

DOI:10.11918/202403014

工业互联网工程供应链应急处置主体融合博弈分析

赵娜¹, 李晓莲¹, 郑大昭²

(1. 哈尔滨商业大学 管理学院, 哈尔滨 150028; 2. 香港理工大学 商学院, 香港 999077)

摘要: 工业互联网工程建设环境不确定性增加, 应急能力逐渐成为工程项目顺利实施的重要影响力量。为提升工业互联网工程供应链应急能力, 考虑主体间融合交互关系, 针对工业互联网工程建设阶段, 对工业互联网工程供应链应急处置主体的博弈关系进行研究, 建立融合演化博弈模型, 揭示工业互联网工程供应链应急处置主体间的融合机理。仿真模拟结果表明: 工业互联网工程供应链企业利益联结是进行应急处置主体融合的关键动力, 互利互惠互信是融合的前提基础; 当企业持续性融合利润增量和所得补贴大于链上其他企业采取阶段性融合策略的影响时, 无论企业初始意愿如何, 参与者都会选择持续性融合策略, 反之演化结果则会出现分化。把握应急处置融合机理, 激励应急处置主体积极参与应急融合, 提高应急处置效率及应急处置能力, 有助于保证供应链稳定, 确保工业互联网工程建设顺利实施。

关键词: 工业互联网工程; 供应链; 应急能力; 主体融合; 演化博弈

中图分类号: C934; TU714

文献标志码: A

文章编号: 0367-6234(2024)09-0076-09

Integrated game analysis of emergency response entities in industrial internet engineering supply chain

ZHAO Na¹, LI Xiaolian¹, ZHENG Dazhao²

(1. School of Management, Harbin University of Commerce, Harbin 150028, China;
2. School of Business, Hong Kong Polytechnic University, Hong Kong 999077, China)

Abstract: With the increase of uncertainty in the construction environment of industrial internet engineering, emergency response capability has gradually become an important factor in ensuring the successful implementation of engineering projects. In order to improve the emergency response ability of industrial internet engineering supply chain, considering the interactive relationships between entities, the game relationship among emergency response entities of industrial internet engineering supply chain is studied in the construction stage of industrial internet engineering projects. A fusion evolutionary game model is established to reveal the integration mechanism of emergency response entities of industrial internet engineering supply chain. The simulation results show that the interest connection of industrial internet engineering supply chain enterprises is the key driving force for the integration of emergency response entities. Mutual benefit, reciprocity and mutual trust serve as the prerequisite basis of successful integration. When the continuous intergration profit increment and income subsidies of participating enterprises outweigh the impact of phased integration strategies adopted by other enterprises on the chain, participants will choose continuous integration strategies regardless of the initial intention of enterprises. Conversely, the evolutionary results will diverge. Understanding the mechanism of emergency response integration and incentivizing active participation of emergency response entities in integration can improve emergency response efficiency and emergency response capacities, ensuring the stability of the supply chain and facilitating the successful implementation of industrial internet project construction.

Keywords: industrial internet engineering; supply chain; emergency capacity; subject fusion; evolutionary game

工业互联网作为设备、人员和环境之间高度协同与共享的智能网络, 成为企业保障供应链韧性的重要抓手^[1], 越来越多的企业开始推动工业互联网工程建设。在与新技术、新设施融合赋能之际, 新老

基建衔接合璧之时, 供应链连接节点数量日益增多, 依存关系日益紧密复杂。当突发公共事件发生时, 任意节点产生的风险都可能会快速传递到供应链上下游, 进而扩散到整个网络^[2]。因此, 工业互联网

收稿日期: 2024-03-05; 录用日期: 2024-04-03; 网络首发日期: 2024-06-25

网络首发地址: <https://link.cnki.net/urlid/23.1235.T.20240624.1644.020>

基金项目: 国家社会科学基金(21BGL124)

作者简介: 赵娜(1982—), 女, 教授, 博士生导师

通信作者: 赵娜, zhaona@hit.edu.cn

工程供应链(industrial internet engineering supply chain, IIESC)如何提升应急能力成为焦点。供应链主体相互影响的特征使得相关主体协同与融合合作成为工业互联网工程管理的重点内容^[3],应急处置主体间的融合机理也成为重要问题之一。而在由应急组成的融合组织中,成员行为相互影响,存在动态演化关系。演化博弈能反映各参与方在有限理性下通过复制动态机制缓慢学习并达到均衡的过程^[4],为分析 IIESC 应急处置主体的合作行为及其演化过程提供了良好的方法与工具^[5-6]。在建 IIESC 相关研究一般聚焦在技术方面或者从定性角度分析工业互联网供应链风险,例如讨论其安全保障、隐私数据保护、安全检测、即插即用工业互联网网关解决方案等问题^[7-10],或是研究企业建设工业互联网平台的决策机理^[11],对应急处置主体的博弈研究较少。因此,本文针对工业互联网工程建设阶段,为提升 IIESC 主体的应急处置能力,通过建立数理博弈模型,揭示 IIESC 应急处置主体间的融合机理,探究如何提高应急处置效率及能力,提出相应对策建议,以保证工业互联网工程建设稳定实施,并补充完善现有研究。

1 IIESC 及其应急处置主体融合

1.1 IIESC

一些学者对工业互联网供应链进行了定义,例如,樊佩茹等^[12]认为工业互联网供应链是在工业互联网架构下,由研发、原材料采购、组装等环节中一组过程和资源构成的网络;张晓菲等^[13]认为工业互联网供应链是指工业互联网相关软硬件产品,或工业互联网平台生产及流通中,相关上下游企业组成的链路结构。工业互联网的发展分为建设和运营两个阶段,建设阶段始于工业互联网项目的建立,止于工业互联网系统通过有效性测试后投入使用^[14]。本文聚焦于工业互联网工程在建过程,将工业互联网供应链描述为工业互联网工程供应链,即为工业互联网工程建设提供产品或服务的供应链,是由为工业互联网工程建设阶段提供相关物资、人员和信息等资源的各主体组成的供应链,以帮助最终实现工业互联网基础设施运营前的建设。

工业互联网工程建设过程中涉及各类主体,如网络提供商、软硬件供应商、底层资源提供商等。在全球新技术革命和突发公共事件频发的双重挑战下,流行病、网络攻击、自然灾害、产品和服务问题或政治动荡等事件都可能导致工程供应链中断^[15-16],延误或中断工业互联网项目^[17]。为保证工业互联

