Effects of Dynamic Quarantine and Nonlinear Infection Rate in a Model for Computer Worms Propagation

Carla M.A. Pinto

*School of Engineering, Polytechnic of Porto,
and Centre for Mathematics, University of Porto,
Rua Dr António Bernardino de Almeida, 431, 4200-072 Porto, Portugal
cap@isep.ipp.pt*

Abstract. We propose a new model for computer worms propagation, using dynamic quarantine and a nonlinear infection rate. The dynamic quarantine is based in epidemic disease control methods and in the principle ‘assume guilty before proven innocent’. This means that the host is blocked whenever its behavior looks suspicious. After a short time, the quarantined computer is released. The nonlinear infection rate is used to capture the dynamics of overcrowded infectious networks and high viral loads. We simulate numerically the model for distinct values of the quarantine times. We observe that increasing the quarantine time decreases the number of infectious hosts in the network.

Keywords: computer worms, nonlinear infection rate, dynamic quarantine

PACS: 00,80

INTRODUCTION

Computer worms propagation has been a major research topic for a considerably large number of researchers, in the last few decades. The extraordinary increase in the number of internet users, with the consequential increase in the number of internet communications, provided a good environment for worms to spread. The propagation of worms is highly damaging, translating in losses of millions of dollars and disrupted productivity [7].

The characteristics of computer worms transmission, in particular their resemblance with infectious diseases propagation, suggested the application of mathematical models for epidemics, to investigate the spreading of worms. Throughout the years, several compartmental models have been applied in this study, namely SI (Susceptible-Infectious), SIR (Susceptible-Infectious-Recovered), SEIR (Susceptible-Exposed-Infectious-Recovered), SIQV (Susceptible-Infectious-Quarantine-Vaccinated), SLB (Susceptible-Latent-Breaking), amongst others [4, 8, 11, 10].

The majority of mathematical models for worm propagation, considers constant quarantine [13, 8]. Nevertheless, this type of quarantine is inefficient, due to the high values of the rate at which new hosts entering the network are patched. Dynamic quarantine methods, based on the principle ‘assume guilty before proven innocent’ have been proposed to mitigate this problem [14, 9, 12]. This dynamic quarantine method diminishes the negative effect of false alarms, produced by worm anomaly detection systems. A host is quarantined whenever he has a suspicious behavior, and after some time he is released from quarantine. Once a host is quarantined, security assistants should inspect it as soon as possible. False quarantined hosts won’t be blocked for a long period, since quarantine is released after some time. This dynamic quarantine method can be built on any worm anomaly detection systems. Other quarantine measures, such as pulse quarantine, have been proposed recently in the literature, due to optimistic results from epidemic models using pulse vaccination [11]. Pulse vaccination allows systems to stabilize at disease-free equilibrium faster than constant vaccination. Pulse vaccination will be the focus of future work.

The incidence rate is extremely important in the modeling of disease dynamics. Usually this incidence rate is a function of the numbers of susceptible and infectious individuals. Nevertheless, these incidence rates are ineffective in the cases of overcrowded infectives and high viral loads. Moreover, the topology of the underlying network may also affect the worm’s spread, suggesting nonlinear infection rates [3, 5, 2]. In this work, we consider nonlinear incidence rates of the form $\beta \frac{IS}{1+I}$ [1], where βI measures the infection force of the disease and $1/(1+I)$ models the inhibition of susceptible nodes due to rising viral prevalences.

Bearing these ideas in mind, the paper is structured as follows. In Section ‘THE MODEL’, we describe the model for worm propagation with pulse quarantine and nonlinear incidence rates. In Section ‘NUMERICAL SIMULATIONS’, we present numerical simulations of the model for distinct values of the quarantine time. Finally, in Section ‘CON-

TABLE 1. Parameter values used in the simulations of model (1).

