Dynamic Control of Fraud Information Spreading in Mobile Social Networks

Yaguang Lin, Xiaoming Wang, Fei Hao, Yichuan Jiang, *Senior Member, IEEE*, Yulei Wu, *Member, IEEE*, Geyong Min, *Senior Member, IEEE*, Daojing He, *Member, IEEE*, Sencun Zhu, Wei Zhao, *Fellow, IEEE*

***Abstract*—Mobile Social Networks (MSNs) provide real-time information services to individuals in social communities through mobile devices. However, due to their high openness and autonomy, MSNs have been suffering from rampant rumors, fraudulent activities and other types of misuses. To mitigate such threats, it is urgent to control the spread of fraud information. The research challenge is: *how to design control strategies to efficiently utilize limited resources and meanwhile minimize individuals' losses caused by fraud information*? To this end, we model the fraud information control issue as an optimal control problem, in which the control resources consumption for implementing control strategies and the losses of individuals are jointly taken as a constraint called *total cost*, and the minimum total cost becomes the objective function. Based on the optimal control theory, we devise the optimal dynamic allocation of control strategies. Besides, a dynamics model for fraud information diffusion is established by considering the uncertain mental state of individuals, we investigate the trend of fraud information diffusion and the stability of the dynamics model. Our simulation study shows that the proposed optimal control strategies can effectively inhibit the diffusion of fraud information while incurring the smallest total cost. Compared with other control strategies, the control effect of the proposed optimal control strategies is about 10% higher.**

***Index Terms*—Mobile social networks, fraud information diffusion, system dynamics, optimal control, simulation.**

I. Introduction

With the boom of the Internet and the rapid popularization of intelligent mobile devices, Mobile Social Networks (MSNs) have grown up to become an important platform for information dissemination [1]. MSNs can provide people with a variety of real-time information services, and have already penetrated into our daily life. The Internet-based MSNs have exhibited their great charm and broad prospect in many application fields, such as instant communication, life service, interactive entertainment, *etc.*, and have attracted extensive attention of the industry and the academia [2], [3].

However, the development of MSNs is like a double-edged sword [4], [5]. When MSNs are increasingly becoming an indispensable part of people's lives, a series of unhealthy phenomena such as fake news, rumors, online promotion and fraudulent activities are becoming more and more rampant, which pose a serious threat on the normal social network activities [6], [7]. Besides, by means of the emerging technologies of intelligent terminals, wireless networks, and online payment in recent years, the high rate of fraud has caused great losses to people [8]. According to the official data released by the security ministry, telecommunications fraud in MSNs has grown at an annual rate of $20\% - 30\%$ [9]. The following are two representative scenarios:

Scenario A: One scenario is the Veracruz incident in August of 2015 [10]. A piece of rumor saying "shootouts and kidnappings by drug gangs happening near schools in Veracruz spread in Twitter and Facebook. This rumor caused severe chaos in the city and many serious car crashes happened amid the hysteria.

Scenario B: Another shocking scenario occurred in August 2016 when a Chinese university professor suffered a telecommunication-based fraud, leading to a serious loss of 17.6 million yuan [11]. Criminals fabricated an elaborate hoax, used the network to transmit fraud information and perform remote frauds to victims.

Fraud information diffusion has become a prominent problem in social networks [12]. Those evidence highlight that effectively controlling the fraud information in MSNs applications is of great significance. Here we define the so-called fraud information as a piece of malicious information or false information, which aims to intentionally cause adverse effects such as mass panic, or defraud victims of their property. In order to cope with the spread of such information in MSNs more effectively, it is an urgent need to study the pattern of fraud information diffusion and further put forward the corresponding control measures.

Previously, some mathematical models have been used to model the diffusion evolutionary process of fraud information in the network. Most of these models are based on the theory of biological infectious disease, because the spread process

Manuscript received XXX, XX, 2019; revised XXX, XX, 2019. This work is supported by the National Natural Science Foundation of China (Grant Nos. 61872228, 61702317, 61601273, 61602289), the Fundamental Research Funds for the Central Universities (Grant No. 2017TS046). (*Corresponding author: Xiaoming Wang*)

Y. Lin, X. Wang, and F. Hao are with the Key Laboratory of Modern Teaching Technology, Ministry of Education, Xi'an, 710062, China, and the School of Computer Science, Shaanxi Normal University, Xi'an 710119, China. (E-mail: light@snnu.edu.cn, wangxm@snnu.edu.cn and fhao@snnu.edu.cn).

Y. Jiang is with the School of Computer Science and Engineering, Southeast University, Nanjing 211189, China. (E-mail: yjiang@seu.edu.cn).

Y. Wu, and G. Min are with the College of Engineering, Mathematics and Physical Sciences, University of Exeter, Exeter, EX4 4QF, U.K. (E-mail: y.l.wu@exeter.ac.uk, and g.min@exeter.ac.uk).

D. He is with the School of Computer Science and Software Engineering, East China Normal University, Shanghai 200062, China. (E-mail: djhe@sei.ecnu.edu.cn).

S. Zhu is with the Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA 16802, USA. (E-mail: sencunzhu@ist.psu.edu).

W. Zhao is with American University of Sharjah, PO Box 26666, Sharjah, U.A.E. (E-mail: zhao8686@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier XXX

of infectious diseases in biology and the diffusion process of fraud information in the network are very similar [13], [14]. The most widely used model is the Susceptible-Infected-Recovered (SIR) model, in which all individuals are divided into three categories: susceptible, infected and recovered [14]. From the perspective of information diffusion, the semantics of susceptible, infected and recovered can fully correspond to the process of fraud information diffusion. If an individual has not yet received any fraud information, it belongs to the susceptible state. If an individual received fraud information and was misled, it belongs to the infected state. If an individual was ever infected and now no longer believes the fraud information, it belongs to the recovered state.

Although the existing SIR based derivation models can correctly describe the transitional relationship and the dynamic evolutionary processes of node states, the spread of fraud information in MSNs shows some new characteristics. Firstly, the information sender and receiver are human beings, and human mental activities are often complex. For example, the individual will likely experience a series of mental activities such as thinking, hesitating and wandering when receiving a piece of information [15], [16]. Secondly, the fraud information diffusion processes in MSNs are the complex results of the continuous interactions of nodes in different states [17]. Thirdly, because of the psychological effect, repeated reception of the same information may give users the feeling of disgust and lead to reverse psychology. The data analysis about 4.4 million Twitter messages diffusion shows that in the process of information diffusion, users will deviate from the original intention of information and produce the phenomenon of emotional transfer [18]. Due to these new characteristics, the existing SIR based inference models fail to describe the evolutionary process of information diffusion accurately. Therefore, if the above characteristics can be taken into account in the model, the dynamic evolution process of fraud information diffusion can be described more effectively.

Besides establishing dynamics models and revealing fraud information diffusion laws, our ultimate goal should be to effectively control the diffusion of fraud information. However, the implementation of any control or intervention for the system will incur a certain "price" [19]. As for the process of controlling fraud information diffusion in MSNs, some operational control measures will inevitably consume a certain amount of precious manpower and material resources. For example, in response to the crisis of fraud information, the government constantly sends authoritative messages to the network to prevent individuals from being misled by it. All this need to cost a lot of limited communication and other resources. Furthermore, fraud information can also cause great harm to individuals [9], [12]. Therefore, how to efficiently utilize limited control resources and minimize losses of individuals by adopting proper control strategies has become an urgent issue to address.

Some of the existing research works can control the diffusion of fraud information to some extent, but there are still some obvious issues [20]–[22]. The first issue is that the they usually adopts a single continuous or pulse control strategy, and mostly do not consider the implementation efficiency of the control strategy and the utilization efficiency of the control resources. The second issue is that while some works have realized the constraint of control resources and transformed the control problem into the optimal dynamic allocation of control resources, they ignore the harm of fraud information diffusion to individuals.

In order to overcome the above limitations, in this paper, we put forward a novel dynamics model, called $SWIR$, which can accurately describe the dynamic process of fraud information diffusion. Importantly, for the sake of efficiently utilizing the limited resources and minimizing the losses of individuals, we establish the optimal control system to solve the optimal dynamic allocation problem of control strategies for fraud information diffusion. The main contributions of this paper are summarized as follows:

- **Fraud information diffusion model:** In consideration of the uncertain mental state of individuals and the transitional relationship of individuals in different states, we establish the $SWIR$ model. It can more effectively describe the dynamic diffusion process of fraud information in MSNs. Additionally, we theoretically analyze the stability of the $SWIR$ model and the trend of fraud information diffusion.
- **Dynamic allocation of the control strategies:** In order to efficiently utilize limited control resources and minimize losses of individuals caused by fraud information, we propose two synergistic control strategies. We take the control resources consumption and the losses of individuals as the *total cost* constraint. Then, we formulate the optimal control problem to minimize the total cost, and model the control strategies as functions varying over time. Finally, based on the optimal control theory, the optimal distribution of the control strategies functions over time is derived.
- **Simulation experiments on datasets:** We validate the correctness and efficiency of the proposed diffusion model and the optimal control strategies on both synthetic datasets and real social network datasets. The results demonstrate that our proposed diffusion model can accurately describe the dynamic diffusion process of fraud information and our proposed control strategies can effectively inhibit the fraud information in MSNs. In particular, the optimal dynamic allocation control strategies can achieve minimum control resources consumption and losses of individuals.

The rest of the paper is organized as follows. In Sec. II, some previous works are reviewed. In Sec. III, we first establish a novel dynamics model of the fraud information diffusion in MSNs. Then, we analyze the trend of fraud information diffusion and the stability of the dynamics model. Consequently, we propose two synergistic control strategies to suppress the spread of fraud information, and derive the optimal distribution of the control strategies. Extensive simulations are conducted in Sec. IV. Sec. V concludes this paper.

II. Related Work

In recent years, research that explores social relationship structure for information diffusion in MSNs has been very

active. Especially, the problem of maximizing the influence of information has attracted the attention from both the academia and industry, and a number of innovative research results [23], [24] have been achieved. Nevertheless, the research on the diffusion and control methods of *fraud information* is merely in its infancy. At present, the research on information diffusion mainly develops along two branches: modeling of the information diffusion process, and control of information diffusion process.

In view of the modeling of the information diffusion process, most scholars use the infectious disease diffusion model, the independent cascade model, the linear threshold model, the real dataset fitting method and so on, to model the spatiotemporal dynamic evolutionary process of information diffusion [17], [25]–[30]. Zhou et al. [17] established a dynamics model for the information propagation problem in MSNs, and discussed how the user preference affects the information diffusion process. Their work provides a new theoretical method for dynamics modeling of the information diffusion, but not for malicious information diffusion. Li et al. [29] introduced a time-dependent payment function based on game theory. Considering the global influence and social influence of users, a time dynamic prediction model of information diffusion in online social network was proposed, which can predict whether the user's diffusion behavior will occur within a specified period of time. However, the model only focuses on the time dynamics of information diffusion, and it does not take into account the spatial impact factors of information diffusion.

