IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Dispersion of Cheating Behaviours in Online Social Networks

Shagufta Samreen[1*], Shilpa.K.S [2], Sneha. K.B[3], Sneha Pal[4], Sagar.B[5]

[1,2,3,4,5]Department of Computer Science, East West Institute of Technology, Bengaluru, India

DOI: https://doi.org/10.26438/ijcse/v7si15.133137 | Available online at: www.ijcseonline.org

Abstract: Social contact are know to be spread through human behaviours. The diffusion process on social networks has also been grip to spread the undesirable dispersion.The main attention is to attract the contagion of malicious or even criminal behaviors in online social networks. Here, we study the social contagion problem of cheating behavior found in the massively multiplayer online role playing game (MMORPG) that provides a lifelike environment with rich and realistic user interactions. It has a strong chance of being noticed by their friends and leading them to cheat themselves due to their abnormal behaviour. In this paper, we show the existence of the dispersion of cheating. We then explore various possible social reinforcement mechanisms after introducing several factors to quantify the effect of social reinforcement on the dispersion and analyze the dynamics of bot diffusion in an extensive user interaction log from a major MMORPG.

Keywords— Dispersion, SVM, Social influence model

I. Introduction

Quantification of collective human behavior poses a unique, century old challenge. Only recently it became most evident in the context of economics and finance, which costs are associated to misconceptions of human collective behavior. The dispersion of behavior has long been studied in marketing, politics and sociology[5]. For instance, social influence takes many forms and can be seen in socialization. Emotions such as happiness and depression have also been shown to be socially contagious even in an online social network devoid of face-to-face interactions ,a user’s emotion is affected by their friends’ emotions. Obesity , and suicide ,as well as positive behaviors such as generosity toward strangers were observed to be socially dispersion as well[8]. The network structure of who is connected to whom can critically affect the extent to which a behavior diffuses across a population .There are two competing hypotheses about how network structure affects diffusion. The “strength of weak ties” hypothesis predicts that networks with many “long ties” will spread a social behavior in which ties are highly clustered[6]. This hypothesis treats the spread of behavior as a simple contagion, such as emotion. The power of long ties is that they reduce the redundancy of the diffusion process by connecting people whose friends do not know each other, thereby allowing a behavior to rapidly spread to other areas of the network.

We focus on MMORPGs among many forms of cyber spaces. MMORPGs provide an ideal opportunity to study human behavior, as they provide a lifelike environment with a rich set of realistic user action types. The importance of understanding cheating behavior in MMORPGs is deeply tied to the very nature of the games. To many game players, the major attraction of MMORPGs is the satisfaction of success and achievement in the game, often measured by the player level. It has an undesirable effect of encouraging some players to cheat to easily accumulate the resources necessary for levelling up. The most common cheating method is to employ a so-called ``game bot", an automated program that typically performs menial and repetitive tasks that humans may find cumbersome or boring. Game bots thus seriously threaten the integrity and the balance of the game as a whole, potentially driving out honest players. These actions of individual players are known in conjunction with their surroundings, i.e. the circumstances under which particular actionsor decisions were taken.

To study the social contagion, we should notice that the behavior diffusion occurs mainly due to two reasons of social contagion and homophily. Social contagion refers the phenomena that the correlated behaviors happen due to the influence of neighbours in the social network. Homophily refers the phenomena that people with similar characteristics exhibit correlated behaviors. When we merely observe the behavior diffusion, it is difficult to distinguish the social contagion and homophily. Many observational studies on behavior contagion fail to distinguish genuine social contagion from homophily and tend to perceive the correlated behaviors as social contagion. The social contagion is exaggerated when it is not distinguished from correlated behaviors. In this study, when we examine the social contagion of malicious behavior in the online community, we test whether correlated behaviors come from social contagion .

II. Related Work

M. Bampo, M. T. Ewing, D. R. Mather, D. Stewart, and M. Wallace.,“The effects of the social structure of digital networks on viral marketing performance”[1] where reduction of the process and investigate the formation of the activated digital network as distinct from the underlying social network and analyse of the actual viral marketing campaign and use the observed data to develop and validate a computer simulation model for viral marketing and the number of simulation experiments were conducted to predict the spread of a viral message within different types of social network structures under different assumptions and scenarios. [2] J. Goldenberg, B. Libai, and E. Müller, “Talk of the network: A complex systems look at the underlying process of word-of-mouth”, where the personal communication between closer and stronger communications that are within an individual's own personal group (strong ties) and weaker and less personal communications that an individual makes with a wide set of other acquaintances and colleagues (weak ties) were identified. Disadvantages of this paper is the effect of strong ties diminishes as personal network size decreases. Market attributes were also found to mediate the effects of weak and strong ties. When personal networks are small, weak ties were found to have a stronger impact on information dissemination than strong ties.[3] T. Heverin and L. Zach, “Use of microblogging for collective sense making during violent crises: A study of three campus shootings”, where analysis of patterns of microblogging communications found that information-sharing behaviors dominated the early response phase of violent crises, and opinion sharing increased over time, peaking in the recovery phase of the crises. The analysis of individual microblogging communications identified various themes in the conversation threads that not only helped individual contributors make sense of the situation but also helped others who followed the conversation. Disadvantages of this paper is It won't support for detecting cheating behavior group [4] J. Kleinberg, “The convergence of social and technological networks” , where the artifacts that have sprung from this development sites broader process at work, a growing pattern of movement through online spaces to form connections with others, build virtual communities, and engage in self-expression was discussed. Disadvatages of this paper was It wont suitable for large and dynamic data.

