DOI:10.11918/202405063

Markov 改进演化博弈评估 ICPS 的动态风险

孙 奕[1],孙子文[1,2]

(1.江南大学 物联网工程学院,江苏 无锡 214122; 2.物联网技术应用教育部工程研究中心,江苏 无锡 214122)

摘 要:为评估网络攻击下工业信息物理系统(ICPS)的动态风险,研究 Markov 改进演化博弈模型。根据 ICPS 中各个漏洞节点,设计从信息域到物理域的系统攻防状态转移图,为 Markov 改进演化博弈分析提供依据。首先,在单阶段攻防过程中,研究加入参数机制的攻防演化博弈模型,求解拥有不同理性程度和探索程度的攻防主体博弈后的收益。其次,在多阶段攻防中,根据单阶段攻防博弈模型,引入转移概率和折现因子,根据攻防状态转移图求解不同漏洞节点的攻击收益,实现对多阶段攻防对抗的动态推演。最后,利用攻击收益大小对 ICPS 的动态风险进行评估。本研究分别进行了数值实验分析以及工业信息物理系统模型仿真,使用沸水发电厂作为仿真对象,通过 Matlab 对 Markov 改进演化博弈评估方法进行仿真,根据攻击收益评估 ICPS 的动态风险。结果表明,研究模型重视攻防双方的差异性,能依据攻防双方理性程度及探索程度的不同,合理求出 ICPS 中攻击者的收益,为 ICPS 遭受网络攻击下的动态风险评估提供理论基础,对提高工业信息物理系统的安全性提供重要参考依据。

关键词:工业信息物理系统(ICPS);演化博弈;Markov 决策;攻击收益;系统评估

中图分类号:TP273 **文献标志码**:A **文章编号**:0367-6234(2025)04-0084-10

Assessment of dynamic risks in ICPS using Markov-improved evolutionary game theory

SUN Yi[1], SUN Ziwen[1,2]

(1. School of Internet of Things Engineering, Jiangnan University, Wuxi 214122, Jiangsu, China; 2. Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi 214122, Jiangsu, China)

Abstract: To evaluate the dynamic risks of industrial cyber-physical saystems (ICPS) under cyber attacks, this study investigates a Markov-improved evolutionary game model. Based on the vulnerability nodes within the ICPS, a system attack-defense state transition diagram from the information domain to the physical domain is designed, providing a foundation for the Markov-improved evolutionary game analysis. First, in the single-stage attack-defense process, an evolutionary game model incorporating a parameter mechanism is studied to determine the payoffs of attack and defense entities with varying degrees of rationality and exploration after the game. Second, in the multi-stage attack-defense process, based on the single-stage attack-defense game model, transition probabilities and discount factors are introduced. The attack payoffs of different vulnerability nodes are calculated according to the attack-defense state transition diagram, enabling dynamic deduction of multi-stage attack-defense confrontations. Finally, the dynamic risks of ICPS are assessed based on the magnitude of attack payoffs. This study conducts numerical experiments and simulations of an industrial cyber-physical system model, using a boiling water power plant as the simulation object. The Markov-improved evolutionary game evaluation method is simulated using Matlab, and the dynamic risks of ICPS are evaluated based on the attack payoffs. The results demonstrate that the proposed model emphasizes the differences between the attack and defense sides, reasonably calculates the attacker's payoffs in ICPS based on the varying levels of rationality and exploration of both parties. This provides a theoretical foundation for the dynamic risk assessment of ICPS under cyber attacks and offers significant reference value for enhancing the security of industrial cyber-physical systems.

Keywords: industrial cyber-physical systems (ICPS); evolutionary games; Markov decisions; attack benefits; system evaluation

信息物理系统(cyber-physical systems,CPS)将网络与物理紧密连接,具有通信、计算、远程协同控制等功能。近年来,随着计算机、通信、工业自动化控制等技术的进一步深度融合,CPS 被广泛运用于

收稿日期:2024-05-27;**录用日期**:2024-07-11;**网络首发日期**:2025-03-17
网络首发地址:https://link.cnki.net/urlid/23.1235.t.20250317.1436.008
基金项目:国家自然科学基金(61373126);中央高校基本科研业务费用专项资金(JUSRP51310A);江苏省自然科学基金(BK20131107)
作者简介:孙 奕(1999—),女,硕士研究生;孙子文(1968—),女,教授,博士生导师
通信作者:孙子文,sunziwen@jiangnan.edu.cn

工业环境,工业信息物理系统(industrial cyber-physical systems,ICPS)应运而生。ICPS 监督、控制和管理现实世界的物理基础设施,是构建现实世界网络化工业基础设施的核心[1]。然而,由于 ICPS 信息系统和嵌入式设备无线网络的结合,以及复杂多变的工业环境影响下,ICPS 容易受到网络攻击,进而造成巨大的损失[2]。合理评估网络攻击给 ICPS 造成的风险[3],可以帮助了解 ICPS 的安全状况,缓解网络攻击对 ICPS 造成的危害。

风险评估方法一般分为静态风险评估和动态风险评估。常见的静态风险评估利用攻击图和攻击树等方法对系统风险程度进行评估,文献[4]根据原子攻击概率结合贝叶斯攻击图建立静态风险评估;文献[5]采用基于对列车控制系统功能架构的攻击树建模对漏洞进行评估。静态风险评估方法大多缺乏灵活性和适应性[4-5],无法应对不同的风险场景和变化。相比之下,动态风险评估往往更灵活,可以根据实时数据和变化情况及时调整并更新应对策略。常见的动态风险评估利用 Petri 网和博弈论等方法对系统风险进行量化评估,文献[6]利用随机博弈 Petri 网对配电网进行风险评估;文献[7]使用基于动态攻击和防御的信息网络脆弱性威胁评估模型,实现对信息网络漏洞威胁的定量评估;文献[8]使用隐马尔可夫模型来评估网络安全风险;文献[9-10]分别利用 Stackelberg 博弈和演化博弈理论,研究拥有 3 个参与者的博弈,同时考虑了防御收益和服务效果,对策略进行了评估。但文献[6]对跨域攻击分析不够充分,对物理损失的定义过于简单;文献[7-9]对于攻防收益量化仅仅考虑 ICPS 遭受网络攻击后的信息损失,没有结合物理损失;文献[10]的研究仅建立在单阶段中的研究,而 ICPS 的攻防过程本质上是多阶段、多状态攻防对抗动态过程,研究 ICPS 动态风险不应就某一特定漏洞节点展开分析,而是要考虑到不同漏洞节点的关联性。

为解决跨域攻击和多阶段攻防博弈研究中的不足,本文改进复制动态方程[11-13],采用 Markov 改进演化博弈计算漏洞节点攻击收益,最终评估 ICPS 动态风险。

1　ICPS 动态风险评估框架

1.1　模型框架

ICPS 的结构通常分为:应用层、传输层和物理层。物理层和应用层之间通过传输层中各种网络协议和网关组件来传输数据信号,传输层包括传输网络和网络节点,主要负责应用层与物理层之间的数据交换和处理。

如图 1 所示沸水发电(boiling water power plant,BWPP)信息物理系统结构图,应用层包含应用服务器、数据库服务器、控制服务器等,物理层包含压力传感器 Se2、液位传感器 Se1、电流传感器 Se3、水位控制 PLC1、进料控制 PLC2、蒸汽排放控制 PLC3、进水阀 V1、进料阀 V2 以及排气阀 V3。

