Passive Benign Worm Propagation Modeling with Dynamic Quarantine Defense

Ossama Toutonji and Seong-Moo Yoo
Electrical and Computer Engineering Department
The University of Alabama in Huntsville
[e-mail: {toutono, yoos}@eng.uah.edu]
*Corresponding author: Seong-Moo Yoo

Received December 15, 2008; revised January 30, 2009; accepted February 3, 2009; published February 23, 2009

Abstract

Worm attacks can greatly distort network performance, and countering infections can exact a heavy toll on economic and technical resources. Worm modeling helps us to better understand the spread and propagation of worms through a network, and combining effective types of mitigation techniques helps prevent and mitigate the effects of worm attacks. In this paper, we propose a mathematical model which combines both dynamic quarantine and passive benign worms. This Passive Worm Dynamic Quarantine (PWDQ) model departs from previous models in that infected hosts will be recovered either by passive benign worms or quarantine measure. Computer simulation shows that the performance of our proposed model is significantly better than existing models, in terms of decreasing the number of infectious hosts and reducing the worm propagation speed.

Keywords: Modeling, passive benign worm, propagation, quarantine, worm attack

The research was partially supported by the Fulbright Scholar Program sponsored by the United States Department of States. Authors deeply appreciate the unknown reviewers' invaluable comments and very quick responses during the review time.

DOI: 10.3837/tiis.2009.01.005

1. Introduction

Worms are automatically self-replicating malicious codes which do not require user interaction to propagate through a network [1][2][3][4][5][6][7][8][9][10][11][12]. A worm seizes the victim machine by running a malicious exploit, and this infected machine will in turn, scan and infect other victims in the network. Lack of network security and mitigation measures can cause the worm attack to propagate through the network infrastructure, consuming overall bandwidth and causing other damage, which is potentially financially devastating. The attackers take advantage of the destructive behavior and vast spread of the worms through the network and take over a great number of systems, amplifying the damage and thus making trace-back more difficult. From a security perspective, worms can endanger networks by propagating without alerting the system, and the payload can be designed to give a worm the capability to propagate through the network, delete files, open a backdoor listener, create zombies with the worm generator, and plant a distributed denial of service flood agent. Notorious examples include the Code Red worm released in 2001, which infected 360,000 hosts in less than fifteen hours [13] and the SQL Slammer worm, launched in 2002, which caused denial of service and infected 75,000 victims within ten minutes [14].

Computer worm modeling is crucial to understanding the dynamic impact of worm attacks, in that it gives a comprehensive approach to identify weaknesses in the worm's propagation, allowing us to identify new methods to prevent and defend against Internet worm infection. Epidemic biological modeling [15][16] has been used in Internet worm modeling, as worm propagation is similar in many aspects to biological viruses.

Staniford et al. used the simple epidemic model to model the spread of Code Red [17]. The KM model [18] modified the simple epidemic model by adding a removal stage for previously infectious hosts, which either recover or die after some period of time. Then, Zou et al. [19] added a quarantine stage to the KM model. Recently, Zhou et al [20] proposed a passive worm propagation model, which added a passively infectious stage to the KM model.

In this paper, we propose a mathematical model that combines both dynamic quarantine and passive benign worms. Unlike other models proposed to date, in our model, some hosts in the passively infectious stage transition to the quarantine stage before they transition to the removed stage. Computer simulations show that the performance of our proposed model is significantly better than existing models, in terms of decreasing both the number of infectious hosts and the worm propagation speed.

This paper is organized as follows. Section 2 introduces related work on worm modeling. Section 3 explains our proposed Passive Worm Dynamic Quarantine model. Section 4 shows the simulation results of the proposed model as compared to three other models and Section 5 concludes the paper.

2. Related Work

The population in the simple epidemic model [17] consists of two types of hosts, susceptible and infectious, as shown in **Fig. 1**. This model assumes that when the host becomes infected, it will never recover. Thus, an infected host will transition from the susceptible stage to the infectious stage without recovery, and it will stay in the infectious stage indefinitely.

