This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2005 proceedings.

On Defending Peer-to-Peer System-based Active Worm Attacks

Wei Yu, Sriram Chellappan[+], Xun Wang [+], Dong Xuan[+]

Computer Science Department,
Texas A&M University, College Station, TX 77843
Email: {weiyu@cs.tamu.edu}
[+]Department of Computer Science and Engineering,
The Ohio State University, Columbus, OH 43210
Email: [+]{chellapp, wangxu , xuan}@cse.ohio-state.edu}

Abstract—***Recent active worm propagation events show that active worms can spread in an automated fashion and flood the Internet in a very short period of time. Our previous results show that P2P systems with large number of hosts can be a potential vehicle for the active worm attacker to achieve fast worm propagation in the Internet. In this paper, we propose a region-based active immunization defense strategy in P2P systems to fight against P2P-based active worm attacks. We develop an analytical approach to evaluate the efficiency of our proposed defense strategy. Our numerical analysis results show that: although P2P-based attacks can significantly improve the attack performance by attacking vulnerable P2P systems, our proposed defense strategy can effectively slow down the worm propagation. We also observe that defense parameters such as defense list size, worm detection success ratio, and immunization rate have sigificant impacts on the performance of our defense strategy.***

Keywords—P2P System, Active Worm Defense

I. INTRODUCTION

Active worms continue to plague the Internet causing billions of dollars in economic damages. Our previous study shows that P2P systems can be a potential vehicle for the active worm attacker to achieve fast propagation [1]. In this paper, we design, develop and analyze defense schemes to fight against such P2P-based active worm attacks. An active worm is defined as a self-propagating and self-replicating network program which can exploit some vulnerability of network hosts and infect other network hosts without human intervention. Active worms have been persistent security threats on the Internet, especially during the last few years. In 2001, the *Code-Red* worm infected 360,000 hosts in 10 hours and caused more than $1.2 billion in economic damage in the first 10 days [2] and the *Slammer* worm in early 2003 achieved a faster propagation rate [3].

P2P computing has been paid much attention in recent past, as it can scalably provide Internet-scale resource sharing. A P2P networked system is a group of Internet nodes that construct their own special-purpose overlay network. The recent surge of P2P applications can be observed by following statistical data collected on Nov 3, 2004: there are a total of 2,256,612 users in the FastTrack P2P system, 2,401,835 users in the eDonkey P2P system, and 1,258,775 users in the Warez P2P system [4]. The P2P systems can become a potential launch pad for attackers to rapidly propagate worms. The key features of P2P systems that worm attackers exploit to achieve fast propagation are the rich and diverse connectivity of the P2P systems, the large user population, and file sharing. Recent worm attack incidents confirm this (e.g., MyDoom worm spreading over the Kazaa P2P system [5].)

Much work has been done in analyzing and modeling virus/worms such as, computer virus model [6], active worm spreading modeling [7], Malware spreading dynamics [8], Code-Red worm modeling [2], and future worm analysis [9]. Besides the worm modeling, some work has been done in defending active worm, such as, cooperative response strategies to prevent the worm propagation [10], Containment-based worm defense [11], and Quarantine-based worm defense [12]. In our previous work [1], we study two P2P-based attack strategies and develop an analytical approach to evaluate the impact of P2P-based attack mechanisms and P2P system related factors such as P2P system topology degree and the P2P system structured/unstructured properties. To the best of our knowledge, there has been no effort devoted exclusively to study the active worm defense in the P2P systems in order to thwart P2P-based worm attacks.

The goal of our work is to propose an effective defense strategy to combat P2P-based worm attacks. We first propose a distributed region-based defense system, where some defense hosts in the P2P perform the task of defense. Our defense approach follows the methodology of adaptive immune systems in biology, i.e., white blood cells called *Lymphocytes* cooperate with each other to detect harmful pathogens and assist in the elimination of *pathogens* in the human body by means of *active-immunization*. Here, our defense hosts conduct the role of lymphocytes and work together to eliminate active worms. We then develop an analytical methodology that can be used qualitatively to better understand the worm defense performance in the P2P system.

