文章编号：1674-0629(2025)06-0051-11　　中图分类号：TM743　　文献标志码：A
DOI：10. 13648/j. cnki. issn1674-0629. 2025. 06. 005

面向电力信息网络安全风险演变的兵棋推演技术

杨祎巍[1,2]，吴建彬[3]，高梓航[3]，梁志宏[1,2]，洪超[1,2]，李攀登[1,2]，张玉健[3]
（1. 南方电网科学研究院，广州 510663；2. 广东省电力系统网络安全企业重点实验室，广州 510663；3. 东南大学网络空间安全学院，南京 211102）

摘要：随着国际形势日趋严峻复杂以及智能化和信息化技术在电力系统中的广泛应用，电力系统已成为网络攻击的重点目标，其网络安全的重要性愈发突显。为了构建研究电力网络安全风险演变的利器，支撑网络安全风险预测指挥工作，提出了一种面向电力网络安全演变的兵棋推演方法，通过策略层面的兵棋仿真推演，构建了基于可组合性和最小操作单元理念的推演框架，实现了大规模电力网络安全场景建模并提高了仿真效率，同时能够高效地识别网络中的潜在风险。通过实验验证，该方法在大规模电力信息网络安全推演中表现出优异的性能，能够为电力网络安全风险演变研究、网络安全策略优化和网络安全指挥作战提供强有力的支撑。

关键词：电力信息网络；网络安全；兵棋推演；拓扑建模；行为建模；威胁发现

Wargaming Technology Towards Cybersecurity Threat Evolution in Power Information Network

YANG Yiwei[1,2], WU Jianbin[3], GAO Zihang[3], LIANG Zhihong[1,2], HONG Chao[1,2], LI Pandeng[1,2], ZHANG Yujian[3]
（1. Electric Power Research Institute, CSG, Guangzhou 510663, China；2. Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou 510663, China；3. School of Cyber Science and Engineering, Southeast University, Nanjing 211102, China）

Abstract: As the international situation becomes increasingly complex and the widespread adoption of intelligent and information technologies in power systems continues, power systems have emerged as prime targets for cyber-attacks, highlighting the critical importance of cybersecurity. To provide a powerful tool for studying the evolution of security risks in power network and support cyber risk prediction and command work, a wargaming-based method is proposed for modeling the evolution of power network security. A deduction framework based on the concepts of composability and minimal operation units is constructed through strategic-level wargaming simulations to achieve large-scale power network security scenario modeling and improve simulation efficiency, while effectively identifying potential risks in the network. Experimental validation demonstrates that the proposed method exhibits superior performance in large-scale power information network security wargaming, providing robust support for research on the evolution of power network security risks, optimization of cybersecurity strategies, and command operations in network security.

Key words: power information network; cybersecurity; wargaming; topology modeling; behavior modeling; threat detection

0　引言

随着新型电力系统的建设发展和数字化技术的深入应用，电力系统可控对象已从传统的以“源”为主逐步扩展到“源网荷储”各个环节，控制规模也因此呈指数级增长[1]。这种扩展不仅增加了系统的复杂性[2]，同时也提高了对电力网络安全防护的需求。尤其是新能源、分布式电源、新型储能设施及

基金项目：广东省电力系统网络安全企业重点实验室开放基金资助项目(150000202303010 3XA00246)。
Foundation item: Supported by the open fund of Guangdong Provincial Key Laboratory of Power System Network Security (150000202303010 3XA00246).

电动汽车的广泛接入，极大丰富了电力系统的构成要素并扩大了网络的攻击范围，加剧了电力网络安全风险挑战[3]。

为保障电力网络安全，风险仿真与威胁发现技术发挥了至关重要的作用[4]。这些技术通过对电力信息网络进行模拟仿真，能够有效地分析和重现网络中的潜在威胁和漏洞，为制定防御策略提供科学依据。特别是对于无法在生产环境中测试的高风险攻击手法，仿真提供了一个安全的测试环境，避免了实际操作中可能导致的电力供应中断风险[5]。

然而，在处理复杂场景时，当前的仿真技术面临高资源消耗和速度效率低下的问题[6]，尤其在涉及全局性大规模电力网络安全推演的情境[7]。这些问题主要有两个成因。首先，随着新型电力系统的发展，设备数量呈指数级增加，传统仿真须处理大量与推演无关的细节，如模拟网络协议栈等，导致资源的消耗显著。其次，电力系统的设备多样性和异构性特点增加了仿真的复杂度。这些设备不仅包括传统的电网控制设备，如继电保护装置和控制保护装置，还包括电力信息网络中的网络设备，以及新能源、分布式电源、新型储能设施等新型电力设施[8]。这种多样性和异构性进一步加剧了仿真的挑战，限制了仿真技术在战略层面的应用潜力[9]。因此，迫切需要通过技术创新优化仿真流程减少资源需求并提升仿真速度，以便更有效地支持电力网络的安全分析与决策制定。

针对现有方法的局限性，本文提出了一种面向电力网络安全演变的兵棋推演技术。本方法利用逻辑和策略层面的仿真，在兵棋推演框架下结合可组合性和最小操作单元理念[10]，构建原子操作集，组合建模电力信息网络中的各类设备和各类攻防行为，以支持全局性的大规模网络安全推演。通过抽象化和实例化的手段，该方法能在兵棋推演框架中模拟复杂的策略和决策过程，显著降低资源消耗，提高仿真效率，同时凭借已构建的攻防行为模型高效地发现网络中的潜在风险，提升电力网络安全保障能力。

本文各章节安排如下：第一部分进行电力网络安全推演的需求分析，阐述现有方法在电力网络安全推演场景中面临的挑战；第二部分提出面向电力网络安全演变的兵棋推演技术，并详细介绍其实现原理和关键技术；第三部分提出除红蓝兵棋对抗之外可用于兵棋建模之上的衍生应用，即威胁发现；第四部分通过实验验证所提出方法的有效性，并对实验结果进行分析；最后一部分总结本文的研究工作，并提出未来的研究方向。

1 电力网络安全推演需求分析

在网络安全威胁研判指挥中，仿真技术是不可或缺的工具，它们帮助研究人员模拟攻击场景、发现潜在威胁并测试防御策略。这些技术通过预警和制定应对措施以增强网络的整体安全性和应变能力。现有的推演网络建立方法主要包括两种途径：通过物理硬件和虚拟化技术创建网络节点和连接，以及利用模拟器的内置组件重现实际网络功能。前者如DVWA、Vulhub等网络攻防靶场平台[11]，利用虚拟网络技术构建交互性强的网络环境，允许安全研究人员在一个受控的虚拟环境中进行攻击和防御实验；后者如NS3[12]、OPNET[13]等网络仿真平台，通过模拟器的内置组件重现具有实际网络功能的元素，如服务器、路由器等，从而能够对网络的行为进行精确模拟和分析。

