2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS) | 978-1-6654-4935-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/MASS52906.2021.00046

Malice-Aware Transaction Forwarding in Payment Channel Networks

Yi Qin*, Qin Hu†, Dongxiao Yu*, Xiuzhen Cheng*
*School of Computer Science & Technology, Shandong University, China
†Department of Computer & Information Science, IUPUI, USA (Corresponding author)
Email: qinyi@sdu.edu.cn, qinhu@iu.edu, dxyu@sdu.edu.cn, xzcheng@sdu.edu.cn

***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 (PCN) 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 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 the PCN. The results of numerous simulation experiments verify the effectiveness of our analysis.**

***Index Terms*—Blockchain, payment channel networks, game theory.**

I. Introduction

As Bitcoin [1] 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 the 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 per second [2], which is still far below meeting the needs in practice.

To solve this problem, the concept of *payment channel* emerges recently to provide an off-chain transaction processing method, which is established between two blockchain nodes with each depositing a certain amount of funds for future instant transactions without waiting 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) [3], transactions can be completed through multiple channels even if the sender and receiver nodes are not directly connected, forming the *payment channel network (PCN)*.

Existing studies about the PCN mainly focus on *systematic* performance improvement, including routing and scheduling algorithm design to improve transaction processing speed [4], [5], channel deposit optimization to extend the availability of channels [2], [6], as well as security and privacy issues [7]–[11]. 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 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 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*. Because we study the equilibrium state and the powerful control strategy of individual players, i.e., zero determinant (ZD) strategy, in the realm of 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 PCN game, to capture the dynamic interactions between blockchain nodes, based on which extensive analysis is conducted to inspire better PCN system design.
- From the micro perspective, we study the Nash equilib-

978-1-6654-4935-9/21/$31.00 ©2021 IEEE
DOI 10.1109/MASS52906.2021.00046

rium of PCN game and explore the existence and power of the dominant ZD strategy regarding the unilateral control of expected payoffs.

- From the macro perspective, we utilize the replication dynamic equation to derive the evolutionarily stable points of the generalized evolutionary PCN game, where the evolutionary stability of ZD strategy is also investigated, providing suggestions for eliciting mutual cooperation in the PCN.
- Multiple 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 the most related work in Section II. We propose the PCN game model in Section III. And Section IV analyzes the Nash equilibrium and the applicability of the powerful ZD strategy, along with the simulation results. Section V calculates the evolutionarily stable points and the evolutionary stability of ZD strategy, which are experimentally verified as well. Section VI concludes the whole paper.

II. Related work

As representative PCNs, lightning network (LN) [3] was designed for Bitcoin, while Raiden network [12] was proposed as an off-blockchain scaling solution for Ethereum. Many existing studies have been devoted to improving the transaction speed and success rate in the PCN. Specifically, some of them study the relationship between the topological structure and the efficiency of transaction processing. The formation of the PCN topology was analyzed in [13], which showed that the centralized structure can make the PCN more efficient and stable. Lange *et al.* [14] studied the attachment strategies' influences on the PCN topology, which further affected the connectivity and benefit of participating nodes. There is also literature focusing 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 [4], which took advantage of both the static and dynamic routing to improve the success rate while decreasing latency and expense. Bagaria *et al.* designed a multi-path routing scheme named *Boomerang* [5], which could build redundant channels to eliminate the risk of participants not performing transaction agreements.

In addition, the optimization of 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 *et al.* [6] proposed the first solution of rebalancing channels' funds, and Pickhardt *et al.* [15] 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.* [2] 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.* [7] demonstrated two attacks, namely *exhausting channels* and *isolating nodes* attacks, where the detailed attacking steps were presented with quantified success rates. Lu *et al.* [16] 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 griefing attack [10] 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 et al. [11] 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.* [10] imposed a new HTLC protocol with a penalty on the adversary to mitigate griefing attack, which has not been put in practice because processing speed has to be sacrificed in this solution. Some basic defense mechanisms against the flood and loot attack was also presented in [11] 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.* [8] analyzed the potential attacks. Tang *et al.* [9] studied the trade-off between the privacy and 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 sustainability of PCN. However, there exists no research on this problem, thus driving this analytical study. Considering the potential attacks aiming at reducing channel lifetime, we model the interactions of PCN nodes and analyze both the characteristics of individuals and groups so as to provide a new perspective with some insights to enhance the system design of the PCN.

