Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 544-552, 2016
ISSN 1990-9233;
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.TAET23637

Propagation Analysis and Prevention Model for Modern Email Malware

[1]*S. Sneha,* [1]*L. Malathi and* [2]*P. Pandian*

[1]Department of CSE, Vivekanandha College of Engineering for Women, TamilNadu, India
[2]Department of Mathematics, VIT University, Vellore, TamilNadu, India

Abstract: Due to the security threats imposed by email-based malware, it is necessary to develop a prevention model to avoid potential damages caused by them. Compared to earlier versions of Mail malware, modern email malware exhibits two characteristics: reinfection and self-start. In reinfection, any healthy or infected recipients open the malicious attached file the modern email malware sends its copy to all users in list. In self-start, compromised computers restart or malicious files have visited the malware and then the malware occupied the memory of the system by spreading its copy. Already some models were developed for analyzing the malware propagation still there is needed to improve the accuracy of the model. The existing approach uses virtual node concept which increases the computational overhead. To address these problems, a novel SEIRI analytical model is proposed to analyze and prevent the modern email malware. Based on the result of the analysis model the impact of parameters in propagation is evaluated and presents the automated email malware detection and control system. Detailed analysis and simulation demonstrate that the proposed model can precisely describe the process of email malware's propagation and detection.

Key words:

INTRODUCTION

In the real world, the email is a essential service for computer users while email malware poses critical security threats. A computer virus is one of the main forms of malicious information spreading on the Internet. According to their propagation mechanisms, researchers categorize computer viruses into scanning-based viruses and topological-based viruses. The email malware is based on the topological viruses. Once an Internet user is infected by an email malware, the computer of this user will send malicious email copies to friends embedded in email lists. When users receive and read the malicious email copies or visit the malicious webpage conducted by the hyperlink, their computers will be infected. The infection processes is repeated from one user to their topologically neighboring users and then spreads quickly, reaching a large scale. Compared with scanning-based computer viruses, topological-based viruses rely on the information contained in a victim's machine to locate new targets. This intelligent mechanism allows far more efficient propagation than scanning-based viruses that make a huge number of wild guesses for every successful infection. Thus, the email malware can infect other victims on most attempts.

Current research on email malware focuses on modeling the propagation dynamics [1], [2], [3], [4], [5] which is a fundamental technique for developing countermeasures to reduce email malware's spreading speed and prevalence. In email malware a user can be infected and send out malware copies only once, no matter whether or not the user visits a malicious hyperlink or attachment again [1], [2], [3], [6]. The modern email malware is far more aggressive to spread in the network than before because of the two new propagation features such as reinfection and self-start. In reinfection, an infected user sends out malware copies whenever this user visits the malicious hyperlinks or attachments. An infected user sends out malware copies when certain events like PC restart are triggered in self-start feature. Because of these two new features [7], [8], [9] a user can be infected multiple times. It is a big challenge to

Corresponding Author: S. Sneha, Department of CSE, Vivekanandha College of Engineering for Women, TamilNadu, India.

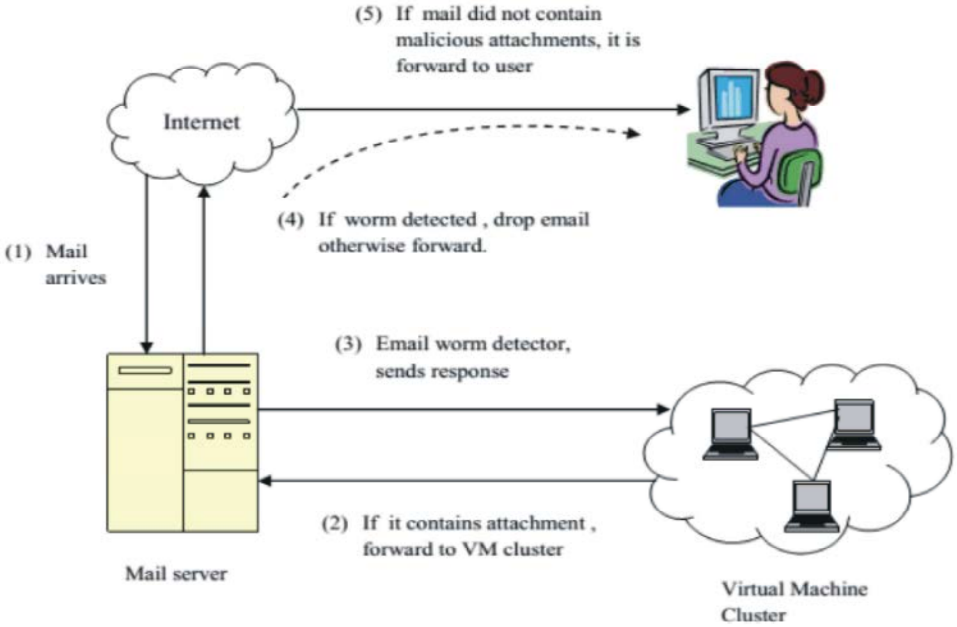
(5) If mail did not contain malicious attachments, it is forward to user
Internet
(4) If worm detected , drop email otherwise forward.
(1) Mail arrives
(3) Email worm detector, sends response
(2) If it contains attachment , forward to VM cluster
Mail server
Virtual Machine Cluster

