DYNAMIC CONTROL OF FRAUD INFORMATION SPREADING IN MOBILE SOCIAL NETWORKS

[1]Mrs.K.Rajitha,[2]S. Sai Nithin,[3]K. Lalu Ajay,[4]P. Krishna Chaitanya,[5]N. Bhaskar
[1] Assistant *Professor,*[2345]*B.Tech Students*
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

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 f 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.

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 . 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. However, the development of MSNs is like a double-edged sword . 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. 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. According to the official data released by the security ministry, telecommunications fraud in MSNs has grown at an annual rate of 20%–30%. The following are two representative scenarios

Scenario A: One scenario is the Veracruz incident in August 2015. A piece of rumor saying "shootouts and kidnappings by drug gangs happening near schools in Veracruz" spread in Twitter and Face book. 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. 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. 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 up 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 of infectious diseases in biology and the diffusion process of fraud information in the network are very similar. The most widely used model is the susceptible-infected recovered (SIR) model, in which all individuals are divided into three categories: 1) susceptible; 2) infected; and 3) recovered. 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. First, 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. Second, the fraud information diffusion processes in MSNs are the complex results of the continuous interactions of nodes in different states. Third, 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. 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”. 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. Therefore, how to efficiently utilize

limited control resources and minimize losses of individuals by adopting proper control strategies have 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. 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.

1) *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. In addition, we theoretically analyze the stability of the *SWIR* model and the trend of fraud information diffusion.

2) *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 to 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.

3) *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 this paper is organized as follows. In Section II, some previous works are reviewed. In Section 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. The extensive simulations are conducted in Section IV. Section V concludes this paper

II. LITERATURE SURVEY

TITLE: Sketch-Based Streaming PCA Algorithm for Network-Wide Traffic Anomaly Detection

AUTHOR: Linfeng Zhang

ABSTRACT: Internet has become an essential part of the daily life for billions of users worldwide, who are using a large variety of network services and applications everyday. However, there have been serious security problems and network failures that

are hard to resolve, for example, botnet attacks, polymorphic worm/virus spreading, DDoS, and flash crowds. To address many of these problems, we need to have a network-wide view of the traffic dynamics, and more importantly, be able to detect traffic anomalies in a timely manner. Spatial analysis methods have been proved to be effective in detecting network-wide traffic anomalies that are not detectable at a single monitor. To our knowledge, Principle Component Analysis (PCA) is the best-known spatial detection method for the coordinated low-profile traffic anomalies. However, existing PCA-based solutions have scalability problems in that they require linear running time and space to analyze the traffic measurements within a sliding window, which makes it often infeasible to be deployed for monitoring large-scale high-speed networks. We propose a sketch-based streaming PCA algorithm for the network-wide traffic anomaly detection in a distributed fashion. Our algorithm only requires logarithmic running time and space at both local monitors and Network Operation Centers (NOCs), and can detect both high-profile and coordinated low-profile traffic anomalies with bounded errors.

TITLE: Vote calibration in community question-answering systems

AUTHOR: Jie Yang

ABSTRACT: User votes are important signals in community question-answering (CQA) systems. Many features of typical CQA systems, e.g. the best answer to a question, status of a user, are dependent on ratings or votes cast by the community. In a popular CQA site, Yahoo! Answers, users vote for the best answers to their questions and can also thumb up or down each individual answer. Prior work has shown that these votes provide useful predictors for content quality and user expertise, where each vote is usually assumed to carry the same weight as others. In this paper, we analyze a set of possible factors that indicate bias in user voting behavior -- these factors encompass different gaming behavior, as well as other eccentricities, e.g., votes to show appreciation of answerers. These observations suggest that votes need to be calibrated before being used to identify good answers or experts. To address this problem, we propose a general machine learning framework to calibrate such votes. Through extensive experiments based on an editorially judged CQA dataset, we show that our supervised learning method of content-agnostic vote calibration can significantly improve the performance of answer ranking and expert ranking.

