应用部分马尔科夫博弈的网络安全主动响应决策模型

胡鹤[1]，胡昌振[2]，姚淑萍[2]
(1.北京理工大学机电学院，100081，北京；2.北京理工大学软件学院，100081，北京)

摘要：针对传统被动响应模型滞后于攻击且频繁误警和虚警导致不当响应的问题，提出一种基于部分马尔科夫博弈(POMG)的主动响应决策模型. 该模型针对入侵过程生成入侵状态转换图，并根据攻击过程中得到的观察事件匹配入侵状态转换图，在考虑状态不确定的情况下确定系统信念状态. 将概率值超过信念状态阈值的状态作为初始节点生成入侵状态转换子图，根据子图的入侵过程确定攻防策略集，最终利用POMG算法选择最优主动响应策略. 实验结果表明，基于POMG的主动响应模型较映射型模型响应速度快67%，平均响应效率高24.5%.

关键词：主动响应；入侵状态转换图；部分马尔科夫博弈；信念状态
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2011)04-0018-07

Decision Model of Optimal Active Response for Network Security Using Partial Observable Markov Game

HU He[1], HU Changzhen[2], YAO Shuping[2]
(1. School of Mechatronical Engineering, Beijing Institute of Technology, Beijing 100081, China;
2. School of Software, Beijing Institute of Technology, Beijing 100081, China)

Abstract: Aiming at the problem that the traditional passive response model lags behind the attacks, and false alarms and missed alarms frequently lead to inappropriate responses, an active response decision-making model based on partial Markov game (POMG) is proposed. The model generates the attack state transmission graph according to the invasion processes. During the invasions, the model determines the system's belief states based on the observations of events so that the attacks are mapped to the nodes of the attack state transmission graph, considering the attacker and the uncertainty of system states. The sub-graphs of the attack state transmission graph are created, in which the belief state value of each sub-graph's initial node is over the belief state threshold. The attack and defense strategy sets are determined according to the invasion process of sub-graphs. The model generates the decision of the optimal active response policies according to POMG algorithm in the end. Experimental results show that the response speed of the active response model based on POMG is 67% faster than the map-based model, and the average response efficiency of the proposed model is 24.5% higher than the map-based model.

Keywords: active response; attack state transmission graph; partial observable Markov game; belief state

收稿日期：2010-07-15. 作者简介：胡鹤(1983—)，女，博士生；胡昌振(联系人)，男，教授，博士生导师. 基金项目：国家"863计划"资助项目(2009AA01Z433).
网络出版时间：2010-01-10 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20110110.0856.003.html

主动响应系统的目标是通过态势感知、风险评估和安全检测等手段对当前网络安全态势进行判断,并根据判断结果实施网络主动防护的安全防护体系[1]. 基于态势感知的主动响应能帮助管理员预先识别网络系统脆弱性以及面临的潜在安全威胁,根据安全需求来选取符合最优成本效益的主动响应策略. 在主动响应研究中,文献[2-4]提出通过入侵检测系统自身的误报率和以往响应方式成功率来自动调整响应映射,减少了误响应和重复报警导致的响应,但该方法响应对象是孤立的攻击动作,不能制定针对攻击过程的响应方案. 文献[5-6]提出一种基于系统收益的入侵响应与容忍的模型,使用攻击图描述系统可能的入侵路径,根据入侵可能造成系统的损失和响应代价选择响应措施,但仅从系统的角度考虑系统利益的最大化,没有将攻击者的因素纳入到模型中. 文献[7-8]使用随机博弈对系统中的攻防关系进行描述和推理,验证了博弈理论对入侵检测和响应的适用性,并使用攻击图描述攻击者的攻击意图和策略,该算法充分发挥了攻击图在进行攻击意图描述方面以及博弈理论在处理攻击者和系统的收益、偏好和策略变化方面的优势,但没有考虑系统状态的不确定性.

本文提出一种基于部分马尔科夫博弈(POMG)的主动响应模型,包括入侵状态转换图和最优响应策略的选取算法,其中基于 POMG 的最优主动响应策略的选取算法为本文研究的重点.

1　主动响应决策模型概述

1.1　模型相关定义

定义 1　入侵状态转换图. 入侵状态变化的有向图,记为一个 4 元组 $G=(S,S_I,S_F,E)$,其中 S 为状态集,包括主机与设备的安全状态,$S_I\subseteq S$ 为初始状态集合,$S_F\subseteq S$ 为目标状态集合,$E\subseteq S\times S$ 是边集,表示状态之间的转移关系. 从初始状态开始,一次攻击的成功作为下一次攻击行为的前提,直至达到攻击目标.

