CS 765, Assignment 2

Guttu Sai Abhishek 180050036

Mulinti Shaik Wajid 180050063

For stubborn mining we have used equal-fork stubborn mining

RESULTS

Values of MPU_{adv} and $MPU_{overall}$ for various values of parameters
n : number of nodes
T_{tx} : Transaction interarrival time(in s)
T_k/hashing_power : Average time to solve block (Tk in s)
Time: Time for which the simulation is run(time to run | no of events ran(in 10^4))
R_{pool} sim: value of R_{pool} calculated using simulation
R_{pool} theo: value of R_{pool} given by theoretical formula
n_honest: no of blocks blocks in main chain of honest
n_adv: no of blocks blocks in main chain of adversary

Number of adversaries is 1. Adv_hash amount of hashing power is given to peer 0(the adversary). Remaining (1-Adv_hash) is distributed among the honest miners.

The formula given by eyal and sirer is

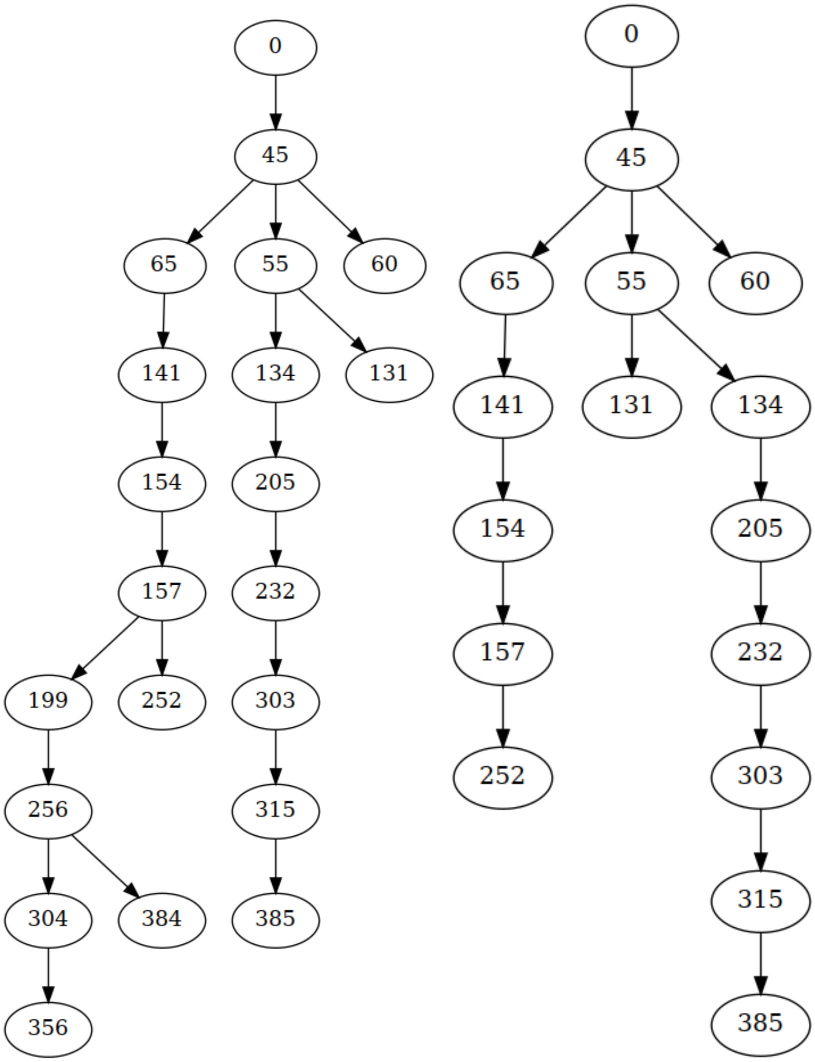
$$R_{pool} = \frac{\alpha(1-\alpha)^2(4\alpha+\gamma(1-2\alpha))-\alpha^3}{1-\alpha(1+(2-\alpha)\alpha)}$$

Type	n	T_{tx}	T_k	ζ	Adv hash	Time	MPU_{adv}	$MPU_{overall}$	n_{honest}	n_{adv}	R_{pool} sim	R_{pool} theo
selfish	50	10	40	0.9	0.35	7.9|4	0.83	0.43	4	5	0.55	0.45
stubborn	50	10	40	0.9	0.35	7.9|4	0.8	0.38	5	4	0.44	---
selfish	50	10	40	0.4	0.35	7|3	0.6	0.33	5	3	0.38	0.4
stubborn	50	10	40	0.3	0.35	7.4|3	0.4	0.47	6	3	0.33	---
selfish	50	10	40	0.2	0.35	7|3	0.5	0.368	5	2	0.28	0.38

selfish	50	10	40	0.9	0.6	7|3	1	0.783	0	18	1	1
stubborn	50	10	40	0.9	0.4	6.6|3	0.71	0.44	3	5	0.625	---
stubborn	50	10	40	0.9	0.7	8.8|4	1	0.591	0	13	1	---
selfish	30	10	40	0.2	0.1	18.5|2	0.25	0.362	16	1	1/17	
stubborn	30	10	40	0.2	0.1	18.5|2	0.25	0.362	16	1	1/17	

1. The values of R_{pool} theo are calculated by assuming that gamma is equal to zeta
2. In the case of selfish mining, according to theory when alpha is 0.35 and gamma is 1, the adversary just manages to have more blocks on the longest chain when compared to honest miners, which can be seen here (5>4).
3. When comparing first and second rows we can see that equal-fork stubborn mining is out-performed by selfish mining for the given parameters
4. In the third row we can see that R_{pool} theo is almost equal to R_{pool} sim
5. When comparing first, third and fifth rows, it can be observed that when value of zeta is decreased to 0.4 from 0.9 R_{pool} decreased from 0.55 to 0.38 which is expected because value of zeta is directly related to gamma, and when zeta is decreased from 0.4 to 0.2 R_{pool} went down to 0.28 from 0.38
6. In case of stubborn mining when value of zeta decreased from 0.9 to 0.3 value of R_{pool} decreased from 0.44 to 0.33
7. In 6th row we can see that when selfish miner has more hashing power when compared all honest miners, selfish miner performs 51% attack and selfish miner generates all blocks in main chain
8. Comparing first and seventh row we can observe that when value of adversary hashing power increases R_{pool} of adversary increased from 0.44 to 0.625
9. From the eighth row, we can observe that when an adversary has majority hashing power, all blocks are created by the adversary.
10. From the ninth and tenth rows we can see that selfish mining/stubborn mining is beneficial when adversary has low hashing power, $MPU_{adversary}<MPU_{overall}$ in this case and it is better for adversary to not use selfish mining/stubborn mining

Blockchain diagrams for parameters mentioned in row-1, for node-0(adversary) and node-1(honest)


0
45
65
55
60
141
134
131
154
205
157
232
199
252
303
256
315
304
384
385
356
0
45
65
55
60
141
131
134
154
205
157
232
252
303
315
385