Fig. 1: System Architecture

investigate modern email malware through mathematical modeling. Most email malware in the last decade, such as Mydoom in 2004, Nyxem in 2006, Here you are" in 2010 and recent unnamed email malware belong to the modern email malware.

The previous analytical model [10] presented the spreading procedure by a susceptible-infected-immunized (SII) process while it cannot accurately estimate the propagation of modern email malware. An SEIRI analytical model is proposed to describe the propagation dynamics of the modern email malware. The spreading procedure can be characterized by a susceptible-exposed-infected-removed-immunized (SEIRI) process. The system architecture of the proposed model is given in Fig. 1.

In this paper, we define virus propagation rules as follows:

- If a susceptible node contacts with an infectious node, then the susceptible node transmits into an exposed node.
- An exposed node will transmit into an infectious node when it gets the malicious mail from the infected node.
- An infectious node will transmit into a recovered state if the user neglects the infected mail.
- An infectious node will transmit into an immunized state if the user immunizes the infected mail.

Related Work: There have been generous efforts in modeling the propagation dynamics of email malware in the last decade. To model the epidemic spreading on topological networks, early researchers adopt differential equations to present the propagation dynamics of malware. Zou *et al*. [11] and Gao *et al*. [2] rely on simulations to model the spread of email malware. Their simulation models avoid the "homogeneous mixing" problem but cannot provide analytical propagation studies. The works [1], [3], [4], [12] propose mathematical models, which have captured the accurate topological information. Wen et al. [12] further addressed the temporal dynamics and the spatial dependence problem in the propagation modeling. However, all these models cannot present the reinfection and self-start processes of modern email malware.

Z. Chen and C. Ji proposed an analytical model that [13] offered the spreading procedure by a susceptible-infected-susceptible (SIS) process. In this model, both susceptible and infected users can be susceptible again. In [1] M. Boguna, R. Pastor-Satorras and A. Vespignani presented the SIR model to describe the email malware propagation. In this model, both susceptible and infected users can be recovered and they would receive lifelong immunity. The work of Chao Wang, Ke Xu and Gaoyu Zhan [9] characterized the propagation dynamics of isomorphic malware, such as P2P malware [1], mobile malware [14], [15] and malware on online social networks [16], [15], [17]. Since these models are based on non-reinfection, they cannot be adopted to present the propagation of modern email malware.

To address the problem of reinfection and self-start Sheng Wen [10], proposed a novel analytical SII model. It cannot accurately estimate the propagation of modern email malware. This model had some minor divergence between the results of SII model and simulations because of the independent assumption.

Problem Statement: Choosing email as the spreading carrier of malware is not a new technique in the last decade. Early versions of email malware work in a "naive" way, that is, a compromised user will send out malware emails only once, after which the user will not send out any further malware copies, even if the user visits the malicious hyperlinks or attachments again. But, modern email malware is far more aggressive in spreading throughout email networks than before. Generally, it is common for the malware emails to reuse the themes but with slight variation on the body of the message and the attachment names. This trick increases the possibility for a user to be infected and particularly prompts the spreading efficiency of the modern reinfection email malware.

Without checking if a computer has been infected before, modern email malware makes use of every chance to spread itself. The malware propagation is based on the mechanisms namely non-reinfection, reflection and self-start [18]. In fact, reinfection is not enough to describe the propagation of modern email malware since most real email malware is the self-start email malware. Compared with the reinfection and the self-start, to model the non-reinfection is simple [9]. Therefore, the two kinds of mechanisms, namely reinfection and self-start are used to characterize the propagation of modern email malware completely.

Reinfection indicates a user may get infected whenever the user visits malicious hyperlink or attachments. The reinfection outperforms the non-reinfection in two aspects as given below:

- A user can be infected again even if the user has been infected before [18].
- A user will send out a malware copy each time the user gets infected.

