CS 765

200020012, Adish Shah
200050093, Akshay Padakanti
200050106, Pinkesh Raghuvanshi

Assignment-2

Contents

1 Selfish Mining

Comparison of RPool values of Adversary for theoretical and practical values:

Based on the value of ζ (the fraction of honest nodes an adversary is connected to), different simulations were conducted for different values of hashing power of adversary.

The theoretical value for Rpool, as obtained in the paper, should be (for $\alpha < 0.5$) :

$$Rpool = \frac{\alpha(1-\alpha)^2[4\alpha + \gamma(1-2\alpha)] - \alpha^3}{1 - \alpha[1 + (2-\alpha)\alpha]}$$

For the purpose of our analysis, we took γ to be the same as ζ, which is fair to an extent, because of the fact that the adversary's blocks are smaller in size (since they only contain the coinbase transaction), and the fact that the adversary doesn't forward any honest block.

For the configuration `nodes = 30`, `endtime = 3000`, `interarrival time = 10`, `block interarrival time = 20`, `z = 0.5` (fraction of fast nodes), the following trends of Rpool were obtained with varying hashing power of adversary.

- $\zeta = \mathbf{0.25}$

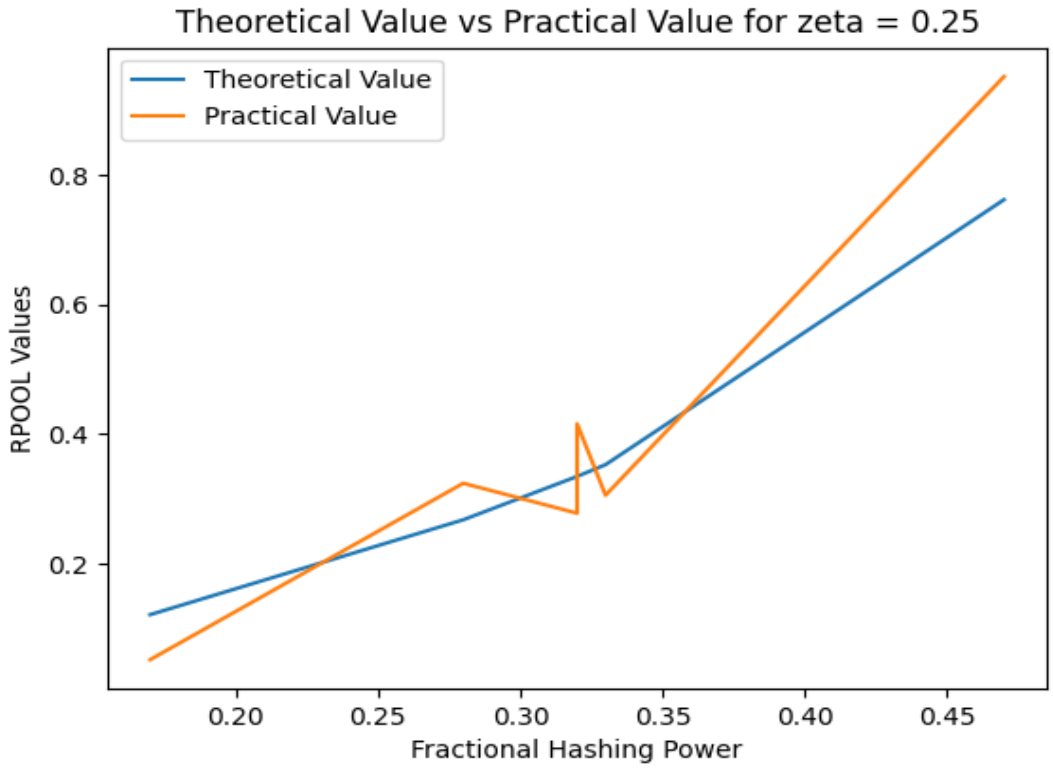

Figure 1: Rpool vs Fraction Hashing Power for Selfish Mining ($\zeta = 0.25$)

```
Fractional Hash Power -> 0.17,   Rpool Theoretical -> 0.12102163391939139,   Rpool Practical -> 0.051470588235294115
Fractional Hash Power -> 0.28,   Rpool Theoretical -> 0.2675970687958001,   Rpool Practical -> 0.32407407407407407
Fractional Hash Power -> 0.32,   Rpool Theoretical -> 0.3345646969887867,   Rpool Practical -> 0.2777777777777778
Fractional Hash Power -> 0.32,   Rpool Theoretical -> 0.3345646969887867,   Rpool Practical -> 0.416
Fractional Hash Power -> 0.33,   Rpool Theoretical -> 0.35276056721780974,   Rpool Practical -> 0.3055555555555556
Fractional Hash Power -> 0.47,   Rpool Theoretical -> 0.762203407925092,   Rpool Practical -> 0.9523809523809523
-----------------------------------------------------------------------------------------
```

Figure 2: Rpool values and Fraction Hashing Power for Selfish Mining ($\zeta = 0.25$)

