第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)07—0134—03 文献标识码：A 中图分类号：TP309

SIRS蠕虫传播模型及其分析

彭俊好[1,2]，徐国爱[1]，朱振荣[1]，杨义先[1]
(1. 北京邮电大学网络与交换技术国家重点实验室信息安全中心，北京 100876；2. 广州大学数学与信息科学学院，广州 510405)

摘 要：提出SIRS蠕虫传播模型并对其稳定性进行分析，当R_0<1 时，网络最终将处于“无病”状态，当R_0>1 时，将出现蠕虫“地方病”。利用CAIDA提供的蠕虫数据进行检验，结果表明模型与实际数据吻合。基于该模型，分析了主机不能保持免疫力、感染蠕虫后及时关机或断开网络、主机主动免疫等不同策略对蠕虫控制的影响。

关键词：蠕虫；传播模型；稳定性

SIRS Worm Propagation Model and Its Analysis

PENG Jun-hao[1,2], XU Guo-ai[1], ZHU Zhen-rong[1], YANG Yi-xian[1]
(1. Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876; 2. College of Math and Information Science, Guangzhou University, Guangzhou 510405)

【Abstract】 SIRS worm propagation model is provided and its stability is anal sized. When R_0<1, worm will disappear finally. When R_0>1, “local plague” of worm will appear. The model fits well with worm data from CAIDA when testing the model with these data. At the same time, the influence on worm control of different policies is analyzed, such as host losing immunity to worm, shutting down host or cutting off network timely when host is infected, and vaccinating actively.

【Key words】 worm; propagation model; stability

1 概述

蠕虫传播模型研究中，主要是利用传染病传播模型的研究成果，结合蠕虫的特点，形成适用于描述蠕虫传播的模型。现有的模型主要有：Two-Factor模型[1]，SIAR模型[2]以及Worm-Anti-Worm模型[3]等。这些模型在一定程度上描述了蠕虫传播的规律，对蠕虫的传播预测与控制起到很好的作用，但这些模型存在以下问题：

(1)未考虑主机恢复后部分不具有对蠕虫免疫力的情况，但用户对蠕虫对抗技术了解程度差异较大，不可能做到所有主机感染恢复后一定具有对该蠕虫的免疫。

(2)对模型稳定性及参数不同取值时对蠕虫控制和预防带来的影响进行分析很少，因而并不利于指导控制和预防。

基于以上问题，本文提出了SIRS蠕虫传播模型并对其稳定性进行了分析，给出了出现“地方病”平衡点的条件。同时利用所提出的SIRS模型，分析了不同策略对蠕虫控制的影响。与以往模型相比，该模型表达式简单易于分析，且在与CAIDA提供的蠕虫CodeRed真实数据[4]吻合方面，都显示出一定优势。

2 SIRS 蠕虫传播模型

根据主机被蠕虫感染情况及对蠕虫的免疫情况，主机可处于 3 种不同状态：易感状态，感染状态，移去状态；相应地，根据主机所处的状态可将它们分为以下 3 类：

(1)易感主机类：该类主机没有被蠕虫感染，具有一定被感染可能性，其数量为 $S(t)$，简记为 S。

(2)感染主机类：该类主机被蠕虫感染，能够感染其他主机，其数量为 $I(t)$，简记为 I。

(3)移去主机类：指从感染类中移去的主机，这类主机包括打上漏洞补丁、关机或被隔离的机器。这类主机既非感染者，也非易感者，但有部分可能由于系统重装或其他原因导致主机成为易感者。这类主机数量为 $R(t)$，简记为 R。

2.1 模型建立

SIRS 模型中主机的状态转换情况如图 1 所示。

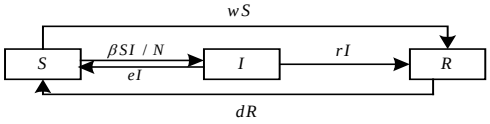

图 1 SIRS 模型状态转换图

(1)由于蠕虫传播时间较短，假定在蠕虫传播期间，主机的总数保持不变，记为 N。

(2)假设单位时间内易感主机进入感染类的数量为 $\beta SI/N$，虽然与实际情况会有点差异，但从模型的求解与真实数据的吻合情况看，其影响很小，大大方便了模型的求解与分析。

(3)由于蠕虫传播的影响，部分易感主机会主动升级系统或打补丁，使主机对蠕虫具有免疫能力，因而进入移去类，单位时间内由易感类进入移去类的主机数量为 $wS(t)$。

(4)对感染主机，其中一部分会进入移去类，另一部分会进入易感类，假定单位时间内由感染类进入易感类和移去类的系数分别为 e 和 r。

(5)单位时间内，移去类的主机有部分主机重新成为易感

基金项目：高等学校博士学科点专项科研基金资助项目(20050013011)

