软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(3):712−723 [doi: 10.3724/SP.J.1001.2012.03997]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于静态贝叶斯博弈的蠕虫攻防策略绩效评估*

刘玉岭[1,2,3+], 冯登国[1], 吴丽辉[4], 连一峰[1,3]

[1](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

[2](信息网络安全公安部重点实验室(公安部第三研究所),上海 201204)

[3](信息安全共性技术国家工程研究中心,北京 100190)

[4](中国科学院 办公厅,北京 100864)

Performance Evaluation of Worm Attack and Defense Strategies Based on Static Bayesian Game

LIU Yu-Ling[1,2,3+], FENG Deng-Guo[1], WU Li-Hui[4], LIAN Yi-Feng[1,3]

[1](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Key Laboratory of Information Network Security of Ministry of Public Security (The 3rd Research Institute of Ministry of Public Security), Shanghai 201204, China)

[3](National Engineering Research Center for Information Security, Beijing 100190, China)

[4](Clerical Office, The Chinese Academy of Sciences, Beijing 100864, China)

+ Corresponding author: E-mail: ylliu@is.iscas.ac.cn

Liu YL, Feng DG, Wu LH, Lian YF. Performance evaluation of worm attack and defense strategies based on static Bayesian game. *Journal of Software*, 2012,23(3):712−723. http://www.jos.org.cn/1000-9825/3997.htm

Abstract: The existing performance evaluation methods of worm attack strategies (defense strategies) are not considered defense strategies (attack strategies) change's influence on attack strategies (defense strategies) and performance evaluation of defense strategies are ignoring the implementation cost. In view of this situation, a performance evaluation model based on static Bayesian game (PEM-SBG) is proposed, and the performance evaluation methods of worm attack and defense mechanisms are presented. The performance evaluation method of defense mechanisms is based on gray multiple attributes theory and considers several evaluation metrics about cost and utility, so the evaluation process is much more comprehensive. Finally, the paper uses simulation tools SSFNet to implement simulation experiments under different attack and defense scenarios and validate the method.

Key words: performance evaluation, static Bayesion game, grey multiple attributes, defense mechanisms

摘 要: 现有蠕虫攻击策略(防护策略)评估方法没有考虑防护策略(攻击策略)变化对攻击策略(防护策略)绩效评估的影响,且防护策略评估忽视了策略实施成本.针对这种情况,构建了基于静态贝叶斯博弈的绩效评估模型(performance evaluation model based on static Bayesian game,简称 PEM-SBG)以及对抗情形下的蠕虫攻防策略绩效评估方法.在模型 PEM-SBG 基础上提出的基于灰色多属性理论的防护策略绩效评估方法,综合考虑了成本类和收益类的多个评估属性,有助于提高评估过程的全面性.针对典型的蠕虫攻防场景.利用仿真工具 SSFNet 进行了模拟

* 基金项目: 国家高技术研究发展计划(863)(2009AA01Z439); 国家高技术产业化项目信息安全专项; 信息网络安全公安部重点实验室(公安部第三研究所)开放基金(C10606)

收稿时间: 2010-07-07; 修改时间: 2010-10-29; 定稿时间: 2011-01-31

实验,验证了所提出的模型和方法的有效性.

关键词: 绩效评估;静态贝叶斯博弈;灰色多属性;防护策略

中图法分类号: TP309 **文献标识码:** A

蠕虫是当前主要的网络安全威胁之一,Code Red v2,Code Red II,Nimda,Slammer,Blaster 等蠕虫在短时间内感染了数以万计的主机[1],如 2001 年 6 月 19 日的 Code Red v2 蠕虫在其开始传播的 14 个小时内感染了近 36 万台主机[2];2003 年 1 月的 Slammer 在 10 分钟之内感染了 90%的易感主机[3].迅速传播的蠕虫一方面会导致巨大的经济损失,如 Code Red v2 导致的直接经济损失超过 26 亿美元[2];另一方面,数量巨大的感染主机可被用于发动大规模网络攻击(如 DDoS 攻击).

在蠕虫攻击过程中,攻击方可以通过调整扫描策略改变蠕虫的传播速度和传播范围,进而获得不同的攻击绩效.防护方同样可以通过调整防护策略达到不同的抑制效果,进而获得不同的防护绩效.理性的攻击者针对防护方可能采取的策略,倾向于选择能最大化攻击效果的攻击策略,而理性的防护方同样如此.因而我们迫切需要一种能够在攻防双方对抗的情形下量化评估蠕虫攻击(防护)绩效的方法,以为蠕虫的攻防过程提供决策支持.

蠕虫攻击者已经尝试了不同的扫描策略[4]:Code Red 和 Slammer 采用了随机扫描整个 IPv4 地址空间的策略;Code Red II 采用了本地优先扫描策略;Blaster 采取了顺序扫描策略.文献[5]将易感主机选择策略分为随机和 P2P 目标列表,感染策略分为合作和非合作,建模分析了它们两两结合的策略对蠕虫传播的影响,其分析工作限定于 P2P 网络且合作的感染策略是不切实际的.文献[4]除了上述扫描策略外,还指出了路由扫描、目标列表扫描、合作扫描、分而治之扫描等扫描策略,并系统地建模分析了各种扫描策略对蠕虫传播的影响.其分析工作针对的是防护方不采取任何防护策略的情形,而实际的蠕虫传播是在扫描策略和防护策略的共同作用下进行的.

