Block Chain : Assignment 1

Ujjawal Upadhyay (B21MT038)
Sindhav Khushal (B21AI039)

Report on OMNeT++ Simulation of Blockchain P2P Network

Abstract

This report details the development and execution of a peer-to-peer (P2P) blockchain network simulation using OMNeT++. The primary goal of the simulation is to analyze the behavior and efficiency of a blockchain network under various conditions, particularly focusing on the impact of adversarial actions within the network.

Table of Contents

1. Introduction

1.1 Background

Blockchain technology has fundamentally transformed how data is stored and transactions are recorded. Simulations of blockchain networks are crucial for understanding potential vulnerabilities and performance issues in a controlled environment before deployment in real-world applications.

1.2 Objectives

The objective of this project is to simulate a blockchain network using OMNeT++ to:

- Analyze how network performance varies with changes in node behavior.
- Evaluate the network's resilience against adversarial attacks.
- Understand the dynamics of mining power utilization under different network conditions.

2. Methodology

The simulation was carried out using OMNeT++, a modular simulation framework that is especially suited for researching network systems. The codebase includes several custom modules written in C++ that define the behaviors of seed and peer nodes within the blockchain network.

3. Simulation Setup

3.1 Network Configuration

The network consists of multiple nodes categorized into seed and peer nodes. The configuration parameters were set in the omnetpp.ini file, including:

- hashPower: The computational power of each node to mine blocks.
- interarrivalTime: The average time between successive blocks.
- isAdversary: Boolean flags set for nodes intended to behave maliciously.

3.2 Source Code Description

- PeerNode: Handles mining operations, transaction verification, and block broadcasting.
- SeedNode: Manages network entries and provides peer list information to new nodes.
- MyMessage.h: Defines the message structure used for node communication.

4. Results and Discussion

The simulation results were collected and analyzed to evaluate network performance metrics such as block generation rates, chain length, and adversary impact on network stability. The findings indicated:

- How network performance is affected by different hash power distributions.
- The efficiency of the gossip protocol in disseminating information.
- The resilience of the network against flooding attacks by adversarial nodes.

5. Conclusion

The simulation demonstrated the effectiveness of the implemented blockchain protocol in ensuring data integrity and availability despite adversarial attempts to disrupt the network. Future work could explore more sophisticated adversarial strategies and defense mechanisms to enhance network security.

6. Appendices

- A: Code Listings: Complete source code for the peer and seed nodes attached in GC submission.
- B: Configuration Files:

```
[General]
network = Net

*.peer[*].hashPower = uniform(0.1, 1.0)
*.peer[*].interarrivalTime = 600  # 1 minutes on average
*.peer[*].isAdversary = false
*.peer[*].floodingRate = 1  # 1 invalid block per second on average

*.peer[0].isAdversary = true
*.peer[1].isAdversary = true
*.peer[2].isAdversary = true

sim-time-limit = 86400s

output-vector-file = ${resultdir}/${configname}-${runnumber}.vec
output-scalar-file = ${resultdir}/${configname}-${runnumber}.sca
```