MPPM: Malware Propagation and Prevention Model in Online SNS

Hui Zhu, Cheng Huang and Hui Li
State Key Laboratory of Integrated Service Networks
Xidian University
Xi'an, China
Email: zhuhui@xidian.edu.cn, xdhuangcheng@gmail.com and lihui@mail.xidian.edu.cn

***Abstract*—With the pervasiveness of online social network service (SNS), many people express their views and share information with others on them, and the information propagation model of online SNS has attracted considerable interest recently. However, the flourish of information propagation model in online SNS still faces many challenges, especially considering more and more malicious software's propagation in SNS. In this paper, we proposed a malware propagation and prevention model based on the propagation probability model, called MPPM, for online SNS. With this model, we can describe the relationships among malware propagation, habits of users and malware detection in online SNS. In specific, based on characteristics of online SNS, we define users' states and the rules of malware propagation with dynamics of infectious disease; then, we introduce the detection factor to affect the propagation of malwares, and present the malwares propagation and prevention in online SNS by dynamic evolution equations; finally, we analyze the factors which influence the malware propagation in online SNS. Detailed analysis and simulation demonstrate that the MPPM model can precisely describe the process of malware's propagation and prevention in online SNS.**

***Keywords*-Social network service; malware prevention; dynamics of infectious disease; dynamic evolution equations.**

I. Introduction

With the pervasiveness of online social network service (SNS), such as Facebook or Twitter, users can express their views and exchange information, and Internet has become an important tool for information exchange. However, traditional malware (like virus, Trojan, backdoor software), which steal users' privacy information, can easily spread by the features of information propagation in online SNS. Specifically, once one user upload a malware to online SNS and pushed it to all his friends, the users who download and execute the malware will become the new malware infected users, and begin to propagate the malware to their friends, then the malware can spread more quickly and the number of infected users has an explosive growth in online SNS[1], [2].

For protecting the security of users' privacy, how to describe the propagation of malware and efficiently prevent the propagation of malware in online SNS have attracted considerable interest recently, and a lot of approaches have been proposed. Since Kephart and White [3] took the first step towards modeling the spread behavior of virus, much effort has been done also in the area of developing a mathematical model for the virus propagation [4]. Fan et al. [5] studied the virus propagation on Facebook, and proposed two models for virus propagation on Facebook: one is based on the Facebook's application platform; another model is based on sending messages to friends. Wang et al. [6] divided all network into different states and proposed a new model to describe the virus propagation in SNS. Piqueira et al. [7] proposed a SAIR model, and defined a node called antidotal node to a new state of node in SNS based on dynamic models of virus [8]. And according to different malware propagation model in SNS, more and more approaches of preventing the spread of malware in SNS have been proposed. Mishra et al. [9] evaluated the effects of anti-virus software on infectious nodes in computer network. And there are many tools or ways to control the spread of virus in SNS [10], even malware detection and prevention models in SNS of smartphones have been researched [11]. However, almost all of the aforementioned models have some limitations [12], almost all proposed models just describe the malware propagation model by epidemiological model, and give stability and bifurcation conditions to simulate their models in online SNS, but they did not consider the SNS characteristics and use them to define the different malware state transitions in online SNS, and didnt propose a practical way to effectively analyze the malware propagation process and prevent the propagation of malware in online SNS.

In this paper, we proposed a new model, called MPPM, to analyze the propagation and prevention of malware in online SNS, and describe the spread of malware in online SNS with the characteristics of SNS. In short, this paper's main contributions focus on two points.

1) We propose a new malware propagation and prevention model in online SNS. In specific, we define several different states for nodes in online SNS based on the characteristics of SNS, and several state transition rules based on dynamics of infectious disease. Then, we introduce the detection factor to affect the propagation of malware, and present the malware's propagation and prevention in online SNS by dynamic evolution equations.
2) We describe the relationships among malware propagation, habits of user and malware detection in online SNS with MPPM, and analyze the factors which influence

978-1-4799-4640-2/14/$31.00 ©2014 IEEE

the malware propagation in online SNS, and using simulation to demonstrate our model is effective. Then, with MPPM, we can choose the optimum scheme to prevent the propagation of malware.

