IPv6 网络中蠕虫传播模型及分析

刘 烃 郑庆华 管晓宏 陈欣琦 蔡忠闽

(西安交通大学机械制造系统工程国家重点实验室 西安 710049)

(西安交通大学智能网络与网络安全教育部重点实验室 西安 710049)

摘 要 IPv6 网络由于其巨大的地址空间,通常被认为对随机扫描蠕虫有天然的抵御能力,该文研究了一种可以在 IPv6 网络中迅速传播的新型网络蠕虫(V6-Worm).基于对 V6-Worm 扫描策略的分析,分别建立简单传染病模型和双因素蠕虫模型来仿真 V6-Worm 的传播趋势.简单传染病模型的仿真结果证明,V6-Worm 拥有比随机扫描蠕虫更快的传播速度;双因素蠕虫模型的仿真结果证明,V6-Worm 拥有更强的对抗蠕虫控制措施的能力,同时在研究中发现主机中存在漏洞的比例是 V6-Worm 传播性能的主要影响因素.最后,文中从防止地址信息泄漏和降低主机存在漏洞比例两个角度,讨论了 V6-Worm 的防御策略.

关键词 IPv6;网络蠕虫;蠕虫扫描策略;蠕虫传播模型;蠕虫防御策略

中图法分类号 TP309

Modeling and Analysis of Worm Propagation in IPv6 Networks

LIU Ting ZHENG Qing-Hua GUAN Xiao-Hong CHEN Xin-Qi CAI Zhong-Min

(*State Key Laboratory for Manufacturing Systems Engineering, Xi'an Jiaotong University, Xi'an* 710049)

(*Key Laboratory for Intelligent Network and Network Security of Ministry of Education, Xi'an Jiaotong University, Xi'an* 710049)

Abstract It is a common belief that IPv6 could defend against random-scanning worms due to its huge address space. However, a new type of worm, V6-Worm, possibly propagating in IPv6 network rapidly, is presented in this paper. Based on the analysis of the scanning strategy of V6-Worm, two models——Simple Epidemic Model (SEM) and Two-Factor Model (TFM) are established for simulating the propagation of V6-Worm. The simulation results of SEM show that V6-Worm can propagate more rapidly in the IPv6 network than the random-scanning worm in the current IPv4 network. Furthermore the simulation results of TFM show that V6-Worm can counter the worm defense strategies better than the random-scanning worms. The results also indicate that the percentage of vulnerable hosts is the key factor affecting V6-Worm's propagating capability. Some defense strategies are discussed focusing on preventing address leakage and reducing the percentage of vulnerable hosts.

Keywords IPv6; Internet worm; worm scanning strategy; worm propagation model; worm defense strategy

---

收稿日期:2006-02-07;**修改稿收到日期**:2006-06-02.**本课题得到国家自然科学基金**(60243001,60574087)、**国家"八六三"高技术研究发展计划项目基金**(2003AA142060)**和国家杰出青年科学基金**(6970025)**资助**.**刘 烃**,男,1981 年生,博士研究生,主要研究方向为下一代互联网中的网络安全.E-mail:tliu@sei.xjtu.edu.cn;l-t@vip.163.com.**郑庆华**,男,1969 年生,教授,博士生导师,主要研究领域为网络信息安全、网络教育理论及技术.**管晓宏**,男,1955 年生,教授,博士生导师,主要研究领域为计算机网络信息安全、系统优化与调度.**陈欣琦**,女,1981 年生,硕士研究生,主要研究方向为下一代互联网中的网络安全.**蔡忠闽**,男,1975 年生,博士,讲师,主要研究方向为网络安全、数据挖掘理论及技术.

1 引 言

随着互联网日益成为人们生活必备条件的同时,它也逐渐成为恶意代码最主要的传播途径.从1988年Morris蠕虫爆发后,网络蠕虫一直是计算机网络安全的最大隐患之一,特别是近几年来,如Code Red、Slammer、WS32.Blaster、Witty等蠕虫的爆发,给整个互联网造成了巨大的损失[1~4].对于下一代网络协议——IPv6[5],人们通常认为:在其128位的巨大地址空间中,蠕虫将难以有效发现其它主机的确切地址,进而无法传播,所以IPv6被认为对蠕虫有天然的抵御能力,成为人们对抗蠕虫的希望[6,7].然而,随着网络性能的发展和蠕虫攻击手段的日趋多样化,蠕虫在IPv6网络中的传播性能逐渐成为人们关注的对象[8].

从网络行为的角度,蠕虫传播的研究主要集中在扫描策略和传播模型两方面.蠕虫利用系统漏洞进行传播之前,需要先进行目标探测.良好的扫描策略能够加快蠕虫的传播,加利福尼亚大学伯克利分校的Weaver等提出的使用理想扫描方式的蠕虫,理论上可以在30分钟内感染整个互联网[9,10].曾在实际IPv4互联网中造成巨大破坏的蠕虫大都采用基于网络层的随机扫描和顺序扫描策略,如Code Red和Slammer完全使用随机扫描,WS32.Blaster先随机扫描某个IP地址并顺序扫描该地址所在的整个网段[11,12].这些扫描策略大都需要对一定子网范围内IP地址进行逐一扫描,而在IPv6网络中一个子网就有64位的地址空间,这使得上述扫描方式无法对IPv6网络构成威胁.近些年来,学术界和地下黑客组织研究了很多基于应用层协议的扫描策略,这些策略不考虑网络层的结构,利用应用层服务的漏洞来获取目标的地址信息,使得蠕虫可以继续在IPv6互联网中传播,如利用即时通信服务网络进行传播的IM蠕虫[13].但基于应用层服务的蠕虫需要目标主机运行相应的服务,如IM蠕虫只能感染运行同类即时通信服务的主机,所以该类蠕虫的影响范围将小于基于网络层扫描策略的蠕虫.

