CS765: Attack Simulation

Team Composition:
Anushka (200050011)
Khyati Patel (200050102)
Shrey Bavishi (200050132)

March 2023

Contents

1 Introduction

Mining attacks on the blockchain consensus mechanism allows a miner or group of miners to gain an unfair advantage over other honest miners.Stubborn mining and selfish mining are two common strategies used by malicious miners in blockchain networks to increase their rewards and undermine the security and decentralization of the system.In this assignment, we have simulated these attacks on top of the discrete-event simulator for a P2P cryptocurrency network, which was built in the last assignment.

Situation	**Selfish Mining**	**Stubborn Mining**
Lead 0', Honest discovers block	Broadcast private block	Continue mining on its private chain
Lead 1, Honest discovers block	Broadcast private block	Broadcast private block
Lead 2, Honest discovers block	Broadcast private chain	Reveal enough private blocks to match the length
Lead $>$ 2, Honest discovers block	Release subchain that ends with block at competition with new honest block	Release subchain that ends with block at competition with new honest block

Table 1: Comparison between adversary behaviour under different attacks in various situation

2 Results

Attack type	**Connectivity**	**Hashing Power of the adversary**	**MPU Average**	**MPU overall**
Selfish	25	5	1.0	0.583658
Selfish	25	15	0.863636	0.51764
Selfish	25	33	0.93023	0.520833
Selfish	50	5	0.6	0.475609
Selfish	50	15	1.0	0.50485
Selfish	50	33	0.976744	0.553191
Selfish	75	5	1.0	0.535211
Selfish	75	15	1.0	0.50370
Selfish	75	33	1.0	0.52325
Stubborn	25	5	0.97058	0.5
Stubborn	25	15	0.98550	0.5
Stubborn	25	33	0.4	0.3333
Stubborn	50	5	0.9	0.5375
Stubborn	50	15	0.98	0.51694
Stubborn	50	33	0.66667	0.428571
Stubborn	75	5	0.71428	0.48
Stubborn	75	15	0.97826	0.510204
Stubborn	75	33	1.0	0.33333

Table 2: Simulation run for 100 nodes

3 Simulation

3.1 Selfish Attack type

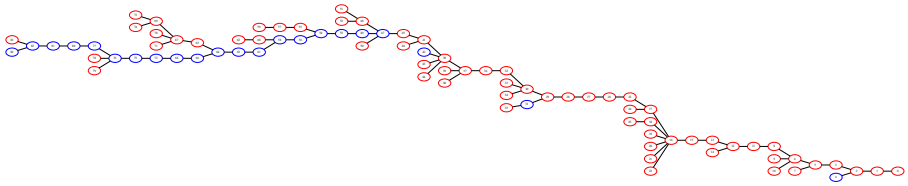

Figure 1: Adversary :: Connectivity : 25 % Hashing Power :15%

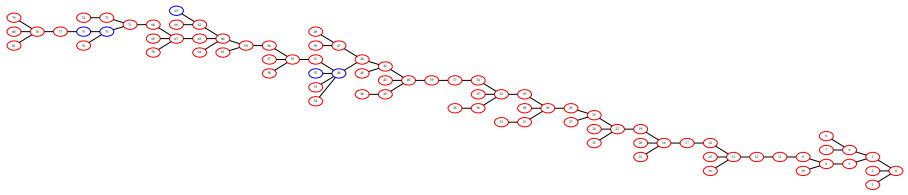

Figure 2: Adversary :: Connectivity : 50 % Hashing Power :5%

3.2 Stubborn Attack type

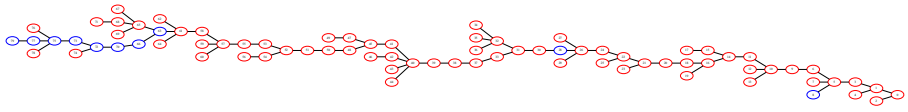

Figure 3: Adversary :: Connectivity : 50 % Hashing Power :5%

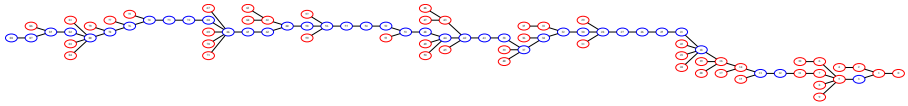

Figure 4: Adversary :: Connectivity : 25 % Hashing Power :33%

4 Observations

4.1 MPU Average Trends

4.1.1 Selfish Attack

- With the increase in connectivity, the MPU average of the adversary decreases
- With the increase in hashing power of the adversary, the MPU average of the adversary goes up.

4.1.2 Stubborn Attack

- With the increase in connectivity, the MPU average of the adversary decreases
- With the increase in hashing power of the adversary, the MPU average of the adversary initially increases ,peaks around 50% and then decreases.

4.2 MPU Overall Trends

4.2.1 Selfish Attack

- With the increase in connectivity, the MPU overall first decreases , minimises around 50% and then increases.
- With the increase in hashing power of the adversary,the MPU overall first decreases , minimises around 50% and then increases.

4.2.2 Stubborn Attack

- With the increase in connectivity, the MPU overall first increases , maximises around 50% and then decreases.
- With the increase in hashing power of the adversary, the MPU overall decreases.

5 Insights

We can deduce the following:

- When there more number of nodes with high hashing power, then the total number of candidate blocks mined is higher.
- Forking is more when the link speed between most nodes is high because the broadcasted blocks reach with a higher delay to the other nodes. Hence more blocks being mined at the same height.
- When hashing power is high but link speed is low this results in even more forking. In this case the ratio of accepted blocks is the lowest given all other conditions are similar.
- While when hashing power is low but link speed is high this results in quite less forking. In this case the ratio of accepted blocks is the highest given that all other conditions are similar.