Research on Benign Worm Based on a Mixed-mode

WEI Xing[1, a *], QU Jingjing[2,b] YANG Xiaojin[3,c]

[1]Guilin University of Aerospace Technology, GUI Lin, China

[2] Guilin University of Aerospace Technology, GUI Lin, China

[3] Guilin University of Aerospace Technology, GUI Lin, China

[a] wxaiqiqi@126.com, [b] qujingjing@guat.edu.cn, [c] yxj@guat.edu.cn

Keywords: Benign Worm; Vicious Worm; hybrid mechanism

Abstract. Research network worms, through inhibiting propagation of vicious network worms, Improve the utilization rate of network, Analysis of the network worms' propagation model, put forward the mathematical model based on hybrid network benign worms, establish the mathematical model of network communication, thus rapid inhibit vicious network worms, Through the simulation of using cladding software method, results show that the model can effectively improve network quality, reduce network resources consumption rate, and improve the network overall performance.

Introduction

In recent years, with the rapid growth of Internet, a network worm of the threat of computer systems and networks is increasing. In recent years, several large-scale outbreaks of malicious worms after the events, people are really aware of the worm spread the serious impact to the network. Currently, the use of worms to fight the worm idea has become popular, for example, in the network, the benign worm take the initiative to kill malicious worm for host vulnerability, and patched, this can to some extent, effectively removing the spread of worms in the network, To some extent, that can effectively remove the worm's spread, in the network, to a certain extent, For example: In the reference [1], the author researched the definition and distinction between benign worms and malicious worms, reference [2] proposed a new model of worm against worm (Worm-Anti-Worm, WAW) model, reflecting the new features of the benign worm against malicious worms, ,there are certain theoretical value. However, most of the benign and malicious worms use the same diffusion, in the fight against the process; the network will also have a great impact, consume a large amount of network resources. Therefore, we propose detection based on active and passive model of mixed inhibition of malignant benign worms way worms, which can effectively exhaust system of a vicious Internet worm's spread, reduce network resource consumption, and improve network efficiency. We propose benign worms based on active and passive mixed model Inhibition of malignant worms, It can effectively exhaust system of a vicious Internet worm's spread, reduce network resource consumption, improve network efficiency.

The basic model of worm propagation

Worm propagation model is the most common method to study the characteristics of worm propagation, as the worm spread and the spread of biological viruses have similar characteristics in acts of self-replication and dissemination, therefore, the mathematical tools we researched the biological mode of virus transmission, that applied to the computer network model of worm propagation, so now most of the mathematical model of worm propagation model are based on spread of infectious diseases, such as: SI (Susceptible-Infectious) model, in the SI model, each host can have two states: easy to infection status and infection status. Infection hosts is expressed as:

$$dI(t)\big/_{dt} = sI(t)[N - I(t)] \qquad (1)$$

Where: $I(t)$ is the number of infected hosts at the t time, N is the total number of all vulnerable hosts in the network, S is the infection rate of the host. However, this model has some limitations. In this model, the parameter types of selection minimal and could not fully consider the network latency, packet loss and other factors on worm propagation; In addition, with the increase in the number of parameters, the model will increase the complexity to the analysis.

In addition, there are some common worm propagation models, for example: SIS (Susceptible Infectious Susceptible)[3], two-factor (Two-Factor)[4], and WAW (Worm-Anti-Worm)[5]. However, these models there are various problems, SIS model does not consider the worm infected host immune condition, which is difficult reflecting the worm propagation behavior; two-factor model does not consider against network worm propagation under the large-scale network; WAW model is not considered not considered the state after healthy worms into the susceptible host and so on).

Modeling and analysis based on benign worm

The spread of worms based on a benign mechanism is a kind of evil against the Internet worm of evil governance mechanisms, the principle is the release of healthy worms in the network, which can kill a vicious Internet worm and infect host immunity. It can repair and clear host, which was infected by a vicious Internet worm, Immured the host may be infected, in the diffusion process, protect the normal host and network resources by users.

