计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(1):25−31 [doi: 10.15888/j.cnki.csa.006758]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于攻防博弈和随机 Petri 网的 DDoS 攻防对抗评估①

李程瑜[1], 齐玉东[1], 王晓虹[2], 司维超[1]

[1](海军航空大学, 烟台 264001)
[2](解放军第 107 医院, 烟台 264001)
通讯作者: 李程瑜, E-mail: yuasd152@163.com

摘　要: 为了对 DDoS 攻防行为进行有效评估以防御 DDoS 攻击, 本文首先对 DDoS 攻防评估研究现状进行了分析, 然后基于随机 Petri 网建立了 DDoS 攻防行为对抗网, 提出了以攻防稳态概率作为攻防行为评估的依据, 紧接着基于攻防博弈提出了攻防博弈策略求解方法, 最后对本文所建立的 DDoS 攻防行为对抗网进行稳态分析并综合考虑攻防行为收益和攻防行为强度两方面因素进行了仿真评估, 评估结果表明本文方法更具合理性和针对性.

关键词: 攻防博弈; 随机 Petri 网; 稳态概率; DDoS 攻防对抗; 评估

引用格式: 李程瑜,齐玉东,王晓虹,司维超.基于攻防博弈和随机 Petri 网的 DDoS 攻防对抗评估.计算机系统应用,2019,28(1):25–31. http://www.c-s-a.org.cn/1003-3254/6758.html

DDoS Attack and Defense Confrontation Evaluation Based on Attack and Defense Game and Stochastic Petri Net

LI Cheng-Yu[1], QI Yu-Dong[1], WANG Xiao-Hong[2], SI Wei-Chao[1]

[1](Naval Aeronautical University, Yantai 264001, China)
[2](107th Hospital of the People's Liberation Army, Yantai 264001, China)

Abstract: In order to effectively evaluate DDoS attack and defense behavior to defend against DDoS attacks, this study first analyzed the current research status of DDoS attack and defense evaluation, and then established DDoS attack and defense behavior confrontation net based on stochastic Petri net. The attack and defense steady state probability is used as the basis for the evaluation of attack and defense behavior. The solution of attack and defense game strategy based on the attack and defense game theory were proposed. In the end, we carried out the stability analysis of the DDoS attack and defense behavior confrontation net, and comprehensively considered the factors of attack and defense behavior gain and attack and defense behavior intensity to simulate and evaluate. The evaluation results show that the method is more reasonable and pertinent.

Key words: attack and defense game theory; stochastic Petri net; steady state probability; DDoS attack and defense confrontation; evaluation

1　引言

分布式拒绝服务攻击[1](Distributed Denial of Service, DDoS) 是一种分布式、协作式、大规模的 DoS 攻击方式, 大多利用 Internet 上已被攻陷的计算机作为“僵尸”, 向某一特定的目标发起密集式的“拒绝服务”请求, 达到将其网络资源和系统资源耗尽的目的, 使之无

① 基金项目: 山东省重点研发计划 (2016YJS02A01)
Foundation item: Key Research and Development Program of Shandong Province (2016YJS02A01)
收稿时间: 2018-07-25; 修改时间: 2018-08-21; 采用时间: 2018-09-07; csa 在线出版时间: 2018-12-07

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

法向真正正常请求的用户提供服务. Web 服务器、DNS 服务器多为最常见的攻击目标, 最终实现带有利益的恶意刷网站流量、Email 垃圾邮件群发、瘫痪竞争对手等违反道德的商业活动的目的. DDoS 攻击作为互联网时代网络安全领域使用频率最高、最易实施和影响范围最广的网络攻击行为, 使军队、国家政府机关、企事业单位面临严峻的网络信息安全威胁和挑战.

