EasyChair Preprint

№ 1514

A New Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools with Defense Cost

Cuiwen Ying, Rongxin Zheng, Jun Shao, Guiyi Wei,
Jianming Kong, Yekun Ren, Hang Zhang and Weiguang Hou

September 14, 2019

A New Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools with Defense Cost

No Author Given

No Institute Given

Abstract. Since almost all new bitcoins nowadays are minted by mining pools, the security of mining pools is quite crucial to the health of the Bitcoin system. Among the attacks targeting mining pools, the distributed denial-of-service (DDoS) is the notable one. Previous research shows that mining pools would launch DDoS attacks on others when the size is relatively large. However, no mining pools claimed responsibility to any DDoS attacks on mining pools till now. In this paper, we refine the previous game-theoretic analysis model by adding a DDoS defense cost, which makes the success possibility of DDoS attacks dynamic. With the modified model, we obtain some new conclusions. More mining cost less attack possibility. We also observe that mining pools will not launch DDoS attacks to others if the success possibility is not large enough.

1 Introduction

Due to the decentralized, crypto-protected, and transparent properties, Bitcoin [**?**] has gained considerable popularity during the past ten years. It has become like a worldwide currency. One reason for this tremendous success is that everybody could be the maker of a new bitcoin. Only if he/she finds a solution to a specific cryptographic puzzle before others, he/she can own the new bitcoins. In other words, more computing resource, more bitcoins. This situation leads to two strategies to earn more bitcoins. One is to increase competitive computing resources, which results in a prosperous market for specialized hardware [**?**]. The other is to collaborate with some other miners to constitute a mining pool, which evolves to that almost all new bitcoins are minted/mined by mining pools currently [**?**].

Due to the importance of the mining pools in the Bitcoin system, many attacks targeted on mining pools have emerged. Among those, the distributed denial of service attacks (DDoS) is the most famous one. The earliest reported DDoS attacks can even go back to 2011 [**?**], and one peak of DDoS incidents on mining pools happened in 2015 [**?**]. We also witnessed that serval mining pools, such as Altcoin.pw [**?**] and GHash.io [**?**], shut down (partially) due to repeated DDoS attacks. Currently, anti-DDoS implementation is a crucial part of the standard configuration for mining pools [**?**]. However, DDoS attacks still happen from time to time [**?**]. It is believed that DDoS attacks come from two kinds of

entities. One is the hackers whose goal is to hijack the attacked mining pool. The other is the competing mining pool who wants to increase the probability of winning the mining competition. Nonetheless, to the best of our knowledge, no mining pool claimed responsibility for any DDoS attack on mining pools till now. A natural question arises about whether the mining pools would really launch the DDoS attack on other mining pools.

Johnson et al. [**?**] responded to the above question by using the game theory. According to their analysis, the relative size of mining pools is a vital factor for the mining pool to choose the strategy between investing in computation and engaging in attack. In particular, large mining pools have a higher possibility to be attacked than small ones, and larger mining pools are more willing to attack smaller ones. In other words, the relative large mining pools would like to launch DDoS attacks on each other. This analysis result is somewhat different from the reality where the large mining pools are living peacefully. In this paper, following Johnson et al.'s method, we would like to re-analyze the DDoS attacks happened between mining pools from game-theoretic point of view.

Our contributions in this paper can be summarized as follows.

- To reflect the fact that the current mining pools are usually equipped with an anti-DDoS system, we add DDoS defense cost into Johnson et al.'s model. This modification makes the success possibility of DDoS attacks dynamic and turns out a new game's equilibria. We also add the operational cost into the mining cost of mining pools in Johnson et al.'s model where the mining cost only contains investment cost.
- With the new analysis model, we obtain some new conclusions. More mining cost, less DDoS attack possibility. The most salient observation is that the relative large mining pools would not DDoS attack each other if the success possibility of attack is not large enough.

Our presentation proceeds as follows. In section 2, we briefly discuss the related work, focusing on the contents related to DDoS victims. In section 3, we develop and analyze a series of game-theoretical models. In section 4, we carry out numerical and graph analysis and expound the practical significance. In section 5, we summarize the research contents and look forward to the future.

