Detection constraint for Harvesting Attack in Proof of Work mining pools

Veronika Kuchta and Yevhen Zolotavkin

Monash University, Clayton, Australia
veronika.kuchta@monash.edu, yevhen.zolotavkin@monash.edu

Abstract. PoW consensus largely depends on mining that mostly happens in the pools where Pay Per Share (PPS) and Pay Per Last N Shares (PPLNS) are the most common reward schemes that are offered to the affiliated miners by pool managers. In this report, we describe detection fonstraint for "pool harvesting" attack that is harmful for honest miners. In order to profit from the attack on PPLNS pool malicious manager declares that a non-existent miner A joins that pool. She then collects the portion of reward that corresponds to the mining power of the proclaimed miner A. We discuss a number of statistical tests that may be used by honest miners in PPLNS pool to detect the attack.

1 General description of attack

Our attention is on the system of two mining pools with different reward principles governed by the same manager. We demonstrated that collective participation in mining process can be exploited by the malicious manager in the environment of compensation mechanisms where reward is proportionally distributed among pool miners in one of the pools.

The number of blocks produced by every miner in PPLNS pool can be described using Poisson distribution [1]. We are the first who propose a lower boundary constraint for the performance of a miner that should be fulfilled in order to avoid negative reaction from the rest of the pool. This constraint depends on the power of the miner and is obtained from One Poisson Mean Test (OPMT) [2]. We introduced a new method for attack that commands malicious manipulations by utilizing PPS pool as a source of the newly mined blocks. According to the method, manager can rely on PPS pool productivity to fulfill the OPMT constraint for a mid-sized miner in the future rapidly. Such projection allows her to safely deffer fractional payments of certain size with the aim of earning interest. The attack is implemented by introducing into the other (PPLNS) pool a non-existent miner A with power p_A who starting from time t_0 redirects all her reward to the manager (see fig. 1). We studied multiple parameters that shape the attack and demonstrated that in some settings the malicious manager is able to maintain steady incentive for attack while remaining undetected by honest miners.

2 Detection constraint

In order to remain undetected by honest miners in PPLNS pool, manager should submit blocks at the rate which corresponds to the declared mining power p_A. In line with the

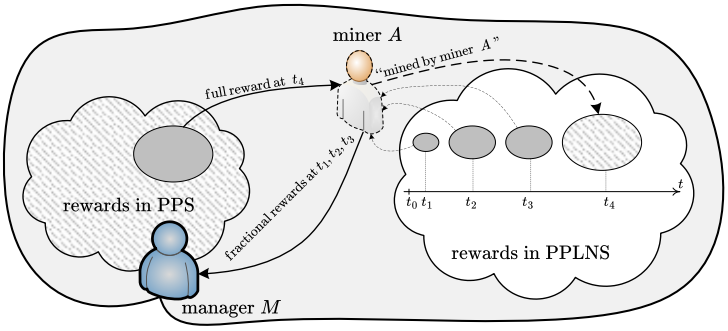

Fig. 1: Generalized scheme of pool harvesting attack.

assumption of honest mining (which is to be verified by the group of honest miners), the number of blocks that were mined by miner A is distributed according to the Poisson distribution with parameter λ. Poisson distribution is commonly used in cases where the probability of a rare event is small meaning that the number of occurrences of those events in a large number of trials is distributed as a Poisson random variable. We will demonstrate that the proposed method of attack supplies λ denoting the number of block submissions from PPS into PPLNS pool such that this λ agrees with the λ_A declared by the attacker.

Test1: One-Poisson-Mean test. This test is to evaluate performance of miner A on time intervals $[t_0, t']$, $t' \leq t_{\mathcal{T}}$. We define X being the number of submitted PPS blocks into PPLNS pool during this time period. We say, that X is a Poisson variable with parameter $\lambda = \mu \cdot t'$, with μ being the expected rate per unit of time.

The probability that $X = x$, for $x = 0, 1, 2, 3, ...$, i.e. X is a natural number of events is defined as follows

$$Pr(X = x) = \frac{e^{-\lambda}\lambda^x}{x!}.$$

The cumulative probability function of X being smaller or equal x is defined in dependence of Gamma function as follows:

$$F_X(x) = Pr(X \leq x) = \sum_{i=0}^{x} \frac{e^{-\lambda}\lambda^i}{i!} = 1 - \frac{1}{x!}\int_0^{\lambda} y^x e^{-\lambda} dy = 1 - F_{\Gamma\beta}(\lambda, x).$$

where $F_{\Gamma\beta}(\lambda)$ is the cumulative distribution function of variable G which is distributed according to the Gamma distribution, $G \sim \Gamma(x+1, \beta)$ with $\beta = 1$ being the rate parameter of gamma distribution function. Poisson test was conducted to test hypothesis

$$(H_0 : \ \lambda \geq \lambda_A \text{ vs. } H_a : \ \lambda < \lambda_A).$$

Assuming that Hypothesis H_0 is true, the probability that H_0 is rejected with significance level α. We define a set $\mathcal{L}_\alpha$ of all λ for which the null hypothesis is true but is

rejected with probability not greater then α. This happens if $\lambda < \lambda_{\min}$, where λ_{min} is defined as follows:

$$\lambda_{\min} = \max_{\lambda_A, \mathcal{L}_\alpha} \lambda^*, \ \left(\lambda^* \in \mathcal{L}_\alpha\right) \leftrightarrow \left(F_{\Gamma\beta}\left(\lambda_A; \lambda^*\right) > 1 - \alpha\right),$$

By comparing the range for λ with $\lambda_{\min}$ we conclude that hypothesis H_0 can not be rejected in favour to H_a with significance level $\alpha = 0.05$ (or lower) in any single trial.

Test 2: χ^2-Goodness of fit test. We use this test to find out that the observed sample distribution is comparable with the expected Poisson distribution. We divide the sampled data (number of events) into intervals. Then we compare the number of events which actually fall into these intervals with the expected number of events in each interval.
Next, we define the Null hypothesis H_0 and the alternative hypothesis H_a of this test as follows: Let $Pois_\lambda$ be the expected Poisson distribution of happening events (t_j) (submitted blocks at time t_j) with parameter λ, and θ be the sampled distribution, then we have

$$H_0 : \vartheta_j = Pois_\lambda(t_j) \ \text{ vs. } \ H_a : \vartheta_j \neq Pois_\lambda(t_j).$$

We define the value of χ^2-goodness of fit test is defined as follows:

$$\chi^2 := \sum_{j \in \mathbb{A}^{t_\mathcal{T}}} \frac{\left(\theta_j - Pois_\lambda(t_j)\right)^2}{Pois_\lambda(t_j)}.$$

References

1. Rosenfeld, M.: Analysis of Bitcoin Pooled Mining Reward Systems. arXiv preprint arXiv:1112.4980 (2011)
2. Weerahandi, S.: Exact Statistical Methods for Data Analysis. Springer New York (2003)