作者简介：彭俊好(1973－)，男，博士研究生，主研方向：网络与信息安全；徐国爱，副教授、博士；朱振荣，博士研究生；杨义先，教授、博士生导师

收稿日期：2007-04-20 **E-mail：**infopjh@126.com

者，其变化率为 d，因而单位时间内由移去类进入为易感类的主机数为 $dR(t)$。

根据图 1 及以上说明可以得到 SIRS 模型的微分方程表示形式如下：

$$\begin{cases} S' = dR + eI - \beta SI / N - wS \\ I' = \beta SI / N - rI - eI \\ R' = rI + wS - dR \\ S + I + R = N, 0 \le S, I, R \le N \end{cases} \tag{1}$$

2.2 模型稳定性分析

为考查模型的稳定性，需求方程的平衡点，只需令方程组右端为 0 求解除 S, I, R 的值即可，由于 $S+I+R=N$，只需求解以下方程组：

$$\begin{cases} d(N-S-I) + eI - \beta SI / N - wS = 0 \\ \beta SI / N - rI - eI = 0 \\ 0 \le S, I \le N \end{cases} \tag{2}$$

解方程组(2)可得 2 个解：

$P_0 = (dN/(d+w), 0)$，$P_+ = (S^*, I^*)$

其中，$S^* = N(r+e)/\beta$；$I^* = (dN\beta - N(w+d)(r+e))/((r+d)\beta)$。

由于 P_0 中 I=0，这是无病平衡点。若令 $R_0 = d\beta/((r+e)(w+d))$，则有：

当 R_0<1 时，$I^* < 0$，P_+不符合条件；当 R_0>1 时，$I^* > 0$，P_+是方程(2)的解，由于感染主机数保持在一定的规模，这是地方病平衡点。

定理 1 当 R_0<1 时，方程(2)有唯一的平衡点 P_0，且是全局渐近稳定的，当 R_0>1 时，方程(1)除存在无病平衡点 P_0外，还存在地方病平衡点 P_+，其中无病平衡点不稳定，地方病平衡点全局渐近稳定。

证明 由前面的讨论可知 R_0<1 时，方程(1)有唯一的平衡点 P_0，当 R_0>1 时，方程(1)除存在无病平衡点 P_0外，还存在地方病平衡点 P_+，下面讨论其稳定性。

令 $\begin{cases} P(S,I) = d(N-S-I) + eI - \beta SI/N - wS \\ Q(S,I) = \beta SI - rI - eI \end{cases}$

记 $\boldsymbol{A} = \begin{vmatrix} \partial P/\partial S & \partial P/\partial I \\ \partial Q/\partial S & \partial Q/\partial I \end{vmatrix}$

(1)在平衡点 P_0，特征方程

$$\det(\lambda \boldsymbol{I} - \boldsymbol{A}) = \begin{vmatrix} \lambda + d + w & d - e + \beta d/(d+w) \\ 0 & \lambda - \beta d/(d+w) + r + e \end{vmatrix} = 0$$

有 2 个特征根：$\lambda_1 = -d - w$，$\lambda_2 = \beta d/(d+w) - r - e$。

易知 $\lambda_1 < 0$，而当 R_0<1 时，$\lambda_2 < 0$；当 R_0>1 时，$\lambda_2 > 0$。根据常微分方程组零解稳定性判别方法[5]可知：当 R_0<1 时，平衡点 P_0是全局渐近稳定的；当 R_0>1 时，平衡点 P_0是不　稳定。

(2)在平衡点 P_+, A的特征多项式为

$$\det(\lambda \boldsymbol{I} - \boldsymbol{A}) = \begin{vmatrix} \lambda + d + w + (\beta d - (w+d)(r+e))/(r+d) & d + r \\ -(\beta d - (w+d)(r+e))/(r+d) & \lambda \end{vmatrix} \equiv$$

$$\lambda^2 + b\lambda + c$$

$$b = d + w + (\beta d - (w+d)(r+e))/(r+d)$$

$$c = (\beta d - (w+d)(r+e))/(r+d)$$

若令对应特征方程的根为 λ_1, λ_2，则有：

$$\lambda_1 + \lambda_2 = -b, \lambda_1 \cdot \lambda_2 = c$$

由 R_0>1 可知 b>0, c>0，因而 λ_1, λ_2 或全为负的实数，或为一对具有负实部的共轭复数，根据常微分方程组零解稳定性判别方法可知：当 R_0>1 时，平衡点 P_+是全局渐近稳定的。

