DYNAMIC FRAUD INFORMATION CONTROL IN SOCIAL NETWORKS

Prashanth reddy vangala[1],Gogineni mounika[2],Kunta mani teja(l)[3]

[1]Assistant Professor,M.Tech.,BRILLIANT GRAMMAR SCHOOL EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS-INTEGRATED CAMPUS

Abdullapurmet (v), hayath nagar (m), r.r dt. Hyderabad

[2]Assistant Professor,M.Tech.,BRILLIANT GRAMMAR SCHOOL EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS-INTEGRATED CAMPUS

Abdullapurmet (V), Hayath Nagar (M), R.R Dt. Hyderabad

Department of CSE (DS),

[3]UG Students, BRILLIANT GRAMMAR SCHOOL EDUCATIONAL SOCIETY'S GROUP OF INSTITUTIONS-INTEGRATED CAMPUS

Abdullapurmet (V), Hayath Nagar (M), R.R Dt. Hyderabad

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

In the era of the Internet and the widespread adoption of intelligent mobile devices, Mobile Social Networks (MSNs) have evolved into a pivotal platform for information dissemination [1]. These networks offer real-time information services, embedding themselves seamlessly into daily life [2]. The allure and expansive potential of Internet-based MSNs have found applications in various fields such as instant communication, life services, and interactive entertainment [3]. However, the development of MSNs comes with inherent challenges, symbolizing a double-edged sword [4] [5]. As MSNs become integral to people's lives, the surge in unhealthy phenomena such as fake news, rumors, online promotion, and fraudulent activities poses a significant threat to normal social network activities [6] [7]. Furthermore, advancements in intelligent terminals, wireless networks, and online payment technologies have contributed to an increased rate of fraud, resulting in substantial losses for individuals [8]. According to official data, telecommunications fraud in MSNs has grown at an annual rate of 20%–30% [9]. Illustrative of this issue are two representative scenarios. Scenario A recounts the Veracruz incident in August 2015, where a rumor circulated on Twitter and Facebook about shootouts and kidnappings by drug gangs near schools, causing chaos and serious accidents in the city [10]. Scenario B involves a Chinese university professor who, in August 2016, fell victim to telecommunication-based fraud, resulting in a substantial loss of 17.6 million Yuan [11]. These scenarios underscore the pervasive problem of fraud information diffusion in social networks [12].

To effectively combat the spread of fraud information in MSNs, it is imperative to understand its diffusion patterns and devise appropriate control measures. Previous attempts using mathematical models, particularly those based on the susceptible-infected-recovered (SIR) model, have drawn parallels between the spread of infectious diseases and fraud information diffusion [13] [14]. However, the complex nature of human mental activities, the continuous interactions of nodes in different states, and the psychological effects on information reception challenge the accuracy of existing models.

This paper proposes a novel dynamics model, the SWIR model, accounting for

the uncertainties in individuals' mental states and their transitions between different states during fraud information diffusion. The SWIR model is designed to provide a more effective depiction of the dynamic diffusion process in MSNs, and its stability and trend analysis are theoretically examined. To address the limitations of existing research, the paper introduces synergistic control strategies, optimizing the dynamic allocation of control resources to minimize total costs while considering the harm to individuals caused by fraud information diffusion.

Simulation experiments on synthetic and real social network datasets validate the effectiveness of the proposed SWIR model and control strategies. The results demonstrate that the model accurately captures the dynamic diffusion process, and the optimal control strategies efficiently inhibit the spread of fraud information in MSNs. In conclusion, this paper offers a comprehensive approach to understanding and controlling fraud information diffusion, emphasizing the importance of minimizing control resource consumption and mitigating individual losses.

II. LITERATURE REVIEW

Online task assignment for crowdsensing in predictable mobile social networks,M. Xiao, J. Wu, L. Huang, R. Cheng, and Y. Wang ,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 makespan 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 makespan sensitive Online Task Assignment (AOTA) algorithm and a Largest makespan 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.