针对蠕虫攻击,研究人员提出了许多防护策略,如内容过滤策略、地址黑名单策略、传播补丁蠕虫、吞噬蠕虫等[2,3,6,7],并对各种防护策略进行了绩效评估.文献[2]针对抑制蠕虫传播的防护策略提出了 3 项评估指标:响应时间、抑制策略、部署场景,并使用分析模型和实验仿真两种方式分析了内容过滤和地址黑名单策略的有效性.作者只是对两种典型抑制策略的有效性进行了分析,缺乏对主动防护策略的分析且评估过程欠缺防护成本的考虑.文献[3]将防护策略分为 Reactive Antibody Defense,Reactive Address Blacklisting,Proactive Protection 和 Local Containment 等 4 类,分析了决定各种策略有效性的关键参数,并通过理论分析和仿真实验的方式分析了 4 类防护策略及相互组合之后的防护效果,其分析同样仅仅是有效性分析.文献[6]将主动蠕虫(active worm)分为 simple patch,spreading patch,nullifying defense 和 sniper defense 这 4 种,从受保护的主机数、攻防双方消耗的网络带宽、攻防双方作用下所能达到的最大扫描速度等指标入手评估了 4 种策略的效果.他们的评估加入了带宽消耗这一成本因素,不过带宽消耗只是防护策略实施成本的一方面,且很多情况下带宽消耗并不是防护方选择策略时的首要考虑因素.与文献[2]相反,此处只分析了主动防护策略的绩效.文献[7]引入子网概念,比较了阻止或降低蠕虫传播速度的被动防护策略和主动为主机打补丁或移除感染主机的主动防护策略的有效性,但仍然没有考虑防护策略实施成本.此外,上述对防护策略的评估只是孤立考虑防护策略变化对蠕虫传播的影响,未考虑攻击策略同时存在变化时蠕虫的传播情形.而在实际攻击中,攻防双方会同时调整各自的策略,任何一方策略的变化均会影响到双方的策略绩效,反过来又会影响到攻防双方策略的选择.

我们需要建立一种统一的绩效评估模型,在攻防双方对抗的情形下量化评估攻防策略的绩效,且防护策略的绩效评估要综合考虑防护策略实施成本、防范性能和适用范围等多方面的评估属性,进而根据绩效评估的结果选择最优的防护策略.

针对上述目标,本文使用博弈论工具对蠕虫攻防场景进行建模,构建了基于静态贝叶斯博弈的绩效评估模型(performance evaluation model based on static Bayesian game,简称 PEM-SBG).在此模型基础上,设定评估属性从多个角度评估防护策略的绩效并把攻防策略的绩效作为攻防策略的收益,最后计算攻防双方策略集的纳什均衡,计算的结果用来指导选择最优的蠕虫防护策略.

本文主要做了以下贡献:

1) 本文建立了基于静态贝叶斯博弈的绩效评估模型 PEM-SBG.该模型可在对抗情形下评估攻防双方的策略集,更加符合真实的攻防场景,而且攻防双方策略集博弈分析后的纳什均衡可以为选择最优的防护策略提供依据;
2) 针对防护策略评估属性众多且各评估属性取值可能不精确、不一致的情形,提出了基于灰色多属性关联分析的防护策略绩效评估方法.绩效计算兼顾了成本和收益两方面,并从多个角度进行评估,评估过程更加全面;
3) 进行了一系列的仿真实验.实验结果表明,本文的 PEM-SBG 模型和绩效计算方法可以在对抗情形下评估攻防双方策略的绩效,并能有效指导防护策略的选择.

本文第 1 节建立基于静态贝叶斯博弈的绩效评估模型 PEM-SBG.第 2 节定义针对蠕虫防护策略的评估属性及其计算方法.第 3 节具体阐述绩效评估方法.第 4 节对本文中模型和方法进行实验分析和验证.最后给出总结和未来工作的展望.

1 PEM-SBG 模型

博弈论是研究具有竞争或对抗性质现象的运筹学理论,其中具有竞争或对抗性质的行为称为博弈行为[14].研究人员使用博弈论工具建模分析了与博弈行为相似的网络攻防行为.文献[8]把网络攻防双方建模为二人非合作博弈模型,并提出了防御图模型、攻防策略分类及其成本量化方法和最优主动防御选取算法.他们的工作为本文提供了基础,本文基于静态贝叶斯博弈,能够体现出攻防双方拥有信息不对称这一特性,且本文的防护策略绩效评估方法兼顾了成本和收益的多个方面.

静态贝叶斯博弈是不完全信息同时行动的博弈:不完全信息是指在博弈时至少有一个参与者不能确定其他参与者的类型,参与者的类型对应着该参与者的收益函数[14];同时,行动是指所有参与者同时选择自己的行动或虽非同时选择但后行动者并不知道先行动者采取了什么具体行动.文献[9]把无线传感器网络中节点和 IDS 之间的交互建模为贝叶斯博弈,加强了路由的安全性,博弈的纳什均衡结果为选择最佳防护策略提供了基础.文献[10]提出了一个博弈论的框架,用来分析攻防节点之间的行为,其中的分析包括了静态贝叶斯博弈和动态贝叶斯博弈.上述工作为本文模型的构建提供了借鉴.

在实际的蠕虫攻防场景中,攻防双方所拥有的信息是不对称的,防护方通常无法确定攻击方使用的攻击策略[9,10],而防护方的策略则一般是攻防双方的共有信息[10].攻防双方选择各自的策略进行博弈,逻辑上可以认为攻防双方是同时行动的.因而,蠕虫攻防双方选择策略的过程可以看做一个二人静态贝叶斯博弈的过程,博弈的结果可用来指导蠕虫防护策略的选取.

1.1 模型定义

在给出模型 PEM-SBG 的定义之前,首先定义模型中用到的术语.

定义 1(类型空间). 指参与者类型的集合.例如文献[10]中,恶意用户和正常用户组成攻击者的类型空间.

定义 2(先验信念空间). 先验信念是指每个参与者在进行博弈时认为其他参与者是某种类型的先验概率,参与者的先验信念空间是该参与者先验信念的集合.

定义 3(行动空间). 指每个参与者在博弈时依据其类型可以做的某种具体选择,参与者的行动空间指该参与者的行动集合.例如文献[10]中,攻击和不攻击构成攻击者的行动空间,检测和不检测构成防护方的行动空间.

