A Letters Journal Exploring the Frontiers of Physics

February 2014

EPL, **105** (2014) 48003
doi: 10.1209/0295-5075/105/48003

www.epljournal.org

Robustness of cooperation on scale-free networks in the evolutionary prisoner's dilemma game

Pei Li and Haibin Duan[(a)]

State Key Laboratory of Virtual Reality Technology and Systems, Beihang University - Beijing 100191, China and Science and Technology on Aircraft Control Laboratory, School of Automation Science and Electrical Engineering, Beihang University - Beijing 100191, China

received 8 November 2013; accepted in final form 17 February 2014
published online 7 March 2014

PACS 89.75.Fb – Structures and organization in complex systems
PACS 02.50.Le – Decision theory and game theory
PACS 89.65.-s – Social and economic systems

Abstract – We have studied the robustness of cooperation on scale-free (SF) networks in the prisoner's dilemma game under different attack strategies. Although previous works have demonstrated that increasing heterogeneity constitutes higher levels of cooperation, we elaborated on this subject further by introducing a parameter α to take into consideration two significant aspects during an attack. We have shown that it is possible to precisely control the cooperation level on SF networks to be robust ($\alpha \ll 0$) or fragile ($\alpha \geq 0$). Moreover, we studied the evolution on SF networks against a different attack strategy, taking over the nodes instead of simply removing the nodes, to address the functional importance of a node. Notably, the network structure remains the same during the evolutionary process under this attack strategy, which allows us to investigate the correlation between the functional significance and survival of cooperation. Our results highlight the underlying mechanism of cooperation behavior on SF networks and have several important implications for public health and networks security.

Introduction. – Cooperation plays a crucial role in the emergence of fascinating patterns and organizational structures both in biological and social systems [1–4]. Mutually cooperative behaviors are ubiquitous throughout the history of evolution [5,6], from the formation of multicellular organisms to the cooperation behavior in animal groups to enhance their survival capability, despite the fact that selfish strategies of the individual may produce better payoffs under the assumption that the participators are rational. Researchers from a broad range of disciplines, from sociology to biology, ecology, economics, mathematics, and physics, have shown great interests in exploring this paradoxical outcome by various means [7–10]. It is conventional to formulate this problem in the framework of the evolutionary game theory [11–14], the dynamic of which is defined by the interaction among players in the group. Since the seminal paper that reveals the network reciprocity by Nowak and May [15], a large body of literature has attached great importance to the evolutionary games on graphs [10,16,17]. Notably, it was fascinating to discover that structured populations provide an optimal playground for the emergence and sustainability of cooperation. Additionally, accumulative evidence shows that heterogeneous network generally favors the emergence of cooperation over homogeneous network and increasing heterogeneity constitutes higher levels of cooperation [7–9,18,19], irrespective of the dilemma adopted as a metaphor for cooperation.

Remarkably, recent extensive numerical works have shown that survival of cooperation has been greatly enhanced in games on scale-free (SF) networks with respect to that on lattice networks [20–22]. As a kind of representative complex network whose degree distribution follows a power law and exhibits high heterogeneity, SF networks have received substantial attention and quickly rise to prominence in physical and other disciplines [23,24]. Great efforts have been made concerning the robustness of cooperation in the evolutionary game on SF networks [25–27], from the dependence on initial conditions and variations in the parametrization [25], to influence of the degree of heterogeneity [26], tolerance to intentional or random removal of nodes [27] and impact of link deletions [28]. More importantly, the underlying mechanism that constitutes the strong robustness of cooperation on SF networks has been elaborated, which may lead to a deeper understanding of

(a) E-mail: hbduan@buaa.edu.cn

the complicated evolutionary dynamic and the sustainability of cooperation. It has been demonstrated that cooperation on SF networks is extremely robust against random deletion of nodes, but declines quickly upon attack in environments prone to defection. That is, the SF network is robust with random errors, but fragile under selective attacks, in other words, robustness and fragility coexist [27,29].