Thus, a recipient may repeatedly receive malware emails from the same compromised user.

Self-start refers to the behavior that malware starts to spread whenever compromised computers restart or certain files are visited. The outperformance of the self-start is given below:

A user has been infected at a particular time. When the user restarts the computer the later time, a malware email copy will be sent to another user because of self-start. Compared with the non-reinfection and the reinfection, another user receives totally 2k+1malware emails if the user sends k emails. Therefore, the self-start mechanism can spread much faster than the non-reinfection and the reinfection models.

To overcome these difficulties an SEIRI analytical model is proposed in this work that can describe the propagation dynamics of the modern email malware [19].

Proposed Model: To overcome the inaccuracy of previous models, we propose an SEIRI model for modern email malware. SEIRI model is different from SIS and SIR models [18], [10] and SII model [10]. In this model, susceptible, exposed and infected users can be removed or immunized.

SEIRI Model: The basic elements for the propagation of modern email malware are nodes and topology information. A node represents a user in the email network. Let random variable *X_i(t)* denote the state of a node *i* at discrete time *t* [9]. Then, we have;

$$X_i(t) = \begin{cases} \mathit{Hea., Healthy} \begin{cases} \mathit{Sus., Susceptible} \\ \mathit{Exp., Exposed} \\ \mathit{Imm., Immunized} \end{cases} \\ \mathit{Inf., Infected} \begin{cases} \mathit{Act., Active} \\ \mathit{Dor., Dormant} \\ \mathit{Rem., Removable} \end{cases} \end{cases} \qquad (1)$$

Initially, all the nodes in the network are susceptible. In the susceptible, state the user has the possibility of getting infected. The susceptible node transits to an active state when the user gets infected. If the user *i* is in the address book of the infected user, then the infection possibility of the user *i* is higher than other user. Therefore, the user transits from the susceptible state to the exposed state. Since the infected user sends out the malware to the user *i* when it is compromised, then the user *i* transits from exposed state to the active state after the user *i* infected. In the active state, the user is infected and also infectious. When the user is infected but not infectious, then the state of the user is switched to dormant state from active state.

