Copyright ⓒ 2010 KSII

The Analysis of Random Propagating Worms using Network Bandwidth

Kwang Sun Ko, Hyunsu Jang, Byuong Woon Park and Young Ik Eom
School of Information and Communication Engineering, Sungkyunkwan University
Suwon 440-746, Republic of Korea
[e-mail: kwangsun.ko@gmail.com, {jhs4071, bwpark, yieom}@ece.skku.ac.kr]
*Corresponding author: Young Ik Eom

Received February 27, 2010; revised April 8, 2010; accepted April 13, 2010; published April 29, 2010

Abstract

There is a well-defined propagation model, named the random constant spread (RCS) model, which explains worms that spread their clones with a random scanning strategy. This model uses the number of infected hosts in a domain as a factor in the worms' propagation. However, there are difficulties in explaining the characteristics of new Internet worms because they have several considerable new features: the denial of service by network saturation, the utilization of a faster scanning strategy, a smaller size in the worm's propagation packet, and to cause maximum damage before human-mediated responses are possible. Therefore, more effective factors are required instead of the number of infected hosts. In this paper, the network bandwidth usage rate is found to be an effective factor that explains the propagations of the new Internet worms with the random scanning strategy. The analysis and simulation results are presented using this factor. The simulation results show that the scan rate is more sensitive than the propagation packet for detecting worms' propagations.

Keywords: Random propagating worms, network bandwidth

A preliminary version of this paper appeared in ICISC 2009, December 1-3, Seoul, Korea. This version includes a further analysis and supporting results on worms' propagation patterns. This research was supported by MKE, Korea under ITRC NIPA -2009-(C1090-0902-0046)

DOI: 10.3837/tiis.2010.04.007

1. Introduction

After the Morris worm [1], which is considered to be the first computer worm on the Internet, there have been many problems caused by various Internet worms. There have been many studies into these worm's propagation methods, because it is required to detect the advent of these worms instantly and stop the worms from spreading. Basically, the pattern the worm uses to select the victim computers is similar to that of human disease. Therefore the initial studies used biological models [2], the classic susceptible and infected epidemic model [3], etc.

Recently, as the research matured, various mathematical and analytical models have been published. Kienzle *et al*. [4] presented a broad overview of recent worm activities. They extracted a number of trends subjectively from their study of past and present worms. These trends in a qualitative perspective, are as follows: commoditization, convergence, social engineering, additional propagation vectors, technology/vulnerabilities, speed of propagation, countermeasure awareness, along with common platforms and software. Qing *et al*. [5] also presented several features. According to their function analysis of the structure of Internet worms, there are four stages in a worm's execution: information collection, probing, attacking, and propagating. The last stage, propagating, is considered to be a very important stage in a worm's outbreak; this stage may be different for each worm in the scanning strategy chosen by the worm. In addition, they categorized the scanning strategy into six classes: the random scan, the sequential scan, the hit-list scan, the routable scan, the DNS scan, and the divide-conquer scan. The paper presented that, in general, the propagation speed using the DNS scan is the slowest, while the speed of the selective random scan and the routable scan is quicker than the rest. Zou *et al*. [6][7][8] present that there are three phases in a worm's propagation: the slow start phase, the fast spread phase, and the slow finish phase. During the slow start phase, the number of infected hosts increases exponentially. After many hosts are infected and are participating in infecting others, the worm enters the fast spread phase, where vulnerable hosts are infected in a fast, near linear speed. When most of the vulnerable computers have been infected, the worm enters the slow finish phase because few vulnerable computers are left and so it is difficult for the worm to search them out. There is further research proposed by Provos *et al*. [9]. To understand the worms' propagation, the random constant spread (RCS) model is very popular [10][11]. (detailed descriptions of the RCS model are explained in Section 2.) However, the RCS model has some difficulties in explaining the propagation of the newly emergent Internet worms because the model uses only the number of infected hosts as the factor for the worm's propagation. In other words, these worms cannot be simulated just using this statistical analysis, which is based on the number of hosts. Additionally, the new worms have several considerable key features: the denial of service by network saturation, the utilization of faster scanning strategies, a smaller propagation packet size, and to cause maximum damage before a human-mediated response is possible. Therefore, a more effective factor is required, instead of just the number of infected hosts, which is generally used by many propagation models as well as the RCS model. In our proposed model, the usage rate of network bandwidth is used as an effective factor. The simulation results show the propagation pattern of a worm using the random scanning strategy.

The remainder of this paper is organized as follows: Section 2 describes the features of the new Internet worms. Section 3 explains the RCS model. Section 4 and Section 5 describe the analysis and simulation results of the propagation of a worm using the random scanning

strategy from the perspective of the network bandwidth usage rate. Finally, Section 6 concludes our paper.

2. The Features of Internet Worms

From previous studies, which features of the new Internet worms should be considered? Especially, which features may be derived in terms of propagation? In this paper, four features are summarized and shown in **Table 1**.