然而，在电力网络安全推演中，尤其在需要处理大规模仿真的场景下现有方法面临多项挑战。电力信息网络的庞大规模和动态性要求策略能快速迭代，但现有技术在性能效率上存在显著限制。例如，攻防靶场平台虽能够提供真实流量和网络协议栈的模拟，但其资源消耗高、仿真速度慢，难以满足需要快速决策的大规模场景下对攻击技战法[14]的仿真需求。网络仿真平台在模拟真实流量和处理仿真形态上具有一定的灵活性，能够模拟复杂的网络行为，但在逻辑和策略级模拟方面依然存在局限，难以满足大规模电力网络推演下的性能要求，阻碍了全局和战略层面对攻击技战法的有效推演。因此，针对电力网络安全推演，迫切需要开发一个专用平台，旨在克服现有技术在性能和规模上的局限，并在逻辑和策略层面提供更灵活、更高效的仿真能力。

兵棋推演作为一种强大的决策支持工具，能够为电力网络的安全推演提供一种新的思路。通过模拟复杂的攻防互动，它能够帮助决策者评估不同策略的效果并预测潜在威胁，从而为电力网络的安全保障提供更具前瞻性的支持。兵棋推演源自军事领域，是“未战而庙算胜者”的智慧体现，结合了策

略、模拟与游戏理论的仿真方法，涉及4个核心元素：棋盘、棋子、规则和想定[15]。其中，“棋盘”代表推演的操作环境，通常是指具体的地理区域或战场地图；“棋子”则代表在这一环境中活动的实体，如军队、设备或系统；“规则”为推演设定了操作限制和行为后果，确保活动遵循既定逻辑；“想定”则设定了推演的场景和条件，提供了行动的背景和目标。随着信息技术的进步，兵棋推演已从手工操作转向信息化、智能化，显著提升了推演的规模和效率。美国战区级联合作战兵棋系统[16]是典型例证，自1982年启动以来已广泛应用于多场军事行动[17]，但目前尚未有网络安全领域兵棋研究的报道。

本文从逻辑与策略层面切入兵棋仿真推演，面向电力网络安全领域提出了一种创新的建模及威胁发现方法。在此方法中，电力信息网络的拓扑及其上的资产被视为推演的“棋盘”，而网络中的攻防行为则视为在网络拓扑上被操作的“棋子”，同时将攻防行为在推演过程中的状态转移及其概率作为“规则”，并将设定各种网络安全威胁场景视为“想定”。这种策略仿真不仅能够模拟现实世界的攻防动态，还有助于分析和制定有效的防御策略。

然而，将复杂的网络攻防动态准确地映射到棋盘和棋子上是网络攻防推演中的一大挑战。这要求从策略和技术层面上高度抽象化处理，确保每一次“棋子”的移动和交互都能真实反映网络环境中的攻防状态。为了优化仿真形态与粒度，本方法并不直接模拟真实流量的复杂无关细节，从而降低了资源消耗，并为大规模网络推演提供了可能性。同时，基于正交分解思想，通过抽象网络行为的原子操作集合构建描述复杂网络攻防的模型，本方法支持快速迭代与评估多样的战术和策略，大幅提升了电力网络推演的效率和实效。如表1所示，与现有的攻防靶场和网络仿真平台相比，本研究提出的电力网络兵棋推演平台在仿真规模、资源消耗及运行速度等方面均有显著优势[13]。通过减少对细节的依赖并聚焦策略模拟，该平台为电力网络安全提供了新的方法论和工具。

表1　网络安全推演平台比较

Tab. 1　Comparison of cybersecurity deduction platforms

推演平台	模拟攻击流量	模拟攻击技战法	仿真形态	资源消耗	运行速度	仿真规模
攻防靶场平台	是	否	物理、虚拟化软件	高	慢	小
网络仿真平台	是	否	细粒度实例化对象	中	中	中
兵棋推演平台	否	是	抽象化实例化对象	低	快	大

2　面向电力网络安全演变的兵棋推演技术

2.1　棋盘：网络拓扑建模

网络拓扑建模是构建电力网络安全兵棋推演框架的基础，其通过构建网络的结构化视图以及网络中各种资产，提供了推演过程中的“棋盘”。这一模型旨在精确捕捉电力网络的物理和逻辑结构，并能够模拟网络中各组件在攻防活动中的动态交互。

在电力网络兵棋推演中，电力信息网络系统被抽象为一个加权图 $G=(V, L, C, B, \alpha, \beta)$，其中：

1）V为网络中的节点集合，每个节点$v \in V$代表网络中的一个资产。

2）$L \subset V \times V$为节点间的边集合，代表资产之间的物理连接或数据链路。

3）C为网络拓扑中各节点的属性空间集合，代表资产可能具有的各种属性。

4）α：$V \to C$为一个将每个节点映射到其属性集合C的函数，描述每个节点的特性与能力，如设备类型、网络安全防护情况等。

5）B为网络拓扑中边的属性空间，代表链路可能具有的属性。

6）β：$L \to B$为一个将每条边映射到其属性集合B的函数，这些属性决定了连接的性质，如带宽、链路性质等。

节点的属性进一步细分为个体属性C_e和全局属性C_g，如表2所示，这使得模拟过程中可以精确处理局部操作影响和整体网络安全状况。个体属性C_e包括设备类型、操作状态、物理位置等，这些属性反映了资产的个体特性和当前状况；全局属性C_g，例如网络安全防护情况、事故发生概率和员工安全意识，为整个网络设定安全政策和环境背景提供了对网络整体安全状况的评估。通过调整映射函数α和β中的属性，系统可以模拟多种攻防场景，评估网络在面对不同威胁时的反应和恢复能力。如通过提升特定节点的“网络安全防护情况”，可探究增强安全措施对防御外部攻击的效果，通过模拟可能的

攻击路径和方法揭示网络潜在脆弱点。

表 2 部分通用资产属性

Tab. 2 Partial universal asset attributes

属性类型	编号	属性名称	编号	属性名称
个体属性	1	设备标识	8	物理损耗程度
	2	设备名称	9	用户列表
	3	设备类型	10	程序列表
	4	运行状态	11	访问控制列表
	5	CPU 利用率	12	文件列表
	6	剩余内存	13	访问控制列表
	7	剩余硬盘量	14	日志文件
全局属性	1	事件发生概率	3	员工安全意识
	2	网络安全防护情况		