Targeting at the problem of information diffusion in the post-disaster rescue network, [30] proposes an information diffusion model based on the probability stopping mechanism in finance, as well as an analysis method based on Markov chain. The model and method can reduce the energy consumption and save the storage space of communication equipment to some extent in small-scale network scenarios. Nevertheless, this method will confront the problem of the explosive growth of state space in large-scale MSNs, so it is difficult to be effectively applied in actual large-scale network scenarios.

From the perspective of big data analysis, some scholars have studied and excavated the rules and influencing factors in the process of information diffusion. Using a large dataset from Twitter about Hurricane Sandy, Yoo et al. [31] empirically examined the impact of key elements on information propagation rates on social media. The analysis results show that internal diffusion through social media networks advances at a significantly higher speed than information in these networks coming from external sources, and the information posted earlier exhibits a significantly higher speed of diffusion than information that is introduced later. Zhu et al. [32] collected several real topics propagating data on Sina Microblog and analyzed individuals' propagation intentions. Results show that the topic with one-sided opinions can spread faster and more widely, and intervention with the opposite opinion is an effective measure to guide the topic propagation. The rules and conclusions found in these works are worthy of our reference in modeling the information diffusion process.

In view of the control of information diffusion process, scholars generally adopt the optimal control method, the pulse control method, the Top-K nodes influence method and so on, to control the spatiotemporal dynamic diffusion process of information in the network [33]. A number of papers [19], [34]–[37] proposed a defensive strategy to disseminate correct messages for combating the spread of malicious information. In [6], [34] it has been proven that the use of fixed costs to maximize the control of malicious information diffusion is an NP-hard problem. This conclusion leads the later researchers to explore the approximate optimal strategies for similar problems.

Inspired by the diffusion process of biological infectious diseases, Chen et al. [36] put forward a "vaccination" control strategy to control the diffusion of malicious information in a time-varying network. Thereafter, they designed a dynamic programming algorithm to minimize the cost of the control strategy, and obtained the distribution of the control signals over time. However, their work assumed that upon receiving information all users immediately participate in the information forwarding activities. They did not consider the time delay caused by the psychological cognition and the interactions between psychology and behavior of users. This results in the low accuracy of control measures.

Borrowing the idea from the control of infectious disease diffusion, Aung et al. [37] presented a method to control the malicious information dissemination in MSNs, and studied the adaptability and extensibility of the SIR model in MSNs. Their results show that the theory of infectious disease spread is effective for modeling and controlling the information diffusion process in MSNs. However, their work has not considered the problem of modeling the dynamics of malicious information diffusion and maximizing the utilization efficiency of system resources. Jeong et al. [35] modeled diffusion process of rumors in social networks by using the traditional infectious disease diffusion model. Considering that users have different interests in information at different times, they put forward three control strategies for rumors at different diffusion stages, and consider optimal control problems to minimize the number of spreaders. Their work takes into account the optimal control of rumors and saves control resources to a certain extent. However, they did not consider the spread characteristics of rumors on social networks, so they did not propose a new diffusion model. Moreover, the proposed control strategies can not be synergistically implemented at the same time, which limits the control effect to a certain extent.

To sum up, fraud information diffusion has become one of the major security threats faced by MSNs. Among the research effort, how to conduct accurate dynamics modeling and design optimal control method for fraud information diffusion are two important problems to be solved. Based on the above works, this paper combines the system dynamics modeling method and the optimal control theory, and studies the dynamics modeling and the optimal control problem of the fraud information diffusion in MSNs.

III. System Models

On the basis of the above descriptions, we first summarize the main challenges to effectively control the spread of fraud

information in MSNs as follows:

- How to establish an information diffusion model to accurately describe the dynamic diffusion process of fraud information in MSNs by considering the uncertain mental states of individuals?
- How to analyze the trend of information diffusion and the stability of the dynamics model from a theoretical point of view, and explore the theory of dynamic evolution of information diffusion model?
- How to determine the optimal distribution of the control strategies, and restrain the diffusion of fraud information under the minimum cost constraint?

To cope with the above three challenges, in this section, we first establish a dynamics model to describe the dynamic evolutionary process of fraud information diffusion in MSNs. Then, we derive the theoretical boundary conditions for persistent diffusion and automatic disappearance of fraud information, and analyze the characteristic solution of the dynamics model, which provide the basis for constructing the optimal control system for the fraud information diffusion in MSNs. Finally, we propose two synergistic control strategies to combat the spread of fraud information in the network, and derive the optimal dynamic allocation of the control strategies.

A. Information Diffusion Model

According to the theory of information cognitive psychology, when users receive a piece of information, they usually go through *thinking*, *trust* and *diffusion*, the three psychological cognitive and behavioral states [15], [16]. Suppose there are N nodes in the network region Θ of a MSN, and nodes can interact and communicate with each other. When fraud information is propagated within the network region Θ, we divide the nodes into four states according to the different situations of the nodes, which are whether the node has received fraud information or not, whether the node has believed fraud information or not, and whether the node has participated in the diffusion of the information or not. As shown in Table I, (1) the susceptible state (S) indicates that the nodes have not received any fraud information, but may be infected with fraud information by other nodes in the network; (2) the wandering state (W) indicates that the nodes have received the fraud information at present and are questioning the authenticity of the information. Such nodes neither believe in the fraud information nor engage in the diffusion of fraud information; (3) the infected state (I) indicates that the nodes believe the received fraud information and are misled by the fraud information to diffuse the information; (4) the recovery state (R) indicates that the nodes in this state no longer believe the fraud information and stop spreading the information. Furthermore, for the sake of clearer presentation, we briefly summarize the notations of the key parameters we will use in the following models (as shown in Table II).

Any node within the network region Θ must belong to one of four states at any time, and each node can be transformed among four states as time passes. Here we define the node state transition rules as follows:

TABLE I: Classification of node states.

Node state	Whether received fraud information	Whether believed fraud information	Whether diffused fraud information
S	No	No	No
W	Yes	Uncertainty	No
I	Yes	Yes	Yes
R	Yes	No	No

TABLE II: Notations in the information diffusion model.

Symbol	Description
α_0	The probability of state transfer occurring in W
β_0	The conditional probability of state transfer occurring in S when it receives the fraud information
θ	The conditional probability of W turning to I when state transfer occurs
ε	The conditional probability of S turning to W when state transfer occurs
ω_0	The conditional probability of I being cured or self reversed to R when it encounters R or I state node
γ_0	The probability of I transferred to R after self healing
ϕ_0	The probability of losing immunity of R
μ	The probability of nodes moving out of Θ
Λ	The number of nodes that are newly moved into Θ

- When the node in S state receives fraud information from nodes in I state, the node will make a state transition with probability β_0. It will either transfer to W state with probability $\varepsilon \times \beta_0$ and enter the process of wandering; or transfer to I state with probability $(1-\varepsilon)\beta_0$, believe the fraud information and participate in the diffusion of the information.
- The node in W state is in the process of thinking and judging the received fraud information. After a period of mental activity, the node will make a state transition with probability α_0. If the node believes the fraud information, it will transfer to I state with probability $\theta \times \alpha_0$, otherwise, it will transfer to R state with probability $(1-\theta)\alpha_0$.
- If the node in I state repeatedly receives the fraud information from other nodes in I state over a period of time, it is no longer willing to believe the fraud information because of its psychological aversion or antagonistic effect. Then, it will transfer to R state with probability ω_0.
- The node in I state contacts nodes in R state and receives the correct information sent by it, and then no longer believes the fraud information held by itself. It will transfer to R state with probability ω_0.
- After a period of time, the node in I state may become aware of the harm of the fraud information, and thus no longer believes the fraud information. Then, it will transfer to R state with probability γ_0.
- After a period of time, a node in R state will gradually lose the awareness of fraud information due to its forgetting psychology, it may be infected again by fraud information in the future. Then, it will transfer to S state with probability ϕ_0.

We have $\beta_0, \varepsilon, \alpha_0, \theta, \omega_0, \gamma_0, \phi_0 \in [0,1]$. In addition, we use $S(t), W(t), I(t), R(t)$ to represent the number of nodes

in S, W, I, R state at any time t, respectively, and use $N(t)$ to represent the total number of nodes within the network region Θ at any time t . Obviously, we have $S(t)+W(t)+I(t)+R(t)=N(t)$. Due to node's activity and the openness of the network, we assume that nodes in various states may leave the network region Θ with probability μ at any time t. At the same time, there are Λ nodes from outside extending the network region Θ at any time t, and we assume that the incoming nodes belong to S state. Accordingly, node states transition relationships in Θ are shown in Fig. 1.

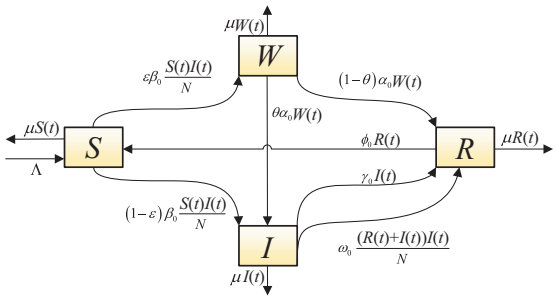


Fig. 1: Node state transition diagram.

Based on the relationships of node state transition proposed above, we can establish the mean field equations for the number of nodes $S(t), W(t), I(t)$ and $R(t)$ as follows:

$$\frac{dS(t)}{dt}=\Lambda+\phi_0 R(t)-\beta_0\frac{S(t)I(t)}{N(t)}-\mu S(t), \tag{1}$$

$$\frac{dW(t)}{dt}=\varepsilon\beta_0\frac{S(t)I(t)}{N(t)}-\alpha_0 W(t)-\mu W(t), \tag{2}$$

$$\begin{aligned}\frac{dI(t)}{dt}=&(1-\varepsilon)\beta_0\frac{S(t)I(t)}{N(t)}+\theta\alpha_0 W(t)-\gamma_0 I(t)\\&-\omega_0\frac{[R(t)+I(t)]I(t)}{N(t)}-\mu I(t),\end{aligned} \tag{3}$$

$$\begin{aligned}\frac{dR(t)}{dt}=&(1-\theta)\alpha_0 W(t)+\gamma_0 I(t)-\phi_0 R(t)\\&+\omega_0\frac{[R(t)+I(t)]I(t)}{N(t)}-\mu R(t).\end{aligned} \tag{4}$$