While inspirational insight for future research in this field has been provided, the underlying cause associated with the robust yet fragile character of SF networks in the evolution of cooperation is still not fully understood. Indeed, it is essential to enhance the robustness in some social, biological and technological networks while robustness may be troublesome when it comes to halting an epidemic [30]. Here we aim to elaborate on this subject further by quantifying the attack intensity using the degree of nodes k, providing an alternative way to delicately control the network to be more robust or fragile. Moreover, we have noticed that attack strategies are not limited to the removal of nodes or edges and it is often the case that the important nodes are taken over [31], such as transmission of viral infections, spread of epidemic and popularity of the internet worm [31]. In particular, the network structure remains the same during the evolutionary process under this attack strategy, allowing us to investigate the correlation between the functional significance and survival of cooperation. Consequently, we further studied the evolution on SF networks against a different attack strategy, taking over the nodes instead of simply removing them.

Evolutionary dynamics. – We consider an evolutionary prisoner's dilemma game with cooperation and defection as the two competing strategies. The prisoner's dilemma is characterized by the following payoffs: mutual cooperation yields the reward R, mutual defection leads to punishment P, the mixed choice gives the cooperator the sucker's payoff S and the defector the temptation T. Following the standard practice, the payoffs are the temptation of defection $T = b$, $R = 1$ for mutual cooperation, and $S = P = 0$ for a cooperator encountering a defector and mutual defection, respectively. In this setup, it guarantees the essential dilemma that whatever the opponent adopts, defection leads to a higher (or at least equal) payoff, thus a dilemma [8,13].

Experiments are conducted on the SF network with average connectivity $\bar{k} = 4$ comprising $N = 3000$ players. The interaction topology we adopt here is generated by means of growth and preferential attachment, which is first proposed by Barabási and Albert [27]. It is worth mentioning that varying the network size does not qualitatively change the reported results and the main conclusions. Initially, each player on the SF network is designated either as a cooperator (C) or defector (D) with equal probability. Evolution of the two strategies occurs in accordance with the Monte Carlo simulation procedure comprising the following three elementary steps. First, a randomly selected player x acquires its accumulative payoff p_x by playing the game with all its k_x neighbors. Next, one randomly chosen member from all the k_x neighbors of x, denoted by y, also acquires its payoff p_y by playing the game with all its k_y neighbors on the SF network. Lastly then, if their payoffs satisfy $p_x < p_y$, player x adopts the strategy s_y of player y with the probability following the Fermi strategy adoption function [32]

$$W\left(s_x \rightarrow s_y\right) = \frac{1}{1 + \exp\left[\left(p_x - p_y\right)/K\right]}, \quad (1)$$

where K determines the amplitude of noise and its inverse $(1/K)$ denotes the intensity of selection (comprehensive investigation in the effect of K can refer to [12]). In this work, K is set to 0.1, following the conventional setup [12, 33], which strongly prefers adopting strategies from more successful players.

Note that all the players update their strategies according to this rule in an asynchronous manner. Each individual is selected once on average during a full Monte Carlo step, which consists of repeating the above elementary steps 3000 times, in accordance with the number of participators. The stationary fraction of cooperators was determined within 20000 full Monte Carlo steps after sufficiently long transients were discarded. To eliminate the effects of heavily fluctuating outputs due to the inherent stochastic ingredients in the evolution process, final results shown below were averaged over 20 realizations for each set of parameter values. Besides, the final fraction of cooperators was the averaged value of the last 500 Monte Carlo steps to warrant appropriate accuracy and ensure observable quantities.

Simulation and analysis. – Motivated by the ubiquitous and pervasive phenomenon in nature and society, such as the appearance of risks, malfunctioning of some components [27,34], and transmission of virus, we introduce some destructive agents on the network, represented by the deletion of nodes. Here we investigate the evolution of cooperation in dependence on the number of deleted nodes δ under two entirely different removal strategies, random deletion and intentional deletion. To test the error tolerance of cooperation evolution on SF networks, δ nodes are selected for removal with equal probability to simulate the malfunctioning of nodes (random deletion). However, a rational agent that attempts to deliberately damage a network will preferentially target the most connected nodes rather than eliminate the nodes randomly, that is, intentional attack. To simulate intentional attacks, the most connected node within the network is selected and removed. Then the node has the largest degree at the time of removal is deleted successively, until δ nodes have been removed. Note that the disconnected nodes are also removed because the completely isolated players contribute nothing to the evolution of cooperation since they have no games to participate in.

