基于随机进程代数的 P2P 网络蠕虫对抗传播特性分析

严 博[1],吴晓平[1],廖 巍[1],李凤华[2]
(1.海军工程大学信息安全系,湖北武汉 430033; 2.北京电子科技学院电子信息工程系,北京 100070)

摘 要: 研究 P2P 网络中良性蠕虫和恶意蠕虫在对抗传播过程中的特性,可为制定合理的蠕虫对抗策略提供科学依据.提出一种基于随机进程代数的 P2P 网络蠕虫对抗传播的建模与分析方法.首先,分析了传播过程中蠕虫之间的对抗交互行为以及网络节点的状态转换过程;然后,利用 PEPA 语法建立了恶意蠕虫初始传播阶段与蠕虫对抗阶段的随机进程代数模型;最后,采用随机进程代数的流近似方法,推导得到能够描述蠕虫传播特性的微分方程组,通过求解该方程组,分析得到 P2P 蠕虫的对抗传播特性.试验结果表明,良性蠕虫可以有效遏制 P2P 网络中的恶意蠕虫传播,但需要根据当前的网络条件制定科学的传播策略,以减少良性蠕虫自身的传播对网络性能的影响.

关键词: 对等网络; 良性蠕虫; 传播模型; 随机进程代数
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2012)02-0293-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.02.014

Propagation Characteristics Analysis of Worm-Anti-Worm in P2P Network Based on Stochastic Process Algebra

YAN Bo[1], WU Xiao-ping[1], LIAO Wei[1], LI Feng-hua[2]
(1. *Department of Information Security, Naval University of Engineering, Wuhan, Hubei* 430033, *China*;
2. *Department of Electronic Engineering, Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*)

Abstract: In order to provide scientific bases for developing rational benign worm propagation policy in P2P networks, the propagation characteristics of benign worms in countering against malicious worms should be detailed researched. In this paper, a modeling and analysis method for propagation of worm-anti-worm in P2P network is proposed based on stochastic process algebra (SPA). Through analyzing the interactions between benign worms and malicious worms and the network node's state transition process, two SPA models are built by using PEPA syntax to describe the malicious worms' initial propagation phase and the worm-anti-worm phase respectively. To analysis these models, the paper makes use of continuous state-space approximation to transform the models into a set of ODEs. Simulation results show that the benign worms can effectively contain the spread of malicious worms, but it should apply scientific propagation policy according to the current network conditions, so as to ease the pressure of the network leaded by the propagation of benign worm.

Key words: P2P network; benign worm; propagation model; stochastic process algebra

1 引言

P2P 蠕虫指的是一类利用 P2P 应用程序和协议的特点、漏洞,在 P2P 网络中传播的蠕虫[1],这种蠕虫比普通蠕虫具有更大的威胁[2]:首先,由于可利用 P2P 节点的缓存列表中的邻居节点来构建攻击列表,P2P 蠕虫不需要探测扫描没有使用的 IP 地址,因此传播速率比普通蠕虫要快得多;其次,由于每次攻击都利用的是有效地址,所以攻击发起的连接成功率很高;最后,P2P 蠕虫攻击很难被检测.如果不能有效对 P2P 蠕虫进行防治,其很容易成为攻击者发动 DDoS 攻击[3]或传播僵尸程序[4]的工具.

近年来,利用良性蠕虫来防治恶意蠕虫的技术逐渐受到相关学者的关注,它的原理是借助良性蠕虫的传

收稿日期:2011-06-08;修回日期:2011-08-25
基金项目:国家自然科学基金(No.71171198);博士后科学基金特别资助(No.201003757);教育部重点项目(No.209156);北京市自然科学基金(No.4102056);新闻出版重大科技工程项目-数字版权保护技术研发工程(No.GXTC-CZ-1015004/05)

播,通过良性蠕虫自动为主机安装补丁或者清除主机上的恶意蠕虫,实现遏制恶意蠕虫传播的目的[5].文献[6]首次尝试通过建立相关模型描述良性蠕虫在网络蠕虫扩散中的动态特征;文献[7]研究了基于平衡树的良性蠕虫扩散策略;文献[8]则研究了一种分而治之的混合型良性蠕虫的传播模型.由于良性蠕虫在传播过程中会长时间扫描网络,自身也会对网络性能产生较大的影响,所以在一定程度上限制了良性蠕虫技术的进一步发展.但是在 P2P 网络中,蠕虫的传播不需要通过扫描来获取有效地址,因此良性蠕虫技术非常适合应用在 P2P 网络的环境中.