2 Related Work

Bitcoin's incentive mechanism encourages miners to mine and disseminate new blocks they have constructed to reap benefits. From the game-theoretic point of view, miner always pursuit higher profit even if they should deviate from the standard mining strategy. This deviation strategy may even be a proactive attack on other miners or mining pools, such as DDoS attacks.

From previous studies, we can find economic expressions to help understand DDoS attacks and possible countermeasures. Christian et al. [**?**] investigated the motivation of a limited group of rational defenders when they were threatened by botnets (e.g., for DDoS attacks). Liu et al. [**?**] established a game theory

model and determined the attacker's strategy through simulation. Li et al. [?] rented a large subset to DDoS attackers, simulating the motive of maintaining botnets. They studied whether profits could be maintained when the effectiveness of DDoS attacks decreased. All the above work focuses on the theoretical defense against DDoS attacks [?].

The research on the incentive of antagonistic behavior is one of our primary concerns. Cremonini and Nizovtsev [?] used game theory to compare attacker decision-making in different scenarios. Clark and Konrad [?] proposed a game model where only one defender and one attacker exist. They showed that the defender would surrender if he/she needs to protect lots of nodes while the attacker only needs to win at only once. Grossklags et al. [?] modeled multiple attackers and found that attackers and defenders had an impact on their inherent interdependence. Fultz and Grossklags [?] solved the problem of strategy selection for attackers and cyber criminals. Schechter and Smith [?] constructed the attacker model in the computer security environment. Manshaei et al. [?] summarized the game theory research on network security and privacy.

In the Bitcoin economic environment, it is naturally appropriate to use game theory model to analyze the incentive of aggression. Vasek et al. [?] pointed out that the possibility of becoming an attacking target was related to the size of the mining pool. Accordingly, Johnson et al. [?] established a game theory model with two participants, big and small mining pools. The alternative strategy is investing in computing power or launch DDoS attacks. They concluded that large mining pools are more likely to be attacked than small ones and are more willing to attack ones smaller than them. Laszka et al. [?] established a model of two mining pools attacking each other and analyzed the long-term impact of DDoS attacks with the migration of miners.

The above work establishes the game theory model of DDoS attack in Bitcoin from different perspectives. However, with people attaching great importance to security issues, all walks of life have put forward higher security requirements. Managers pay a cost in security defense, and the strength of defense measures will have different degrees of impact on the results of DDoS attacks. Besides, it is also necessary to identify the cost of positive strategies. To find out the incentives of mining pools choosing their strategies under new circumstances, we organize the study.

3 Game model

Our model is mainly to further analyze the incentives of Bitcoin mining pool operators to launch distributed denial of service attacks on other mining pools. Bitcoin mining pool operators will choose whether to attack other mining pools based on their utility. In 2014, Johnson et al. considered that affect the income of pool operators only two parameters,which are the linear cost and the probability of successful attack.We will build on them to further analyze the parameters that affect pool operators' utility and their impact on operators' motivations.

In each model, we only pay attention to the income of two participants, a big player B and a small player S. By comparing the sizes, player B's computing power to mine bitcoin is stronger than S's. The third entity R represents the remaining operators in the bitcoin mining market.B and S are not affected by R attacks,so R is not a player in the sense of game model.In equations, we use the same symbols B, S and R as Johnson's to represent the computing power values of the various players. The sum of the computing power of the entire Bitcoin network is 1.

In our model,each player's decision space contains a binary choice-either to invest in computing power or to launch a DDOS attack against ohter strategic player. They can only be one choice at a time. The difference between two players choices will make up different Strategic combinations, and the utility function will change accordingly.players have made strategic choices before we calculate their utility, they may generate invest computation costs or attack costs.We calculate their final utility.

3.1 Improved Model with Operation Cost

Same as the model of Johnson's,We assume that the bitcoin mining market increases computational power at a fixed rate of ϵ over the game's time.The computational power of each player in the market is in balance.In order to keep up with the the market, the base strategy of each player's is to maintain market equilibrium through investing in computation.An alternative strategy for each player is to use the resources that have been used for increase the computation to initiate a DDoS attack against the other strategic player.we assume that DDoS attacks are successful only with fixed probability 1-σ.

