ISSN : 0974 - 7435 Volume 10 Issue 13

2014

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(13), 2014 [7416-7421]

Study of computer virus propagation models in networks based on the stability and control

Hongxia Chen[1], Yongkang Huang[2]
[1]Guangxi Industrial Vocational and Technical university, Nanning Guangxi 530001, (CHINA)
[2]Guangxi Institute of Chinese Academy of Science and Technology Development, Nanning Guangxi 530022, (CHINA)

ABSTRACT

This paper mainly studies computer virus propagation models in networks based on the stability and control. The method of this study is through the learning of computer virus emergence, infection and transmission characteristics from the essence to proceed with further discussion and exploration. Then from the perspective of the stability and control, qualitative analysis is carried out and corresponding coping strategies are put forward to deal with the current three common types of the infection and spread of computer viruses in networks. Through the theoretical knowledge and the study of infection and transmission correlation mechanism about network virus control in different types of networks, two kinds of computer virus infection and spread models are built. The first is SIS Model, and the second is SIR Model. Then the two models will be deeply analyzed and explored through building mathematical models, and the two kinds of computer virus infection and spread models are compared and analyzed scientifically based on in-depth analysis. And that is very important for coping with computer virus control popular in network at present.

KEYWORDS

Computer viruses; Propagation models; Qualitative analysis.

INTRODUCTION

Nowadays with the constantly upgrading and rapid development of the information technology, the efficiency and speed of network information transmission has been improved a lot to a certain degree. Information stability and security following has been paid attention to by the network experts and people gradually.

With the continuous development of network technology, computer has gradually entered into people's lives, and the arrival of the information age has brought convenient life for people, so the dependence on the Internet is more and more strong[1-3].

However, as is known to all, the highly developed internet brings people all sorts of convenient life while at the same time with many problems following. The network security problem has gradually become the focus of people's attention. Among the complex problems, the computer virus infection and spread is a very prominent and serious problem. Every year the loss caused by computer virus on the Internet is enormous. What's more the infection and spread of computer viruses in essence endanger the information security of the users directly.

It is well known that work centrality of network information security is the realization of the security transmission of network information data and information privacy, avoiding the network information data changed by some unauthorized entities. The changes may be the steal or modify of the data information.

In the problems of network data transmission and information secrecy, leakage and falsification of information data caused by computer virus is the most common. However, the computer virus problem has not been effectively resolved since the emergence of the computer virus to nowadays. The emergence and invasion of the computer virus destroyed the normal storage, processing and transmission of information, bringing huge economic losses to the people[4].

While with the improvement of electronic components core technology in electronic information industry, the average operating speed of the related computer hardware has qualitatively upgraded. The application of various new technologies makes the internet information start swelling, following by the constantly upgraded of the computer virus. When one kind of computer virus appears, there may be more variants of computer software virus following by. This is an inevitable phenomenon, because computer viruses need to constantly updating themselves to survive[5].

Three are more new variant types of computer virus, so it is difficult to check and kill virus. As for a country, the harmful of the computer virus spreading on the networks of the country is huge. At the level of national- security, its harm is not less than the military weapons. Considering the overall safety level of national political, economic, cultural development, it is necessary to carry out this study, and this study is also very urgent need.

THE RESEARCH STATUS OF COMPUTER VIRUS PROPAGATION MODELS IN NETWORKS BASED ON THE STABILITY AND CONTROL

The concepts and theories related to computer virus. About twenty years ago, in the article of theory and experiment of computer virus, the virus is defined as a type of program, and through modifying the other application, the program can release a suitable copy into the other program, and this method is called infection. And with the characteristics of infection, the virus takes advantage of the user rights to infect their programs in the computer system or the networks. Moreover each infected program also becomes the virus program and this kind of process is constantly going on.