2.Predicting the evolution of hot topics: A solution based on the online opinion dynamics model in social network,L. Jiang, J. Liu, D. Zhou, Q. Zhou, X. Yang, and G. Yu, 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 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.

3. An on-demand coverage based self-deployment algorithm for big data perception in mobile sensing networks,Y. Lin et al,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.

III.EXISTING SYSTEM:

In the current landscape of Mobile Social Networks (MSNs), the proliferation of fraud information spreading has become a significant concern. The existing systems often rely on traditional security measures and static control strategies that struggle to keep pace with the dynamic nature of fraudulent activities. These systems typically lack the adaptability and real-time response capabilities required to effectively mitigate the ever-evolving tactics employed by malicious actors in

spreading fraud information within MSNs.

IV.PROPOSED SYSTEM:

The proposed system introduces a paradigm shift by incorporating dynamic control mechanisms to counteract the spread of fraud information in Mobile Social Networks. Leveraging advanced machine learning algorithms and real-time data analysis, the system aims to identify patterns, anomalies, and emerging trends associated with fraudulent activities. By dynamically adjusting control measures based on the evolving threat landscape, the proposed system seeks to enhance the responsiveness and effectiveness of fraud information control. Additionally, the integration of user behavior analysis and sentiment detection algorithms contributes to a more holistic approach in identifying and thwarting fraudulent content.

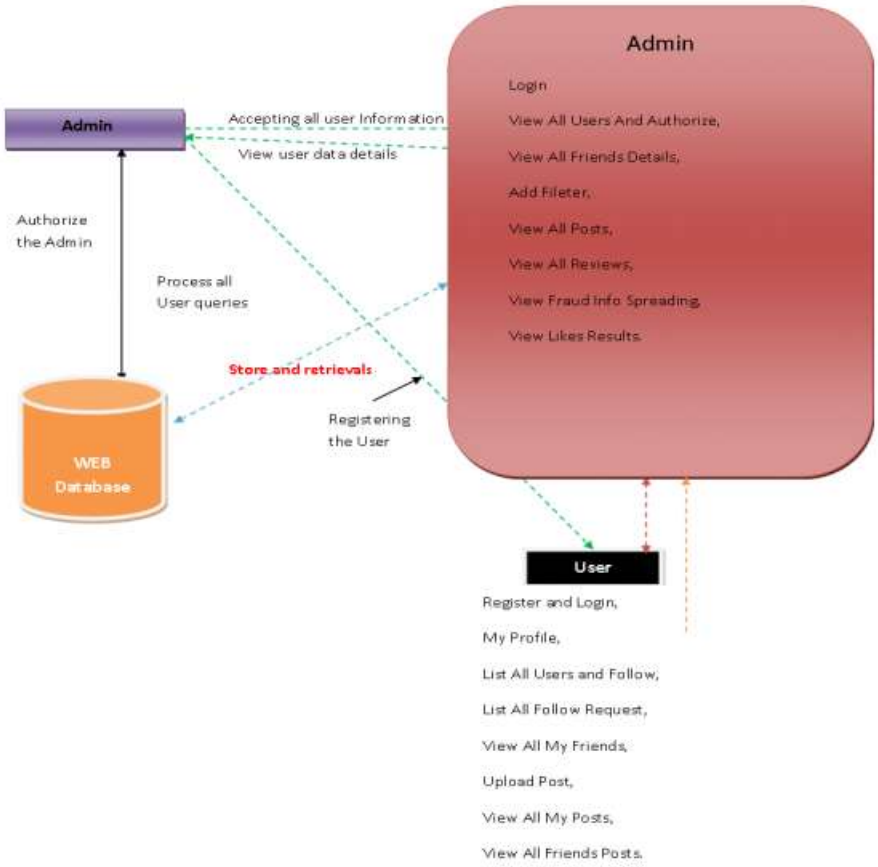

Fig 1 : System diagram

V.IMPLEMENTATION

Modules:

Admin

User

Modulesdescsription:

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 fingerprint and Login Once Login is successful user can perform some operations like List All Users and Follows, 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.