Eqs. (1)-(4) constitute a nonlinear dynamics system model, and the initial values of the model are defined as:

$$S(0)\geq 0,\ W(0)\geq 0,\ I(0)\geq 0,\ R(0)\geq 0. \tag{5}$$

The total number of nodes $N(t)$ varying over time in the network Θ is as follows:

$$\frac{\mathrm{d}N(t)}{dt}=\Lambda-\mu N(t). \tag{6}$$

By solving Eq. (6), we have $N(t)=N(0)\mathrm{e}^{-t}+\frac{\Lambda}{\mu}$ and $\lim_{t\to+\infty}N(t)=\frac{\Lambda}{\mu}$. It can be seen that the total number of nodes $N(t)$ tends to be stable at $t\to\infty$, that is, the maximum node capacity of the network is $\frac{\Lambda}{\mu}$. Let $s(t)=\frac{S(t)}{N(t)}$, $w(t)=\frac{W(t)}{N(t)}$, $i(t)=\frac{I(t)}{N(t)}$ and $r(t)=\frac{R(t)}{N(t)}$. As such, $s(t)$, $w(t)$, $i(t)$ and $r(t)$ refer to the proportions of nodes in S, W, I and R state, respectively. Thereafter, let $\tau=\mu t$, $\beta=\frac{\beta_0}{\mu}$, $\alpha=\frac{\alpha_0}{\mu}$, $\omega=\frac{\omega_0}{\mu}$, $\gamma=\frac{\gamma_0}{\mu}$, $\phi=\frac{\phi_0}{\mu}$, and $s(\tau)$, $w(\tau)$, $i(\tau)$, $r(\tau)$ satisfy the following differential equations:

$$\frac{ds(\tau)}{d\tau}=1+\phi r(\tau)-\beta s(\tau)i(\tau)-s(\tau), \tag{7}$$

$$\frac{dw(\tau)}{d\tau}=\varepsilon\beta s(\tau)i(\tau)-\alpha w(\tau)-w(\tau), \tag{8}$$

$$\begin{aligned}\frac{di(\tau)}{d\tau}=&(1-\varepsilon)\beta s(\tau)i(\tau)+\theta\alpha w(\tau)-\gamma i(\tau)\\&-\omega(r(\tau)+i(\tau))i(\tau)-i(\tau),\end{aligned} \tag{9}$$

$$\begin{aligned}\frac{dr(\tau)}{d\tau}=&(1-\theta)\alpha w(\tau)+\omega(r(\tau)+i(\tau))i(\tau)\\&+\gamma i(\tau)-\phi r(\tau)-r(\tau).\end{aligned} \tag{10}$$

Eqs. (7)-(10) constitute a nonlinear dynamics system model, called $SWIR$ model. We have $s(\tau)+w(\tau)+i(\tau)+r(\tau)=1$, and it satisfies the initial conditions:

$$s(0)\geq 0; w(0)\geq 0; i(0)\geq 0; r(0)\geq 0. \tag{11}$$

Next, we replace τ with t, and make $r(t)=1-s(t)-w(t)-i(t)$. We simplify the set of differential equations Eqs. (7)-(10) as follows:

$$\begin{cases}\dfrac{ds(t)}{dt}=&1+\phi(1-s(t)-w(t)-i(t))\\&-\beta s(t)i(t)-s(t)\\ \dfrac{dw(t)}{dt}=&\varepsilon\beta s(t)i(t)-\alpha w(t)-w(t)\\ \dfrac{di(t)}{dt}=&(1-\varepsilon)\beta s(t)i(t)+\theta\alpha w(t)-\gamma i(t)\\&-\omega(1-s(t)-w(t))i(t)-i(t)\end{cases} \tag{12}$$

We define the feasible region of Eq. (12) as Ω, indicating the non-negative cone and its lower dimensional face. We study Eq. (12) in $A=\{(s(t),w(t),i(t))\in\Omega\,|0\leq s(t)+w(t)+i(t)\leq 1\}$. Obviously, A is positively invariant with respect to Eq. (12). Then, let the value of each differential equation in Eq. (12) equal to 0, that is, the system is in a stable state, we have:

$$\begin{cases}\dfrac{ds(t)}{dt}=&1+\phi(1-s(t)-w(t)-i(t))\\&-\beta s(t)i(t)-s(t)=0\\ \dfrac{dw(t)}{dt}=&\varepsilon\beta s(t)i(t)-\alpha w(t)-w(t)=0\\ \dfrac{di(t)}{dt}=&(1-\varepsilon)\beta s(t)i(t)+\theta\alpha w(t)-\gamma i(t)\\&-\omega(1-s(t)-w(t))i(t)-i(t)=0\end{cases} \tag{13}$$

By solving Eq.(13), the equilibrium points of Eq. (12) can be obtained, which are $P_0(1,0,0)$ and $P^*(s^*,w^*,i^*)$. Here, in order to simplify the expression, let's make:

$$\begin{aligned}a=&(1-\varepsilon)(\phi d+\beta)(\beta+\omega+\theta\alpha d)-(1+\phi)\omega d,\\ b=&(1-\varepsilon)\phi\beta+\phi\theta\alpha d+\omega\phi+(1+\phi)\omega d,\\&-(\omega+\gamma+1)(\phi d+\beta)\\ c=&-\phi(\omega+\gamma+1),\\ d=&\frac{\varepsilon\beta}{\alpha+1}.\end{aligned}$$

Then we can get $P^*(s^*, w^*, i^*)$ as follows:

$$\begin{cases} s^* = \dfrac{-b+\sqrt{b^2-4ac}}{2a} \\ w^* = \dfrac{\varepsilon\beta s^*(1+\phi)(1-s^*)}{\phi\varepsilon\beta s^* + (\phi+\beta s^*)(\alpha+1)} \\ i^* = \dfrac{(\alpha+1)(1+\phi)(1-s^*)}{\phi\varepsilon\beta s^* + (\phi+\beta s^*)(\alpha+1)} \end{cases}$$

Obviously, P_0 is a disease-free equilibrium of Eq. (12), and P^* is a endemic equilibrium of Eq. (12) [38].

Without loss of generality, we assume $K = (w, i, s)^T$, then Eq. (12) can be rewritten as:

$$\frac{dK}{dt} = F(Z) - V(Z), \tag{14}$$

in which:

$$F(Z) = \begin{pmatrix} \varepsilon\beta si \\ 0 \\ 0 \end{pmatrix},$$

$$V(Z) = \begin{pmatrix} \alpha w + w \\ (\varepsilon-1)\beta si - \theta\alpha w + \omega(1-s-w)i + \gamma i + i \\ -1 - \phi(1-s-w-i) + \beta si + s \end{pmatrix}.$$

The disease-free equilibrium of K about Eq. (12) is $K_0 = (w_0, i_0, s_0)^T = (0, 0, 1)^T$. Let $DF(Z_0)$ and $DV(Z_0)$ be:

$$DF(Z_0) = \begin{pmatrix} F_1 & 0 \\ 0 & 0 \end{pmatrix},\ DV(Z_0) = \begin{pmatrix} V_1 & 0 \\ J_1 & J_2 \end{pmatrix},$$

where F_1 and V_1 are the 2×2 matrix. Because $w(t)$ and $i(t)$ are the proportions of wandering state nodes and infected state nodes respectively, so we define:

$$F_1 = \left(\frac{\partial F_i(Z_0)}{\partial Z_j}\right),\ V_1 = \left(\frac{\partial V_i(Z_0)}{\partial Z_j}\right),$$

where $i = 1, 2;\ j = 1, 2$. By solving the above formulas, we can further obtain that:

$$F_1 = \begin{pmatrix} 0 & \varepsilon\beta \\ 0 & 0 \end{pmatrix},\ V_1 = \begin{pmatrix} \alpha+1 & 0 \\ -\theta\alpha & (\varepsilon-1)\beta+\gamma+1 \end{pmatrix}.$$

Considering that V_1 is a nonsingular matrix, we have:

$$F_1 {V_1}^{-1} = \begin{pmatrix} \dfrac{\theta\alpha\varepsilon\beta}{(\varepsilon\beta-\beta+\gamma+1)(\alpha+1)} & \dfrac{\varepsilon\beta}{(\varepsilon-1)\beta+\gamma+1} \\ 0 & 0 \end{pmatrix}$$

Therefore, we can further define the basic reproduction number of Eq. (12) as:

$$R_0 = \rho\left(F_1 {V_1}^{-1}\right) = \frac{\theta\alpha\varepsilon\beta}{(\varepsilon\beta-\beta+\gamma+1)(\alpha+1)}.$$

in which $\rho\left(F_1 {V_1}^{-1}\right)$ is the spectral radius of $F_1 {V_1}^{-1}$. The basic reproduction number R_0 of Eq. (12) is closely related to the stability of equilibrium point [38], and we will analyze it in detail in the following Section.

B. System Stability Analysis

By analyzing the stability of the equilibrium point of Eq. (12), we can accurately predict the future diffusion trend of fraud information in the network [38]. If the disease-free equilibrium $P_0(1, 0, 0)$ in Eq. (12) is stable, the diffusion of fraud information will finally die out; if the endemic equilibrium $P^*(s^*, w^*, i^*)$ in Eq. (12) is stable, the fraud information will continuously propagates and the number of nodes in infected state will finally reach a constant level.

First, we analyze the stability of the $P_0(1, 0, 0)$ in Eq. (12). We have the following conclusion:

Theorem 1. *The disease-free equilibrium $P_0(1, 0, 0)$ of Eq. (12) is globally stable in the range of set A if and only if the $R_0 \le 1$. If $R_0 > 1$, $P_0(1, 0, 0)$ is unstable in the range of set A, and the solutions of Eq. (12) starting sufficiently close to $P_0(1, 0, 0)$ in A move away from $P_0(1, 0, 0)$ except that those starting on invariant x-axis approach $P_0(1, 0, 0)$ along this axis.*

Proof. We first construct an auxiliary Lyapunov equation as follows:

$$L = \frac{\theta}{\alpha+1}w + \frac{1}{\alpha}i. \tag{15}$$

Substituting $\frac{ds(t)}{dt}$ and $\frac{di(t)}{dt}$ of Eq. (12) into the above equation, the derivative equation about the solutions of Eq. (12) can be obtained as follows:

$$\begin{aligned} L' =& \frac{-(\alpha+1)\left[(\varepsilon-1)\beta s + \gamma + \omega(1-s-w) + 1\right] i}{\alpha(\alpha+1)} \\ &+ \frac{\alpha\theta\varepsilon\beta si}{\alpha(\alpha+1)} \\ \le& \frac{\left[\alpha\theta\varepsilon\beta - (\alpha+1)(\varepsilon\beta-\beta+\gamma+1)\right] si}{\alpha(\alpha+1)} \\ =& \frac{(\varepsilon\beta-\beta+\gamma+1)(R_0-1)si}{\alpha} \le 0. \end{aligned} \tag{16}$$

From Eq. (16), we can obtain that if and only if $w = 0$ and $i = 0$, L' takes the maximum value as 0 when $R_0 \le 1$. The maximum invariant set in $\{(s, w, i) : L' = 0\}$ is the $\{P_0(1, 0, 0)\}$. When $R_0 \le 1$, the global stability of the $P_0(1, 0, 0)$ follows the LaSalle invariance principle [39]. □

Then, we analyze the stability of the $P^*(s^*, w^*, i^*)$ in Eq. (12). We have the following conclusion:

Theorem 2. *If $R_0 > 1$, the endemic equilibrium $P^*(s^*, w^*, i^*)$ of Eq. (12) is locally asymptotically stable.*

Proof. First, we construct the following equation. It is worth noting that we omit the (t) in the equation for the sake of conveniently formulation.

$$\begin{cases} f(s, w, i) = \dfrac{ds}{dt} = 1 + \phi(1-s-w-i) \\ \qquad\qquad - \beta si - s \\ g(s, w, i) = \dfrac{dw}{dt} = \varepsilon\beta si - \alpha w - w \\ h(s, w, i) = \dfrac{di}{dt} = (1-\varepsilon)\beta si + \theta\alpha w \\ \qquad\qquad - \omega(1-s-w)i - \gamma i - i \end{cases} \tag{17}$$