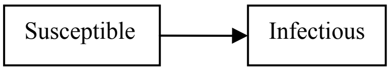

Fig. 1. Simple epidemic model

The Kermack-McKendrick epidemic model [18] considers an additional removal stage, where an infected host stay infected or gains immunity and thus is no longer susceptible or infectious. The host transitions from the susceptible to the infectious to the removal stage, as shown in **Fig. 2**.

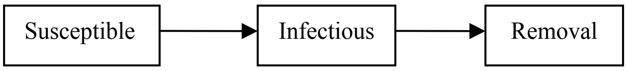

Fig. 2. Kermack-McKendrick epidemic model

Quarantine defense is a mitigation tool used to isolate any host on the network exhibiting suspicious behavior [21]. The concept has been adopted from quarantine methods used in infectious disease epidemiology. Zou et al. [19] proposed a dynamic quarantine where a host exhibiting suspicious behavior will be assumed "guilty before proven innocent." The main idea for the Zou model is that the traffic will be blocked on any port, for any host on the network, when a particular port behaves in a suspicious way for a defined period. This model is based on two observations: (1) Using a short quarantine time will have a very minor effect on network performance, and (2) The adjustable alert rate and the ability to increase the sensitivity of detection will yield opportunities to detect more worms. Fig. 3 shows a block diagram of the dynamic quarantine defense.

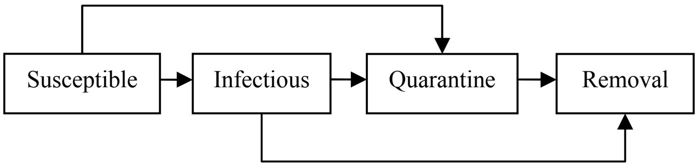

Fig. 3. Dynamic quarantine worm model

Benign worms, as proposed by Zhou et al. [20], are beneficial worms that counter the original malignant worms. Benign worms are representative of mitigation measures like patching and high-quality security configurations. The concept of benign worms is similar to medical vaccination against malignant viruses. A vaccine produced from a weakened, inactivated, or synthetically engineered virus is injected into a patient to illicit an immune response from the body. When the body is subsequently infected by the live virus, a vaccinated host will be better prepared to respond to the infection. Similarly, a host is deliberately infected with benign worms in order to protect the host from future infections.

Benign worms are either passive or active [20]. A *passive benign worm* infects a host in the network, and remains dormant until a malignant worm attacks. This attack will trigger a defensive response where the passive benign worm counters the malignant worm attack. An *active benign worm* defends against malignant worms by scanning the IP addresses in the network and compromising malignant worms in infected hosts. Fig. 4 shows the benign passive worm model.

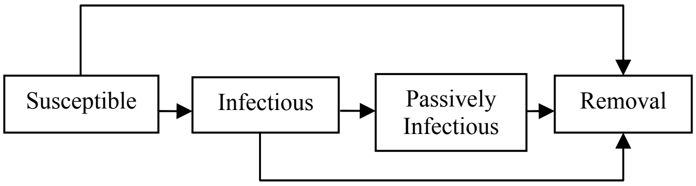

Fig. 4. Benign passive worm model

Even though all the aforementioned mitigation techniques contribute to decreasing the number of infectious hosts and help reduce the worm's propagation rate, they cannot, completely combat the widespread propagation of epidemic worms alone, and additional measures should be taken. The next section presents our proposed model, which combines the mitigation technique of passive worms with dynamic quarantine measures.

3. Passive Benign Worms with Dynamic Quarantine

We propose a new method to combat network worm infections by combining passive benign worms with a dynamic quarantine. A dynamic quarantine isolates hosts exhibiting suspicious behavior, while passive worms work to eliminate the malignant worms in infected hosts. This dual method, which we call the Passive Worm Propagation Quarantine (PWDQ) model, results in a more comprehensive approach to worm defense. The PWDQ model classifies hosts as being in one of five different stages, and any host can potentially be in any of these stages at any time:

(1) A *susceptible host* is vulnerable to worm infection.

(2) An *infectious host* has been infected by malicious worms.

(3) A *passively infectious host* has been infected by passive worms.