The early virus theory mainly studies the definition and infectious way of the virus program, based on the Turing machine model and recursive function model, and etc. The model mainly describes infection form of the file virus through the state transitions of the Turing machine or the form of recursive function. Kannan and other people study the worm propagation model based on random scan and point out that the worms have active aggression and strong ability of infection. Meanwhile the strategy of firewall collaboration is proposed. That is P2P worm propagation model in the peer-to-peer network.

THE THEORIES RELATED TO COMPUTER VIRUS

The computer virus made by the programmer is constantly changing, so there are various species, of which the characteristics are different. However, the traditional computer virus mainly includes general characteristics such as operability, infectivity, non-authorization, concealment, destructibility and so on. Meanwhile with the development of computer technology and antiviral technology, new characteristics appears such as anti-analyticity, decoy, multiple transmission, deformability, the remote control feature, target diversification, comprehensive attack means and etc. A more effective method coping with virus and solution can be found, only widely understanding the characteristics and development trend of computer virus[6].

The infectivity of computer virus

The infectivity of computer virus is one of the basic features of computer virus. It is well known that the computer virus is essentially a program made by people. But unlike most of the normal computer programs, once the program enters into the computer system and gets the CPU execution, it will seek for the suitable program or storage medium without user knowing according to the predetermined manner of programmer. After determining the suitable object, the program inserts its virus code to replicate and spread. The types of the infected files that predefined by the programmer and the way of searching the suitable infected object provide reference for programmers who look for and determine the virus programs, and also provide a basis for predicting the spread characteristics and speed of the virus. That is the infectivity of the computer virus[7].

The non-authorization of computer virus

The non-authorization of computer virus is a very prominent characteristic of computer virus. Generally speaking, computer viral program hidden in the normal program gets control power of the computer system actually without the users knowing, when the normal program of a user is infected. And for the computer user, the purpose of the virus program and the relevant activities are not allowed and unknown. And the result can not be predicted, either. From the perspective of computer system, all the operations performed by the virus program are not allowed by the user and is non-authorization.

CONTROL STRATEGY OF COMPUTER VIRUS PROPAGATION IN NETWORKS BASED ON THE STABILITY

In fact, the factors involved in the computer virus control based on the stability are extensive, with both the types of networks and evolution speed of the computer virus variants referring to. The variants and evolution of computer virus has no rules, or in other words not stable enough and uncontrollability, so from the perspective of the relative stability, the study of network computer virus control is carried out just from different network types. This paper adopts virus control methods in the following three types to conduct the qualitative study[8].

VLAN virus control

The inflection and spread of computer virus in the VLAN shows a very strong character, in general it is fast speed of inflection and strong ability of transmission. Once one node has been inflected, data of this node will have problem featuring overwrite file. Sometimes one computer is inflected by some type of virus, when using the VLAN network, and file system of the computer connected with this network will have many suffix called exe file. As we all know, the executable exe file is the common file name of the computer virus. Once the problem appears, any data read operation of the computer cannot be carried out, or the virus will spread indefinitely until the file system is completely annexed and covered and into endless loop, causing system crash and the loss of data. The only operation in this case we can do is completely storage formatting, in this way these executable files can be cleared off the storage. From this point of view, the disposing of computer virus is difficult, involving a systemic operation. As for the control of computer virus in VLAN networks, some suggestions are given to prevent the loss of VLAN from computer virus or to minimize the loss[9].

The first is to guarantee the security of terminal computer security in VLAN network. Some common anti-virus software or computer security management software are installed including security guards run by 360 safe, Kaspersky anti-virus software and other antivirus software abroad. The virus data need to update regularly after installing to ensure the security software the ability of killing computer virus program. Secondly, the user of VLAN network shall regulate their habits of using internet, visiting no toxic site, and the cheating program shall not be connected, either. Thirdly, some important files of ours shall be saved by data remote and made a backup, or be sent to a remote mail server to temporarily store the important file or stored in the hard disk. Finally, to the individual or the unit that has better condition, some efficient and safe network management software platform can be used. As for some rich unit, internal VLAN network composed by security hardware systems can be established, and a computer virus checking mechanism is installed in the gateway to monitor the possible virus. Once any computer viruses are found in the networks, some effective measures will be adopted to deal with them, reducing the loss to the minimum.

