第 13 卷 第 4 期
2012 年 8 月
解放军理工大学学报(自然科学版)
Journal of PLA University of Science and Technology (Natural Science Edition)
Vol. 13 No. 4
Aug. 2012

基于 OPNET 的 BotNet 最优步长传播仿真

杨　云[1]，胡谷雨[1]，李华波[1]，罗　隽[2]
(1.解放军理工大学 指挥自动化学院,江苏 南京 210007;2.海军指挥学院,江苏 南京 211800)

摘　要:僵尸网络(BotNet)主要采用蠕虫扫描的方式进行传播,传统的蠕虫传播策略主要在扩散效率和扫描准确性上进行折衷,共性缺点是存在对同一主机重复扫描和网络之间交叉扫描的严重问题,会对互联网产生严重的流量冲击,降低BotNet的隐蔽性。为解决这一共性问题,根据互联网的无尺度特性,在对比传统网络蠕虫传播策略优缺点的基础上,结合前向神经网络现有的BP学习算法对BotNet传播进行了分析,从理论上提出一种计算BP近似最优步长的算法,并通过OPNET建立传播攻击模型进行了仿真验证。结果表明,该算法有效地提高了BotNet在无尺度网络中的传播性能。

关键词:僵尸网络;神经网络;BP算法;OPNET
中图分类号:TP393.4　　文献标识码:A　　文章编号:1009-3443(2012)04-0383-05

Simulation of optimal step size propagation of BotNet based on OPNET

YANG Yun[1], *HU Gu-yu*[1], *LI Hua-bo*[1], *LUO Jun*[2]
(1. Institute of Command Automation, PLA Univ. of Sci. & Tech., Nanjing 210007, China;
2. Naval Command College, Nanjing 211800, China)

Abstract: BotNet mainly uses worm scan strategies to propagate. Traditional strategies always make compromise design between diffusion efficiency and scan accuracy, and their general defects focus on the repeat scanning process, which imports serious Internet traffic problem and decreases the invisibility of BotNet. To solve the problem, a comparative analysis of the advantages and disadvantages of the traditional propagation strategies was made, the existing BP feedforward neural network learning algorithm was used to analyze the spreading of BotNet, and an algorithm proposed to calculate the approximate optimal step size of BP. An OPNET simulation shows that the algorithm can effectively improve the performance of the spreading of BotNet in scale-free network.

Key words: BotNet; neural network; BP algorithm; OPNET

BotNet,俗称僵尸网络,是从传统计算机病毒、蠕虫、木马和后门工具的基础上进化,并通过相互融合发展而成的一种新型恶意代码形态[1],是攻击者出于恶意目的传播僵尸程序控制大量主机而组成的网络,以其一对多的命令与控制机制为主要特征[2],是当前互联网最为严重的安全威胁之一。

BotNet不同于病毒、网络钓鱼等特定的安全事件,也不是个体病毒的感染发作,而是一个或多个攻击性网络的建立,以及在特定时间内对特定对象的群体式攻击。BotNet的建立依赖于Bot程序的传播,若不考虑攻击节点向控制中心的注册及双方的交互过程,可将Bot程序的传播过程看作BotNet的组网过程[3]。研究BotNet如何隐蔽传播的算法和策略问题,将有利于更好地检测和应对其带来的安全威胁。

本文在对比传统蠕虫传播方法的基础上,根据互联网的无尺度特性,将前向神经网络中基于BP学习算法的最优步长传播策略引入到BotNet传播

收稿日期:2011-11-04.
基金项目:国家自然科学基金资助项目(60603029).
作者简介:杨　云(1981－),男,博士生,工程师;研究方向:军事通信网;E-mail:mafia.cnnet@gmail.com.

