Measuring the Hazard of Malicious Nodes in Information Diffusion over Social Networks

Hangjing Zhang*, Yuejiang Li†, Yang Hu*, Yan Chen* and H. Vicky Zhao†
* School of Info. and Comm. Engr., Univ. of Electronic Science and Technology of China, P. R. China
† Dept. of Automation and Inst. for Artificial Intelligence, Tsinghua Univ.
Beijing National Research Center for Info. Science and Technology (BNRist), P.R. China

***Abstract*—Social networks have become prevalent in our daily life: people learn, discuss, and spread different kinds of information through social networks every day. While bringing a lot of convenience, the prevalence of social networks creates the security challenge. The information released and/or spread by malicious nodes can be wrong, misleading or even virus, which may lead to bad influences and severe consequences. Therefore, understanding the information diffusion process and the hazard impact of malicious nodes' behaviors to the information diffusion is critical. In this paper, we utilize the evolutionary game theory to measure the hazard influence of malicious nodes to the information diffusion over social networks, by investigating the information diffusion dynamics and evolutionary stable strategies. Finally, simulations are conducted to validate the theoretic analysis and illustrate the impact of the malicious nodes.**

I. INTRODUCTION

With the popularization of network, information dissemination over Internet becomes easy and flexible with low cost and high speed. Nevertheless, it creates the security challenge at the same time. Especially over social network, when the information is wrong or misleading, people are apt to be misguided and then may be the disseminator. Furthermore, if the content of information is detrimental, virus for instance, it could incur severe consequences and incalculable damages. Therefore, it is of crucial importance to model information diffusion process over social networks with malicious nodes, to figure out how information sent by malicious nodes propagates among social networks, and to estimate the impact to the whole network.

Frameworks to model the information diffusion can be generally divided into two categories. The first category focuses on macro exploration, usually adopting machine learning or data mining techniques to predict the dynamics or properties of network. Based on historical information given by early measures, [1]–[6] investigated the characterization of the dynamics of information propagation in social media applications. Hao et al. proposed a matrix factorization based predictive model and used gradient descent to optimize objective function [7]. The authors in [8] studied diffusion of preference on social networks by a rank-learning based data-driven approach. The second category models the information diffusion from the microscopic aspect, i.e., emphasizing more on the decisions and motivation of individuals. Based on the correlation, Lee et al. in [9] proposed a probabilistic model to estimate the probability of a user's adoption using the naive Bayes classifier. The authors in [10]–[12] proposed information diffusion models to study the spreading by defining different objective functions for each user and then solving the corresponding minimization or maximization problem.

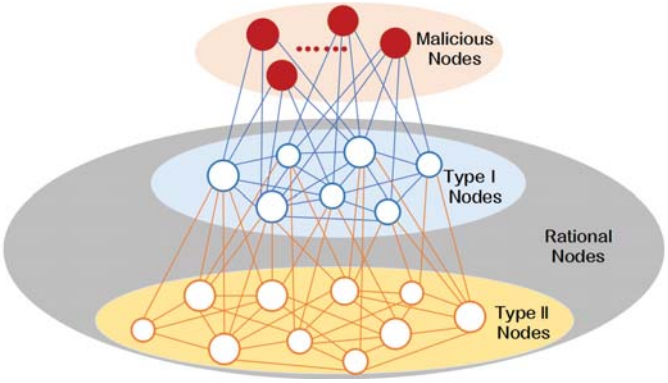


Fig. 1. An illustration of the social network with type I nodes, type II nodes, and malicious nodes.

Evolutionary game theory (EGT) has also been utilized to study the information diffusion, which provides an alternative mechanism to understand the microscopic interactions among nodes. The authors in [13]–[16] proposed an evolutionary game theoretic framework to model the dynamic information diffusion process among nodes in social networks. However none of these pay attention to social networks with malicious users, whose behaviors are very different from rational nodes. In this paper, we propose to utilize graphical EGT to analyze the hazard impact of malicious nodes to the information diffusion over social networks. We divide the rational nodes into two types: type I nodes which are directly connected to the malicious nodes and type II nodes which are not, and analyze them respectively, to derive the evolution dynamics and the corresponding evolutionary stable strategies (ESSs). Finally, simulation results are conducted to validate the theoretic analysis and show that the existence of malicious nodes can increase the proportion of rational nodes adopting the strategy of forwarding information.