网项目的顺利实施,各主体会进行应急处置。而 IIESC 作为为工业互联网项目目标服务的链条,具有临时性特征^[18],应急处置主体在进行融合决策时可能也会受到临时性组织的影响,从而导致供应链应急处置主体融合缺乏足够的稳定性和连续性。

1.2 IIESC 应急处置主体融合

工业互联网作为新基建的重要组成部分,其供应链安全直接影响着工业互联网安全^[13]。如今社会面临着多元化、急速变迁的新型风险,应再造应急治理共同体以应对频发的突发公共事件风险^[19],即随着企业面临突发事件概率的增加,企业需要关注内外部应急能力,联合供应链利益相关方进行资源和能力的协调,不断提高供应链应急能力,以便更有效地规避、控制或应对风险,快速从危机中恢复。相比于传统信息化建设,工业互联网复杂程度更高,其建设过程中需要持续的技术、资金和人员投入。现阶段,中国工业互联网的建设大多集中在数字化基础较好、对自身数字化转型定位清晰的大型信息通信或制造企业,即企业主导的工业互联网^[14]。在企业主导的工业互联网中,企业致力于构建工业互联网合作生态,在此情形下,以资源整合、协同信任和信息共享为基础的融合治理是应急管理的必然趋势,以融合方式提升应急能力,能够减少资源浪费,提高应急能力建设效率。

应急合作是通过参与、协调与互动有效整合并协调多元主体优势资源,以应对突发事件的合作行为,是一个贯穿事前、事中、事后全过程的动态闭环链^[20]。深度融合是主体跨越组织边界、结成利益共同体,以实现优势互补和资源共享,形成互利共生状态^[21]。结合应急合作与深度融合概念,本文将 IIESC 应急处置主体融合定义为以 IIESC 企业为主体,基于主体的资源禀赋和环境,通过整合、学习、渗透等“双向融合”,带动各类资源优化重组,使应急能力达到所需状态,是基于多主体协同、流程整合、多要素整合而形成的一种互利共生关系的过程,最终目标是提升应急能力以保证在突发公共事件下工业互联网工程的顺利实施。因此应急处置主体融合是融合方向、动力、基础与成效的有机结合,见图 1。

1) 融合方向,分为向内融合和向外融合。向内融合是应急处置主体在内部进行的自我探索和建设的过 程,是企业通过组织结构优化、业务流程优化、实施技术管理等措施对自身应急能力的提升,有助于增强企业内在稳定性。向外融合是应急处置主体与其他主体互动交流、协同建设应急能力的过程,有助于增强企业外部稳定性。

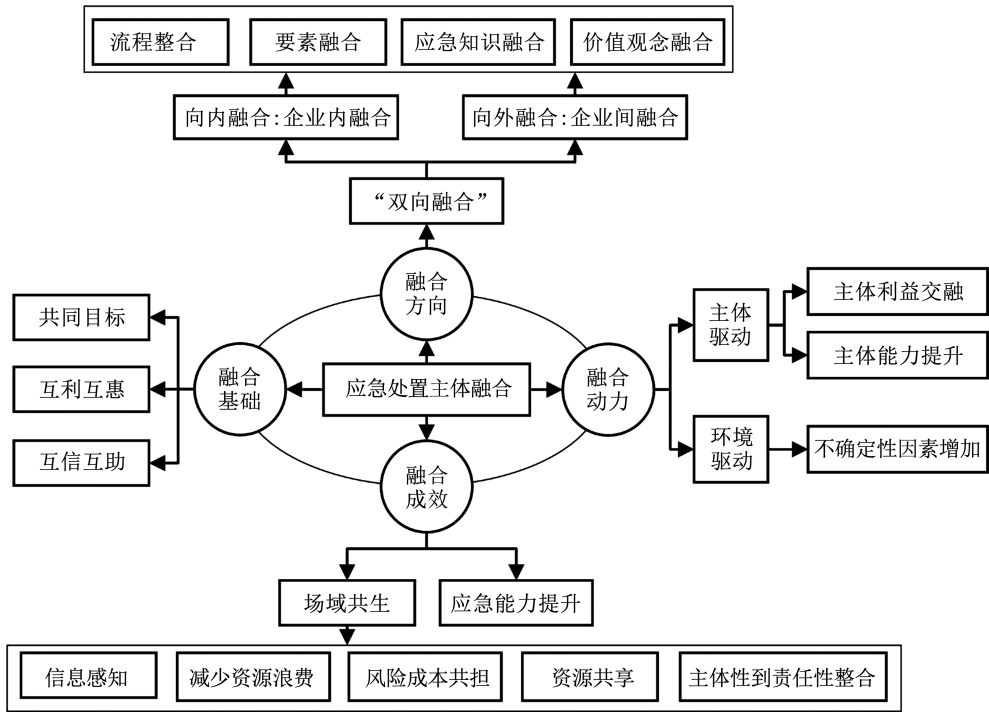


图 1 IIESC 应急主体融合内涵解析框架

Fig.1 IIESC emergency subject fusion connotation analysis framework

2) 融合基础。共同目标、互利互惠和互信互助是应急处置主体融合的基础,良好的基础能够保证应急处置主体融合系统持续运行及融合效应的实现。为在演化发展中维持各参与者的利益平衡,应急处置主体融合系统中各主体会调整其行为反应^[22]。

3) 融合动力。应急处置主体融合的动力可分为主体驱动和环境驱动。主体驱动主要体现在两大方面:一是 IIESC 中各主体利益交融,突发公共事件可能会导致工业互联网工程的中断或延迟,会影响各利益相关主体,各主体会通过融合合作实现风险和应急管理,追求效益最大化;二是主体能力提升, IIESC 企业通过融合实现优势互补、减少资源浪费,更高效地提升自身能力。环境驱动是指不确定性因素的增加使得企业意识到应急能力提升与应急融合的重要性。

