Qin Y, Hu Q, Yu DX *et al.* Generous or selfish? Weighing transaction forwarding against malicious attacks in payment channel networks. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 37(4): 888–905 July 2022. DOI 10.1007/s11390-022-2032-x

# Generous or Selfish? Weighing Transaction Forwarding Against Malicious Attacks in Payment Channel Networks

Yi Qin[1] (秦 毅), Qin Hu[2,*], Dong-Xiao Yu[1] (于东晓), *Senior Member*, *IEEE*, and Xiu-Zhen Cheng[1] (成秀珍), *Fellow*, *IEEE*

[1] *School of Computer Science and Technology, Shandong University, Qingdao 266237, China*

[2] *Department of Computer and Information Science, Indiana University-Purdue University Indianapolis Indianapolis 46202, U.S.A.*

E-mail: qinyi@sdu.edu.cn; qinhu@iu.edu; {dxyu, xzcheng}@sdu.edu.cn

Received November 19, 2021; accepted June 8, 2022.

**Abstract** Scalability has long been a major challenge of cryptocurrency systems, which is mainly caused by the delay in reaching consensus when processing transactions on-chain. As an effective mitigation approach, the payment channel networks (PCNs) enable private channels among blockchain nodes to process transactions off-chain, relieving long-time waiting for the online transaction confirmation. The state-of-the-art studies of PCN focus on improving the efficiency and availability via optimizing routing, scheduling, and initial deposits, as well as preventing the system from security and privacy attacks. However, the behavioral decision dynamics of blockchain nodes under potential malicious attacks is largely neglected. To fill this gap, we employ the game theory to study the characteristics of channel interactions from both the micro and macro perspectives under the situation of channel depletion attacks. Our study is progressive, as we conduct the game-theoretic analysis of node behavioral characteristics from individuals to the whole population of PCN. Our analysis is complementary, since we utilize not only the classic game theory with the complete rationality assumption, but also the evolutionary game theory considering the limited rationality of players to portray the evolution of PCN. The results of numerous simulation experiments verify the effectiveness of our analysis.

**Keywords** blockchain, payment channel network, game theory

## 1 Introduction

As Bitcoin① prevails in the cryptocurrency market, blockchain has received explosively increasing attention from both academia and industry, making the development of this distributed ledge technology advance greatly. By employing the decentralized cryptocurrency system, financial transactions can be successfully conducted without the help and management of third-party centralized institutions but all by distributed blockchain nodes, providing transparency and manipulation-proof experiences to users. However, there exists one major disadvantage that it takes a long time to achieve transaction confirmation among a large number of peer-to-peer nodes, thus leading to low scalability, e.g., Bitcoin handling seven transactions per second, and impeding the large-scale application of cryptocurrency in real-world applications. Even though Ethereum operates with a relatively higher transaction processing speed of 15 transactions per second [1], it is still far below the needs in practice.

To solve this problem, the concept of payment channel has emerged recently to provide an off-chain transaction processing method, which is established between two blockchain nodes with each depositing a certain

Regular Paper

Special Section of MASS 2020–2021

A preliminary version of the paper was published in the Proceedings of MASS 2021.

The work was partially supported by the National Key Research and Development Program of China under Grant No. 2019YFB2102600, and the National Natural Science Foundation of China under Grant Nos. 62122042, 61971269 and 61832012.

*Corresponding Author

①Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, Apr. 2022.

amount of funds for future instant transactions without waiting for the global on-chain confirmation. Only when the channel is closed will the latest state of the balance be published on the main chain. By this means, the blockchain system can process transactions in an efficient way. Further, with the help of Hashed Time-lock Contract (HTLC)②, transactions can be completed through multiple channels even if the sender and the receiver nodes are not directly connected, forming the payment channel network (PCN).

Existing studies about PCN mainly focus on systematic performance improvement, including the routing and scheduling algorithm design to improve the transaction processing speed [2, 3], channel deposit optimization to extend the availability of channels [1, 4], and security and privacy issues [5–9]. Nevertheless, the node-level behavior and decision inspections are largely overlooked, which turns out to be the essential procedure affecting the formation and sustainability of PCN, especially in the case of malicious attacks aiming at exhausting channel deposits or isolating certain nodes.

In this paper, we analyze the PCN from the perspective of individual node's decision on whether to help in forwarding incoming transactions for others, with the concern of potential malicious attacks depleting the balance of channels during the relaying process. Specifically, we employ the game theory to model the interactions between connected nodes with the awareness of various channel attacks, and analyze the behavior characteristics of nodes from both the micro (individual) and the macro (group) angles. Our study is progressive as the individual behavior is first investigated in the PCN game between any two adjacent channels, and then the collective characteristics of all channels' interactions are uncovered in the evolutionary PCN game. Our analysis is also complementary. We study the equilibrium state and the powerful control strategy of individual players, i.e., the zero-determinant (ZD) strategy, in the realm of the classic game theory with the assumption that all players are wise and intelligent enough; then, we examine the evolutionarily stable points and strategy by taking advantage of the evolutionary game theory with the relaxed assumption of ideal game players. In summary, our main contributions can be listed as follows.

- We establish a game-theoretic model, termed as the PCN game, to capture the dynamic interactions between blockchain nodes, based on which extensive analysis is conducted to inspire a better PCN system design.
- From the micro perspective, we study the Nash equilibrium of the PCN game; afterwards, the existence and the power of the ZD strategy regarding the unilateral control of expected payoffs are explored in both the infinite and the finite rounds of repetitive games to cover all possible situations.
- From the macro perspective, we utilize the replication dynamic equation to derive the evolutionarily stable points of the generalized evolutionary PCN game, and we also investigate the evolutionary stability of the ZD strategy in a simple-to-complex manner, discussing the case of playing against one other strategy and multiple other strategies to draw some insights on eliciting mutual cooperation in the PCN.
- Extensive simulation experiments are carried out with the observations indicating that the experimental and analytical results are well-matched and therefore our analysis is effective.

The organization of the rest paper is as follows. We summarize related work in Section 2. We propose the PCN game model in Section 3. And Section 4 analyzes the Nash equilibrium and the applicability of the powerful ZD strategy. Section 5 calculates the evolutionarily stable points and the evolutionary stability of the ZD strategy. Section 6 verifies the effectiveness of our analysis by extensive simulation experiments. Section 7 concludes the whole paper.

## 2 Related Work

As representative PCNs, lightning network (LN)② was designed for Bitcoin, while Raiden network③ was proposed as an off-blockchain scaling solution for Ethereum. Many existing studies have been devoted to improving the transaction speed and the success rate in the PCN. Specifically, some of them focus on the relationship between the topological structure and the efficiency of transaction processing. The formation of the PCN topology was analyzed in [10], showing that the centralized structure can make the PCN more efficient and stable. Lange *et al.* [11] studied the attachment strategies' influence on the PCN topology, which further affects the connectivity and the benefit of participating nodes. There is also related literature fo-

②The Bitcoin lightning network: Scalable off-chain instant payments, Jan. 2016. http://lightning.network/lightning-network-paper.pdf, Apr. 2022.

③https://raiden.network, Apr. 2022.

cusing on designing routing algorithms and transaction scheduling mechanisms for a higher payment success rate. A new routing algorithm for reducing the balance skewness of channels was proposed in [2], which took advantage of both the static and the dynamic routing to improve the success rate while decreasing latency and expense. Bagaria *et al.* designed a multi-path routing scheme named Boomerang [3], which could build redundant channels to eliminate the risk of participants not performing transaction agreements.

In addition, the optimization of the channel balance has been widely studied because the depletion of one-way funds can easily lead to the closure of channels and result in higher costs for PCN nodes to re-establish channels. Khalil and Gervais [4] proposed the first solution of rebalancing channels' funds, and Pickhardt and Nowostawski [12] continued to study the redistribution of the balance to improve channels' capacity, which laid the foundation for processing more big transactions. Besides, Li *et al.* [1] proposed an algorithm to determine the best amount of initial funds put into the channels to extend the channel lifetime and increase the number of transactions that can be processed.

Recently, the security issue of PCN has received great attention from researchers. Rohrer *et al.* [5] demonstrated two attacks, namely exhausting channels and isolating nodes attacks, where the detailed attacking steps were presented with quantified success rates. Lu *et al.* [13] proposed a low-cost attack named bank run attack which can significantly reduce the transaction capacity to paralyze the whole PCN. These attacks are based on the principle of the griefing attack [8] which is mounted by controlling a channel on the payment path to refuse the contract and then locking the deposits of each channel from the payer to the receiver for a period of time. Harris and Zohar [9] presented a flood and loot attack by creating multiple conflicting transactions, which may cause the congestion of submitting arbitration to blockchain, and thus the malicious nodes are able to steal the funds before the victims receive arbitration results. Other studies are committed to solving or mitigating malicious attacks in PCN. Banerjee *et al.* [8] imposed a new HTLC protocol with a penalty on the adversary to mitigate griefing attacks, which has not been put in practice because the processing speed has to be sacrificed in this solution. Some basic defense mechanisms against the flood and loot attack were also presented in [9] although the authors claimed that the attack cannot be completely eliminated due to the function of HTLC. For various private properties of the PCN, i.e., channel, balance, routing, and payment, Kappos *et al.* [6] analyzed the potential attacks. Tang *et al.* [7] studied the trade-off between the privacy and the utility in releasing noisy channel balances for the shortest-path routing mechanism.

Given the variety of attacks in PCN without effective control schemes, the participation behavior of PCN nodes can be unpredictable, which may negatively affect the formation and the sustainability of PCN. The recent work using the infinitely repeated game and the evolutionary game with two strategies to model this problem is studied in [14]. Considering the potential attacks aiming at reducing the channel lifetime, we model the interactions of PCN nodes and analyze the characteristics of both individuals and groups by considering infinitely and finitely repeated games, as well as two strategies (ZD strategy and one other strategy) and multiple strategies (ZD strategy and multiple other strategies) in the evolutionary game, so as to provide a more scientific and comprehensive perspective with some insights to enhance the system design of the PCN.

## 3 Game Formulation

To mitigate the challenge of blockchain scalability, payment channels are established between two nodes to process transactions in an off-chain manner. By using the deposits in the channel, both ends can conduct frequent transactions quickly. A PCN composed of multiple channels allows payments to cross the channel network under the condition that the intermediate channels cooperate to forward transactions. Here we represent the PCN as a graph $G\langle V, E\rangle$, where $V = \{v_1, v_2, \cdots, v_N\}$ denotes the set of nodes with $N$ denoting the total number of blockchain nodes in the PCN and $E = \{e_1, e_2, \cdots, e_K\}$ denotes the set of payment channels with $K$ being the total number of channels. An exemplary PCN is illustrated in Fig.1.

Each intermediate node can decide whether to use its own existing channel with the limited deposit to assist in forwarding others' transactions. Considering that forwarding transactions is via a concrete channel which has a certain amount of deposits available to be used for transactions, we focus on the action of each node in terms of deciding whether to forward a coming transaction through a specific channel or not. In detail, we consider the interactions between any pair of adjacent channels with the choices of cooperation and defection, denoted as $C$ and $D$, respectively, which can be modeled as a two-player game. Here the chan-

nel choosing strategy $C$ will participate in forwarding transactions to help complete transactions between non-adjacent nodes, while the channel with strategy $D$ will refuse to forward the coming transactions and only use the deposits to meet its own transaction needs.

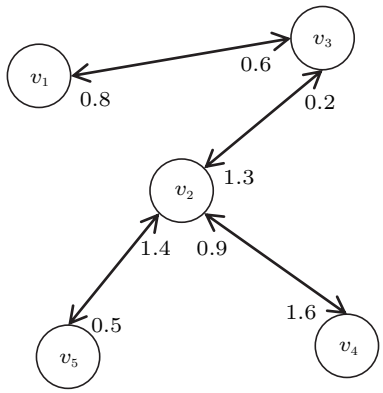



Fig.1. Example of the PCN. This graph contains five blockchain nodes and four channels, and the numbers at both ends of the channel represent the deposits invested by the nodes, which can be used to conduct instant transactions between the connected nodes. For example, there is a channel between $v_2$ and $v_5$ with 1.4 and 0.5 respectively, which means that $v_2$ has the ability to pay 1.4 to $v_5$ immediately while $v_5$ can pay 0.5 to $v_2$ instantly.

Clearly, different behaviors bring different payoffs to the channels in the PCN. To capture all possible situations, we define the parameters affecting any channel $e_k$'s payoff as follows.

• *Natural Profit* (*denoted as* $r_k$). Compared with processing a transaction on the blockchain, using the payment channel can reduce block packing cost and time delay for committing the transaction to the main chain, which is defined as the natural profit of a channel.