定义 2　有向边. 入侵状态转换图中连接 2 个状态节点的有向边,为攻击者引起状态改变采取的单一攻击行为,如权限提升、漏洞增加等,记为 $e=(a,v,q(s'|s,a))$,其中 a 为攻击的操作,v 为该攻击所依赖的漏洞的标识,$q(s'|s,a)\in[0,1]$为攻击从状态 s 转换到状态 s'的可能性,表示攻击成功的概率.

定义 3　攻击策略. 在状态 s_i 下,攻击策略为入侵者从状态 s_i 开始成功实现攻击目标引起的状态变迁过程,为 $p=\{s_i,\cdots,s_g\}(s_i\in S,s_g\in S_F)$.

定义 4　信念状态. 系统可能处于的所有的状态集合,以及在该集合上的概率分布,记为 l 维的信念状态向量 $\boldsymbol{B}=\{b(s_1),b(s_2),\cdots,b(s_l)\}$,其中 $b(s_i)$为攻击处于状态 s_i 的概率,$l=|S|$为状态空间的维数. 令 $v_i=b(s_i)$,则 $v_i\in[0,1]$, 且 $\sum_{i=0}^{l-1}[v_i]=1.0$.

1.2　模型结构

基于 POMG 的主动响应决策模型分为 2 层,包括态势感知层和策略选择层. 态势感知层生成入侵状态转换图,模拟攻击者入侵网络的所有可能路线,根据观察事件估计当前系统信念状态;策略选择层根据当前系统信念状态进行状态求精,确定攻防策略集,利用 POMG 理论确定攻击意图和最优模糊策略. 模型框架如图 1 所示.

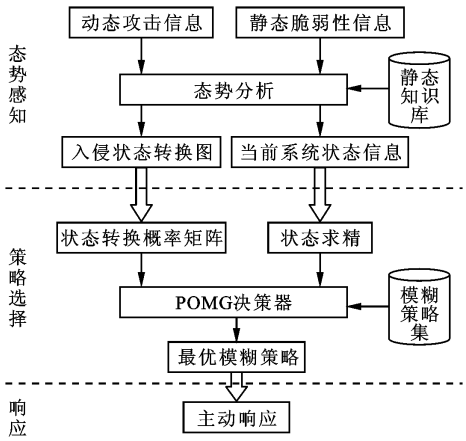

图 1　网络安全主动响应决策模型框图

2　基于 POMG 的策略选择模型

2.1　策略选择模型的描述

根据图 1 中模型策略选择层的功能和结构,将基于 POMG 的策略选择模型用 7 元组来描述,记为 $\Omega=(S,A,Q,R,O,Z,\Theta)$,其中:$S=\{s_0,s_1,\cdots,s_g\}$为系统的状态集;$A=\{A_a,A_d\}$为攻防双方的策略集,$A_a=\{a_1,a_2,\cdots,a_m\}$为攻击方的策略集,$A_d=\{d_1,d_2,\cdots,d_n\}$为系统的策略集;$Q$ 为状态转换函数集,每一个状态转换函数 $q(s'|s,a)\in[0,1]$对应入侵状态转换图中的每条有向边;R_i, $\forall i\in\{a,d\}$, $SA_i\to R_i$ 为参与人 i 的收益函数;$O=\{o_1,o_2,\cdots,o_w\}$为一个有限的观察事件集,每个观察事件 o_i 是状态的不完全反应;Z 为系统的观察函数集,每个观察函数 $z(o|s_i)$表示系统于状态 s_i 观察到 o 的概率;Θ 为参数集,包括观察符合度阈值 λ 和信念状态阈值 θ.

2.2 POMG 理论分析

主动响应由系统获得的观察事件来驱动，需要完成信念更新和策略选择[9]. 系统根据获得的观察事件确定入侵行为，进行信念状态更新. 以 $B'=\tau(\boldsymbol{B},o)$ 表示在信念状态 $\boldsymbol{B}$ 下得到观察 o 后的信念状态. 定义观察 o 与当前信念状态 $\boldsymbol{B}$ 的符合度为

$$W(\boldsymbol{B},o)=\sum_{s\in S}z(o\left|s\right.)b(s) \tag{1}$$

符合度表示观察 o 与目标系统的相关性和可信度，当 $W(\boldsymbol{B},o)\geqslant\lambda$ 时，认为当前对环境状态的估计与得到的观察事件 o 是一致的. 防护方根据观察事件 o 更新信念状态[10]. 设 $b(s)\in B,b'(s)\in B'$，则信念状态 $\boldsymbol{B}$ 下执行动作 a 并得到观察 o 时，可由贝叶斯理论得

$$b'(s)=\frac{z(o\left|s\right.)\sum\limits_{s'\in S}b(s')q(s\left|s',a\right.)}{\sum\limits_{o'\in O}z(o'\left|s\right.)\sum\limits_{s'\in S}b(s')q(s\left|s',a\right.)} \tag{2}$$