The rest of paper is organized as follows: P2P-based active worm attacks are introduced in Section II. In Section III, we study the worm defense strategy, model and analyze the defense system. Numerical analysis results are given in Section IV. Conclusion of this paper and future work are discussed in Section V.

II. P2P-BASED ACTIVE WORM ATTACKS

In this paper, we consider the following three attack models: a purely random-based attack which has been adopted by many worms [2][3] and two P2P-based attack strategies - an offline P2P-based approach and an online P2P-based approach.

1) Pure Random-based Scan (PRS): In this strategy, worm-infected hosts do not have any prior vulnerability knowledge or active/ inactive information of other hosts. The worm host randomly selects the IP addresses of victim targets from the global IP address space and launches the worm attack. When the new host is infected, it continuously attacks the Internet by using the same methodology. In this paper, this attack strategy is treated as the baseline attack, as it has been widely adopted by many worms such as, Code-Red and Slammer.

2) Offline P2P-based Hit-list Scan (OPHLS): In this strategy, we assume that worm-infected hosts collect all IP address information of the P2P system offline, denoted as the hit-list. Worm-infected hosts launch the attack against hosts in the hit-list. In this attack strategy, all newly infected hosts

This work was partially supported by NSF under grant No. ACI-0329155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

continuously attack the hit-list until all hosts in the hit-list have been scanned. Then, all worm-infected hosts continue to attack the Internet via PRS.

3) Online P2P-based Scan (OPS): In this strategy, after joining the P2P system, the worm-infected host immediately initiates an attack against its P2P neighbors with its full attack capacity. At the same time, the worm-infected hosts can also attack the Internet via PRS if extra attack capacity is available. To illustrate this, an example is given: Say A_1 is the worm infected host with attack capability 6 (i.e., it is able to attack 6 hosts simultaneously) and A_1 has three P2P neighbors B_1, B_2, and B_3. A_1 then starts to use 50% of its attack capability to attack B_1, B_2, and B_3 and the rest of the attack capability (50%) to attack the Internet via PRS. Assuming that B_2 and B_3 are vulnerable hosts and infected, these two newly infected hosts will continuously attack their P2P neighbors and the Internet by repeating the attack cycle of A_1. After that, A_1 will use 100% of its attack capability to attack the Internet via PRS.

Due to space limitations, we do not include detailed analysis of the above worm attack approaches. Interested readers can find the details in [1].

III. DEFENDING P2P-BASED ACTIVE WORM ATTACKS

In this section, we first introduce the worm defense strategy which combats two P2P-based worm attacks discussed in Section II. Then we model and analyze our defense system.

A. Worm Defense Strategy

The goal of our work here is to design an effective defense strategy against P2P-based worm attacks. We first propose a distributed region-based defense system, where some defense hosts in P2P systems perform the task of defense. Based on the defense role, defense hosts are classified into two categories: one is the normal defense host and the other is the region defense leader. The normal defense host just performs the local worm detection, reports the local worm abnormal information to the region leader, and executes the defense command from the defense region leader. The region leader host can determine the presence of a worm attack on the defense region based on gathered information.

Our defense follows the methodology of adaptive immune systems in biology where, white blood cells called *Lymphocytes* cooperating with each other to detect harmful pathogens and assist in the elimination of *pathogens* in the human body by means of *active-immunization*. Here, our defense hosts assume the role of lymphocytes and work together to eliminate active worms.

The worm detection component in each defense host proactively pre-analyzes the incoming/outgoing traffic and reports preliminary information or alarms to its defense region leader. The region leader can fuse the collected information based on correlation mechanisms, i.e., behavior similarity to identify the attack due to specific ports being scanned repetitively, etc. With the information correlation, the defense region leader can estimate whether the defense region is under worm attack based on the worm detection rule, i.e., at least K defense hosts are under the worm attack.