III. METHODOLOGY

1.DATASET Collection: The data we analyzed comes from Aion, an MMORPG serviced by NCSoft, Inc., a major Korean game developer and service provider. First released in Korea in 2008, Aion is now serviced in China, Japan, Taiwan, Australia, Europe, North America, and Russia. We used the data from a server among over 40 servers. The game company operates several servers to maintain clients and increases servers as users increases. Users can select a server when they start a game. Thus, it can be said that the data collected from a server among many server is a random sample. The data contains anonymized records of in-game interactions and bot detection events between December 21, 2010, and March 21, 2012. In total, 94,444 unique characters were played by 39,416 unique players, among these 14,326 characters of 11,259 players were suspected of gamebot use. A total of3,629,282 actions were detected to be taken by gamebots.

2. FRIENDSHIP NETWORK The social interactions occur on the social network of players as the pathway, and thus the network structure has an important effect on the diffusion process. Here we examine the social network of players in our data set. In Aion, a user can send a request to become friends to other users. When the users accept the request, they become friends as like Facebook. The user can make friends at maximum 100. Users sometimes unfriend to make a new friend.

The diameters of the friendship network of two MMORPGs tend to be relatively small, generating the small network. The clustering coefficients for two networks are much lower than those of other social networks. This indicates the lack of triads in the friendship network in MMORPGs, in other words, a friend of my friend is not likely to be a friend of mine. In addition, the average path length of online game networks is similar to Flick and Facebook networks while the clustering coefficient is much lower. The high clustering coefficient and low average path length indicates the small-world network, but the online game network does not exhibit the small world property. The social behavior shows a complex contagion that requires contact with multiple sources of infection before one adopts a behavior. The highly clustered network, especially small-world network, promotes the diffusion of behavior over the network by causing social reinforcement, meaning that in an MMORPG the malicious behavior may not infiltrate the entire network.

3.**DIFFUSION OF CHEATING BEHAVIORS** We considered game characters that did not use bots until January 14 (three weeks after our observation period began) as new bot users. We then traced the bot adoption on the social network of January 13. On the basis of the first day when tracking on the bot diffusion starts(January14),963of the 19,833 characters start using the game bot. Among the 19,833characters,10,508participateinafriendshipnetwork, and 128 characters are suspected to be new bot users in the friendship network. The bot adoption rate starts from 0.012 and reaches 0.11 in 40 days, after which it plateaus as showninFig.1.We traced the bot adoption rate as a function of time to determine to what degree the bot users penetrate the friendship network. The rate starts at 0.012 (128/10,508) and saturates at 0.11 (4,507/10,508).

First, we measure how many friends use the game bot. This is a direct social reinforcement from friends, which will make users more likely to adopt the game bot. This metric takes into account social reinforcement through non-redundant information memory characteristic that does not consider the repetitive signal from friends. In some cases, initiation of the behavior takes places through peer imitation, so the number of peers who take behavior is a significant reinforcement factor.

Second, we measure how many times botting friends use the game bot. This is the total cheating action count of friends of a user. Behavior is learned from peers' behavior, so the frequency of signal from peers affects the adopters' decision.

Third, we examine the effect of users' number of friends on behavior adoption. Social capital is embedded resource in social networks and is commonly represented as social ties that facilitate the flow of information and enhances the outcomes of actions. Criminal behaviors have been shown to be influenced by social ties such as friendship ties and kinship ties.

Fourth, we normalize the direct social reinforcement through the number of friends, equal to the number of bot-using friends divided by the total number of friends. This second metric assumes that 10 bot-using friends among 10 friends and 10 bot-using friends among 100 friends will have different effects on bot adoption.

Fifth, assuming that people who use bots more often should have more influence than those who do not, we introduce a measure equal to the total number of bot usages (cheating actions) by the most frequent user among ones' friends. Influentials can have the different influence. The probability of contagion increases with more exposure to and association with high–frequency users.

