A New Worm Exploiting IPv4-IPv6 Dual-stack Networks

Qinhua Zheng[1], Ting Liu[1], Xiaohong Guan[1, 2], Yu Qu[1], Na Wang[1]

[1] SKLMS Lab and MOE KLNNIS Lab, Xi'an Jiaotong University, P. R. China

[2] Center for Intelligent and Networked Systems and TNLIST Lab, Tsinghua University, P. R. China

qhzheng@mail.xjtu.edu.cn, {tliu, xhguan, yqu, nwang}@sei.xjtu.edu.cn

ABSTRACT

It is commonly believed that the IPv6 protocol can provide good protection against network worms due to its huge address space. However, it is proved to be incorrect by our study on the new "dual-stack worm" which can spread in IPv4-IPv6 dual-stack networks. It is found in this paper that the dual-stack worm can collect the IPv6 addresses of all running hosts on the link-local quickly and effectively, which may result in accelerated worm spreading on the IPv6 link-locals. This worm applies a two-level scanning mechanism to find its targets in dual-stack networks, which is investigated by exploring its similarity to the self-replicating behaviors of biological viruses. Based on the ideas of classifying the population into different species or patches, we categorized all vulnerable hosts into two species and separated all dual-stack hosts into several patches to model the propagation of this worm by differential equations. Simulation is performed to validate the worm propagation model and to study the propagation of the worm in various dual-stack networks with different patch parameters. The simulation results show that the worm is able to spread much faster in IPv4-IPv6 dual-stack network than that in the pure IPv4 Internet. It is also noted that the dual-stack links may influence the propagation of the worm in the Internet.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection —*Invasive software.*

General Terms

Algorithms, Security

Keywords

Network security; IPv6; dual-stack network; worm propagation model

1. INTRODUCTION

In recent years, many IPv6 networks have been developed and deployed, such as "Internet 2" and "Moonv6" in US, "NRENs" in Europe, "JGN" in Japan, and "CNGI" in China [1]. Generally, the evolution from current IPv4 networks toward IPv6 would go from "isolated islands" to gradual global saturation, and the IPv4-IPv6 dual-stack would be the solution in the transition [2]. Much thought and attention have been paid to the transition to IPv6, and lots of works have already been started on evaluating the security implications during this period [3, 4]. Since the Internet has been plagued by many worms, it is desired to explore the activities of the worms in IPv4-IPv6 dual-stack networks.

The random address space scanning is the most popular mechanism adopted by the worms to detect vulnerable targets in IPv4 networks (for simplicity, random-scanning is used to represent it). The effectiveness of this mechanism attributes to the 32-bit IPv4 address which allows the random-scanning worms to scan all possible hosts [5, 6]. It is commonly believed that the IPv6 protocol can provide better protection against these worms due to its 128-bit address huge space, so that the probability to hit a valid address in the IPv6 address space by random-scanning is very low. Thus, the transition from IPv4 to IPv6 is considered as an effective approach to preventing worms from spreading [7].

It is found in this paper that the dual-stack worm can collect the IPv6 addresses of all active hosts on the link-local quickly and effectively, which may result in accelerated worm spreading on the IPv6 subnets. In fact, those "isolated IPv6 islands" would actually become the "hotbeds" for the dual-stack worm, especially in the worm-propagation starting phase. In other words, one infected host could infect all vulnerable hosts on the same link in a short time, while it may take much longer time to infect the hosts in IPv4 networks with random-scanning mechanism. As a result, the deployment of IPv6 is unable to prevent the propagation of worm as what was expected, but rather has opposite effect.

Since it is dangerous to release a real worm into actual networks, modeling and simulation are performed to analyze the characteristics of the worm propagation and to investigate the defense strategies. In this paper, the dual-stack worm is investigated by exploring its similar scanning strategy to the self-replicating behaviors of biological viruses. Learning form the epidemiologists who classify people into different species or patches according to their races, sexes and ages to study the propagation of biological viruses, we categorized all vulnerable hosts into two "species" and separated all IPv6 hosts into several "patches" to model the propagation of the dual-stack worm by differential equations [8]. Simulation is performed to validate the worm propagation model and to investigate the propagation of dual-stack worm in various dual-stack networks with different patch parameters. The simulation results show that the worm can spread in IPv4-IPv6 dual-stack network much faster than in the

This work is supported in part by NSFC (60574087, 60633020), 863 High Tech Development Plan (2006BAK11B02) and 111 International Collaboration Program of China.

WORM'07, November 2, 2007, Alexandria, Virginia, USA.

pure IPv4 Internet with random-scanning, and the structure of the IPv6 links may influence the propagation of the worm.

The rest of this paper is organized as follows. Section 2 surveys the related work. The IPv4-IPv6 dual-stack network and dual-stack worm are discussed in Section 3. The propagation of dual-stack worm is modeled in Section 4 and validated by comparing the results from model and simulators in Section 5. Section 6 is the conclusion of this paper.