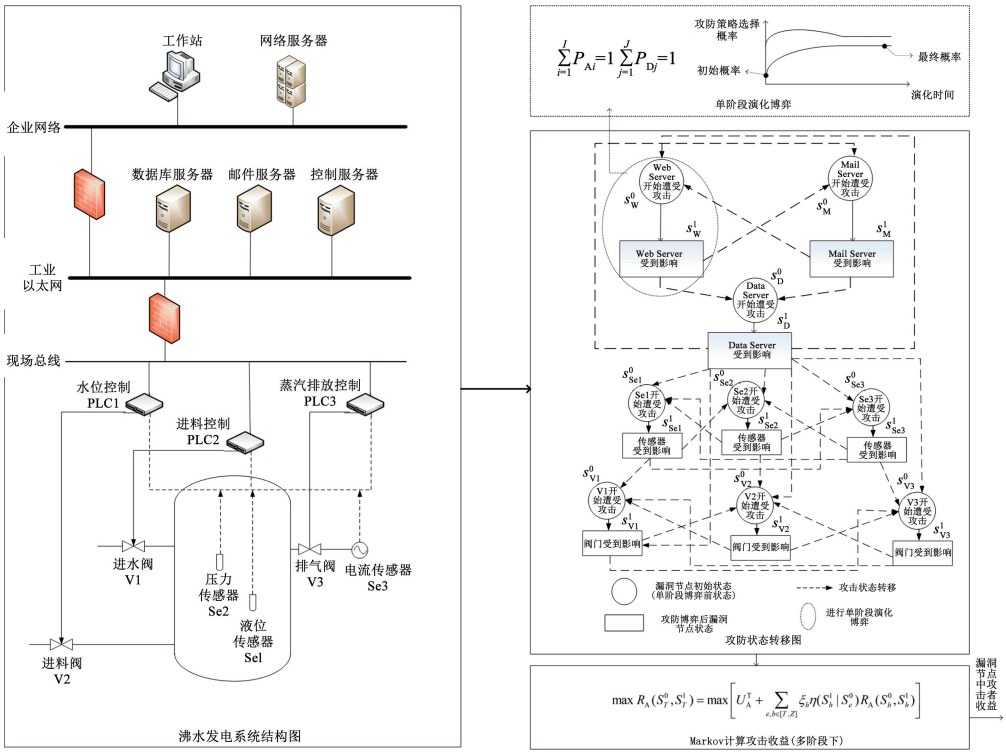

图 1　ICPS 动态风险评估框架

Fig. 1　ICPS dynamic risk assessment framework

为评估 ICPS 的动态风险,本文建立攻防博弈模型,该模型包含 3 个模块:1)攻防状态转移图模块。用以描述攻击者从信息域到物理域对漏洞节点进行跨域攻击行为的路径及跳转概率;2)单阶段演化博弈模块。设计了攻防双方基于不同理性与探索程度的改进演化博弈;3)Markov 计算攻击收益模块。在求出单阶段攻防双方收益的基础上,结合 Markov 决策,得到系统各个漏洞节点的攻击收益,最后通过攻击收益评估 ICPS 动态风险。

1.2 演化博弈

在 ICPS 演化博弈过程中,攻防双方能在一定时间内通过使用不同的策略到达演化平衡的状态,但是这种平衡状态往往会因为攻防双方博弈目标、策略偏好等的改变而被破坏。在 ICPS 中,攻击和防御行为通常是针对系统整体和不同类型节点的多阶段攻防,攻击者对于防御者信息的掌握通常相对有限,需要根据攻防收益对各个策略的选择概率做出调整,直到概率选择趋于稳定。

攻击者在漏洞节点之间的攻击选择过程可以分为单阶段和多阶段演化博弈两种情况。在单阶段演化博弈中,攻击者攻击一个漏洞节点并达到稳定状态。然而,攻击者通常不会满足于当前状态,而是会选择攻击周边的漏洞节点。这样,漏洞节点之间形成了联系,攻击者会进行多阶段演化博弈。在每个漏洞节点上,攻击者和防守者通过演化博弈过程寻找稳定状态。一旦稳定状态被打破,攻击者会以不同的概率跳转到下一个状态,继续演化博弈,这种过程会持续进行,从而形成多阶段的演化博弈[14]。此时系统处于不断“演化—跳变—演化”的动态过程见图 2。

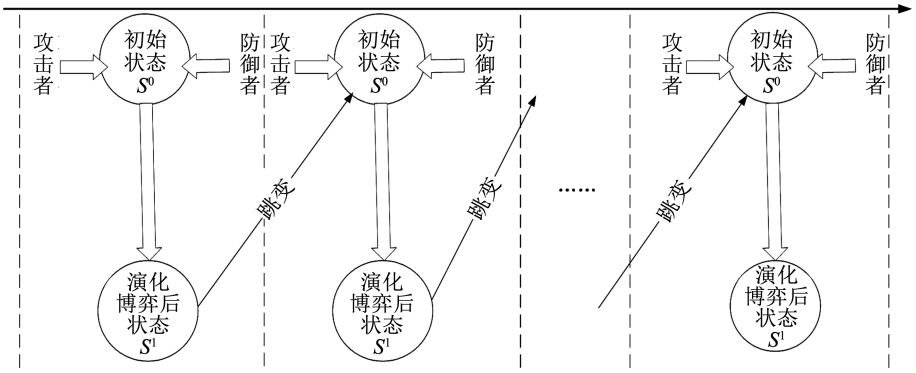

图 2 多阶段演化博弈过程

Fig. 2 Multi-stage evolutionary game process

2 博弈设计

2.1 博弈模型

定义 1 单阶段工业信息物理系统攻防演化博弈模型可以用一个四元组(Q,M,P,U)表示,其中:$Q=(Q_A,Q_D)$为参与者的集合(Q_A为攻击者集合,Q_D为防御者集合);$M=(M_A,M_D)$为博弈过程中的策略集(M_A为含有 I 个策略的攻击策略集,M_D为含有 J 个策略的防御策略集);$P=(P_{Ai},P_{Dj})$为博弈过程中攻防两方的策略概率集(P_{Ai}为攻击者选择第 i 个攻击策略的概率,P_{Dj}为防御者选择第 j 个防御策略的概率,$\sum_{i=1}^{I}P_{Ai}=1$,$\sum_{j=1}^{J}P_{Dj}=1$且$P_{Ai}\in[0,1]$,$P_{Dj}\in[0,1]$);$U=(U_A,U_D)$为博弈过程中的收益集(U_A为攻击者的收益集,U_D为防御者的收益集)。

2.2 信息域到物理域漏洞节点的攻防收益量化

用公共漏洞评分体系 2.0 定义可利用性 α 为

$$\alpha = 2 \times AV \times AC \times Au \tag{1}$$

式中:AV、AC、Au 分别为访问向量、访问复杂度和认证,量化方法见表 1。

表 1 可利用性决定因素量化表

Tab. 1 Quantitative table of determinants of availability

决定因素	度量指标	量化数值
AV	Local/Adjacent/Network	0.395/0.646/1.000
AC	High/Medium/Low	0.35/0.61/0.71
Au	Multiple/Single/None	0.450/0.560/0.704

参考文献[7-9],结合漏洞的特点和 ICPS 的框架构建不同漏洞攻击下攻防收益矩阵,见表 2。表中:A_{profit}为攻击者在漏洞成功攻击后的获益,A_{cost}为攻击者利用漏洞攻击所付出的成本,D_{profit}为防御者在成功修复漏洞后的获益,D_{cost}为防御者成功修复漏洞后付出的成本,$-A_{cost}$为在攻击者选择攻击且防御者选择防御下的攻击收益,$A_{profit}-A_{cost}+(1-\alpha)\times E_{Loss}$为攻击者攻击且防御者防御时的防御收益,$1.25(D_{profit}-D_{cost})+\alpha\times E_{Loss}$为攻击者攻击

且防御者不防御时的攻击收益, $-A_{\text{profit}}-\alpha\times E_{\text{Loss}}$ 为攻击者攻击且防御者不防御时的防御收益, D_{cost} 为攻击者不攻击且防御者防御时的攻击收益, $-D_{\text{cost}}$ 为攻击者不攻击且防御者防御时的防御收益,当不攻击不防御时,攻防双方收益均为 0。

表 2　漏洞节点攻防收益

Tab. 2　Vulnerable node attack and defense benefits

攻击者策略	防御者策略	
	防御	不防御
攻击	$-A_{\text{cost}}, A_{\text{profit}}-A_{\text{cost}}+(1-\alpha)\times E_{\text{Loss}}$	$1.25(D_{\text{profit}}-D_{\text{cost}})+\alpha\times E_{\text{Loss}}, -A_{\text{profit}}-\alpha\times E_{\text{Loss}}$
不攻击	$D_{\text{cost}}, -D_{cost}$	0,0