为使良性蠕虫在有效遏制恶意蠕虫传播的同时,尽可能减少对网络负荷的影响,需要根据蠕虫在对抗传播中的特点,科学的制定良性蠕虫的传播策略.但由于在实际的网络环境中进行蠕虫传播实验代价非常大,也会对网络造成危害,所以目前对蠕虫传播规律的研究多采用建立数学模型和仿真的方法.本文提出了一种基于随机进程代数(Stochastic Process Algebra,SPA)的复合型主动良性 P2P 蠕虫传播模型与分析方法,该方法能够精确描述蠕虫在对抗过程中的交互行为,并考虑了网络带宽对蠕虫传播的影响,利用随机进程代数的流近似方法,预测蠕虫的传播趋势,分析得到 P2P 网络中的蠕虫对抗传播的各种特性.

2 随机进程代数及其流近似方法

SPA 是在经典进程代数的基础上,给系统中的每个活动联系一个用于表现持续时间或概率特性的随机变量,从而到达实现对系统性能量化评价的目的.SPA 有很多种,本文中使用的 SPA 建模语言为 Hillston 提出的性能评价进程代数(Performance Evaluation Process Algebra,PEPA)[9].令系统所有动作的集合为 A,且有 $a\in A$,$L\subseteq A$,以及用以表征动作持续时间指数分布延迟的参数 $r\in\mathbf{R}^+$,此参数也称作动作的执行速率,则 PEPA 的语法定义如下:

$$P::=(a,r).P \mid P+Q \mid P<L>Q \mid P/L \mid C$$

这五组操作算子分别表示系统构件的前缀(Prefix)、选择(Choice)、合作(Cooperation)、隐藏(Hiding)和常量定义(Constant)等活动操作.有关 PEPA 更详细的介绍可以参考文献[9].

对 SPA 模型进行分析,通常是借助 SPA 的操作语义,将模型转变为 CTMC 进行分析.随着模型元素的增多及系统复杂程度的提高,常常会遇到状态空间爆炸问题,而 SPA 的流近似方法则是一种解决该问题的有效方法.由于 P2P 网络上节点数量巨大,利用 PEPA 语法建立蠕虫的对抗传播模型后,在分析过程中必然会遇到状态空间爆炸的问题,所以需要通过流近似的方法进行分析,下面简要介绍一下基于 PEPA 模型的流近似方法[10].

设在一个 PEPA 模型中某一类构件 P 共有 n 种不同的派生状态,则可用向量 $\boldsymbol{P}(t)=(N(P_1,t),N(P_2,t),\cdots,N(P_n,t))$ 表示该类构件在时刻 t 所处的状态,其中 $N(P_i,t),(1\leqslant i\leqslant n)$,表示此时处于 P_i 状态的构件数量,在不会引起歧义的情况下,也可简写为 $P_i(t)$.函数 $\rho_a(P_i,System(t))$ 表示系统 $System$ 中,在时刻 t 构件 P 在执行活动 a 时,状态 P_i 的构件数量变化的速率.根据上述信息,在经过很短的一段时间 δt 后,状态为 P_i 的构件数量变化情况:

$$P_i(t+\delta t)-P_i(t)=-\sum_{K:P_i\xrightarrow{a}P_j}\rho_a(Pi,System(t))\delta t+\sum_{K:P_j\xrightarrow{b}P_i}\rho_b(P_j,System(t))\delta t \tag{1}$$

式(1)等号右边前半部分表示的是状态 P_i 的构件通过执行相关的动作变迁至其余状态而导致自身减少的数量,后半部分则表示的是其余状态变迁为 P_i 状态而导致的 P_i 状态构件增加的数量,将式(1)两边同时除以 δt,并令 $\delta t\to 0$,则有:

$$\frac{\mathrm{d}P_i(t)}{\mathrm{d}t}=\sum_{K:P_i\xrightarrow{a}P_j}\rho_a(P_i,System(t))+\sum_{K:P_j\xrightarrow{b}P_i}\rho_b(P_j,System(t)) \tag{2}$$

有关式(1)和式(2)详细的推导过程,可参考文献[10].在推导得到系统全部构件对应的微分方程后,根据系统的初始状态,通过求解该常微分方程组就能得到模型中构件各状态的数量随时间的变化情况.