By expanding $f(s,w,i)$, $g(s,w,i)$, $h(s,w,i)$ in a Taylor series at $P^*(s^*,w^*,i^*)$, then we can obtain the linear approximation equation of Eq. (12) as follows:

$$\begin{cases} \dfrac{ds}{dt} = f_s(s^*,w^*,i^*)\,s + f_w(s^*,w^*,i^*)\,w \\ \qquad\quad + f_i(s^*,w^*,i^*)\,i \\ \dfrac{dw}{dt} = g_s(s^*,w^*,i^*)\,s + g_w(s^*,w^*,i^*)\,w \\ \qquad\quad + g_i(s^*,w^*,i^*)\,i \\ \dfrac{di}{dt} = h_s(s^*,w^*,i^*)\,s + h_w(s^*,w^*,i^*)\,w \\ \qquad\quad + h_i(s^*,w^*,i^*)\,i \end{cases} \tag{18}$$

Substituting $s(t), w(t), i(t)$ of Eq.(12) into the above equation, we have:

$$\begin{cases} \dfrac{ds}{dt} = (-\beta i^* - \phi - 1)\,s + (-\phi)\,w \\ \qquad\quad + (-\beta s^* - \phi)\,i \\ \dfrac{dw}{dt} = (\varepsilon\beta i^*)\,s + (-\alpha - 1)\,w + (\varepsilon\beta s^*)\,i \\ \dfrac{di}{dt} = [(1-\varepsilon)\,\beta i^* + \omega i^*]\,s + (\theta\alpha + \omega i^*)\,w \\ \qquad + [(1-\varepsilon)\,\beta s^* + \omega s^* + \omega w^* - \omega - \gamma - 1]\,i \end{cases} \tag{19}$$

Furthermore, we derive Jacobian matrix $J(P^*)$ of the approximate linear system (19) at $P^*(s^*,w^*,i^*)$ as follows:

$$J(P^*) = \begin{pmatrix} -\beta i^* - \phi - 1 & -\phi & -\beta s^* - \phi \\ \varepsilon\beta i^* & -\alpha - 1 & \varepsilon\beta s^* \\ (1-\varepsilon)\,\beta i^* + \omega i^* & \theta\alpha + \omega i^* & e \end{pmatrix}, \tag{20}$$

where:

$$\begin{aligned} &s^* = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, w^* = \frac{\varepsilon\beta s^*(1+\phi)(1-s^*)}{\phi\varepsilon\beta s^* + (\phi + \beta s^*)(\alpha+1)}, \\ &i^* = \frac{(\alpha+1)(1+\phi)(1-s^*)}{\phi\varepsilon\beta s^* + (\phi + \beta s^*)(\alpha+1)}, \\ &a = (1-\varepsilon)(\phi d + \beta)(\beta + \omega + \theta\alpha d) - (1+\phi)\,\omega d, \\ &b = (1-\varepsilon)\,\phi\beta + \phi\theta\alpha d + \omega\phi + (1+\phi)\,\omega d \\ &\quad - (\omega + \gamma + 1)(\phi d + \beta), \\ &c = -\phi(\omega + \gamma + 1),\ d = \frac{\varepsilon\beta}{\alpha+1}, \\ &e = (1-\varepsilon)\,\beta s^* + \omega s^* + \omega w^* - \omega - \gamma - 1. \end{aligned}$$

Let characteristic equation $|\lambda E - J(P^*)| =$

$$\begin{vmatrix} \lambda + \beta i^* + \phi + 1 & \phi & \beta s^* + \phi \\ -\varepsilon\beta i^* & \lambda + \alpha + 1 & -\varepsilon\beta s^* \\ -(1-\varepsilon)\,\beta i^* - \omega i^* & -\theta\alpha - \omega i^* & \lambda - e \end{vmatrix} = 0\ ,$$

in which E is a 3×3 unit matrix. By simplifying the above equations, we have:

$$|\lambda E - J(P^*)| = \lambda^3 + A_1\lambda^2 + A_2\lambda + A_3 = 0,$$

where:

$$\begin{aligned} A_1 &= B - D + \alpha + 1, \\ A_2 &= B - D - \beta D + \beta\alpha - D\alpha - C\phi - C\beta s^* + \beta\varepsilon\phi i^* \\ &\quad - \alpha\beta\theta\varepsilon s^* - \beta\varepsilon\omega s^* i^*, \\ A_3 &= -C\phi - C\alpha\phi - \beta(D + D\alpha + Cs^* + C\alpha s^*) \\ &\quad + \varepsilon\phi\beta\left(\omega {i^*}^2 + \alpha\theta i^* - Cs^* - Di^*\right) \\ &\quad + \varepsilon\beta^2 s^*\left(\omega {i^*}^2 + \alpha\theta i^* - \alpha\theta - \omega i^*\right), \\ B &= \beta i^* + \phi + 1, C = -(1-\varepsilon)\,\beta i^* - \omega i^*, \\ D &= (1-\varepsilon)\,\beta s^* + \omega s^* + \omega w^* - \omega - \gamma - 1. \end{aligned}$$

Further, we can obtain $A_1A_2 - A_3 > 0$. According to the Routh-Hurwitz stability criterion [40], the $P^*(s^*,w^*,i^*)$ of Eq. (12) has local asymptotic stability. □

C. Optimal control strategies

Next, we show how to efficiently utilize limited control resources and minimize losses of individuals caused by the diffusion of fraud information. First of all, we propose the following two synergistic control strategies for fraud information diffusion, which can assist individuals in different states to achieve better control effect.

- **Prevention**: we take proactive measures of providing immunity for the nodes in the W state. For instance, by sending volunteers to communicate, persuade and educate, some nodes will not believe in the received fraud information, and transfer to the R state with probability σ. The intensity of the implementation of the prevention control strategy is denoted as $u(t)$.
- **Correction**: we take proactive measures of treatment for the nodes in the I state. By publishing authoritative information in MSNs, some nodes in the I state will no longer believe the received fraud information, and transfer to the R state with probability η. The intensity of the implementation of the correction control strategy is represented as $v(t)$.

Through the artificial intervention of the above control strategies, if the $SWIR$ model has a disease-free equilibrium and it is stable, we can accelerate the extinction time of fraud information in the network. If the $SWIR$ model has an endemic equilibrium and it is stable, we can promote the extinction of fraud information in the network.

According to the control strategies proposed above, we improve the $SWIR$ model as $controlled - SWIR$ model:

$$\begin{cases} \dfrac{ds(t)}{dt} = 1 + \phi r(t) - \beta s(t)\,i(t) - s(t) \\ \dfrac{dw(t)}{dt} = \varepsilon\beta s(t)\,i(t) - \alpha w(t) - w(t) - \sigma u(t)\,w(t) \\ \dfrac{di(t)}{dt} = (1-\varepsilon)\,\beta s(t)\,i(t) + \theta\alpha w(t) - \gamma i(t) \\ \qquad\quad - \omega[r(t) + i(t)]\,i(t) - i(t) - \eta v(t)\,i(t) \\ \dfrac{dr(t)}{dt} = (1-\theta)\,\alpha w(t) + \omega[r(t) + i(t)]\,i(t) \\ \qquad\quad + \gamma i(t) - \phi r(t) - r(t) + \sigma u(t)\,w(t) \\ \qquad\quad + \eta v(t)\,i(t) \end{cases} \tag{21}$$

Obviously, the system (21) has the same initial condition (11) as the above $SWIR$ model, and has the following boundary conditions of control strategies:

$$0 \leq u(t) \leq u_{\max},\ 0 \leq v(t) \leq v_{\max}. \tag{22}$$

Among them, $u_{\max}$ and $v_{\max}$ represent the upper bound of control strategies $u(t)$ and $v(t)$ respectively, and $0 \leq u_{\max} \leq 1,\ 0 \leq v_{\max} \leq 1$. Besides, we assume $u(t)$ and $v(t)$ are convex functions.

We hope that fewer users in the network are infected by fraud information. We assume that the loss caused by fraud information to the system is proportional to the proportions of nodes in I state, and the benefit of the system is proportional to the proportion of nodes in R and S states. In other words, the larger $i(t)$, the more nodes that were affected by fraud information and the greater the system losses. On the contrary, the larger $r(t)$and $s(t)$, the more nodes in the system not harmed by the fraud information and the greater benefit of the system. Additionally, suppose that the control resources consumption for implementing control strategies of $u(t)$ and $v(t)$ are $mu^2(t)$ and $nv^2(t)$ at any time t, respectively, where m and n are positive constants. Note that, we do not impose a strong assumption on the quadratic form of control resources consumption since any other form of convex function could also be used here to derive the solution. It is assumed that all losses, benefits and control resources consumption can be accumulated over the entire period of time $[0, T]$, and we define the cumulative total cost function of the system as:

$$\begin{aligned} J(u(t), v(t)) = \int_0^T & [qi(t) + mu^2(t) + nv^2(t) \\ & - ps(t) - pr(t)]\, dt. \end{aligned} \tag{23}$$

Among them, q and p are positive constants, which represent the losses of individuals in I state and the system benefits of individuals in R or S states, respectively. Because $u(t)$ and $v(t)$ are convex functions, here we assume $J(u(t), v(t))$ is convex function.

As such, within the entire control time $[0, T]$, the ultimate objective of the optimal control system is that the fraud information in the network is completely controlled and the cumulative total cost of the system is minimal. Thus, we explore the optimal distribution of control strategies $u^*(t)$ and $v^*(t)$ over time, which satisfy:

$$J(u^*(t), v^*(t)) = \min\left[J(u(t), v(t)) \,|(u(t), v(t)) \in U\right], \tag{24}$$

where $U = \{u(t), v(t) \,|0 \leq u(t) \leq u_{\max},\ 0 \leq v(t) \leq v_{\max}\}$.

