Assignment 1

Sameer Sharma (B21CS066)
Shalin Jain (B21CS070)

September 29, 2024

1 Objective

The assignment focuses on simulating a blockchain network over a peer-to-peer (P2P) network using OMNeT++ Discrete Event Simulator. The goal is to establish a connected network where peer nodes interact through seed nodes, broadcast messages, check peer liveness, and simulate Proof-of-Work (PoW) mining.

2 Network Structure

The network is composed of two types of nodes:

1. **Seed Nodes**: Facilitate network entry by providing peer details.
2. **Peer Nodes**: Perform blockchain operations such as block mining, message gossiping, and liveness checking.

3 Key Functionalities

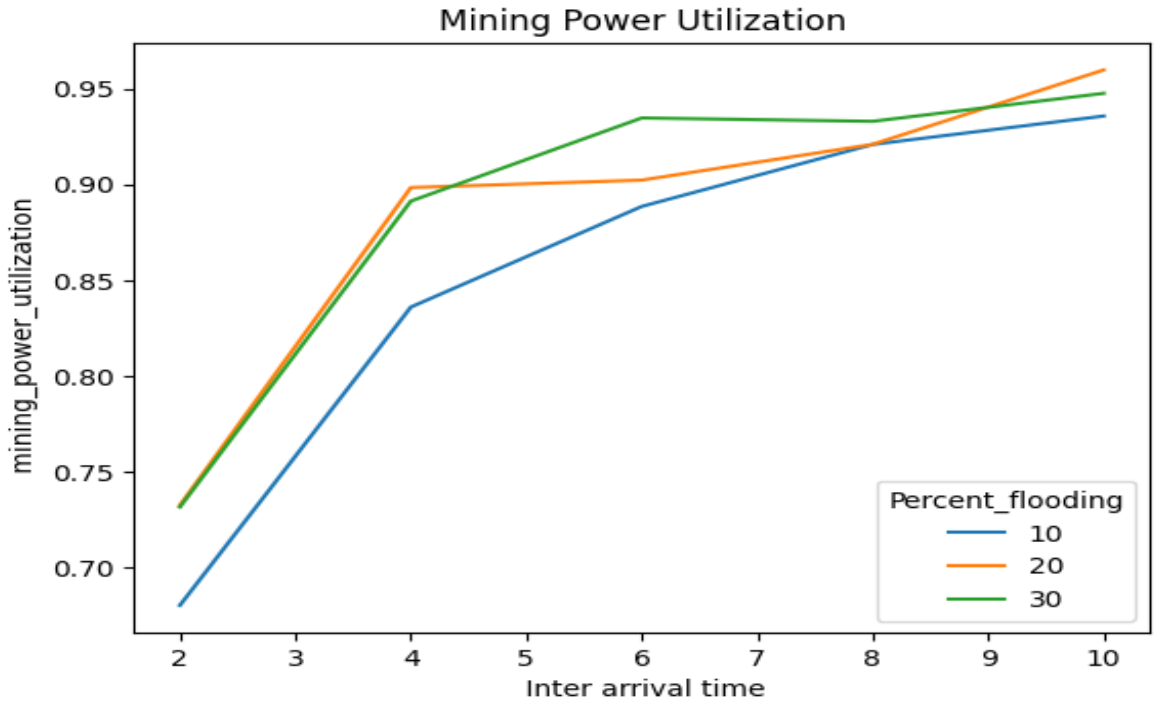
1. **Peer Registration**: Peer nodes register with seed nodes and establish TCP connections with other peers.
2. **Gossip Protocol**: Nodes broadcast messages every 5 seconds, ensuring that each message travels through the network only once by maintaining a Message List (ML).
3. **Liveness Checking**: Every 13 seconds, peers send liveness requests to connected peers. A peer is marked "dead" after three consecutive failures.
4. **Proof-of-Work Mining**: Peers mine blocks following the PoW protocol, with exponential wait times based on their hash power.
5. **Block Mining & Validation**: Blocks are validated and appended to the chain if they meet certain criteria (hash verification).

4 Attack Simulation

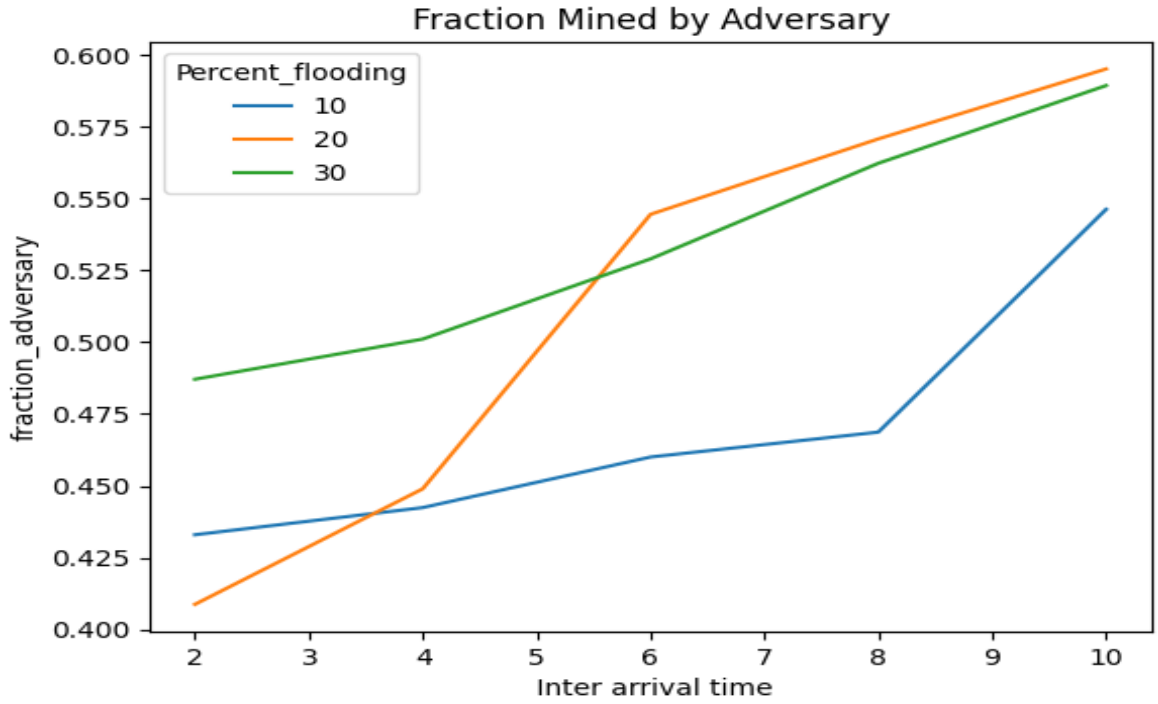
The assignment includes simulating a Block Flooding Attack, where an adversary node floods the network with invalid blocks, potentially stalling honest miners.

Below are given plots of mining power uitilization and fraction mined by adversary when the simulation is run for **1 hour** and for inter-arrival-time from **2 to 5 seconds** and for nodes flooded are **10%, 20% and 30%**.

Mining Power Utilization



Fraction Adversary Mined



Blockchain