2.2 棋子:攻防行为建模

在电力网络安全兵棋推演中，攻防行为作为“棋子”，是电力网络安全兵棋推演的核心角色，其直接决定了推演棋盘中的各类资产属性的变化以及推演的博弈与评分。攻防行为规则细化了参与者在模拟网络环境中的具体互动内涵，包括单一的攻击或防御动作和复杂的多步骤攻防策略。通过模拟这些从简单到复杂的攻防行为，兵棋推演能够再现网络的攻防动态，提供安全洞察，帮助防御者评估防御策略的有效性，并及时发现系统的安全漏洞。同时攻防行为的建模与资产特性紧密关联，形成“棋子”与“棋盘”之间的战术互动。

尽管现有网络安全建模方法[18]为攻防互动建模提供了框架[19]，但通常缺乏与资产模型的互动，同时难以应对电力信息网络复杂场景高性能、扩展性和可复用性的要求[20]。为此，本文引入一种策略级的逻辑抽象模拟方法，其基于原子操作的“裂解-组合”理念，将攻防行为分解为具体的原子操作集Ω，并在兵棋推演的策略层面建模重新组合，形成新的攻防模型。其中Ω原子操作集定义为：

$$\Omega = \left\{ o_i = \left(n_i, h_i, e_i \right) \right\} \tag{1}$$

式中：o_i为第i个操作；n_i为第i个标识操作的具体名称，如“程序安装”、“访问控制检查”等；h_i为第i个操作需要的输入参数，详细描述执行条件或数据；e_i为第i个操作预期达到的效果，如“数据泄露”或“权限提升”。

此方法根据攻击行为所期望达到的具体效果，从而精确裂解攻防行为，构成原子操作集Ω，如表3所示。这些原子操作不仅能够明确描述每个行为的具体效果，还因为其基于效果的泛化设计，能够在组合后广泛适用于多样的攻击和防御策略。

表 3 部分原子操作

Tab. 3 Partial atomic operations

编号	方法名称	编号	方法名称
1	个体属性查看	13	访问控制检查
2	个体属性修改	14	文件列表更新
3	全局属性查看	15	文件扫描
4	全局属性修改	16	文件查看
5	流量可达判断	17	补丁列表修改
6	关联设备扫描	18	补丁扫描
7	用户列表更新	19	日志查看
8	用户属性检查	20	日志更新
9	程序列表更新	21	扫描范围内设备
10	社工欺骗	22	按照位置查找设备
11	程序执行	23	按属性查找设备
12	访问控制列表更新	24	成功概率计算

此外，由于该方法未采用对真实流量等无关信息的模拟，优化了仿真粒度，使其降低了资源消耗、提升了运行速度。因此，原子操作的泛化能力和高效的建模粒度共同增强了该方法在大规模电力网络安全推演中的应用潜力，为策略层面的决策提供了强大支撑。

攻击模型A描述了通过特定原子操作序列实施的攻击行为，旨在达成特定的网络破坏或数据获取目标。它被定义为：

$$A = \left\{ \left(s, E \right) \right\} \tag{2}$$

$$s = \{ combine\left(o_i, \cdots, o_j \right), o_k \in \Omega \} \tag{3}$$

$$E = effect\left(s \right) \tag{4}$$

式中：s为原子操作的有序组合，这些操作是从原子操作集Ω中根据攻击策略精心挑选的；$combine$为一个组合函数，描述了根据特定的逻辑和条件将操作o_i，$\cdots$，o_j组合在一起，包括操作的并行、串行执行，以及基于特定拓扑条件的动态选择；$E = effect\left(s \right)$为该序列操作预期达到的综合效果，例如数据泄漏、系统破坏或权限提升等。

防御模型D则针对潜在的攻击模式设计防御策略，通过执行预防措施来抵御或缓解攻击的影响。防御模型定义为：

$$D = \left\{ \left(s, R \right) \right\} \tag{5}$$

$$s = \{\, combine\left(o_x, \cdots, o_y\right) | o_r \in \Omega \,\} \tag{6}$$

$$R = result(s) \tag{7}$$

式中 $R = result(s)$ 为该有序防御操作组合 s 预期达到的综合效果，旨在阻断攻击的进程或减轻其后果。

将攻击模型 A 和防御模型 D 结合，形成一个全面的攻防模型 M，它不仅反映了攻击策略和防御措施的互动，也提供了对攻防结果的预测。

$$\begin{aligned} M = \{(O, Q, E) | O = combine(A, D),\\ Q = D.R, E = A.E \,\} \end{aligned} \tag{8}$$

式中：O 为攻击和防御操作的综合原子操作序列，由 A 和 D 中选择的操作通过 $combine$ 函数集成；Q 为防御操作的结果 $D.R$，这些结果作为防御成功的前提条件，必须在攻击行为之前得到满足；E 为攻击操作所希望达到的效果 $A.E$，定义了攻击成功后预期的网络状态变化。

2.3　规则：状态转移概率

在电力网络安全兵棋推演中，规则是对攻防行为进行系统化和量化约束的条件，其中核心的是概率规则，概率规则专注于复杂攻防场景中的状态转移过程，量化了不同攻防行为之间的转移概率，揭示了这些行为的可能性与不确定性。通过概率规则，兵棋推演能够模拟并预测网络安全事件的演化路径，从而评估不同策略和行动对网络资产状态的影响。具体而言，概率规则能分析从一个状态到另一个状态的转移概率，为攻防行为的风险评估和策略决策提供定量支持。

为了更加精确地刻画这一过程，并描述实际网络安全事件中的复杂攻防行为，引入了状态迁移图，如图 1 所示，通过节点表示不同的安全状态，通过边表示状态之间的转移。每一条边都由特定的原子操作触发，展示了从一个状态到另一个状态的转移过程。结合概率规则，状态迁移图能够更加精确地量化不同攻防行为之间的转移概率，从而反映它们的可能性和不确定性。

攻防流程状态迁移图 $G = (S, T)$ 的组成如下。

1）状态集合 S 包含该攻防行为模型下该节点的所有可能状态，每个状态代表了其在特定时间点的状态，如 a_{state_0} 就表示节点 a 的 state_0 状态。这些状态可以是具体的如“系统尚未受到攻击”，“系统被提权”或“数据被窃取”等。其中，a_{state_x} 表示该状态迁移图的失败终止状态，a_{state_y} 表示最终攻击目标成功实现状态，同时可能还涉及其他相关节点设备的状态，如 b_{state_0}。

$$S = \left\{a_{\text{state}_0}, a_{\text{state}_x}, \cdots, a_{\text{state}_y}, b_{\text{state}_0}\right\} \tag{9}$$

