A New Ecology Model for Internet Worm Security Threat Evaluation

Wang XiaoPeng*, Wang Bailing, Liu Yang, He Hui and Sun Yunxiao

Department of Computer Science & Technology
Harbin Institute of Technology at Weihai, Shandong, China
**winxp_007@hotmail.com*

Abstract

Welchia worms were launched to terminate the Blaster worms and patch the vulnerable hosts. They created complex worm interactions as well as detrimental impact on infrastructure. Worm propagation analysis, including exploring mechanisms of predator-prey worms' propagation and formulating effects of network/worm parameters, has great importance for worm containment and host protection. In this paper, an integrated worm ecology model is given to study the propagation of such worms. The analytical results provide insights of the worm design and impact to network. The simulation results verify the correctness of our model and show the effectiveness of the worm model by applying it to the LiOn/Cheese and MSBlaster/Welchia.

Keywords: *Internet Ecology, Network Security, Worm*

1. Introduction

Worm propagates through network, and attacks the vulnerability, which exists in much extensively used software, to exhaust the network resource. Since the first worm created in 1988 [1], the security threat posed by worms has steadily increased, especially in the last ten years. The Code Red worm and Nimda worm incidents of 2001 have shown us how vulnerable our networks are and how fast a worm can spread.

The reason for internet worm to be hard to control is that Internet is so open, complex and immense that causes us having no way to know or control all the hosts connected to internet. The worms will stay in the hosts and attack other hosts for a long period if the uncontrolled hosts are infected with worms. So the key to control the Internet worm is to find the solution to recovering those uncontrolled hosts.

Recently, people begin to study the active countermeasure with friendly worm which can be posted to the remote hosts to recover them actively. The typical examples are as follows:

2001, worm Cheese was released to Internet against worm LiOn [2].

2001, worm CodeGreen and CRClean [3] were developed against worm CodeRed, but both of them were not released to Internet.

2003, worm Welchi [4] was released to Internet against worm MSB laster.

But the result is not very prefect. Especially, Welchi has caused a mass of loss and high impact on Internet. There is no successful and influential case on worm countermeasure until now due to the absence of theoretical model and the corresponding experiments.

In the following, we try to characterize and analyze the model of active SIworms and simulate the aftereffect when releasing the SIworms to Internet to kill the worms.

2. Traditional protection systems and Vulnerabilities

There are two main categories of traditional worm protection system: Host-based Intrusion Prevention System (HIPS) and Network-based Intrusion Prevention System (NIPS).

2.1. Host-based Intrusion Prevention System

HIPS are located between the application layer and the kernel of the operating system, thus intercepting system calls from the ground, including reading and writing requests to the disk, network connection requests and attempting to read and write memory, and so on [6, 7]. For example, some applications cannot overwrite some system files, if it is attempted to overwrite system files, then HIPS can overwrite it hijacked and mark it illegal.

2.2. Network-based Intrusion Prevention System

NIPS are real time analysis systems. They hijack network packets, judge for suspicious actions, and then decide whether to discard or release. NIPS actually borrow some IDS methods to judge harmful connection and malicious code. For example some NIPS mark permitted behaviors (such as port scanning) with responding tag [8, 9]. If the attacker shows corresponding action, NIPS can tell this as an intrusion attempt, and cut off the current connection.

2.3. Limitations of Traditional Protection Models

Due to the disorder of the hosts on the network, manager can't install HIPS on each host. Let alone that HIPS cannot protect from network attacks. Even if the host is protected, it is still unable to access to network properly. NIPS play an important role in network attack. However, it is not perfect, as follows:

1. Outbreak helpless

Most networks are now switched networks, but NIPS are still part of the edge protection, which only monitoring data to and from the local area network. This results that the NIPS is unable to timely detect worm of mobile devices such as laptop computers when they temporarily access to a network. It is possible that worm outbreaks have erupted in local area network when the NIPS exception. at this time NIPS can at best prevent the spread of epidemic to the external network, while it is powerless to the epidemic outbreak.

