IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 16, 2018, accepted April 26, 2018, date of publication May 7, 2018, date of current version June 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2834220

Contagion of Cheating Behaviors in Online Social Networks

JIYOUNG WOO[1], SUNG WOOK KANG[2], HUY KANG KIM[3], AND JUYONG PARK[4]

[1]Department of Big Data Engineering, Soonchunhyang University, Asan 31538, South Korea
[2]Data Analysis and Modeling Team, NCSOFT, Seongnam 13595, South Korea
[3]Graduate School of Information Security, Korea University, Seoul 02841, South Korea
[4]Graduate School of Culture Technology, KAIST, Daejeon 34141, South Korea

Corresponding author: Huy Kang Kim (cenda@korea.ac.kr)

This work was supported in part by Korea University and in part by the Soonchunhyang University Research Fund under Grant 20160854.

ABSTRACT Human behaviors are known to spread through social contact. The diffusion process on social networks has also been leveraged to understand the spread of undesirable contagion. The contagion of malicious or even criminal behaviors in online social networks is just beginning to attract attention. 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. Because cheating users boast an abnormal thus conspicuous degree of success, it has a strong chance of being noticed by their friends and leading them to cheat themselves. To detect and prevent cheating, it is beneficial to understand this dynamic as a contagion problem. In this paper, we show the existence of the contagion of cheating. We then explore various possible social reinforcement mechanisms after introducing several factors to quantify the effect of social reinforcement on the contagion and analyze the dynamics of bot diffusion in an extensive user interaction log from a major MMORPG.

INDEX TERMS Diffusion model, social contagion, social network, online game.

I. INTRODUCTION

Human behaviors are known to spread through social contact. The contagion of behavior has long been studied in marketing [1], [2], politics [3], and sociology [4], [5]. The word-of-mouth effect, for instance, is a central instrument in viral marketing campaigns, while the transmission and adoption of opinions is crucial in understanding various political and social issues. The diffusion process on social networks has also been leveraged to understand the spread of undesirable behaviors. For instance, the spread of the use of drugs, tobacco, and alcohol has been explored using various diffusion models, identifying a significant level of contagion between people [6]–[8]. Santonja *et al.* [9] and Romero *et al.*'s [10] epidemic models are well known for describing how extreme behaviors spread in a population, validated by political activity data. Emotions such as happiness and depression have also been shown to be socially contagious [11]; even in an online social network devoid of face-to-face interactions, a user's emotion is affected by their friends' emotions [12]. Obesity [13], [14], and suicide [15], which are regarded as personal issues, were also found to be socially contagious. Positive behaviors such as generosity toward strangers were observed to be socially contagious as well [16], [17]. The major principle behind it being understood to be that helping others without expecting a direct reciprocation can still produce a roundabout and indirect reciprocation.

With the wide adoption of online social network services as a preferred communication medium, social network analysis has proven itself useful for observing and understanding large-scale user behavior diffusion. For instance, Centola [18] performed experiments to trace the diffusion of health-related behaviors in online communities, analyzing the impact of the users' network characteristics on the behavior adoption. Romero *et al.* [10] studied the adoption of specific functionality of Twitter, finding differences in the adoption patterns between topics. The social network structure has been shown to play an important role in shaping people's behaviors, for instance by Christakis and Fowler [19] who reported evidence that generous behavior can indeed ripple through social networks. Hodas and Lerman [20] studied URL forwarding behavior in Digg and Twitter.

Here we study the social contagion problem of cheating behavior found in a cyber space, especially the game

bot problem. The cheating in a cyber space has been an social issue and a research topic in [21] and [22]. Previous works showed that the social network structure can be used for detecting cheating behaviors. They proposed a novel method to detect cheater groups. Beyond this finding, we aim to identify what factors of the social mechanism affect cheating behavior not merely social network. Our study tickles more fundamental issue of contagion process on the social network which forms a basis of malicious group detection.

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 leveling 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.

To study the social contagion, we should notice that the behavior diffusion occurs mainly due to two reasons [23]–[25] of social contagion and homophily. Social contagion refers the phenomena that the correlated behaviors happen due to the influence of neighbors 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 or not following the method in [23] and [24].

Our key contributions are summarized as follows: First, we introduced social reinforcement factors from related literature to show the social contagion of cheating behavior. We showed that as social reinforcement increases, the likelihood of the malicious behavior adoption increases until social reinforcement reaches a certain level. We showed our findings are consistent with the previous works reporting that likelihood to be involved in crime increases positively with the proportion of participants, but decreases after a certain point in case when the participants are being banned. Second, we presented a novel statistical model and analysis framework to distinguish homophily and social influence for cheating behavior. Our proposed model developed the previous model used in examining social influence for behavior that increase positively with the proportion of participants. Third, we performed the large-scale data analysis on a popular online game and showed the evidence of social contagion of malicious behavior in online games.

The remainder of our paper is organized as follows: We begin by showing the existence of the contagion of cheating. We then introduce several factors to quantify the contagion, explore various possible social reinforcement mechanisms, and analyze the dynamics of bot diffusion in an extensive user interaction data from a major MMORPG.

II. BACKGROUND

A. GAMES AND CHEATING BEHAVIORS

Players cheat in MMORPGs to easily level up and accumulate cyber assets, critical to increasing their success in the game and upgrading their abilities. MMORPGs are typically designed so that players must complete certain missions to achieve higher levels and accumulate in cyber assets. These missions often require repetitive actions, thereby prompting players to find the shortcut through illegitimate means. One of the most prevalent tools for cheating is the game bot that performs actions for the player. Because of the strongly social and interactive nature of MMORPGs, such tactics are easily spread to other players and seriously damage the integrity of the game. It is now well known that a so-called ''gold-farming groups'', enterprise-level businesses that operate a massive set of coordinated bots exist for real capital gain.

Game bots thus seriously threaten the integrity and the balance of the game as a whole, potentially driving out honest players. For this reason, using game bots is the leading cause of player banning in Aion, the MMORPG that we analyze here. Because a bot user may boast an abnormal thus conspicuous degree of success, it may have a high chance of getting noticed by their friends and leading them to adopt bots themselves. This mechanism is, however, not without any inhibitory control: the persistent threat of being banned from the game. Therefore, it is interesting and potentially beneficial to understand this dynamic as a contagion problem, as most current approaches to game bot detection and prevention focus on individual activity pattern analysis based on the hypothesis that cheaters would act significantly differently from non-cheaters. Game providers typically maintain large-scale logs of user interactions, allowing researchers to study human actions to a degree rarely afforded by other online services. MMORPGs have been the subjects of research on social interactions between users [26], [27]. The contagion of malicious or even criminal behavior in online game world, on the other hand, is just beginning to attract attention [28]–[30]. Blackburn *et al.*'s work [30] showed that cheating behavior spreads through a social mechanism: the number of cheater friends of a fair player is correlated with the likelihood of her becoming a cheater in the future. Based on this observation, we will examine social mechanism in various perspectives and provide statistical significance of social contagion, which has not been mentioned in previous works.

