网络蠕虫传播方法及仿真研究

蒋建春，文伟平，王业君，卿斯汉

（1. 中国科学院 软件研究所，北京 100080，2。中国科学院 信息安全技术工程研究中心，北京 100080）

摘要：网络蠕虫成为网络系统安全的重要威胁。本文首先分析了网络蠕虫的组成结构和工作机制，然后重点研究了网络蠕虫的不同类型传播方法，并提供不同条件下仿真的实验结果。最后给出了网络蠕虫的传播发展趋势与未来的研究方向。

关键词：网络蠕虫；传播；仿真

1 引言

网络蠕虫是一种综合黑客技术和计算机病毒技术，无需计算机使用者干预即可自动运行的攻击程序代码，它通过利用网络系统中所存在漏洞的节点主机，从一个节点传播到另外一个节点[1]。1988 年著名的“小莫里斯”蠕虫事件成为网络蠕虫攻击的先例[2]，随着网络技术应用的深入，网络蠕虫对网络系统安全的威胁日益增加。在网络环境下，多模式化的传播途径和复杂的应用环境使网络蠕虫的发生频率增高、传播变强、影响面更广，造成的损失也更大。网络蠕虫运行机制可以粗分为三个阶段：易感目标发现、感染易感目标和攻击代码执行。其中，网络蠕虫发现易感目标取决于所选择的传播方法，好的传播方法使网络蠕虫以最少的资源找到网上易传染的主机，进而能在短时间内扩大传播区域。本文主要研究网络蠕虫的传播方法，其余部分组织如下，第二部分研究了网络蠕虫的传播方法，这一部分主要分析现有网络蠕虫的传播方法，包括选择性随机扫描、顺序扫描、基于目标列表的扫描、基于路由的扫描、基于 DNS 扫描等；第三部分用仿真实验方法，重点讨论不同条件下的网络蠕虫传播效果；最后是结论，对网络蠕虫传播的发展趋势与未来的研究方向进行了分析。

2 网络蠕虫传播方法

网络蠕虫利用系统漏洞进行传播，良好的传播方法能够加速蠕虫传播，使网络蠕虫以最少的时间找到互联网上易感的主机。根据网络蠕虫发现易感主机方式进行分类，传播方法分成以下三类，即随机扫描、顺序扫描、选择性扫描。选择性扫描是网络蠕虫发展方向，进一步可以细分为选择性随机扫描、基于目标列表的扫描、基于路由的扫描、基于 DNS 扫描、分而治之扫描。

2.1 随机扫描

随机扫描是指网络蠕虫会对整个 IP 地址空间的随机抽取一个地址进行扫描，这样网络蠕虫感染下一个目标是非确定性。“Slammer”蠕虫的传播方法就是采用随机扫描感染[3]。

2.2 顺序扫描

顺序扫描是指网络蠕虫根据感染主机的地址信息，按照本地优先原则，选择它所在网络内的 IP 地址进行传播。顺序扫描又可称为“子网扫描”。若蠕虫扫描的目标地址 IP 为 A，则扫描的下一个地址 IP 为 A+1 或者 A−1。一旦扫描到具有很多漏洞主机的网络时就会达到很好的传播效果。该策略使得网络蠕虫避免扫描到未用地址空间，不足地方是对同一台主机可能重复扫描，引起网络拥塞。“W32.Blaster”是典型的顺序扫描蠕虫[4]。

2.3 选择性扫描

网络蠕虫改善传播效果方法是提高扫描准确性，快速发现易感的主机。目前，有三种措施可以采取，一是减少扫描未用的地址空间；二是在主机漏洞密度高的地址空间发现易感主机；三是增加感染源。网络蠕虫选择性扫描就是在事先获知一定信息条件下，有选择搜索下一个感染目标主机。

