无尺度网络下具有双因素的僵尸网络传播模型

黄 彪 成淑萍 欧阳晨星 谭 良
(四川师范大学计算机学院 四川省可视化计算与虚拟现实重点实验室 成都 610068)
(中国科学院计算技术研究所 北京 100080)

摘 要 随着网络技术的发展,僵尸网络逐渐成为Internet上最具威胁的攻击平台。而现今的网络是随机网络、无尺度网络等构成的一个复杂网络。结合无尺度的特性,考虑僵尸网络传播过程中部分主机的免疫特性与网络阻塞特征,提出一种无尺度网络下具有双因素的僵尸网络传播模型。该模型基于Internet的实际情况,重点考虑了无尺度网络的拓扑结构,并结合了僵尸网络中部分脆弱主机由于提前从易感染的网络中移除而具有的免疫特征情况与传播过程中的网络流量阻塞情况。Matlab仿真结果表明,这种传播模型更符合真实网络中僵尸网络的传播规律。

关键词 无尺度网络,僵尸网络,僵尸程序,传播模型,免疫特征,网络流量阻塞
中图法分类号 TP393 **文献标识码** A

Botnet Propagation Model with Two-factor on Scale-free Network

HUANG Biao CHENG Shu-ping OUYANG Chen-xing TAN Liang
(Visual Computing and Virtual Reality Key Laboratory of Sichuan Province, College of Computer, Sichuan Normal University, Chengdu 610068, China)
(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China)

Abstract With the developing of network, botnet has become a major threat attack platform to Internet. The current network is a complex network consisting of the random network and the scale-free network. This paper, combining the features of scale-free network, immunity and network traffic congestion, proposed a new botnet propagation model with two-factor on Scale-free network. This model considers carefully the real situation of the Internet, especially the Scale-free network topology, immunity of the host removed from the susceptible network in advance and network traffic congestion. Simulation result shows that the botnet propagation model more exactly satisfies the practical propagation laws and infection characteristics of bot on Internet.

Keywords Scale-free network, Botnet, Bot, Propagation model, Immunity, Network traffic congestion

1 引言

当今社会的网络不再是单一的随机网络,而是由随机网络、无尺度网络构成的一个复杂网络。无尺度网络中绝大部分节点与其他节点连接的度很小,但有部分节点却与网络中大量节点都有连接,这些节点的度非常大,称为集散节点,这些集散节点的连通情况会影响整个网络。

无尺度网络的研究在1999年有了很大进展,Barabasi和Albert[1]在研究中发现实际网络中一个节点的度为k的概率服从"幂次定律"。随后他们提出了BA模型,其反映了无尺度网络的两个重要特性:增长性和择优连接性。自BA模型提出以后,对无尺度网络的研究有了很大进展。"小世界"网络特性是现实世界网络当中普遍存在的一种现象,小世界特性即是在一个小范围内,消息和信息等传递的速度非常快,Watts和Strogatz对这一现象进行了总结。Watts和Strogatz通过对ER模型的研究并结合自然界的小世界效应提出了著名的WS模型[2]。WS模型的提出掀起了复杂网络研究的热潮[3]。虽然现在对于无尺度网络的特点有了较广泛的研究,对无尺度网络下的蠕虫传播也有分析和探讨[4],但是关于无尺度网络下的僵尸网络传播模型却尚未有很好的文献进行阐述。

僵尸网络作为现代网络的高效率攻击平台,是当前网络安全领域面临的主要威胁之一。僵尸网络是由一些受恶意代码影响、被控制的计算机组成的网络;攻击者出于恶意目的通过传播僵尸程序来控制大量主机,并通过一对多的命令方式与其他主机进行通信[5]。僵尸网络经过基于IRC协议的僵尸网络、基于HTTP协议的僵尸网络、基于DNS协议的僵尸网络、基于P2P协议的僵尸网络的演化后,其构建技术更加复杂、生命更加顽强。