过程中,在提高 Bot 程序传播效率的同时,降低了传播过程对骨干网络造成的影响,提高了 BotNet 传播的隐蔽性。

1 BotNet 的传播策略

目前,BotNet 主要采用蠕虫技术进行传播扩散,但它区别于传统蠕虫的典型特征在于其传播具有可控性[4],这主要是因为攻击者往往更关注 BotNet 的隐蔽扩散和长期控守特性,不盲目追求最快速度传播。相比之下,传统的蠕虫传播策略只关注如何在被发现和查杀之前传播到更大的范围,并不关注对被感染主机的后续控制问题。

在感染一台主机过程中,Bot 程序的蠕虫传播模块产生的流量直接影响到 Bot 程序自身的隐蔽性,而对网络产生的流量冲击主要取决于发起扫描的 Bot 主机到目标主机的路径,因此可以把流量影响的问题转化为蠕虫选择目标主机策略的问题。

在经典的蠕虫传播策略中,均匀随机扩散策略采用随机扫描 IP 的方式传播,会产生大量的异常流量。本地优先扩散策略为同一子网赋予较大的传播概率,在提高攻击命中率的同时局限了传播范围。基于目标列表和基于路由信息的扩散策略利用了预先生成的 IP 地址列表,但在提高传播准确性的同时增大了每个蠕虫程序的负载量,而在此基础上改进的分治扩散[4,5]策略虽然巧妙降低了蠕虫负载,但仍然存在严重的"坏点[6]"问题。

这些传播策略有一个共性,就是在任意时刻,任意一个蠕虫都有可能对同一台主机进行探测,只不过是存在概率大小的问题,因而导致了 2 个严重问题。一是多台主机会对同一台主机进行重复扫描;二是不同网络之间存在相互扫描的冗余流量问题。

这 2 个问题都会对互联网产生不必要的流量冲击,从而降低整个 BotNet 的隐蔽性。针对第一个问题,采用有序化传播策略和分级化[7]传播策略,利用 Internet IP 地址的按块、连续分配特点,按广度优先的方式进行传播,可有效避免 Bot 的扫描空间重复的问题;针对第二个问题,一般手动划分扫描区域,然后采用最优步长算法进行传播。传统的最优步长算法中,基于先验知识的随机判断方法传播速度快,但准确度和效率低下。同时在实际网络中,由于区域划分的无序性,很多时候最优步长也只是近似值,如果为了精度不断计算将耗时费力。因此,本文提出了基于 BP 的最优步长式传播,使得 Bot 程序在传播过程中不仅避免了扫描空间的重复,而且提高了扫描效率。

2 基于 BP 的最优步长算法改进

实证研究发现,大量的实际网络可以被认为是无尺度网络。最著名的无尺度网络模型是 1999 年 Barabási 和 Albert 建立的 Barabási-Albert 无尺度网络模型[8,9](BA 模型或 BA 网络)。

在无尺度网络里,所有病毒都可在网络中传播和长期存在,即便是那些传染力很低的病毒也是如此。由于集散节点会连接到很多其他节点、所以任何一个遭受病毒入侵的节点,都将连带感染至少一个集散节点。而一旦有集散节点被感染,它就会把病毒传播给众多的其他节点,其中也包括其他的集散节点,这就导致了病毒在整个网络里的传播。

1986 年,Rumelhart 提出了反向传播 BP(back-propagation)学习算法,该算法的学习过程由正向和反向传播 2 部分构成。在正向传播中,每一个节点的状态只影响到下一层网络。如果输出层输出的结果与目标值间有误差,则转入反向传播过程,将误差信号沿原来的连接通路返回,通过修改各父节点的权值,逐次地向输入层传播去进行计算,再经过正向传播过程。这 2 个过程的反复运用,使得误差信号最小。

虽然 BP 算法通过动态调整正向和反向传播过程中各层节点权值参数,能够适用于多层网络,但它只是一种最速下降寻优算法,收敛速度很慢,且当学习速率较大时数值稳定性很差。为此,许多学者提出不少改进的 BP 算法。有的是在广义 Delta 规则中加入动量项以加快收敛速度,但动量系数的取值是根据经验获得的,并无规律可循,这就使得学习算法的稳定性无法得到保证。

