Defending against the Propagation of Active Worms

Xiang Fan
School of Management and Information Systems
Central Queensland University, Australia
x.fan2@cqu.edu.au

Yang Xiang
School of Management and Information Systems
Centre for Intelligent and Networked Systems
Central Queensland University, Australia
y.xiang@cqu.edu.au

Abstract

Recently, active worms such as the Code Red worm of 2001 and the Slammer worm of 2003, both of which adopted the uniform scanning approach, have caused significant financial loss due to their rapid propagation over the Internet. Current defense mechanisms, due to their inherent drawbacks, respond too slowly compared to the propagation of active worms which scan uniformly. This paper presents the results from our study on defending against the propagation of active worms which employ the uniform scanning approach. Our major contributions in this paper are first, we proposed a novel defense mechanism and compared it to other defense mechanisms; and second, we evaluated the effectiveness of this defense mechanism using results of the simulation experiments conducted and found the appropriate value of one of its parameters. In the future, detailed implementation of the proposed defense mechanism is to be studied.

1. Introduction

Internet worms can be classified according to the technique by which they discover new targets to infect: scanning, pre-generated target list, internally generated target lists, or passive monitoring [1]. Active worms are those which employ the first three as their target discovery technique. Scanning could be implemented differently, which leads to several different approaches such as uniform scanning, localized scanning [2], sequential scanning [3], routable scanning [4], selective scanning [4], or importance scanning [5, 6]. The uniform scanning approach probes each IP address from within the whole IPv4 address space with equal probability. This scanning approach has been employed by such famous worms as the Code-RedI v1 and v2 worms [2] and the Slammer worm [7]. A pre-generated target list is also termed as a 'hit-list' [8]. 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 could be used to create a 'flash' worm [9], capable of infecting all vulnerable hosts extremely rapidly. 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 [10]. 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 another example of employing this target discovery technique.

Recently, active worms such as the Code Red worm of 2001[11] and the Slammer worm of 2003 [7], both of which adopted the uniform scanning approach, have caused significant financial loss due to their rapid propagation over the Internet. Current defense mechanisms, due to their inherent drawbacks, respond too slowly compared to the propagation of active worms which scan uniformly. In this paper, we propose a novel defense mechanism and evaluate its effectiveness using results from our simulation experiments.

2. Related work

During propagation of active worms, an infected host will connect to as many different hosts as fast as possible. Hence, by limiting the number of 'new' connections allowed per unit time, we can greatly slow down scanning rate of active worms [12]. Such rate limiting at individual hosts or edge routers yields a slowdown that is linear in the number of hosts or routers with the rate limiting filters [13]. Rate limiting at the backbone routers, however, is substantially more

978-0-7695-3492-3/08 $25.00 © 2008 IEEE
DOI 10.1109/EUC.2008.75

effective because it renders a slowdown comparable to deploying rate limiting filters at every individual host that is covered [13]. However, rate limiting has no effects on active worms with slow scanning rate, because the limit on the rate has to be high enough to let the normal traffic through. Instead of limiting scan rate, we can also possibly prevent a worm from spreading by limiting total number of allowable scans [14]. This is a promising countermeasure since it is much more feasible than rate limiting.

Deployment of Network Address Translation (NAT) can slow down the spread of active worms employing the localized scanning approach [15]. This is due to decreased hitting probability caused by decreased vulnerability density inside NAT. Network Address Space Randomization (NASR) [16] could be utilized to defend against active worms employing the pre-generated target list (hit-list) target discovery technique. The idea behind NASR is to render hit-list information stale by forcing nodes to frequently change their IP addresses [16].

Chen and Tang proposed a distributed anti-worm (DAW) architecture [17] which would automatically slow down or even halt worms propagation within an Internet service provider's (ISP's) network. Furthermore, the DAW system ensures sufficient time for human reaction by the use of the temporal rate-limit algorithm that constrains the maximum scanning rate of any infected host and the spatial rate-limit algorithm that constrains the combined scanning rate of all infected hosts in a network.