III. 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 limited deposit to assist in forwarding others' transactions. Considering that forwarding transactions is via a concrete channel which has a certain amount of deposit

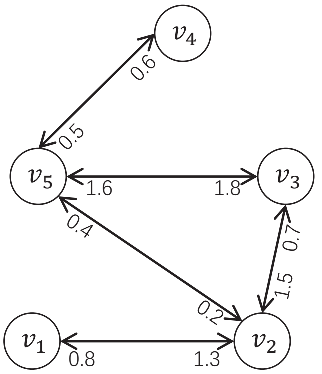


Fig. 1. An example of the PCN. The numbers at both ends of the channel represent the deposits invested by blockchain nodes, which can be used to conduct instant transactions between the connected nodes.

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 channel 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.

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:

- Natural profit (denoted as r_k): Compared with process 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 (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 (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 (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 brevity of expression, we consider two adjacent channels e_x, $e_y \in E$, which have a point of intersection node in the PCN. Both e_x and e_y can select either C or D, which respectively means that they will relay transactions for each other or not. The four strategy combinations for channels e_x and e_y generate different payoffs as follows: (i) 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; (ii) 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 can not collect transaction fees but avoid potential loss c_y, so e_x can obtain $r_x + f_x - c_x$ while e_y has payoff $r_y + a_y$; (iii) on the contrary, when e_x defects but e_y cooperates, e_x obtains $r_x + a_x$ and e_y gains $r_y + f_y - c_y$; and (iv) in the case that both e_x and e_y choose defection, they cannot meet transaction needs of each other, so they only have the basic payoffs r_x and r_y. Subsequently, channels' payoff vectors can be denoted as follows:

$$\mathbf{S}_x = (S_x^1, S_x^2, S_x^3, S_x^4)^\top = \begin{bmatrix} r_x + f_x + a_x - c_x \\ r_x + f_x - c_x \\ r_x + a_x \\ r_x \end{bmatrix}, \quad (1)$$

$$\mathbf{S}_y = (S_y^1, S_y^2, S_y^3, S_y^4)^\top = \begin{bmatrix} r_y + f_y + a_y - c_y \\ r_y + a_y \\ r_y + f_y - c_y \\ r_y \end{bmatrix}. \quad (2)$$

And the payoff matrix is shown in Fig. 2.

e_y e_x	C	D
C	$r_y + f_y + a_y - c_y$ $r_x + f_x + a_x - c_x$	$r_y + a_y$ $r_x + f_x - c_x$
D	$r_y + f_y - c_y$ $r_x + a_x$	r_y r_x

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

Definition III.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 participating in forwarding transactions or not, and get payoffs $\mathbf{S}_x$ and $\mathbf{S}_y$, 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.

IV. Microcosmic analysis of the PCN game

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

A. Nash equilibrium

Given the payoff matrix defined in the above section, we can derive the Nash equilibrium in three different parameter cases.

Theorem IV.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 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 strategy D according to $r_x + f_x - c_x > r_x$. Thus, no matter channel e_y chooses strategy C or D, e_x prefers cooperation to obtain the best 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 constitutes a Nash equilibrium. □

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

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

B. Control analysis of the 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 opponent, regardless of the opponent strategy [17]. In the PCN, since a large number of transactions need to be processed, there are long-term interactions between channels, and the result of 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 $\mathbf{p} = (p_1, p_2, p_3, p_4)$, where each component represents the probability of choosing cooperation correspondingly. And e_y's mixed strategy is denoted as $\mathbf{q} = (q_1, q_2, q_3, q_4)$ analogously.

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

$$M = \begin{bmatrix} p_1q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2q_3 & p_2(1-q_3) & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3q_2 & p_3(1-q_2) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4q_4 & p_4(1-q_4) & (1-p_4)q_4 & (1-p_4)(1-q_4) \end{bmatrix}. \quad (3)$$

Let $\mathbf{v}$ be the stable vector of the above transition matrix. According to [17], after the determinant elementary transformation and based on Cramer's rule, the dot product of $\mathbf{v}$ and any vector $\mathbf{f} = (f_1, f_2, f_3, f_4)$ is

$$\begin{aligned} \mathbf{v} \cdot \mathbf{f} &= \mathbf{D}(\mathbf{p}, \mathbf{q}, \mathbf{f}) \\ &= det \begin{bmatrix} -1 + p_1q_1 & -1 + p_1 & -1 + q_1 & f_1 \\ p_2q_3 & -1 + p_2 & q_3 & f_2 \\ p_3q_2 & p_3 & -1 + q_2 & f_3 \\ p_4q_4 & p_4 & q_4 & f_4 \end{bmatrix}. \end{aligned} \quad (4)$$