After the worm attack is detected and the worm infected region is identified, worm response will be performed by the defense hosts associated with the defense region. Similar to Microsoft shield [13] and IBM worm killer signal [14], the P2P defense host has lightweight capability to perform active defense i.e., counter-worm host immunization, which reduces the number of infected/vulnerable hosts during the attack run-time. This active-based defense strategy is also motivated by following real anti-worm examples from recent years: the counter-worm (Welchia) was launched to generate simple patching and immunize hosts infected by Blaster worm [15], CRClean counter-Worm was designed to add a filter to block the worm traffic and immunize the hosts that attempted to attack [16]. In general, when the target host (note that it can be vulnerable but uninfected or infected) being immunized by the defense host, the target host becomes a non-vulnerable host.

B. Model Parameters

In order to formally analyze defense system performance in the P2P systems, we list the following parameters which have the largest impact on worm defense performance.

1) Attack and P2P Parameters: a) The attack scan rate - S and the Internet's initial worm infected instances - M_0: these two parameters represent the attack capability from the worm attacker perspective. Intuitively, the larger these values are, the faster the worm propagates. *b) P2P Topology degree*: It defines the number of P2P neighbors maintained by the P2P host locally. *c) Size of P2P system*: It defines the number of hosts in the P2P system. It will have an impact on both offline and online P2P-based attack strategies.

ii) Defense parameters: a) Defense list size: It defines the set of P2P hosts conducting the worm defense activity in the P2P system. *b) The worm detection success ratio*: It defines the probability for the worm detection software (installed at the single defense host) to successfully detect the worm attack. Similar to the traditional intrusion detection software, worm detection software also has certain false alarm and false positive rates. This parameter models the general properties of intrusion detection software. *c) The worm defense region size*: It models a defense region with G P2P defense hosts within g P2P overlay hops. To simplify our analysis, we consider the defense region size G as the unit for both worm detection and anti-worm defense. *d) The worm defense immunization rate*: It defines the rate which the defense hosts can initiate the anti-worm reaction simultaneously to immunize other P2P hosts. Table 1 lists all notations for the worm propagation and defense modeling.

T	Total IP addresses in the Internet
S	Scan rate (number of hosts per unit time that the worm can simultaneously try to scan)
M_0	Initial number of infected hosts
P_1	Probability of IP addresses being utilized by hosts
P_2	Probability of real host in the Internet being vulnerable to worm infection
P_3	Probability of hosts in the P2P system to be vulnerable to worm infection
R_1	Size of the 'P2P' system
θ	Topology degree of the structured P2P system
$M(i)$	Number of infected hosts at time i in the whole Internet
$N(i)$	Number of vulnerable hosts at time i in the whole Internet
$E(i)$	Number of newly infected hosts added at time i in the whole Internet (initial value E(0)=0)
$M(i,X)$	Number of infected hosts at time i, where M(i, 0) is the number of infected hosts in the 'non-P2P' system (hosts not in any P2P system) and M(i, 1) is the number of infected hosts in the 'P2P' system.
$N(i,X)$	Number of vulnerable hosts at time i, where N(i, 0) is the number of vulnerable hosts in the 'non-P2P' system and N(i, 1) is the number of vulnerable host in the 'P2P'

	system (N(0, 0) = $T*P_1*P_2$ is the number of initial vulnerable hosts in 'non-P2P' system and N(0, 1) = R_1*P_3 is the number initial vulnerable hosts in the 'P2P' system)
E(i,X)	Number of newly infected hosts added at time *i*, where *E(i,0)* is the number of newly infected hosts added at time *i* in the 'non-P2P' system and *E(i,1)* is the number of newly infected hosts added at time *i* in the 'P2P' system
H	The threshold value for the threshold-based worm detection scheme
P	The portion of P2P hosts selected in the defense list, which construct the defense overlay in the 'P2P' system
P_s	The probability of defense hosts successfully generates alarms
D	The time taken for the defense region to detect the worm attack
G	Defense region size
L	The immunization rate for the anti-worm defense

Table 1: Notations for Worm Defense Modeling in the P2P System

C. Assumptions

We assume that there are two logical systems: one is called a 'P2P' system, which generalizes P2P systems in the Internet, and the other is called a 'non-P2P' system, which represents the rest of Internet. As our analysis considers the average case, we assume that each host in the 'P2P' system or 'non-P2P' system has a certain probability to be vulnerable. At initial time, we assume that there are a certain number of infected hosts are in the 'P2P' system.