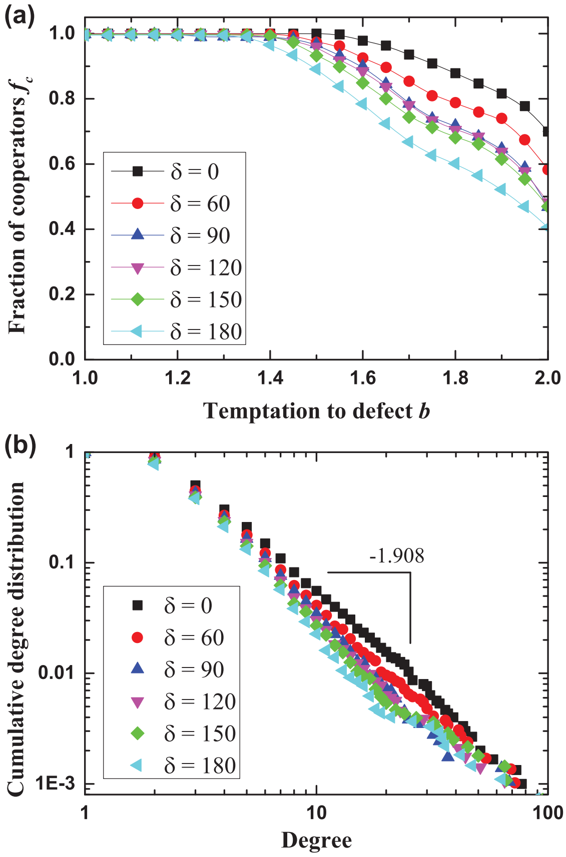

Fig. 1: (Colour on-line) Results for different values of δ under error conditions (random removal of nodes). (a) Fraction of cooperators in dependence on the temptation to defect b. Lines connecting the symbols are just to guide the eye. (b) Cumulative degree distributions.

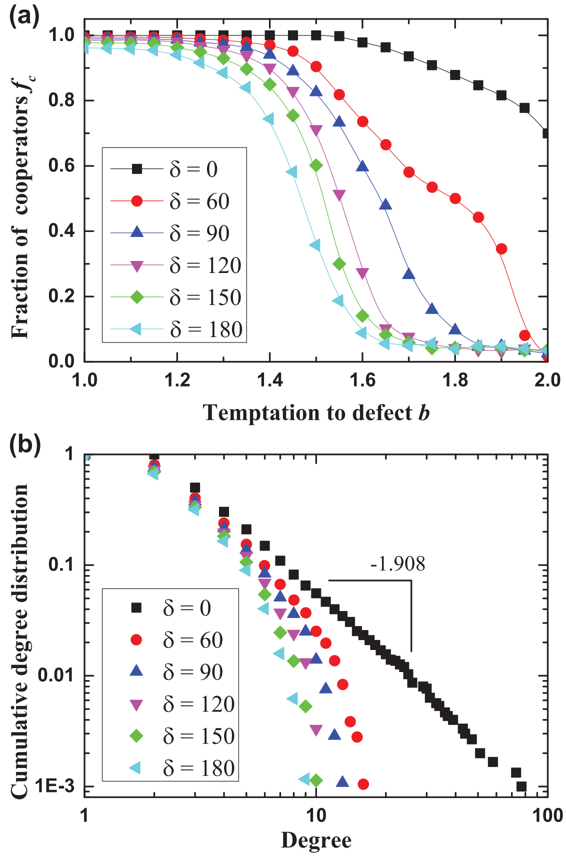

Fig. 2: (Colour on-line) Results for different values of δ under intentional attack (removal of nodes with the highest degree). (a) Fraction of cooperators in dependence on the temptation to defect b. Lines connecting the symbols are just to guide the eye. (b) Cumulative degree distributions.