僵尸网络对现今的网络已经造成了严重的威胁,各个国家的安全部门都在对僵尸网络进行研究和分析。2004年,CNCERT/CC发现攻击流量来自庞大的被植入某特定恶意

到稿日期:2011-12-19 返修日期:2012-03-16 本文受国家自然科学基金面上项目(60970113)资助。
黄 彪(1988-),男,硕士,主要研究方向为网络安全;成淑萍(1988-),女,硕士,主要研究方向为网络安全;欧阳晨星(1986-),男,硕士,主要研究方向为网络安全;谭 良(1973-),男,博士,教授,主要研究方向为信息安全、网络计算。

程序的计算机群，该机群的数目达到近 10 万台，来自河北的某黑客通过境内外多台服务器秘密操纵这些计算机。被操纵控制的计算机中，有 6 万多台位于我国境内，其中还包括一些政府和其他重要部门的计算机[6]。2006 年 Symantec 公司监测数据表明[7]，中国大陆被僵尸网络控制的主机数所占全世界总数的比例从上半年的 20%增长到下半年的 26%，超过美国，成为最大的僵尸网络受害国。其实，僵尸网络所需要的技术原理在 20 世纪 90 年代中期就已成熟。由此可以看出，僵尸网络已经成为国内乃至全世界的网络安全领域最为关注的危害之一。

目前的僵尸网络传播模型均是根据蠕虫的传播模型得出的。但是僵尸程序的传播与蠕虫传播并不完全一样，僵尸程序的传播是受控的，与蠕虫的不受控、自动传播是不同的。所以可以通过蠕虫的传播模型来对僵尸网络的传播进行分析与研究。现今研究中，已经提出的网络蠕虫传播模型包括基本的 SEM 模型[8]、KM 模型[9]，以及考虑蠕虫反制机制的双因素模型[10]等。但是这些模型没有考虑僵尸程序本身的特点，因此不能直接用于描述僵尸网络的传播。虽然在 2006 年 Dagon[11]提出了一个基于时区的僵尸网络传播模型，但是该模型一方面对当前融合了多种传播形式的僵尸网络没有进行系统和全面的描述；另一方面并没有考虑到部分主机的免疫特性，所以对僵尸网络的传播的描述仍不够准确。

本文结合无尺度网络的特点以及僵尸网络的传播特性，提出一种无尺度网络下具有双因素的僵尸网络传播模型。该模型不仅考虑了无尺度网络的两个重要特性：增长性和择优连接性，还考虑了僵尸网络传播过程中可能遇到的因素：①人们通过检测手段预知到网络中可能存在恶意程序，而进行预先免疫处理，令部分安全措施较弱的主机从危险网络中移除；②随着被感染的主机增多，网络中由僵尸程序产生的通信数据包使网络的通信流量增大，网络出现拥塞现象，数据包传送延时增加，其感染速度受到影响。仿真结果表明，这种传播模型对于僵尸网络在无尺度网络下的传播的描述比较准确。

2 相关工作

对于无尺度网络的特性，国内外专家都进行了大量研究与分析。文献[12]从统计力学的角度分析和考察了无尺度网络的基本特征，介绍了无尺度网络最常用的 BA 模型以及几种以其为基础的修正模型的构造原理。文献[1]提出无尺度网络具有一些其他网络所不具有的特征，其中最重要的是“集散节点的马太效应”和“鲁棒性和脆弱性共存”这两个特征。集散节点的马太效应：在无尺度网络中节点是不断增加的，而新加入的节点会根据“择优连接性”选择那些连接度更大的节点建立连接，这就会使得集散节点的连接数不断增大，而大多数节点的连接数却很小，呈现出马太效应。同时，由于集散节点的存在，使得无尺度网络表现出鲁棒性与脆弱性共存的特点。但对恶意程序在网络上如何传播并未涉及。文献[13]对病毒在无尺度网络上的传播进行了仿真研究，通过构建一个 BA 模型，对病毒的传播进行模拟，并且对传播过程中受到的各种影响进行了讨论。文献[4]对如何构建无尺度的蠕虫传播模型，提出了 3 种方法，分别为基于 BA 模型的传播、基于随机游走的蠕虫传播、基于节点适应度的蠕虫传播。但是这些文献都只针对了无尺度网络下蠕虫的传播。虽然僵尸网络的传播类似蠕虫，但是由于其的可控制性，它并不能直接使用蠕虫的传播模型。

