International Journal of Modern Physics B
Vol. 37, No. 2 (2023) 2350014 (21 pages)

DOI: 10.1142/S0217979223500145

Modeling strategies to protect investors from financial fraud collapses on social networks

Jinbiao Jin

Scientific Research Center, Zhejiang Shuren University, Hangzhou 310015, P. R. China
1113994458@qq.com

Hong Liu

School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, P. R. China

Contemporary Business and Trade Research Center of Zhejiang Gongshang University, Hangzhou 310018, P. R. China
llh@mail.zjgsu.edu.cn

Yunyan Han* and Anding Zhu†

School of Management and E-Business, Zhejiang Gongshang University, Hangzhou 310018, P. R. China

Contemporary Business and Trade Research Center of Zhejiang Gongshang University, Hangzhou 310018, P. R. China
**20020200077@pop.zjgsu.edu.cn*
†*zhuad@mail.zjgsu.edu.cn*

Received 23 April 2022
Revised 10 July 2022
Accepted 30 July 2022
Published 5 September 2022

Financial fraud is more likely to spread and produce serious and adverse results through social networks. This study investigates four protection strategies: the uniform protection strategy, the random protection strategy, the targeted protection strategy, and the acquaintance protection strategy based on the potential-investor-divestor (PID) model. The simulation results show that the targeted protection strategy is the best solution for both ER and BA networks. The random protection strategy is the least efficient solution, as it requires spreading a large number of anti-fraud messages to achieve a relatively

†Corresponding author.

good performance. The acquaintance protection strategy performs closely to the targeted protection strategy in terms of social dynamics. However, the uniform protection strategy is better than the acquaintance protection strategy, as it involves fewer victims when it collapses. This study suggests that the regulators should protect investors from financial fraud collapses by promoting the financial literacy education and regulating the behaviors of influential people.

Keywords: Financial fraud; social network; complex network; financial risk; PID model.

PACS numbers: 05.45.−a

1. Introduction

Digital finance benefits financial services users, digital finance providers, and the economy, facilitating financial inclusion in both developing and developed economies.[1] However, the rapid prevalence of digital finance also exposes more individuals to be exposed to various new types of financial fraud crimes.[2,3] Financial fraud can be broadly defined as an illegal or unethical activity that aims to take money or other assets from victims by deceits. Peer-to-Peer (P2P) lending is popular in China over the past few years. At its peak, China had more than 6600 P2P lending platforms with an annual transaction volume of approximately CNY 340 billion in 2017.[4] P2P lending was developed as an innovative micro-financial solution to bridge the small business capital gap.[5,6] However, for many years, P2P lending has been associated with negative news (e.g., financial fraud, platform collapses, and investor protests).[7] The Chinese government determined to eliminate the entire P2P lending sector after 2019.[8]

There was a lack of regulation experience concerning P2P lending because it was regarded as a technological innovation of finance. Thus, many techniques have been developed to assess and mitigate its risks. Emekter *et al.* found that credit grade, debt-to-income ratio, FICO score (i.e., the credit score used by most banks and credit card issuers to assess an individual's creditworthiness), and revolving line utilization played important roles in loan defaults.[9] Xu *et al.* developed a data mining project to detect loan request fraud (including types and features) with the help of large volumes of data from a variety of sources.[10] Chen *et al.* utilized not only several machine learning schemes but also resampling and cost-sensitive mechanisms to predict the default risk of P2P lending by processing imbalanced datasets.[11] Other studies have tried to solve the trust problem from the perspectives of participant behavior and information quality. Yang addressed the idea that lenders might behave positively when perceiving a borrower's photograph as projecting trustworthiness and happiness.[12] Caldieraro *et al.* proposed and tested a theory in which countersignaling provided a mechanism to attenuate information asymmetry about financial products.[13] Cai *et al.* found that the borrowers' likelihood of successful funding is significantly associated with the interest rate, loan duration, loan amount, number of verifications, credit grade, and overdue repayment.[14]