Table 1. The Summary of the Features of New Internet Worms

Feature	Descriptions
Denial of service by network saturation	Denial of service is defined as a state of the computer system when it cannot do its proper job, and recently this includes the state of the network resources. It is considered to be one of the main Internet attack methods. That is to say, attackers exploit vulnerabilities in the computer systems or exhaust the system or network resources. Denial of service attacks saturate the resources of the networks (or systems), or overflow their workload in a short time, so they cannot provide normal service.
Utilization of a faster scanning strategy	Previous studies show that the scanning strategy used by a worm is the most important factor compared to others, such as the total number of susceptible hosts, the threaded number of worms in an infected host, and so on. It is also considered that the new emergent Internet worms tend to choose a faster scanning strategy to cause much damage with little effort. However, this is not always true.
Smaller size of a worm's propagation packet	Generally, as the size of a worm's propagation packet becomes smaller, more packets can be generated within a unit time and then used for propagation under limited network or system resources. The size of the packet is related to the propagation. For example, the size of Code Red is 4 Kbytes, and Slammer is 404 bytes. It is reported that Slammer is two orders of magnitude faster than Code Red.
Maximum damage before human-mediated response	Code Red I in 2001 is reported as infecting almost 360,000 hosts over 14 hours [12]. Slammer in 2003 infected more than 90% of the vulnerable hosts within 10 minutes. About 75,000 distinct IP addresses that were sending its propagation packets were monitored in the first 30 minutes in its early stage [13]. This evidence shows that the propagation of the new emergent Inernet worms cannot be limited or defeated by human-mediated responses any more.

As seen in **Table 1**, new Internet worms make a denial of service attack by network saturation, use a faster scanning strategy, propagate with smaller size of packets, and damage the network or system resources before a human-mediated response is possible. In this paper, a worm using the random scanning strategy in the propagating stage is considered with these features even though the random scan is not the fastest.

3. The Random Constant Spread (RCS) Model

This is a model based on the epidemiology in which the worm propagation is similar to that of a disease in human beings. In the RCS model, a worm generally sends its propagation packets using random scanning strategy. That is to say, it randomly selects IP addresses based on an effectively seeded random number generator, sends its propagation packet, and eventually

infects all of the susceptible hosts in a domain. During the fast propagation, the number of infected victims increases exponentially until there is no susceptible host or all hosts are infected, but actually it does not do so because there may be some removal processes that affect the propagation: human countermeasures, system or network failures, security patches, etc. There are two popular models: the Kermack-Mekendrick model [14] and the Two-factor model [15]. However, the RCS model cannot explain all the propagations of detected or undiscovered worms.

For example, Code Red II spreads its propagation packets based on the local strategy. An infected host gives priority to sending propagation packets to destinations belonging to the same local network, because generally most hosts in the same local network adopt a homogeneous security policy. Others move in on other susceptible hosts based on specific lists, such as email lists or connected network drives. For these reasons, there are no exact propagation model, including the RCS model, until the worm's source code is made public or reverse engineering of its binary code is analyzed.

3.1 The analysis results of previous worms

First, a very notorious worm, Code Red I, is selected because the raw data has been given to researchers to analyze its propagation at the Cooperative Association for Internet Data Analysis (CAIDA) [16]. In this paper, we also analyze this raw data to see if there are any particular features of interest. This data is processed into two types of data, and the result is shown in **Fig. 1**.

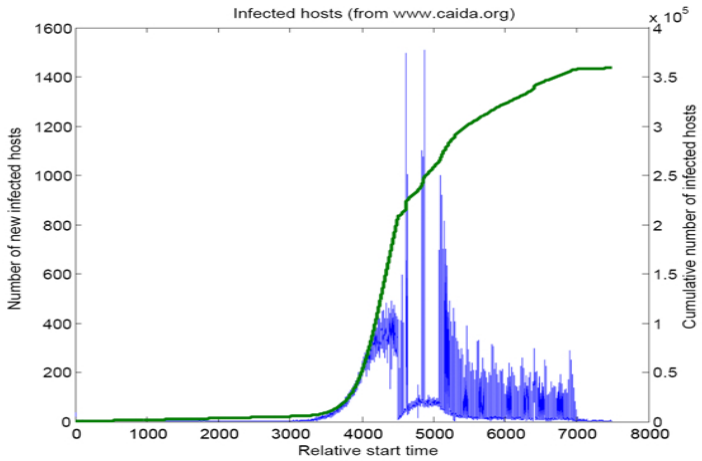

Fig. 1. The graph based on both the numbers of new infected hosts and the cumulative number of infected hosts done by Code Red I. The x-axis shows the relative elapsed time. The left y-axis shows the number of newly infected hosts, and the right y-axis shows the cumulative number of infected hosts