4) 融合成效。通过应急处置主体融合,各主体能够实现场域共生和应急能力提升,使各主体责任、权力与利益相互匹配,调动应急处置主体的积极性。

应急处置主体融合强调建设商、服务商、供应商等工业互联网企业之间的紧密应急合作与协同,在融合时不仅仅考虑主体知识水平的融合^[23],还考虑要素融合、流程整合等方面。针对应急融合问题,徐选华等^[23]提出了基于主体知识水平的融合方法。考虑到主体决策行为对应急融合的影响,本文聚焦不在融合方法的提出,而在主体间的交互机制上,因此后文利用演化博弈模型分析应急处置主体的融

合决策及其演化规律。

2 演化博弈模型构建

应急处置主体融合过程中企业的行为选择是基于自身利益考量而进行相互博弈的结果,各主体会因为利益、信任、自主性等问题改变行为和决策,参与主体之间的行为会影响整个应急融合的结果,他们的抉择符合博弈论的范式。本文运用演化博弈模型分析 IIESC 企业应急融合的演化路径、融合系统的稳定性及影响因素,作出如下假设:

IIESC 系统中存在企业 A 和 B 两类有限理性的博弈参与主体^[24]。当突发事件发生时,企业为减缓或控制风险会与相关企业展开合作,然而在应急处置主体融合系统中,企业的主观能动性会受到经济效益的约束,企业参与的应急融合可能是持续性的,也可能是阶段性的。持续性融合(P)是指 IIESC 企业在应急融合中,有意愿将临时的应急组织长期化,与相关企业建立长期合作关系,共同开展应急能力提升工作,并在日常工作中保持密切的沟通和协调;阶段性融合(S)是指企业在工业互联网工程建设期间进行的临时性合作,针对工业互联网工程建设情况共同展开应急能力提升工作。因此设定 IIESC 企业在应急处置融合过程中的应急行为策略集合是 {持续性融合,阶段性融合}。

企业之间不存在补贴机制。企业应急行为的补贴措施由第三方实施^[25],即应急小组。工业互联网工程建设中,企业日常对各种数据进行收集和分析。

当发生突发事件时,涉事环节相关企业或人员需及时向工业互联网应急小组汇报,并联系企业或人员为应急处置的实施提供安全支持;应急事件结束后,应急小组需要对实施情况进行评估。因此,应急小组会对参与持续性融合的企业根据其成本予以补贴,记补贴系数为 μ ,而选择阶段性融合的企业不能得到该补贴。

企业之间存在外部效应。IIESC 合作伙伴风险是阻碍工业互联网工程建设的最根本因素^[14]。由于企业间的关系也会对应急融合产生重要影响,因此将企业间相互影响的作用纳入模型,即当企业 A 和企业 B 都选择或有一方选择持续性融合策略时,企业能够获得正向或负向外部效应,记企业 A 对企业 B 的外部效应系数为 θ_1 ,企业 B 对企业 A 的外部

效应系数为 $\theta_2(\theta_i(0,1),i=1,2)$ 。

企业对突发事件进行应急处置融合能够获得物质利益与非物质利益(声誉、社会认可等)。当企业参与阶段性融合时,企业能够获得收益 w ;企业选择持续性融合时能够获得增益,增量为 $rw,r>0$ 为持续性融合增益系数。同时,企业需要付出阶段性融合成本 c ,包括前期沟通、信息共享、信任建立等成本,持续性融合成本增量为 $pc,p>0$ 为成本增量系数。

在有限理性下,企业 A 面对突发公共事件选择持续性融合的概率为 $x(x \in [0,1])$,企业 B 面对突发公共事件选择持续性融合的概率为 $y(y \in [0,1])$,则突发公共事件应急融合博弈模型支付矩阵见表 1。

表 1 IIESC 企业博弈支付矩阵

Tab.1 IIESC enterprise game payment matrix

企业 A	企业 B	
	持续性融合(P) y	阶段性融合(S) $1-y$
持续性融合(P) x	$(1+r)w - (1-\mu)(1+p)c + \theta_2(1+r)w$ $(1+r)w - (1-\mu)(1+p)c + \theta_1(1+r)w$	$(1+r)w - (1-\mu)(1+p)c - \theta_2w$ $w - c + \theta_1(1+r)w$
阶段性融合(S) $1-x$	$w - c + \theta_2(1+r)w$ $(1+r)w - (1-\mu)(1+p)c - \theta_1w$	$w - c$ $w - c$

企业 A 选择策略 P、S 的期望收益、平均期望收益及其复制动态方程分别为

$$U_{A1} = y[(1+r)w - (1-\mu)(1+p)c + \theta_2(1+r)w] + (1-y)[(1+r)w - (1-\mu)(1+p)c - \theta_2w]$$

$$U_{A2} = y[w - c + \theta_2(1+r)w] + (1-y)(w - c)$$

$$U_A = xU_{A1} + (1-x)U_{A2}$$

$$G(x) = \frac{dx}{dt} = x(U_{A1} - U_A) = x(1-x)(U_{A1} - U_{A2}) = x(1-x)(\mu c - pc + rw - \theta_2w + \mu pc + \theta_2wy)$$

式中: U_{A1} 、 U_{A2} 分别为企业 A 持续性融合、阶段性融合策略的期望收益, U_A 为企业 A 平均期望收益, $G(x)$ 为复制动态方程。

企业 B 选择策略 P、S 的期望收益、平均期望收益及其复制动态方程分别为

$$U_{B1} = x[(1+r)w - (1-\mu)(1+p)c + \theta_1(1+r)w] + (1-x)[(1+r)w - (1-\mu)(1+p)c - \theta_1w]$$

$$U_{B2} = x[w - c + \theta_1(1+r)w] + (1-x)(w - c)$$

$$U_B = yU_{B1} + (1-y)U_{B2}$$

$$G(y) = \frac{dy}{dt} = y(U_{B1} - U_B) = y(1-y)(U_{B1} - U_{B2}) = y(1-y)(\mu c - pc + rw - \theta_1w + \mu pc + \theta_1wx)$$

式中: U_{B1} 、 U_{B2} 分别为企业 B 持续性融合、阶段性融合策略的期望收益, U_B 为企业 B 平均期望收益, $G(y)$ 为复制动态方程。