3 主动良性蠕虫及其传播分析

3.1 主动良性蠕虫分类

主动良性蠕虫是指能够主动的查找目标并传播的良性蠕虫[11].根据蠕虫的防御行为,主动良性蠕虫又可以分为安装补丁的主动良性蠕虫,掠夺的主动良性蠕虫,以及复合型的主动良性蠕虫.安装补丁的主动良性蠕虫可以主动发现有漏洞的主机,并且给其安装补丁;掠夺的主动良性蠕虫可以主动清除被恶意蠕虫感染的主机上的蠕虫;复合型的主动良性蠕虫则同时具有以上两类良性蠕虫的功能.文献[5]指出,复合型的主动良性蠕虫对恶意蠕虫的抑制效果要明显优于其余两类主动良性蠕虫,因此本文将重点研究复合型的主动良性蠕虫在 P2P 网络中的传播特点.

3.2 良性 P2P 蠕虫传播分析

在一个存在复合型的主动良性蠕虫对抗恶意蠕虫感染的P2P网络中,节点主机可以划分为4类状态[6]:(1)易感类(Suspicious):主机既没有被恶意蠕虫感染也没有被良性蠕虫感染;(2)感染类(Infectious):主机被恶意蠕虫感染但没有被良性蠕虫感染;(3)良性感染类(Benignly Infectious):主机被良性蠕虫感染;(4)恢复类(Recovered):主机即不会被恶意蠕虫感染也不会被良性蠕虫感染.

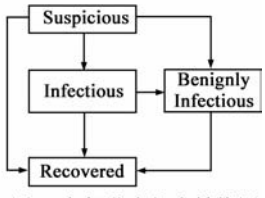


图1 主机节点状态转换图

在复合型的主动良性蠕虫进入网络后,主机间的状态转换如图 1 所示.易感类主机节点可以经蠕虫感染转换为感染类,也可以经良性蠕虫感染而转换为良性感染类;感染类主机节点上的恶意蠕虫可以被良性蠕虫清除而转换为良性感染类;易感类、感染类和良性感染类的节点都可以通过安装补丁转换为恢复类.

4 良性 P2P 蠕虫传播的 PEPA 模型

4.1 模型假设

良性蠕虫的投放时间一定会迟于恶意蠕虫在 P2P 网络上的出现时间,为了更加准确的研究良性蠕虫的传播特点,必须分两阶段来建立蠕虫的传播模型,即恶意蠕虫初始传播阶段和蠕虫对抗阶段.此外网络带宽也是影响蠕虫传播速度的一个重要因素,必须在模型中加以考虑.因此以下将在文献[12]的基础上,根据 P2P 网络上良性蠕虫与恶意蠕虫在对抗过程中的交互行为,建立蠕虫传播的 PEPA 模型,且模型符合以下假设:(1)网络中各节点无差异,且总数不随时间变化;(2)感染类节点和良性感染类节点发动感染一次其他节点的时间符合泊松分布;(3)不考虑恢复类节点由于系统重装或还原而重新变为易感类节点的情况;(4)除采用良性蠕虫外,不存在其他对抗恶意蠕虫传播的行为.

4.2 恶意蠕虫初始传播阶段的 PEPA 模型

假设在恶意蠕虫的初始传播阶段,蠕虫利用系统一个未知漏洞进行传播,网络对其基本没有任何防御能力,其传播速率只与感染类节点的数量和网络带宽有关,而网络中的节点主机只有易感染类 S 和感染类 I 两种状态.此时感染类主机节点可以速率 α 随机选择节点列表中的节点目标发起感染行为($infect_1$),并占用 P2P 网络的空闲状态的带宽 Net 传播蠕虫;被利用来传播恶意蠕虫的网络连接用 Net_1 表示,蠕虫在网络中以速率 β 传输至另一端的节点($infectS$);若另一端的节点为易感类节点,则在被感染后转换为感染类节点,若本身也是感染类节点,则状态保持不变;此外,蠕虫在传输过程中也可能由于干扰或超时而导致传输失败($fail$).综上所述,在恶意蠕虫初始传播阶段 P2P 网络上各构件的 PEPA 表达式为:

$$S = (infectS, T).I$$
$$I = (infect_1, \alpha).I + (infectS, T).I$$
$$Net = (infect_1, T).Net_1$$
$$Net_1 = (infectS, \beta).Net + (fail, \gamma).Net$$

式中的 T 表示该活动需与其他构件被动同步,活动的执行速率由同步发起方决定.根据以上 PEPA 表达式,可得恶意蠕虫初始传播阶段系统的 PEPA 描述等式 $System_1$,L_1 为构件之间的同步活动,且 $L_1 = \{infect_1, inftectS\}$.

