DESIGN INCENTIVE MECHANISM FOR MULTIPLE MALICIOUS USERS DETECTION IN SOCIAL NETWORKS

[1]V. Nirmala,[2]B. Janardhan

[1]Assistant Professor ,[2]MCA Student

[1]MCA Department,

[1,2] Annamacharya PG college of Computer Studies , Rajampet, Y.S.R kadapa, Andhra Pradesh, India

Abstract*:*

Design Incentive Mechanism for Multiple Malicious Users Detection in Social Network Recent work focus on Social networks, a new technology drastically increasing on security related issues a dramatic popularity based malicious user detection is one of fundamental issues. So many works focused on active detecting malicious users by validating signal correlation based on large scale social networks familiar with digital marketing. In existing system works limited with terrible impact on the network, in terms of degrading the network's performance, reducing the network's efficiency and even disabling the whole network. In proposed work, designing a new inducement based on mechanisms to encourage the participation of users, which yields inferences problem, to solve this issues. Proposing inducement mechanism which designed in two categories Full and partial information. All existing works focused on full information based but neglecting partial based information also leads major issues especially in social networks it may allow attackers to grab details regarding customers in social networks like twitter, Facebook, LinkedIn etc. When malicious users perform abnormal activities such as advertisement inject, the users who are the victims of these activities can report them to the system administrator

IndexTerms- Introduction, design incentive mechanism, multiple malicious users detection, social networks-

1. Introduction

The past few years have witnessed the dramatic popularity of social networks. They greatly facilitate our daily lives and connect us with a world-wide virtual society. Meanwhile, security issues in these networks are attracting more and more research attention, one of which is the malicious user's detection. For example, the author's collected one-month sample of Twitter data, examined 25 million unique URLs and found that over two million URLs are scams, malware, and phishing. It is also shown in that 3.6 million U.S. adults lost a total of 3.2 billion dollars due to phishing attacks in 2007. Therefore, the malicious users in social networks have a terrible impact on the network, in terms of degrading the network's performance, reducing the network's efficiency, increasing the cost or even disabling the whole network. It is pressing to detect malicious users and isolate them efficiently most existing works are concerned with actively detecting malicious nodes. One approach is focusing on data received by sensors. If some data do not meet the certain criteria such as spatial correlation or frequency correlation, there may be malicious nodes. For example, sensory data in wireless sensor networks are usually location dependent. The malicious nodes can be identified if their reported data are far discrepant from that of nearby sensor nodes. Another approach that is frequently adopted is to measure the degree of the consistency of the nodal behavior in social networks.

However, it is challenging to employ previous studies for malicious user detection in social networks. First of all, the number of nodes is extremely large in social networks. It is thus time-consuming for the system administrator to examine each node. Further, malicious nodes typically discontinuously attack other nodes for some specific tasks. It is extremely difficult to differentiate them by their historical behaviors, since the difference between normal nodes and malicious nodes is not that conspicuous. Also, mistaking normal nodes as malicious nodes will impair the reputation of system operator, discouraging users from joining the networks. In this project, we propose an approach to detect malicious users in large-scale social networks from a radical new perspective. The system administrator is not directly participated in the detection process. Instead, it the power of normal users in the social networks to accomplish such a difficult goal, i.e., users sourcing the detection tasks to the users. When malicious users perform abnormal activities such as cyber-attack or advertisement injection, the users who are the victims of these activities can report them to the system administrator. Obviously, in such a way, the detection cost for malicious cost can be significantly reduced since no additional overhead is incurred. Also, the detection accuracy can be increased. One fundamental issue in users sourcing based approach is inducement mechanism design. Since different users have different preferences for these malicious activities, many users may choose to stay silent without a proper incentive. Further, malicious users may provide compensation for the victims to keep them silent. For example, a malicious user may send an advertisement to user alongside with a coupon or monetary reward. In such case, incentive provision is critical to encourage the participation of users.