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

$$\begin{aligned} E_x &= \frac{\mathbf{v} \cdot \mathbf{S}_x}{\mathbf{v} \cdot \mathbf{1}} = \frac{\mathbf{D}(\mathbf{p}, \mathbf{q}, \mathbf{S}_x)}{\mathbf{D}(\mathbf{p}, \mathbf{q}, \mathbf{1})}, \\ E_y &= \frac{\mathbf{v} \cdot \mathbf{S}_y}{\mathbf{v} \cdot \mathbf{1}} = \frac{\mathbf{D}(\mathbf{p}, \mathbf{q}, \mathbf{S}_y)}{\mathbf{D}(\mathbf{p}, \mathbf{q}, \mathbf{1})}, \end{aligned} \quad (5)$$

where $\mathbf{1}$ is a unit vector with four elements being 1. We can find the payoffs in (5) are linearly related with their payoff vectors. Hence, when computing a linear combination of the above two expected payoffs, with α, β, and γ being constant parameters, we have

$$\begin{aligned} \alpha E_x + \beta E_y + \gamma &= \frac{\mathbf{v} \cdot (\alpha \mathbf{S}_x + \beta \mathbf{S}_y + \gamma \mathbf{1})}{\mathbf{v} \cdot \mathbf{1}} \\ &= \frac{\mathbf{D}(\mathbf{p}, \mathbf{q}, \alpha \mathbf{S}_x + \beta \mathbf{S}_y + \gamma \mathbf{1})}{D(\mathbf{p}, \mathbf{q}, \mathbf{1})}. \end{aligned} \quad (6)$$

And (6) can be calculated by substituting $\mathbf{f}$ in (4) with $\alpha \mathbf{S}_x + \beta \mathbf{S}_y + \gamma \mathbf{1}$ in the numerator and $\mathbf{1}$ in the denominator. By observing (4), we can realize that the second and 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 $\mathbf{f}$, resulting in the determinant being zero. Taking e_x as an example, if its strategy $\mathbf{p}$ makes the second column of (4) proportionate to $\alpha \mathbf{S}_x + \beta \mathbf{S}_y + \gamma \mathbf{1}$, then the numerator in (6) 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.

1) e_x unilaterally sets e_y's payoff: When $\alpha = 0$, $E_y = -\gamma/\beta$ holds, which means that e_x's strategy $\mathbf{p}$ makes the second column of (4) equal to $\beta \mathbf{S}_y + \gamma \mathbf{1}$, e_x can unilaterally set e_y's expected payoff E_y. Specifically, $\mathbf{p}$ can be solved by the following four equations,

$$\begin{cases} p_1 = 1 + \beta(r_y + f_y + a_y - c_y) + \gamma \\ p_2 = 1 + \beta(r_y + a_y) + \gamma \\ p_3 = \beta(r_y + f_y - c_y) + \gamma \\ p_4 = \beta r_y + \gamma \end{cases}. \quad (7)$$

Then p_2 and p_3 can be resolved with p_1 and p_4 to eliminate parameters β and γ,

$$\begin{aligned} p_2 &= \frac{p_1(S_y^2 - S_y^4) - (1+p_4)(S_y^2 - S_y^1)}{S_y^1 - S_y^4} \\ &= \frac{p_1 a_y - (1+p_4)(c_y - f_y)}{f_y + a_y - c_y}, \\ p_3 &= \frac{(1-p_1)(S_y^4 - S_y^3) + p_4(S_y^1 - S_y^3)}{S_y^1 - S_y^4} \\ &= \frac{(1-p_1)(c_y - f_y) + p_4 a_y}{f_y + a_y - c_y}. \end{aligned} \tag{8}$$

So e_y's expected payoff is:

$$E_y = \frac{(1-p_1)r_y + p_4(r_y + f_y + a_y - c_y)}{(1-p_1) + p_4}. \tag{9}$$

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

Theorem IV.3. *When $c_y < f_y$, we divide the situation in two cases according to the relationship between $f_y - a_y$ and c_y: (i) When $c_y > f_y - a_y$, e_x can control $E_y \in [r_y + f_y - c_y, r_y + a_y]$; (ii) if $c_y \leq f_y - a_y$, e_x cannot set E_y's range unilaterally.*