- $\zeta = \mathbf{0.5}$

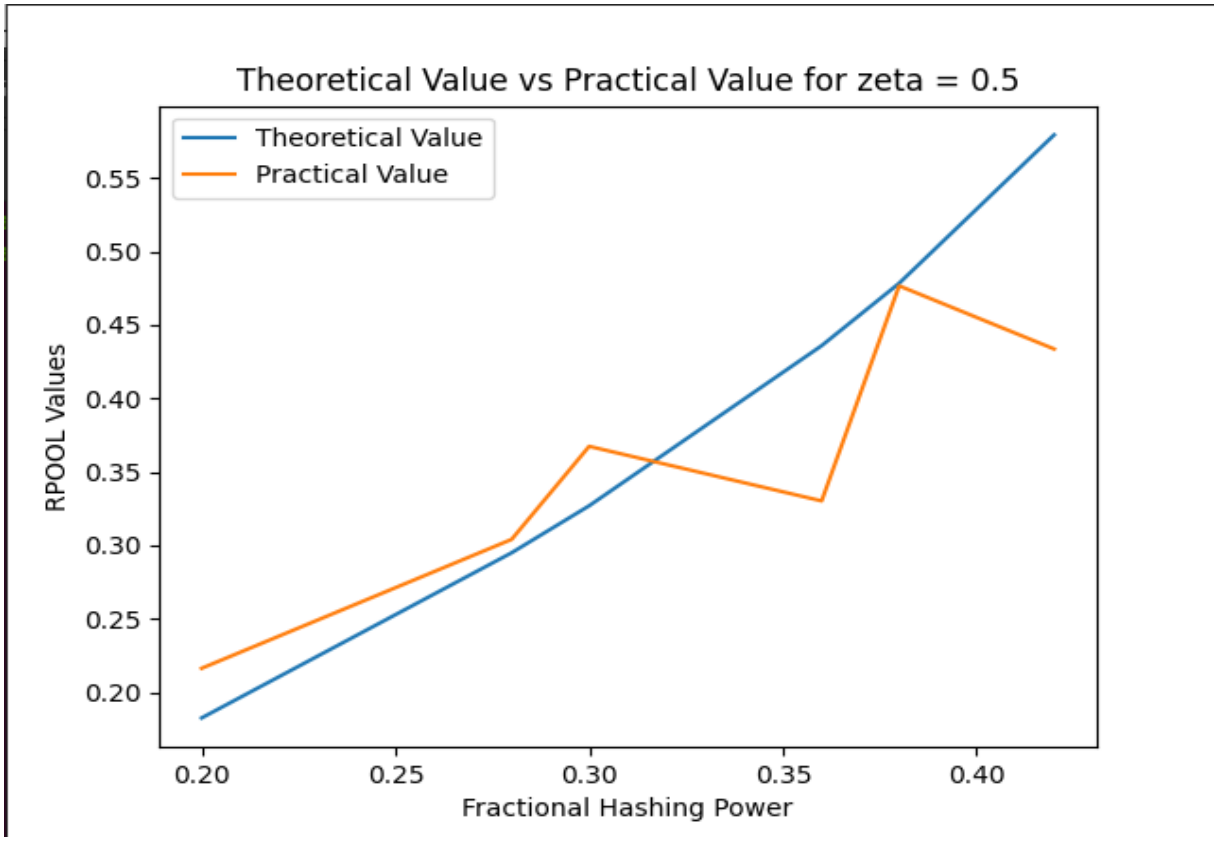

Figure 3: Rpool vs Fraction Hashing Power for Selfish Mining ($\zeta = 0.5$)

```
Fractional Hash Power -> 0.2,   Rpool Theoretical -> 0.18241758241758246,   Rpool Practical -> 0.21621621621621623
Fractional Hash Power -> 0.28,   Rpool Theoretical -> 0.29488351744504,   Rpool Practical -> 0.304
Fractional Hash Power -> 0.3,   Rpool Theoretical -> 0.32687385740402186,   Rpool Practical -> 0.3673469387755102
Fractional Hash Power -> 0.36,   Rpool Theoretical -> 0.43589160053900283,   Rpool Practical -> 0.330188679245283
Fractional Hash Power -> 0.38,   Rpool Theoretical -> 0.4783721171180506,   Rpool Practical -> 0.4766355140186916
Fractional Hash Power -> 0.42,   Rpool Theoretical -> 0.579441862935132,   Rpool Practical -> 0.4336283185840708
-----------------------------------------------------------------------------------------
```

Figure 4: Rpool values and Fraction Hashing Power for Selfish Mining ($\zeta = 0.5$)