基于对蠕虫传播机制的分析和各种网络条件对蠕虫传播的影响而建立的网络蠕虫传播模型,能够充分反映蠕虫的传播行为,识别网络蠕虫传播链中存在的薄弱环节,同时可以预测网络蠕虫可能带来的威胁.由于蠕虫和传染病的传播方式有着较大的相似性,在实际研究中常利用各种传染病动力学模型来建立蠕虫的传播模型,如常见的简单传染病模型(Simple Epidemic Model,SEM)、Kermack-Mckendrick模型[12].考虑到网络限制和人为控制等因素对蠕虫传播的影响,邹长春等人在对Code Red蠕虫的研究中,建立的双因素模型(Two-Factor Model,TFM)更是精确地仿真了蠕虫传播的整个过程[14].

本文为验证IPv6网络是否对蠕虫具有抵御能力,研究了一种专门针对IPv6网络的蠕虫——V6-Worm,通过对其扫描策略的分析,认为该蠕虫可以在IPv6网络中传播,并建立其传播模型进行仿真.仿真结果证明:在IPv6网络中,蠕虫不但可以继续传播,而且将具有更强的传播能力.由此,本文认为:IPv6网络本身并不能阻止蠕虫的传播,IPv6网络环境中蠕虫的发现、控制、防卫仍将是网络安全的挑战性问题.

本文第2节介绍并分析V6-Worm的扫描策略;第3节给出V6-Worm传播模型;第4节是仿真结果及分析;最后是全文总结和工作展望.

2 V6-Worm的扫描策略

2.1 V6-Worm的扫描策略

IPv6的单播地址为128位,其中后64位是接口标识符,可以由主机自动生成;前64位是子网标识符,需要通过配置来指派并进行有效性验证[5].为简化主机配置,IPv6同时支持有状态的地址自动配置[15](存在DHCPv6服务器时的地址配置)和无状态的地址自动配置[16](没有DHCPv6服务器时的地址配置).在无状态的地址配置中,链路上的主机可以自动配置链路本地地址,并根据路由器发送的路由器公告(Router Advertisement,RA)报文,自动配置站点本地地址和全球单播地址,具体过程如图1所示.

如图2所示,在实验中31台的IPv6主机通过两个交换机(D-Link DES1024R)连接到IPv6路由器(华为NE40)上,再通过该路由器连接到CERNET2(中国第二代教育科研网).当感染了V6-Worm的主机A将一个伪造的RA报文发送到网络中,其目标IP地址为所有节点(all-node)多播地址(FF02::1),源IP地址为感染V6-Worm主机的本地链路地址.本链路中的节点收到该伪造的RA报文后,将根据该报文的路由器信息为自己配置新的全球单播或者站点本地地址.为了保证新配置的地址在本地链路

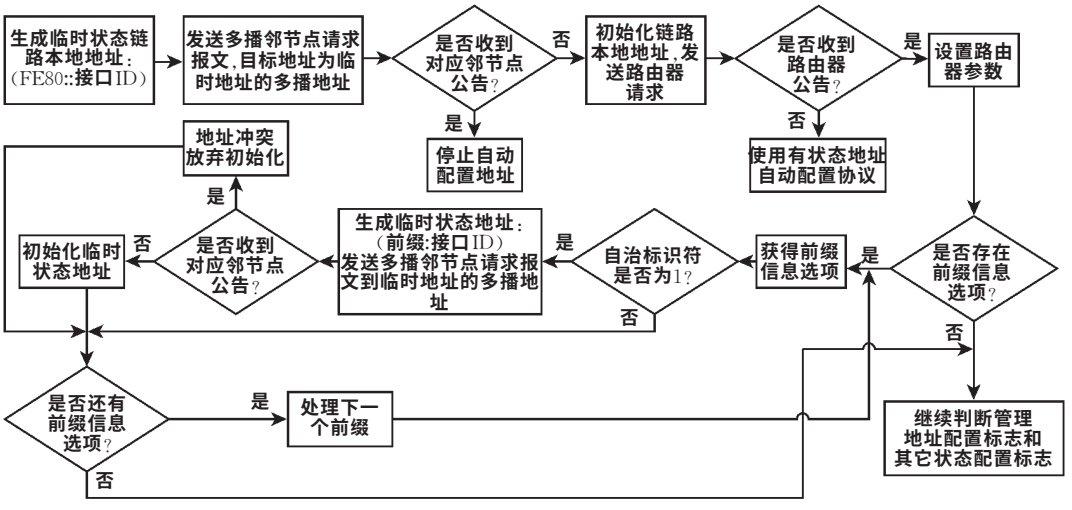


图 1　主机地址的自动配置过程

内具有唯一性，本地链路中所有节点都必须先进行重复地址检测(Duplicate Address Detection，DAD)过程，在该过程中每个节点都需要向特定多播地址发送多播侦听报告(Multicast Listener Report，MLR)报文和邻节点请求(Neighbor Solicitation，NS)报文[16,17]. 由于这些报文是为了验证自动配置所生成的地址是否与本地链路内其它节点的地址有重复，所以本地链路内每一台 IPv6 主机都将收到来自其它主机的验证报文.