攻击策略集由用攻击状态转换图的子图确定. 攻击子图包括初始状态 s_i 及所有子节点，记为 D，$D\subseteq G$. D 的初始节点为 $s_i\in S$，满足

$$b(s_i)\geqslant\theta \tag{3}$$

式中：θ 为信念状态阈值. θ 的设定关系到预测算法的准确性：θ 值过大，会降低响应的主动性；θ 值过小，会提高误响应率. 策略 p 在状态 s_i 下的收益函数为

$$R_p(s_i)=R(s_i,a_p)+\sum_{s_j\in S}q(s_j\left|s_i,a_p\right.)R_{p-a_p}(s_j) \tag{4}$$

式中：a_p 为当前策略的根节点指定的动作；$q(s_j\left|s_i,a_p\right.)$ 为在 a_p 作用下系统由状态 s_i 转换到 s_j 的概率；$p-a_p$ 为策略 p 在第一个节点之后的剩余计划；$R_{p-a_p}(s_j)$ 为在状态 s_j 下剩余策略 $p-a_p$ 的收益函数[11].

系统状态具有不确定性，故根据系统所有可能状态，取在该状态下执行策略 p 时对应收益的数学期望，得到在信念状态 $\boldsymbol{B}$ 下策略 p 的收益函数为

$$R_p(b)=\sum_{s\in S}b(s)R_p(s) \tag{5}$$

攻防双方的收益函数集合可用一个矩阵表示，如当攻防策略数均为 3 时，收益函数矩阵可表示为

$$\boldsymbol{R}=\begin{bmatrix}R_{11}^{\mathrm{a}},R_{11}^{\mathrm{d}} & R_{12}^{\mathrm{a}},R_{12}^{\mathrm{d}} & R_{13}^{\mathrm{a}},R_{13}^{\mathrm{d}}\\ R_{21}^{\mathrm{a}},R_{21}^{\mathrm{d}} & R_{22}^{\mathrm{a}},R_{22}^{\mathrm{d}} & R_{23}^{\mathrm{a}},R_{23}^{\mathrm{d}}\\ R_{31}^{\mathrm{a}},R_{31}^{\mathrm{d}} & R_{32}^{\mathrm{a}},R_{32}^{\mathrm{d}} & R_{33}^{\mathrm{a}},R_{33}^{\mathrm{d}}\end{bmatrix} \tag{6}$$

式中：每组元素 $(R_{ij}^{\mathrm{a}},R_{ij}^{\mathrm{d}})$ 分别为响应策略 p_j^{d} 对攻击策略 p_i^{a} 执行后攻击者和防御者的收益，如表示响应策略 p_3^{d} 对攻击策略 p_2^{a} 执行后攻防双方的收益分别为 R_{23}^{a} 和 R_{23}^{d}.

令攻防双方的混合策略分别为 $A_{\mathrm{a}}=\{a_1,a_2,\cdots,a_m\}$ 和 $A_{\mathrm{d}}=\{d_1,d_2,\cdots,d_n\}$ 的概率分布为 $p_{\mathrm{a}}=(p_{\mathrm{a}1},p_{\mathrm{a}2},\cdots,p_{am})$ 和 $p_{\mathrm{d}}=(p_{\mathrm{d}1},p_{\mathrm{d}2},\cdots,p_{\mathrm{d}n})$，且满足 $0\leqslant p_{ai}\leqslant 1,0\leqslant p_{\mathrm{d}j}\leqslant 1$，且 $\sum\limits_{i=1}^{m}p_{ai}=1,\sum\limits_{j=1}^{n}p_{\mathrm{d}j}=1$，则攻防双方的期望收益分别用下式计算

$$R_{\mathrm{a}}(p_{\mathrm{a}},p_{\mathrm{d}})=\sum_{i}^{m}p_{ai}\Big[\sum_{j}^{n}p_{\mathrm{d}j}R_{\mathrm{a}}(a_i,d_j)\Big] \tag{7}$$

$$R_{\mathrm{d}}(p_{\mathrm{a}},p_{\mathrm{d}})=\sum_{j}^{n}p_{\mathrm{d}j}\Big[\sum_{i}^{m}p_{ai}R_{\mathrm{d}}(a_i,d_j)\Big] \tag{8}$$