II. EVOLUTIONARY GAME FORMULATION

Generally, a social network can be modeled as a graph, where users are represented as nodes and connections are represented as edges. As shown in Fig.1, in our information

diffusion model, a social network graph consists of $(M+N)$ rational nodes, who adopt a specific strategy updating rule, and f_{max} malicious nodes, who use a fixed malicious strategy. We assume that rational nodes update their strategies in accordance to the DB updating rule: a random player is chosen to abandon his/her current strategy (Death process), then the chosen player adopts one of his/her neighbors' strategies with the probability being proportional to their fitness (Birth process). Other updating rules such as birth-death (BD) and imitation (IM) can be analyzed similarly [17]. The objectives of rational nodes are to maximize their fitness, while malicious nodes are different from rational ones, which are often paid to spread harmful information.

Due to the existence of malicious nodes, rational nodes could be further categorized into two types: M type I nodes which are directed connected to the malicious nodes, and N type II nodes which are not directly connected to the malicious nodes. We assume that each rational node has k rational neighbors, whose distribution is $\lambda(k)$, i.e., when randomly choosing one rational node, the probability of the chosen node with k rational neighbors is $\lambda(k)$. Notice that for type I rational nodes, apart from k rational neighbors, there are extra f malicious nodes as neighbors with probability distribution $\mu(f)$. In other words, every type I rational node has $(k+f)$ neighbors while type II rational node only has k neighbors.

In this paper, we assume that when a user receives one piece of information, he/she only has two choices: forwarding denoted as S_f, and not forwarding as S_n. For a rational user, he/she chooses the strategy based on the DB updating rule, while for a malicious user, he could only adopt S_f mimicking the scenarios that hackers deliberately spread computer virus or some people are employed to spread misleading information. In our daily life, when we are first exposed to some new information, we generally cannot distinguish the reputation of the disseminators over social network, and thus always treat them equally. In such a case, no matter which type the rational user is, the payoff matrix is the same since there is no information about whether the neighbor is malicious or which type the neighbor is. Then payoff matrix can be written as follows

$$\begin{array}{c} \\ S_f \\ S_n \end{array} \begin{array}{c} \begin{array}{cc} S_f & S_n \end{array} \\ \begin{pmatrix} u_{ff} & u_{fn} \\ u_{nf} & u_{nn} \end{pmatrix} \end{array} \tag{1}$$

where u_{ff}, u_{fn}, u_{nn} denotes the payoffs for two nodes when they both adopt S_f, one adopts S_f while the other adopts S_n, and they both adopt S_n, respectively. Apparently, $u_{fn} = u_{nf}$, i.e., the payoff matrix is symmetric. In graphical evolutionary game theory [18], [19], the player strategy update rule directly depends on the fitness of the players, i.e.:

$$\pi = (1-\alpha)B + \alpha U \tag{2}$$

where B is the baseline fitness, and U is the payoff which consists of u_{ij} defined before. α is the selection strength satisfying $0 < \alpha < 1$ and controlling the proportion of current payoff to the whole fitness.

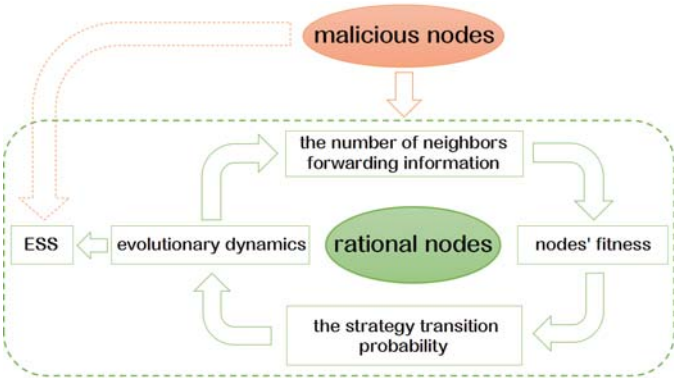


Fig. 2. System model: an illustration of how malicious nodes influence the evolution dynamics and ESS.