而僵尸网络传播模型的研究，也是从分析一些经典蠕虫的传播模型入手的，比如 SEM、KM 和双因素传播模型。Streftaris 在文献[8]中阐述了网络蠕虫的传播和生物病毒的传播在自我复制和传播行为上有着相似的特点，同时提出了一种简单传染病模型——SEM 模型，这种模型的基本假设为：蠕虫传播的网络环境为一个全连通的结构，蠕虫代码可以从被感染主机直接传送到目标主机；网络中的每台主机有易感染状态和被感染状态；一台主机一旦被感染后，就始终保持被感染的状态。可是由于 SEM 模型太过于理想，对于蠕虫传播过程中受到的各种影响，如网络拥塞、主机从感染状态恢复到正常状态等都未进行考虑和分析，因此它并不符合网络中蠕虫的传播。Frauenthal 等人[9]在 SEM 模型的基础上考虑了受感染主机的 3 种状态，即易感染、被感染和免疫状态，提出了 KM 模型。这种模型虽然考虑了免疫状态的主机但没有考虑到受感染主机的补丁更新和升级后进入非易感染状态，因此不能很好地反应蠕虫传播的真实情况。文献[10]在传统的蠕虫传播模型 SEM 模型和 KM 模型的基础上，提出了一种双因素蠕虫传播模型，这种模型考虑了蠕虫传播过程中的两个因素：①蠕虫的传播过程中，存在人为的应对措施，那些特别脆弱的易感染主机会在未被感染前就从蠕虫传播环境中被移除；②蠕虫传播过程中引起的网络拥塞。但僵尸程序不同于蠕虫，所以只能借鉴蠕虫的传播模型来研究僵尸网络的传播，而不能直接套用。

所以，要想很好地描述无尺度下的僵尸网络，就要从无尺度的特征和网络中主机的免疫特性和网络流量的阻塞因素入手。

3 无尺度网络下具有双因素的僵尸网络传播模型

为了更好地描述无尺度网络下的僵尸网络，就需要考虑僵尸网络传播过程中的两个影响因素：第一点为僵尸网络本身的免疫特征，第二点为网络中造成的流量阻塞。在考虑这两个因素的前提下，再结合无尺度的特性构建的僵尸网络更符合真实网络中的情况。

3.1 僵尸网络的免疫特征

僵尸程序是根据蠕虫程序发展而来，根据一些经典的蠕虫传播可以得出僵尸网络的传播模型。在 2006 年，Dagon 等人[11]提出的僵尸网络传播模型反应了僵尸网络的上下线状态，并且也考虑了网络中的主机从感染状态恢复到正常状态的情况，但是文献[10]中提到的双因素蠕虫传播模型中考虑的免疫状态是两种情况，而这两种情况都符合僵尸网络的传播特性。因此提出的免疫特征包括两个方面：(1)部分被感染主机通过打补丁等措施从感染状态恢复到正常状态的情况；(2)在无尺度网络中，僵尸网络传播一段时间以后，人们会意识到该网络中存在恶意程序，从而预先移除一些尚未被感染但是安全措施较低且有安全漏洞的主机。这种免疫特征不仅在蠕虫网络中存在，在僵尸网络的传播中同样存在。

3.2 网络流量阻塞

在真实的网络中，特别是在无尺度网络中，随着被感染的主机增多，网络中由僵尸程序产生的通信数据包使网络的通信流量增大，网络出现拥塞现象，数据包传送延时增加，其感染速度受到影响。所以随着网络流量拥塞程度的增大，感染代码实际的扫描速率将会随之下降，从而降低了僵尸程序的

传播速度。随着被感染主机数的增加，僵尸程序传播中产生的数据包数量也在不断增加，从而引起网络拥塞，导致僵尸程序的感染率下降，感染率就不能再用一个常数来描述，感染率会随着网络感染的情况发生变化。

