Sensors & Transducers

© 2013 by IFSA
http://www.sensorsportal.com

Research on Propagation Model of Malicious Programs in Ad Hoc Wireless Network

[1] Weimin GAO, [1] Lingzhi ZHU, [2] Junbin LIANG

[1] School of Computer and Information Science, Hunan Institute of Technology,
Hengyang 421002, China
[2] School of Computer and Electronics Information, Guangxi University,
Nanning 530004, China
[1] Tel.: 86-734-3452102, fax: 86-734-3452222
E-mail: gwmhy@163.com

Received: 22 October 2013 /Accepted: 9 January 2014 /Published: 31 January 2014

Abstract: Ad Hoc wireless network faces more security threats than traditional network due to its P2P system structure and the limited node resources. In recent years, malicious program has become one of the most important researches on international network security and information security. The research of malicious programs on wireless network has become a new research hotspot in the field of malicious programs. This paper first analyzed the Ad Hoc network system structure, security threats, the common classification of malicious programs and the bionic propagation model. Then starting from the differential equations of the SEIR virus propagation model, the question caused by introducing the SEIR virus propagation model in Ad Hoc wireless network was analyzed. This paper improved the malicious program propagation model through introducing the network topology features and concepts such as immunization delay, and designed an improved algorithm combined with the dynamic evolution of malware propagation process. Considering of the network virus propagation characteristics, network characteristics and immunization strategy to improve simulation model experiment analysis, the experimental results show that both the immunization strategy and the degrees of node can affect the propagation of malicious program. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Propagation models, Immune strategy, Malicious programs, Ad Hoc wireless network, Security threats.

1. Introduction

With the increasingly extensive application of portable wireless devices, wireless networks have gradually become an indispensable part for daily network facilities. However, due to the vulnerabilities of wireless networks, for example, the openness of media, terminal mobility, dynamic changes of network topology, cooperative algorithm, lack of centralized monitoring and administrative points, an increasing number of malicious programs have emerged in wireless network, leading to great threaten to wireless network security. Especially because of the diversified routes of transmission and complex application of these malicious programs, mobile networks information security breach incidents are more frequent, spreading faster, covering a wider range and causing greater damage.

In research of propagation models of malicious programs, an integration of epidemic models and propagation characteristics of malicious programs is a frequently used method. Robert G. conducted the research on the behavior of worms on the Mobile Ad hoc Network (MANET) based on SIS propagation models in first. He considered the impact of the worm propagation delay and bandwidth constraints on worm propagation, but ignored the impact of human measures. Abdelmajid Khelil and other scientists researched the epidemic model of information diffusion on MANET. SIR/WS model described malicious programs propagation in wireless sensor network was proposed in [1, 4]. The model, based on IEEE 802.15.4 Standard, discovered that infected nodes propagated malicious programs with a broadcast mode, and provided the relation between the number of infected nodes and infectious rate as well as immunization rate. A propagation dynamics model based on the analysis of the Bluetooth malware propagation process [2, 3] is established by means of theoretical derivation after abstracting the function of Bluetooth protocols and the mobility of Bluetooth devices into several statistical metrics. The model illustrates that the introduction of authentication mechanism can greatly decrease the propagation speed of Bluetooth malware. A virus model was constructed in paper [5-8] where viruses spread on a increasingly evolving Internet and analyzed the dependence of the density for infected computers on its topology. All the results obtained here indicate that the larger the rate of network evolvement is, the faster virus spreads.

Previous studies usually consider that each node in the network (infectivity) is equal to the node of degree K, even if at each time step, a node and its neighbor nodes are all contacting [9]. However, this assumption does not hold in the propagation process of many practical. For example: in the Internet network if the router to ask, there is no exchange of data packet will not appear [10] virus propagation in the network; in the global aviation network, if no one is related to the travel activities in different city, the virus is unlikely in the different regions of the diffusion of [11]; in the social network, no mosquito bites there is no typical dengue virus infection [12] in a population of similar situations in real life there are many times. In the process of communication, network nodes in the appeal and node degree and is not directly related to K, but depends on the interaction between nodes or network transmission material [14], Yanjin etc. [15] establish a real-time network risk evaluation model. According to the network intrusion own characteristics and propagation models of malicious programs, assets and attack, combines assets evaluation system and network integration evaluation system, considering from the application layer, the host layer, network layer may be factors that affect the network risks. The new model improves the ability of intrusion detection and prevention than that of the traditional passive intrusion prevention systems.

