

Accelerating the Propagation of Active Worms by Employing Multiple Target Discovery Techniques

Xiang Fan, and Yang Xiang

School of Management and Information Systems
Centre for Intelligent and Networked Systems
Central Queensland University
North Rockhampton, Queensland 4701 Australia
{x.fan2, y.xiang}@cqu.edu.au

Abstract. Recently, active worms have done significant damage due to their rapid propagation over the Internet. We studied propagation mechanisms of active worms employing single target discovery technique and various combinations of two or three different target discovery techniques from attackers' perspective. We performed a series of simulation experiments to investigate their propagation characteristics under various scenarios. We found uniform scanning to be an indispensable elementary target discovery technique of active worms. Our major contributions in this paper are first, we proposed the discrete time deterministic Compensation Factor Adjusted Propagation (CFAP) model of active worms; and second, we suggested the combination of target discovery techniques that can best accelerate propagation of active worms discovered from results of the comprehensive simulations. The significance of this paper lies in it being very beneficial to understanding of propagation mechanisms of active worms, and thus building effective and efficient defense systems against their propagation.

Keywords: Network Security; Invasive Software; Worms; Propagation; Modeling

1 Introduction

Kienzle and Elder defined a worm as 'malicious code (standalone or file-infecting) that propagates over a network, with or without human assistance' [1]. Weaver et al. defined a computer worm as 'a program that self-propagates across a network exploiting security or policy flaws in widely-used services' [2]. In this paper, we define active worms as those which actively self-propagate across a network exploiting security or policy flaws in widely-used services by employing scanning, pre-generated target list, or internally generated target lists (target lists for short) as their target discovery technique. The Code Red worms of 2001 (Code-RedI v1, Code-RedI v2, and CodeRedII) employed various types of scanning as their target discovery techniques [3]. The Slammer (sometimes called Sapphire) worm of 2003 employed uniform scanning as its target discovery technique [4]. The most recent Witty worm of 2004 employed scanning as its target discovery technique as well [5]. If IP

addresses of vulnerable hosts could be obtained in advance, there exists an opportunity to employ pre-generated target list as a worm's target discovery technique. Pre-generated target list is also termed as 'hit-list' [6]. Internally generated target lists are lists found on infected hosts which contain information about other potential vulnerable hosts. The Morris Internet Worm of 1988 employed internally generated target lists as its target discovery technique [7].

Recently, active worms have done significant damage due to their rapid propagation over the Internet. For example, the Code Red worm caused about \$2.6 billion financial loss in July and August 2001 alone [8]. The situation of worm defenders will be worsened if worms stop propagation by using some self-stopping mechanisms [9] after they have successfully infected nearly all vulnerable hosts. For example [3], the Code Red worms propagated for a time, then stopped propagating, and then focused all of its intention on executing a Distributed Denial of Service (DDoS) [10] attack on a specific host.

According to Xiang et al. [11], an active worm is not limited to employing single target discovery technique only, and thus future active worms could employ multiple target discovery techniques simultaneously in an attempt to accelerate their propagation. To find an effective countermeasure against this sort of future worms, we studied propagation mechanisms of active worms employing single target discovery technique only, and a combination of two or three different target discovery techniques from attackers' perspective. We also performed a series of simulation experiments to investigate their propagation characteristics under various scenarios.

2 Related Work

Life cycle of a worm from when it is released to when it finishes infecting vulnerable hosts, consists of the initialization phase, the network propagation phase, and the payload activation phase [12]. In the network propagation phase, a worm attempts to infect its target hosts by performing a sequence of actions including target acquisition, network reconnaissance, attack, and infection. Since target acquisition and network reconnaissance together essentially dictate target discovery technique(s) employed by a worm, we derived the significance of target discovery techniques in shaping a worm's propagation characteristics from its life cycle in [11].

Scanning could be implemented differently, which leads to several different types such as uniform scanning, preferential scanning, sequential scanning [13], routable scanning [14], selective scanning [14], or importance scanning [15]. In the case where the distribution of vulnerable hosts is not available in advance, self-learning that information will be incorporated into the implementation of importance scanning [16]. An incomplete hit-list could be used to increase the number of initially infected hosts and thus accelerate a worm's propagation. A complete hit-list creates a 'flash' worm [17], capable of infecting all vulnerable hosts extremely rapidly. An active worm attacking a flaw in peer-to-peer applications could easily get lists of peers from their victims and use those peers as the basis of their attack, which gives an example of employing the internally generated target lists as one's target discovery technique.