• *Profit from Helping Relay Transactions* (*denoted as* $f_k$). When $e_k$ chooses strategy $C$, assisting in routing a neighbor's transactions, it obtains some profits by collecting transaction fees from the forwarded transactions.

• *Profit from Transactions Being Relayed by a Neighbor* (*denoted as* $a_k$). When $e_k$'s neighboring channel cooperates in relaying transactions from $e_k$, it can benefit from reducing the cost of sending these transactions on-chain.

• *Loss of Being Attacked* (*denoted as* $c_k$). General attacks include but are not limited to denial-of-service, channel exhaustion, and node isolation, which result in cooperative channels' funds being locked for a period of time or even being terminated, thus leading to economic loss.

For the simplicity and the brevity of expression, we consider two adjacent channels $e_x$, $e_y \in E$, which have a point of the intersection node in the PCN. Both $e_x$ and $e_y$ can select either $C$ or $D$, which means that they will relay transactions for each other or not respectively. The four strategy combinations for channels $e_x$ and $e_y$ generate different payoffs as follows. 1) When $e_x$ and $e_y$ cooperate concurrently, they both obtain transaction fees and payoffs from their own transactions being relayed. And they also need to bear the potential losses caused by malicious attacks. Thus, $e_x$ and $e_y$ obtain payoffs $r_x + f_x + a_x - c_x$ and $r_y + f_y + a_y - c_y$, respectively. 2) If $e_x$ chooses cooperation while $e_y$ chooses defection, $e_x$ does not get the benefit of transaction demand being satisfied by $e_y$, and $e_y$ cannot collect transaction fees but avoid potential loss $c_y$, so that $e_x$ can obtain $r_x + f_x - c_x$ while $e_y$ has payoff $r_y + a_y$. 3) On the contrary, when $e_x$ defects but $e_y$ cooperates, $e_x$ obtains $r_x + a_x$ and $e_y$ gains $r_y + f_y - c_y$. 4) In the case that both $e_x$ and $e_y$ choose defection, they cannot meet transaction needs of each other; therefore, they only have the basic payoffs $r_x$ and $r_y$. Subsequently, channels' payoff vectors can be denoted as follows.

$$\begin{aligned} \boldsymbol{S}_x &= (S_x^1, S_x^2, S_x^3, S_x^4)^{\mathrm{T}} = \begin{pmatrix} r_x + f_x + a_x - c_x \\ r_x + f_x - c_x \\ r_x + a_x \\ r_x \end{pmatrix}, \\ \boldsymbol{S}_y &= (S_y^1, S_y^2, S_y^3, S_y^4)^{\mathrm{T}} = \begin{pmatrix} r_y + f_y + a_y - c_y \\ r_y + a_y \\ r_y + f_y - c_y \\ r_y \end{pmatrix}. \end{aligned} \tag{1}$$

And the payoff matrix is shown in Fig.2.

| $e_x$ \ $e_y$ | Cooperation | Defection |
|---|---|---|
| Cooperation | $r_x+f_x+a_x-c_x$ / $r_y+f_y+a_y-c_y$ | $r_x+f_x-c_x$ / $r_y+a_y$ |
| Defection | $r_x+a_x$ / $r_y+f_y-c_y$ | $r_x$ / $r_y$ |

Fig.2. Payoff matrix of two adjacent channels in the PCN.

**Definition 1** (PCN Game). *In the PCN game, any two adjacent channels* $e_x$ *and* $e_y$ *as players can choose strategies* $C$ *and* $D$*, indicating whether the channels participate in forwarding transactions or not, and get payoffs* $\boldsymbol{S}_x$ *and* $\boldsymbol{S}_y$*, respectively.*

In the following, we first study the problem of dominant interest in the interactions between any pair of channels from a micro perspective, which can reveal some clues about the optimal actions of individual players in the PCN game. After that, we study the evolution process of the PCN game from a macro perspective to show the overall behavior trend, which may help us understand the collective characteristics of the PCN and thus direct us to better design and use it.

## 4 Microscopic Analysis of PCN Game

In this section, we study the interactions between any two adjacent channels in the PCN game as defined above from a microscopic perspective. Specifically, we first analyze the Nash equilibrium of the PCN game, and then investigate a powerful control strategy under both the infinitely and the finitely repeated game scenarios.

### 4.1 Nash Equilibrium

Given the payoff matrix defined in Section 3, we can derive the Nash equilibrium in two different parameter cases.

**Theorem 1**. *When $c_x < f_x$ and $c_y < f_y$, a Nash equilibrium is reached when both $e_x$ and $e_y$ choose strategy $C$.*

*Proof.* To derive the Nash equilibrium in the two-player game, we can start from focusing on the best action of one of the players. In our problem, we first study the optimal strategy of channel $e_x$ by considering all possible actions of $e_y$. When $e_y$ chooses strategy $C$, $e_x$'s payoff of choosing strategy $C$ is more than that of choosing strategy $D$ since $r_x + f_x + a_x - c_x > r_x + a_x$ given the condition $c_x < f_x$. When $e_y$ chooses strategy $D$, $e_x$'s payoff of choosing strategy $C$ is more than that of choosing strategy $D$ according to $r_x + f_x - c_x > r_x$. Thus, no matter whether channel $e_y$ chooses strategy $C$ or $D$, $e_x$ prefers cooperation to obtain the better payoff. In the same way, we can conclude that $e_y$ will choose cooperation for more payoffs. Therefore, both players in the game choosing cooperation constitute a Nash equilibrium. □

**Theorem 2**. *If $c_x > f_x$ and $c_y > f_y$, there is a Nash equilibrium when both channels choose strategy $D$.*

The proof of Theorem 2 is similar to that of Theorem 1. For the sake of brevity, we omit the details here.

### 4.2 Control Analysis of Zero-Determinant Strategy

The emergence of the zero-determinant (ZD) strategy allows a player to unilaterally enforce a linear relationship between the payoffs of its own and the opponents, regardless of the opponent strategy [15]. In the PCN, since a large number of transactions need to be processed, there are long-term interactions between channels, and the result of the strategy choice will leave an impact on the next round of interaction. Under the condition of $e_x$ and $e_y$ choosing strategy profile $(CC, CD, DC, DD)$ in the previous round, we define $e_x$'s mixed strategy as $\boldsymbol{p} = (p_1, p_2, p_3, p_4)$, where each component represents the probability of choosing cooperation correspondingly. And $e_y$'s mixed strategy is denoted as $\boldsymbol{q} = (q_1, q_2, q_3, q_4)$ analogously.

With the above definitions of $\boldsymbol{p}$ and $\boldsymbol{q}$, the process of the repeated game can be regarded as a Markov decision process, and its transition matrix $\boldsymbol{M}$ is expressed as

$$\boldsymbol{M} = \begin{pmatrix} p_1q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2q_3 & p_2(1-q_3) & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3q_2 & p_3(1-q_2) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4q_4 & p_4(1-q_4) & (1-p_4)q_4 & (1-p_4)(1-q_4) \end{pmatrix}. \quad (2)$$

Let $\boldsymbol{v}$ be the stable vector of the above transition matrix. According to [15], after the determinant elementary transformation and based on Cramer's rule, the dot product of $\boldsymbol{v}$ and any vector $\boldsymbol{f} = (f_1, f_2, f_3, f_4)$ is

$$\boldsymbol{v} \cdot \boldsymbol{f} = \boldsymbol{G}(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{f}) = \det \begin{pmatrix} -1 + p_1q_1 & -1 + p_1 & -1 + q_1 & f_1 \\ p_2q_3 & -1 + p_2 & q_3 & f_2 \\ p_3q_2 & p_3 & -1 + q_2 & f_3 \\ p_4q_4 & p_4 & q_4 & f_4 \end{pmatrix}. \quad (3)$$

Besides, the expected payoffs of channels $e_x$ and $e_y$ can be calculated as follows:

$$\begin{aligned} E_x &= \frac{\boldsymbol{v} \cdot \boldsymbol{S}_x}{\boldsymbol{v} \cdot \boldsymbol{1}} = \frac{\boldsymbol{G}(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{S}_x)}{\boldsymbol{G}(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{1})}, \\ E_y &= \frac{\boldsymbol{v} \cdot \boldsymbol{S}_y}{\boldsymbol{v} \cdot \boldsymbol{1}} = \frac{\boldsymbol{G}(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{S}_y)}{\boldsymbol{G}(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{1})}, \end{aligned} \quad (4)$$

where $\boldsymbol{1}$ is a unit vector with four elements being 1. We can find the payoffs in (4) are linearly related with their payoff vectors. Hence, when computing a linear

combination of the above two expected payoffs, with $\alpha$, $\beta$, and $\gamma$ being constant parameters, we have

$$\begin{aligned}&\alpha E_x+\beta E_y+\gamma\\=&\frac{\boldsymbol{v}\cdot(\alpha \boldsymbol{S}_x+\beta \boldsymbol{S}_y+\gamma \mathbf{1})}{\boldsymbol{v}\cdot\mathbf{1}}\\=&\frac{\boldsymbol{G}(\boldsymbol{p},\boldsymbol{q},\alpha \boldsymbol{S}_x+\beta \boldsymbol{S}_y+\gamma \mathbf{1})}{\boldsymbol{G}(\boldsymbol{p},\boldsymbol{q},\mathbf{1})}.\end{aligned}\tag{5}$$

And (5) can be calculated by substituting $\boldsymbol{f}$ in (3) with $\alpha \boldsymbol{S}_x+\beta \boldsymbol{S}_y+\gamma \mathbf{1}$ in the numerator and $\mathbf{1}$ in the denominator. By observing (3), we can realize that the second and the third columns of the determinant are only related to the strategies of $e_x$ and $e_y$, respectively, which means both $e_x$ and $e_y$ are capable of choosing strategies to make one column proportional to $\boldsymbol{f}$, resulting in the determinant being zero. Taking $e_x$ as an example, if its strategy $\boldsymbol{p}$ makes the second column of (3) proportionate to $\alpha \boldsymbol{S}_x+\beta \boldsymbol{S}_y+\gamma \mathbf{1}$, then the numerator in (5) becomes zero. Therefore, the linear combination of the two payoffs, i.e., $\alpha E_x+\beta E_y+\gamma=0$, is established. Without the loss of generality, we continue to assume that $e_x$ uses the ZD strategy as an exemplary case in the following.

#### 4.2.1 *Analysis of $e_y$'s Payoff*

When $\alpha=0$, $E_y=-\gamma/\beta$ holds, which means that $e_x$'s strategy $\boldsymbol{p}$ makes the second column of (3) equal to $\beta \boldsymbol{S}_y+\gamma \mathbf{1}$, $e_x$ can unilaterally set $e_y$'s expected payoff $E_y$. Specifically, $\boldsymbol{p}$ can be solved by the following four equations,

$$\begin{cases}p_1=1+\beta(r_y+f_y+a_y-c_y)+\gamma,\\p_2=1+\beta(r_y+a_y)+\gamma,\\p_3=\beta(r_y+f_y-c_y)+\gamma,\\p_4=\beta r_y+\gamma.\end{cases}$$

Then $p_2$ and $p_3$ can be resolved with $p_1$ and $p_4$ to eliminate parameters $\beta$ and $\gamma$,

$$\begin{aligned}p_2=&\frac{p_1(S_y^2-S_y^4)-(1+p_4)(S_y^2-S_y^1)}{S_y^1-S_y^4}\\=&\frac{p_1a_y-(1+p_4)(c_y-f_y)}{f_y+a_y-c_y},\\p_3=&\frac{(1-p_1)(S_y^4-S_y^3)+p_4(S_y^1-S_y^3)}{S_y^1-S_y^4}\\=&\frac{(1-p_1)(c_y-f_y)+p_4a_y}{f_y+a_y-c_y}.\end{aligned}\tag{6}$$

Therefore $e_y$'s expected payoff is:

$$E_y=\frac{(1-p_1)r_y+p_4(r_y+f_y+a_y-c_y)}{(1-p_1)+p_4}.\tag{7}$$

Now we discuss the controlling results of the ZD strategy with different parameter settings.