2.3.1 选择性随机扫描

选择性随机扫描是指网络蠕虫按照一定信息搜索下一个感染目标主机，将最有可能存在漏洞主机的地址集作为扫描的地址空间，以提高扫描效率。网络蠕虫的选择性随机扫描包含两个方面的技术点，一是网络蠕虫扫描对象是经过挑选的，互联网地址空间中未分配的或者保留的地址块不在扫描之列。二是网络蠕虫所选的扫描对象是非确定的，而是由网络蠕虫按照一定的算法随机生成目标地址。“CodeRed”的传播采用了选择性随机扫描策略[5]。

2.3.2 基于目标列表的扫描

基于目标列表扫描是指网络蠕虫在寻找受感染的目标前，预先生成一份可能易传染的目标列表，然后对该列表进行攻击尝试和传播[6]。网络蠕虫采用目标列表扫描实际上将初始的蠕虫传染源分布在不同地址空间，以提高传播速度。UC Berkeley 的 Nicholas C Weaver 实现一个基于目标列表扫描试验性 Warhol 蠕虫，理论推测该蠕虫能在 30 分钟内感染整个互联网。

2.3.3 基于路由的扫描

基于路由的扫描是指网络蠕虫根据网络中路由信息，如 BGP 路由表信息，有选择地扫描 IP 地址空间，以避免扫描无用的地址空间[7]。采用随机扫描的网络蠕虫会对未分配的地址空间进行探测，而这些地址大部分在互联网上是无法路由的，因此会影响到蠕虫的传播速度。如果网络蠕虫能够知道哪些 IP 地址是可路由的，则它能够更快、更有效地进行传播，并能逃避一些对抗工具的检测。 基于路由的扫描利用利用 BGP 路由表公开的信息，减少蠕虫扫描地址空间，提高了蠕虫的传播速度，理论计算路由扫描蠕虫的感染率是采用随机扫描蠕虫感染率的 3.5 倍[7]。基于路由的扫描不足是网络蠕虫传播时必须携带一个路由 IP 地址库，蠕虫代码量大。另外一个不足是，在使用保留地址空间的内部网络中，采用基于路由的扫描网络蠕虫传播会受到限制。目前，基于路由的扫描的网络蠕虫还处于理论研究阶段。

2.3.4 基于 DNS 扫描

基于 DNS 扫描是指网络蠕虫从 DNS 服务器获取 IP 地址来建立目标地址库，该扫描策略的优点在于获得的 IP 地址块具有针对性和可用性强的特点。本文认为，基于 DNS 扫描适宜于搜索易感染的服务器。基于 DNS 扫描的不足是：①网络蠕虫难于得到有 DNS 记录的地址完整列表；②目标地址列表中地址数并不完全出现在域名服务器中。例如“CodeRed I”所感染的主机中几乎一半没有 DNS 记录[8]。

2.3.5 分而治之扫描

分而治之扫描是网络蠕虫之间相互协作快速搜索易感染主机的一种策略，网络蠕虫发送地址库的一部分给每台被感染的主机，然后每台主机再去扫描它所获得的地址。主机 A 感染了主机 B 后，主机 A 将它自身携带的地址分出一部分给主机 B，然后主机 B 开始扫描这一部分地址。文献[7]中提出了基于 BGP 信息进行分而治之扫描的策略。分治扫描策略通过将扫描空间分成若干个子空间，各子空间由已感染蠕虫的主机负责扫描，这样就可能提高网络蠕虫的扫描速度，同时避免重复扫描。分而治之扫描策略的不足是存在“坏点”问题。在蠕虫传播的过程中，如果一台主机死机或崩溃，那么所有传给它的地址库就会丢失，这个问题发生的越早，影响就越大。