3 模型检验

为考查模型的合理性，本文利用蠕虫 Code Red 爆发时 CAIDA 收集的真实数据进行检验。在本模型中，令 N=400 000, β =0.015 3, r=0.002, d=0.000 001, e=0.000 3, w=0.000 01，对模型进行求解，并绘制当前染病主机数 I 与时间 t 的变化曲线，曲线与真实数据有很好的吻合；同时对邹长春提出的蠕虫传播 Two-Factor 模型的求解进行比较，本模型与真实数据更接近，如图 2 所示。

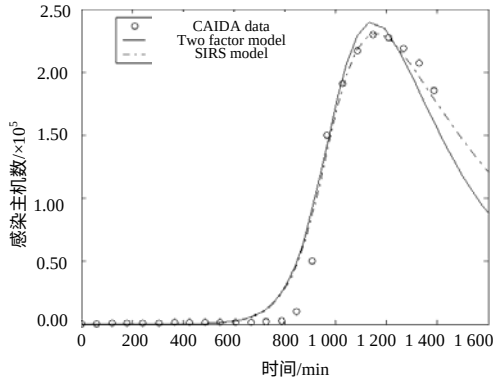

图 2　模型数值解与真实数据的比较

4 不同策略对蠕虫控制的影响

由第 2 节模型稳定性分析可知，R_0=1 是是否出现“地方病”的门限，下面分析不同策略对 R_0取值以及蠕虫控制的影响。

(1)主机不能保持免疫力会导致蠕虫“地方病”的形成。主机感染蠕虫后，通过打补丁或升级操作系统主机可以获得对该蠕虫的免疫力，但由于重装系统或其他原因又会导致已获免疫力的主机免疫能力的消失，这一点往往不会引起用户的足够重视，但这一举措会对蠕虫控制带来很坏的影响，轻者减缓蠕虫控制速度，重者将导致“地方病”的产生。

由于当 d>0 时，R_0是 d增函数，d越大，R_0越大，当 R_0<1 时，蠕虫爆发的规模随 d增大而增大，控制时间随 d增大而延长；当 R_0>1 时出现“地方病”，而若 d=0，有 R_0=0，不可能出现“地方病”。在本模型中，分别取 d=0.000 01, 0.000 1, 0.000 3, 0.000 5, 0.000 8，感染主机数随时间变化趋势如图 3 所示。从图中可以发现，d取这些值时都导致“地方病”出现，且随着 d增大，“地方病”越严重，感染主机数维持在更高的数量上。

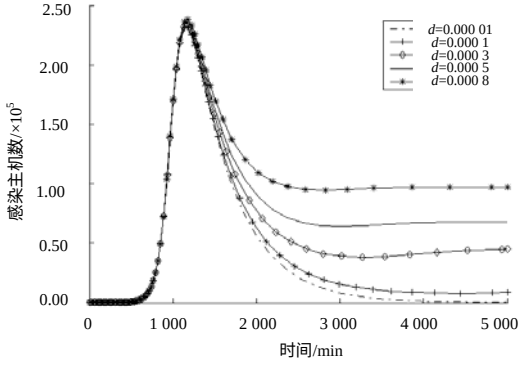

图 3　d 不同取值对蠕虫控制的影响

(2)感染蠕虫后及时关机或断开网络会加速蠕虫的有效

控制。分析本模型可以发现，r增大，R_0减小，出现“地方病”的可能性减小，且蠕虫爆发规模及持续时间都随之大大减小。在本模型中，分别取r=0.001, 0.002, 0.003, 0.004, 0.005，感染主机数随时间变化趋势如图 4 所示。尽快发布漏洞补丁提高主机的免疫能力是提高r的一种手段，但另一种最简便有效的办法是关机或断开网络，加速属于感染类的主机数的减少，达到提高r值的目的。

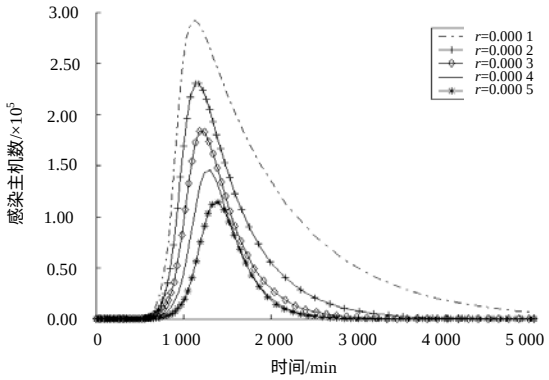

图 4　r 不同取值对蠕虫控制的影响

(3)主动免疫速度加快将有效控制蠕虫的传播。由$I'=\beta SI/N-rI-eI$可知，当$\beta S/N>(r+e)$时，I值增加；$\beta S/N<(r+e)$时，I值减小。为加快蠕虫的控制，一方面可采取措施提高r及e的值，另一方面，尽快减少S值，使易感类主机转化为移去类主机，也就是加快易感主机的主动免疫，即增大w值。由$R_0=d\beta/((r+e)(w+d))$可知，w增大，R_0减小，“地方病”平衡点出现可能性减小。在本模型中，分别取w=0.000 01, 0.000 1, 0.000 2, 0.000 3, 0.000 4，感染主机数随时间变化趋势如图 5 所示。另外，安装防火墙、及时升级杀毒软件可以降低主机被蠕虫成功攻击的可能性，使模型中β值减小，R_0减小，将使蠕虫爆发规模即持续时间减小，若$\beta<(r+e)$，蠕虫不可能爆发起来。