B. SOCIAL LEARNING

Behavior is acquired and shaped through imitation or modeling of others' behaviors; this entire process is referred as observational learning [31]. Reinforcement plays a role in learning. Cognitive behavior can be directly reinforced and can act as discriminative cues for other behaviors [31]. Social reinforcement is a form of conditioned reinforcement in which the reinforcer is involved some sort of interaction with others. Social reinforcement can be positive or negative. Positive social reinforcement can be defined as an event following response that increases the likelihood that the performer will repeat the response again under similar circumstances; similar to reward. Negative reinforcement can be defined as an event following response that removes an averse condition and increases the likelihood that the performer will repeat the response again under similar circumstances. Social learning theory and social reinforcement theory explain central learning concepts through reinforcement [32]. The general explanations of deviant behaviors such as crime, delinquency, drug addiction, and suicide come from social learning theory and more elaborate social reinforcement theory [33]–[37]. Deviant behaviors and criminal behaviors in the offline world are shown to be supportive of or consistent with social learning in much previous research [31]. However, the behaviors in online lack supportive studies.

The behavior diffusion does not happen just because of the social contagion. People who lay on the social network often exhibit correlated behaviors. This occurs mainly due to two reasons [23]–[25]. One is social contagion and the other is homophily. Social influence or social contagion means that the action of a user is triggered by their friends' actions [23]. Homophily or social correlation means that users often befriend others who are similar to themselves and thus perform similar actions [38]. It is particularly important to be mindful of the distinction between homophily and social influence because they are often confounded in observational social network studies [25]. A failure to do so would lead to an overestimation of the impact of influence in a contagion study.

Thus, the key challenge is to distinguish between homophily-driven diffusion and influence-based contagion, critical to the success of contagion management [24]. Some studies [23]–[25] pointed out this fallacy and suggested the methods that distinguish social contagion and homophily. Anagnostopoulos *et al.* [23] proposed a shuffle test and an edge-reverse test, which are applicable when the time-stamp of a user action is available. The shuffle test is based on the idea that if social influence does not play a role even though an agent's probability of activation is correlated with his or her friends', the timing of such activation should be independent of the timing of other friends' activation. The edge-reverse test, on the other hand, reverses the direction of all the edges and compares the diffusion process before and after. Therefore, if homophily leads the diffusion process, the reversing edge does not affect the diffusion dynamic.

The social contagion of cheating is exaggerated when it is not distinguished from correlated behaviors. It is also important to distinguish homophily and social contagion because proper intervention strategies differ for two cases. When a perceived contagion is due to homophily rather than social contagion, the intervention strategy should be designed based on the segmentation on population characteristics. The intervention strategies for social contagion should be designed from peer-to peer methods focusing on the network structure which provides the channel of contagion [24]. 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 or not following the method in [23] and [24].

III. EXPERIMENTS

A. DATASET

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 game bot use. A total of 3,629,282 actions were detected to be taken by game bots.

B. 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 [18], [39]–[41]. 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.

TABLE 1. Network information of a mature game (Aion), a recently launched game (ArcheAge), and two popular online social networks.

Social networks	Nodes, #	Links, #	Diameter	Avg. degree	CC[b] \Avg. path length
Aion (as of Jan-13)	18,761	80,026	15	4.3	0.073 \5.22
ArcheAge	11,433	33,724	13	3.0	0.076 \5.42
Facebook [a]	63,730	817,090	N/A	25.7	0.22 \7.0
Flickr	2,302,924	22,838,276	27	20.9	0.18\5.67
YouTube	3,223,588	9,376,594	21	5.8	0.09\5.10

[a] Facebook refers the New Orleans network
[b] CC: Clustering coefficient

Table 1 presents the characteristics of the friendship network of Aion. We referred Son *et al.*'s work [27] to compare the online game network with other online social networks. The Facebook network collected from Facebook New Orleans networks [42], the Flicker network [43], [44], and Youtube referenced in [45]. The Aion data as of Jan-13 is retrieved from a server from 44 servers. Compared with well-known social networks, Aion tends to have fewer friends, resulting in a smaller network. For comparison, we examined another MMORPG, ArcheAge. ArcheAge is a recently launched MMORPG developed by XLgames; its social network is still in its initial stage, and thus presumably free of game bots. The ArcheAge dataset includes all users' information in three months after pre-launching.

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 [18]. 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.

C. 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 (January 14), 963 of the 19,833 characters start using the game bot. Among the 19,833 characters, 10,508 participate in a friendship network, 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 shown in Fig. 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)

As shown in Fig. 1, the diffusion process occurs slowly, with no sudden outbreak or infiltration into the entire network. According to the threshold model, one of the representative contagion model, people usually require contacts with multiple sources of "infection" before being convinced to adopt a behavior [46]. To test the effect of social reinforcement on bot adoption, we measure social reinforcement

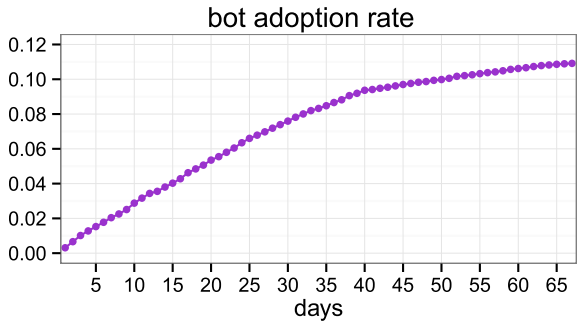

FIGURE 1. The rate of new adopters over total active characters in time order.

from various perspectives. In social contagion, memory of cumulative information typically plays an important role as reinforcement. The memory of cumulative information about the social behavior comes from redundant or non-redundant information [47]. Thus, we firstly measure the effect of redundant information and non-redundant information in terms of following two metrics.

1) 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 [48], so the number of peers who take behavior is a significant reinforcement factor. Previous research demonstrated a relationship between association with conforming or deviant peers and delinquent behavior [48]–[51]. Thus, the number of cheating friends is tested its effect on adoption of malicious behavior.

