BRLA-P2P: A Byzantine-Resistant Learning Automata Framework for Resilient Peer-to-Peer Content Distribution

Ekaba Bisong

1 Problem Statement and Motivation

Peer-to-peer (P2P) networks are now a key model for distributed content sharing, enabling file and video sharing. But the size and decentralised nature of these networks make it hard to ensure reliable content distribution when malicious nodes are present. As P2P networks grow to millions of nodes, the threat of Byzantine behaviour becomes increasingly critical, with malicious peers capable of disrupting network operations through content pollution, routing table manipulation, and coordinated attacks.

2 Current State of the Art

Content distribution in P2P systems has evolved through several architectural paradigms, from early unstructured networks like Gnutella to more sophisticated structured approaches using Distributed Hash Tables (DHTs) like Chord and Kademlia. These systems showed decentralised content sharing is possible, but they have major reliability and security issues. BitTorrent introduced innovative incentive mechanisms through its tit-for-tat approach, establishing a foundation for cooperative content distribution. But these methods are ineffective against Byzantine foes who can use content pollution and routing attacks to exploit the system.

Traditional content delivery networks (CDNs) have solved distribution issues with centralised infrastructures, using extensive edge server networks from Akamai and Cloudflare. While effective, these approaches incur substantial infrastructure costs and introduce potential single points of failure. Peer-assisted CDNs try to close this gap by merging centralised control with P2P content delivery, but they still lack strong security and adaptive resource allocation.

Consensus mechanisms and trust-based protocols have been the main focus of existing P2P approaches in Byzantine fault tolerance. Systems like BFT-CAN and Byzantine-resilient DHT have theoretical security guarantees but struggle with practical scalability due to their high message overhead and complex validation protocols. These systems often use static security measures that can't adapt to changing attack patterns or network conditions. Learning Automata (LA) research has demonstrated significant potential in addressing dynamic resource allocation problems in distributed systems. The evolution of Object Migration Automata (OMA) through variants like TPEOMA has shown particular promise in solving partitioning problems efficiently. But LA's current methods lack Byzantine resistance and haven't been studied in content distribution, where dynamic content placement and routing decisions greatly affect system performance.

3 Proposed Approach

We suggest BRLA-P2P, a new framework that combines Byzantine resistance with Learning Automata to make a robust peer-to-peer content distribution system. Our framework adds Byzantine detection and resistance features to TPEOMA's content distribution mechanisms. At its core, BRLA-P2P uses Learning Automata to dynamically optimise content placement and routing decisions, while simultaneously defending against Byzantine behaviours that could compromise distribution integrity.

The framework uses a multi-faceted approach to content distribution that combines reputation-based peer selection, behavioural pattern analysis for Byzantine detection, and adaptive learning mechanisms for content placement. For content distribution, we employ Partition Size Required (PSR) features to manage dynamic content replication

and placement across the network. This is coupled with an adaptive learning mechanism that continuously adjusts distribution strategies based on peer behaviour and network conditions.

To ensure resilience, our Byzantine detection component monitors peer interactions during content distribution, analysing both direct observations and transitive trust relationships. The Learning Automata component will adapt content distribution patterns in response to detected malicious behaviour, automatically routing around compromised nodes while maintaining efficient content delivery paths. We will empirically evaluate this integrated approach's performance in content distribution efficiency, Byzantine resistance, and system scalability under various network conditions and attack scenarios.

4 Expected Deliverables

The project will deliver a comprehensive framework including:

- Design and implementation of the BRLA-P2P framework integrating Learning Automata with Byzantine resistance capabilities.
- Development of simulation testbed for experimental evaluation.
- Empirical analysis of Byzantine detection accuracy and false positive rates across different network conditions.
- Performance evaluation comparing BRLA-P2P against existing P2P content distribution approaches.
- Comprehensive analysis of system scalability and overhead characteristics.

5 Project Timeline

Date	Milestone
February 7	Project proposal submission
February 21	First biweekly update – Preliminary literature review and baseline setup
March 7	Midterm update – Framework architecture and core algorithms
March 21	Third biweekly update – Evaluation methodology and initial results
April 4	Final presentation
April 11	Final report submission

Resources

The project website is publicly accessible at: `https://ekababisong.org/brlap2p`

References

- Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*.
- Narendra, K. S., & Thathachar, M. A. L. (2012). *Learning Automata: An Introduction*. Prentice Hall.
- Sit, E., & Morris, R. (2002). Security Considerations for Peer-to-Peer Distributed Hash Tables. In *International Workshop on Peer-to-Peer Systems*.
- Shirvani, T., et al. (2018). TPEOMA: Transitivity Pursuit Enhanced Object Migration Automata. *Evolving Systems*.
- Omslandseter, M., et al. (2021). A Learning-Automata Based Solution for Non-Equal Partitioning: Partitions with Common GCD Sizes. *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*.
- Stoica, I., Morris, R., Karger, D., Kaashoek, M. F., & Balakrishnan, H. (2001). Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications. In *ACM SIGCOMM Computer Communication Review*.
- Maymounkov, P., & Mazieres, D. (2002). Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02)*.

- Nygren, E., Sitaraman, R., & Sun, J. (2010). The Akamai Network: A Platform for High-Performance Internet Applications. *SIGOPS Operating Systems Review*, 44(3), 2–19.
- Pathan, A. S. K., Buyya, R., & Vakali, A. (2008). *Content Delivery Networks: State of the Art, Insights, and Imperatives*. Springer.
- Krishnamurthy, B., & Wills, C. E. (2000). On the Use and Performance of Content Distribution Networks. *ACM SIGCOMM Computer Communication Review*, 30(4), 169–182.