(4) A *quarantined host* has exhibited suspicious behavior and consequently, has been quarantined.

(5) For the purposes of this paper, a *removed host* is a formerly susceptible, infectious, or passively infectious host (that may or may not have been quarantined), which has gained immunity and is no longer infectious/susceptible.

We base our model on the following assumptions: (1) The worm is capable of scanning the whole domain and multiple machines concurrently. (2) The passive benign worms are incapable of completely compromising the worm infection. (3) Any port on any host with suspicious behavior will be quarantined. (4) The quarantine rates of the hosts differ depending on the host stage. (5) The passive worm will infect a machine when a worm infection has been detected.

The mathematical representation of our model is based on two factors - the dynamic countermeasures against worm propagation and the reduction in the worm infection rate [13]. We also consider both the propagation of the passive worm and the dynamic quarantine defense as new factors. **Fig. 5** shows a block diagram of the proposed worm model, and **Table 1** shows the notation and the initial values of the model.

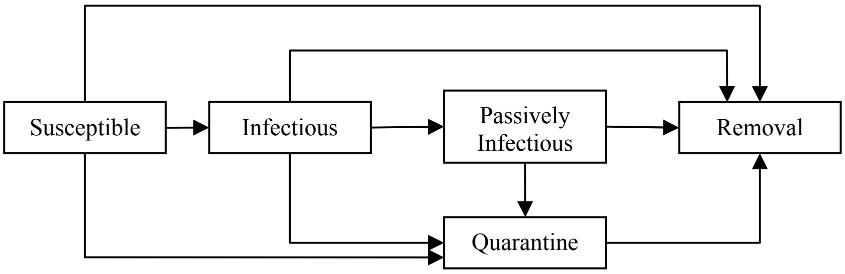

Fig. 5. PWDQ worm model

Table 1. Notations and initial values of the model

Notation	Explanation	Initial value
I(t)	Number of infectious hosts at time t	I(0)=1
S(t)	Number of susceptible hosts at time t	S(0)=949,999
U(t)	Number of passively infectious hosts at time t	U(0) = 50,000
R(t)	Number of removed hosts from the infectious population at time t	R(0)=0
Q(t)	Number of removed hosts from the susceptible population at time t	Q(0)=0
P(t)	Number of removed hosts from the passively infectious population at time t	P(0)=0
K(t)	Number of infectious quarantine hosts at time t	K(0)=0
F(t)	Number of susceptible quarantine hosts at time t	F(0)=0
Z(t)	Number of passive quarantine hosts at time t	Z(0)=0
H(t)	Number of removed hosts from the quarantine stage at time t	H(0)=0
$\beta(t)$	Infection rate at time t	$\beta(0) = 8 * 10^{-7}$
η	Parameter of infection rate	3
α	Removal rate of infectious hosts	0.05
μ	Removal rate of susceptible hosts	$6 * 10^{-8}$
θ	Removal rate of passively infectious hosts	0.004
N	Total number of hosts under consideration	1,000,000
T	Quarantine time	10
λ_1	Quarantine rate of infectious hosts	0.025
λ_2, λ_3	Quarantine rate of, susceptible, and passive hosts	0.00002315
q_1	Effective quarantine probability of infectious hosts	
q_2, q_3	Effective quarantine probability of susceptible and passive hosts	

According to **Fig. 5**, a susceptible host could become infected and transition to the infectious stage. The infected host can in turn be compromised by passive worms and transition to the passively infected stage. Some percentage of hosts exhibiting suspicious behavior will transition to the quarantine stage, where they will be released after the specified amount of time has elapsed. Any host can gain immunity (from countermeasures beyond the scope of this paper) and end up in the removal stage.

According to [20], the number of hosts that transition from the susceptible stage to the infectious state is $\beta(t)I(t)S(t)$, and the number that transition from the infectious stage to the passively infectious state is $\beta(t)I(t)U(t)$. Also, the number of hosts that transition from the susceptible stage, the infectious stage and the passively infectious stage, to the removal stage are $\mu(I(t)+R(t))S(t)$, $\alpha I(t)$, and $\theta U(t)$, respectively.