2) 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. According to Krohn *et al.*'s work [48], the adopters' usage frequency is shown to have significant effects on social learning. In behavior adoption, the number of signals from peers who engage in a behavior is examined as a reinforcement factor.

3) 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. The previous research explains the social ties work as surveillance and prevent the crime behaviors [52], [53]. Deviant behaviors have been shown to have the impact of dyadic social ties on initiation and cessation such as teenagers' smoking [54], [55]. Even personal health problem such as obesity also has been shown to have the effects of social ties [13].

4) 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.

5) 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. Akers [31] found the greater reinforcement for abuse from higher use over more moderate use.

6) 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 [32], [48]. Punishment works as negative reinforcement that decreases the likelihood that the response will be produced again under similar circumstances [32]. Observing friends being banned will work as negative social reinforcement.

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. 2. 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.

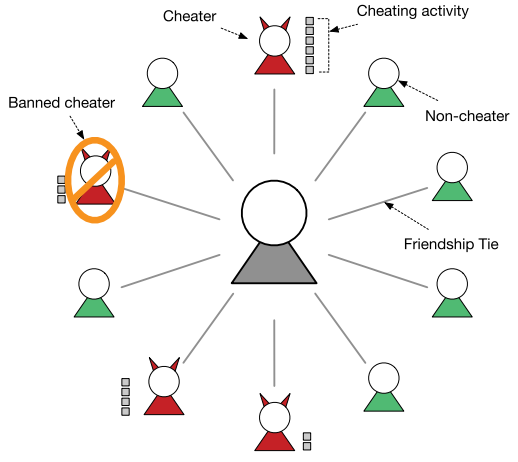

FIGURE 2. Social reinforcement mechanism.

The social reinforcement factors, I, K, I/K and M that show different CDF patterns for adopters and non-adopters as shown in Fig. 3. We compare CDFs to test the effect of social reinforcement on bot adoption. The solid line and dotted line represent the CDF of non-adopters and bot adopters respectively. The difference between the solid line and dotted line indicates that these two user types have different distributions in terms of social reinforcement factors. (a) S, (b) I, (c) K, (d) M, (e) I/K, (f) Y The experimental findings are quantified as the hazard ratio. To define the hazard ratio, the hazard rate should be defined in advance. The hazard rate is the event occurring rate per unit time, which indicates how likely a user experience contagion given that the user is still innocent at that time. The hazard ratio is the ratio of the hazard rates corresponding to the conditions described by two conditions of a control group and treatment group. To show how to calculate the hazard ratio, we firstly need to introduce the hazard rate.

$$h(t) = \lim_{\Delta t \to 0} \frac{\text{observed events in interval}[t, t + \Delta t]/N(t)}{\Delta t} \tag{1}$$

where N(t) is the number of risk events (contagion events in our case) at the beginning of an interval. The hazard ratio is estimated by the regression model with the log hazard rate as a function of baseline hazard rate h_0(t) and k risk factors, X.

$$log h(t) = f(h_0(t), \alpha + \beta_1 \cdot X_1 + \cdots + \beta_k \cdot X_k) \tag{2}$$

β_k is hazard ratio of X_k

In our case, it can be interpreted as the increment of risks of becoming bot users from users who have no bot friends and who have bot friends. We use the discrete-time hazard model [56] to estimate the hazard ratio. This regression-type model estimates regression coefficients corresponding to each variable in the model. Additionally, it gives p-values for testing the significance of each coefficient. We did not provide the coefficient estimation results that fail in the significance test. The hazard ratio and 95% confidence intervals corresponding to each factor are displayed in Table 2.

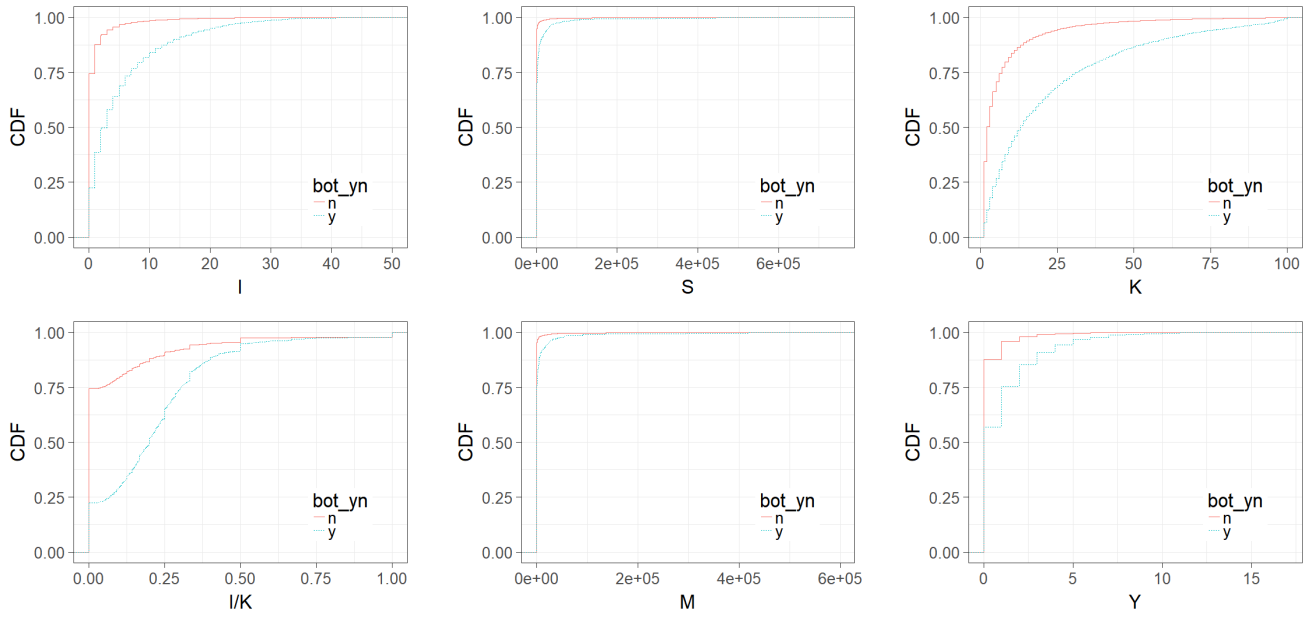

FIGURE 3. The cumulative distribution functions (CDFs) of new bot adopters(denoted as 'y') and non-adopters(denoted as 'n') according to social reinforcement.

TABLE 2. Hazard ratios and their 95% confidence intervals for bot usage adoption according to significant factors. The ratios and their intervals are generated from the Cox proportional hazards model.