2.4 网络蠕虫传播因素综合分析

假设计算机网络中每台主机保持两种状态：易感染状态和感染状态。N 是易感染的主机数，I_t 为t时刻已被感染的主机数，β 是流行病模型的感染参数，α 为主机感染率，Ω 是蠕虫扫描IP地址空间，η 是感染蠕虫主机的平均扫描速率，p 是扫描漏洞主机数 N 的命中概率；则网络蠕虫的SEM（Simple Epidemic Model）模型微分方程表示为[7]：

$$\frac{dI_t}{dt} = \beta I_t[N - I_t]$$

假设 I_0 是 $t = 0$ 时的感染蠕虫数，则任意时刻的感染蠕虫的数表示为：

$$I_t = \frac{I_0 N}{I_0 + (N - I_0)e^{-\beta N t}} \qquad (1)$$

将$\alpha=\beta N$ 定义成感染率,文献[8]给出α计算公式如下:

$$\alpha=\eta\cdot\frac{N}{\Omega} \qquad (2)$$

由公式（1）和（2）得知,要增加I_t的值，就设法提高蠕虫的感染率α。根据公式（2），α值增加依赖于η和Ω。选择性随机扫描、基于路由的扫描随机扫描、基于 DNS 扫描都是从减少扫描 IP 地址空间Ω来改善网络蠕虫的传播效果，而顺序扫描、基于目标列表的扫描则是通过提高蠕虫主机的平均扫描速率η来增强网络蠕虫的传播能力。 然而，网络蠕虫在实际传播过程中，除了与其采取传播算法相关外，而且也同网络蠕虫传播的环境影响,例如地址空间单位主机的漏洞数、网络带宽、网络类型、安全阻断干扰等。因此，感染率α不是一个固定的，而是随时间和蠕虫对应环境动态地进行变化。参照公式（2），本文给出另外一个计算感染率α的公式:

$$\alpha=(\eta_{\max}-kt)\frac{N(t)}{\Omega_1+\Omega_2} \qquad (3)$$

其中，$\eta_{\max}-kt$表示蠕虫主机的扫描速率,$\eta_{\max}$表示蠕虫主机最大扫描速率,k是变化参数；Ω_1表示在使用的 IP 地址空间，Ω_2表示未使用的 IP 地址空间，$\Omega=\Omega_1+\Omega_2$；$N(t)$表示t时刻所对应的易感染的主机数。由公式（3）得知，网络蠕虫在初始时期，其传播能力最强，然后是逐步降低；当网络蠕虫扫描到地址空间出现$\Omega_2\rangle\rangle\Omega_1$时，又因$N(t)\le\Omega_1$，因此蠕虫感染率$\alpha$趋向零，这也表明在采用 IPv6 地址将有助于抑制网络蠕虫的传播；当$|\Omega_1-\Omega_2|$比较小时，选择性扫描的优势难以体现出来；在易感染的主机数密集情况下，即$\frac{N(t)}{\Omega}$比值比较大的时候，感染率α将增强，但是由于蠕虫传播会消耗掉网络资源，蠕虫的扫描速率将会下降，所以感染率α不会持续增长。根据上述分析，网络蠕虫传播能力的关键影响因素有三个：①目标地址空间选择；②搜索易感染主机速率；③易感染主机分布；各种扫描策略的差异主要在于目标地址空间的选择。网络蠕虫感染一台主机的时间取决于蠕虫搜索到易感染主机所需要的时间。因此，网络蠕虫快速传播的关键在于设计良好的扫描策略。在已出现网络蠕虫实例中，蠕虫的实现常常采用多种混合的扫描策略。表一是关于网络蠕虫的统计分析数据。

表 1　网络蠕虫传播策略统计分析表

传播策略 / 蠕虫实例	随机扫描	顺序扫描	选择性随机扫描
CodeRed I	有	无	有
CodeRed II	有	无	有
Nimda	有	无	无
Slammer	有	无	无
Blaster	有	有	无
Lion Worm	有	无	无
震荡波	有	无	有