As seen in **Fig. 1**, from the cumulative number of infected hosts we can roughly partition it into four phases. During the first phase time interval ($0 < t < 3{,}500$), the worm starts finding susceptible hosts necessary to spread until the number of infected hosts increases enough to be a stepping-stone. The time required by this interval is variable to the network environment and lasts until it is assured that the number of infected hosts reaches the value needed to exponentially spread. During the second phase ($3{,}500 < t < 4{,}500$), based on the amount of previously infected hosts, the cumulative number of infected hosts increases exponentially until it reaches about 60% of the total susceptible hosts. During the third phase ($4{,}500 < t < 7{,}000$), the cumulative number of infected hosts increases linearly. The reasons for why this

phenomenon exists will be explained later. During the last phase (7,000 < t), the propagation of the worm becomes slower and then stops due to most susceptible hosts being infected, removal processes such as human countermeasures and network failures have occurred, or its own expiration mechanism is activated. (Code Red I stopped its propagation at 00:00 UTC on July 20, 2001 by its own expiration mechanism.)

These four partitioned phases can be called the slow start phase, the exponential spread phase, the linear spread phase, and the slow finish phase and are shown in **Fig. 2**.

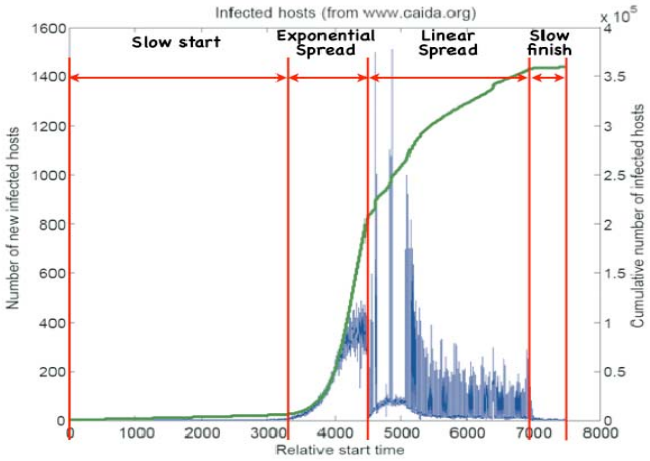

Fig. 2. The four partitioned phases from the raw data of Code Red I

We include one additional phase, the *linear spread* phase, from the analysis results, even though previous research [10] showed only three phases (as mentioned before) in the simple epidemic model. Additionally, to find the unknown features of the propagation, an enlarged part of **Fig. 1** is presented, which includes the *exponential spread* phase and the *slow finish* phase.

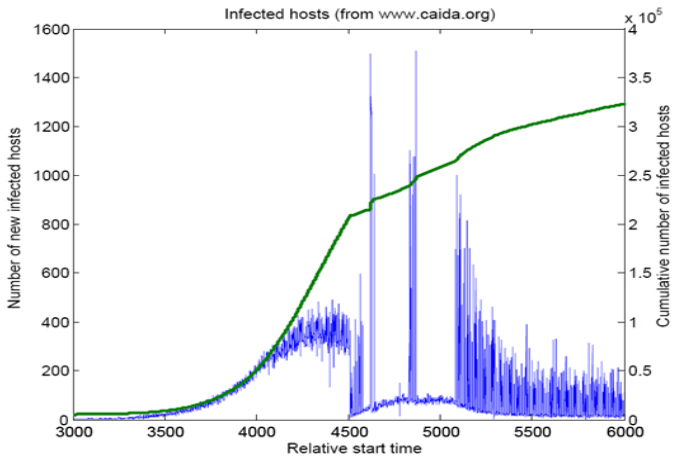

Fig. 3. The enlarged graph has both the number of the newly infected hosts and the cumulative number of infected hosts done by Code Red I, including the *exponential spread* phase and the *slow finish* phase. The x-axis shows the relative start time elapsed. The left y-axis shows the number of newly infected hosts, and the right y-axis shows the cumulative number of infected hosts

As seen in **Fig. 3**, there is an important phase-transition around 4,500 of the x-axis in the cumulative number of infected hosts. That is to say, the exponentially increased rate of the cumulative number suddenly becomes linear. Additionally, two more facts can be found from the view of the number of newly infected hosts.

- **At time *t*, the increase rate of the newly infected hosts is stable within 4, 000 < *t* < 4, 500**
  The numbers of newly infected hosts within this interval are less than those within 5,100 < *t* < 5,200 even if it is temporary. The increasing rate of newly infected hosts is stable, while the total numbers of infected hosts increase exponentially. For these reasons, it cannot be recognized by human countermeasures, such as security patches or removal processes, to be done against the propagation. Additionally, during the exponential increase of the cumulative numbers of the infected hosts, the worm's propagation does not need to be stable.
- **At time *t*, the numbers of new infected hosts suddenly drop within 4, 600 < *t* < 5, 100**
  The numbers of new infected hosts within this interval are a little more than those in the *slow start* phase, and there are two short intervals in which the numbers of new

  infected hosts are suddenly higher than other intervals. For these, it is considered for some countermeasures to be done in order to stop the propagation of Code Red I during the interval. However, it is not explained why the numbers of new infected hosts suddenly become high?