定义 4(效用). 指参与者在博弈时依据其类型和所选择的行动而能够获得的收益.

定义 5. PEM-SBG 模型是一个多元组 $PEM\text{-}SBG=\{Aa,Ad;Ta,Td;Pa,Pd;\mu a,\mu d\}$,其中,$a,d$ 表示蠕虫攻击方与防护方.各参数的具体含义如下:

1) Ta,Td 为参与者 a,d 的类型空间.本文中,攻击方类型空间为采用各种扫描策略的攻击方,防护方类型为两参与者的共有信息[10],即防护方只有一种类型.如果攻击方有 n 个攻击策略,具体表示如下:

$$Ta=\{Ta_i\},1\leqslant i\leqslant n;Td=\{Td\}.$$

2) Pa,Pd 为参与者 a,d 的先验信念空间,具体见表 1;

3) Aa,Ad 为参与者 a,d 的行动空间.本文中,攻击方的行动空间为攻击(attack)、不攻击(not attack),防护方行动空间为防护策略集合.假设存在 m 个防护策略,则攻防双方的行动空间见表 2;

4) $\mu a,\mu d$ 为参与者 a,d 的效用.

Table 1 Prior beliefs space and prior beliefs of attacker and defender

表 1 攻防双方先验信念空间及先验信念

先验信念空间	先验信念
$Pa=P(Td)$	$P(Td)=1$
$Pd=\{P(Ta_i)\},1\leqslant i\leqslant n$	$P(Ta_i)=P_i,1\leqslant i\leqslant n$ 且 P_i 之和为 1

Table 2 Action space of attacker and defender

表 2 攻防双方行动空间

攻击方行动空间	防护方行动空间
$Aa(P(Ta_i))=\{\text{Attack,Not Attack}\}$	$Ad(Td)=\{DP_j\}$
$1\leqslant i\leqslant n$	DP_j 为防护策略且 $1\leqslant j\leqslant m$

效用反映了攻防双方的偏好关系,攻防双方选择不同的策略会得到不同的效用.在博弈过程中,为了最大化自己的效用,攻防双方会采用不同的策略进行博弈.效用直接影响着攻防双方策略的选择,本文把攻防策略的绩效作为攻防双方的效用,并在第 3 节中详细介绍攻防双方策略的绩效评估方法.

1.2 最优防护策略选择方法

在不同的攻防场景中,攻击方可以采取不同的攻击策略,防护方如何从防护策略集中选择最优的防护策略就成为关键问题.本文首先建立基于模型 PEM-SBG 的攻防双方的静态贝叶斯博弈;然后,博弈分析攻防双方的策略,并根据博弈结果选择最优的防护策略.

在博弈过程中,每个参与者在给定己方类型和其先验信念空间的情形下,倾向于选择使自己的期望效用达到最大化的策略,最终各参与者会达到一种均衡,即纳什均衡.此时,任何参与者改变其策略所获得的效用都不会大于均衡状态下的效用.蠕虫攻防策略博弈中的纳什均衡表示均衡时的防护策略效用最大,即此策略的防护绩效最好.安全管理员应该优先选择该防护策略,因而纳什均衡结果可指导选择最优防护策略.

定义 6. 在 PEM-SBG 模型中,策略组合 $s=(s_1,s_2)$是一个纯策略贝叶斯纳什均衡.如果对每一参与者 i 及对 i 的类型空间 T_i 中的每一个 t_i,参与者 i 的策略 $s_i(t_i)$满足:

$$\max_{a_i\in A_i}\sum_{t_{-i}}\{u_i[s_i,s_{-i}(t_{-i}),a_i;t_i]p_i(t_{-i}\mid t_i)\},$$

其中,a_i 表示参与者 i 的行动空间 A_i 中的某一个行动;参与者 i 的信念 $p_i(t_{-i}|t_i)$描述了 i 在给定自己的类型 t_i 时,对另一参与者可能的类型 t_{-i} 的不确定性;定义中,求最大值的和是对 t_{-i} 求和,即对另一参与者的各种可能的类型组合求和.

2 评估属性定义

评估蠕虫防护策略既要考虑策略产生的防护效果即策略收益,又要考虑策略的实施成本,且实施成本是安全管理员选择防护策略的重要依据.而现有的评估工作忽略成本因素[2,3,7]或仅考虑部分成本因素[6].本文认为,策略实施成本既包括由于购买设备、实施维护而产生的经济性支出,又包括性能和社会影响上的支出.下面定义蠕虫防护策略绩效评估中的评估属性.

定义 7. 评估属性 EM 为二元组 $EM=\langle CEM,PEM\rangle$,其中,$CEM$ 为成本类评估属性,PEM 为收益类评估属性.

定义 8. 成本类评估属性 CEM 是评估防护策略实施成本的属性集合,为五元组$\langle CPM,RT,RC,FN,SM\rangle$,具体含义及计算方法如下:

1) CPM 为购置维护费用,是评估实施防护策略需购买设备、维护设备、培训使用人员等费用的属性.