Three parameters, q_1, q_2, and q_3, the effective quarantine probability of infectious hosts and susceptive hosts, respectively, are defined in [19] as follows:

$$q_1 = \frac{\lambda_1 \mathrm{T}}{1+(\lambda_1+\alpha)\mathrm{T}} \tag{1}$$

$$q_2 = q_3 = \frac{\lambda_2 T}{1+\lambda_2 T} \tag{2}$$

We observe the following facts on the quarantine probabilities:

a) The susceptible hosts may not be infected yet with worms.

b) The bad worms in the passively infectious hosts may have been overcome with passive benign worms.

c) From a) and b), we can conclude that the bad worm scanning activities in both susceptible hosts and the passively infected hosts are minimal. In this case the quarantine rate has been set to small sensitivity.

d) However, in infectious hosts, bad worms start scanning the network for new targets. In this case, more suspicious activities should be detected, and the quarantine rate has been set to a higher level.

Therefore, the suspicious activities in both the susceptible and passively infectious hosts are very small compared to the infectious hosts. Consequently, we can assume that q_3, the effective quarantine probability of passively infectious hosts, is equal to q_2, that of susceptible hosts.

Then, the number of hosts transited from the susceptible ($F(t)$), the infectious ($K(t)$), and passively infectious ($Z(t)$), respectively, stage to the quarantine stage at time t is given as follows:

$$K(t) = q_1 I(t) \tag{3}$$

$$F(t) = q_2 S(t) \tag{4}$$

$$Z(t) = q_3 U(t) \tag{5}$$

Thus, $H(t)$, the total number of hosts that transition from the quarantine stage to the removal stage, is as follows:

$$H(t) = q_1 I(t) + q_2 S(t) + q_3 U(t) \tag{6}$$

We set the value of quarantine rates λ_1, λ_2, λ_3 by examining the required level of sensitivity for different types of hosts. The anomaly detection program is set to a higher sensitivity to detect worm activities. In our case λ_1 is greater than $\lambda_{2,}$ and $\lambda_{3\,,}$ where malignant worm activity in the infectious stage is higher than in the susceptible and passively infectious stages.

Then, the change in the number of infectious hosts $I(t)$ from time t to time $t + \Delta\, t$ in time is represented by the following equation:

$$I(t+\Delta t)-I(t)=\beta(t)I(t)S(t)\Delta t-\beta(t)I(t)U(t)\Delta t-\frac{dR(t)}{dt}\Delta t-\frac{dK(t)}{dt}\Delta t \tag{7}$$

Hence

$$\frac{dI(t)}{dt}=\beta(t)I(t)S(t)-\beta(t)I(t)U(t)-\frac{dR(t)}{dt}-\frac{dK(t)}{dt} \tag{8}$$

We can base the set of differential equations of the proposed model on the same concept. Also, based on the two-factor model, we can express the equation of the infection rate $\beta(t)$ as

$$\beta(t)=\beta_0(1-\frac{I(t)}{N})^{\eta} \tag{9}$$

The set of differential equations for PWDQ model are:

$$\frac{dS(t)}{dt}=-\beta(t)I(t)S(t)-\frac{dQ(t)}{dt}-\frac{dF(t)}{dt} \tag{10}$$

$$\frac{dI(t)}{dt}=\beta(t)I(t)S(t)-\beta(t)I(t)U(t)-\frac{dR(t)}{dt}-\frac{dK(t)}{dt} \tag{11}$$

$$\frac{dU(t)}{dt}=\beta(t)I(t)U(t)-\frac{dP(t)}{dt}-\frac{dZ(t)}{dt} \tag{12}$$

$$\frac{dP(t)}{dt}=\theta U(t) \tag{13}$$

$$\frac{dR(t)}{dt}=\alpha I(t) \tag{14}$$

$$\frac{dQ(t)}{dt}=\mu(I(t)+R(t))S(t) \tag{15}$$

$$\begin{aligned}\frac{dF(t)}{dt}&=q_2\frac{dS(t)}{dt}\\ \frac{dK(t)}{dt}&=q_1\frac{dI(t)}{dt}\end{aligned} \tag{16}$$