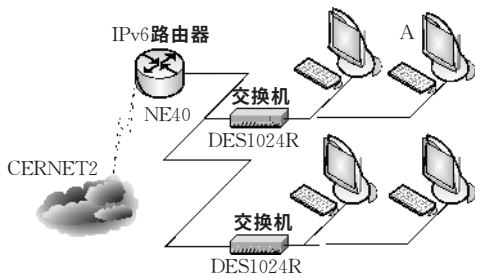


图 2　IPv6 实验网络结构图

如图 3 所示，通过对网络进行监听，可以捕获到各个节点所发送的多播报文，在分析这些报文时发现：MLR 报文的源 IP 地址字段即为该节点的本地链路地址；NS 报文的目标地址(target address)字段为该节点申请的全球单播地址. V6-Worm 无需对整个 IPv6 巨大的地址空间进行全面扫描，只要发送一个伪造的 RA 报文，即可通过分析其它节点响应的报文得到所有本地链路中在线主机的地址信息. 基于这些地址信息，V6-Worm 不仅可以确定后续攻击和传播目标的 IP 地址，而且可以保证这些目标就是当时本地链路中所有的在线主机，从而快速感染整个子网.

当感染了 V6-Worm 的主机完成对本地子网的

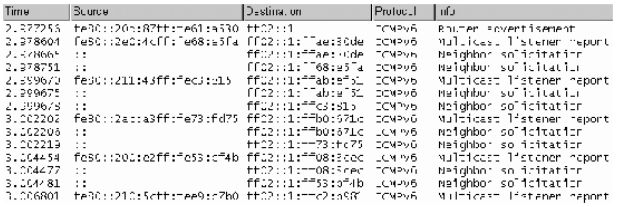


图 3　伪造的 RA 报文和链路中节点的响应报文

攻击后，可以利用各种基于应用层服务的蠕虫扫描机制进行子网间的传播，如利用 IM 蠕虫[13]、DNS 蠕虫[8]等. 由于应用层扫描策略不受 IPv6 网络的限制，而 V6-Worm 又可以全面快速地感染整个 IPv6 子网，这将使得蠕虫在整个 IPv6 网络中快速传播. 应用层蠕虫已经被众多学者广泛研究，所以本文接下来部分将着重研究 V6-Worm 在子网内的传播模型.

2.2　V6-Worm 传播性能的假设

V6-Worm 与 IPv4 中的随机扫描蠕虫的重要区别在于扫描策略：后者需要通过对整个地址空间的扫描来确定攻击目标；而 V6-Worm 仅仅只攻击在线的 IPv6 主机. 显然，不论是从效率还是从隐蔽性上来看，V6-Worm 都要优于后者. 尽管随机扫描蠕虫为提高命中率，也进行了很多改进，如基于路由的扫描方式、基于 DNS 的扫描方式[12]等，但由于得不到网络的拓扑结构，无法避免对无效地址的探测，所以效率上不可能超越 V6-Worm，由此提出本文的第一个命题.

命题 1.　相比随机扫描蠕虫，V6-Worm 在本地链路内具有更快的传播速度.

在 IPv4 网络中，存在一种理想化的蠕虫——Flash 蠕虫，它假定每个感染源都拥有整个网络中所有存在漏洞主机的地址列表，它们随机地在这些

相同的地址列表中选择攻击目标，可以保证每次攻击都能命中一台存在漏洞的主机，使得在蠕虫爆发的初期每次的攻击都将增加一个感染源，瞬间攻陷整个互联网[11,12]. 但是当今互联网结构复杂，主机的信息也在不断更新，漏洞主机的地址信息难以获得，而且也不可能实时更新；另一方面庞大的漏洞主机地址列表将远远超过蠕虫本身的大小，很难将其随着蠕虫的传播而传递，所以 Flash 蠕虫更多是用来描述蠕虫攻击的上限速度和极限条件. V6-Worm 是动态获取本地链路中所有正在运行的 IPv6 主机地址列表，如果能找到普及率更高的漏洞，使得蠕虫的攻击可以对大部分系统有效，V6-Worm 将成为至今为止最接近蠕虫传播理论上限速度的实际蠕虫. 鉴于是理想化的蠕虫，即使在考虑各种影响因素的网络环境中，也可以迅速传播，甚至可以赶在人们采取相应大规模控制措施之前感染整个互联网[9]. 由此提出本文的第二个命题.

命题 2. 相比随机扫描蠕虫，V6-Worm 在本地链路内将拥有更强的对抗外界影响的能力.

3 V6-Worm 的传播模型

为了验证在传播速度和对抗外界影响因素能力两方面，V6-Worm 是否比随机扫描蠕虫具有更好的性能，本文中特意利用在研究 Code Red 蠕虫时较为成熟的两种模型：SEM 和 TFM，为 V6-Worm 建立其在 IPv6 网络环境中的传播模型.

3.1 简单传染病模型

本小节的分析基于以下假设：① 网络中所有的主机只存在三种状态：免疫、易被感染和感染源；② 处于易被感染状态的主机一旦被处于感染源状态的主机攻击，马上变成感染源并保持状态不变，而免疫主机始终保持免疫状态；③ 在相同的网络内，假设每一个主机有相同的概率被感染源攻击，同时每一个感染源也以相同的概率攻击其它主机.

为了方便描述，给出以下变量定义：

N 表示系统内主机总数；

V 表示系统中存在的易被感染主机和感染源总数；

$I(t)$ 表示在时刻 t 感染源的数量；

$S(t)$ 表示在时刻 t 易被感染的主机数，且满足 $V=S(t)+I(t)$；

k 表示感染源平均攻击速度.