However, the systemic risk caused by the platform-level crashes will be much greater than individual transaction-level risks. Moreover, the COVID-19 pandemic

aggravated the occurrence of new digital financial fraud crimes.[15] Zhu *et al.* found that the traditional Ponzi schemes operate more easily through social networks, resulting in more damage to society.[7] Feng *et al.* also reported another case study of the "5.03" pyramid scheme, which expanded to several provinces. Every entrants were required to pay CNY 3800 to CNY 69,800 to purchase 1–21 copies of virtual products.[16] The pyramid scheme is similar to multilevel marketing. In many illegal cases, entrants were "brainwashed" into persuading their social connections to join the scheme. Senior salespeople lured the recruited victims into buying more products by promising more commissions.[17] Additionally, digital finance motivates other crowdfunding business models (e.g., reward-based crowdfunding and donation-based crowdfunding).[18] Vasek and Moore analyzed the supply and demand for Bitcoin-based Ponzi schemes and identified three types of scams. They also found that the scammer can elongate the scam life by frequently interacting with their victims, such as by posting more than a quarter of the comments in a related thread.[19]

When a large-scale scheme collapses, it leads to the severe disruption and harm to the victims as well as the economy.[20] According to Zhu *et al.*'s work, the high speed of fraud diffusion is key to alleviate the interest burden and to extend the final scale of Ponzi schemes.[7] Keep and Nat argued that the multilevel marketing model facilitates the growth of pyramid scheme fraud, creating victims rather than customers because internal consumption resembles neither employee purchases nor a buying club without a significantly external customer base.[21] Lee and Lee found strong evidence that the P2P lending market shares some characteristics of online markets with respect to herding behavior.[22] Similarly, Luo and Lin also reported the herd effect, as friend bids, and bid counts impose significant effects on the decision-making time of investors.[23] Xu *et al.* constructed models of fraud exposure recognition (FER) and fraud victimhood recognition (FVR) by utilizing a machine learning method to investigate a nationwide survey involving 36,202 participants.[24]

Several technological and financial tools have been developed to detect fraud and prevent would-be victims from financial fraud on large-scale online financial platforms.[9–11] However, these tools cannot detect the systemic risk of the online financial platform.[25] Furthermore, it is difficult to detect the internal mechanisms because most financial fraud schemes present a complex network structure among the investors and intermediaries.[17,26] There are few references in the literature that address preventing people from becoming victims of financial fraud collapses. Wang *et al.* developed a new graph attentive network model for P2P lending fraud detection based on text information and/or user relationship information.[27] Chen *et al.* proposed the SADPonzi platform based on a semantic-aware detection approach to identify Ponzi schemes in Ethereum smart contracts. They applied their SADPonzi platform to all 3.4 million smart contracts in Ethereum and identified 835 Ponzi scheme contracts, with over USD 17 million invested by victims.[28] In addition, Fu *et al.* developed a model to predict P2P trading volume by employing the TextCNN

model to classify the sentiment of investor comments and obtain the time series of changes in sentiment.[29] However, most of the time, financial fraud schemes are often not easily recognized at their start.[16,21] In addition, with the rapid development of digital finance, many new types of financial fraud schemes appear in the form of innovative financial technology, misleading victims, and blinding them to potential risks.[16,18,19] Therefore, improving individuals' digital financial literacy becomes another strategy to prevent and protect the population from financial fraud schemes.