$$\frac{dZ(t)}{dt} = q_3 \frac{dU(t)}{dt}$$

$$\frac{dH(t)}{dt} = \frac{dF(t+T)}{dt} + \frac{dK(t+T)}{dt} + \frac{dZ(t+T)}{dt} \tag{17}$$

$$I(t) + R(t) + S(t) + Q(t) + U(t) + P(t) + K(t) + F(t) + Z(t) = N \tag{18}$$

4. Simulation

Most of simulation parameters used in this paper are same as [19] and [20]. The initial values used are shown in Table 1. Since the initial values of λ_2 and λ_3 are very small compared to the initial value of $\lambda_{1,}$ we used the values of λ_2 and λ_3 after multiplied by 500.

The models below show the effects of changing the simulation parameters (i.e., number of passive worms, quarantine rate of infectious hosts, and quarantine time), on worm propagation. Our simulation compared the number of infectious hosts in a PWDQ-defended population with a conventional PWP–defended population, in order to elucidate the advantages, if any of a combined defense.

4.1 Comparison of four models, KM (Kermack-McKendrick), PWP, DQ (Dynamic Quarantine) and PWDQ models

Using Matlab, we first simulated the KM model as a baseline, and then separately implemented the PWP and DQ models. Finally, we designed our PWDQ model by combining the PWP and DQ defenses. The four models share the same parameters. **Fig. 6** shows the number of infectious hosts for each of the four models, where the *x*-axis represents the time and the *y*-axis represents the number of infectious hosts. The result shows a noticeable decrease and a reduced propagation speed for the infectious hosts in our PWDQ model than for the three other models, due to the use of a combined passive worm and quarantine defense. These results support our expectation that combining mitigation methods will reduce the propagation speed of malicious worms and decrease the number of infectious hosts.

4.2 Initial number of passive worms

Fig. 7 shows the effect of increasing the number of initially passively infected hosts in the infectious host population. In this simulation, we increase the number of initially passive hosts several times, by between 1% and 10%, while the rest of the parameters remain constant. Here, ‘I:U-1%’ means the infectious population when *U*(*t*) is 1% of *N*, and *A* = *U* + *P*. The result shows a corresponding decline in the number of infectious hosts as the number of initially passively infectious hosts is increased. We noticed that the initial number of passive worms greatly affects the number of infectious hosts. This result is consistent with the results in [20].

4.3 Quarantine time and quarantine rate of infectious hosts

Fig. 8 shows the effect of the quarantine rate on worm propagation. As expected, the results show that increasing the quarantine rate yields a decline in both the worm propagation speed and in the number of infectious hosts.

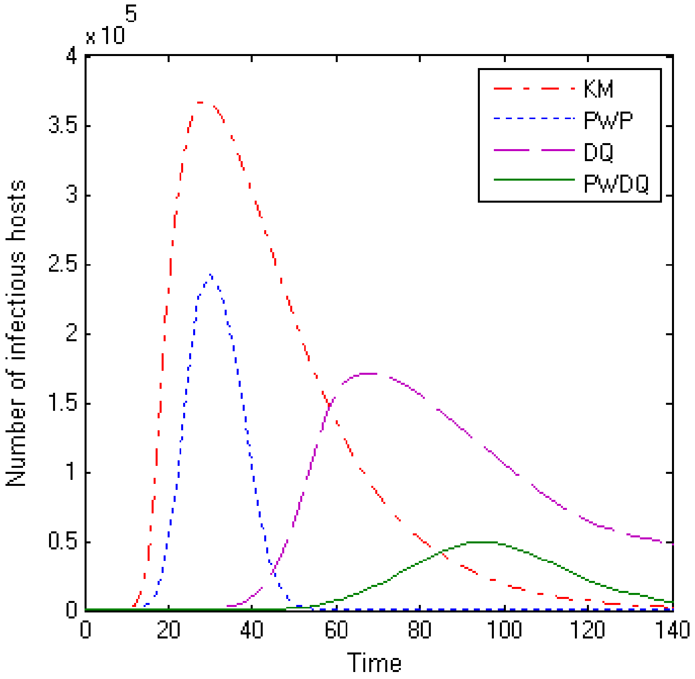

Fig. 6. Comparison between four models, in terms of the number of infectious hosts