The rest of paper is organized as follow. In Section II, we formalize the system model and requirements. In Section III, we propose the representations of online SNS with malware propagation. Then, we proposed the malware propagation and prevention model in online SNS with accurate definitions and dynamic evolution equations in Section IV, followed by detailed analysis and simulation are proposed in Section V. Finally, we draw our conclusions and identify some future work in Section VI.

II. System Model and Requirements

In this section, we formalize the system model and requirements of malware propagation and prevention in online SNS, and identify the design goal of MPPM.

A. System Model

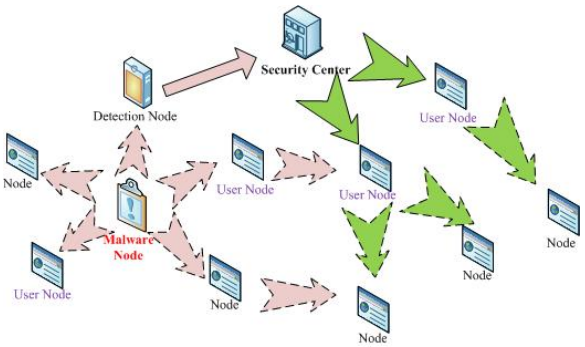

Fig. 1. System model of online SNS with malware

As shown in Fig. 1, we proposed an essential system model for online social network. In specific, we classify the process of information propagation into malware propagation and patch propagation, according to the different kinds of users in online SNS; and we assume that there is only one malware infected user in SNS at first time, and the malware can transmitted themselves to all the infected users' friends and infects friends which have not been patched for the malware; furthermore, there are some detection users which are deployed by a security center in online SNS, and malwares must be detected when they transmit themselves to this kind of users; at the same time, users who register themselves in security center and have not been infected, can receive the patches from security center to anti the malware, and will not be infected by the malware; in addition, the patches may transmit themselves to their friends by patched users.

B. Requirements

According to the aforementioned system model, the most important requirements of protecting users in online SNS is to prevent the spreading of the malware. And because the malware changes quickly than the patches, the problem "how to deal with the malwar" can be converted to the problem "how quickly we can prevent the propagation of malware" and give all compute nodes in online SNS a new patch to anti the malware. Therefore, the following requirements should be satisfied in MPPM for online SNS.

1) *Malware propagation*. The model should describe the propagation of malware by the characteristics of online SNS in detail. In specific, once a user in online SNS is infected by a malware, then it will disseminate the malware to all its friends, and its friends' habits will determine whether they will be infected.
2) *Malware prevention*. The model should describe the relationships among malware propagation, habits of user and malware detection in online SNS. Specifically, after detection users detect the malware, the registered users may disseminate the patch to all their friends according to their habits; at the same time, the malware is also disseminated by infected users.

III. Representation of Online SNS with Malware

In this section, we present an abstract representation of online SNS with malware propagation and detection, and the representation consists of a series of nodes and relationships. Our intent is not to represent any concrete SNS, but to identify the key elements of online SNS upon which impact on the malware propagation and prevention. Therefore, according to the characteristics which determine the propagation of malware in online SNS, we construct the representation of online SNS with malware as a graph, and the online SNS can be characterized by the following core components.

A. Nodes

Let N be the set of nodes, which is represented as a collection of users' accounts, and each account $N_i \in x$ is uniquely identified for one user in SNS. All nodes can be classified into three types, according to the relationships between users and security center.

- N_s, the set of nodes which register themselves in security center as a user. If security center knows any malware, they can receive the patches of the malware from security center, and will be immunized which means cannot be infected forever, then they can choose to transmit patches to their neighbors. However, if the malware is not detected by security center, the N_s nodes can be infected, transmit the malware to their friends, and cannot be immunized forever. We define N_s nodes with considering the worst situation that if the node is infected, it will never become normal.
- N_u, the set of nodes which not register themselves in security center as a user. They cannot receive the patches from the security center, but they can be infected by malware and receive patches from their friends, being immunized like N_s, and they can also choose to transmit patches to their friends. However, if the N_u nodes don't choose to receive patches from its neighbors and not to

be immunized, they can be infected and disseminate the malware to their friends.

