A Game Theoretic Analysis on Block Withholding Attacks Using the Zero-Determinant Strategy

Title	A Game Theoretic Analysis on Block Withholding Attacks Using the Zero-Determinant Strategy
Publication Type	Conference Paper
Year of Publication	2019
Authors	Hu, Qin, Wang, Shengling, Cheng, Xiuzhen
Conference Name	2019 IEEE/ACM 27th International Symposium on Quality of Service (IWQoS)
Date Published	jun
Keywords	bitcoin, Bitcoin's incentive system, block withholding attack, block withholding attacks, blockchain, conventional game theory, data mining, delays, distributed system, game theoretic analysis, game theoretic security, game theory, Games , human factors, macroscopic utility, mutual attacks, open mining pools, Predictive Metrics, pubcrawl, Scalability, security of data, security threats, ZD adopter, ZD player, Zero-Determinant strategy
Abstract	In Bitcoin's incentive system that supports open mining pools, block withholding attacks incur huge security threats. In this paper, we investigate the mutual attacks among pools as this determines the macroscopic utility of the whole distributed system. Existing studies on pools' interactive attacks usually employ the conventional game theory, where the strategies of the players are considered pure and equal, neglecting the existence of powerful strategies and the corresponding favorable game results. In this study, we take advantage of the Zero-Determinant (ZD) strategy to analyze the block withholding attack between any two pools, where the ZD adopter has the unilateral control on the expected payoffs of its opponent and itself. In this case, we are faced with the following questions: who can adopt the ZD strategy? individually or simultaneously? what can the ZD player achieve? In order to answer these questions, we derive the conditions under which two pools can individually or simultaneously employ the ZD strategy and demonstrate the effectiveness. To the best of our knowledge, we are the first to use the ZD strategy to analyze the block withholding attack among pools.
DOI	10.1145/3326285.3329076
Citation Key	hu_game_2019

security of data Scalability game theory pubcrawl bitcoin blockchain Data mining distributed system delays security threats Games Human Factors Predictive Metrics game theoretic security Bitcoin's incentive system block withholding attack block withholding attacks conventional game theory game theoretic analysis macroscopic utility mutual attacks open mining pools ZD adopter ZD player Zero-Determinant strategy