WLAN virus control

The computer virus control in WLAN network is based on the VLAN network. In order to avoid the computer virus inflection in WLAN networks, the first thing to do is protect the computers in the VLAN from inflecting by the virus. This is a premise, and how to guarantee the WLAN network computer without intrusion of computer viruses is another important work needed in this study. Generally speaking, according to the feedback virus database figure of the security management software in VLAN networks, virus database in WLAN network is established, and any virus involved in the database can be checked and killed through security antivirus software. The new virus variants shall be recorded and wrote to the database, too. The methods of computer virus control in WLAN networks include the following points: Firstly, as for the WLAN networks, antivirus software or safety management software are installed in the terminal system of all the computers, for the purpose of checking and killing the virus. And the information of the computer virus is also recorded to give feedback to the computer virus database, preventing the similar virus from invading the computer system. Secondly, effective control measures of the computer virus are carried out on the borders of WLAN network interchange. To be specific speaking, some security hardware equipments are installed to improve security protection capability of WALN network[10].

MAIL virus control

With the development of the communications, mail has become an effective way to spread information. However, email virus starts to influence the network security. So measures shall be adopted to resolve the problems. For some large enterprises, the office automation system is used, and in which the mail server is its composition. In this case, defensive and monitoring measures are employed in mail server to automatically intercept and kill the email containing the virus and sent the processed email to the user. As for the users who do not belong to the office automation system, the computer security software must be started to process the virus when opening some unknown email.

STUDY OF COMPUTER VIRUS PROPAGATION MODELS IN NETWORKS BASED ON THE STABILITY AND CONTROL

There are various computer virus propagation models, several typical computer viruses propagation models are mainly introduced here.

SIS Model

Model Establishment

SIS Model is also called Susceptible-Infected-Susceptible. As for this model, the node of the internet is usually divided into two basic states. One is susceptible state and the other is infected state. The picture below gives the abbreviation of the two states, one is S and the other is T. Under some given condition, S can be transformed into T, and the processing is reversible. That is to say, susceptible state can be transformed into infected state under a certain condition. Therefore the infected state can be suppressed into susceptible state, under the condition of response timely and relatively scientific computer technology is employed. However this is not definitely thing. The relatively scientific and rational computer technology is mainly referring to the using of antivirus software or virus avoidance measures. The SIS model is shown as Figure 1.

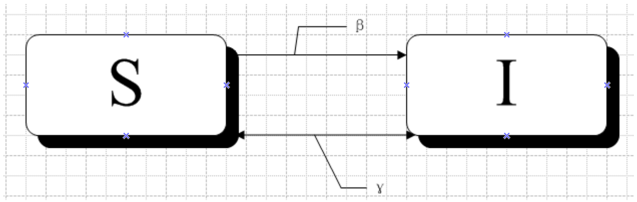

Figure 1 : SIS model

Differential equation of mathematical model establishment

From the picture we can see two codes served as condition, one is β and the other is γ. The specific meanings of the codes in the formula are as follows: β represents the probability infected by the virus, and γ represents the probability of virus checking and killing. The mathematical model expressed in the form of differential equation is as follows:

$$\begin{cases} \dfrac{dS}{dt} = -\beta SI + \gamma I \\ \dfrac{dI}{dt} = \beta SI - \gamma I \\ S(0) = N - I_0 \\ (0) = I_0 \end{cases}$$

As for the differential equation above, each letter represents a meaning respectively, and the letter N represents total number of network nodes at a certain time.

The analysis of the results

βSI represents the increasing total number of network nodes in the process of transmission from the susceptible state to the infected state. While γSI represents the increasing total number of network nodes from the infected state to the susceptible state. I_0 stands for the total number of infected nodes in the initial state of the internet. Compared the two model, the latter is injected with a virus immune entity in the node of susceptible state. However the former is without this feature.