根据混合策略纳什均衡[7]，得到混合均衡策略 $(p_{\mathrm{a}}^*,p_{\mathrm{d}}^*)$，即满足

$$\forall\, p_{\mathrm{a}},R_{\mathrm{a}}(p_{\mathrm{a}}^*,p_{\mathrm{d}}^*)\geqslant R_{\mathrm{a}}(p_{\mathrm{a}},p_{\mathrm{d}}^*) \tag{9}$$

$$\forall\, p_{\mathrm{d}},R_{\mathrm{d}}(p_{\mathrm{a}}^*,p_{\mathrm{d}}^*)\geqslant R_{\mathrm{d}}(p_{\mathrm{a}}^*,p_{\mathrm{d}}) \tag{10}$$

2.3 策略选择模型的实现

策略选择模型的实现步骤如下：

(1)初始化入侵状态转换图 $G=(S,S_{\mathrm{I}},S_{\mathrm{F}},E)$；

(2)根据获得的观察 o，利用式(1)计算 o 与信念状态的符合度 $W(B,o)$；

(3)当 $W(B,o)\geqslant\lambda$ 时，利用式(2)更新信念状态；

(4)确定系统最可能处于的状态集 S_b，即 $\forall\, s_i\in S_b,b(i)\geqslant\theta$；

(5)生成入侵状态转换子图 $D\subseteq G$，包含节点集 S_b 及其所含节点的子结点；

(6)构建攻击策略集合 $A_{\mathrm{a}}=\{a_1,a_2,\cdots,a_m\}$ 和响应策略集合 $A_{\mathrm{d}}=\{d_1,d_2,\cdots,d_n\}$；

(7)利用式(5)对每一个 $a_i\in A_{\mathrm{a}},d_j\in A_{\mathrm{d}}$ 计算攻防双方在当前信念状态下的值函数 R_{ij}^{a} 和 R_{ij}^{d}；

(8)利用式(6)生成攻防策略的 $m\times n$ 维收益矩阵 $\boldsymbol{R}$；

(9)调用混合策略均衡求解算法，确定攻击意图和最优主动响应策略.

2.4 策略选取算法复杂性分析

基于 POMG 主动响应策略是在入侵过程中动态生成的，故响应必须满足实时性来确保及时适应环境变化. 设 T_{B} 为更新信念分布的时间，T_{S} 为选择策略的时间. 在最坏情况下，一次响应决策所耗费的时间为

$$T_{\mathrm{R}}=T_{\mathrm{B}}+T_{\mathrm{S}} \tag{11}$$

若更新信念分布的时间复杂度为 $O(|S|)$，计

算收益函数的复杂度为 $O(|A||S|^2)$[9],因此通常情况下执行一次主动响应决策的时间复杂度为 $O(|A||S|^2)$,这使得主动响应决策的时间复杂度是多项式级别的,保证了系统运行时的实时性. 然而,观察事件的数目随系统监控子网的规模增大而增加,并发的观察事件过多将导致系统不能处理新的观察事件,因而需要依据 IP 地址的多层次特征划分建立模型的空间[12],在每个 C 类子网中设置代理,建立基于 POMG 的主动响应决策模型.

3　实验与仿真

3.1　实验环境的建立

为验证基于 POMG 主动响应决策模型的有效性,搭建实验网络,其中外部网和各自楼层交换机管理一个 C 类子网,如图 2 所示.

将外部网划分管理域[13](D_1,D_2,D_3,D_4),如图 3 所示. 在图 3 中:D_1 为非军事区;D_2 和 D_3 内的所有主机可访问 D_1 内的 Mail 服务器、VPN 服务器和 Web 服务器;除 D_4 内的主机 H_{10} 和 D_3 的主机 H_9 能访问 D_2 的 SQL 服务器外,限制其他主机对 D_2 的访问;D_4 内的主机 H_{10} 能访问 D_3 内的服务器 H_7;IDS 负责监控各自域内的网络攻击事件,提供实时的攻击数据.