国内外众多科研机构和人员针对 DDoS 攻防评估做了大量研究, 并取得了一定的成果, 文献[2]提出一种应对 DDoS 攻击防范机制的评估分类标准, 指出在评估一种防御机制中应用的一些标准参数, 但缺乏具体实验比较. 文献[3]提出 DDoS 防御机制评估框架, 但该方法需要一个严格假设才能清楚区分攻击包和合法包, 在实际的网络攻防对抗中难以做到. 文献[4]提出了一种基于多属性决策的 DDoS 防御策略遴选算法, 综合考虑了各方面评估指标, 为防御策略的选取提供了参考并通过模拟实验验证了方法的有效性. 文献[5]提出一种基于战略博弈的 DDoS 攻防绩效评估方法, 构建了基于博弈论的攻防策略模型, 定义攻防效用函数, 通过求解混合策略纳什均衡得到攻防最优策略. 上述评估方法仅从攻防结果中指标值变化或攻防行为收益的角度对 DDoS 防御策略进行评估较为片面, 属于静态评估, 缺乏对攻防过程的考虑并且得出最优防御措施缺乏针对性. 目前缺少一个综合考虑攻防对抗过程及结果的 DDoS 攻防行为评估方法.

本文的主要思想是综合考虑攻防对抗过程及结果, 从攻防行为强度和攻防收益两方面进行 DDoS 攻防行为评估, 首先基于随机 Petri 网理论建立 DDoS 攻防对抗网络, 然后对 DDoS 攻防对抗网络中的攻防行为进行攻防博弈分析, 得出攻防双方的攻防策略, 攻防策略即攻防行为选择概率, 将其赋予 DDoS 攻防对抗网展开攻防对抗过程, 依据攻防对抗网稳态概率对攻防行为进行评估.

2 基于随机 Petri 网的 DDoS 攻防行为对抗网

本文基于随机 Petri 网针对 DDoS 攻防行为, 建立了攻防行为对抗网, 具体的有关随机 Petri 网的定义可参考文献[6].

2.1 相关定义

定义 1. 攻防收益

将攻击行为对系统造成的损害程度定义为攻击收益, 攻击行为 i 的收益表示为R_i^a; 将防御行为对受攻击系统的恢复程度定义为防御收益, 防御行为 j 的收益表示为R_j^d.

定义 2. 攻防策略

假设攻击方有 n 个攻击行为可供选择, 防御方有 m 个防御行为可供选择, 用π_i^a表示攻击方选择攻击行为 i 的概率, 用π_j^d表示防御方选择防御行为 j 的概率, 则定义攻击方选择攻击行为的策略为π^a, 定义防御方的选择防御行为策略为π^d:

$$\pi^a=(\pi_1{}^a,\pi_2{}^a,\cdots,\pi_n{}^a)\pi_1{}^a+\pi_2{}^a+\cdots+\pi_n{}^a=1$$
$$\pi^d=\left(\pi_1{}^d,\pi_2{}^d,\cdots,\pi_n{}^d\right)\pi_1{}^d+\pi_2{}^d+\cdots+\pi_n{}^d=1$$

定义 3. 攻防行为强度

将单位时间内攻防行为产生或清洗攻击流量的能力视为攻防行为的强度, 用λ表示.

定义 4. DDoS 攻防行为对抗网

用一个九元组来表示一个 DDoS 攻防行为对抗网, $ADSPN=(N,P,T,F,\pi,\lambda,R,U,S)$, 其中:

(1) N={Na, Nd}, Na 代表攻击方, Nd 代表防御方;

(2) $P=P1\cup P2\cup\cdots\cup Pn$为库所集合, 表示攻防双方可能所处的状态;

(3) T=$A\cup D$ 为攻防行为集合, A={a_1, a_2,…, a_n}表示攻击行为集合; D={d_1, d_2,…, d_m}表示防御行为集合;

(4) $F\in I\cup O$ 为弧的集合, 其中 $I\subseteq P\times T$, $O\subseteq T\times P$, 同时 $P\cap T=\varphi$且 $P\cup T\neq\varphi$, 其中表示空集合;

(5) π: $T\rightarrow$[0, 1], 表示瞬间变迁的选择概率即攻击行为或者防御行为的选择概率;

(6) λ={$\lambda1$, $\lambda2$,…, λn}, 表示攻防行为强度;

(7) R: $T\rightarrow${$R1$, $R2$,…, Rn}表示攻击或防御行为执行后带来的收益;

(8) S 为标识集合, 常用 $S0$ 表示 $ADSPN$ 的初始状态.