Digital financial literacy (DFL) is defined as an individual's ability to acquire the knowledge, skills, confidence, and competencies to safely use digitally delivered financial products and services and make informed financial decisions. Engels *et al.* found that more financially knowledgeable individuals have a higher propensity to detect financial fraud.[30] In addition, Cross argued that digital financial fraud should be seen as an area of specialization within current cybercrime and high-tech crime units. He advocated that the police use whatever means necessary to improve their responses on behalf of fraud victims.[31] Iacopini *et al.* proposed a simplicial complex and contagion to present the high-order feature of social systems because they noticed pairwise interactions are not often enough to characterize social contagion processes.[32] Li *et al.* proposed a competing spreading model of two SIS-like epidemics in a simplicial complex, focusing on the influence of higher-order interactions on the critical behavior of the social system.[33] Likely, Wang *et al.* proposed a generalized k-core percolation model to investigate the robustness of the higher-order dependent networks.[34] Nie *et al.* presented a coevolution epidemics spread model on a temporal higher-order social network, which considers synergistic, competitive, and asymmetric interactions.[35]

Zhu *et al.* investigated the effect of investor risk warning on preventing Ponzi scheme diffusion.[36] However, there is still a lack of investigation on the effects of DFL education and risk warning against spreading financial frauds. In this study, we attempt to compare four protection strategies: the uniform protection strategy, the random protection strategy, the targeted protection strategy, and the acquaintance protection strategy by adopting from the four corresponding immunization strategies. Investor risk warning is regarded as a mass, random immunization against spreading fraud. The results showed that the random immunization strategy would take effect by postponing the peak position of the system balance as well as suppressing the peak values of the system balance.[36] However, it is the least efficient solution, as it requires spreading a large number of anti-fraud messages to achieve a relatively good performance. Otherwise, the targeted protection strategy aims to prevent influential individuals from participating fraud schemes. The regulator promotes the DFL education to increase the vigilance of potential victims, which is regarded as uniform protection strategy. The regulator enhances the DFL education by conveying anti-fraud messages to a random population and asking them to invite their connections to improve their DFL, which is regarded as acquaintance

protection strategy. After we compare the four protection strategies, we find that the uniform protection strategy is better than the acquaintance protection strategy, as it involves fewer victims when it collapses. Additionally, we find that the regulators can protect investors from financial fraud collapses by promoting financial literacy education and regulating the behaviors of influential people.

The rest of the paper is organized as follows: the basic financial fraud collapse model is formulated in Sec. 2. Four types of protection strategies derived from immunization strategies are formulated in Sec. 3. Then, the numerical simulations are conducted in Sec. 4, with the main conclusions and discussion presented in Sec. 5.

2. The Model and Assumptions

2.1. *The basic model*

Zhu *et al.* proposed the basic potential-investor-divestor (PID) model for a Ponzi scheme spread through social networks.[7] The PID model captures the nature of Ponzi schemes by integrating fraud diffusion dynamics into economic outcomes. The model traces the money flowing in and out of the scheme and evaluates the systemic risk at the different stages of the entire scheme life. Zhu *et al.* proposed a mass random immunization model to protect investors.[36] According to their strategy, each investor should be informed with a random probability. This scenario occurs because the regulator cannot distinguish investors from the normal population. The regulator does not know who the investors are and when the investors will be recruited into the fraud scheme. If the investors are informed earlier than recruited, they will ignore the deceptive information. The rapid development of big data technology provides opportunities for regulators to target protected individuals. In this study, the authors aim to compare four protection strategies derived from the immunization strategies.

First, we inherit the assumptions and notations of the fraud scheme from Ref. 36. We suppose that the investors' network $G(V, E)$ is an undirected, closed social network with N nodes (i.e., investors). Initially, all investors are potential investors (P). The potential investors become investors (I) after they receive the deceptive messages and are recruited into the scheme. The investors become divestors (D) after they withdraw their funds. Similar to the classical susceptible-infected-recovered (SIR) epidemic model, the PID model assumes that the *spreading rate* is λ, and the *withdrawal rate* is μ. Furthermore, we need to analyze the financial outcomes of the scheme. We thus suppose that the amount of each investor's principal is W. The investors are promised with an *interest rate* of return of a constant π for each *interest-calculating period* (ICP), which is denoted by τ. Let $F^{\text{in}}(t)$ denotes the fund inflow function and $F^{\text{out}}(t)$ denotes the fund outflow function. Therefore, the fund flowing through the system with respect to the t is $F(t) = F^{\text{in}}(t) - F^{\text{out}}(t)$, and the balance of the system is $B(t) = \int_0^t F(u)du$.