为了确保在无尺度网络中 Bot 程序的传播具备良好的可控性和智能化特性,可以将 BP 网络中的近似最优步长学习算法[10]应用到 Bot 程序的设计中,使 Bot 程序在实施传播时,能够根据上层网络输入的传播目标列表信息和输出反馈进行动态学习调整,从而有效避免不同网络之间存在的扫描冗余流量问题。

假设 BotNet 所在环境为 m 层网络,设各个节点的输入和输出关系函数为 f,由 $k-1$ 层的第 j 个节点到 k 层的第 i 个节点的结合权值为 W_{ij},并设第 k 层 i 单元输入的总和为 u_i^k,输出为 v_i^k,则各变量之间的关系为:

$$v_i^k = f(u_i^k); u_i^k = \sum_j W_{ij} v_j^{k-1}。$$

BP 算法的本质就是通过调整 W_{ij} 来求取误差信号函数，可得

$$R = \frac{1}{2}\sum_j (v_j^k - \lambda_j)^2,$$

λ_j 是输出单元的期望输出，利用非线性中的最快下降法，使权值沿着误差函数的负梯度方向改变，其权值 W_{ij} 的增量

$$\Delta W_{ij} = -\varepsilon \frac{\partial \lambda}{\partial w_{ij}},$$

ε 为 Bot 程序下一步传播的步长，是本文中的研究重点。首先从原式出发：

$$\Delta W_{ij} = W_{ij}^{k+1} - W_{ij}^k = -\varepsilon \frac{\partial \lambda}{\partial w_{ij}}。$$

因为网络的无尺度性，计算精确步长时间较长，且性能提高不一定明显，因此本文尝试对其求近似的最优步长：由于 $\Delta W_{ij} = W_{ij}^{n+1} - W_{ij}^n$，得到

$$W_{ij}^{n+1} = W_{ij}^n - \varepsilon \frac{\partial \lambda}{\partial w_{ij}}。$$

为求得近似最优步长，需在 W_{ij}^n 处对 $\lambda(W_{ij}^n - \varepsilon \frac{\partial \lambda}{\partial w_{ij}})$ 进行泰勒展开，得到

$$\lambda(W_{ij}^n - \varepsilon \frac{\partial \lambda}{\partial w_{ij}}) \approx \lambda(W_{ij}^n) - \varepsilon \frac{\partial \lambda}{\partial w_{ij}} + \varepsilon \frac{\partial \lambda}{2\partial w_{ij}} H(W_{ij}^k),$$

其中，$H(W_{ij}^k)$ 为 W_{ij} 的 Hesse 矩阵[10]。对上式两端对 ε 导数并令其等于零，则可得到近似最佳步长：

$$\varepsilon_k = \frac{\frac{\partial \lambda}{\partial w_{ij}}}{H(W_{ij}^k)}。$$

由于网络的无尺度性和不确定性，近似最优步长的求解速度更快，因此更加适合 Bot 程序快速传播，其性能本文将通过 OPNET 仿真进行研究。

3　基于 OPNET 的 BotNet 传播模型仿真

3.1　无尺度网络模型设计

由于本文研究的的 BotNet 是在无尺度网络条件下传播的，Bot 程序传播的过程实际上是智能蠕虫模块对目标网络的自动攻击过程。因此，在 OPNET 所提供的标准模块基础上，增加多协议模块，构造一个多级互通，内部级联的广域网模型，可在各种基于 TCP/IP 协议的仿真网络环境中运行。如图 1 所示。在该网络模型中，存在一个服务器簇和 3 个客户网络。为实现最优步长选择，网络内部遵循 OSPF 协议。