2）迁移关系 T 表示状态之间的转换，每个转换由一个四元组表示，包括起始状态、结束状态、触

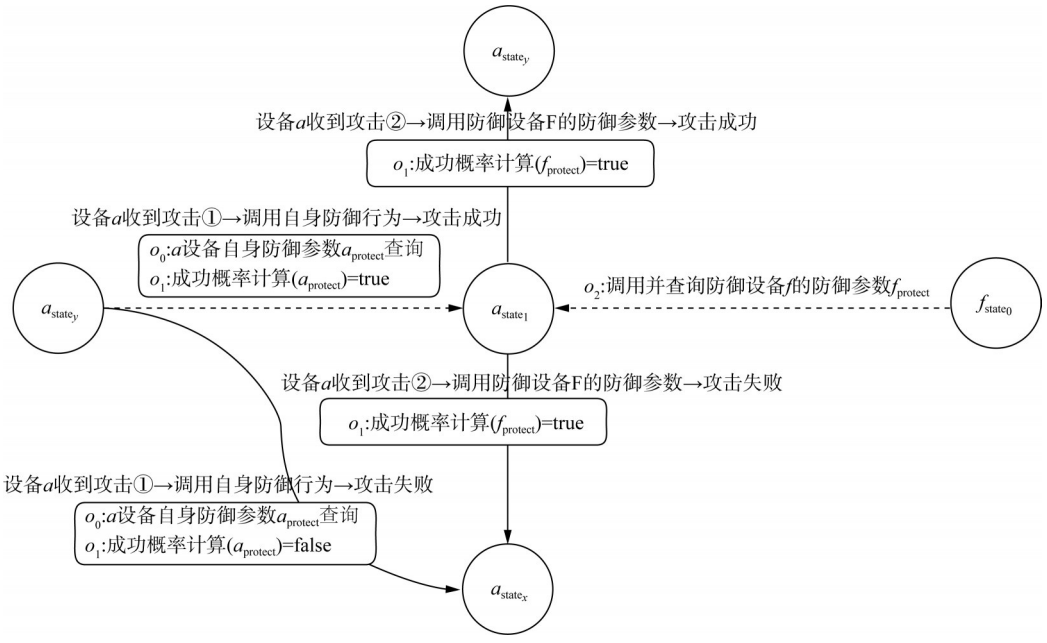

图 1　状态迁移图示意图

Fig. 1　Illustrative diagram of state transitions

发这一变化的原子操作及可能存在的状态转移概率。具体而言，迁移关系T反映了从一个状态到另一个状态的转移过程。每条边直接关联到模型M中定义的具体攻击或防御操作，以及该原子操作所涉及的概率规则。例如，某些状态转移可能包含一定的失败概率，或者根据系统状态和防御策略的不同，转移的成功概率会随着参数的不同有所不同。其公式表示如下。

$$T=\{(a_{\text{state}_i},a_{\text{state}_j},o_k,p_{o_k})|a_{\text{state}_i},a_{\text{state}_j}\in S,o_k\in M.O\} \tag{10}$$

式中：p_{o_k}为转移的概率，用于量化不同攻防行为之间的转移可能性；o_k为触发状态转移的操作；$M.O$为攻防模型M的操作集合。在状态转移过程中，转移的概率p_{o_k}对于每一条状态迁移，表示从状态a_{state_i}转移到a_{state_j}的概率，这一概率是基于攻防行为和防御策略的执行效果来确定的，不同的攻防行为可能导致不同的状态转移概率。而在实际推演过程中，概率参数的确定应借攻防行为的历史数据分析以及推演的场景想定确定，同时需要引入适当的随机化参数以作现实世界不可预测的干扰项，以增强推演真实性。

为了直观展示各状态之间的转移，本文使用状态迁移概率来描述不同攻防模型中各状态之间的转移关系。当两个状态之间的转换涉及概率时，状态之间的转移可通过式(11)来表示。

$$P\left(a_{\text{state}_i}\rightarrow a_{\text{state}_j}\right)=p\left(r_i,f_{\text{state}_f},f_{\text{protect}},\cdots,d_{\text{state}_w},d_{\text{attack}}\right) \tag{11}$$

式中：P标识a_{state_x}转移至a_{state_y}的概率，其由一个概率功能p得到，p的入参涉及一个随机影响源r_i、其自身和其他与其相关设备的状态，如防御设备f的状态f_{state_f}、攻击设备d的状态d_{state_w}，以及涉及的防御参数，如设备f的防御参数f_{protect}与设备d的攻击参数d_{attack}。这些关联设备的状态和参数共同作为概率函数p的入参得到状态转换的概率P。

在实际推演中，设备的不同状态及其变化受到各类因素的影响。如图1所示，设备a的状态迁移示意图展示了设备的4种主要状态：初始状态、成功遭受攻击1的状态、攻击目标失败的状态以及总攻击目标成功的状态。在推演过程中，其他安全设备如设备f的防御状态(例如f_{state_0})也会影响转移概率的计算。这些防御参数不仅对攻击过程中的转移概率有直接影响，还能够反映出不同防御策略在不同攻击场景中的有效性。

2.4 想定:推演场景设定

在电力网络安全兵棋推演中，“想定”指的是对推演场景的具体设定，它包括网络拓扑结构、攻防行为模型的选择以及适用的推演规则与概率规则。想定的核心目的是在特定攻防环境下重建网络安全态势，以便为策略评估、风险预测及应急响应提供科学依据。

具体而言，在每个想定场景中，网络拓扑作为推演的基础，定义了网络中各资产的属性及其相互连接的状态，构建了推演的“棋盘”。攻防行为模型则描述了攻击者与防御者在该特定场景中可能采取的策略与行动，作为推演中的“棋子”。而推演规则与概率规则为这些行为提供了量化的约束，决定了攻防行为的执行逻辑、状态转移的可能性及其对网络安全态势的影响。

通过设定这些设定推演能够在特定网络结构与行为模型的框架下模拟真实攻防过程并评估不同策略和行为对网络安全状态的影响，这为网络安全风险预测、策略优化及应急响应决策提供了理论支撑和实践指导。

3 基于组合搜索的威胁发现算法

在电力网络安全兵棋推演的研究框架下，本文进一步提出基于组合搜索的威胁发现算法，如表4算法1所示，作为对除用于红蓝双方兵棋推演之外的衍生应用扩展。该算法利用兵棋推演所构建的详尽网络拓扑和由攻防行为模型组合而成的攻防流程状态迁移图，通过图搜索技术全面识别潜在的攻击路径，由特定攻防流程状态迁移得到的威胁检测算法发现脆弱点，从而打造威胁发现能力。

其包含两个模块如下。

1）图搜索模块：利用可包括深度优先搜索(depth-first search，DFS)、广度优先搜索(breadth-first search，BFS)以及A*算法在内的多种图搜索算法。这些算法的选用取决于其在特定场景下的性能和效果，确保在整个网络拓扑中进行全面而精准的遍历。