Based on these facts, we can wonder why there is a transition from the *exponential spread* phase to the *linear spread* phase. Is there any particular reason? For this, an analytic point of view having two aspects may be considered. First, some countermeasures, like security patches and the removal of susceptible or infected hosts, help stop worms from propagating. The other reason is that the worms propagate so rapidly that network saturations seem to be happening at many of the bottleneck network nodes. It seems the key reason for the transition is due to the latter rather than the former. That is to say, it can be inferred that huge propagation packets produce denials of network service. In this situation, monitoring the usage rate of the network bandwidth may make it possible to detect a worm's propagation because network bandwidth is one of limited resources of the Internet and can be a sensitive factor in determining whether or not something wrong is occurring.

3.2 The previous research results

There is another study showing that the network bandwidth can be an important factor to determine a worm's propagation. According to Moore *et al*. [13], in principle, a host infected by Slammer can send propagation packets at 300,000 scans per second at 100 Mbps.

However, in practice, the host can send propagation packets at a maximum of 26,000 scans per second because of the limited network bandwidth and packet overhead found in the intermediate network nodes. This shows that Slammer can send its propagation packets at 4,000 scans/second in the early spreading phase over the Internet. The propagation phase of Slammer is reported to change from the exponential spread phase to the slow finish phase without a linear spread phase due to the limitations of network bandwidth. This is shown in **Fig. 4** and **Fig. 5**.

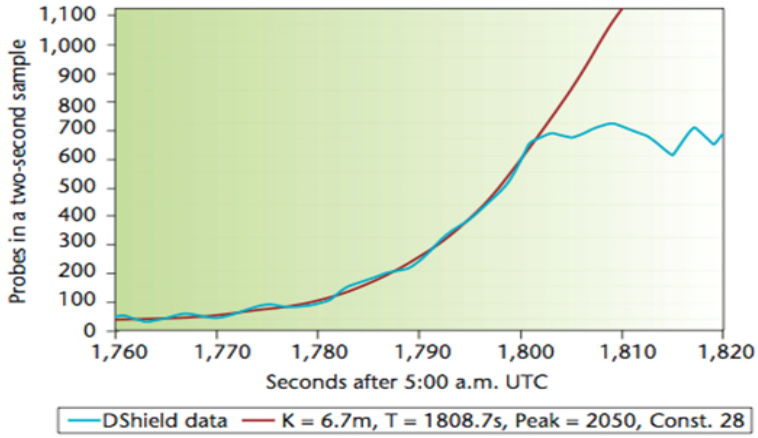

Fig. 4. The comparison between the RCS model and the Slammer data from the Distributed Intrusion Detection System (Dshield) data set

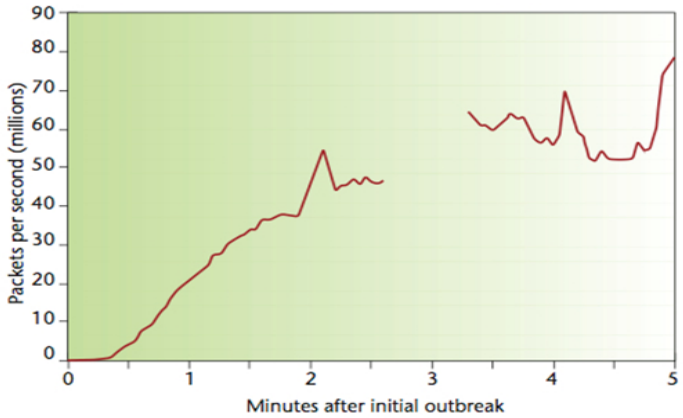

Fig. 5. The propagation of Slammer is measured at the University of Wisconsin Advanced Internet Lab (WAIL) tarpit, an unused network that logs packet traffic. The scanning rate is scaled to estimate the Internet-wide scanning rate. A transient data-collection failure temporarily interrupted this data set approximately two minutes and 40 seconds after Slammer began to spread

The two cases, both the analysis results of Code Red and the research results of Slammer, show that network bandwidth is the most important and sensitive factor that affects worm propagation. Therefore, the usage rate of the network bandwidth can make it possible to determine whether or not a worm is sending propagation packets.