Regarding to the worm defense in the 'P2P' system, we assume that we can deploy the worm defense software at a number of hosts in the 'P2P' system. We do not consider the possibility that defense hosts immunize the hosts in 'non-P2P' system. We assume that when a P2P host receives the immunization reaction from the defense host it becomes immune immediately. Similar to the worm attack victim selection for the PRS, we assume that immunized P2P hosts are also evenly distributed in the defense region.

D. Defense Analysis

We now describe the analysis of the P2P-based attack and defense strategy using discrete time to conduct recursive analysis and approximate the worm propagation [1]. In the following, we list several theorems which present the formulas to compute *E(i,1)*, *M(i,1)* and *N(i,1)* under defending different P2P-based worm attacks. Due to the space limitation, we only list the result of defending Offline P2P-based hit-list scan and Online P2P-based scan for Structured P2P system.

1) Defending Offline P2P-based Hit-list Scan (OPHLS_DE)

Theorem 1: For the *OPHLS* approach, with $M(i,1)$, $N(i,1)$, $M(i,0)$, and $N(i,0)$ at time i in the 'P2P' system, the next tick will have

$$M(i+1,1)=\begin{cases} M(i,1)+E(i+1,1), & i<D \\ M(i,1)+E(i+1,1)-P*L\dfrac{M(i,1)}{P_3} & i\geq D \end{cases} \quad (1)$$

$$N(i+1,1)=\begin{cases} N(i,1)-E(i+1,1), & i<D \\ N(i,1)-E(i+1,1)-R_1P*L(1-\dfrac{M(i,1)}{R_1P_3}) & i\geq D \end{cases} \quad (2)$$

$$M(i+1,0)=M(i,0)+E(i+1,0),$$
$$N(i+1,0)=N(i,0)-E(i+1,0), \quad (3),$$

where, $D=\min(i)$ satisfying $X(i)\geq H$,

$$X(i+1)=X(i)+(G*P-X(i))P_s(1-(1-\frac{1}{P})^{S*M(i,1)G/R_1}$$

$$E(i+1,1)=\begin{cases} N(i,1)[1-(1-\dfrac{1}{R_1})^{S*M(i,1)}] & if \quad M(i,1)<R_1P_3 \\ 0 & if \quad M(i,1)\geq R_1P_3 \end{cases}$$

$$E(i+1,0)=\begin{cases} 0 & if \quad M(i,1)<R_1P_3 \\ N(i,0)[1-(1-\dfrac{1}{T})^{S*M(i,0)+S*M(k,1)}] & if \quad M(i,1)\geq R_1P_3 \end{cases}$$

$M(0,1)=M_0$, $M(0,0)=0$, $N(0,1)=R_1P_3$, $G=\sum_{t=0}^{g}\theta^t$,

$N(k,0)=T*P_1*P_2-R_1*P_3$, $M(k,0)=M(k-1,1)$,

($k=\min(i)$ for i satisfying the condition $M(i,1)\geq R_1P_3$),

$M(i)=M(i,1)+M(i,0)$, $N(i)=N(i,1)+N(i,0)$.

