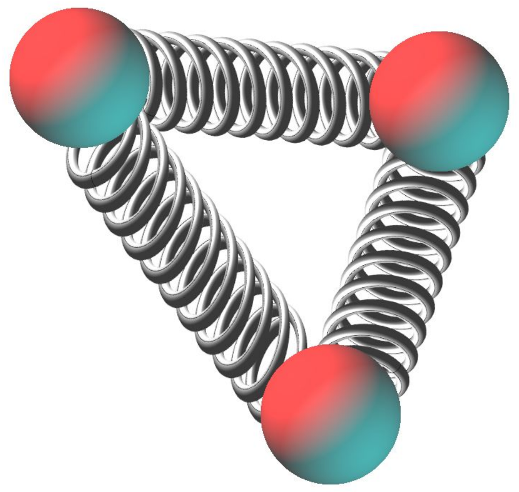
Research Project

Using Weighted Voting to Accelerate Blockchain Consensus

Author : Filip Błaszczyk
(F.J.Blaszczyk@student.tudelft.nl))

Supervisor: Jérémie Decouchant (J.Decouchant@tudelft.nl)
Responsible Professor: Rowdy Chotkan (R.M.Chotkan-1@tudelft.nl)

Introduction



To enhance upon the seminal Nakamoto consensus, which relies on proof-of-work, permissionless systems have increasingly turned to mechanisms where a node's voting power depends on a weight metric. Berger's algorithm, AWARE [1], demonstrated that using more nodes than strictly necessary (i.e., 3f + 1 + Δ instead of 3f + 1), employing two possible vote weights, and employing an optimization algorithm (simulated annealing) to determine the weight of each node (Vmin or Vmax) and its role (leader or backup) can enhance performance. However, Berger et al.'s algorithm has not been proven to tolerate faulty nodes before and after optimization. This project aims to address this scientific gap.

OBJECTIVES

- Add detection mechanism to AWARE for selecting nodes lying about latencies
- Examine the performance of the enhanced algorithm.

[1] Christian Berger, Hans P. Reiser, Joao Sousa, and Alysson Bessani. AWARE: Adaptive Wide-Area Replication for Fast and Resilient Byzantine Consensus. IEEE Transactions on Dependable and Secure Computing, 19(3):1605–1620, May 2022.

[2] Jeffrey Seibert, Sheila Becker, Cristina Nita-Rotaru, and Radu State. Securing Virtual Coordinates by Enforcing Physical Laws. In 2012 IEEE 32nd International Conference on Distributed Computing Systems, pages 315–324, Macau, China, June 2012. IEEE.

RESEARCH

METHODOLOGY

To enhance the AWARE algorithm, we integrate Vivaldi network coordinates and Newtonian invariants, addressing the critical need for accurate latency management in distributed systems. **Vivaldi Algorithm** : The Vivaldi algorithm positions nodes in an n-dimensional Euclidean space where distances represent real-world latency estimations. This is modeled using dynamic springs, with each connection behaving like a spring that adjusts based or real-time latency measurements.

Newtonian Invariants :

- **Centroid Stability (IN1)** : Monitors the geometric center of a node and its neighbors. Any displacement from the origin indicates potential malicious activity or network asymmetry, helping to counteract these influences.
- **Damping Force Reduction (IN3)** : Focuses on the reduction of force magnitudes as the system approaches equilibrium.

By integrating Vivaldi coordinates and Newtonian invariants, our approach ensures more accurate and stable latency management

