计算机科学
COMPUTER SCIENCE

变电站远程监控网络攻击路径自动发现方法

史俊楠, 陈泽茂, 张立强

引用本文

史俊楠, 陈泽茂, 张立强. 变电站远程监控网络攻击路径自动发现方法[J]. 计算机科学, 2025, 52(12): 339-350.

SHI Junnan, CHEN Zemao, ZHANG Liqiang. Automatic Attack Path Discovery Method for Substation Remote Monitoring Network [J]. Computer Science, 2025, 52(12): 339-350.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250100143

变电站远程监控网络攻击路径自动发现方法

史俊楠　陈泽茂　张立强
武汉大学国家网络安全学院　武汉 430072
武汉大学空天信息安全与可信计算教育部重点实验室　武汉 430072
(2018302180081@whu.edu.cn)

摘　要　随着变电站从孤立系统发展为跨越IT和OT的复杂联网系统,其面临的安全威胁日益严峻,识别针对变电站远程监控网络的潜在攻击路径变得尤为重要。针对该问题,提出了一种基于MITRE ATT&CK框架的自动化攻击路径规划方法,将MITRE ATT&CK技术作为攻击原语,基于Cyber Kill Chain进行攻击阶段映射,在构建形式化的威胁模型的基础上,设计了PDDL(Planning Domain Definition Language)描述自动生成方法,将网络攻击路径发现问题转换为通用的自动规划问题,实现了对攻击路径的细粒度的自动化分析。实验结果表明,该方法有效降低了对用户专业知识的依赖,能够结合具体的网络拓扑信息,自动生成全面且具有实战指导价值的攻击路径,为自动化渗透测试及安全防护体系建设提供了有力支持。

关键词:变电站远程监控网络;自动化攻击路径发现;威胁建模;规划领域定义语言;MITRE ATT&CK框架
中图分类号　TP393

Automatic Attack Path Discovery Method for Substation Remote Monitoring Network

SHI Junnan,CHEN Zemao and ZHANG Liqiang
School of Cyber Science and Engineering,Wuhan University,Wuhan 430072,China
Key Laboratory of Aerospace Information Security and Trusted Computing,Ministry of Education,Wuhan University,Wuhan 430072,China

Abstract　As substations evolve from isolated systems to complex networks spanning IT and OT,the security threats they faced are increasing,making the identification of potential attack paths in remote monitoring networks crucial. This paper presents an automated attack path planning method based on the MITRE ATT&CK framework. It treats ATT&CK techniques as attack primitives and maps attack stages using the Cyber Kill Chain. A formalized threat model is constructed,and a PDDL-based method for automatic generation is proposed,transforming the attack path discovery problem into a general automated planning issue for fine-grained analysis. Experimental results show that this method reduces reliance on user expertise,generates comprehensive and practically valuable attack paths based on specific network topology,and provides strong support for automated penetration testing and security defense system development.

Keywords　Substation remote monitoring network,Automated attack path discovery,Threat modeling,Planning domain definition language,MITRE ATT&CK framework

1　引言

智能变电站作为关键基础设施,广泛分布于不同的地理位置,已经从一个没有互联网访问和远程连接功能的孤立系统,发展成跨越IT与OT的复杂联网系统。互联网的接入虽然带来了便利,但也引入了新的安全风险。早在2015年,Kyivoblenergo电力公司的7个110 kV变电站和23个35 kV变电站就因攻击者通过入侵远程监控网络,实施隐蔽且复杂的攻击,导致了严重的物理损害[1]。在这种背景下,自动化识别潜在攻击路径可为智能变电站的自动化渗透测试和安全防护体系建设提供有效支持。

近年来,智能变电站的网络安全问题日益得到关注。Chai等[2]分析了智能变电站面临的网络威胁,总结了4类安全威胁,但作者仅对这4类威胁进行了概念描述,缺乏深入分析。Kolosok等[3]梳理了针对智能变电站的多种具体攻击手段,但没有结合其网络结构进行分析,导致缺乏针对性。Khodabakhsh等[4]与Gaspar等[5]结合智能变电站的网络架构分析了各组件的脆弱性,但未能对攻击行为进行准确描述,

到稿日期:2025-01-22　返修日期:2025-05-03
基金项目:国家重点研发计划(2022YFC3102805);工业互联网数据安全检测响应与溯源系统(TC220H055)
This work was supported by the National Key Research and Development Program of China(2022YFC3102805) and Industrial Internet Data Security Detection,Response,and Traceability System(TC220H055).
通信作者:陈泽茂(chenzemao@whu.edu.cn)

导致其成果难以应用到自动化渗透测试等安全实践中。Jbair等[6]将攻击者战术、技术与通用知识库(Adversarial Tactics, Techniques, and Common Knowledge, ATT&CK)攻击知识图谱[7]引入工业控制系统的威胁建模过程,为安全实践提供了理论支持,但其攻击树的构建依赖手工分析,缺乏自动化方法。

攻击路径自动化发现研究主要聚焦3类方法:基于智能规划的方法、基于强化学习的方法以及基于大模型的方法[8]。智能规划方法基于环境初始条件,生成实现预定目标的最优行动序列。Boddy等[9]使用智能规划方法解决攻击路径发现问题。Wang等[10]基于规划领域定义语言(Planning Domain Definition Language, PDDL)[11]实现了跨越IT与OT的攻击路径发现方法,但该方法要求使用者具备丰富的网络安全知识并人工配置PDDL文件。强化学习的方法则通过动态试错机制探索网络攻击路径。Wang等[12]将专家经验编码为结构化知识库并与深度学习算法融合,提升了攻击路径的可解释性。然而,在变电站异构设备场景中,该方法需针对不同设备特性人工提取知识规则,成本较高。Liu等[13]结合ATT&CK框架与强化学习,在航空管理系统中生成了细粒度攻击序列。但该方法依赖于高质量的数据集,而变电站运营商通常对网络数据发布持谨慎态度,这限制了其在变电站场景中的应用。大模型方法通过预训练知识库与上下文推理能力,动态生成攻击路径。Happe等[14]利用ATT&CK框架验证了大模型在自动化渗透领域的可行性,但尚未应用到具体的工业场景中。Deng等[15]基于大语言模型开发了自动化渗透测试工具PentestGPT,其攻击路径发现机制依赖于用户输入目标和环境信息,并通过与测试环境的交互反馈来生成完整攻击链。然而,在智能变电站场景中,单次交互可能造成严重的物理后果。