SIR Model

The emphasis of this section is SIR model, SIR is short for Susceptible-Infected-Removed. And the design of SIR model is based on SIS model and is just the development of the above model.

Model Establishment

The node of the networks in SIR model is divided into three states, besides the susceptible state（S）and infected state (I) in SIS model, immune state (R)is added. And the node of R state has the ability of antiviral, avoiding the virus infection and the proliferation of the virus. Figure 2 is the virus infection model in SIR model.

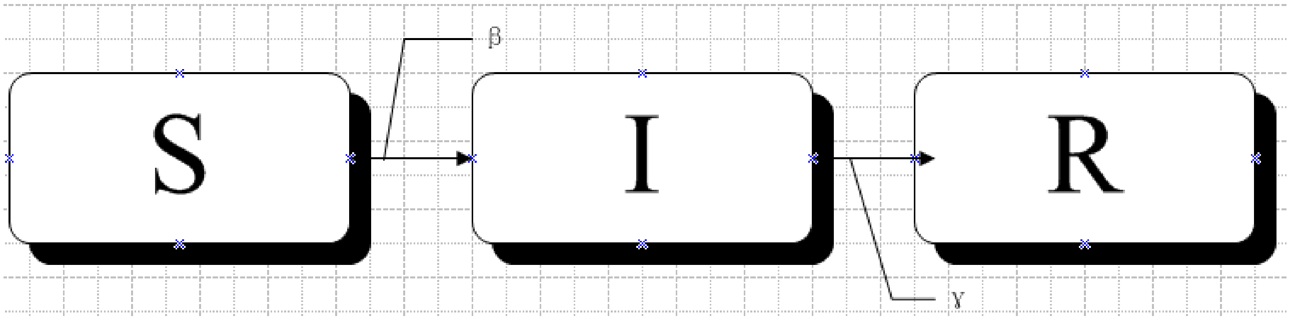

Figure 2 : SIR Model diagram

Differential equation of mathematical model establishment

The meanings of the two parameters including β and γ in the above picture are the same as last chapter. Similarly, the mathematical model expressed in the form of differential equation is as follows:

$$\begin{cases} \dfrac{dS}{dt} = -\beta SI \\ \dfrac{dI}{dt} = \beta SI - \gamma I \\ \dfrac{dR}{dt} = \gamma I \\ S(0) = N - I_0, I(0) = I_0, R(0) = 0 \end{cases}$$

The analysis of the results

From the differential equation and SIR model diagram, we can see that this model has improved a lot in the study of virus propagation and infection depression, controlling the computer virus infection rate of node through operating the value of the β and γ. And some professional antivirus suppression measures have been carried out to control the speed of computer virus in the process and achieved good results.

Comparative analysis of the SIS model and SIR model

This section mainly analyzes the relationship between the SIS model and SIR model. According to the introduction of the last two sections, compare and analyze the two models through the TABLE 1 below.

TABLE 1 : The contrast between the SIS model and SIR model

Model	The prevention and control ability of the virus	The memory of virus	The applied network types
SIS model	Certain ability	No memory function	VLAN WLAN
SIR model	Strong ability	Has memory function	VLAN WLAN MLAN

SEIR model

The third model is SEIR model, and the application of this model in the propagation and control of computer virus is rare, because of the difficulty application of the model in practice. Pictorial diagram is given below and simple analysis is carried out shown as Figure 3.