We investigate the inducement mechanism to encourage the user participation in the malicious user detection in social network. Interestingly, we consider that the malicious users may provide incentives to the normal users when it performs malicious activities towards user ui. For example, if a malicious user wants to get users' profile information, providing some incentives can keep more users silent. Besides, users' preferences are typically different for malicious activities. Some users are more tolerant of advertisement injection than other users. We adopt contract theory to tackle our problem i.e., we construct contractual arrangements as incentive mechanism for system administrator to encourage users to help detect the malicious user.

•We introduce a novel, efficient, and effective approach, i.e., users sourcing, to detect malicious users in social networks. Based on this, in order to encourage sufficient users to perform detecting tasks, we formulate the incentive mechanism design problem.

•We solve the inducement mechanism design problem in two scenarios: full information of users' preferences and partial information of users' preferences. In full information scenario, we design the optimal incentive mechanism by ordering users' preferences. In partial information scenario, assuming that we only have statistical information about users' preferences, we transform this problem to an optimization problem and solve it by exploring the form of its solution.

Purpose

The application purpose is identifying the malicious users based on inducement mechanism in large scale social networks.

Scope

The scope is detecting the malicious users in social network by users' source using the users profile information with full and partial information.

Existing Work

Recent Research work focus on Social networks, new technology drastically increasing security related issues being this situation a high dramatic popularity based malicious user detection is one of fundamental issues. So many researchers focused on active detecting malicious users by verifying signal correlation based on social networks familiar with digital marketing but secured base information is another issue. In existing system works limited with terrible impact on the network, in terms of degrading the network's performance, reducing the network's efficiency and even disabling the whole network.

limitations

- The malicious user cannot be easily detected by the system administrator of nearly users.
- Most existing works focus on actively detecting malicious users by verifying signal correlation. It may not work well in social networks.

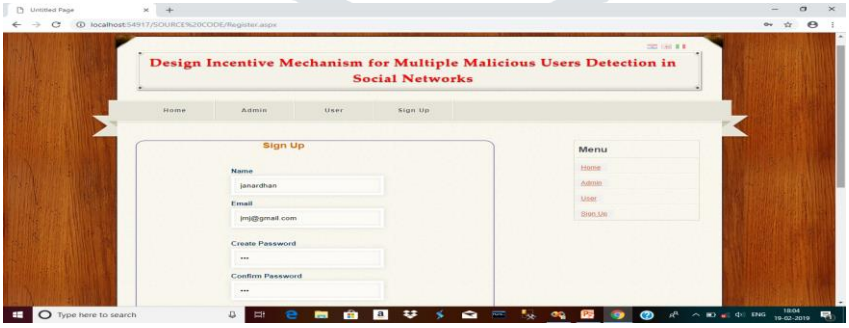
Proposed Work

In proposed work, designing a new incentive based mechanisms to encourage the participation of users in partial or full information, which yields inferences problem, to solve this issue. Proposing incentive mechanism which designed in two categories Full and partial information. All existing works focused on full information based but neglecting partial based information also leads major issues especially in social networks it may allow attackers to grab details regarding customers like what app, twitter, Facebook etc. When malicious users perform abnormal activities such as advertisement inject, the users who are the victims of these activities can report them to the system administrator.

Advantages

- The malicious users can be detecting by administrator easily.
- It is designed with the optimal inducement mechanism by ordering user's preferences.
- It will effectively be identifying the malicious user's because it will identify based on the user's feedback.

IV. RESULTS AND DISCUSSION



Screen 1: Sign Up

Description: Open Signup page for enter the fields to user signup.

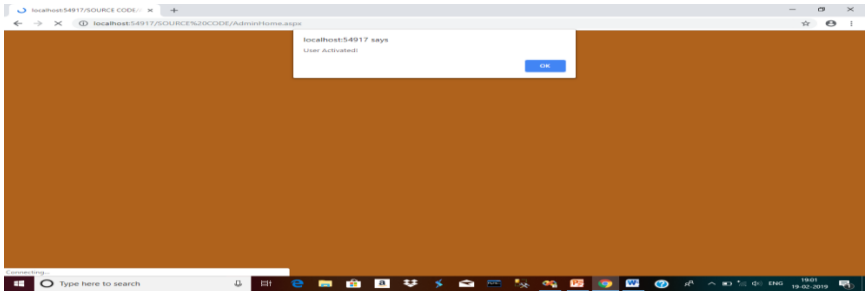
Screen 2: Profile Picture
Description: Upload the profile picture to User.

