Assignment 2 Report

Nagendra Singh, 200050081
Manish Kumavat, 200050071

March 19, 2023

1 Comparisons of Two attacks

Check the files **Selfish.pdf** and **Stubborn.pdf** for the blockchain in case of selfish and stubborn respectively. The parameters used are $n = 100$, $\zeta = 50\%$ and hash fraction of adversery= 0.25.

Some key differnce points between these two attack:

- Selfish Mining Attack involves forking the chain by keeping discovered blocks private.
- Adversary mines on own private branch while honest nodes mine on public chain.
- If adversary mines more blocks, they develop a longer lead over public chain.
- Contrary to Selfish Mining, Stubborn Mining Attack maintains competition with honest chain.
- Adversary reveals only next block on private chain to match length of public chain.
- Stubborn mining allows honest chain to grow, resulting in forks composed of more than one block.
- Selfish mining kills off honest chain, resulting in forks composed of a single block.
- Selfish mining is preferred for low mining power values, while stubborn mining is more beneficial for mining power close to 0.5.
- Stubborn mining wastes effort of honest miners, giving higher return than selfish mining attack for large hashing power.

2 Experimental results and thoretical limits

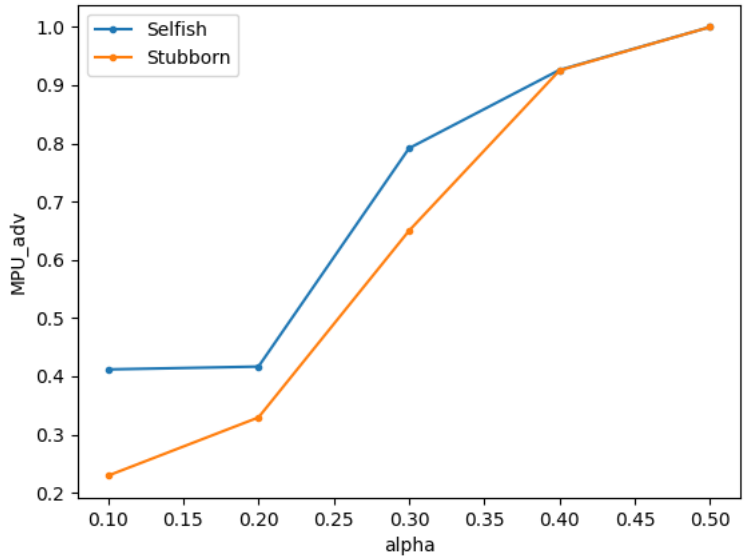
2.1 Variation with hash fraction of adversary

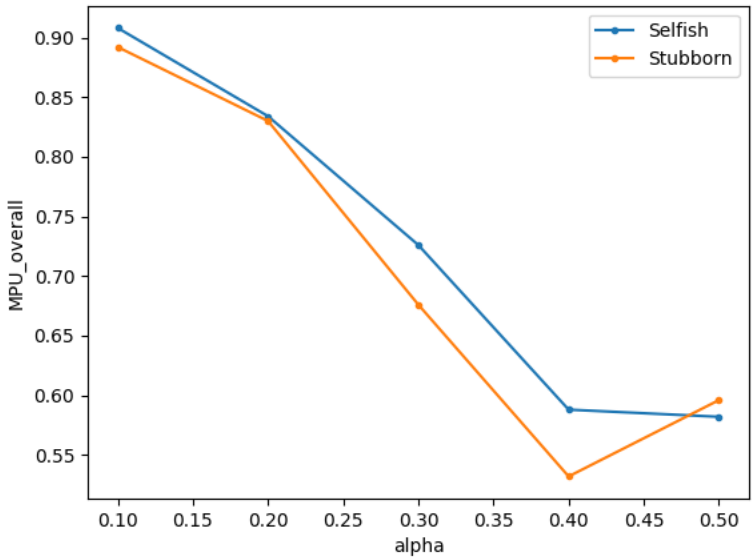
Let **R_pool** be fraction of attacker blocks in the main chain and $gamma_0$ and $gamma_1$ are the theoretical limits as per Eyal and Sirer paper.

Selfish Mining Attack					
Hash fraction	0.1	0.2	0.3	0.4	0.5
Zeta	0.5				
MPU_adv	0.411765	0.416667	0.791667	0.926267	1.000
MPU_Overall	0.908	0.834	0.726	0.588	0.582
gamma_0	0.03564	0.12967	0.27313	0.48372	1.000
gamma_1	0.10919	023516	0.38062	0.56744	1.00000
R_pool	0.046255	0.12466	0.366391	0.683673	0.996564

Stubborn Mining Attack					
Hash fraction	0.1	0.2	0.3	0.4	0.5
Zeta	0.5				
MPU_adv	0.229167	0.329268	0.65	0.925439	1.000
MPU_Overall	0.892	0.83	0.676	0.532	0.596

The experimental graph R_pool values are sandwiched between the gamma=0 and gamma=1 values. Here gamma_0 and gamma_1 are the theoretical estimates given in the Eyal and Sirer paper. In the experimental scenario, the gamma value is between 0 and 1, hence it's expected that the R_pool values will lie in between the gamma_0 and gamma_1 band.
Now let us compare the effect of alpha (adversary hash power) on both attacks:-





In the selfish mining attack, we can observe that the MPU_adv and MPU_overall trends exhibit opposite behaviors. As the adversary's mining power alpha increases, MPU_adv increases. This is expected because, with a higher mining power, the attacker has a greater fraction of blocks entering

the main chain, as it can easily overpower the honest blocks. Consequently, MPU_overall decreases, as more blocks generated by honest miners go to waste, reducing the number of honest blocks in the main chain.

In the stubborn mining attack, when the hashing power increases, the adversary's mining power becomes helpful, and we observe an increase in MPU_adv with alpha. For MPU_overall, the trend is similar to the selfish mining attack. The overall ratio decreases as the fraction of hashing power from honest miners decreases. Therefore, the adversary can waste more honest blocks, obtaining a greater advantage.

3 Variation with zeta

Selfish Mining Attack				
Zeta	0.25	0.5	0.75	1
Hash fraction	0.3			
MPU_adv	0.580645	0.791667	0.636364	0.636364
MPU_Overall	0.776	0.726	0.77	0.8
gamma_0	0.17313			
gamma_1	0.38062			
R_pool	0.185567	0.366391	0.218182	0.1925

Stubborn Mining Attack				
Zeta	0.25	0.5	0.75	1
Hash fraction	0.3			
MPU_adv	0.335404	0.565476	0.657143	0.7423
MPU_Overall	0.676	0.676	0.706	0.708

- The experiments studied the effect of zeta, which represents the fraction of honest nodes to which the adversary is connected, on both stubborn and selfish mining attacks.
- The adversary's hash power was set to 35
- Zeta plays a crucial role in the stubborn mining attack since it heavily relies on winning the competition at every block. The higher the direct connections of the adversary, the greater the chances of the adversary's block winning the competition.
- The zeta parameter does not significantly affect the selfish mining attack. However, the MPU_{adv} value has a slight maximum at zeta 0.5 due to the adversary receiving faster updates of newly created blocks and mining on new honest blocks.
- The optimal zeta should be achieved somewhere in the middle, as observed in the maximum at zeta 0.5.
- The $MPU_{overall}$ in both attacks remains more or less constant and is not significantly affected by varying the zeta parameter, but there is a slight decrease in the $MPU_{overall}$ ratio due to MPU_{adv} increasing and honest miners' blocks struggling to get into the chain.