为解决现有智能变电站安全研究难以落地实践以及现有的攻击路径自动发现方法不适应变电站场景的问题,本文结合MITRE ATT&CK框架,构建了智能变电站远程监控网络的形式化安全分析模型,并提出了一种基于PDDL的自动化攻击路径发现方法。该方法减少了对用户专家知识的依赖,提高了攻击路径发现的自动化水平。

本文的主要贡献如下:

1)提出了一种结合MITRE ATT&CK和Cyber Kill Chain[16]的攻击路径发现方法,充分利用开源网络安全知识库为变电站远程监控网络的攻击路径提供细粒度分析;

2)基于形式化模型自动生成PDDL描述文件,将网络攻击路径发现问题转换为通用的自动规划问题并与现有工具进行集成,提高了攻击路径发现的自动化程度;

3)实验结果表明,所提方法在降低对用户专业知识依赖的同时,能够自动生成全面且具有实战指导价值的攻击路径。

本文第1章阐述变电站远程监控网络面临的安全问题和研究现状;第2章构建了变电站远程监控网络威胁分析的形式化模型;第3章根据形式化模型设计了对应的PDDL描述自动生成算法及具体实现;第4章通过实验验证了所提方法的可行性;最后进行总结。

2 变电站远程监控网络的形式化建模

本章基于IEC 61850标准构建变电站网络环境模型,并结合MITRE ATT&CK框架构建攻击者行为空间。网络环境模型与攻击者行为空间结合,形成变电站远程监控网络的威胁模型。

2.1 智能变电站网络模型

基于IEC 61850标准的智能变电站的网络环境,主要包含电力远程监控网络的网络拓扑、设备以及数据交互等系统本身环境信息。图1描述了一个可能的IEC 61850网络拓扑及其数据流图,该网络通过多种智能电子设备(Intelligent Electronic Device, IED)实现电力系统的实时监控,核心组件包括合并单元(Merging Unit, MU)、保护和控制IED(Protection & Control IED, P&C IED)、测量IED(Measurement IED, ME IED)及断路器(Circuit Breaker, CB)。

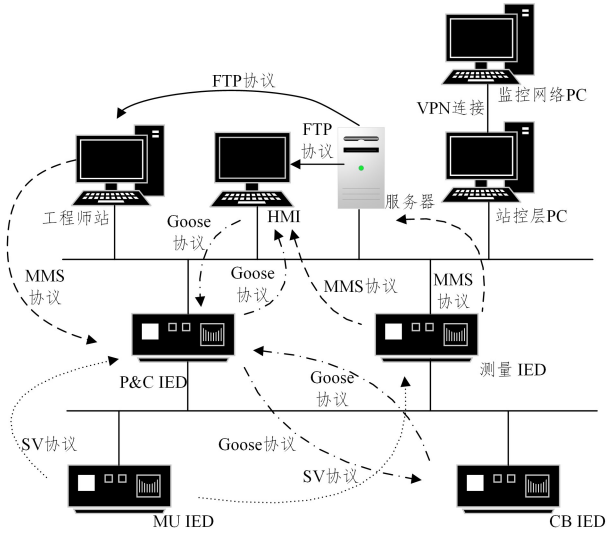

图1 IEC 61850智能变电站数据流图

Fig. 1 Data flow diagram of IEC 61850 smart substation

1)MU IED→P & C IED、测量IED:MU IED以固定周期对电流与电压值进行采样,广播发送SV(Sampled Value)数据包给相关间隔层设备;P & C IED通过保护算法判断系统是否正常运行并实施保护操作;测量IED实时监控测量值信息,向站控层设备发送诊断报告。

2)P & C IED→CB IED:P & C IED检测到故障发生时,通过Goose(Generic Object Oriented Substation Event)协议向CB IED发送跳闸命令。根据IEC 61850-8-1,此类报文在第一次发送后,需要按照2^n($n=1,2,3,\cdots$)ms重复发送。

3)CB IED→P & C IED:在系统运行期间,CB IED通过Goose协议周期性向P & C IED发送断路器状态信息。当接收到P & C IED的控制命令时,CB IED以快速重传机制向P & C IED发送Goose报文。

4)P & C IED、测量IED→HMI:在系统正常运行期间,间隔层设备向站控层的HMI周期性地发送测量值信息以及系统状态信息,通常这些消息被映射到MMS(Manufacturing Message Specification)协议中[17]。在系统发生故障时,间隔层IED向站控层的HMI发送突发Goose消息。

5）HMI→P & C IED：在一些异常情况下，或在系统维护期间，需要维护人员通过 HMI 手动控制断路器，即 HMI 向 P & C IED 发送突发的 Goose 命令。

6）测量 IED→服务器：间隔层设备除了向站控层设备发送周期性测量消息外，也会通过 MMS 协议发送事件记录信息、故障录波数据、设备本身的自我诊断信息以及历史数据与统计信息等对实时性要求不高的数据。