Different propagation models are employed to study real networks with different spreading modes; classical models include Susceptible-Infected (SI) Model, Susceptible-Infected-Susceptible (SIS) Model, Susceptible-Infected-Removed (SIR) Model and Susceptible-Exposed--Infected-Removed (SEIR) Model. Scale-free networks are fragile for virus spread and attacks; this necessitates affiant immune strategy for a network. Typical strategies being recently studied include random immunization, acquaintance immunization, target immunization, and a variety of improved strategies. This thesis studied the topology of networks, combined with the dynamic evolution of malicious propagation process to design an improved algorithm of Malicious Program Propagation in Ad Hoc network. However in the real world, most real networks exhibit scale-free, so we design a dynamic immune strategy. The detailed work is as follows.

Section 2 describes Ad Hoc wireless network and security threats; Section 3 describes common malicious programs and propagation models; Section 4 gives detailed descriptions of the algorithm of the improved algorithm of malicious Program Propagation in Ad Hoc network; section 5 describes dynamic immune strategy; Section 6 describes our simulation results and analysis. Finally, we conclude in Section 7.

2. Wireless Ad Hoc Network and Security Threats

Ad Hoc wireless network, also named wireless multi-hop network, is a self-organizing network which is composed by several mobile nodes and there's no need for fixed infrastructure. As the network structure is shown in Fig. 1, mobiles nodes form a distributed autonomous system by interconnecting the wireless channels.

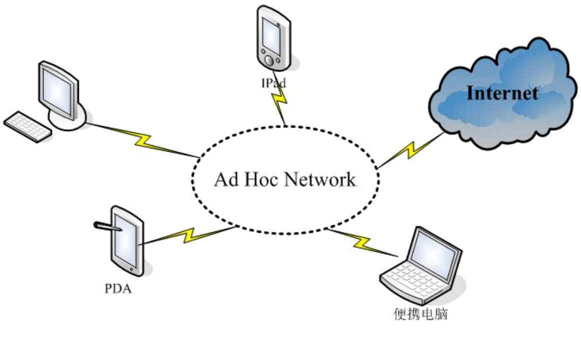

Fig. 1. Structure of Wireless Ad Hoc Network.

Moreover, each node is a router to discover and maintain the routing functions to other nodes. This system could run separately or be connected to fixed networks through gateway or an interface. Ad Hoc Wireless network could set up a mobile communication network anytime and anyplace without the support of fixed infrastructure and the pre-allocation of host computer. Each node is mobile and can communicate to others with a peer mode. In addition, the wireless Ad Hoc network has high interoperability and usually applies network route protocol of distributed control. Compared with centralized structured networks, wireless Ad Hoc network has stronger robustness and invulnerability. As a result, it is widely used in conferences, emergencies, expeditions and military actions.

Wireless network is congenitally deficient in some aspects, such as open media, terminal mobility, dynamic network topology, lack of centralized monitoring or clear defense line, so there are great risks in wireless network security. Security threat is defined as the dangers caused by some people, objects or events to the confidentiality, integrity, availability or legal use of a resource, and it can be divided into technical threat and content threat. Technical threat is the threats that are caused by the use of certain technical means or vulnerability of wireless networks, and content threat indicates the threat caused by certain impact on subjective cognition of network users with content and properties of information propagating in networks.

From the perspective of application range of wireless networks and users' demand, the present security threats of network security include 4 areas:

1) Interruption: malicious programs use illegal means to attack availability of the network and destroy software and hardware resources in mobile Internet system so that the network does not work.

2) Modification: malicious programs attack the integrity of networks, modify network elements of the mobile network contents in business database, and modify the order of the messages for delay or replay.

3) Eavesdropping: malicious programs attack the confidentiality of networks through wire tapping and electromagnetic leakage in transmission link of wireless network, which result in disclosure of confidential information or acquisition useful information by analyzing the business flow. A number of criminals can accurately extract the information through eavesdropping techniques, and expose the confidential information or take it for criminal activities.

4) Falsification: criminals attack networks authenticity through injecting falsified or false information into networks, impersonating legal users to access mobile networks, replaying the captures legal information for illegal purposes, inserting malicious programs such as worms, Trojan and logical bombs to damage the proper functioning of mobile networks, or denying receiving or sending of messages.