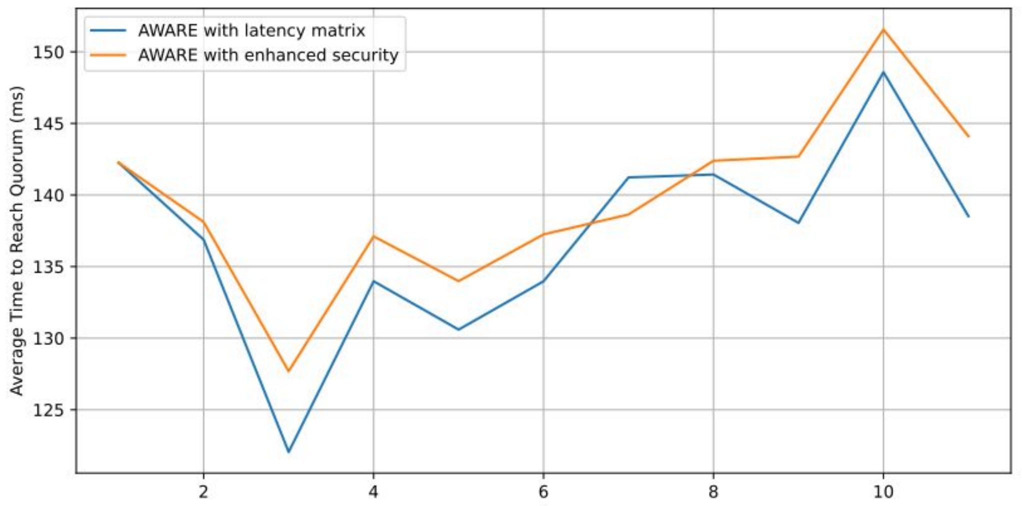


Figure 1: Comparison of quorum time formation between normal AWARE and enhanced protocol in the network without attack. Latency data is taken from Wonder Network.

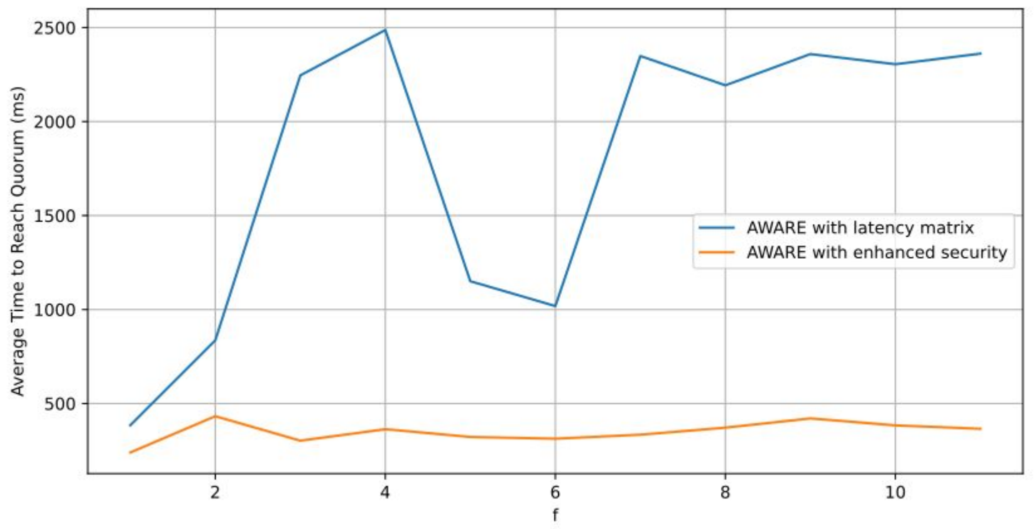


Figure 2: Comparison of quorum time formation between normal AWARE and enhanced protocol in the network with Deflation Attack . Latency data is taken from Wonder Network.

