VACCINE: War of the Worms in Wired and Wireless Networks

Sapon Tanachaiwiwat and Ahmed Helmy
Department of Electrical Engineering
University of Southern California, CA, 90089
{tanachai, helmy}@usc.edu

Abstract*—The highlight of worm outbreaks in 2004 was a new phenomenon called 'War of the Worms' between NetSky, Bagle and MyDoom worm variants. Their aftermaths caused the record-high of 12 outbreaks in first quarter alone. This war created complex interactions among worms referring to one worm terminating another worm. In this paper, we try to answer the following questions: How much does this scenario affect individual worm propagation?, How can one worm win this war?, How do other factors such as mobility and protocol affect worm interaction? And how can we use worms as a defense mechanism? We propose a new worm propagation model (based upon and extending beyond the epidemic model) focusing on worm interaction, which dramatically alters the phase transition characteristics of single-type worm propagation. We validate our worm interaction model using realistic data and extensive ns-2 simulations. This study provides the first work to compare worm propagation and interaction of multiple types of worms in wired and wireless networks. The main finding of this study is that for worms to survive, they must terminate each other with balanced speed. Based on this study, we believe there is great potential for a new security paradigm to use non-malicious worms to fight malicious worms in what is similar to network vaccination.

I. INTRODUCTION

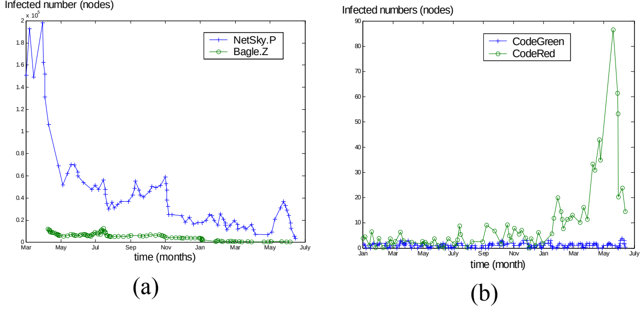
Worms represent a major threat to everyone using the Internet. Recently, there have been several worm attacks including NetSkys, Bagles and MyDooms [4]. Worms are usually combined with other serious malicious codes such as viruses, Trojans, and backdoors. Worms can be categorized as network worms and email worms. Network worms such as Code Red, Nimda and Sasser are user-independent; they scan vulnerable machines and infect them immediately. Mass-mailing worms such as Melissa, Love Bugs, NetSky, and Bagle, however, usually require users' interaction by the use of email attachments or shared files in peer-to-peer networks. Recently the first wireless worm, Cabir, has also propagated into mobile networks via blue tooth. This worm can seriously deplete the power of handheld devices. It also requires users to open attached file ".sis", similar to the email worm scheme. Several worm propagation models have been investigated in earlier work [2, 7]. However, those worm propagation models have not considered the interaction among different worm types, and, as we shall show, are inadequate to model war of the worms.

In 2004, majority of worm outbreaks are caused by the "War of the Worms" between NetSky, Bagle and MyDoom. The Bagle worms caused 15 outbreaks, NetSky 7 and MyDoom is 3 [4]. This war caused the highest outbreaks in one quarter with 12 outbreaks. The war of the worms creates unprecedented dynamic and complex scenarios. Our study shows that the interaction causes significant change in the traditional one-type propagation pattern. Furthermore, different types of interactions, i.e. indirect, one-sided or two-sided, show entirely different patterns. Originally propagation patterns of worms follow variants of phase transition patterns. Those variations are caused by human intervention and network congestion [7]. In some cases, however, worm propagation does not follow epidemic-based models. Fig.1 shows the number of infected hosts (based on real user reports [4]), which does not show the phase transition characteristic.

Worm interaction refers to the scenario where worms terminate other worms. One-sided interaction means one worm type terminating other worm type (Prey/Predator). Two-sided interaction means two worm types terminating each other (Predator/Predator). Indirect interaction means two worm types simply coexist without terminating each other. We develop a novel worm interaction model (Section II) extending the epidemic model [1]. We further study how worms interact in various types of scenarios including wired and wireless networks. We investigate whether non-malicious worms can be used to terminate malicious worm similar to Code Green terminating Code Red. However, we find that simply injecting a worm to fight back might not be adequate, but the worm must fight back with a scan rate greater than that of the malicious worm. Based on the insight developed in our study, we propose a high-level protocol framework called **VACCINE** (*Virus Combat via Coexistence and INtEraction*) which presents a new paradigm of network security that fights worms using controlled non-malicious worms.