We summarized the factor(s) improved by active worms employing the various target discovery techniques to accelerate their propagation in [11].

Mathematical models developed to model propagation of infectious diseases have been adapted to model propagation of computer worms [13]. In epidemiology area, both deterministic and stochastic models exist for modeling the spreading of infectious diseases [14-17]. In network security area, both deterministic and stochastic models of active worms based on their respective counterpart in epidemiology area have emerged. Deterministic models of active worms could be further divided into two categories: continuous time and discrete time.

For a finite population of size N , the classical simple epidemic model [13-16] could be defined by the following single differential equation:

$$\frac{dI(t)}{dt} = \beta I(t)[N - I(t)], \quad (1)$$

where $I(t)$ denotes the number of infectious hosts at time t ; and β stands for the pairwise rate of infection in epidemiology studies [17]. Let $i(t)$ stand for the fraction of the population that are infectious at time t , the following differential equation could be derived:

$$\frac{di(t)}{dt} = N\beta i(t)[1 - i(t)]. \quad (2)$$

Differential equation (2) has the following general analytical solution:

$$i(t) = \frac{e^{N\beta(t-T)}}{1 + e^{N\beta(t-T)}}, \quad (3)$$

which is the logistic equation. A particular analytical solution of differential equation (2) given its initial condition $i(0) = I(0) / N$ is as follows:

$$i(t) = \frac{I(0)}{I(0) + [N - I(0)]e^{-N\beta t}}. \quad (4)$$

The classical general epidemic model (Kermack-McKendrick model) [13-16] improves the classical simple epidemic model by considering removal of infectious hosts due to patching. The two-factor worm model [18] extends the classical general epidemic model by accounting for removal of susceptible hosts due to patching and considering the pairwise rate of infection as a variable rather than a constant. The Analytical Active Worm Propagation (AAWP) model [19] takes into account the time an infectious host takes to infect other hosts. The time to infect a host is an important factor for the spread of active worms [20]. Since propagation of active worms is a discrete event process, the discrete time deterministic model of active worms (the AAWP model) given above is more accurate than its continuous time counterparts in the deterministic regime.

Rohloff and Basar presented a stochastic density-dependent Markov jump process propagation model [21] for active worms employing the uniform scanning approach drawn from the field of epidemiology [14, 17]. Sellke et al. presented a stochastic Galton-Watson Markov branching process model [22] to characterize the propagation of active worms employing the uniform scanning approach.

3 Mathematical Analysis and the Proposed Model

For the classical simple epidemic model (1) given in the last section, Fig. 1 shows the dynamics of I_t -- denoted by $I(t)$ in equation (1) -- as time goes on for a certain set of parameters [23].

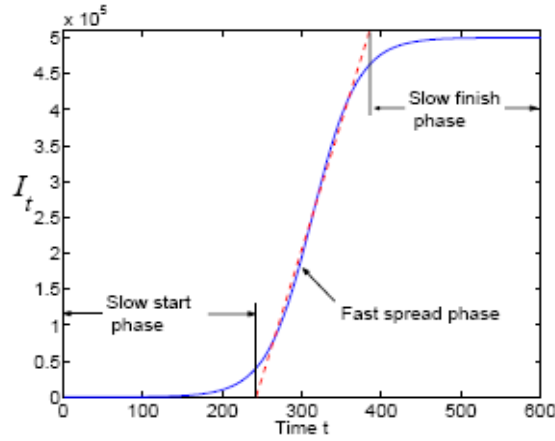


Fig. 1. Classical simple epidemic model

According to Fig. 1, we can roughly partition a worm's propagation into three phases: the slow start phase, the fast spread phase, and the slow finish phase. During the slow start phase, since $I_t \ll N$, model (1) becomes:

$$\frac{dI_t}{dt} \approx N\beta I_t, \quad (5)$$

which means that the number of infectious hosts increases exponentially approximately. After a certain number of susceptible hosts are infected and then participate in infecting others, the worm enters its fast spread phase where susceptible hosts are infected at a fast, nearly constant rate. When most susceptible hosts have been infected, the worm enters its slow finish phase because the few susceptible hosts leftover are difficult for the worm to find.