3. The proposed novel defense mechanism

We believe the spirit of Distributed Active Defense System (DADS) which was proposed in [18] to defend against Distributed Denial of Service (DDoS) attacks could also be employed in creating a novel defense mechanism to slow down or even stop the propagation of active worms which scans uniformly. The very essence of that spirit is to push defense sphere as close as possible towards attacking sources. Based on that spirit, we created our novel defense mechanism, which is distributed, collaborative and networked. Figure 1 illustrated the deployment of the proposed defense mechanism.

As Figure 1 shows, the proposed defense mechanism is deployed on the ingress edge routers of the protected network. Such protection is achievable at a national level since each country is connected to the rest of the world by a small number of edge routers. Therefore, we are able to push defense sphere towards attacking sources. The defense mechanism is distributed since it is deployed on each of those edge routers. Besides, the edge routers share all traffic information coming into the network protected by them, which is analyzed by the defense mechanism to identify IP addresses of attacking hosts. In other words, the defense mechanism deployed on each of those edge routers collaborates with each other to detect attacking hosts. Once an attacking host is identified, all incoming traffic from that host into the protected network will be blocked by the edge routers. In other words, those edge routers need to share the information on IP addresses of all identified attacking hosts. To facilitate information sharing among the edge routers, a dedicated network with very high communication efficiency could be employed to connect those edge routers. In this sense, the defense mechanism is networked.

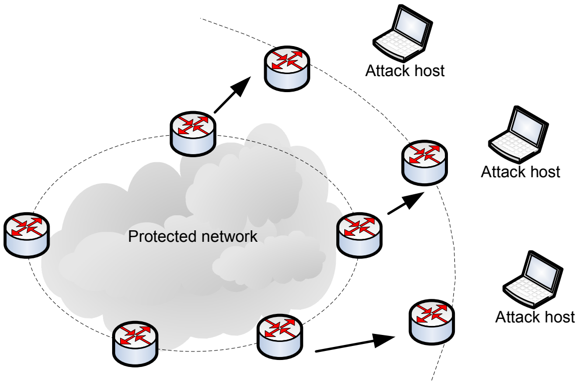


Figure 1. The deployment of the proposed defense mechanism

Since only the edge routers rather than all hosts participate in defense, the proposed defense mechanism consumes as few resources as possible. Due to the collaborative nature of this defense mechanism, it will detect as many attacking sources as possible. Another important merit of this defense mechanism is its ability to block worm packets at the point close to attacking hosts rather than hosts being attacked.

4. Simulation Experiments

4.1. Setup of the simulation experiments

We conducted a series of simulation experiments for various scenarios in an attempt to assess the effectiveness of the proposed defense mechanism. Setup of the simulation experiments is detailed as follows.

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 1/28 to explore worm dynamics. According to Weaver et al. [19], 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 [19].

We divided the class A /8 subnet into two /9 subnets containing equal number of IP addresses and called them subnet P and subnet U, respectively. Subnet P will be under the protection of the proposed novel defense mechanism, while subnet U will not. We assume initially there is no infected and thus infectious host inside subnet P and all initially infected hosts are inside subnet U. Only uniform scanning was simulated. It was also assumed that susceptible hosts are uniformly distributed in the above /8 subnet with vulnerability density approximately equivalent to that of the Slammer worm and average worm scanning rate to be equivalent to the Slammer's average scanning rate. All simulations started with only 1 initially infected host, which is equivalent to 28 initially infected hosts in the Slammer's case.

The combined incoming traffic from subnet U to subnet P via all ingress edge routers of subnet P in a period *T* is analyzed at the end of that period by the proposed defense mechanism deployed on those edge routers to identify IP addresses of attacking hosts. Let *M* denote the minimum number of distinct IP addresses a host sends packets to per unit time in order to be considered as spreading worm packets. So, if a host in subnet U sends packets to *M* or more distinct IP addresses in the period *T*, it will be identified by the proposed defense mechanism as spreading worm packets. If a host in subnet U sends packets to *MT* / 2 or more distinct IP address inside subnet P, it will be identified by the proposed defense mechanism as spreading worm packets. Once identified, all incoming traffic from those infectious hosts in subnet U to subnet P will be blocked by the edge routers from the end of the period *T*. Since a host in subnet U might get infected and start to send out infectious packets at any point in the period *T*, the above threshold value *MT* / 2 needs to be adjusted to reflect this. In our simulations, we simply let it be *MT* / 2 / 2, which is *MT* / 4, since we might consider in average a host in subnet U will get infected and start to send out infectious packets at the middle point in the period *T*.