3 模型分析

令 $G(x) = 0, G(y) = 0$,根据微分方程稳定性,当 x, y 满足 $G(x) = 0, \partial G(x)/\partial x < 0$ 或 $G(y) = 0, \partial G(y)/\partial y < 0$ 时,该策略处于稳定状态。因此可以得到企业 A 和企业 B 的局部均衡点,分别为 $(0,0)$ 、 $(0,1)$ 、 $(1,0)$ 、 $(1,1)$, $D(x_D) = [(p - \mu - \mu p)c - rw]/\theta_1w + 1, y_D = [(p - \mu - \mu p)c - rw]/\theta_2w + 1$ 。可以利用雅可比矩阵(J)分析平衡点的稳定性问题,根据上述复制动态方程可得到

$$J = \begin{bmatrix} \frac{\partial G(x)}{\partial x} & \frac{\partial G(x)}{\partial y} \\ \frac{\partial G(y)}{\partial x} & \frac{\partial G(y)}{\partial y} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

式中: $a_{11} = -(2x - 1)(\mu c - pc + rw - \theta_2w + \mu pc + \theta_2wy), a_{12} = -\theta_2wx(x - 1), a_{21} = -\theta_1wy(y - 1), a_{22} = -(2y - 1)(\mu c - pc + rw - \theta_1w + \mu pc + \theta_1wx)$ 。

令 $T = rw + \mu(1+p)c - cp$,有

$$\det J = a_{11}a_{22} - a_{12}a_{21} = (2x - 1)(2y - 1)(T - \theta_2w + \theta_2wy)(T - \theta_1w + \theta_1wx) -$$

$$\theta_1 \theta_2 w^2 xy(x-1)(y-1)$$

$$\text{tr } J = a_{11} + a_{22} = (1-2x)(T-\theta_2 w + \theta_2 wy) + (1-2y)(T-\theta_1 w + \theta_1 wx)$$

从而可得该系统 5 个均衡点的 $\det J$ 和 $\text{tr } J$, 见表 2。

表 2 演化均衡点的 $\det J$ 和 $\text{tr } J$

Tab. 2 Det J and $\text{tr } J$ of evolutionary equilibrium points

均衡点	$\det J$	$\text{tr } J$
(0,0)	$(T-\theta_2 w)(T-\theta_1 w)$	$(T-\theta_2 w) + (T-\theta_1 w)$
(0,1)	$-T(T-\theta_1 w)$	$\theta_1 w$
(1,0)	$-(T-\theta_2 w)T$	$\theta_2 w$
(1,1)	T^2	$-2T$
D	$-T^2 \frac{(T-\theta_2 w)(T-\theta_1 w)}{\theta_1 \theta_2 w^2}$	0

当 $\det J > 0, \text{tr } J < 0$ 时, 均衡点为演化稳定策略 (evolutionary stable strategy, ESS)。由表 2 可知, 均衡点 D 的 $\text{tr } J = 0$, 均衡点 (0,1) 和 (1,0) 的 $\text{tr } J > 0$, 因此这些点必然不是 ESS, 剩余两个均衡点需要根据 T 的大小进行判断, 可得到以下命题:

命题 1 当 $T < 0$ 时, 只有 (0,0) 是 ESS。此时持续性融合所得收益增量和补贴小于其成本增量, 对应的占优策略为 (S,S)。

此条件下融合主体之间相互影响作用较大, 应急融合系统中补贴力度较小, 企业进行持续性融合的成本较大, 各主体选择持续性融合的概率均为最低。IIESC 企业在工业互联网工程建设期间就相关问题开展阶段性的应急处融合, 获得较小利润 w 。图 2 为演化博弈均衡点相位图。由图 2(a) 可知, (0,0) 为稳定均衡点。无论博弈双方初始意愿如何, 经过反复博弈后最终会选择阶段性融合。现实中造成企业难以实现持续性融合的原因较为复杂, 缺乏长期目标、利益分配、技术或文化差异、利益相

关者的重要程度等都会对应急处融合持续性参与决策产生影响。

命题 2 当 $T > \theta_1 w, T > \theta_2 w$ 时, 只有 (1,1) 是 ESS。此条件下持续性融合所得收益增量和补贴大于其成本增量及另一方选择阶段性融合的影响, 此时演化趋势为 (P,P)。

命题 2 表明, 如果要保证所有参与者都持续性地参与融合, 确保 IIESC 应急能力有效提升, 需要重视参与者之间相互影响作用的大小。当持续性融合收益增量小于成本增量及利益相关者决策造成的影响时, 应急小组的补贴需要能够弥补他们之间的差额。持续性融合能够帮助工业互联网工程企业实现长期合作, 形成发展合力。

命题 3 在 $0 < T < \theta_1 w, 0 < T < \theta_2 w$ 条件下, IIESC 应急处融合主体融合系统的 ESS 有 (1,1) 和 (0,0)。

此条件下持续性融合所得收益增量和补贴大于其成本增量, 但是不能抵消利益相关者带来的影响, 此时折线 ADC 是博弈系统收敛于不同状态的临界线, 见图 2(c)。在区域 I 中, 企业持续性融合概率均大于临界值, 系统向 (1,1) 收敛; 在区域 III 中, 系统向 (0,0) 收敛; 而在区域 II 和 IV 中, IIESC 企业持续性融合具有不稳定性。当系统的初始状态位于折线 ADC 的右上方 (区域 $ABCD$) 时, 企业 A 和企业 B 的策略选择向 (P,P) 收敛, 实现帕累托最优, 此时, 至少有一方认为持续融合应急处合作所带来的收益会大于成本; 同理, 当系统的初始状态位于折线 ADC 的左下方 (区域 $AOCD$), 博弈最终收敛于 (S,S), 此时至少有一方认为持续融合所带来的收益会小于成本。 $ABCD$ 的面积越大, 企业博弈的长期均衡结果收敛于 (P,P) 的概率越大, $S_{ABCD} = 1 - (x_D + y_D)/2$, 影响企业持续性融合的因素有 $p, \mu, c, r, w, \theta_1, \theta_2$ 。