通过对效益损失的计算,量化遭受攻击下的系统物理损失,得到系统效益函数[15] $E(t)$。t 时刻的系统效益函数 $E(t)$ 为 t 时刻的产品产量 $x(t)$ 和产品质量 $y(t)$ 的函数为

$$E(t)=f(x(t),y(t)) \tag{2}$$

某一物理组件被攻击成功后性能下降导致的物理效益损失 E_{Loss} 为

$$E_{\text{Loss}}=\left|E(0)\times(t_{\text{end}}-t_0)-\int_{t_0}^{t_{\text{end}}}E(t)d(t)\right| \tag{3}$$

式中:$E(0)$ 为 ICPS 正常工作时的系统效益, t_0、t_{end} 分别为效益开始下降、效益完全恢复的时间节点。

效益函数曲线见图 3。

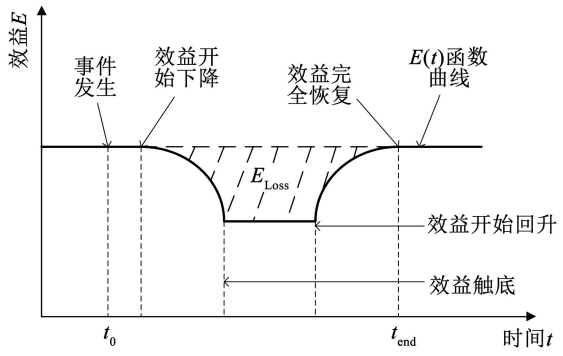

图 3　效益函数曲线

Fig. 3　Benefit function curve

2.3　加入参数机制的演化博弈计算推导

演化博弈能体现出攻防双方在长期对抗过程中的最优决策,即当到某一阶段时任意一方改变策略选择概率,攻防两方都不能获取更多收益时,就到达演化稳定阶段,此时攻防两方的收益视为最优收益,攻防两方的策略选择概率看作最优策略选择概率。

图 4 中 3 条曲线 Y_1、Y_2、Y_3 分别为攻防博弈双方策略选择概率在不同初始状态下的演化轨迹,截取博弈过程中不同时间节点 t_0、t_1、t_n 上攻防二者的轨迹状态可以看出,即便双方最初策略选择概率不一致,也能在足够的演化时间内到达稳定的状态,此时 P_{Ai}^* 和 P_{Dj}^* 为最优策略选择概率。

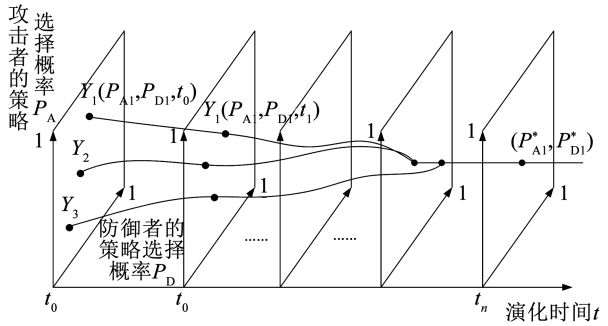

图 4　攻防演化博弈原理

Fig. 4　Principle of offensive and defensive evolutionary game theory

由于攻防复制动态方程推导类似,本文仅从防御者的角度研究演化博弈。

2.3.1　一般演化博弈

一般演化博弈为:

$$\sum_{j=1}^{J}P_{\text{D}j}=1 \tag{4}$$

$$U_{\text{D}j}=\sum_{i=1}^{I}P_{\text{A}i}b_{ij} \tag{5}$$

$$\overline{U_{\text{D}}}=\sum_{j=1}^{J}P_{\text{D}j}U_{\text{D}j} \tag{6}$$

$$\frac{\text{d}P_{\text{D}j}}{\text{d}t}=P_{\text{D}j}[U_{\text{D}j}-\overline{U_{\text{D}}}] \tag{7}$$

式中:b_{ij}、a_{ij} 分别为防御者和攻击者在选择攻击策略 i 和防御者策略 j 时对应的防御和攻击收益, $U_{\text{D}j}$ 为防御策略 j 的期望防御收益, $\overline{U_{\text{D}}}$ 为平均防御收益, $\frac{\text{d}P_{\text{D}j}}{\text{d}t}$ 为防御者策略 j 的选择概率随时间变化率,引入 Boltzmann 概率分布[16],加入探索因子 τ 可得

$$P_{\text{D}j}(k)=\frac{\exp(\tau U_{\text{D}j}(k))}{\sum_{l=1}^{J}\exp(\tau U_{\text{D}l}(k))} \tag{8}$$

式中: $P_{\text{D}j}(k)$ 为防御者在某一博弈阶段的第 k 次攻防博弈中选择策略 j 的概率, $U_{\text{D}j}(k)$ 为防御方在某一阶段的第 k 次攻防对抗中选择防御策略 j 所获得的期望收益,由式(7)、(8)可推导出[17]:

$$\frac{\text{d}P_{\text{D}j}}{\text{d}t}=P_{\text{D}j}\partial\tau[U_{\text{D}j}-\overline{U_{\text{D}}}]+P_{\text{D}j}\partial\sum_{l=1}^{J}P_{\text{D}l}\ln\frac{P_{\text{D}l}}{P_{\text{D}j}} \tag{9}$$

设置步长参数 $\partial=\frac{1}{\tau}$,可得

$$\frac{\text{d}P_{\text{D}j}}{\text{d}t}=\underbrace{P_{\text{D}j}[U_{\text{D}j}-\overline{U_{D}}]}_{\text{一般复制动态方程}}+\underbrace{\frac{1}{\tau}P_{\text{D}j}\sum_{l=1}^{J}P_{\text{D}l}\ln(\frac{P_{\text{D}l}}{P_{\text{D}j}})}_{\text{突变方程}} \tag{10}$$

式中:第 1 项为一般复制动态方程,表示仅在当前信息条件下所能选择的最优策略;第 2 项为突变方程,体现攻防双方在未知信息中尝试各种新策略,不断

尝试进行调整的探索过程,凸显出现实条件下攻防的不确定性和多样性[17]。

2.3.2 加入参数机制的演化博弈

虽然一般复制动态方程下的演化博弈基于有限理性的假设出发,但是没有考虑到现实世界中攻防双方理性程度存在差异性这一问题[13-18]。本文采用加入参数机制的复制动态方程来解决这一问题(见式(14)),合理设置了攻防双方本身理性程度参数 $\lambda_A(0\leqslant\lambda_A)$,$\lambda_D(0\leqslant\lambda_D)$来定义防御者认知能力,以此主导博弈结果。

加入参数机制的复制动态方程考虑了博弈中的攻防双方拥有着一定的理性程度的情况,但攻防双方个体之间还存在着学习能力上的区别,因此不同攻防双方达到纳什均衡的过程和结果有着差异。加入参数机制的复制动态方程没有抹杀掉攻防双方间的认知差异和选择偏好,于是引入条件转移概率 C_{lj},C_{lj}为策略 l 到策略 j 的条件转移概率,描述着策略选择的更新规则[16]:

$$\frac{\mathrm{d}P_{\mathrm{D}j}}{\mathrm{d}t}=\left[\sum_{l=1}^{J}P_{\mathrm{D}l}c_{lj}-\sum_{y=1}^{J}P_{\mathrm{D}j}c_{jy}\right] \tag{11}$$

ICPS 系统的攻防博弈涉及到攻击者和防御者之间复杂的互动。而 Boltzmann 概率考虑了双方在不同环境和条件下的行为适应性和动态变化[16],能够准确描述防御者在不同情境下选择策略的概率变化,非常符合 ICPS 博弈的特性,于是再次引入 Boltzmann 概率分布,可得

$$C_{lj}=\frac{\exp(\lambda_{\mathrm{D}}U_{\mathrm{D}j})}{\sum_{l=1}^{J}\exp(\lambda_{\mathrm{D}}U_{\mathrm{D}l})} \tag{12}$$