3. Common Malicious Programs and Propagation Models

Malicious program is any software program translated from computers or networks which aims to destroy the user's computer system without the user's knowledge. Malicious programs can be divided into two categories, one has to rely on a host and the other can run independently. A malicious program that needs a host are actually a segment of a program, it cannot be separated from specific application programs, utility facility programs or system programs. While an independent malicious program is a complete program that can be run directly. The common mobile malicious programs are shown in Fig. 2.

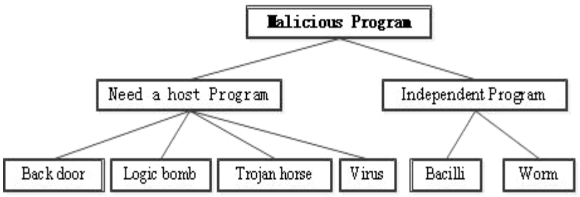

Fig. 2. Common malicious programs.

Malicious programs have the basic features of computer viruses, which are similar to biological viruses in areas such as infection, duplication and parasitism, etc. Many researchers divide malicious program models into 3 categories based on the mature theoretical models in biology: SIS model, SIR model and SEIR model.

In Susceptible-Infected-Susceptible (SIS) model, nodes are divided into 2 statuses: susceptible status (S) and infected status (I). Once susceptible nodes are infected by malicious programs and become infected nodes, infected nodes will transmit virus to infect other nodes. When it is infected, an S node becomes an I node and an I node becomes S node when it is cured. Therefore, viruses may repeatedly transmit within the propagation range and always survive. The propagation model is shown in Fig. 3(a).

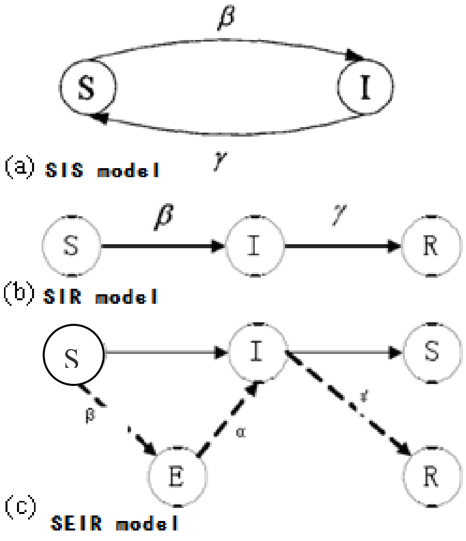

Fig. 3. Common propagation model.

Susceptible-Infected-Removed model includes an additional immune node (R) on the basis of SIS model, and R node does not get infected. In this model, two constants, β and γ, are given, β is the probability of S node getting infected in unit time, and γ indicates the probability of I node getting cured in unit time. The propagation model is shown in Fig. 3(b).

Susceptible-Exposed-Infected-Removed model includes an additional incubation node (E) on basis of SIR model. E node indicates a node which has been inserted virus code but has not shown virus features, i.e. a node has not been activated yet. In addition, a constant α is given in SEIR model, and α is the incubation period or propagation rate of virus. The propagation model is shown in Fig. 3(c).

4. Buildup of Propagation Model of Malicious Program in Wireless Ad Hoc

SIS and SIR are propagation models of two epidemic diseases in biology, so direct utilization of them for research on propagation of malicious program would cause deviation and errors, e.g. no external impact on virus propagation is taken into consideration in the two models, and only constant β and γ are related to the status conversion of nodes. While in SEIR model, a node may be paralyzed or immune after getting infected, so in a specific period it would not infect other nodes in the network. Thus, SEIR model is a classically used propagation model. In the following research on improvement of propagation model of malicious programs in wireless Ad Hoc is conducted based on SEIR model.

4.1. Differential Equation of SEIR Propagation Model

SEIR model proposes the propagation process of malicious programs in uniform network based on mean field theory, in which infected nodes or immune nodes have the conversion rate δ of becoming S nodes again. Assuming I(t) represents the number of hosts with infection at the moment of t; r(t) represents the number of hosts getting immune at the moment of t; S(t) indicates the number of all hosts have been infected at the moment of t; β is the infection rate; and γ is the recovery rate of the hosts removed from infected ones. Thus, SIR model can be formulated with the following differential equations:

$$\frac{dI(t)}{dt} = \beta I(t)s(t) - \gamma I(t) \tag{1}$$

$$\frac{dS(t)}{dt} = -\beta S(t)I(t) - \delta R(t) \tag{2}$$

$$\frac{dR(t)}{dt} = \gamma I(t) - \delta R(t) \tag{3}$$

For SEIR model, when an infected node is getting immune, it is equivalent to the case that this node is removed from the entire network node hosts, thus the total number of network nodes turns to N-1 from N. Fig. 4 shows the propagation trend of malicious programs in SIR model. In Fig. 4, the number of nodes is taken as N=104, infection rate β=10-7, when the number of copies of malicious program S(0)=3, the recovery rate is γ=10-3. It can be seen that finally the total number of nodes and the number of the infected hosts in the entire network will become 0.

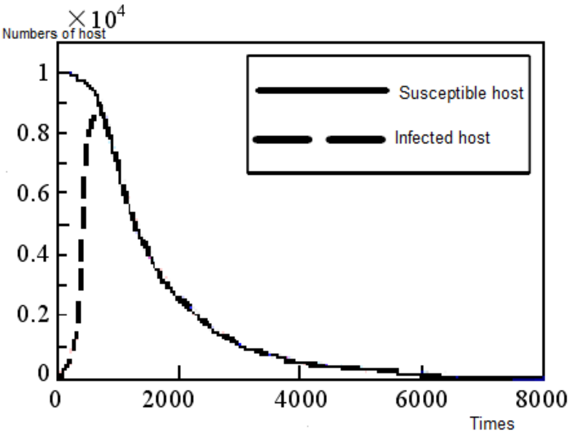

Fig. 4. Propagation trend of malicious program in SEIR model.

Two problems will occur if SEIR model is applied in wireless Ad Hoc network: firstly, as the model takes the average connectivity as the only topology metric, it cannot acquire the diversity of connectivity in mobile environment; secondly, it is insensitive to velocity of nodes, which would cause the predicted value of infection rate of malicious program lower than it is in practical application.

4.2. Basic Definitions to Improve SEIR Model

To solve the problems in SEIR model, and given that propagation of malicious programs is accompanied with dynamic evolution of the network, speed parameter of nodes and connectivity change caused by mobility, it is necessary to implement appropriate improvements. The improved model applies similar status of nodes with nodes in SEIR model: susceptible status, infected status and immune status. While the new model introduces 2 additional concepts, i.e. network topological property and immunization strategy. To facilitate the discussion, basic definitions in the improved model are given as below:

Propagation rate: in each unit time, infected nodes spread virus to neighbor nodes, and ratio of the number of infected nodes and the number of neighbor nodes is named as propagation rate, represented by α.

Infection rate: in each unit time, each susceptible node has a certain probability to receive one or several copies of virus from its neighbor nodes, the probability is the infection rate represented by constant β. To distinguish the infection rate of each node, β_k is used to indicate the infection rate of the susceptible node with a degree of k.

Immunization rate: after taking a specific immunization strategy, in each unit time, each non-cured node has a certain probability to receive one or several copies of vaccine and become immune node, this probability is the immunization rate represented by constant γ. Similarly, to distinguish the immunization rate of each node, γ_k is used to indicate the immunization rate of the susceptible node with a degree of k.

Immunization strategy: some time after operation of network virus, inevitably corresponding human measures will be taken to search and kill the virus to prevent its propagation. In this case, some nodes will become immune after repeated infections and cures, and immunization will prevent virus propagation, but virus propagation will have impact on immunization effect in return.

Immunization delay: implementation of immunization strategy has certain delay to outbreak of virus, and this delay is named as immunization delay, and represented with T_{delay} .

5. Propagation Process of Malicious Program and Algorithm Design of Improved Model

Propagation rate is used to measure the propagation process from the view of virus propagating source, while infection rate is used to measure the propagation process from the view of propagating objective of malicious programs; infection rate is not only related with propagation rate, but also impacted by node degree. In researches on propagation of malicious programs, usually propagation process from infected nodes to other nodes is divided into 4 stages: information collection, scanning & probing, attach and penetrating and self-evolution.