In the literature [14]–[16], α is assumed to be very small, representing the limit of weak selection. We would also adopt this assumption in remaining part.

To evaluate the hazard of malicious nodes on the whole network, we define p_f the percentage of rational nodes with S_f among all rational nodes, and p_{fi} the proportion of type i (I or II) nodes adopting S_f among all type i nodes. We call p_f, p_{f1}, p_{f2} as population state. Correspondingly, $\dot{p_f}, \dot{p_{f1}}, \dot{p_{f2}}$ are population dynamics. Since rational nodes' neighbors are different, we analyze type I nodes and type II nodes respectively in the following.

III. Theoretic Analysis

In this section, we study the evolutionary dynamics and ESS to figure out the effects of malicious users. The procedures of the theoretic analysis are shown in Fig. 2.

A. Evolutionary Dynamics of Type I Nodes

According to (2), the fitness for the type I node could be derived as

$$\pi_{f1} = 1 - \alpha + \alpha\left[k_f u_{ff} + (k+f-k_f)u_{fn}\right], \tag{3}$$

and

$$\pi_{n1} = 1 - \alpha + \alpha\left[k_f u_{fn} + (k+f-k_f)u_{nn}\right], \tag{4}$$

where k_f is the number of nodes with strategy S_f among all neighbors, π_{f1} and π_{n1} are the fitness of nodes adopting S_f and S_n, respectively.

With the DB strategy updating rule, when a node is randomly chosen to change the current strategy, he/she adopts one of his neighbors' strategies with probability proportional to the fitness of that strategy. The probabilities transited to strategy S_f and strategy S_n are denoted as P_{to_f1} and P_{to_n1}, respectively, and can be derived as

$$P_{to\_f1} = \frac{k_f \pi_{f1}}{k_f \pi_{f1} + (k+f-k_f)\pi_{n1}}, \tag{5}$$

and

$$P_{to\_n1} = \frac{(k+f-k_f)\pi_{n1}}{k_f \pi_{f1} + (k+f-k_f)\pi_{n1}}. \tag{6}$$

In each round, one of $(M+N)$ nodes would be selected to update randomly. The probability of the chosen node being type I node with S_f is $p_{f1}M/(M+N)$ and the probability of the chosen node being type I node with S_n is $(1-p_{f1})M/(M+N)$. When the selected node is a type I node adopting S_f, it may deviate from S_f to S_n, which leads to the percentage of users adopting S_f among type I nodes, also known as p_{f1}, decreasing by $1/M$ with probability

$$Prob\left(\Delta p_{f1}=-\frac{1}{M}\right)=\frac{M}{M+N}p_{f1}P_{to\_n1}. \quad (7)$$

On the contrary, when the selected one is type I node adopting S_n, the population state p_{f1} would increase by $1/M$ if the center node changes his strategy from S_n to S_f with probability

$$Prob\left(\Delta p_{f1}=\frac{1}{M}\right)=\frac{M}{M+N}(1-p_{f1})P_{to\_f1}. \quad (8)$$

Then combining two scenarios above, the evolutionary dynamics of the proportion of type I nodes adopting strategy S_f can be derived as follows

$$\begin{aligned}\dot{p}_{f1}&=\mathbf{E}\left[Prob\left(\Delta p_{f1}=-\frac{1}{M}\right)\left(-\frac{1}{M}\right)+Prob\left(\Delta p_{f1}=\frac{1}{M}\right)\frac{1}{M}\right]\\&=\frac{1}{M+N}\mathbf{E}\left[\frac{k_f}{k+f}-p_{f1}+\alpha\cdot\frac{-\Phi k_f^3+(\Phi-\Phi_n)(k+f)k_f^2+(k+f)^2\Phi_n k_f}{(k+f)^2}\right],\end{aligned} \quad (9)$$

where $\Phi=u_{ff}-2u_{fn}+u_{nn}$ and $\Phi_n=u_{fn}-u_{nn}$.