7）工程师站→P & C IED：在智能变电站的维护期间，工程师站可以对 P&C IED 进行配置更改，如电流速断定值、过电流定值以及动作特性的设置。

8）服务器→工程师站、HMI：站控层设备可以通过多种协议进行数据交换，如站控层工程师站、HMI 可使用 FTP 协议与服务器之间进行文件传输。

2.2 攻击者行为空间分析

行为空间指攻击者可能采取的攻击行为。本节结合 MITRE ATT&CK 开源框架，针对企业网络与工控网络分别提取攻击者的策略与技术，对攻击者可能的攻击行为进行建模。

ATT&CK 是开源的威胁知识框架，系统性地描述了网络攻击者的行为、技术手段及目标战术，旨在支持组织增强威胁检测与防御能力。其覆盖范围包括企业网络、移动设备及工业控制系统。电力远程监控系统融合了企业网络与工业控制系统的特性，基于 ATT&CK 框架可实现对其关键组件与核心流程的有效覆盖。MITRE ATT&CK 框架中的战术（Tactics）定义了攻击者行为的目标动因，如工控系统中的 Initial Access，Execution，Persistence 和 Command and Control 等战术，这些战术天然具备顺序关系，与 Cyber Kill Chain 的阶段模型相对应。每个战术包含相应的技术（Techniques），构成了攻击者的行为空间。通过结合战术的顺序逻辑和技术的具体描述，可提取各技术的前置条件和后置条件，从而为攻击路径发现提供理论基础。

ATT&CK 中的 Techniques 是攻击者为实现战略目标所采取的具体技术，每项 Techniques 都对应着一项或多项 Tactics。攻击者使用 Techniques 时大致遵循如表 1 所列的排序。以入侵智能变电站中的工程师站并篡改 P&C IED 配置引发电力故障为例，攻击者可根据 Cyber Kill Chain 的各阶段展开攻击：首先，通过 Nmap 等工具扫描网络以获取目标信息；侦察之后，基于系统漏洞（如 CVE-2017-0144）针对性地开发恶意载荷；利用弱密码登录工程师站，并上传恶意软件；随后，攻击者通过恶意软件进行权限提升；在此基础上，攻击者安装后门程序，以建立稳定的远程控制通道；最后，攻击者通过远程控制通道篡改 P&C IED 的配置文件，触发断路器误动，从而引发电力故障。这一过程表明，攻击者的每个行动步骤均受系统当前状态的制约，同时会改变系统状态。基于这一特性，可构建全面的攻击行为空间模型，系统化描述攻击路径的前置条件、后置条件及状态演化关联。

攻击行为空间可由五元组（Action，Description，Target，Precondition，Effects）构成。其中，Action 代表攻击者执行的攻击动作，可使用 ATT&CK 的 Techniques 编号表示，如 T0802 等；Description 表示对该动作的详细描述；Target 代表攻击者的攻击目标，包括主机、网络和工控设备等类型；Precondition 代表攻击者执行 Action 的前置条件；Effects 代表攻击行为的后果，即后置条件，前、后置条件通过攻击目标与攻击所属阶段生成。

表 1 ATT&CK 战术与 Cyber Kill Chain 的网络攻击阶段映射表及前后置条件分析

Table 1 Mapping of ATT&CK Tactics to Cyber Kill Chain phases and analysis of pre-conditions and post-conditions

Cyber Kill Chain 各阶段	针对工业控制系统 ATT&CK Tactics	针对企业网络的 ATT&CK Tactics	攻击的前置条件	攻击的后置条件
Reconnaissance	Discovery，Collection	Reconnaissance，Discovery，Collection	攻击者决定攻击目标	攻击者获取攻击目标信息
Weaponization	—	Resource Development	攻击者完成侦察	攻击者开发出攻击载荷
Delivery	Initial Access，Lateral Movement	Initial Access，Lateral Movement	攻击者可接触攻击目标且拥有特定攻击工具	攻击目标携带攻击载体
Exploitation	Privilege Escalation	Privilege Escalation	攻击目标携带攻击载体	攻击目标可执行代码
Installation	Execution	Execution	攻击目标可执行代码	攻击目标被攻击者妥协
Command and control	Command and Control，Persistence	Command and Control，Persistence	攻击目标被攻击者妥协	攻击者建立了与目标系统的外部控制通道
Actions on objectives	Impact，Impair Process Control，Inhibit Response Function	Exfiltration，Credential Access，Impact	攻击者拥有与攻击目标的通信信道	攻击者完成攻击目标

2.3 智能变电站远程监控网络的威胁建模

为梳理智能变电站远程监控网络面临的安全威胁，从设备节点、网络节点、脆弱性、攻击技术以及通信关系等方面构建威胁模型。

定义 1（智能变电站远程监控网络的威胁模型） 针对智能变电站远程监控网络的威胁模型定义为 $G=\langle N_{\text{device}}, N_{\text{network}}, V, T, E, f, g, P\rangle$，模型中各元素的定义见后文。

定义 2（设备节点集） N_{device} 表示系统中的设备节点集合，任意设备节点 $d_i \in N_{\text{device}}$ 可表示为 $d_i=(id, type, ip, mac, function, sta, component)$。其中，$id$ 表示设备的唯一标识；ip 和 mac 分别表示设备的 IP 地址与 MAC 地址；$function$ 描述设备功能；sta 表示设备状态，如是否在线以及开放端口号等；$component$ 表示系统组件，包括固件、操作系统版本等信息。

定义 3（网络节点集） N_{network} 表示系统中的网络节点集合，网络节点 $n_i \in N_{\text{device}}$ 可表示为 $n_i=(type, protocols)$，其中 $type$ 表示网络类型，$protocols$ 表示网络中存在的通信协议。

定义 4（脆弱性集合） V 表示 N_{device} 与 N_{network} 存在的脆弱性集合，任意脆弱性 $v_i \in V$ 可表示为 $v_i=(id, node, name,$

description)。其中，*id* 是脆弱性的唯一编号，$node \in N_{device} \cup N_{network}$ 表示脆弱性影响对象，*name* 是脆弱性名称，*description* 是对脆弱性的详细描述。