According to equation (4),

$$i_t = \frac{I_0}{I_0 + (N - I_0)e^{-N\beta t}}. \quad (6)$$

Letting $a = I_0$, $b = N - I_0$, and $c = -N\beta$ will transform equation (3.2) to:

$$i_t = \frac{a}{a + be^{ct}}. \quad (7)$$

The first derivative of is worked out and shown as follows:

$$\frac{di_t}{dt} = \frac{-abce^{ct}}{(a + be^{ct})^2}. \quad (8)$$

We can then work out the second derivative of and let it equal to 0:

$$\frac{d^2 i_t}{dt^2} = 0. \quad (9)$$

This will lead to $i_t = 50\%$. In other words, the maximum rate at which susceptible hosts are infected is achieved at the moment when 50% of susceptible hosts are infected.

We define fast spread as that with a rate not less than half of the maximum rate, which will lead to $i_t \approx 15\%$ and 85% . In other words, according to our definition of fast spread, when less than 15% of susceptible hosts are infected, the worm is in its slow start phase; when more than 85% of susceptible hosts are infected, the worm is in its slow finish phase; in between, the worm is in its fast spread phase.

It is obvious that in order to accelerate a worm's propagation, we must try to let the worm infect the first 15% susceptible hosts and enter its fast spread phase as soon as possible. On the other hand, the last 15% susceptible hosts leftover are not important for attackers if infection of 85% susceptible hosts will serve their purposes, which is usually the case.

Next, we present our proposed discrete time deterministic Compensation Factor Adjusted Propagation (CFAP) model of active worms employing uniform scanning as their target discovery technique. Let η and Ω stand for a worm's scanning rate and scanning space, respectively. Assume at time t , there exist I_t infectious hosts. Then at time $t + 1/\eta$, by assuming the probability of different infectious hosts hitting the same susceptible host to be 0, there will be $I_{t+1} = I_t + \Delta I_t$ infectious hosts, where

$$\Delta I_t = \frac{I_t(N - I_t)}{\Omega}. \quad (10)$$

During the process that more and more susceptible hosts are infected and then participate in infecting others, the probability of different infectious hosts hitting the same susceptible host is not a constant. Therefore, the actual number of newly infected hosts is less than that predicted by equation (10). Here, we introduce a compensation factor denoted by C_t to account for the difference between them, which varies as time goes on. Therefore, our discrete time deterministic CFAP model could be described by the following difference equation:

$$I_{t+1} = I_t + \frac{I_t(N - I_t)}{\Omega} - C_t. \quad (11)$$

There exist two methods to determine C_t , which are mathematical analysis or simulation. To predict C_t in a closed form (i.e., with no or very little iteration), mathematical analysis is usually employed. However, in some situations it could be very difficult, if not impossible, to derive a formula of C_t as a function of t . Then, we have to perform simulation experiments to find approximate value of C_t at each time t .

4 Simulation Experiments

There are four different ways to study the characteristics of a piece of self-propagating code, which are using test beds, performing real world experiments, creating mathematical models, and performing simulation experiments [24]. Among them, simulation experiments are often very effective tools to understand complex processes.

We systematically examined propagation characteristics of active worms employing single target discovery technique only, and a combination of two or three different target discovery techniques by conducting a series of simulation experiments under various scenarios. In order to reduce simulation time, we performed our simulation experiments in a class A /8 subnet. In other words, we used scale-down by a factor of $1/2^8$ to explore worm dynamics. According to Weaver et al. [25], scale-down introduces two notable artifacts: a bias towards more rapid propagation (propagation curve being shifted to the left due to scale-up of the density of initially infected hosts), and an increase in stochastic effects. Although these artifacts are significant, scale-down can still capture general behavior as long as the scale-down factor is not too extreme [25]. Therefore, scale-down is an efficient way to understand complex processes if the scale-down factor is appropriately chosen.

Our simulation experiments were based on the assumption that susceptible hosts are uniformly distributed in the above address space with vulnerability density approximately equivalent to that of the Slammer worm. We also assumed average worm scanning rate to be equivalent to the Slammer's as well. All simulations started with only 1 initially infected host, which is equivalent to 2^8 initially infected hosts in the Slammer's case.