Our contributions in this paper are

- We build new worm interaction models. We validate our models through extensive simulations. We consider a rich set of parameters including wired and wireless topology with different types of interactions.
- Based on our analysis, we conclude that for worms to survive in two-sided interaction scenarios, they must terminate each other with balanced scan rate. Moreover, for one-sided interaction, surprisingly the predator must be more aggressive than the predator in the two-sided interaction to terminate all opponents. Also, a small delay in deploying security countermeasures can cause significant drop in worm removal effectiveness.
- Based on the insight developed in this study, we propose a new paradigm for network security through the **VACCINE** protocol framework and provide guidelines for designing such protocol in the future.



(a)

(b)

Figure. 1 One-year infected numbers of famous interacting worms (a) NetSky.Q and Bagle.Z (b) Code Green and Code Red [4] do not show phase transition characteristic usually observed when using traditional epidemic models.

II. WORM INTERACTION MODEL

We aim to build a worm propagation model that captures worm interaction as a key factor. The basic epidemic model [1] cannot directly explain such interaction (see II.B and simulation results in Section III). Hence our model builds upon and extends beyond the conventional epidemic model to accommodate the notion of interaction.

The basic operation of a worm is to find susceptible nodes to be infected. The main goal of attackers is to have their worms infect the largest amount of hosts in the least amount of time. However, recently the goal of attackers, e.g. NetSky worm, has been expanded to eliminate opposing worms. NetSky worms terminate multiple types of worms such as MyDoom, MiMail and Bagle. Only resilient Bagle worms fight NetSky and hence the two-sided interaction occurs. Thus we want to investigate the worm propagation behavior caused by this and other types of interactions. Moreover, we want to find out whether the interaction makes the infected number of hosts deviate significantly from the basic epidemic model. We choose to use two generic types of interacting worms (i.e. Type A and B) as our basis throughout the paper.

We assume that both types share the same characteristic of infection preference. Moreover, each worm type has complete knowledge of local network address range. Every node is susceptible to both types of worms.

Next we introduce worm interaction factors: (a) Scan rate ratio and (b) Initial infection ratio. Then we explain the basic epidemic model and related variables. After that we extend the basic epidemic model to build Worm Interaction Model for (i) indirect, (ii) one-sided and (iii) two-sided interaction (We focus on competitive interaction only as opposed to collaborative interaction).

A. Worm interaction factors

Two proposed worm interaction factors of worm propagation model are defined and investigated.

- **Scan rate ratio**

Scan rate ratio is the ratio of scan rate of one worm type to another worm type. Let Γ_{BA} be a scan rate ratio of worm type B to type A.

$$\Gamma_{BA} = \frac{SR_B}{SR_A} \tag{1}$$

where SR_B and SR_A = scan rates of worm type B and A.

- **Initial infected host ratio (Hit list size ratio)**

Initial infected host ratio is the ratio of initial infected host of one worm type to another worm type. Let Λ_{BA} be an initial infected host ratio of worm type B to type A

$$\Lambda_{BA} = \frac{I_{B(0)}}{I_{A(0)}} \tag{2}$$

where $I_{B(0)}$ and $I_{A(0)}$ = number of initial infected hosts of worm type A and B at their initial released times.

B. Epidemic Model

From [1], the basic epidemic model which was developed for the study of biological infectious diseases also has been used to explain the behavior of self-replicating network worms [5]. The rate of infection increases when either effective contact rate of the disease or current susceptible hosts or current number of infected hosts increases (or all of them increase). The effective contact rate was assumed to be constant during infection period. Let N be the size of population, $I(t)$ be the number of infected hosts at time t, β be effective contact rate (The effective contact rate is derived from the ratio of scan rate and size of population.), and $S(t)$ which equals to N- $I(t)$ be the susceptible hosts.

The fundamental epidemic equation is shown below.

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)] \tag{3}$$

In (4), let $R(t)$ be the number of removed hosts i.e. immune or dead hosts and γ be the removal rate, and $I(t)$ be infectious hosts which can infect others then

$$\frac{dR(t)}{dt} = \gamma I(t) \tag{4}$$

$$I(t) = N - S(t) \tag{5}$$

C. Interaction Types

To understand the interaction types, the following terms are defined.