Proof: There are $N(0,1)=R_1P_3$ vulnerable hosts in the 'P2P' system and the size of the 'P2P' system is R_1. Since there are *N(i,1)* vulnerable hosts that have not been infected, *1* scan adds the following newly infected hosts in the 'P2P' system at time i is $N(i,1)[1-(1-\frac{1}{R_1})^1]$. There are $S*M(i,1)$ scans at time *i*, thus we can easily get

$$E(i+1,1)=N(i,1)[1-(1-\frac{1}{R_1})^{S*M(i,1)}], if \quad M(i,1)<R_1P_3. \quad (4).$$

When $M(i,1)\geq R_1P_3$, the 'P2P' system has been fully attacked. We have

$$E(i+1,1)=0 \quad if \quad M(i,1)\geq R_1P_3. \quad (5)$$

As each defense region includes P2P hosts in g P2P hops and the P2P system topology degree is θ, the number of hosts in each defense region can be approximated as $G=\sum_{t=0}^{g}\theta^t$. We define P_i as the probability of the defense region being scanned. As the P2P system has R_1/G defense regions, there are $S*M(i,1)*G/R_1$ scans being used to attack a single defense region and P_i can be calculated as following:

$$P_i=1-(1-\frac{1}{P})^{SM(i,1)G/R_1} \quad (6)$$

Let's define *X(i)* (*X(0)=0*) as the number of defense hosts that have been scanned by the worm attack at time i. Considering the worm detection software detection probability P_s, *X(i+1)* can be calculated by

$$X(i+1)=X(i)+(G*P-X(i))P_iP_s \quad (7)$$

Considering that the region leader uses the threshold-based worm detection scheme, the average worm detection delay can be calculated as

$$D=\min(i) \text{ satisfying } X(i)\geq H \quad (8)$$

When the worm attacker is taking an offline-based approach and there are total *M(i,1)* infected hosts in the 'P2P' system at time i, the average infection degree (as the percentage of vulnerable hosts that has been infected in the 'P2P' system) is $M(i,1)/(R_1*P_3)$. With a worm immunization rate L and the effective P2P defense host number R_1*P, the number of vulnerable hosts which have not been infected and can be immunized by the defense reaction at time i is

$$R_1P*L(1-\frac{M(i,1)}{R_1P_3}) \quad (9)$$

Thus, considering the worm detection system delay *D*, the recursive formula to calculate *N(i,1)* is given by

$$N(i+1,1)=\begin{cases}N(i,1)-E(i+1,1), & i<D\\ N(i,1)-E(i+1,1)-R_1P*L(1-\dfrac{M(i)}{R_1P_3}) & i\geq D\end{cases} \quad (10)$$

Similarly, the number of worm infected hosts which will be immunized by our defense reaction is

$$R_1PL\frac{M(i,1)}{R_1P_3}=P*L\frac{M(i,1)}{P_3} \quad (11)$$

Thus, the recursive function to calculate *M(i)* is

$$M(i+1,1)=\begin{cases}M(i,1)+E(i+1,1), & i<D\\ M(i,1)-E(i+1,1)-P*L\dfrac{M(i,1)}{P_3} & i\geq D\end{cases} \quad (12)$$

The calculations of *E(i+1,0)*, *M(i+1,0)*, and *N(i+1,0)* are the same as the Theorem 2 in [1]. Q.E.D

2) Depending Online P2P-based scan for Structured P2P system (OPSS_DE)

Theorem 2: In the *OPSS* approach, with $M(i,1)$, $N(i,1)$, $M(i,0)$, and $N(i,0)$ at time i in the 'P2P' system, the next tick will have

$$M(i+1,1)=\begin{cases}M(i,1)+E(i+1,1), & i<D\\ M(i,1)+E(i+1,1)-\min\left(\left\lceil\dfrac{M(i,1)}{G*P_3}\right\rceil G*P,R_1P\right)*L*\dfrac{M(i,1)}{\left\lceil\frac{M(i,1)}{G*P_3}\right\rceil G*P_3} & i\geq D\end{cases} \quad (13)$$

$$N(i+1,1)=\begin{cases}N(i,1)-E(i+1,1), & i<D\\ N(i,1)-E(i+1,1)-\min\left(\left\lceil\dfrac{M(i,1)}{G*P_3}\right\rceil G*P,R_1P\right)*L*(1-\dfrac{M(i,1)}{\left\lceil\frac{M(i,1)}{G*P_3}\right\rceil G*P_3}) & i\geq D\end{cases} \quad (14)$$