Finally, we count the number of banned friends because of bot usage. This acts as the inhibitory factor in bot adoption. The rudimentary form of learning is largely governed by rewarding and punishing consequences for behavior.

The followings are possible reinforcing or inhibiting factors of malicious social behavior.
1) The number of cheating friends *I*
2) Total cheating action count of friends *S*
3) The total number of friends *K*
4) The fraction of cheating friends *I*=*K*
5) Cheating action count of the most frequently cheating friend *M* (extreme-score)
6) The number of friends banned from the game because of cheating *Y* (anti-score)

We study the impact of each variable, as shown in Fig. 1. We group the players into new bot adopters and non-adopters, excluding ongoing bot users. We found that the more friends and more bot-using friends one has, they have a higher tendency to adopt game bots. However, the total cheating count of a friend appears to have a limited effect. The user's cohort of friends (center) comprises two different classes of users with regard to cheating behavior in an online game: cheaters (red) and normal, non-cheaters (green). For each cheater we have the number of cheating actions they took(squares). Some cheaters have been banned from the game (enclosed in an orange oval). We define five variables that quantify the potential influence of the cohort composition on the central user's adoption of cheating behavior: The total number of cheaters (four in this case, including banned users), the total cheating action count of one's friends, the total number of friends, the fraction of cheaters among one's friends (0:4), and the cheating actions of the most active cheater (6). As a factor that may inhibit one's desire to adopt a cheating action, the number of friends banned from cheating (1) was introduced.

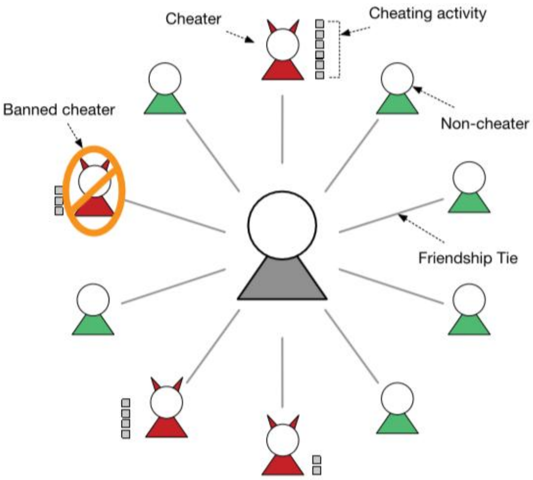
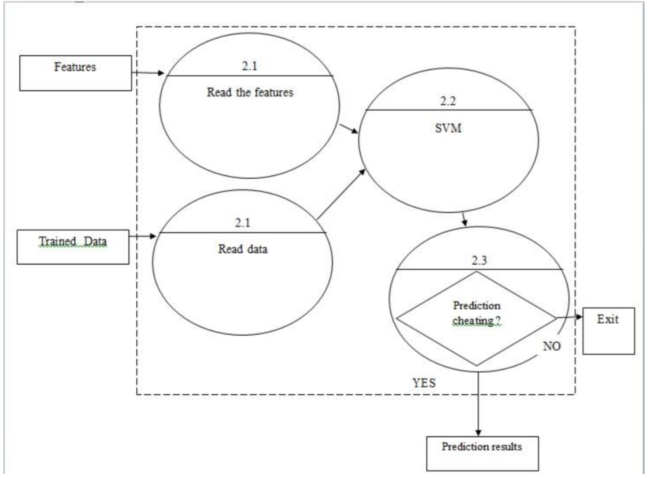


FIG1: System architecture

4.SOCIAL INFLUENCE MODEL We develop the social influence model to investigate how social influence affects to bot adoption. Based on the data analysis of previous sections, we derive the bot diffusion probability function at first. the rate of adoption according to the number of infective neighbors increases until the rate of bot-using friends over total friends reaches 33%; afterward, the rate decreases. To describe the relationship between the positive and the negative effects of the ratio of bot-using friends over total friends on the infection probability, we incorporate two terms ,one representing the polynomial increase as a function of I/k and other indicating the exponential delay.

IV. DESGIN

The figure 2 shows the data flow diagram. The features are extracted from pre-processing method and the features are read to the system. The trained data which is present in the system is also been read. These data are sent to the SVM where KNN algorithm is used to predict the behaviours. Then it can be segregated to cheating or non cheating behaviours. As per the predictions the non cheaters are existed for their further processing and the cheater will be existed from system completely.