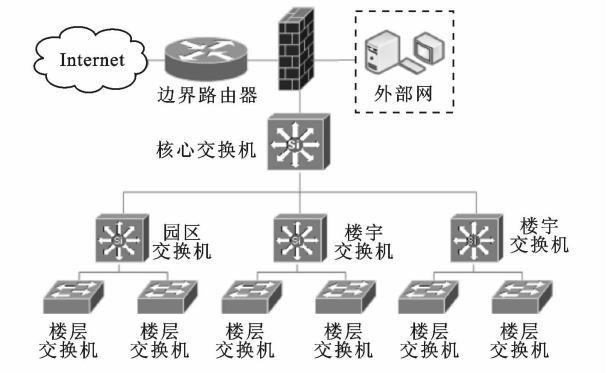

图 2　网络实例拓扑

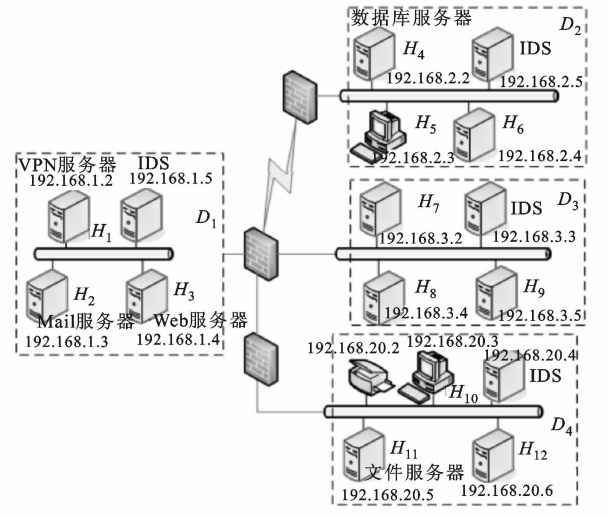

图 3　外部网管理域

对图 3 主机进行弱点分析,得到对应的弱点信息如表 1 所示.

表 1　主机信息

主机	操作系统和应用程序	漏洞编号
H_1	Check Point VPN-1 Server 4.1	CVE-2004-0040
H_2	Windows 2003 server, IIS 5.0 web server	CVE-2002-0364 CVE-2006-2379
H_3	Windows 2000	CVE-2001-0504
H_4	Windows XP, SQL	CVE-2004-1306 CVE-2004-0893 CVE-2003-0004
H_7	Windows 2000	CVE-2007-0038
H_8	Windows XP	CVE-2006-2370
H_9	RedHat Linux 9.0	CVE-2003-0252
H_{10}	Windows 2003	CVE-2004-0897
H_{11}	Windows 2003 server, Titan FTP server 6.0.3	CVE-2004-0575 CVE-2008-0702

3.2　入侵状态转换图的生成

依据图 3 中关联网络配置信息和已知攻击行为规则,找出可利用的所有攻击行为,如表 2 所示.

表 2　可利用的攻击行为

符号	攻击名称
a_1	Checkpoint VPN buffer overflow
a_2	IIS buffer overflow
a_3	Remote command
a_4	httpd remote buffer overflow
a_5	sshd remote buffer overflow
a_6	Indexing Service remote buffer overflow
a_7	local buffer overflow

从响应策略库选出可用的响应策略信息,并考虑无响应措施的情况. 实验中响应策略集 $Q=\{q_1,q_2,q_3,q_4,q_5,q_6\}$,各响应策略分别为{安装 VPN-1 Server 补丁,安装 IIS 补丁,暂停 Mail Server 服务,安装 SQL Server 补丁,取消 suid_root,不采取响应措施}. 根据攻击者在域间主机中攻击状态的转换关系,可得到入侵状态转换图 G,如图 4 所示.

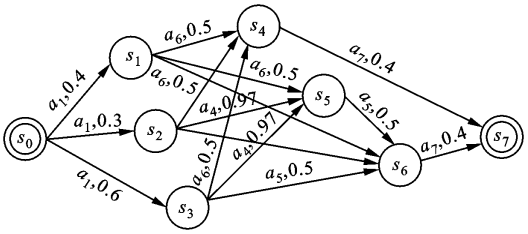

图 4 攻击状态转换图

3.3 攻击意图和最优响应策略决策

初始信念状态为 $B=\{1,0,0,0,0,0,0\}$. 利用攻击行为 a_1 对实验网络进行攻击，某时刻得到 DMZ 域的 IDS 报警，记为观察 o_1. 设 $\lambda=0.2$ 且 $\theta=0.65$，依据式(1)计算符合程度 $W(\boldsymbol{B},o_1)=0.6>\lambda$，说明观察与信念状态 $\boldsymbol{B}$ 吻合. 更新信念状态 $B_1=\{0,0.77,0.05,0.05,0.2,0,0\}$，$b(s_1)=0.77$，大于设定的 θ 阈值 0.65，得到子图 D 如图 5 所示.

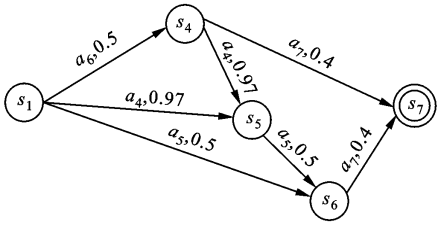

图 5 攻击状态转换子图

分析图 5 中存在的 4 条可能的攻击策略，如表 3 所示.