2.2. *The homogeneous network*

Referring to Ref. 36, let $p(t)$, $i(t)$, and $d(t)$ denote the normalized density of potential investor, investor, and divestor, respectively, such that the entire population of $p(t)$, $i(t)$, and $d(t)$ is 1. The initial conditions of the basic model are $i(0) = \epsilon$, $p(0) = 1-\epsilon$, and $d(0) = 0$, where $\epsilon \ll 1$ is a small positive value. The basic investor diffusion model can be written as the following equation:

$$\begin{cases} \dfrac{di(t)}{dt} = \lambda\overline{k}p(t)i(t) - \mu i(t), \\ \dfrac{dp(t)}{dt} = -\lambda\overline{k}p(t)i(t), \\ \dfrac{dd(t)}{dt} = \mu i(t), \end{cases} \tag{1}$$

where $\overline{k}$ is the average degree of the homogeneous investor network.

According to the spreading mechanism, the fund flux function can be calculated by aligning every ICP. Therefore, the fund flux $F(m\tau, \tau)$ within the mth ICP duration $[m\tau, (m+1)\tau]$ can be written as the following equation:

$$\begin{aligned} F(m\tau, \tau) &= F^{\text{in}}(m\tau, \tau) - F^{\text{out}}(m\tau, \tau) \\ &= NW \int_{m\tau}^{(m+1)\tau} \lambda\overline{k}p(t)i(t)dt \\ &\quad - NW \int_{m\tau}^{(m+1)\tau} \mu i(t)dt - NW\pi i(m\tau). \end{aligned} \tag{2}$$

2.3. *The inhomogeneous network*

Switching to the scenario of an inhomogeneous investor network, the densities of potential investors, investors and divestors are sorted by degree k, namely, $p_k(t)$, $i_k(t)$, and $d_k(t)$. The inhomogeneous network version of the PID model can be modified as shown in the following equation:

$$\begin{cases} \dfrac{di_k(t)}{dt} = \lambda k p_k(t) \displaystyle\sum_{k'} i_{k'}(t)P(k'|k) - \mu i_k(t), \\ \dfrac{dp_k(t)}{dt} = -\lambda k p_k(t) \displaystyle\sum_{k'} i_{k'}(t)P(k'|k), \\ \dfrac{dd_k(t)}{dt} = \mu i_k(t), \end{cases} \tag{3}$$

where $P(k'|k)$ is the conditional probability that an edge departing from a node with degree k arrives at a node with degree k'.

Likely, the fund flux function of Eq. (2) with node degree k can be modified as the following equation:

$$F_k(m\tau, \tau) = F_k^{\text{in}}(m\tau, \tau) - F_k^{\text{out}}(m\tau, \tau)$$

$$= NW \int_{m\tau}^{(m+1)\tau} \lambda k p_k(t) \sum_{k'} i_{k'}(t) P(k'|k) dt$$

$$- NW \int_{m\tau}^{(m+1)\tau} \mu i_k(t) dt - NW \pi i_k(m\tau). \quad (4)$$

Therefore, the overall fund flux function for all nodes can be written as the following equation:

$$F(m\tau, \tau) = \sum\nolimits_k P(k) F_k(m\tau, \tau), \quad (5)$$

where $P(k)$ is the probability of nodes with degree k.

