MANAGING FRAUD INFORMATION PROPOGATION IN MOBILE SOCIAL NETWORKS

Kandika Aparna,Assistant professor CSE,Vaagdevi College of Engineering (Autonomous),India
P.Poojitha,UG Student,CSE, Vaagdevi College of Engineering(Autonomous),India
H.Nandhini,UG Student,CSE, Vaagdevi College of Engineering(Autonomous),India
D.Samatha,UG Student,CSE, Vaagdevi College of Engineering(Autonomous),India
MD.Amaanuddin,UG Student,CSE, Vaagdevi College of Engineering (Autonomous),India

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, MSNshave 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 modelfor 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 dynamicsmodel. 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: MSN, rampant rumors, fraudulent activities, fraud information, optimal control strategies.

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 theacademia [2], [3]. However, the development of MSNs is like a double-edged sword [4], [5]. WhenMSNs 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 becomingmore 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 MSNshas 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 2015 [10]. A piece of rumor saying"shootouts and kidnappings by drug gangs happening near schools in Veracruz" spread in Twitterand Face book. This rumor caused severe chaos in the city and many serious car crashes happenedamid 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 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.

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 needto 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 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 [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.

LITERATURE SURVEY

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 solvethe problems, we propose an Average makespan sensitive Online Task Assignment (AOTA)[15] 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 ratiosof 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.

1. Predicting and utilizing the evolution trend of hot topics is critical for contingency managementand 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 concludingthe 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 theevolution trend of an event. The quantitative predictions of the HK model cannot be used to makedecisions, whereas the results of the OOD model are proved to be acceptable.

2. Mobile Sensing Networks have been widely applied to many fields for big data perception suchas 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[18] algorithm for big data perception based on mobile sensing networks in this paper. Firstly, by considering characteristics of mobile sensing nodes, we extendthe 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 intelligentlydecide 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, theaverage 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.

PROBLEM STATEMENT

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 [13], [14]. The most widelyused model is the susceptible-infected recovered (SIR) model, in which all individuals are divided into three categories: 1) susceptible; 2) infected; and 3) 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 informationin 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 [15], [16]. Second, the fraud information diffusion processes in MSNs are the complex results of the continuous interactions of nodes in different states [17]. Third, because of the psychological effect, repeated reception of the same information may give users the feelingof 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 newcharacteristics, 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.

PROPOSED SYSTEM

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 ofthis 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[23]. It can more effectively describe the dynamic diffusion process of fraud information inMSNs. In addition, we theoretically analyze the stability of the *SWIR* model and the trend of fraudinformation 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 t o 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 overtime 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[24],[25]. In particular, the optimal dynamic allocation control strategies can achieve minimum control resources consumption and losses of individuals.

IMPLEMENTATION

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 bechanged

to accepted or else the status will remains as waiting.

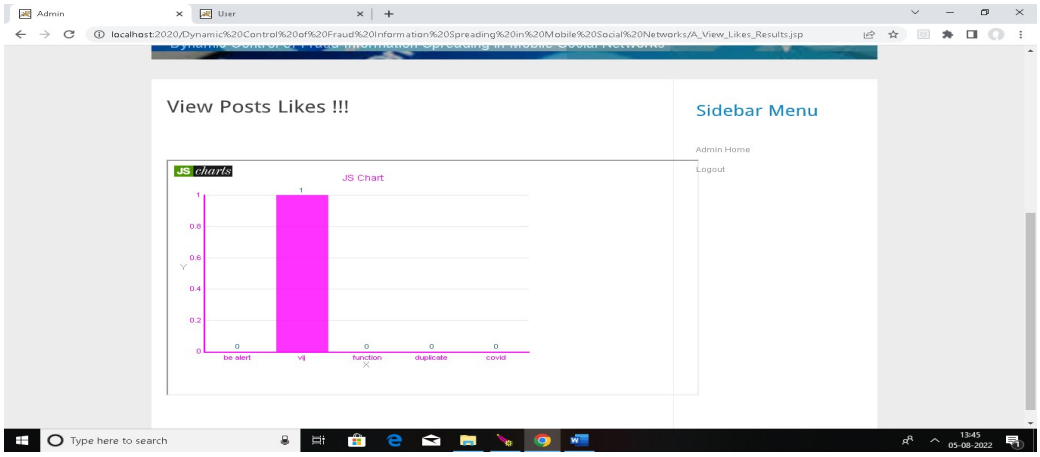
User

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.

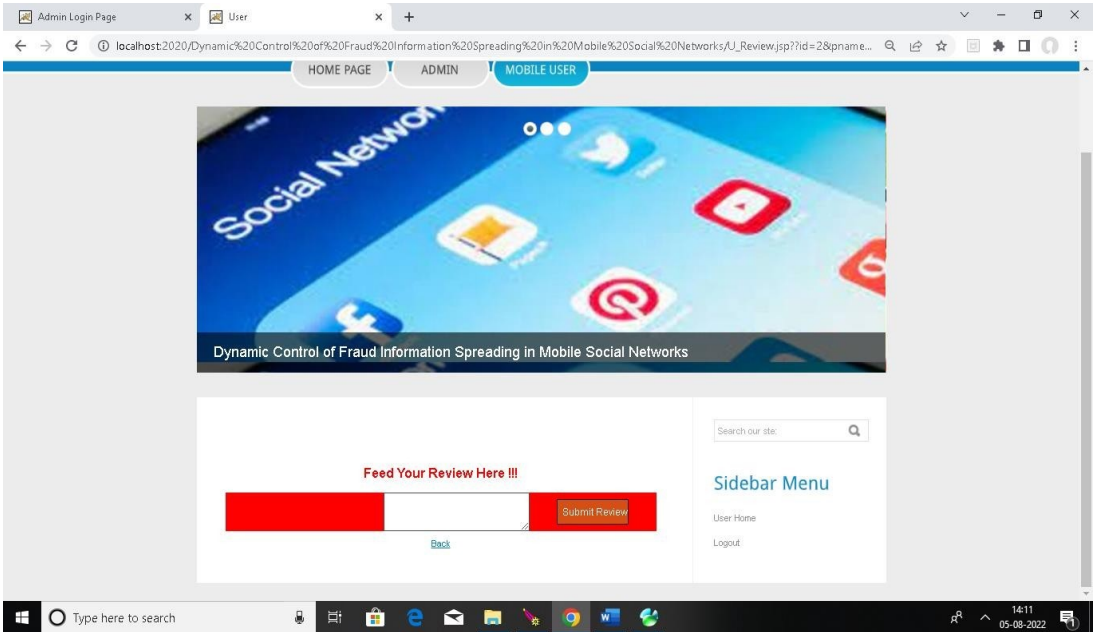
Searching Users to make friends

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.

3.EXPECTED RESULT



view posts likes



Feed user reviews here

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 SWIRdynamics 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 cognitionon information diffusion.

REFERENCES

[1] M. Xiao, J. Wu, L. Huang, R. Cheng, and Y. Wang, "Online task assignmentfor crowdsensingin 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 perceptionin 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 OriginalLiar 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 theSIR 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.

