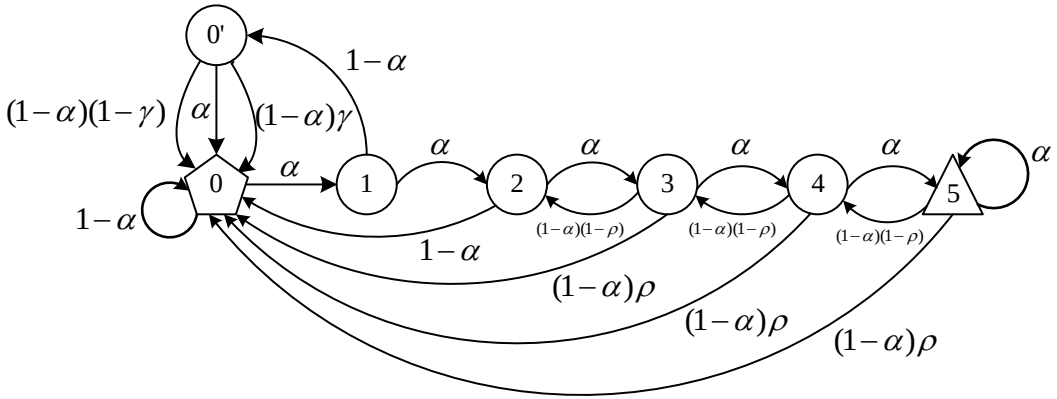
To Be Detected or Not: A Hybrid Selfish Mining Attack and Countermeasures

Yilei WANG , Junxi ZHU , Zhaojie WANG , Andrea BRACCIALI, Minghao ZHAO, Wenjian LUO, Huiyu ZHOU

Frontiers of Computer Science, DOI: 10.1007/s11704-026-51791-9

Problems & Ideas

- Problems of conventional selfish mining attacks:
  - Either the existing attacks yield high rewards but carries a high risk of detection due to its high fork rate.
  - or the existing attacks avoid to be detected, resulting in lower attack rewards.
- Ideas: A hybrid selfish mining attack, where the attacker combines the one-time releasing attack and the SM1.

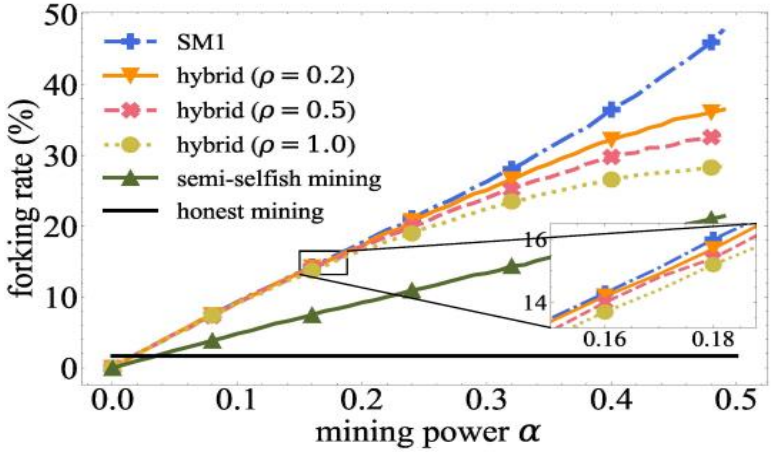


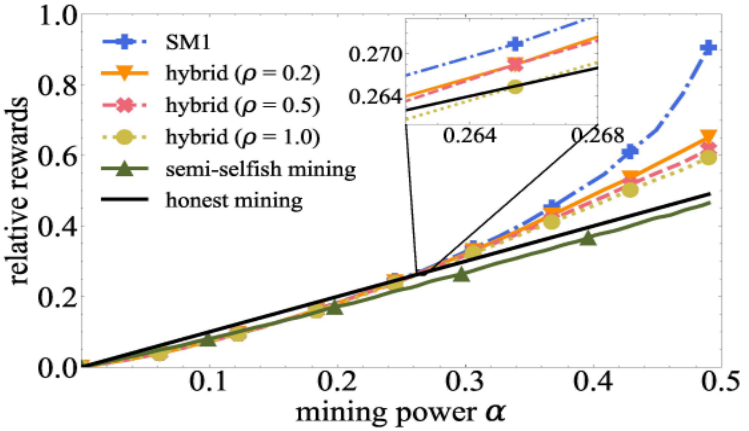
The Hybrid Attack

This is a Markov decision process of the hybrid attack. The numbers in polygon, circle and triangle denote the states. The arrows denote the state transition, the number over which denotes the transitionprobability.

Main Contributions

- Contributions:
  - The one-time releasing attack is proposed, where the attacker releases all private blocks at their convenience, provided the private chain is longer than 2.
  - a hybrid selfish mining attack, where the at tacker adopts the one-time releasing attack with probability and the SM1 with probability 1 – ??.
  - A disparity-assisted plane sweep-based rendering method to weaken interpolation errors caused by bad pixels in the disparity maps.





Interpolation and stereo results yielded by each method versus the iteration time. Left: the average PSNR values of interpolation; Right: the average error rates at 0.5-pixel threshold of stereo.