3.3 无尺度网络特性

无尺度网络是当今网络中普遍存在的网络，它有两个主要特性：增长性和择优连接性[14]。增长性是指网络建立初始时，只有少数几个节点，每隔一段时间加入一些新的网络节点，并建立新加节点到已有节点的若干边；而择优连接性是指新节点与一个已经存在的节点 i 相连的概率 π_i 与节点的度、之间满足如下关系：

$$\pi_i=\frac{k_i}{\sum_j k_j} \tag{1}$$

式中，$\sum_j k_j$ 为网络中各节点度数的总和。每个单位时间有 m 条边加入网络，以 t 记录时间的增长，$\sum_j k_j=2mt$。经过 t 时间步后，这个算法会产生一个节点数 $N=t+m_0$、边数为 m_t 的网络。运用平均域理论[12]对模型进行分析，可以得出模型的度分布为：

$$p(k)=\frac{2m^2t}{(m_0+t)}k^{-3} \tag{2}$$

BA 网络模型的度具有幂律型分布，其度分布的幂律规律也被证明广泛存在于现实网络中。因此要研究僵尸网络在无尺度网络上的传播模型，就要结合无尺度网络的这两个特性。

3.4 传播模型

在传播模型中假定僵尸程序的感染率为 β_0。由于是无尺度网络，因此感染主机 i 传播僵尸程序的概率 β_i 还受到其节点度的影响，即 i 的度数越大，其能感染的主机数会相应增多，传播的成功率也相应变高[15]；同时，随着感染主机数量的增多，网络中传送的数据包数量也在不断增加，从而引起网络的阻塞，降低僵尸程序的传播速度，因此感染主机 i 的感染率为：

$$\beta_i=\beta_0\left(1-\frac{I(t)}{N(t)}\right)^{\eta}\frac{k_i}{\sum_j k_j}$$

由于网络中共有 $I(t)$ 个感染主机，根据上式可得单位时间内的感染率：

$$\beta=\sum_{i=1}^{i=I(t)}\beta_i k_i \tag{3}$$

定义无尺度网络中 t 时间步时，$I(t)$ 是被感染的主机数，$S(t)$ 为易感染的主机数，N 表示网络中最初的易感染主机数，而网络中的易感染主机总数为一个 t 相关的函数 $N(t)=m0+t$。考虑到受害主机上下线的状态[11]，定义 $I'(t)$ 为当前在线的感染主机数；$S'(t)$ 为当前在线的易感染主机数；$\alpha(t)$ 为 t 时刻的主机在线比率，$\alpha(t)$ 的值在白天达到最高峰，夜晚由于大部分计算机下线，此值到达低谷。因此在 t 时刻已经被感染和易感染主机数量分别为：

$$I'(t)=\alpha(t)I(t) \tag{4}$$

$$S'(t)=\alpha(t)S(t) \tag{5}$$

下面描述部分主机从感染状态变为免疫状态而从网络中被移除的情况，根据最基本的 KM 蠕虫传播模型[9]，被感染主机在持续发送蠕虫数据包一段时间后，被关闭或者计算资源被耗尽，无法继续发送蠕虫数据包，或者被感染主机在被感染一段时间后，经过用户处理，从感染状态恢复，并对此蠕虫免疫，不会被再次感染。定义 $R(t)$ 为 t 时刻从感染状态恢复到免疫状态的主机数；γ 为恢复率，从 KM 模型可以得出：

$$dR(t)/dt=\gamma I'(t) \tag{6}$$

虽然 KM 模型讨论的是把从感染状态恢复的主机从网络中移除的情况，但是从易感染状态到免疫状态的变化过程较为复杂。根据文献[10]提出的双因素蠕虫传播模型，在蠕虫最开始传播的时候，用户并不会知道网络中存在蠕虫，相应的防御措施采用较少。随着蠕虫数量的增长，被感染的主机越来越多，人们对蠕虫传播的关注程度逐渐增加，因此对易感染主机进行预先免疫处理，令其从蠕虫环境中移除。定义这种进行了提前免疫处理的易感染主机为 $Q(t)$；$J(t)$ 为在 t 时刻已被感染的主机数，即 $I(t)+R(t)$；μ 为修正系数，具体根据恶意程序的传播情况进行调整：