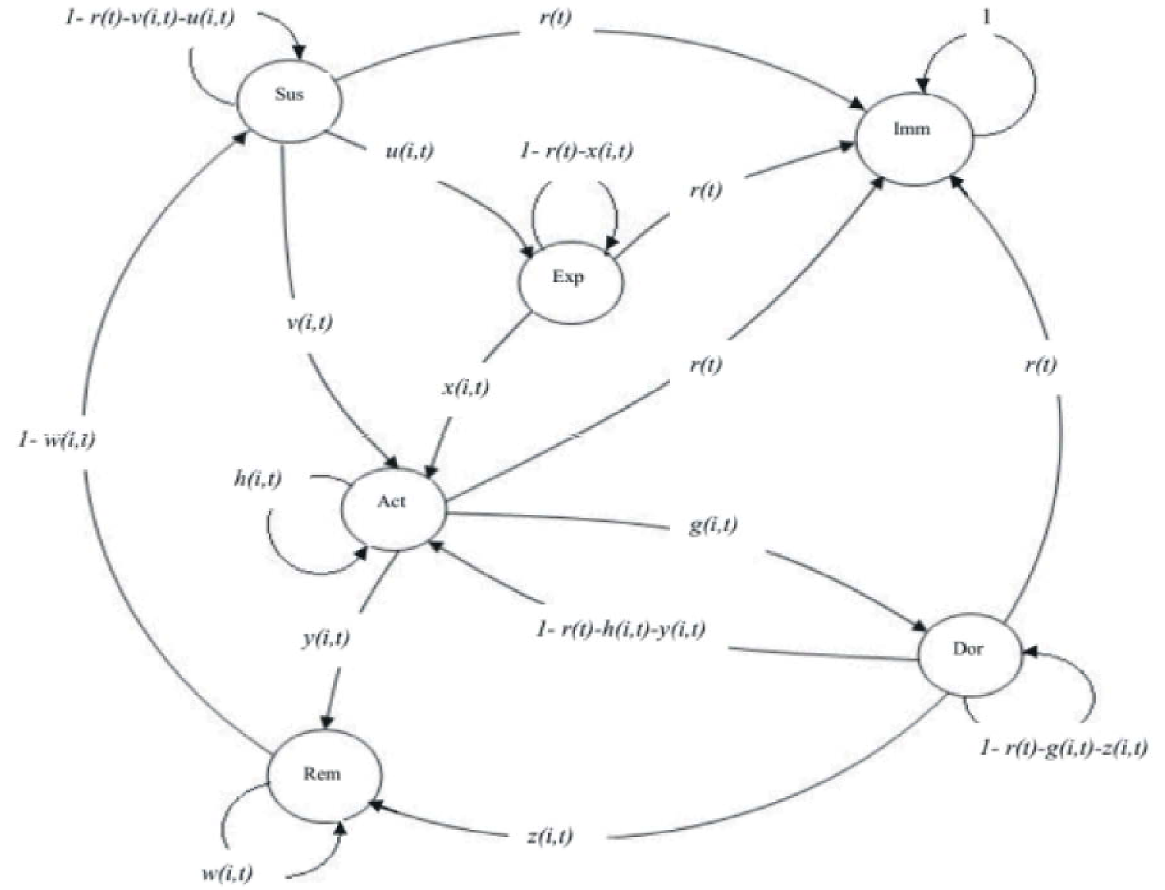

Fig. 2: State transition graph

When the user *i* is in an active state or dormant state, then the user *i* is transited to removable state. Once the user transits to removable state then the user, *i* has moved to the susceptible state again. Whatever the state an arbitrary node is at, it may transit to the immunized state [19].

Let *r(t)* is the probability of immunization. *h(i, t)* is the probability that, an arbitrary node is in the active state. *g(i, t)* is probability that, node *i* transits from dormant to active state. *v(i, t)* is the probability that, node *i* transits from susceptible to active state. *u(i, t)* be the probability that node *i* transits from susceptible to exposed state. *w(i, t)* is the probability that node i is in the removable state. *x(i, t)* is the probability that the node *i* moved to active state from exposed state. *y(i, t)* is the probability that the node *i* transits from an active state to removable state. *z(i, t)* is the probability that the node *i* transits from a dormant state to removable state. In SEIRI Model, an M by M square matrix with elements pij is used to describe a topology, [9] as in,

$$\begin{pmatrix} p_{11} & \cdots & p_{1M} \\ \vdots & p_{ij} & \vdots \\ p_{M1} & \cdots & p_{MM} \end{pmatrix} p_{ij} \in [0,1] \tag{2}$$

where in pij represents the probability of user j visiting a deceptive malware email received from user i. If pij is equal to zero, it means the email address of user j is not in the contact list of user i.

Therefore, the matrix reflects the topology of an email network. In this model, assume the states of neighbouring nodes are dependent.

The infection of email malware depends on unwary email users checking new emails and visiting those malicious ones. In fact, this process involves two components in the modeling. First, we introduce the flag variable $open_i(t)$. We define *open (t)=1*, if the user is checking new emails at time t, otherwise $open_i(t)=0$. Let T_i denote the email checking period of user i, then we have, [9].

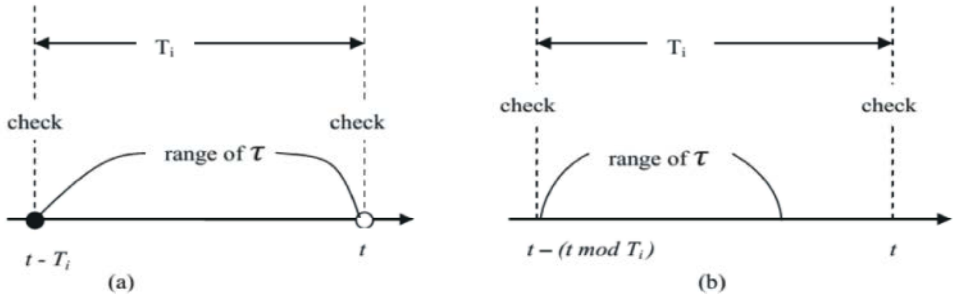

Fig. 3: Different cases of variable τ. (a) User cheeks now emails at current time t; (b) user does not cheek emails at current time t

$$P(open_i(t) = 1) = \begin{cases} 0\ , otherwise \\ 1, t \bmod T_i = 0 \end{cases} \tag{3}$$

Note that different users have different values of T_i. An email user may receive multiple emails at the different time, but read all of them at one time when the user checks the mailbox. Supposing that an arbitrary user *i* checks new emails at time *t*, then those emails who will be checked at time *t* are the ones which arrived at user *i* after the user's last checking action of her mailbox. It is significant to obtain the number of such emails for our modeling. Thus, we introduce a variable *t* to indicate an arbitrary time between the time of user *i*'s last email checking action and the current time *t* (excluding t). The value of t has two forms depending on if user checks emails at current t or not [9]. Then, we have

$$\begin{cases} t - T_i \le \tau < t, & if\ open_i(t) = 1 \\ t - (t \bmod T_i) \le \tau < t, & otherwise \end{cases} \tag{4}$$

A compromised user can only spread malware to the neighboring users in email networks. Thus, for each email user in networks, we record and accumulate every newly arrived malicious email from neighboring users at each t and finally obtain the joint infection probability of each user who checks those emails.