企业一般以年为单位作此类成本预算,且设备使用年限一般较长,所以计算公式为

$$CPM=C_e(1+I)^n/n+C_m \tag{2-1}$$

其中,C_e 表示购买设备的花费,n 为设备预期使用年限,I 为银行利率,C_m 为一年内投入的维护和培训费用;

2) *RT* 为响应时间,是评估攻击发生时防护策略反应速度的属性,单位为小时.文献[2]将响应时间定义为检测到恶意行为、把该信息传播到所有参与防护的主机和激活防护策略并使其生效的时间之和;文献[3]没有考虑激活策略的时间,而将响应时间定义为产生并传播抗体的时间;本文借鉴文献[2]中的定义,给出计算公式如下:

$$RT=T_s-T_0 \tag{2-2}$$

其中,T_0 是检测到攻击的时间,T_s 为防护策略生效的时间;

3) *RC* 为资源消耗,是评估防护策略实施后处理器、内存、网络带宽等使用率的属性.资源消耗既包括防护策略的消耗,又包括攻击者和正常用户的消耗.一般地,存在攻击和不存在攻击时,资源的消耗是不同的,实际评估时要依据两种情况分别使用下面公式进行计算.文献[6]使用了攻防双方消耗的带宽作为评估指标,本文在此基础上加入了主机资源消耗.计算时选取关键主机和关键链路,对其资源消耗情况进行加权平均,计算公式如下:

$$RC=\left(\sum_{i=1}^{n}k_i(C_i+M_i)+\sum_{j=1}^{m}\lambda_j B_j\right)\Big/(2n+m) \tag{2-3}$$

4) *FN* 为漏报率,是评估由于不能完全检测出已感主机和/或感染数据包,未检测出的已感主机和/或感染数据包会继续传播,从而导致防护策略具有不同性能的属性,计算公式为

$$FN=1-D(t)/I(t) \tag{2-4}$$

其中,$I(t)$表示截止时间点 t 的已感主机数,$D(t)$表示时间点 t 防护策略检测出的已感主机数;

5) *SM* 为社会因素,是评估非技术能力所能控制的成本的属性,如法律限制[7].社会因素由评估人员根据评估环境、评估要求的不同而设定.

Table 3 Parameters meaning of resource consumption attribute

表 3 资源消耗属性参数含义

m	关键链路数
n	关键主机数
k_i	第 i 台主机的重要性,由风险评估结果得出,$0\leqslant k_i\leqslant 1$ 且$(k_1+k_2+\ldots+k_n)=1$
λ_j	第 j 条链路的重要性,$0\leqslant \lambda_j\leqslant 1$ 且$(\lambda_1+\lambda_2+\ldots+\lambda_m)=1$
M_i	第 i 台主机的内存利用率 $0\leqslant M_i\leqslant 1$
C_i	第 i 台主机的 CPU 利用率 $0\leqslant C_i\leqslant 1$
B_j	第 j 条链路上已使用带宽与该链路的最大带宽之比,$0\leqslant B_j\leqslant 1$

定义 9. 收益类评估属性 *PEM* 是评估防护策略抑制蠕虫传播或清除蠕虫效果的属性,为二元组 $PEM=\langle NIH,DAD\rangle$,具体含义如下:

1) *NIH* 为感染主机数,是衡量蠕虫攻击范围的属性,为截止特定时间时感染主机的数目.感染主机数为最常用的评估属性[1−7],时间点 t 时的感染主机数用 $I(t)$表示;

2) *DAD* 为攻击破坏度,是衡量蠕虫攻击速度的属性.文献[6]中使用了最大扫描速度作为评估属性,而扫描速度只是影响攻击速度的一个因素,除此之外还受易感主机数、易感主机分布情况等因素影响.本文在其基础上,从攻击的实际后果角度出发,将攻击破坏度定义为攻击过程中最大感染主机数与达到该最大感染主机数所用时间之比,计算公式为

$$DAD=I_{\max}/(T_m-T_0) \tag{2-5}$$

其中,$I_{\max}$为蠕虫攻防过程中最大的感染主机数,T_m为达到最大感染主机数时的时间,T_0为检测到攻击的时间.

3 绩效评估方法

本节在第 1 节构建的 PEM-SBG 模型基础之上,根据第 2 节中定义的绩效评估属性,详细阐述攻防策略的绩效评估方法,并把评估得出的绩效作为攻防双方的效用.

3.1 攻击策略绩效评估方法

在蠕虫攻击过程中,攻击方期望感染尽可能多的主机[2,3],因而本文把感染主机数引入攻击方策略绩效的评估,提出如下的计算公式:

$$\mu=I(t)/N \tag{3-1}$$

其中,$I(t)$为截止时间点 t 的感染主机数;N 为总的易感主机数,易感主机数可为估计值且 $N\geqslant I_{\max}$,$I_{\max}$ 为蠕虫攻防过程中最大的感染主机数.

3.2 防护策略绩效评估方法

不同于攻击方,防护方期望用最小的付出获得最大的收益,因而防护策略绩效评估要考虑成本、收益两方面的因素综合得出.

由于攻防场景和评估条件的不同,第 2 节定义的评估属性得出的值可能并不精确,且同一防护策略的各个评估属性值的单位也不同.如何根据评估属性的值得出防护策略的综合绩效值,就成了一个棘手的问题.而灰色多属性理论能够很好地处理精确值和估计值、定性值和定量值混杂存在的情况,它只需保证不同防护策略的同一评估属性的值单位一致,同一策略不同属性间的评估值单位则可不同.灰色多属性理论还具有学习性能,它可以从数据本身观察到真实的内在特征.基于上述原因,本文提出了基于灰色多属性的防护策略绩效评估方法.

防护策略的绩效评估方法的具体步骤为:首先,根据第 2 节的方法计算防护策略各评估属性的值,并用矩阵 $\boldsymbol{X}$ 表示防护策略评估属性值的矩阵,矩阵 $\boldsymbol{X}$ 的 m 行对应 m 种防护策略,n 列对应 n 项评估属性,k 行 j 列的值表示第 k 种防护策略的第 j 项评估属性的值,用 x_{kj} 表示;其次,确定理想策略,即成本最小、收益最大的策略,把理想策略的评估属性值作为矩阵 $\boldsymbol{X}$ 的第 0 行;最后,使用灰色多属性关联分析方法计算各防护策略绩效与理想策略绩效的关联度,用此关联度作为防护策略的绩效.