Proof. By observing (9), 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), λ cannot be negative. Under the condition of $c_y < f_y$, $p_2 \geq 0$ and $p_3 \leq 1$ are satisfied with any feasible p_1 and p_4. Subsequently, we calculate the constraints $p_2 \leq 1$ and $p_3 \geq 0$, and obtain

$$\begin{cases} \lambda \geq \frac{f_y - c_y}{a_y} \\ \lambda \leq \frac{a_y}{f_y - c_y} \end{cases}.$$

When $c_y > f_y - a_y$, λ has solutions and E_y is inversely proportional to λ. So 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 $c_y \leq f_y - a_y$ there is not a feasible solution or no more than one fixed value, therefore e_x cannot control E_y's range. □

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

Proof. According to (8), $0 \leq p_2, p_3 \leq 1$ can only be met at a single point of $\mathbf{p} = (1,1,0,0)$ in the case of $c_y > f_y + a_y$. Thus, e_x cannot control E_y's range. □

Theorem IV.5. *In the case of $f_y < c_y < f_y + a_y$, when $p_4 \in (0, \frac{a_y + f_y - c_y}{c_y - f_y + a_y})$, E_y has the minimum value of $r_y + \frac{p_4 a_y}{1+p_4}$; 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 λ is, the smaller E_y is. To derive the minimum value of E_y, we need to calculate the maximum of λ 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., $p_2 \leq 1$ and $p_3 \geq 0$. Thus, we only need to focus on the conditions of making $p_2 \geq 0$ and $p_3 \leq 1$, which leads to

$$\begin{cases} \lambda \leq \frac{a_y + f_y - c_y}{a_y p_4} - \frac{c_y - f_y}{a_y} \\ \lambda \leq \frac{a_y + f_y - c_y}{(c_y - f_y) p_4} - \frac{a_y}{c_y - f_y} \end{cases}.$$

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 λ. 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 $\lambda \geq 0$, 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 $f(p_4) \leq 0$, and thus the first inequality limits a smaller value of λ; while if $p_4 \in (\frac{a_y + f_y - c_y}{c_x - f_x + a_x}, \frac{a_y + f_y - c_y}{a_y})$, $f(p_4) \geq 0$ and we know that the second inequality becomes the limits of lambda. Given the maximum λ, 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 (9), 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 $r_y + f_y + a_y - c_y$. □

2) e_x tries to set its own 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 (4) equal to $\alpha \mathbf{S}_x + \gamma \mathbf{1}$, we can express p_2 and p_3 with p_1 and p_4 as follows

$$\begin{aligned} p_2 &= \frac{(1+p_4)(S_x^1 - S_x^2) - p_1(S_x^4 - S_x^2)}{S_x^1 - S_x^4} \\ &= \frac{(1+p_4)a_x - p_1(c_x - f_x)}{f_x + a_x - c_x}, \\ p_3 &= \frac{-(1-p_1)(S_x^3 - S_x^4) - p_4(S_x^3 - S_x^1)}{S_x^1 - S_x^4} \\ &= \frac{-(1-p_1)a_x - p_4(c_x - f_x)}{f_x + a_x - c_x}. \end{aligned} \tag{10}$$

By calculating the expressions of α and γ, we have

$$E_x = \frac{(1-p_1)r_x + p_4(r_x + f_x + a_x - c_x)}{(1-p_1) + p_4}. \tag{11}$$

Then we consider the scope limitation under different parameter cases.

Theorem IV.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: (i) When $c_x < f_x - a_x$, e_x can control $E_x \in [r_x + a_x, r_x + f_x - c_x]$; (ii) in the case of $c_x \geq f_x - a_x$, e_x cannot set the range of E_x unilaterally.*

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

The proofs of the above three theorems are similar to those of Theorems IV.3-IV.5, which are omitted here to avoid redundancy.

3) Experimental evaluation: To evaluate the control power of the ZD strategy, we conduct a series of simulations to study the impact of payoff parameters on the payoff range and report the results in Figs. 3-6. 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 IV.3, where the experimental results are shown in Fig. 3. We can see from Fig. 3(a) that E_y's range is $[2.6, 3.2]$, which satisfies the boundary range given by λ. 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. The two subgraphs in the first row of Fig. 3(b) show the change of E_y with p_4 when $p_1 = 0.4$ and $p_1 = 0.8$ respectively, and the second row indicates the effect of p_1 on E_y when $p_4 = 0.2$ and $p_4 = 0.6$ respectively.