To reveal the robust yet fragile nature of games on SF networks, the average level of cooperation f_c in dependence on b for different values of deleted nodes δ on SF networks due to error and attack, are depicted in fig. 1(a) and fig. 2(a), respectively. Results presented in fig. 1(a) demonstrated that the network almost holds the same level of cooperation at a fixed value of b with different values of δ although the fraction of cooperators dropped slightly under random removal of nodes when compared with the original network, which suggests that random deletions make little difference to cooperation. Apparently, these facts verify the robustness of cooperation on SF networks against random errors, in accordance with previous studies [29,35]. Conversely, density of cooperators declines dramatically under intentional removal of highly connected nodes, as is shown in fig. 2(a). Furthermore, fascinating facts can be deduced from the results, that is, the higher the δ, the smaller the possibility that cooperators are able to survive when competing against defectors. To this end, it can be argued that the robust network is turned into a vulnerable one by removing some highly connected nodes and is easy to be occupied by defectors.

Degree heterogeneity may provide a possible explanation for the impact of error and attack on the evolution of cooperation [5–7]. Here we quantify the heterogeneity by calculating the cumulative degree distribution $D(k)$ of newly yielded networks under these two different circumstances [7], which is defined for a network with N nodes as $\sum_{i=k}^{N-1} N_i/N$, where N_i denotes the number of nodes with i edges, as is illustrated in fig. 1(b) and fig. 2(b). The fit gives that the slope of the cumulative degree distribution for the original network is equal to -1.908 on a double logarithmic graph (see the black symbols in fig. 1(b)). Again we could find that random removal of nodes (error) contributes little to changes of network structure for different values of δ, that is, the effect of random deletions on network structure is negligible. On the other hand, targeted attack on the nodes with high connectivity (attack) leads to less heterogeneity. Note that the change of degree heterogeneity becomes slight as the value of δ increases (see the green and cyan symbols in fig. 1(b)) since the network is disintegrated into more isolated components with large value of δ. It is natural to link different densities of cooperators resulting from error and attack to the heterogeneity changes as they are closely resembling in the trend. Therefore, it seems reasonable to argue that the resulting degree heterogeneity difference is responsibile for both the supreme tolerance of cooperation on error, and its fragility on attack for high temptations to defect.

As the most efficient attack strategy, intentional attack on the most connected node is not always available in many realistic cases since it requires adequate information about the network. Accordingly, the highest-degree node can be removed only with a certain probability under an intentional attack. We also noticed that targeted attacks on nodes with higher connectivity are much more lethal for cooperation on SF networks than random error, which suggests that the vulnerability of a node is closely related to its degree. Considering the above two facts, the probability that a node becomes inactive during an attack can be analyzed quantitatively using the following function [34]:

$$P(k_i) = \frac{k_i^\alpha}{\sum_{i=1}^{N} k_i^\alpha}, \quad -\infty < \alpha < \infty. \tag{2}$$

The parameter α takes into consideration two facts, intrinsic network vulnerability (α_1) and external knowledge of the network (α_2), which can be represented by $\alpha = \alpha_1 + \alpha_2$. Apparently, nodes with lower degree are more vulnerable when $\alpha < 0$, while nodes with larger k are more vulnerable when $\alpha > 0$.

In order to gain more insight into how the inherent network property and defense strategy would affect the robustness of cooperation evolution on SF networks, we study the fraction of cooperators with 180 nodes deleted when the attack is undertaken with different values of α. As expected, nodes with higher degree are more likely to be deleted and the network becomes more vulnerable as α increases, evidenced by the relatively lower level of cooperation in fig. 3(a). We should note that the network shares almost the same level of cooperation when $\alpha = 2$ and $\alpha = 3$, which is somewhat surprising at first glance. However, the results with $\alpha = 2$ and $\alpha = 3$ can be explained perfectly by the following theoretical analysis. The probability w that one of the n highest connected nodes in a network with N nodes is destroyed under an attack quantified by eq. (2) can be formulated as