In the simulation experiments, the proposed defense mechanism will make a decision at the end of the period *T* as to which IP addresses ought to be blocked based on the analysis of all incoming traffic during that period. However, until the end of the period *T*, an infectious host in subnet U which has not yet been identified in previous periods is still able to infect susceptible hosts in subnet P. The proposed defense mechanism will discard all traffic information in previous periods. We believe if we shorten the duration of the period *T*, this defense mechanism's performance ought to be improved. Therefore, the period *T* is an important parameter of the proposed defense mechanism, whose impacts on its effectiveness are to be investigated fully.

Since our proposed defense mechanism only checks incoming traffic from subnet U to subnet P, an infectious host in subnet U is still able to infect susceptible hosts in that subnet and an infectious host in subnet P is still able to infect susceptible hosts in both subnets.

In order to eliminate variation in results from different simulation runs, 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 systematically examined propagation characteristics of active worms employing the uniform scanning approach under no defense and under the proposed defense mechanism by conducting a series of simulation experiments for the following various scenarios.

4.2. Propagation under no defense

Based on the setup and the assumptions given in the last sub-section, we conducted simulation experiment for the scenario without defense. Results of the simulation are illustrated by Figures 2 and 3.

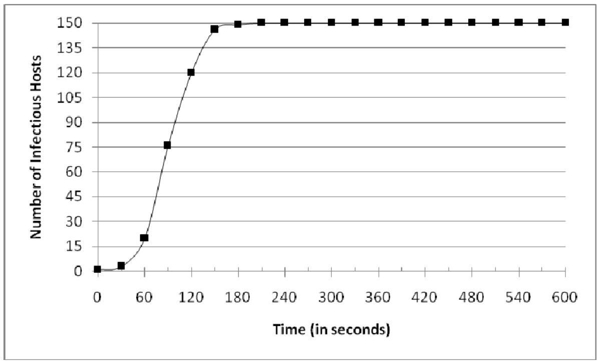


Figure 2. Propagation in subnet U under no defense

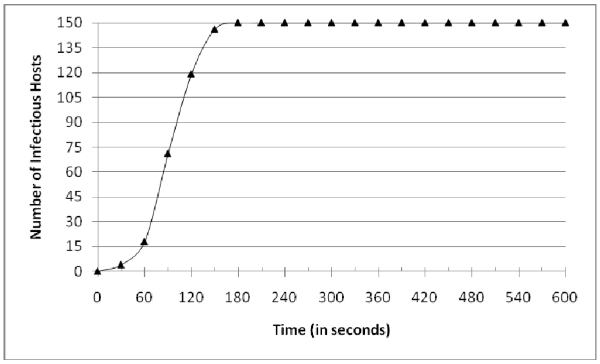


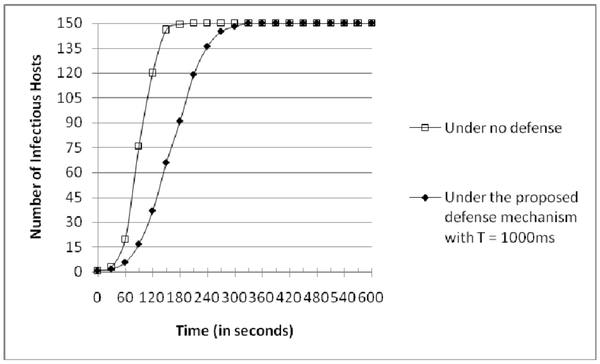
Figure 3. Propagation in subnet P under no defense

The propagation curves in Figures 2 and 3 show that under the given parameters, time spent by active worms employing the uniform scanning approach to infect over 90% susceptible hosts in subnets U and P is approximately 135 seconds, which sets the benchmark to be compared to.