2. RWLATED WORK

Since the breakouts of Morris in 1988, more and more attentions are paid to model and analyze the propagation of worms. Moore et al. for the first time used the Random Constant Spread (RCS) to model the spread of Code Red [9]. Zou et al. presented a "two-factor" worm model that considered the effects of both human countermeasures and congestion caused by extensive worm scan traffic [10]. Xie et al. proposed the random "moonwalks" to analyze the propagation of worms [11]. Griffin et al. explored the spread of worms in scale-free networks and showed that the speed of worm spreading is related to the scale-free structure of network [12]. Since we consider worm spreading in dual-stack networks, the propagation differences among different links are taken into account.

Many new worms have been investigated for preventing them from spreading. Staniford et al. showed that hit-list worm could spread to the whole Internet within a few minutes [13]. And Antonatos et al. pointed out that this worm could be prevented by randomizing the network address space [14]. Wong et al. analyzed network traffic traces and presented an in-depth study on the effects of two mass-mailing worms-"SoBig" and "MyDoom", and Ishibashi et al. investigated how to detect these worms by mining DNS traffic data [15, 16]. Chen et al. designed a self-learning worm, and demonstrated that this worm could accurately estimate the underlying vulnerable-host distribution [7]. Ma et al. studied the "self-stopping" worm, which made it harder for anti-worm mechanisms to identify the infected hosts by instructing infected hosts to halt infection activity after the vulnerable population is subverted [17].

In recent years, more and more researchers considered the security problem in IPv6 network. Warfield et al. discussed the security implications of IPv6 and proposed some solutions [3]. Convery et al. compared the threats between IPv6 and IPv4 and evaluated the mechanisms of those threats [4]. Yang simulated the propagation of random scanning worms in IPv6 networks, and presented several methods to reduce the IPv6 address space [18]. Kamra et al. showed that an intelligent worm could exploit the DNS necessary for any network, and modeled the behavior of such a worm in IPv6 Internet [5]. Bellovin et al. outlined a number of techniques that scanning worms can use in an IPv6 Internet to locate potential targets [6]. However, up to date, little work has been found on the simulation and analysis of worms in dual-stack networks.

3. DUAL-STACK WORM

3.1 IPv4-IPv6 Dual-stack Network

The key to a successful IPv6 transition is its compatibility with the IPv4 hosts and routers. Maintaining deploying IPv6 while keeping its compatibility with IPv4 will streamline the task of transiting the current Internet structure to IPv6. Dual-stack technology is considered to be the most straightforward mechanism for the IPv6 hosts to remain compatible with the IPv4-only hosts, as both IPv4 and IPv6 protocol stacks operate in parallel [2]. This technology is supported by most commercial OS, such as Windows XP/Vista and Red Hat 9.0. The dual-stack transition could be transparent to the users with three phases:

Starting phase: In this phase, the dual-stack islands start emerging with the hosts in these islands operating dual-stack. The islands are connected by IPv4 Internet, using various tunneling mechanisms, such as 6over4, 6to4, etc.

Growth phase: The IPv6 Internet in global scale marks this stage. More and more IPv4-only nodes run dual-stack connected by IPv6 links. Various applications would be updated to support IPv6 and more and more users are attracted by various particular IPv6 net services.

Mature phase: When the IPv6 Internet covers most parts once belonged to IPv4, IPv6-only hosts would gradually replace the dual-stack hosts, and accordingly IPv6-only network would finally take the place of dual-stack network.

Although the IPv6 Internet has already been deployed in many countries, the IPv4-IPv6 Internet is still at its infancy. Thus, the study of dual-stack worm propagation in this paper is mainly restricted to the first two phases.

3.2 Dual-stack Worm Analysis

Clearly the dual-stack network is a necessary in new Internet technology development. In order to spread rapidly in IPv4-IPv6 Internet, a two-level scanning strategy has been designed for the dual-stack worm to detect the vulnerable hosts. According to this strategy, the dual-stack worm could be separated into two attack stages: IPv6 attack and IPv4 attack, as Fig.1 shows.

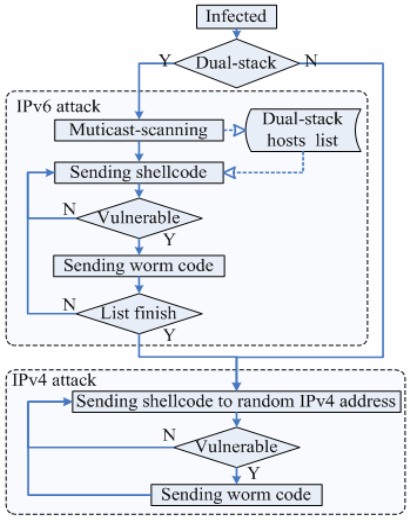


Fig.1 Flow chart of dual-stack worm

In IPv6 network, there are many information sources where the worm could collect the IPv6 address information of hosts, such as neighbor discovery (ND), routing tables, multicast ping and so on [6]. In our research, we discover the dual-stack hosts will respond when some packets has sent to the multicast IPv6 address. Thus,