**Theorem 3**. *If $c_y<f_y$, we divide the situation into two cases according to the relationship between $f_y-a_y$ and $c_y$: 1) if $c_y>f_y-a_y$, $e_x$ can control $E_y\in[r_y+f_y-c_y,r_y+a_y]$; 2) if $c_y\leqslant f_y-a_y$, $e_x$ cannot set $E_y$'s range unilaterally.*

*Proof.* By observing (7), $E_y$ is the weighted average of $r_y$ and $r_y+f_y+a_y-c_y$, and the weights are $1-p_1$ and $p_4$ respectively. We can re-express $E_y$ as $r_y+\frac{f_y+a_y-c_y}{1+\lambda}$ with $\lambda=\frac{1-p_1}{p_4}$. Since both $p_1$ and $p_4$ belong to (0,1), $\lambda$ cannot be negative. Under the condition of $c_y<f_y$, $p_2\geqslant 0$ and $p_3\leqslant 1$ are satisfied with any feasible $p_1$ and $p_4$. Subsequently, we calculate the constraints $p_2\leqslant 1$ and $p_3\geqslant 0$, and obtain

$$\begin{cases}\lambda\geqslant\dfrac{f_y-c_y}{a_y},\\\lambda\leqslant\dfrac{a_y}{f_y-c_y}.\end{cases}$$

When $c_y>f_y-a_y$, $\lambda$ has solutions and $E_y$ is inversely proportional to $\lambda$. Therefore we get the maximum $E_y$ when $\lambda=\frac{f_y-c_y}{a_y}$, and the minimum $E_y$ with $\lambda=\frac{a_y}{f_y-c_y}$. While if $c_y\leqslant f_y-a_y$, there is not a feasible solution or no more than one fixed value; therefore $e_x$ cannot control $E_y$'s range. □

**Theorem 4**. *If $c_y>f_y+a_y$, $e_x$ cannot unilaterally set $E_y$'s range.*

*Proof.* According to (6), $0\leqslant p_2,p_3\leqslant 1$ can only be met at a single point of $\boldsymbol{p}=(1,1,0,0)$ in the case of $c_y>f_y+a_y$. Thus, $e_x$ cannot control $E_y$'s range. □

**Theorem 5**. *In the case of $f_y<c_y<f_y+a_y$, if $p_4\in(0,\frac{a_y+f_y-c_y}{c_y-f_y+a_y})$, $E_y$ has the minimum value of $r_y+\frac{p_4a_y}{1+p_4}$; if $p_4\in(\frac{a_y+f_y-c_y}{c_x-f_x+a_x},\frac{a_y+f_y-c_y}{a_y})$, $E_y$ has the minimum value of $r_y+\frac{p_4(c_y-f_y)}{1-p_4}$. In addition, $E_y$ is $r_y$ when $p_4=0$ and $p_1\neq 1$, and $E_y$ has a maximum value of $r_y+f_y+a_y-c_y$ when $p_1=1$ and $p_4\neq 0$.*

*Proof.* Because of $r_y<r_y+f_y+a_y-c_y$ in this case, the larger the parameter $\lambda$ is, the smaller the payoff $E_y$ is. To derive the minimum value of $E_y$, we need to calculate the maximum value of $\lambda$ under the constraints of $p_1$, $p_2$, $p_3$ and $p_4$ belonging to [0, 1]. For any feasible $p_1$ and $p_4$, two inequalities are naturally satisfied, i.e., $p_2\leqslant 1$ and $p_3\geqslant 0$. Thus, we only need to focus on the conditions of making $p_2\geqslant 0$ and $p_3\leqslant 1$, which leads to

$$\begin{cases}\lambda\leqslant\dfrac{a_y+f_y-c_y}{a_yp_4}-\frac{c_y-f_y}{a_y},\\\lambda\leqslant\dfrac{a_y+f_y-c_y}{(c_y-f_y)p_4}-\frac{a_y}{c_y-f_y}.\end{cases}$$

Because these two inequalities need to be satisfied at the same time, we need to compare the values of two expressions on the right side of the inequalities and take the smaller one as the maximum value of $\lambda$. Subtracting the second expression from the first one, we can get a function of $p_4$ that can be expressed as $f(p_4) = \frac{c_y - f_c - a_y}{a_y(c_y - f_y)}(\frac{f_y + a_y - c_y}{p_4} + f_y - a_y - c_y)$. Since $\lambda \geqslant 0$, we can derive the domain of $f(p_4)$ as $p_4 \in (0, \frac{a_y + f_y - c_y}{a_y})$. By calculating the first derivative of $f(p_4)$, we can obtain that $f(p_4)$ is a monotonically increasing function with a zero point $p_4 = \frac{a_y + f_y - c_y}{c_x - f_x + a_x}$, which means when $p_4 \in (0, \frac{a_y + f_y - c_y}{c_y - f_y + a_y})$, we have $f(p_4) \leqslant 0$, and thus the first inequality limits a smaller value of $\lambda$; while if $p_4 \in (\frac{a_y + f_y - c_y}{c_x - f_x + a_x}, \frac{a_y + f_y - c_y}{a_y})$, $f(p_4) \geqslant 0$ and we know that the second inequality becomes the limits of $\lambda$. Given the maximum $\lambda$, we can get $E_y$'s minimum value as $r_y + \frac{p_4 a_y}{1 + p_4}$ and $r_y + \frac{p_4(c_y - f_y)}{1 - p_4}$. Finally, two special cases are considered. When $p_4 = 0$ and $p_1 \neq 1$, according to (7), there exists $E_y = r_y$. And when $p_1 = 1$ and $p_4 \neq 0$, which means $\lambda = 0$, we have $E_y$ with a maximum value of $r_y + f_y + a_y - c_y$. □

#### 4.2.2 Analysis of $e_x$'s Payoff

Specifically, $e_x$ may set $\beta = 0$, yielding $E_x = -\gamma/\alpha$. In this way, $e_x$ can set its own expected payoff unilaterally without any impact of $e_y$'s strategy. Through the analogous calculation with the second column of (3) equal to $\alpha \boldsymbol{S}_x + \gamma \mathbf{1}$, we can express $p_2$ and $p_3$ with $p_1$ and $p_4$ as follows:

$$\begin{aligned} p_2 &= \frac{(1 + p_4)(S_x^1 - S_x^2) - p_1(S_x^4 - S_x^2)}{S_x^1 - S_x^4} \\ &= \frac{(1 + p_4)a_x - p_1(c_x - f_x)}{f_x + a_x - c_x}, \\ p_3 &= \frac{-(1 - p_1)(S_x^3 - S_x^4) - p_4(S_x^3 - S_x^1)}{S_x^1 - S_x^4} \\ &= \frac{-(1 - p_1)a_x - p_4(c_x - f_x)}{f_x + a_x - c_x}. \end{aligned}$$

By calculating the expressions of $\alpha$ and $\gamma$, we have

$$E_x = \frac{(1 - p_1)r_x + p_4(r_x + f_x + a_x - c_x)}{(1 - p_1) + p_4}. \tag{8}$$

Then we consider the scope limitation under different parameter cases.

**Theorem 6**. *When $c_x < f_x$, we can derive two types of results according to the relationship between $f_x - a_x$ and $c_x$: 1) when $c_x < f_x - a_x$, $e_x$ can control $E_x \in [r_x + a_x, r_x + f_x - c_x]$; 2) in the case of $c_x \geqslant f_x - a_x$, $e_x$ cannot set the range of $E_x$ unilaterally.*

**Theorem 7**. *When $c_x > f_x + a_x$, if $p_4 \in (0, \frac{c_x - f_x - a_x}{c_x - f_x + a_x})$, the maximum of $E_x$ is $r_x + \frac{p_4(c_x - f_x)(f_x + a_x - c_x)}{(1 + p_4)(c_x - f_x - a_x)}$, while if $p_4 \in (\frac{c_x - f_x - a_x}{c_x - f_x + a_x}, \frac{c_x - f_x - a_x}{c_x - f_x})$, the maximum of $E_x$ is $r_x + \frac{p_4 a_x(f_x + a_x - c_x)}{(1 - p_4)(c_x - f_x) - a_x}$. And in the case of $p_1 = 1, p_4 \neq 0$, the minimum value of $E_x$ is $r_x + f_x + a_x - c_x$, and if $p_4 = 0, p_1 \neq 1$, the maximum value of $E_x$ is $r_x$.*

**Theorem 8**. *When $f_x < c_x < f_x + a_x$, $e_x$ cannot unilaterally set its own payoff range.*

The proofs of the Theorems 6–8 are similar to those of Theorems 3–5, which are omitted here to avoid redundancy.

### 4.3 Existence of Zero-Determinant Strategy in Finitely Repeated Games

Most of the existing researches on the ZD strategy are carried out in the scenario of infinitely repeated games. While in our considered PCN game, it can be observed that the channels are bound to exhaust the preallocated deposits and then deconstruct the payment channels temporarily or permanently from the PCN. In this subsection, we consider a more realistic scenario where channels are playing finitely repeated games with each other, and then the new version of the ZD strategy in this case is analyzed.

We define a discount factor $\omega \in (0, 1)$ to present the probability of a next game round taking place given the current round. Then $\omega^n$ is the probability for the occurrence of the $n$-th round and the probability that the next round does not happen is $1 - \omega$. We give the probability of cooperation of any two players in the $t$-th round ($t \in \{0, 1, 2, \cdots\}$) game with different combinations of strategies as

$$\boldsymbol{u}(t) = (u_{CC}(t), u_{CD}(t), u_{DC}(t), u_{DD}(t)),$$

where $u_{CC}(t)$ is the probability that both players cooperate in round $t$, $u_{CD}(t)$ is the probability that $e_x$ cooperates and $e_y$ defects in round $t$, and so forth. The normalization is given by $u_{CC}(t) + u_{CD}(t) + u_{DC}(t) + u_{DD}(t) = 1$. We refer to the first round of the repeated game as round 0 and denote the cooperation probabilities of $e_x$ and $e_y$ in the first round as $\eta_x$ and $\eta_y$ respectively. The initial probability corresponding to different states is

$$\boldsymbol{u}(0) = (\eta_x \eta_y, \eta_x(1 - \eta_y), (1 - \eta_x)\eta_y, (1 - \eta_x)(1 - \eta_y)).$$

Then the expected payoff of channel $e_x$ in round $t$ can be calculated by $\boldsymbol{u}(t)\boldsymbol{S}_x$, and thus, the expected per-round payoff of $e_x$ in the finitely repeated game is the

accumulated expected payoffs until the $t$-th round divided by the number of rounds, which is

$$E_x = \frac{\sum_{t=0}^{\infty} \omega^t \boldsymbol{u}(t)\boldsymbol{S}_x}{(1-\omega)^{-1}} = (1-\omega)\sum_{t=0}^{\infty}\omega^t \boldsymbol{u}(t)\boldsymbol{S}_x.$$

Given the state transition probability matrix $\boldsymbol{M}$ in (2), we have $\boldsymbol{u}(t) = \boldsymbol{u}(0)\boldsymbol{M}^t$. By substituting $\boldsymbol{u}(t)$ and calculating the limit of the summation $\boldsymbol{M}^t$, the above equation can be further written as

$$E_x = (1-\omega)\boldsymbol{u}(0)\sum_{t=0}^{\infty}(\omega\boldsymbol{M})^t\boldsymbol{S}_x = (1-\omega)\boldsymbol{u}(0)(\boldsymbol{I}-\omega\boldsymbol{M})^{-1}\boldsymbol{S}_x,$$

where $\boldsymbol{I}$ is a 4×4 identity matrix. Similarly, the expected per-round payoff of $e_y$ is given by

$$E_y = (1-\omega)\boldsymbol{u}(0)(\boldsymbol{I}-\omega\boldsymbol{M})^{-1}\boldsymbol{S}_y. \tag{9}$$

Similar to the infinitely repeated game, we study the case of $e_x$ using the ZD strategy as an example to make a linear relationship between the payoffs hold, i.e., $\alpha E_x + \beta E_y + \gamma = 0$. Via setting $\alpha = 0$, $e_x$ can control $E_y$, and with $\beta = 0$, $e_x$ can control its own payoff $E_x$. Considering that $e_y$'s strategy has no impact on the effectiveness of ZD, we set $\boldsymbol{q} = (1,1,1,1)$ and $\boldsymbol{q} = (0,0,0,0)$ to calculate $e_x$'s strategy.