2.2 DDoS 攻防行为描述

选取典型的 DDoS 攻防对抗行为作为构建 DDoS 攻防对抗网的行为集合.

2.2.1 攻击行为

(1) TCP 连接洪水攻击

TCP 连接洪水攻击是在 TCP 连接创建阶段对服务器资源进行攻击的. 攻击者可以利用大量受控主机, 通过快速建立大量恶意的 TCP 连接占满被攻击服务

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

器的连接表, 使目标无法接受新的 TCP 连接请求, 从而达到拒绝服务攻击的目的.

(2) SYN 洪水攻击[7]

SYN 洪水攻击是最经典的一种拒绝服务攻击方式, 攻击者利用大受控主机发送大量的 TCP SYN 报文, 使服务器打开大量的半开连接, 占满服务器的连接表, 从而影响正常用户与服务器建立会话, 造成拒绝服务.

(3) Sockstress 攻击

Sockstress 攻击是一种慢速攻击 TCP 连接的方法. 在 TCP 传输数据时, 先将数据包临时存储在接收缓冲区中, 该缓冲区的大小是由 TCP 窗口表示的. 如果 TCP 窗口大小为 0, 则表示该缓冲区已被填满, 发送端停止发送数据, 直到接收端窗口发生更新. Sockstress 攻击就是利用该原理长时间维持 TCP 连接, 以达到拒绝服务攻击的目的.

2.2.2 防御行为

(1) 攻击的治理[8,9]

对 DDoS 攻击的治理就是对攻击源节点的治理, 发现并阻断 DDoS 攻击的源节点, 能够从源头停止正在进行的 DDoS 攻击.

(2) 攻击的缓解[10]

缓解 DDoS 攻击的主要方法是对网络流行清洗, 即设法将恶意的网络流量从全部流量中去除, 只将正常的网络流量交付给服务器.

2.3 DDoS 攻防行为对抗网

根据 2.2 节攻防行为描述, 我们首先构建攻击方攻击行为 Petri 网和防御方防御行为 Petri 网, 然后将攻击方和防御方的攻防行为 Petri 网进行组合, 构成 DDoS 攻防行为对抗网.

在图 1 中, 库所表示攻击方所处状态; 瞬间变迁表示攻击方对攻击行为的选择, 包含选择概率参数π; 连续变迁表示攻击行为的执行过程, 包含行为执行强度参数λ.

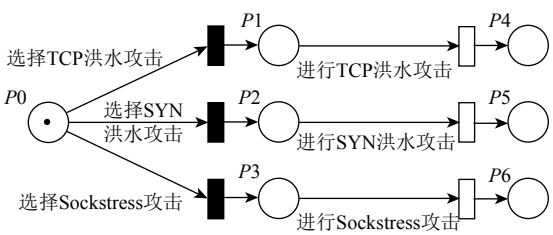

图 1 攻击行为 Petri 网

在图 2 中, 库所表示防御方所处状态; 瞬间变迁表示防御方对防御行为的选择, 包含选择概率参数π; 连续变迁表示防御行为的执行过程, 包含行为执行强度参数λ.

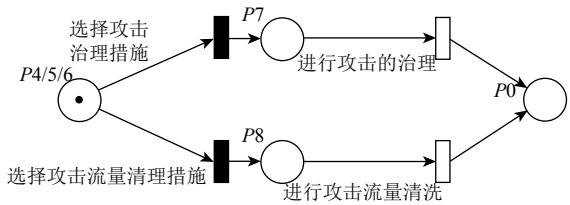

图 2 防御行为 Petri 网

攻击和防御是在网络攻防中是对立同一的整体, 二者相互依存. 在 DDoS 攻防对抗中, 攻击方首先进行攻击, 防御方检测到攻击后会采取防御行为抵御攻击, 然后攻击方会调整攻击策略再次攻击, 防御方也会调整策略进行防御, 这就形成一个循环的攻防对抗过程. 我们依据这个过程将攻击方和防御方的攻防行为 Petri 网进行组合, 构成 DDoS 攻防行为对抗网, 如图 3 所示.

