CS 765 Assignment 2: Simulation of Double Selfish Mining Attack

Hruday Nandan Tudu - 210050067
Shikhar Parmar - 210050145
Pratiksha Deka - 210050122

March 2024

1 Introduction

We've expanded upon our prior assignment by integrating a double selfish mining attack, involving two independent non-colluding selfish miners. Through simulation, we've examined the behaviors of both honest and selfish miners. BlockRec additionally handles scenarios specific to attackers, such as selfish mining strategies, by manipulating private and public blockchains and broadcasting blocks to neighbors. In BlockGen, additionally When the generated block is intended for the private chain, it increments the lead and adds a new BlockGen event to continue the process of block generation.

2 Observations

ζ^1	$MPU_{node_{adv1}}$	ζ^2	$MPU_{node_{adv2}}$	$MPU_{node_{overall}}$
10	0.0	10	0.0	0.592
10	0.33	20	0.5	0.606
10	0.0	30	0.333	0.6
10	0.0	40	0.77	0.562
10	0.333	60	0.4	0.562
20	0.0	20	0.571	0.516
20	0.4	40	0.5	0.531
20	0.25	60	1.0	0.6
30	0.714	30	0.333	0.451
30	0.5	60	0.6	0.562
30	0.0	50	1.0	0.681
40	0.428	10	0.0	0.580
10	0.0	10	0.0	0.592

Table 1: n=20, $T_{tx} = 0.5s$, I(block mean interarrival time)$= 5s$

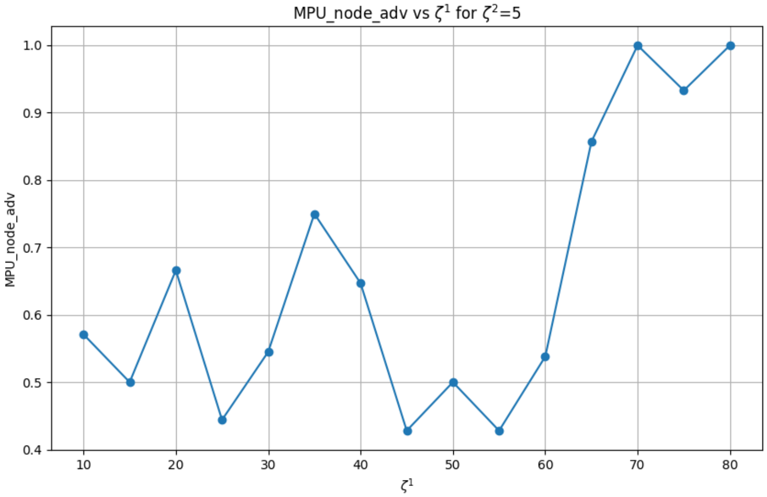

Figure 1: MPU_{adv} vs ζ^1

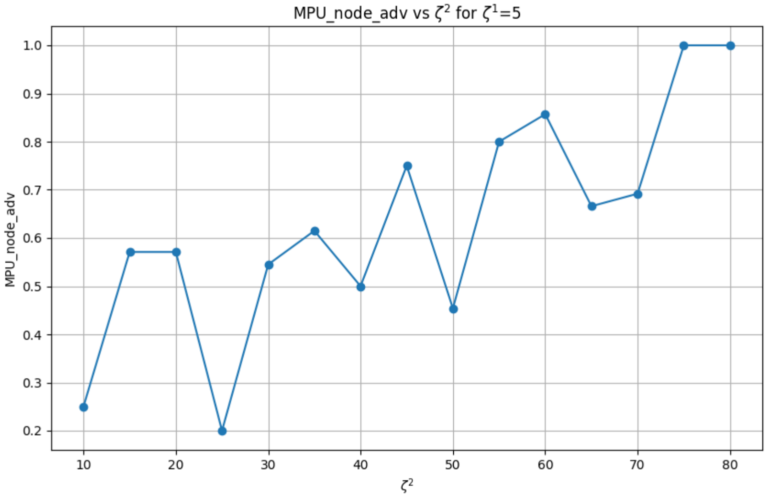

Figure 2: MPU_{adv} vs ζ^2

As the mining power increases the $MPU_{node_{adv}}$ also increases. When the attacker possesses an exceptionally high hashing power, they can consistently release blocks faster than the honest nodes. This results in a situation where for every block generated by the honest nodes, the attacker releases another block, maintaining two chains simultaneously. Eventually, the chain controlled by the attacker prevails, leading to a scenario where the blockchain is evenly split between the honest and attacker-controlled chains

When the attacker possesses lower hashing power, they may occasionally fail to maintain dominance across all potential chains resulting in increasing branching hence decreasing $MPU_{node_{overall}}$.