$$w = \frac{\int_{k_n}^{k_{\max}} W(k)\, P(k)\, \mathrm{d}k}{\int_{m}^{k_{\max}} W(k)\, P(k)\, \mathrm{d}k}, \tag{3}$$

where $W(k) = k^{-\lambda}$ is the power-law degree distribution of SF networks, whereby λ is typically in the range $2 < \lambda < 3$. Besides, m denotes the minimum degree and $k_{\max} \sim N^{1/(\lambda-1)}$ the maximum degree of the nodes in the network. k_n is the minimum degree of the nodes that belongs to the n highest connected nodes. Substituting $W(k)$ and $P(k)$ into eq. (3), we can express w as a function of α and λ for $N \gg n \gg 1$:

$$w = \frac{1 - n^{(\lambda-1-\alpha)/(\lambda-1)} m^{\alpha+1-\lambda}}{1 - N^{(\lambda-1-\alpha)/(\lambda-1)} m^{\alpha+1-\lambda}}. \tag{4}$$

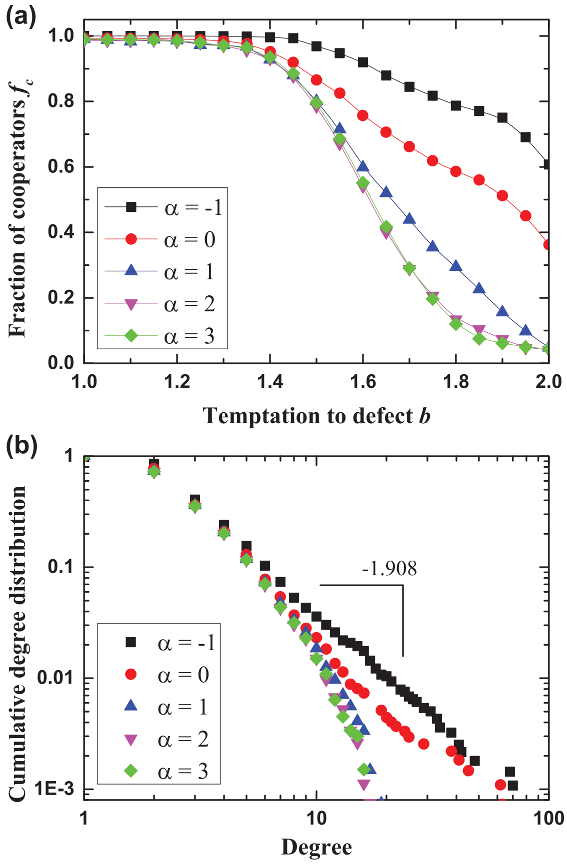

Fig. 3: (Colour on-line) Results for different values of α under removal strategy. (a) Fraction of cooperators in dependence on the temptation to defect b. Lines connecting the symbols are just to guide the eye. (b) Cumulative degree distributions.

Intuitively, the larger the value of α for a specific network (fixed λ), the higher the probability w that one of the n highest nodes becomes inactive. Notably, w approximates 1 when $\alpha > \lambda - 1$ and the increment of α makes little difference to the value of w. More specifically, w shares almost the same value when $\alpha = 2$ and $\alpha = 3$ since $\lambda = 2.908$ in our setting, which is consistent with the results depicted in fig. 3(a). It is also instructive to find that the cases $\alpha = 0$ and $\alpha = \infty$ are corresponding to random attack and intentional attack, respectively.

As further evidence supporting the facts that heterogeneity plays an important role in facilitating high levels of cooperation, cumulative degree distributions resulting from different α are shown in fig. 3(b). This figure exhibits rather similar characteristics compared with the evolution results in fig. 3(a), which confirms the hypothesis that the robust nature in SF network is closely associated with the heterogeneous structure of it to some extent. By identifying the cumulative degree distribution of the network under attack with different values of α, we found that nodes with higher degree indeed contribute a lot to the maintenance of the network structure and this kind of nodes are essential for the robustness of the network. Taking the parameter α into consideration, the cooperation on SF networks could be fragile ($\alpha \geq 0$) or robust ($\alpha \ll 0$), providing new perspectives on how to control the robustness of this kind of network. For instance, we can take actions to enhance the protection of the significant nodes (reducing α_1), thereby lowering the probability that a node becomes inactive during an attack. While in other cases, we can attempt to have a better understanding of the network when we want to destroy it, leading to a higher α. In this case, the network can be expected to be vulnerable.