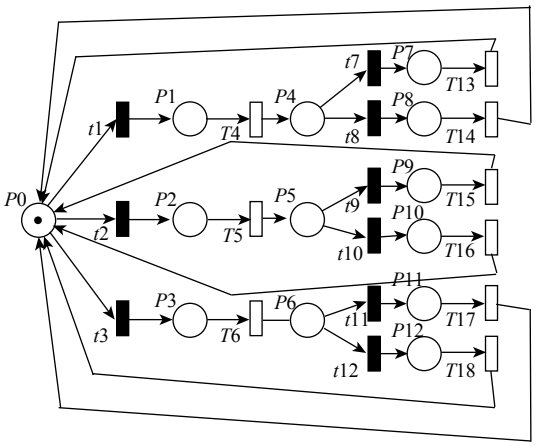

图 3 DDoS 攻防对抗网

DDoS 攻防对抗网中库所及变迁具体含义如表 1 和表 2 所示.

在 DDoS 攻防对抗网中, 我们以攻击方准备发动攻击作为初始状态, 攻击方发动攻击, 防御方对攻击行为展开防御使得攻击失效, 攻击方会再次发动攻击, 攻防对抗循环进行, 最终攻防对抗网会达到一个稳定状态, 即攻防双方会处于某个攻防状态的稳定概率, 我们依此来对攻防行为进行评估.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 1 DDoS 攻防对抗网库所含义

库所	含义
*P*0	攻击方准备发动攻击
*P*1	攻击方处于 TCP 洪水攻击状态
*P*2	攻击方处于 SYN 洪水攻击状态
*P*3	攻击方处于 Sockstress 攻击状态
*P*4	防御方准备对 TCP 洪水攻击进行防御
*P*5	防御方准备对 SYN 洪水攻击进行防御
*P*6	防御方准备对 Socktress 攻击进行防御
*P*7	防御方处于对 TCP 攻击源进行阻断状态
*P*8	防御方处于对 TCP 攻击流量进行清洗状态
*P*9	防御方处于对 SYN 攻击源进行阻断状态
*P*10	防御方处于对 SYN 攻击流量进行清洗状态
*P*11	防御方处于对 Sockstress 攻击源进行阻断状态
*P*12	防御方处于对 Sockstress 攻击流量进行清洗状态

表 2 DDoS 攻防对抗网变迁含义

变迁	含义
*t*1	攻击方选择 TCP 洪水攻击
*t*2	攻击方选择 SYN 洪水攻击
*t*3	攻击方选择 Sockstress 攻击
*t*7/*t*9/*t*11	防御方选择阻断攻击源
*t*8/*t*10/*t*12	防御方选择攻击流量清洗
*T*4	攻击方进行 TCP 洪水攻击
*T*5	攻击方进行 SYN 洪水攻击
*T*6	攻击方进行 Sockstress 攻击
*T*13	防御方对 TCP 洪水攻击源进行阻断
*T*14	防御方对 TCP 洪水攻击流量进行清洗
*T*15	防御方对 SYN 洪水攻击源进行阻断
*T*16	防御方对 SYN 洪水攻击流量进行清洗
*T*17	防御方对 Sockstress 攻击源进行阻断
*T*18	防御方对 Sockstress 攻击流量进行清洗

3 基于攻防博弈的 DDoS 攻防策略求解方法

对于 DDoS 攻防对抗网, 攻防博弈的双方为攻击方和防御方, 在攻防博弈过程中, 攻防双方作为理性的局中人均以最大化自身收益作为选择攻防行为的准则, 一方的收益是在另一方的损失下得到的, 因此我们用零和博弈来描述攻击方和防御方两个局中人的博弈关系, 将防御方看做是与攻击方收益相反的局中人.