Modeling Propagation Dynamics: We use the values 0 and 1 to substitute the healthy state and the infected state, respectively. Given a topology of an email network with M nodes, the expected number of infected users at time t, n(t), is computed as in, [9].

$$\begin{aligned} n(t) &= \left[\sum_{i=1}^{M} X_i(t)\right] = \sum_{i=1}^{M} E[X_i(t)] \\ &= \sum_{i=1}^{M} [(0P(X_i(t) = 0) + (1P(X_i(t) = 1))] = \sum_{i=1}^{M} P(X_i(t) = 1) \\ &= \sum_{i=1}^{M} P(X_i(t) = inf) \qquad (5) \end{aligned} \tag{5}$$

The expected number of infected nodes, *n(t)*, is equal to the sum of the probability of each node being infected a time *t*, $P(X_i(t) = inf)$. As shown in Fig. 3, a susceptible node and an exposed node can be compromised and be at the infected state and an infected node can be recovered and be at the immunized state. The state transitions help us derive the computation of $P(X_i(t) = inf)$ [9] by difference equations as follows:

$$P(X_i(t) = inf) = (1 - r(t))P(X_i(t-1) = inf) + v(i, t)P(X_i(t-1) = Sus) + x(i, t)P(X_i(t-1) = Exp) \tag{6}$$

For the computation of $P(X_i(t) = Sus)$ we have,

$$P(X_i(t) = Sus) = 1 - P(X_i(t) = inf) - P(X_i(t) = Exp) - P(X_i(t) = Imm) \tag{7}$$

For the computation of $P(X_i(t) = Imm)$ we have,

$$P(X_i(t) = Exp) = u(i, t)P(X_i(t) = Sus) + (1 - r(t))P(X_i(t-1) = Inf) + (1 - x(i, t)P(X_i(t-1) = Inf \tag{8}$$

For the computation of $P(X_i(t) = Imm)$ we have,

$$P(X_i(t) = Imm) = P(X_i(t-1) = Imm) + r(t).\ [1 - P(X_i(t-1) = Imm)] \tag{9}$$

Once we obtain the values of v(i, t), x(i, t) and r(t), the value of $P(X_i(t) = Inf)$ can be computed by the iteration of the above equations, (6), (7), (8) and (9).

In fact, there are three preconditions for an arbitrary user being infected by email malware, which is given below:

- The user has not been immunized;
- The user checks mailbox for new emails;
- The user unwarily visits one received malware emails.

When the first and the second preconditions are satisfied, we use *s(i, t)* to represent the probability of user *i* visiting malware emails from neighboring nodes. Then, the infection probability *v(i, t)* and *x(i, t)* can be derived as in,

$$v(i, t) = s(i, t), P(open_i(t) = 1)(1 - r)(t)) \quad (10)$$

$$x(i, t) = s(i, t), P(open_i(t) = 1)(1 - r(t))(1 - u(i, t)) \quad (11)$$

In our SEIRI model, an arbitrary user *i* visit malicious hyperlinks or attachments with probability p_{ji} when reading malware emails from a neighboring user *j*. We use N_i to denote the set of neighboring nodes of node i after removing unknown nodes. Then, we can compute *s(i, t)* as in,

$$s(i, t) = \Pi_{j\epsilon Ni}[1 - p_{ji} \,.\, P(X_j(\tau) = Act)] \quad (12)$$

where in the event $X_j(\tau) = Act$ means that the node *j* is infected and sends out a malware mail copy to neighboring nodes at time τ.

Considering different values that the variable τ may take, we disassemble the equation (12) by excluding t 1 from the range of value τ. There are two cases. First, as shown in Fig. 3a, user does not check new emails in the mailbox at time *t1*. Thus, we have,

$$\prod_{j\in N_i}[1 - p_{ji}.P(X_j(\tau) = Act)] =$$
$$\prod_{j\in N_i,\tau\neq t-1}[1 - p_{ji}.P(X_j(\tau) = Act)] \times \prod_{j\in N_i}[1 - p_{ji}.P(X_j(t-1) = Act)] \quad (13)$$

$$= (1 - s(i, t-1).\Pi_{j\in N_i}[1 - p_{ji}.P(X_j(t-1) = Act)] \quad (14)$$

Second, as shown in Fig. 3b, user checks new emails in the mailbox at time t1. Thus, the malware email copies received at time t are those sent at time t1by the infected neighboring users. The variable t only takes the value t1. In this case, we have,

$$\prod_{j\in N_i}[1 - p_{ji}.P(X_j(\tau) = Act)] =$$
$$\prod_{j\in N_i}[1 - p_{ji}.P(X_j(t-1) = Act)] \quad (15)$$