#### 4.3.1 Analysis of $e_y$'s Payoff

As mentioned earlier, $E_y = \frac{-\gamma}{\beta}$. When $e_y$ adopts strategies $\boldsymbol{q} = (1,1,1,1)$ and $\boldsymbol{q} = (0,0,0,0)$, we denote the matrix in (2) as $\boldsymbol{M}_{y,1111}$ and $\boldsymbol{M}_{y,0000}$, respectively. Then, referring to (9) we have $(1-\omega)\boldsymbol{u}(0)(\boldsymbol{I} - \omega\boldsymbol{M}_{y,0000})^{-1} = (1-\omega)\boldsymbol{u}(0)(\boldsymbol{I}-\omega\boldsymbol{M}_{y,1111})^{-1}$ for any $\eta_y \in [0,1]$. According to the conclusion in [16], we can derive $p_2$ and $p_3$ as follows:

$$\begin{aligned} p_2 &= \frac{p_1 a_y - (\frac{1}{\omega}+p_4)(c_y - f_y)}{f_y + a_y - c_y}, \\ p_3 &= \frac{(\frac{1}{\omega}-p_1)(c_y-f_y) + p_4 a_y}{f_y + a_y - c_y}. \end{aligned} \tag{10}$$

By substituting $\boldsymbol{p}$ in (9) we can obtain

$$E_y = \frac{(1-\bar{\omega}\eta_x - \omega p_1)S_y^4 + (\bar{\omega}\eta_x + \omega p_4)S_y^1}{1-\omega p_1 + \omega p_4},$$

which is clearly independent of the strategy and the initial cooperation probability of $e_y$, i.e., $\boldsymbol{q}$ and $\eta_y$. In the above equation, $\bar{\omega} = 1-\omega$ for brevity. This equation indicates that $e_x$'s control over $E_y$ depends on the value of $\eta_x$, $\omega$, and $\boldsymbol{p}$. Besides, $\omega$ is related to the expected number of repeated rounds in the finitely repeated game. In the following, we identify the condition for $\omega$ under which the ZD strategy exists. According to (10), we can see that the ZD strategy exists if and only if

$$0 \leqslant p_1 a_y - \left(\frac{1}{\omega}+p_4\right)(c_y - f_y) \leqslant f_y + a_y - c_y, \tag{11}$$

and

$$0 \leqslant \left(\frac{1}{\omega}-p_1\right)(c_y-f_y) + p_4 a_y \leqslant f_y + a_y - c_y, \tag{12}$$

for $0 \leqslant p_1, p_4 \leqslant 1$ and $f_y + a_y - c_y > 0$. If $c_y > f_y + a_y$, by calculating $0 \leqslant p_2, p_3 \leqslant 1$, we have $\omega \geqslant 1$ and the ZD strategy does not work. Therefore, we only need to analyze the limitation that $f_y + a_y > c_y$ as following.

**Theorem 9**. *When $c_y < f_y$, $\omega$ needs to be satisfied as $\omega \geqslant \frac{f_y - c_y}{f_y + a_y - c_y}$.*

*Proof.* In this case, we can figure out

$$\begin{cases} \omega \geqslant \dfrac{f_y - c_y}{(1-p_1)a_y + (1-p_4)(f_y - c_y)}, \\ \omega \geqslant \dfrac{f_y - c_y}{p_1(f_y - c_y) + p_4 a_y}. \end{cases}$$

$\omega$ must be greater than the minimum values on the right side of the two inequalities. Therefore, we obtain the condition of $\omega \geqslant \frac{f_y - c_y}{f_y + a_y - c_y}$. □

**Theorem 10**. *When $f_y < c_y < f_y + a_y$, the basic condition $\omega$ needs to meet is $\omega \geqslant \frac{c_y - f_y}{a_y}$.*

*Proof.* Any effective assignments of $p_1$ and $p_4$ satisfy the second inequality of (11) and the first inequality of (12), thereby we focus on the other two inequalities, respectively. We have

$$\begin{cases} \omega \geqslant \dfrac{c_y - f_y}{p_1 a_y - p_4(c_y - f_y)}, \\ \omega \geqslant \dfrac{c_y - f_y}{(p_1 - 1)(c_y - f_y) + (1-p_4)a_y}. \end{cases}$$

Under the most relaxed conditions, $\omega$ needs to be greater than the minimum on the right side of the inequalities. Obviously, both inequalities have a minimum of $\frac{c_y - f_y}{a_y}$. □

#### 4.3.2 Analysis of $e_x$'s Payoff

We continue to analyze player $e_x$ trying to unilaterally set its own payoff in the finitely repeated game. By setting $\beta = 0$, $e_x$ sets its own payoff, at this point,

$E_x$ is independent of $e_y$'s strategy, and $p_2$ and $p_3$ can be expressed as follows:

$$p_2 = \frac{(\frac{1}{\omega} + p_4)a_x - p_1(c_x - f_x)}{f_x + a_x - c_x},$$

and

$$p_3 = \frac{-(\frac{1}{\omega} - p_1)a_x - p_4(c_x - f_x)}{f_x + a_x - c_x}.$$

Further, the payoff of $e_x$ becomes

$$E_x = \frac{(1 - \bar{\omega}\eta_x - \omega p_1)S_x^4 + (\bar{\omega}\eta_x + \omega p_4)S_x^1}{1 - \omega p_1 + \omega p_4},$$

which is only dependent on the strategy and initial cooperation probability of $e_x$, i.e., $\boldsymbol{p}$ and $\eta_x$. Then we identify the condition for $\omega$ under which the ZD strategy works. $p_2$ and $p_3$ must be in the range of $[0, 1]$ on the condition that $p_1$ and $p_4$ also fall into this range, thereby we have

$$0 \leqslant \left(\frac{1}{\omega} + p_4\right) a_x - p_1(c_x - f_x) \leqslant f_x + a_x - c_x,$$

and

$$0 \leqslant -\left(\frac{1}{\omega} - p_1\right) a_x - p_4(c_x - f_x) \leqslant f_x + a_x - c_x.$$

When $f_x < c_x < f_x + a_x$, $\omega$ has a minimum of 1, which does not satisfy the condition for a finite number of repetitions. Therefore we study the other two cases as follows.

**Theorem 11**. *When $c_x < f_x$, $\omega$ needs to be satisfied as $\omega \geqslant \frac{a_x}{f_x + a_x - c_x}$.*

**Theorem 12**. *When $c_x > f_x + a_x$, the condition of $\omega \geqslant \frac{a_x}{c_x - f_x}$ should be satisfied.*

The proof of these two theorems is similar to those of the previous Theorem 9 and Theorem 10, and thus we omit them for brevity.

## 5 Macroscopic Analysis of PCN Game

Generally, since there are a number of channels in PCN, they can be regarded as a population, where each channel interacts with the adjacent channels in a continuous manner. By investigating the large number of two-player PCN games between each pair of adjacent channels, we can study the evolution of the whole population with the help of the evolutionary game theory, which is termed as the evolutionary PCN game. Specifically, we analyze the state that the entire population can reach from two aspects: replication dynamic analysis and the evolutionary stability of the ZD strategy.

### 5.1 Replication Dynamic Analysis

A channel is defined as an evolutionary player if it adjusts strategies such as cooperation or defection according to some optimization scheme to maximize its payoff. In this paper, we use the Fermi evolutionary rule [17, 18] as an update rule of channels' strategies, which is based on the assumption that players' strategies in an evolutionary game obtain more payoffs by imitating neighbors' strategies and converging to a stable state. The specific manifestation of this rule is that all the channels in the evolutionary PCN game, randomly select one adjacent channel to compare their payoffs and decide whether or not to learn this neighbor's strategy after each round of the game. Following the update rule, the final channels' payoffs and strategies reach a stable state. In this case, we want to figure out what state the channels will converge to during the evolution process and the effect of the parameters on the stable state.

*Theoretical Analysis.* The replication dynamics can well describe how players in a game gradually achieve the stability of their strategies by imitating and learning the strategies of their opponents. In the following, we use this method to study the stable state of strategies in the evolutionary PCN game.

We assume that $\theta$ is the percentage of channels choosing the cooperation strategy and then $1 - \theta$ is the percentage of channels adopting the defection strategy. In other words, in the evolutionary PCN game, the probability of each participant channel, e.g., $e_z$, encountering the opponent with the strategy $C$ is $\theta$, and the probability of encountering the opponent with the strategy $D$ is $1-\theta$. We define the payoff vector of $e_z$ as $\boldsymbol{S}_z = (S_z^1, S_z^2, S_z^3, S_z^4)^{\mathrm{T}}$, corresponding to the payoff of $e_z$ when the strategy combinations of $e_z$ and its opponents are $(CC, CD, DC, DD)$, which can be similarly defined according to (1),

$$\boldsymbol{S}_z = \begin{pmatrix} r_z + f_z + a_z - c_z \\ r_z + f_z - c_z \\ r_z + a_z \\ r_z \end{pmatrix}.$$

Then the expected payoff of $e_z$ choosing cooperation, denoted as $E_z^C$, can be expressed as the weighted sum of $S_z^1$ and $S_z^2$ corresponding to the strategies of $e_z$ and the opponent being $CC$, and $CD$, where the probabilities of the two cases are $\theta$ and $1-\theta$, respectively. Thus, we have

$$E_z^C = \theta S_z^1 + (1 - \theta)S_z^2.$$

While if $e_z$ chooses defection, $e_z$ and any opponent can produce strategy combinations of $DC$ and $DD$. Then we can calculate the expected payoff of $e_z$ choosing defection, denoted as $E_z^D$, based on $S_z^3$ and $S_z^4$ as follows,

$$E_z^D = \theta S_z^3 + (1-\theta) S_z^4.$$

As a random player, $e_z$ also adopts $C$ and $D$ with the probabilities $\theta$ and $1-\theta$, respectively, leading to its average expected payoff being expressed as

$$\widehat{E_z} = \theta E_z^C + (1-\theta) E_z^D.$$

According to Malthusian replication dynamic equation [19], the growth rate of $\theta$, denoted as $F(\theta)$, can be expressed by:

$$F(\theta) = \theta(E_z^C - \widehat{E_z}) = \theta(1-\theta)(f_z - c_z), \quad (13)$$

which is based on the fact that the higher the payoff brought by the strategy $C$ for any player, the higher the growth rate of the percentage of channels adopting the strategy $C$.

Given $F(\theta^*) = 0$, we name that $\theta^*$ is the evolutionary stable solution of the replication dynamic equation if $F'(\theta^*) < 0$. It means that even any accidental changes in the strategies of some players make $\theta$ deviate from $\theta^*$, the replication dynamic can restore $\theta$ to $\theta^*$. In mathematics, this is equivalent to that when $\theta < \theta^*$, the dynamic equation leads to $F(\theta) > 0$ in order to guarantee $\theta$'s increasing trend. On the contrary, if $\theta > \theta^*$, then $F(\theta) < 0$ has to hold to make $\theta$ decline. Therefore the derivative of $F(\theta)$ must be less than zero in the steady state $\theta^*$. Therefore, we calculate the equilibrium points by setting $F(\theta) = 0$, which has two feasible solutions, i.e., $\theta_1 = 0$, and $\theta_2 = 1$. And we can calculate the derivative of $F(\theta)$ as

$$F'(\theta) = (1-2\theta)(f_z - c_z). \quad (14)$$

**Theorem 13**. *If $c_z < f_z$, $\theta = 1$ is an evolutionarily stable point of the evolutionary PCN game.*

*Proof.* When $c_z < f_z$, there exists $F(\theta) > 0$ for any $\theta \in (0,1)$ according to (13), which indicates that $\theta$ increases over time until $\theta = 1$. By substituting $\theta = 1$ into (13) and (14), we have $F(1) = 0$ and $F'(1) < 0$. Therefore, $\theta = 1$ is the evolutionarily stable point in this case. If some channels' strategies accidentally change to $D$ leading to $\theta < 1$, the growth rate $F(\theta) > 0$ makes $\theta$ increase toward 1. □

**Theorem 14**. *If $c_z > f_z$, $\theta = 0$ is an evolutionarily stable point of the evolutionary PCN game.*

*Proof.* In the case of $c_z > f_z$, $F(\theta) < 0$ holds for $\theta \in (0,1)$ referring to (13), and $\theta$ is decreasing over time as long as there are channels choosing $C$ in the PCN. When $\theta = 0$, we can calculate $F(0) = 0$ and $F'(0) = f_z - c_z < 0$ from (13) and (14). Therefore $\theta = 0$ is the evolutionarily stable point when $c_z > f_z$. If there are few mutations of channels' strategies resulting in $\theta > 0$, these channels will update their strategies to bring $\theta$ back to 0 gradually owing to the growth rate $F(\theta) < 0$. □

**Theorem 15**. *If $c_z = f_z$, the current system is in a stable state.*

*Proof.* When $c_z = f_z$, $F(\theta) = 0$ is always true, which means that the change rate of $\theta$ is 0; therefore each channel in the PCN does not change its strategy, and the initial state remains stable. □

### 5.2 Evolutionary Stability of ZD Strategy

In this subsection, we explore the evolutionarily stable strategy (ESS) of the evolutionary PCN game with the involvement of the ZD strategy. In order to scientifically reveal the stability of the ZD strategy in population and comprehensively understand the role of the ZD strategy in the evolutionary game, we consider two cases: 1) there is only one other strategy in the population of channels besides the ZD strategy, and 2) there exist multiple strategies in the population in addition to the ZD strategy. To carry out the analysis in a simple-to-complex way, we first investigate the case of the ZD strategy vs one other strategy, and then the case of the ZD strategy vs multiple other strategies in the following.