定义 5. 攻防效用函数

用$U^a\left(a_i,d_j\right)$表示攻击方采取行为 a_i, 防御方采取行为 d_j 时攻击方的收益函数, $U^d\left(d_j,a_i\right)$表示攻击方采取行为 a_i, 防御方采取行为 d_j 时防御方的收益函数, 具体求解公式如下:

$$U^a(a_i,b_j)=R_i^a-R_j^b$$
$$U^d(b_j,a_i)=R_j^b-R_i^a$$

定义 6. 攻防策略纳什均衡

假设π^{a*}、π^{d*}分别为攻防双方最大化自身收益的攻防策略, 用$E\left(\pi^a,\pi^d\right)$表示为攻击方采用策略$\pi^a$、防御方采用策略$\pi^d$时双方博弈的收益期望, 计算公式为:

$$E\left(\pi^a,\pi^d\right)=\sum_{\forall a_i\in A}\sum_{\forall d_i\in D}{\pi_i}^a{\pi_j}^dU^a(a_i,d_i)$$

那么攻防策略纳什均衡应满足以下两个条件:

(1) $E\left(\pi^{a*},\pi^{b*}\right)\geqslant E\left(\pi^a,\pi^{b*}\right)$

(2) $E\left(\pi^{a*},\pi^{b*}\right)\geqslant E\left(\pi^{a*},\pi^b\right)$

当攻防博弈达到纳什均衡时, 双方所选择的策略都是应对对方的最优策略, 攻防双方所获得的收益都是最大的, 任何一方都不会主动降低自身收益去改变策略. 假设攻防博弈双方都是理性的局中人, 它们均要最大化自己的效用. 攻防双方零和博弈纳什均衡策略具体求解步骤如下:

(1) 输入攻防双方所有攻防行为收益:

$$R_1^a,R_2^a,\cdots,R_n^a$$

$$R_1^d,R_2^d,\cdots,R_m^d$$

(2) 根据攻防行为收益函数$U^a(a_i,b_j)$和$U^d(b_j,a_i)$求得攻防行为博弈矩阵 **B**:

$$\mathbf{B}=\begin{bmatrix}\left(U^a(a_1,b_1),U^d(b_1,a_1)\right) & \left(U^a(a_1,b_2),U^d(b_2,a_1)\right) & \cdots & \left(U^a(a_1,b_m),U^d(b_m,a_1)\right)\\ \left(U^a(a_2,b_1),U^d(b_1,a_2)\right) & \left(U^a(a_2,b_2),U^d(b_2,a_2)\right) & \cdots & \left(U^a(a_2,b_m),U^d(b_m,a_2)\right)\\ \vdots & \vdots & & \vdots\\ \left(U^a(a_n,b_1),U^d(b_1,a_n)\right) & \left(U^a(a_n,b_2),U^d(b_2,a_n)\right) & \cdots & \left(U^a(a_n,b_m),U^d(b_m,a_n)\right)\end{bmatrix}$$

(3) 将得到的攻防行为博弈矩阵输入 Gambit 软件中, 利用 Gambit 软件中 Qre 工具计算攻防策略纳什均衡.

(4) 输出 DDoS 攻防对抗行为攻防策略纳什均衡(π^{a*},π^{b*}).

上述步骤求得的攻防策略将会给 DDoS 攻防对抗网中瞬时变迁选择概率的设置提供依据.

4 稳态分析与仿真评估

4.1 稳态分析

文献[11]已经证明, 一个随机 Petri 网同构于一个

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

连续时间马尔科夫链, 所以本文所建立的 DDoS 攻防对抗网也同构于一个连续时间马尔可夫链 (MC), 将 DDoS 攻防对抗网在随机 Petri 网仿真软件 PIPE 上进行仿真, 得到与之同构的马尔可夫链如图 4 所示.