In our model,We assume that the cost of keeping up with the mining market is proportional to the size of the player's increased computing power, and the cost of launching a DDoS attack is proportional to the size of the attacked player.In order to maintain the computation,players also need to pay a certain operating cost,which is proportional to its own size.If player S invests power in computation, she brings a increased computation cost of $\gamma\varepsilon B$ and operating cost of $\beta B(\varepsilon+1)$;if S initiates a DDoS attack on player B, it results in a cost of λB and his own operating costs of βS. Under the same conditions, we assume that the cost of launch a DDoS attack should less than the cost of investing in computation, so for our numerical illustrations, we choose an assignment $\lambda < \gamma$.

The revenue of each player is determined by their strategy and computation power. If both player B and S choose to invest in computation to keep up with the market, player B's income is the ratio of his computing power to market computing power. The cost he has to spend is the cost of input computing power and operating cost,then player B's utility is

$$\frac{B(1+\varepsilon)}{(B+S+R)(1+\varepsilon)} - \gamma\varepsilon B - \beta B(1+\varepsilon) = \frac{B}{B+S+R} - \gamma\varepsilon B - \beta B(1+\varepsilon);$$

similarly,the utility for player S is

$$\frac{S}{B+S+R} - \gamma\varepsilon S - \beta S(1+\varepsilon).$$

If both players launth DDoS attacks on each other,they have to pay for operating costs,in addition,player B need to spend the attack cost λS and player S need to spend the attack cost λB. At this time, the utility of Player B is

$$\frac{\sigma_B}{\sigma(B+S)+R(1+\varepsilon)} - \lambda S - \beta B.$$

If player S initiates DDoS attack against player B,while B keeps up with the market,then the utility of B is

$$\frac{\sigma B(1+\varepsilon)}{(\sigma B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - \beta B(\varepsilon+1).$$

The analysis of the utility expression of player S is similar to the above, and we will not be repeated here.The full payoff matrix for each player is summarized in Table1 and Table 2. From this, we derive each players best responses to each of the the other player s strategies. Then we use best response conditions to classify the game s Nash equilibria. Finally, we provide numerical illustrations for the game's equilibria

Table 1. Payoff Matrix for B with Imperfect DDoS and Operating Costs

		B	
		Computation	DDoS
S	Computation	$\frac{B}{B+S+R} - \gamma\varepsilon B - \beta B(\varepsilon+1)$	$\frac{B}{B+(\sigma S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - \beta B$
	DDoS	$\frac{\sigma B(1+\varepsilon)}{(\sigma B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - \beta B(\varepsilon+1)$	$\frac{\sigma_B}{\sigma(B+S)+R(1+\varepsilon)} - \lambda S - \beta B$

Table 2. Payoff Matrix for S with Imperfect DDoS and Operating Costs

		B	
		Computation	DDoS
S	Computation	$\frac{S}{B+S+R} - \gamma\varepsilon S - \beta S(\varepsilon+1)$	$\frac{\sigma S(1+\varepsilon)}{B+(\sigma S+R)(1+\varepsilon)} - \gamma\varepsilon S - \beta S(\varepsilon+1)$
	DDoS	$\frac{S}{(\sigma B+R)(1+\varepsilon)+S} - \lambda B(1+\varepsilon) - \beta S$	$\frac{\sigma S}{\sigma(B+S)+R(1+\varepsilon)} - \lambda B - \beta S$

Best-Response Strategies If player S invests in the computation, then for player B, investing in the computation is a best response if

$$\frac{B}{B+S+R} - \gamma\varepsilon B - \beta B(\varepsilon+1) \geq \frac{B}{B+(\sigma S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - \beta B \quad (1)$$

and player B initiates a DDOS attack is a best responses if

$$\frac{B}{B+S+R} - \gamma\varepsilon B - \beta B(\varepsilon+1) \leq \frac{B}{B+(\sigma S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - \beta B \quad (2)$$