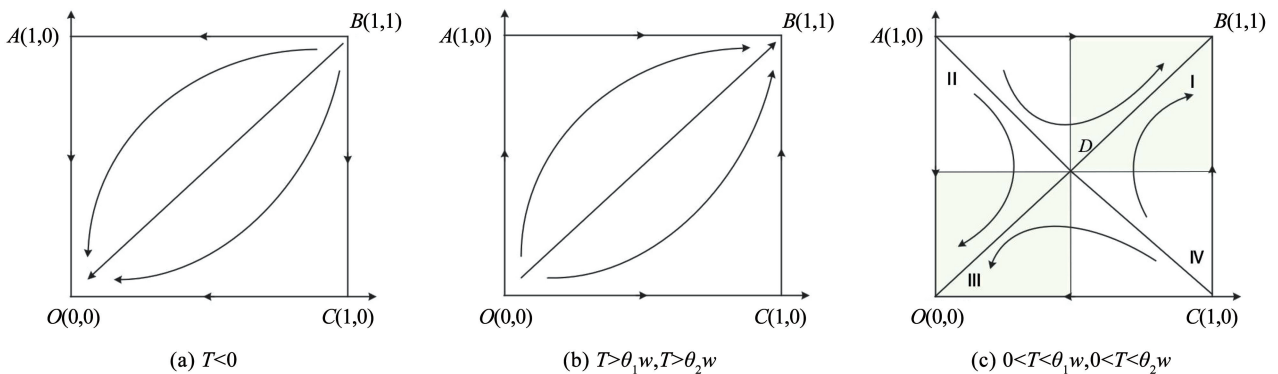


图 2 演化博弈均衡点相位图

Fig. 2 Evolutionary game equilibrium point phase diagram

4 数值分析

为直观反映各参数对主体策略的影响,利用 MATLAB 构建仿真模型对演化博弈进行数值分析。基于前文分析的 3 种不同条件分别对参数初始值进行设定:1) $T < 0$ 时,假设 $c = 100, p = 1, w = 150, r = 0.3, \mu = 0.2, \theta_1 = \theta_2 = 0.2$; 2) $T > \theta_1 w, T > \theta_2 w$ 时,假设 $c = 100, p = 1, w = 150, r = 1, \mu = 0.2, \theta_1 = \theta_2 = 0.2$; 3) $0 < T < \theta_1 w, 0 < T < \theta_2 w$ 时,假设 $c = 100, p = 1, w = 150, r = 0.5, \mu = 0.2, \theta_1 = \theta_2 = 0.2$ 。

企业初始意愿对演化结果的影响见图 3。图 3(a) 模拟了当参与者初始策略选择的概率均为

0.5 时,3 种条件下 IIESC 企业的策略演化结果。由图 3 可知:在条件 1) 下,参与主体选择持续性融合的概率逐渐趋近于 0,即企业会选择阶段性融合策略;在条件 2) 下,参与主体选择持续性融合的概率逐渐趋近于 1,即企业会选择持续性融合策略;在条件 3) 下,随着时间的推移,主体的策略与其初始意愿有关。为进一步验证演化路径的稳定性,对参与主体不同初始值下的博弈进行模拟。在条件 1) (图 3(b)) 和条件 2) (图 3(c)) 下,演化结果不受企业初始意愿的影响;而在条件 3) (图 3(d)) 下,演化结果出现分化,计算可得点 D 的坐标为 (0.5, 0.5), 图中所得结果与前文理论分析相符。

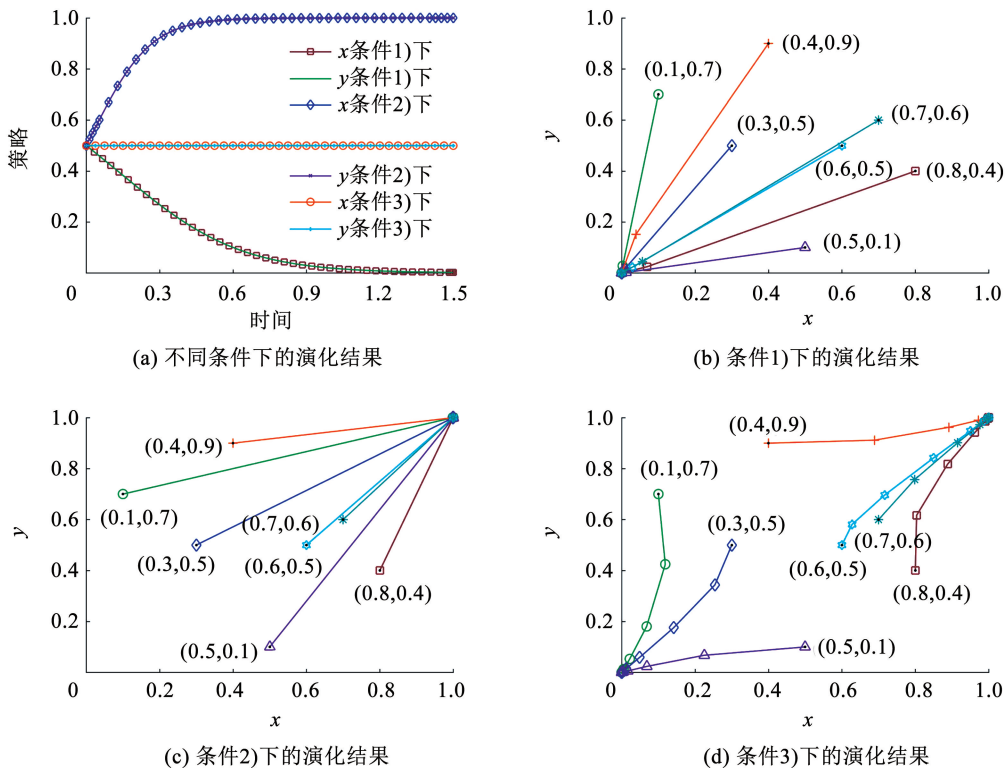


图 3 企业初始意愿对演化结果的影响

Fig. 3 Influence of initial intention of enterprises on evolution results

由于在满足条件 1) 和条件 2) 的情况下演化结果不会出现分化,因此为分析各参数对演化结果的影响,以条件 3) 的参数设定为基准,将 x, y 初始值设置为 0.6、0.5,模拟持续性融合收益增量系数、成本增加系数、收益成本比、补贴系数、外部效应系数对演化结果的影响。

收益和成本增量系数及其比值对博弈系统演化的影响见图 4。由图 4 可知, IIESC 企业持续性融合成本增量系数与双方策略选择成反比,收益增量系数与收益成本比成正相关。随着成本增量系数的增加, x, y 趋向于 0 的速度越快;随着收益增量系数与

