Research on Network Worms Propagation by Simulation based on SSFNet

ZHANG Ran, LI Yan

School of Software Engineering, Beijing University of Technology, Beijing, China

ranranzh@bjut.edu.cn

Abstract: How to analyze and depict the propagation characteristic of network worms is the basis of researching on worm defense. In this paper, network worms were researched on and the propagation behavior of network worms based on simple epidemic model in the self-defined campus network was simulated by SSFNet, which is an open source network simulation tool. Then the propagation speed of several network worms based on different scanning strategies was analyzed and compared. The simulation results show that the worm scanning strategies impact the network worm propagation speed tremendously.

Keywords: network security; SSFNet; worm; propagation model

基于 SSFNet 的网络蠕虫传播仿真研究

张 然，李 艳

北京工业大学软件学院，北京，中国，100124

ranranzh@bjut.edu.cn

【摘要】如何对网络蠕虫的传播特性进行准确地分析和刻画是研究蠕虫防御的基础。本文对网络蠕虫进行了分析研究，采用开源网络仿真工具 SSFNet，在自定义的校园网络环境中对基于简单流行病模型的网络蠕虫的传播行为进行了仿真，并对几种基于不同扫描策略的网络蠕虫的传播速度进行了分析和比较。仿真结果表明，蠕虫扫描策略对蠕虫的传播速度有着极大的影响。

【关键词】网络安全；SSFNet；蠕虫；传播模型

1 引言

自 1988 年 Morris 蠕虫问世以来，近年来又接连爆发了 Code Red、Slammer、Blaster、Sasserr 等蠕虫，给互联网用户造成了巨大的经济损失，引起了世界各国对网络安全问题的关注。网络蠕虫利用系统漏洞进行自动传播，具有极大的破坏性。随着网络应用及复杂性的增加，网络蠕虫逐渐成为网络系统安全的重要威胁。为了更好地对抗网络蠕虫，需要对网络蠕虫传播特性进行准确地分析和刻画。

然而，由于网络蠕虫的特有的破坏性使得蠕虫传播的相关研究不能在真实的网络中进行实际传播实验，因此通过蠕虫传播策略及相关算法的描述，利用仿真软件来模拟蠕虫的传播过程是一个很好的解决手段，保证了实验环境的安全性。

基金项目：北京工业大学青年科研基金（No. 97025001200701）。
Foundation Item：The Youth Science Foundation of Beijing University of Technology（No. 97025001200701）.

2 蠕虫的功能结构、扫描策略及传播模型

Morris 蠕虫爆发后，Spafford 从技术角度对蠕虫进行了定义，“蠕虫是一段代码，它能够独立运行并把一个包含自身所有功能的副本传播到其它的计算机上。”为了区分蠕虫和病毒，他还重新定义了病毒，“病毒是一段代码，能把自身加到其它程序包括操作系统上；它不能独立运行，需要由它的宿主程序运行来激活它。”从这两个定义中，可以看出蠕虫强调自身的主动性和独立性，同时，也鲜明地反映出蠕虫的两个特性：网络传播和主动攻击。

文伟平等人在其论文[1]中总结了蠕虫的功能模块，其结构大致类似于郑辉的统一功能模块划分方式[2]。如图 1 所示，文伟平等总结的蠕虫功能模块分为主体功能模块和辅助功能模块。其中，主体功能模块

978-1-935068-01-3 © 2009 SciRes.

包括信息搜集、扫描探测、攻击渗透、自我推进等四大模块；辅助功能模块包括实体隐藏、宿主破坏、信息通信、远程控制、自动升级等五大模块。

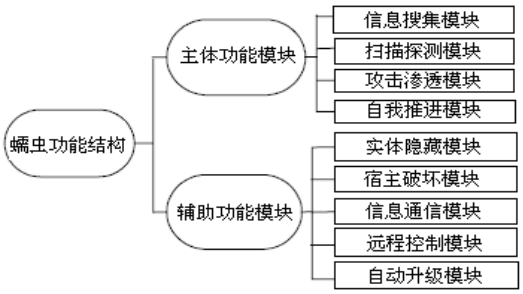

Figure 1. Functional structure of network worms
图 1. 网络蠕虫的功能结构

从蠕虫主体功能模块实现可以看出，蠕虫的攻击行为可以分为 4 个阶段，即信息收集、扫描探测、攻击渗透和自我推进。如图 2 所示。信息收集主要完成对本地和目标节点主机的信息汇集；扫描探测主要完成对具体目标主机服务漏洞的检测；攻击渗透利用已发现的服务漏洞实施攻击；自我推进完成对目标节点的感染。