Then, we introduce the optimal control theory [41] to analyze the existence and uniqueness of the solution of the $controlled - SWIR$ system. We have:

Theorem 3. *For the $controlled - SWIR$ system (21) with given initial condition, there exists a optimal distribution of the control strategies $u^*(t), v^*(t)$ such that $J(u^*(t), v^*(t)) = \min\left[J(u(t), v(t)) \,|(u(t), v(t)) \in U\right]$ in a time step $[0, \tau]$.*

Theorem 4. *For a time step $[0, \tau]$, the optimal distribution of control strategies $u^*(t), v^*(t)$ satisfying the $J(u^*(t), v^*(t)) = \min\left[J(u(t), v(t)) \,|(u(t), v(t)) \in U\right]$ is unique.*

The detailed proof of Theorem 3 and Theorem 4 can be easily found in [41], we will not provide in this paper. Next, we use the optimal control theory to solve the optimal distribution of the control strategies $u^*(t), v^*(t)$ and the distribution of the corresponding system state variables $s^*(t), w^*(t), i^*(t)$ and $r^*(t)$. First, we construct a Lagrangian equation L for solving the optimal solution of the problem (24) as follows:

$$L = qi(t) + mu^2(t) + nv^2(t) - ps(t) - pr(t). \tag{25}$$

Furthermore, we transfer the problem (24) into finding the minimal value of the Lagrangian equation L. Accordingly, we define the Hamiltonian function H for the problem (24) as follows:

$$\begin{aligned} H = & L + \lambda_s(t)\frac{ds(t)}{dt} + \lambda_w(t)\frac{dw(t)}{dt} + \lambda_i(t)\frac{di(t)}{dt} \\ & + \lambda_r(t)\frac{dr(t)}{dt}, \end{aligned} \tag{26}$$

where $\lambda_s(t), \lambda_w(t), \lambda_i(t), \lambda_r(t)$ are the adjoint functions to be determined appropriately. Assuming that $\lambda_s^*(t), \lambda_w^*(t), \lambda_i^*(t), \lambda_r^*(t)$ are the values of adjoint equations $\lambda_s(t), \lambda_w(t), \lambda_i(t), \lambda_r(t)$ at the optimal solution of $u^*(t), v^*(t)$. Substituting (21) and (25) to (26), we have:

$$\begin{aligned} H = & qi(t) + mu^2(t) + nv^2(t) - ps(t) - pr(t) + \lambda_s(t) \\ & \times [1 + \phi r(t) - \beta s(t) i(t) - s(t)] + \lambda_w(t) \\ & \times [\varepsilon\beta s(t) i(t) - \alpha w(t) - w(t) - \sigma u(t) w(t)] \\ & + \lambda_i(t)[(1-\varepsilon)\beta s(t) i(t) + \theta\alpha w(t) - \omega(r(t) \\ & + i(t))i(t) - \gamma i(t) - i(t) - \eta v(t) i(t)] \\ & + \lambda_r(t)[(1-\theta)\alpha w(t) + \omega(r(t) + i(t)) i(t) \\ & + \gamma i(t) - (\phi+1) r(t) + \sigma u(t) w(t) + \eta v(t) i(t)]. \end{aligned} \tag{27}$$

After that, we use the the Pontryagin minimum principle to solve the optimal solution of the problem (24) [42]. It is assumed that the set of optimal solutions satisfying the system (21) at time t is $M = [s^*(t), w^*(t), i^*(t), r^*(t), u^*(t), v^*(t), \lambda_s^*(t), \lambda_w^*(t), \lambda_i^*(t), \lambda_r^*(t)]$. There must be a non-trivial vector function $\lambda(t) = [\lambda_s(t), \lambda_w(t), \lambda_i(t), \lambda_r(t)]$ of M that satisfies the following conditions:

$$\frac{dk(t)}{dt} = \frac{\partial H[k^*(t), l^*(t), \lambda(t), t]}{\partial \lambda}, \tag{28}$$

$$\frac{\partial H[k^*(t), l^*(t), \lambda(t), t]}{\partial l} = 0, \tag{29}$$

$$\frac{d\lambda(t)}{dt} = -\frac{\partial H[k^*(t), l^*(t), \lambda(t), t]}{\partial k}, \tag{30}$$

where $k(t) \in \{s(t), w(t), i(t), r(t)\}$, $k^*(t) \in \{s^*(t), w^*(t), i^*(t), r^*(t)\}$, $l(t) \in \{u(t), v(t)\}$, $l^*(t) \in \{u^*(t), v^*(t)\}$.

According to the condition Eq. (30) and the Hamiltonian function Eq. (26), we can obtain the adjoint functions of the system as follows:

$$\begin{aligned} \frac{d\lambda_s^*(t)}{dt} = & -\frac{\partial H}{\partial s(t)} = p - (-\beta i(t) - 1)\lambda_s^*(t) \\ & - \varepsilon\beta i(t)\lambda_w^*(t) - (1-\varepsilon)\beta i(t)\lambda_i^*(t), \end{aligned} \tag{31}$$

$$\begin{aligned}\frac{d\lambda_w^*(t)}{dt} =& -\frac{\partial H}{\partial w(t)} = (\alpha+1+\sigma u(t))\lambda_w^*(t) \\ &- \theta\alpha\lambda_i^*(t) - [(1-\theta)\alpha+\sigma u(t)]\lambda_r^*(t),\end{aligned} \tag{32}$$

$$\begin{aligned}\frac{d\lambda_i^*(t)}{dt} =& -\frac{\partial H}{\partial i(t)} = -q+\beta s(t)\lambda_s^*(t) - \varepsilon\beta s(t)\lambda_w^*(t) \\ &- [(1-\varepsilon)\beta s(t) - \omega r(t) - 2\omega i(t) - \gamma - 1 \\ &- \eta v(t)]\lambda_i^*(t) - (\omega r(t) + 2\omega i(t) + \gamma \\ &+ \eta v(t))\lambda_r^*(t),\end{aligned} \tag{33}$$

$$\begin{aligned}\frac{d\lambda_r^*(t)}{dt} =& -\frac{\partial H}{\partial r(t)} = p - \phi\lambda_s^*(t) + \omega i(t)\lambda_i^*(t) \\ &- (\omega i(t) - \phi - 1)\lambda_r^*(t),\end{aligned} \tag{34}$$

When $t = T$, the boundary conditions of the system (31) - (34) are:

$$\lambda_s^*(T) = \lambda_w^*(T) = \lambda_i^*(T) = \lambda_r^*(T) = 0. \tag{35}$$

Further, according to Eq. (26) and Eq. (29), we can derive the following equations:

$$\frac{\partial H}{\partial u(t)} = 2mu^*(t) + (\lambda_r^*(t) - \lambda_w^*(t))\sigma w^*(t) = 0, \tag{36}$$

$$\frac{\partial H}{\partial v(t)} = 2nv^*(t) + (\lambda_r^*(t) - \lambda_i^*(t))\eta i^*(t) = 0. \tag{37}$$

Considering the bound property on $u^*(t)$ and $v^*(t)$, from Eq. (36) and Eq. (37), we can obtain the optimal distribution of the control strategies $u^*(t)$ and $v^*(t)$ over time t as follows:

$$u^*(t) = \begin{cases} 0 & if\ \psi_1 < 0 \\ u_{\max} & if\ \psi_1 > u_{\max} \\ \psi_1 & otherwise, \end{cases} \tag{38}$$

$$v^*(t) = \begin{cases} 0 & if\ \psi_2 < 0 \\ v_{\max} & if\ \psi_2 > v_{\max} \\ \psi_2 & otherwise, \end{cases} \tag{39}$$

in which $\psi_1 = (\lambda_w^*(t) - \lambda_r^*(t))\sigma w^*(t)/2m$, $\psi_2 = (\lambda_i^*(t) - \lambda_r^*(t))\eta i^*(t)/2n$.

Then, we rewrite the expressions of $u^*(t)$ and $v^*(t)$:

$$u^*(t) = \max\{\min\{\psi_1, u_{\max}\}, 0\}, \tag{40}$$

$$v^*(t) = \max\{\min\{\psi_2, v_{\max}\}, 0\}. \tag{41}$$

Finally, combining Eq. (40), Eq. (41), $controlled-SWIR$ model (21) and adjoint functions Eqs. (31) - (34), we obtain the optimal control system for fraud information in MSNs as follows:

$$\frac{ds(t)}{dt} = 1 + \phi r(t) - \beta s(t) i(t) - s(t), \tag{42}$$

$$\begin{aligned}\frac{dw(t)}{dt} =& \varepsilon\beta s(t) i(t) - \alpha w(t) - w(t) \\ &- \sigma w(t)\max\{\min\{\psi_1, u_{\max}\}, 0\},\end{aligned} \tag{43}$$

$$\begin{aligned}\frac{di(t)}{dt} =& (1-\varepsilon)\beta s(t) i(t) + \theta\alpha w(t) - \gamma i(t) \\ &- i(t) - \eta i(t)\max\{\min\{\psi_2, v_{\max}\}, 0\} \\ &- \omega(r(t) + i(t)) i(t),\end{aligned} \tag{44}$$

$$\begin{aligned}\frac{dr(t)}{dt} =& (1-\theta)\alpha w(t) + \omega(r(t) + i(t)) i(t) + \gamma i(t) \\ &- r(t) + \sigma w(t)\max\{\min\{\psi_1, u_{\max}\}, 0\} \\ &- \phi r(t) + \eta i(t)\max\{\min\{\psi_2, v_{\max}\}, 0\},\end{aligned} \tag{45}$$

$$\begin{aligned}\frac{d\lambda_s^*(t)}{dt} =& p - (-\beta i(t) - 1)\lambda_s^*(t) - \varepsilon\beta i(t)\lambda_w^*(t) \\ &- (1-\varepsilon)\beta i(t)\lambda_i^*(t),\end{aligned} \tag{46}$$

$$\begin{aligned}\frac{d\lambda_w^*(t)}{dt} =& (w(t) + 1 + \sigma\max\{\min\{\psi_1, u_{\max}\}, 0\}) \\ &\times \lambda_w^*(t) - \theta\alpha\lambda_i^*(t) - [(1-\theta)\alpha \\ &+ \sigma\max\{\min\{\psi_1, u_{\max}\}, 0\}]\lambda_r^*(t),\end{aligned} \tag{47}$$

$$\begin{aligned}\frac{d\lambda_i^*(t)}{dt} =& -q + \lambda_s^*(t)\beta s(t) - \varepsilon\beta s(t)\lambda_w^*(t) - [(1-\varepsilon) \\ &\times \beta s(t) - \omega r(t) - \eta\max\{\min\{\psi_2, v_{\max}\}, 0\} \\ &- 2\omega i(t) - \gamma - 1]\lambda_i^*(t) - (\omega r(t) + 2\omega i(t) \\ &+ \gamma + \eta\max\{\min\{\psi_2, v_{\max}\}, 0\})\lambda_r^*(t),\end{aligned} \tag{48}$$

$$\begin{aligned}\frac{d\lambda_r^*(t)}{dt} =& p - \phi\lambda_s^*(t) + \omega i(t)\lambda_i^*(t) \\ &- (\omega i(t) - \phi - 1)\lambda_r^*(t).\end{aligned} \tag{49}$$

Eqs. (42) - (49) constitute the optimal control system, the system has boundary conditions Eq. (11), Eq. (22) and Eq.(35)

IV. Simulation Results

In this section, we verify the effectiveness of the proposed information diffusion model and the correctness of the stability analysis theory firstly. Secondly, we use the iterative method with a Runge-Kutta fourth order scheme to solve the optimal dynamic allocation of control strategies and the cumulative total cost of the system in the case of different control strategies being implemented [43].

In addition, in order to verify efficiency and practicality of our proposed control strategies, we compare the effect of the control strategies to fraud information diffusion on the synthetic datasets and the real social network datasets, respectively. The real social network datasets we used are the Twitter datasets collected by Arizona State University, which record the information interaction of nodes on the Twitter network [44]. The datasets consist of two parts, the first part is the set of nodes, including the attributes of all nodes, and the second part is the set of node interaction records, which records all information exchanges among all nodes. The original datasets contain more than 11 million nodes and 85 million relations. Because of the limited storage capacity and computing resources, we randomly chose one hundred thousand nodes (ID from 371408 to 471407) and their interaction records to carry out our experiments. Through 500 experiments shown in the Fig. 2, we verify the randomness and universality of the nodes we choose.