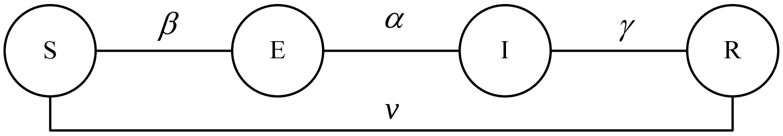

Figure 3 : SEIR model

The picture below is mathematical model of the SEIR model, using differential equation to express.

$$\begin{cases} \dfrac{dS}{dt} = -\beta SI + vI \\ \dfrac{dE}{dt} = \beta SI - \alpha E \\ \dfrac{dI}{dt} = \alpha E - (v+\gamma)I \\ \dfrac{dR}{dt} = \gamma I \\ S(0) = N - I_0, E(0) = 0, I(0) = I_0, R(0) = 0 \\ \end{cases}$$

In this model, the meanings ofβandγremain the same as in picture 1. but two symbols including αandʋare added. αrefers to the probability of transmission from the E state to I state andʋrefers to the probability of transmission from the infected state to susceptible state.

CONCLUSIONS

At present, the fast development of China internet provides convenient life for people. But at the same time, there are also many problems followed by. The problem of network security has become the focus of people’s attention on the internet. In the various network problems, the infection and propagation of computer virus is a very outstanding issue needed to be solved sonly. It is well known that the loss brought by computer virus is great. And the infection and propagation of computer virus directly endangered the information security of the internet users from the essence. This study mainly learns the emergence, infection and transmission characteristics of computer virus from the essence to proceed with further discussion and exploration. And the infection and propagation of the computer virus is proposed. Then from the perspective of the stability and control, qualitative analysis is carried out and corresponding coping strategies are put forward to deal with the current three common types of the infection and spread of computer viruses in networks. From this study we can see clearly that China shall strengthen the research of the computer virus model and control measure, and build a full range of virus defense system to ensure the security of network. The internet users shall regulate their own behaviors on the internet and meantime improve the cognitive and discernment ability of computer virus.

REFERENCES

[1] B.Ek?io?lu, A.Nadarajan; Structural Analysis of Conical Carbon Nanofibers, Carbon, **44(2)**, 360-373 **(2006)**.

[2] Y.Saito, T.Arima; Features of Vapor-Grown Cone-Shaped Graphitic Whiskers Deposited in the Cavities of Wood Cells, Carbon, **45(2)**, 248-255 **(2007)**.

[3] Ch.-T. Lin, W.-C. Chen, M.-Y. Yen, L.-S. Wang, C.-Y. Lee, T.-S. Chin, T.-T. Chiu; Cone-Stacked Carbon Nanofibers with Cone Angle Increasing along the Longitudinal Axis, Carbon, **45(2)**, 411-415 **(2007)**.

[4] A.D.Lueking, H.R.Gutierrez, D.A.Fonseca, E.Dickey; Structural Characterization of Exfoliated Graphite Nanofibers, Carbon, **45(4)**, 751-759 **(2007)**.

[5] J.Vera-Agullo, H.Varela-Rizo, J.A.Conesa, A.Cristina, M.César, M.-G. Ignacio; Evidence for Growth Mechanism and Helix-Spiral Cone Structure of Stacked-Cup Carbon Nanofibers, Carbon, **45(14)**, 2751-2758 **(2007)**.

[6] M.H.Al-Saleh, U.Sundararaj; A Review of Vapor Grown Carbon Nanofiber/Polymer Conductive Composites, Carbon, **47(1)**, 2-22 **(2009)**.

[7] C.-W. Huang, H.-C. Wu, W.-H. Lin, Y.-Y. Li; Temperature Effect on the Formation of Catalysts for Growth of Carbon Nanofibers, Carbon, **47(3)**, 795-803 **(2009)**.

[8] J.Zhao, L.Liu, Q.Guo, J.Shi, G.Zhai, J.Song, Z.Liu; Growth of Carbon Nanotubes on the Surface of Carbon Fibers, Carbon, **46(2)**, 380-383 **(2008)**.

[9] L.Zhu, J.Xu, F.Xiao, H.Jiang, D.W.Hess, C.P.Wong; The Growth of Carbon Nanotube Stacks in the Kinetics-Controlled Regime, Carbon, **45(2)**, 344-348 **(2007)**.

[10] Sumio; Helical Microtubules of Graphitic Carbon, Nature, **354(7)**, 56-58 **(1991)**.