- N_d, the set of nodes which register themselves in security center as a detector. If malware are transmitted to them, they can detect the malware and report to security center as first time; then, security center make the patches and transmit to all N_s nodes. We define this node with considering that the N_d node will never be infected and cannot transmit the patches to other, and they just detect the data and tell the security center to analyze the data.

However, except from N nodes in online SNS, there is another kind of node which is not as a user node in all nodes of SNS, called SC which means security center. These set of nodes which can receive malware from N_d nodes and transmit patches to all N_s nodes to make them be immunized.

B. Relationships among Nodes

Let R be the set of the relationships between any two nodes in online SNS, which is decided by node's type, and can be classified into the following two major categories.

- R_n, the relationship between N_s and N_u, which represents the neighbor relationships. N_s and N_u can access each other and transmit information bidirectionally according to the friendships in online SNS.
- R_{sn}, the relationships between N_d and $SC/N_u/N_s$, which represents the semi-neighbor relationship, and can be classified into three categories.
  - R_s, the relationship between N_s and SC. For instance, SC can transmit patches to make immunized directionally, but N_s cannot access SC to ask any patches.
  - R_{do}, the relationship between N_d and SC. For example, N_d can just transmit received data to SC for analysis directionally, but SC cannot be accessed by N_d nodes.
  - R_{di}, the relationship between N_d and N_u/N_s. For example, N_u and N_s can transmit malware to N_d nodes, but N_u and N_s cannot receive the malware from N_d nodes.

IV. The Malware Propagation and Prevention Security Model

In this section, we define the node states of N_s and N_u, and present the dissemination rules of states, then, we describe the malware propagation and prevention model according to these definitions.

A. States of Nodes

According to the characteristics of online SNS and propagation probability model, N_s and N_u nodes' states in online SNS with malware can be classified into two major categories: *susceptible state* and *infected state*.

- *Susceptible state* means that the node can receive the malware or patches from their neighbors or security center, and have some opportunities to receive the malware or patches. For example, the nodes in *susceptible state* may be infected by the malware, which means the node executed the malware. Every N_s and N_u node begins with *susceptible state* except the source node with malware.
- *Infected state* means that N_s and N_u nodes received the malware or patches from its neighbors and execute them. It also can be divided into two categories: *immunized state* and *malware disseminated state*.
- *Immunized state* represents that the node has executed the patches and cannot be infected by the malware when it accepts the information from neighbors. This state can only happen in nodes with patches expect the N_d nodes and SC nodes which are immunized forever. And there are two ways for other nodes to get patches.
  - N_s nodes can receive patch from SC when the malware has been detected by N_d;
  - N_u nodes may receive patches from their friends who have been patched.
- *Disseminated state* means that the node who can propagate the malware or patches to other nodes. We assume that N_d nodes never propagate patches and SC nodes and just broadcast the patches to all N_s nodes, so there are just N_s nodes and N_u nodes can propagate the information. If the nodes have installed the malicious software, they will propagate the malware to their friends, and we call it the as *malware disseminated state*. If the nodes are patched, they may propagate patches to their neighbors, and we call it as *patch disseminated state*.

However, we need to emphasize that if the nodes have infected by the malware, then they cannot install patches, which means they cannot transfer from *malware disseminated state* to *immunized state*, and vice versa.

Definition 1: In malware propagation process, the nodes in online SNS have three final states (*susceptible*, *immunized*, and *malware disseminated*) and two temporary states (*received*, *accepted*).

1) The final states mean the node state must be one of them in any time.
2) The temporary states are the intermediate process of the final states, which can help us to analyze the malware propagation and prevention.

B. Dissemination Rules

According to the characteristics of online SNS, state transitions of nodes in SNS depend on not only its own state, but also the states of its neighbors. Therefore, the dissemination rules are defined as follow.