During the simplification in (9), we use Maclaurin series $\frac{a+b\alpha}{c+d\alpha}=\frac{a}{c}+\frac{bc-ad}{c^2}\alpha+O(\alpha)$ to transfer fraction to polynomial, which facilitates the computation of expectation. Because α is a very small value due to weak selection, the higher order term $O(\alpha)$ can be omitted in (9).

In each round, the center node is randomly selected and their neighbors' strategies are not correlative. Therefore, to connect k_f with p_{f1} and fully understand the dynamics of type I nodes, we model the strategies of rational neighbors as a Bernoulli sequence. We regard the probability of encountering a rational neighbor adopting S_f as p_f under the assumption that the network is large enough. It should be emphasized that p_f here is the proportion among rational nodes, without counting malicious nodes whose strategies are always S_f. However, when one of center node's neighbors is adopting S_f, it can be either rational node or malicious node. In such a case, the probability for one of type I node's neighbors adopting S_f is $p_{total\_f}=\frac{M_f+N_f+f_{max}}{M+N+f_{max}}\approx p_f+\frac{f_{max}}{M+N+f_{max}}$, where M_f and N_f are the number of nodes adopting S_f among type I nodes and type II nodes, respectively. The approximation is reasonable under the assumption that f_{max} is small compared with $M+N$, i.e., the number of malicious nodes is smaller than the number of rational nodes.

Among all of the center node's neighbors, there are k_f nodes with S_f and $(k+f-k_f)$ nodes with S_n, and the probability of such a configuration is

$$\theta(k,k_f)=\binom{k}{k_f}\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right)^{k_f}\left(1-p_f-\frac{f_{max}}{M+N+f_{max}}\right)^{k+f-k_f}. \quad (10)$$

With (10), the moments of k_f can be obtained as follows

$$\begin{aligned}\mathbf{E}(k_f)&=k\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right),\\\mathbf{E}(k_f^2)&=(k^2-k)\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right)^2+k\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right),\\\mathbf{E}(k_f^3)&=k(k-1)(k-2)\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right)^3+3k(k-1)\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right)^2+k\left(p_f+\frac{f_{max}}{M+N+f_{max}}\right).\end{aligned} \quad (11)$$

Combining (9) with (11), the evolution dynamics of type I nodes could be derived as (14). From (14), we observe that $\dot{p}_{f1}$ depends on both p_{f1} and p_f, which means that nodes are affected not only by those with the same type, but also all other nodes including malicious nodes.

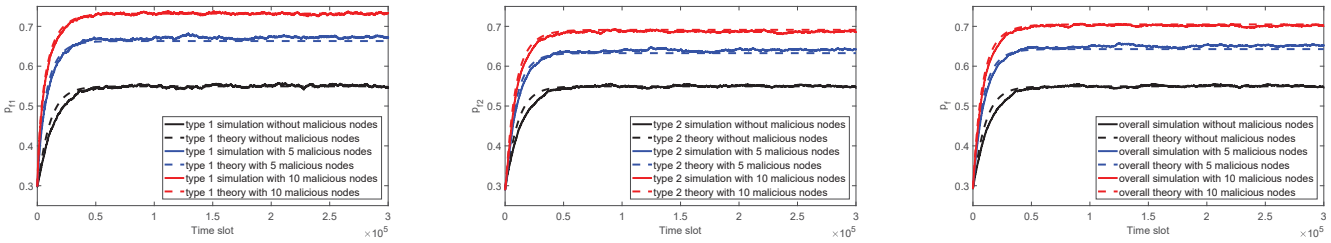
B. Evolutionary Dynamics of Type II Nodes