表 3 攻击策略

符号	攻击策略
p_1	$s_1\rightarrow s_4\rightarrow s_7$
p_2	$s_1\rightarrow s_4\rightarrow s_5\rightarrow s_6\rightarrow s_7$
p_3	$s_1\rightarrow s_5\rightarrow s_6\rightarrow s_7$
p_4	$s_1\rightarrow s_6\rightarrow s_7$

依据式(4)和式(5)计算每一对攻防策略的代价[14-15]，可得到 POMG 攻防策略的收益矩阵为

$$\boldsymbol{R}=$$

	q_1	q_2	q_3	q_4	q_5	q_6
p_1	410,180	760,270	870,150	670,170	730,180	550,0
p_2	410,180	760,270	870,170	630,170	630,170	550,0
p_3	650,380	650,210	730,130	870,290	970,210	890,0
p_4	650,340	630,340	760,160	870,280	970,210	890,0

依据式(7)和式(8)求解上述矩阵建立的攻防双方混合策略时的纳什均衡，得到其纳什均衡结果 $p=\left(\frac{67}{159},0,\frac{92}{159},0\right)$，$q=\left(\frac{28}{53},0,0,0,0,\frac{25}{53}\right)$，即最优攻击策略为攻击者分别以概率 $\frac{92}{159}$ 和 $\frac{67}{159}$ 选择攻击策略 p_3 和 p_1，最优响应策略为防护方分别以概率 $\frac{28}{53}$ 和 $\frac{25}{53}$ 选择响应策略 q_1 和 q_6.

为评估模型的准确率，定义误响应率 F_w 为阻止的合法连接数 N_L 占总响应数 N_R 的比重，即

$$F_w=\frac{N_L}{N_R} \tag{12}$$

修改阈值 θ 的大小，计算系统的误响应率随阈值大小的变化，如图 6 所示.

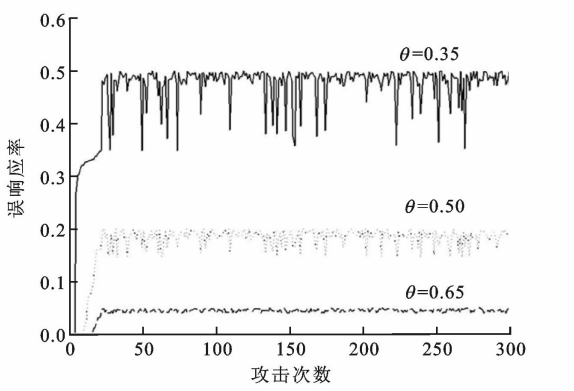

图 6 阈值的设定对误响应率的影响对比

从图 6 中可以发现：$\theta=0.35$ 时，误响应率较高(50%)，且波动较大；$\theta=0.5$ 时，误响应率接近 20%，波动相对较小；$\theta=0.65$ 时，误响应率稳定地趋于 5%. 这是因为阈值 θ 取 0.65 时能实现攻击状态的匹配，同时避免了大多数误响应.

3.4 响应结果对比

定义响应效率为

$$E_R=1-\frac{R_L}{R_M} \tag{13}$$

式中：R_L 表示响应后入侵给系统带来的残余损失；R_M 表示攻击的总损失[14].

针对单次攻击对映射型响应模型[4]和基于 POMG 的主动响应模型进行了 3 组对比实验. 根据图 4 选取攻击策略 $p_5\{s_0,s_1,s_4,s_7\}$，$p_6\{s_0,s_2,s_5,s_6,s_7\}$ 和 $p_7\{s_0,s_3,s_6,s_7\}$ 对系统进行攻击，得到不同响应模型的响应结果如表 4 所示.

响应结果表明，基于 POMG 的主动响应模型能在攻击刚发生时将其阻止(攻击被阻止的状态分别为 s_1、s_2 和 s_3)，优于映射型的响应模型，系统收益和响应效率高于映射型. 同时，其响应时间比映射型快 67%，响应更迅速.

表 4　单次响应效果对比

模型	攻击策略	系统收益	攻击被阻止的状态	响应效率/%	响应时间/s
映射	p_5	443	s_4	43.4	538
	p_6	286	s_6	48.1	1441
	p_7	323	s_6	42.2	956
POMG	p_5	606	s_1	41.2	245
	p_6	572	s_2	78.4	351
	p_7	587	s_3	66.7	372

实验中外网主机和内网主机间共有连接 18 215 条，含 199 次外网对内网的攻击，其余都是合法连接. IDS 共发出了 236 次报警，针对真实的攻击报警有 161 次，在这 161 次报警中重复报警 40 次，有 25 次攻击未检测到. 依据映射型和基于 POMG 响应模型的算法进行响应，结果如表 5 所示.