2）威胁检测模块：威胁检测模块通过匹配网络拓扑中的节点与特定状态迁移图中的初始状态，

表4　基于组合搜索的威胁发现算法

Tab. 4　Threat detection algorithm based on combinatorial search

算法1：基于组合搜索的威胁发现算法 threatDetect(G, G_{status})

输入：网络拓扑图 $G=(V,L)$
　　状态迁移图 $G_{status}=(V_{status},E_{status})$
输出：受潜在威胁的设备节点集合 $\Sigma_{threats}$

$\Sigma_{threats} \leftarrow \varnothing$
$start \leftarrow Start(G_{status})$
for all $node \in V$ **do**
　while $Match(node, start)$ **do**
　　$start \leftarrow graphSearch(start, G_{status})$
　　$node \leftarrow graphSearch(node, G)$
　if $start == End(G_{status})$ **do**
　　$\Sigma_{threats} \leftarrow \Sigma_{threats} \cup node$
　return $\Sigma_{threats}$

检测节点是否具有与特定攻防流程相关的潜在威胁。若具有潜在威胁，则对每个节点的状态变化根据状态迁移图进行跟踪，直到到达状态图的终点，这标志着该节点受到了潜在威胁。

该算法的时间复杂度主要受到两个因素影响，具体如下。

1）图搜索算法：无论采用深度优先搜索还是广度优先搜索，图搜索的时间复杂度在理想情况下通常为 $O(|V|+|L|)$，其中 V 表示图中的顶点数量，L 表示边数量。这反映了算法需要处理每个顶点和边至少一次，以确保图的完全覆盖；

2）威胁检测算法：假设每个节点的威胁检测函数具有 $O(z)$ 的时间复杂度，当该函数应用于图中的每个节点时，整体的时间开销为 $O(|V|\times z)$。因此，算法的总体时间复杂度估计为 $O(|V|\times z+|L|)$。

综上所述，本文提出的基于组合搜索的威胁发现算法面向兵棋推演中构建的网络拓扑和攻防行为模型，扩展了推演框架的应用。通过结合状态迁移图，算法能够识别潜在的安全威胁，进一步为电力信息网络的安全性提供支持。这一扩展使得兵棋推演不仅局限于红蓝兵棋对抗，还能为威胁检测和风险发现提供支撑。

4　建模实例及实验分析

为验证本文提出的建模方法和威胁发现算法的有效性，本节在电力网络安全兵棋推演框架内进行了详细的安全建模。这包括涉及多节点的单一攻防行为以及包含多个攻防行为组合的复合攻防模型。基于这些已构建的模型，本文进一步在不同规模的网络节点下执行威胁发现算法的性能测试，以及节点攻击平均成功率从而评估该算法在处理各种规模网络节点时的效能。

4.1　攻防行为建模案例

为确保本文提出的建模方法和威胁发现算法的有效性，本节选择了两种具体的模拟案例进行详细分析：一种基于分布式拒绝服务攻击（distributed denial of service attack，DDoS）和防火墙防御的简单模型，另一种是包含多个攻防行为的复杂攻防模型-高级持续性威胁（advanced persistent threat，APT）攻防模型。两个案例覆盖了单节点和多节点的攻防互动，涵盖了从简单到复合的多种攻防行为，以展示原子操作集的应用并验证本文建模方法的实用性，同时全面展示本建模方法在应对电力网络实际安全威胁中的应用效果。

4.1.1　DDoS攻防模型

在DDoS攻防模拟案例中，本节构建了一个场景，其中外部攻击节点通过发送大量请求试图使目标节点过载，并导致服务中断；而其中的防火墙节点通过流量过滤功能用以缓解该攻击的影响。该模型的状态迁移图如图2所示，其详细描绘了攻防模型的启动、进行和成功和失败各个阶段状态的转移。

其中攻击的最终目标状态 a_{state_y} 为使节点 a 过载的成功状态，a_{state_x} 则为最终目标失败的终止状态。其中涉及到的攻击和防御原子操作序列 O 如式（12）所示。