the dual-stack worm collects the addresses of all active hosts on IPv6 link-locals by sending packets to that address, which called as multicast-scanning. Dual-stack worm send an Echo Request (ICMPv6 Type 128) or a spurious Router Advertisement (ICMPv6 Type 134) to FF02::1 (link-local scope all-nodes multicast address) [19, 20]. And then, the addresses of dual-stack hosts could be obtained from the respondent Echo Replay (ER) packets or Neighbor Solicitation (NS) packets. As shown in Fig.2, it is more expeditious and simple to acquire the addresses from the ER packets than the NS packets, because all ER packets will arrive in 0.1 second and the link-local address is recorded in the IPv6 header. All NS packets would be collected in 1 second. And we have to analyze the "Source Link-Layer Address option" of these NS packets to get the address. In the experiment, we discover that the Windows Vista will not reply to ICMPv6 Echo Requests, but will respond to spurious Router Advertisement, which applies the default configuration (see Fig.2.b). Therefore, the dual-stack worm could choose appropriate multicast-scanning mechanism to acquire the addresses of susceptible hosts as entirely and quickly as possible.

In the IPv4 attack stage, dual-stack worm creates the random IPv4 addresses by its stochastic number generator. Both of dual-stack or v4-only infected hosts applies this mechanism to find targets in the global IPv4 Internet.

Time	Source	Destination	Info	
4.021	fe80::216:ecff:fe20:73c	ff02::1	Echo request	
4.021	fe80::211:43ff:fec3:950	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::211:43ff:fec3:9c2	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::200:e2ff:fe5f:ad38	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::216:ecff:fe38:df7c	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::216:ecff:fe11:9c78	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::200:e2ff:fe42:be98	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::20d:87ff:fe61:aa08	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::214:2aff:fef2:dae	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::200:e2ff:fe4c:c7dc	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::219:21ff:fe0f:cf9e	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::20e:cff:fe3c:747b	fe80::216:ecff:fe20:73c	Echo reply	Victim F
4.021	fe80::216:ecff:fe33:aa02	fe80::216:ecff:fe20:73c	Echo reply	
4.021	fe80::20f:1fff:fec8:1114	fe80::216:ecff:fe20:73c	Echo reply	Victim E
4.025	fe80::216:ecff:fe1e:463	ff02::1:ff20:73c	Neighbor solicitation	
4.025	fe80::216:ecff:fe20:73c	fe80::216:ecff:fe1e:463	Neighbor advertisement	
4.026	fe80::216:ecff:fe1e:463	fe80::216:ecff:fe20:73c	Echo reply	

(a) ICMPv6 Echo Request

Time	Source	Destination	Info	
28.357	fe80::216:ecff:fe20:73c	ff02::1	Router advertisement	
28.383	::	ff02::1:ffc8:1114	Neighbor solicitation	Victim E
28.386	fe80::94d3:f4fe:78da:7ce8	ff02::16	Multicast Listener Report Message v2	
28.412	::	ff02::1:ff11:9c78	Neighbor solicitation	
28.452	::	ff02::1:ff21:3571	Neighbor solicitation	
28.470	::	ff02::1:ffc3:7be	Neighbor solicitation	
28.474	::	ff02::1:ffa1:3e0	Neighbor solicitation	
28.484	::	ff02::1:ff33:aa02	Neighbor solicitation	
28.491	::	ff02::1:ff20:73c	Neighbor solicitation	
28.564	::	ff02::1:ffda:7ce8	Neighbor solicitation	
28.564	fe80::94d3:f4fe:78da:7ce8	ff02::16	Multicast Listener Report Message v2	
28.586	::	ff02::1:ff1e:463	Neighbor solicitation	Windows Vista
28.600	::	ff02::1:fff2:dae	Neighbor solicitation	
28.601	::	ff02::1:ff9b:1699	Neighbor solicitation	
28.603	::	ff02::1:ffc3:aff	Neighbor solicitation	
28.611	::	ff02::1:ff35:9133	Neighbor solicitation	
28.707	::	ff02::1:ff3c:747b	Neighbor solicitation	Victim F
28.710	::	ff02::1:ff33:8dfc	Neighbor solicitation	
28.712	::	ff02::1:ffc3:950	Neighbor solicitation	

(b) Spurious Router Advertisement

Fig.2 The responses of multicast-scanning

3.3 Dual-stack Worm Propagation Experiment

To investigate the worm propagation, a dual-stack worm is developed to demonstrate its propagation characteristics in actual dual-stack networks. The dual-stack worm acquired the target addresses based on the two-level scanning strategy, and the worm program spreads to vulnerable hosts by exploiting DCOM RPC of Windows XP as W32.Blaster.Worm (first described in Microsoft security Bulletin MS03-026).

As shown in Fig.3, six victim hosts and one Releaser & Console host locate in the experimental network and connected by IPv4 Internet. There are two vulnerable hosts and twenty-eight immune hosts in dual-stack network 1, and three vulnerable hosts and thirty-five immune hosts in dual-stack network 2. Since only a few hosts are vulnerable, the dual-stack worm uses twelve parallel threads to detect whether the hosts are susceptible, and applies one port to send worm code. In the experiment, we discover that each thread needs about 3 seconds to detect an address and the attacked host needs 2 seconds to download the worm code. In the propagation experiment, all data packets are captured and recorded. On the basis of these packets, the propagation of the dual-stack worm is shown as a tree structure in Fig.4.