- We define a node as a detection node with the probability of P_1 in online SNS, which means the density of N_d nodes in N nodes is P_1. And the N_d nodes' density can influence the result of state transitions, which means that, if the node is N_d nodes, it will not deal with the received information and transmit the information to SC nodes. If the SC nodes identify the information as malware, it will generate patches and immunized all N_s nodes which have not been infected by malware. Therefore, P_1 determines

TABLE I
THE DEFINITION OF NOTATIONS

Notation	Definition
$N(k,t)$	Number of the degree *k* nodes in *t*.
$S(k,t)$	Number of the degree *k* susceptible nodes in *t*.
$A(k,t)$	Number of the degree *k* accepted nodes in *t*.
$MD(k,t)$	Number of the degree *k* malware disseminated nodes in *t*.
$C(k,t)$	Number of the degree *k* detection nodes in *t*.
$I(k,t)$	Number of the degree *k* immunized nodes in *t*.
$PD(k,t)$	Number of the degree *k* patch disseminated nodes in *t*.

the probability that N_d may detect the malware and the time when a malware will be detected.

- The N_s and N_u nodes may accept the node by the probability of P_2, then we can obtain the probability that the node's state is transferred from susceptible state to accepted state when it received an information.
- The information may be patch or malware by the probability of $P(t)$ and $1-P(t)$, respectively. The probability may change with the propagation of malware, and can be calculated by other state transition probability and nodes' density in online SNS.
- The N_s and N_u nodes which are immunized nodes may propagate patch by the probability of P_3, while N_s and N_u nodes which are infected by malware must propagate the patch by the probability of 1.
- At the beginning, there are none nodes with patch until the information with malware meets the N_d nodes in probability. The N_d nodes can make all N_s nodes which are not infected by malware patched and as the probability of P_3 to propagate the patch. If N means the numbers of nodes in online SNS and P_{md} means the density of nodes in accepted information state before malware detected by N_d nodes. We call the time when a malware is detected as checkpoint c, it can be determined with the situation that $P_{md} \times P_1 \times \ N \geq 1$.

When a malware starts to propagated, both N_s and N_u nodes are in *susceptible state*. And the nodes in online SNS will come to an equilibrium state at the end of propagation. Both N_s and N_u nodes will become immunized state or malware disseminated state. And there are two stages when malware propagation.

- The detection node have not detected the malware, and $P(t)$ is 0, because there is only malware propagation in online SNS;
- Malware have been detected by N_d nodes, and there are malware and patch propagation in online SNS.

Finally, we defined the number of nodes with different states as Tab. I, and the relationship of the number can be described as $N(k,t) = S(k,t) + MD(k,t) + I(k,t)$.

C. Propagation and Prevention model

Malware propagation in online social networks depends on the type of a propagation model, and the model can be accepted as a graph structure which inputs states of every individual and returns a new state of the individual according to its interactions with other individuals. This process continues until all the interactions between individuals are exhausted. **Assumption 1**: In time *t*, a node *x* is in *susceptible state*, and $P_{x(s\to s)}$ means the probability of node *x* is still in *susceptible state* in the time period $[t, t+\Delta t]$.

$$P_{x(s\to s)} = (1 - \Delta t(1 - P_2 + P_1 P_2))^j$$

Wherein, $j = j(t)$ represents the number of the neighbors in disseminated state of *x* in time *t*.

Assumption 2: If node *x* contains *k* neighbors, *j* is the random variable which satisfies the equation.

$$\prod(j,t) = \binom{k}{j} (P(k,t))^j (1 - P(k,t))^{k-j}$$

Wherein, $P(k,t)$ means the probability of a disseminated node connects a susceptible node which has *k* neighbors. And let $P(k'k)$ be the degree correlation function which denotes the neighbor probability between the node with *k* neighbor and the degree *k'* node; Pk' be the function of degree distribution; $P(i_{k'} s_k)$ be the probability of a degree *k'* node is in *disseminated state*, when it connects with a degree *k* susceptible node; $D_d(k',t), D_{pd}(k',t), D_{md}(k',t), D_a(k',t)$ be the density of disseminated nodes, patch disseminated nodes, malware disseminated nodes, and accepted nodes in the degree *k'* nodes in time *t*, respectively. Then, we can get the $P(k,t)$ as follow.

$$\begin{aligned} P(k,t) &= \sum_{k'} P(k'|k) P(i_{k'}|s_k) \\ &= (1 - P(t) + P(t)P_3) \sum_{k'} P(k'|k) D_a(k',t) \end{aligned}$$