Inspired by the ubiquitous phenomenon that nodes in real-world networks are often taken over rather than simply removed [31], we stress this problem further by studying evolution on SF networks against a different attack strategy, taking over the nodes with defectors, for error and attack, respectively. Surprisingly, cooperation under this attack strategy is much weaker than that under deletion, as it can be seen in figs. 4(a) and (b). Under the taking-over strategy, the density of cooperators drops monotonously from 0.8 to less than 0.4 when $\delta = 60$ (fig. 4(a)), while in the same case the network under the deletion attack strategy maintains a higher cooperation level (fig. 1(a)), as the temptation to defect b increases from 1 to 2. When one refers to the results presented in fig. 4(a) under error conditions, it follows that when $\delta = 60$, the network keeps a relatively high level of cooperation and as δ increases, the number of cooperators goes down. Nevertheless, the level of cooperation has declined dramatically when compared with the original network, which suggests the less robustness of cooperation under this taking-over strategy.

The results presented in fig. 4(b) under intentional attack confirm that the taking-over strategy is lethal to the network. As we can see from the plot, the fraction of defectors on the network declines soon to 0 under intentional attack, irrespective of the number of nodes δ to be invaded. Evidently, only about 0.2 cooperators survive when $b = 1$ and the network is taken over by defectors when $b = 1.2$ as $\delta = 180$, indicating the destructive power of this attack strategy. The entire network is occupied by the defectors as b increases for different δ, which means the system undergoes a transition in which the cooperation-facilitative effect deteriorates. For large b, cooperators are dominated by defectors, which is an unfavorable scenario for the sustainability of cooperation. In this situation, defectors occupying the hubs exhibit an evolutionary advantage with their cooperative competitors as they get higher payoffs. At this point, we can conclude that attack type of taking-over enables the defectors to grow into impact clusters even though only a small proportion of nodes are inactive in the initial state.

Since we have demonstrated the significance of the parameter α engaged in the evolutionary game, it is also important to inspect the game dynamics for different α in the taking-over case. Figure 4(c) shows the cooperation density f_c in dependence on b for different values of α, whereby it can be observed that nodes with less neighbors are more likely to be occupied for small value of α ($\alpha = -1$), thus only a small proportion of players are affected by this attack, which ensures the cooperator domination state. In this case, the non-essential nodes are taken over with higher probability for small α. When approaching larger α, hubs are occupied by defectors, which warrants that defectors outperform cooperators and give rise to compact defector clusters. It is inspiring to find