4.3. Propagation under the proposed defense mechanism

We have also investigated propagation characteristics of active worms employing the uniform scanning approach under the proposed defense mechanism. As we mentioned in the last sub-section, the period *T* is an important parameter of the proposed defense mechanism, whose impacts on its effectiveness are to be investigated fully. Therefore, we conducted a series of simulations with varying duration of the period *T*.

Comparisons of propagation in subnet U under no defense to under the proposed defense mechanism with various values of *T* are illustrated by Figure 4.



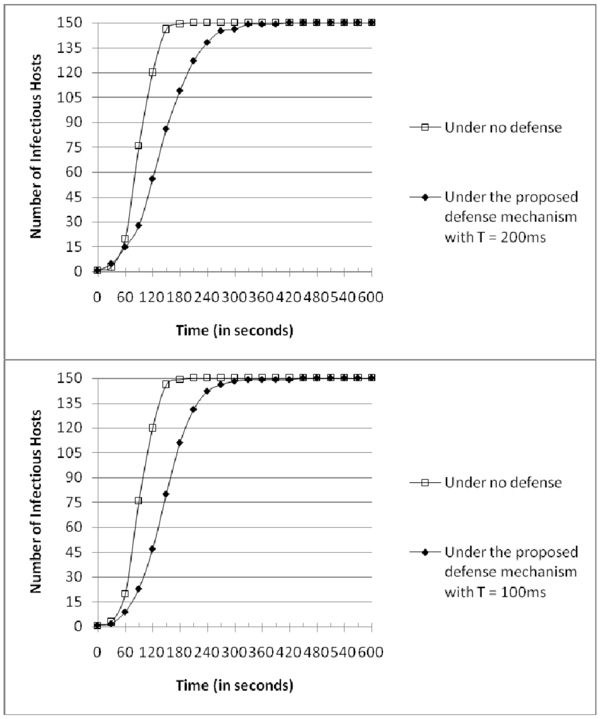


Figure 4. Propagation in subnet U

A comparison of propagation in subnet P under no defense to under the proposed defense mechanism with various values of *T* is illustrated by Figure 5.

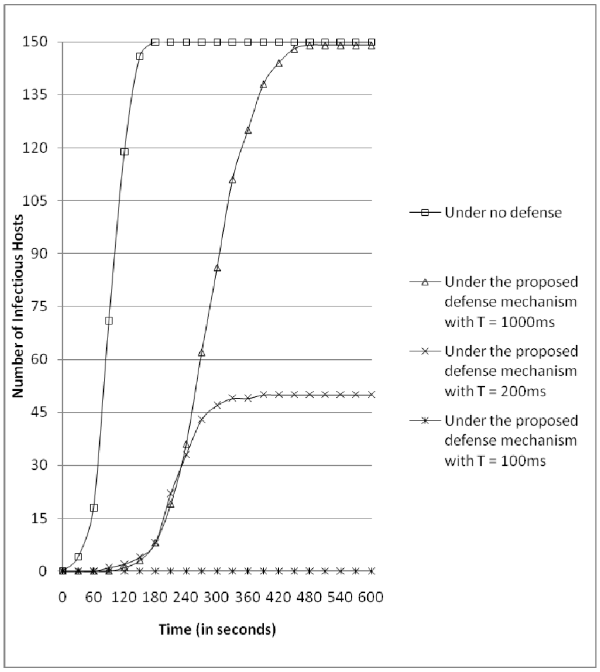


Figure 5. Propagation in subnet P

A summary of time spent to infect over 90% susceptible hosts in subnets U and P under no defense and under the proposed defense mechanism with various values of *T* is given by Table 1.