灰色多属性关联分析方法的算法流程见算法 1.利用矩阵 $\boldsymbol{X}$ 和灰色多属性关联分析方法计算防护策略关联度的步骤如下:

第 1 步,正规化处理矩阵 $\boldsymbol{X}$ 中数据,设 γ_{kj} 为正规化处理后矩阵中 k 行 j 列的值,则

$$\gamma_{kj}=m\times x_{kj}/(x_{1j}+x_{2j}+\ldots+x_{mj}).$$

第 2 步,在正规化后的矩阵 $\boldsymbol{X}$ 中,使用公式 $\Delta_{kj}=|\gamma_{kj}-\gamma_{0j}|$ 计算差序列.其中,γ_{kj} 为正规化处理后矩阵中 k 行 j 列的值,γ_{0j} 为矩阵 $\boldsymbol{X}$ 的第 0 行 j 列的值.

第 3 步,在第 2 步得出的差序列中,计算两极最大差 $\Delta_{\max}$ 即所有元素的最大者和两极最小差 $\Delta_{\min}$ 即所有元素的最小者.

第 4 步,使用公式 $\eta_{kj}=(\Delta_{\min}+\Delta_{\max})/(\Delta_{kj}+\Delta_{\max})$ 计算矩阵 $\boldsymbol{X}$ 中防护策略评估属性值的关联系数 η_{kj}.

第 5 步,确定各评估属性的权重,第 j 种评估属性的权重为 W_j,后面第 3.3 节将详细介绍评估属性权重的确定方法.

第 6 步,加权得出各防护策略的关联度,第 k 项防护策略的关联度 $\theta(k)$ 的计算公式为

$$\theta(k)=\sum_{j=1}^{n}w_j r_{kj}.$$

算法 1. 灰色多属性关联分析方法 *Compute-Grey-Degree-of-Association*(X).

Input: Matrix $\boldsymbol{X}=(x_{kj})$,$0\leqslant k\leqslant m$,$1\leqslant j\leqslant n$;

Output: *Grey-Degree-of-Association* R_i,$1\leqslant i\leqslant m$.

BEGIN

1. For each element x_{kj} in Matrix $\boldsymbol{X}$

2. $\gamma_{kj} := m \cdot x_{kj} \Big/ \sum_{k=1}^{m} x_{kj}$

3. For each k from 1 to m

4. For each j from 1 to n

5. $\Delta_{kj} := |\gamma_{0j} - \gamma_{kj}|$

6. Let $\Delta_{\max} := \max_{k,j} \Delta_{kj}, \Delta_{\min} := \min_{k,j} \Delta_{kj}$

7. For each k from 1 to m

8. For each j from 1 to n

9. $\eta_{kj} := \dfrac{\Delta_{\min} + \Delta_{\max}}{\Delta_{kj} + \Delta_{\max}}$

10. w_j:=*Compute-Weight*(***X***)

11. $\theta(k) := \sum_{j=1}^{n} w_j \gamma_{kj}$

END

3.3 评估属性权重确定方法

在防护策略绩效评估方法中,需要确定各评估属性的权重,本节将详细介绍评估属性权重的确定方法.

现有确定权重的方法中,一是专家依据经验确定评估属性的权重,优点是简单直接且最大程度的反映以往的历史积累,缺点是权重随意和实时变通性不强;二是利用熵权法由现有数据集计算得出各评估属性的权重,优点是理论依据强且权重随着数据集的变化而变化,缺点是忽略以往历史数据的积累.考虑到上述两种方法的优缺点.本文综合使用上述方法计算评估属性的权重.针对易于由专家经验给出权重的属性,由专家直接指定,剩余评估属性的权重则利用熵权法进行计算,具体算法流程见算法 2.算法 2 的主要步骤如下:

第 1 步,如果专家指定第 j 种评估属性的权重为 W_j,则从总权重 1 中减去这些评估属性的权重,最后得到的值 t 即为使用熵权法计算的所有评估属性权重的和.

第 2 步,使用如下公式计算第 j 项评估属性下第 k 个策略评估属性值的比重:

$$f_{kj} = x_{kj} \Big/ \sum_{k=1}^{m} x_{kj}.$$

第 3 步,如果 f_{kj}=0,则 $f_{kj}\ln f_{kj}$=0,然后计算评估属性的熵值,第 j 项评估属性熵值的计算公式如下:

$$e_j = -\frac{1}{\ln m} \sum_{k=1}^{m} f_{kj} \ln f_{kj}.$$

第 4 步,计算得出各评估属性的权重,第 j 项评估属性的权重 W_j 的计算公式为

$$w_j = (1 - e_j) \times t \Big/ \sum_{j=1}^{n} (1 - e_j).$$

算法 2. 评估属性权重确定方法 *Compute-Weight*(***X***).

Input: Matrix $\boldsymbol{X}=(x_{kj}),1 \leqslant k \leqslant m,1 \leqslant j \leqslant n$;

Output: *Weight* $w_j,1 \leqslant j \leqslant n$.

BEGIN

1. For j from 1 to n

2. If $w_j \neq 0$

3. t:=1−w_j

4. $f_{kj} := x_{kj} \Big/ \sum_{k=1}^{m} x_{kj}$

5. If f_{kj}:=0

6. $f_{kj}\ln f_{kj}:=0$

7. Let $l:=1/\ln m$

8. $e_j:=-l\sum_{k=1}^{m} f_{kj}\ln f_{kj}$

9. $w_j:=(1-e_j)\times t\Big/\sum_{j=1}^{n}(1-e_j)$

END

3.4 绩效评估流程

在实际的蠕虫攻防策略绩效评估过程中,使用上面的模型和评估方法,安全管理员可以依据下述评估流程开展评估工作:

第 1 步,依据 PEM-SBG 模型中的定义和评估现场的情况,确定攻防双方的类型空间和行动空间.