$$M(i+1,0)=M(i,0)+E(i+1,0),$$
$$N(i+1,0)=N(i,0)-E(i+1,0), \quad (15),$$

where, $D=\min(i)$ satisfying $X(i)\geq H$,

$$X(i+1)=X(i)+(G*P-X(i))P_s(1-(1-\frac{1}{P})^{S*M(i,1)/\left\lceil\frac{M(i,1)}{G*P_3}\right\rceil}$$

$$E(i+1,0)=N(i,0)[1-(1-\frac{1}{T})^{(M(i,0)+M(i,1))*S-\min(\theta,S)*E(i,1)}],$$

$$E(i+1,0)=N(i,0)[1-(1-\frac{1}{R_1})^{\min(\theta,S)*E(i,1)}],$$

$$M(0,0)=0, M(0,1)=M_0, N(0,0)=T*P_1*P_2-R_1*P_3,$$

$$G=\sum_{t=0}^{g}\theta^t,\ N(0,1)=R_1*P_3,\ N(i)=N(i,1)+N(i,0).$$

Proof: With the OPSS worm infection result [1], we can get the result by using the similar procedures in Theorem 1.

IV. PERFORMANCE EVALUATIONS

A. Evaluation Model

1) Metrics: We define the following metrics to evaluate the worm propagation effectiveness - the worm infection ratio over time, which defines the time taken to successfully achieve the infection ratio – *infected host number/total vulnerable host number in the* Internet. From the worm defense perspective, the higher the performance value, the worse is the defense effect.

2) Evaluation Systems: i) System Parameters. The general system is defined by the nine tuple: <A, T, S, M_0, P_1, P_2, P_3, R_1, θ>, in particular defining the system configuration parameters, where *A* defines a three tuple of <*PRS, OPHLS, OPSS*> to identify different attack strategies with other parameters having the same definitions in Table 1. ii) *Worm defense*. The general worm defense system is defined by the six element tuple <*B, P, P_s, H, G, L*>, in particular defining the system defense configuration parameters, where *B* defines a tuple of <*OPHLS_DE, OPSS_DE*> to identify the defense systems for different attack strategies with other parameters having the same definitions in Table 1. We use numerical analysis to obtain our performance data.

B. Performance Results

In this section, we report the performance results along with observations. All the data shown start at time 45 (due to the infection ratio being very small in the time interval [0, 45] due to the large number of vulnerable hosts). In all the defense performance data, the general worm propagation system is configured as <*, 2^{32}, 6, 1, 0.25, 0.2, 0.2, 10000, 4 >.