Considering the practical significance of the parameters used in the simulations, we randomly set the default values for the basic parameters, as shown in Table III. Note that we set q much larger than m and n because we consider that the loss caused by fraud information to an infected individual

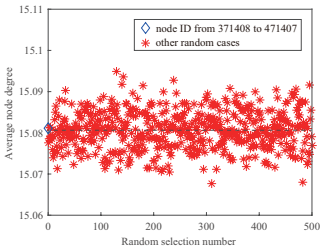


Fig. 2: Random experiments on node selection.

is much more expensive than taking the corresponding control strategy. The synthetic datasets we use is a randomly generated network whose parameters are derived from Table III.

TABLE III: Basic parameters in our simulations.

Parameter	Description	Value
Λ	The number of adding into individuals	100
μ	The rate of moving out individuals	0.1
u_{1max}	The upper bound of $u(t)$	1
v_{2max}	The upper bound of $v(t)$	1
σ	The probability of prevention	0.9
η	The probability of correction	0.9
q	The system loss weight caused by an infected individual	20
p	The system income weight caused by a susceptible or recovered individual	0.2
m	The cost weight of conducting the prevention strategy	0.6
n	The cost weight of conducting the correction strategy	0.8

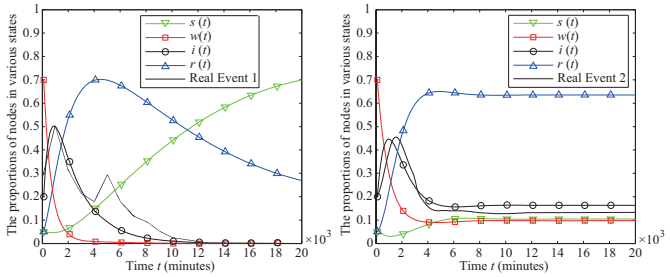
A. Diffusion model validation

In order to validate the correctness of the dynamic evolutionary process and stability analysis theory of the fraud information diffusion model, we simulate the proposed model in two scenarios with different information diffusion capabilities. According to the two real events (we will introduce them later), some reasonable node state transition probabilities and scenario parameter values that we fit are shown as follows:

- **Scenario 1:** We set parameters $\beta_0 = 0.1$, $\alpha_0 = 0.16$, $\gamma_0 = 0.05$, $\phi_0 = 0.01$, $\varepsilon = 0.9$, $\theta = 0.9$. Then $R_0 = 0.356$. We test the temporal evolution of the proportions of various state nodes in the presence of disease-free equilibrium in the network.
- **Scenario 2:** We set parameters $\beta_0 = 0.6$, $\alpha_0 = 0.1$, $\gamma_0 = 0.03$, $\phi_0 = 0.01$, $\varepsilon = 0.9$, $\theta = 0.4$. Then $R_0 = 1.5429$. We test the temporal evolution of the proportions of various state nodes in the presence of endemic equilibrium in the network.

In the absence of any control intervention, we simulate the diffusion process of fraud information in two scenarios. In order to eliminate the influence of different initial states on the diffusion process of fraud information, we carried out simulations under the same initial state ($s(0) = 0.05, w(0) = 0.7, i(0) = 0.2$ and $r(0) = 0.05$). The simulation results are shown in Fig. 3.

From Fig. 3 (a), we can see that in the case of $R_0 \leq 1$, $i(t)$ gradually decreases after a rapidly increasing. After a period of time, there are only two kinds of nodes in the system, which belong to either S or R states, and the fraud information will not be diffused again. As we can see from Fig. 3 (b), in the case of $R_0 > 1$, the fraud information begins to show the trend of spreading. Nevertheless, after the peak, as $r(t)$ increase, $i(t)$ decreases. Finally, the values of $s(t)$, $w(t)$, $i(t)$ and $r(t)$ become stable. In this stable state, the fraud information will constantly spread unless some external interventions or control measures are taken. The simulation results in Fig. 3 fully illustrate that the evolutionary relationship of various state nodes is closely related to R_0, which conforms to our stability analysis conclusions of the diffusion model. That is, in the case of $R_0 \leq 1$, the fraud information will automatically die out. On the contrary, the fraud information will constantly spread and reach a steady state. In addition, we select two sets of data records of real events spreading in real networks. The Real Event 1 in Fig. 3 (a) represents the trends of diffusion of the derivative topic of "Shenzhen sports car accident in May 2012" collected from Sina Weibo [45], and the Real Event 2 in Fig. 3 (b) represents the trends of rumor diffusion on Sina Weibo after the serious earthquake in Japan, 2011 [46]. We can see that the changing trend of $i(t)$ in $SWIR$ model in Fig. 3 (a) is well fitted to the trend of the Real Event 1, and we can get the same result from $i(t)$ and Real Event 2 in Fig. 3 (b), which also verifies the correctness and practicability of our proposed information diffusion model.



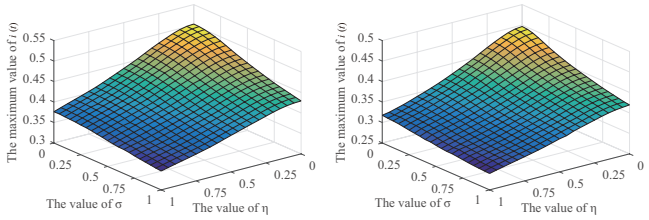
(a) Scenario 1 (b) Scenario 2

Fig. 3: The dynamic evolution of the proportions of individuals in case of no control strategy employed.

B. Validation on dynamic allocation of control strategies

In this section, we simulate the control effect of our proposed control strategies on the spread of fraud information. Firstly, we explore the influence of the parameters σ and η related to the control strategies prevention and correction on the infected nodes in the network, where σ and η represent the probabilities of successful implementation of the control strategies prevention and correction, respectively. When the optimal control strategies are adopted, the simulation results in Scenario 1 and Scenario 2 are shown in Fig. 4.

We can see that with the increasing probability of successful implementation of control strategies, the maximum proportion of individuals infected by fraud information $i(t)$ in the network decreases significantly. This shows that the maximum spreading area of fraud information has been controlled in



(a) Scenario 1 (b) Scenario 2

Fig. 4: The impact of the probabilities of successful implementation of control strategies on the maximum $i(t)$.

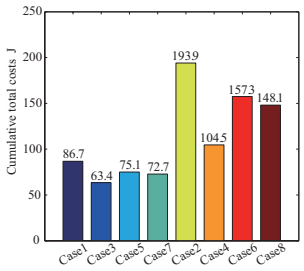


Fig. 5: The cumulative total costs of the system in Cases 1-8.

both scenarios. Furthermore, we can find that both σ and η are positively related to the effect of optimal control strategies. Especially, the change of η has a slightly greater impact on the control strategy than that of σ. It indicates that the control effect of the correction control strategy is slightly stronger than the prevention control strategy, because the correction control strategy directly affects the I state individuals in the network.

Then, we use our proposed diffusion model and control strategies to simulate the dynamic evolution of fraud information on the synthetic datasets and the real Twitter datasets under the default parameter configuration. We use $i(t)$ and $i'(t)$ to represent the proportions of infected state nodes in time t on the synthetic datasets and the real Twitter datasets, respectively, and we use $w(t)$ and $w'(t)$ to represent the proportions of wandering state nodes in time t on the synthetic datasets and the real Twitter datasets, respectively. We investigate and compare the effects of different control strategies on fraud information diffusion and the cumulative total costs of the system in the following Cases.

Case 1: all control strategies are not implemented in Scenario 1, i.e., $u(t) = 0,\ v(t) = 0$.

Case 2: all control strategies are not implemented in Scenario 2, i.e., $u(t) = 0,\ v(t) = 0$.

Case 3: two control strategies prevention and correction are implemented in Scenario 1, i.e., $u(t) \neq 0,\ v(t) \neq 0$.

Case 4: two control strategies prevention and correction are implemented in Scenario 2, i.e., $u(t) \neq 0,\ v(t) \neq 0$.

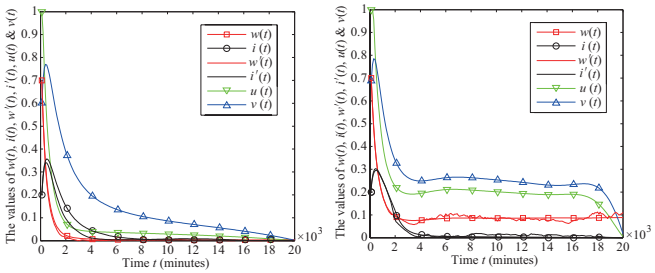
Case 5: only prevention control strategy is implemented in Scenario 1 , i.e., $u(t) \neq 0,\ v(t) = 0$.

Case 6: only prevention control strategy is implemented in Scenario 2 , i.e., $u(t) \neq 0,\ v(t) = 0$.

Case 7: only correction control strategy is implemented in Scenario 1 , i.e., $u(t) = 0,\ v(t) \neq 0$.

Case 8: only correction control strategy is implemented in Scenario 2 , i.e., $u(t) = 0,\ v(t) \neq 0$.

The dynamic evolution of the proportions of individuals in Case 1 and Case 2 is consistent with that in Fig. 3 (a) and Fig. 3 (b), respectively. Because Fig. 3 (a) and Fig. 3 (b) demonstrate the dynamic evolution of the proportions of individuals without any control strategy implemented ($u(t) = 0,\ v(t) = 0$) in Scenario 1 and Scenario 2, respectively. We first give the cumulative total costs of the system in Cases 1-8, which are shown in Fig. 5. Then, the simulation results of the Cases 3-8 are shown in Figs.6-8.

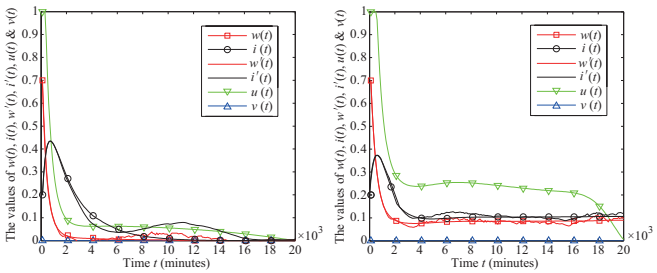


(a) Case 3 (b) Case 4

Fig. 6: The dynamic allocation of the control strategies and the dynamic evolution of the proportions of individuals with control strategies $u(t) \neq 0,\ v(t) \neq 0$.

Fig. 6 demonstrates the dynamic evolution of the proportions of individuals in infected and wandering states and the dynamic allocation of the optimal control strategies over time in Case 3 and Case 4, respectively. Clearly, in the case of implementing two control measures, i.e., prevention and correction, $i(t)$ in both scenarios are obviously reduced, which fully demonstrates that the fraud information has been obviously controlled. Compared to Case 1, Case 3 shows that the peak value of $i(t)$ has decreased significantly. In addition, the same conclusion can be obtained from the comparison of Case 4 and Case 2. This proves the effectiveness of our proposed optimal control strategies in suppressing the diffusion of fraud information. In particular, the cumulative total costs of the system caused by the optimal dynamic allocation of the control strategies in the Case 3 and Case 4 are the smallest, which are 63.4 and 104.5, respectively (see Fig. 5). The results indicate that the proposed optimal control strategies can not only reduce the propagation of fraud information at a small cost, but also minimize the losses of the system caused by fraud information. Finally, we can see that the changing trends of the proportions of individuals in the synthetic datasets are exactly the same as that in the real Twitter datasets. This shows our proposed models are practical and effective.