If player S initiates a DDoS attack, then for player B,investing in computation is a best response if

$$\frac{\sigma B(1+\varepsilon)}{(\sigma B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - \beta B(\varepsilon+1) \geq \frac{\sigma B}{\sigma(B+S)+R(1+\varepsilon)} - \lambda S - \beta B \quad (3)$$

and player B invests in DDoS is a best response if

$$\frac{\sigma B(1+\varepsilon)}{(\sigma B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - \beta B(\varepsilon+1) \leq \frac{\sigma B}{\sigma(B+S)+R(1+\varepsilon)} - \lambda S - \beta B \quad (4)$$

In the same way, we can also use the same idea to analyze the best-response strategies of player S.

equilibria First, both players investing in DDOS attack that is a Nash Equilibrium whenever

$$\frac{\sigma B}{\sigma(B+S)+R(1+\varepsilon)} - \lambda S - \beta B \geq \frac{\sigma B(1+\varepsilon)}{(\sigma B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - \beta B(\varepsilon+1) \quad (5)$$

and

$$\frac{\sigma S}{\sigma(B+S)+R(1+\varepsilon)} - \lambda B - \beta S \geq \frac{\sigma S(1+\varepsilon)}{B+(\sigma S+R)(1+\varepsilon)} - \gamma\varepsilon S - \beta S(\varepsilon+1) \quad (6)$$

Second, both players investing in computing is an equilibrium if

$$\frac{B}{B+S+R} - \gamma\varepsilon B - \beta B(\varepsilon+1) \geq \frac{B}{B+(\sigma S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - \beta B \quad (7)$$

and

$$\frac{S}{B+S+R} - \gamma\varepsilon S - \beta S(\varepsilon+1) \geq \frac{S}{(\sigma B+R)(1+\varepsilon)+S} - \lambda B(1+\varepsilon) - \beta S \quad (8)$$

Third, an equilibrium in which player S launchs a DDoS attack against player B while B invests in computation may occur when

$$\frac{\sigma B(1+\varepsilon)}{(\sigma B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - \beta B(\varepsilon+1) \geq \frac{\sigma B}{\sigma(B+S)+R(1+\varepsilon)} - \lambda S - \beta B \quad (9)$$

and

$$\frac{S}{(\sigma B+R)(1+\varepsilon)+S} - \lambda B(1+\varepsilon) - \beta S \geq \frac{S}{B+S+R} - \gamma\varepsilon S - \beta S(\varepsilon+1) \quad (10)$$

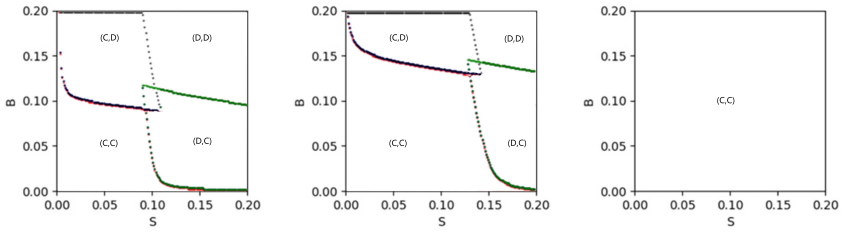
Finally, when the roles of B and S are interchanged in the two inequalities of the former case, B can performs a DDoS attack on S, and S invests the computation to achieve an equilibrium,when

$$\frac{B}{B+(\sigma S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - \beta B \geq \frac{B}{B+S+R} - \gamma\varepsilon B - \beta B(\varepsilon+1) \quad (11)$$

and

$$\frac{\sigma S(1+\varepsilon)}{B+(\sigma S+R)(1+\varepsilon)}-\gamma\varepsilon S-\beta S(\varepsilon+1)\geq\frac{\sigma S}{\sigma(B+S)+R(1+\varepsilon)}-\lambda B-\beta S \quad (12)$$