$$dQ(t)/dt=\mu S'(t)J(t) \tag{7}$$

可以看出，$Q(t)$ 的变化与 $J(t)$ 变化关系密切，并且与 $S'(t)$ 相关。因为考虑了 $Q(t)$，并且根据双因素蠕虫传播模型可知在 t 时刻的易感染主机数为：

$$S(t)=N-I(t)-R(t)-Q(t) \tag{8}$$

由于 β 表示感染率，因此再考虑到感染主机上下线的状态，可得 $S(t)$ 的变化情况为：

$$dS(t)/dt=-\beta S'(t)I'(t)-dQ(t)/dt \tag{9}$$

综上所述，根据方程(3)—(9)得到僵尸网络增长的方程组：

$$\begin{cases}\beta=\sum_{i=1}^{i=I(t)}\beta_0\left(1-\frac{I(t)}{N(t)}\right)^{\eta}\frac{k_i^2}{\sum_j k_j}\\ I'(t)=\alpha(t)I(t)\\ S'(t)=\alpha(t)S(t)\\ dR(t)/dt=\gamma I'(t)\\ dQ(t)/dt=\mu S'(t)J(t)\\ S(t)=N-I(t)-R(t)-Q(t)\\ dS(t)/dt=-\beta S'(t)I'(t)-dQ(t)/dt\end{cases} \tag{10}$$

化简方程组(10)，可以知道这种无尺度网络下具有免疫特征的僵尸网络被感染主机数 $I(t)$ 的变化情况为：

$$dI(t)/dt=\sum_{i=1}^{i=I(t)}\beta_0\left(1-\frac{I(t)}{N(t)}\right)^{\eta}\frac{k_i^2}{\sum_j k_j}\alpha^2(t)I(t)[N(t)-I(t)-R(t)-Q(t)]-\gamma\alpha(t)I(t)$$

4 模型仿真与比较

4.1 模型仿真

根据以上提出的微分方程，使用 MATLAB 进行仿真，可以得出感染主机的变化情况。设 $I(0)=10$，$S(0)=N-I(0)$，$R(0)=Q(0)=0$，$N=1000000$，$\beta_0=0.0000008$，$\mu=0.00000006$，$\alpha=0.6$，$\gamma=0.05$，$\eta=2$，因此感染主机的变化情况如图 1 所示。

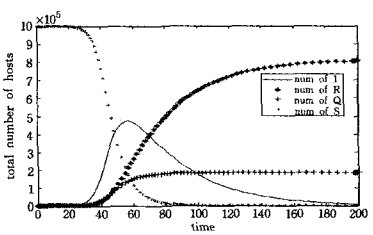

图 1 无尺度网络下具有双因素的僵尸网络传播模型

通过分析图 1 的 4 种曲线可以看出，被感染主机数 $I(t)$ 的数量随着时间的增长逐渐增加。由于刚开始的网络中感染

的主机数很少，因此感染节点的度很小，僵尸程序传播的速度比较慢。但在时间步到达 35 以后，由于僵尸程序感染了无尺度网络中的集散节点，因此僵尸程序开始大规模传播，而感染主机的数量也开始急速增长，到时间步 60 左右的时候达到最大值，接近 500000 台主机。但是随着感染程序的传播，也不断有被感染主机恢复到免疫状态或者从易感染网络中移除，即 R 和 Q 的增加。随着时间的推移，被移除主机的数量逐渐增大，I 的值慢慢变小，最终在时间步为 200 的时候减少为 0 台，至此僵尸程序传播结束。

在感染的初始阶段，$I(t)$ 的增加速度快于感染后阶段 $I(t)$ 的减少速度。这是因为，随着被感染主机的增多，加入僵尸网络的主机数增多，网络中的通信流量将增大，网络就会开始出现拥塞现象，感染代码实际的扫描速率也将会随之下降，从而影响了僵尸程序的传播速度。