Predator: A worm type that terminates another worm type.

Prey: A worm type that is terminated by another worm type.

A predator can also be a prey at the same time for some other type of worm.

- **Indirect interaction**

When there is no direct interaction among worm types (i.e., without predators or preys), worms simply compete for available resources such as bandwidth and CPUs of the same network or hosts. Worms' propagations are only influenced by shared resources. Their infection number and susceptible hosts of one worm type are not directly dependent on those of another type. If we assume there is no worm removal from human action or worm; then both γ_B and γ_A (removal rate for worm type A and B) become 0 in the epidemic model equation (4). To confine our model to worm interaction only, then we assume no human intervention. The effective contact rate at time t is reduced exponentially by the congestion caused by the increase of infected hosts' traffic (for fixed scan rate). η describes the network congestion behavior [7]. Both types share the same network infrastructure and hence equally suffered by η. The infected hosts and susceptible hosts of type A and type B can be overlapped during infection.

- **One-sided interaction (Prey/Predator Model)**

When there is one prey and one predator worm, we consider this as one-sided interaction. Let A be preys and B be predators. Prey's infection rate is now decreased with the increase of predator's effective contact rate. Predator's infection rate and effective contact rate are still the same as of indirect interaction. Prey's removal rate depends on the number of predators $I_B(t)$, predator's scan rate SR_B, and the probability that predators find preys when infecting the susceptible hosts. Furthermore, prey's removal process will stop after predators infect all susceptible hosts.

- **Two-sided interaction (Predator/Predator Model)**

This two-sided interaction extends from the one-sided interaction. Now both of worms are predator and prey at the same time. We call them both simply predators. Their infection rates are now decreased with the increase of the other's effective contact rate. Key differences from previous two interactions is the condition $I_A(t) + I_B(t) \leq N$. Now the numbers of infected hosts are dependent on infection by the other type (if no patching is applied). When the Γ_{BA} is 1.0, the infection process will run indefinitely. The number of infected nodes will fluctuate around the half of possible infected nodes. If Γ_{BA} is not equal to 1.0, the slower worm will always be completely terminated, no matter Γ_{BA} will be.

III. SIMULATION RESULTS

To validate our Worm Interaction Model, we test the network worm propagation using ns-2 simulation. Our goal is to have better understanding of worm propagation in a rich set of environments. We simulate two types of worms, type A and type B (which may have different scan rates and initial number of infected hosts). We do not model human interaction but only focus on worm interaction and related network environments only. With small packet size, similar to Slammer worm, the simulated worm propagation is bandwidth-limited [5] which means its scan rate can be as fast as computers or networks could transmit packets.

Fig. 2 shows that, for one-sided interactions, predator worms are not effectively terminating prey worms even with high $\boldsymbol{\Gamma_{BA}}$, if they do not deploy patch (or false signature) to prevent re-infection from prey worms.

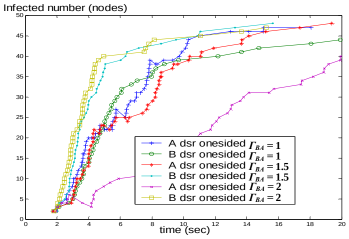


Figure 2. The worm removal in one-sided interactions without patching is not effective even with high $\boldsymbol{\Gamma_{BA}}$ on DSR network. It only slows down the opposing worms but does not eliminate them (wireless network, 50 nodes, random topology).

For two-sided interaction, fig. 3 shows significantly different characteristics from the epidemic model especially in wireless network. Fig. 4 shows equilibrium of two-sided interaction in wired network.

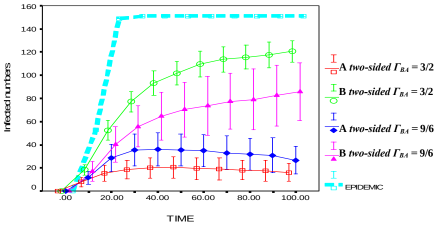


Figure. 3 Effects of scan rate ratio on two-sided interactions on DSR networks are shown. The epidemic model cannot directly explain the interaction effect. Scan rate ratio of type B to A (Γ_{BA}) is the major factor for predicting worm interaction pattern at Γ_{BA} = 1.5 (3:2 and 9:6 scan/sec) in wireless network, 150 nodes, random topology.