收益成本比的增加, x, y 趋向于 1 的速度越快。结果表明,持续性融合成本越小、收益越大,企业越愿意持续参与融合应急。由于持续性融合成本的存在,企业参与持续性融合的收益未必会更高,因此企业在选择策略时会受到成本的影响,所以第三方需要通过一些措施来不断降低企业持续参与融合应急的成本,如第三方可以利用信息技术提升融合效率,同时要根据实际应急能力水平和应急情况,改善信息资源质量和优化功能以更好地促进各企业的资源、能力互补,提高应急融合的行动效率。企业自身需要注意加强对共享资源的学习、吸收和转化能力,

从而提升企业持续性融合应急时的收益率。

补贴系数和外部效应系数对博弈系统演化的影响见图 5。由图 5(a)可知,补贴系数与双方策略选择成正比。随着补贴系数的增加, x, y 趋近 1 的速度越快。可见,在实际应急工作中应突出第三方的作用。由于 IIESC 中各企业相互合作建设工业互联网工程,应急小组作为应急过程中的重要主体,应该充分发挥监管联结作用,促进各方资源整合和企业间的沟通交流、提高企业间的信任和监管效率以及降低企业应急融合的成本,根据企业目标对不同利

益相关者实施不同的激励或约束策略,并不断完善反馈机制,以充分调动 IIESC 企业持续性融合的积极性。由图 5(b)可知,外部效应系数与双方策略选择成反比。其他参与者采取阶段性融合策略会产生消极影响,可能迫使企业改变参与持续性融合的意见,因此在应急处置主体融合中,要不断完善沟通机制,明确应急融合中各主体的权责关系,降低外部效应的影响。同时,企业需要定期评估自身行为,加强社会责任感,降低企业对其他主体的负面影响。

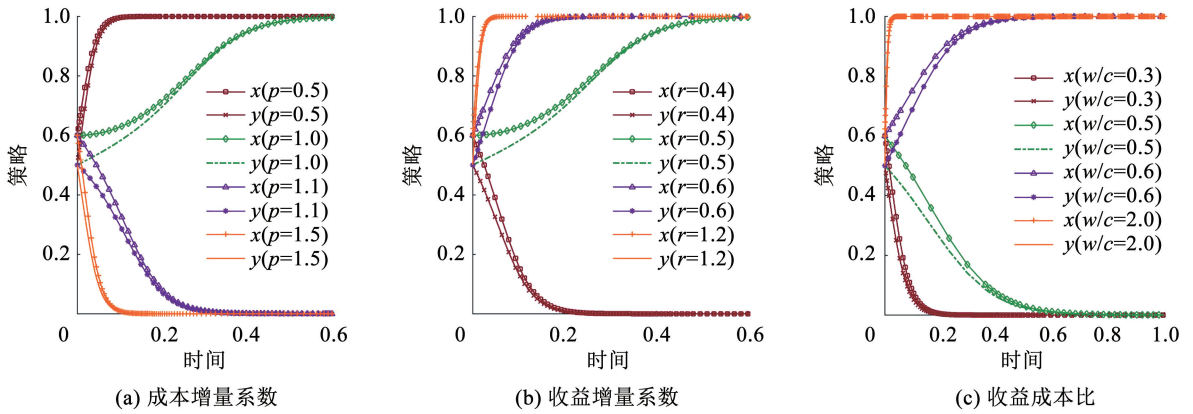


图 4 收益和成本增量系数及其比值对博弈系统演化的影响

Fig. 4 Effect of incremental coefficients of benefits and costs and their ratios on evolution of game systems

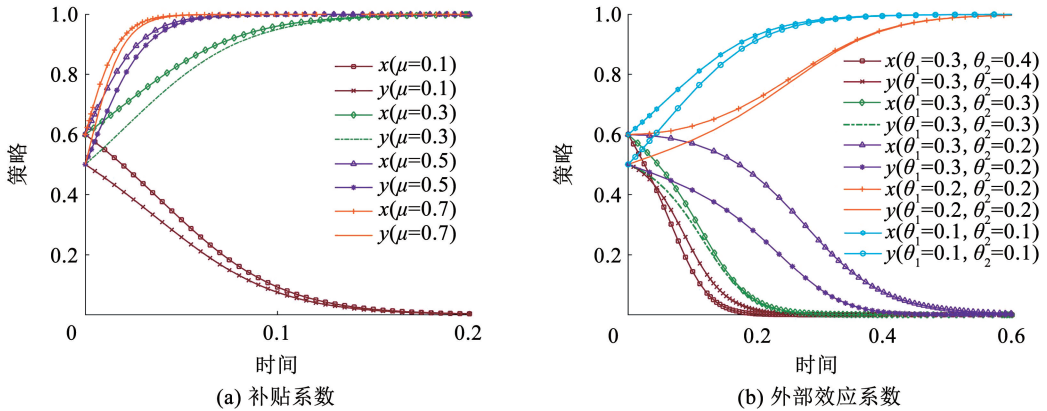


图 5 补贴系数和外部效应系数对博弈系统演化的影响

Fig. 5 Effect of subsidy coefficient and external effect coefficient on evolution of game system

5 结 论

本文在应急处置主体融合的基础上,通过建立演化博弈模型探究 IIESC 企业应急处置融合行为演化策略,并利用数值分析模拟各参数对 IIESC 企业融合策略演化趋势的影响,得到如下结论:

1)从工程建设角度定义工业互联网供应链,即为工业互联网工程建设提供产品或服务的供应链,

由为工业互联网工程建设阶段提供相关物资、人员和信息等资源的各主体组成。结合应急合作与深度融合概念,将 IIESC 应急处置主体融合定义为以 IIESC 企业为主体,基于主体的资源禀赋和环境,促使各类资源优化重组,使应急能力达到所需状态,是融合方向、动力、基础与成效的有机结合。IIESC 企业利益联结、环境变化和能力提升是他们参与应急融合的动力,共同目标、互利互惠、互信互助是应急

融合的基础。IIESC 应急处置主体融合有助于企业高效提升应急能力,保证工业互联网工程顺利建设。

2) 利用演化博弈模型研究 IIESC 应急处置主体融合的行为策略和考虑外部效应的重要性。研究发现:应急处置融合时,IIESC 主体选择持续性融合的概率与收益增量成正比,与成本增量、外部效应成反比,提高持续性融合收益、降低成本、减弱企业间的影响能够使应急处置主体融合更长效。