Via adjusting c_y to 1.8, Fig. 4(a) shows the payoff range of e_y that e_x can control under the condition of $f_y < c_y < f_y + a_y$. Fig. 4(b) is with the same setting as Fig. 3(b). 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(a) shows 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, so that $c_x < f_x$ 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. 5(b) 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 Fig. 6(a), when we set c_x as 3 so that $c_x > f_x + a_x$ is satisfied as mentioned in Theorem IV.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, so we fix p_1 as 0.9 and 1, p_4 as 0 and 0.1 in Fig. 6(b) to show the change of E_x.

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

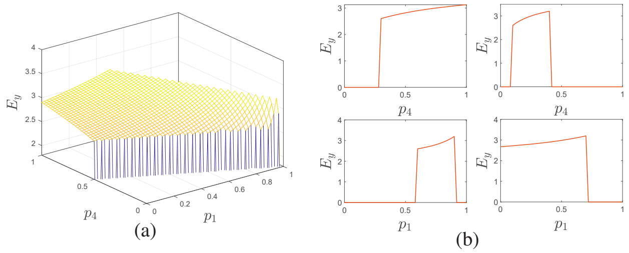


Fig. 3. Range of E_y controlled by the ZD strategy when $f_y - a_y < c_y < f_y$.

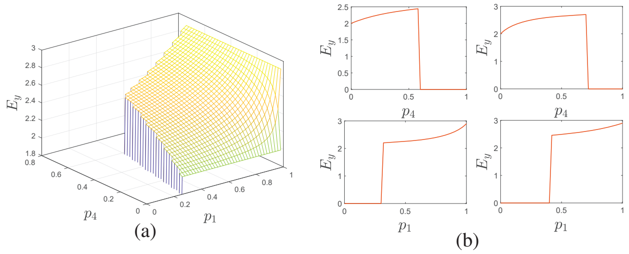


Fig. 4. Range of E_y controlled by the ZD strategy when $f_y < c_y < f_y + a_y$.

V. Macroscopic analysis of the PCN game

Generally, since there are a number of channels in the 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.

A. Replication dynamic analysis

A channel is defined as an evolutionary player if it adjusts strategy according to some optimization scheme to maximize its payoff. In this paper, we use Fermi evolutionary rule [18], [19] 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 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.

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.

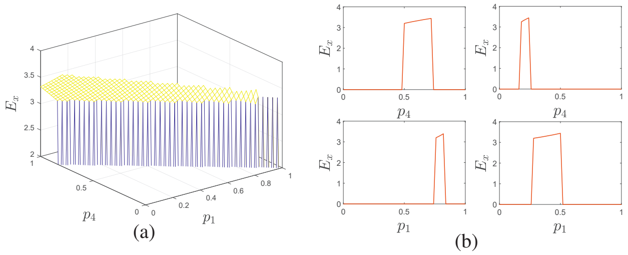


Fig. 5. Range of E_x controlled by the ZD strategy when $c_x < f_x - a_x$.

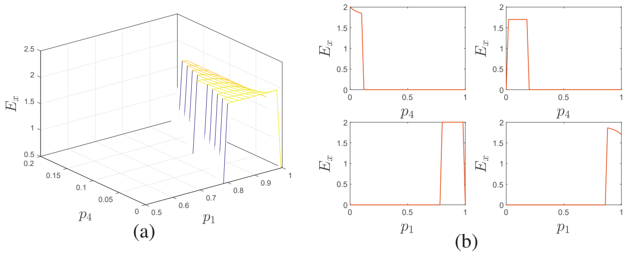


Fig. 6. Range of E_x controlled by the ZD strategy when $c_x > f_x + a_x$.

We assume that θ 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 θ, and the probability of encountering the opponent with the strategy D is $1-\theta$. We define the payoff vector of e_z as $\mathbf{S}_z = (S_z^1, S_z^2, S_z^3, S_z^4)^\top$, corresponding to the payoff of e_z when the strategy combinations of e_z and its opponent are (CC, CD, DC, DD), which can be similarly defined according to (1),

$$\mathbf{S}_z = \begin{bmatrix} r_z + f_z + a_z - c_z \\ r_z + f_z - c_z \\ r_z + a_z \\ r_z \end{bmatrix}. \tag{12}$$

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 θ 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 θ 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 [20], the growth rate of θ, denoted as $F(\theta)$, can be expressed by:

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

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 it.