Actually, the difference of equations (14) and (15) are caused by user checking newly arrived emails at time t1. Then unified expression of (14) and (15) is given below:

$$\prod_{j\in N_i}[1 - p_{ji}.P(X_j(\tau) = Act)] =$$
$$\left[1 - s(i, t-1).\left(1 - P\,(open_i(t-1) = 1)\right)\right].$$
$$\Pi_{j\in N_i}[1 - p_{ji}.P(X_j(t-1) = Act)] \quad (16)$$

Now, the equation (12) becomes,

$$s(i, t) = 1 - [1 - s(i.\, t-1).\ (1 - P\ (open_i(t-1) = 1))] \times \Pi_{j\epsilon Ni}$$
$$[1 - P_{ij}\ .\ P(X_j\ (t-1) = Act)] \quad (17)$$

In equation (17), different measures of $P(X_j(t-1) = Act)$ and Ni may lead to different spreading performance. The algorithm of SEIRI model is determined by following steps,

Step 1: Read the network structure to initialize the network data, user's mail checking probability and mail opening probability based on (2), (3) & (4).

Step 2: Select a number of initially infected nodes.

Step 3: Update the user's average mail opening probability and checking time by (15),

$$\prod_{j\in N_i}[1 - p_{ji}.P(X_j(\tau) = Act)]$$

Here the event $X_j\ (\tau) = Act$ means that the node j is infected and sends out a malware mail copy to neighboring nodes at time τ.

In the case of user's checking email,

Step 4: If the virus were removed then update the state of the user as healthy.

Step 5: If virus was not removed but opened then the nodes will be infected and also infect their neighbor nodes (12), $s(i, t) = \Pi_{j\epsilon Ni}\ [1 - p_{ij}\ .\ P(X_i(\tau) = Act)]$

Step 6: The receiver can remove or immunize the email (9), $P(X_i\ (t) = Imm) = P(X_i(t-1) = Imm) + r(t), [1 - P(X_i(t-1) = Imm)]$, update their states to healthy and new checking time (15).

Step 7: Compute number of infected nodes by using the $s(i, t)$ value.

Step 8: Repeat the step 3 to find the average infected nodes by using (16),
$\Pi_{j\epsilon Ni}\ [1 - p_{ij}\ .\ P(X_j(\tau) = Act)]$

Step 9: The overall spreading performance can be calculated by using (17), here different measures of $P(X_j(t - 1) = Act$ and Ni may lead to different spreading performance.

Simulation and Results: In proposed SEIRI model the evaluation is based on the existing analytical model. In real-world scenarios, the spread of most email malware is typically impossible to track given the directed, topological manner in which they spread. Some email malware, like Nyxem [3], once compromising a computer, will automatically generate a single http request for the URL of an online statistics page. However, the statistics of Nyxem [9] also cannot present a precise investigation on the spread of email malware due to the legitimate access, repeated probes and DDoS attacks to the web page. It should be pointed out that there is no real data set available for the evaluation of models of modern email malware.

In this paper, we build the topology according to the previous analysis of real email networks. The topology has 100, 000 nodes [9]. The degree for each node was reproduced by the Power-law distribution. Moreover, the probability of users being infected by their friends (p_{ij}), the email checking period (T_i) and the event triggering period (R_i) are mainly decided by human factors. These parameters will follow the Gaussian distribution. Note that the Gaussian distribution generator may provide unrealistic values, such as $P_{ij} < 0$ and $T_i < 1$. In this experiment, these values are replaced with the minimums of their realistic range. Thus, if $P_{ij} < 0$, $T_i < 1$ and $R_i < 1$, we let $p_{ij} = 0$ $T_i = 1$ and $R_i = 1$ [9].

The impacts of various parameters on the accuracy of the modeling are evaluated.

First, the accuracy with different distributions of Ti and Ri are evaluated. In this experiment, the topology has the same settings, the curves of our SEIRI model are close to the simulations even if the distributions of Ti and Ri are different.