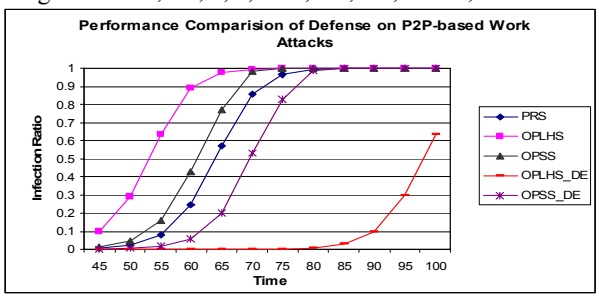

Figure 1: Performance Comparison of All Defense Strategies

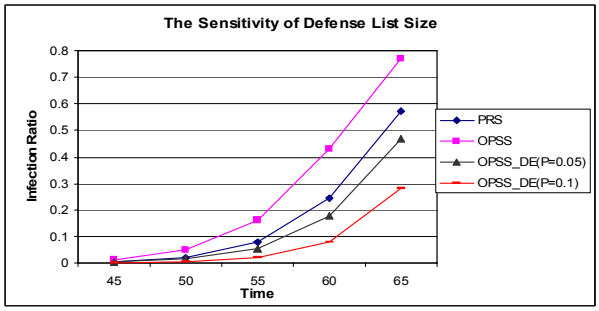

Figure 2: The Sensitivity of Defense List Size

1) Comparison among defense performance for different P2P-based attack strategies: Figure 1 shows the data for the sensitivity of attack performance for the corresponding defense system reacting to different attack strategies. The general worm defense system is configured as <*, *0.05, 0.5, 3, 500, 2*>. From this figure, we make following observations: a) Our defense strategy effectively slows down the worm propagation for both *OPLHS* and *OPSS* attack strategies. The result matches our expectation – our defense system can effectively immunize the number of both worm infected hosts and vulnerable hosts during the worm attack time, which significantly slows down the worm propagation in the whole Internet. Note that our simulated P2P system only has 10000 hosts, which is far smaller than total Internet IP addresses 232. We see that defending on P2P systems can only slow down the P2P-based worm propagation on the global Internet without changing the stable infected ratio. b) The defense perform on OPLHS strategy achieves better worm defense performance than *OPSS*. This can be explained – for the *OPLHS* attack strategy, almost all attack resources are applied to attack the P2P system. Our defense system can effectively decrease the number of both worm infected hosts and vulnerable hosts during the attack time, which can significantly slow down the

worm propagation in the Internet. For the *OPSS* attack strategy, the worm is attacking the 'P2P' system through the P2P topology and some attack resources are still applied to the 'non-P2P' system. Thus, the defense performance of *OPSS* is worse than *OPLHS*.

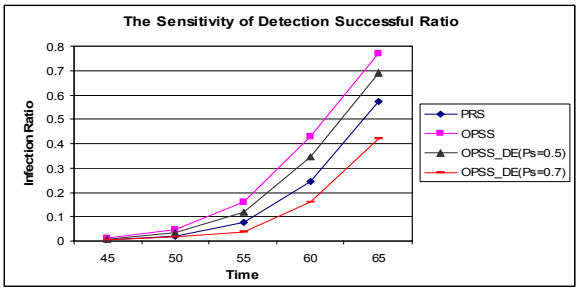

Figure 3: The Sensitivity of Detection Successful Ratio

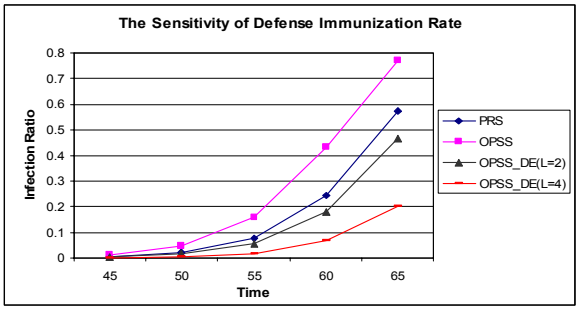

Figure 4: the Sensitivity Defense Immunization Rate

2) The sensitivity of defense list size: Figure 2 shows the data for the sensitivity of defense performance for different defense list sizes. The general defense system is configured as <*, *, *0.5, 3, 500, 2*>. In the legend, *OPSS_DE (#)* defines the P2P-based attacks for the structured P2P system with # portion of P2P hosts selected as the defense hosts. We make the following observations: For our defense strategy, an increase of defense list size achieves better defense performance. This matches our expectation – a larger defense lists size makes more P2P hosts involved in the worm defense reaction, which causes fast worm detection and stronger defense reaction. More infected and vulnerable P2P hosts are immunized and better worm defense performance is achieved.

3) The sensitivity of worm detection successful ratio: Figure 3 shows the data for the sensitivity of defense performance for different worm detection successful ratios. The general defense system is configured as <*, 0.05, *, 3, 500, 2*>. In the legend, *OPSS_DE (#)* defines the P2P-based attack for the structured P2P system with worm detection success ratio #. We make the following observations: For the P2P system worm defense strategy, an increase of the worm detection successful ratio achieves better defense performance. This matches our expectation - the larger worm detection success ratio achieves the fast worm detection, which causes the defense reaction to be triggered early. Thus, more infected and vulnerable P2P hosts become immune and the overall worm propagation slows down.