2. Recognition errors

This is mainly reflected in the two aspects: an attack instead of the exception; the exception but not to attack. For the former we call false negatives, which we call false positives. If Exception thresholds are defined too high, it can result in high false negative rates. This is obviously not to play a protective role, and cause illusion of safety to the security managers. If exception thresholds are defined too low, it can lead to high false positive rate. High false positive rate of IDS, at most there will be more false alarms; and the NIPS will cut off access directly, which is bound to affect the normal access to the network. That is a very serious problem.

3. Bandwidth affection

NIPS are real-time online monitoring systems. Therefore, the processing power of the system determines the bandwidth of a network outlet. Obviously NIPS can easily become a network bottleneck, which is concern to many IT managers.

NADIR [11, 12], as the earlier system, applies a distributed data collecting technology, then set using the expert system for analysis and processing, the system response to attacks focused mainly on passive, no active protection. CSM is a peer based distributed intrusion detection system, each endpoint is a communication between the host-based IDS, IDS is not centralized control, but on a point-to-point, as CSM is still not active defensive capability. Describes a distributed firewall system, the main idea is the use of centralized control; each terminal is only passively follow the control center to configure rules for data filtering. NADIR is a point-to-point, intrusion prevention systems, NADIR is installed each host in the Network Node, each Node in the protection of its own security while they are provided in the network neighborhood. In this way, other hosts on the network attacker in advance can be blacklisted.

From the above analysis we can see that traditional protection system mainly protect against intrusion, attack, and so on, which has been entirely inapplicable to worm containment. In order to effectively control the Worms epidemic, we must abandon the traditional passive defense strategy, and apply proactive policy. So we made use of friendly worms for worm confrontational, which is effective in curbing the epidemic.

3. Simulation on Worms and SIworms Propagation

In order to describe the simulation clearly, we will give some definitions first.

Definition 1 Susceptible Host: If a host has a vulnerability, which can be exploited by a worm to enter the host, but the worm has not infected it, we call it a susceptible host.

Definition 2 Immune Host: If a host is immune to the worm, and the worm has never infected it, we call it an immune host.

Definition 3 Transparent Infected Host: If a host has been infected with a worm, and the worm didn’t close the backdoor or the vulnerability, such as worm Sasser, we call the host a transparent susceptible host.

Definition 4 Recessive Infected Host: If a host has been infected with a worm, but the worm closed the backdoor or the vulnerability, such as worm LiOn, we call the host a transparent susceptible host.

Definition 5 SIworm: The *SIworm* is a friendly worm that can recover the susceptible hosts and then the host will become an *immune host* and be immune to the worm forever.

Definition 6 IRworm, Removed Host: The IRworm is a friendly worm that can recover the infected hosts, and then the infected host will become a removed host and be immune to the worm. The removed host is different from the immune host due to the different original state.

Definition 7 Starting Time: It is a time, from which we begin to observe the transformation of the hosts in the network. Any time can be the starting time, but there are different parameters in different starting time. For example, suppose we detect a new worm occurred in network at time t, then we could denote time t is the starting time, and begin to research on the number transformation of the infected hosts in network.

Definition 8 Initiative Value: It is the value of the parameters, such as the number of the infected hosts, the worm propagation rate and so on, at the starting time.

J. C. Frauenthal’s K-M epidemic model considers the removal process of infectious hosts

[5]. It assumes that during the epidemic situation some infectious hosts either recover or die. Once a host dies or recovers from the disease, it will be immune to the disease forever. There are also four states in our model: susceptible state, infected state, immune state and second immune state. From the worm's point of view, SIworm and IRworm remove some hosts from worm spreading circulation, including both hosts that are infected and hosts that are still susceptible. In other words, the removal process consists of two parts: removal of the infected hosts and removal of susceptible hosts. The states transition can be described as the Figure 1.