式中:λ_D 越大,防御者越理性;λ_D 越小,防御者越不理智。将式(12)代入式(11),结合式(4)可得

$$\frac{\mathrm{d}P_{\mathrm{D}j}}{\mathrm{d}t}=\sum_{l=1}^{J}P_{\mathrm{D}l}\frac{\mathrm{e}^{\lambda_{\mathrm{D}}U_{\mathrm{D}j}}}{\sum_{l=1}^{J}\mathrm{e}^{\lambda_{\mathrm{D}}U_{\mathrm{D}l}}}-\sum_{y=1}^{J}P_{\mathrm{D}j}\frac{\mathrm{e}^{\lambda_{\mathrm{D}}U_{\mathrm{D}y}}}{\sum_{j=1}^{J}\mathrm{e}^{\lambda_{\mathrm{D}}U_{\mathrm{D}j}}}=$$

$$\sum_{l=1}^{J}P_{\mathrm{D}l}\frac{\mathrm{e}^{\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{ij}}}{\sum_{l=1}^{J}\mathrm{e}^{\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{il}}}-\sum_{y=1}^{J}P_{\mathrm{D}j}\frac{\mathrm{e}^{\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{iy}}}{\sum_{j=1}^{J}\mathrm{e}^{\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{ij}}}\sum_{l=1}^{J}P_{\mathrm{D}l}=1$$

$$\frac{\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{ij})}{\sum_{l=1}^{J}\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{il})}-P_{\mathrm{D}j} \tag{13}$$

将式(10)中的一般复制动态方程加入含攻防双方理性程度的参数 λ_D,结合式(13)可得

$$\frac{\mathrm{d}P_{\mathrm{D}j}}{\mathrm{d}t}=\frac{\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{ij})}{\sum_{l=1}^{J}\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{il})}-P_{\mathrm{D}j}+\frac{1}{\tau}P_{\mathrm{D}j}\sum_{l=1}^{J}P_{\mathrm{D}l}\ln\frac{P_{\mathrm{D}l}}{P_{\mathrm{D}j}} \tag{14}$$

同理可得

$$\frac{\mathrm{d}P_{\mathrm{A}i}}{\mathrm{d}t}=\frac{\exp(\lambda_{\mathrm{A}}\sum_{j=1}^{J}P_{\mathrm{D}j}a_{ij})}{\sum_{l=1}^{I}\exp(\lambda_{\mathrm{A}}\sum_{j=1}^{J}P_{\mathrm{D}j}a_{lj})}-P_{\mathrm{A}i}+\frac{1}{\tau}P_{\mathrm{A}i}\sum_{l=1}^{I}P_{\mathrm{A}l}\ln\frac{P_{\mathrm{A}l}}{P_{\mathrm{A}i}} \tag{15}$$

2.4 演化博弈稳定均衡求解

当单阶段演化达到稳定均衡状态时,攻防群体选择不同策略随时间的变化率应为 0,即 $\frac{\mathrm{d}P_{\mathrm{A}i}}{\mathrm{d}t}=0$ 且 $\frac{\mathrm{d}P_{\mathrm{D}j}}{\mathrm{d}t}=0$。在单阶段演化博弈中,$(S_{\mathrm{A}}^{*},S_{\mathrm{D}}^{*})$ 为该阶段的演化博弈均衡策略,此时攻防双方对应的攻防博弈收益最高,即

$$\begin{cases}U_{\mathrm{D}}(S_{\mathrm{A}}^{*},S_{\mathrm{D}}^{*})\geqslant U_{\mathrm{D}}(S_{\mathrm{A}},S_{\mathrm{D}}^{*})\\ U_{\mathrm{A}}(S_{\mathrm{A}}^{*},S_{\mathrm{D}}^{*})\geqslant U_{\mathrm{A}}(S_{\mathrm{A}}^{*},S_{\mathrm{D}})\end{cases} \tag{16}$$

单阶段演化博弈均衡解求解公式为

$$\begin{cases}P_{\mathrm{D}j}\in[0,1],P_{\mathrm{A}i}\in[0,1]\\ \sum_{j=1}^{J}P_{\mathrm{D}j}=1,\sum_{i=1}^{I}P_{\mathrm{A}i}=1\\ 0=\frac{\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{ij})}{\sum_{l=1}^{J}\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}b_{il})}-P_{\mathrm{D}j}+\frac{1}{\tau}P_{\mathrm{D}j}\sum_{l=1}^{J}P_{\mathrm{D}l}\ln\frac{P_{\mathrm{D}l}}{P_{\mathrm{D}j}}\\ 0=\frac{\exp(\lambda_{\mathrm{A}}\sum_{j=1}^{J}P_{\mathrm{D}j}a_{ij})}{\sum_{l=1}^{I}\exp(\lambda_{\mathrm{A}}\sum_{j=1}^{J}P_{\mathrm{D}j}a_{lj})}-P_{\mathrm{A}i}+\frac{1}{\tau}P_{\mathrm{A}i}\sum_{l=1}^{I}P_{\mathrm{A}l}\ln\frac{P_{\mathrm{A}l}}{P_{\mathrm{A}i}}\end{cases} \tag{17}$$

在 Markov 改进演化博弈中,多阶段博弈由每个阶段中各自独立的单阶段演化博弈组成,是属于有限博弈,因此一定存在混合策略下的纳什均衡[13]。

采用动态规划法,求解多阶段演化博弈均衡解如下:

$$\begin{cases}\max R_{\mathrm{D}}(S_T^0,S_T^1)=\max\left[U_{\mathrm{D}}^{\mathrm{T}}+\sum_{e,h\in[T,Z]}\xi_h\eta(S_h^1\mid S_e^0)R_{\mathrm{D}}(S_h^0,S_h^1)\right]\\ \max R_{\mathrm{A}}(S_T^0,S_T^1)=\max\left[U_{\mathrm{A}}^{\mathrm{T}}+\sum_{e,h\in[T,Z]}\xi_h\eta(S_h^1\mid S_e^0)R_{\mathrm{A}}(S_h^0,S_h^1)\right]\\ \frac{\mathrm{d}P_{\mathrm{D}j}^{\mathrm{T}}}{\mathrm{d}t}=\frac{\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}^{\mathrm{T}}b_{ij}^{\mathrm{T}})}{\sum_{l=1}^{J}\exp(\lambda_{\mathrm{D}}\sum_{i=1}^{I}P_{\mathrm{A}i}^{\mathrm{T}}b_{il}^{\mathrm{T}})}-P_{\mathrm{D}j}^{\mathrm{T}}+\frac{1}{\tau}P_{\mathrm{D}j}^{\mathrm{T}}\sum_{l=1}^{J}P_{\mathrm{D}l}^{\mathrm{T}}\ln\frac{P_{\mathrm{D}l}^{\mathrm{T}}}{P_{\mathrm{D}j}^{T}}=0\\ \frac{\mathrm{d}P_{\mathrm{A}i}^{\mathrm{T}}}{\mathrm{d}t}=\frac{\exp(\lambda_{\mathrm{A}}\sum_{j=1}^{J}P_{\mathrm{D}j}^{\mathrm{T}}a_{ij}^{\mathrm{T}})}{\sum_{l=1}^{J}\exp(\lambda_{\mathrm{A}}\sum_{j=1}^{J}P_{\mathrm{D}j}^{\mathrm{T}}a_{lj}^{\mathrm{T}})}-P_{\mathrm{A}i}^{\mathrm{T}}+\frac{1}{\tau}P_{\mathrm{A}i}^{\mathrm{T}}\sum_{l=1}^{I}P_{\mathrm{A}l}^{\mathrm{T}}\ln\frac{P_{\mathrm{A}l}^{\mathrm{T}}}{P_{\mathrm{A}i}^{T}}=0\\ P_{\mathrm{D}j}^{\mathrm{T}}\in[0,1],P_{\mathrm{A}i}^{\mathrm{T}}\in[0,1];\sum_{j=1}^{J}P_{\mathrm{D}j}^{\mathrm{T}}=1,\sum_{i=1}^{I}P_{\mathrm{A}i}^{\mathrm{T}}=1\end{cases} \tag{18}$$

式中: $R_A(S_T^0,S_T^1)$ 、$R_D(S_T^0,S_T^1)$ 分别为 T 阶段下博弈后攻击者和防御者的目标函数,其中 T、Z 作为角标时表明对应符号处于 T 或 Z 阶段,Z 为最终阶段; S_e^0 为在漏洞节点 e 上单阶段演化博弈开始前的初始状态,S_h^1 为在漏洞节点 h 上单阶段演化博弈稳定后的状态,$\eta(S_h^1|S_h^0)$ 为状态 S_h^1 到状态 S_h^0 的转移概率。