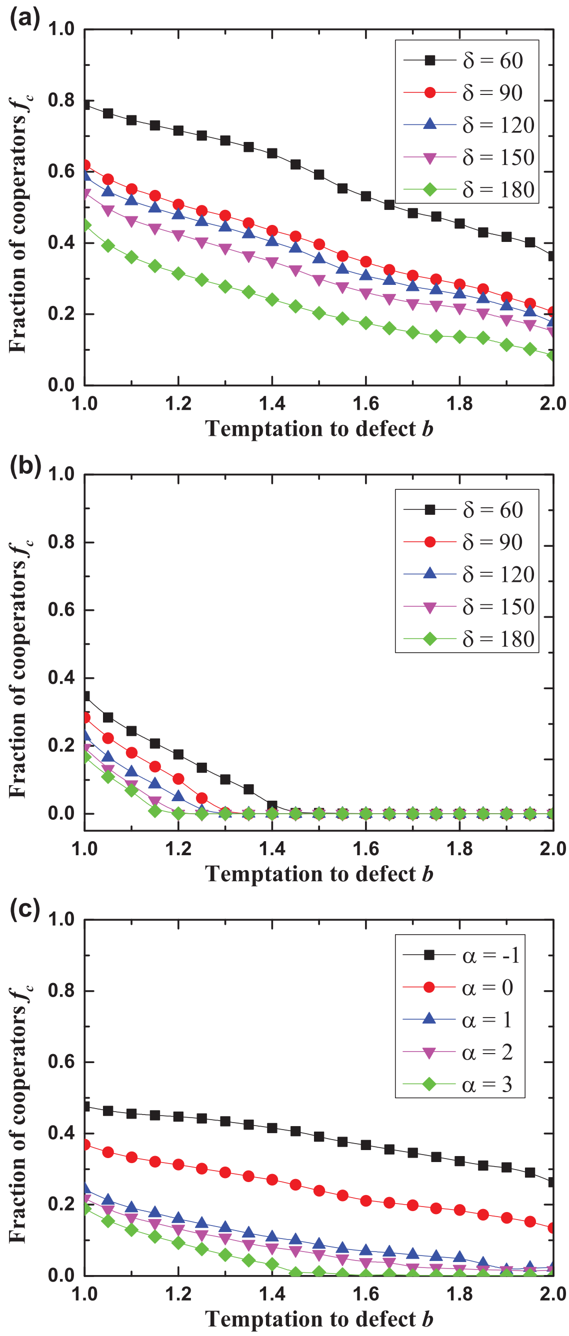

Fig. 4: (Colour on-line) Fraction of cooperators in dependence on the temptation to defect b under the taking-over strategies. Lines connecting the symbols are just to guide the eye. (a) Under error (randomly take over nodes) for different values of δ. (b) Under intentional attack (take over nodes with the highest degree) for different values of δ. (c) Under the taking-over strategy quantized by different values of α.

that although some highly connected nodes are intrinsically vulnerable, an exquisite defense strategy is still able to guarantee $\alpha < 0$. Remarkably, the results depicted above provide a potential explanation for the functional significance of the hubs since the structure remains the same during the evolutionary process. The heterogeneous effect for enhancing cooperation is counteracted by the nodes occupied by the defectors.

Conclusions. – In summary, we have studied the robustness of cooperation on scale-free networks in the prisoner's dilemma game under different attack strategies. Although it has been demonstrated that increasing heterogeneity constitutes higher levels of cooperation, we attempt to elaborate on this subject further by introducing a parameter α to quantify the intrinsic network vulnerability and external knowledge of the network during attack. We have shown that it is possible to precisely control the cooperation level on SF networks to be robust ($\alpha \ll 0$) or fragile ($\alpha \geq 0$), which is especially useful since robustness is of great significance in some social, biological and technological networks while it may be troublesome when it comes to halting an epidemic.

Previous works concerning the robustness of cooperation mainly focus on the structural significance, in which the importance of a node is often measured by the magnitude of changes in the network structure, such as heterogeneity, by the removal of a node. To address this problem, we studied the evolution on SF networks against a different attack strategy, taking over the nodes instead of simply removing the nodes. It is of great importance that the network structure remains the same during the evolutionary process under this attack strategy, which allows us to investigate the correlation between the functional significance and survival of cooperation. To this end, both the structural significance and the functional significance in maintaining high levels of cooperation in the prisoner's dilemma game are studied in our work. We hope that our study concerning the robustness of cooperation on SF networks could provide implications for public health and computer network security and be inspirational for future efforts aimed in this direction.

* * *

This work was partially supported by Natural Science Foundation of China (NSFC) (Grant Nos. 61333004 and 61273054), National Key Basic Research Program of China (973 Project) (Grant Nos. 2014CB046401 and 2013CB035503), Top-Notch Young Talents Program of China, and National Magnetic Confinement Fusion Research Program of China (Grant No. 2012GB102006).