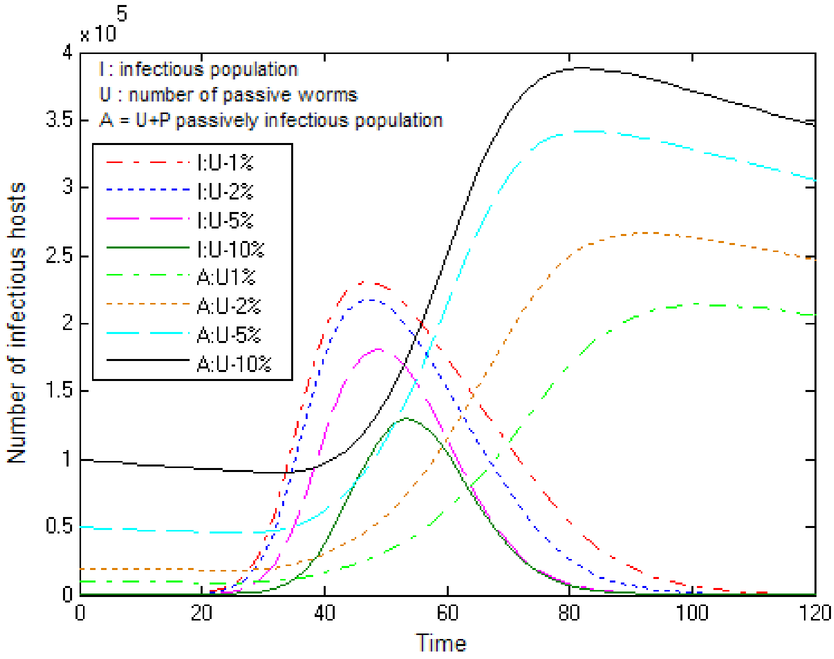

Fig. 7. Effect of the initial number of passive worms

Fig. 9 shows the effect of increasing the quarantine times (which are between 20 and 60 seconds) on worm propagation. As expected, a longer holding-time in quarantine diminishes the propagation rate of a worm and lowers the total number of infectious hosts.