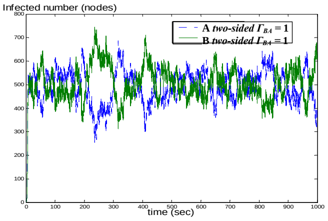


Figure. 4 Effect of scan rate ratio on two-sided interactions in large wired local area network (star-topology, 1000 nodes) is clearly shown here. With equal scan rate of type B and A, the interaction will run indefinitely, otherwise it will diminish proportionally to Γ_{BA}. SR_A = 2 scan/sec, SR_B = 2 scan/sec (Γ_{BA}=1.0)

IV. VACCINE FRAMEWORK

From the lessons we learn from this work, we expect non-malicious worm to be an effective tool to combat malicious worm with greater *scan rate*. However, to know the scan rate of infected malicious worm is not easy task. To learn such scan rate is not to terminate the malicious worm immediately. Rather we observe the infected machine or transforming the original malicious code to anti-worm code which contain original attack strategy. Unless applicable patch is applied to the infected host, the hosts may be re-infected. The patch can be carried with non-malicious worm's payload or downloaded from trusted anti-virus sites. The non-malicious worm's signature should be known by intrusion detection system (local network or ISP level) to prevent their termination or accidental leakage. We propose a dynamic incremental scan rate scheme for the non-malicious worms to adapt to the malicious worm's scan rate. Initial results are shown in Fig.5.

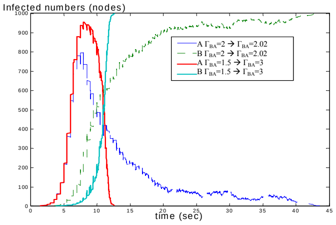


Figure 5. Effects of delayed removal on two-sided interaction with dynamic incremental scan rate (DIS) are shown. Once DIS is deployed with appropriate increasing factor, it shows immediate improvement. A is a malicious worm, B is a non-malicious worm (wired network, star topology, 1000 nodes)

V. SUMMARY AND FUTURE WORK

Based on our worm interaction study, we find that worm interaction causes drastic change in the worm propagation model. Such interaction cannot be explained by earlier works based on the epidemic model even when the removal process is used. We identify three types of interactions: indirect interaction, one-sided interaction, and two-sided interaction that show significantly different patterns of propagation. We developed a new worm propagation model which is validated through extensive simulations. Interactions have more impact on mobile nodes than on wired network. With indirect interaction, faster worms always completely infect all hosts first but slower worms rapidly gain the momentum after that. Hence, slower worm will not suffer much for having such lower scan rate. With one-sided interaction, surprisingly the victim worms can not be eliminated easily unless the predator has extremely high *scan rate ratio* even more than *scan rate ratio* of the two-sided interaction. For two-sided interaction, both worm types will survive forever if they terminate one another with equal scan rate. Scan rate ratio has much more impact on worm propagation pattern than initial infected host ratio. We shall further develop the VACCINE architecture, protocol and evaluate it in a test bed. Worm interactions in different mobility models will be explored. More details on our worm interaction models and simulation results can be found in [6].

VI. REFERENCES

[1] J.C.Frauenthal. *Mathematical Modeling in Epidemiology*. Springer-Verlag,New York,1988

[2] A. Ganesh, L. Massoulie and D. Towsley, *The Effect of Network Topology on the Spread of Epidemics*, in INFOCOM 2005.

[3] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, "Internet Quarantine: Requirements for Containing Self Propagating Code", in INFOCOM 2003.

[4] Trend Micro Annual Virus Report 2004 http://www.trendmicro.com

[5] N. Weaver, S. Staniford, V. Paxson, *Very Fast Containment of Scanning Worms*, 13th USENIX Security Symposium, Aug 2004

[6] S. Tanachaiwiwat, A. Helmy, "*VACCINE: War of the Worms in Wired and Wireless Networks*", Technical Report CS 05-859, Computer Science Department, USC

[7] C. C. Zou, W. Gong and D. Towsley, " *Code red worm propagation modeling and analysis*" Proceedings of the 9th ACM CCS 2002