For type II nodes, the difference from type I nodes is that they are not directly connected with malicious nodes, which means that the number of neighbors of type II nodes is k rather than $(k+f)$. In such a case, the fitness can be written as

$$\pi_{f2}=1-\alpha+\alpha\left[k_f u_{ff}+(k-k_f)u_{fn}\right], \quad (15)$$

$$\begin{aligned}\dot{p}_{f1}=\sum_k\sum_{f=0}^{f_{max}}&\left\{\frac{f(1-p_{f1})+k(p_{total\_f}-p_{f1})}{(M+N)(k+f)}+\frac{\alpha k(1-p_{total\_f})}{(M+N)(k+f)^2}\right.\\&\left.\left[(k-1)(k-2)\Phi p_{total\_f}^2+[(2f+1)(k-1)\Phi+(k+f)(k-1)\Phi_n]p_{total\_f}+f^2\Phi+f(k+f)\Phi_n\right]\right\}\mu(f)\lambda(k).\end{aligned} \quad (14)$$

$$\dot{p}_{f2}=\sum_k\left\{\frac{p_{total\_f}-p_{f2}}{M+N}+\frac{\alpha(k-1)p_{total\_f}(1-p_{total\_f})}{(M+N)k}\left[(k-2)\Phi p_{total\_f}+\Phi+k\Phi_n\right]\right\}\lambda(k). \quad (19)$$



(a) The proportion of type I nodes adopting S_f. (b) The proportion of type II nodes adopting S_f. (c) The proportion of all rational nodes adopting S_f.

Fig. 3. Simulation results of the evolution dynamics under the payoff matrix PM1: $u_{ff} = 0.3$, $u_{fn} = 0.8$, $u_{nn} = 0.2$

and

$$\pi_{n2} = 1 - \alpha + \alpha \left[k_f u_{fn} + (k - k_f) u_{nn} \right]. \tag{16}$$

Similarly, the probabilities transited to strategy S_f and strategy S_n are denoted as P_{to_f2} and P_{to_n2}, respectively, and can be derived as

$$P_{to\_f2} = \frac{k_f \pi_{f2}}{k_f \pi_{f2} + (k - k_f)\pi_{n2}}, \tag{17}$$

and

$$P_{to\_n2} = \frac{(k - k_f)\pi_{n2}}{k_f \pi_{f2} + (k - k_f)\pi_{n2}}. \tag{18}$$

According to [16], the evolution dynamics of the proportion of type II nodes with S_f , i.e., $\dot{p}_{f2}$, can be written as (19). We can observe that due to the absence of malicious nodes, the dynamics would be more precise, which simplifies the solution to ESS as shown in the next subsection.

C. ESS Analysis

To obtain the evolution dynamics of p_f, we combine (14) and (19) with weights proportional to the number of type I nodes and II nodes as follows

$$\begin{aligned}
\dot{p}_f &= \frac{M}{M+N}\dot{p}_{f1} + \frac{N}{M+N}\dot{p}_{f2} \\
&= \sum_k \frac{\lambda(k)}{(M+N)^2}(1 - p_{total_f})(a p_{total_f}^2 + b p_{total_f} + c) \\
&= \sum_k \frac{\lambda(k)}{(M+N)^2}\left(1 - p_f - \frac{f_{max}}{M+N+f_{max}}\right) \times \\
&\left[a p_f^2 + \left(\frac{2a f_{max}}{M+N+f_{max}} + b\right) p_f + a\left(\frac{f_{max}}{M+N+f_{max}}\right)^2 + \frac{b f_{max}}{M+N+f_{max}} + c \right],
\end{aligned} \tag{20}$$

where

$$\begin{aligned}
a &= \alpha(k-1)(k-2)\left(\sum_{f=0}^{f_{max}} \frac{kM\mu(f)\Phi}{(k+f)^2} + \frac{N\Phi}{k}\right), \\
b &= \alpha(k-1)\left[\sum_{f=0}^{f_{max}} \frac{\mu(f)kM}{k+f}\left(\frac{(2f+1)\Phi}{k+f} + \Phi_n\right) + \frac{N\Phi}{k} + N\Phi_n\right], \\
c &= \sum_{f=0}^{f_{max}} \frac{M\mu(f)}{k+f}\left(\frac{\alpha k f^2}{k+f}\Phi + \alpha k f \Phi_n + f\right).
\end{aligned} \tag{21}$$