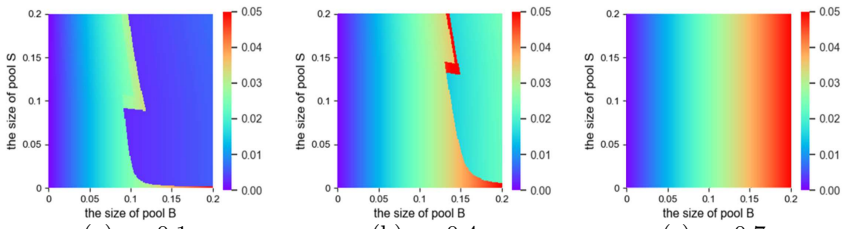
Figs. 1(a),1(b) and 1(c) show the equilibrium strategy prfiles for players (B, S)



(a) σ=0.1 (b) σ=0.4 (c) σ=0.7

Fig. 1. Equilibrium strategy profiles for various values of B and S and different probabilities of attack failure.

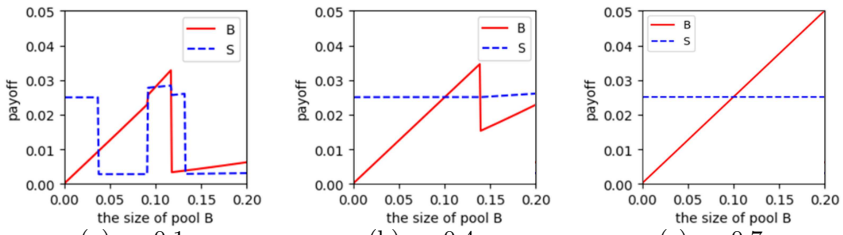
as a function of the players' sizes. The letters C and D abbreviate computation and DDoS, respectively. The probability of attack failure is $\sigma = 0.1$, $\sigma = 0.4$,$\sigma = 0.7$ respectively. The increase in computational power is $\varepsilon = 0.1$, and the linear cost factors for investing into computation and DDoS are $\gamma = 0.001$ and $\lambda = 0.001$.The linear coefficient of operating cost is $\beta = 0.001$. *Numerical*



(a) σ=0.1 (b) σ=0.4 (c) σ=0.7

Fig. 2. The equilibrium payoff of Player B (the red portions represent higher utility). When there are multiple equilibria, the figure shows the average return. The probability of attack failure σ are different.

Ilustrutions The above three sets of graphs show the characteristics of the Nash equilibrium for different values of B and S.Figure 1 divides the parameter space according to the equilibrium policy distribution set of players B and S.Figure 2 shows the payoff of player B as a function of the relative sizes of B and S, where the area with multiple equilibria is calculated as the average payoff.The average



(a) σ=0.1 (b) σ=0.4 (c) σ=0.7

Fig. 3. Equilibrium payoff of players B (solid) and S (dot-ted) as a function of B for $S = 0.1$. The probability of attack failure is $\sigma = 0.1$, $\sigma = 0.4$,$\sigma = 0.7$ respectively.

payoffs of players B and S (for fixed S) are shown as a function of B in Figure 3 .

Figure 1 shows the different distributions of players equilibrium strategies of various values of σ.When $\sigma = 0.1$, two players of relatively smaller size will not invest in DDoS attacks because they have to pay costs (attack costs and operating costs),as they are the best choose to invest in their own computation prowess.If the power of both players is relatively large, then there are no motivation to cooperate with each other.In some areas, one player always has a greater incentive to DDoS if his opponent has invested in the computation.Larger players having slightly more incentive to attack.When σ increases gradually,the probability of attacks failure is more and more big, players have less incentive to attack , players will prefer to invest in computation, to ensure more stable income.In addition,there is a region for players of medium and comparable sizes, in which the game has two competing equilibria.The strategic dynamic in this region is similar to the classical game of battle of the sexes.And with the possible exception of an extremely large player, the payoffs are generally higher for a player whose size lies just below the threshold for being attacked.

3.2 Improved Model with Defense Costs

Our second model combines the features of imperfect DDoS attacks and linear costs for player investment choices and operating costs and linear costs for defense DDoS attack. Here we assume that the cost of defending against DDoS attacks is directly proportional to the size of the investment player.The probability of DDoS attacks are successful is the ratio of the attack cost of the attacking player to the defense cost of the attacked player.We introduce the notation x to represent the factor of defense cost of players B and S.