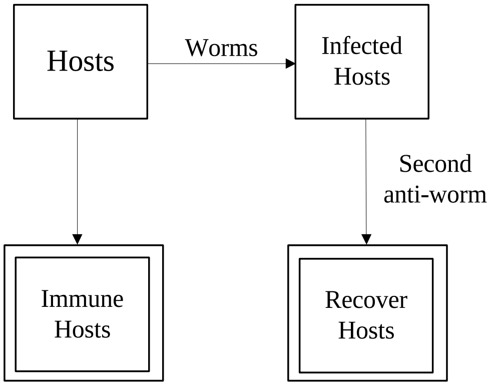


Figure 1. State Transition of Vulnerable Hosts

Note that the IRworm is same to SIworm, if the vulnerable host becomes a recessive infected host after worm infects it. Here, we only simulate the scenarios that the vulnerable host becomes a transparent infected host, and then we have to send out both the SIworm and the IRworm to contain the worms.

We simulate four scenarios. The first one is the classical simple epidemic model, which is same to that figured in [10]. There are two states in this model without any recover function. Then the state transition of the vulnerable hosts is susceptible host → infected host. In the second scenario, we simulate that only SIworms are sent out to contain worms, and then the state transition of the vulnerable hosts is susceptible host → removed host; susceptible host → immune host. In the third scenario, we simulate that only IRworms are sent out to contain worms, and then the state transition of the vulnerable hosts is susceptible host →second infected host → removed host. At last, we simulate that both of SIworm and IRworm are sent out to contain worms. Then the state transition of the vulnerable hosts is susceptible host →second infected host → removed host; susceptible host → immune host.

For the purpose of comparison, we plot the simulation results of the four scenarios in Figure 2. (Suppose the total number of the hosts under consideration is M=10,000, 0.04 percent of the total hosts are infected with worm, 0.03 percent of the total hosts are infected with SIworm, 0.03 percent of the total hosts are infected with IRworm, and the propagation rate of the three worms is 4 scans/s.)

Comparing our simulation curves in Figure 2, we observe that, by only sending SIworm (the curve under considering SIworm in Figure 2), we cannot recover all of the infected hosts and can only reach a dynamic balance. If only sending IRworm (the curve under considering IRworm in Figure 2), we can recover all of the vulnerable hosts at last, but it is much slower and the peak value is nearly same to the classical simple epidemic model simulation. Only by sending both SIworm and IRworm, the vulnerable hosts can be recovered clearly and fast, as curved in Figure 2.

Note that if increasing the propagation rate of SIworm and IRworm, the peak value of the curve under considering SIworm and IRworm will decrease fast. But the corresponding impact to network will increase too.

4. Numerical Analysis on Worms and SIworms Propagation

SIworm is also a worm, and it can bring extra traffic load to network if it is lost of control, just like worm welchi. So we have to set up a numerical model to evaluate the situation under the countermeasure. And in this part, we will give a farther research on the numerical model of the propagation based on the simulation above. By use of the numerical model, we can forecast the worm epidemic situation under active countermeasure and not under active countermeasure.

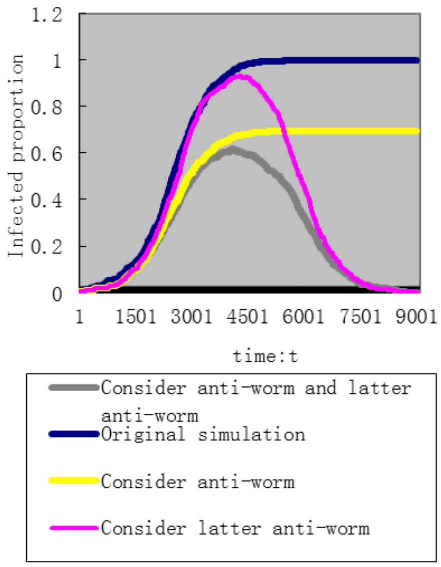


Figure 2. Worm Simulation based on Different Model

Add also, we deem the number of hosts is not important, but the proportion of the hosts in every state is important. So we use the proportion value as the main parameters of our model.