Note that the a, b, c in (21) are coefficients of the quadratic equation in (20). From (20), we could find that by setting $\dot{p_f} = 0$, there are three possible ESSs, i.e., $p_f^* = 1 - \frac{f_{max}}{M+N+f_{max}}$ and two roots to the quadratic equation $a p_f^{*2} + \left(\frac{2a f_{max}}{M+N+f_{max}} + b\right) p_f^* + a\left(\frac{f_{max}}{M+N+f_{max}}\right)^2 + \frac{b f_{max}}{M+N+f_{max}} + c = 0$, which both lie between 0 and 1.

Compared with the results in [16] that ESS would be 0 under the condition $u_{nn} > u_{fn}$, in (20) none of the three ESSs is equal to zero. This is because although not forwarding the information may be beneficial to nodes, the existence of malicious nodes with S_f would largely influence some rational nodes to deviate from current strategy to S_f. In other words, with malicious nodes in social network, the proportion of rational nodes adopting S_f increases. The more malicious nodes in the network, the larger p_f would be at the ESS, which we can observe from the roots of the quadric equation in (20). It should also be noted that when there is no malicious node in the social network, i.e., there is no type I node, the results would reduce back to those in [16], for $f_{max} = 0$, $c = 0$ and $\mu(0) = 1$.

IV. Simulation Results

In this section, we conduct simulations to validate the proposed evolutionary game theoretic model, and evaluate the hazard of malicious users to the whole social network. Without loss of generality, we first consider a uniform network with degree $k = 25$. The malicious neighbors of type I nodes are assumed to be evenly distributed, i.e., $\mu(f) = 1/f_{max}$, $1 \le f \le f_{max}$.

We first evaluate the performance under different number of malicious nodes, and the results are shown in Fig. 3. Specifically, we generate 1500 rational nodes with 500 type I nodes and 1000 type II nodes, and initialize each of them with a random strategy: 30% with S_f and 70% with S_n. The weak selection parameter α is set to be 0.025. The payoff matrix is set as $PM1: \ u_{ff} = 0.3, u_{fn} = 0.8, u_{nn} = 0.2$. The evolutionary states of p_{f1}, p_{f2} and p_f, i.e., the proportion of nodes adopting S_f among type I nodes, the proportion of nodes adopting S_f among type II nodes, and the proportion of nodes adopting S_f among type I and type II nodes, under the scenarios $f_{max} = 0$, $f_{max} = 5$ and $f_{max} = 10$, are shown in Fig.3(a), 3(b) and 3(c). We can see that the theoretic

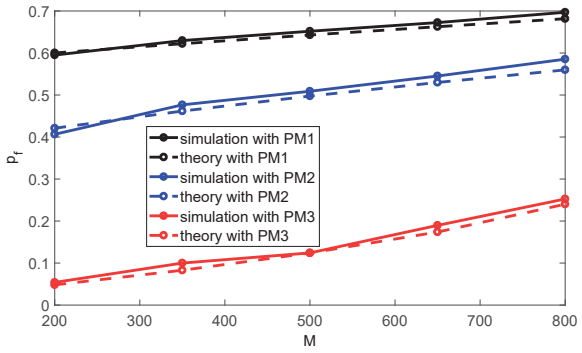


Fig. 4. The comparison with different M under three different payoff matrices.