In order to eliminate variation in results from different simulation runs for each certain scenario, we performed 10 simulation runs for each scenario using the simulator implemented in C programming language custom made for our simulation experiments. Results from all simulation runs are then averaged to produce final result for each scenario. We repeated our simulation experiments and got exactly the same average results, which indicated that stochastic effects could be eliminated, and the scale-down factor chosen was appropriate.

4.1 Simple Scenarios

Before we studied propagation characteristics of active worms employing a combination of two or three different target discovery techniques, we had studied propagation characteristics of active worms employing only one of the following target discovery techniques: uniform scanning; a complete hit-list; or internally generated target lists.

The above three kinds of active worms became the first 3 scenarios to be simulated, which are summarized in Table 1. Propagation rate of active worms employing uniform scanning only was our baseline to be compared to. Since an incomplete hit-list only cannot let a worm infect more hosts than those in the list, in practice it must be combined with other target discovery technique(s). Therefore, we chose a complete hit-list as one of the above 3 fundamental target discovery

techniques. Average size of internally generated target lists was a candidate factor whose influence on a worm's propagation characteristics was to be investigated.

Table 1. A summary of the 3 simple scenarios simulated

Scenario Type	Scenario Code	Target Discovery Technique Employed
Simple	U	Uniform Scanning Only
Simple	H100%	A Complete Hit-list Only
Simple	I1	Internally Generated Target Lists Only with Average Size of 1
Simple	I2	Internally Generated Target Lists Only with Average Size of 2
Simple	I3	Internally Generated Target Lists Only with Average Size of 3

Table 2. A summary of simulation results of the 3 simple scenarios

Scenario Type	Scenario Code	Average Time (in seconds) to Infect 99% Susceptible Hosts
Simple	U	142
Simple	H100%	1
Simple	I1	Indefinite (maximum infection rate 7% achieved in 1 second)
Simple	I2	Indefinite (maximum infection rate 79% achieved in 1 second)
Simple	I3	Indefinite (maximum infection rate 94% achieved in 1 second)

According to the results (Table 2) from our simulation experiments, a complete hit-list makes a worm propagate extremely rapidly. However, the feasibility of this approach is discounted by the extreme difficulties that will be encountered by attackers in gathering such a list. Due to their exactly same propagation mechanism, an incomplete hit-list lets a worm infect all susceptible hosts in the list as soon as a complete hit-list does. Therefore, an incomplete hit-list is a more feasible approach. It is obvious that active worms only employing internally generated target lists with average size not greater than 3 cannot achieve infection of over 99% susceptible hosts. An explanation to this phenomenon could be that less than 99% of all susceptible hosts are in the combined internally generated target lists of all susceptible hosts infected. However, average size of internally generated target lists has a great influence on the maximum infection rate (maximum percentage of susceptible hosts a worm can infect). A slight increase in average size from 1 to 3 leads to a dramatic increase in the maximum infection rate. Furthermore, maximum infection rates are achieved in 1 second for all average sizes (1, 2, or 3). As we mentioned earlier in this paper, infection of 85% susceptible hosts would usually serve attackers' purposes. Therefore, internally generated target lists with average size of 3 (with maximum infection rate of 94%) could be employed by active worms to accelerate their propagation. A comparison of propagation curves of the 3 simple scenarios is illustrated by Fig. 2.