4. The Network Bandwidth Usage Rate

The RCS model uses two factors: a susceptible host and an infected host. The former is a host that is vulnerable to a worm. The latter is a host that has been infected by a worm and sends propagation packets. Let N denote the number of susceptible hosts in a network, and β the scan rate of a worm. Additionally, let I denote the number of infected hosts. At time t, the increasing rate of the infected hosts dI_t/dt is defined as follows:

$$dI_t/dt = \beta I_{t-1}(N - I_t) \quad (1)$$

Equation (1) is the basic equation of the RCS model; the increasing rate of infected hosts continuously rises until all susceptible hosts are totally infected.

In this paper, (1) is used to define the network bandwidth usage rate. To simulate the network bandwidth usage rate by a worm using the random scanning strategy, several notations are defined. At time t, let WB_t and NB_t denote the network bandwidth usage rate used by the worm traffic and the normal traffic, respectively. The total network bandwidth usage rate TB_t can be defined as $TB_t = WB_t + NB_t$, however, during the propagation of a speedy worm in a short time, the usage rate of the normal traffic may be considered to be a constant value, that is, $NB_t=C$. Therefore, the total network bandwidth usage rate TB_t can be defined as $TB_t = WB_t + C$. The network bandwidth usage rate used by a worm is reported to be proportional to the worm's scan rate as well as the size of its propagation packet. The network bandwidth usage rate during the propagation of a worm can be derived from (1) as follows:

$$dWB_t/dt = \epsilon_{IPv4}\, I_t \beta P_{size}(B - WB_t) \tag{2}$$

In (2), the effective value, ε_{IPv4}, is a constant value that is defined by the portion of IPv4 addresses that are assigned by the Internet Assigned Numbers Authority (IANA) [17] as public IP addresses. According to the research results, the portion is about 65.2% except for reserved or private IP addresses; only 21.2% have not been allocated, with 13.7% reserved. These percentages are considered in this context as a sequence of 256 '/8s', where each '/8' corresponds to 16,777,216 unique address values. Actually, the reserved and unallocated portions are not vulnerable to a worm's propagation packets. Even though the distribution of valid addresses is geographically and hierarchically biased, various mechanisms like Classless Inter-Domain Routing (CIDR) or using a private IPv4 address can make the distribution uniform on the Internet in terms of network bandwidth. Additionally, only the random scanning strategy is addressed in our paper. The value P_{size} is the size of a worm's propagation packet, and B is the rate of the allocated network bandwidth. Using (2), the simulation results are presented later with the network bandwidth usage rate is explained as an effective factor to detect whether a worm propagates or not, dependant on a worm's scan rate or the size of its propagation packet. The RCS model, which uses the number of infected hosts, and the proposed model, which uses the network bandwidth usage rate, are simulated with a network simulator and compared to find which factor is more effective in detecting a worm's propagation.

5. The Simulation

One of popular network simulators, NS-2 [18], is used to draw concretely numerical values, and reliable results are presented using MATLAB [19] based on the drawn values. That is to say, it is difficult to define the network bandwidth usage rate over the Internet in specific defined values, so an abstract network is configured and reliable parameters are drawn. The abstract network organized using NS-2 is shown in **Fig. 6.**

The parameters (the number of nodes on the Internet, network bandwidth, and so on) for this simulation are based on previous research results. The size of a propagation packet is 404 bytes, the worm's scan rate is 4,000 scans per a second, and UDP protocol is used for the propagation.

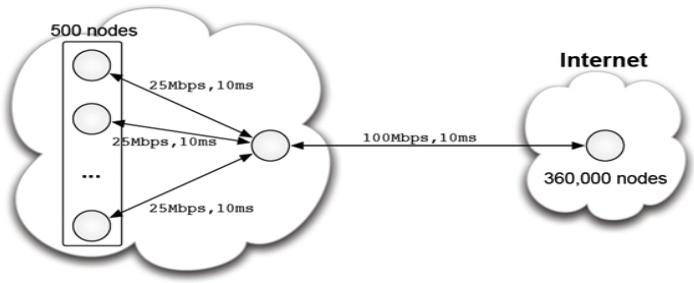

Fig. 6. The abstract network organization using NS-2

As seen in **Fig. 6**, the left side represents a protected network, and the right the Internet constituted with 360,000 nodes. First, a worm propagates within the right hand Internet side. Second, the number of infected hosts increases as time goes on, and finally, the worm propagates to the protected network on the left. In this case, when the allocated network bandwidth at the gateway of the protected network is 100 Mbps (the delay time is 10ms), the number of propagation packets passing through the network link is monitored during a time unit. After several simulations, about 13,200 propagation packets per time unit pass through the network link, and approximately 42.8% of network bandwidth is used. Based on these results, the ratio between a propagation packet and the number of propagation packets, that saturate the allocated network bandwidth, is 1 to 13,200. The correlation is simulated between the network bandwidth usage rate and either the scan rate or the propagation packet size using MATLAB. First, the simulation environment is configured to be similar to the propagation of a worm using the RCS model. All the hosts in this network are susceptible, and the four phases are present. An additional parameter K is used for this simulation. Staniford *et al.* [11] applied the value K, which is (the number of susceptible hosts) * (scan rate), to the Code Red model and determined that K to be 1.8 for the time scale of one hour. In this paper, we determined, however, that K is 1.4 after many scan rate trials for this simulation. The values of the parameters are shown in **Table 2**.