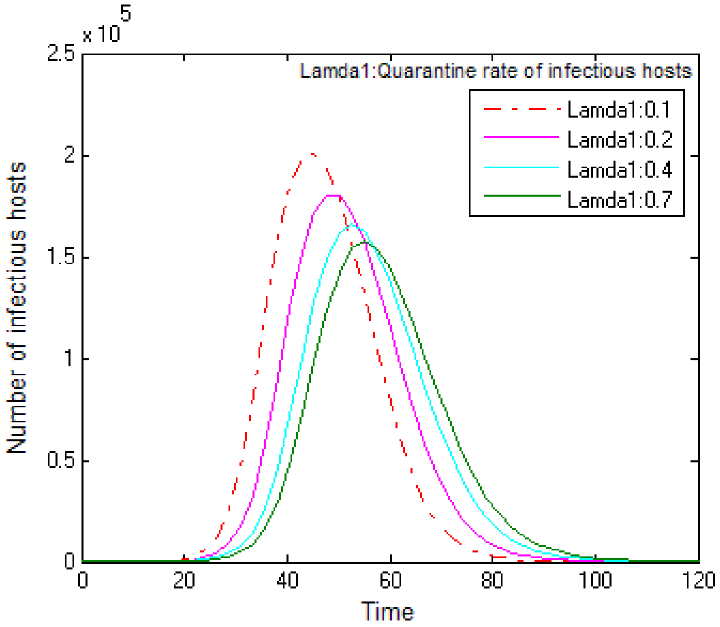

Fig. 8. Effect of quarantine rate

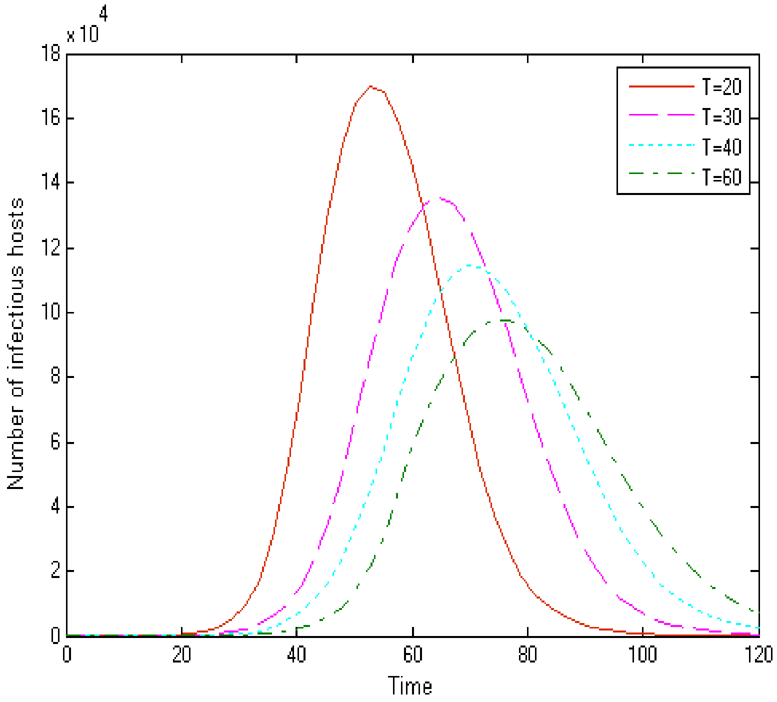

Fig. 9. Effect of quarantine time

The comparison shows that using more stringent criteria for our model, such as those of the first set of parameters, will enable us to design a model that more effectively counters worm propagation. It will not only decrease the number of infectious hosts but also reduce the speed of worm propagation through the network.

5. Conclusion

Modeling of combined mitigation techniques to help test the effects of worm infection on more secure networks has unlocked a new area of research. To the best of our knowledge, this has not been explored. Combating malicious worms is complicated and difficult, due to the widespread propagation of worms. Studies show that implementing passive benign worms or quarantine defenses alone cannot effectively contain worm epidemics. Clearly, further measures are needed to combat worms. Our new Passive Worm Dynamic Quarantine model aims to fill this gap; our comprehensive approach combines two types of mitigation techniques. The PWDQ models show a noticeable decline in the infectious population compared to either the PWP or quarantine models, as well as a decline in the propagation speed. Additional simulations, involving changing the initial values of selected parameters, show that a further decline in the infectious host population can be achieved by increasing the number of passively infected hosts and/or by increasing the quarantine rate/time of infectious hosts. Our future research will investigate more effective types of benign worms that could be combined with quarantine defense tools, in order to further reduce the infectious population.

References

[1] P. Li, M. Salour, and X. Su, "A Survey of Internet Worm Detection and Containment," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 1, pp. 20-35, 1st quarter, 2008.

[2] E. Skoudis and L. Zeltsr, *Malware, Fighting Malicious Code*, Pearson Education, 2004.

[3] J. Kim, W.O. Wilson, U. Aickelin, and J. McLeod, "Cooperative Automated Worm Response and Detection ImmuNe Algorithm (CARDINAL) Inspired by T-cell Immunity and Tolerance," Proc. *Int'l Conf. on Artificial Immune Systems*, *LNCS 3627*, Banff, Canada, 2007.

[4] J. Kim, S. Radhakrishnan, and S.K. Dhall, "Measurement and Analysis of Worm Propagation on Internet Network Topology," Proc. *Int'l Conf. on Computer Communications and Networks* (*ICCCN'04*), pp. 495-500, Chicago, Oct. 2004.

[5] F. Castaneda, E.C. Sezer, and J. Xu, "Worm vs. Worm: Preliminary Study of an Active Counter-Attack Mechanism," Proc. *2003 ACM Workshop on Rapid Malcode* (*WORM'04*), pp. 83-93, Washington, DC, Oct. 2004.