III. SYSTEM ANALYSIS & DESIGN

3.1 EXISTING SYSTEM

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 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: 1) modeling of the information diffusion process and 2) 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 spatio-temporal dynamic evolutionary process of information diffusion. Wen *et al.* 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.* 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, Liu and Kato proposed an information diffusion model based on the probability stopping mechanism in finance, as well as an analysis method based on the Markov chain. The model and the 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.* 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.* 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.

Disadvantages

- The system is less effective due to lack of thinking, trust, and diffusion, the three psychological cognitive and behavioral states.
- The system doesn't effective since gradually lose the awareness of fraud information due to its forgetting psychology, it may be infected again by fraud information in the future.

3.2 PROPOSED SYSTEM

In order to overcome the above limitations, in the proposed system, the system 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.

1) *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. In addition, we theoretically analyze the stability of the *SWIR* model and the trend of fraud information diffusion.

2) *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.

3) *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.

Advantages:

- The proposed system establishes an information diffusion model to accurately describe the dynamic diffusion process of fraud information in MSNs by considering the uncertain mental states of individuals.
- The system analyzes the trend of information diffusion and the stability of the dynamics model from a theoretical point of view and explores the theory of dynamic evolution of information diffusion model.

SYSTEM ARCHITECTURE

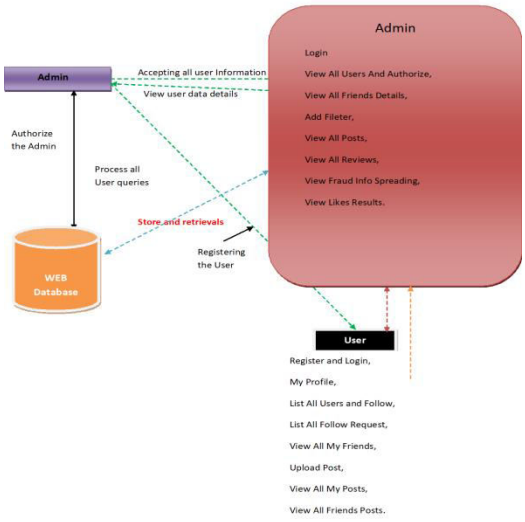

Fig :SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

Admin:

In this module, the Admin has to login by using valid user name and password. After login successful he can perform some operations such as View All Users And Authorize,View All Friends Details,Add Filter,View All Posts,View All Reviews,View Fraud Info Spreading,View Likes Results.

Friend Request & Response

In this module, the admin can view all the friend requests and responses. Here all the requests and responses will be displayed with their tags such as Id, requested user photo, requested user name, user name request to, status and time & date. If the user accepts the request then the status will be changed to accepted or else the status will remains as waiting

User:

In this module, there are n numbers of users are present. User should register before performing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Verify finger print and Login Once Login is successful

user can perform some operations like List All Users and Follow,List All Follow Request,View All My Friends,Upload Post,View All My Posts,View All Friends Posts.

Searching Users to make friends

In this module, the user searches for users in Same Network and in the Networks and sends friend requests to them. The user can search for users in other Networks to make friends only if they have permission.