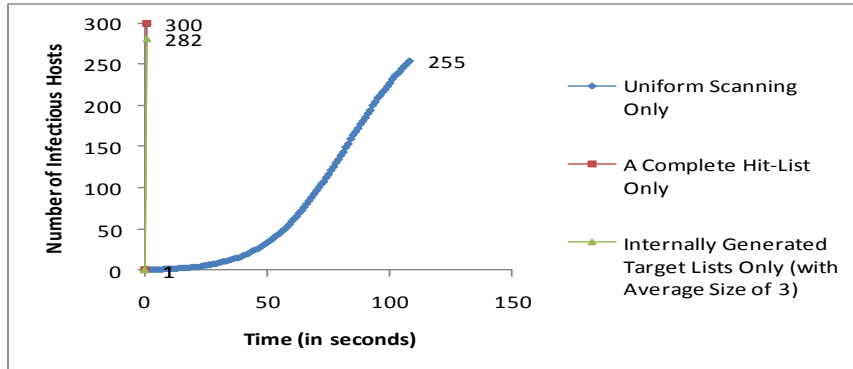


Fig. 2. A comparison of propagation curves of the 3 simple scenarios

4.2 Scenarios with Moderate Complexity

Then, propagation characteristics of active worms employing a combination of two different target discovery techniques formed the focus of our research. As we mentioned earlier in this paper, in order to accelerate a worm's propagation, we must try to let the worm infect the first susceptible hosts and enter its fast spread phase as soon as possible. According to our simulation results of the above 3 simple scenarios, both an incomplete hit-list and internally generated target lists can let a worm infect a certain percentage of susceptible hosts in just one second. Therefore, each of these two target discovery techniques could be followed by uniform scanning to let the worm infect those susceptible hosts leftover. In our simulation experiments, active worms employing an incomplete hit-list followed by uniform scanning as their target discovery techniques would sequentially probe all those hosts in the hit-list prior to employing uniform scanning. Active worms employing internally generated target lists followed by uniform scanning would sequentially probe all those hosts in the target lists generated in process prior to employing uniform scanning.

The above two kinds of active worms formed the basis of our 6 scenarios with moderate complexity to be simulated, which are summarized in Table 3. Since we intended to shorten a worm's slow start phase, in which less than of susceptible hosts are infected, an incomplete hit-list with size up to 15% of the number of all susceptible hosts was employed. Both size of incomplete hit-list and average size of internally generated target lists were candidate factors whose influences on a worm's propagation characteristics were to be investigated. We have simulated a limited number of scenarios. More scenarios could be investigated to determine the relationship between average time to infect 99% susceptible hosts and size of hit-list, and the relationship between average time to infect 99% susceptible hosts and average size of internally generated target lists.

Table 3. A summary of the 6 simulated scenarios with moderate complexity

Scenario Type	Scenario Code	Target Discovery Techniques Employed
Moderate	H5%+U	An Incomplete Hit-list with Size = 5% of the Number of All Susceptible Hosts; Followed by Uniform Scanning
Moderate	H10%+U	An Incomplete Hit-list with Size = 10% of the Number of All Susceptible Hosts; Followed by Uniform Scanning
Moderate	H15%+U	An Incomplete Hit-list with Size = 15% of the Number of All Susceptible Hosts; Followed by Uniform Scanning
Moderate	I1+U	Internally Generated Target Lists with Average Size of 1; Followed by Uniform Scanning
Moderate	I2+U	Internally Generated Target Lists with Average Size of 2; Followed by Uniform Scanning
Moderate	I3+U	Internally Generated Target Lists with Average Size of 3; Followed by Uniform Scanning

Table 4. A summary of simulation results of the 6 scenarios with moderate complexity

Scenario Type	Scenario Code	Average Time (in seconds) to Infect 99% Susceptible Hosts
Moderate	H5%+U	99
Moderate	H10%+U	89
Moderate	H15%+U	85
Moderate	I1+U	60
Moderate	I2+U	36
Moderate	I3+U	21

According to the results (Table 4) from our simulation experiments, an incomplete hit-list with size of 5% of the number of all susceptible hosts followed by uniform scanning accelerates a worm's propagation dramatically. However, this approach's capability to accelerate active worms' propagation is diminishing while size of the hit-list is increasing. Active worms employing internally generated target lists followed by uniform scanning performed especially well under all average sizes (1, 2, or 3) of the target lists. Here, average size of the target lists has a great influence on a worm's propagation rate. The larger the average size becomes, the faster the worm propagates.

We have also investigated propagation characteristics of active worms employing both an incomplete hit-list and internally generated target lists as their target discovery techniques. According to our simulation results of the 3 simple scenarios, an incomplete hit-list ought to be employed prior to internally generated target lists because generally the former is more effective to boost the number of initially infected hosts. Therefore, in our simulation experiments, active worms employing both an incomplete hit-list and internally generated target lists as their target discovery techniques would sequentially probe all those hosts in the hit-list prior to sequentially probing all those hosts in the target lists generated in process. Our simulation results show that active worms employing internally generated target lists with average size not greater than 3 cannot achieve infection of over 99% susceptible hosts, even if the number of initially infected hosts is boosted by an incomplete hit-list of size up to 15% of the number of all susceptible hosts. A simple and efficient way to infect those leftover susceptible hosts is by uniform scanning. Therefore, we believe

uniform scanning is an indispensable elementary target discovery technique of active worms.