There are two instances: the first is after being infected, the susceptible host becomes transparent infected and the second is that the vulnerable host becomes recessive infected. We will give different numerical model according to different instance.

Table 1. Notation in this Paper

Notation	Definition
M	Total number of hosts under consideration
S(t)	The proportion of susceptible hosts at time t.
I(t)	The proportion of infected hosts at time t.
$R_S(t)$	The proportion of immune hosts with SIworm at time t.
$R_I(t)$	The proportion of removed hosts with IRworm at time t.
R(t)	The proportion of immune hosts. $R(t)= R_S(t)+ R_I(t)$
α	The worm propagation rate
γ_S	The SIworm propagation rate
γ_I	The IRworm propagation rate

4.1. Vulnerable Hosts Become Recessive Infected

Let M denote the total number of the hosts under consideration; R_S(t) denote the proportion of immune hosts with SIworm at time t; S(t) denote the proportion of susceptible hosts at time t, γ_S denote the SIworm propagation rate. Then the change in the number of the immune hosts with SIworm R_S(t) from time t to time t +Δt follows the equation:

$$M \times R_S(t+\Delta t) - M \times R_S(t) = [\gamma_S \times S(t)] \times [M \times R_S(t)] \times \Delta t \tag{1}$$

In Eq. (1), γ_S × S(t) is the probability for an SIworm to scan the susceptible hosts, and M × R_S(t) is the total number of the SIworm at time t.

Let RI(t) denote the proportion of immune hosts with IRworm at time t; I(t) denote the proportion of infected hosts at time t, γI denote the IRworm propagation rate. Then the change in the number of the removed hosts with IRworm RI(t) from time t to time t +Δt follows the equation:

$$M \times R_I(t+\Delta t) - M \times R_I(t) = [\gamma_I \times I(t)] \times [M \times R_I(t)] \times \Delta t \tag{2}$$

In Eq. (2), γI × I(t) is the probability for a IRworm to scan the infected hosts, and M × RI(t) is the total number of the IRworm at time t.

Referring to Eq.(1) and Eq.(2) the change in the number of the infected hosts from time t to time t+Δt follows the equation:

$$\begin{aligned} &M \times I(t+\Delta t) - M \times I(t) = \\ &[\alpha \times S(t)] \times [M \times I(t)] \times \Delta t - [\gamma_I \times I(t)] \times [M \times R_I(t)] \times \Delta t \end{aligned} \tag{3}$$

And the change in the number of the susceptible hosts from time t to time t+Δt follows the equation:

$$\begin{aligned} &M \times S(t+\Delta t) - M \times S(t) = \\ &-[\gamma_S \times S(t)] \times [M \times R_S(t)] \times \Delta t - [\alpha \times S(t)] \times [M \times I(t)] \times \Delta t \end{aligned} \tag{4}$$

Note that S(t) + I(t) + R(t) = M and R(t) = RS(t) + RI(t) holds for any time t. Hence, we have

We refer to the model described by Eq(5) as the recessive countermeasure model, and the propagation worm Lion and worm Cheese belongs to this model by setting γS=0. In fact, SIworm and IRworm will not propagate forever, and then we model the life cycle of SIworm as a function of time, *i.e.*, Fi(t).

4.2. Vulnerable Hosts Become Transparent Infected

In this situation, the IRworm is same to SIworm, and then $\gamma_S = \gamma_I = \gamma$. Let R(t) denote the sum of R_S(t) and R_I(t), then we have

$$R_S(t)' = \gamma \times S(t) \times R(t) \tag{6}$$

And

$$R_I(t)' = \gamma \times I(t) \times R(t) \tag{7}$$

Substituting Eq.(6) and Eq.(7) into Eq(5) yields a new differential equation. We refer to this worm model described by the new equation as the transparent countermeasure model, and the propagation of worm MSBlaster and worm welchi belongs to this model. Because of the limit of the paper, we will not give the solution of this model, and the solution can be obtained by referring to the recessive countermeasure model we gave above.