With continuous evolution of the network, malicious programs will ceaselessly spread, and the propagation process of a malicious program during dynamic evolution of Ad Hoc network is as shown in Fig. 6. Assuming that when the unit time t=1, No. 1 node is in infected status (represented with black circles), and the other nodes are in susceptible status (represented with hollow circles). When t=2, susceptible nodes No.2, 3 and 4 are infected by their neighbor node No. 1 and become infected nodes. When t=3, a new susceptible node, No. 9, selects to connect to No. 1 node with high degree, meanwhile No. 9 node has a certain probability to get infected by No. 1 node. When t=4, the infected No.1 node becomes immune node after measurements of researching and killing malicious programs.

In networks with different topological structures, due to differences in scanning means and other techniques applied in propagation of malicious programs, infection rate and propagation cycle also differ. However, from the view of entire network, characteristics of behaviors that malicious programs attack and penetrate into networks are very similar; objective of research on propagation model of malicious model is just to research the propagation rules of malicious programs in networks. Thus, in order to eliminate the impact of technical details on propagation rules of malicious programs, technical details such as link bandwidth among different nodes and infection rate of different malicious programs to a node are not taken into account, and only the basic common characteristics of malicious programs in propagation process are extracted for research.

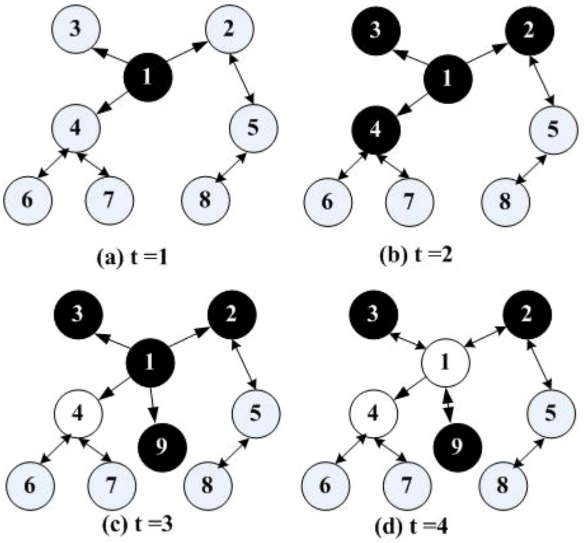

Fig. 5. Propagation process of virus.

According to the propagation process of malicious program in dynamic network as shown in Fig. 5, it can be seen that propagation of malicious program is equivalent to an infinite loop, and the terminal condition is that all the infected nodes in the network are cured after taking immunization strategies. The algorithm design is as follows:

Algorithm 1: Improved Algorithm of Malicious Program Propagation in Ad Hoc Model

```
{
scanf (Infected nodes set I; Susceptible nodes set S; Incubation boundary Set E; Propagation rate $\beta$);
printf (end mark or null);
times=0;
/*Starting from initial unit time*/
n=1;
 /*Starting from No. 1 node, n∈I*/
While(I!=NULL)
/*Infected nodes exist in the network*/
{
if (n is an infected node)
Find all neighbor nodes of Node n;
/*can be determined according to adjacent matrix*/
Node n propagates malicious program to each neighbor node at infection rate of β, if a neighbor node is not immune, its status will become infected node.
Immunization strategy is taken to infected nodes;
  else
BFS（n）;
 /*depth-first search of other infected nodes in the network */
Times++;
/*enter propagation of next unit time*/
}
/* endwhile */
}
```

Assuming the researched Ad Hoc wireless network is a stochastic network with a small fluctuation range, and degree of each node is almost the same. $\overline{K}$ is used to represent the average degree of any node with degree of k, so K=$\overline{K}$, and the infection rate of a susceptible node with degree of k is λ_k=|1-(1-i)^K | β, since nodes in Ad Hoc network have the same characteristics, the average infection rate λ_k of a susceptible node with degree of k can also be approximately equal to λ_k . Therefore, according to differential equations of SIR propagation model, propagation model equations of malicious program in Ad Hoc network can be deduced ad follows:

Equation (4, 5) (No immunization propagation stage) is:

$$\frac{ds}{dt}=-\overline{\lambda}s,\frac{di}{dt}=\lambda s,\frac{dr}{dt}=0 \quad (4)$$

$$\frac{ds}{dt}=-\overline{\lambda}s-\gamma s,\frac{di}{dt}=\lambda s-\gamma i,\frac{dr}{dt}=\gamma(s+i) \quad (5)$$

From Equation 1 and 2, threshold value of virus outbreak in propagation process of malicious program does not exist, which indicates that if no human immunological control measures are taken in Ad Hoc networks, malicious programs will always propagate. λ_k =|1-(1-i) ^{K} | β is substituted into Equation 4 and 5, $\frac{di}{dt}=(s-s^{\overline{k}+1})\beta$ can be obtained through deduction, i.e. propagation velocity of malicious programs in the network is an increasing function to node average degree $\overline{K}$, i.e. the closer the connection is between nodes, the faster the propagation of malicious program will be in the network.