4.3 Complex Scenarios

Finally, propagation characteristics of active worms employing a combination of three different target discovery techniques were examined. In our simulation experiments, active worms employing an incomplete hit-list followed by internally generated target lists followed by uniform scanning as their target discovery techniques would sequentially probe all those hosts in the hit-list prior to sequentially probing all those hosts in the target lists generated in process. Once those lists were exhausted, they would start uniform scanning.

The above kind of active worm formed the basis of our 9 complex scenarios to be simulated, which are summarized in Table 5. Both size of incomplete hit-list and average size of internally generated target lists were candidate factors whose influences on a worm's propagation characteristics were to be investigated. We have simulated a limited number of scenarios. More scenarios could be investigated to determine the relationship between average time to infect 99% susceptible hosts and size of hit-list and average size of internally generated target lists.

Table 5. A summary of the 9 complex scenarios simulated

Scenario Type	Scenario Code	Target Discovery Technique(s) Employed
Complex	H5%+I1+U H5%+I2+U H5%+I3+U	An Incomplete Hit-list with Size = 5% of the Number of All Susceptible Hosts; Followed by Internally Generated Target Lists with Average Size of 1, 2, or 3; Followed by Uniform Scanning
Complex	H10%+I1+U H10%+I2+U H10%+I3+U	An Incomplete Hit-list with Size = 10% of the Number of All Susceptible Hosts; Followed by Internally Generated Target Lists with Average Size of 1, 2, or 3; Followed by Uniform Scanning
Complex	H15%+I1+U H15%+I2+U H15%+I3+U	An Incomplete Hit-list with Size = 15% of the Number of All Susceptible Hosts; Followed by Internally Generated Target Lists with Average Size of 1, 2, or 3; Followed by Uniform Scanning

Table 6. A summary of simulation results of the 9 complex scenarios

Scenario Type	Scenario Code	Average Time (in seconds) to Infect 99% Susceptible Hosts
Complex	H5%+I1+U	54
Complex	H5%+I2+U	34
Complex	H5%+I3+U	18
Complex	H10%+I1+U	55
Complex	H10%+I2+U	36
Complex	H10%+I3+U	19
Complex	H15%+I1+U	53
Complex	H15%+I2+U	35
Complex	H15%+I3+U	18

According to the results (Table 6) from our simulation experiments, an additional incomplete hit-list only accelerates a worm's propagation slightly, compared to the results of the last 3 scenarios in Table 4. Increasing size of the hit-list has little effect on a worm's rate of propagation. However, average size of internally generated target lists has a great influence on a worm's rate of propagation. The larger the average size becomes, the faster the worm propagates. In other words, the results indicate the combination of the three different target discovery techniques is not the best for attackers taking into account the added effort they have to make to build the worm. We suggest internally generated target lists with average size of 3 followed by uniform scanning is the most effective and efficient among all approaches examined in this paper to accelerate propagation of active worms.

5 Conclusions and Future Work

This paper provides a reasonably comprehensive but not exhaustive coverage of various target discovery techniques that future active worms might employ to accelerate their propagation. We derived from mathematical analysis that in order to accelerate a worm's propagation, we must try to let the worm infect the first 15% susceptible hosts and enter its fast spread phase as soon as possible.

A hit-list lets a worm infect all susceptible hosts in the list in an extremely short period. When followed by uniform scanning, an incomplete hit-list's capability to accelerate a worm's propagation is diminishing while size of the hit-list is increasing. When not followed by uniform scanning, internally generated target lists with average size not greater than 3 cannot let a worm achieve infection of over 99% susceptible hosts, no matter the number of initially infected hosts is boosted by an incomplete hit-list of size up to 15% of the number of all susceptible hosts or not. However, when followed by uniform scanning, internally generated target lists performed especially well. The larger the average size becomes, the faster the worm propagates. An additional incomplete hit-list only accelerates the worm's propagation slightly.