$$System_1 = (S[m-i] \parallel I[i]) < L_1 > Net[n]$$

4.3 蠕虫对抗阶段的 PEPA 模型

恶意蠕虫在自由传播一段时间后,复合型的主动良性蠕虫开始投放到网络中.此时网络的各节点除了有易感类 S 和感染类 I 外,还出现了良性感染类 B,并且这三类节点都可以通过安装补丁转换成恢复类 R.具体的过程是:良性感染类节点以速率 η 对 P2P 网络中的节点发起良性感染行为($infect_2$);被用来传播良性蠕虫的网络连接用 Net_2 表示,良性蠕虫以速率 μ 传输至另一端节点($infectB$);如果另一端节点为易感类或感染类,则在被良性蠕虫感染后节点转换为良性感染类,而良性感染类节点则不受影响;与恶意蠕虫的传播一样,良性蠕虫在传播过程中也可能由于干扰或超时而导致传输失败($fail$).则在良性蠕虫投放阶段 P2P 网络上各构件的 PEPA 表达式为:

$$S = (infectS, T).I + (infectB, T).B + (patch, \delta_1).R$$
$$I = (infect_1, \alpha).I + (infectS, T).I + (infectB, T).B + (patch, \delta_2).R$$
$$B = (infect_2, \eta).B + (infectS, T).B + (infectB, T).B + (patch, \delta_3).R$$
$$R = STOP$$
$$R = (infectS, T).R + (infectB, T).R$$
$$Net = (infect_1, T).Net_1 + (infect_2, T).Net_2$$
$$Net_1 = (infectS, \beta).Net + (fail, \gamma).Net$$
$$Net_2 = (infectB, \mu).Net + (fail, \gamma).Net$$

由此可得在良性蠕虫初始投放后,蠕虫对抗阶段系统的 PEPA 描述等式 $System_2$,j 为良性蠕虫的投放数量,i' 为此时感染类节点的数量,易知当前易感类节点的数量为 $(m - i' - j)$,n_1 和 n_2 分别表示当前空闲连接和被占用连接的数量,L_2 为构件之间的同步活动,且 $L_2 = \{infect_1, infectS, infect_2, infectB\}$.

$$System_2 = (S[m - i' - j] \parallel I[i'] \parallel B[j]) < L_2 > (Net[n_1] \parallel Net_1[n_2])$$

4.4 蠕虫传播的连续状态模拟

用向量 $\boldsymbol{C}(t)$ 和向量 $\boldsymbol{N}(t)$ 分别来表示在 t 时刻 P2P 网络中的主机节点和网络带宽的状态，则有 $\boldsymbol{C}(t)=(S(t),I(t),B(t),R(t))$，$\boldsymbol{N}(t)=(Net(t),Net_1(t),Net_2(t))$. 令良性蠕虫的投放时间为 t'，则利用第 2 节中 PEPA 模型的流近似方法，可推导得到在恶意蠕虫初始传播阶段构件各状态数量的微分方程. 以下以恶意蠕虫初始传播阶段易感类节点的数量 $S(t)$ 为例，说明微分方程的推导过程. 由式(2)及恶意蠕虫初始传播阶段的 PEPA 模型可得：

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t}=-\rho_{infectS}(S,System_1(t))$$
$$=-\rho_{infectS}(S,\boldsymbol{C}(t)<L_1>\boldsymbol{N}(t)) \quad (3)$$

由于动作 *infectS* 是由 Net_1 状态的构件触发，S 状态的构件与其被动同步，所以两种状态构件数量变化的速率完全由 Net_1 状态的构件确定. 故由动作 *infectS* 的执行速率等于 β 可得，在 t 时刻两种状态构件数量变化的速率等于 $(\beta Net_1(t))$，而又由于当 S 状态的构件数量为 0 时，不具备执行同步动作的条件，显然此时两种状态构件数量变化的速率为 0. 综上所述，可得：

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t}=-\beta F_S(t)Net_1(t) \quad (4)$$

其中 $F_s(t)$ 为：$F_S(t)=\begin{cases}1, & S(t)>0\\ 0, & S(t)=0\end{cases}$.