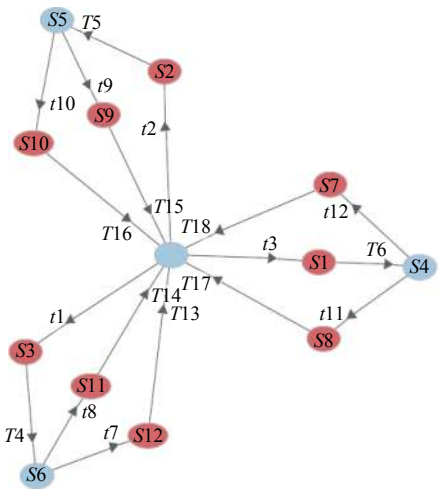

图 4 同构的马尔可夫链

在图 4 中, *S*0、*S*4、*S*5、*S*6 为消失状态, 因为它们所关联的库所触发瞬间变迁, 不存在稳态概率; *S*1、*S*2、*S*3、*S*7 、*S*8、*S*9、*S*10 、*S*11、*S*12 为有形状态, 存在稳态概率. 其中, *S*3 表示攻击方处于 TCP 连接洪水攻击状态、*S*2 表示攻击方处于 SYN 洪水攻击状态、*S*1 表示攻击方处于 Sockstress 攻击状态; *S*12 表示防御方处于对 TCP 连接洪水攻击源进行阻断状态、*S*11 表示防御方处于对 TCP 连接洪水攻击流量清洗状态、*S*9 表示防御方处于备对 SYN 洪水攻击源进行阻断状态、*S*10 表示防御方处于对 SYN 洪水攻击流量清洗状态、*S*8 表示防御方处于对 Sockstress 攻击源进行阻断状态、*S*7 表示防御方处于对 Sockstress 攻击流量清洗状态. 根据同构马尔可夫链中有形状态之间的转换关系, 我们可以得到稳定状态的可达标识集, 如表 3 所示.

表 3 可达标识集

	*P*0	*P*1	*P*2	*P*3	*P*4	*P*5	*P*6	*P*7	*P*8	*P*9	*P*10	*P*11
*S*1	0	0	0	1	0	0	0	0	0	0	0	0
*S*2	0	0	1	0	0	0	0	0	0	0	0	0
*S*3	0	1	0	0	0	0	0	0	0	0	0	0
*S*7	0	0	0	0	0	0	0	0	0	0	0	0
*S*8	0	0	0	0	0	0	0	0	0	0	0	1
*S*9	0	0	0	0	0	0	0	0	0	1	0	0
*S*10	0	0	0	0	0	0	0	0	0	0	1	0
*S*11	0	0	0	0	0	0	0	0	1	0	0	0
*S*12	0	0	0	0	0	0	0	1	0	0	0	0

4.2 仿真评估

首先我们只考虑攻防行为收益, 根据攻防效用函数建立攻防博弈矩阵, 如表 4 所示.

表 4 攻防博弈矩阵

攻击行为	防御行为	
	1 阻断攻击源	2 清洗攻击流量
1 TCP 洪水攻击	(1, –1)	(6, –6)
2 SYN 洪水攻击	(3, –3)	(5, –5)
3 Sockstress 攻击	(5, –5)	(4, –4)

根据攻防博弈矩阵使用软件 Gambit 使用软件计算攻防策略纳什均衡, 图 5 描述了计算攻防策略纳什均衡的过程.

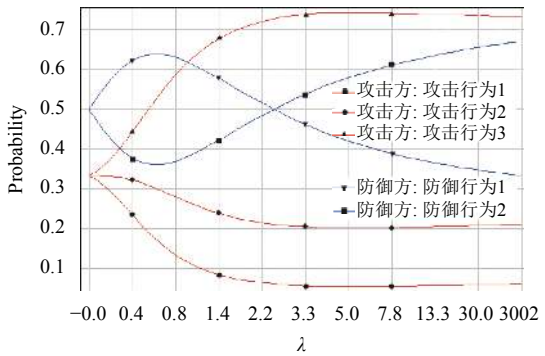

图 5 攻防策略纳什均衡计算结果

由图 5 可知, 最终收敛的值即为攻防策略纳什均衡, 计算结果为:

$$\pi^{a*} = (0.0612, 0.2180, 0.7278)$$

$$\pi^{b*} = (0.3333, 0.6667)$$

由此可知, 攻击方为了最大化自身收益, 最有可能采取 Sockstress 攻击, 而对防御方而言, 针对各类 DDoS 攻击最优的防御措施是对攻击流量进行清洗.