In this study, assuming the network is physically connected, all the host nodes has the vulnerability in the same probability; and will not change over time; network topology is static, it will not affect the spread of Internet worms; in the network, there is only vicious worm A and benign worm B, vicious worm A does not know there are worm B and will not attack them; vicious worm A infected all vulnerable hosts growth over time in the network; The benign worm B patched the vulnerability host, that is Influenced by vicious worm A. and killed vicious worm A, repaired loopholes.

At any time t, in the network, the host status is only one of the easy infection status, infection status, benign infection status and recovery status, and the easy infection status can be conversion into infection status by vicious worm A, also the easy infection status can be conversion into benign infection status by benign worm B, infection status can be conversion into benign infection status by benign worm B, benign infection status can be conversion into recovery status by repaired loopholes.

Assuming the network environment and the host state, the parameters of this model described in Table 1.

Table 1 The parameters defined in the model

parameters	description
$I(t)$	At the t time, the number of host which is infected by vicious worm A in the network
$S(t)$	At the t time, the number of host which is easy to infect by vicious worm A in the network
$R(t)$	At the t time, the number of host which is recovered
$Q(t)$	At the t time, the number of host which is susceptible to vicious worm A and patch holes
$B(t)$	At the t time, the number of host which is infected by benign worm B in the network
$b\mathrm{i}(t)$	At the t time, the rate of vicious worm A infected the hosts in the network
$b\mathrm{b}_{\mathrm{m}}(t)$	At the t time, the hosts is easy to infect by vicious worm A, and the rate of the hosts is infected by benign worm B in the network
$b\mathrm{b}_{\mathrm{n}}(t)$	At the t time, the hosts is infect by vicious worm A, and the rate of the hosts is infected by benign worm B in the network
N	The number of the total hosts in the network

The model of passive detection by benign worm

When benign worm B using passive detection, the principle is that benign worm B is not active to detect the susceptible hosts and infected hosts in the network, which is reached by vicious worms A, once exposed, to benign worm B will be killing the vicious worms A, therefore its propagation model is:

$$\begin{cases} I'(t) = b\,i(t)S(t)I(t) - R'(t) \\ B'(\mathrm{t}) = R'(t) = g\,I(t) + b\,b_n(t)B(t)I(t) \\ S'(t) = -B'(t) - I'(t) \\ b\,i(t) = b\,i_0\left[1 - I(t)/N\right]^h \\ N = I(t) + S(t) + B(t) \end{cases}$$

(2)

Hybrid detection model of benign worm

In the early actual network, when the benign Worm B and vicious A worm into the network simultaneously, they are using the same detection mechanism, therefore, detection of the host is chosen randomly, and its spread is fast, relatively simple, but because two worms are transmitted in the network, the result is that the consumption of network resources is greater, increase the network burden. if uses passive detection mechanism in the network, then benign worm B will not be active to find vicious worm A, while lowering the consumption of network resources, but its spread is slow, not rapid response of vicious worm. In summary, active detection mechanism and passive detection mechanisms have their own advantages and disadvantages, so we combine the advantages of both, hybrid detection mechanisms in the network, in the early network, benign worm B uses active detection mechanism; increase over time, benign Worm B use passive detection mechanism, at this time, the propagation model such as the expression (1), benign worm B gradually removes vicious worm A, and repairs loopholes.

Simulation and analysis of experiments

In order to analysis the propagation law of benign worm, the simulation experiment in the network, We use the simulation software of MATLAB to proves the three detection mechanism respectively, got the malicious worms spread curve over time, as shown in figure 1,this paper analysis the simulation results in detail, proved the practicability and validity of hybrid detection mechanism.

In this simulation, we take the node number of hosts: N=1000000, $b\,b_0 = 8\times10^{-7}$, $b\,b_{00} = 1.6\times10^{-6}$, $b\,i_0 = 8\times10^{-7}$, $g = 0.05$, $m = 6\times10^{-8}$, $h = 3$, the time difference of benign worm B and vicious worm A appears is 20. Simulation results show that vicious worm propagation curve, the number of the different detecting mechanisms by vicious worm compared in Figure. 1.