- $\zeta = \mathbf{0.75}$

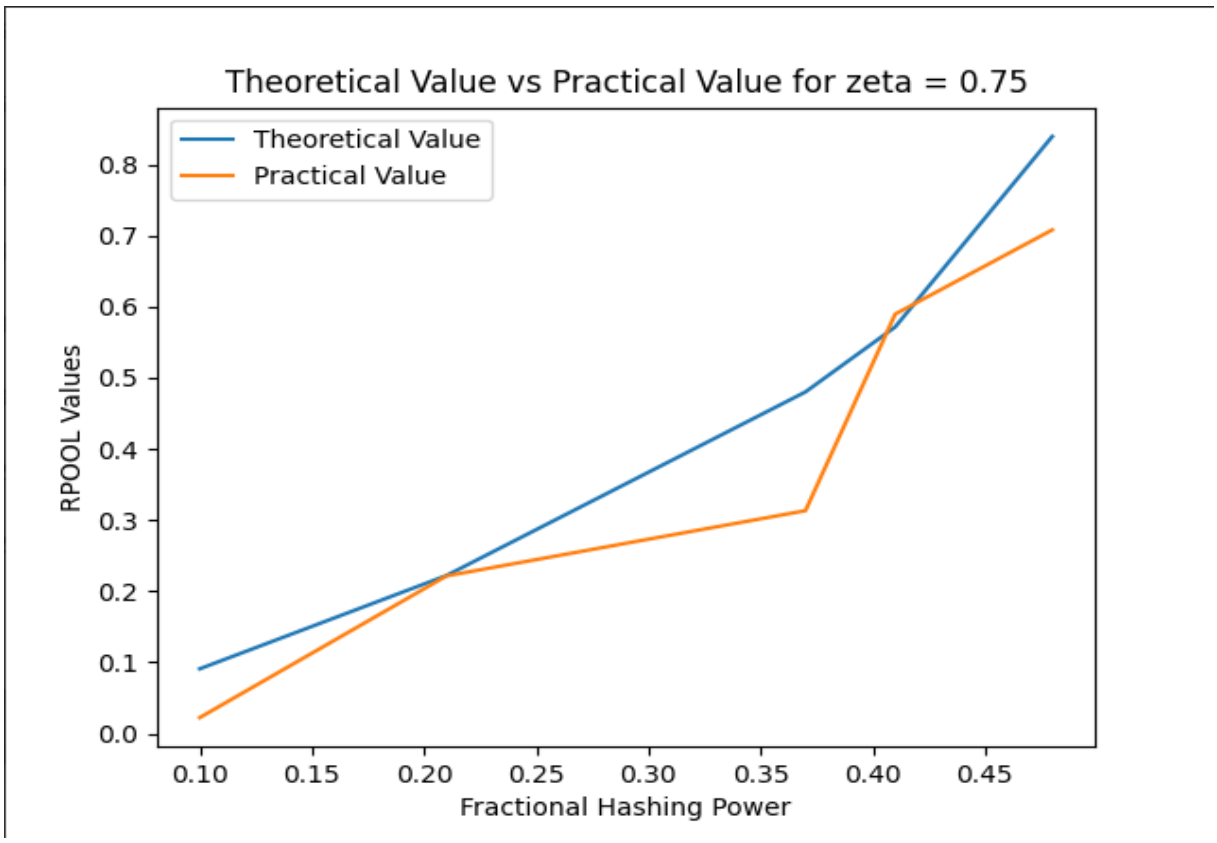

Figure 5: Rpool vs Fraction Hashing Power for Selfish Mining ($\zeta = 0.75$)

```
Fractional Hash Power -> 0.1,   Rpool Theoretical -> 0.09080590238365495,   Rpool Practical -> 0.022222222222222223
Fractional Hash Power -> 0.21,   Rpool Theoretical -> 0.22198063879188987,   Rpool Practical -> 0.22142857142857142
Fractional Hash Power -> 0.37,   Rpool Theoretical -> 0.4800893074402795,   Rpool Practical -> 0.31313131313131315
Fractional Hash Power -> 0.41,   Rpool Theoretical -> 0.5714185782765919,   Rpool Practical -> 0.5894736842105263
Fractional Hash Power -> 0.48,   Rpool Theoretical -> 0.8392762909913305,   Rpool Practical -> 0.7078651685393259
--------------------------------------------------------------------------------
```

Figure 6: Rpool values and Fraction Hashing Power for Selfish Mining ($\zeta = 0.75$)

From the graph we can observe that the values of Rpool from simulation is roughly the same as theoretical value, which was expected. Because of this, if can also be confirmed that the value of Rpool increases with ζ (analogous to γ). There is a little noise in the pattern of the observed data, which can perhaps be decreased by further increasing the simulation time, so that we have more number of instances to derive the data from.

2 Stubborn Mining

Comparison of RPool values of Adversary for Selfish Mining and Stubborn Mining with same configs:

As suggested in the Problem Statement, our stubborn mining policy is a combination of Lead-stubborn mining and Equal Fork stubborn mining from the paper.
For same configurations of nodes, interarrival times, ζ values, adversary hash scaling factor, simulation was run and following data was observed.

Note: The **fractional hash power scale** (alpha scale) attribute scales the hashing power of adversary compared to other honest blocks. Further, it is normalised in the code during initialisation of the nodes.

Zeta (Fraction of honest nodes adversary is connected) = 0.25

- **Fractional Hash Power Scale = 5**

  Selfish Mining Rpool value = **0.0454545**
  Stubborn Mining Rpool value = **0.03883495**

Figure 7: Selfish Mining for $\zeta = 0.25$ and alpha scale = 5

Figure 8: Stubborn Mining for $\zeta = 0.25$ and alpha scale = 5

- **Fractional Hash Power Scale = 10**

  Selfish Mining Rpool value = **0.229007**
  Stubborn Mining Rpool value = **0.116504**