图中的 R 表示主机从被感染状态恢复到免疫状态的数量。在传播刚开始时，由于被感染的主机数很小，因此并没有采取措施令主机从感染状态恢复到正常状态。但是随着 I 的不断增大，在时间步为 40 的时候，用户采取各种处理手段来清除僵尸程序，并且在 I 的值达到最大时，依然保持原有的速度增长，直到网络中没有感染主机的存在，即 I 的值变为 0。

Q 表示未被感染的主机提前进行了预防措施，在 I 增长了一段时间以后，人们意识到网络中可能存在恶意程序，从而采取了免疫措施让易感染的主机从网络中移除。在僵尸程序十分活跃的时候，被移除的主机数也相应增多，因此 Q 的数量随着 I 的增长而增加，并且在僵尸程序传播了 50 个时间步以后，Q 的增加速度加快。当 I 增大到最大值时，僵尸程序的传播减慢，僵尸网络的活跃程度降低，从网络中移除的主机数量就停止增长，保持 180000 台的数量。

S 为网络中存在的易感染主机。S 的数量随着感染主机的增加而减小，在 I 增长到最大值后的一小段时间，S 的数量减小到 0 台，意味着网络中所有主机在时间步为 90 的时候都被感染过一次或者已经从易感染网络中移除。

4.2 仿真比较

在相同的条件下，对无尺度网络下的僵尸网络传播模型进行仿真，如图 2 所示。

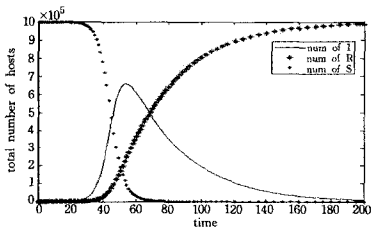

图 2　基于时区的僵尸网络传播模型

把图 2 与图 1 进行比较，图 2 只考虑了主机从感染到免疫的状态，而未考虑主机未被感染前就从网络中被移除的情况，所以感染主机的数量比图 1 中的更多，达到了近 650000 台。虽然感染开始的时间同样是时间步为 25 时，达到感染主机最大值的时间也同样是在时间步 60 左右，图 2 与图 1 中的僵尸程序生存周期也相似，但是因为考虑的情况不够全面，所以感染主机 I 的数量太大，网络中被感染主机数过多，这并不符合真实环境中僵尸程序的传播情况。

同样对双因素蠕虫的传播模型进行仿真，结果如图 3 所示。

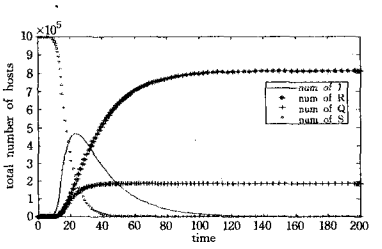

图 3　双因素蠕虫的传播模型

把图 3 与图 1 进行比较可以看出，双因素蠕虫传播模型的感染主机数增长得更快。在时间步为 10 的时候就开始了增长，而图 1 中的 I 是在时间步为 30 左右才开始增长，说明蠕虫传播不受控，是自动传播，所以恶意程序传播的效率更高，在很短的时间内就达到了感染主机的最大值。但是由于传播快，因此相应的感染主机被免疫和被移除的速度更快，因此图 3 中的最大感染主机数为 480000 台。而 I 在 100 分钟时就趋近于 0，传播结束，因此图 3 中的蠕虫传播的生命周期比图 1 的僵尸程序更短。

图 3 中的蠕虫并没有考虑网络中主机上下线的状态，因此感染主机数 S 在时间步为 40 的时候降为 0，即在这个时刻网络中所有主机已经被感染过一次，较图 1 中的被感染速度更快。由于蠕虫的快速传播，而 Q 的数量由于主机的在线情况不同，图 3 中的 Q 比图 1 中的被移除数更多，因此其并不符合僵尸程序受控的特点。