V. V.OUTPUT SCREENSHOTS

Fig1:Home Page

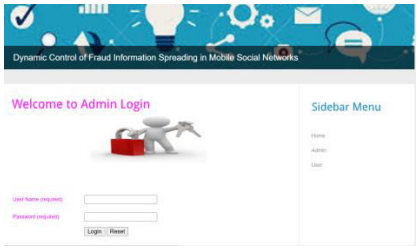

Fig2:Admin Login

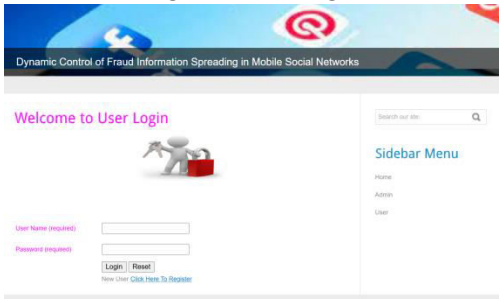

Fig3:User Login

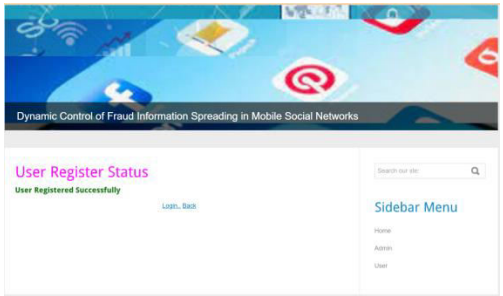

Fig4:User Register Status

Fig5: Admin Accept New Users Page

Fig6:Admin View Posts of Users

Fig7.View like Results in Admin Page

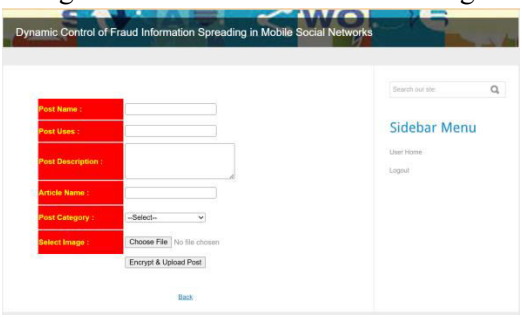

Fig8 User Uploading Post Page

VI. CONCLUSION

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. First, 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.

FUTURE SCOPE

The future scope of the project "Dynamic Control of Fraud Information Spreading in Mobile Social Networks" includes the integration of advanced machine learning techniques, such as deep learning and reinforcement learning, to improve fraud detection accuracy in real-time. It also involves exploring behavioral profiling and contextual analysis for more refined fraud detection. The project can expand to cross-platform fraud control by collaborating with other social networks and using blockchain technology to ensure data integrity and transparency. Additionally, privacy-preserving methods like federated learning and differential privacy should be incorporated to protect user data while detecting fraudulent activities. The system's scalability can be enhanced by using distributed computing and cloud infrastructure to handle large volumes of data efficiently. Further, the project can include user education tools, ethical AI implementation, and compliance with global regulations, while exploring decentralized control mechanisms and fraud prevention across different domains, such as e-commerce and IoT networks. Long-term monitoring, reporting systems, and collaborative tools for stakeholders could provide continuous improvements, ensuring dynamic and adaptive fraud mitigation strategies.

REFERENCES

[1] M. Xiao, J. Wu, L. Huang, R. Cheng, and Y. Wang, "Online task assignment for crowdsensing in predictable mobile social networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2306–2320, Aug. 2017.

[2] L. Jiang, J. Liu, D. Zhou, Q. Zhou, X. Yang, and G. Yu, "Predicting the evolution of hot topics: A solution based on the online opinion dynamics model in social network," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[3] Y. Lin *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, May 2018.

[4] Y. Wang, A. V. Vasilakos, J. Ma, and N. Xiong, "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, Feb. 2015.

[5] L.-X. Yang, P. Li, Y. Zhang, X. Yang, Y. Xiang, and W. Zhou,"Effective repair strategy against advanced persistent threat: A differential game approach," *IEEE Trans. Inf. Forensics Security*, vol. 14,
no. 7, pp. 1713–1728, Jul. 2019.

[6] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategiesfor restraining rumor spreading in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2789–2800, Mar. 2017.

[7] L.-X. Yang, P. Li, X. Yang, Y. Wu, and Y. Y. Tang, "On the competition of two conflicting messages," *Nonlin. 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.*

Netw., vol. 35, no. 4, pp. 686–698, 2013.
[9] R. A. Raub, A. H. N. Hamzah, M. D. Jaafar, and K. N. Baharim, "Using subscriber usage profile risk score to improve accuracy of telecommunication fraud detection," in *Proc. IEEE CYBERNETICSCOM*, 2016,pp. 127–131.
[10] J. Ma *et al.*, "Detecting rumors from microblogs with recurrent neural networks," in *Proc. IJCAI*, 2016, pp. 3818–3824.