第 2 步,使用第 3.1 节和第 3.2 节的方法评估不同攻防场景下攻击策略集和防护策略集中每一个策略的绩效.攻防双方选择其类型空间中的不同类型或其行动空间中的不同行动代表了不同的攻防场景,所以策略绩效的评估要依据攻防双方选择类型和行动的不同逐个进行.具体步骤将在第 4.2 节中结合实验给出.

第 3 步,确定攻防双方的先验信念空间.先验信念可由系统防护日志等记录中统计得出或由安全管理员根据经验进行设定.

第 4 步,把策略的绩效作为效用建立 PEM-SBG 模型,求解该模型的纳什均衡,安全管理员根据求解结果选择最佳防护策略.

3.5 方法对比分析

本节对比分析了本文方法和传统评估方法,结果见表 4.表 4 中√表示相关方法具有此项,⊙表示相关方法提到了该项而实际计算中并未使用或者仅使用了该项的一部分.可以看出:本文方法可以在对抗情形下评估攻防双方的策略绩效,而传统方法只是对攻击策略或防护策略的单方评估;本文方法的评估属性更为全面地反映了真实的攻防场景,且通过对攻防策略集的博弈,可以为安全管理员选择最优防护策略提供理论依据.

Table 4 Contrast of conclusions drawn by our method and traditional methods

表 4 传统方法与本文方法的对比结果

评估方法	评估属性							攻击策略评估	防护策略评估	防护策略建议
	CPM	RT	RC	FN	SM	NIH	DAD			
Moore D 方法[2]		√				√			√	
BRUMLEY D 方法[3]		√		⊙		√			√	√
ZOU C C 方法[4]						√		√		
M.NICOL D 方法[6,7]		√	⊙		⊙	√	⊙		√	
本文方法	√	√	√	√	√	√	√	√	√	√

4 实验与分析

本节通过仿真实验验证本文提出的 PEM-SBG 模型和攻防策略绩效评估方法的有效性.

4.1 实验基本情况

仿真工具 Scalable Simulation Framework(SSFNet)[11]是研究人员常用的仿真蠕虫传播的工具,通过设定不同的参数,可以模拟不同的蠕虫攻防场景.与文献[2]相同,为了网络环境的真实性,实验中使用的拓扑结构为从 Route Views Project[12]中得出的自治系统(autonomous system,简称 AS)连接数据集,采用的是 2009 年 5 月 10 日的数据集,其中共有 15 198 个 AS.

本文选取蠕虫的扫描策略为攻击方策略,并仿真了 3 种典型扫描策略作为攻击方的策略集:Code Red 和 Slammer 使用的随机扫描策略(random scan,简称 RS);Code Red II 使用的本地优先扫描策略(local preference

scan,简称 LPS);传播起始阶段最为迅速的目标列表扫描策略(hit-list scan,简称 HLS).文献[4]详细介绍了上述扫描策略.在防护策略集方面,选取了内容过滤(content filtering,简称 CF)、地址黑名单(address blacklisting,简称 ABL)这两种典型的被动抑制型防护策略[2,3,7],以及传播补丁蠕虫(spreading patch worm,简称 SPW)、吞噬蠕虫(nullifying worm,简称 NW)这两种典型的主动对抗型防护策略[6,7].

设定实验的初始参数见表 5.其中,本地优先扫描采用"/2"网络的扫描,即扫描空间被分为 4 个网络;策略覆盖度指防护策略所保护的主机与所有主机之比.

Table 5 Initialization parameters of experiment

表 5 实验初始参数

参数名称	初始值	参数名称	初始值
易感主机数	360 000	初始感染主机数(蠕虫)	1
初始感染主机数(SPW)	1	初始感染主机数(NW)	1
目标列表中的主机数	5	本地优先扫描的网络数	4
策略启动时间(SPW)	1	策略启动时间(NW)	1
策略启动时间(CF)	0.1	策略启动时间(ABL)	0.1
策略覆盖度	0.95	漏报率	0.05

4.2 攻防策略绩效评估

4.2.1 攻击策略绩效评估

与文献[2]相同,实验中的感染主机数为攻击发生 24 小时时的感染主机数,则攻击策略的绩效评估过程为:

首先计算攻击方依据其类型 RS 选择行动 Attack,防护方选择行动 SPW 时的攻击策略绩效.根据 SSFNet 仿真得出感染主机数为 298501.8,利用公式(3-1)可以得出此时的绩效为 298501.8/360000=0.8291716666666666.当防护方选择其他行动时的攻击策略绩效评估与此类似.

然后计算攻击方依据其类型 RS 选择行动 Not Attack 时的攻击策略绩效.由于不攻击时感染主机数为 0,所以此时无论防护方选择何种行动,攻击策略的绩效均为 0.

当攻击方依据其类型(HLS,LPS)选择行动 Attack 或 Not Attack 时,攻击策略绩效评估过程与上面评估过程类似,在此就不再赘述.

4.2.2 防护策略绩效评估

下面部分以攻击方依据其类型 RS 选择行动 Attack,防护方选择 4 种防护策略为其行动时的绩效评估过程为例介绍评估方法.

首先获取防护策略的评估属性值并表示为矩阵 $\boldsymbol{X}$,其中,生效时间、漏报率、感染主机数、攻击破坏度由 SSFNet 仿真得到.同样,感染主机数为攻击发生 24 小时的感染主机数,购置维护费用和资源消耗可由安全管理员根据公式(2-1)、公式(2-3)计算得出,此处取两者的估计值且暂不考虑社会因素.

其次确定理想策略.因为理想策略的成本最小,所以成本类评估属性取值为 0;同时,理想策略的收益最大,即感染主机数和攻击破坏度均为 0.最后得出的矩阵 $\boldsymbol{X}$ 如图 1 所示,矩阵的 7 列依次代表评估属性购置维护费用、响应时间、资源消耗、漏报率、社会因素、感染主机数和攻击破坏度,5 行依次代表理想策略、SPW、NW、CF 和 ABL.