Table 2. The Summary of the Features of the New Internet Worms

Parameters	Values
Number of susceptible hosts	5×2^{16}
Scan rate	K / (the number of susceptible hosts)
Size of a propagation packet	1

After several simulations using these parameters, the simulation results of the RCS model using MATLAB are shown in **Fig. 7**. Next, as described in (2), ε_{IPv4} (= 0.6758), β (= $1.4/(5\times2^{16})$), and P_{size} (= 32) are set regardless of the simulation time t. The simulation results are shown in **Fig. 8**.

As seen in **Fig. 8**, the reason why the ratio of the network bandwidth on the y-axis is used is to prove that it is more sensitive, compared with the number of infected hosts used by the RCS model. The factor of the network bandwidth usage rate cannot be described with numerical values, so the relative ratio needs to be presented to explain the proportional values between our effective factor and that of the RCS model. Additionally, we simulated how a worm's scan rate affects the network bandwidth usage rate based on this fact; the correlation result is illustrated in **Fig. 9**.

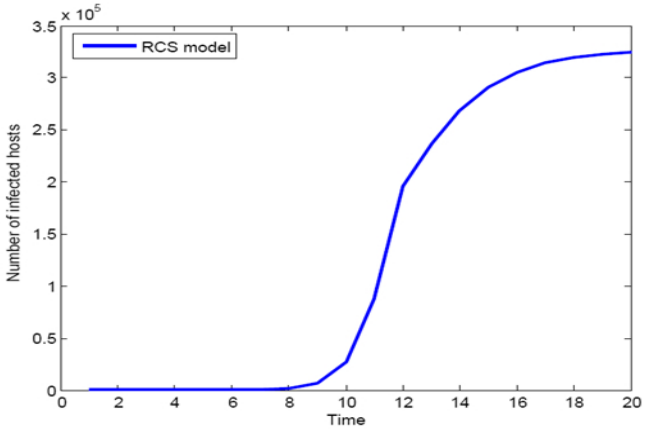

Fig. 7. The simulation results of the RCS model using MATLAB (The x-axis shows the simulation time, and the y-axis shows the number of infected hosts.)

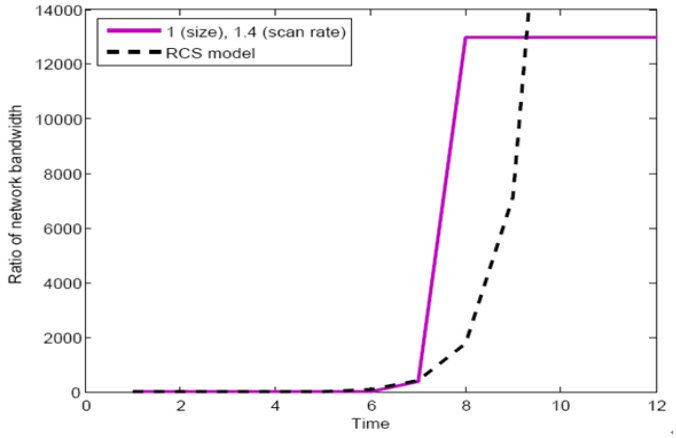

Fig. 8. The simulation result of the network bandwidth usage rate compared with the RCS model (the x-axis shows the simulation time, and the y-axis shows the relative network ratio of the bandwidth occupied by our proposed model.)

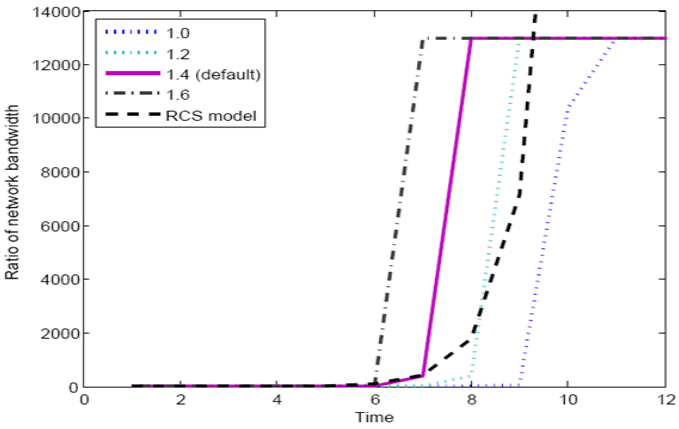

Fig. 9. The correlation between the network bandwidth usage rate and the worm's scan rate (the x-axis shows the simulation time, and the y-axis shows the relative ratio of the network bandwidth occupied by our proposed model.)