表 5　响应结果对比

模型	阻止攻击数	响应率/%	误响应率/%	总收益	平均响应效率/%	平均响应时间/s
映射	130	80.7	2.8	6 991	42.9	749.1
POMG	145	90.1	4.3	12 916	67.4	293.4

表 5 中基于映射型的响应由于没有充分考虑入侵过程，系统响应率较低(80.7%)，而且平均响应效率较低(42.9%)；基于 POMG 的响应，由于每次都将系统的模糊状态、攻击者的后继动作以及系统响应措施的收益纳入博弈理论进行理性分析，在确保系统收益最大时响应，因此系统的响应率较高(90.1%)及平均响应效率较高(67.4%)，且系统的总体收益较高(12 916). 由于算法引入 了状态的不确定性，因此虽然避免了大多数误响应，但 POMG 模型的误响应率(4.3%)仍比映射型模型的误响应率(2.8%)要高.

4　结束语

本文提出了一种基于 POMG 的主动响应决策模型. 在借鉴攻防博弈模型对网络安全攻防建模的基础上，利用入侵状态转换图确定攻防策略集，且针对系统存在状态信息不完全问题，引入信念状态空间到决策系统中，考虑了系统状态的不确定性. 实验结果证明，基于 POMG 的模型能在响应代价较小的情况下提高响应速度和处理能力，并能避免大多数误响应. 下一步工作的重点是研究各子网响应代理间的信息交互，分析外部攻击事件对子网内部环境的影响，建立子网协同响应机制.

参考文献：

[1] 张永铮，方滨兴，迟悦，等. 用于评估网络信息系统的风险传播模型 [J]. 软件学报，2007，18(1)：137-145.
ZHANG Yongzheng，FANG Binxing，CHI Yue，et al. Risk propagation model for assessing network information systems [J]. Journal of Software，2007，18(1)：137-145.

[2] CARVER C，HILL J M，SURDU J R. A methodology for using intelligent agents to provide automated intrusion response [C]// Proceedings of the 2000 IEEE Workshop on Information Assurance and Security. Los Alamitos，CA，USA：IEEE Computer Society，2000：110-116.

[3] RAGSDALE D，CARVER C，HUMPHRIES J，et al. Adaptation techniques for intrusion detection and intrusion response system [C]// The IEEE International Conf on Systems，Man，and Cybernetics. Los Alamitos，CA，USA：IEEE Computer Society，2000：2344-2349.

[4] MUSMAN S，FLESHER P. System of security managers' adaptive response tool [C]// Proceedings of DARPA Information Survivalability Conference and Exposition. Los Alamitos，CA，USA：IEEE Computer Society，2000：56-68.

[5] FOO Bingrui，WU Yusung，MAO Yuchun，et al. ADEPTS：adaptive intrusion response using attack graphs in an E-commerce environment [C]// Proceedings of the 2005 International Conference on Dependable Systems and Networks. Los Alamitos，CA，USA：IEEE Computer Society，2005：508-517.

[6] WU Yusung，FOO Bingrui，MAO Yuchun，et al. Automated adaptive intrusion containment in systems of interacting services [J]. Computer Networks，2007，5(51)：1334-1360.

[7] LYE K W，WING M J. Game strategies in network security [J]. International Journal of Information Security，2005，4(1/2)：71-86.

[8] 石进，郭山清，陆音，等. 一种基于攻击图的入侵响应方法 [J]. 软件学报，2008，19(10)：2746-2753.
SHI Jin，GUO Shanqing，LU Yin，et al. An intrusion response method based on attack graph [J]. Journal of Software，2008，19(10)：2746-2753.

[9] 张波. 不确定情形下的规划及行动：理论与应用 [D]. 合肥：中国科学技术大学计算机科学与技术学院，2001.

[10] 王伟，陈秀真，管晓宏，等. 深度防卫的自适应入侵检测系统 [J]. 西安交通大学学报，2005，39(4)：339-346.
WANG Wei，CHEN Xiuzhen，GUAN Xiaohong，et al. Defense-in-depth adaptive intrusion detection system [J]. Journal of Xi′an Jiaotong University，2005，39(4)：339-346.