6. Dynamic Immunization Strategy

As plenty of outbreaks of infectious diseases or computer viruses have significantly impacted human life in history, immunization strategies are brought by researchers to avoid or relive such damages. For scale-free networks, as the spread threshold is zero, virus could quickly spread and reach steady state if only virus have positive spread probability, which implying the fragility of scale-free networks. Studies of recent years discovered that most real network topologies own a scale free feature. But in the real world, most real networks exhibit scale-free, thus, finding a better immune strategy becomes particularly important for a network.

The network virus invasion within a short period of time will make the wireless Ad hoc network that faces the danger of paralysis, so how to effectively deal with the virus attacks, thereby protecting the key node to complete the basic perceptual tasks which is the serious challenge faced by the network. Immunity is an important method to control the network virus propagation, node once is immured, and means to connect edges are removed, so it can reduce the transmission of the virus. At present, people discuss more immune strategy including stochastic immunization, target immunity and acquaintance immunization. Infection node in wireless Ad hoc network acquired immunity by immunization strategy, the new network will be generated after feedback immunization.

Suppose a network G= (V, E), the number of nodes is nodesum in network, while the number of edges is edgesum. Among of them: V=$v_1v_2v_3v_{nodesum}$, E=$e_1e_2e_3e_{edgesum}$. In each step of the iterative process, node calculation in equation 6.

$$node(i)^{value}=oldnode(i)+\sum_{j=1}^{nodesum}a_{ij}*oldnodeV(j) \quad (6)$$

Because of the importance of nodes in a dynamic network is the mutual influence and change, the importance of network will not only influence its neighbor nodes, but also is influenced by the importance of neighbor node. Each of node influence is an iteration process, when the network after finite iterations, the importance of nodes in the network will not change, so the network is also considered to reach steady state. Dynamic immune strategy algorithm is described as follows.

```
Algorithm 2: DYNAMIC immunization strategy
{
Input: A network topology, the number of columns of A is 2, the number of rows is the number of edges in a network, each column corresponds to A
```

network of connected edges, nodes number nodesum and the number of edges edgesum, the number of immune nodes for m;

```
    Step 1:D=ones (1, nodesum);
    / * record the state of each node, and is initialized to 1, B=A; new network B for each generated after immunization, the initialization of A*/;
    Step 2:for i=1 to M
    2.1: the importance of computing nodes in B network value;
    2.2: immune importance value node J maximum, D (J) =3;
    2.3: remove all edges connected to this j node, the new network B formed the next immunity;
    Endfor;
    Step 3: returns an array of D[l... Nodesum];
    }
```

7. Analysis of Simulation Experiment

As the concept of immunization delay is introduced in the improved propagation model of malicious program, the improved propagation model divide propagation process into 2 stages: non-immunization stage and immunization stage. Non-immunization stage starts at the initial unit moment, since there is no immunization in the network in this process, malicious programs can arbitrarily propagate; in each init time, infected node infects neighbor nodes at the propagation rate of β, and susceptible nodes become infected nodes with probability of λ_k. Immunization stage starts at the moment once an immune node emerges in the network, and in each unit time, susceptible nodes become infected nodes at rate of λ_k or become immune nodes at rate of γ, infected nodes also become immune nodes at rate of γ. As deduced in the above equations, infection rate of nodes in the network is closely related to degrees of nodes. Taking Ad Hoc network as the research object, a simulation experiment is conducted to verify the above deduction.

For better illustration of impact of the improved model on performance of malicious programs propagation, a simulation experiment is conducted in MATLAB with the purpose of verifying that if algorithm analysis of the improved model is in line with the deduction of above equations. Setting of basic parameters is shown as Table 1, and simulative results acquired by modifying values of the infection rate β is shown in Fig. 6.

In Fig. 6, r indicates the ratio of number of infected nodes/total number of nodes; t is the unit time, simulation results show that the probability of a node with higher degree getting infected from an infected node is higher than a node with lower degree, so propagation time of malicious programs in the network is short; and once the virus breaks out, they immediately gather together and spread fast. Certainly, immunization strategies can be taken to eliminate the malicious programs detected in the network, while if partition of the network is not before the malicious programs propagate to nodes with high degree, immunization strategies would become invalid.