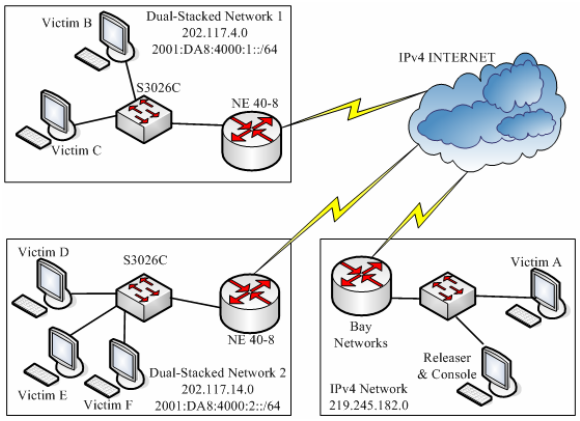


Fig.3 Experimental network structure

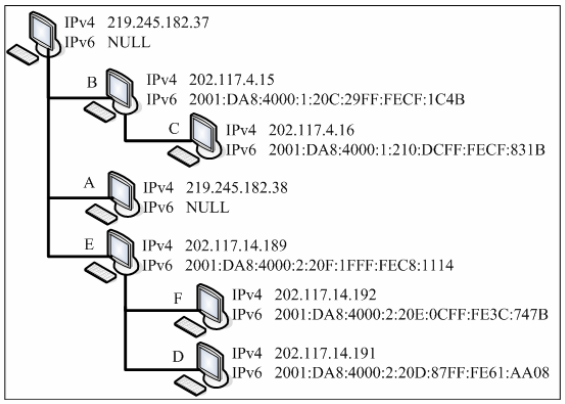


Fig.4 Tree chart of worm propagation

4. WORM PROPAGATION MODEL

It is difficult for one simple model to describe the propagating process of the dual-stack worm in the IPv4-IPv6 Internet, since this worm has different spreading characteristics on the different links, which is similar to the biological viruses spreading in different species. Therefore, according to the running stacks, all the vulnerable hosts were divided into two "species": IPv4-only nodes (Species A) and dual-stack nodes (Species B). Considering that the dual-stack nodes run dual-stack on the link-local and are connected together by the IPv4 links, we separated the Species B into m "patches" (expressed by B_1, B_2,…, B_m) which are the IPv6 subnets in actual network. This is similar to the method that the population is classified into different groups according to the races, sexes, and ages when the epidemiologists analyze how

viruses spread in human society. We firstly model the propagation of the dual-stack worm inside the species and patches, and then investigate how the worm spread across them. To facilitate the modeling, the notations are defined in Table 1.

4.1 Propagation in Species A

The dual-stack worm is able to select the scanning methods automatically. When an IPv4-only host is infected, it will directly use random-scanning to find the IPv4 nodes. Random-scanning worm propagation can be modeled by the classic susceptible-infected epidemic model. The rate of new infections in the model is given by:

$$\frac{dI(t)}{dt} = \frac{k \cdot S(t) \cdot I(t)}{\Omega}. \quad (1)$$

Once the vulnerable hosts have been detected, they could download the worm code in 2 seconds and run it immediately. The times of the infected hosts collect dual-stack host addresses or generate a random IPv4 address are very short. Therefore, we assume that the susceptible host will start to attack when it is scanned by an infected host.

Table 1. Notations in this paper

Notation	Definition
$I(t)$	Number of all infected hosts at time t
$I_A(t)$	Number of infected hosts in Species A at time t
$I_B(t)$	Number of infected hosts in Species B at time t
$I_{Bi}(t)$	Number of infected hosts in i^{th} patch at time t
$S_A(t)$	Number of susceptible hosts in Species A at time t
$S_B(t)$	Number of susceptible hosts in Species B at time t
$S_{Bi}(t)$	Number of susceptible hosts in i^{th} patch at time t
N_B	Number of dual-stack hosts in Species B
N_{Bi}	Number of dual-stack hosts in i^{th} patch
m	Number of the patches in Species B
q	Probability that a host is vulnerable
p	Probability that a scan hits an exist host
k	Average scan rate of infected hosts
Ω	The space of IPv4 address
τ	The duration of IPv6 attack

When a dual-stack host is infected, it will firstly use the multicast-scanning method to collect the addresses of all dual-stack hosts in link-local, and attack these address lasting about $\tau = N_{Bi} \cdot 3/12$ seconds (12 parallel attack threads and 3 seconds for each address). Then it will continue its attack in the same way as IPv4-only infected hosts. Thus, at time t, the vulnerable hosts can be attacked by two sources: the infected hosts in Species A -- $I_A(t)$; and the infected hosts in Species B at τ seconds before t -- $I_B(t\text{-}\tau)$. Thus, the infection model of dual-stack worm propagation in Species A is :

$$\frac{dI_A(t)}{dt} = k \cdot \frac{S_A(t)}{\Omega} \cdot [I_A(t) + I_B(t-\tau)]. \quad (2)$$