定义 5(攻击技术集合) T 表示 ATT&CK 中攻击者的技术，即攻击行为空间集合，$t_i \in T$ 可表示为 $t_i = (action, description, precondition, effects)$。其中，*action* 表示攻击者的具体技术，为 ATT&CK 中的 Techniques 编号；*description* 为对其的描述；*precondition* 与 *effects* 分别表示执行攻击技术的前置条件和后置条件。

定义 6(连接关系集合) E 表示连接关系集合，$e_i \in E$ 表示为 $e_i = (n\_f, n\_t, protocols)$。其中，$n\_f$ 与 n_t 表示连接关系的起点与终点，属于设备节点或网络节点；*protocols* 表示节点之间的通信协议。

定义 7(脆弱性映射) 脆弱性映射 f 用于表示设备节点或网络节点拥有的脆弱性，可表示为 $f: N_{device} \cup N_{network} \rightarrow V$。对于节点 n_i，$f(n_i) = \{v_1, v_2, \cdots\}$ 表示与节点关联的脆弱性集合。

f 映射的实现主要依赖于渗透测试工具的使用以及已知的漏洞数据库，如使用 metasploit 等自动化渗透测试工具对系统进行渗透测试，或通过 CVE 和 NVD 等已知漏洞数据库以及厂商的安全公告分析设备的类型、操作系统版本、硬件平台等信息，确定设备可能面临的脆弱性。

定义 8(攻击技术映射) 攻击技术映射 g 用于表示攻击者针对脆弱性可利用的攻击技术，可表示为 $g: V \rightarrow T$。对于脆弱性 v_i，$g(v_i) = \{t_1, t_2, \cdots\}$ 表示与脆弱性相关的 ATT&CK 攻击技术集合。

g 映射的实现是当前的研究热点。Abdeen 等[18]开源了基于文本相似性自动关联 CVE 条目与 ATT&CK Techniques 的工具 SMET。通过这两层映射，可直接建立设备与攻击技术的对应关系，表示为 $g(f(n_i)) = \{f(v_1), f(v_2), \cdots\} = \{t_1, t_2, t_3, t_4, \cdots\}$。在实际的应用中，脆弱性对应的攻击技术较为固定。用户对设备进行脆弱性分析后，可自然得出攻击者针对该设备可利用的攻击技术集合。

定义 9(攻击路径) P 表示攻击者为实现攻击目标可采取的攻击序列，表示为 $P = \{x_1, x_2, \cdots, x_n\}$。其中，$n = 1, 2, 3, \cdots$；$x_i = (node, (t_1, t_2, \cdots, t_n))$，$node \in N_{network} \cup N_{device}$ 且 $t_i \in T$。

给定威胁模型 G 以及攻击目标 *goal*，假设系统初始状态为 S_0，其随着攻击者执行攻击动作 T 而更新。攻击路径发现问题可形式化表示为：

$$P = \left\{ \begin{array}{c} \pi = (x_1, \cdots, x_n) \in P \mid \forall i \in [1, n]: \\ (1)\, x_i = (node_i, T_i = (t_{i1}, \cdots, t_{ik})) \wedge node_i \in N_{network} \cup N_{device}; \\ (2)\, \forall t_{ij} \in T_i, precondition(t_{ij}) \in S_{i,j-1} \wedge t_{ij} \in g(f(node_i)); \\ (3)\, \forall j \in [1, |T_i|], S_{i,j} = Update(S_{i,j-1}, effects(t_{ij})); \\ (4)\, \forall i \in [1, n-1]: \exists e \in E, e = (node_i, node_{i+1}, protocols); S_{i+1,0} = S_{i,|T_i|}; \\ (5)\, goal \in S_{n,|T_n|} \end{array} \right\}$$

3 威胁模型的 PDDL 描述自动生成方法

通过形式化构建变电站远程监控网络的威胁模型，攻击路径发现问题得以系统化。本章提出了一种基于变电站威胁模型的 PDDL 描述自动生成方法。该方法基于 PDDL 的标准语法规则，针对变电站远程监控网络的攻击场景进行了适配，将网络攻击路径发现问题转换为通用的规划问题。首先自动生成领域定义文件(Domain Definition)和问题定义文件(Problem Definition)，继而通过 SGPlan 等规划器对文件进行解析，自动生成可行的攻击路径序列。

3.1 领域定义文件元素设计

领域定义是对规划问题的抽象描述，定义了该领域内的通用元素和规则。领域定义一般由类型定义(Types)、动作定义(Actions)、常量(Constants)以及谓词定义(Predicates)等元素组成。

Types 是一种用于对规划问题中涉及的对象进行分类的机制，将具有相似性质或用途的对象归为一类。威胁模型 G 包含设备、网络、脆弱性以及攻击技术 4 类实体节点。设备包括监控网络设备、站控层设备、间隔层设备以及过程层设备；网络包括监控网络、站控层网络以及间隔层网络。基于 G 中的实体节点，对应设计领域定义文件中的 Types。

Actions 是系统状态转换的原因。在智能变电站远程监控网络的攻击场景中，攻击动作导致系统状态的改变。PDDL 的 Actions 对应威胁模型中的 T。在 PDDL 中，Actions 一般由参数、前提条件、效果等定义。参数用于明确动作的作用对象，对应 G 中的 N_{device} 与 $N_{network}$；前提条件用于表明攻击的前置条件；效果用于表明攻击对设备或网络造成的影响，对应 G 中的攻击技术手段 t 的 preconditions 与 effects 属性。