Table 1. Experiment parameter setting.

Parameter	Setting value	Meaning
N	5000	Number of nodes
I	10	Infected nodes
E	0	Boundary set
S	4000	Susceptible nodes
α	0.75	Infection rate
γ	0.6	Immunization rate

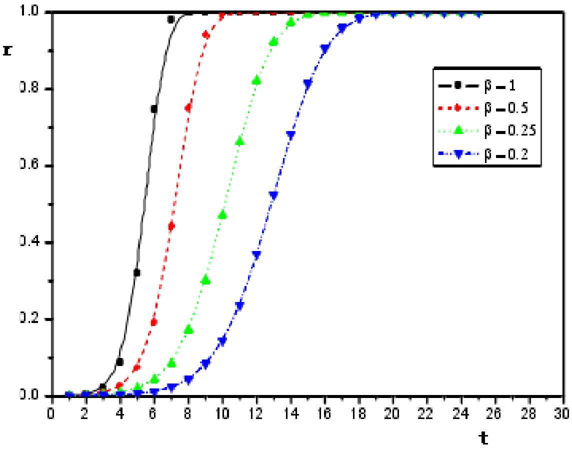

Fig. 6. Results of simulation experiment.

In addition, in order to simulation the immune strategy, the difference of infected network compare the modified model to the original SEIR propagation model, hypothesis γ_k =0.06, β =0.5, γ =0.3, after adopted the dynamic of immunization strategy, the number of infected nodes I in network with time curve are shown in Fig. 7.

Here as can be seen, in the t=22 step before, after used dynamic immunization strategy the outbreak rate than unused immunization strategy the outbreak of the virus slightly faster, but when the time step number t>22, the use of dynamic immunization strategy after the outbreak of the virus becomes slow, the number of nodes in network eventually infected for 2489; no immune strategy the network continued to grow after t=23, until t=36, to slow down, almost reached the steady state, the number of nodes in the network eventually infected for 3021, than the use of dynamic immune strategy infected nearly 530 node.

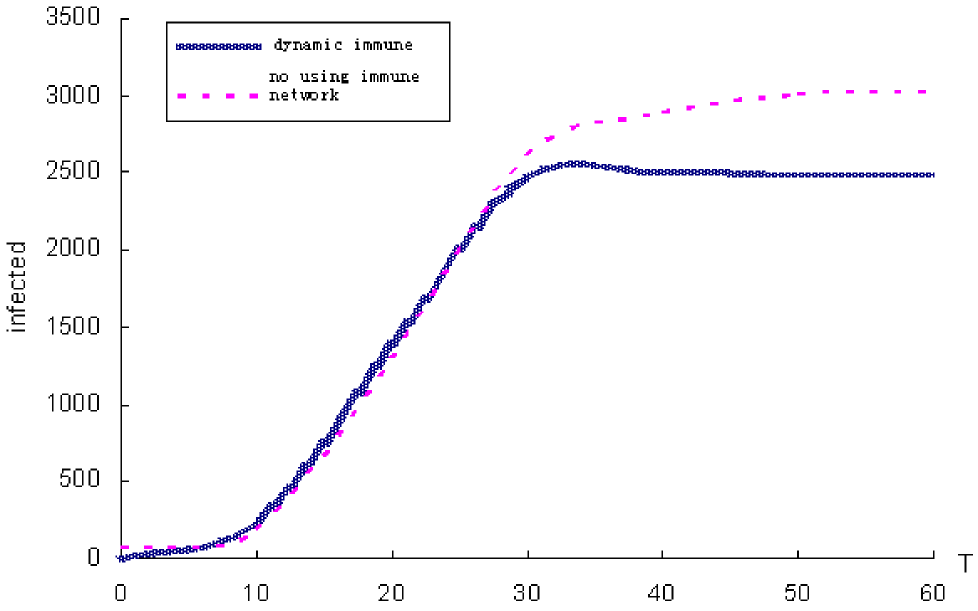

Fig. 7. Dynamic immune strategy used before and after compared chart.