3 网络蠕虫传播仿真实验

由于网络蠕虫的破坏性，蠕虫的传播实验一般不用实际互联网试验，而是主要用仿真和数学模型来进行分析。目前，用于网络蠕虫的仿真软件有 DdoSVax、SSFNet、NWS [9] ，本文拟用 NWS 软件包仿真不同条件下网络蠕虫传播情况。NWS 是一个自由软件包，它能实现主机、网络、软件、漏洞等仿真。在 NWS 基础上，仿真实现了不同的初始蠕虫数量、漏洞分布情形下，网络蠕虫的传播效果。图 1 是关于初始蠕虫数量对网络蠕虫传播影响，由图可知，初始蠕虫数量增加，感染主机的数量是递增速度要快，随着传播时间的推移，网络蠕虫传播变缓。在防治网络蠕虫方面，根据图 1 分析，关键是要在早期对网络蠕虫进行控制。

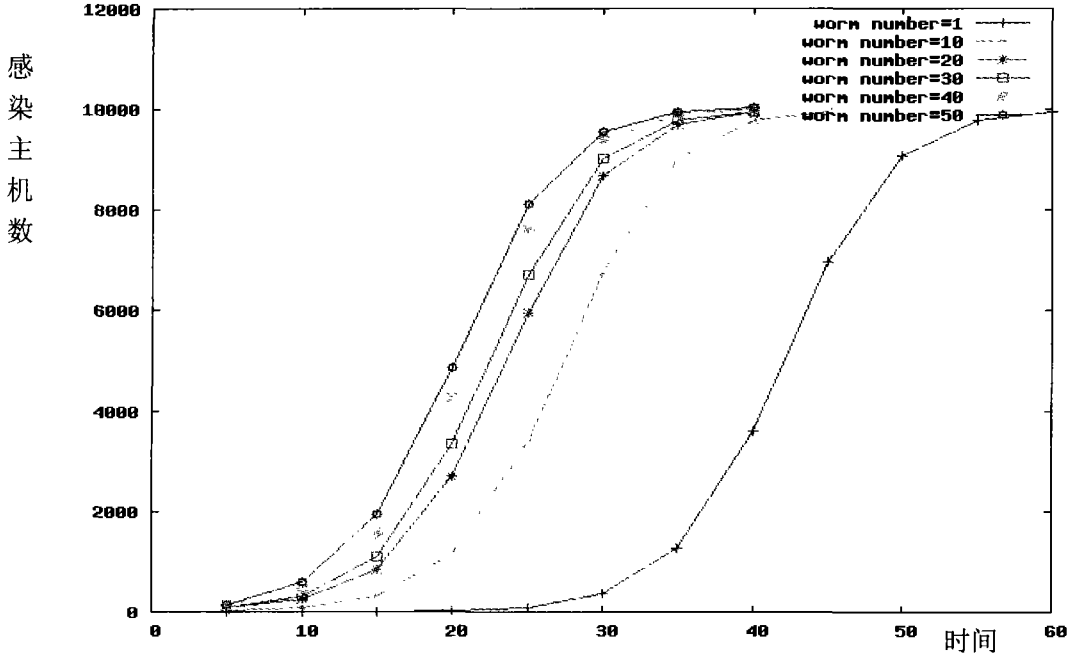

图 1 初始蠕虫数量对网络蠕虫传播影响效果图

图 2 是不同的漏洞分布对网络蠕虫传播影响分析图，通过图 2，我们可以分析，随着漏洞分布密度越大，网络蠕虫的传播速率受到影响，其原因可能是受蠕虫感染的主机越多，则消耗网络资源就逐步递增，而某个网络资源是固定，当传播到一定数量后，网络蠕虫就会因资源有限，传播速度下降。由此我们分析，若构造一个虚拟的漏洞分布密度高的网络，用于欺骗网络蠕虫，从而将会抑制网络蠕虫的传播。

