www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

MANAGING FRAUD INFORMATION PROPOGATION IN MOBILE SOCIAL NETWORKS

[1] Mr. A. Sandeep,[2] T. Sri Vardhini,[3] S. Sneha,[4] T. Nikhil,[5] V. Narendar Reddy
[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 [8]. 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

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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.

1.1 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.

1.2 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.

1.3 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: Online task assignment for crowdsensing in predictable mobile social networks

Author: M. Xiao, J. Wu, L. Huang, R. Cheng, and Y. Wang.

Abstract: Mobile crowdsensing is a new paradigm in which a crowd of mobile users exploit their carried smart phones to conduct complex sensing tasks. In this paper, we focus on the make span sensitive task assignment problems for the crowdsensing in mobile social networks, where the mobility model is predicable, and the time of sending tasks and recycling results is non-negligible. To solve the problems, we propose an Average make span sensitive Online Task Assignment (AOTA) algorithm and a Largest makespa n sensitive Online Task Assignment (LOTA) algorithm. In AOTA and LOTA, the online task assignments are viewed as multiple rounds of virtual offline task assignments. Moreover, a greedy strategy of small task first assignment and earliest-idle-user-receive-task is adopted for each round of virtual offline task assignment in AOTA, while the greedy strategy of large task first assignment and earliest idle user-receive-task is adopted for the virtual offline task assignments in LOTA. Based on the two greedy strategies, both AOTA and LOTA can achieve nearly optimal online decision performances. We prove this and give the competitive ratios of the two algorithms. In addition, we also demonstrate the significant performance of the two algorithms through extensive simulations, based on four real MSN traces and a synthetic MSN trace.

Title: Predicting the evolution of hot topics: A solution based on the online opinion dynamics model in social network

Author: L. Jiang, J. Liu, D. Zhou, Q. Zhou, X. Yang, and G. Yu.

Abstract: Predicting and utilizing the evolution trend of hot topics is critical for contingency management and decision-making purposes of government bodies and enterprises. This paper

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

proposes a model named online opinion dynamics (OODs) where any node in a social network has its unique confidence threshold and influence radius. The nodes in the OOD are mainly affected by their neighbors and are also randomly influenced by unfamiliar nodes. In the traditional opinion model, however, each node is affected by all other nodes, including its friends. Furthermore, many traditional opinion evolution approaches are reviewed to see if all nodes (participants) can eventually reach a consensus. On the contrary, OOD is more focused on such details as concluding the overall trend of events and evaluating the support level of each participant through numerical simulation. Experiments show that OOD is superior to the improvement of the original Hegselmann- Krause (HK) model, HK-13 and HK-17, with respect to qualitative predictions of the evolution trend of an event. The quantitative predictions of the HK model cannot be used to make decisions, whereas the results of the OOD model are proved to be acceptable.

Title: An on-demand coverage based self-deployment algorithm for big data perception in mobile sensing networks.

Author: Y. Lin et al

Abstract: Mobile Sensing Networks have been widely applied to many fields for big data perception such as intelligent transportation, medical health and environment sensing. However, in some complex environments and unreachable regions of inconvenience for human, the establishment of the mobile sensing networks, the layout of the nodes and the control of the network topology to achieve high performance sensing of big data are increasingly becoming a main issue in the applications of the mobile sensing networks. To deal with this problem, we propose a novel on-demand coverage based self-deployment algorithm for big data perception based on mobile sensing networks in this paper. Firstly, by considering characteristics of mobile sensing nodes, we extend the cellular automata model and propose a new mobile cellular automata model for effectively characterizing the spatial–temporal evolutionary process of nodes. Secondly, based on the learning automata theory and the historical information of node movement, we further explore a new mobile cellular learning automata model, in which nodes can self-adaptively and intelligently decide the best direction of movement with low energy consumption. Finally, we propose a new optimization algorithm which can quickly solve the node self-adaptive deployment problem; thus, we derive the best deployment scheme of nodes in a short time. The extensive simulation results show that the proposed algorithm in this paper outperforms the existing algorithms by as much as 40% in terms of the degree of satisfaction of network coverage, the iterations of the algorithm, the average moving steps of nodes and the energy consumption of nodes. Hence, we believe that our work will make contributions to large- scale adaptive deployment and high-performance sensing scenarios of the mobile sensing networks.

Firstly, by considering characteristics of mobile sensing nodes, we extend the cellular automata model and propose a new mobile cellular automata model for effectively characterizing the spatial–temporal evolutionary process of nodes. Secondly, based on the learning automata theory and the historical information of node movement, we further explore a new mobile cellular learning automata model, in which nodes can self-adaptively and intelligently decide the best direction of movement with low energy consumption. Finally, we propose a new optimization algorithm which can quickly solve the node self- adaptive deployment problem; thus, we derive the best deployment scheme of nodes in a short time.

III. SYSTEM ANALYSIS

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.

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.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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 diffuse.

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

PROPOSED SYSTEM

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.

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.

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.

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 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. resources and minimize losses of individuals caused by fraud information, we propose two synergistic control strategies.

IV. IMPLEMENTATION

MODULES

- Admin
- User

MODULE DESCRIPTION

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 Networ3k7s to make friends only if they have permission.

In this module, there are n numbers of users are

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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.

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.

V. SCREENSHOTS

FIG 1 : ADMIN HOME PAGE

FIG 2: VIEW USERS AND AUTHORISE

FIG 3 : ALL REQUEST AND RESPONSE

FIG 4 : ADD FILTERS

FIG 5: VIEW ALL USERS POSTS

FIG 6: VIEW ALL USERS REVIEWS

FIG7:USER HOME PAGE

FIG 8: USER PROFILE

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

VI. CONCLUSION

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

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

We have shown it is possible to assess the likelihood that an user is responsible for a leak, based on the overlap of his data with the leaked data and the data of other users, and based on the probability that objects can be 'guessed´ by other means. Our model is relatively simple, but we believe it captures the essential tradeoffs. The algorithms we have presented implement a variety of data distribution strategies that can improve the distributor's chances of identifying a leader in further research work.

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 strategies for 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. (Aug. 2016). Tsinghua University Teachers Cheated 17 million 600Thousand?
11. The Original Liar Used This Psychological Routine! [Online].
12. Available: http://www.bestchinanews.com/Domestic/2426.html
13. M. Sahin, “Over-the-top bypass: Study of a recent telephony fraud,” in Proc. ACM CCS, 2016, pp. 1106–1117.
14. 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, Feb. 2016.
15. 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, Jan./Mar. 2016.