Constants 指在规划问题中不可变化的实体或参数。在威胁模型 G 构建完成后，攻击者的行为空间也随之确定。攻击者若在设备 *device* 执行攻击动作 t，必须满足 $t \in g(f(device))$。在 PDDL 中可用语句 Has-techniques ?device t 表示条件是否满足，device 用变量表示，t 用常量，表示可使表达式更简洁。PDDL 的 Constants 对应 Actions 的攻击动作名称。

Predicates 可用于描述领域中对象之间的关系或对象的属性。对象之间的关系主要体现在设备或网络节点之间是否相连，对象的属性可分为设备本身属性和与安全相关属性。设备本身属性主要指设备的类别；安全相关属性是对攻击者攻击进度的描述，如表示某台设备是否被妥协，攻击信道是否建立等。PDDL 谓词设计旨在形式化描述系统状态及其在攻击过程中的变化，具体设计如表 2 所列。攻击者通过 T1087 技术识别监控网络设备 Host 的邮箱账户后，谓词 Information-Collected(Host)由 False 转为 True，标志目标情报收集完成。随后，攻击者基于 T0865 技术向该邮箱投递钓鱼邮件载荷，谓词 Payload-delivered(Host)状态更新为 True，此时攻击者可以进一步实施后续攻击，如权限提升、设备妥协以及横向移动等。

表 2 PDDL 谓词设计

Table 2 PDDL predicates design

Predicates 取值	简写	描述
Information-Collected	IC	设备或网络的信息是否被攻击者收集
Payload-created	PC	攻击者是否创建了用于攻击的载荷
Payload-delivered	PD	设备是否携带攻击载荷
Code-Executed	CE	攻击者是否在设备上拥有执行恶意代码的能力
Compromised	CD	网络或设备是否被妥协
C&C-established	CC	攻击者是否建立了与目标系统的外部控制通道
Objective-achieved	OA	攻击目标是否生成
Connected	CO	表明设备和网络是否相连
Target-selected	TS	攻击者初步选取攻击目标
Has-techniques	HT	攻击者针对设备 D 可使用的攻击技术 T

3.2 问题定义文件元素设计

问题定义描述特定的规划实例，指定了环境的初始状态与目标状态。问题定义文件由对象(Objects)、初始状态(Init)和目标(Goal)组成。

Objects 用于表示问题规划实例中的所有对象，其由威胁模型 G 中所有的实体节点构成。Init 描述了规划开始时，系统中各个对象的状态和属性。威胁模型 G 中的 E 描述了设备和网络之间的连接关系，g 和 f 描述了设备和攻击技术之间的对应关系。PDDL 的 Init 对应 E，g 和 f。Goal 描述了规划问题期望达到的最终状态。该部分由用户自定义，生成方式与 Init 相同。

BlackEnergy 是一款针对电力系统的恶意软件。图 2 展示了基于 BlackEnergy 攻击构建的威胁模型，并以此为例说明 PDDL 元素在路径规划中的作用。

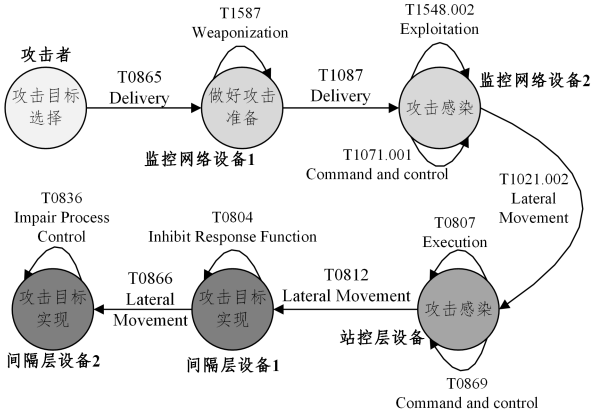

图 2 Blackenergy 攻击示例

Fig. 2 Example of Blackenergy attack

图 2 中包括多个 ATT&CK 技术，基于这些技术生成相应的 Actions 和 Constants，表示攻击者可能采取的所有行动。Objects 包括所有设备和攻击技术。Init 主要描述了设备之间的连接信息及可对设备实施的攻击技术。攻击开始时，仅攻击者自身被视为妥协对象，Goal 则设定为间隔层设备的妥协。

图 3 展示了 BlackEnergy 攻击路径的规划结果，各虚线框对应单台设备的状态迁移轨迹，呈现了攻击者从初始入侵到目标设备被攻陷的全过程。在这一过程中，攻击者利用不同的攻击手段逐步扩展对目标系统的控制，最终实现对间隔层设备的妥协。每执行一个攻击动作，对应的设备状态就会发生相应变化，这些状态变化通过 Predicates 进行描述，从而反映出攻击的演变过程。