When both ζ^1 and ζ^2 are comparable within the blockchain network, their influence on block generation becomes more evenly distributed. As a result, the network experiences increased competition, leading to more frequent branching and creation of alternative chains. This increased branching scenario ultimately results in a lower ($MPU_{node_{overall}}$).When there's a notable difference between the magnitudes of ζ^1 and ζ^2, it implies that one adversary possesses significantly more mining power than the other. In such cases, the adversary with higher mining power can dominate block generation more easily, leading to a more centralized control over the blockchain. Consequently, the competition among miners diminishes as the dominant adversary consistently outpaces the other. This reduced competition results in fewer instances of branching and alternative chain creation, ultimately leading to a higher Mining Power Unit ($MPU_{node_{overall}}$)

n	$MPU_{node_{adv1}}$	$MPU_{node_{adv2}}$	$MPU_{node_{overall}}$
5	0.0	0.5	0.6896
10	0.5	0.22	0.636
15	0.0	0.75	0.64
20	0.0	0.166	0.5
25	0.666	0.22	0.485
30	0.0	0.71	0.518
40	0.66	0.4	0.56
50	0.2	0.875	0.607

Table 2: $\zeta^1 = 10$,$\zeta^2 = 50$, $T_{tx} = 0.5s$, I(block mean interarrival time)$= 5s$

As the blockchain expands, there's a tendency for the network to experience more branching or the creation of alternative chains due to factors like block propagation. Consequently, the $MPU_{node_{overall}}$ decreases.

$T_{tx}(s)$	$MPU_{node_{adv1}}$	$MPU_{node_{adv2}}$	$MPU_{node_{overall}}$
0.1	0.428	0.0	0.578
1	1.0	0.5	0.588
7	0.416	0.0	0.583
15	0.428	0.8	0.676
20	0.375	0.0	0.689

Table 3: n=20, I(block mean interarrival time)$= 5s$, $\zeta^1 = 50$, $\zeta^2 = 10$

When the transaction interarrival mean time (T_{tx}) decreases, transactions generates faster resulting in more number of blocks. This heightened competition often results in more frequent branching within the blockchain network, as a consequence of increased branching, the ($MPU_{node_{overall}}$) decreases.

I**(block mean interarrival time)**	$MPU_{node_{overall}}$
0.5	0.38
1	0.45
5	0.75
10	0.8

Table 4: Network(n=20, $T_{tx} = 5s$, $\zeta^1 = 50$, $\zeta^2 = 10$

As I(block mean interarrival time) of blocks decreases, it implies that new blocks are generated more frequently. This leads to a higher likelihood of multiple branches forming within the blockchain. With increased branching, the ($MPU_{node_{overall}}$), decreases.

2.1 Blockchain Tree

Here n=20, $T_{tx} = 0.5s$, $\zeta^1 = 5$, $\zeta^2 = 30$, $I = 5s$. Red represents adversary1's block and blue represents adversary2's block and the green represents honest node's block. $MPU_{overall} = 0.5$ for attacker's tree and $MPU_{overall} = 0.489$ for honest tree.

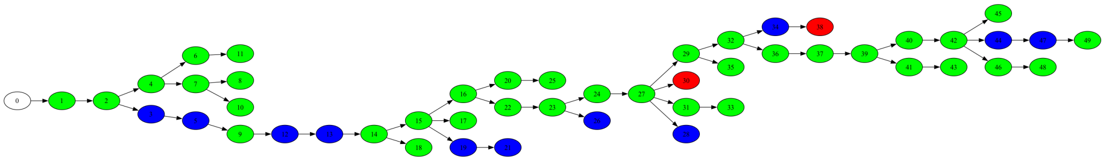

Figure 3: Attacker's Tree

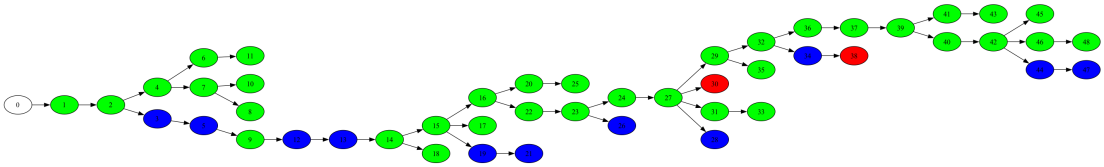

Figure 4: Honest miner's Tree

Here n=20, $T_{tx} = 0.5s$, $\zeta^1 = 20$, $\zeta^2 = 20$, $I = 5s$. $MPU_{overall} = 0.516$ for attacker's tree and $MPU_{overall} = 0.516$ for honest tree.