4.2 Propagation in Species B

Each vulnerable host in Species B could be found by the infected hosts with multicast-scanning or random-scanning. Therefore, $I_B(t)$ is divided into two kinds: $\overline{I_B}(t)$, found by multicast scanning; and $\underline{I_B}(t)$, found by random-scanning. If one host in the B_i patch has been infected, the probability of other vulnerable host on the same link to be detected by multicast-scanning within a unit time is $\overline{p} = k \cdot [I_{Bi}(t) - I_{Bi}(t-\tau)]/N_{Bi}$, and the probability found by the hosts with random-scanning is $\underline{p} = k \cdot [I_A(t) + I_B(t-\tau)]/\Omega$. The ratio between these two probabilities is:

$$\overline{p}/\underline{p} = \frac{\Omega \cdot [I_{Bi}(t) - I_{Bi}(t-\tau)]}{N_{Bi} \cdot [I_A(t) + I_B(t-\tau)]} \gg 1. \quad (3)$$

Assume $\underline{I}_{Bi}(t) = 1$, that is, the first host infected in B_i and represent this by the step function: $u(t\text{-}T_i)\text{-}u(t\text{-}T_i\text{-}\tau)$, where T_i is the time for the first host infected in the i^{th} patch and called as "the infection time" of i^{th} patch. Given these assumptions, we model the propagation of dual-stack worm in the i^{th} patch as bellow:

$$\begin{cases} \dfrac{d\overline{I_{Bi}}(t)}{dt} = \dfrac{k \cdot S_{Bi}(t)}{N_{Bi}} \cdot [\overline{I_{Bi}}(t) - \overline{I_{Bi}}(t-\tau) + u(t-T_i) - u(t-T_i-\tau)] \\ \overline{I_{Bi}}(t) = 0 \qquad t \le T_i \\ \underline{I}_{Bi}(t) = 1 \qquad t \ge T_i \end{cases}. \quad (4)$$

The dual-stack worm spreading in the different patches with various q and $S_{Bi}(0)$ is simulated. The duration for the worm to infect 99% of susceptible hosts on the same links are listed in the Table 2.

Table 2. Duration for dual-stack worm to infect 99% of the susceptible hosts in one link (seconds)

$q \backslash S_{Bi}$	5	10	20	40	80
0.2	5	6	7	7	8
0.1	10	11	12	13	15
0.05	18	20	23	25	28
0.02	52	66	81	98	>300

The results in Table 2 show that almost the entire link can be infected within τ seconds. Hence, the term $-\frac{k \cdot S_{Bi}(t)}{N_{Bi}} \cdot [\overline{I_{Bi}}(t-\tau) + u(t-T_i-\tau)]$ in (4) can be ignored and the analytical solution of model (4) is:

$$\begin{cases} \overline{I_{Bi}}(t) = \dfrac{S_{Bi}(0)}{1 + (N_{Bi} \cdot q - 1) \cdot e^{-k \cdot q \cdot (t-Ti)}} - 1 \qquad t > T_i \\ \overline{I_{Bi}}(t) = 0 \qquad t \le T_i \\ \underline{I}_{Bi}(t) = 1 \qquad t \ge T_i \end{cases}. \quad (5)$$

The worm with multicast-scanning propagates much faster than that with random-scanning. Substituting the process of worm spreading on the i^{th} patch by a step function:

$$\overline{I_{Bi}}(t) = (S_{Bi}(0) - 1) \cdot u(t - T_i - \theta_i), \quad (6)$$

where θ_i is the average infected time:

$$\theta_i = \frac{1}{S_{Bi}(0)-1}\cdot\int_{T_i^+}^{+\infty}\frac{d\overline{I_{Bi}}(t)}{dt}\cdot(t-T_i)\cdot dt = \frac{N_{Bi}\cdot\ln(S_{Bi}(0))}{(S_{Bi}(0)-1)\cdot k}. \quad (7)$$

When all susceptible hosts in species B are infected, the $\overline{I_B}(t)$ is:

$$\overline{I_B}(t)\Big|_{t=+\infty} = \sum_{i=1}^{m}(S_{Bi}(0)-1) = S_B(0)-m, \quad (8)$$

and $\underline{I_B}(t)$ is:

$$\underline{I_B}(t)\Big|_{t=+\infty} = I_B(t)-\overline{I_B}(t)\Big|_{t=+\infty} = m. \quad (9)$$

All of these m infected hosts are found by random-scanning, and distributed in m patches. The sequence -- i of each patch is rearranged to insure the infection time $T_i<T_{i+1}$.

4.3 Propagation in Dual-stack Networks

Assuming all dual-stack networks are uniform, we get $S_{Bi}(0)=N_B/m$, $\theta_i=\theta=N_B\cdot\ln(N_B/m)/(N_B-m)\cdot k$, $\tau=N_B/4\cdot m$. Replacing $S_{Bi}(0)$ and θ_i in (6), we derive the propagation model in Species B as:

$$\frac{d\overline{I_B}(t)}{dt} = \sum_{i=1}^{m}(\frac{N_B}{m}-1)\cdot\delta(t-T_i-\theta). \quad (10)$$