包含的网络设备及其具体功能如下：

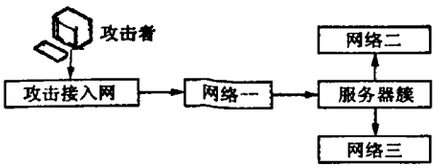

图 1　BotNet 的无尺度网络传播模型

Fig. 1　Propagation model of scale-free BotNet

(1) 服务器簇：该簇中使用 OPNET 提供的标准服务器模型，并对其应用层对应模块进行了替换。除了提供 HTTP、FTP、Database 3 种标准服务外，还可在仿真中根据需要打开新的端口。

(2) 网络一、二、三：模拟真实的互联网结构，使用思科路由器将来自广域网的 IP 数据包进行转发。

(3) 攻击接入网：模拟一般攻击者所在的网络环境，用户可以进行的活动包括 WEB 浏览和 FTP 文件传输。

(4) 攻击者(attack_source)：使用 OPNET 标准客户端的基础上对其 IP 封装模块进行了替换。在仿真时该节点以不同的速率对服务器簇进行 Bot 攻击。

3.2　Bot 传播流程

以简单传播自身的的 Bot 程序为例，进程结构如图 2 所示。

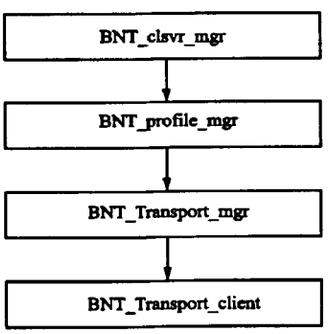

图 2　Bot 传播进程结构

Fig. 2　Process structure of Bot propagation

作为网络管理进程，BNT_clsvr_mgr 主要负责攻击属性的解析以及服务器对各种服务请求的应答。BNT_profile_mgr 为 profile 管理进程，确定在什么时刻开始进行攻击和通知攻击管理子进程攻击的目标、下一跳的步长以及攻击的速率。进程 BNT_Transport_mgr 是进程 BNT_profile_mgr 的子进程，主要负责控制攻击的持续时间和攻击的速率。进程 BNT_Transport_client 负责具体执行攻击行为，TCP 连接请求数据包都是由该进程发出的。

(1) 网络管理进程 BNT_clsvr_mgr。其功能是攻击属性的解析和服务器监听端口的打开。攻击属性的解析主要涉及到相关数据类型的定义以及解析函数的设计,而服务器端口的打开则不需要对网络管理进程进行修改。由于在 BNT_clsvr_mgr 中已经包含了作为服务器端的所有功能,内部数据包括以下几个枚举类型:

BNTT_Application_type:指定不同应用类型的标识;BNTT_AppType:指定不同的应用类型,如 Http 和 Transport 等;BNTT_Application_Name:指定不同的应用名称,例如 Database_Query 和 Email Remote_Login 等,都是 BotNet 的传播方式;BNTT_AppPort:指定服务器端针对不同服务所打开的端口号。

(2) profile 管理进程 BNT_profile_mgr。通过图 3 可以发现,该进程一直处于"wait"也即阻塞状态中,可以通过不同的条件进行激活。

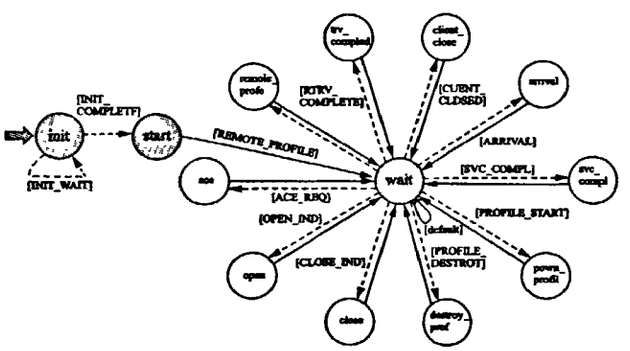

图 3 进程 BNT_profile_mgr 状态

Fig. 3 State diagram of process BNT_profile_mgr

由于需要测试改进后最优步长的性能,对图中的各种状态进行相应的修改,如"arrival"状态代表收到远端发来的各种业务包,包括握手信息、管理命令等,"spawnprofile"状态则负责为业务规格中所包含的每一项应用创建并激活相应的应用管理进程,而"close"状态负责控制业务规格的间隔和持续时间。