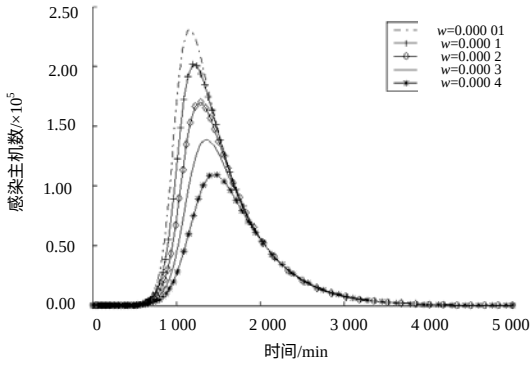

图 5　w 不同取值对蠕虫控制的影响

5　结束语

本文提出并分析了 SIRS 蠕虫传播模型，利用 CAIDA 提供的数据进行检验，结果表明该模型能比 Two-Factor 模型更好地与实际情况吻合，且模型简单，易于分析模型的稳定性及不同策略对蠕虫控制的影响。

参考文献

[1] Zou Changchun, Gong Weibo. Code Red Worm Propagation Modeling and Analysis[C]//Proc. of the 9th ACM Symp. on Computer and Communication Security. Washington D. C., USA: [s. n.], 2002.

[2] 杨　峰, 段　海, 新李星. 网络蠕虫扩散中蠕虫和良性蠕虫交互过程建模与分析[J]. 中国科学 E 辑(信息科学), 2004, 34(8): 841-856.

[3] 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(8): 1208-1219.

[4] Moore D. The Spread of the Code-Red Worm[Z]. (2007-01-31). http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml.

[5] 马知恩, 周义仓. 常微分方程的定性与稳定性方法[M]. 北京: 科学出版社, 2001.

（上接第 133 页）

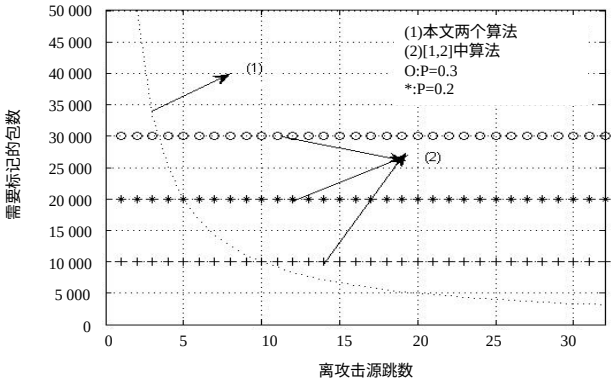

图 6　路由器需要标记包的数量比较

4　结束语

本文所提的两个算法采用可变概率包标记思想，消除了虚假标记信息导致路径重构时带来的不确定性，提高了 PPM 算法思想的安全性，而且可变概率包标记使路由器标记负担更加合理；算法通过在路由器中记录 IP 地址片断的发送信息，对包分片进行有序发送，大大减少了路径重构时需要包的数量。

参考文献

[1] Savage S, Wetherall D, Karlin A, et al. Network Support for IP Traceback[J]. IEEE/ACM Transactions on Networking, 2001, 9(3): 226-237.

[2] Park K, Lee H. On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack[C]//Proc. of IEEE INFOCOM'01. Alaska, USA: IEEE Press, 2001.

[3] Liu Jenshiuh, Lee Z, Chung Y. Efficient Dynamic Probabilistic Packet Marking for IP Traceback[C]//Proc. of the 11th International Conference on Networks. Sydney, Australia: [s. n.], 2003.

[4] Snoeren A C, Patridge C. Single-packet IP Traceback[J]. IEEE/ACM Transactions on Networking, 2002, 10(6): 721-734.

[5] Bellovin S. ICMP Traceback Messages[Z]. (2000-03-10). http://www.research.att.com/smb/papers/draft-bellovin-itrace-00.txt.

[6] Burch H, Cheswick B. Tracing Anonymous Packets to Their Approxmate Source[C]//Proc. of USENIX Conference. Los Angeles, California, USA: [s. n.], 2000.

[7] Stone R. Center Track: An IP Overlay Network for Tracking DoS Floodings[C]//Proc. of USENIX Security Symposium. Washington D. C., USA: [s. n.], 2000.