8. Conclusions

Ad Hoc network is an innovative mobile computer network, which not only can independently operate, but also can be taken as a supplementary of current networks with a fixed infrastructure. Its own uniqueness gives it a promising development. In addition, numerous problems demanding prompt solution also lie in research on Ad Hoc networks that include design of routing protocol with energy conservation strategy, security assurance, multicast functions, Quality of service (QOS), other extended characters, and management of Ad Hoc network, etc.

Based on the problem that infection rate of malicious programs predicted that the traditional models are lower than the actual value in the practical application, this paper conducts an improvement to the propagation model of malicious programs through the introduction of concepts for network topological characteristics and immunization. Also, an improved algorithm is designed with the combination of a dynamic evolution of network topology and propagation process of malicious programs. According to the experiment, the improved model has favorable effects on restraining propagation of malicious programs. Therefore, research on propagation mechanism of malicious program in the wireless environment and the improvement of epidemic models have significant promotion force for control of malicious programs in networks.

Acknowledgements

This work is partially supported by National Natural Science Foundation of China under grant (No. 61103245) and Hengyang Science &Pan Project (No. 2009KG55).

References

[1]. Qing Sihan, Weng Weiping, Jiang Jianchun, et al., A new worm warning method based on web-like interrelations, *Journal of Communications*, Vol. 25, No. 7, 2004, pp. 62-70.

[2]. Wen Weiping, Qing Sihan, et al., Worm research and development, *Journal of Software*, Vol. 15, No. 8, 2004, pp. 1208-1219.

[3]. Manju Jose, S. K. Srivatsa, Performance evaluation and comparison of facsimile transmission in IP and PSTN networks, in *Proceedings of the International Conference on Software and Computer Applications (ICSCA' 12)*, 2012.

[4]. Chen Bo, Fang Bingxing, Yun Xiaochun, Research on methods of distributed worm detection and restrain, *Journal of Communications*, Vol. 28, No. 2, 2007, pp. 9-16.

[5]. C. Bettstetter, Giovanni Resta, Paolo Santi, The node distribution of the random waypoint mobility mobility for wireless ad hoc networks, *IEEE Transactions on Mobile Computing*, Vol. 2, No. 3, 2003, pp. 257-269.

[6]. Yingqiang Ding, Gangtao Han, Xiaomin Mu, A distributed localization algorithm for wireless sensor network based on the two-hop connection relationship, *New trend in Innovations in Information Technology*, Vol. 7, No. 7, 2010, pp. 1657-1663.

[7]. M. Y. Liu, W. B. Li and X. Pei, Convex optimization algorithms for cooperative localization vehicles, *Acta Automatica Sinica*, Vol. 36, No. 5, 2010, pp. 704-710.

[8]. Q. Zhou, H. S. Zhu and Y. J. Xu, Smallest enclosing circle based localization approach for wireless sensor networks, *Journal on Communications*, Vol. 29, No. 11, 2008, pp. 84-90.

[9]. J. P. Sheu, P. C. Chen and C. S. Hsu, A distributed localization scheme for wireless sensor networks with improved grid-scan and vector-based refinement, *IEEE Transactions on Mobile Computing*, Vol. 7, No. 9, 2008, pp. 1110-1123.

[10]. Thomas Ciza, N. Balakrishnan, Performance enhancement of intrusion detection systems using advances in sensor fusion, in *Proceedings of the 11th International Conference on Information Fusion*, 30 June 2008, pp. 1-7.

[11]. Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou, Francois Spies, A global security architecture for intrusion detection on computer networks, *Computers & Security*, Vol. 27, Issue 1, 2008, pp. 30-47.

[12]. Vasilios Katos, Network intrusion detection: Evaluating cluster, discriminant, and logit analysis, *Information Sciences*, Vol. 177, No. 15, 2007, pp. 3060-3073.

[13]. Agustín Orfila, Javier Carbó, Arturo Ribagorda, Autonomous decision on intrusion detection with trained BDI agents, *Computer Communications*, Vol. 9, No. 31, 2008, pp. 1803-1813.

[14]. Vincent Toubiana, Houda Labiod, Laurent Reynaud, Yvon Gourhant, A global security architecture for operated hybrid WLAN mesh networks, *Computer Networks*, Vol. 54, Issue 2, 2010, pp. 218-230.

[15]. Jin Yang, Tang Liu, Ling Xi Peng, Xue Jun Li, Gang Luo, Multilevel network security monitoring and evaluation model, *Journal of software*, Vol. 6, No. 5, 2011, pp. 798-805.