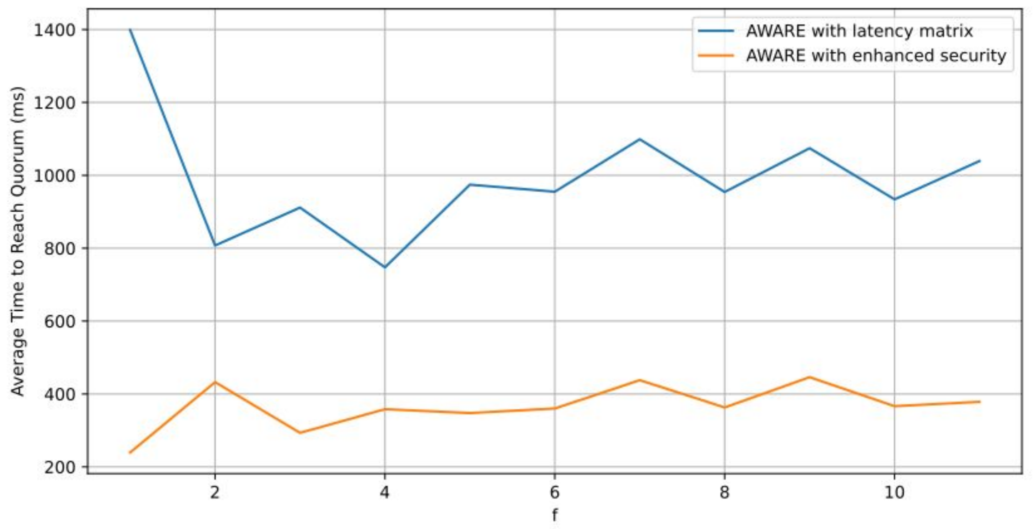


Figure 3: Comparison of quorum time formation between normal AWARE and enhanced protocol in the network with Inflation Attack. Simulation data is taken from Wonder Network.

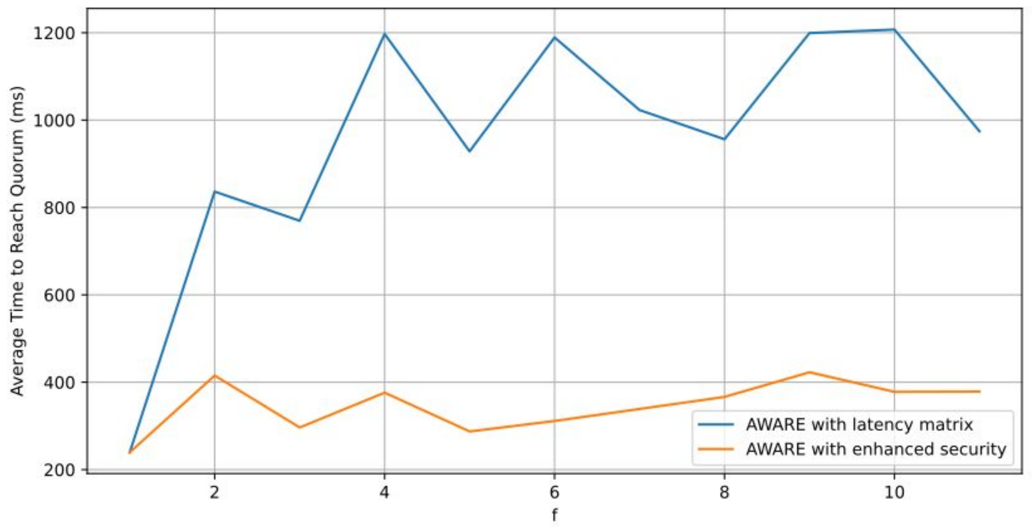


Figure 4: Comparison of quorum time formation between normal AWARE and enhanced protocol in the network with Oscillation Attack. Simulation data is taken from Wonder Network.

CONCLUSION

RESULTS

The enhanced algorithm performed exceptionally well on the King and WonderNetwork datasets, effectively detecting and disregarding malicious nodes, thus maintaining lower average quorum collection times. However, irregularities were noted in the PlanetLab dataset due to outliers causing nodes to be more spread out in Vivaldi space, impacting system stabilization.

LIMITATIONS

The simulations are limited to networks with a maximum size of 49 nodes. They are computation-only and do not account for how various scenarios play out in real-life networks. The attacks used for comparison are basic ones derived from Vivaldi. Attacks targeting not only AWARE but also Vivaldi simultaneously should be further examined.

CONCLUSION

The results indicate that the enhanced AWARE algorithm improves system robustness and stability under normal and attack conditions. Further development involves deploying the enhanced algorithm in real-world distributed systems to assess practical efficacy and resource requirements. Future research should also compare this algorithm with other latency protection methods and explore integrating machine learning techniques for further refinement.