CS765- Assignment-2

Simulation of P2P network

200050012- Anushka Dubey
200050056- Kajal
200050083- Naman Singh Rana

In this assignment simulated different attacks, namely selfish mining attack and stubborn mining attack, on top of the discrete-event simulator for a P2P cryptocurrency network, that we built in the last assignment. For this we created a special attacker node (node 0), there is only 1 attacker node and the rest are honest nodes.

Below are the observations and insights we obtained after running the simulations on different values of parameters.

Observations

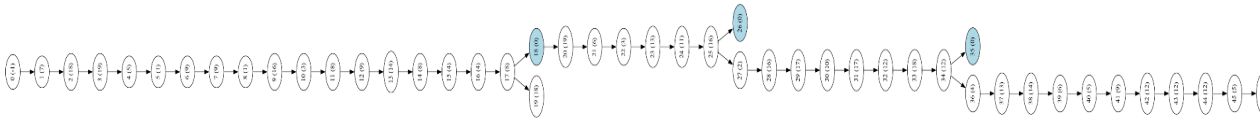
Varying the parameters

We experimented by varying different parameters(n,z0,z1,T_{tx},T_k, zeta(fraction of nodes connected to adversary node), adversary mining power) and got the following results:

Selfish Mining Attack:

- Varying **adversary mining power**:

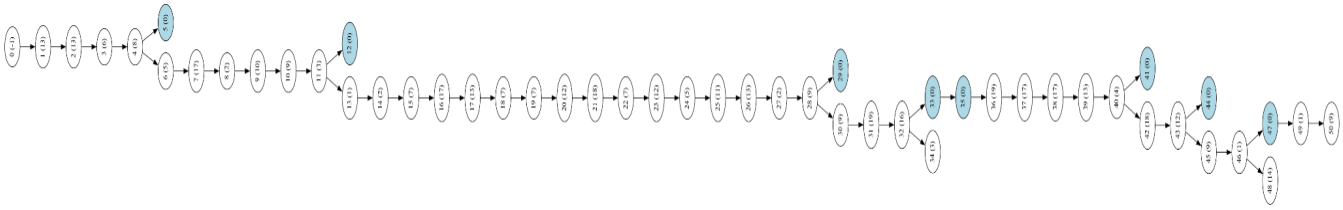
1. n = 20, z0 =0.5, z1 =1, T_{tx} =10 ms, T_k= 600 ms, zeta =0.5, **adversary mining power=0.1**



MPU Adv: 0.25

MPU All: 0.92

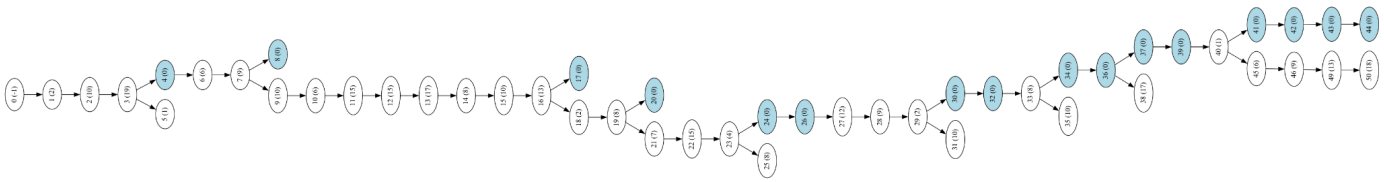
2. n = 20, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, zeta = 0.5, **adversary mining power = 0.2**



MPU Adv: 0.375

MPU All: 0.86

3. n = 20, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, zeta = 0.5, **adversary mining power** = **0.3**

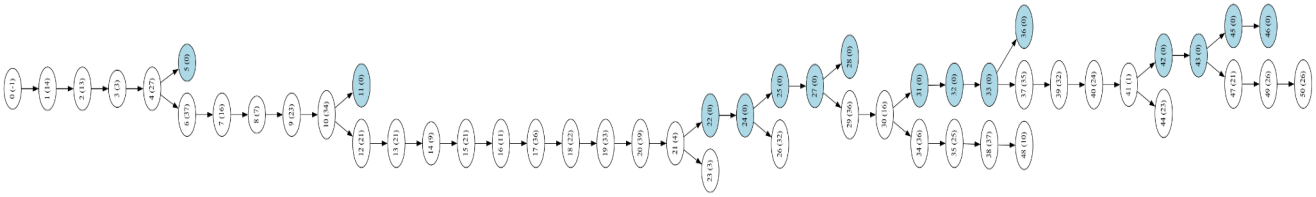


MPU Adv: 0.81

MPU All: 0.7

- Varying **zeta**:

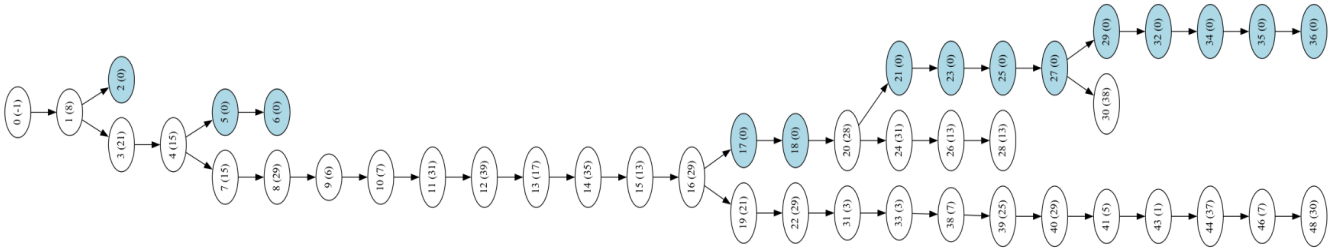
1. n = 40, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, **zeta = 0.25**, adversary mining power = 0.3



MPU Adv: 0.6

MPU All: 0.74

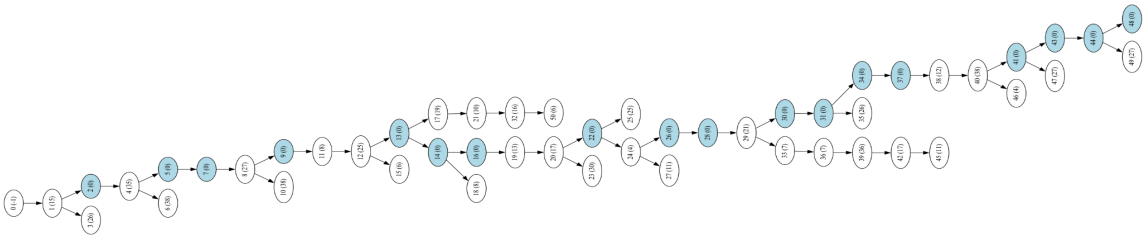
2. n = 40, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, **zeta = 0.5**, adversary mining power = 0.3



MPU Adv: 0.78

MPU All: 0.5681818181818182

3. n = 40, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, **zeta = 0.75**, adversary mining power = 0.3

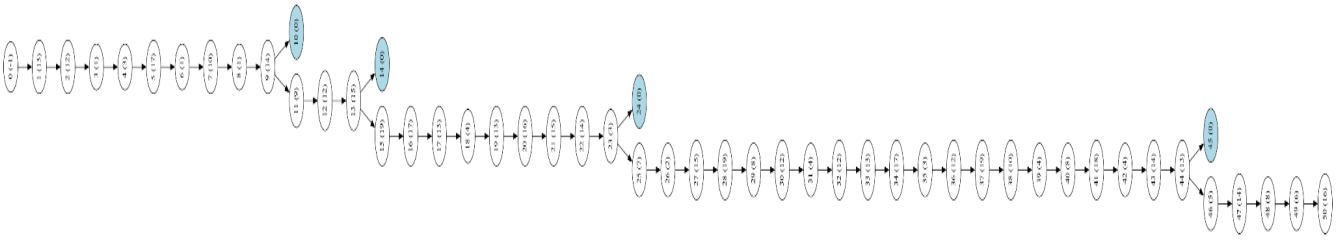


MPU Adv: 0.94

MPU All: 0.58

Stubborn Mining Attack:

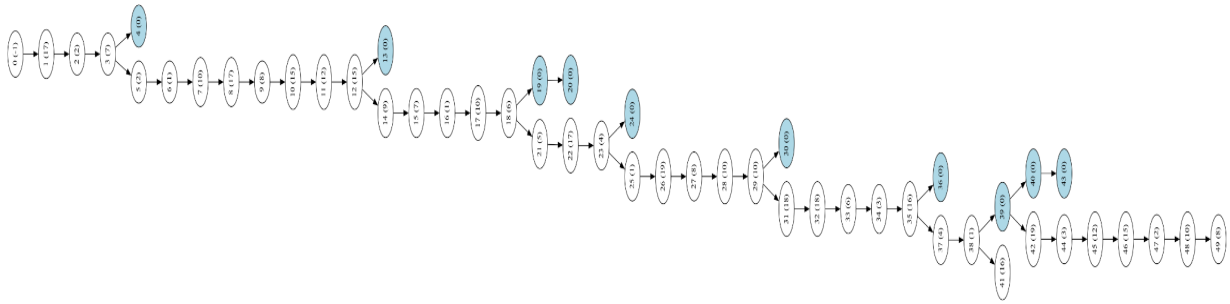
- Varying **adversary mining power**:
    1. n = 20, z0 =0.5, z1 =1, T_{tx} =10 ms, T_k= 600 ms, zeta =0.5, **adversary mining power=0.1**



MPU Adv: 0.333

MPU All: 0.88

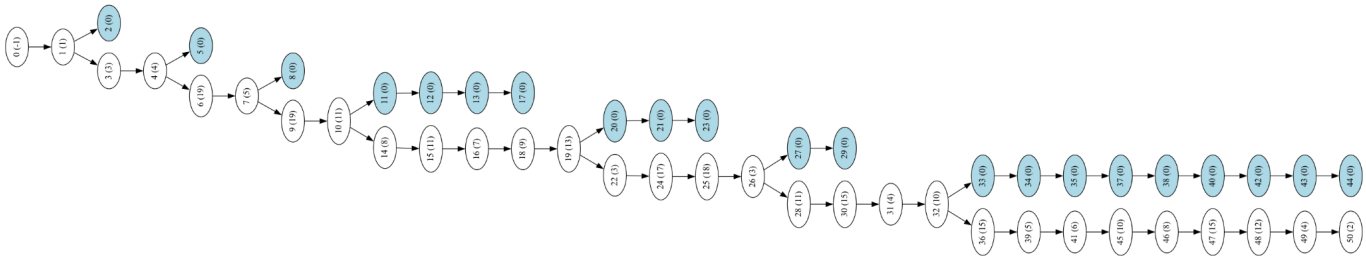
2. n = 20, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, zeta = 0.5, **adversary mining power = 0.2**



MPU Adv: 0.1

MPU All: 0.7959183673469388

3. n = 20, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, zeta = 0.5, **adversary mining power** = **0.4**

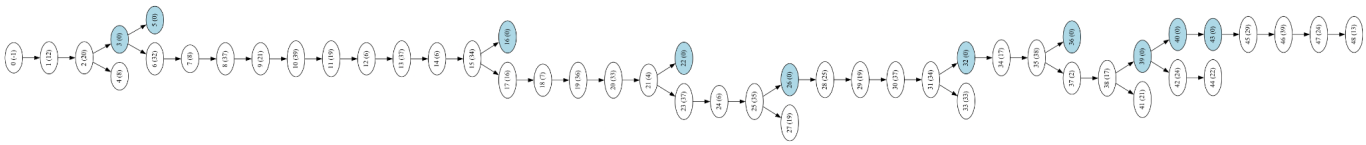


MPU Adv: 0.428

MPU All: 0.58

- Varying **zeta**:

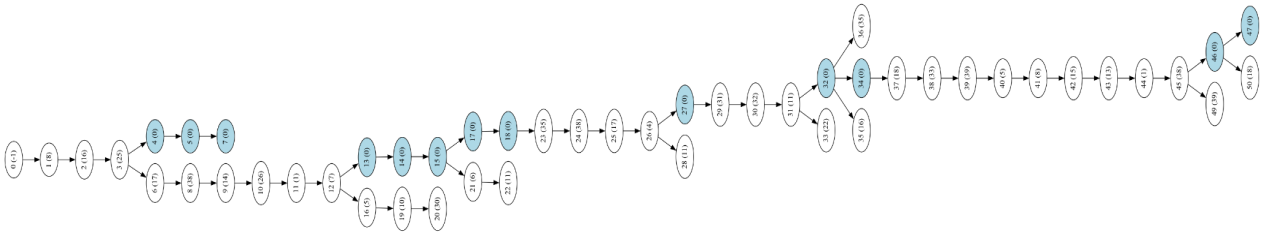
    1. n = 40, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, **zeta = 0.25**, adversary mining power = 0.3



MPU Adv: 0.6

MPU All: 0.791

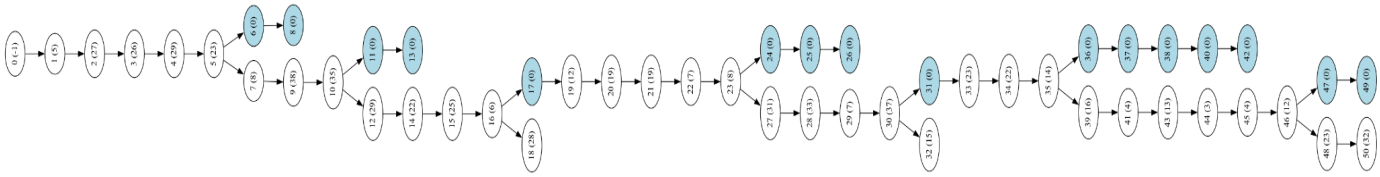
    2. n = 40, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, **zeta = 0.5**, adversary mining power = 0.3



MPU Adv: 0.69

MPU All : 0.71

3. n = 40, z0 = 0.5, z1 = 1, T_{tx} = 10 ms, T_k = 600 ms, **zeta = 0.75**, adversary mining power = 0.3



MPU Adv: 0.6

MPU All: 0.68

Theoretically calculated MPU_{ADV}

Varying Gamma :

Alpha (hashing power of ADV)	Gamma (zeta)	MPU_{ADV}
0.3	0.25	0.3
0.3	0.5	0.32687385740402186
0.3	0.75	0.3537477148080438

Varying Alpha :

Alpha	Gamma (zeta)	MPU_{ADV}
0.1	0.5	0.07241770715096482
0.2	0.5	0.18241758241758246
0.3	0.5	0.32687385740402186

Insights :

From the above results, we can conclude the following:

1) On **increasing adversary mining power**,
    - For Selfish mining attack: The total number of blocks mined by the adversary node increases and the total number of blocks mined by honest nodes decreases. **MPU_{adv} increases**. We can't comment on MPU_{All}. The theoretically calculated MPU_{Adv} differs from the actual MPU_{Adv}. This is because of various reasons such as, we can't exactly calculate gamma, for the sake of calculation we took gamma to be equal to zeta, i.e. the fraction of nodes connected to the adversary node, because gamma depends directly on zeta, more number of nodes connected directly to the adversary node more the chances of them receiving its block first. But directly equating gamma with zeta is not exactly right since there are a number of reasons that could affect gamma such as latencies, we ignored these factors for the theoretical calculations. Though calculated MPU_{Adv} differs from the actual MPU_{Adv}, the pattern followed is same i.e. on increasing hashing power,MPU_{Adv} increases.
    - For Stubborn mining attack: **MPU_{All} decreases**, since the main goal of stubborn mining attack is to make the honest nodes do useless work. This can be easily seen from the results obtained from the experiments we performed.

2) On **increasing** zeta,
    - For Selfish mining attack: On increasing zeta, gamma (fraction of nodes mining on the block produced by the adversary node) increases, since the adversary is well connected in the network, the blocks produced by him will reach the other nodes quickly. And since gamma is increasing so will MPU_{Adv}. This can be easily seen from the results obtained from the experiments we performed.
    - For Stubborn mining attack: On increasing zeta, **MPU_{All} decreases**, since the more well connected the adversary node is in the network, the blocks produced by him will reach the other nodes quickly, and lesser nodes will mine on honest chain, so MPU_{All} will decrease. This can be seen from the results obtained from the experiments we performed.