$$O=combine(o_1,o_2,o_3,o_4,o_5,o_6) \tag{12}$$

1）流量可达性判断（o_1）：评估是否存在从攻击发起点到目标节点的网络路径。若流量可达，则继续执行；否则，攻击终止并标记为失败。

2）访问控制检查（o_2）：检查目标节点是否有启用访问控制机制（例如白名单）。如访问受控，进入防火墙检测阶段；无访问控制则攻击失败。

3）扫描路径防火墙（o_3）：确定攻击路径上是否存在防火墙及其配置的流量过滤。无防火墙时攻击直接成功；若有防火墙，进行成功概率计算。

4）个体属性修改（o_4）：无防火墙或成功绕过防火墙后，修改目标节点个体属性，如增加CPU使用

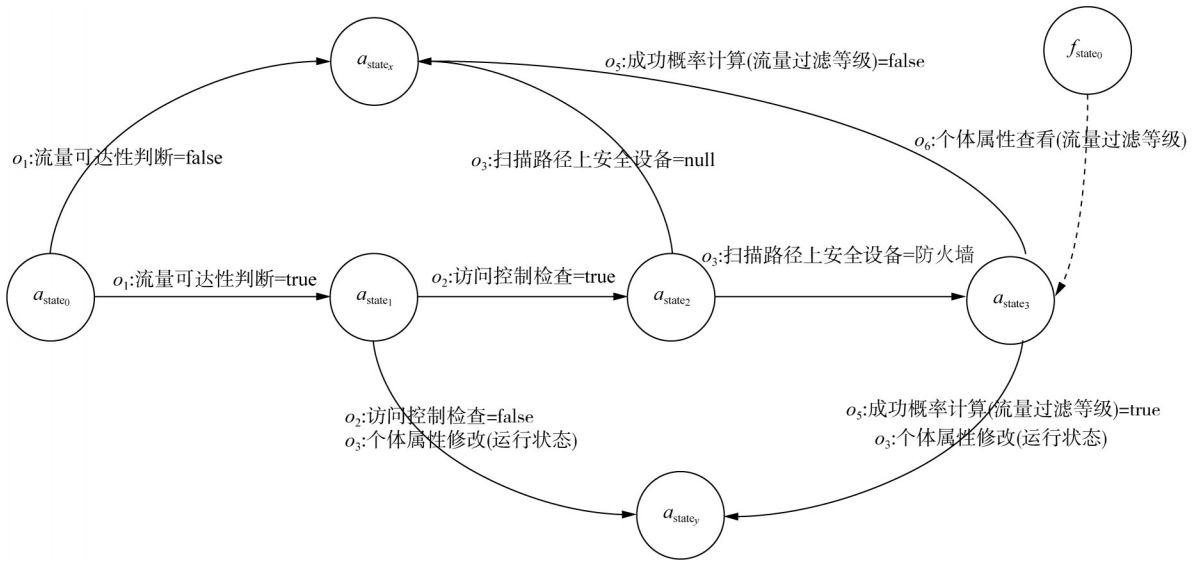

图2 DDoS攻防模型状态迁移图

Fig. 2 State transition diagram of DDoS attack-defense model

率、降低带宽和内存等，模拟DDoS攻击影响。成功实现属性修改则达到攻击的终极目标。

5）成功概率计算（o_5）：基于防火墙设备的流量过滤级别（o_6）计算攻击绕过防火墙的可能性。绕过成功则进入下一阶段；则攻击终止。

6）个体属性查看（o_6）：查看设备（防火墙）的流量过滤级别。根据这一级别，执行成功概率计算（o_4），判断攻击是成功绕过防火墙。

通过上述原子操作序列的逻辑组合，本文在兵棋推演框架下成功完成DDoS攻防模型的建模。

4.1.2 APT攻防模型

APT模型涵盖了一个完整的攻击链，从电子邮件钓鱼、恶意载荷部署到敏感数据窃取等多个阶段，并设有相应的防御行为：邮件安全过滤、员工安全意识驱动、杀毒软件和敏感文件加密。状态迁移图如图3所示，展示了攻击的可能路径和各阶段的状态变化，包括：最终状态a_{state_y}代表了攻击的最终目标，即窃取到敏感数据；而若中途攻击链条由于防御行为断裂，状态则将迁移为攻击失败的终止状态a_{state_x}。

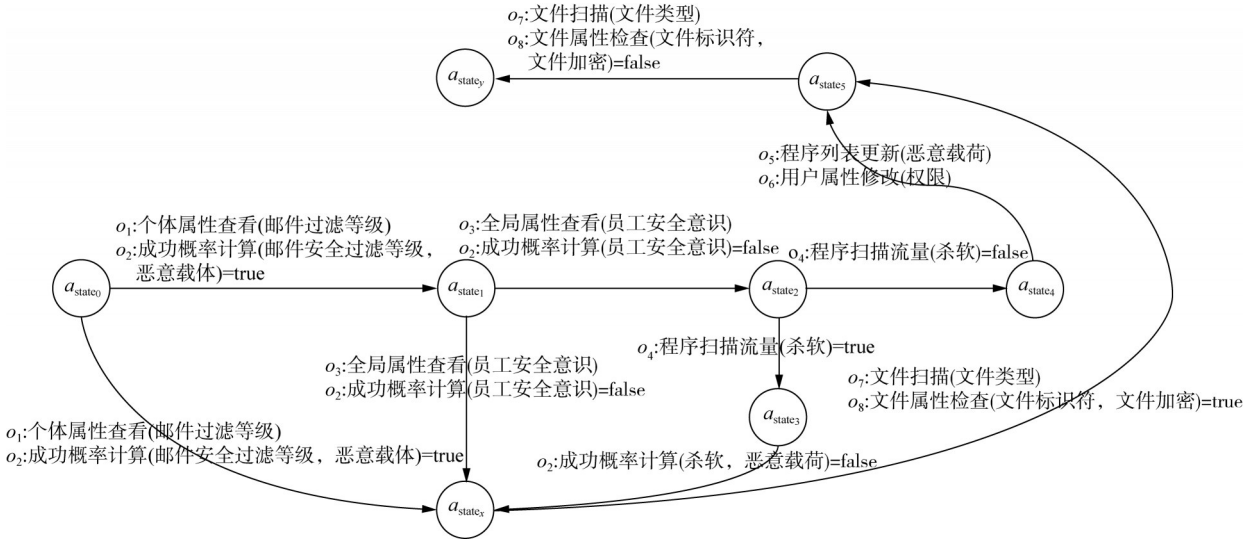

图3 APT攻防模型状态迁移图

Fig. 3 State transition diagram of the APT attack-defense model

其中涉及到的原子操作综合序列 O 由 8 个原子操作组合而成，包括：

1）个体属性查询（o_1）：对受攻击系统的设备信息进行查询，以确定目标设备的属性。

2）成功概率计算（o_2）：根据攻击参数和防御措施，评估攻击成功的概率。

3）全局属性查询（o_3）：检查系统的全局安全设置，如“员工安全意识”。

4）程序扫描（o_4）：扫描系统中的运行程序，如杀毒软件，以确认攻防行为的互动。

5）程序列表更新（o_5）：在系统中添加运行程序，如在成功突破防御后，部署恶意载荷以便进行进一步的控制和数据窃取。

6）用户属性修改（o_6）：篡改系统中的用户权限或访问控制，扩大攻击者的控制权限。

7）文件扫描（o_7）：对目标系统的文件进行扫描，如寻找敏感数据或加密文件。

8）文件属性检查（o_8）：对文件的属性进行核查，如查看是否未加密导致可以被窃取。

4.2　威胁发现算法性能测试

为确保测试的有效性和可靠性，本文通过特定算法随机生成了不同规模的网络拓扑，模拟从数万至数百万节点的电力信息网络环境，以真实反映潜在的各种网络情况，相关实验环境见表 5。

表 5　威胁发现算法实验环境

Tab. 5　Experimental environment for threat detection algorithms

实验环境	实验参数
编程语言	Java
内存容量	16 GB
CPU 型号	Intel i5-9300H CPU @ 2. 40 GHz
操作系统	Windows 11

在本实验中，利用此前构建的 DDoS 攻防模型与 APT 攻防模型的状态迁移图，实现具体的威胁检测程序。对于 DDoS 攻击的威胁发现，结果如图 4 所示。测试结果显示，随着网络拓扑中节点数量的增加，威胁检测算法的执行时间呈现出线性增长，但总体耗时维持在秒级。特别是在节点数量达到近千万级别的大规模网络中，算法的执行时间维持在 2 s 以内，表明了算法在大规模环境下的高效性。

而对于涵盖多重攻防行为的 APT 攻防模型，其威胁检测的复杂性相对更高，其性能测试结果如图 5 所示。测试结果显示，威胁检测算法的执行时间同样呈现出线性增长，即使网络节点数增加到近千万，算法的执行时间仍控制在 25 s 以内。这一性能表现证明了该算法在应对包含多个攻防行为的复杂场景时，具备良好的扩展性和高效性。