Whether opponents invest computation or initiate a DDoS attack, player B and S must incur a cost of $xB(1 + \varepsilon)$ or $xS(1 + \varepsilon)$ to defend against DDoS attacks.In addition,if player B invests in computation,she incurs costs of $\gamma\varepsilon B$ and $\beta B(\varepsilon + 1)$ which used to increase and maintain computation power.While if player B initiates a DDoS attack against player S,she results in a cost of $\lambda S(1+\varepsilon)$

when player S invests computation or a cost of λS when player S initiates a DDoS attack.

Unlike our first model, the probability of a player failing to initiate a DDoS attack has changed. The probability of attack failure is changed to the ratio of the defense cost of attacked to the attacker's attack cost.If S attack against B,the probability of failure is $\frac{xB}{\lambda S}$,we use the symbol σ' to indicate.And if B attack against S,the probability of failure is $\frac{xS}{\lambda B}$,we use the symbol σ'' to indicate.The new payoffs (with defense costs) for players B and S are summarized in Table 3 and 4.

Table 3. Payoff Matrix for B with Imperfect DDoS and Defense Costs

		B	
		Computation	DDoS
S	Computation	$\frac{B}{B+S+R} - \gamma\varepsilon B - xB(1+\varepsilon) - \beta B(\varepsilon+1)$	$\frac{B}{B+(\sigma''S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - xB - \beta B$
	DDoS	$\frac{\sigma' B(1+\varepsilon)}{(\sigma' B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - xB(1+\varepsilon) - \beta B(\varepsilon+1)$	$\frac{\sigma' B}{(\sigma' B+\sigma''S)+R(1+\varepsilon)} - \lambda S - xB - \beta B$

Table 4. Payoff Matrix for S with Imperfect DDoS and Defense Costs

		B	
		Computation	DDoS
S	Computation	$\frac{S}{B+S+R} - \gamma\varepsilon S - xS(1+\varepsilon) - \beta S(\varepsilon+1)$	$\frac{\sigma''S(1+\varepsilon)}{B+(\sigma''S+R)(1+\varepsilon)} - \gamma\varepsilon S - xS(1+\varepsilon) - \beta S(\varepsilon+1)$
	DDoS	$\frac{S}{(\sigma' B+R)(1+\varepsilon)+S} - \lambda B(1+\varepsilon) - xS - \beta S$	$\frac{S\sigma''}{(\sigma' B+\sigma''S)+R(1+\varepsilon)} - \lambda B - xS - \beta S$

*Best-Responsrt Strategies*If player S invests in computation,then investing in computation is a best response for player B if

$$\frac{B}{B+S+R} - \gamma\varepsilon B - xB(1+\varepsilon) - \beta B(\varepsilon+1) \geq \frac{B}{B+(\sigma''S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - xB - \beta B; \tag{13}$$

and launching a DDoS is a best response if

$$\frac{B}{B+S+R} - \gamma\varepsilon B - xB(1+\varepsilon) - \beta B(\varepsilon+1) \leq \frac{B}{B+(\sigma''S+R)(1+\varepsilon)} - \lambda S(1+\varepsilon) - xB - \beta B. \tag{14}$$

If player S initiates a DDoS attack,then investing in computation is a best response for player B if

$$\frac{\sigma' B(1+\varepsilon)}{(\sigma' B+R)(1+\varepsilon)+S} - \gamma\varepsilon B - xB(1+\varepsilon) - \beta B(\varepsilon+1) \geq \frac{\sigma' B}{(\sigma' B+\sigma''S)+R(1+\varepsilon)} - \lambda S - xB - \beta B; \tag{15}$$

and investing in DDoS is a best response if

$$\frac{\sigma' B(1+\varepsilon)}{(\sigma' B+R)(1+\varepsilon)+S}-\gamma\varepsilon B-xB(1+\varepsilon)-\beta B(\varepsilon+1)\leq\frac{\sigma' B}{(\sigma' B+\sigma'' S)+R(1+\varepsilon)}-\lambda S-xB-\beta B; \tag{16}$$