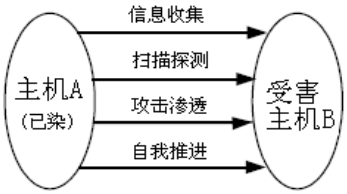

Figure 2. Execute mechanism of network worms
图 2. 网络蠕虫的工作机制

蠕虫利用系统漏洞进行传播首先要进行主机探测。ICMP Ping 包和 TCP SYN，FIN，RST 及 ACK 包均可用来进行探测。良好的扫描策略能够加速蠕虫传播，理想化的扫描策略能够使蠕虫在最短时间内找到互联网上全部可以感染的主机。按照蠕虫对目标地址空间的选择方式进行分类，扫描策略包括：选择性随机扫描、顺序扫描、基于目标列表的扫描、分治扫描、基于路由的扫描、基于 DNS 扫描等。

理想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，并可以预测网络蠕虫可能带来的威胁。人们在研究网络蠕虫的过程中发现，网络蠕虫的传播特性和生物学中的流行病毒有许多相同之处，因此大多数的蠕虫研究都仿照简单传染病模型来对蠕虫传播特性进行建模。目前，比较流行的蠕虫传播模型除了简单流行病模型（Simple Epidemic Model）外，还有 SIS（Susceptible-Infectious-Susceptible）模型、SIR（Susceptible-Infective-Recovered）模型、Kermack-Mckendrick 模型、双要素（Two-Factor）模型、Worm-Anti-Worm 模型（简称 WAW 模型）等。

3 基于 SSFNet 的网络蠕虫传播仿真

3.1 SSFNet 与 NS2 的比较

SSFNet[3][4]是一个 Internet 网络协议的仿真和建模软件，以基于 Java 和 C++的 SSF（scalable simulation framework）的软件框架所组成。作为教育和科学研究用途的 SSFNet 是开放软件，允许用户按需要进行补充和修改。SSFNet 最大的特点在于其良好的可扩展性，与传统的仿真软件相比，它占用资源小得多，对操作系统有广泛的支持，运算效率高。另外，SSFNet 自带由 Michael Liljenstam 博士编写的蠕虫仿真实验包 SSF.App.Worm，能够模拟蠕虫传播的 SI、SIS、SIR 传染病模型，同时用户可以自行修改相关代码，实现自定义蠕虫传播模型。因此可以通过改写蠕虫包 SSF.App.Worm，模拟基于不同模型的蠕虫传播过程。

NS2（Network Simulator, version 2）是由美国加州 Lawrence Berkeley 国家实验室等单位开发的开源免费网络仿真软件。NS2 由 C + + 和 Otcl 两种语言实现，为兼顾效率和仿真速度，内核用 C ++ 编写，完成具体协议的仿真和模拟；前端用 Tcl 语言编写，完成网络环境的搭建以及参数的设置和更改。NS2 仿真器的功能非常强大，可扩展性强，执行效率高，目前已广泛应用于局域网、广域网、无线移动网和卫星网络的仿真。

研究表明，NS2 只能在拥有多个至强 CPU、8G 内存的较高配置上提供 1000 个节点的仿真模拟。对于 NS2，如图 3 所示，随着连接数的增大，它所需的仿真时间比 SSFNet 少。但是，如表 1 所示，Java 实现的 SSFNet 每次连接消耗的核心内存远比 NS2 少。综合仿真时间和内存消耗两方面因素，SSFNet 较 NS2 具有更好的仿真性能。因此，这里选用 SSFNet 做为网络蠕虫模拟实验的模拟工具。

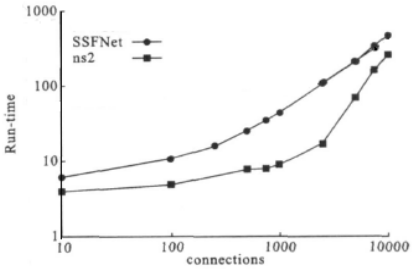

Figure 3. The number of connections of SSFNet and ns2
图 3. SSFNet 和 ns2 连接数的比较

Table 1. Comparison of memory consumption of SSFNet and ns2
表 1. SSFNet 和 ns2 内存消耗的比较