Screen 3: Account Created successfully
Description: User account was created successfully**.**

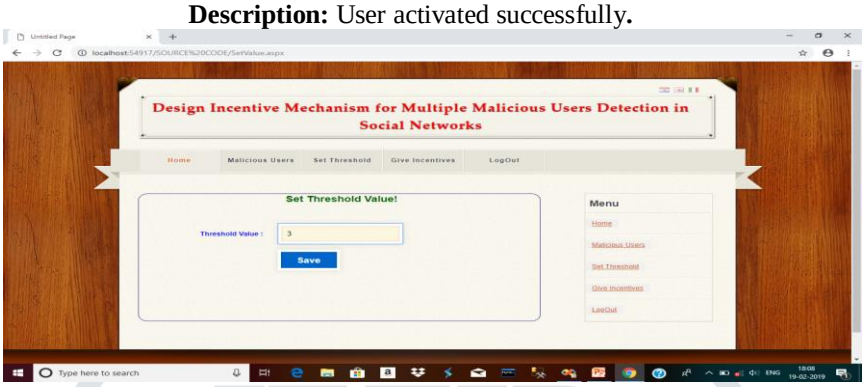
Screen 4: Account Not Activated
Description: User sign in page but account was not activated yet**.**

Screen 5: Admin Sign In
Description: Admin sign in page enter the username and password then sign in the page

Screen 6: Activate Users
Description: In this screen admin can activate the inactivate user

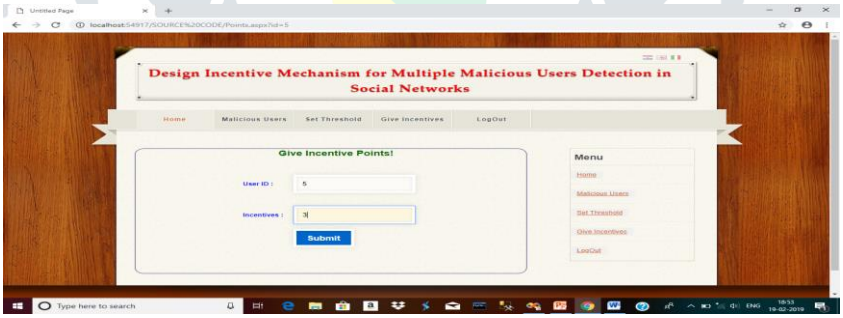


Screen 7: User Activated
Description: User activated successfully**.**



Screen 8: Set Threshold Value
Description: In this screen admin can alert the set threshold value to users.

Screen 9: Give Incentives to Users
Description: Admin can give incentives to activate users.

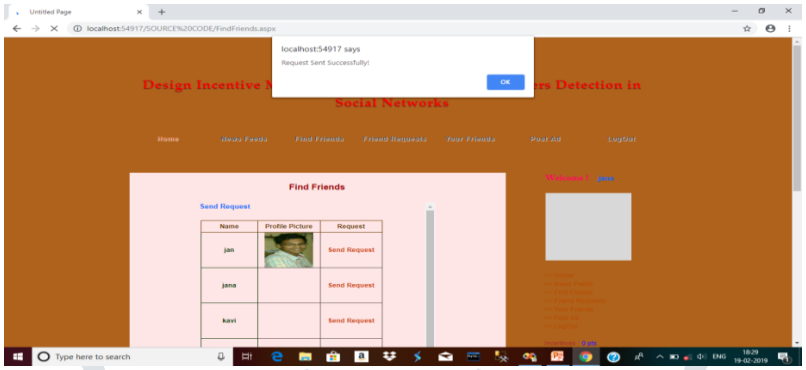


Screen 10: Give Incentive Points
Description: Admin can be give incentive points to use

Screen11: Share post
Description: In this screen User Can Share the post.

Screen 12: Find Friends

Description: In this screen user can find the friends and send the friend request.