最后,根据矩阵 $\boldsymbol{X}$ 和第 3.2 节中的方法计算各防护策略的绩效与理想策略绩效的关联度,并把策略的关联度作为防护策略的绩效.最后得出的关联度即 4 种防护策略绩效为(0.19606467375712386,0.27651489529250795,0.264280586228981,0.26313984472139607).

在上面的绩效计算过程中,评估属性的权重由第 3.2 节中的算法 2 确定,结果为

(0.10128171820583047,0.11212689541639352,0.045505368472781235,
0.16787653668345207,0,0.28686690843601537,0.28634257278553626).

当攻击方依据其类型 RS 选择行动 Not Attack 时,防护方选择 4 种防护策略为其行动时,矩阵 $\boldsymbol{X}$ 的评估属性生效时间、漏报率、感染主机数、攻击破坏度取值为 0,防护策略绩效计算过程与上面过程类似.

同理可以得出攻击方依据其类型(HLS,LPS)选择行动 Attack 或 Not Attack,防护方选择 4 种防护策略为其行动时的防护策略绩效.

$$\boldsymbol{X}=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.1 & 1 & 0.3 & 0 & 0 & 298501.8 & \dfrac{298501.8}{86400} \\ 0.1 & 1 & 0.5 & 0 & 0 & 0 & \dfrac{28.134592}{9120} \\ 0.8 & 0.1 & 0.1 & 0.05 & 0 & 48.49901 & \dfrac{48.49901}{86400} \\ 0.8 & 0.1 & 0.2 & 0.05 & 0 & 318.6406 & \dfrac{318.6406}{86400} \end{pmatrix}$$

Fig.1 Initialization matrix

图 1 初始矩阵 $\boldsymbol{X}$

4.3 最优防护策略选择

首先使用第 4.2 节的评估过程得出不同攻防场景下的攻防策略绩效(效用);然后设定攻防双方的先验信念空间,本文假设防护方认为攻击方类型为 RS,HLS,LPS 的先验信念为 0.7,0.2,0.1,防护方只有一种类型,所以攻击方先验信念为 1;最后使用博弈论工具 Gambit[13]建立如图 2 所示的贝叶斯博弈树,并计算该博弈的贝叶斯纳什均衡,纳什均衡结果见表 6.

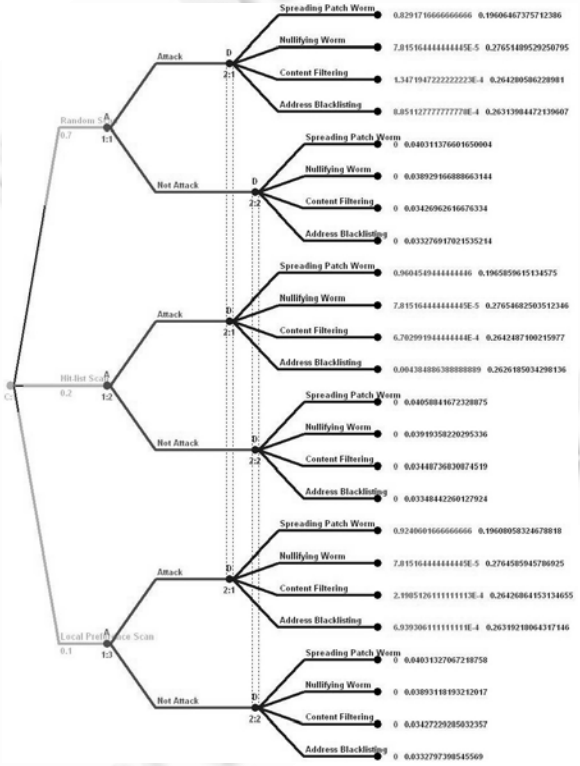


Fig.2 Bayesian game tree of worm attack and defend strategies

图 2 蠕虫攻防策略贝叶斯博弈树

Table 6 Pure strategy Bayesian Nash equilibrium

表 6 纯策略贝叶斯纳什均衡

先验信念	贝叶斯纳什均衡
$P(RS)=0.7$	$((Aa(RS)=\{Attack\}$
$P(HLS)=0.2$	$Aa(HLS)=\{Attack\}$
$P(LPS)=0.1$	$Aa(LPS)=\{Attack\}, Ad(Td)=\{NW\}, (0.7,0.2,0.1))$

表 6 中的纯策略贝叶斯纳什均衡含义为:在防护方的先验信念为 0.7,0.2,0.1 的情形下,攻击方依据其类型(RS,HLS,LPS)均选择 Attack,防护方选择吞噬蠕虫策略.出现该纳什均衡的原因在于:在攻击方的 3 种类型下,攻击方选择攻击的效用均大于选择不攻击时的效用,防护方选择吞噬蠕虫策略的效用最大即综合绩效最好.此博弈结果说明攻击方倾向于攻击,防护方在选取防护策略时应该优先考虑吞噬蠕虫策略.

接下来,在其他评估属性的值及博弈条件保持不变的情形下,分析某一个评估属性值的变化对绩效评估及博弈结果的影响.把社会因素纳入计算,假设 SPW 和 NW 的社会因素为 0.8,此时的矩阵 $\boldsymbol{X}$ 如图 3 所示.

$$\boldsymbol{X}=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.1 & 1 & 0.3 & 0 & 0.8 & 298501.8 & \frac{298501.8}{86400} \\ 0.1 & 1 & 0.5 & 0 & 0.8 & 0 & \frac{28.134592}{9120} \\ 0.8 & 0.1 & 0.1 & 0.05 & 0 & 48.49901 & \frac{48.49901}{86400} \\ 0.8 & 0.1 & 0.2 & 0.05 & 0 & 318.6406 & \frac{318.6406}{86400} \end{pmatrix}$$

Fig.3 New matrix

图 3 新矩阵 $\boldsymbol{X}$

同理,使用第 4.2 节的评估过程得出攻防策略绩效,并再次使用 Gambit 工具建立贝叶斯博弈并计算贝叶斯纳什均衡,纳什均衡结果见表 7.