近似最优步长确定主要依靠"svc_compl"状态,由于 BP 算法的学习过程包括网络中工作信号的正向传播和误差信号的反向传播 2 部分,需要该获取数据包"arrival"时的网络状态,同时读取"spawnprofile"中设定好的业务信息,因此需要在"spawnprofile"状态中加入相应的代码。

其中,application_mgr_prohandle_ptr = (Prohandle *) prg_cmo_alloc (cmo_handle, sizeof (Prohandle) * int_traffic_growth_factor); int_traffic_growth_factor 是仿真属性,表示下一个传播目标的增长因子,即公式中的 ε_r。

(3) 传播管理进程 BNT_Transport_mgr。其状态转移图如图 4 所示,根据各种与攻击相关的参数对具体的攻击行为进行管理。

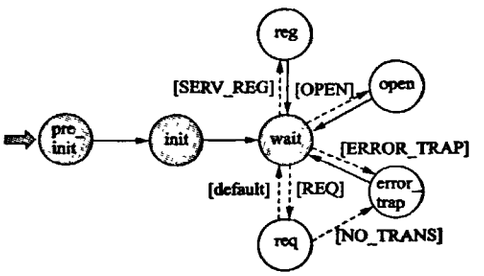

图 4 进程 BNT_Transport_mgr 状态

Fig. 4 State diagram of process BNT_Transport_mgr

图中:"wait"的作用是转移条件的判断;"init"的作用是初始化变量,可以看到攻击管理进程共包含了 4 个主要状态(reg、open、error_trap、req);状态"reg"是常规网络连接中的握手过程;状态"error_trap"是错误处理机制;状态"req"的作用是当攻击的持续时间到达时结束攻击并销毁攻击管理进程;状态"open"的作用是在攻击开始后根据攻击的速率激活执行攻击行为的子进程 BNT_Transport_client 以完成攻击。

(4) 攻击执行进程 BNT_Transport_client。用于发起攻击连接和传播 Bot 程序,该进程只包含 2 个状态——"Server_config"状态和"register"状态。与传统特洛伊木马类似,Bot 的传播在确定了服务器地址之后,便向其发送注册包,完成该目标传播与控制,收到注册包记为攻击成功一次。

"Server_config"状态。通过 Opnet 核心函数 op_pro_para_access()获取由攻击管理进程传来的变量内存地址,该地址是指向服务器或者某域名的结构指针,在结构体 BNTT_client_Transport_Params_Info 包含了与具体攻击行为相关的各种属性,如服务器地址,端口等等。

"register"状态。将上述变量代入函数 app_session_open(),向服务器模块发出进行 TCP 连接的请求,成功后销毁本进程。

3.3 仿真结果分析

在传播过程仿真中,仿真条件设置如下:

① 为防止攻击速率过高造成服务器假死问题,

设置服务器允许的最大半连接总数为 400。

② 考虑到攻击过程中服务器业务进程的响应时延问题，设置服务器最大半连接超时阈值为 200 s。

输出的仿真结果包括攻击成功的概率、服务器故障时间以及攻击速率等，由于攻击成功概率 p 可以直观地表现传播的效果，所以本文选择其作为仿真结果输出，其公式为：

$p \approx$传播成功的次数 / 连接请求总数量。

当然，网络中不包含攻击行为时，少数合法用户也有可能会有失败连接，因此这里使用约等号。分别在服务器的半连接超时时间、服务器允许的最大半连接数(所有端口的半连接数)、攻击者的服务请求速率以及用户请求速率不同的情况下对模型输出的仿真结果 p 进行了统计分析。