Factor	Mean of hazard ratio	Lower bound	Upper bound
I	1.041	1.032	1.051
K	1.011	1.008	1.014
I/K	3.222	2.834	3.662
S	1.000	1.000	1.000
M	1.000	1.000	1.000

I/K has the highest hazard ratio, implying that the ratio of I/K has the largest influence on game bot adoption. Contrary to expectation, banning game bot users has minimal effect on game bot usage. On the individual level, the results show that a higher I/K increases the likelihood of adoption. In Fig. 4, we first take log-scale of I/K to carefully read the distribution at the lower value of I/K and then categorize the percentiles of the log scale of I/K to highlight the inflection point. We take granular categorization at the lower and higher values of I/K percentiles to highlight the decrease of the adoption rate in the higher value. The x-axis represents the I/K category divided by the percentiles of the log scale of I/K. I/K are categorized into 7 classes with $I/K = 0$ for class 0, $0 < I/K \leq 0.083$ for class 1, $0.083 < I/K \leq 0.132$ for class 2, $0.132 < I/K \leq 0.212$ for class 3, $0.212 < I/K \leq 0.333$ for class 4, $0.333 < I/K \leq 0.5$ for class 5, and $0.5 < I/K \leq 2.718$ for class 6.

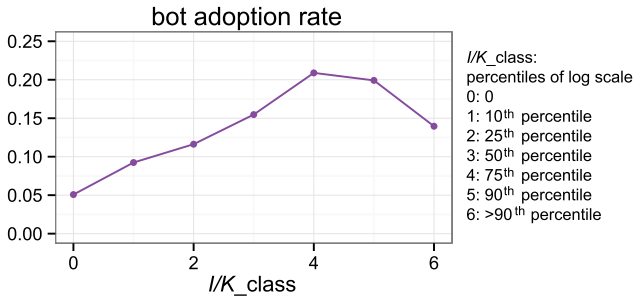

FIGURE 4. The bot adoption rate according to I/K.

The result implies that social reinforcement from many friends makes a game player significantly more susceptible to the lure of game bots. However, when the ratio exceeds 1/3, the likelihood rather decreases; presumably, as more friends get involved in cheating, one may begin to sense that the risk of being discovered is increasing and attempt to be cautious. This point is not uncommonly observed in the case of crime contagion. For example, a strong negative relationship between perceived certainty of being caught and the frequency of piracy was found to exist with the presence of social reinforcement [37], [57].

The secondary issue related to adoption is the level of commitment that users make to bot usage. Bot players who continuously use bots may intensify social reinforcement, and cause a vicious cycle in which a user who receives more social reinforcement in turn generates stronger social reinforcement. We measure the level of commitment in terms of how long the character uses the game bot, namely usage period, and how frequently the character uses the game bot, namely, the usage frequency.

As shown in Fig. 5, we track how the level of commitment varies as I/K increases. The left panel shows the usage period, which indicates how long the user used the game bot;

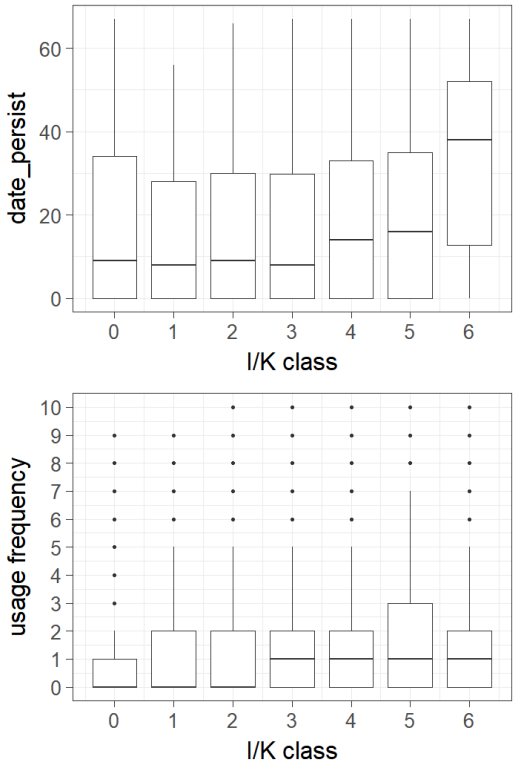

FIGURE 5. The level of engagement as a function of social reinforcement.

the right panel shows the usage frequency that indicates how frequently the user uses the game bot. We observed that the average of usage duration increases as I/K increases, the usage time. However, the usage frequency does not change as I/K increases. This suggests that there is a somewhat effect of social reinforcement on participants' level of engagement in terms of life-time with the adopted behavior.

D. RISK OF RETENTION

For game companies, the users who continuously use game bots are the most problematic because they continue to intensify social reinforcement to their friends. We track the number of characters who continue to use the game bot over time, as shown in Fig. 6. Approximately 20% of users continue to use game bots five days after they started using game bots.

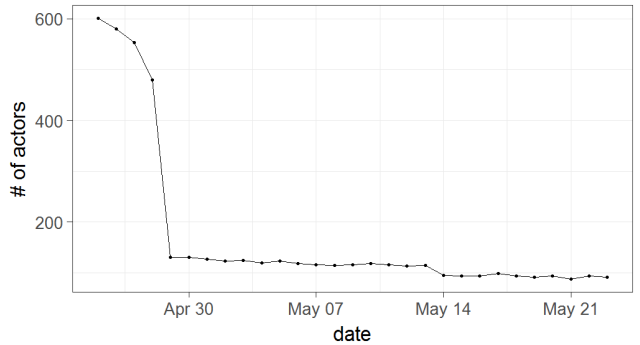

FIGURE 6. The number of sustained cheaters according to time.

Further, we investigate the effect of social reinforcement on the risk of retention. We test whether social reinforcement from friends may influence a player to cease the bot use. We draw the cumulative distribution according to the social reinforcement factors of two user groups. Users in the first group (namely, retained users) continue to use the game bot, while the users in the second group (namely, past users) have stopped using the game bots. The results are shown in Fig. 7. The cumulative distribution functions (CDFs) of retained users (keep) and past users (stop) are presented according to the degree of social reinforcement measured by each metric. The solid line and dotted line represent the CDFs of retained users and past users respectively. We test the effect of social reinforcement on bot usage retention. (a) S, (b) I, (c) K, (d) I/K, (e) Y, (f) Y/K.

Interestingly, Y seems to be the most significant, as the group that continues to use bots has a higher Y. To normalize the effect of the number of friends on Y, we derive an anti–ratio as the number of bot friends over friends, Y/K. When we normalize the effect of banning, the effect of banning also diminishes. The hazard ratio and 95% confidence intervals of retention according to significant factors are displayed in Table 3. I/K has the highest hazard ratio of retention.