同理可得在恶意蠕虫初始传播阶段关于状态 I、Net、Net_1 的微分方程：

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t}=\beta F_S(t)Net_1(t) \quad (5)$$

$$\frac{\mathrm{d}Net(t)}{\mathrm{d}t}=-\alpha F_{Net}(t)I(t)+\beta(F_S(t)+F_I(t))Net_1(t)+\gamma Net_1(t) \quad (6)$$

$$\frac{\mathrm{d}Net_1(t)}{\mathrm{d}t}=-\beta(F_S(t)+F_I(t))Net_1(t)-\gamma Net_1(t)+\alpha F_{Net}(t)I(t) \quad (7)$$

给定初始条件 $\boldsymbol{C}(0)=(m-i,i,0,0)$，以及 $\boldsymbol{N}(0)=(n,0,0)$，在 $[0,t']$ 时间范围内，解由式(4)～式(7)组成的微分方程组，可求得在良性蠕虫投放时间 t' 前，恶意蠕虫的传播趋势以及网络状态的变化情况.

同样的方法可推导得到，在 t' 时刻投放良性蠕虫后由 PEPA 模型派生出的微分方程组：

$$\frac{\mathrm{d}S(t)}{\mathrm{d}t}=-\beta F_S(t)Net_1(t)-\mu F_S(t)Net_2(t)-\delta_1 S(t) \quad (8)$$

$$\frac{\mathrm{d}I(t)}{\mathrm{d}t}=-\mu F_I(t)Net_2(t)-\delta_2 I(t)+\beta F_S(t)Net_1(t) \quad (9)$$

$$\frac{\mathrm{d}B(t)}{\mathrm{d}t}=-\delta_3 B(t)+\mu(F_S(t)+F_I(t))Net_2(t) \quad (10)$$

$$\frac{\mathrm{d}R(t)}{\mathrm{d}t}=\delta_1 S(t)+\delta_2 I(t)+\delta_3 B(t) \quad (11)$$

$$\frac{\mathrm{d}Net(t)}{\mathrm{d}t}=-\alpha F_{Net}(t)I(t)-\eta F_{Net}(t)B(t)+\beta(F_S(t)+F_I(t)+F_B(t))Net_1(t)+\mu(F_S(t)+F_I(t)+F_B(t))Net_2(t)+\gamma(Net_1(t)+Net_2(t)) \quad (12)$$

$$\frac{\mathrm{d}Net_1(t)}{\mathrm{d}t}=-\beta(F_S(t)+F_I(t)+F_B(t))Net_1(t)-\gamma Net_1(t)+\alpha F_{Net}(t)I(t) \quad (13)$$

$$\frac{\mathrm{d}Net_2(t)}{\mathrm{d}t}=-\mu(F_S(t)+F_I(t)+F_B(t))Net_2(t)-\gamma Net_2(t)+\eta F_{Net}(t)B(t) \quad (14)$$

该方程组的初始条件为：$\boldsymbol{C}(t')=(m-i'-j,i',j,0)$，$\boldsymbol{N}(t')=(n_1,n_2,0)$，其中 i'、n_1、n_2 分别为在恶意蠕虫初始传播阶段，在时刻 t' 时，$I(t)$、$Net(t)$、$Net(t)$ 的函数值.

5 传播特性分析

为了进一步验证上一节中建立的良性蠕虫传播 PEPA 模型的正确性，本节将通过 Matlab 软件，利用龙格—库塔法仿真计算上节中 PEPA 模型所派生出的微分方程组. 在仿真实验中，模型的部分参数取值如表 1 所示.

表 1 模型参数取值

参数	取值	参数	取值	参数	取值
α	0.25	η	0.25	δ_2	1.0e－5
β	0.6	μ	0.6	δ_3	0.05
γ	0.09	δ_1	1.0e－5	m	3.0e＋5

5.1 恶意蠕虫初始传播阶段的特性分析

在恶意蠕虫的初始传播阶段，由于恶意蠕虫利用的是系统的未知漏洞，并且暂时也没有采用有效的手段遏制其传播，所以在该阶段恶意蠕虫基本是自由传播，其传播速率只与感染类节点的数量和网络带宽有关. 图 2 显示了当恶意蠕虫的初始投放数量 i 等于 10，网络最大可支持的连接数量 n 等于 60000 时，易感类节

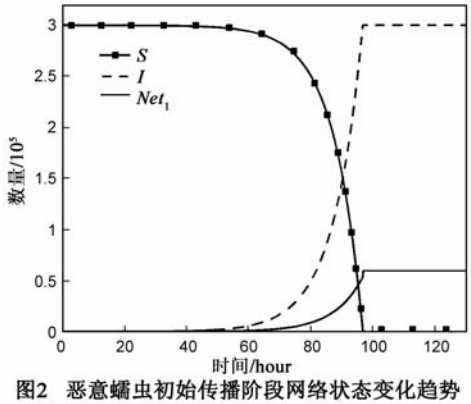


图2 恶意蠕虫初始传播阶段网络状态变化趋势

点、感染类节点,以及被占用网络连接数量的变化趋势.从结果中可以看出,如果不采取有效手段遏制蠕虫的传播,只需要四天左右的时间这种恶意蠕虫就可以感染 P2P 网络中所有的节点,并极大的占用网络带宽,给网络的正常运行带来巨大的危害.