[6] S.H. Selke, N.B. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," *IEEE Trans. on Dependable and Secure Computing*, vol. 5, no. 2, pp. 71-86, April 2008.

[7] X. Yan and Y. Zou, "Optimal Internet Worm Treatment Strategy Based on the Two-Factor Model," *ETRI Journal*, vol. 30, no. 1, pp. 81-88, Feb. 2008.

[8] H. Zhou, Y. Wen, and H. Zhao, "Modeling and Analysis of Active Benign Worms and Hybrid Benign Worms Containing the Spread of Worms," Proc. *IEEE Int'l Conf. on Networking* (*ICN'07*), 2007.

[9] Z. Chen, L. Gao, and K. Kwiat, "Modeling the Spread of Active Worms," Proc. *IEEE INFOCOM*, vol. 3, pp. 1890-1900, 2003.

[10] R. Dantu, J. Cangussu, and A. Yelimeli, "Dynamic Control of Worm Propagation," Proc. *Int'l Conf. Information Technology: Coding and Computing* (*ITCC*), 2004.

[11] J. Kim, S. Radhakrishnan, and J. Jang, "Cost Optimization in SIS Model of Worm Infection," *ETRI Journal*, vol. 28, no. 5, pp. 692-695, 2006.

[12] F. Wang, Y. Zhang, and J. Ma, "Modeling and Analysis of a Self-Learning Worm Based on Good Point Set Scanning," *Wireless Communications and Mobile Computing*, Early View, Nov. 2008.

[13] D. Moore, C. Shannon, and J. Brown, "Code Red: a Case Study on the Spread and Victims of an

Internet Worm," Proc. *2nd ACM SIGCOMM Workshop on Internet Measurement*, Marseille, France, Nov. 2002.

[14] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford,, and N. Weaver, "Inside the Slammer Worm," *IEEE Magazine of Security and Privacy*, vol. 1, no. 4, pp. 33-39, 2003.

[15] D. J. Daley and J. Gani, *Epidemic Modeling: An Introduction*, Cambridge, Studies in Mathematical Biology, 2001.

[16] C.C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," *9th ACM Symp. on Computer and Communication Security*, pp. 138-147, Washington DC, 2002.

[17] S. Staniford, V. Paxson, and W. Weaver, "How to Own the Internet in Your Spare Time," *11th Usenix Security Symposium*, San Francisco, Aug. 2002.

[18] J.O. Kephart, D.M. Chess, and S.R. White, "Computers and Epidemiology," *IEEE Spectrum*, vol. 30, no. 5, pp. 20-26, 1993.

[19] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Internet Quarantine: Requirements for Containing Self-Propagating Code," Proc. *IEEE INFOCOM*, San Franciso, vol. 3, pp. 1901-1910, Mar.-Apr. 2003.

[20] C.C. Zou, W. Gong, and D. Towsley, "Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," Proc. *2003 ACM Workshop on Rapid Malcode* (*WORM'03*), Washington, DC, Oct. 2003.

[21] H. Zhou, Y. Wen, and H. Zhao, "Passive Worm Propagation Modeling and Analysis," Proc. *IEEE Int'l Conf. on Computing in the Global Information Technology*, Guadelope, French Caribbean, pp. 32, Mar. 2007.

Ossama Toutonji is a Ph.D. student of Electrical Engineering at the University of Alabama in Huntsville (UAH), Huntsville, Alabama - USA. He earned his MSE in Electrical Engineering in UAH. His research interests are in the areas of information assurance in computer networks, especially worm modeling.

Seong-Moo Yoo is an Associate Professor of Electrical and Computer Engineering at UAH. Before joining UAH, he was an Assistant Professor at Columbus State University, Columbus, Georgia – USA. He earned his MS and PhD in Computer Science at the University of Texas at Arlington, Arlington, Texas – USA. His research interests include computer network security, wireless network routing, and parallel computer architecture. He has co-authored over 60 scientific articles in refereed journals and international conferences.