在时间 δ 内，某台感染了 V6-Worm 的主机 A 将产生 $k\delta$ 次攻击，对于一台特定的易被感染的主机 B，被 A 攻击到的概率为

$$\begin{aligned} p &= 1-(1-1/N)^{k\cdot\delta} \\ &= 1-[1-k\cdot\delta/N+k\cdot\delta\cdot(k\cdot\delta-1)/(2\cdot N^2)-\cdots] \\ &\approx k\cdot\delta/N \end{aligned} \tag{1}$$

在时刻 t，感染源的数量为 $I(t)$，易被感染主机的数量为 $V-I(t)$. 由于地址列表中每个节点只会有一条记录，所以主机 A 不会重复攻击同一台主机，由此推断 A 的有效攻击（攻击到易被感染主机）次数为 $[V-I(t)]p$. 若 δ 足够小，则可以不考虑在时刻 t 到 $t+\delta$ 的时间内，两个感染源攻击同一台易被感染主机的情况，由此推论出在 t 到 $t+\delta$ 的时间内，被攻击到的易被感染的主机数量为 $I(t)[V-I(t)]p$. 那么在时刻 $t+\delta$ 有

$$I(t+\delta)=I(t)+I(t)\cdot[V-I(t)]\cdot k\cdot\delta/N \tag{2}$$

取 $\delta\to 0$，可以得到

$$\begin{aligned} \mathrm{d}I(t)/\mathrm{d}t &= I(t)\cdot[V-I(t)]\cdot k/N \\ &= G\cdot I(t)\cdot[V-I(t)] \end{aligned} \tag{3}$$

其中 G 称为感染因子，表达式为

$$G=k/N \tag{4}$$

设在 $t=0$ 时，感染源的初始值为 $I(0)$，方程(3)的解析解为

$$I(t)=\frac{I(0)\cdot V}{I(0)+[V-I(0)]\mathrm{e}^{-GVt}} \tag{5}$$

考虑到 V6-Worm 在攻击之前，需要获取本地链路内正在运行的 IPv6 主机地址列表，而该过程包括公告伪造 RA 报文并等待其它节点的响应报文，这意味着每一个易感主机在成为感染源之后，并不能第一时间具有向外攻击能力. 为了描述这种延迟，本文参照传染病研究中的对疾病潜伏期的描述方式[18]，加入延迟因子 ξ——被攻击的易被感染主机需要经过时间 ξ 才能变成新的感染源，代入表达式(3)得到考虑延迟因子的 V6-Worm 传播模型

$$\mathrm{d}I(t)/\mathrm{d}t=G\cdot I(t-\xi)\cdot[V-I(t)] \tag{6}$$

而对于基于随机扫描的蠕虫，由于其探测的空间不是确切的主机列表，而是某些地址空间，假设探测的地址空间为 Ω，可以推断其传播模型与 V6-Worm 相似，它们的区别仅仅在于前者的感染因子 $G_{v4}=k/\Omega$.

3.2 双因素蠕虫模型

蠕虫在实际环境中传播时，将受到很多因素的影响，其中存在两个在 SEM 中不曾考虑，却又无法忽视的因素[15]：

(1) 人为控制. 当蠕虫开始传播时，网络或者主

机的使用者将逐渐发现蠕虫的行为，并进行各种控制操作，如升级系统，启动防火墙，清除主机上蠕虫等等，这些措施使得主机从已感染和易被感染的状态转化成免疫状态，限制蠕虫的快速传播；

(2) 蠕虫自身干扰. 蠕虫在传播过程中产生的流量不单影响正常网络访问，同时也将对自身的传播起到限制作用，这一点主要表现在感染因子不再是一个常量，它与网络中感染源的数量有关.

考虑到人为控制将使得已感染和易被感染状态的主机变成免疫状态，V 将不再是一个常量，设为 $V(t)$. 同时把人为控制的结构分成两个部分：易被感染主机通过人为控制成为免疫主机，记为 $X(t)$；已被感染主机通过人为控制成为免疫主机，记为 $Y(t)$，应满足 $V(t)=V(0)-X(t)-Y(t)$. 设已被感染主机恢复因子为 λ，使得 $Y(t)$ 满足

$$\mathrm{d}Y(t)/\mathrm{d}t=\lambda \cdot I(t) \tag{7}$$

而人为控制对易被感染主机的影响取决于两个因素：当前存在的易被感染主机总数 $S(t)$，存在漏洞的主机越多，单位时间内可能转变的也会越多，即 $X(t)$ 与 $S(t)$ 成正比；曾被感染过的主机总数越多，蠕虫将受到越多关注，导致恢复速度加快，所以 $X(t)$ 与 $[I(t)+Y(t)]$ 也成正比. 设易被感染主机恢复因子 μ，使得 $X(t)$ 满足

$$\mathrm{d}X(t)/\mathrm{d}t=\mu \cdot S(t) \cdot [I(t)+Y(t)] \tag{8}$$

考虑到蠕虫传播产生的流量会限制自己的传播速度，建立关于 $G(t)$ 的模型

$$G(t)=G(0) \cdot [1-I(t)/V(t)]^{\eta} \tag{9}$$

其中 η 用于调整 $G(t)$ 对于 $I(t)$ 敏感程度. 当 $\eta=0$ 时，$G(t)$ 为常数，即不考虑蠕虫传播对自身的干扰.