In addition, the balance of the system accumulated until the mth ICP for both homogeneous and inhomogeneous networks can be written as the following equation:

$$B(m\tau) = \sum_{j=0}^{m} F(j\tau, \tau). \quad (6)$$

3. The Protection Strategies

There are many immunization and vaccination strategies in the literature to prevent individuals from being infected by risks and mitigate the overall epidemic losses.[37] From a regulatory perspective, there are four typically nonbehavioral immunization strategies, i.e., uniform, random, targeted, and acquaintance.[38,39] Similar to immunization and vaccination strategies, the regulator promotes protection campaigns by disseminating anti-fraud messages to agents or enhancing financial literacy education. Zhu *et al.* presented the effect of the random immunization strategy against financial diffusion in the investor social network.[36] Four nonbehavioral protection strategies will be compared in the next sections.

3.1. *Uniform protection strategy*

From an immunity point of view, the uniform immunization strategy will have the effect of reducing the spreading rate by a factor $g(0 < g < 1)$.[39–42] That is, the spreading rate λ will be suppressed to $\lambda(1-g)$. Here, the regulator promotes financial literacy education, which increases the vigilance of agents. Although the agents have not received the anti-fraud messages before they are recruited to the fraud scheme, they are highly likely to see through the fraud or at least become more cautious. This can also be regarded as a proportional reduction of the spreading rate.

3.2. *Random protection strategy*

From an immunity point of view, the random immunization strategy means that a fraction of the population $g(0 < g < 1)$ is selected randomly to be vaccinated.[38,39,43,44] This strategy can be regarded as randomly removing a proportion

(i.e., g) of the entire population at the beginning. The vaccinated agents will prevent diffusion. In fact, the regulator can spread the anti-fraud messages (e.g., flyers) to comprehensive agents. If these agents receive the messages and become vigilant about financial fraud, they will be vaccinated agents. According to the results of Zhu *et al.*,[36] the random protection strategy takes effect by postponing the peak position of the system balance as well as suppressing the peak values of the system balance, which helps reduce the scheme's scale concerning the total number of investors and amount of principal involved.

3.3. *Targeted protection strategy*

From an immunity point of view, the targeted immunization strategy achieves a higher efficiency, which is a method that progressively immunizes the nodes of the highest degree.[38–42,44] The target immunization strategy proves to be more efficient for scale-free networks.[39,40] The targeting purpose is to identify the more influential nodes. Bai *et al.* selected the set containing nodes with maximal degrees as the vaccinated targets.[38] Peng *et al.* considered progressively immunizing the node with the highest sum of weights of its outward links.[39] Other targeting strategies include the effective degree of vertex,[45] the highest-betweenness links or nodes,[46,47] and influential nodes.[48,49] In this study, we choose the fraction of nodes $g(0 < g < 1)$ with maximal degrees $(\sum_k P(k > k_{\text{threshold}}) = g)$ as the targeted immunization nodes.[38,39] This targeted strategy is realistic. The regulator focuses on the most influential agents with the professional and social advantages to influence other agents (e.g., fund managers, opinion leaders, Internet celebrities, and even active users on social networking sites). These agents are not difficult to delineate. If these agents are supervised and do not spread financial fraud information, they will be the vaccinated agents. Therefore, the regulator can protect investors from financial fraud collapses by supervising targeted agents.

3.4. *Acquaintance protection strategy*

From an immunity point of view, targeted immunization requires global information to delineate the targeted agents. However, much fraud diffusion may be dynamic and initially hidden. The regulator cannot trace the global situation. Most of the time, the regulator employs the reporting mechanism. If some victims report fraud, the regulator will warn the related contacts. This is similar to the acquaintance immunization strategy. The advantage of the acquaintance immunization strategy is that it only requires local information.[39,41,44] In this study, we consider the acquaintance immunization by choosing a random fraction of the agents $\{v_i \,|\, i = 1, 2, \ldots, gN/2\}$ $(0 < g < 1)$ and one random agent of their neighbors.[39] Agents with a larger degree have a higher probability of being chosen when their contacts are randomly chosen to be vaccinated. Hence, the acquaintance immunization strategy is supposed to be efficient without global information. In fact, the regulator enhances the financial literacy education by conveying anti-fraud messages to a random population and

asking the participants to invite their relatives or friends to improve their financial literacy.