TABLE 3. Hazard ratios and their 95% confidence intervals for bot retention according to significant metrics. The ratios and their intervals are generated from the Cox proportional hazards model.

Factor	Mean of hazard ratio	Lower bound	Upper bound
I	1.017	1.011	1.023
Y	1.071	1.047	1.096
I/K	2	1.67	2.395

E. 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. As mentioned above in Fig. 4, 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 the other indicating the exponential decay as a function of I/K. The incorporation of such two terms results in the reflection point in Fig. 4. To satisfy the properties of the probability function that the probability should range between 0 and 1 and the sum of probability over all possible values should be one, we normalize the Equation 3. like the gamma distribution function. The gamma distribution function has similar terms with Equation 3.

$$f(x) \propto x^{\alpha} \cdot \exp(-x/\beta), \quad \text{where } x = I/K \text{ and } 0 \leq x \leq 1 \tag{3}$$

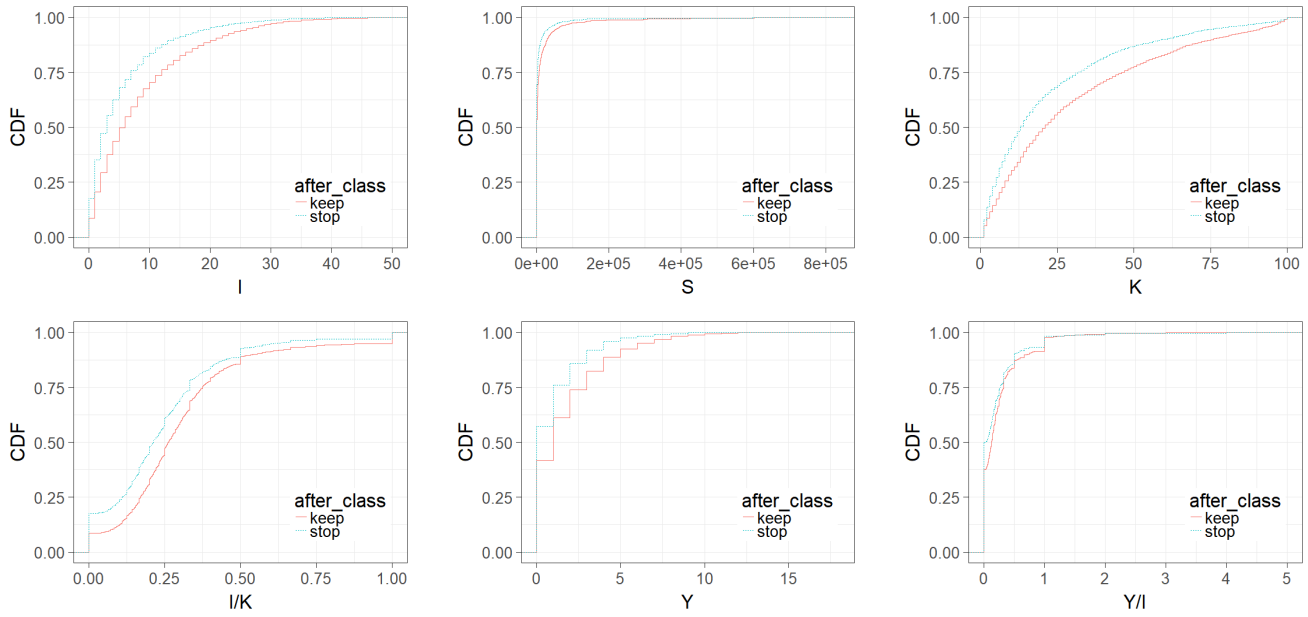

FIGURE 7. The cumulative distribution functions (CDFs) of retained users (keep) and past users (stop) according to social reinforcement factors.

Followings describe the gamma distribution.

$$g(x) = \frac{\beta^{\alpha} \cdot x^{\alpha} \cdot \exp(-x/\beta)}{\Gamma(\alpha)}, \quad \text{s.t. } 0 \le x$$
$$\int_0^{\infty} g(x)dx = 1$$
$$G(x) = \frac{\gamma(\alpha, \beta \cdot x)}{\Gamma(\alpha)}$$
$$\gamma(\alpha, \beta \cdot x) = (\beta \cdot x)^{\alpha} \cdot \Gamma(\alpha) \cdot \exp(-\beta \cdot x) \cdot \sum_{i=1}^{\infty} \frac{\beta \cdot x^{i}}{\Gamma(\alpha + i + 1)} \tag{4}$$

To meet the basic requirement of probability that the probability should range between 0 and 1 and the sum of probability over all possible data should be one, the bot adoption probability function should satisfy the following condition.

$$\int_0^1 f(x)dx = 1$$
$$\text{in other words} \quad F(1) - F(0) = 1 \tag{5}$$

We derive an appropriate function form for f(x) as follows

$$f(x) = A \cdot g(x)$$
$$F(x) = A \cdot \frac{\gamma(\alpha, \beta \cdot x)}{\Gamma(\alpha)}$$
$$F(1) - F(0) = 1$$
$$F(1) = A \cdot (\beta)^{\alpha} \Gamma(\alpha) \cdot \exp(-\beta) \cdot \sum_{i=1}^{\infty} \frac{\beta^{i}}{\Gamma(\alpha + i + 1)}$$
$$F(0) = 0$$
$$A = \frac{1}{\beta^{\alpha} \cdot \Gamma(\alpha) \cdot \exp(-\beta) \cdot \sum_{i=1}^{\infty} \frac{\beta^{i}}{\Gamma(\alpha+i+1)}}$$
$$f(x) = \frac{x^{\alpha} \cdot \exp(-x/\beta)}{\Gamma(\alpha)^2 \cdot \exp(-\beta) \cdot \sum_{i=1}^{\infty} \frac{\beta^{i}}{\Gamma(\alpha+i+1)}}$$
$$f(x) = \frac{x^{\alpha} \cdot \exp(-x/\beta + \beta)}{\Gamma(\alpha)^2 \cdot \sum_{i=1}^{\infty} \frac{\beta^{i}}{\Gamma(\alpha+i+1)}} \tag{6}$$

After deriving the bot adoption probability function, two parameters can be estimated through the maximum likelihood estimation. Under the approximation of the infection probability, the likelihood of observed data is computed as follows:

$$L(\alpha, \beta) = \prod_{Y_x} f(x) \cdot \prod_{N_x} (1 - f(x)) \tag{7}$$

where Y_x indicates the number of bot-adopters with x ratio of bot-using friends and N_x indicates the number of non–adopters with x ratio of infective neighbors.