把表达式(7)和(9)代入式(6)，建立感染源主机的模型

$$\mathrm{d}I(t)/\mathrm{d}t=G(t) \cdot I(t-\xi) \cdot S(t)-\lambda \cdot I(t) \tag{10}$$

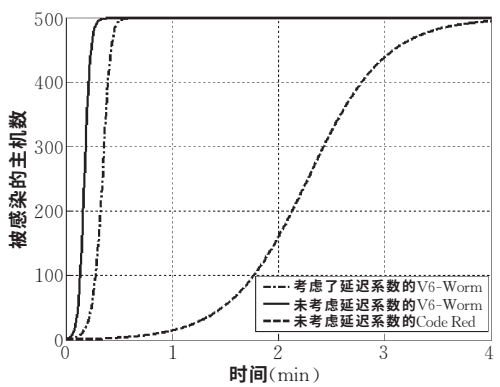
利用上述结论，总结出完整的双因素蠕虫传播模型：

$$\begin{cases} \mathrm{d}I(t)/\mathrm{d}t=G(t) \cdot I(t-\xi) \cdot S(t)-\lambda \cdot I(t) \\ \mathrm{d}X(t)/\mathrm{d}t=\mu \cdot S(t) \cdot [I(t)+Y(t)] \\ \mathrm{d}Y(t)/\mathrm{d}t=\lambda \cdot I(t) \\ G(t)=G(0) \cdot [1-I(t)/V(0)]^{\eta} \\ V(t)=V(0)-X(t)-Y(t)=I(t)+S(t) \\ V(0)=V_0;\ I(0)=I_0;\ S(0)=V_0-I_0 \\ G(0)=k/\Omega;\ X(0)=Y(0)=0 \end{cases} \tag{11}$$

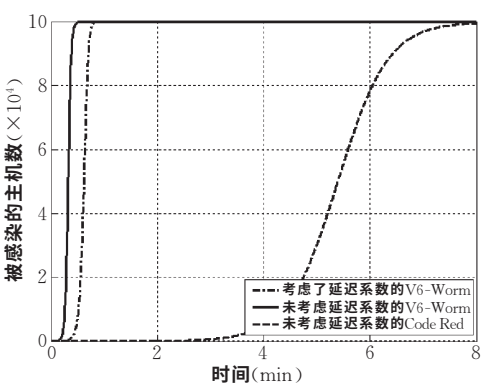
4　仿真结果分析及控制策略

4.1　基于 SEM 对 V6-Worm 传播速度的分析

为了比较 V6-Worm 与随机扫描蠕虫的传播速度，首先基于 SEM 对 Code Red 蠕虫(典型的随机扫描蠕虫)进行了仿真实验. 假设 Code Red 以平均攻击速度 $k=358/\mathrm{min}$[19]，在一个存在 5000 台主机的 B 类网(拥有约 2^{16} 个 IP 地址)和一个存在 1000000 台主机的 A 类网(拥有约 2^{24} 个 IP 地址)中传播①，其中 10% 的主机存在可利用的漏洞. 再将上述两个子网都移植到 IPv6 子网中(IPv6 的子网地址空间为 2^{64})，假设 V6-Worm 的延迟时间为 $\xi=2\mathrm{s}$，并与 Code Red 具有相同的平均攻击速度 $k=358/\mathrm{min}$，基于 SEM 得到其仿真结果如图 4 所示.



(a) 在B类网规模网络中的仿真结果



(b) 在A类网规模网络中的仿真结果

图 4　V6-Worm 与 Code Red 传播速度的对比

在实验假设的 B 类网中，Code Red 感染 90% 的主机需要 3.079min，感染 99% 的主机需要 3.957min；而在相同规模的 IPv6 子网中，即使考虑

① 参见 http://www.geohive.com/global/geo.php?xml=ec_inet&xsl=ec_inet，互联网上有 267541177 台主机，占用整个 IPv4 地址空间的 6.2%，为了统计方便设 B 类网中有 5000 台，占地址空间的 7.8%，A 类网中有 1000000 台，占地址空间的 6%.

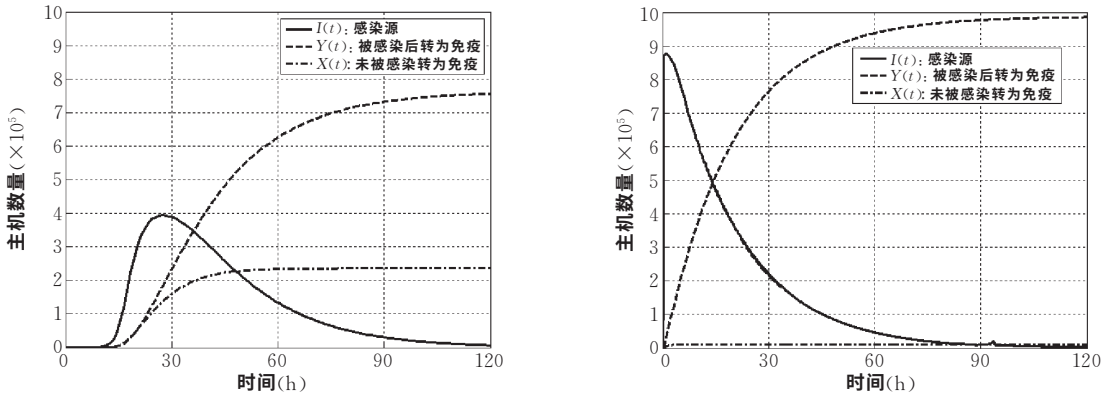
了延迟因子的 V6-Worm 感染相同比例主机分别只需要 0.423 min 和 0.495 min，仅为前者需要时间的 13.74%和 12.51%.