3) 应急小组的激励策略是影响企业策略选择的重要因素,当应急小组对持续性融合的补贴大于成本增量和外部效应与收益增量之差时,无论参与者初始意愿如何,博弈系统最终都会收敛于(持续性融合,持续性融合)。因此,在应急融合中要建立并完善定期联系、信息共享、监测预警、联动响应的融合联动机制。

本文在研究应急能力的提升问题时一定程度上依赖于参数值设定,未来研究应结合实证数据,对现有研究进行补充完善。

参考文献

- [1] ANGELOPOULOS S, BENDOLY E, FRANSOO J, et al. Digital transformation in operations management: fundamental change through agency reversal [J]. *Journal of Operations Management*, 2023, 69(6): 876. DOI:10.1002/joom.1271
- [2] WANG Jiepeng, ZHOU Hong, JIN Xiaodan. Risk transmission in complex supply chain network with multi-drivers [J]. *Chaos, Solitons & Fractals*, 2021, 143(1): 110259. DOI:10.1016/j.chaos.2020.110259
- [3] ZHAO Na. Managing interactive collaborative mega project supply chains under infectious risks[J]. *International Journal of Production Economics*, 2019, 218: 275. DOI:10.1016/j.ijpe.2019.06.008
- [4] 贺一堂, 谢富纪. 产-学研协同创新的随机演化博弈分析[J]. *管理评论*, 2020, 32(6): 150
HE Yitang, XIE Fuji. Stochastic evolutionary game analysis on the industry-university-institute collaboration innovation [J]. *Management Review*, 2020, 32(6): 150. DOI:10.14120/j.cnki.cn11-5057/f.2020.06.011
- [5] 薛小龙, 韩喜双, 王要武. 工程项目谈判行为的动态演化分析[J]. *哈尔滨工业大学学报*, 2010, 42(11): 1775
XUE Xiaolong, HAN Xishuang, WANG Yaowu. Dynamic evolution of negotiation behaviors in construction projects [J]. *Journal of Harbin Institute of Technology*, 2010, 42(11): 1775
- [6] 周晓阳, 李长长, 刘莹, 等. 工业互联网平台、开发商与企业的三方协作演化策略——兼论政府补贴和收益共享的作用[J]. *中国管理科学*, 2024, 32(1): 276
ZHOU Xiaoyang, LI Zhangzhang, LIU Ying, et al. Tripartite cooperation evolutionary strategy of industrial internet platform, developer and enterprise: the role of government subsidies and revenue sharing[J]. *Chinese Journal of Management Science*, 2024, 32(1): 276. DOI:10.16381/j.cnki.issn1003-207x.2021.2558
- [7] ZHAO Jiang, WU Dan. The risk assessment on the security of industrial internet infrastructure under intelligent convergence with the case of G. E.'s intellectual transformation [J]. *Mathematical Biosciences and Engineering*, 2022, 19(3): 2896. DOI:10.3934/mbe.2022133
- [8] XUE Yudai, WANG Jingsong, SHI Kai, et al. A privacy-preserving model for blockchain-based data sharing in the industrial internet [J]. *Transactions on Emerging Telecommunications Technologies*, 2024, 35(4): e4749. DOI:10.1002/ett.4749
- [9] QURESHI K N, RANA S S, AHMED A, et al. A novel and secure attacks detection framework for smart cities industrial internet of things[J]. *Sustainable Cities and Society*, 2020, 61: 102343. DOI:10.1016/j.scs.2020.102343
- [10] LIU Chao, SU Ziwei, XU Xun, et al. Service-oriented industrial internet of things gateway for cloud manufacturing[J]. *Robotics and Computer-Integrated Manufacturing*, 2022, 73: 102217. DOI:10.1016/j.rcim.2021.102217
- [11] 白仲林, 金琼. 工业企业互联网平台赋能决策的机理与实证研究——基于结构化离散博弈模型的分析[J]. *南开经济研究*, 2022(8): 3
BAI Zhonglin, JIN Qiong. The mechanism and empirical research of empowerment decision by industrial enterprise internet platform: analysis based on the structured discrete game model[J]. *Nankai Economic Studies*, 2022(8): 3. DOI:10.14116/j.nkes.2022.08.001
- [12] 樊佩茹, 李俊, 王冲华, 等. 工业互联网供应链安全发展路径研究[J]. *中国工程科学*, 2021, 23(2): 56
FAN Peiru, LI Jun, WANG Chonghua, et al. Security development path for industrial internet supply chain [J]. *Strategic Study of CAE*, 2021, 23(2): 56. DOI:10.15302/J-SSCAE-2021.02.008
- [13] 张晓菲, 卢春景, 于盟. 工业互联网供应链安全风险研究[J]. *网络空间安全*, 2020, 11(7): 23
ZHANG Xiaofei, LU Chunjing, YU Meng. Research on the security risk of industrial internet supply chain [J]. *Cyberspace Security*, 2020, 11(7): 23
- [14] WEI Shouyuan, ZHU Yuming, ZHANG Jing, et al. Analysis on risk factors of enterprise dominant industrial internet build-up[C]//2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). Macao: IEEE, 2019: 1169. DOI:10.1109/ieem44572.2019.8978841
- [15] LAGUIR I, MODGIL S, BOSE I, et al. Performance effects of analytics capability, disruption orientation, and resilience in the supply chain under environmental uncertainty [J]. *Annals of Operations Research*, 2023, 324(1/2): 1269. DOI:10.1007/s10479-021-04484-4
- [16] LIANG Chen, ZHU Minghao, LEE P K C, et al. Combating extreme weather through operations management: evidence from a natural experiment in China[J]. *International Journal of Production Economics*, 2024, 267: 109073. DOI:10.1016/j.ijpe.2023.109073
- [17] KARNIOUCHINA K, SARANGEE K, THEOKARY C, et al. The impact of the covid-19 pandemic on restaurant resilience: lessons, generalizations, and ideas for future research[J]. *Service Science*, 2022, 14(2): 121. DOI:10.1287/serv.2021.0293
- [18] 朱建波, 时茜茜, 张劲文, 等. 考虑保险机构参与的重大工程风险管理激励模型[J]. *中国管理科学*, 2022, 30(6): 1