The log likelihood is expressed as

$$\log(L) = \sum_{Y_x} f(x) + \sum_{N_x} \big(1 - f(x)\big) \tag{8}$$

The analytical form of α and β are estimated to maximize the log likelihood through

$$\frac{\partial L}{\partial \alpha} = 0, \quad \frac{\partial L}{\partial \beta} = 0, \tag{9}$$

For experiments, we adopt the heuristic method to derive optimal values of α and β. The heuristic method seeks optimal values of parameter with an objective function including parameters in an iterative way. We especially employed the simulated annealing algorithm. The simulated annealing algorithm works as follows. At each step, the algorithm randomly selects a solution close to the current one, evaluate a selected one in terms of object function, and then decides to

move to it or not based on two probabilities, one is the probability which the algorithm moves to a better one between a new solution and the current one, the other is the probability which the algorithm moves to a worse solution. During the iterative process, the former probability increases to 1 and the later probability decreases to 0. In our case, the objective function is defined as Equation (8). The parameters, α and β, are randomly chosen and then are optimized according to the principles of the simulation annealing algorithm. We used MATLAB package for parameter optimization with options of the number of maximum iteration to 1000, the termination condition specified by objective function change to 1e-6 and the lower bound and upper bound of two parameter to -100 and 100 respectively.

F. EVIDENCE OF SOCIAL INFLUENCE

To fit the probability function to the actual data, we estimate the adoption probability of a user with a currently active neighbors. We performed a shuffle test that randomly shuffles the adoption time and regenerates the diffusion process. On the original and regenerated data sets, we measured the social correlation and compared the results. We estimated the two parameters over a diffusion period of 51 days. The estimated value of α for the original and shuffled data sets are displayed in Fig. 8. These cumulative distribution functions display the distribution of the positive factor of social correlation for the original data and shuffled data. The two data sets have different distributions. This indicates that shuffling affects the positive factor of social correlation that determines the adoption probability for a given number of bot friends.

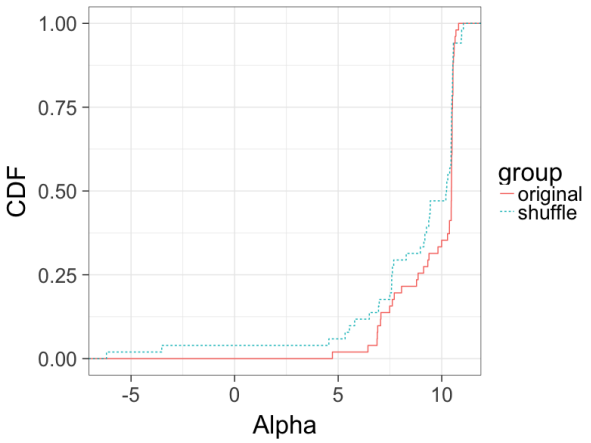

FIGURE 8. The distributions of positive factor of social reinforcement derived from the original data set and the shuffled data set.

We estimated β in a similar fashion. The distribution of β also shows differences between the original data set and shuffled data set as shown in Fig. 9. The factor is converted into integer values and categorized into integer classes. The distributions of the original and shuffled data sets differ. This indicates that shuffling also affects the negative factor of social correlation that determines the adoption probability for a given number of bot friends. Thus, we see the existence of the contagion of cheating behaviors in MMORPGs. Specifically, we found that the social reinforcement measured by the ratio of bot friends over total friends has the strongest effects on the likelihood of adoption and the commitment in terms of usage time. To verify the difference of α and β through the statistical test, we performed the non-parametric paired test that tests if the difference between two variables is significant or not when we do not guarantee the normal distribution of data in concern. We employed the Wilcoxon signed-rank test, which is to assess whether two-related population mean ranks differ when populations cannot be assumed to be normally distributed [58]. The null hypothesis is that the median of the distribution of the parameters of the original data and the shuffled data is zero. In other words,the difference between two paired data is not significant. The statistics of Wilcoxon signed-rank test is the rank sum of the absolute differences between two values, denoted as V.

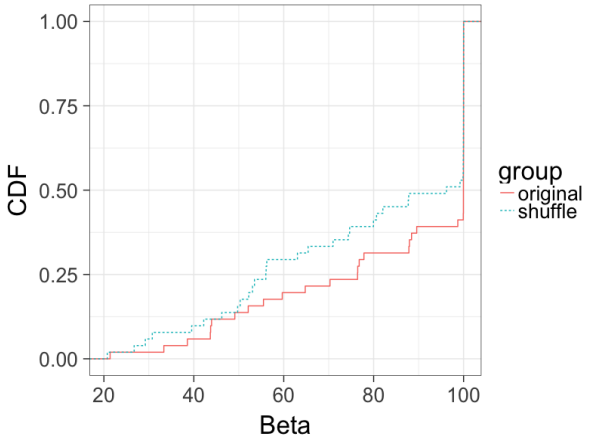

FIGURE 9. The distribution of negative factor of social reinforcement derived from the original data set and the shuffled data set.

We performed the statistical test for the difference of original data and shuffled data regarding two parameters. We derived α and β on a daily basis for original and shuffled data. Apparently, the means of α and β derived from the original dataset are larger than those from shuffled dataset. To test the significance of this difference, we performed one-sided t-test. The results are shown in Table 4. The null hypotheses that indicates the mean values of the original data are equal to the values of shuffled dataset. Two sample data are different reject the null hypothesis with the significance level of 10%. The p-values of α and β are less or equal to 10%. Thus, we conclude that with the significance level of 10% the social influence of bot usage is significant.

TABLE 4. The results of t-test to verify the significance of differences between original and shuffled data in terms of positive social correlation and negative social correlation.

	Test	Statistics		p–value	
α	$t-test$	t	1.76	$Pr >= \bar{t}$	0.04
β	$t-test$	t	1.28	$Pr >= \bar{t}$	0.10

G. DISCUSSION

Previous studies on behavior contagion showed that social reinforcement increases the likelihood of behavior adoption. For example, in health-related behavior, redundant signals significantly increase the likelihood of adoption; social reinforcement from multiple health companions made participants much more willing to adopt the behavior [18]. Similarly, Case and Katz [59] report that an individual's likelihood to be involved in crime varies positively with the proportion of others that are involved in crime. However, when misbehavior results in a penalty such as being banned or confiscated, social reinforcement that exceeds a certain threshold decreases the likelihood of adoption. In online games, even though players are not banned immediately after they are caught cheating, they are afraid of being disclosed when a large portion of their group engages in cheating. 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. To reduce the burden on game masters and the costs to employ them, we suggest that game masters carefully examine high-risk users; moreover, our study can help identify high-risk players. Users who have a high ratio of bot-using friends over total friends should be considered high-risk. In addition, we found that delayed banning is ineffective in preventing the contagion of cheating behavior. Once a user starts to use game bots, banning will not compel them to stop cheating. Users with a high influence ratio tend to continue cheating; thus, we recommend that game companies perform targeted monitoring and selective banning to maximize the banning effect.