Equilibria First,both players initiating DDoS attacks is a Nash equilibrium whenever

$$\frac{\sigma' B}{(\sigma' B+\sigma'' S)+R(1+\varepsilon)}-\lambda S-xB-\beta B\geq\frac{\sigma' B(1+\varepsilon)}{(\sigma' B+R)(1+\varepsilon)+S}-\gamma\varepsilon B-xB(1+\varepsilon)-\beta B(\varepsilon+1); \tag{17}$$

and

$$\frac{\sigma''}{(\sigma' B+\sigma'' S)+R(1+\varepsilon)}-\lambda B-xS-\beta S\geq\frac{\sigma'' S(1+\varepsilon)}{B+(\sigma'' S+R)(1+\varepsilon)}-\gamma\varepsilon S-xS(1+\varepsilon)-\beta S(\varepsilon+1); \tag{18}$$

Second,both players investing in computation is an equilibrium if

$$\frac{B}{B+S+R}-\gamma\varepsilon B-xB(1+\varepsilon)-\beta B(\varepsilon+1)\geq\frac{B}{B+(\sigma'' S+R)(1+\varepsilon)}-\lambda S(1+\varepsilon)-xB-\beta B; \tag{19}$$

and

$$\frac{S}{B+S+R}-\gamma\varepsilon S-xS(1+\varepsilon)-\beta S(\varepsilon+1)\geq\frac{S}{B+S+R}-\gamma\varepsilon S-xS(1+\varepsilon)-\beta S(\varepsilon+1); \tag{20}$$

Third,an equilibrium in which S conducts a DDoS attack against B while B invests in computation may occur when

$$\frac{\sigma' B(1+\varepsilon)}{(\sigma' B+R)(1+\varepsilon)+S}-\gamma\varepsilon B-xB(1+\varepsilon)-\beta B(\varepsilon+1)\geq\frac{\sigma' B}{(\sigma' B+\sigma'' S)+R(1+\varepsilon)}-\lambda S-xB-\beta B; \tag{21}$$

and

$$\frac{s}{(\sigma' B+R)(1+\varepsilon)+S}-\lambda B(1+\varepsilon)-xS-\beta S\geq\frac{S}{B+S+R}-\gamma\varepsilon S-xS(1+\varepsilon)-\beta S(\varepsilon+1); \tag{22}$$

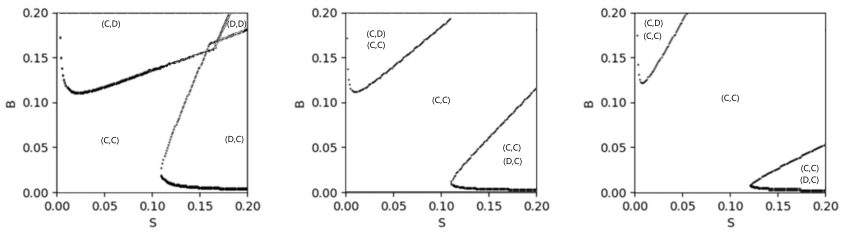
Finally,an equilibrium in which B conducts a DDoS attack against S while S invests in computation may occur when

$$\frac{B}{B+(\sigma'' S+R)(1+\varepsilon)}-\lambda S(1+\varepsilon)-xB-\beta B\geq\frac{B}{B+S+R}-\gamma\varepsilon B-xB(1+\varepsilon)-\beta B(\varepsilon+1); \tag{23}$$

and

$$\frac{\sigma'' S(1+\varepsilon)}{B+(\sigma'' S+R)(1+\varepsilon)}-\gamma\varepsilon S-xS(1+\varepsilon)-\beta S(\varepsilon+1)\geq\frac{\sigma''}{(\sigma' B+\sigma'' S)+R(1+\varepsilon)}-\lambda B-xS-\beta S; \tag{24}$$