Let P_4 be the density of N_s nodes in $(1-P_1)N$ nodes in online SNS, U_{md} and U_i be the density of N_u nodes in *malware disseminated state* and *immunized state*, S_{md} and S_i be the density of N_s nodes in *malware disseminated state* and *immunized state*, respectively. Then, we can calculate $P(t)$ as follow.

$$P(t) = \begin{cases} 0 & , P_{md} P_1 N < 1 \\ \dfrac{(S_i(t) + U_i(t))P_3}{(S_i(t) + U_i(t))P_3 + U_{md}(t) + S_{md}(t)} & , P_{md} P_1 N \geq 1 \end{cases}$$

According to [13], we can obtain the degree correlation function

$$P(k'|k) = \frac{k' P(k')}{\overline{k}}$$

, and $\overline{k}$ is the average degree of the network. And $P(k,t)$ can be described as follows.

$$P(k,t) = \frac{1 - P(t) + P(t)P_3}{\overline{k}} \sum_{k'} k' P(k') D_a(k',t)$$

Then, we can get the average propagation probability $\overline{P}_{(s\to s)}(k,t)$ of the degree *k* nodes still in *susceptible state*

in time segment $[t, t+\Delta t]$.

$$\begin{aligned}\overline{P}_{(s\to s)}(k,t) &= \sum_{j=0}^{k}\binom{k}{j}(1-\Delta t(1-P_2+P_1P_2))^j \\ &\quad P(k,t)^j(1-P(k,t)))^{k-j} \\ &= \left(1-\frac{1}{\bar{k}}(1-P_2+P_1P_2)(1-P(t)+\right. \\ &\quad \left. P(t)P_3)\Delta t\sum_{k'}k'P(k')D_a(k',t)\right)^k\end{aligned}$$

And we can get the average propagation probability $\overline{P}_{(s\to a)}(k,t)$ of the degree k nodes in *infected state* in the time segment$[t, t+\Delta t]$.

$$\bar{P}_{s\to a}(k,t) = 1-P_1-\bar{P}_{s\to s}(k,t)$$

Then, the nodes' number of acceptable state of degree k susceptible nodes' changing in $[t, t+\Delta t]$ can be described as follow.

$$\begin{aligned}A(k,t+\Delta t) &= A(k,t)+(N(k,t)-A(k,t)-C(k,t)) \\ &\quad \left(1-P_1-\left(1-\frac{1}{\bar{k}}(1-P_2+P_1P_2)\right.\right. \\ &\quad (1-P(t)+P(t)P_3) \\ &\quad \left.\left.\Delta t\sum_{k'}k'P(k')D_a(k',t)\right)^k\right)\end{aligned}$$

At the checkpoint, $A(k,t)$ will be changed because there are N_s nodes which are not infected by malware have been immunized, and $A(k,t)$ can be calculated as $A(k,t)=A(k,t)+N(k)S_i$. Then, we can also get the formulas to describe the density changes of the nodes of *malware disseminated state*, *patch disseminated state* and *immunized state* with time *t*. In the same way, we can get $MD(k,t+\Delta t)$, $I(k,t+\Delta t)$ and $PD(k,t+\Delta t)$.

V. Simulations and Analysis

In this section, we will validate the proposed MPPM model through experiments on real data of social network, and various settings in MPPM were simulated to estimate the influence to malware propagation and prevention in SNS.

A. The Dataset Description

To validate the proposed model, we first generate the social network based on the Enron Network Data [14], which has 36692 nodes and the average degree is 10.22. And the initial degree distribution is shown in Fig. 2.

B. Simulation and Discussion

We focus on analyzing the influence of various parameters' settings to the density of different nodes in MPPM, such as the different security environment which means the different density of N_d and N_s nodes. The details of the experiments are as follows.