IV. CONCLUSIONS

We provided evidence of the social contagion of malicious behavior in online games. We explored the effect of social reinforcement on the adoption of malicious behavior. The results showed that as social reinforcement increases, the likelihood of the malicious behavior adoption 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 and finally compares with previous works [60] and [61].

ACKNOWLEDGMENT

All data used in this study is deposited in the following web site, *http* : *//ocslab.hksecurity.net/game_contagion*, for any duplication or experiments.

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] D. P. Fan and R. D. Cook, "A differential equation model for predicting public opinions and behaviors from persuasive information: Application to the index of consumer sentiment," *J. Math. Sociol.*, vol. 27, no. 1, pp. 29–51, 2003.

[5] J. Kleinberg, "The convergence of social and technological networks," *Commun. ACM*, vol. 51, no. 11, pp. 66–72, 2008.

[6] D. M. Gorman, J. Mezic, I. Mezic, and P. J. Gruenewald, "Agent-based modeling of drinking behavior: A preliminary model and potential applications to theory and practice," *Amer. J. Public Health*, vol. 96, no. 11, pp. 2055–2060, 2006.

[7] R. Ho, "The intention to give up smoking: Disease versus social dimensions," *J. Social Psychol.*, vol. 138, no. 3, pp. 368–380, 1998.

[8] D. C. Rowe and J. L. Rodgers, "Adolescent smoking and drinking: Are they 'epidemics?'" *J. Stud. Alcohol Drugs*, vol. 52, no. 2, pp. 110–117, 1991.

[9] F. J. Santonja, A. C. Tarazona, and R. J. Villanueva, "A mathematical model of the pressure of an extreme ideology on a society," *Comput. Math. Appl.*, vol. 56, no. 3, pp. 836–846, 2008.

[10] D. M. Romero, B. Meeder, and J. Kleinberg, "Differences in the mechanics of information diffusion across topics: Idioms, political hashtags, and complex contagion on twitter," in *Proc. 20th Int. Conf. World Wide Web*, 2011, pp. 695–704.

[11] E. Hatfield and J. T. Cacioppo, *Emotional Contagion*. Cambridge, U.K.: Cambridge Univ. Press, 1994.

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

[13] N. A. Christakis and J. H. Fowler, "The spread of obesity in a large social network over 32 years," *New England J. Med.*, vol. 357, no. 4, pp. 370–379, 2007.

[14] A. L. Hill, D. G. Rand, M. A. Nowak, and N. A. Christakis, "Infectious disease modeling of social contagion in networks," *PLoS Comput. Biol.*, vol. 6, no. 11, p. e1000968, 2010.

[15] M. Gould, P. Jamieson, and D. Romer, "Media contagion and suicide among the young," *Amer. Behavioral Sci.*, vol. 46, no. 9, pp. 1269–1284, 2003.

[16] C. M. Barry and K. R. Wentzel, "Friend influence on prosocial behavior: The role of motivational factors and friendship characteristics," *Develop. Psychol.*, vol. 42, no. 1, p. 153, 2006.

[17] M. Tsvetkova and M. W. Macy, "The social contagion of generosity," *PLoS ONE*, vol. 9, no. 2, p. e87275, 2014.

[18] D. Centola, "The spread of behavior in an online social network experiment," *Science*, vol. 329, no. 5996, pp. 1194–1197, 2010.

[19] N. A. Christakis and J. H. Fowler, "Social contagion theory: Examining dynamic social networks and human behavior," *Statist. Med.*, vol. 32, no. 4, pp. 556–577, Feb. 2013.

[20] N. O. Hodas and K. Lerman, "The simple rules of social contagion," *Sci. Rep.*, vol. 4, Mar. 2014, Art. no. 4343.

[21] A. Mukherjee, B. Liu, and N. Glance, "Spotting fake reviewer groups in consumer reviews," in *Proc. 21st Int. Conf. World Wide Web*, 2012, pp. 191–200.

[22] L. Wang, J. Niu, and J. J. P. C. Rodrigues, "GMA: An adult account identification algorithm on sina weibo using behavioral footprints," *Future Generat. Comput. Syst.*, to be published, doi: 10.1016/j.future.2017.08.032.

[23] A. Anagnostopoulos, R. Kumar, and M. Mahdian, "Influence and correlation in social networks," in *Proc. 14th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2008, pp. 7–15.

[24] 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.

[25] 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.

[26] M. Szell and S. Thurner, "Measuring social dynamics in a massive multiplayer online game," *Social Netw.*, vol. 32, no. 4, pp. 313–329, 2010.

[27] 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.