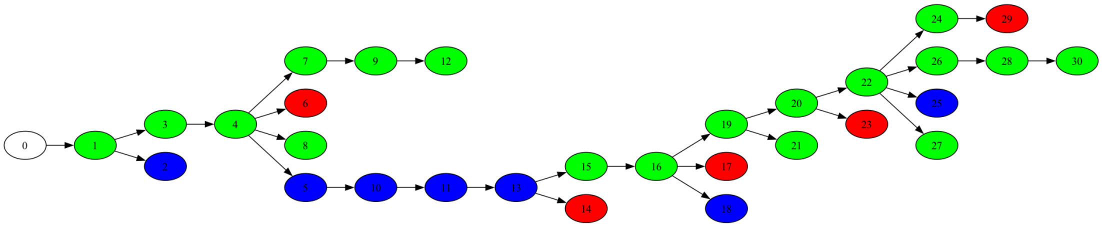

Figure 5: Attacker's Tree

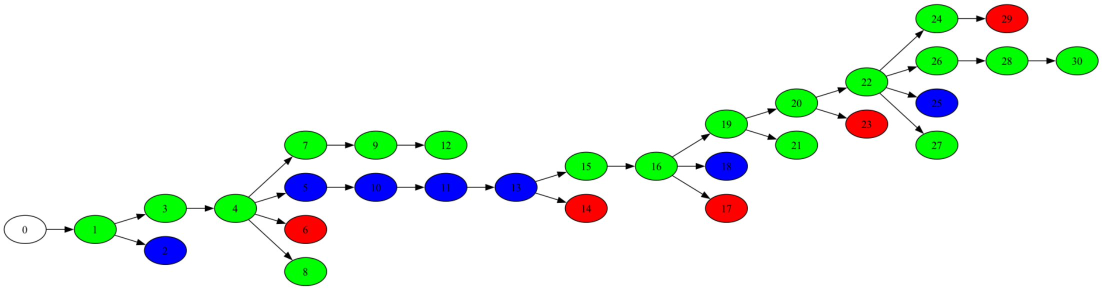

Figure 6: Honest miner's Tree

Here n=20, $T_{tx} = 0.5s$, $\zeta^1 = 30$, $\zeta^2 = 60$, $I = 5s$. $MPU_{overall} = 0.562$ for attacker's tree and $MPU_{overall} = 0.562$ for honest tree.

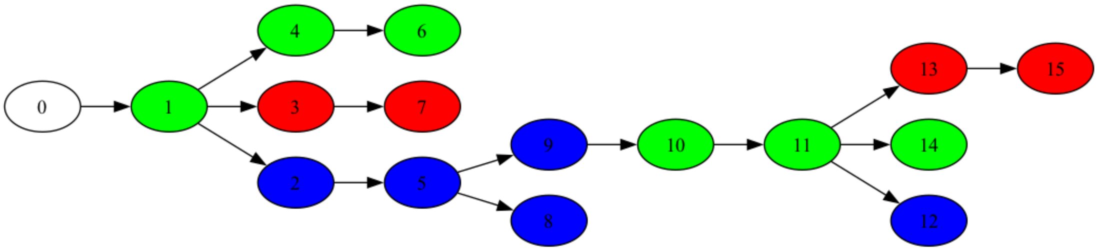

Figure 7: Attacker's Tree

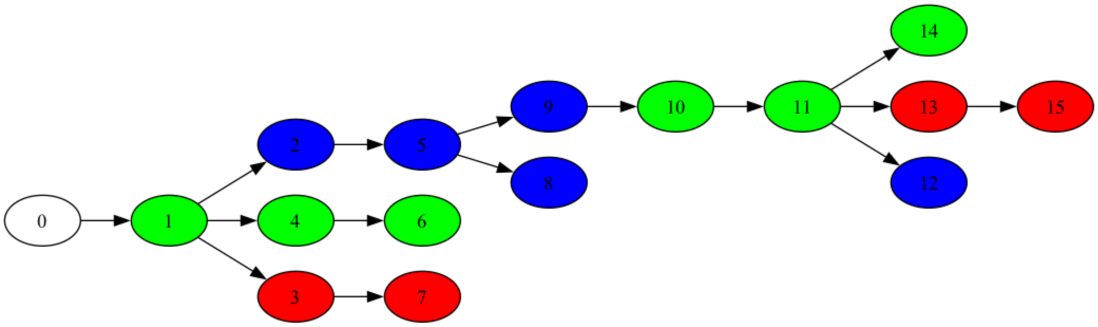

Figure 8: Honest miner's Tree