5. Impact Analysis

From result of the numerical solution and simulation, we can conclude that SIworm and IRworm can contain the worm epidemic effectively. But both of them are also worms, and they will bring extra traffic load to network. In this part, we will analyze the impact they bring to the network. We analyze two scenarios, the first is the impact after worm cheese was sent out to kill worm LiOn, and the second is the impact after worm welchi was sent out to kill worm MSBlaster. The prior belongs to recessive propagation model and the later belongs to the transparent propagation model. We give some definitions first.

$$\begin{cases} S(t)' = -\alpha \times S(t) \times I(t) - R_S(t)' \\ I(t)' = \alpha \times S(t) \times I(t) - R_I(t)' \\ R_S(t)' = \gamma_S \times S(t) \times R_S(t) \times F_S(t) \\ R_I(t)' = \gamma_I \times I(t) \times R_I(t) \times F_I(t) \\ F_i(t) = \begin{cases} 1 & t \geq t_{Si} And \quad t \leq t_{Ei} \\ 0 & t < t_{Si} Or \quad t > t_{Ei} \end{cases} i = S, I \\ R(t) = R_S(t) + R_I(t) \\ 0 \leq S(t), I(t), R(t) \leq 1 \\ S(t) + I(t) + R(t) = 1 \\ \alpha > 0, \gamma_S \geq 0, \gamma_I \geq 0, \gamma_I + \gamma_S > 0 \end{cases} \qquad (5)$$

Definition 9 Worm Effective Touch Factor δ: We model it as a function of time, *i.e.*, δ(t). From the point of network, if one worm scan is sent out in one unit time, there is one effective touch to network. So δ(t) is the product of the worm propagation rate α and the number of worms M*I(t), where I(t) is the proportion of the infected hosts at time t. Then we have:

$$\delta(t) = \alpha * M * I(t) \qquad (8)$$

Definition 10 Worms Absolute Impact Factor λ(t)： Suppose there are N kinds of worms in network, and the proportion of each worm is $I_n(t)$ (0≤n<N). Then:

$$\lambda(t) = \sum_{n=0}^{N-1} \delta_n(t) \qquad (9)$$

So we have the absolute impact factor in the classical simple epidemic model:

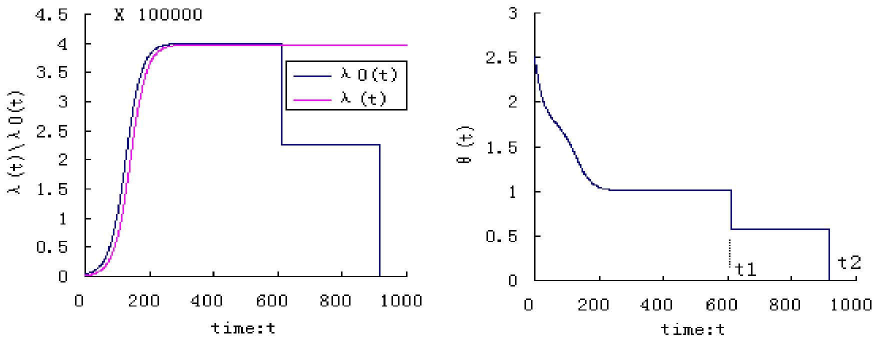
$$\begin{cases} \lambda_0(\mathrm{t}) = \delta_0(t) \\ \lambda(t) = \delta_I(t) + \delta_{Rs}(t) + \delta_{Ri}(t) \end{cases} \qquad (10)$$

Definition 11 Worms Relative Impact Factor θ(t):

$$\theta(t) = \frac{\lambda(t)}{\lambda_0(t)} \tag{11}$$

We analyze the worms absolute impact factor λ(t) and the worms relative impact factor θ(t). Note that F(t) is a switch function, that means the friendly worm will kill itself after the system time exceeds its threshold. Add also, the curves of θ(t) and λ(t) will not be a straight line at time t1 and t2, because the system time in different host is not consistent with each other in fact. Here we deem the influences in large number of hosts are counteracted, and plot them in perfect situation.