Tool	Build	Build/run
Java-SSFNet	27.5Kb	53.3Kb
ns2	52.2Kb	93.3Kb

3.2 基于简单流行病模型的网络蠕虫传播仿真

自定义一个校园网络拓扑：由 6 个主干路由器构成的主干网，其余 32 台路由器按等级组成多个 AS（Autonomous Systems），分布在主干路由器周围。每个 AS 要么是一个客户机簇(请求数据的主机群)，要么就是一个服务器簇(为客户机提供所请求的服务的主机群)。除了 6 个主干簇(构成它们内部之间的 3 个 C/S 簇对)是挨着的，其它 C/S 簇对的布局原则是尽量分散，目的是确保产生的流量能散布在整个网络的各个部分。场景所描述的校园网络拓扑如图 4 所示。

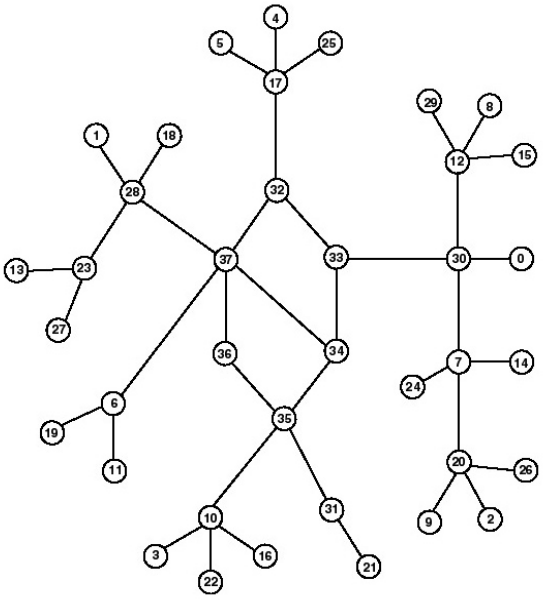

Figure 4. Network topology on the macroscopical AS level
图 4. 宏观 AS 级网络拓扑图

在校园网络总体拓扑布局图中，每个圆圈代表一个 AS。数字代表 AS 的网络 ID 号。偶数 AS 是客户机簇，奇数 AS 是服务器簇。一个偶数表示的客户机簇和一个奇数表示的服务器簇是成双成对的。（如，0 号客户机簇匹配 1 号服务器簇，2 号客户机簇匹配 3 号服务器簇，以此类推。）中间 6 个路由器（标号 32 至 37）构成了主干网。实现时，模拟中的校园网络结构在 campus.dml 中定义。

在上述场景中，我们对基于简单流行病模型的 Code Red II 蠕虫在校园网内的传播情况进行仿真。仿真结果如图 5 所示，显示了 Code Red II 蠕虫攻击的校园网络中所有的被感染主机数及其被感染时间。图 6 为 Code Red II 第一次实际爆发时对被感染主机数量的评估。对比图 4 和图 5，可以看出本次仿真的结果和实际趋势是相符的，但由于校园网内的主机数是固定的，即校园网是一个主机数一定的子网，所以开始蠕虫的传播很快，但随着越来越多的易感染主机被蠕虫传染后变成被感染主机，易感染主机数减少，势必导致校园网中的新感染的主机数减少。

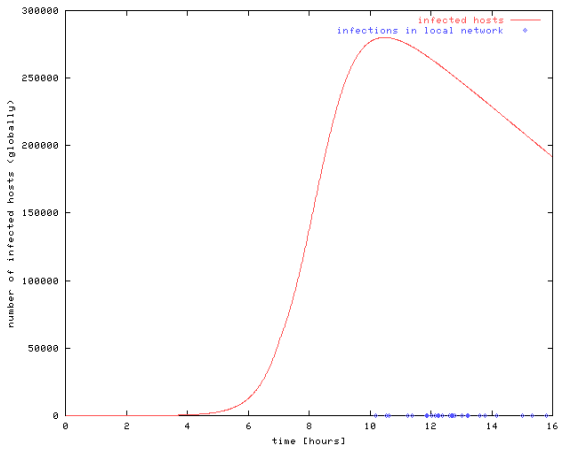

Figure 5. The campus network worm attack simulation scenario
图 5. 被蠕虫攻击的校园网络模拟场景

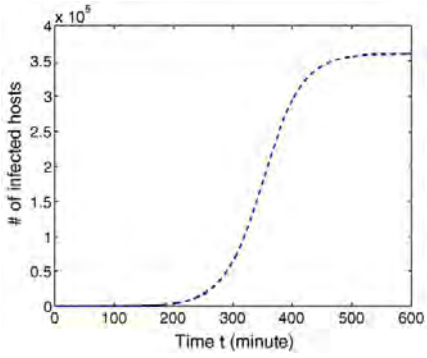

Figure 6.The number of infected hosts for Code Red II outbreaking
图 6. Code Red II 第一次爆发时被染主机数

978-1-935068-01-3 © 2009 SciRes.