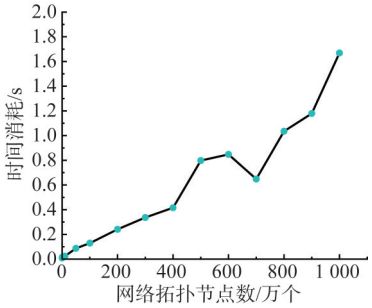

图 4　DDoS 攻击威胁发现性能测试

Fig. 4　Performance testing of DDoS attack threat detection

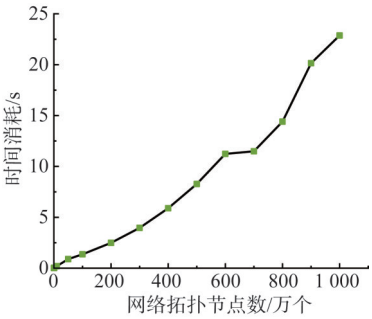

图 5　APT 攻击威胁发现性能测试

Fig. 5　Performance testing of APT attack threat detection

为了进一步验证威胁发现算法的效果，本实验在由 100 000 个节点构成的网络拓扑上测试了节点的成功攻击概率。实验统一调整并改变各原子操作的防御参数，同时引入随机源以模拟现实中的不确定性。在此基础上，对两种攻击模型下节点的平均攻击成功率进行了评估。实验中，将单个节点的攻击成功率超过 80 %的节点定义为脆弱节点。需要注意的是，实际推演中防御概率参数和随机源应基于实际的攻防行为及历史数据进行个性化配置。

实验结果显示，随着防御参数的整体提高，节点的平均攻击成功率逐渐下降，如图 6 所示；同时，脆弱节点的数量也随之减少，如图 7 所示，其中 DDoS 的脆弱节点数量由于仅涉及一次防御操作的概率计算，所以脆弱节点数相对 APT 攻击更多。

综合前述建模案例和威胁发现实验，本文通过

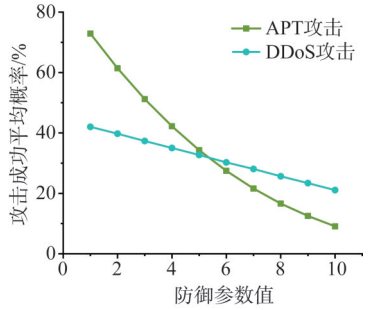

图6 节点平均攻击成功率测试

Fig. 6 Node average attack success rate test

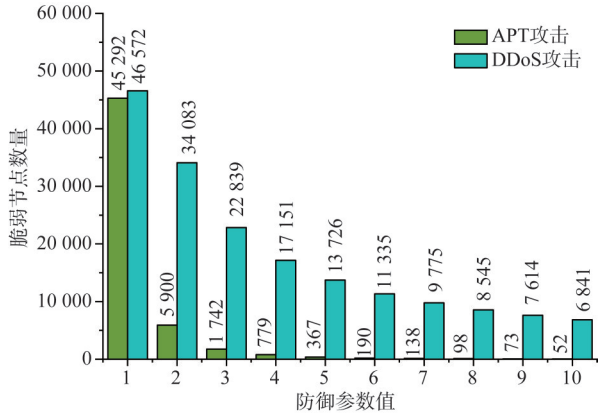

图7 不同防御参数下脆弱节点数量

Fig. 7 Number of vulnerable nodes under different defense parameters

具体的模拟案例验证了所提方法在不同规模攻防场景中的可用性。实验结果表明，在大规模网络拓扑下威胁发现算法能够快速识别威胁，并且防御参数的不同设置显著影响攻击成功概率。总体而言，本文提出的兵棋推演方法有效模拟攻防互动，并为电力网络的安全防护和策略优化提供支持。

5 结语

本文提出了一种面向电力网络安全风险演变的兵棋推演方法，旨在解决现有模拟技术在大规模电力网络推演中的低效和高资源消耗问题，填补了网络安全风险兵棋推演的空白。该方法通过抽象化处理模拟细节降低资源需求，并结合扩展性需求，可利用原子操作集构建灵活的建模框架，适应多变的安全威胁。在此基础上利用攻防行为建模生成的状态迁移图，并结合智能图搜索技术，可快速识别潜在的安全威胁。实验结果显示该方法能够对复杂的网络攻防事件进行建模，同时在大规模电力网络推演中可有效减少计算资源消耗，显著提升推演效率，为风险演变规律研究和网络攻防辅助决策提供坚实支撑。

在已提出电力网络兵棋推演框架下，可以进一步探索整合人工智能技术以自动化攻防策略生成和优化，实现更加智能化的决策，提升策略的灵活性和实际应用中的适应性。此外，研究还可通过与RTDS等电力系统仿真软件[21]或数字孪生技术[22-24]相结合，将网络攻防的后果投射到基础电力设施中，实现仿真网络的虚实结合，从而增强跨领域攻击的防御能力，全面提升电力网络安全的预见性和响应效率。

参考文献

[1] 盛戈皞，钱勇，罗林根，等. 面向新型电力系统的电力设备运行维护关键技术及其应用展望[J]. 高电压技术，2021，47(9)：3072－3084.
SHENG Gehao，QIAN Yong，LUO Lingen，et al. Key technologies and application prospects for operation and maintenance of power equipment in new type power system[J]. High Voltage Engineering，2021，47(9)：3072－3084.

[2] 单茂华，姚建国，杨胜春，等. 新一代智能电网调度技术支持系统架构研究[J]. 南方电网技术，2016，10(6)：1－7.
SHAN Maohua，YAO Jianguo，YANG Shengchun，et al. Study on architecture of new generation of dispatching technical supporting system for smart grid [J]. Southern Power System Technology，2016，10(6)：1－7.

[3] 胡金炜，张玉健，蔡莹，等. 虚拟电厂网络安全研究综述及展望[J]. 中国电机工程学报，2025，45(8)：2876－2899.
HU Jinwei，ZHANG Yujian，CAI Ying，et al. Review and prospect on cyber security of virtual power plant[J]. Proceedings of the CSEE，2025，45(8)：2876－2899.

[4] YOHANANDHAN R V，ELAVARASAN R M，MANOHARAN P，et al. Cyber-physical power system (CPPS)：a review on modeling，simulation，and analysis with cyber security applications [J]. IEEE Access，2020 (8)：151019－151064.

[5] 孙正龙，赵靖博，庄钧植，等. 基于OPC的电力信息物理系统仿真平台研究[J]. 电力系统及其自动化学报，2022，34(5)：70－78.
SUN Zhenglong，ZHAO Jingbo，ZHUANG Junzhi，et al. Research on simulation platform of cyber-physical power system based on OPC [J]. Proceedings of the CSU-EPSA，2022，34(5)：70－78.

[6] 闫健恩. 大规模网络安全事件仿真平台关键技术研究[D]. 哈尔滨：哈尔滨工业大学，2018.

[7] 符永铨，赵辉，王晓锋，等. 网络行为仿真综述[J]. 软件学报，2022，33(1)：274－296.
FU Yongquan，ZHAO Hui，WANG Xiaofeng，et al. State-of-the-art survey on network behavior emulation [J]. Journal of Software，2022，33(1)：274－296.