再对无尺度网络下的僵尸网络传播模型进行仿真[16]，如图 4 所示。

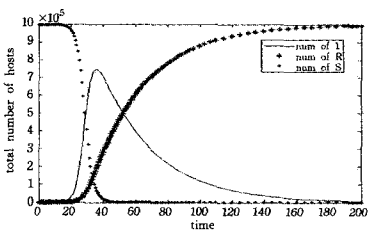

图 4　无尺度网络下的僵尸网络传播模型

把图 4 与图 1 进行比较可以看出，由于无尺度网络的择优连接性，而图 4 并没有考虑免疫特征 Q 的情况，因此图 4 所示的这种僵尸网络传播速度更快。在时间步为 20 时就开始有大量主机被感染，比图 1 中大规模传播的时间更早。在时间步接近 40 的时候被感染主机数达到最大值，为 730000 台，由于免疫情况考虑不足，因此感染的最大主机数比图 1 更多。这种僵尸程序的生存周期较短，并不符合真实网络中僵尸网络的传播。

在相同条件下对具有免疫特征的僵尸网络传播模型进行仿真，结果如图 5 所示。

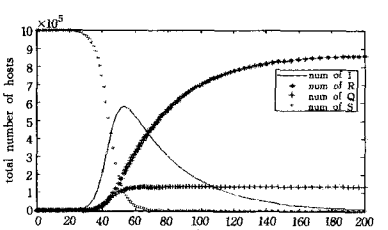

图 5　具有免疫特征的僵尸网络传播模型

（下转第 114 页）

Workflow Language [J]. Inf. Syst., 2005, 30(4): 245-275

[15] van der Aalst W M P, Aldred L, Dumas M, et al. Design and Implementation of the YAWL System [C] // Proc of 16th International Conference Advanced Information Systems Engineering. 2004: 142-159

[16] Xie J G, Tan Q P, Cao G R. Modeling and Analyzing Web Service Behavior with Regular Flow Nets [C] // Proc of International Conference on Web Information Systems and Mining and International Conference on Artificial Intelligence and Computational Intelligence. 2009: 309-319

[17] Wynn M T, Edmond D, van der Aalst W M P. Achieving A General, Formal and Decidable Approach to the OR-join in Workflow using Reset Nets [C] // Proc of 26th International Conference Applications and Theory of Petri Nets. 2005: 423-443

[18] 曹国荣，谭庆平，吴浩，等. 规范流网中 OR-join 任务的语义及使能判定算法[J]. 计算机科学与探索，2010，4(6)：542-551

(上接第 81 页)

分析图 5，并与图 1 进行比较可以看出，被感染主机 I 的数量在时间步为 30 的时候开始迅速增加，并在接近时间步为 60 的时候达到最大值，为 580000 台，感染的情况与图 1 有相似之处。但是该种僵尸程序开始大规模传播的时间比图 1 更早，因为这种僵尸网络在传播时没有根据节点度的多少来进行感染，是比较理想的一种情况，对僵尸网络在无尺度网络下的传播没有很好的描述。

最后对具有网络阻塞特征的僵尸网络传播模型进行仿真，如图 6 所示。

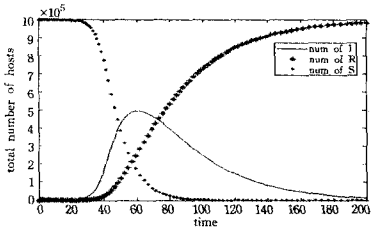

图 6　具有网络阻塞特征的僵尸网络传播模型

把图 6 与图 1 进行比较，由于网络阻塞的情况相似，僵尸程序在时间步接近 50 的时候达到传播的最大数量，并且感染的最大数量为 500000 台，与图 1 相同。但是由于没有考虑主机提前免疫的情况，所有 R 的值比图 1 更大。而且加上没有考虑无尺度网络的集散节点存在，所以在感染主机达到最大值以后，感染主机下降的速度明显没有图 1 快，这是因为图 1 中随着集散节点从感染被恢复到正常状态，I 的下降速度会随着时间步的增加下降得更快。所以图 6 也不能很好地反应出真实网络的僵尸程序传播情况。