Figure 3 (a) shows that the maximum impact after sending out worm cheese to network is same to the maximum impact that worm LiOn cause. But the differentia is that the peak value arrives early, and the whole curve is moved ahead after cheese was sent out. Figure 3 (b) shows that the maximum of θ(t) occurs at the starting time.



(a)Worms Relative Impact (b) Worms Absolute Impact

Figure 3. Worm LiOn and Worm Cheese Impact Analysis

6. Conclusions

This article proposed a model of worm against worm propagation. According to this model, the network epidemic could be simultaneously analyzed and forecasted both before and after releasing friendly worms and the index of worm propagation impact could also be quantified.

Later work will focus on the following areas:

1. to reduce the effects of immune worms;

2. to design platform to release and to monitor friendly worms, through which the worm propagation could also be constantly monitored.

Acknowledgements

This research was supported by the National Science Nature Foundation of China under Grant No 61170262.

References

[1] L. Ting and Z. Qinghua, “Modeling and Analysis of Worm Propagation in IPv6 Networks”, Chinese Journal of Computers, **(2006)**, pp. 1337-1345.

[2] Z. Xinyu, “A Coordinated Worm Detection Method Based on Local Nets”, Journal of Software, **(2007)**, pp. 412-421.

[3] N. C. and J. D. Fulp, “A methodology for evaluation of host-based intrusion prevention systems and its

application", Proceedings of the 2006 IEEE Workshop on Information Assurance, **(2006)**, pp. 378-379.

[4] Y. Feng and D. Haixin, "Modeling and analyzing of the interaction between worms and antiworms during network worm propagation", Science in China, **(2005)**, pp. 91-106.

[5] J. C. Frauenthal, "Mathematical Modeling in Epidemiology", Springer-Verlag, New York, **(1980)**.

[6] T. Gong and Z. -x. Cai, "Normal model and BPNN-Based Immunization of Anti-Worm Web System", International Journal of Multimedia and Ubiquitous Engineering, vol. 1, no .3, **(2006)** September, pp. 23-36.

[7] L. Aiping, M. Jiajia and J. Yan, "High Assurance Architeture of Streaming Data Integration System about Security Threat Monitor", International Journal of Database Theory and Application, vol.1, no.1, **(2008)** December, pp. 37-44.

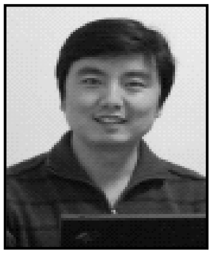
[8] P. S. Priya and G. Sumathi, "An Improved Security and Trusting Model for Computational Grid", International Journal of Grid and Distributed Computing, vol. 4, no. 1, **(2011)** March, pp. 57-66.

[9] C. Chakraborty, "Structural Characterization of Worm Images Using Trace Transform and Backpropagation Neural Network", vol. 5, no. 3, **(2012)** September, pp. 27-48.

[10] S. Staniford, V. Paxson and N. Weaver, "How to Own the Internet in Your Spare Time", Proc. of the 11th USENIX Security Symposium, **(2002)**.

Authors

Wang Xiaopeng, Engineer, he is working for Harbin Institute of Technology (abstract as HIT). His research is mainly on informa security, network security.



Wang Bailing is working for Harbin Institute of Technology (abstract as HIT) as an associate professor. He got the Ph.D. degree from HIT in 2006. His research is mainly on information security, network security, parallel computing.

Liu Yang, Associate Professor, his research fields include Network information Security Technology, Internet of Things Security Technology, etc. He has participated in many projects of Ministry of Information Industry and National Science, and he has published over 20 academic papers in journals and conferences both home and abroad.

He Hui is working for Harbin Institute of Technology at Weihai as an engineer. His research is mainly on dependable computing, embedded computing.