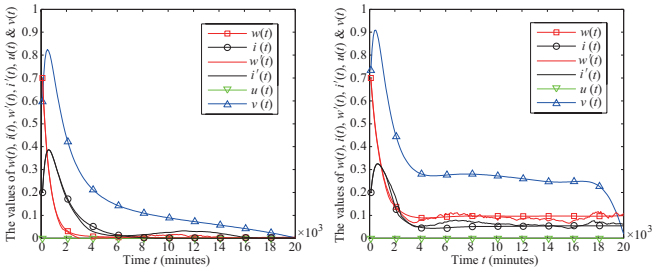
Fig. 7 shows the dynamic evolution of the proportions of individuals in infected and wandering states and the dynamic allocation of the single prevention control strategy over time in Case 5 and Case 6, respectively. We can see that in the case of only implementing the prevention control strategy, $i(t)$ in both scenarios have relatively declined, and the fraud information has been controlled to some extent, which proves



(a) Case 5 (b) Case 6

Fig. 7: The dynamic allocation of the control strategies and the dynamic evolution of the proportions of individuals with control strategies $u\left(t\right) \neq 0,\ v\left(t\right) = 0$.

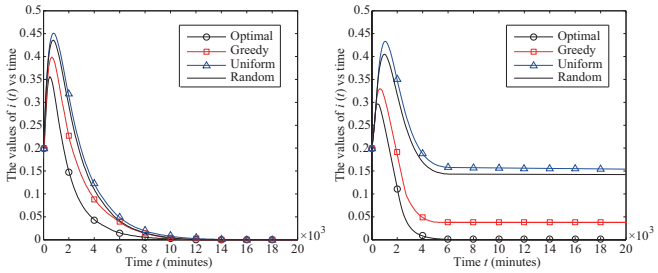
the effectiveness of prevention control strategy in suppressing fraud information dissemination. However, by contrast, the values of $i(t)$ and $i'(t)$ in Case 5 and Case 6 are higher than that in Case 3 and Case 4. It shows that the single prevention control strategy is far less effective than the optimal control strategies of the two control measures. Moreover, the cumulative total cost caused by the optimal dynamic allocation of the prevention control strategy alone is greater than that in optimal control strategies with two control measures in Scenario 1 and Scenario 2, which are 75.1 and 157.3 respectively (see Fig. 5). This explains that in the case of limited costs, the effect of implementing the single prevention control strategy to control fraud information diffusion is not ideal, so the cumulative loss of the system is more severe. Finally, we can still see that the simulation results under the synthetic datasets are consistent with those in the real Twitter datasets. The fluctuations of $w'(t)$ and $i'(t)$ are due to the nonuniform of social contacts and relationships among nodes in the real Twitter datasets.



(a) Case 7 (b) Case 8

Fig. 8: The dynamic allocation of the control strategies and the dynamic evolution of the proportions of individuals with control strategies $u\left(t\right) = 0,\ v\left(t\right) \neq 0$.

Fig. 8 shows the dynamic evolution of the proportion of individuals in infected and wandering states and the dynamic allocation of the single correction control strategy over time in Case 7 and Case 8, respectively. We can draw conclusions that in the case of only implementing the correction control strategy, the values of $i(t)$ in both scenarios will decline, and the diffusion of fraud information will be controlled. However, compared to other cases, it can be seen that the single correction control strategy is not as effective as the optimal control strategies with two control measures, but slightly better than the single prevention control strategy. At the same time, the cumulative total costs caused by the optimal dynamic allocation of single correction control strategy are greater than that of optimal control strategies with two control measures in the Scenario 1 and Scenario 2, which are 72.7 and 148.1 respectively (see Fig. 5). However, the cumulative total costs caused by the single correction control strategy are less than that of the single prevention control strategy. This fully demonstrates that correction control measure is more effective in response to the nodes in I state.



(a) Scenario 1 (b) Scenario 2

Fig. 9: The dynamic evolution of the proportions of I state individuals with different control strategies.

In addition, we then compare our proposed optimal control strategies with the existing control strategies. We modify the heuristic information diffusion control strategy proposed by [47] slightly to adapt to the information diffusion model proposed in this paper, and we call the modified strategy Greedy. In the *Greedy control strategy*, as long as the control resources used to control fraud information are sufficient, the system greedily adopts the strongest control strategy ($u\left(t\right) = 1,\ v\left(t\right) = 1$), until the control resources are exhausted. Moreover, we compare the proposed optimal control strategies with the Uniform control strategy and Random control strategy. The *Uniform control strategy* means that the system distributes control resources evenly to each control time step. That is to say, the same intensity control strategy is adopted in each time step ($u\left(t\right) = f,\ v\left(t\right) = g$, where $0 \leq f \leq 1$, $0 \leq g \leq 1$, f and g are constants). Similarly, the *Random control strategy* means that the system randomly allocates control resources to each control time step, i.e. the intensity of the control strategy adopted in each time step is random ($u\left(t\right) = j,\ v\left(t\right) = k$, where $0 \leq j \leq 1$, $0 \leq k \leq 1$, j and k are random variables). On the premise of the same control resources and control time, the control effects of the above four strategies on fraud information in two scenarios are shown in Fig. 9.

Fig. 9 demonstrates the dynamic evolution of the proportions of I state individuals over time in Scenario 1 and Scenario 2 under different control strategies. From Fig. 9, we can see that under the premise of consuming the same control resources, the proportion of I state individuals in the network is the least when the optimal control strategies is adopted. There is no doubt that the optimal control strategies has the best effect on the control of fraud information diffusion in the

network. The Greedy control strategy takes the greatest control in the early stage of the spread of fraud information, which can restrain the spread of fraud information to a certain extent. However, fraud information cannot be completely eradicated because of the excessive consumption of resources. Overall, the control effect of the proposed optimal control strategies is about 10% higher than that of the other control strategy. The Random control strategy and the Uniform control strategy do not have an efficient allocation scheme for control resources, resulting in poor control effect on fraud information.

To summarize, the optimal control strategies combined with the two control measures can minimize the cumulative total costs in the case of completely controlling the diffusion of fraud information. In addition, the effectiveness and efficiency of the proposed optimal control strategies are demonstrated by comparing the trends of the dynamic evolution of individuals and the cumulative total costs in Cases 1-8.

V. Conclusions

The goal of this paper is to put forward the optimal control strategies to efficiently utilize limited control resources and minimize losses of individuals caused by the diffusion of fraud information. Firstly, a novel $SWIR$ dynamics model is proposed to describe the dynamic evolutionary process of fraud information diffusion in MSNs. Thereafter, this paper analyzes and proves the information diffusion trends and stability of the dynamics model. In particular, this paper proposes two synergistic control strategies to suppress the spread of fraud information, and derives the optimal dynamic allocation of the control strategies. Finally, we validate the efficiency of our proposed diffusion model and optimal control strategies in both synthetic datasets and real social network datasets.

This paper can provide a theoretical basis and a feasible technical approach for the applications of controllable information diffusion based on MSNs, and further promote the development and application of information diffusion and optimal control technology in MSNs. In the future, we will further study the diffusion modeling and control of coupling of positive and negative information. In addition, we will also study the impact of users' social identity cognition on information diffusion.

References

[1] M. Xiao, J. Wu, L. Huang *et al.*, "Online task assignment for crowdsensing in predictable mobile social networks," *IEEE Trans. Mob. Comput.*, vol. 16, no. 8, pp. 2306–2320, 2017.

[2] L. Jiang, J. Liu, D. Zhou *et al.*, "Predicting the evolution of hot topics: A solution based on the online opinion dynamics model in social network," *IEEE Trans. Syst. Man Cybern. -Syst.*, 2018.

[3] Y. Lin, X. Wang, F. Hao *et al.*, "An on-demand coverage based self-deployment algorithm for big data perception in mobile sensing networks," *Future Gener. Comput. Syst.*, vol. 82, pp. 220–234, 2018.

[4] Y. Wang, A. V. Vasilakos, J. Ma *et al.*, "On studying the impact of uncertainty on behavior diffusion in social networks," *IEEE Trans. Syst. Man Cybern. -Syst.*, vol. 45, no. 2, pp. 185–197, 2015.

[5] L. Yang, P. Li, Y. Zhang *et al.*, "Effective repair strategy against advanced persistent threat: A differential game approach," *IEEE Trans. Inf. Forensic Secur.*, vol. 14, no. 7, pp. 1713–1728, 2019.

[6] Z. He, Z. Cai, J. Yu *et al.*, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2789–2800, 2017.

[7] L.-X. Yang, P. Li, X. Yang *et al.*, "On the competition of two conflicting messages," *Nonlinear Dyn.*, vol. 91, no. 3, pp. 1853–1869, 2018.

[8] R. Nash, M. Bouchard, and A. Malm, "Investing in people: The role of social networks in the diffusion of a large-scale fraud," *Soc. Networks*, vol. 35, no. 4, pp. 686–698, 2013.

[9] R. A. Raub, A. H. N. Hamzah, M. D. Jaafar *et al.*, "Using subscriber usage profile risk score to improve accuracy of telecommunication fraud detection," in *proc. IEEE CYBERNETICSCOM*, 2016, pp. 127–131.

[10] J. Ma, W. Gao, P. Mitra *et al.*, "Detecting rumors from microblogs with recurrent neural networks." in *Proc. IJCAI*, 2016, pp. 3818–3824.

[11] "Tsinghua university teachers cheated 17 million 600 thousand? the original liar used this psychological routine!" http://www.bestchinanews.com/Domestic/2426.html, Aug. 2016.

[12] M. Sahin, "Over-the-top bypass: Study of a recent telephony fraud," in *proc. ACM CCS*, 2016, pp. 1106–1117.

[13] K. Zhu and L. Ying, "Information source detection in the sir model: A sample-path-based approach," *IEEE/ACM Trans. Netw.*, vol. 24, no. 1, pp. 408–421, 2012.

[14] Z. Chen, K. Zhu, and L. Ying, "Detecting multiple information sources in networks under the sir model," *IEEE Trans. Netw. Sci. Eng.*, vol. 3, no. 1, pp. 17–31, 2016.

[15] A. Y. Khrennikov, *Information dynamics in cognitive, psychological, social, and anomalous phenomena*. Springer Science & Business Media, 2013, vol. 138.

[16] R. Lachman, J. L. Lachman, and E. C. Butterfield, *Cognitive psychology and information processing: An introduction*. Psychology Press, 2015.

[17] W. Zhou, W. Jia, M. Haghighi *et al.*, "A sword with two edges: Propagation studies on both positive and negative information in online social networks," *IEEE Trans. Comput.*, vol. 64, no. 3, pp. 640–653, 2015.

[18] E. Kušen, M. Strembeck, G. Cascavilla *et al.*, "On the influence of emotional valence shifts on the spread of information in social networks," in *Proc. IEEE/ACM ASONAM*, 2017, pp. 321–324.