REFERENCES

[1] Axelrod R. and Hamilton W. D., *Science*, **211** (1981) 1390.
[2] Milinski M., *Nature*, **325** (1987) 433.
[3] Fehr E. and Fischbacher U., *Nature*, **425** (2003) 785.
[4] Ohtsuki H., Hauert C., Lieberman E. and Nowak M. A., *Nature*, **441** (2006) 502.
[5] Duan H.-B., Deng Y.-M., Wang X.-H. and Xu C.-F., *PLoS ONE*, **8** (2013) e72035.
[6] Luo Q.-N. and Duan H.-B., *Sci. China Technol. Sci.*, **56** (2013) 2473.
[7] Santos F. C., Pacheco J. M. and Lenaerts T., *Proc. Natl. Acad. Sci. U.S.A.*, **103** (2006) 3490.
[8] Perc M. and Szolnoki A., *Phys. Rev. E*, **77** (2008) 011904.
[9] Perc M. and Wang Z., *PLoS ONE*, **5** (2010) e15117.
[10] Moreira J. A., Pacheco J. M. and Santos F. C., *Sci. Rep.*, **3** (2013) 152.
[11] Wang Z., Szolnoki A. and Perc M., *Sci. Rep.*, **3** (2013) 1183.
[12] Szabó G., Vukov J. and Szolnoki A., *Phys. Rev. E*, **72** (2005) 047107.
[13] Szolnoki A., Perc M. and Danku Z., *EPL*, **84** (2008) 50007.
[14] Gómez-Gardeñes J., Gracia-Lázaro C., Floría L. M. and Moreno Y., *Phys. Rev. E*, **86** (2012) 056113.
[15] Nowak M. A. and May R. M., *Nature*, **359** (1992) 826.
[16] Szabó G. and Fáth G., *Phys. Rep.*, **446** (2007) 97.
[17] Wang Z., Szolnoki A. and Perc M., *EPL*, **97** (2012) 48001.
[18] Santos F. C., Santos M. D. and Pacheco J. M., *Nature*, **454** (2008) 213.
[19] Santos F. C., Pinheiro F. L., Lenaerts T. and Pacheco J. M., *J. Theor. Biol.*, **299** (2012) 88.
[20] Poncela J., Gómez-Gardeñes J., Floría L. M., Moreno Y. and Sánchez A., *EPL*, **88** (2009) 38003.
[21] Liu R.-R., Rong Z., Jia C.-X. and Wang B.-H., *EPL*, **91** (2010) 20002.
[22] Yang H.-X., Wu Z.-X. and Du W.-B., *EPL*, **99** (2012) 10006.
[23] Albert R. and Barabási A.-L., *Rev. Mod. Phys.*, **74** (2002) 47.
[24] Boccaletti S., Latora V., Moreno Y., Chavez M. and Hwang D.-U., *Phys. Rep.*, **424** (2006) 175.
[25] Poncela J., Gómez-Gardeñes J., Floría L. and Moreno Y., *New J. Phys.*, **9** (2007) 184.
[26] Yang Z., Zhou T., Hui P. M. and Ke J.-H., *PLoS ONE*, **7** (2012) e49663.
[27] Perc M., *New J. Phys.*, **11** (2009) 033027.
[28] Jiang L.-L., Perc M., Wang W.-X., Lai Y.-C. and Wang B.-H., *EPL*, **93** (2011) 40001.
[29] Doyle J. C., Alderson D. L., Li L., Low S., Roughan M., Shalunov S., Tanaka R. and Willinger W., *Proc. Natl. Acad. Sci. U.S.A.*, **102** (2005) 14497.
[30] Moreira A. A., Andrade J. S. jr, Herrmann H. J. and Indekeu J. O., *Phys. Rev. Lett.*, **102** (2009) 018701.
[31] Ueno T. and Masuda N., *J. Theor. Biol.*, **254** (2008) 655.
[32] Szabó G. and Töke C., *Phys. Rev. E*, **58** (1998) 69.
[33] Du W.-B., Cao X.-B., Zhao L. and Hu M.-B., *Physica A*, **388** (2009) 4509.
[34] Gallos L. K., Cohen R., Argyrakis P., Bunde A. and Havlin S., *Phys. Rev. Lett.*, **94** (2005) 188701.
[35] He X. and Zhang J., *PLoS Genet.*, **2** (2006) e88.