Table 7 Pure strategy Bayesian Nash equilibrium

表 7 纯策略贝叶斯纳什均衡

先验信念	贝叶斯纳什均衡
$P(RS)=0.7$	$((Aa(RS)=\{Attack\}$
$P(HLS)=0.2$	$Aa(HLS)=\{Attack\}$
$P(LPS)=0.1$	$Aa(LPS)=\{Attack\}, Ad(Td)=\{CF\}, (0.7,0.2,0.1))$

根据表 7 可以得出,此时攻击方仍然依据其类型(RS,HLS,LPS)选择 Attack,但防护方选择内容过滤策略.虽然此时吞噬蠕虫策略的感染主机数仍为最小,但该策略的其他评估属性的值比较大(如社会属性),导致该策略的综合绩效不是最好.由此可见,在其他条件保持不变的情况下,任何评估属性值的变化均有可能导致防护策略绩效的变化,进而影响到最优防护策略的选择结果.

以上实验结果表明,本文提出的 PEM-SBG 模型和攻防策略绩效评估方法可以有效地评估攻防策略的绩效,并反映了成本和收益两方面因素对防护策略绩效的影响,博弈分析绩效评估的结果可以指导最优防护策略的选择.

5 小 结

本文建立了基于静态贝叶斯博弈的绩效评估模型 PEM-SBG,并在此模型基础之上提出了蠕虫攻防策略绩效评估方法.定义了多个评估属性,使用灰色多属性理论从成本和收益的角度对防护策略进行绩效评估;然后计算建立的静态贝叶斯博弈的纳什均衡,纳什均衡的结果可以用来指导防护策略的选择.最后,通过仿真实验验证了本文模型和方法的有效性.

未来工作包括改进攻击方的效用计算函数,从多属性的角度对攻击方的绩效进行评估;研究攻防双方均具

有私人信息情形下的博弈;另一方面,由于本质上蠕虫攻防是不完全信息多阶段攻击,在攻击过程中,可以动态地调整防护策略,不同的防护策略构成了不同的阶段,因而可以采用动态博弈的理论对蠕虫攻防过程进行分析研究.

References:

[1] Staniford S, Paxson V, Weaver N. How to own the Internet in your spare time. In: Proc. of the 11th USENIX Security Symp. 2002. 149−167.

[2] Moore D, Shannon C, Voelker GM. Internet quarantine: Requirements for containing self-propagating code. In: Proc. of the 22nd Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2003). 2003. 1869−1879. [doi: 10.1109/INFCOM.2003.1209212]

[3] Brumley D, Liu LH, Poosankam P, Song D. Design space and analysis of worm defense strategies. In: Proc. of the 2006 ACM Symp. on Information, Computer and Communications Security (ASIACCS 2006). 2006. 125−137. [doi: 10.1145/1128817.1128837]

[4] Zou CC, Towsley D, Gong WB. On the performance of Internet worm scanning strategies. Performance Evaluation, 2006,63(7): 700−723. [doi: 10.1016/j.peva.2005.07.032]

[5] Wei Y. Analyzing the performance of Internet worm attack approaches. In: Proc. of the 13th Int'l Conf. on Computer Communications and Networks (ICCCN 2004). 2004. 501−506. [doi: 10.1109/ICCCN.2004.1401717]

[6] Nicol DM, Liljenstam M. Models and analysis of active worm defense. In: Proc. of the MMM-ACNS 2005. LNCS 3685, Heidelberg: Springer-Verlag, 2005. 38−53. [doi: 10.1007/11560326_4]

[7] Liljenstam M, Nicol DM. Comparing passive and active worm defenses. In: Proc. of the 1st Int'l Conf. on the Quantitative Evaluation of Systems (QEST 2004). 2004. 18−27. [doi: 10.1109/QEST.2004.1348012]

[8] Jiang W, Fang BX, Tian ZH, Zhang HL. Evaluating network security and optimal active defense based on attack-defense game model. Chinese Journal of Computers, 2009,32(4):817−827 (in Chinese with English abstract).

[9] Mohi M, Movaghar A, Zadeh PM. A Bayesian game approach for preventing DoS attacks in wireless sensor networks. In: Proc. of the 2009 WRI Int'l Conf. on Communications and Mobile Computing. 2009. 507−511. [doi: 10.1109/CMC.2009.325]

[10] Liu Y, Cristina C, Hong M. A Bayesian game approach for intrusion detection in wireless ad hoc networks. In: Proc. of the 2006 Workshop on Game Theory for Communications and Networks. 2006. [doi: 10.1145/1190195.1190198]

[11] Scalable simulation framework. http://www.ssfnet.org/homePage.html

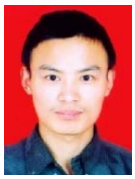
[12] University of Oregon route views project. http://www.routeviews.org

[13] Mckelvey, Richard D, Mclennan. Gambit: Software tools for game theory. Version 0.2007.01.30. 2007. http://www.gambit-project.org

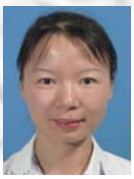
[14] Gibbons R. A Primer in Game Theory. Financial Times Prentice Hall, 1992.

附中文参考文献:

[8] 姜伟,方滨兴,田志宏,张宏莉.基于攻防博弈模型的网络安全测评和最优主动防御.计算机学报,2009,32(4):817−827.



刘玉岭(1982—),男,山东济南人,博士生,主要研究领域为网络安全,绩效评估.



吴丽辉(1974—),女,博士,主要研究领域为网络安全.

冯登国(1965—),男,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为网络与系统安全.

连一峰(1974—),男,博士,副研究员,主要研究领域为网络安全,绩效评估.