Second, the accuracy with different distributions of p_{ij} is also evaluated. The same topologies are used in this experiment. We let Ti and Ri follow Gaussian distribution $N(40, 20^2)$. As shown in Fig. 4, the results of our SEIRI model are close to the results of simulations. The SII model achieves better performance in accuracy when the infection probabilities pij are averagely higher.

Third, the accuracy in different topologies is evaluated. In this experiment, we let Ti and Ri follow Gaussian distribution $N(40, 20^2)$ and the infection probability pij follow $N(0.5, 0.2^2)$ [9]. As shown in Fig. 5, the proposed SEIRI model is effective in various topologies with different power-law exponents α and means of degrees E(D).

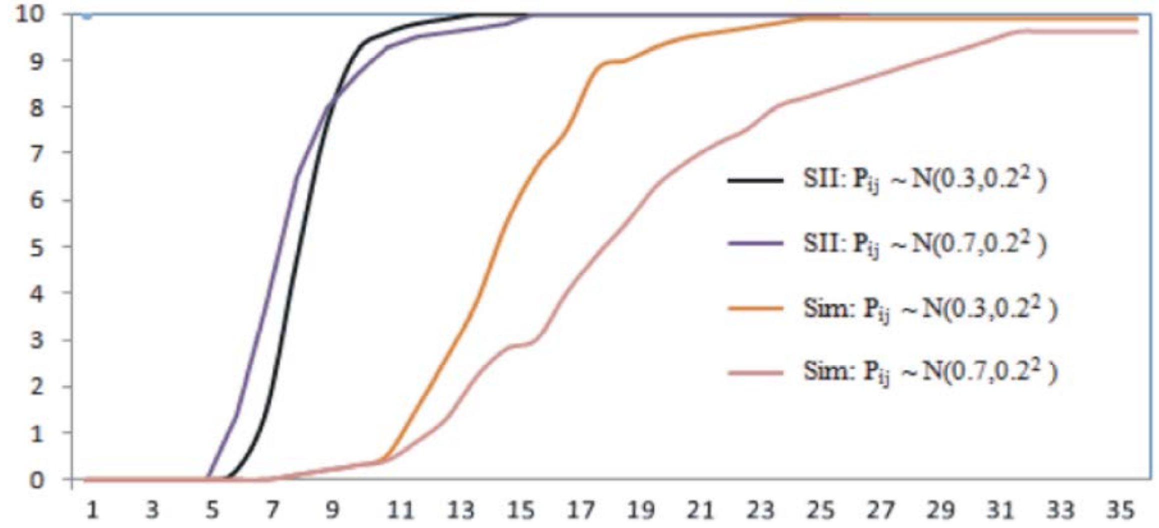

Fig. 4: The accuracy with different distributions

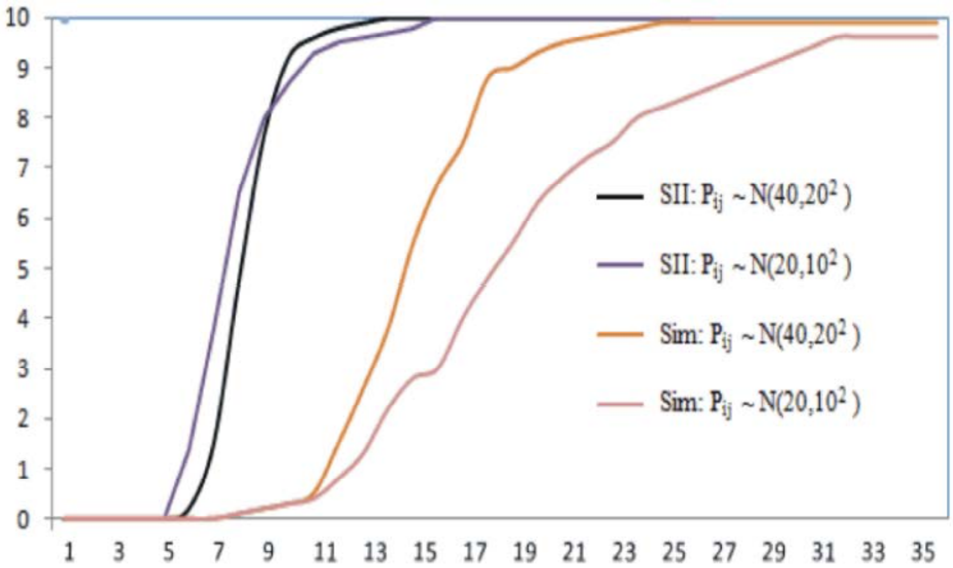

Fig. 5: The accuracy with different distributions of Ti and Ri

CONCLUSION

In this paper, we have proposed a novel SEIRI model for the propagation of modern email malware. This model is able to address two critical processes that are reinfection and self-start. By introducing a group of difference equations, the repetitious spreading processes caused by the reinfection and the self-start was presented. The experiments showed that the result of the proposed SEIRI model is closest to the simulations. For the future work, there are some unsolved problems like spatial dependence and temporal dynamics. A new simulation must be designed to contain real system samples, to analyze the malware behaviors against these samples after elaborate malware updating. The objectives of this simulation are to avoid systems threats before being infected by real malware.