在实验假设的 A 类网中，Code Red 感染 90%的主机需要 6.425 min，感染 99%的主机需要 7.549min；而在相同规模的 IPv6 子网中，即使考虑了延迟因子的 V6-Worm 感染相同比例主机分别只需要 0.702 min 和 0.774 min，仅为前者需要时间的 10.93%和 10.25%.

从 SEM 的仿真结果可以发现：即使考虑了延迟因子的影响，V6-Worm 在本地链路内的传播速度也要远远超过 Code Red 在 IPv4 子网中的传播速度，由此证明命题 1 成立.

4.2 基于 TFM 对 V6-Worm 传播范围的分析

为了比较 V6-Worm 与随机扫描蠕虫的传播范围，首先假设 Code Red 在整个 IPv4 网络中传播（拥有 2^{32} 个 IP 地址），参照邹长春等人对 Code Red 研究的结论，对 TFM 中的参数做如下设定：$N=10000000$，$V_0=1000000$，$I_0=1$，$\eta=3$，$\mu=0.06/V_0$，$\lambda=0.05$，$G_{V4}(0)=0.8/V_0$，得到仿真结果如图 5(a)所示. 再将上述网络移植到 IPv6 子网中，并假设 V6-Worm 的传播速度和恢复速度与 Code Red 的相同，基于表达式(4)得到 $G_{V6}(0)=340/V_0$，其它参数保持不变，得到仿真结果如图 5(b)所示.



(a) Code Red的传播仿真结果　　(b) V6-Worm的传播仿真结果

图 5　V6-Worm 与 Code Red 传播范围的对比

仿真结果显示，在蠕虫传播的初期，Code Red 在时刻 $t=27.5$ 时达到传播的顶峰，网络中处于感染源状态的主机达到 394600 台占到 V_0 的 39.46%；V6-Worm在时刻 $t=1.1$ 时即达到传播的顶峰，较前者快 24 倍，而网络中处于感染源状态的主机达到 878100 台占到 V_0 的 87.81%，为前者的 2.28 倍. 当蠕虫的影响结束时，在 Code Red 的仿真结果中发现有 236600 台存在漏洞的主机在被感染前已经免疫，而在 V6-Worm 的仿真结果中仅有 11100 台，为 Code Red 的 4.7%.

从 TFM 的仿真结果可以发现：V6-Worm 在存在各种干扰因素的网络环境中，其感染能力要远远超过 Code Red，由此证明命题 2 成立.

4.3 V6-Worm 的关键参数分析

比较 V6-Wom 和随机扫描蠕虫的传播模型，差别在于攻击的地址空间 Ω，如 4.2 节的模型，对于 V6-Worm 其攻击目标的空间为 $\Omega_{V6}=N=10000000$，而对于随机扫描蠕虫该值为 $\Omega_{V4}=2^{32}=4294967296$，表达式(4)显示感染因子与探测、攻击的空间成反比，推得两种蠕虫感染因子的初值相差 429 倍，这导致 V6-Worm 传播速度远远超过随机扫描蠕虫. 通过分析表达式(5)发现：$I(t)$ 的传播趋势主要取决于分母部分的指数函数 e^{-GVt}，其中

$$G \cdot V = k \cdot V/N = k \cdot \rho \qquad (12)$$

$\rho=V/N$ 表示存在漏洞主机在所有主机中的比例. 当平均攻击速度 k 一定时，ρ 将决定 V6-Worm 的传播性能. 沿用 3.3.2 节中的模型，在 ρ 取不同值的情况下进行仿真实验，仿真结果如图 6 所示.

仿真结果显示，当 ρ 达到 100%时，V6-Worm 将与 Flash 蠕虫具有相似的传播特性——瞬间感染整个网络中所有存在漏洞的主机；随着 ρ 的下降，蠕虫达到传播顶峰所需的时间逐渐增加，并且在顶峰时感染源主机所占的比例也逐渐下降；当 $\rho=0.023\%$ 时（在 2^{32} 台主机中有 1000000 台存在漏洞），V6-Worm 与 Code Red 呈现出相似的传播速度和感染范围.

上述仿真结果证明：存在漏洞的主机在所有主机中的比例是影响 V6-Worm 传播的主要影响因素；V6-Worm 传播的速度和传染范围与其所针对系统漏洞的普及率成正比.

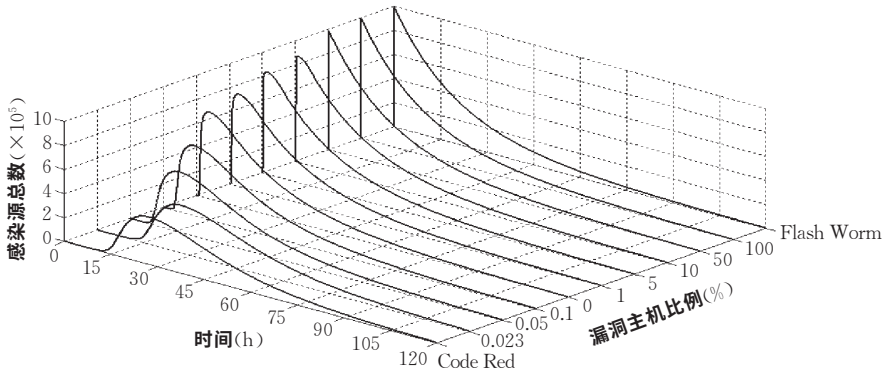


图 6　V6-Worm 在不同漏洞主机的比例子网中的传播模型

4.4　V6-Worm 的防御策略

通过对 V6-Worm 传播模型(6)和(11)的分析，发现 V6-Worm 最大的特点就是拥有更快的目标获取机制和更精确的攻击范围. 对此，本文基于 IPv6 网络的特点从阻止蠕虫获得地址列表和降低漏洞主机比例两个方面提出了相应的防御策略.