[19] K. Kandhway and J. Kuri, "Using node centrality and optimal control to maximize information diffusion in social networks," *IEEE Trans. Syst. Man Cybern. -Syst.*, vol. 47, no. 7, pp. 1099–1110, 2017.

[20] A. Nematzadeh, E. Ferrara, A. Flammini *et al.*, "Optimal network modularity for information diffusion." *Phys. Rev. Lett.*, vol. 113, no. 8, pp. 088 701: 1–5, 2014.

[21] K. Kandhway and J. Kuri, "How to run a campaign: Optimal control of sis and sir information epidemics," *Appl. Math. Comput.*, vol. 231, no. 1, pp. 79–92, 2014.

[22] X. Wang, Y. Lin, Y. Zhao *et al.*, "A novel approach for inhibiting misinformation propagation in human mobile opportunistic networks," *Peer Peer Netw. Appl.*, vol. 10, no. 2, pp. 377–394, 2017.

[23] Q. Zhao, C. Wang, P. Wang *et al.*, "A novel method on information recommendation via hybrid similarity," *IEEE Trans. Syst. Man Cybern. -Syst.*, vol. 48, no. 3, pp. 448–459, 2018.

[24] Y. Jiang and J. C. Jiang, "Diffusion in social networks: A multiagent perspective," *IEEE Trans. Syst. Man Cybern. -Syst.*, vol. 45, no. 2, pp. 198–213, 2015.

[25] L.-X. Yang, X. Yang, and Y. Y. Tang, "A bi-virus competing spreading model with generic infection rates," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 1, pp. 2–13, 2018.

[26] D. Zhao, L. Wang, Z. Wang *et al.*, "Virus propagation and patch distribution in multiplex networks: Modeling, analysis, and optimal allocation," *IEEE Trans. Inf. Forensic Secur.*, vol. 14, no. 7, pp. 1755–1767, 2019.

[27] C. Liu, X. Zhan, Z. Zhang *et al.*, "How events determine spreading patterns: information transmission via internal and external influences on social networks," *New J. Phys.*, vol. 17, no. 11, p. 113045, 2015.

[28] Z. Zhang, C. Liu, X. Zhan *et al.*, "Dynamics of information diffusion and its applications on complex networks," *Phys. Rep.*, vol. 651, pp. 1–34, 2016.

[29] D. Li, S. Zhang, X. Sun *et al.*, "Modeling information diffusion over social networks for temporal dynamic prediction," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 9, pp. 1985–1997, 2017.

[30] J. Liu and N. Kato, "A markovian analysis for explicit probabilistic stopping-based information propagation in postdisaster ad hoc mobile networks," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 1, pp. 81–90, 2016.

[31] E. Yoo, W. Rand, M. Eftekhar *et al.*, "Evaluating information diffusion speed and its determinants in social media networks during humanitarian crises," *J. Oper. Manag.*, vol. 45, pp. 123–133, 2016.

[32] H. Zhu, Y. Kong, J. Wei *et al.*, "Effect of users opinion evolution on information diffusion in online social networks," *Physica A*, vol. 492, pp. 2034–2045, 2018.

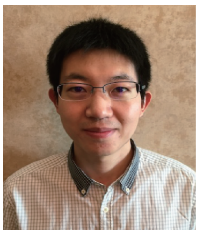
[33] X. Zhan, C. Liu, G. Zhou *et al.*, "Coupling dynamics of epidemic spreading and information diffusion on complex networks," *Appl. Math. Comput.*, vol. 332, pp. 437 – 448, 2018.
[34] Z. Zhu, G. Cao, S. Zhu *et al.*, "A social network based patching scheme for worm containment in cellular networks," in *Handbook of optimization in complex networks*. Springer, 2012, pp. 505–533.
[35] Y. D. Jeong, K. S. Kim, and I. H. Jung, "Optimal control strategies depending on interest level for the spread of rumor," *Discrete Dyn. Nat. Soc.*, vol. 2018, pp. 9 158 014: 1–15, 2018.
[36] P. Y. Chen, S. M. Cheng, and K. C. Chen, "Optimal control of epidemic information dissemination over networks." *IEEE Trans. Cybern.*, vol. 44, no. 12, pp. 2316–2328, 2014.
[37] C. Y. Aung, G. G. M. N. Ali, M. Zhao *et al.*, "Information epidemics control for data delivery in opportunistic networks," in *proc. IEEE ICC*, 2016, pp. 1–6.
[38] D. J. Luc, B. Bissila, and T. Mavoungou, "Stability analysis of deterministic cholera model," *J. Progress. Res. Math.*, vol. 7, no. 2, pp. 962–974, 2016.
[39] B. Ding and C. Ding, "Recurrence and lasalle invariance principle," *Syst. Control Lett.*, vol. 93, pp. 64–68, 2016.
[40] M. A. Choghadi and H. A. Talebi, "The routh-hurwitz stability criterion, revisited: The case of multiple poles on imaginary axis," *IEEE Trans. Autom. Control*, vol. 58, no. 7, pp. 1866–1869, 2013.
[41] D. E. Kirk, *Optimal control theory: an introduction*. Springer, 1970.
[42] E. Casas, J. P. Raymond, and H. Zidani, "Pontryagin's principle for local solutions of control problems with mixed control-state constraints," *SIAM J. Control Optim.*, vol. 39, no. 4, pp. 1182–1203, 2016.
[43] Z. Bartoszewski and Z. Jackiewicz, "Nordsieck representation of two-step rungeckutta methods for ordinary differential equations," *Appl. Numer. Math.*, vol. 53, no. 2, pp. 149–163, 2015.
[44] R. Zafarani and H. Liu, "Social computing data repository at ASU," 2009. [Online]. Available: http://socialcomputing.asu.edu
[45] X. Zhang, X. Chen, Y. Chen *et al.*, "Event detection and popularity prediction in microblogging," *Neurocomputing*, vol. 149, pp. 1469–1480, 2015.
[46] N. Zhang, H. Huang, M. Duarte *et al.*, "Risk analysis for rumor propagation in metropolises based on improved 8-state icsar model and dynamic personal activity trajectories," *Physica A*, vol. 451, pp. 403 – 419, 2016.
[47] P. Wu and L. Pan, "Scalable influence blocking maximization in social networks under competitive independent cascade models," *Comput. Netw.*, vol. 123, pp. 38–50, 2017.

Yaguang Lin received the B.S. degree in computer science and technology from Xi'an Technological University, China, in 2013. He is working toward the Ph.D. degree with the School of Computer Science, Shaanxi Normal University, China. He's also a visiting Ph.D. student at the Department of Computer Science, Georgia State University, USA, from 2018. His research interests include information diffusion, rumor blocking and mobile social networks.

Xiaoming Wang received the Ph.D. degree in computer software and theory from Northwest University, China, in 2005. He was a senior visiting scholar at the Department of Computer Science, Georgia State University, USA, from 2007 to 2008. He is currently a Professor and the Dean with the School of Computer Science, Shaanxi Normal University, China. He has served as a reviewer/editor for many journals. He has published 3 books and more than 100 scientific articles. His main research interests include information diffusion, mobile social networks, social computing and ubiquitous computing.

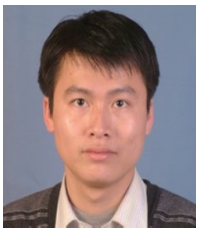
Fei Hao received the Ph.D. degree from Soonchunhyang University, South Korea, in 2016. He is currently an Associate Professor with the School of Computer Science, Shaanxi Normal University, China. His research interests include social computing, ubiquitous computing and mobile cloud computing. He have received five best paper awards from KISM 2012, GreenCom 2013, MUE 2015, UCAWSN 2015, CUTE 2016. He is a recipient of the IEEE Outstanding Leadership Award at CPSCom 2013 and the IEEE Outstanding Service Awards at SmartData 2017 and DSS 2018.

Yichuan Jiang received the Ph.D. degree in computer science from Fudan University, Shanghai, China, in 2005. He is currently a Full Professor with the Distributed Intelligence and Social Computing Laboratory, School of Computer Science and Engineering, Southeast University, Nanjing, China. He has published over 80 scientific articles in refereed journals and conference proceedings. His current research interests include multi-agent systems, social networks and social computing. He is a recipient of the Best Paper Award and the Best Student Paper Award from PRIMA and ICTAI.

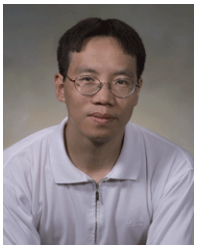


Yulei Wu received the B.S. degree in Computer Science and Ph.D. degree in Computing and Mathematics from the University of Bradford, UK, in 2006 and 2010, respectively. He is currently a Lecturer in Computer Science, University of Exeter. His main research focuses on future internet architecture and technologies, smart network management, cloud computing, big data for networking, and analytical modelling and performance optimisation. He has published over 50 research papers in prestigious international journals and at reputable international conferences.

Geyong Min received the B.S. degree in Computer Science from Huazhong University of Science and Technology, China, in 1995, and the Ph.D. degree in Computing Science from the University of Glasgow, United Kingdom, in 2003. He is currently a Professor in the Department of Mathematics and Computer Science, University of Exeter, United Kingdom. His research interests include future internet, computer networks, wireless communications, multimedia systems, information security, high performance computing, ubiquitous computing, modelling and performance engineering.



Daojing He received the B.Eng. and M. Eng. degrees from Harbin Institute of Technology, China, in 2007 and 2009, all in computer science, and the Ph.D. degree from Zhejiang University, China, in 2012. He is currently a Professor in the School of Computer Science and Software Engineering, East China Normal University, China. His research interests include network and systems security. He is on the Editorial Boards of some international publications such as IEEE Communications Magazine.



Sencun Zhu received the B.S. degree from Tsinghua University, Beijing, China, in 1996, the M.S. degree from the University of Science and Technology of China, Beijing, China, in 1999, and the Ph.D. degree from George Mason University, Fairfax, VA, USA, in 2004. He is an Associate Professor with Penn State University. His research interests include network and systems security and software security. He is the editor-in-chief of EAI Transactions on Security and Safety, an associate editor of IEEE Transactions on Mobile Computing (TMC) and Wiley Journal on Security and Privacy.

Wei Zhao received the undergraduation degree in physics from Shaanxi Normal University, Xi'an, China, and the M.S. and Ph.D. degrees in computer and information sciences from the University of Massachusetts, Amherst, MA, USA, in 1983 and 1986, respectively. He is currently with the American University of Sharjah, U.A.E. He also served as the 8th Rector of the University of Macau, Macau, China, the Dean of the School of Science, Rensselaer Polytechnic Institute, Troy, NY, USA, the Director for the Division of Computer and Network Systems, U.S. National Science Foundation, Arlington, VA, USA, the Senior Associate Vice President for Research, and a Professor of computer science in Texas A&M University, College Station, TX, USA. He was the Founding Director of the Texas A&M Center for Information Security and Assurance. As an elected IEEE fellow, he has made significant contributions in distributed computing, realtime systems, computer networks, cyber security, and cyber-physical systems.