Table 1. A summary of time spent to infect over 90% susceptible hosts

	Time spent to infect over 90% susceptible hosts in subnet U (in seconds)	Time spent to infect over 90% susceptible hosts in subnet P (in seconds)
Under no defense	135	136
Under the proposed defense mechanism with *T* = 1000ms	236	379
Under the proposed defense mechanism with *T* = 200ms	226	Indefinite (with maximum infection rate of approximately 33%)
Under the proposed defense mechanism with *T* = 100ms	224	Indefinite (with maximum infection rate of 0%)

Comparisons of propagation in subnet U and subnet P under the proposed defense mechanism with various values of *T* are illustrated by Figures 6, 7 and 8.

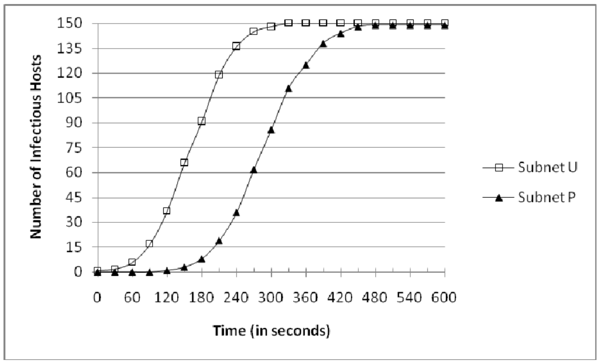


Figure 6. A comparison of propagation under the proposed defense with T = 1000ms

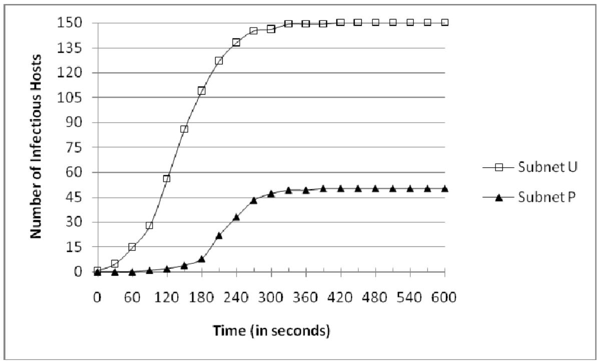


Figure 7. A comparison of propagation under the proposed defense with T = 200ms

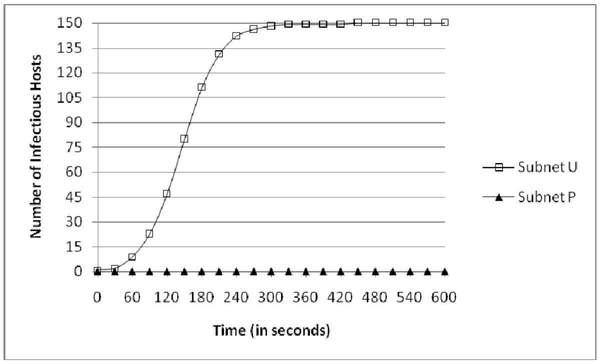


Figure 8. A comparison of propagation under the proposed defense with T = 100ms

According to above results of the simulation experiments, the proposed defense mechanism does slow down, stop or even make totally impossible propagation of active worms which scan uniformly in the protected subnet P (Figure 5). It is also able to slow down propagation of active worms which scan uniformly in the unprotected subnet U but to a less extent (Figure 4). This is because the slowdown of propagation in the protected subnet will contribute to the slowdown of propagation in the unprotected subnet.

However, shortening the duration of the period *T* has little impact on a worm's propagation characteristics in the unprotected subnet (Table 3 and Figure 4). On the other hand, shortening the duration of the period *T* has significant impact on a worm's propagation characteristics in the protected subnet (Table 3 and Figure5). The shorter the duration of the period *T* becomes the more effective the proposed defense mechanism will be. When *T* decreases to 200ms, active worms which scan uniformly will be made unable to infect over 90% susceptible hosts in the protected subnet and the maximum percentage of susceptible hosts in the protected subnet they are able to infect is approximately 33%. In other words, propagation in the protected subnet will stop once approximately 33% of susceptible hosts in the protected subnet have been infected. When *T* further decreases to 100ms, active worms which scan uniformly will be made unable to propagate in the protected subnet at all, which is our paramount objective. As illustrated by Figures 6, 7 and 8 and shown by Table 3, the proposed defense mechanism is effective on defending against the propagation of active worms which scan uniformly if the parameter *T* is chosen appropriately.