设计目标函数 R,用于判断攻防双方策略的优劣[18]。如图 2 所示的多阶段下演化博弈过程所示,引入漏洞节点 h 上的贴现因子 $\xi_h(0\leqslant\xi_h\leqslant1)$ 计算未来折扣收益值,将未来收益折算成基于初始阶段的折扣收益。攻防双方的目标是使各自的目标函数达到最大值,在此基础上,采用动态规划法[13]求解多阶段演化博弈均衡解,多阶段博弈均衡求解见式(18)。

由 Markov 决策准则,一定存在 $(S_{D,T}^*,S_{A,T}^*)$ 可得[13]

$$\begin{cases} S_{D,T}^* \in \operatorname{argmax} R_D(S_T^0,S_T^1) \\ S_{A,T}^* \in \operatorname{argmax} R_A(S_T^0,S_T^1) \end{cases} \tag{19}$$

式中, $S_{A,T}^*$ 、$S_{D,T}^*$ 分别为对应攻击者和防御者在 T 阶段中的最优防御策略。

本文的 Markov 改进演化博弈研究方法对比分析见表 3。

表 3　对比分析

Tab. 3　Comparative analysis

文献	行为理性	范围	博弈过程	阶段	分析过程	具体应用
文献[6]	非完全理性	信息域到物理域	随机博弈 Petri 网	多阶段	简单	风险评估
文献[7]	完全理性	信息域	Stackelberg 博弈	多阶段	简单	信息网络脆弱性评估
文献[8]	完全理性	信息域	改进 HMM 博弈	多阶段	详细	网络风险评估
文献[9]	完全理性	信息域	Stackelberg 博弈和 Markov 博弈混合	多阶段	详细	防御策略智能决策
文献[10]	非完全理性	信息域	三方演化博弈	单阶段	详细	研究进化稳定策略
本文	非完全理性	信息域到物理域	改进演化博弈和 Markov 博弈混合	多阶段	详细	ICPS 风险评估

3　仿真与分析

3.1　数值实验分析加入参数机制的博弈模型

定义攻防收益矩阵为 $\begin{bmatrix} a_{11},b_{11} & a_{12},b_{12} \\ a_{21},b_{21} & a_{22},b_{22} \end{bmatrix}$, 由式(17)可得

$$\begin{cases} \dfrac{\exp(\lambda_A(P_{D1}a_{11}+(1-P_{A1})a_{12}))}{\exp(\lambda_A(P_{D1}a_{11}+(1-P_{D1})a_{12}))+\exp(\lambda_A(P_{D1}a_{21}+(1-P_{D1})a_{22}))}- \\ P_{A1}+\dfrac{1}{\tau}P_{A1}(1-P_{A1})\ln\dfrac{1-P_{A1}}{P_{A1}}=0 \\ \dfrac{\exp(\lambda_D(P_{A1}b_{11}+(1-P_{A1})b_{21}))}{\exp(\lambda_D(P_{A1}b_{11}+(1-P_{A1})b_{21}))+\exp(\lambda_D(P_{A1}b_{12}+(1-P_{A1})b_{22}))}- \\ P_{D1}+\dfrac{1}{\tau}P_{D1}(1-P_{D1})\ln\dfrac{1-P_{D1}}{P_{D1}}=0 \end{cases} \tag{20}$$

设攻击者和防御者分别有两个策略,其对应的攻防收益矩阵为 $\begin{bmatrix} 1,2 & 3,2 \\ 2,1 & 1,2 \end{bmatrix}$, 设置初始攻防双方对于自身两个策略的初始选择概率都为 0.5。

如图 5 所示为分析加入参数机制的博弈模型中初始状态对策略选择的影响,模拟不同初始攻防策略选择下双方对策略的选择概率演化过程,此时令 $\lambda_A=\lambda_D=1$, $\tau=100$, 改变 P_{A1} 和 P_{D1} 的初始值。由图 5可以看出,无论初始攻防策略如何选择,防御者与攻击者的稳定策略都是相同的。

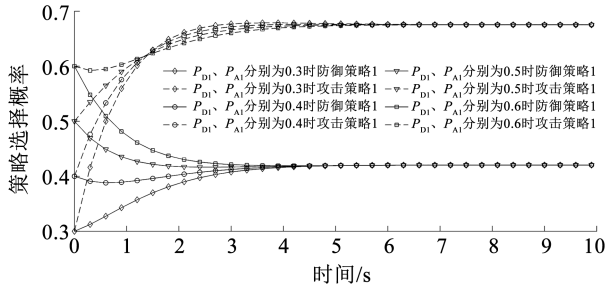

图 5　不同初始概率下策略选择概率演化图

Fig. 5　Evolution diagram of strategy selection probabilities under different initial probabilities

为进一步分析探索因子对策略选择概率的影响,令 $\lambda_A=\lambda_D=1$, 改变 τ 的值使其从 0.010 0 ~ 1 000,不同 τ 下演化博弈稳定状态时策略选择概率随着 τ 的改变而改变的轨迹(见图 6)。从图 6中可以看出,在 $\tau=0.010\ 0$ 时,攻击者对策略 1 的策略选择概率为 0.502 9,防御者对策略 1 的策略选择概率为 0.497 3,这是因为初始的时候探索因子较小,代表着攻防双方对彼此的信息处于很不了解的状态,以探索行为为主。随着探索因子的增大,探索行为的比重减小,此时攻防双方对彼此信息的了解比较全面,对策略的选择也逐渐稳定下来,可以看出当 $\tau\geqslant80$ 时,攻防双方的最终策略选择概率不再改变。

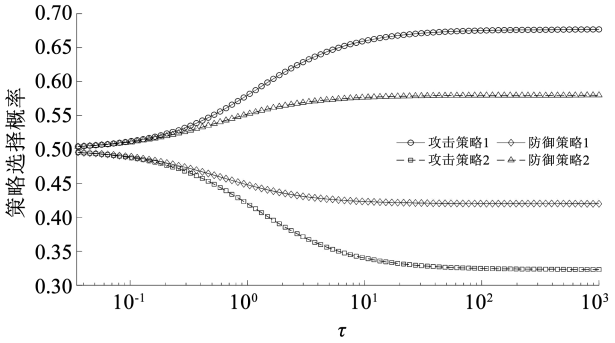

图 6 不同探索因子下攻防双方博弈均衡时的策略选择概率

Fig. 6 Probabilities of strategy selection in game equilibrium between offense and defense under different exploration factors

设置 $\tau=100$,$\lambda_A=5$,改变防御方的理性程度使其从 0 上升至 350(见图 7)。在 $\lambda_D=0$ 时,此时防御者没有理性主导选择,丧失了对自己两个策略的优劣判断能力,因而对所拥有的策略进行随机选择,即两个策略的选择概率都为 0.500 0。随着防御者理性程度的上升,防御者对其策略的概率选择有一个大的变动,且固定理性程度下的攻击者会根据防御者的理性程度对自己的策略进行修改,但最终的策略选择概率会趋于稳定。在 $\lambda_D=300$ 时,防御者对其策略 1 的选择概率变为 0.270 0,并且随着理性程度的攀升,概率趋于稳定,这是因为在 $\lambda_D\geqslant 300$ 之后,防御者的理性程度相较于攻击者来说足够大,很难再作为博弈均衡时策略选择概率变化的主导因素。

设置 $\tau=1\,000$,即仅考虑理性程度的影响时,当 $\lambda_A=\lambda_D\geqslant 100$ 时,攻防双方具有高度理智,此时攻击者纳什均衡解(1,0)与完全理性纳什均衡解一致[19],但比起完全理性下的博弈,本文更加强调参与者的理性特征,反应真实的策略选择规律。