4.4.1　阻止蠕虫获得地址列表策略

V6-Worm 利用 IPv6 中无状态地址自动配置过程中的漏洞，通过伪造 RA 报文，从本地链路中各个节点回应的报文中获取地址信息，使得攻击命中率大幅提高，从而加速蠕虫传播. 如果可以禁止普通主机发送 RA 报文，禁止节点对未经授权的 RA 返回任何报文，或者对于发往节点请求多播地址的报文使用交换机制，都可以使 V6-Worm 无法得到攻击目标地址，不能进行高效的传播.

(1) 禁止普通主机发送 RA 报文. 在网络的监控端，记录本地链路中合法的路由器信息，若其它主机试图伪造成路由器，则对该行为进行报警和其它控制手段，使得蠕虫无法发送伪造的 RA 报文. 但由于需要确认路由器合法性，要求路由器等网络设备相对固定，所以该方式只适用于拓扑结构相对固定的网络.

(2) 禁止节点对未经认证的 RA 返回任何报文. 在网络中设置一个认证中心，每一个合法的路由器都将在认证中心取得认证，普通主机在收到 RA 报文后，根据 RA 报文中的信息到认证中心进行路由器身份认证，若认证成功则进行配置，若认证失败则认为该路由器无效，放弃该 RA 报文. 这种方式不要求网络结构固定，支持新的路由器临时接入网络，但由于需要引入认证中心，将加大系统实现的复杂度. 考虑到 IPv6 要求支持 IPSec，如果可以把该机制利用 IPSec 来实现，将成为一种行之有效的方式.

(3) 对发往节点请求多播地址的报文使用交换机制：对于发往特定多播地址的报文，路由器和交换机只将其转交给申请监听该多播地址的节点，使得节点回应的 NS 报文只能被特定节点收到，避免了地址信息的泄漏. 在路由器和交换机上需要维护相当大的地址对应表，使得效率降低，同时要求现有的底层交换机更换或者升级，这使得该方案需要相当大的投入.

4.4.2　降低漏洞主机比例策略

通过 4.3 节的分析可以发现，漏洞主机比例 ρ 是影响 V6-Worm 传播的关键参数之一，通过降低 ρ 可以减缓 V6-Worm 的传播速度、缩小危害范围. 降低 ρ 主要方法有三种：降低网络的同构性、减少漏洞主机数量和增加空地址.

(1) 降低网络同构性要求主机尽可能使用不同的操作系统和应用软件，对于任意操作系统和应用软件的漏洞都只能威胁到网络中部分主机，从而降低 ρ. 但是现实网络中大部分的主机都在使用少数几种操作系统和应用软件，如针对 Windows 操作系统 LSASS 漏洞的“Sasser”蠕虫，感染超过 1800 万台主机，占到全球主机总数的 3%[20]. 在不干涉用户正常使用的前提下，很难让网络的同构性降低到预期的效果，但降低网络同构性不仅可以抑制蠕虫传播，还可以抵抗各种基于系统漏洞的攻击方式，所以对于特定的网络，降低网络同构性是保证安全的一种有效选择.

(2) 当网络中主机总数相对固定时，使用主动式安全漏洞检测器(AVCCN)[21]来发现主机上存在的安全漏洞，进而减少存在漏洞的主机，将 ρ 降低到一定阈值以下，实现减缓 V6-Worm 的传播速度. 这种方式不干涉用户的正常使用，更适合普通网络环境使用.

(3) 降低 ρ 除了减少漏洞主机的绝对数量 K 以外，另一种可行的办法就是增加 N. 网络中的主机

总数难以出现大量的增长，但是由于 V6-Worm 认为所有做出应答回复的 IPv6 地址均为有效目标，所以通过在网络中加入大量的空地址（这些空地址并不对应有效主机，只对伪造的 RA 报文发送相应的响应报文）使得 N 增大，进而 ρ 减小. 同时在这些空地址上接收到的信息还可以用检测网络是否出现异常行为，因为正常情况下这些空地址应该接收不到任何数据报文.

5 总结及工作展望

通过对 V6-Worm 的分析及仿真实验，我们认为：IPv6 网络不但对于蠕虫传播的天然抵抗能力是相当有限的，甚至可能成为将来蠕虫传播的主要途径. 而且，与 IPv4 网络中的随机扫描蠕虫相比，V6-Worm 具有更快的传播速度，更强的传播能力，这对于蠕虫的防御和控制方法将提出新的挑战，也为 IPv6 的安全运行带来潜在威胁.

本文对于蠕虫传播的研究主要是针对蠕虫在 IPv6 本地链路子网内的传播模型，而实际网络中的主机多分布在不同的子网中，所以本研究的后续工作将着重于研究复合型扫描策略蠕虫在 IPv6 网络中的传播模型和防御机制.