然后我们综合考虑攻防行为强度和攻防行为收益, 将攻防博弈求解纳什均衡得到攻防行为策略赋予 DDoS 攻防对抗网, 作为瞬间变迁选择执行概率参数π. 针对 DDoS 攻击而言, 攻击流量大小是衡量攻击强度的重要指标, 我们以处理攻击流量的速率作为衡量攻击强度参数λ的依据. 由于洪水攻会要在短时间内发送大量的攻击流量, 而慢速攻击不需要在短时间发送大量流量, 所以洪水攻击较慢速攻击而言攻击强度较大; 针对于洪水攻击, 对攻击流量清理会比阻断攻击源在短时间内处理攻击流量更多, 所以其行为强度较大, 而针对慢速攻击, 阻断攻击源会比对攻击流量清理在短

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

时间内处理攻击流量更多, 因此其行为强大较大.

对 DDoS 攻防对抗网变迁参数设置如表 5 所示, 使用随机 petri 网建模软件 PIPE 对 DDoS 攻防对抗网进行仿真, 进行稳态概率求解, 最终求得稳态概率:

$$p(S3)=0.0545;\ p(S2)=0.09706;\ p(S1)=0.06481$$
$$p(S12)=0.00908;\ p(S11)=0.06481$$
$$p(S9)=0.03235;\ p(S10)=0.12943$$
$$p(S8)=0.32405;\ p(S7)=0.21605$$

$$\pi_{t1}=\frac{p(S3)}{p(S3)+p(S2)+p(S1)}$$

$$\pi_{t2}=\frac{p(S2)}{p(S3)+p(S2)+p(S1)}$$

$$\pi_{t3}=\frac{p(S1)}{p(S3)+p(S2)+p(S1)}$$

$$\pi_{t7}=\frac{p(S12)}{p(S12)+p(S11)}$$

$$\pi_{t8}=\frac{p(S11)}{p(S12)+p(S11)}$$

$$\pi_{t9}=\frac{p(S9)}{p(S9)+p(S10)}$$

$$\pi_{t10}=\frac{p(S10)}{p(S9)+p(S10)}$$

$$\pi_{t11}=\frac{p(S8)}{p(S8)+p(S7)}$$

$$\pi_{t12}=\frac{p(S10)}{p(S9)+p(S10)}$$

表 5 DDoS 攻防对抗网参数设置

变迁	λ	π
$t1$		0.0612
$t2$		0.2180
$t3$		0.7278
$t7/t9/t11$		0.3333
$t8/t10/t12$		0.6667
$T4$	2	
$T5$	1	
$T6$	0.2	
$T13$	1	
$T14$	4	
$T15$	1	
$T16$	2	
$T17$	3	
$T18$	1	

我们用以上公式对上述攻防双方所处攻防状态的概率进行处理, 使得结果更加清晰, 得到:

攻击方攻击状态概率

$$\pi^{a'}=(0.2519,0.4486,0.2995)$$

防御方针对三种攻击的防御状态概率

$$\pi^{d'}=(0.1111,0.8889)$$

$$\pi^{d''}=(0.2000,0.8000)$$

$$\pi^{d'''}=(0.6000,0.4000)$$

由此可知, 对于攻击方而言, 攻击方最可能处于 SYN 洪水攻击状态, 即最可能发动 SYN 洪水攻击; 而对防御方而言, 针对于洪水攻击, 防御方最可能采取攻击流量清洗措施, 针对于慢速攻击而言防御方最可能采取阻断攻击源措施抵御 DDoS 攻击.