At time T_r, the first infected host is in B_r, and there is no infected host in the $B_{r+1},\ldots,B_m$. The average rate of worm-spreading in these patches before T_{r+1} is $f_r(t)$:

$$f_r(t) = \frac{k}{\Omega}\cdot[(m-r)\cdot\frac{N_B}{m}-(\underline{I_B}(t)-r)]\cdot[I_A(t)+I_B(t-\tau)]. \quad (11)$$

During $[T_r, T_{r+1}]$, $\underline{I_B}(t)$ is between r and $r+1$. Thus, $\underline{I_B}(t)-r$ in (11) is no more than 1, and much less then $(m-r)\cdot N_B/m$. Therefore, $f_r(t)$ can be approximated as:

$$f_r(t) = \frac{k}{m\cdot\Omega}\cdot(m-r)\cdot N_B\cdot[I_A(t)+I_B(t-\tau)]. \quad (12)$$

From (10) and (12), the model of worm propagating in species B can be written as:

$$\begin{aligned}\frac{dI_B(t)}{dt} &= \frac{d\overline{I_B}(t)}{dt}+\frac{d\underline{I_B}(t)}{dt}\\ &= \sum_{i=1}^{m}(\frac{N_B}{m}-1)\cdot\delta(t-T_i-\theta)+f_{i-1}(t)\cdot[u(T_i)-u(T_{i-1})]\end{aligned}, \quad (13)$$

where T_0=0.

At T_0, the average rate of the worm-spreading in Species B is $f_0(t)$, and thus the average time of the first infection patch -- T_1 is:

$$\int_{T_0}^{T_1} f_0(t)dt = \underline{I_B}(T_1) = 1. \quad (14)$$

With T_1 the average time of the each infection patch T_2, T_3,…, T_m can be calculated one by one based on:

$$\int_{T_r}^{T_{r+1}} f_r(t)dt = \underline{I_B}(T_{r+1})-r = 1. \quad (15)$$

In summary, the propagation model of dual-stack worm in IPv4-IPv6 Internet is expressed as:

$$\begin{cases}\dfrac{dI_A(t)}{dt} = k\cdot\dfrac{S_A(t)}{\Omega}\cdot[I_A(t)+I_B(t-\tau)]\\ \dfrac{dI_B(t)}{dt} = \sum_{i=1}^{m}(\dfrac{N_B}{m}-1)\cdot\delta(t-T_i-\theta)+f_{i-1}(t)\cdot[u(T_i)-u(T_{i-1})]\\ f_i(t) = \dfrac{k\cdot(m-i)\cdot N_B\cdot[I_A(t)+I_B(t-\tau)]}{m\cdot\Omega}\\ \int_{T_i}^{T_{i+1}} f_i(t)dt = 1 \qquad i=0,1\ldots m-1\\ \theta = \dfrac{N_B\cdot\ln(N_B/m)}{(N_B-m)\cdot k}\\ \tau = N_B/4\cdot m\end{cases}. \quad (16)$$

5. NUMERICAL SIMULATION AND COMPARATIVE STUDY

It is risky to release an actual worm into the Internet for simulating. In order to evaluate the performance of the propagation model developed in (16), a discrete time worm-propagation simulator based on the physical worm infection process is developed. How the dual-stack worm propages in the hybrid network is simulated by this simulator to compare with that calculated by the differential equation model (16).

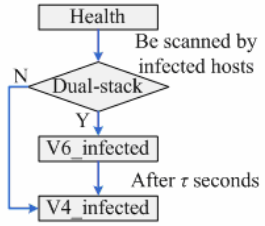


Fig.5 State transition of susceptible hosts

In the simulator, the parameters of the dual-stack worm are set as those of the well-known random-scanning worm - Code Red. We set the vulnerable host population N = 360000, $I_A(0)$ = 1 and $I_B(0)$ = 0 at the beginning. And the scan rate of infected host k follows normal distribution $N(240,100^2)$, which is slower than Code Red rate $N(358,100^2)$ [21]. Every susceptible host is defined as a node with several attributes, such as fixed ID number and scan rate, and variable node-states. Three node-states are defined in this simulator, and the transitions between the different node states are shown in Fig.5. Three modules: "Null", "Multicast-scan" and "Random-scan", are implemented to simulate the behaviors of the nodes in "healthy", "v6_infected" and "v4_infected", respectively. At each discrete-time interval, every node will run one scan module according to its state.

The propagations of dual-stack worm are simulated with several groups of parameters. In each group, 1000 samples run with the same parameters but different seeds from the random number generator. The sums of the infected nodes versus times in simulating these samples are ranked to reflect the propagation rate. Those corresponding to the 25th (top 2.5%), 500th (median), and 975th (bottom 2.5%) in terms of propagation rate are compared with that calculated by solving the differential equation (16). In present paper, the results in three different groups are shown in Fig 6. Results in group 1 are shown in Fig.6.a, where 10% of vulnerable hosts (36000) run dual-stack and are separated into 2000 subnets; results in group 2 are shown in Fig.6.b, where

20% of vulnerable hosts (72000) run dual-stack and are separated into 2000 patches; results in group 3 are shown in Fig.6.c, where 72000 vulnerable dual-stack hosts are separated into 6000 patches. It is observed that the mathematical model in (16) well matches the mean propagation rate of the dual-stack worm. We compared the dual-stack worm with Code Red and Blaster which are the well-known random-scanning worm and local-prefer scanning worm, respectively. Although both of them have faster scan rate than the dual-stack worm, the dual-stack worm could spread much faster than them, as shown in Fig.6.