#### 5.2.1 ZD vs One Other Strategy

In the evolutionary PCN game involving the ZD strategy, we first consider that there are two types of strategies for channels, i.e., the ZD strategy and the other well-known strategies (denoted as OT). For a strategy $T$ to be an ESS, it has to satisfy the following definition [20].

**Definition 2** (Evolutionarily Stable Strategy). *$T$ is an ESS if for an arbitrary strategy $J \neq T$, there exists either $E(T,T) > E(J,T)$, or $E(T,T) = E(J,T)$ and $E(T,J) > E(J,J)$, where the profit function $E(T,J)$ is the payoff of the player with strategy $T$ when playing against the other one taking strategy $J$.*

We define the channel choosing the ZD strategy as $e_{\mathrm{ZD}}$, and its mixed strategy is denoted as $\tilde{\boldsymbol{p}} = (\tilde{p}_1, \tilde{p}_2, \tilde{p}_3, \tilde{p}_4)$. Similarly, a channel adopting OT is expressed as $e_{\mathrm{OT}}$, and its strategy is denoted as $\tilde{\boldsymbol{q}} =$

$(\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4)$. Here we consider four classical strategies as examples, including the unconditional defection (ALLD), unconditional cooperation (ALLC), win-stay-lose-shift (WSLS) and tit-for-tat (TFT) strategies. When $e_{\rm OT}$ chooses the ALLD strategy, $\tilde{\boldsymbol{q}} = (0, 0, 0, 0)$; when $e_{\rm OT}$ chooses the ALLC strategy, $\tilde{\boldsymbol{q}} = (1, 1, 1, 1)$; when $e_{\rm OT}$ chooses the WSLS strategy, $\tilde{\boldsymbol{q}} = (1, 0, 0, 1)$; and if $e_{\rm OT}$ chooses the TFT strategy, $\tilde{\boldsymbol{q}} = (1, 0, 1, 0)$.

Next, under several strategies introduced above, when ZD players choose to control the opponents' or their own payoffs, we can analyze ZD's ESS features in the evolutionary PCN game as follows.

1) *Analysis of $e_{\rm OT}$'s Payoff.* The payoffs of channels playing against $e_{\rm ZD}$ are determined by $\tilde{p}_1$ and $\tilde{p}_4$, such as $E_y$ in (7). When $e_{\rm ZD}$ plays the game with $e_{\rm OT}$, we have $e_{\rm OT}$'s payoff

$$E_{(\rm OT,\ ZD)} = \frac{(1-\tilde{p}_1)r_{\rm OT} + \tilde{p}_4(r_{\rm OT} + f_{\rm OT} + a_{\rm OT} - c_{\rm OT})}{(1-\tilde{p}_1) + \tilde{p}_4},$$

and $e_{\rm ZD}$'s payoff

$$E_{(\rm ZD,\ OT)} = \frac{\boldsymbol{G}(\tilde{\boldsymbol{p}}, \tilde{\boldsymbol{q}}, \boldsymbol{S}_{\rm ZD})}{\boldsymbol{G}(\tilde{\boldsymbol{p}}, \tilde{\boldsymbol{q}}, \boldsymbol{1})},$$

which is dependent on both players' strategies, and can be calculated using (3). Since the above equation can be over-length, we do not fully expand the expression here. We know that $e_{\rm ZD}$ enforces the payoff regardless of the opponent's strategy, which implies that it also enforces this on another ZD player. Therefore, when the opponent takes the ZD strategy, we have $E_{(\rm ZD,\ ZD)} = E_{(\rm OT,\ ZD)}$. When $e_{\rm OT}$ plays the game with another $e_{\rm OT}$, the payoff of $e_{\rm OT}$ changes according to what the specific OT strategy $e_{\rm OT}$ adopts. In detail, when OT is the ALLD strategy, $E_{(\rm OT,\ OT)} = r_{\rm OT}$. When OT is the ALLC strategy or the WSLS strategy, $E_{(\rm OT,\ OT)} = r_{\rm OT} + f_{\rm OT} + a_{\rm OT} - c_{\rm OT}$. When OT is the TFT strategy, $E_{(\rm OT,\ OT)} = r_{\rm OT} + (f_{\rm OT} + a_{\rm OT} - c_{\rm OT})/2$. Here we have the payoff vectors $\boldsymbol{S}_{\rm ZD}, \boldsymbol{S}_{\rm OT}$ for $e_{\rm ZD}$ and $e_{\rm OT}$, respectively, which represent their respective payoffs under different combinations of strategies.

In the above cases, we compare the relationship between different payoffs to determine which strategy is the ESS.

**Theorem 16.** *If $E_{(\rm ZD,\ OT)} > E_{(\rm OT,\ OT)}$, the ZD strategy is ESS. If $E_{(\rm ZD,\ OT)} < E_{(\rm OT,\ OT)}$, the opposing strategy is ESS.*

*Proof.* When $e_{\rm ZD}$ chooses to set the opponent's payoff, both $e_{\rm OT}$ and $e_{\rm ZD}$ who play with $e_{\rm ZD}$ have the payoff controlled by $e_{\rm ZD}$, thereby the payoffs $E_{(\rm ZD,\ ZD)}$ and $E_{(\rm OT,\ ZD)}$ are equivalent. We determine the existence of ESS by using the second condition in Definition 2. In our case, only when $E_{(\rm ZD,\ OT)} > E_{(\rm OT,\ OT)}$, ZD is the ESS and vice versa. □

2) *Analysis of $e_{\rm ZD}$'s Payoff.* We denote $e_{\rm ZD}$'s payoff according to (8) as

$$E_{(\rm ZD,\ OT)} = \frac{(1-\tilde{p}_1)r_{\rm ZD} + \tilde{p}_4(r_{\rm ZD} + f_{\rm ZD} + a_{\rm ZD} - c_{\rm ZD})}{(1-\tilde{p}_1) + \tilde{p}_4},$$

while $E_{(\rm ZD,\ ZD)} = E_{(\rm ZD,\ OT)}$. And the payoff of $e_{\rm OT}$ playing against $e_{\rm ZD}$ is denoted as

$$E_{(\rm OT,\ ZD)} = \frac{\boldsymbol{G}(\tilde{\boldsymbol{p}}, \tilde{\boldsymbol{q}}, \boldsymbol{S}_{\rm OT})}{\boldsymbol{G}(\tilde{\boldsymbol{p}}, \tilde{\boldsymbol{q}}, \boldsymbol{1})}.$$

The payoff of $e_{\rm OT}$ against another $e_{\rm OT}$ is $E_{(\rm OT,\ OT)}$, and its value is decided by the specific OT strategy adopted. Similarly, the determination of the ESS depends on the four payoffs of both sides in the game.

**Theorem 17.** *If $E_{(\rm ZD,\ OT)} > E_{(\rm OT,\ ZD)}$, or $E_{(\rm ZD,\ OT)} = E_{(\rm OT,\ ZD)}$ and $E_{(\rm ZD,\ OT)} > E_{(\rm OT,\ OT)}$, the ZD strategy is the ESS. If $E_{(\rm OT,\ OT)} > E_{(\rm ZD,\ OT)}$, or $E_{(\rm OT,\ OT)} = E_{(\rm ZD,\ OT)}$ and $E_{(\rm OT,\ ZD)} > E_{(\rm ZD,\ ZD)}$, the opposing strategy is the ESS.*

The procedure of the proof is similar to that of Theorem 16, thereby we omit it for brevity.

### 5.2.2 ZD vs Multiple Other Strategies

In Subsection 5.2.1, we analyze the evolutionarily stable strategies between the ZD strategy and one other well-known strategy. However, in reality, different channels may choose different strategies in order to achieve high payoffs, resulting in multiple other strategies coexisting in the population. Therefore, in this subsection, we consider whether the ZD strategy can maintain the stability in the process of population evolution by controlling ZD players' opponents' payoffs or ZD players' own payoffs given the existence of multiple other strategies. We assume that the number and the distribution of channels with different strategies are uniform in the population, and the probability of each channel encountering different opponents with different strategies is the same. At the end of each round of the game, all channels utilize the Fermi evolutionary rule to update their strategies to attain higher payoffs in the next round of the game. As the repeated game evolves, the strategy selection of channels in the population will be stable. If it turns out to be a single strategy dominating the whole population, the final output of the evolutionarily stable strategy is similar to what we studied in Subsection 5.2.1; or there may be a mixed evolutionarily stable state of multiple strategies.

We study the performance of $e_{\mathrm{ZD}}$ in terms of controlling the opponent's and its own payoffs when there are multiple different strategies $\{\mathrm{OT}_1, \mathrm{OT}_2, ..., \mathrm{OT}_k\}$ with the number of other strategies $k \geqslant 2$ in the population besides the ZD strategy. In the following, we discuss two situations where $e_{\mathrm{ZD}}$ is utilized to set up its opponent's and its own payoffs.

1) *Analysis of $e_{\mathrm{OT}}$'s Payoff.* When $e_{\mathrm{ZD}}$ unilaterally controls the benefits of its opponents, any channel in the PCN that plays a game with $e_{\mathrm{ZD}}$ receives the same average expected payoff, including $e_{\mathrm{ZD}}$, i.e., $E_{(\mathrm{ZD},\ \mathrm{ZD})} = E_{(\mathrm{OT}_i,\ \mathrm{ZD})}$, $\forall i \in \{1, 2, ..., k\}$. Then we explore the constraints that need to be satisfied when different strategies are evolutionarily stable strategies in the population.

**Theorem 18**. *If there exists $\sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)} > \sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)}$, $\forall i \in \{1, 2, ..., k\}$, the ZD strategy is the ESS. If $\sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)} > \sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)}$ and $\sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)} > \sum_{j=1}^{k} E_{(\mathrm{OT}_m,\ \mathrm{OT}_j)}, \forall m \in \{1, 2, ..., k\}, m \neq i$, the $\mathrm{OT}_i$ strategy is the ESS.*

*Proof.* In each round of the game, we assume that the total number of games between each channel and adjacent channels is $t$, and each channel has the same probability of interaction with channels of other strategies. Therefore, the expected payoff of the channels with different strategies can be denoted as

$$E_{\mathrm{ZD}} = \frac{t}{k+1}\left(E_{(\mathrm{ZD},\ \mathrm{ZD})} + \sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)}\right),$$

$$E_{\mathrm{OT}_i} = \frac{t}{k+1}\left(E_{(\mathrm{OT}_i,\ ZD)} + \sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)}\right).$$

Channels randomly select an adjacent channel at the end of each round and compare their payoffs to determine whether to imitate the opponent's strategy. Therefore, when $e_{\mathrm{ZD}}$'s expected payoff is higher than that of other strategies, the ZD strategy is the learning goal of the whole population, and the evolution of the population will present only ZD as an ESS. Because $E_{(\mathrm{ZD},\ \mathrm{ZD})} = E_{(\mathrm{OT}_i,\ \mathrm{ZD})}$, the comparison of payoffs between different strategies only needs to focus on $\sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)}$ and $\sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)}, \forall i \in \{1, 2, ..., k\}$, where $\sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)} > \sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)}$, $\forall i \in \{1, 2, ..., k\}$ means $e_{\mathrm{ZD}}$ obtains the highest expected payoff, and thus the ZD strategy is the ESS. For an arbitrary $\mathrm{OT}_i$ strategy, when $\sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)} > \sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)}$ and $\sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)} > \sum_{j=1}^{k} E_{(\mathrm{OT}_m,\ \mathrm{OT}_j)}, \forall m \in \{1, 2, ..., k\}, m \neq i$, $\mathrm{OT}_i$ obtains a higher payoff than the ZD and other strategies; therefore the $\mathrm{OT}_i$ is the ESS. □

2) *Analysis of $e_{\mathrm{ZD}}$'s Payoff.* In this case, the $e_{\mathrm{ZD}}$'s expect payoff is not influenced by its opponents' strategies. We use the following theorem to illustrate the evolutionary stability of the ZD strategy in a population where multiple strategies coexist.

**Theorem 19**. *If $E_{(\mathrm{ZD},\ \mathrm{ZD})} > \frac{1}{k+1}\left(E_{(\mathrm{OT}_i,\ \mathrm{ZD})} + \sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)}\right)$, $\forall i \in \{1, 2, ..., k\}$, the ZD strategy is the ESS. If $E_{(\mathrm{OT}_i,\ \mathrm{ZD})} + \sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)} > E_{(\mathrm{ZD},\ \mathrm{ZD})} + \sum_{j=1}^{k} E_{(\mathrm{ZD},\ \mathrm{OT}_j)}$ and $E_{(\mathrm{OT}_i,\ \mathrm{ZD})} + \sum_{j=1}^{k} E_{(\mathrm{OT}_i,\ \mathrm{OT}_j)} > E_{(\mathrm{OT}_m,\ ZD)} + \sum_{j=1}^{k} E_{(\mathrm{OT}_m,\ \mathrm{OT}_j)}, \forall m \in \{1, 2, ..., k\}, m \neq i$, the $\mathrm{OT}_i$ strategy is the ESS.*

The proof is similar to that of Theorem 18. For the sake of brevity, we omit the details here.