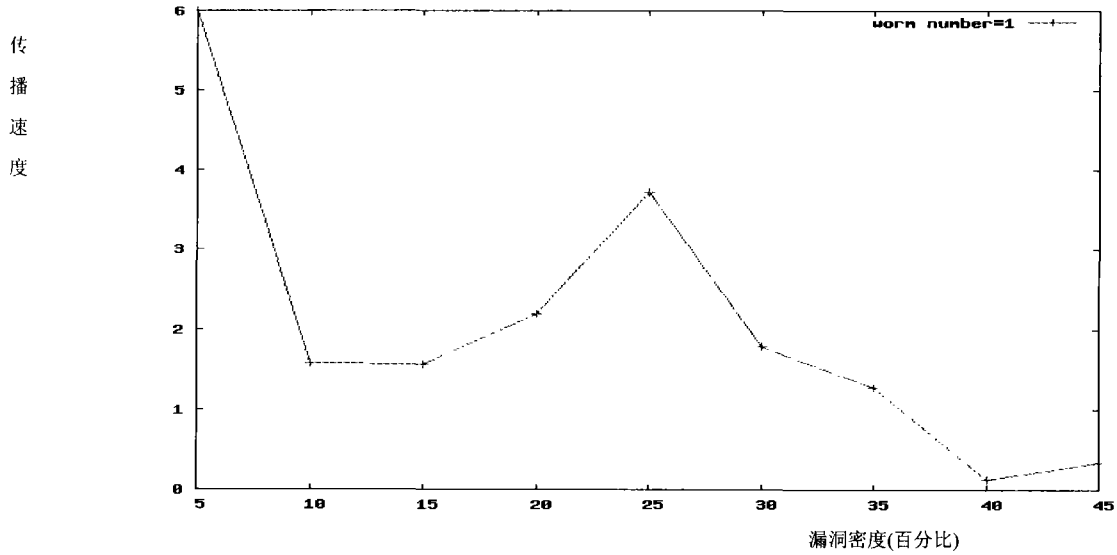

图 2 不同的漏洞分布对网络蠕虫传播影响分析效果图

4 结论

本文主要分析了网络蠕虫的组成结构和工作机制，然后重点研究了网络蠕虫的不同类型传播方法，并给出数学分析模型和不同条件下仿真的实验结果。由于网络信息及结构复杂性，网络蠕虫传播具有相当的复杂性和行为不确定性，网络蠕虫的传播能力将会从以下几方面进行改进：

- 避免扫描无用地址空间，如定向传播易感地址空间；
- 智能型网络蠕虫，如根据受害计算机节点的资源产生不同的线程；
- 无状态的、多线程的扫描技术；
- 多条传播途径的网络蠕虫。

我们未来的网络蠕虫传播研究重点将是建立蠕虫传播数学模型以及构建模拟实际网络环境的测试床。

参考文献：

[1]文伟平，卿斯汉，蒋建春，王业君. 网络蠕虫研究进展[J]. 软件学报（已录用）.

[2]Spafford EH. The Internet Worm Program: An Analysis. Technical Report CSD--TR--823, Department of Computer Science, Purdue University. 1988. 1～29.

[3] David Moore, Vern Paxson etc.The Spread of the Sapphire/Slammer Worm[EB/OL].
http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

[4] Blaster Worm Analysis[EB/OL].http://www.eeye.com/html/Research/Advisories/AL20030811.html

[5]eEye Digital Security. CodeRedII Worm Analysis[EB/OL]. http://www.eeye.com/html/Research/Advisories/AL20010804.html

[6]Weaver N. Warhol Worms: The Potential for Very Fast Internet Plagues. http://www.cs.berkeley.edu/~nweaver/warhol.html.

[7] Zou CC, Towsley D, Gong W, Cai S. Routing Worm: A Fast, Selective Attack Worm based on IP Address Information. Umass ECE Technical Report TR-03-CSE-06, November, 2003.

[8]Cliff C. Zou, Lixin Gao, Weibo Gong, and Don Towsley. Monitoring and Early Warning for Internet Worms. In 10th ACM Conference on Computer and Communication Security (CCS'03), Oct. 27-31, Washington DC, USA, 2003.

[9]Survey of Worm Traffic Simulators: Course project for Security and Privacy in Computing[EB/OL].
http://www-users.cs.umn.edu/~htalkad/files/worm.pdf