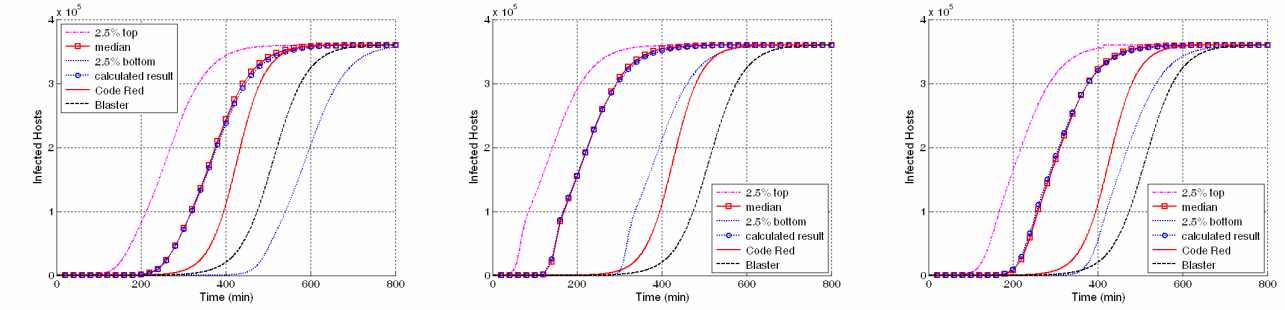
Although the dual-stack worm spreading rates are quite different, the shapes of the propagation curves are quite similar. The infection time spans among 1%, 10%, 50%, 90% and 99% of all vulnerable hosts infected are listed in Table 3. It is shown that the model in (16) can match these time spans pretty well and could be used to predict the propagation of the dual-stack worm.

We use worm-propagation model (16) to simulate the dual-stack worm spreading in different species, and show the results in Fig.7. The susceptible hosts in species B not only would be discovered by the all infected hosts in the network using random-scanning, but also would be attacked by the infected hosts in the same patch using multicast-scanning. Thus, before the worm infects half of all Species A, it has spread whole Species B. Therefore, the dual-stack worm spread with approximate speed after it has infected 50% of all susceptible ones. As previous assumption, the average scan rate of dual-stack worm is slower than that of Code Red, so the dual-stack worm spreads faster at the beginning, and slower at the end.

The equation (13) reveals that the large N_B and the small m can accelerate the propagation of dual-stack worm in Species B. And the equation (2) reveals that $I_B(t)$ can increase its spreading in Species A. That is why in the Group 2 the worm propagates faster, and the peak of the spreading speed is larger and comes earlier than others. Fig.6 and Fig.7 confirm that the propagation of the dual-stack worm is influenced by the structure of dual-stack networks.

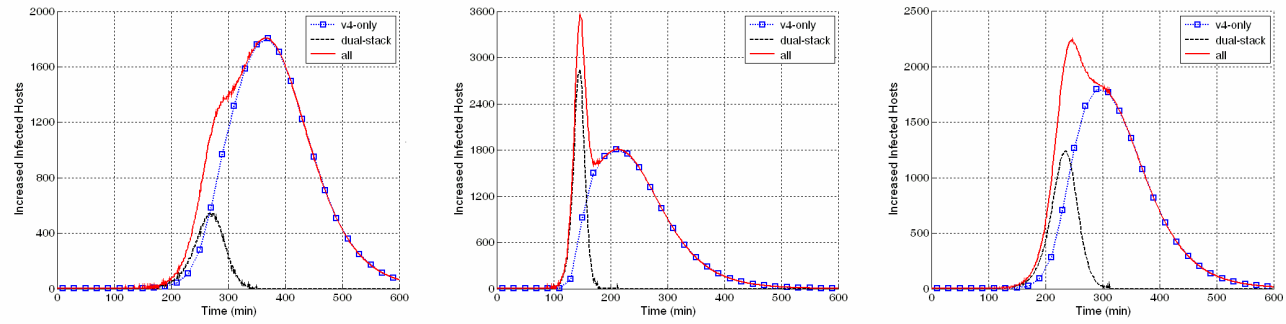
Table. 3 The time spans of the vulnerable hosts infected (min)

	Group 1: N_B =36000, m=2000				Group 2: N_B =72000, m=2000				Group 3: N_B =72000, m=6000				Code
	25th	500th	975th	model	25th	500th	975th	model	25th	500th	975th	model	Red
1%-10%	51	53	55	53	20	20	19	20	42	41	40	41	80
10%-50%	93	93	92	92	70	70	68	69	71	72	71	72	74
50%-90%	104	103	104	105	104	106	104	105	93	94	95	97	73
90%-99%	104	108	109	110	105	106	108	109	104	106	115	109	76



(a) Group 1: NB =36000, m=2000 (b) Group 2: NB =72000, m=2000 (c) Group 3: NB =72000, m=6000