[8] 张智刚，康重庆. 碳中和目标下构建新型电力系统的挑战与展望[J]. 中国电机工程学报，2022，42(8)：2806－2819.
ZHANG Zhigang，KANG Chongqing. Challenges and

prospects for constructing the new-type power system towards a carbon neutrality future[J]. Proceedings of the CSEE, 2022, 42(8): 2806 - 2819.

[9] 王子骏，刘杨，鲍远义，等. 电力系统安全仿真技术：工程安全、网络安全与信息物理综合安全[J]. 中国科学：信息科学，2022，52(3)：399 - 429.
WANG Zijun , LIU Yang, BAO Yuanyi, et al. Power system security simulation technologies: engineering safety, network security and cyber-physical integrated security [J]. Scientia Sinica(Informationis), 2022, 52(3):399 - 429.

[10] 张童. 面向服务的语义可组合仿真关键技术研究[D]. 合肥：国防科学技术大学，2008.

[11] 李馥娟，王群. 网络靶场及其关键技术研究[J]. 计算机工程与应用，2022，58(5)：12 - 22.
LI Fujuan, WANG Qun. Research on cyber ranges and its key technologies [J]. Computer Engineering and Applications, 2022, 58(5):12 - 22.

[12] SALUJA A K, DARGAD S A, MISTRY K. A detailed analogy of network simulators—NS1, NS2, NS3 and NS4 [J]. Internationnal Journal on Future Revolution in Computer Science & Communication Engineering, 2017(3): 291 - 295.

[13] BIAN D, KUZLU M, PIPATTANASOMPORN M, et al. Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance[C]//2015 IEEE Power & Energy Society General Meeting, July 26 - 30, 2015, Denver, USA. New York: IEEE, 2015: 1 - 5.

[14] 吉梁，张士莹，王逸鹤. 网络攻防技战法及对策建议浅析[J]. 网络安全和信息化，2023(4):38 - 41.
JI Liang, ZHANG Shiying, WANG Yihe. Preliminary analysis of network attack and defense techniques and countermeasure recommendations [J]. Cybersecurity & Informatization, 2023(4): 38 - 41.

[15] 彭春光，鞠儒生，杨建池，等. 现代兵棋推演技术分析[J]. 系统仿真学报，2009，21(S2)：97 - 100.
PENG Chunguang, JU Rusheng, YANG Jianchi, et al. Analysis of technology of modern wargaming [J]. Journal of System Simulation, 2009, 21(S2):97 - 100.

[16] 常非. 美军主要推演和仿真系统模型体系与建模机制研究[J]. 军事运筹与系统工程，2015，29(2)：75 - 80.
CHANG Fei. The research on the U. S. military′s main wargaming and simulation system model architecture and modeling mechanism [J]. Military Operations Research and Systems Engineering, 2015, 29(2): 75 - 80.

[17] ANDY B, DAVID L P. Multi-resolution modeling in the JTLS-JCATS federation [R]. Orlando: The MITRE Corporation, 2003.

[18] 童和钦，倪明，赵丽莉，等. 基于关联矩阵的面向对象网络攻击建模方法研究与实现[J]. 电力信息与通信技术，2020，18(11)：1 - 8.
TONG Heqin, NI Ming, ZHAO Lili, et al. Research and implementation of correlation matrix based object-oriented modelling method for the cyber-attack [J]. Electric Power Information and Communication Technology, 2020, 18(11): 1 - 8.

[19] ADEPU S, MATHUR A. Generalized attacker and attack models for cyber physical systems[C]//2016 IEEE 40th annual computer software and applications conference (COMPSAC), June 10 - 14, 2016, Atlanta, USA. New York: IEEE, 2016: 283 - 292.

[20] 齐剑男，司光亚，王艳正，等. 基于网络攻防效果的电力信息物理系统模型[J/OL]. 系统工程与电子技术，1 - 11(2024 - 10 - 10)[2021 - 01 - 13]. http://kns. cnki. net/kcms/detail/11. 2422. TN. 20210112. 1328. 016. html.
QI Jiannan, SI Guangya, WANG Yanzheng, et al. On modeling of power cyber-physical system for the effect of cyber attack-defence[J/OL]. Systems Engineering and Electronics, 1 - 11(2024 - 10 - 10)[2021 - 01 - 13]. http://kns. cnki. net/kcms/detail/11. 2422. TN. 20210112. 1328. 016. html.

[21] 郦元天，郝正航，陈卓，等. 电力实时仿真器的关键指标及评价方法[J]. 南方电网技术，2025，19(5):128 - 136.
LI Yuantian, HAO Zhenghang, CHEN Zhuo, et al. Key indicators and evaluation methods for real-time power system simulators[J]. Southern Power System Technology, 2025, 19(5): 128 - 136.

[22] 吕金壮，廖毅，石延辉，等. 数字孪生技术在特高压直流系统中的应用实践[J/OL]. 南方电网技术，1 - 10[2024 - 06 - 30]. http://kns. cnki. net/kcms/detail/44. 1643. TK. 20240627. 2107. 013. html.
LÜ Jinzhuang, LIAO Yi, SHI Yanhui, et al. Application practice of digital twin technology in UHVDC systems [J/OL]. Southern Power System Technology, 1 - 10[2024 - 06 - 30]. http://kns. cnki. net/kcms /detail/44. 1643. TK. 20240627. 2107. 013. html.

[23] 刘婴，孙庆凯，许泽凯，等. 能源互联网中的数字孪生技术体系、应用与挑战[J]. 中国电力，2024，57(1)：230 - 243.
LIU Zhao , SUN Qingkai, XU Zekai, et al. System, applications and challenges of digital twin technology in Energy Internet[J]. Electric Power, 2024, 57(1): 230 - 243.

[24] 章耀耀，侯勇，叶海，等. 继电保护数字孪生技术应用展望[J]. 电力系统保护与控制，2023，51(12)：178 - 187.
ZHANG Yaoyao, HOU Yong, YE Hai, et al. Application prospect for relay protection digital twin technology[J]. Power System Protection and Control, 2023, 51(12): 178 - 187.

收稿日期：2024-12-18

作者简介：

杨祎巍(1982)，男，高级工程师(教授级)，博士，研究方向为智能电网安全，网络安全技术及密码应用技术，yangyw@csg. cn；

吴建彬(2001)，男，硕士研究生，研究方向为区块链安全应用、智能电网安全，jianbin. woo@gmail. com；

张玉健(1984)，男，通信作者，副教授，硕士生导师，博士，研究方向为智能电网安全，区块链与系统安全，yjzhang@seu. edu. cn。