Given $F(\theta^*) = 0$, we name that θ^* 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 θ deviate from θ^*, the replication dynamic can restore θ to θ^*. In mathematics, this is equivalent to that when $\theta < \theta^*$, the dynamic equation leads to $F(\theta) > 0$ in order to guarantee θ's increasing trend. On the contrary, if $\theta > \theta^*$, then $F(\theta) < 0$ has to hold to make θ decline. So the derivative of $F(\theta)$ must be less than zero in the steady state θ^*. 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

$$F'(\theta) = (1 - 2\theta)(f_z - c_z). \tag{14}$$

Theorem V.1. *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 θ 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 θ increase toward 1. □

Theorem V.2. *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), θ 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). So $\theta = 0$ 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 θ back to 0 gradually owing to the growth rate $F(\theta) < 0$. □

Theorem V.3. *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 θ is 0, so each channel in the PCN does not change its strategy, and the initial state remains stable. □

B. Evolutionary stability of the ZD strategy

In this section, we explore the evolutionarily stable strategy (ESS) of the evolutionary PCN game with the involvement of the ZD strategy. For a strategy T to be an ESS, it has to satisfy the following definition [21]:

Definition V.1 (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.

In the evolutionary PCN game involving the ZD strategy, we can assume that there are two types of strategies for channels, i.e., ZD strategy and other well-known strategies (denoted as OT). We define the channel choosing the ZD strategy as e_{ZD}, and its mixed strategy is denoted as $\tilde{\mathbf{p}} = (\tilde{p}_1, \tilde{p}_2, \tilde{p}_3, \tilde{p}_4)$. Similarly, a channel adopting OT is expressed as e_{OT}, and its strategy is denoted by $\tilde{\mathbf{q}} = (\tilde{q}_1, \tilde{q}_2, \tilde{q}_3, \tilde{q}_4)$, including the unconditional defection (ALLD), unconditional cooperation (ALLC), and win-stay-lose-shift (WSLS) strategies as examples. When e_{OT} chooses the ALLD strategy, $\tilde{\mathbf{q}} = (0,0,0,0)$; when e_{OT} chooses the ALLC strategy, $\tilde{\mathbf{q}} = (1,1,1,1)$; while if e_{OT} chooses the WSLS strategy, $\tilde{\mathbf{q}} = (1,0,0,1)$.

Next, under the several strategies introduced above, when ZD players choose to control the opponent's or their own payoffs, respectively, we can analyze its ESS feature in the evolutionary PCN game.

1) When e_{ZD} tries to set the payoff of the opponent: The payoffs of channels playing against the e_{ZD} is determined by $\tilde{p}_1$ and $\tilde{p}_4$ as shown in (9). When e_{ZD} plays the game with e_{OT}, we have e_{OT}'s payoff

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

and e_{ZD}'s payoff as

$$E(ZD,OT) = \frac{\mathbf{D}(\tilde{\mathbf{p}}, \tilde{\mathbf{q}}, \mathbf{S}_{ZD})}{\mathbf{D}(\tilde{\mathbf{p}}, \tilde{\mathbf{q}}, \mathbf{1})},$$

which is dependent on both players' strategies, and can be calculated using (4). Since the above equation can be overlength, we do not fully expand the expression here. We know that e_{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 ZD strategy, we have $E(ZD,ZD) = E(OT,ZD)$. When e_{OT} plays the game with another e_{OT}, the payoff of e_{OT} changes according to what the specific OT strategy they adopt. In detail, when OT is the ALLD strategy, $E(OT,OT) = r_{OT}$. When OT is the ALLC strategy or the WSLS strategy, $E(OT,OT) = r_{OT} + f_{OT} + a_{OT} - c_{OT}$. Here we have the payoff vectors $\mathbf{S}_{ZD}, \mathbf{S}_{OT}$ for e_{ZD} and e_{OT}, which represent their respective payoffs under different combinations of strategies.

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

Theorem V.4. *If $E(ZD,OT) > E(OT,OT)$, the ZD strategy is the ESS. If $E(ZD,OT) < E(OT,OT)$, the opposing strategy is the ESS.*

Proof. When e_{ZD} chooses to set the opponent's payoff, both e_{OT} and e_{ZD} who play with e_{ZD} have the payoff controlled by e_{ZD}, so the payoffs $E(ZD,ZD)$ and $E(OT,ZD)$ are equivalent. We determine the existence of ESS by using the second condition in Definition V.1. In our case, only when $E(ZD,OT) > E(OT,OT)$, ZD is the ESS and vice versa. □

2) When e_{ZD} tries to set its own payoff: We denote e_{ZD}'s payoff from (11) as

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

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

$$E(OT,ZD) = \frac{\mathbf{D}(\tilde{\mathbf{p}}, \tilde{\mathbf{q}}, \mathbf{S}_{OT})}{\mathbf{D}(\tilde{\mathbf{p}}, \tilde{\mathbf{q}}, \mathbf{1})}.$$