Screen 13: Request Sent Successfully

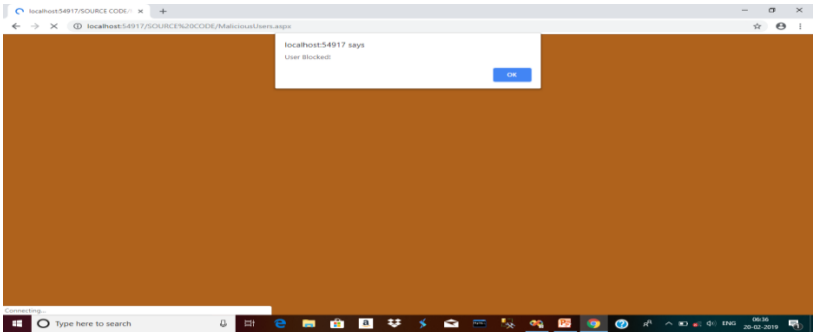
Description: In this screen user can sent friend request successfully.

Screen 14: View Friend Requests

Description: In this screen user can view the friend requests then accept or ignore based on users.

Screen 15: Malicious users

Description: In this screen can be seen the malicious users of promoting irrelevant products.



Screen 16: User Blocked

Description: In this screen admin is blocked the malicious user.

Screen 17: Account was blocked

Description: In this screen appeared the user account is blocked.

Conclusions

In this project, we investigated the malicious user detection in the social networks using user sourcing, considering that the malicious user may avoid being reported normal users through providing some inducement and users have different preferences for the malicious user.Corresponding incentive schemes were also devised. We have also conducted simulations to illustrate the impact of different factors on the total cost of the system. **Future Enhancements:**In the future work, we will consider the collective impact of multiple malicious users and the inducement mechanism design for scenarios where different users may have different distribution of its preference. Also, we will consider that the malicious user may optimize the constant incentive *B*. In such case, the malicious user may want to maximize its own payoff and the system may want to minimize its cost. The problem can be transformed as a game.

.**References**

[1] J. Chen, Q. Yu, B. Chai, Y. Sun, Y. Fan, and X. Shen, "Dynamic channel assignment for wireless sensor networks: a regret matching based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 1, pp. 95–106, 2015.

[2] J. Chen, J. Li, S. He, T. He, Y. Gu, and Y. Sun, "On energy-efficient trap coverage in wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 10, no. 1, pp. 2:1–2:29, 2013.

[3] G. Han, C. Zhang, L. Shu, and J. J. Rodrigues, "Impacts of deployment strategies on localization performance in underwater acoustic sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 3, pp. 1725–1733, 2015.

[4] Y. Zhang, S. He, and J. Chen, "Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks," *IEEE/ACM Transactions on Networking*, 2015. DOI: 10.1109/TNET.2015.2425146, to appear.

[5] C. Zhou, Z. Shi, Y. Gu, and N. A. Goodman, "DOA estimation by covariance matrix sparse reconstruction of coprime array," in *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, pp. 2369–2373, 2015.

[6] M. Dong, X. Liu, Z. Qian, A. Liu, and T. Wang, "Qoe-ensured price competition model for emerging mobile networks," *IEEE Wireless Communications*, vol. 22, no. 4, pp. 50–57, 2015.

[7] L. Kong, L. He, X.-Y. Liu, Y. Gu, M.-Y. Wu, and X. Liu, "Privacypreserving compressive sensing for crowdsensing based trajectory recovery," in *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*, pp. 31–40, 2015.

[8] K. Wei, M. Dong, K. Ota, and K. Xu, "CAMF: Context-aware message forwarding in mobile social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2178–2187, 2015.

[9] J. Liu, N. Kato, J. Ma, and N. Kadowaki, "Device-to-device communication in lte-advanced networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1923–1940, 2015.

[10] J. Liu, X. Jiang, H. Nishiyama, and N. Kato, "Performance modelling for relay cooperation in delay tolerant networks," *Springer Mobile Networks and Applications*, vol. 18, no. 2, pp. 186–194, 2013.

[11] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang, "Big data-driven optimization for mobile networks toward 5g," *IEEE Network*, vol. 30, no. 1, pp. 44–51, 2016.