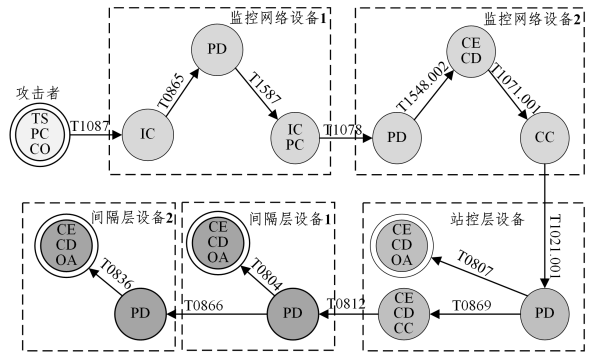

图 3 Blackenergy 攻击路径规划结果

Fig. 3 Result of Blackenergy attack path planning

3.3 PDDL 描述自动生成算法

图 4 给出了 PDDL 描述自动生成算法的总体框架，共分为威胁模型构建、PDDL 文件生成与攻击路径发现 3 个阶段。

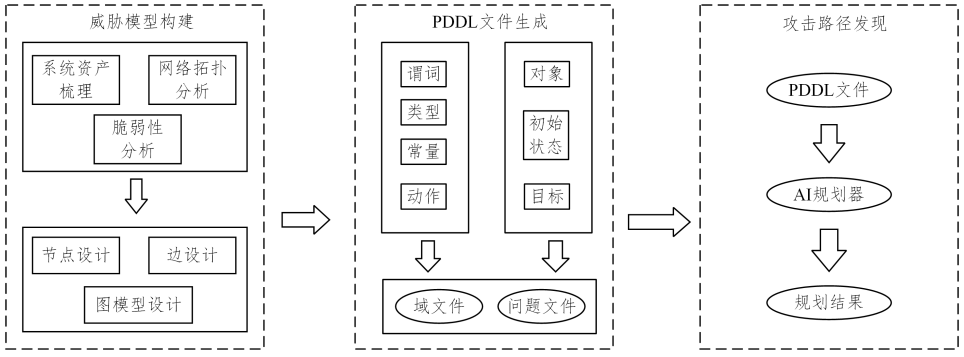

图 4 PDDL 自动生成算法总览

Fig. 4 Overview of PDDL automatic generation algorithm

在威胁模型构建阶段，通过对变电站监控网络的资产梳理、网络拓扑分析以及脆弱性评估，完成了系统的形式化建模，并采用 Neo4j 作为数据存储解决方案。图 5 展示了基于 Neo4j 的图数据结构，用于表达设备与网络之间的连接关系、设备和网络所具备的脆弱性及其与 ATT&CK 技术之间的关联。图中的设备节点对应威胁模型中的 N_{device}，表示网络拓扑中的设备实体；脆弱性节点对应威胁模型中的 V，用以表示设备具备的脆弱性；技术节点对应威胁模型中的 T，表示针对某个脆弱性可利用的攻击技术。

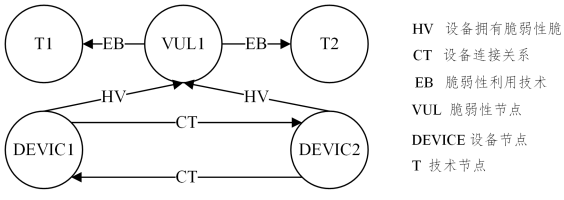

图 5 基于 Neo4j 的图数据结构

Fig. 5 Graph data structure based on Neo4j

具体而言，设备或网络的连接关系根据实际的网络拓扑结构生成，并通过图结构展现。此外，ATT&CK 技术的每一个节点，如 T0836 等，均在图中独立表示。脆弱性节点作为系统脆弱性抽象的表示，具体描述了潜在的安全问题，如不可信的固件供应商、账户权限控制不足等。脆弱性节点与相应的技术节点建立关联后，便可作为复用模块，在系统中进行动态更新和调整。相关人员根据设备的操作系统版本、固件版本及安全配置等信息，对脆弱性进行评估，从而建立设备节点与 ATT&CK 技术节点之间的有效连接。

表 3 列出了 Neo4j 节点的设计，其主要基于变电站远程监控网络的网络结构进行设计。整个设计分为四大类节点，即设备节点、网络节点、脆弱性节点和技术节点，每一类节点都有其特定的属性，旨在描述变电站中不同实体的相关特征。将网络节点作为独立节点进行建模，可以清晰地表达不同层次之间设备的网络连接方式，突出各类网络的特点，便于描述一些针对通信消息进行修改的攻击手段。

表 3 Neo4j 节点设计

Table 3 Neo4j node design

节点类别	描述	属性
STATION_DEVICE	站控层设备	name, ip, mac, function
BAY_DEVICE	间隔层设备	name, ip, mac, function
PROCESS_DEVICE	过程层设备	name, mac, function
STATION_NET	站控层网络	name, protocols
PROCESS_NET	过程层网络	name, protocols
VULNERABILITY	脆弱性	ID, name, description
TECHNIQUES	攻击技术	name, tactic, description

Neo4j 的边设计如表 4 所列，用于建立节点之间的关系；关系结构如图 5 所示。

表 4 Neo4j 边设计

Table 4 Neo4j edge design

边类别	描述
HAS_VULNERABILITY	连接 VULNERABILITY 与各类 DEVICE 节点，表明设备拥有的脆弱性
EXPLOITED_BY	连接 TECHNIQUES 与 VULNERABILITY，表明攻击者可利用的攻击技术
CONNECTS_TO	连接 DEVICE 节点与 NET 节点，表明设备接入的网络

构建威胁模型后，进入 PDDL 文件生成阶段，根据图数据库生成 PDDL 的元素，再将这些元素组装成 PDDL 的域文件与问题文件。

算法 1 描述了 PDDL 领域定义文件 domain. pddl 的自动生成过程。其主要包括 types, constants, predicates 以及 actions 4 类主要元素：types 根据图数据库 G 中的节点类型生成；constants 为域文件中的常量，根据 G 中的 T 节点生成，如 T836 等；predicates 根据表 2 生成，用于描述系统所处的状态；每一个常量对应一个 action，即攻击者可能采取的攻击动作。除此之外，根据网络杀伤链的每个阶段生成默认攻击动作，生成文件如图 6 所示。

算法 1 PDDL 领域定义文件生成算法

输入：(G, T)