4) The sensitivity of defense immunization rate: Figure 4 shows the data for the sensitivity of defense performance for different defense immunization rates. The general defense system is configured as <*, 0.05, 0.5, 3, 500, *>. In the legend, *OPSS_DE (#)* defines the P2P-based attack for the structured P2P system with defense immunization rate #. We make the following observations: For our defense strategy, an increase in immunization rate slows down worm propagation performance. This matches our expectation – a larger worm immunization rate makes the worm defense reaction stronger, which causes more infected and vulnerable P2P hosts to be immunized in the given time. Thus, the overall worm propagation is slowed down.

V. Final Remarks and Future Work

We have studied an *active-immunization* scheme to defend against P2P-based worm attacks. In summary, our contributions include the following: 1) we design a region-based *active immunization* defense strategy; 2) we develop an analytical approach to analyze the efficiency of the defense performance and study defense parameters. Based on performance evaluation results, we obtain some observations: our proposed defense strategy can effectively slow down Internet worm propagation and some parameters related to worm defense have an impact on the worm defense.

This work can be extended in several ways: designing other effective worm detection schemes and intelligent defense strategies to effectively improve the defense performance, designing a fast worm Internet alarm system based on large and distributed P2P systems, and combining router-based worm defense approaches with our work to counter worm attack across the entire Internet.

References

[1] W. Yu, C. Boyer, S. Chellappan, and D. Xuan, "*Peer-to-Peer System-based Active Worm Attacks: Modeling and Analysis*", In Proceedings of IEEE International Conference on Communication (ICC), May 2005.

[2] C. C. Zhou, W. Gong, and D.Towsley, "*Code Red Worm Propagation Modeling and Analysis*", In 9-th ACM Conference on Computer and Communication Security (CCS), Nov. 18-22, Washington DC, USA, 2002.

[3] D. Moore, V. Paxson, and S. Savage, "*Inside the Slammer Worm*", IEEE Magazine of Security and Privacy, July, 2003.

[4] Slyck news, "*http://www.slyck.com*".

[5] Mydoom, "*http//www.f-secure.com/tools*".

[6] J. O. Kephart and S. R. White, "*Measuring and Modeling Computer Virus Prevalence*", In Proceedings of IEEE Symposium on Security and Privacy, 1993.

[7] Z. S. Chen, L.X. Gao, and K. Kwiat, "Modeling *the Spread of Active Worms*", In Proceedings of IEEE Infocom, 2003.

[8] M. Garetto, W.B. Gong, and D. Tonsley, "*Modeling Malware Spreading Dynamics*", In Proceedings of IEEE Infocom, 2003.

[9] S. Staniford, V. Paxson, and N. Weaver, "*How to Own the Internet in Your Spare Time*", In Proceedings of the 11-th USENIX Security Symposium, 2002.

[10]. D. Nojiri, J. Rowe, and K. Levitt, "*Cooperative Response Strategies for Large Scale Attack Mitigation*", In Proceedings of DARPA Information Survivability Conference and Exposition - Volume I, 2003.

[11] S. Staniford, "*Containment of Scanning Worms in Enterprise Network*", Journal of Computer Security, 2003.

[12] C. C. Zou, W. Gong, and D. Towsley, "*Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense*", *In Proceedings of IEEE Worm*, 2003.

[13] H. J. Wang, C. X. Guo, D. R. Simmon, and A. Zugenmaier, "*Shield Vulnerability-Driven Network Filters for Preventing Known Vulnerability Exploits*", In Proceedings of ACM SIGCOMM 2004, Portland, OR, August, 2004.

[14] J. O. Kephart and S. R. White, "*Measuring and Modeling Computer Virus Prevalence*", In Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, 1993.

[15] J. Leyden. "*Blaster variant offers 'fix' for pox-ridden Pcs*", http:// www.theregister.com/ 2003/08/19/, August 2003.

[16] M. Kern, "*Re: Codegreen beta release*", http:// www.securityfocus.com/ archive/82/211462, September 2001.