综上所述，要对当今网络中的僵尸网络进行确切的描述与分析，就需要考虑无尺度网络的特点以及僵尸程序传播过程中的免疫特征与网络阻塞特征，因此图 1 的传播模型更加符合真实的僵尸网络传播。

结束语　随着科技的发展，僵尸网络作为一个可控的高效攻击平台，得到黑客们的广泛认同和利用[17]，攻击者通过各种手段来增强僵尸网络的隐蔽性和鲁棒性，在传播方面也融合了传统恶意代码的传播方式，这就增加了网络安全人员对其发现、监测以及预防的难度。鉴于当今网络的无尺度性，考虑僵尸网络在无尺度网络下的传播其有重要意义。由于僵尸程序的传播继承自蠕虫病毒，因此了解无尺度网络下的僵尸网络就需要从蠕虫的传播模型着手。传统的蠕虫模型并不能很好地反应出僵尸网络的特征。本文提出的传播模型，结合了无尺度网络的增长性和择优连接性，并考虑了部分主机未被感染前就通过免疫措施将其从脆弱状态转为免疫状态的情况，以及网络流量阻塞的因素。这种模型比传统的僵尸网络传播模型更符合真实网络。

参 考 文 献

[1] Barabasi A L, Albert R. Emergence of Scaling in Random Networks[J]. Science Magazine, 1999, 286(5439): 509-512

[2] Watts D J, Strogatzx S H. Collective Dynamics of "Small-World" Networks[J]. Nature, 1998, 393(6684): 440-442

[3] Liu Li-juan. Research on Dyamic Etworking of Scale-Free Network[R]. TP393. Harbin Institute of Technology, 2007

[4] 洪征，吴礼发，王元元. 三种构建无尺度蠕虫网络的蠕虫传播模型[J]. 吉林大学学报，2008，38(3)：690-694

[5] 张伟. 僵尸网络综述[J]. 软件导刊，2008，7(9)：188-189

[6] http://www.isc.org.cn/20020417/ca290326.htm

[7] Symantec Inc. Symantec Internet security threat report: Trends for July 06～December06. VolumeXI. 2007[OL]. http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf

[8] Streftaris G, Gibson G J. Statistical Inference for Stochastic Epidemic Models[C] // Proc. of the 17th IWSM. Chania: [s. n.], 2002: 609-616

[9] Frauenthal J C. Mathematical Modeling in Epidemiology[M]. New York: Springer-Verlag, 1980

[10] Zou C C, Gong W, Towsley D. Worm propagation modeling and analysis under dynamic quarantine defense[C] // Proceedings of the ACM CCS Workshop on Rapid Malcode. 2003: 51-6

[11] Dagon D, Zou C C, Lee W. Modeling botnet propagation using time zones[C] // Proc. of the 13th Annual Network and Distributed System Security Symp(NDSS 2006). 2006

[12] 刘浩广，蔡绍洪，张玉强. 无标度网络模型研究进展[J]. 大学物理，2008，27(4)：43-47

[13] 李涛，关治洪，吴正平. 病毒在无标度网络上的传播及控制仿真研究[J]. 计算机应用研究，2007，24(12)：177-182

[14] Wang L, Zhao X, Pei D, et al. Observation andAnalysis of BGP Behavior under Stress[C] // Internet Measurement Workshop. France, November 2002

[15] Kim J, Radhakrishnan S, Dhall S K. Measurement and analysis of worm propagation on Internet network topology[C] // Proc. of the IEEE Int'l Conf. on Computer Communications and Networks(ICCCN2004). 2004: 495-500

[16] 黄彪，谭良，欧阳晨星，等. 无尺度网络下具有免疫特征的僵尸网络传播模型[J]. 计算机应用研究，2012，29(3)：1028-1031

[17] 黄彪，谭良. 无尺度半分布式 P2P 僵尸网络的构建[J]. 计算机工程，2012，38(11)：130-132