s vs. 2.81s).
- Network Stability: PAT reduced the stale rate from 72.76% (Turbine) to 1.18%, surpassing even hybrid approaches. This ensures near-perfect synchronization.
- Security Validation: Fig. 2 confirms that while a static leader results in zero entropy, the rotating leader scenario maintains high entropy ($H(X) > 3.7$), keeping the maximum parent recurrence rate below 10%. This validates that PAT is resilient to path-based attacks without random links.

Ⅳ. Conclusion

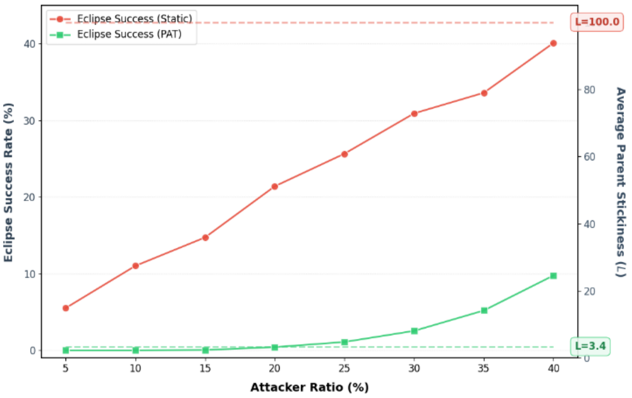

Fig. 2. Eclipse attack success rate and parent stickiness (***L***) as a function of the attacker ratio.

We proposed PAT, a novel propagation protocol that resolves the scalability-security trade-off in P2P networks. By leveraging a two-pass assignment and intrinsic leader rotation, PAT achieves optimal latency and robust security. We conclude that consensus dynamics can serve as first-class design primitives for network-layer optimization. Future work will extend PAT to heterogeneous bandwidth environments.

ACKNOWLEDGMENT

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-RS-2021-II211835) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation).

REFERENCES

[1] A. Yakovenko, Solana: A new architecture for a high performance blockchain, 2018.

[2] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008.

[3] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," OSDI, 1999.

[4] E. Heilman et al., "Eclipse attacks on Bitcoin's peer-to-peer network," USENIX Security, 2015.

[5] I. Baumgart and S. Mies, "S/Kademlia: A practicable approach towards secure key-based routing," ICPADS, 2007.

[6] F. Ritz et al., "Simulating Block Propagation in Large-Scale Blockchain Networks," IEEE Blockchain, 2020.

[7] T. Yoo et al., "Trust-Defined Network: A panoramic P2P framework," Computer Comm., 2025.

[8] M. R. Garey and D. S. Johnson, Computers and Intractability, 1979.

[9] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2006.

[10] S. Jajodia et al., Moving Target Defense, Springer, 2011.