The payoff of e_{OT} against another e_{OT} is $E(OT,OT)$, whose 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 V.5. *If $E(ZD,OT) > E(OT,ZD)$, or $E(ZD,OT) = E(OT,ZD)$ and $E(ZD,OT) > E(OT,OT)$, the ZD strategy is the ESS. If $E(OT,OT) > E(ZD,OT)$, or $E(OT,OT) = E(ZD,OT)$ and $E(OT,ZD) > E(ZD,ZD)$, the opposing strategy is the ESS.*

The procedure of the proof is similar to that of Theorem V.4, so we omit it for brevity.

C. Experimental evaluation

We validate the results of replication dynamic analysis by simulating the process of the evolutionary PCN game. We simulate 1000 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. We assume that the initial proportion of C players in the whole PCN population is 0.4 and channels play a random pairing game with its neighbors. After each round of 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 game. According to Fig. 7, 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 $c_x > f_x$, channels tend to take the strategy D finally, so $\theta = 0$ is an evolutionarily stable point. In addition, when $c_x = f_x$, channels remain stable without changing their strategies.

In Fig. 8, we study whether the ZD strategy is an ESS in the evolutionary PCN game. We assume that when a ZD player, i.e., e_{ZD}, sets the payoff of opponent, e_{ZD} makes the payoff as small as possible; when e_{ZD} sets its own payoff, e_{ZD} makes the payoff as large as possible. Similarly, we set the initial percentage of the ZD players to 0.4. Fig. 8(a) shows the change in the number of ZD players playing against three other strategies when setting the payoff range of e_{OT}, where we set r_{OT}, f_{OT}, a_{OT}, c_{OT} as 2, 1.5, 1.2, 1.8 and $\tilde{p}_1 = 0.99, \tilde{p}_4 = 0.01$. Fig. 8(b) shows the convergence of the ZD players when e_{ZD} controls its own payoff, where we set

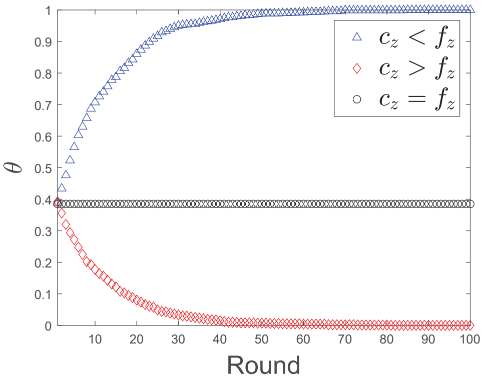
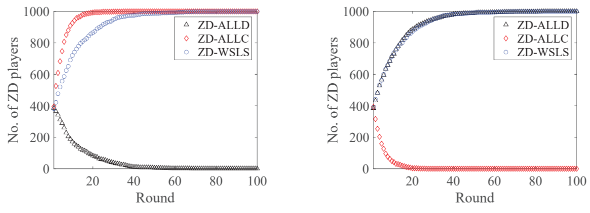


Fig. 7. Evolutionarily stable points of the replication dynamic.

r_{ZD}, f_{ZD}, a_{ZD}, c_{ZD} as 2, 1.8, 1.2, 0.3 and $\tilde{p}_1 = 0.2, \tilde{p}_4 = 1$. When e_{ZD} controls the opponent's payoff, if OT is ALLD, $E(ZD, OT) < E(OT, OT)$ is satisfied, then ZD players will gradually disappear; while if e_{OT} takes the ALLC or WSLS strategy, $E(ZD, OT) > E(OT, OT)$ holds, channels tend to learn the ZD strategy, which means that the ZD strategy is an ESS. This is consistent with Theorem V.4. When e_{ZD} sets its own optimal payoff, if OT is ALLC, e_{ZD} will learn from e_{OT} gradually because $E(OT, OT) > E(ZD, OT)$; while if OT is ALLD or WSLS, $E(ZD, OT) > E(OT, ZD)$ holds, then ZD strategy will spread to the whole population, becoming an ESS in this case, which verifies Theorem V.5.



(a) e_{ZD} sets the opponent's payoff (b) e_{ZD} sets its own payoff

Fig. 8. The evolution of the ZD players.

