Name : Agung Panjimasjaya

Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack

Summary:

Selfish mining is a well-known attack where a selfish miner, under certain conditions, can gain a disproportionate share of reward by deviating from the honest behavior.

In this paper, we take an in-depth look at the mining attack strategy space, and make several interesting revelations. We investigate strategies that increase the revenue of the attacker.

- Selfish mining is not optimal for a large parameter space.
- An attacker's revenue is increased by non-trivial combi-
- nations of stubborn mining and network-level attacks.
- Systematic exploration of strategy space.

This mining model has three main parameters:

- Hashpower of attacker: the fraction of the network's total hashpower controlled by the attacker, henceforth referred to as "Alice".
- Hashpower of the honest public (i.e., Bob): the fraction of the hashpower of the remaining network, henceforth referred to as "Bob".
- Alice's network influence : fraction of Bob's network (in terms of hashpower) that will mine on Alice's (i.e., the attacker's) block when Alice and Bob have released a block at (approximately) the same time resulting in an equal length fork.

Detecting and inferring attacks. Eclipse attacks and stubborn mining can likely be detected if they occur in practice. One way is by observing the stale block rate – a stale block is one that has valid transactions and proof-of-work, but is ultimately excluded from the main chain.

Eclipse attacks can benefit the victim. As it turns out, the "victim" of an eclipse attack can sometimes even profit from the attack, even when the attacker uses the optimal strategy (as shown in Figure 16). In such cases, Alice and Lucy effectively have a mutually beneficial relationship and share their increased revenue relative to Bob.