输出：(types, constants, predicates, actions)

```
1. / * 生成 PDDL 的类型和常量 * /
2. for each node in G do
3.     add node. type to types
4.     if node. type == TECH do
5.         add node. name to constants
6.     end if
7. end for
8. / * 根据元素设计生成 PDDL 谓词 * /
9. Generate predicates from design
10. / * 生成 PDDL 动作 * /
11. for each TECHNIQUES in G do
12.     ATTACK_PHASE = T(TECHNIQUES)
13.     Generate action from ATTACK_PHASE
14.     add action to actions
15. end for
16. Generate default-actions
17. add default-actions to actions
18. Generate domain. pddl
19. return domain. pddl
```

```
(define (domain attackpath_discovery)
  (:requirements :strips :fluents :equality)
  (:types                                          实体类型
    OUT_DEVIC STATION_DEVIC BAY_DEVICE - Device
    OUTSIDE_NET STATION_NET PROCESS_NET - Net
    VULNERABILITY - Vulnerability
    TECHNIQUES - Techniques
  )
  (:constants                                      常量
    T0864 RE DE EX IN CC AC..... - Techniques
  )
  (:predicates                                     谓词设计
    (Vulnerability ?v)
    (connected ?d1 ?d2)
    (Information-Collected ?d)
        .....
  )
  (:action T0864Delivery                           动作设计
    :parameters(?device1 ?device2)
    :precondition
    (and
      (or (Device ?device1) (Net ?device1))
      (or (Device ?device2) (Net ?device2))
      (connected ?device1 ?device2)
      (Compromised ?device1)
      (Information-Collected ?device2)
      (has-techniques ?device1 T0864)
    )
    :effect (Payload-delivered ?device2)
  )
```

图 6 领域定义文件示例

Fig. 6 Example of domain definition file

算法 2 描述了 PDDL 问题定义文件 problem. pddl 的自动生成过程。objects 用于表示系统实体，依据图数据的节点生成；inits 用于表达系统状态，依据图数据库中的边生成；goal 表示系统的攻击目标，可自行设定。生成文件如图 7 所示。

算法 2 PDDL 问题定义文件生成算法

输入：G

输出：(objects，inits，goal)

1. / * 生成 PDDL 对象 * /
2. for each node in G do
3. add node. name to objects
4. end for
5. / * 生成 PDDL 初始状态 * /
6. for each DEVICE in G do
7. add connected-neighbor to inits
8. for eachTECH in G do
9. add DEVICE-TECH to inits
10. end for
11. add DEVICE-TECH-default to inits
12. end for
13. / * 生成 PDDL 目标 * /
14. Generate goals
15. Generate problem. pddl
16. RETURN problem. pddl

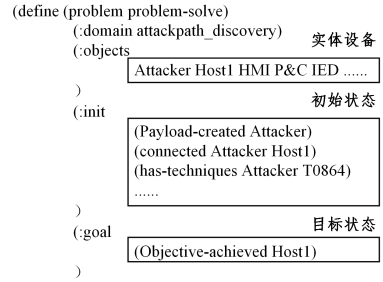

图 7 问题定义文件示例

Fig. 7 Example of problem definition file

生成 PDDL 描述文件后，可选取多种规划器进行路径规划，本文选取 SGPlan。该规划器采用爬山算法，不断选择最佳的可行动作进行搜索，直至达到目标状态或无法继续优化为止。在变电站监控网络场景中(见图 1)存在多个数据流。根据所选定的数据流，domain. pddl 文件中设备之间的连接状态需要进行相应的修改。图 8 中的 6 个子图展示了一条数据流中多条攻击路径的发现过程。

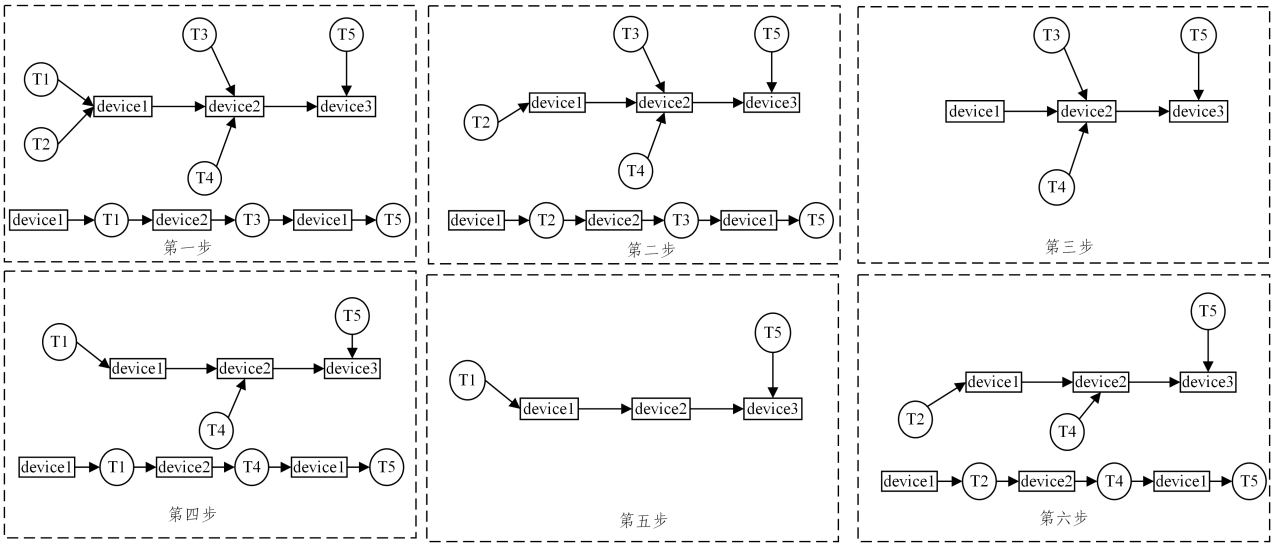

图 8 攻击路径发现示例

Fig. 8 Example of attack path discovery

假设存在设备连接路径：device1→device2→device3。攻击者在 device1 上可利用 T1 与 T2 两种攻击技术，在 device2 上可利用 T3 和 T4 两种攻击技术，在 device3 上使用攻击技术 T5 达成攻击目标。其中，T1 与 T2 属于网络杀伤链的同一攻击阶段，T3 与 T4 同理。攻击者初始位置位于 device1，为达到攻击目标，存在如图 8 所示的 4 条攻击路径。在第一条路径的起始设备上，删除当前路径中使用的攻击技术 T1，仅保留 T2 可用，并重新规划出新的路径 T2→T3→T5。接着，删除当前路径中 device1 的剩余攻击技术 T2，此时 device1 无法提供可用技术，规划器无法生成新的路径。随后，依次恢复 device1 的所有攻击技术，从 device2 开始，删除其当前路径中使用的技术 T3，再次进行路径规划。当所有设备的攻击技术都已逐一尝试删除，且无法生成新的路径时，路径生成结束。