Through Theorem 18 and Theorem 19, we derive the conditions for the ZD strategy to become an ESS when multiple strategies exist in the population. In the continuous repeated games, players with different strategies will get different payoffs, which can be utilized to speculate on the opponent's strategy and then consider whether they should imitate the opponent's strategy to obtain higher payoffs. Therefore, in the population of payment channels, when $e_{\mathrm{ZD}}$ obtains the highest profit, it will be finally adopted by all channels in the PCN.

However, note that if the conditions for any strategy to become an ESS cannot be fully satisfied, which means no single strategy can outperform the others, then the population will eventually reach a mixed evolutionary stable state consisting of multiple strategies.

## 6 Experimental Evaluation

In this section, we conduct a series of experiments to validate the control power and the existence of the ZD strategy in the cases of infinitely and finitely repeated games, as well as the evolutionarily stable points and the evolutionary stability of the ZD strategy when playing against one other strategy and multiple other strategies in the evolutionary PCN game.

### 6.1 ZD Strategy in Infinitely Repeated Game

To evaluate the control power of the ZD strategy in the infinitely repeated game, we conduct a series of simulations to study the impact of payoff parameters on the payoff range and report the results in Figs.3–10. When $e_x$ sets $e_y$'s payoff, we set $r_y, f_y, a_y$, and $c_y$ as

2, 1.5, 1.2 and 0.9, respectively, to testify $E_y$'s range when $c_y < f_y$ and $c_y > f_y - a_y$ hold in Theorem 3, where the experimental results are shown in Figs.3 and 4. We can see from Fig.3 that $E_y$'s range is $[2.6, 3.2]$, which satisfies the boundary range given by $\lambda$. We set $E_y$ as 0 when $p_2 \notin [0,1]$ or $p_3 \notin [0,1]$, to distinguish the effective range that $e_x$ can control. Fig. 4(a) and Fig.4(b) show the change of $E_y$ with $p_4$ when $p_1 = 0.4$ and $p_1 = 0.8$ respectively, and Fig.4(c) and Fig.4(d) indicate the effect of $p_1$ on $E_y$ when $p_4 = 0.2$ and $p_4 = 0.6$ respectively.

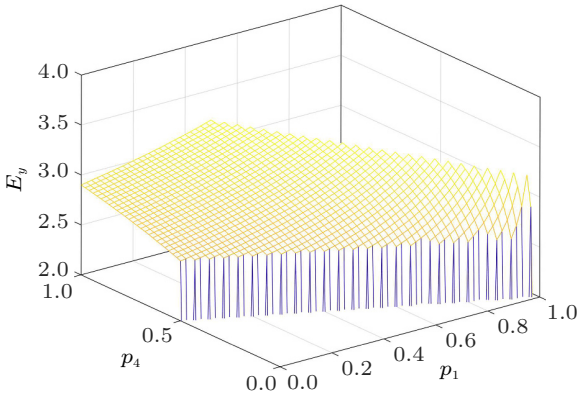



Fig. 3. Range of $E_y$ controlled by the ZD strategy when $f_y - a_y < c_y < f_y$ [14].

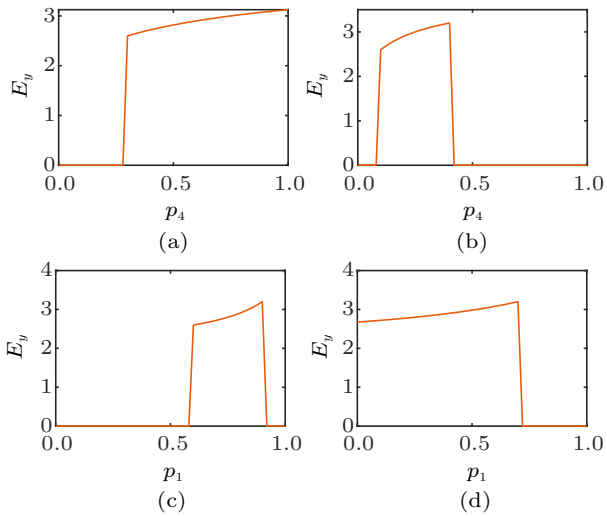



Fig.4. Effect of $p_1$ and $p_4$ on $E_y$ when $f_y - a_y < c_y < f_y$ [14]. (a) $p_1 = 0.4$. (b) $p_1 = 0.8$. (c) $p_4 = 0.2$. (d) $p_4 = 0.6$.

Via adjusting $c_y$ to 1.8, Figs.5 and 6 show the payoff range of $e_y$ that $e_x$ can control under the condition of $f_y < c_y < f_y + a_y$. Fig.6 is with the same setting as Fig. 10. Based on the experimental results, when $p_4 \in (0, 0.6)$, $E_y$ has the minimum value of $2 + \frac{1.2p_4}{1+p_4}$; when $p_4 \in (0.6, 0.75)$, $E_y$ has the minimum value of $2 + \frac{0.3p_4}{1-p_4}$. And when $p_4 = 0, p_1 \neq 1$, $E_y$ reaches the minimum 2; when $p_1 = 1, p_4 \neq 0$, $E_y$ obtains the maximum 2.9.

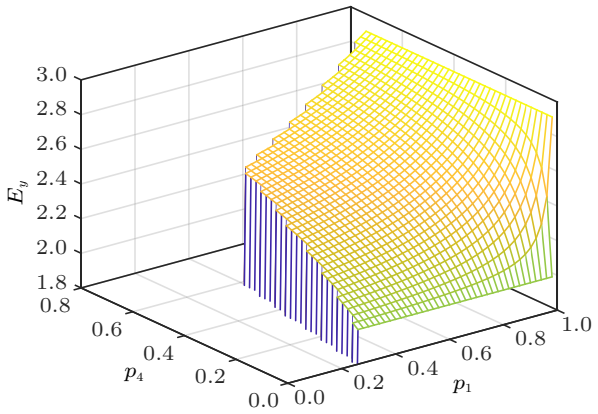



Fig. 5. Range of $E_y$ controlled by the ZD strategy when $f_y < c_y < f_y + a_y$ [14].

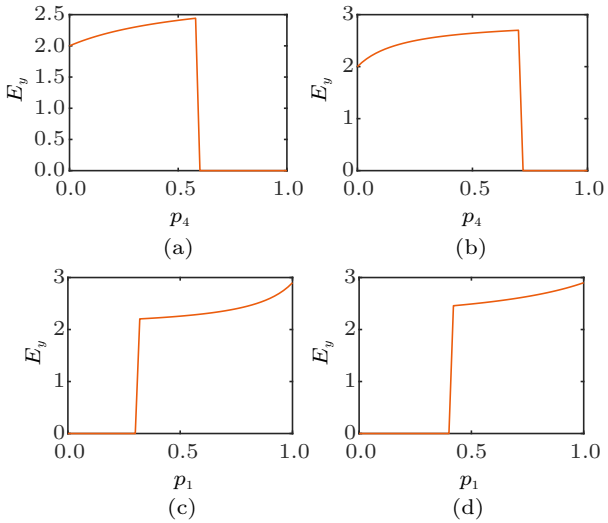



Fig.6. Effect of $p_1$ and $p_4$ on $E_y$ when $f_y < c_y < f_y + a_y$ [14]. (a) $p_1 = 0.4$. (b) $p_1 = 0.8$. (c) $p_4 = 0.2$. (d) $p_4 = 0.6$.

Fig.7 and Fig.8 show that when $e_x$ uses the ZD strategy to control its own payoff, where we set $r_y, f_y, a_y$, and $c_y$ as 2, 1.5, 1.2 and 0.06 respectively, $c_x < f_x$ and $c_x < f_x - a_x$ hold. According to the experimental results, the range of $E_x$ is [3.2, 3.44]. And Fig.8 shows the range of $E_x$ when $p_1 = 0.4$, $p_1 = 0.8$, $p_4 = 0.2$, and $p_4 = 0.6$. As shown in Figs.9 and 10, when we set $c_x$ as 3 so that $c_x > f_x + a_x$ is satisfied as mentioned in Theorem 7, the maximum value of $E_x$ is $2 - \frac{p_4}{6(1+p_4)}$ when $p_4 \in (0, \frac{1}{9})$, and the maximum value of $E_x$ is $2 - \frac{1.2p_4}{1-p_4}$ when $p_4 \in (\frac{1}{9}, \frac{1}{5})$. And in the case of $p_1 = 1, p_4 \neq 0$, there is a minimum payoff of 1.7, while if $p_4 = 0, p_1 \neq 1$, $E_x$ has a maximum value of 2. In this case, the feasible region of $E_x$ is small, and thus we fix $p_1$ as 0.9 and 1

respectively, and $p_4$ as 0 and 0.1 respectively in Fig.10 to show the change of $E_x$.

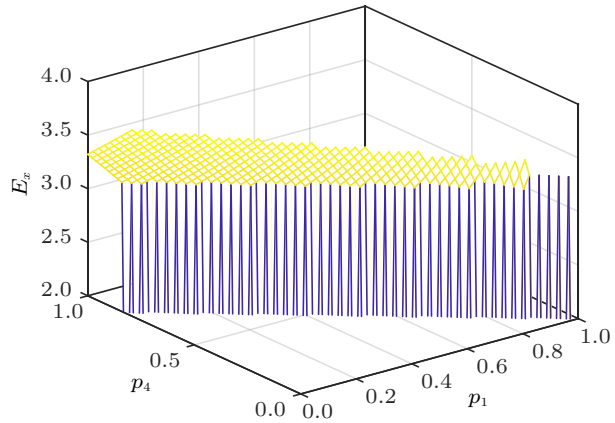



Fig. 7. Range of $E_x$ controlled by the ZD strategy when $c_x < f_x - a_x$ [14].

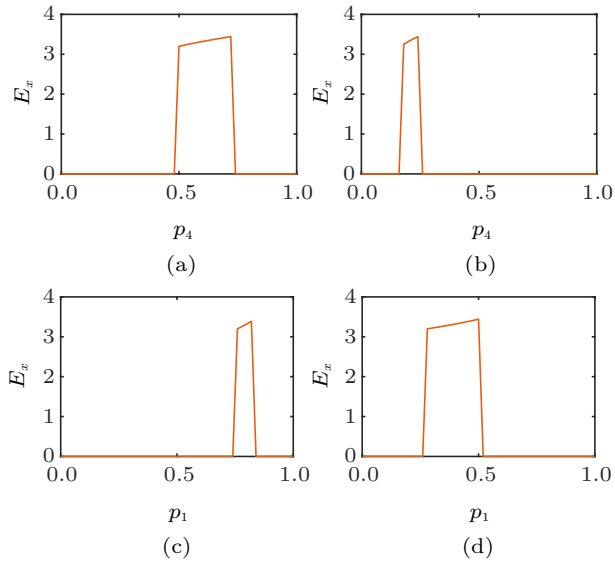



Fig.8. Effect of $p_1$ and $p_4$ on $E_x$ when $c_x < f_x - a_x$ [14]. (a) $p_1 = 0.4$. (b) $p_1 = 0.8$. (c) $p_4 = 0.2$. (d) $p_4 = 0.6$.

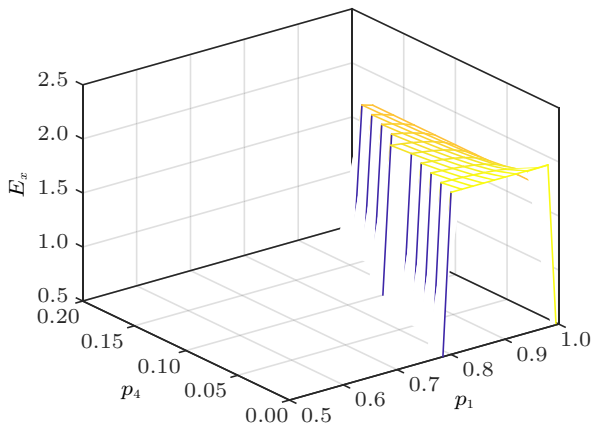



Fig. 9. Range of $E_x$ controlled by the ZD strategy when $c_x > f_x + a_x$ [14].