3.3 网络蠕虫扫描策略对传播速度的影响

基于不同扫描策略的网络蠕虫其传播速度往往不一样。这里我们对 Code Red 蠕虫、BGP 路由蠕虫和目标列表蠕虫的传播情况进行了仿真比较。

采用上述 Code Red II 蠕虫用到的相同参数，即 N=360,000（蠕虫传播前网络中易感染主机的数目），$\eta = 358$ /分钟（蠕虫的平均扫描速率），I(0)=10（初始时刻被感染主机的数量）。假定当黑客将原始的 Code Red 改进成 BGP 路由蠕虫和目标列表蠕虫时，蠕虫扫描率不变，即$\eta = 358$ /分钟，BGP 路由蠕虫的 I(0)=10，目标列表蠕虫的目标列表大小为 10,000，即 I(0)=10,000。图 7 显示了目标列表蠕虫（Hit-list worm）、BGP 路由蠕虫（BGP routing worm）和原始的 Code Red 蠕虫的传播。与 BGP 路由蠕虫相比，目标列表蠕虫有目标列表，因而能够在短时间内感染更多的易感染主机，但是目标列表蠕虫由于有较大的扫描空间Ω，因此它的感染速度较慢。

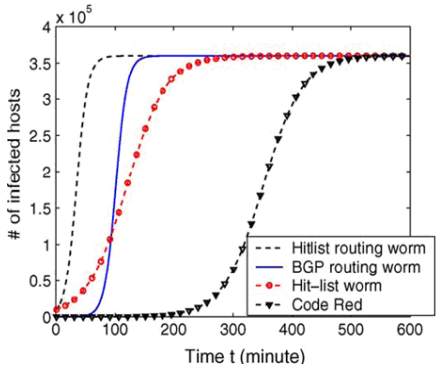

Figure 7. Propagation trend of Code Red worm, BGP routing worm and Hit-list worm

图 7. Code Red 蠕虫、BGP 路由蠕虫和目标列表蠕虫的传播

由于目标列表蠕虫和路由蠕虫采用不同的方法加快它们的传播速度，可以简单地结合这两种方法制造一种新的“目标列表路由蠕虫”（Hit-list routing worm）。这种蠕虫的传播情况在图 7 中也有显示。由图 7 可知，该蠕虫吸取了目标列表蠕虫和路由蠕虫两者的优点，它只需要不到 50 分钟的时间就可完成感染，而传统的 Code Red 需要 500 分钟才能完成。由此也可以看出，路由蠕虫通过缩小扫描空间提高传播速度，目标列表蠕虫通过获得大量的易感染主机地址来提高传播速度。

4 结论

根据基于 SSFNet 的网络蠕虫试验床的基本原理和实现技术，我们对现有的蠕虫试验床进行进一步开发，在该试验床中搭建了一个模拟的校园网络环境，并实现了基于流行病模型的蠕虫 Code Red II 在该网络中的传播。将该蠕虫在仿真环境下的实验数据与其第一次在互联网中爆发的实际数据进行对比，可以看出该蠕虫实验床的仿真具有较高真实性，同时发现在大规模网络中，蠕虫扫描策略对蠕虫的传播速度有着极大的影响。

“知己知彼，百战不殆”。通过基于 SSFNet 的仿真实验，不仅克服了传统网络蠕虫实验方法安全性低、成本高的缺点，而且可以让我们更好地掌握网络蠕虫的普遍传播规律及其传播影响因素，从而为设计蠕虫预警系统和制定蠕虫对抗措施提供指导。

References (参考文献)

[1] Wen Weiping, Qing Sihan, Jiang Jianchun. Research and Development of Internet Worms[J]. Journal of Software. 2004, 15(08):1208-1219
文伟平, 卿斯汉, 蒋建春,等. 网络蠕虫研究与进展[J]. 软件学报,2004,15(08):1208-1219.

[2] Zhen Hui. Internet worm research[D]. Nankai University, 2003.
郑辉.Internet 蠕虫研究[D]. 南开大学, 2003.

[3] Richard Blum. Translator: Liang Jinkun. Network Performance Toolkit: Using Open Source Testing Tools. Beijing: Publishing House of Tsinghua. 2005.6.
Richard Blum, 梁金昆译. 网络性能开源工具包[M]. 北京:清华大学出版社. 2005.6.

[4] SSF——Scalable Simulation Framework[Z]. [2006-10-10]. http://www.ssfnet.org

[5] M. Liljenstam, Y. Yuan, etc., A mixed abstraction level simulation model of large-scale internet worm infestations, MASCOTS. IEEE, October 2002.