为考察不同网络带宽下,初始传播阶段感染恶意蠕虫的主机节点的数量变化趋势,在保持其余参数不变的情况下,只改变网络最大可支持的连接数量 n 的值,分析了 n 在 7500 至 75000 范围内变化时,易感类节点数量随时间的变化情况,如图 3 所示.从结果中可以看出,在 n 小于 30000 时,网络带宽对恶意蠕虫传播速度的影响比较明显,而在 n 大于 30000 时,主机节点的状态变化趋势基本上差异不大,网络带宽已不是影响恶意蠕虫传播的主要因素.

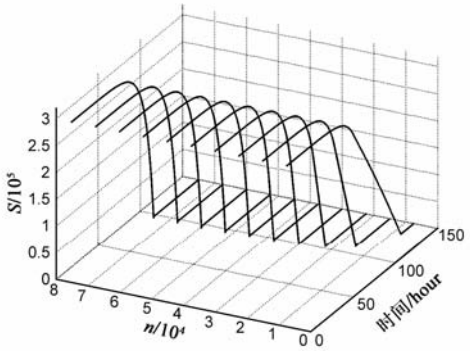


图3　不同网络带宽下易感类主机数量变化趋势

5.2　蠕虫对抗阶段的特性分析

在图 2 的基础上,继续研究在进入蠕虫对抗阶段后网络状态的变化情况.假设在恶意蠕虫传播 25 个小时后($t'=25$),复合型主动良性 P2P 蠕虫开始投放到网络中,且初始投放的数量为 3,即 $j=3$.求解由式(4)~式(7)组成的微分方程组,计算得到在第 25 小时各函数的数值,并将其作为求解微分方程组式(8)~式(14)的初始条件.图 4 显示了仿真得到的蠕虫对抗阶段的网络状态变化趋势,从仿真结果中可以看出,复合型主动良性 P2P 蠕虫可以有效遏制 P2P 网络中恶意蠕虫的传播,但其自身的传播也会占用大量的网络带宽,特别是在 138 小时左右,当感染类节点基本上清除后,由于良性蠕虫的继续传播,可用带宽 *Net* 还会在一段时间内继续减少,并经历一段"阵痛"后才开始回升.所以此时应该停止全部或部分良性蠕虫的传播,或者降低良性蠕虫的传播速率,以保证给用户留出足够的可用带宽,这样即达到了遏制恶意蠕虫传播的目的,又克服了良性蠕虫自身的传播对网络带宽造成的影响.

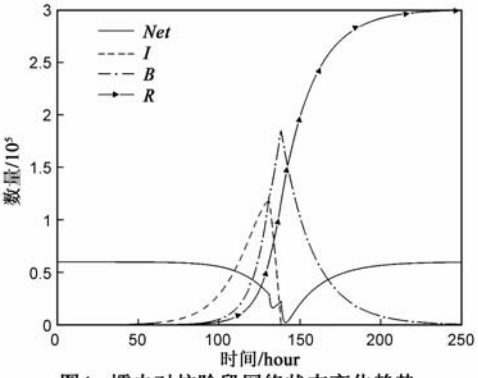


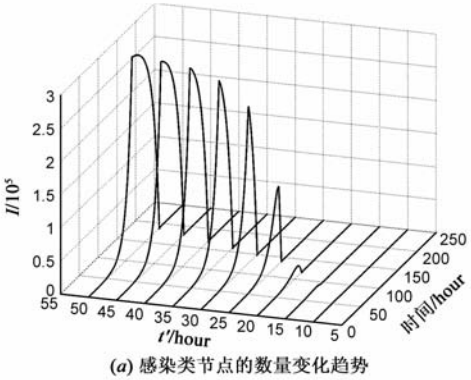
图4　蠕虫对抗阶段网络状态变化趋势

5.3　投放条件分析

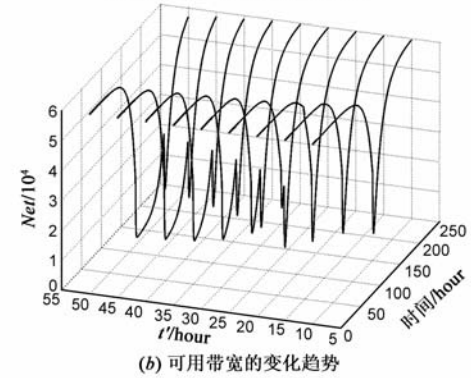
良性蠕虫的初始投放条件不同,对遏制恶意蠕虫传播的效果也会产生影响,通常这些条件包括良性蠕虫投放时间、投放数量、感染速率、安装补丁的速率等.以下主要分析良性蠕虫的投放时间和投放数量这两个条件对遏制效果产生的影响.