[28] J. Woo, A. R. Kang, and H. K. Kim, "Modeling of bot usage diffusion across social networks in MMORPGs," in *Proc. Workshop SIGGRAPH Asia*, 2012, pp. 13–18.
[29] J. Woo, A. R. Kang, and H. K. Kim, "The contagion of malicious behaviors in online games," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 543–544, 2013.
[30] J. Blackburn, N. Kourtellis, J. Skvoretz, M. Ripeanu, and A. Iamnitchi, "Cheating in online games: A social network perspective," *ACM Trans. Internet Technol.*, vol. 13, no. 3, 2014, Art. no. 9.
[31] R. L. Akers, *Deviant Behavior: A Social Learning Approach*. Belmont, CA, USA: Wadsworth Pub. Co., 1977.
[32] A. Bandura and D. C. McClelland, *Social Learning Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1977.
[33] A. R. Harris, "Imprisonment and the expected value of criminal choice: A specification and test of aspects of the labeling perspective," *Amer. Sociol. Rev.*, vol. 40, no. 1, pp. 71–87, 1975.
[34] A. R. Harris, "Sex and theories of deviance: Toward a functional theory of deviant type-scripts," *Amer. Sociol. Rev.*, vol. 42, no. 1, pp. 3–16, 1977.
[35] W. W. Eaton, Jr., "Mental hospitalization as a reinforcement process," *Amer. Sociol. Rev.*, vol. 39, no. 2, pp. 252–260, 1974.
[36] R. F. Meier and W. T. Johnson, "Deterrence as social control: The legal and extralegal production of conformity," *Amer. Sociol. Rev.*, vol. 42, no. 2, pp. 292–304, 1977.
[37] W. F. Skinner and A. M. Fream, "A social learning theory analysis of computer crime among college students," *J. Res. Crime Delinquency*, vol. 34, no. 4, pp. 495–518, 1997.
[38] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a feather: Homophily in social networks," *Annu. Rev. Sociol.*, vol. 27, pp. 415–444, Aug. 2001.
[39] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.
[40] E. M. Rogers, *Diffusion of Innovations*. New York, NY, USA: Simon and Schuster, 2010.
[41] J. Borge-Holthoefer, A. Rivero, and Y. Moreno, "Locating privileged spreaders on an online social network," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 85, p. 066123, Jun. 2012.
[42] B. Viswanath, A. Mislove, M. Cha, and K. P. Gummadi, "On the evolution of user interaction in Facebook," in *Proc. 2nd ACM Workshop Online Social Netw.*, 2009, pp. 37–42.
[43] A. Mislove, H. S. Koppula, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Growth of the flickr social network," in *Proc. 1st Workshop Online Social Netw.*, 2008, pp. 25–30.
[44] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in *Proc. 7th ACM SIGCOMM Conf. Internet Meas.*, 2007, pp. 29–42.
[45] H. Kwak, Y. Choi, Y.-H. Eom, H. Jeong, and S. Moon, "Mining communities in networks: A solution for consistency and its evaluation," in *Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf.*, 2009, pp. 301–314.
[46] J. Goldenberg, S. Han, D. R. Lehmann, and J. W. Hong, "The role of hubs in the adoption process," *J. Marketing*, vol. 73, no. 2, pp. 1–13, 2009.
[47] W. Wang, M. Tang, H.-F. Zhang, and Y.-C. Lai, "Dynamics of social contagions with memory of nonredundant information," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 92, no. 1, p. 012820, 2015.
[48] M. D. Krohn, W. F. Skinner, J. L. Massey, and R. L. Akers, "Social learning theory and adolescent cigarette smoking: A longitudinal study," *Social Problems*, vol. 32, no. 5, pp. 455–473, 1985.
[49] S. R. Burkett and E. L. Jensen, "Conventional ties, peer influence, and the fear of apprehension: A study of adolescent marijuana use," *Sociol. Quart.*, vol. 16, no. 4, pp. 522–533, 1975.
[50] G. F. Jensen, "Parents, peers, and delinquent action: A test of the differential association perspective," *Amer. J. Sociol.*, vol. 78, no. 3, pp. 562–575, 1972.
[51] J. F. Short, Jr., "Differential association and delinquency," *Social Problems*, vol. 4, no. 3, pp. 233–239, 1957.
[52] W. Skogan, "Fear of crime and neighborhood change," *Crime Justice*, vol. 8, no. 1, pp. 203–229, 1986.
[53] M. D. Krohn, "The Web of conformity: A network approach to the explanation of delinquent behavior," *Social Problems*, vol. 33, no. 6, pp. s81–s93, 1986.
[54] P.-H. Chen, H. R. White, and R. J. Pandina, "Predictors of smoking cessation from adolescence into young adulthood," *Addictive Behaviors*, vol. 26, no. 4, pp. 517–529, 2001.
[55] L. M. Powell, J. A. Tauras, and H. Ross, "The importance of peer effects, cigarette prices and tobacco control policies for youth smoking behavior," *J. Health Econ.*, vol. 24, no. 5, pp. 950–968, 2005.
[56] R. G. Miller, Jr., *Survival Analysis*, vol. 66. Hoboken, NJ, USA: Wiley, 2011.
[57] R. C. Hollinger and L. Lanza-Kaduce, "The process of criminalization: The case of computer crime laws," *Criminology*, vol. 26, no. 1, pp. 101–126, 1988.
[58] F. Wilcoxon, "Individual comparisons by ranking methods," *Biometrics Bull.*, vol. 1, no. 6, pp. 80–83, 1945.
[59] A. C. Case and L. F. Katz, "The company you keep: The effects of family and neighborhood on disadvantaged youths," Nat. Bureau Econ. Res., Cambridge, MA, USA, Work. Paper 3705, May 1991. [Online]. Available: http://www.nber.org/papers/w3705, doi: 10.3386/w3705.
[60] Y. Xia, X. Ren, Z. Peng, J. Zhang, and L. She, "Effectively identifying the influential spreaders in large-scale social networks," *Multimedia Tools Appl.*, vol. 75, no. 15, pp. 8829–8841, 2016.
[61] L. Alsuwaidan and M. Ykhlef, "Information diffusion predictive model using radiation transfer," *IEEE Access*, vol. 5, pp. 25946–25957, 2017.

JIYOUNG WOO received the B.S., M.S., and Ph.D. degrees in industrial engineering from KAIST in 2000, 2002, and 2006, respectively. From 2008 to 2010, she was a Researcher with the Artificial Intelligence Laboratory, Arizona University, USA. From 2010 to 2016, she was a Research Professor with the Graduate School of Information Security, Korea University. She is currently a Professor with the Big Data Engineering Department, Soonchunhyang University. Her research interests include data mining and business intelligence.

SUNG WOOK KANG received the B.S. degree in software engineering from the Kumoh National Institute of Technology, South Korea, in 2014, and the M.S. degree in information security engineering from Korea University in 2016. From 2014 to 2016, he was a Researcher with the Hacking and Countermeasure Research Lab, Korea University. He is currently a member of the Data Analysis and Modeling Team, NCSOFT, South Korea. His research interests include data mining and machine learning.

HUY KANG KIM received the B.S. degree in industrial management and the M.S. and Ph.D. degrees in industrial and systems engineering from KAIST in 1998, 2000, and 2009, respectively. He founded A3 Security Consulting, South Korea, the first information security consulting company, in 1999. He was the Technical Director and the Head of the Information Security Department, NCSOFT, from 2004 to 2010. He is currently an Associate Professor with the Graduate School of Information Security, Korea University. His research interests include solving security problems in online games based on the user behavior analysis and data mining.

JUYONG PARK received the Ph.D. degree in physics from the University of Michigan. He currently focuses on biological, technical, and social networks. He specializes in analytical methods for network analysis and networks of sports, culture, and online games. He is an Associate Professor with the Graduate School of Culture Technology, Korea Advanced Institute of Science and Technology.