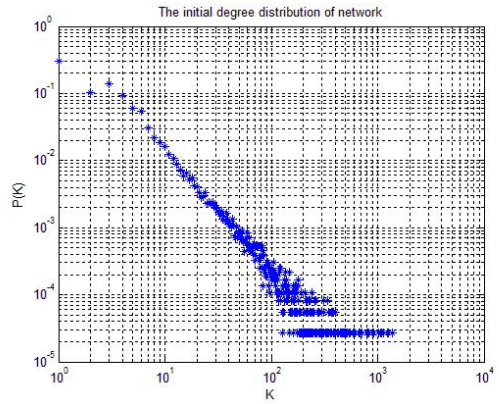

Fig. 2. The initial degree distribution of Enron Network Data

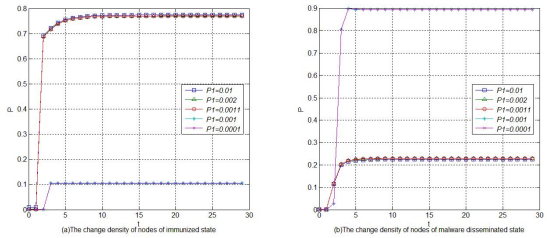

Fig. 3. The density's evolution with *t* when different settings of P_1. (a) *The immunized state* (b) *The malware disseminated state*

1) Influence of the Density of Detection Nodes in SNS: We set $P_2=0.1$, $P_3=0.2$, $P_4=0.8$, and times of iteration $T=300$ which is the round number of information dissemination, then choose various values of P_1(0.01, 0.002, 0.0011, 0.001 and 0.0001) to simulate the density evolution with *t* for the nodes of *immunized state* and *malware disseminated state*. The density's evolution of nodes with different P_1 is shown in Fig. 3. And we can get the following factors.

- The larger P_1 is, more quickly the checkpoint happens.
- The larger P_1 is, more nodes can be immunized in final.
- There is a large difference of the density's evolution with P_1 between 0.0011 and 0.001.

According to the above factors, we can get the following conclusions. The larger P_1 is, more detection nodes in online SNS, more quickly checkpoints happens. Factor-1 verify the judgment of the defined checkpoint of MPPM, which means we can detect the earlier in SNS and we can react more quickly. Because of early detection, nodes can propagate the patch in SNS earlier, and more nodes will be immunized, and factor-2 can be explained. However, the nodes of above two states in SNS may have a huge different density with little changes of P_1, because of our judgment of checkpoint in SNS. Although we give a judgment of the checkpoint happening, the checkpoint just happens in probability, which means nobody can know what time the checkpoint may happen accurately. Therefore, if we give a definite value of checkpoint, the final density of nodes of SNS will have a sudden and big change with little change of P_1, because little changes of

P_1 may change the checkpoint suddenly, and Factor-3 can be answered. The density of detection nodes in SNS has a great influence about the result of our model, and the larger P_1 is, more nodes are immunized. We know that P_1 cannot be large, because that will change more nodes to be detection nodes and will cost more resource.

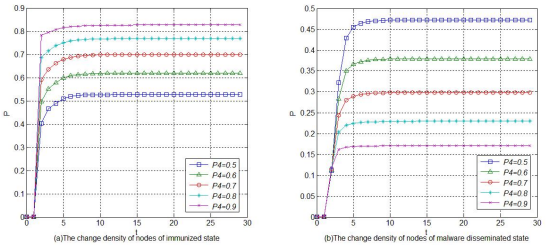

Fig. 4. The density's evolution with *t* when different settings of P_4. (a) *The immunized state* (b) *The malware disseminated state*

2) Influence of the Density of Registered User Nodes: We set $P_1 = 0.002$, $P_2 = 0.1$, $P_3 = 0.2$, and times of iteration $T = 300$ which is the round number of information dissemination, then choose various values of P_4 (0.5, 0.6, 0.7, 0.8 and 0.9) to simulate the density evolution with *t* for the nodes of *immunized state* and *malware disseminated state*. The density's evolution of nodes with different P_4 is shown in Fig. 4. And we can get the following factors.

- The larger P_4 is, there will be more immunized nodes in final.
- The larger P_4 is, more quickly the immunized nodes increase, and have a sudden explosive growth when checkpoint happens.