5. Conclusions and future work

This paper presents the results from our study on defending against the propagation of active worms which employ the uniform scanning approach. Our major contributions in this paper are first, we proposed a novel defense mechanism and compared it to other defense mechanisms; and second, we evaluated the effectiveness of this defense mechanism using results of the simulation experiments conducted and found the appropriate value of one of its parameters. In the future, detailed implementation of the proposed defense mechanism is to be studied.

6. References

[1] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A Taxonomy of Computer Worms," in *WORM '03*, Washington D.C., USA, 2003, pp. 11-18.

[2] D. Moore, C. Shannon, and J. Brown, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm," in *IMW '02*, Marseille, France, 2002, pp. 273-284.

[3] C. C. Zou, D. Towsley, and W. Gong, "On the Performance of Internet Worm Scanning Strategies," University of Massachusetts Technical Report: TR-03-CSE-07, 2003.

[4] C. C. Zou, D. Towsley, W. Gong, and S. Cai, "Routing Worm: A Fast, Selective Attack Worm Based on IP Address Information," in *PADS '05*, 2005, pp. 199-206.

[5] Z. Chen and C. Ji, "Importance-Scanning Worm Using Vulnerable-Host Distribution," in *IEEE GLOBECOM*, 2005, pp. 1779-1784.

[6] Z. Chen and C. Ji, "A Self-Learning Worm Using Importance Scanning," in *WORM '05*, Fairfax, VA, USA, 2005, pp. 22-29.

[7] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," in *IEEE Security & Privacy*. vol. 1, 2003, pp. 33-39.

[8] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time," in *Security '02*, San Francisco, CA, USA, 2002, pp. 149-167.

[9] S. Staniford, D. Moore, V. Paxson, and N. Weaver, "The Top Speed of Flash Worms," in *WORM '04*, Washington D.C., USA, 2004, pp. 33-42.

[10] E. H. Spafford, "The Internet Worm Program: An Analysis," *ACM SIGCOMM Computer Communication Review,* vol. 19, pp. 17-57, 1989.

[11] H. Berghel, "The Code Red Worm: Malicious Software Knows No Bounds.," in *Communications of the ACM*. vol. 44, 2001, pp. 15-19.

[12] M. M. Williamson, "Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code," in *IEEE ACSAC*, Las Vegas, NV, USA, 2002, pp. 61-68.

[13] C. Wong, C. Wang, D. Song, S. Bielski, and G. R. Ganger, "Dynamic Quarantine of Internet Worms," in *DSN '05*, Florence, Italy, 2004, pp. 73-82.

[14] S. Sellke, N. B. Shroff, and S. Bagchi, "Modeling and Automated Containment of Worms," in *DSN '05*, 2005, pp. 528-537.

[15] M. A. Rajab, F. Monrose, and A. Terzis, "On the Impact of Dynamic Addressing on Malware Propagation," in *WORM '06*, Fairfax, VA, USA, 2006, pp. 51-56.

[16] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending against Hitlist Worms Using Network Space Randomization," in *WORM '05*, Fairfax, VA, USA, 2005, pp. 1-11.

[17] S. Chen and Y. Tang, "DAW: A Distributed Antiworm System," *IEEE Transactions on Parallel and Distributed Systems,* vol. 18, pp. 893-906, 2007.

[18] Y. Xiang, W. Zhou, and M. Chowdhury, "A Survey of Active and Passive Defence Mechanisms against DDoS Attacks," (Technical Report), TR C04/02, School of Information Technology, Deakin University, Australia 2004.

[19] N. Weaver, I. Hamadeh, G. Kesidis, and V. Paxson, "Preliminary Results Using Scale-Down to Explore Worm Dynamics," in *WORM '04*, Washington D.C., USA, 2004, pp. 65-72.