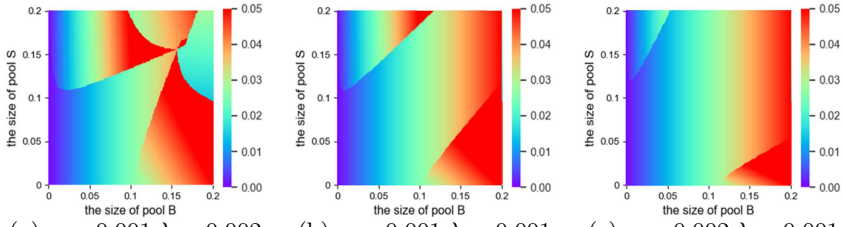
Figs. 4(a),4(b) and 4(c) show the equilibrium strategy prfiles for players (B, S) as a function of the players' sizes. The letters C and D abbreviate computation



(a) $x = 0.001$,$\lambda = 0.002$ (b) $x = 0.001$,$\lambda = 0.001$ (c) $x = 0.002$,$\lambda = 0.001$

Fig. 4. Equilibrium strategy profiles for various values of B and S and different linear coefficients of DDoS and defense.

and DDoS, respectively.The increase in computational power is $\varepsilon = 0.1$, and the linear cost factors for investing into computation is $\gamma = 0.001$.The linear coefficient of operating cost is $\beta = 0.001$.In order to reflect the impact of different defense costs and attack cost factors on the player's strategy, we have three different combinations of values, $x = 0.001$,$\lambda = 0.002$,$x = 0.001$,$\lambda = 0.001$ and $x = 0.002$,$\lambda = 0.001$, respectively. *Numerical Illustration* The above three sets

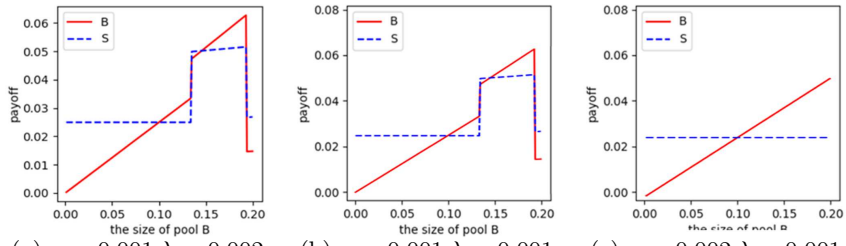


(a) $x = 0.001$,$\lambda = 0.002$ (b) $x = 0.001$,$\lambda = 0.001$ (c) $x = 0.002$,$\lambda = 0.001$

Fig. 5. The equilibrium payoff of Player B (the red portions represent higher utility). When there are multiple equilibria, the figure shows the average return.The linear coefficients of DDoS and defense are different.

of graphs show the features of the Nash equilibrium for different values of B and S.Figure 4 divides the parameter space according to the equilibrium policy distribution set of players B and S.Figure 5 shows the payoff of player B as a function of the relative sizes of B and S, where the area with multiple equilibria is calculated as the average payoff.The average payoffs of players B and S (for fixed S) are shown as a function of B in Figure 6 .

As we see in figure 4 (compared to operational cost model), the probability of a successful attack by a mine pool is not only related to the size of its own and opponents, but also to its own attack cost factor and opponent's defense cost factor.Players are still incentivized to attack large players.When the opponent's defense cost coefficient is gradually greater than their own attack cost coefficient,



(a) $x = 0.001, \lambda = 0.002$ (b) $x = 0.001, \lambda = 0.001$ (c) $x = 0.002, \lambda = 0.001$

Fig. 6. Equilibrium payoff of players B (solid) and S (dot-ted) as a function of B for $S = 0.1$.The ratio of $\frac{x}{\lambda}$ are $\frac{x}{\lambda} < 1, \frac{x}{\lambda} = 1$ and $\frac{x}{\lambda} > 1$ respectively.

the failure rate of attack will increase, the scope of mine pools initiate DDoS attack will be smaller and smaller.The situation in which two larger mines will initiate a DDoS attack will gradually decrease until it disappears.For small pools, attacking large pools will bring in more revenue.

4 Conclusion

It is a folklore that mining pools would launch DDoS attacks to other mining pools. The previous research [**?**] even shows that relative large mining pools are willing to attack each other by a game-theoretic analysis. In this paper, we further extended the result by adding defense cost into the previous game-theoretic model. Our analysis shows that the probability of launching DDoS attacks is related to the mining cost and success possibility of DDoS attacks.