REFERENCES

1. Fan, W. and K.H. Yeung, 2011. “Online Social Networks-Paradise of Computer Viruses, ”Physica A: Statistical Mechanics and Its Applications, 390(2): 189-197.
2. Garetto, M., W. Gong and D. Towsley, 2003. “Modeling malware spreading dynamics,” in Proc. INFOCOM’03, vol. 3, San Francisco, CA, Apr. 2003, pp: 1869-1879.
3. Wen, S., W. Zhou, Y. Wang, W. Zhou and Y. Xiang, 2012. “Locating Defense Positions for Thwarting the Propagation of Topological Worms, ”IEEE Comm. Letters, 16(4): 560-563.
4. Xiong, J., 2004. “Act: Attachment Chain Tracing Scheme for Email Virus Detection and Control, ”Proc. ACM Workshop Rapid Malcode (WORM ’04), pp: 11-22.
5. Zou, C.C., D. Towsley and W. Gong, 2007. “Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms, ” IEEE Trans. Dependable and Secure Computing, 4(2): 105-118.
6. Wen, S., W. Zhou, J. Zhang, Y. Xiang, W. Zhou and W. Jia, 2013. “Modeling Propagation Dynamics of Social Network Worms, ” IEEE Trans. Parallel and Distributed Systems, 24(8): 1633-1643.
7. Calzarossa, M. and E. Gelenbe, 2004. Performance Tools and Applications to Networked Systems: Revised Tutorial Lectures. Springer-Verlag.
8. Serazzi, G. and S. Zanero, 2003. “Computer Virus Propagation Models, ” Proc. 11th IEEE/ACM Int’l Conf. Modeling, Analysis and Simulations of Computer and Telecomm. Systems (MASCOTS ’03), pp: 1-10.
9. Sheng Wen, Yang Xiang and Weijia Jia, 2014. ‘Modeling and Analysis on the Propagation Dynamics of Modern Email Malware’, IEEE Transactions on Dependable and Secure Computing, 11(4).

10. Sneha, S., L. Malathi and R. Saranya, 2015. “A Survey on Malware Propagation Analysis and Prevention Model”, International Journal of Computer Applications (0975 – 8887), 131(11).
11. Zou, C.C., D. Towsley and W. Gong, 2007. “Modeling and Simulation Study of the Propagation and Defense of Internet E-Mail Worms, ” IEEE Trans. Dependable and Secure Computing, 4(2): 105-118.
12. Gao, C., J. Liu and N. Zhong, 2011. “Network Immunization and Virus Propagation in Email Networks: Experimental Evaluation and Analysis, ”Knowledge and Information Systems, 27: 253-279.
13. Chen, Z. and C. Ji, 2005. “Spatial-Temporal Modeling of Malware Propagation in Networks, ”IEEE Trans. Neural Networks, 16(5): 1291-1303.
14. Wang, Y., D. Chakrabarti, C. Wang and C. Faloutsos, 2003. “Epidemic Spreading in Real Networks: An Eigenvalue Viewpoint, ”Proc. 22nd Int’l Symp. Reliable Distributed Systems (SRDS), pp: 25-34.
15. Yanping Zhang, Tingting Sun and Shu Zhao, 2012. “A Novel Model to Restrain Email Virus Propagation”, IEEE International Conference on Granular Computing.
16. Ganesh, A.J., L. Massouli and D.F. Towsley, 2005. “The Effect of Network Topology on the Spread of Epidemics, ”Proc. IEEE INFOCOM ’05, pp: 1455-1466.
17. Yan, G. and S. Eidenbenz, 2009. “Modeling Propagation Dynamics of Bluetooth Worms (Extended Version), ”IEEE Trans. Mobile Computing, 8(3): 353-368.
18. Reshma Sharafudeen, 2015. “RS (Reinfection & Self-start) Analysis on the propagated email malware”, IRJET, pp: 2.
19. Regan, R., J. Renuka and V. Sanmugasundari, 2015. “Malicious programs analysis propagation in online social networks”, AENSI, 9(21) Special 2015.