- ZHU Jianbo, SHI Qianqian, ZHANG Jinwen, et al. An incentive model in risk management of mega project considering insurance company involved [J]. Chinese Journal of Management Science, 2022, 30(6): 1. DOI:10.16381/j.cnki.issn1003-207x.2019.2067
- [19] 詹国辉, 戴芬园. 应急治理共同体: 风险社会中突发公共事件治理的新议题[J]. 哈尔滨工业大学学报(社会科学版), 2022, 24(6): 75
- ZHAN Guohui, DAI Fenyuan. Emergency governance community: new topic of public emergency governance in risk society [J]. Journal of Harbin Institute of Technology(Social Sciences Edition), 2022, 24(6): 75. DOI:10.16822/j.cnki.hitskb.2022.06.008
- [20] 王红梅, 石银凤, 郭小倩. 重大突发公共卫生事件应急合作网络演化及绩效研究——以武汉市应对新冠肺炎疫情为例[J/OL]. 管理评论. (2023-01-18)[2024-02-06]. <https://kns.cnki.net/kcms/detail/11.5057.F.20230118.0930.002.html>
- WANG Hongmei, SHI Yinfeng, GUO Xiaoqian. Evolution and performance of cooperation network for major public health emergencies: a case study of Wuhan's response to COVID-19[J/OL]. Management Review. (2023-01-18)[2024-02-06]. <https://kns.cnki.net/kcms/detail/11.5057.F.20230118.0930.002.html>
- [21] 张旭雯, 迟银明, 何声升, 等. 共生视角下校企创新主体深度融合的内在过程机理研究——基于沈鼓集团与大连理工大学探索性案例[J]. 科技进步与对策, 2023, 40(14): 12
- ZHANG Xuwen, CHI Jingming, HE Shengsheng, et al. Internal mechanism of deep integration of university-industry innovation subjects from the symbiotic perspective: the exploratory case of Shenyang Blower and Dalian University of Technology[J]. Science & Technology Progress and Policy, 2023, 40(14): 12. DOI:10.6049/kjbydc.Q202207468
- [22] 赵俊, 陈旭梅, 刘志硕, 等. 航权资源双边谈判的序贯互惠博弈建模与分析[J]. 哈尔滨工业大学学报, 2022, 54(3): 1
- ZHAO Jun, CHEN Xumei, LIU Zhishuo, et al. Modeling and analysis of sequential reciprocal game problem of bilateral negotiation for air traffic rights resources [J]. Journal of Harbin Institute of Technology, 2022, 54(3): 1. DOI:10.11918/202112043
- [23] 徐选华, 周黎洁. 应急环境下双重大规模行为主体知识融合方法及在方案排序中的应用[J]. 控制与决策, 2024, 39(5): 1675
- XU Xuanhua, ZHOU Junjie. Knowledge fusion method and application in alternative sorting of dual large-scale behavior agents under emergency environments [J]. Control and Decision, 2024, 39(5): 1675. DOI:10.13195/j.kzyjc.2022.1012
- [24] 郭亚男, 安实, 麦强. 考虑参照依赖的突发公共卫生事件预警信息公开策略研究[J]. 运筹与管理, 2023, 32(2): 139
- GUO Yanan, An Shi, MAI Qiang. Research on the strategy of warning disclosure for public health emergencies based on reference dependence [J]. Operations Research and Management Science, 2023, 32(2): 139. DOI:10.12005/orms.2023.0057
- [25] FURLAN A, GRANDINETTI R, DE TONI A F. Managing the lean-agile paradox in complex environments [J]. Systems, 2023, 11(5): 258. DOI:10.3390/systems11050258

(上接第 37 页)

- [15] MADRY A, MAKELOV A, SCHMIDT L, et al. Towards deep learning models resistant to adversarial attacks [C]//6th International Conference on Learning Representations, ICLR 2018. Vancouver: ICLR, 2018: 149806
- [16] KURAKIN A, GOODFELLOW I J, BENGIO S. Adversarial machine learning at scale [C]//5th International Conference on Learning Representations, ICLR 2017. Toulon: ICLR, 2017: 149804
- [17] MA Xingjun, NIU Yuhao, GU Lin, et al. Understanding adversarial attacks on deep learning based medical image analysis systems [J]. Pattern Recognition, 2021, 110: 107332. DOI:10.1016/j.patcog.2020.107332
- [18] RAGHUNATHAN A, XIE S M, YANG F, et al. Adversarial training can hurt generalization [EB/OL]. (2019-06-14). <https://arxiv.org/abs/1906.06032>
- [19] QIAN Zhuang, HUANG Kaizhu, WANG Qiufeng, et al. A survey of robust adversarial training in pattern recognition: fundamental, theory, and methodologies [J]. Pattern Recognition, 2022, 131: 108889. DOI:10.1016/j.patcog.2022.108889
- [20] XU Yuhui, XIE Lingxi, XIE Cihang, et al. BNET: batch normalization with enhanced linear transformation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(7): 9225. DOI:10.1109/TPAMI.2023.3235369
- [21] HUANG Lei, QIN Jie, ZHOU Yi, et al. Normalization techniques in training DNNs: methodology, analysis and application [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2023, 45(8): 10173. DOI:10.1109/TPAMI.2023.3250241
- [22] DONG Jiahua, WANG Lixu, FANG Zhen, et al. Federated class-incremental learning [C]//2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). New Orleans: IEEE, 2022: 10154. DOI:10.1109/CVPR52688.2022.00992
- [23] Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity. CSE-CIC-IDS2018 on AWS [DB/OL]. [2024-02-04]. <https://www.unb.ca/cic/datasets/ids-2018.html>
- [24] ZUECH R, HANCOCK J, KHOSHGOFTAAR T M. Detecting web attacks using random under sampling and ensemble learners [J]. Journal of Big Data, 2021, 8(1): 75. DOI:10.1186/s40537-021-00460-8
- [25] MEZINA A, BURGET R, TRAVIESO-GONZÁLEZ C M. Network anomaly detection with temporal convolutional network and U-net model [J]. IEEE Access, 2021, 9: 143608. DOI:10.1109/ACCESS.2021.3121998