According to the above factors, we can get the following conclusions. If more users in SNS register themselves in security center, the density of N_s nodes will become larger. When the malware is detected, there are more nodes can be patched at the first time, and less nodes with no patch will be left, so the immunized nodes are more and increase quickly, answering the factor-1 and factor-2. We want more nodes become N_s nodes, however, there may be not enough N_s nodes in online SNS and that will cause a great influence in malware propagation process.

VI. Conclusion

In this paper, we proposed a malware propagation and prevention model based on the propagation probability model, called MPPM, to describe the relationship among malware propagation, habits of user and malware detection in online SNS. We defined a few states of nodes and propagation and prevention rules based on dynamics of infectious disease to describe the detection factor to affect the propagation of malwares, and present the malware's propagation and prevention in online SNS by dynamic evolution equations. Then, we simulate the density's evolution of the nodes of susceptible, immunized and malware disseminated state with time respectively, and analyzed the impact of security settings about malware propagation, detection, prevention on real SNS data. The results show that the proposed MPPM can describe the malware propagation accurately and can help to prevent malware propagation effectively. In our future work, we intend to analyze the impact of the information's features in online SNS to further verify the proposed MPPM.

Acknowledgment

The authors would like to thank the reviewers for detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported by National Natural Science Foundation of China (No.61303218); National Science & Technology Major Projects (No.2012ZX03001009); Fundamental Research Foundations for the Central Universities of China (No.K5051301017); Kunshan Innovation Institute of Xidian University and 111 Project (B08038).

References

[1] K. Thomas and D. M. Nicol, "The koobface botnet and the rise of social malware," in *Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on*. IEEE, 2010, pp. 63–70.

[2] S. Choney, "Notorious Zeus banking Trojan is gaining speed on Facebook," http://www.msnbc.msn.com/technology/notorious-zeus-banking-trojan-gaining-speed-facebook-6C10213925, 2013, [Online; accessed 19-October-2013].

[3] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*. IEEE, 1991, pp. 343–359.

[4] M. R. Faghani and H. Saidi, "Malware propagation in online social networks," in *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on*. IEEE, 2009, pp. 8–14.

[5] W. Fan and K. Yeung, "Online social networkslparadise of computer viruses," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 2, pp. 189–197, 2011.

[6] C. Wang, K. Xu, and G. Zhang, "A seir-based model for virus propagation on sns," in *Emerging Intelligent Data and Web Technologies (EIDWT), 2013 Fourth International Conference on*. IEEE, 2013, pp. 479–482.

[7] J. R. C. Piqueira and V. O. Araujo, "A modified epidemiological model for computer viruses," *Applied Mathematics and Computation*, vol. 213, no. 2, pp. 355–360, 2009.

[8] J. R. Piqueira, A. A. de Vasconcelos, C. E. Gabriel, and V. O. Araujo, "Dynamic models for computer viruses," *Computers & Security*, vol. 27, no. 7, pp. 355–359, 2008.

[9] S. K. P. Bimal Kumar Mishraa, "Effect of anti-virus software on infectious nodes in computer network: A mathematical model," *Physics Letters A*, vol. 376, no. 35, p. 2389C2393, 2012.

[10] B.-H. Liu, Y.-P. Hsu, and W.-C. Ke, "Virus infection control in online social networks based on probabilistic communities," *International Journal of Communication Systems*, 2013.

[11] X. Wei, N. C. Valler, M. Faloutsos, I. Neamtiu, B. A. Prakash, and C. Faloutsos, "Smartphone viruses propagation on heterogeneous composite networks," in *Network Science Workshop (NSW), 2013 IEEE 2nd*. IEEE, 2013, pp. 106–109.

[12] F. Iram, F. Muhammad, L. Young-Koo, and L. Sungyoung, "Modm: Multi-objective diffusion model for dynamic social networks using evolutionary algorithm," *The Journal of Supercomputing*, vol. 66, no. 2, pp. 738–759, 2013.

[13] B. Xu and L. Liu, "Information diffusion through online social networks," in *Emergency Management and Management Sciences (ICEMMS), 2010 IEEE International Conference on*. IEEE, 2010, pp. 53–56.

[14] J. Leskovec, "Stanford Large Network Dataset Collection," http://snap.stanford.edu/data/, 2007, [Online; accessed 19-May-2013].