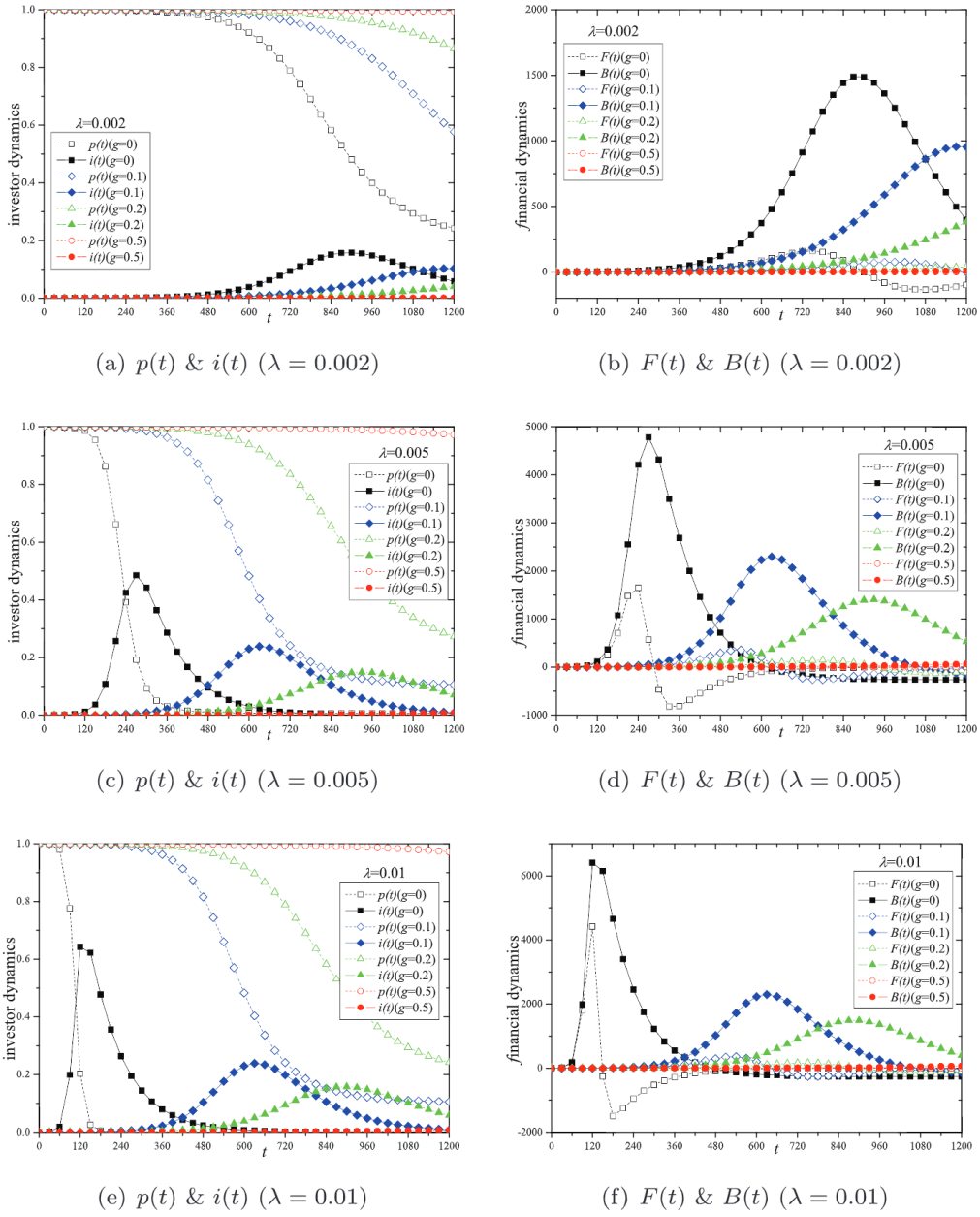
4. Numerical Simulations

In this study, the Erdös-Rényi (ER) random network is implemented to simulate the homogeneous network.[50] We generate ER networks with $N = 10{,}000$ and $\overline{k} \approx 10$. As a comparison, the Barabási-Albert (BA) scale-free network is used to simulate an inhomogeneous network.[51] We generate BA networks with $N = 10{,}000$ and control parameters of $(m_0, m) = (5, 5)$. Without loss of generality, we set other parameters as $\mu = 0.01$, $\tau = 30$ (approximately one month), and $\pi = 0.008$ (equivalent to a 10% annual interest rate). Every type of simulation is realized 100 times. To compare different protection strategies, we employ the same indicator of protection intensity, g.

4.1. *The performance of the uniform protection strategy*

The performance of uniform protection strategies on the ER network and BA networks are demonstrated in Figs. 1 and 2, respectively. We compare three groups of spreading rates, i.e., $\lambda = 0.002$, $\lambda = 0.005$, and $\lambda = 0.01$. Obviously, the larger the spreading rate, the greater the peak of $i(t)$, and the earlier the peak time [referring to Figs. 1(a), 1(c), 1(e) and 2(a), 2(c), 2(e)]. On the other hand, the uniform protection strategy not only suppresses the peak of $i(t)$, but also delays the arrival of the peak. For the same λ, with the increase in protection intensity g, the spread scale decreases. However, the uniform protection strategy performs better in the ER network than in the BA network. For example, in the case of $g = 0.5$ (i.e., half the population has received financial literacy education), the spreading will be totally controlled in the ER network, and be suppressed to a very low level in the BA network (i.e., the peaks of $i(t)$ are approximately 0.1 for both $\lambda = 0.005$ and $\lambda = 0.01$) [referring to Figs. 2(c) and 2(e)].