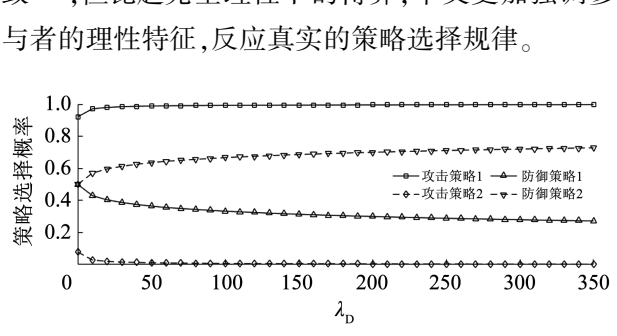

图 7 防御者不同理性程度下博弈均衡时的策略选择概率

Fig. 7 Probabilities of strategy selection in game equilibrium under different rationality levels of defenders

为研究收益矩阵对博弈的影响,设置 $\lambda_A=\lambda_D=1$,忽略探索因子的影响,使 $\tau=100$,改变 b_{11} 的数值(见图 8)。可见随着 b_{11} 的增加,防御者对策略 1 的策略选择概率也随之上升。

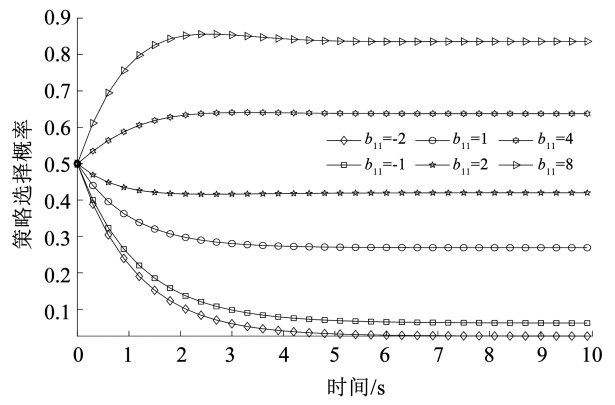

图 8 防御策略 1 的选择概率与 b_{11} 的关系

Fig. 8 Relationship between the selection probability of defense strategy 1 and b_{11}

在一般演化博弈下,由式(4)~(7)可以求出防御者对于策略 2 的选择概率为 0,而当攻防双方理性程度较高时,设 $\lambda_A=\lambda_D=10$,防御者对于策略 2 的选择概率为 0.058 0,接近一般演化博弈下的结果,但一般演化博弈未能直观的用数据体现攻防双方的理性程度,而是以一个较高理智的两方博弈者的角度来进行策略的选择,不贴近于现实。在不了解对方理性程度的情况下盲目使用一般演化博弈来判断,很可能造成自己收益的亏损。从防御者的视角进行举例,$\lambda_A=1$,$\lambda_D=10$,$\tau=100$ 时,一般演化博弈下防御者会认为攻击者以(1,0)的概率选择攻击策略,就用(0.300 0,0.700 0)的概率选择防御策略,实际上攻击者受于理性程度的制约,会用(0.823 4,0.176 6)的概率进行策略选择,此时防御收益 $U_D=1.947\,0$。当知道攻击者的理性程度并对双方策略做出判断之后,防御者的策略选择概率为(0.148 3,0.851 7),此时防御者收益 $U_D=1.973\,8$。由此可见,改进后的防御收益大于前者,当攻防收益矩阵中的数值更大的时候,差距就会更加明显。这是因为防御者理性程度高于攻击者,在大致了解假定双方理性程度并假定好参数的前提下使用改进演化博弈,求出的均衡解下的收益必然比不考虑攻防双方理性程度差异性的一般演化博弈要高,符合 ICPS 攻防博弈逻辑。

在风险评估中,改进演化博弈能让双方参与者基于对对方行为习惯(理性程度的判断和探索程度)的深入理解做出策略选择,有效地评估和预测对手可能的反应,从而更准确地制定出优化自身利益的策略,在不确定性和变化中保持相对稳定的收益水平。

3.2　评估 BWPP 动态风险的实验仿真与分析

采用沸水发电系统作为实验对象,以验证本文评估方法的有效性[20]。假设有一个网络攻击者,根据攻防状态转移图实现攻击,每个节点各有一个防御者选择防御策略。攻击者攻击 ICPS 时,不仅仅只考虑其中某个组件,而是会根据受攻击系统特性以及自己的攻击目的,设计影响链路,建立信息域到物理域的跨域攻击路径。本文通过 Nessus 扫描实验信息系统,结合国家信息安全漏洞库信息,参考文献[13,18]的方法在分析路由文件、漏洞信息的基础上,根据攻击在信息层和物理层的传播特点,构建跨域攻击下各阶段的攻防状态转移图(见图 1)。其中,各个状态间的转移概率见表 4。

表 4　阶段间的状态转移概率表

Tab. 4　State transition probability table between stages

状态转移	转移概率	状态转移	转移概率	状态转移	转移概率
$S_W^1 \to S_M^0$	0.4	$S_W^1 \to S_D^0$	0.6	$S_M^1 \to S_W^0$	0.2
$S_M^1 \to S_D^0$	0.8	$S_D^1 \to S_M^0$	0.2	$S_D^1 \to S_W^0$	0.2
$S_D^1 \to S_{Se1}^0$	0.1	$S_D^1 \to S_{Se2}^0$	0.1	$S_D^1 \to S_{Se3}^0$	0.1
$S_D^1 \to S_{V1}^0$	0.1	$S_D^1 \to S_{V2}^0$	0.1	$S_D^1 \to S_{V3}^0$	0.1
$S_{Se1}^1 \to S_{Se2}^0$	0.2	$S_{Se1}^1 \to S_{Se3}^0$	0.1	$S_{Se1}^1 \to S_{V1}^0$	0.7
$S_{Se2}^1 \to S_{Se3}^0$	0.1	$S_{Se2}^1 \to S_{Se1}^0$	0.1	$S_{Se2}^1 \to S_{V2}^0$	0.8
$S_{Se3}^1 \to S_{Se1}^0$	0.4	$S_{Se3}^1 \to S_{Se2}^0$	0.2	$S_{Se3}^1 \to S_{V3}^0$	0.4
$S_{V1}^1 \to S_{V2}^0$	0.7	$S_{V1}^1 \to S_{V3}^0$	0.3	$S_{V2}^1 \to S_{V3}^0$	0.4
$S_{V2}^1 \to S_{V1}^0$	0.6	$S_{V3}^1 \to S_{V1}^0$	0.5	$S_{V3}^1 \to S_{V2}^0$	0.5

表 5 列举沸水发电系统中常见的 4 个漏洞信息[21],为攻防收益量化做准备。

表 5　BWPP 常见漏洞信息表

Tab. 5　BWPP common vulnerability information table

所在位置	CVE 编号	base 向量	可利用性
网络服务器	CVE - 2015 - 1635	AV:N/AC:L/Au:N/C:C/I:C/A:C	0.999 68
邮件服务器	CVE - 2004 - 0840	AV:N/AC:L/Au:N/C:C/I:C/A:C	0.999 68
数据库服务器	CVE - 2015 - 7417	AV:N/AC:M/Au:S/C:N/I:P/A:N	0.683 20
传感器/阀门	CVE - 2013 - 3957	AV:N/AC:L/Au:N/C:P/I:P/A:P	0.999 68

在 ICPS 信息域的漏洞节点中,攻击者往往在成功利用漏洞后不立即采取措施,并等待一段时间,以此提高攻击的效果和成功率,同时减少被发现的风险。此外,攻击者会通过利用信息域中漏洞实现提升权限和获取更多信息的目的,这些目的在单阶段下可看作只有信息方面的损失而与物理域中各类物理器件的运作无关,因此令信息域中漏洞节点的物理效益损失 $E_{\text{Loss}}=0$;在物理域的漏洞节点中,一般认为控制器节点难以被网络入侵,因此图 1 中攻防状态转移图不出现控制器相关状态,即控制器处不进行攻防博弈。而传感器和阀门被网络攻击者利用漏洞攻击,导致了阀门产生了不同程度的脱离正常运转的情况,造成了不同的物理效益损失。

在阀门和传感器遭受攻击的情况下考虑到 6 种攻击场景:1)进水阀关闭;2)排气阀关闭;3)进料阀全开;4)液位传感器测量数据被修改为 0;5)压力传感器测量数据被修改为 0;6)电流传感器测量数据被修改为 0。