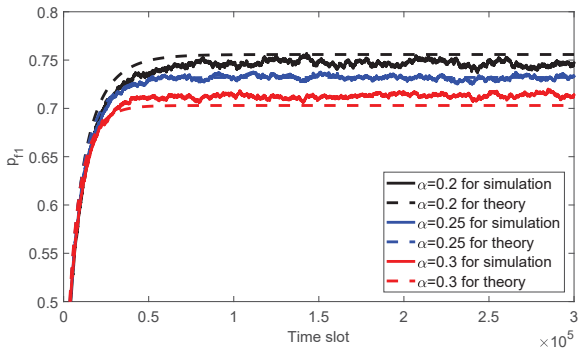


Fig. 5. The comparison with different weak selection parameter α.

results fit well with the simulation results, about 0.75% relative error with 5 malicious users and 0.54% relative error with 10 malicious users.

From Fig.3, we can also observe that as the number of malicious nodes increases from 0 to 10, the proportion of rational nodes adopting S_f increases for both type I nodes and type II nodes. For instance, in Fig.3(c), compared with the baseline, i.e. the black curve, the ESS of p_f increases by 17% with 5 malicious users and by 28.3% with 10 malicious users. Comparing Fig.3(a), (b) and (c), we observe that the proportion of type I nodes adopting S_f is the higher than that of type II nodes. This is because under malicious users' direct influence, type I nodes are apt to adopt S_f. Affected by type I nodes, though not directly connected to those malicious nodes, some type II nodes tend to deviate from their current strategies to S_f. Hence, the ESS of all rational nodes is largely enhanced compared with the baseline. It should be noted that the baselines in Fig.3(a), (b) and (c) are same, because without malicious nodes, there is no difference between type I nodes and type II nodes.

Next, we evaluate the impact of the proportion of type I nodes among all rational nodes to the ESS of p_f with different payoff matrices, and the results are shown in Fig.4. In this simulation, we assume that there are 5 malicious nodes in the network. The total number of rational nodes remains constant as 1500, while the number of type I nodes M changes from 200 to 800. From Fig.4, we can see that for all payoff matrices, the ESS increases as M increases. Specifically, when the proportion of type I nodes increases 10%, the ESS increases about 0.041 under $PM1$, 0.034 under $PM2$ and 0.025 under $PM3$, respectively. This phenomenon shows that more connected links between malicious nodes and rational nodes will improve the information diffusion.

In Fig.5, we evaluate the effect of the weak selection parameter α on p_f by fixing the payoff matrix as $PM1$ and the number of malicious users as 10. The implication of α is the relative contribution of the interaction between nodes to fitness. Thus, a bigger α means that at each round of strategy update, surrounding environment becomes more important to the fitness. We consider three cases: $\alpha = 0.02$, $\alpha = 0.025$ and $\alpha = 0.03$. In Fig. 5, it can be observed that as α increases, the ESS would decrease, which can be analyzed from (20) and (21). From this result, one can learn that in practice, it is better to maintain vigilance towards received information, i.e., maintain a relatively large α. In this way, the p_f would decrease, reducing the diffusion of detrimental information or computer virus.

V. Conclusion

In this paper, we employ graphical EGT to investigate the hazard of malicious nodes in information diffusion over social networks. Due to the existence of malicious nodes, we divide rational nodes into two types: type I nodes which are directly connected to the malicious nodes and type II nodes which are not directly connected to the malicious nodes. Based on EGT, we theoretically analyze the evolutionary dynamics and ESS for type I nodes and type II nodes, respectively. Theoretic derivations and simulation results show that the existence of malicious nodes can increase the proportion of rational nodes adopting the strategy of forwarding information. The more the number of malicious nodes, the larger the ESS of the proportion of rational nodes adopting the strategy of forwarding information. Also, the influence of the malicious nodes to the type I nodes is larger than that to the type II nodes due to the direct connection of the type I nodes.