参考文献[5,12]中针对基于博弈的 DDoS 攻防对抗评估方法, 只考虑攻防收益, 通过建立攻防博弈矩阵求得到 DDoS 攻防对抗评估结果为:

$$\pi^{a*}=(0.0612,0.2180,0.7278)$$

$$\pi^{d*}=(0.3333,0.6667)$$

将本文得到 DDoS 攻防对抗评估结果与用文献[5,12]方法得到的结果进行对比可以看出, 运用博弈论和随机 Petri 网思想综合考虑攻防行为强度和攻防行为收益评估出最优攻击行为是 SYN 洪水攻击, 同时攻击行为概率相差较小, 表明评估结果更加贴近实际, 并且防御行为评估具有针对性, 对于不同攻击行为, 本文方法能评估得出针对其最有效的防御行为.

5 结束语

本文基于随机 Petri 网建立了 DDoS 攻防对抗网, 基于博弈论思想进行攻防博弈, 得出攻防行为策略并赋予攻防对抗网, 综合考虑攻防行为收益和攻防行为强度两方面针对 DDoS 攻防行为进行攻防对抗并评估, 得出的评估结果比只运用博弈论思想考虑攻防行为收益得到的评估结果更加合理且具有针对性. 本文的研究成果可运用于攻击行为的预测和防御策略的主动选取并提前部署.

下步工作就是结合评估结果对实际 DDoS 攻防对抗实验进行验证, 通过实际验证结果对本文所建立的攻防对抗网参数进行优化, 使其更具准确性和通用性.

参考文献

1 鲍旭华, 洪海, 曹志华. 破坏之王: DDoS 攻击与防范深度

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

剖析. 北京: 机械工业出版社, 2014.
2 Mölsä JVE. A taxonomy of criteria for evaluating defence mechanisms against flooding DoS attacks. Blyth A. EC2ND 2005. London: Springer, 2006. 13–22.
3 Meadows C. A cost-based framework for analysis of denial of service in networks. Journal of Computer Security, 2001, 9(1-2): 143–164. [doi: 10.3233/JCS-2001-91-206]
4 黄亮, 冯登国, 连一峰, 等. 一种基于多属性决策的 DDoS 防护措施遴选方法. 软件学报, 2015, 26(7): 1742–1756. [doi: 10.13328/j.cnki.jos.004673]
5 石盼, 连一峰. 基于战略博弈的 DDoS 攻防绩效评估方法. 计算机工程, 2009, 35(3): 195–198. [doi: 10.3969/j.issn.1000-3428.2009.03.066]
6 林闯. 随机 Petri 网和系统性能评价. 北京: 清华大学出版社, 2000.
7 Jalan R, Kamat G, Szeto RWL. Mitigating TCP SYN DDoS attacks using TCP reset. US, 20180034848. [2018-02-01].
8 庄建儿. 浅析网络 DDoS 攻击与治理. 通讯世界, 2015, (1): 33–34. [doi: 10.3969/j.issn.1006-4222.2015.01.021]
9 何亨, 胡艳, 郑良汉, 等. 云环境中基于 SDN 的高效 DDoS 攻击检测与防御方案. 通信学报, 2018, 39(4): 2018068.
10 刘航, 曹建新, 张新建. 流量清洗系统在防御 DDoS 攻击中的应用. 科技信息, 2010, (20): 249. [doi: 10.3969/j.issn.1673-1328.2010.20.251]
11 German R, Kelling C, Zimmermann A, *et al*. TimeNET-a toolkit for evaluating non-Markovian stochastic Petri nets. Proceedings of the 6th International Workshop on Petri Nets and Performance Models. Durham, NC, USA. 1995. 210-211.
12 张尚韬. 基于不完全信息静态博弈的 DDoS 防御机制评估方法研究. 佛山科学技术学院学报 (自然科学版), 2017, 35(6): 12–16.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net