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.

VII.REFERENCES

[1] M. Xiao, J. Wu, L. Huang, R. Cheng, and Y. Wang, "Online task assignmentfor crowdsensing in predictable mobile social networks," IEEETrans. 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 theevolution of hot topics: A solution based on the online opinion dynamicsmodel in social network," IEEE Trans. Syst., Man, Cybern., Syst., to bepublished.

[3] Y. Lin *et al.*, "An on-demand coverage based self-deployment algorithmfor 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 impactof 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 differentialgame 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," IEEETrans. 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 competitionof 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 roleof 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, "Usingsubscriber usage profile risk score to improve accuracy of telecommunicationfraud detection," in *Proc*. IEEE

CYBERNETICSCOM, 2016,pp. 127–131.

[10] J. Ma et al., "Detecting rumors from microblogs with recurrent neuralnetworks," in Proc. IJCAI, 2016, pp. 3818–3824.

[11] (Aug. 2016). Tsinghua University Teachers Cheated 17 Million 600Thousand? The Original Liar Used This Psychological Routine![Online]. Available: http://www.bestchinanews.com/Domestic/2426.html

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

[13] K. Zhu and L. Ying, "Information source detection in the SIR model: Asample-path-based approach," IEEE/ACM Trans. Netw., vol. 24, no. 1,pp. 408–421, Feb. 2016.

[14] Z. Chen, K. Zhu, and L. Ying, "Detecting multiple information sourcesin networks under the SIR model," IEEE Trans. Netw. Sci. Eng., vol. 3,no. 1, pp. 17–31, Jan./Mar. 2016.

[15] A. Y. Khrennikov, Information Dynamics in Cognitive, Psychological,Social, and Anomalous Phenomena, vol. 138. New York, NY, USA:Springer, 2013.

[16] R. Lachman, J. L. Lachman, and E. C. Butterfield, CognitivePsychology and Information Processing: An Introduction. London, U.K.:Psychology, 2015.

[17] S. Wen, M. S. Haghighi, C. Chen, Y. Xiang, W. Zhou, and W. Jia, "Asword with two edges: Propagation studies on both positive and negativeinformation in online social networks," IEEE Trans. Comput., vol. 64,no. 3, pp. 640–653, Mar. 2015.

[18] E. Kušen, M. Strembeck, G. Cascavilla, and M. Conti, "On the influenceof emotional valence shifts on the spread of information in socialnetworks," in *Proc*. IEEE/ACM ASONAM, 2017, pp. 321–324.

[19] K. Kandhway and J. Kuri, "Using node centrality and optimal control tomaximize information diffusion in social networks," IEEE Trans. Syst.,Man, Cybern., Syst., vol.

47, no. 7, pp. 1099–1110, Jul. 2017.

[20] A. Nematzadeh, E. Ferrara, A. Flammini, and Y.-Y. Ahn, "Optimalnetwork modularity for information diffusion," Phys. Rev. Lett., vol. 113,no. 8, 2014, Art. no. 088701.

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

[22] X. Wang, Y. Lin, Y. Zhao, L. Zhang, J. Liang, and Z. Cai, "Anovel approach for inhibiting misinformation propagation in humanmobile opportunistic networks," Peer-to-Peer Netw. Appl., vol. 10, no. 2,pp. 377–394, 2017.

[23] Q. Zhao, C. Wang, P. Wang, M. Zhou, and C. Jiang, "A novel method oninformation recommendation via hybrid similarity," IEEE Trans. Syst.,Man, Cybern., Syst., vol. 48, no. 3, pp. 448–459, Mar. 2018.

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

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