(1) 良性蠕虫投放时间对遏制效果影响分析

假定恶意蠕虫的初始投放数量 i 等于 10,良性蠕虫的初始投放数量 j 等于 3,网络最大可支持的连接数量 n 等于 60000.图 5(a)和图 5(b)分别显示了良性蠕虫投放时间 t' 在 10 至 50 范围内变化时,感染类节点数量和可用带宽数量的变化趋势比较.从图 5 中可以看出,良性蠕虫的投放时间越早,对遏制恶意蠕虫传播的效果越好,并且如果投放时间较早,网络可用带宽的降低主要是由良性蠕虫的传播引起的,此时可适当降低良性蠕虫的感染速率,并提高良性感染类节点主机安装补丁的速率,以减轻网络的负担.



(a) 感染类节点的数量变化趋势

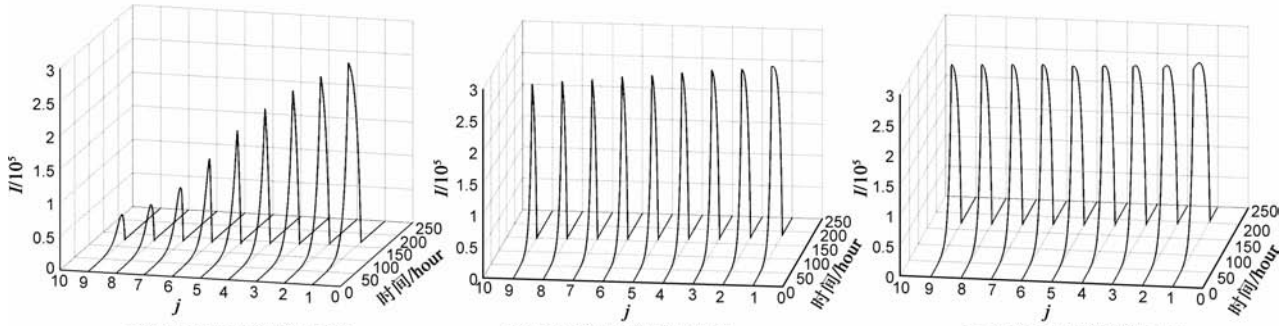


(b) 可用带宽的变化趋势

图5　良性蠕虫投放时间对遏制效果的影响

(2) 良性蠕虫初始投放数量对遏制效果影响分析

继续假定恶意蠕虫的初始投放数量 i 等于 10,网络最大可支持的连接数量 n 等于 60000. 图 6(a)和图 6(b)分别显示了在良性蠕虫投放时间 t' 等于 30、40 和 50 时,不同的良性蠕虫初始投放数量对遏制恶意蠕虫传播的效果比较. 从图中很容易看出,良性蠕虫投放时间越晚,不同的良性蠕虫初始投放数量对遏制恶意蠕虫传播的效果差异越小.



(a) 良性蠕虫投放时间t'=30 (b) 良性蠕虫投放时间t'=40 (c) 良性蠕虫投放时间t'=50

图6 良性蠕虫初始投放数量对遏制效果的影响

6 结论

分析网络蠕虫传播特性,传统上常常利用的传染病学的传播模型,它是一种基于感染类节点在网络所有节点中的密度来研究蠕虫传播的方法,而本文采用的随机进程代数的方法本质上则是基于的是网络节点之间的交互频率和同步行为,显然这更符合 P2P 网络的实际特点. 并且,利用 SPA 的语法,能够精确描述 P2P 网络中各网络组件之间的交互行为,更便于分析不同条件下蠕虫的传播特点. 仿真试验结果表明,利用良性蠕虫对抗的方法可有效遏制 P2P 网络中恶意蠕虫的传播,但良性蠕虫自身的传播也会对网络性能造成影响,因此必须根据其投放时的条件以及网络状态,分析预测 P2P 网络中蠕虫的对抗传播特性,制定科学的良性蠕虫投放和传播策略,合理控制良性蠕虫的传播速度和规模,以尽量减轻其对网络性能的影响.