References

[1] H. Pinto, J. M. Almeida, and M. A. Gonçalves, "Using early view patterns to predict the popularity of youtube videos," in *Proceedings of the Sixth ACM International Conference on Web Search and Data Mining*, ser. WSDM '13. New York, NY, USA: ACM, 2013, pp. 365–374. [Online]. Available: http://doi.acm.org/10.1145/2433396.2433443

[2] G. Szabo and B. A. Huberman, "Predicting the popularity of online content," *Commun. ACM*, vol. 53, no. 8, pp. 80–88, Aug. 2010. [Online]. Available: http://doi.acm.org/10.1145/1787234.1787254

[3] Y. Wang and B. Zheng, "On macro and micro exploration of hashtag diffusion in twitter," in *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, Aug 2014, pp. 285–288.

[4] J. Lehmann, B. Gonçalves, J. J. Ramasco, and C. Cattuto, "Dynamical classes of collective attention in twitter," in *Proceedings of the 21st International Conference on World Wide Web*, ser. WWW '12. New York, NY, USA: ACM, 2012, pp. 251–260. [Online]. Available: http://doi.acm.org/10.1145/2187836.2187871

[5] Y. Cao, P. Shao, L. Li, and Y. Cao, "Topic propagation model based on diffusion threshold in blog networks," in *2011 International Conference on Business Computing and Global Informatization*, July 2011, pp. 539–542.

[6] X. Lu and Yidong Cui, "The study of micro-blog information diffusion model based on community structure detection," in *2012 6th International Conference on New Trends in Information Science, Service Science and Data Mining (ISSDM2012)*, Oct 2012, pp. 612–616.

[7] X. Hao, G. Sheng, Z. Yu, L. Juncen, P. Huacan, and G. Jun, "Predicting information diffusion via matrix factorization based model," in *2014 4th IEEE International Conference on Network Infrastructure and Digital Content*, Sep. 2014, pp. 257–261.

[8] C. Tsai, J. Lou, W. Lu, and S. Lin, "Exploiting rank-learning models to predict the diffusion of preferences on social networks," in *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, Aug 2014, pp. 265–272.

[9] J.-R. Lee and C.-W. Chung, "A new correlation-based information diffusion prediction," in *Proceedings of the 23rd International Conference on World Wide Web*, ser. WWW '14 Companion. New York, NY, USA: ACM, 2014, pp. 793–798. [Online]. Available: http://doi.acm.org/10.1145/2567948.2579241

[10] X. Ding, Z. Wu, W. Chen, Y. Liu, Y. Xie, and S. Cai, "Modeling complex social contagions in big data era," in *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, March 2017, pp. 830–834.

[11] Z. Jin-lou, L. Zhi-bin, and Y. Jian-nan, "Modeling of information diffusion based on network dimension-force," in *2011 International Conference on Management Science Engineering 18th Annual Conference Proceedings*, Sep. 2011, pp. 18–27.

[12] B. Wang, G. Chen, L. Fu, L. Song, and X. Wang, "Drimux: Dynamic rumor influence minimization with user experience in social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 10, pp. 2168–2181, Oct 2017.

[13] C. Jiang, Y. Chen, and K. J. R. Liu, "Modeling information diffusion dynamics over social networks," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2014, pp. 1095–1099.

[14] ——, "Graphical evolutionary game for information diffusion over social networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 4, pp. 524–536, Aug 2014.

[15] ——, "Evolutionary dynamics of information diffusion over social networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 17, pp. 4573–4586, Sep. 2014.

[16] X. Cao, Y. Chen, C. Jiang, and K. J. Ray Liu, "Evolutionary information diffusion over heterogeneous social networks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 2, no. 4, pp. 595–610, Dec 2016.

[17] H. Ohtsukia and M. A. Nowak, "The replicator equation on graphs," *Journal of Theoritic Biology*, vol. 243, pp. 86–97, Nov. 2006.

[18] P. Shakarian, P. Roos, and A. Johnson, "A review of evolutionary graph theory with applications to game theory," *Biosystems*, vol. 107, no. 2, pp. 66 – 80, 2012.

[19] M. A. Nowak and K. Sigmund, "Evolutionary dynamics of biological games," *Science*, vol. 303, no. 5659, pp. 793–799, 2004. [Online]. Available: https://science.sciencemag.org/content/303/5659/793