仿真运行 40 次，每 8 次为一组，同组中攻击速率固定，对于采用普通传播方式和基于最优步长计算的方法，分别输出仿真结果如图 5 所示。

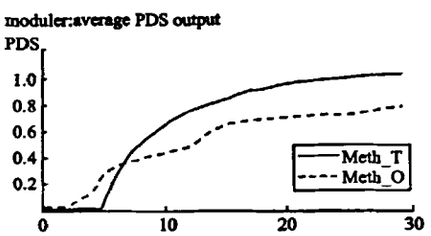

图 5　不同传播方式攻击速率对比

Fig. 5　Attack rate of different propagation method

从图 5 中可以看出，在每秒 8 个连接请求之前，根据传统方式进行攻击的成功概率要高于根据近似最优步长算法，但二者的成功概率都很小(低于 0.4)；在增加到每秒 20 个请求时，采用近似最优步长算法的攻击成功概率比原算法有明显的增加(接近 20%)。可知在服务器设置相同的条件下，采用最优步长的传播速度更快。

4　结　语

本文在对比传统网络蠕虫传播行为基础上，将 BP 神经网络中的近似最优步长传播策略引入到 BotNet 传播过程中，提高了 Bot 传播的效率，和传统的网络蠕虫扩散策略相比，该策略使 BotNet 在提高了传播速度的同时，降低了在传播过程中对网络造成的影响，极大地提高了 BotNet 传播的隐蔽性。

参考文献：

[1] RAJAB M A, ZARFOSS J, MONROSE F, et al. A multifaceted approach to understanding the Botnet phenomenon[C]. Proc of 6th ACM Internet Measurement Conf (IMC 2006). Rio de Janeiro: ACM Press, 2006.

[2] 诸葛建伟，韩心慧，周勇林，等. 僵尸网络研究[J]. 软件学报，2008,19(3):702-715.
ZHUGE Jian-wei, HAN Xin-hui, ZHOU Yong-lin. Research and development of botnets[J]. Journal of Software, 2008,19(3):702-715. (in Chinese).

[3] 吴　玲. 蠕虫型僵尸工具的传播模型及检测技术研究[D]. 成都：成都电子科技大学，2008.

[4] KEPHART J O, WHITE S R. Measuring and modeling computer virus prevalence [C]. Oakland: Proc of the IEEE Symp on Security and Privacy, 1993.

[5] WU Jiang, VANGALA S, GAO Li-xin, et al. An effective architecture and algorithm for detecting worms with various scan techniques[C]. Califormia: Standford University Press, 2004.

[6] 文伟平. 网络蠕虫研究与进展[J]. 软件学报，2004,15(8):1208-1219.
WEN Wei-ping. Research and development of internet worms[J]. Journal of Software, 2004,15(8):1208-1219. (in Chinese).

[7] 张　焱，汪永益，余　跃. 一种基于蠕虫的大规模 BotNet 传播策略[J]. 网络安全技术与应用，2008(12):58-60.
ZHANG Yan, WANG Yong-yi, YU Yue. A large-scale botNet propagation policy based on worm[J]. Network Security Technology & Application, 2008(12):58-60. (in Chinese).

[8] BARABÁSI A L, ALBERT R. Emergence of scaling in random networks[J]. Science, 1999, 286:509-512.

[9] BARABÁSI A, ALBERT R, JEONG H. Mean-field theory for scale-free random networks[J]. Physica A, 1999, 272:173-187.

[10] 侯宝臣，邓飞其. B-P 神经网络近似最优步长的研究[J]. 组合机床与自动化加工技术，2010(4):47-48.
HOU Bao-chen, DENG Fei-qi. The study of approximate optimal step size of B-P neural network[J]. Modular Machine Tool & Automatic Manufacturing Technique, 2010(4):47-48. (in Chinese).

(责任编辑：徐金龙)