参考文献[22]中 V1、V2 和 V3 的数学模型,仿真得出 BWPP 物理组件遭受攻击后压力动态变化图,见图 9。系统效益函数 $E(t)$ 包含的产品产量 $x(t)$ 和质量 $y(t)$ 分别用发电电量和质量表示。在 BWPP 中,假设遭受攻击时系统的发电质量仍能保持稳定,即 $y(t)$ 不变,在攻击下电量输出和压力的变化趋势相同,因此用压力来体现 $E(t)$。t_0 时刻 BWPP 中的 3 个液位传感器分别开始遭受攻击,此时压力为 108 kg/cm^2。t_{end} 时刻根据压力程度来选择,罐内能承受的最大压力值为 250 kg/cm^2,超过最大压力值即会有爆炸的可能性,此时系统运行会中断,中断时刻作为 t_{end}。当没有超过 250 kg/cm^2 时,取 1 000 s 作为攻击测试结束时间 t_{end}。根据式(2)、(3)求出物理效益损失 E_{Loss},见表 6。

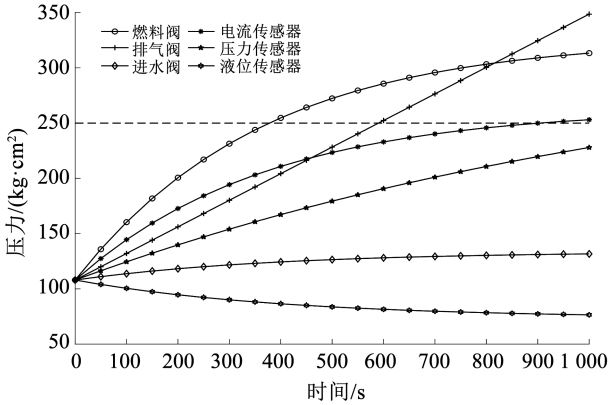

图 9　BWPP 物理组件遭受攻击后压力动态变化

Fig. 9　Dynamic changs in pressure after BWPP physical components are attacked

表 6 不同攻击下系统的物理效益损失

Tab. 6 Physical benefit loss of the system under different attacks

攻击设备	攻击结束时 t_{end}	效益损失 E_{Loss}
Se1	1 000.0	21.47
Se2	1 000.0	67.33
Se3	903.7	101.23
V1	1 000.0	16.28
V2	378.5	33.71
V3	590.3	43.13

参考文献[23]中对 A_{profit}、A_{cost}、D_{profit}、D_{cost} 的定义方式,结合防御策略库的信息,根据表 2 中的定义方式,针对表 4 中不同位置存在的常见漏洞信息,计算不同漏洞节点下的攻防收益数值,生成攻防收益矩阵,见表 7。表中,攻击收益矩阵和防御收益矩阵的横坐标自上到下分别表示攻击者利用漏洞攻击和不攻击,纵坐标自左到右分别表示防御者选择防御和不防御措施。

表 7 不同漏洞节点攻防收益量化矩阵

Tab. 7 Quantification matrix of attack and defense benefits for different vulnerability nodes

S_W		S_M		S_D	
攻击收益	防御收益	攻击收益	防御收益	攻击收益	防御收益
$\begin{bmatrix}-6.6 & 28.0\\ 10.2 & 0\end{bmatrix}$	$\begin{bmatrix}34.5 & -36.6\\ -10.2 & 0\end{bmatrix}$	$\begin{bmatrix}-8.1 & 9.9\\ 14.2 & 0\end{bmatrix}$	$\begin{bmatrix}7.4 & -8.2\\ -14.2 & 0\end{bmatrix}$	$\begin{bmatrix}-11.7 & 27.1\\ 13.4 & 0\end{bmatrix}$	$\begin{bmatrix}26.2 & -28.8\\ -13.4 & 0\end{bmatrix}$
S_{Se1}		S_{Se2}		S_{Se3}	
攻击收益	防御收益	攻击收益	防御收益	攻击收益	防御收益
$\begin{bmatrix}-17.1 & 30.4\\ 43.2 & 0\end{bmatrix}$	$\begin{bmatrix}7.5 & -22.7\\ -43.2 & 0\end{bmatrix}$	$\begin{bmatrix}-5.6 & 81.3\\ 95.7 & 0\end{bmatrix}$	$\begin{bmatrix}14.3 & -70.3\\ -95.7 & 0\end{bmatrix}$	$\begin{bmatrix}-16.1 & 109.4\\ 53.4 & 0\end{bmatrix}$	$\begin{bmatrix}16.3 & -106.0\\ -53.4 & 0\end{bmatrix}$
S_{V1}		S_{V2}		S_{V3}	
攻击收益	防御收益	攻击收益	防御收益	攻击收益	防御收益
$\begin{bmatrix}-15.6 & 22.6\\ 32.4 & 0\end{bmatrix}$	$\begin{bmatrix}21.2 & -19.5\\ -32.4 & 0\end{bmatrix}$	$\begin{bmatrix}-19.4 & 45.5\\ 22.8 & 0\end{bmatrix}$	$\begin{bmatrix}17.4 & -44.9\\ -22.8 & 0\end{bmatrix}$	$\begin{bmatrix}-17.1 & 51.9\\ 52.1 & 0\end{bmatrix}$	$\begin{bmatrix}7.5 & -46.7\\ -52.1 & 0\end{bmatrix}$

假设攻防双方理性程度相等,即 $\lambda_A = \lambda_D = 1$。BWPP 比较成熟,可认为攻防双方对彼此了解,令探索因子 $\tau = 100$。同等对待现在和未来攻防收益的价值,即令 $\xi_h = 0.5$,这些参数与表 6 中已经求得的 BWPP 常见漏洞节点中的攻防收益数值一起代入式(18),迭代 1 000 次求出表 8 中的攻防策略及收益。

表 8 可以看出,在物理域中,攻击者的收益 $U_{V1} < U_{V2} < U_{Se1} < U_{V3} < U_{Se3} < U_{Se2}$,一般情况下认为攻击者收益与漏洞节点风险程度成正相关,即攻击者攻击漏洞节点收益越大,该漏洞节点越容易遭受攻击,风险越大。可以评估物理域中漏洞节点的风险程度为:V1 < V2 < Se1 < V3 < Se3 < Se2。由此可见,压力传感器遭受攻击的可能性较大,应适时做好 BWPP 中压力传感器的防御措施。

表 8 均衡策略收益

Tab. 8 Equilibrium strategy benefits

状态	攻击策略选择概率	防御策略选择概率	攻击收益	防御收益	状态	攻击策略选择概率	防御策略选择概率	攻击收益	防御收益
W	0.1,0.9	0.8,0.2	17.19	-13.91	Se3	0.3,0.7	0.6,0.4	51.83	-50.28
M	0.5,0.5	0.3,0.7	15.15	-13.20	V1	0.4,0.6	0.3,0.7	24.85	-23.17
D	0.2,0.8	0.6,0.4	22.63	-19.84	V2	0.3,0.7	0.5,0.5	26.43	-26.11
Se1	0.6,0.4	0.3,0.7	31.88	-29.17	V3	0.5,0.5	0.4,0.6	35.39	-35.25
Se2	0.5,0.5	0.4,0.3	57.17	-51.79					

本文设置如下两条沸水发电系统中的常见攻击路径,其中:路径 1 为 $S_W^0 \to S_W^1 \to S_D^0 \to S_D^1 \to S_{Se1}^0 \to S_{Se1}^1 \to S_{V1}^0 \to S_{V1}^1$,路径2为 $S_M^0 \to S_M^1 \to S_D^0 \to S_D^1 \to S_{Se1}^0 \to S_{Se1}^1 \to S_{V1}^0 \to S_{V1}^1$。对比两条路径可以发现,其仅有第 1 阶段不相同,计算出第 1 条路径中攻击者收益为 96.55,第 2 条路径攻击者收益为 94.51,第 1 条路径攻击收益大于第 2 条,更符合攻击者的期望,显然第 1 条路径中 S_W 节点应该更值得防御者关注。对攻击者来说,路径 1 的收益更高,这是由于网络服务器的重要程度通常比较高,一旦被攻陷,整个网络系统都将处于被动的局面。为降低第 1 条路径的发生概率,应当尽量减小其他漏洞节点到 S_W 的状态转移概率,若能使得概率为 0,则路径 1 便不可能实现,就可以满足防御方期望。