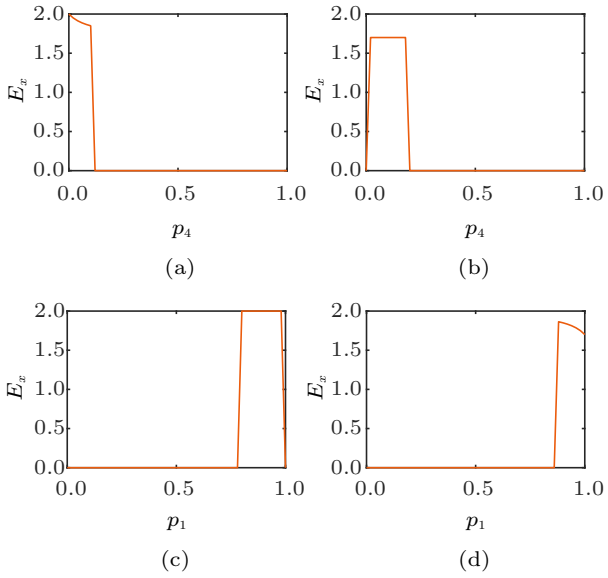



Fig.10. Effect of $p_1$ and $p_4$ on $E_x$ when $c_x > f_x + a_x$ [14]. (a) $p_1 = 0.9$. (b) $p_1 = 1$. (c) $p_4 = 0$. (d) $p_4 = 0.1$.

In the cases of other parameters discussed, including the case of $c_y < f_y - a_y$ in Theorem 3 and Theorem 4, and the case of $c_x \geqslant f_x - a_x$ in Theorem 6 and Theorem 8, $E_y$ and $E_x$ cannot be controlled in a range, and we do not show their results here.

### 6.2 ZD Strategy in Finitely Repeated Game

We carry out a set of simulations to explore the impacts of payoff parameters on $\omega$ enabling the ZD strategy in the finitely repeated game. In detail, we focus on whether $p_2$ and $p_3$ belong to [0, 1] when $\omega$ changes. When $e_x$ uses the ZD strategy to control $e_y$'s payoff, we set $f_y, a_y$ and $c_y$ as 1.5, 0.6 and 0.1, respectively. When $c_y < f_y$, we set $p_1, p_4 = 1$, and calculate $p_2$ and $p_3$ to determine the condition $\omega$ needs to satisfy. To better distinguish the eligibility of $p_2$ and $p_3$, we set them as $-0.1$ when they are not in [0, 1]. As shown in Fig.11(a), we can see that when $\omega$ is greater than 0.7, that is, $\omega \geqslant \frac{f_y - c_y}{f_y + a_y - c_y}$ and $p_2$ and $p_3$ are feasible. Similarly, when we set $c_y$ to 1.8, the condition of $f_y < c_y < f_y + a_y$ is satisfied. As shown in Fig.11(b), we can see that $\omega$ must be greater than 0.5, that is, $\omega \geqslant \frac{c_y - f_y}{a_y}$, which is the most basic condition for the ZD strategy to be effective. Figs.12(a) and 12(b) show the lower bounds of $\omega$ when $e_x$ chooses to control its own payoff, when $c_x < f_x$ and $c_x > f_x + a_x$, respectively.

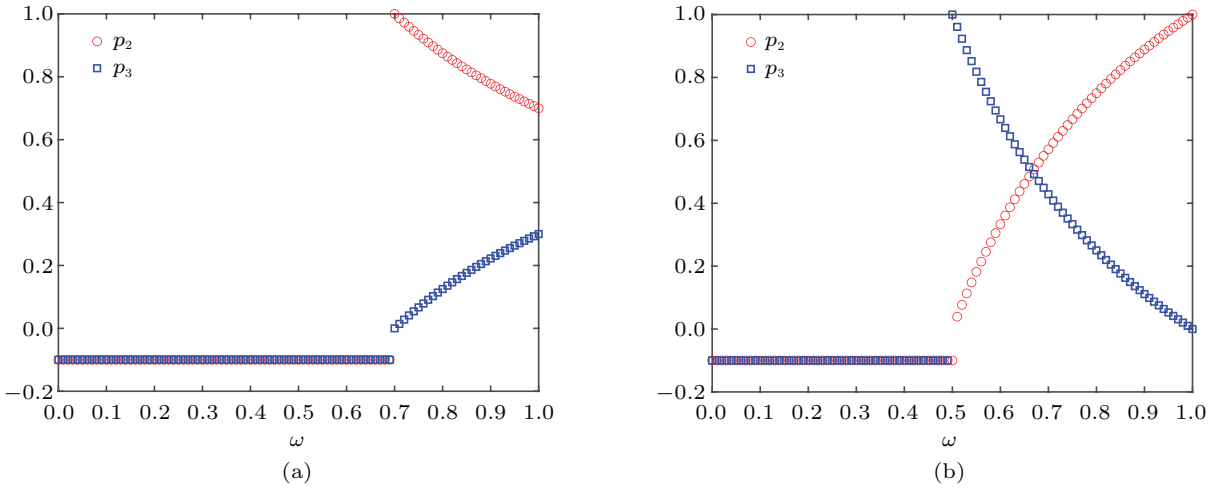



Fig.11. Impact of $\omega$ on ZD strategy controlling $E_y$ in the finitely repeated games. (a) $c_y < f_y$. (b) $f_y < c_y < f_y + a_y$.

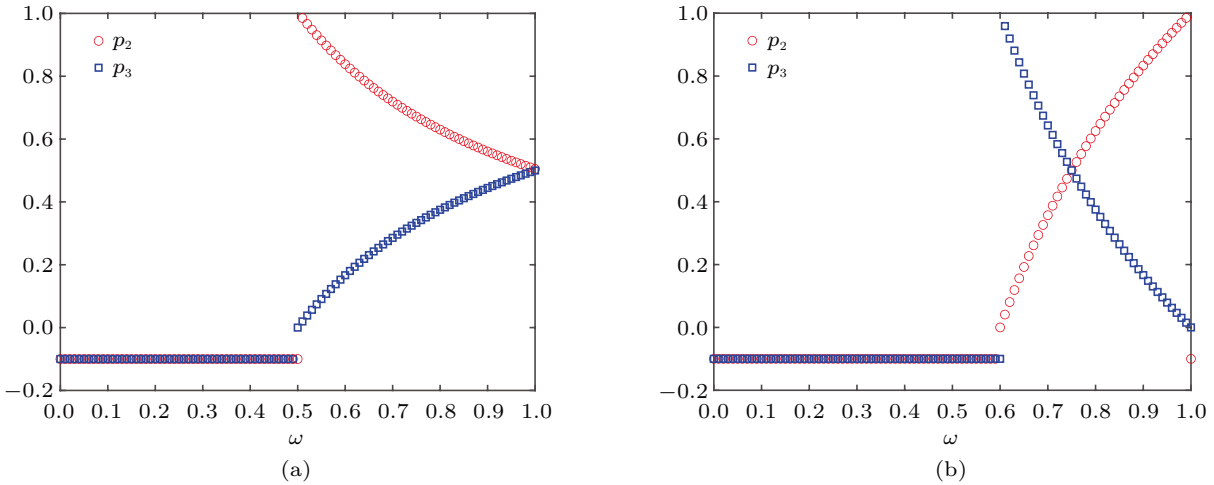



Fig.12. Impact of $\omega$ on ZD strategy controlling $E_x$ in the finitely repeated games. (a) $c_x < f_x$. (b) $c_x > f_x + a_x$.

### 6.3 Replication Dynamic of Evolutionary PCN Game

We validate the results of replication dynamic analysis by simulating the process of the evolutionary PCN game. We simulate 1 000 channels to represent the PCN with random connections between channels. Furthermore, we set $r_z$, $f_z$, and $a_z$ as 2, 1.5, and 1.2, respectively, while $c_z$ as 0.5, 2.5, 1.5 to satisfy the relationship between $c_z$ and $f_z$ in three different cases shown in Fig.13. We assume that the initial proportion of the channels choosing the cooperation strategy in the whole PCN population is 0.4 and the channels play a random pairing game with their neighbors. After each round of the game, each channel randomly selects an opponent. If the opponent's payoff is higher than its own, it learns the opponent's strategy. We verify our analysis by observing the evolution of the popular strategy in 100 consecutive rounds of the game. According to Fig. 13, when $c_x < f_x$, the channels tend to take the strategy $C$, and accordingly, $\theta = 1$ is the evolutionarily stable point. In the case of $c_x > f_x$, the channels tend to take the strategy $D$ finally, and thus $\theta = 0$ is an evolutionarily stable point. In addition, when $c_x = f_x$, the channels remain stable without changing their strategies.

### 6.4 Stability of ZD Strategy in Evolutionary PCN Game

To verify the stability of the ZD strategy in the evolutionary PCN game, we design several experiments to simulate the situations of the ZD strategy vs one other strategy and the ZD strategy vs multiple other strategies, and the results are shown in Fig. 14 and Fig. 15, respectively. We construct a PCN with 1 000 channels.

And we assume that when a ZD player, i.e., $e_{\mathrm{ZD}}$, sets the payoff of the opponent, $e_{\mathrm{ZD}}$ makes the payoff as small as possible; while when $e_{\mathrm{ZD}}$ sets its own payoff, $e_{\mathrm{ZD}}$ makes the payoff as large as possible.

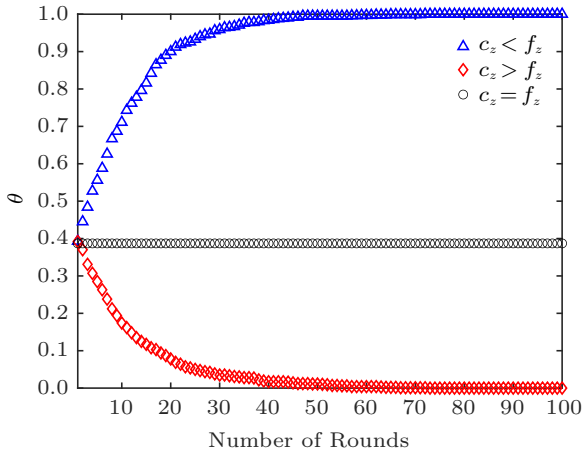



Fig.13. Evolutionarily stable points of the replication dynamic.

For the case of ZD vs one other strategy, we play 100 consecutive rounds of the game and set the initial percentage of the ZD players as 0.4. Fig.14(a) shows the change in the number of ZD players playing against four different strategies when setting the payoff range of $e_{\mathrm{OT}}$, where we set $r_{\mathrm{OT}}$, $f_{\mathrm{OT}}$, $a_{\mathrm{OT}}$, $c_{\mathrm{OT}}$ as 2, 1.5, 1.2, 1.8 and $\tilde{p}_1 = 0.99$, $\tilde{p}_4 = 0.01$, respectively. Fig.14(b) shows the convergence of the number of ZD players when $e_{\mathrm{ZD}}$ controls its own payoff, where we set $r_{\mathrm{ZD}}$, $f_{\mathrm{ZD}}$, $a_{\mathrm{ZD}}$, $c_{\mathrm{ZD}}$ as 2, 1.8, 1.2, 0.3 and $\tilde{p}_1 = 0.2$, $\tilde{p}_4 = 1$, respectively. By observing Fig.14, we can see that when $e_{\mathrm{ZD}}$ controls the opponent's payoff, if OT is ALLD, $E_{(\mathrm{ZD},\ \mathrm{OT})} < E_{(\mathrm{OT},\ \mathrm{OT})}$ is satisfied, and then ZD players will gradually disappear; while if $e_{\mathrm{OT}}$ takes the ALLC, WSLS or TFT strategy, $E_{(\mathrm{ZD},\ \mathrm{OT})} > E_{(\mathrm{OT},\ \mathrm{OT})}$ holds, and channels tend to learn the ZD strategy, which means that the ZD strategy is an ESS. This is consistent with Theorem 16. When $e_{\mathrm{ZD}}$ sets its own optimal payoff, if OT is ALLC or TFT, $e_{\mathrm{ZD}}$ will learn from $e_{\mathrm{OT}}$ gradually because $E_{(\mathrm{OT},\ \mathrm{OT})} > E_{(\mathrm{ZD},\ \mathrm{OT})}$; while if OT is ALLD or

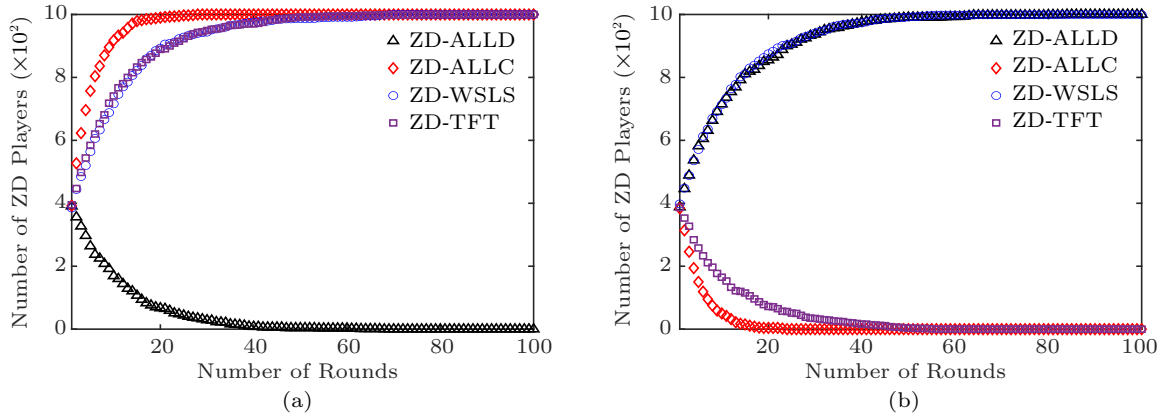



Fig.14. Evolution of the ZD players when one other strategy exists in the PCN. (a) $e_{\mathrm{ZD}}$ sets the opponent's payoff. (b) $e_{\mathrm{ZD}}$ sets its own payoff.