Parameter	Value
p	0.2
ϕ	0.5
β	0.1
μ	0.00001
ω	0.00000006
λ_1	0.2
λ_2	0.00002315
T	10
γ	0.004

CLUSIONS', we state the main conclusions of this work and sketch future resaerch directions.

THE MODEL

The computers are denoted by nodes and can be at one of four possible states: susceptible (S), infectious (I), recovered (R), and quarantined (Q). The transitions between states are modelled by the following system of ordinary differential equations:

$$\begin{aligned}
 \frac{dS}{dt} &= p\mu - f(I, S) - (\mu + \omega + q_2)S \\
 \frac{dI}{dt} &= f(I, S) - (q_1 + \mu + \gamma)I \\
 \frac{dR}{dt} &= (1 - p)\mu + \gamma I + \phi Q + \omega S - \mu R \\
 \frac{dQ}{dt} &= q_2 S + q_1 I - (\phi + \mu)Q
 \end{aligned} \tag{1}$$

where $f(I, S) = \frac{0.01I}{1+I} S$.

The susceptible computers join the network at a rate μ , $1 - p$ of which is patched and move to the recovered state, R . All computers 'die' at a rate μ . The total number of hosts in this network is unchanged, since 'death' and 'birth' rates are the same.

Susceptible hosts, S , with security vulnerabilities, are infected by worms at a rate $f(I, S)$, and move to the infectious class, I , or are directly patched, at a rate ω , and move to the recovered class, R . Infectious hosts may be manually patched at a rate γ and move to class R . Both susceptible, S , and infectious, I , computers can be detected by the misuse detection system and then constantly quarantined at rates q_2 and q_1 , respectively. These rates are given by:

$$q_1 = \frac{\lambda_1 T}{1 + (\lambda_1 + \psi)T}, \quad q_2 = \frac{\lambda_2 T}{1 + \lambda_2 T} \tag{2}$$

where parameters λ_1 and λ_2 describe, respectively, the quarantine probability of infected hosts and susceptible hosts, which are related to the intrusion detection system. We consider $\lambda_1 > \lambda_2$, since the effect of false positives concerning susceptible hosts has to be reduced. The computers at the quarantined state, Q , are vaccinated against worms, by repairing and then patching, at rate ϕ .

The dynamic quarantine strategy applied here has two advantages. The first one deals with false positives. A false positive quarantined healthy host will be quarantined only for a short time. The second advantage is that higher false alarm rates are more tolerable than with constant quarantine, thus infected hosts may be detected earlier.

NUMERICAL SIMULATIONS

In this section we simulate the model (1) for distinct values of the quarantine time T , and for distinct nonlinear incidence rates. The initial condition is $S(0) = 999990$, $I(0) = 10$, $R(0) = 0$, and $Q(0) = 0$. The parameter values are given in Table 1.

The value of $\lambda_1 = 0.2/sec$, for the quarantine rate of infectious hosts, means that, on average, an infectious host can propagate for more or less $5sec$ before it is detected and quarantined. The quarantine rate of susceptible computers

is set to $\lambda_2 = 0.00002315/sec$, indicating that the worm anomaly detection program will give on average twice false alarms for a healthy host per day.

In Figure 1, we depict the dynamics of the variables of model (1) for $T = 10$.

FIGURE 1. Dynamics of the variables of model (1) for $T = 10$. The model approaches a stable worm-free equilibrium.

Figures 2-3 depict the dynamics of the variables of model (1) for distinct values of T . We observe that as T increases the system approaches faster the worm-free equilibrium. We need to find a commitment between the ‘optimal’ quarantine time and the least amount of time a host should be quarantined in real systems, to reduce the effects of false positives.

FIGURE 2. Dynamics of the variables of model (1) for $T = 10, 20, 40$. The model approaches a stable worm-free equilibrium. Note that as T increases the system approaches faster the worm-free equilibrium.