Fig.6 The propagation comparison among the Dual-stack worm, Code Red and Blaster



(a) Group 1: N_B =36000, m=2000 (b) Group 2: N_B =72000, m=2000 (c) Group 3: N_B =72000, m=6000

Fig.7 The spreading rate comparison between dual-stack hosts and v4-only hosts

6. CONCLUSION

A dual-stack worm which can spread in IPv4-IPv6 dual-stack network is investigated in present paper. A two-level scanning strategy is applied by this new worm. The multicast-scanning is adopted to obtain the addresses of all active dual-stack hosts on the link-local in a few seconds, which accelerate the worm propagation in local subnets. The random IPv4 address space scanning is applied to find targets out of the link-local. By releasing the dual-stack worm into an experiment network, it is found and first demonstrated that this worm can exist and fast spread in an actual IPv4-Ipv6 dual-stack network. The spreading behaviors are modeled by classifying the vulnerable hosts into different "species" and "patches". The differential equations are proved to be effective and accurate enough to model the propagation of the dual-stack worm. Thus, it can be used for virus spreading prediction. The simulation results of the worm propagation show that the worms can spread faster in the next-generation Internet than that at the moment. It is also noticed that the structure of the network can influence the propagation of the dual-stack worm. Thus, it is necessary to consider the worm defenses in the future Internet construction.

7. REFERENCES

[1] T. Chown. IPv6 Initiatives within the European National Research and Education Networks (NRENs). Proc. Symposium on Applications and the Internet Workshops 2003.

[2] D. G. Waddington, F. Chang. Realizing the Transition to IPv6. IEEE Magazine of Communications, June 2002.

[3] M.H.Warfield. Security Implications of IPv6. [Online]. http://www.blackhat.com/presentations/bh-federal-03/bh-federal-03-warfield/bh-fed-03-paper-warfield.doc

[4] S. Convery, D.Miller. IPv6 and IPv4 threat comparison and best-practice evaluation (v 1.0). [Online]. http://seanconvery.com/v6-v4-threats.pdf.

[5] A. Kamra, H. H. Feng, V. Misra, A. D. Keromytis. The effect of DNS delays on worm propagation in an IPv6 Internet. In:Proc. of the IEEE INFOCOM 2005, 2005.

[6] S. Bellovin, B. Cheswick, A. Keromytis. Worm propagation strategies in an IPv6 Internet. [Online]. http://www.cs.columb ia.edu/~smb/papers/v6worms.pdf

[7] Z. Chen, C. Ji. A self-learning worm using importance scanning. Proc. ACM CCS 3nd Workshop on Rapid Malcode (WORM'05), November 2005.

[8] K Cooke, P Van den Driessche, and X Zou. Interaction of maturation delay and nonlinear birth in population and epidemic models. J. Math. Biol., 1999, 39: 332~352.

[9] D. Moore, C. Shannon, and J. Brown. Code-Red: A case study on the spread and victims of an Internet worm. Proc. 2nd ACM SIGCOMM Workshop on Internet Measurement, 2002.

[10] Cliff C. Zou, WB Gong, D. Towsley. Code Red worm propagation modeling and analysis. In: Proc. of the 9th ACM Symp. on Computer and Communication Security. 2002.

[11] Y. Xie, et al. Worm origin identification using random moonwalks. Proc. IEEE Symposium on Security and Privacy, 2005.

[12] C. Griffin, R. Brooks. A note of the spread of worms in Scale-free networks. IEEE Transactions on System, Man, Cybernetics, VOL. 36, NO. 1, Feb 2006.

[13] S. Staniford, D. Moore, V. Paxson, and N. Weaver. The top speed of flash worm. In: V. Paxson, ed. Proc. of the 2004 ACM Workshop on Rapid Malcode. 2004.

[14] S. Antonatos et al. Defending against hitlist worms using network address space randomization. Proc. ACM CCS 3nd Workshop on Rapid Malcode. 2005.

[15] C. W. Wong, S. Bielski, J. M. McCune, and C. Wang. A Study of Mass-mailing Worms. Proc. ACM CCS 2nd Workshop on Rapid Malcode (WORM'04), October 2004.

[16] K. Ishibashi, M. Ishino. Detecting Mass-Mailing worm infeceted hosts by mining DNS traffic data. Proc. SIGCOMM'05 Workshops on Mining Network Data. 2005.

[17] J. Ma, G. M. Voelker, and S. Savage. SelfStopping Worms. Proc. ACM CCS 3nd Workshop on Rapid Malcode. 2005.

[18] J. Yang. Fast worm propagation in IPv6 networks. http://www.cs.virginia.edu/~jy8y/FinalProjectReport.pdf

[19] A. Conta and S. Deering. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6. RFC 2463, Internet Engineering Task Force, Dec. 1998.

[20] T. Liu, Q. H. Zheng, X. H. Guan, X. Q. Chen and Z. M. Cai. Modeling and Analysis of Worm Propagation in IPv6 Networks. Chinese Journal of computers, VOL. 39, NO. 8, 2005.

[21] Cliff C. Zou, WeiBo Gong, Don. Towsley and Lixin Gao. The monitoring and early detection of Internet worms. IEEE/ACM Transactions on networking, VOL. 13, NO. 5, 2005.