As seen in **Fig. 9**, when the ratio between the propagation packet and the number of propagation packets, which saturate the allocated network bandwidth (100 Mbps), is 1 to 13,200, it is shown that the required time to saturate the allocated network bandwidth varies. The default value of the scan rate, 1.4, definitely takes a shorter time to saturate the network bandwidth compared the RCS model. However, the smaller values of 1.0 or 1.2 occasionally take more time. The value of 1.6 takes the shortest time. Additionally, when the scan rate increases about 60%, from 1.0 to 1.6, it takes a shorter time, by approximately four times, to saturate the network bandwidth. Even though a worm's scan rate increases about 14.2% from 1.4 to 1.6 upon simulation, it takes just about one simulation time to saturate the allocated network bandwidth. These results show that the scan rate a worm uses has an affect on the network bandwidth usage rate and therefore the detection time of the worm on the network. Another simulation is illustrated in **Fig.10**. This includes the correlation results between the size of the worm's propagation packet and the network bandwidth usage rate.

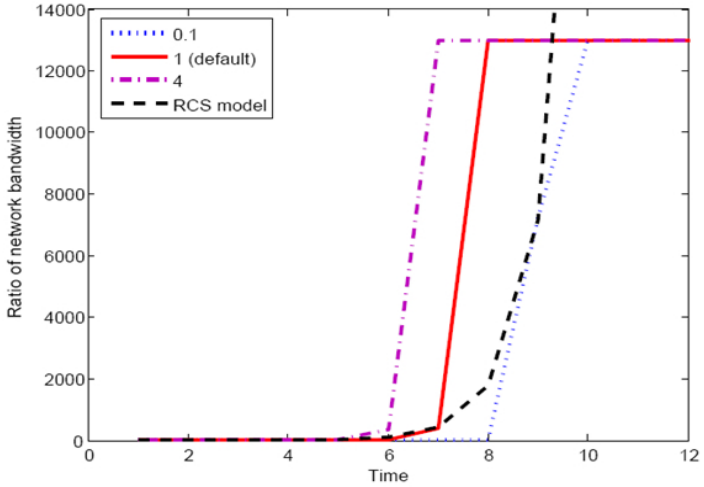

Fig. 10. The correlation between the network bandwidth usage rate and the size of the propagation packet (the x-axis shows the simulation time, and the y-axis shows the relative ratio of the network bandwidth used by our proposed model.)

As seen in **Fig. 10**, when the ratio between a worm's propagation packet and the number of propagation packets, which saturate the allocated network bandwidth (100 Mbps), is also 1 to 13,200, it is shown that the required time to saturate the allocated network bandwidth varies. In this simulation, three different packet sizes, 0.1, 1 (default), and 4, are used because the graph is drawn vertically for every size larger than 4, and the graphs are not explicitly presented when the size is 0.5 or when it is from 1.5 to 3.5, based on the simulation time unit.

The default value takes a shorter time to saturate the network bandwidth, however, the value, 0.1, takes much more time as compared to the RCS model. Even though the size of a propagation packet increases four times when moving from 1 to 4, it takes just one simulation time to saturate the network. Additionally, even though the size of the propagation packet increases forty times when moving from 0.1 to 4, it takes just about three simulation times to saturate the allocated network bandwidth. These results also show that the size of a propagation packet which a worm affects the network bandwidth usage rate and the detection time of the worm on the network. The simulation results shown in **Fig. 9** and **Fig. 10** explain that both the scan rate and the size of a worm packet can saturate the allocated network bandwidth, however, the detection time of the worm is delayed when the rate is low and the

size is small. So the usage rate of the network bandwidth is not always an effective factor to detect new emergent Internet worms. But when the features of the worms (as mentioned before) are considered, the network bandwidth is more effective than the number of infected hosts used by the RCS model. Additionally, considering the features of the new Internet worms, the smaller size of the propagation packet and the utilization of the faster scanning strategy can be related to the size of the worm's propagation packet and its scan rate, respectively. The latter is more sensitive than the former, as shown in the simulation results. This simulation is done assuming that the normal traffic is considered to be 0 ($TB_t = WB_t + 0$).

However, it may take a shorter time to saturate real networks, because normal traffic always exists ($TB_t = WB_t + C$). Consequently, the network bandwidth usage rate can allow the worms' propagation to be detected at an early stage, so more time is given to protect our valuable networks.

6. Conclusions and Future Work

There have been many research results and studies on modeling the propagations of various Internet worms. The RCS model is a well-defined propagation model based on the number of infected hosts.

However, it is difficult to explain the propagations of the new emergent Internet worms with the RCS model to ensure detection at an early stage. Additionally, the new worms have several considerable new features: the denial of service by network saturation, the utilization of the faster scanning strategy, the smaller size of the worm's propagation packet, and so cause maximum damage before human-mediated responses are possible. These features also make it difficult and much harder to notice when a worm propagates. Therefore, instead of the number of infected hosts, a more effective factor is required to detect new Internet worms.