FIGURE 3. Dynamics of the variables of model (1) for $T = 10, 20, 40$. The model approaches a stable worm-free equilibrium. Note that as T increases the system approaches faster the worm-free equilibrium.

CONCLUSIONS

We study a model for computer worm propagation that includes dynamic quarantine and nonlinear incidence rate. We simulate numerically the model for distinct values of the quarantine time, T . We observe that as T increases, the model approaches asymptotically faster the worm-free equilibrium. Future work will focus on the analysis of the stability of equilibria and the use of other nonlinear incidence rates.

ACKNOWLEDGMENTS

The authors wish to thank Fundação Gulbenkian, through *Prémio Gulbenkian de Apoio à Investigação 2003*, Polytechnic of Porto, through the *PAPRE*, and the European Regional Development Fund through the program COMPETE and the Portuguese Government through the FCT - Fundação para a Ciência e a Tecnologia, under the project PEst-C/MAT/UI0144/2013 for financial support.

REFERENCES

1. V. Capasso, *A generalization of the Kermack-McKendrick deterministic epidemic model*, *Mathematical Biosciences* **42**(1–2) 43–61 (1978).
2. C. Gan, X. Yang, W. Liu, Q. Zhu, X. Zhang, *An epidemic model of computer viruses with vaccination and generalized nonlinear incidence rate*, *Appl. Math. Comput.* **22** 265–274 (2013).
3. H.W. Hethcote, P. van den Driessche, *Some epidemiological models with nonlinear incidence*, *J. Math. Biol.* **29**(3) 271–287 (1991).
4. J.O. Kephart, S.R. White, *Directed-graph epidemiological models of computer viruses*, IEEE Symposium on Security and Privacy 343–359 (1991).
5. T. Li, Z. Guan, Y. Wang, *Bifurcation dynamics of a worm model with nonlinear incidence rates*, Proceedings of the Control and Decision Conference (CCDC), 2011 Chinese, 3326–3328 (2011).
6. W.-m. Liu, H.W. Hethcote, S.A. Levin, *Dynamical behavior of epidemiological models with nonlinear incidence rates*, *J. Math. Biol.* **25** 359–380 (1987).
7. P. Szor, *The Art of Computer Virus Research and Defense*, Addison-Wesley Professional (2005).
8. F.W. Wang, Y.K. Zhang, C.G. Wang, J.F. Ma, S.J. Moon, *Stability analysis of a SEIQV epidemic model for rapid spreading worms*, *Comput Secur.* **29**(4) 410–418 (2009).
9. W. Yang, G.-r. Chang, Y. Yao, X.-m. Shen, *Stability analysis of P2P Worm Propagation Model with Dynamic Quarantine Defense*, *Journal of Networks*, **6**(1) 153–162 (2011).
10. L.-X. Yang, X. Yang, *A new epidemic model for computer viruses*, *Commun. Nonl. Sci. Numer. Simul.*, **19**(6) 1935–1944 (2014).
11. Y. Yao, L. Guo, H. Guo, G. Yu, F.-x. Gao, X.-j. Tong, *Pulse quarantine strategy of internet worm propagation: Modeling and analysis*, *Computers & Electrical Engineering*, **38**(5) 1047–1061 (2012).
12. Y. Yao, X.-w. Xie, H. Guo, F.-x. Gao, G. Yu, *The Worm Propagation Model with Dual Dynamic Quarantine Strategy*, *Intelligent Computing and Information Science Communications in Computer and Information Science*, **135** 497–502 (2011).
13. Y.K. Zhang, F.W. Wang, Y.Q. Zhang, J.F. Ma, *Worm propagation modeling and analysis based on quarantine*, Proceedings of the 3rd international conference on information security (InfoSecu'04) 69–75 (2004).
14. C.C. Zou, W. Gong, D. Towsley, *Worm propagation modeling and analysis under dynamic quarantine defense*, WORM'03 Proceedings of the 2003 ACM workshop on Rapid malware 51–60 (2003).