VI. Conclusion

In this paper, we propose a game model for the PCN as well as conduct progressive and complementary analyses based on this model to study the behavior characteristics of channels under the scenario with malicious attacks. Based on the classic game theory with the complete rationality assumption, we study the two-player game from a microcosmic perspective, which reveals the impacts of parameters and strategy choices on the individual characteristics. Furthermore, taking advantage of the evolutionary game theory with the limited rationality of players, we study the group behavior from a macroscopic perspective, which serves as a foundation for portraying the evolution of the PCN. Through analyzing the behavioral characteristics of channel interactions from individuals to the whole population of PCN, we can provide guidance for individuals' optimization and eliciting mutual cooperation in the PCN. Extensive simulation experiments verify the effectiveness of our analysis.

Acknowledgment

This work was supported in part by the National Key Research and Development Program of China under grant 2019YFB2102600, the National Natural Science Foundation of China (NSFC) under grants 61832012 and 61971269, and the US NSF under grant CNS-2105004.

References

[1] S. Nakamoto., "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.

[2] P. Li, T. Miyazaki, and W. Zhou, "Secure balance planning of off-blockchain payment channel networks," in *IEEE Conference on Computer Communications*, 2020, pp. 1728–1737.

[3] T. D. Joseph Poon, "The bitcoin lightning network: Scalable off-chain instant payments," http://lightning.network/lightning-network-paper.pdf.

[4] S. Lin, J. Zhang, and W. Wu, "FSTR: funds skewness aware transaction routing for payment channel networks," in *IEEE/IFIP International Conference on Dependable Systems and Networks*, 2020, pp. 464–475.

[5] V. K. Bagaria, J. Neu, and D. Tse, "Boomerang: Redundancy improves latency and throughput in payment-channel networks," in *International Conference of Financial Cryptography and Data Security*, 2020, pp. 304–324.

[6] R. Khalil and A. Gervais, "Revive: Rebalancing off-blockchain payment networks," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 823, 2017.

[7] E. Rohrer, J. Malliaris, and F. Tschorsch, "Discharged payment channels: Quantifying the lightning network's resilience to topology-based attacks," in *IEEE European Symposium on Security and Privacy Workshops*, 2019, pp. 347–356.

[8] G. Kappos, H. Yousaf, A. M. Piotrowska, S. Kanjalkar, S. Delgado-Segura, A. Miller, and S. Meiklejohn, "An empirical analysis of privacy in the lightning network," *CoRR*, vol. abs/2003.12470, 2020.

[9] W. Tang, W. Wang, G. C. Fanti, and S. Oh, "Privacy-utility tradeoffs in routing cryptocurrency over payment channel networks," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 4, no. 2, pp. 29:1–29:39, 2020.

[10] P. Banerjee, S. Mazumdar, and S. Ruj, "Griefing-penalty: Countermeasure for griefing attack in bitcoin-compatible pcns," *CoRR*, vol. abs/2005.09327, 2020.

[11] J. Harris and A. Zohar, "Flood & loot: A systemic attack on the lightning network," in *ACM Conference on Advances in Financial Technologies*, 2020, pp. 202–213.

[12] "The raiden network," https://raiden.network/.

[13] Z. Avarikioti, L. Heimbach, Y. Wang, and R. Wattenhofer, "Ride the lightning: The game theory of payment channels," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, J. Bonneau and N. Heninger, Eds., vol. 12059, 2020, pp. 264–283.

[14] K. Lange, E. Rohrer, and F. Tschorsch, "On the impact of attachment strategies for payment channel networks," *CoRR*, vol. abs/2102.09256, 2021.

[15] R. Pickhardt and M. Nowostawski, "Imbalance measure and proactive channel rebalancing algorithm for the lightning network," *CoRR*, vol. abs/1912.09555, 2019.

[16] Z. Lu, R. Han, and J. Yu, "Bank run payment channel networks," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 456, 2020.

[17] W. H. Press and F. J. Dyson, "Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 109, no. 26, p. 10409—10413, June 2012.

[18] A. Traulsen, M. A. Nowak, and J. M. Pacheco, "Stochastic dynamics of invasion and fixation," *Physical Review E*, vol. 74, no. 1, p. 011909, 2006.

[19] G. Szabó and C. Tőke, "Evolutionary prisoner's dilemma game on a square lattice," *Physical Review E*, vol. 58, no. 1, p. 69, 1998.

[20] P. D. Taylor and L. B. Jonker, "Evolutionary stable strategies and game dynamics," *Mathematical Biosciences*, vol. 40, no. 1, pp. 145–156, 1978.

[21] J. M. Smith, *Evolution and the Theory of Games*. Cambridge University Press, 1982.