Our major contributions in this paper are first, we proposed a new discrete time deterministic model of active worms; and second, we suggested the combination of target discovery techniques that can best accelerate propagation of active worms discovered from results of the comprehensive simulations. The research is from attackers' perspective. We believe it can be very beneficial to understanding of propagation mechanisms of active worms, and thus building effective and efficient defense systems against their propagation.

In order to counter super fast propagation of future active worms employing the various combinations of multiple target discovery techniques, novel mechanisms need to be discovered since current ones, due to their inherent drawbacks, respond too slowly compared to propagation of even active worms employing single target discovery technique.

References

1. Kienzle, D.M., Elder, M.C.: Recent Worms: A Survey and Trends. WORM '03, Washington D.C., USA (2003) 1-10
2. Weaver, N., Paxson, V., Staniford, S., Cunningham, R.: A Taxonomy of Computer Worms. WORM '03, Washington D.C., USA (2003) 11-18
3. Moore, D., Shannon, C., Brown, J.: Code-Red: A Case Study on the Spread and Victims of an Internet Worm. IMW '02, Marseille, France (2002) 273-284
4. Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., Weaver, N.: Inside the Slammer Worm. IEEE Security & Privacy, Vol. 1 (2003) 33-39
5. Shannon, C., Moore, D.: The Spread of the Witty Worm. IEEE Security & Privacy, Vol. 2 (2004) 46-50
6. Staniford, S., Paxson, V., Weaver, N.: How to Own the Internet in Your Spare Time. Security '02, San Francisco, CA, USA (2002) 149-167
7. Spafford, E.H.: The Internet Worm Program: An Analysis. ACM SIGCOMM Computer Communication Review 19 (1989) 17-57
8. Berghel, H.: The Code Red Worm: Malicious Software Knows No Bounds. Communications of the ACM 44 (2001) 15-19
9. Ma, J., Voelker, G.M., Savage, S.: Self-Stopping Worms. WORM '05, Fairfax, VA, USA (2005) 12-21
10. Xiang, Y., Zhou, W., Chowdhury, M.: A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. (Technical Report), TR C04/02, School of Information Technology, Deakin University, Australia (2004)
11. Xiang, Y., Fan, X., Zhu, W.: Propagation of Active Worms: A Survey. International Journal of Computer Systems Science and Engineering (2008) Accepted
12. Ellis, D.: Worm Anatomy and Model. WORM '03, Washington D.C., USA (2003) 42-50
13. Anderson, R.M., May, R.M.: Infectious Diseases of Humans: Dynamics and Control. Oxford University Press, Oxford (1991)
14. Andersson, H., Britton, T.: Stochastic Epidemic Models and Their Statistical Analysis. Springer-Verlag, New York (2000)
15. Bailey, N.T.: The Mathematical Theory of Infectious Diseases and Its Applications. Hafner Press, New York (1975)
16. Frauenthal, J.C.: Mathematical Modeling in Epidemiology. Springer-Verlag, New York (1980)
17. Daley, D.J., Gani, J.: Epidemic Modelling: An Introduction. Cambridge University Press, Cambridge (1999)
18. Zou, C.C., Gong, W., Towsley, D.: Code Red Worm Propagation Modeling and Analysis. CCS '02, Washington D.C., USA (2002) 138-147
19. Chen, Z., Gao, L., Kwiat, K.: Modeling the Spread of Active Worms. IEEE INFOCOM (2003) 1890-1900
20. Wang, Y., Wang, C.: Modeling the Effects of Timing Parameters on Virus Propagation. WORM '03, Washington D.C., USA (2003) 61-66
21. Rohloff, K., Basar, T.: Stochastic Behavior of Random Constant Scanning Worms. 14th ICCCN, San Diego, CA, USA (2005) 339-344
22. Sellke, S., Shroff, N.B., Bagchi, S.: Modeling and Automated Containment of Worms. DSN '05 (2005) 528-537
23. Zou, C.C., Towsley, D., Gong, W.: On the Performance of Internet Worm Scanning Strategies. University of Massachusetts (2003)
24. Wagner, A., Dubendorfer, T.: Experiences with Worm Propagation Simulations. WORM '03, Washington D.C., USA (2003) 34-41