In this paper, analysis and simulation results are presented about the propagation of worms using the random scanning strategy based on the network bandwidth usage rate, which can be considered to be a factor to detect the worms' appearances. The simulation results explain that the scan rate is more sensitive than the size of propagation packet in detecting the worms' propagation. There is a problem, a false-positive phenomenon, which is left for future work.

References

[1] Morris worm. http://en.wikipedia.org/wiki/Morris worm.
[2] Norman T. J. BAILEY, "The Mathematical Theory of Epidemics," *Hafner Publishing Co*, 1957.
[3] H.W. Hethcote, "The Mathematics of Infectious Diseases," *In SIAM Review*, vo.42, no.4, pp. 599-653, 2000.
[4] D.M. Kienzle, M.C. Elder, "Recent worms: a survey and trends," in *Proc. of the ACM Workshop on Rapid Malcode*, pp.1-10, 2003.
[5] S. Qing, W. Wen, "A survey and trends on Internet worms," *Computers & Security*, vol.24, pp. 334-346, 2005.
[6] C.C. Zou, D. Towsley, W. Gong, S. Cai, "Advanced Routing Worm and Its Security Challenges," *Simulation*, vol.82, no.1, pp.75-85, 2006.
[7] C.C. Zou, D. Towsley, W. Gong, "Modeling and Simulation Study of the Propagation and Defense of Internet Email Worm," *IEEE Transactions on Dependable and Secure Computing*, vol.4, no.2, pp.105-118, 2007.
[8] C.C. Zou, W. Gong, D. Towsley, L. Gao, "The monitoring and early detection of internet worms," *IEEE/ACM Transactions on Networking (TON)*, vol.13, no.5, pp.961-974, 2005.
[9] N. Provos, J. McClain, K. Wang, "Search Worms," in *Proc. of the 4th ACM Workshop on*

Recurring Malcode, pp.1-8, 2006.
[10] D. Moore, C. Shannon, G.M. Voelker, S. Savage, "Internet Quarantine: Requirements for Containing Self-Propagating Code," in *Proc. of IEEE Conference(INFOCOM 2003)*, 2003.
[11] S. Staniford, V. Paxson, N. Weaver, "How to Own the Internet in Your Spare Time," in *Proc. of the 11th USENIX Security Symposium*, pp.149-167, 2002.
[12] D. Moore, C. Shannon, "Code-Red: a Case Study on the Spread and Victims of an Internet Worm," in *Proc. of the 2002 ACM SIGCOMM Internet Measurement Workshop*, pp.273-284, 2002.
[13] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver, "Inside the Slammer Worm," *IEEE Security & Privacy*, vol.1, no.4, 2003.
[14] J.C. Frauenthal, "Mathematical Modeling in Epidemiology," *Springer-Verlag*, 1980.
[15] C.C. Zou, W. Gong, D. Towsley, "Code Red Worm Propagation Modeling and Analysis," in *Proc. of CCS02*, 2002.
[16] CAIDA (Cooperative Association for InternetData Analysis). http://www.caida.org.
[17] IANA (Internet Assigned Numbers Authority). http://www.iana.org.
[18] The network simulator: NS-2. http://www.isi.edu/nsnam/ns.
[19] The MathWorks. http://www.mathworks.com.

Kwang Sun Ko received a B.S. degree from Sungkyunkwan University, Korea, in 1997, a M.S. degree and Ph.D. degree from Sungkyunkwan University, Korea in 2004 and 2007, respectively. He is currently as a director with Financial Security Agency, Seoul and is a subject of biographical record in the Marquis Who's Who in the World 27th Ed., 2010. His research interests include network security, Linux, and security strategy.

Hyunsu Jang received a B.S. and M.S. degrees from Sungkyunkwan University, Korea, in 2002 and 2005. He is currently studying for the Ph.D. degree at the Department of Electrical and Computer Engineering, Sungkyunkwan University. His research interests include mobile agent, mobile agent systems, multi-agent system, and ubiquitous computing.

Byuong Woon Park received a B.S. degree from Hansung University, Korea, in 1997, a M.S. degree from Sungkyunkwan University, Korea, in 2002. He is currently studying for the Ph.D. degree at the Department of Electrical and Computer Engineering, Sungkyunkwan University. His research interests include mobile security, mobile agent, mobile computing, and distributed computing.

Young Ik Eom received a B.S., M.S. and Ph.D. degrees from the Department of Computer Science and Statistics of Seoul National University, Korea, in 1983, 1985 and 1991, respectively. He was a visiting scholar in the Department of Information and Computer Science at the University of California, Irvine from Sep. 2000 to Aug. 2001. Since 1993, he is a professor at Sungkyunkwan University in Korea. His research interests include distributed computing, system software, mobile agent systems and system security.