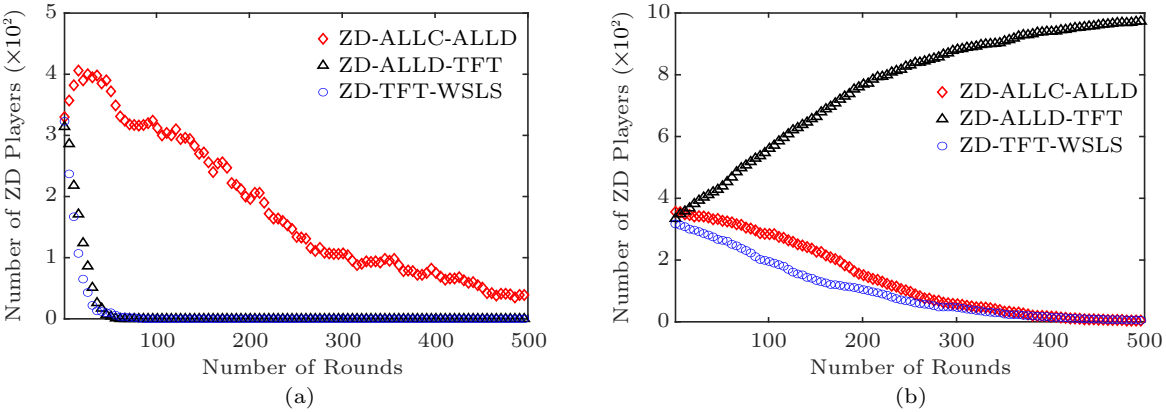



Fig.15. Evolution of the ZD players when multiple strategies coexist in the PCN. (a) $e_{\mathrm{ZD}}$ sets the opponent's payoff. (b) $e_{\mathrm{ZD}}$ sets its own payoff.

WSLS, $E_{(\mathrm{ZD},\ \mathrm{OT})} > E_{(\mathrm{OT},\ \mathrm{ZD})}$ holds, and then the ZD strategy will spread to the whole population, becoming an ESS in this case, which verifies Theorem 17.

Next, we set the initial state of the PCN population containing the ZD strategy and two other strategies to study whether the ZD strategy is an ESS for the case of ZD vs multiple other strategies. As mentioned in Subsection 5.2.2, we assume that channels adopting each strategy are evenly distributed throughout the population, and they are homogeneous with the impact factors in the payoff component under different situations, which are represented as $r, f, a, c$ respectively. We simulate 500 consecutive rounds of the game and three different scenarios with multiple strategies coexisted, including {ZD, ALLC, ALLD}, {ZD, ALLD,TFT}, and {ZD, TFT, WSLS}. When $e_{\mathrm{ZD}}$ controls the opponent's payoff, we set $r, f, a$, and $c$ to be 2, 1.5, 1.2, and 1.8, respectively, with $p_1$ and $p_4$ being 0.26 and 0.11, respectively. From Fig. 15(a), we can see that the ZD strategy is not an ESS in any of the three scenarios. ZD players gradually evolve to learn other strategies in the evolution process. In other words, $e_{\mathrm{ZD}}$ cannot help itself to get the most out of the game by controlling its opponent's payoff at a low level. Fig. 15(b) shows the evolution of the population when $e_{\mathrm{ZD}}$ chooses to control its own payoff. Here we set $r, f, a$ and $c$ to be 2, 1.5, 1.2, and 0.2, respectively, and $p_1$ and $p_4$ to be 0.9 and 0.1, respectively. When ZD coexists with ALLC and ALLD or TFT and WSLS, the number of ZD players will gradually decrease to 0, which means that in both scenarios, $e_{\mathrm{ZD}}$ cannot control their expected payoffs higher than other strategies. Thus, the ZD strategy is not an ESS in the corresponding evolutionary PCN games. While if ZD coexists with ALLD and TFT, $e_{\mathrm{ZD}}$'s payoff is higher than those of ALLD and TFT, and thus the ZD strategy gradually expands into the whole population. At this time, the ZD strategy is an ESS.

## 7 Conclusions

To investigate the characteristics of channels' transaction forwarding behaviors in the presence of malicious attacks in PCN, we proposed a game model and proceed with progressive and complementary analyses. Relying on the classical game theory and the assumption of complete rationality, we studied the Nash equilibrium of the PCN game, as well as the existence and power of the ZD strategy in both the infinitely and finitely repeated games from a micro perspective. Furthermore, we resorted to the evolutionary game theory for the case of bounded rationality to analyze the evolutionarily stable points and the evolutionary stability of the ZD strategy when playing against other strategies from a macro perspective.

Through analyzing the behavioral characteristics of channel interactions from individuals to the whole population of PCN, we can derive the following conclusions. Studying the impact of forwarding costs and attacked losses on Nash equilibrium could act as a reference for PCN users to initiate transactions. Besides, users may adopt the ZD strategy to empower themselves to gain comparative advantages. Furthermore, the management agency of the PCN can check the areas with high risks of malicious attacks according to the overall evolution status, based on which appropriate incentives can be supplied to promote widespread forwarding of transactions.

In the future, we plan to relax the assumptions of the PCN game model to adapt to more realistic scenarios for revealing further results. In addition, we propose to detect the malicious nodes and evaluate the benefits of different behaviors under attack risks accurately with the help of reinforcement learning, so as to enable users to make wise decisions for transaction forwarding.

## References

[1] Li P, Miyazaki T, Zhou W. Secure balance planning of off-blockchain payment channel networks. In *Proc. the IEEE Conference on Computer Communications*, Jul. 2020, pp.1728-1737. DOI: 10.1109/INFOCOM41043.2020.9155375.

[2] Lin S, Zhang J, Wu W. FSTR: Funds skewness aware transaction routing for payment channel networks. In *Proc. the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Jun. 29-Jul. 2, 2020, pp.464-475. DOI: 10.1109/DSN48063.2020.00060.

[3] Bagaria V K, Neu J, Tse D. Boomerang: Redundancy improves latency and throughput in payment-channel networks. In *Proc. the 24th International Conference on Financial Cryptography and Data Security*, Feb. 2020, pp.304-324. DOI: 10.1007/978-3-030-51280-4_17.

[4] Khalil R, Gervais A. Revive: Rebalancing off-blockchain payment networks. In *Proc. the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Oct. 30-Nov. 3, 2017, pp.439-453. DOI: 10.1145/3133956.3134033.

[5] Rohrer E, Malliaris J, Tschorsch F. Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks. In *Proc. the 2019 IEEE European Symposium on Security and Privacy Workshops*, Aug. 2019, pp.347-356. DOI: 10.1109/EuroSPW.2019.00045.

[6] Kappos G, Yousaf H, Piotrowska A M, Kanjalkar S, Delgado-Segura S, Miller A, Meiklejohn S. An empirical analysis of privacy in the lightning network. In *Proc.*

*the 25th International Conference on Financial Cryptography and Data Security*, Mar. 2021, pp.167-186. DOI: 10.1007/978-3-662-64322-8_8.

[7] Tang W, Wang W, Fanti G C, Oh S. Privacy-utility tradeoffs in routing cryptocurrency over payment channel networks. *Proc. ACM Meas. Anal. Comput. Syst.*, 2020, 4(2): Article No. 29. DOI: 10.1145/3392147.

[8] Banerjee P, Mazumdar S, Ruj S. Griefing-penalty: Countermeasure for griefing attack in bitcoin-compatible PCNs. arXiv:2005.09327, 2020. https://arxiv.org/abs/2005.09327, May 2022.

[9] Harris J, Zohar A. Flood & loot: A systemic attack on the lightning network. In *Proc. the 2nd ACM Conference on Advances in Financial Technologies*, Oct. 2020, pp.202-213. DOI: 10.1145/3419614.3423248.

[10] Avarikioti Z, Heimbach L, Wang Y, Wattenhofer R. Ride the lightning: The game theory of payment channels. In *Proc. the 24th International Conference on Financial Cryptography and Data Security,* Feb. 2020, pp.264-283. DOI: 10.1007/978-3-030-51280-4_15.

[11] Lange K, Rohrer E, Tschorsch F. On the impact of attachment strategies for payment channel networks. In *Proc. the IEEE International Conference on Blockchain and Cryptocurrency*, May 2021. DOI: 10.1109/ICBC51069.2021.9461104.

[12] Pickhardt R, Nowostawski M. Imbalance measure and proactive channel rebalancing algorithm for the lightning network. In *Proc. the IEEE International Conference on Blockchain and Cryptocurrency*, May 2020. DOI: 10.1109/ICBC48266.2020.9169456.

[13] Lu Z, Han R, Yu J. General congestion attack on HTLC-based payment channel networks. In *Proc. the 3rd International Conference on Blockchain Economics, Security and Protocols*, Nov. 2021, Article No. 2. DOI: 10.4230/OASIcs.Tokenomics.2021.2.

[14] Qin Y, Hu Q, Yu D, Cheng X. Malice-aware transaction forwarding in payment channel networks. In *Proc. the 18th IEEE International Conference on Mobile Ad Hoc and Smart Systems*, Oct. 2021, pp.297-305. DOI: 10.1109/MASS52906.2021.00046.

[15] Press W H, Dyson F J. Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent. *Proceedings of the National Academy of Sciences of the United States of America*, 2012, 109(26): 10409-10413. DOI: 10.1073/pnas.1206569109.

[16] Govaert A, Cao M. Zero-determinant strategies in finitely repeated $n$-player games. arXiv:1910.07858, 2019. http://arxiv.org/abs/1910.07858, Oct. 2021.

[17] Traulsen A, Nowak M A, Pacheco J M. Stochastic dynamics of invasion and fixation. *Physical Review E*, 2006, 74(1): Article No. 011909. DOI: 10.1103/PhysRevE.74.011909.

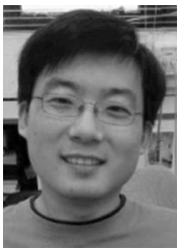
[18] Szabó G, Tőke C. Evolutionary prisoner's dilemma game on a square lattice. *Physical Review E*, 1998, 58(1): 69-73. DOI: 10.1103/PhysRevE.58.69.

[19] Taylor P D, Jonker L B. Evolutionary stable strategies and game dynamics. *Mathematical Biosciences*, 1978, 40(1/2): 145-156. DOI: 10.1016/0025-5564(78)90077-9.

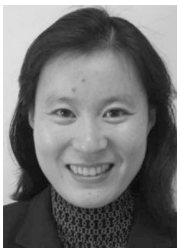
[20] Smith J M. Evolution and the Theory of Games (1st edition). Cambridge University Press, 1982.

**Yi Qin** received his B.E. degree in computer science and technology from Shandong University, Qingdao, in 2019, where he is currently pursuing his Master degree with the School of Computer Science and Technology. His research interests include blockchain and payment channel networks.

**Qin Hu** received her Ph.D. degree in computer science from the George Washington University, Washington, in 2019. She is currently an assistant professor with the Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, Indianapolis. Her research interests include wireless network, mobile security and privacy, crowdsourcing/crowdsensing, and blockchain.



**Dong-Xiao Yu** received his B.Sc. degree in information and computational science from Shandong University, Qingdao, in 2006, and his Ph.D. degree in computer science from The University of Hong Kong, Hong Kong, in 2014. He became an associate professor in the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, in 2016. He is currently a professor in the School of Computer Science and Technology, Shandong University, Qingdao. His research interests include wireless networks, distributed computing and graph algorithms.



**Xiu-Zhen Cheng** received her M.S. and Ph.D. degrees in computer science from University of Minnesota, Twin Cities, in 2000 and 2002, respectively. She was a faculty member at the Department of Computer Science, The George Washington University, Washington, from 2002–2020. Currently she is a professor of computer science at Shandong University, Qingdao. Her research focuses on blockchain computing, security and privacy, and Internet of Things. She is a fellow of IEEE.