Figure 9: Selfish Mining for $\zeta = 0.25$ and alpha scale = 10

Figure 10: Stubborn Mining for $\zeta = 0.25$ and alpha scale = 10

- **Fractional Hash Power Scale = 15**

  Selfish Mining Rpool value = **0.336207**
  Stubborn Mining Rpool value = **0.5**

Figure 11: Selfish Mining for $\zeta = 0.25$ and alpha scale = 15

Figure 12: Stubborn Mining for $\zeta = 0.25$ and alpha scale = 15

Zeta (Fraction of honest nodes adversary is connected) = 0.5

- **Fractional Hash Power Scale = 5**

  Selfish Mining Rpool value = **0.234375**
  Stubborn Mining Rpool value = **0.27102803738**

Figure 13: Selfish Mining for $\zeta = 0.5$ and alpha scale = 5

Figure 14: Stubborn Mining for $\zeta = 0.5$ and alpha scale = 5

- **Fractional Hash Power Scale = 10**

  Selfish Mining Rpool value = **0.451327**
  Stubborn Mining Rpool value = **0.510638**

Figure 15: Selfish Mining for $\zeta = 0.5$ and alpha scale = 10

Figure 16: Stubborn Mining for $\zeta = 0.5$ and alpha scale = 10

- **Fractional Hash Power Scale = 15**

  Selfish Mining Rpool value = **0.717391**
  Stubborn Mining Rpool value = **0.758621**

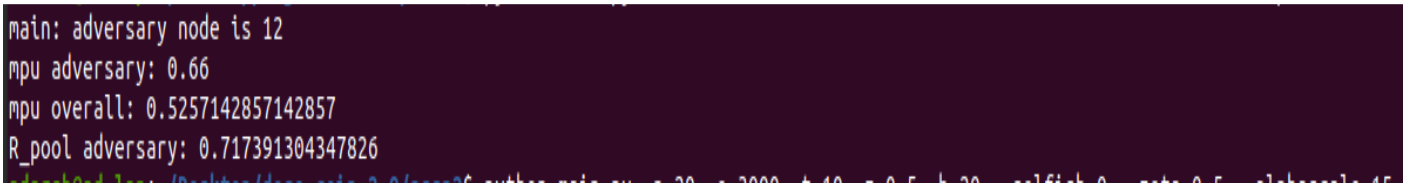

Figure 17: Selfish Mining for $\zeta = 0.5$ and alpha scale = 15

Figure 18: Stubborn Mining for $\zeta = 0.5$ and alpha scale = 15

Zeta (Fraction of honest nodes adversary is connected) = 0.75

- **Fractional Hash Power Scale = 5**

  Selfish Mining Rpool value = **0.191667**
  Stubborn Mining Rpool value = **0.238095**

Figure 19: Selfish Mining for $\zeta = 0.75$ and alpha scale = 5

Figure 20: Stubborn Mining for $\zeta = 0.75$ and alpha scale = 5

- **Fractional Hash Power Scale = 10**

  Selfish Mining Rpool value = **0.392857**
  Stubborn Mining Rpool value = **0.4081632**

Figure 21: Selfish Mining for $\zeta = 0.75$ and alpha scale = 10

Figure 22: Stubborn Mining for $\zeta = 0.75$ and alpha scale = 10

- **Fractional Hash Power Scale = 15**

  Selfish Mining Rpool value = **0.6704545**
  Stubborn Mining Rpool value = **0.9444444**

Figure 23: Selfish Mining for $\zeta = 0.75$ and alpha scale = 15

Figure 24: Stubborn Mining for $\zeta = 0.75$ and alpha scale = 15

So, we can see that stubborn mining outperforms selfish mining at almost every set of parameters in the given reasonable range, except for low values of ζ and α ($\zeta = 0.25$ and Fractional Hash Power Scale ≤ 10). So, our observations are pretty consistent with the pattern of the results in the paper for Stubborn Mining.