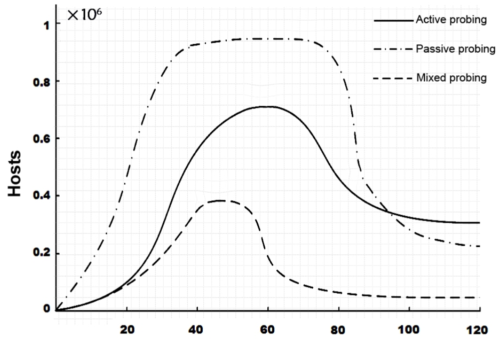

Figure 1. The change number of vicious worm use different detection mechanism in plans

By Figure.1, we can see the benign worm B that use hybrid detection mechanism can effectively inhibit the spread of vicious worm A in the network, the spread of vicious worms A is smaller peak, and shorter duration, reduce the network resources consumption, improve network utilization and network performance. Therefore, the model is feasible and reliable in practice.

In addition, through analysis of Figure 1, we can know the network, when using active detection mechanism, the benign worm B will take the initiative to detect vicious worms A at the beginning time, over the time, the number of benign worm B is gradually increasing, worm A has grow in a short time, finally reached the peak, then gradually reduced, the curve is relatively stable; when using passive detection mechanism, at the early time, vicious worm A is faster growth, peaked after a period of time, and for a long time at a high value of the state, and the number of benign worm B is less in a short time, over the time, the number of benign worm B is gradually increasing, the number of vicious worm A is gradually decreasing, but use mixed-detection mechanisms, vicious worm A small increase in the early, peak in a short time, then is killed quickly by benign worm B, and finally reached the lowest value, consumes less network resources, the result show that in practice, hybrid detection mechanisms is better than active detection mechanism and passive detection mechanisms, that can reduce the number of vicious worm A, it is more practical.

Summary

For internet worm takes up a large amount of network bandwidth, this is a series of problems, for example reduce the resource utilization and so on, this paper proposes a benign worm with mixing mechanism, mathematical model and detection mechanism is analyses, finally, through the network simulation experiment compared the three kinds of mechanisms about active detection, passive detection, mixed detection, the results show that the proposed mixed mechanism is feasible, and more effective compared with other two kinds of mechanism, in the actual network applications, this model can solve a series of problems, for example the benign worms against malignant worms, reducing the consumption of the network resources, improve the network utilization. But how, in the different network application environment, improve the efficiency of benign worm against malignant worms, and the network effect of benign worms spread itself, will discuss in the future research work.

Acknowledgment

Thanks to Guangxi Natural Science Funds(No.2014GXNSFBA118286), and The Department of education scientific research project of Guangxi(No.YB2014433),(No.YB2014431),and The funding achievement of the project of outstanding young and middle-aged excellent teachers' training in high er education institutions of Guangxi.

References

[1] Wang Bailing & Fang Bingxing & Yun Xiaochun; The Propagation Model and Analysis of Worms Together with Anti-worms [J]; WSEAS Transactions on Information Science and Applications, vol.4, 2004, pp.967-982.

[2] Wen Weiping & Qing Si-Han & Jiang Jianchun and so on; Research and Development of Internet worms [J]; Software, vol.15, 2004,pp.1208-1219.

[3] Wang.Y & Wang.CX; Modeling the effects of timing parameters on virus propagation.In; Staniford S, ed.Proc. of the ACM CCS Workshop on Rapid Malcode(WORM 2003); Washington,2003.

[4] Zou CC & Gong W & Towsley D; Code Red worm propagation modeling and analysis.In; Proc.of the 9th ACM Symp.on Computer and Communication Security; Washington, 2002,pp.138-147.

[5] Wang Xiaorong & Wu Tiejun; Flow shop scheduling problems ant colony optimization method [J]; Systems Engineering Theory and Practice, vol. 5, 2003, pp.65–71.