Additionally, the larger the spreading rate is, the worse the financial outcome [referring to Figs. 1(b), 1(d), 1(f) and 2(b), 2(d), 2(f)]. That is, the larger the spreading rate is, the greater the peak of $F(t)$ and $B(t)$, which means that the scheme will involve a larger scale of money and cause more losses when it collapses. The uniform protection strategy will help mitigate the collapse scales in both the ER network and BA network. For the same λ, with the increase in protection intensity g, the entire scale ($B(t)$) will be suppressed, especially in the ER network. For the case of $g = 0.5$, the peaks of $B(t)$ are suppressed to almost 0 in the ER network, and a very low level in the BA network (i.e., the peaks of $B(t)$ are approximately 1000 for both $\lambda = 0.005$ and $\lambda = 0.01$) [referring to Figs. 2(d) and 2(f)]. Therefore, the uniform protection strategy plays a positive role in suppressing both the population and financial scales, which implies that the individuals will be protected from financial fraud collapses if they receive financial literacy education.



(a) $p(t)$ & $i(t)$ ($\lambda = 0.002$) (b) $F(t)$ & $B(t)$ ($\lambda = 0.002$)

(c) $p(t)$ & $i(t)$ ($\lambda = 0.005$) (d) $F(t)$ & $B(t)$ ($\lambda = 0.005$)

(e) $p(t)$ & $i(t)$ ($\lambda = 0.01$) (f) $F(t)$ & $B(t)$ ($\lambda = 0.01$)

Fig. 1. (Color online) Uniform Protection Strategy: Comparison of investor and financial dynamics with different protection intensity gs of different spreading rate λs in ER networks with uniform immunization.

4.2. *The performance of the random protection strategy*

The performance of random protection strategies on the ER network and BA networks are demonstrated in Figs. 3 and 4, respectively. Similar to the uniform protection strategy, we compare three groups of spreading rates, i.e., $\lambda = 0.002$, $\lambda = 0.005$, and $\lambda = 0.01$. Obviously, the larger the spreading rate, the greater the peak of $i(t)$, and the earlier the peak time [referring to Figs. 3(a), 3(c), 3(e)