V. ALGORITHM

KNN algorithm is used to predict the behaviours

```
Classify($\mathbf{X},\mathbf{Y},x$) //$\mathbf{X}$: training data, $\mathbf{Y}$: class labels of $\mathbf{X}$, $x$:unknown sample
    for $i = 1$ to $m$ do
        Compute distance $d(\mathbf{X}i,x)$
    end for
    Compute set $I$ containing indices for the $k$ smallest distances
        $d(\mathbf{X}i\ ,x)$
    return majority label for $\{\mathbf{Y}i$ where $i \in I\}$
```

The distance is calculate by using Euclidean Distance Formula

$$\mathbf{d(q,p)}=\sqrt{\sum_{i=1}^{n}(\boldsymbol{q_i}-\boldsymbol{p_i})^2}$$

VI. RESULTS AND DISCUSSION

As a result, they are reluctant to participate in the group's misbehavior.. Game companies employ game masters to manually monitor game play and detect abnormal user behavior. Here, the user within the cluster who are friends with each other will be able to interact with the system.once the cheating behaviour is been predicted they have been blocked to enter the system. Fig 3 will show that

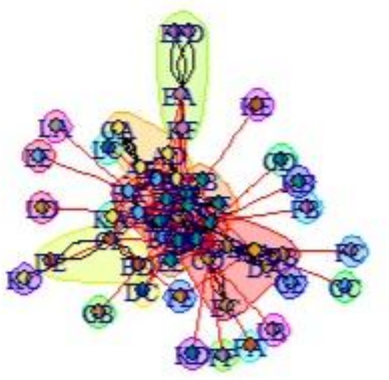


Fig 3: Cluster of cheaters and non cheaters

VII. CONCLUSION AND FUTURE SCOPE

Our main aim provided in this paper is the social contagion of malicious behavior in online games.We also explored the effect of social reinforcement on the adoption of malicious behavior which result showed that social reinforcement increases. Since it increases likelihood of the malicious behavior adoption also increases until social reinforcement reaches a certain level. Further, we presented a statistical analysis framework using data from a large social system to distinguish homophily and social influence. As a future work, we plan to perform an study that identifies influential spreaders of cheating behavior in online, investigates the effect of influential spreader on the diffusion process.

Our main aim provided in this paper is the social contagion of malicious behavior in online games.We also explored the effect of social reinforcement on the adoption of malicious behavior which result showed that social reinforcement increases. Since it increases likelihood of the malicious behavior adoption also increases until social reinforcement reaches a certain level. Further, we presented a statistical analysis framework using data from a large social system to distinguish homophily and social influence. As a future work, we plan to perform an study that identifies influential spreaders of cheating behavior in online, investigates the effect of influential spreader on the diffusion process.

ACKNOWLEDGMENT

The authors would like to thank the handling associate editor and all the anonymous reviewers for their constructive comments.

REFERENCES

[1] M. Bampo, M. T. Ewing, D. R. Mather, D. Stewart, and M. Wallace,``The effects of the social structure of digital networks on viral marketing performance," *Inf. Syst. Res.*, vol. 19, no. 3, pp. 273_290, 2008.

[2] J. Goldenberg, B. Libai, and E. Müller, ``Talk of the network: A complex systems look at the underlying process of word-of-mouth,'' *Marketing Lett.*, vol. 12, no. 3, pp. 211_223, 2001.

[3] T. Heverin and L. Zach, ``Use of microblogging for collective sensemaking during violent crises: A study of three campus shootings,'' *J. Amer. Soc. Inf. Sci. Technol.*, vol. 63, no. 1, pp. 34_47, 2012.

[4] J. Kleinberg, ``The convergence of social and technological networks,'' *Commun. ACM*, vol. 51, no. 11, pp. 66_72, 2008

[5] M. Szell and S. Thurner, ``Measuring social dynamics in a massive multiplayer online game,'' *Social Netw.*, vol. 32, no. 4, pp. 313_329, 2010.

[6] C. R. Shalizi and A. C. Thomas, ``Homophily and contagion are generically confounded in observational social network studies,'' *Sociol. Methods Res.*, vol. 40, no. 2, pp. 211_239, 2011.

[7] S. Aral, L. Muchnik, and A. Sundararajan, ``Distinguishing influence based contagion from homophily-driven diffusion in dynamic networks,'' *Proc. Nat. Acad. Sci. USA*, vol. 106, no. 51, pp. 21544_21549, 2009.

[8] L. Coviello *et al.*, ``Detecting emotional contagion in massive social networks,'' *PLoS ONE*, vol. 9, no. 3, p. e90315, 2014.

[9] S. Son, A. R. Kang, H.-C. Kim, T. Kwon, J. Park, and H. K. Kim, ``Analysis of context dependence in social interaction networks of a massively multiplayer online role-playing game,'' *PLoS ONE*, vol. 7, no. 4, p. e33918, 2012.

[10] A. Mislove, H. S. Koppula, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, ``Growth of the _ickr social network,'' in *Proc. 1st Workshop Online Social Netw.*, 2008, pp. 25_30.