参考文献

[1] S Hatahet, A Bouabdallah, C Yacine. A new worm propagation threat in bit torrent: Modeling and analysis[J]. Telecommunication Systems, 2010, 45(2-3): 95-109.

[2] 冯朝胜,秦志光,劳伦斯·库珀特等. P2P 网络中沉默型蠕虫传播建模与分析[J]. 计算机研究与发展,2010,47(3):500-507.
Feng Chao-sheng, Qing Zhi-guang, Laurence Cuthbert, et al. Reactive worms propagation modeling and analysis in peer-to-peer networks[J]. Journal of Computer Research and Development, 2010, 45(2-3): 95-109. (in Chinese)

[3] 孙长华,刘斌. 分布式拒绝服务攻击研究新进展综述[J]. 电子学报,2009,37(7):1562-1570.
Sun Chang-hua, Liu Bin. Survey on new solutions against distributed denial of service attacks[J]. Acta Electronica Sinica, 2009, 37(7): 1562-1570. (in Chinese)

[4] 柴胜,胡亮,梁波. 一种 p2p Botnet 在线检测方法研究[J]. 电子学报,2011,39(4):906-912.
Chai Sheng, Hu Liang, Liang Bo. The p2p Botnet Online Detect Approach Research[J]. Acta Electronica Sinica, 2011, 39(4): 906-912. (in Chinese)

[5] 周翰逊,赵宏. 主动良性蠕虫和混合良性蠕虫的建模与分析[J]. 计算机研究与发展,2007,44(6):958-964.
Zhou Han-xun, Zhao Hong. Modeling and analysis of active-benign worms and hybrid-benign worms[J]. Journal of Computer Research and Development, 2007, 44(6): 958-964. (in Chinese)

[6] 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),2004,34(8):841-856.
Yang Feng, Duan Hai-xin, Li Xing. Modeling and analysis on the interaction between the internet worm and anti-worm[J]. Science in China (Ser. E), 2004, 34(8): 841-856. (in Chinese)

[7] 王佰玲,方滨兴,云晓春,等. 基于平衡树的良性蠕虫扩散策略[J]. 计算机研究与发展,2006,43(9):1593-1602.
Wang Bai-ling, Fang Bin-xing, Yun Xiao-chun, et al. A new friendly worm propagation strategy based on diffusing tree[J]. Journal of Computer Research and Development, 2006, 43(9): 1593-1602. (in Chinese)

[8] 周翰逊,赵宏,闻英友. 分而治之的混合型良性蠕虫的建模与分析[J]. 计算机研究与发展,2009,46(7):1110-1116.
Zhou Han-xun, Zhao Hong, Wen Ying-you. Modeling and analysis of divide-and-rule-hybrid-benign worms[J]. Journal of Computer Research and Development, 2009, 46(7): 1110-1116. (in Chinese)

[9] J Hillston. A Compositional Approach to Performance Modeling

[D]. Edinburgh: University of Edinburgh, 1994.
[10] V Galpin. Continuous approximation of PEPA models and Petri nets[J]. International Journal of Computer Aided Engineering and Technology, 2010, 2(4): 324 – 339.
[11] C Frank, C S Emre, J Xu. WORM vs. worm: Preliminary study of an active counter-attack mechanism[A]. Proceeding of the 2004 ACM CCS Workshop on Rapid Malcode[C]. Washington, USA: ACM Press, 2004. 83 – 93.
[12] J T Bradley, S T Gilmore, J Hillston. Analyzing distributed Internet worm attacks using continuous state-space approximation of process algebra models[J]. Journal of Computer and system Science, 2008, 74(6): 1013 – 1032.

作者简介

严　博　男,1984 年 10 月生于江西丰城,海军工程大学信息安全系博士研究生.研究方向为计算机网络安全、网络性能评价与优化.
E-mail: ybnav@163.com

吴晓平　男,1961 年 5 月生于山西新绛,海军工程大学信息安全系教授,博士生导师.主要研究方向为信息安全,系统工程.
E-mail: wxp8@sohu.com

廖　巍　男,1980 年 2 月生于湖北襄阳,海军工程大学信息安全系讲师,博士.主要研究方向为数据库与网络安全.
E-mail: liaowei_2000@163.com

李凤华　男,1966 年 3 月生于湖北浠水,北京电子科技学院电子信息工程系教授,博士生导师.主要研究方向为网络安全与可信计算.
E-mail: lfh@besti.edu.cn