以 BWPP 系统为例,对 ICPS 的漏洞节点进行评估,可以对系统中容易遭受攻击的漏洞节点进行合理预测,同时对其进行针对性的防范。相比于一些风险评估方案[10],不再是把漏洞节点看成独立的个体,而是考虑攻击者攻击每一个漏洞节点之间的联系,再加入考虑攻防双方理性程度和探索程度的改进演化博弈,得到 ICPS 中各漏洞节点的攻击者收益,以此评估动态风险,能对系统的防护起到真实全面的指导作用。

4　结　论

1)从 ICPS 实际出发,根据系统组件,构建了从信息域到物理域的 ICPS 攻防状态转移图。

2)设计了加入参数机制的复制动态方程来改进一般演化博弈,能让单阶段中攻防双方的决策和收益与双方理性程度和探索程度相关;

3)引入了 Markov 的无后效性,开展研究多阶段下的演化博弈,得到攻击路径下各个漏洞节点的攻击收益,从而评估节点。

4)本文构建了自定义理性程度和探索程度下攻防双方随时间变化的策略演化微分方程,通过单阶段数值实验结果验证了方法的合理性,与一般演化博弈中不区分理性程度相比,对 ICPS 的攻防博弈研究更有普适性。并且通过沸水发电系统进行实验分析,结果表明,Markov 改进演化博弈能根据各个漏洞节点的攻防双方理性和探索程度不同求出攻击收益,从而评估风险情况,且结果符合现实情况。

参考文献

[1] IRRAM F, ALI M, NAEEM M, et al. Physical layer security for beyond 5G/6G networks: emerging technologies and future directions [J]. Journal of Network and Computer Applications, 2022, 206: 103431. DOI: 10.1016/j.jnca.2022.103431

[2] LANGNER R. Stuxnet: dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49. DOI: 10.1109/MSP.2011.67

[3] CHERDANTSEVA Y, BURNAP P, BLYTH A, et al. A review of cyber security risk assessment methods for SCADA systems [J]. Computers & Security, 2016, 56: 1. DOI: 10.1016/j.cose.2015.09.009

[4] 罗智勇,杨旭,刘嘉辉,等. 基于贝叶斯攻击图的网络入侵意图分析模型[J]. 通信学报, 2020, 41(9): 160
LUO Zhiyong, YANG Xu, LIU Jiahui, et al. Network intrusion intention analysis model based on Bayesian attack graph[J]. Journal on Communications, 2020, 41(9): 160. DOI: 10.11959/j.issn.1000-436x.2020172

[5] DONG Huiyu, WANG Hongwei, TANG Tao. An attack tree-based approach for vulnerability assessment of communication-based train control systems[C]//2017 Chinese Automation Congress (CAC). Jinan: IEEE, 2017: 6407. DOI: 10.1109/CAC.2017.8243932

[6] QIAN Jiawei, SHI Pengcheng, MU Qiang. Based on random game Petri net model CPS risk assessment and defense decision of distribution network [C]//2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). Changsha: IEEE, 2021: 764. DOI: 10.1109/AEMCSE51986.2021.00158

[7] XIONG Juxia, WU Jinzhao. Construction of information network vulnerability threat assessment model for CPS risk assessment[J]. Computer Communications, 2020, 155: 197. DOI: 10.1016/j.comcom.2020.03.026

[8] HU Jingjing, GUO Shuangshuang, KUANG Xiaohui, et al. I-HMM-based multidimensional network security risk assessment[J]. IEEE Access, 2019, 8: 1431. DOI: 10.1109/ACCESS.2019.2961997

[9] 陈子涵, 程光. 基于 Stackelberg-Markov 非对等三方博弈模型的移动目标防御技术[J]. 计算机学报, 2020, 43(3): 512
CHEN Zihan, CHENG Guang. Moving target defense technology using Stackelberg Markov asymmetrical trilateral game model[J]. Chinese Journal of Computers, 2020, 43(3): 512. DOI: 10.11897/SP.J.1016.2020.00512

[10] YANG Pengxi, GAO Fei, ZHANG Hua. Multi-player evolutionary game of network attack and defense based on system dynamics[J]. Mathematics, 2021, 9(23): 3014. DOI: 10.3390/math9233014

[11] ZHANG Hengwei, TAN Jinglei, LIU Xiaohu, et al. Cybersecurity threat assessment integrating qualitative differential and evolutionary games [J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 3425. DOI: 10.1109/TNSM.2022.3166348

[12] CHEN Fang, GOU Chengling, GUO Xiaoqian, et al. Prediction of stock markets by the evolutionary mix-game model[J]. Physica A: Statistical Mechanics and its Applications, 2008, 387(14): 3594. DOI: 10.1016/j.physa.2008.02.023

[13] MA Runnian, ZHANG Enning, WANG Gang, et al. Network defense decision-making method based on improved evolutionary game model[J]. Journal of Electronics & Information Technology, 2023, 45(6): 1970. DOI: 10.11999/JEIT220585

[14] 张恒巍, 黄健明. 基于 Markov 演化博弈的网络防御策略选取方法[J]. 电子学报, 2018, 46(6): 1503.
ZHANG Hengwei, HUANG Jianming. Network defense strategy selection method based on Markov evolutionary game [J]. Acta Electronica Sinica, 2018, 46(6): 1503. DOI: 10.3969/j.issn.0372-2112.2018.06.033

[15] WEI Dong, JI Kun. Resilient industrial control system (RICS): concepts, formulation, metrics, and insights [C]//2010 3rd international Symposium on Resilient Control Systems. Idaho Falls: IEEE, 2010: 15. DOI: 10.1109/ISRCS.2010.5603480

[16] GABETTA G, TOSCANI G, WENNBERG B. Metrics for probability distributions and the trend to equilibrium for solutions of the Boltzmann equation[J]. Journal of Statistical Physics, 1995, 81(5): 901. DOI: 10.1007/BF02179298

[17] TUYLS K, VERBEECK K, LENAERTS T, et al. A selection-mutation model for q-learning in multi-agent systems [C]// Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems. Melbourne: ACM, 2003: 693. DOI: 10.1145/860575.860687

[18] 张勇, 谭小彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495
ZHANG Yong, TAN Xiaobin, CUI Xiaolin, et al. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2011, 22(3): 495. DOI: 10.3724/SP.J.1001.2011.03751

[19] LI Yuzhe, QUEVEDO D E, DEY S, et al. A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems [J]. IEEE Transactions on Signal and Information Processing Over Networks, 2017, 3(1): 1. DOI: 10.1109/TSIPN.2016.2611446

[20] OROJLOO H, AZGOMi M A. A stochastic game model for evaluating the impacts of security attacks against cyber-physical systems[J]. Journal of Network and Systems Management, 2018, 26(4): 929. DOI: 10.1007/s10922-018-9449-0

[21] HUANG Kaixing, ZHOU Chunjie, TIAN Yuchu, et al. Assessing the physical impact of cyberattacks on industrial cyber-physical systems[J]. IEEE Transactions on Industrial Electronics, 2018, 65(10): 8153. DOI: 10.1109/TIE.2018.2798605

[22] 周翔荣, 孙子文. 工业信息物理系统漏洞节点的攻击图评估方法[J]. 控制工程, 2024, 31(12): 2256
ZHOU Xiangrong, SUN Ziwen. Attack graph evaluation method for vulnerable nodes in industrial cyber physical systems[J]. Control Engineering of China, 2024, 31(12): 2256. DOI: 10.14107/j.cnki.kzgc.20220418

[23] 杨林. 动态网络环境下攻防博弈威胁预测和防御方法研究[D]. 长沙:国防科技大学, 2020
YANG Lin. Research on threat prediction and defensemethod of dynamic network attack anddefense game[D]. Changsha: National University of Defense Technology, 2020. DOI: 10.27052/d.cnki.gzjgu.2020.000644

(编辑　张　红)