[11] 李响，陈小平. 一种动态不确定性环境中的持续规划系统[J]. 计算机学报，2005，7(28)：1163-1170.
LI Xiang，CHEN Xiaoping. A real-time planning system in dynamic nondeterministic environments [J]. Chinese Journal of Computers，2005，7(28)：1163-1170.

[12] 安喜锋，李伟华，刘尊，等. 网络安全协同防卫系统研究与实现[J]. 西安交通大学学报，2008，42(12)：1495-1499.
AN Xifeng，LI Weihua，LIU Zun，et al. Research and implementation of network security cooperative defense system [J]. Journal of Xi′an Jiaotong University，2008，42(12)：1495-1499.

[13] 韩宗芬，陶智飞，杨思睿，等. 一种基于自治域的协同入侵检测与防御机制[J]. 华中科技大学学报：自然科学版，2006，12(34)：53-55.
HAN Zongfen，TAO Zhifei，YANG Sirui，et al. Cooperative intrusion protection based on security zone [J]. Journal of Huazhong University of Science and Technology：Nature Science Edition，2006，12(34)：53-55.

[14] LEE W，FAN W，MILLER M，et al. Toward cost-sensitive modeling for intrusion detection and response [J]. Journal of Computer Security，2002，10(1/2)：5-22.

[15] WANG L，ISLAM T，LONG T，et al. An attack graph-based probabilistic security metric [J]. Lecture Notes in Computer Science，2008 (5094)：283-296.

[本刊相关文献链接]

网络安全协同防卫系统研究与实现. 西安交通大学学报，2008，42(12)：1495-1499.

面向变异分析的协议安全测试方法. 西安交通大学学报，2009，43(12)：11-15.

无线局域网自适应安全管理框架及其应用. 西安交通大学学报，2010，44(4)：34-38.

基于隐马尔可夫模型的无线局域网媒体接入控制层入侵检测方法. 西安交通大学学报，2009，43(12)：26-30.

可废除并发签名机制. 西安交通大学学报，2009，43(12)：45-49.

一种新的动态批密钥更新算法. 西安交通大学学报，2009，43(12)：65-69.

无线局域网802.1X协议安全性分析与检测. 西安交通大学学报，2009，43(10)：52-55.

基于随机密钥预分布模型的安全定向扩散协议. 西安交通大学学报，2007，41(12)：1423-1426.

一种新型的分布式隐私保护计算模型及其应用. 西安交通大学学报，2007，41(8)：954-958.

一种修复网络拓扑的Steiner树移动控制算法. 西安交通大学学报，2011，45(2)：39-43.

一种信号强度感知的Ad Hoc网络节点移动控制算法. 西安交通大学学报，2011，45(2)：107-110.

可演化网络中移动代理的性能分析及优化方法. 西安交通大学学报，2010，44(12)：5-9.

一种高吞吐量的无线传感器网络多信道MAC协议. 西安交通大学学报，2010，44(12)：32-37.

PPTL模型检测器实现的一个关键技术. 西安交通大学学报，2010，44(10)：24-29.

传感器数据中事件样本与错误样本的系统化区分框架. 西安交通大学学报，2010，44(10)：30-35.

一种改进的加权质心定位算法. 西安交通大学学报，2010，44(8)：1-4.

面向服务级别协议的核实与规划服务质量系统框架研究. 西安交通大学学报，2010，44(6)：1-5.

使用交叉熵检测和分类网络异常流量. 西安交通大学学报，2010，44(6)：10-15.

采用离散粒子群算法的网格任务安全级调度. 西安交通大学学报，2010，44(6)：21-26.

无线传感器网络多轮任务调度算法. 西安交通大学学报，2010，44(6)：27-32.

利用蚁群优化的非均匀分簇无线传感器网络路由算法. 西安交通大学学报，2010，44(6)：33-38.

针对事件驱动型传感器网络的多路径编码路由协议. 西安交通大学学报，2010，44(6)：39-45.

面向移动节点不确定性特征的自组网路由协议. 西安交通大学学报，2010，44(6)：46-50.

分层信标驱动的无线Mesh网多播差错控制协议. 西安交通大学学报，2010，44(6)：51-56.

利用服务质量参数值预测的Web服务选择方法. 西安交通大学学报，2010，44(6)：57-61.

多P2P覆盖网络的带宽分配方法. 西安交通大学学报，2010，44(4)：5-8.

面向信息系统的生存性恢复机制. 西安交通大学学报，2010，44(4)：18-22.

基于状态机的802.1X协议攻击检测方法. 西安交通大学学报，2010，44(4)：52-56.

一种支持大规模应用层组播的混合拓扑覆盖网络. 西安交通大学学报，2010，44(2)：11-14.

（编辑　刘杨）