致 谢 陈秀真博士、姚婷婷博士和秦涛博士对本文的完成提出了很多宝贵的意见，在此一并表示感谢！

参 考 文 献

1 Spafford E. H.. The Internet worm program: An analysis. Department of Computer Science, Purdue University, West Lafayette: Technical Report CSD-TR-823, 1988, 1～29

2 Moore D., Shannon C., Brown J.. Code-Red: A case study on the spread and victims of an Internet worm. In: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement, Pittsburgh, 2002, 273～284

3 Zheng Hui. Internet worm research[Ph. D. dissertation]. College of Information Technologies Science, Nankai University, Tianjin, 2003(in Chinese)
(郑 辉. Internet 蠕虫研究[博士学位论文]. 南开大学信息技术科学学院，天津，2003)

4 Shannon C., Moore D.. The spread of the witty worm. IEEE Security & Privacy, 2004, 2(4): 46～50

5 Hinden R., Deering S.. Internet Protocol Version 6 (IPv6) Addressing Architecture. RFC 3513, Internet Engineering Task Force, 2003

6 Wagner A. *et al*. Experiences with worm propagation simulations. In: Proceedings of the 2003 ACM Workshop on Rapid Malcode (WORM'03), Washington, 2003, 34～41

7 Zou C. C. *et al*. Routing worm: A fast, selective attack worm based on IP address information. Electrical and Computer Engineering Department, University of Massachusetts: Technical Report TR-03-CSE-06, 2003

8 Kamra A. *et al*. The effect of DNS delays on worm propagation in an IPv6 Internet. In: Proceedings of the IEEE INFOCOM 2005, Miami, 2005, 2405～2414

9 Staniford S., Paxson V., Weaver N.. How to own the Internet in your spare time. In: Proceedings of the 11th Usenix Security Symposium, San Francisco, 2002, 149～167

10 Staniford S. *et al*. The top speed of flash worm. In: Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM'04), Washington, 2004, 33～42

11 Zou C. C. *et al*. On the performance of Internet worm scanning strategies. Electrical and Computer Engineering Department, University of Massachusetts: Technical Report TR-03-CSE-07, 2003

12 Wen Wei-Ping *et al*. Research and development of Internet worms. Journal of Software, 2004, 15(8): 1208～1219 (in Chinese)
(文伟平等. 网络蠕虫研究与进展. 软件学报，2004，15(8)：1208～1219)

13 Mannan M., Oorschot P. C.. On instant messaging worms, analysis and countermeasures. In: Proceedings of the 2005 ACM Workshop on Rapid Malcode (WORM'05), Fairfax, 2005, 41～50

14 Zou C. C., Gong W. B., Towsley D.. Code red worm propagation modeling and analysis. In: Proceedings of the 9th ACM Symposium on Computer and Communication Security, Washington, 2002, 138～147

15 Droms R. *et al*. Dynamic host configuration protocol for IPv6 (DHCPv6). RFC 3315, Internet Engineering Task Force, 2003

16 Thomson S., Narten T.. IPv6 stateless address autoconfiguration. RFC 2462, Internet Engineering Task Force, 1998

17 Narten T., Nordmark E., Simpson W.. Neighbor discovery for IP version 6 (IPv6). RFC 2461, Internet Engineering Task Force, 1998

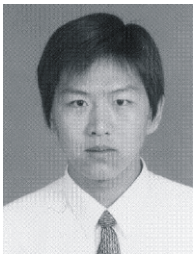
18 Yuan San-Ling. Study on the epidemic models with delays [Ph. D. dissertation]. School of Science, Xi'an Jiaotong University, Xi'an, 2001(in Chinese)
(原三领. 含时滞流行病模型的研究[博士学位论文]. 西安交通大学理学院，西安，2001)

19 Zou C. C. *et al*. The monitoring and early detection of Internet worms. IEEE/ACM Transactions on Networking, 2005, 13(5): 961～974

20 Zhang Yun-Ka *et al*. Analysis and prevention of "Sasser" worm. Computer Engineering, 2005, 31(18): 65～67(in Chinese)
(张运凯等. "震荡波"蠕虫分析与防范. 计算机工程，2005，31

(18)：65～67)

21 Chen Xiu-Zhen. The method of holoinformation security checking and evaluation for computer networks [Ph. D. dissertation]. School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, 2005(in Chinese)
(陈秀真. 全息网络安全检测与评估方法的研究[博士学位论文]. 西安交通大学电子与信息工程学院，西安，2005)



LIU Ting, born in 1981, Ph. D. candidate. His current research interests include network security in the next generation Internet.

ZHENG Qing-Hua, born in 1969, professor, Ph. D. supervisor. His research interests include natural language processing, network security and theory of E-learning.

GUAN Xiao-Hong, born in 1955, professor, Ph. D. supervisor. His research interests include network security, system optimization and scheduling.

CHEN Xin-Qi, born in 1981, M. S. candidate. Her research interests include network security in the next generation Internet.

CAI Zhong-Min, born in 1975, Ph. D., lecturer. His research interests include network security and data mining.

Background

The research presented in this paper was supported by the National Natural Science Foundation of China under grant No. 60243001; The National High Technology Research and Development Program (863 Program) of China under grant No. 2003AA142060; The National Outstanding Young Investigator of China under Grant No. 6970025.

The current research project is one of the research thrusts of the Ministry of Education Key Lab for Intelligent Network and Network Security (MEKLINNS) with its members from inter-disciplinary areas in systems engineering, computer science and engineering, and circuit and systems. The main tasks of the MEKLINNS include organizing and coordinating the research teams, undertaking research projects on intelligent network and network security. The current focuses of MEKLINNS include:

Theory and applications of complex networked systems;

Networks and information security;

Networked and remote education;

Parallel and network computation;

Networked data acquisition and information fusion;

Network security chips and boards.

Through the close collaboration among the members of MEKLINNS, significant progress has been made in developing an integrated network security system with defense-in-depth strategy.