在实际应用中，针对某一设备的攻击技术可能无法覆盖整个 Cyber Kill Chain 的所有阶段，这可能导致某些攻击阶段的缺失。为了确保攻击路径规划在缺失阶段仍能继续进行，可以引入缺省项来代替这些未覆盖的攻击技术。使用缺省项不仅能够提高攻击路径生成的容错能力，增强路径规划的鲁棒性，还能模拟攻击者可能使用的未知技术，从而提高路径规划结果的全面性。

4 实验与评估

本章利用如表 5 所列的工具进行攻击路径发现实验。

Microsoft Threat Modeling Tool(MS-TMT)基于 STRIDE 模型自动识别系统威胁,SG_TMT 是 Lars Halvdan Fla[19] 利用 MS-TMT 创建的用于智能变电站威胁识别的模板。Neo4j 用于以图结构存储威胁模型,Python 连接 Neo4j 数据库生成 PDDL 描述文件,SGPlan 根据该文件规划攻击路径。

表 5 实验工具

Table 5 Experiment tools

工具	版本
Microsoft Threat Modeling Tool	7.3.31026.3
Neo4j	community-5.22.0
Python	3.8.12
SGPlan	5.2.2

智能变电站远程监控网络属于典型的 IT 与 OT 融合场景,图 9 清晰地展示了 IT 与 OT 的具体分工及其协同作用。其中,远程主机 1、远程主机 2 和远程主机 3 分别作为工程师、维护人员和系统管理员的操作终端,通过 IT 技术实现了对智能变电站内部设备的接入,为远程管理与维护提供了技术支持。而在智能变电站网络内部,工程师站、HMI、间隔层及过程层设备则构成了 OT 的核心部分,这些设备专注于电力系统的实时运行控制,负责数据采集、状态监测以及设备间的高效交互,确保了电力系统的高实时性和可靠性。

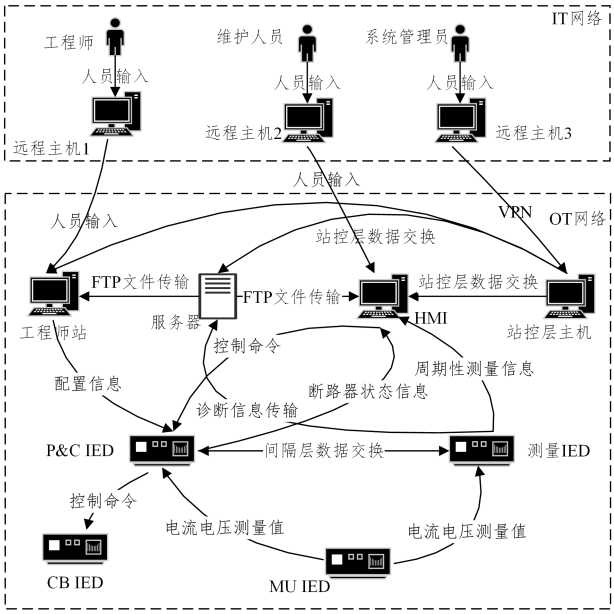

图 9 实验场景

Fig. 9 Experimental scenario

本章首先使用 SG_TMT 对该系统进行威胁识别,识别出可能存在的安全隐患。随后,基于识别结果对该场景进行形式化威胁建模,并开展攻击路径发现实验。最后,对规划结果进行分析和验证,以评估本文方法的易用性及规划结果的有效性。

4.1 自动化威胁识别实验

本节利用 SG_TMT 对该系统进行威胁识别,对应 PDDL 描述自动生成算法中的系统资产梳理和脆弱性分析阶段,结果用于攻击路径发现实验环节中的威胁模型构建。生成的威胁分析结果如表 6 所列,共包括欺骗、篡改、拒绝服务、信息泄露、未授权访问以及内部人员共 127 个安全威胁,分析报告中包括了攻击者可用的 ATT&CK 技术。根据 SG_TMT 的分析与已有的研究,变电站监控网络的远程主机以及站控层设备存在较多高危漏洞,间隔层与过程层的 IED 漏洞较少,但仍可能存在缺少权限管理或未知漏洞,智能变电站中的 IED 供应链可能存在不可信的参与者且大多数 IED 存在 Telnet 与 SSH 的通信信道[20],其本身可能存在硬件木马[21]使得远程攻击成为可能,攻击者侵入变电站网络与对应 IED 建立连接后便可执行恶意操作。IEC 61850 协议属于公开协议,且明码通信,同时 Goose 协议与 SV 协议具备较严格的时间要求,这阻碍了安全机制的实施。除此之外,工作人员的安全意识薄弱,培训不足,以及缺乏对安全政策的严格执行,都会增加网络的安全风险,即使技术防护措施到位,也可能因人为疏忽或操作失误而使系统被攻破。

表 6 MS-TMT 自动化威胁识别结果

Table 6 Automated threat identification results of MS-TMT

威胁类别	威胁数量	MITRE ATT&CK 技术
欺骗	15	T0865,T0863,T0856,T0848,T0855
篡改	30	T0836,T0838,T0823,T0806,T0874,T0873,T0858,T0843,T0839,T0835,T0821,T0889,T0871,T0834
拒绝服务	32	T0803,T0804,T805,T0816,T0881,T0835,T0857,T0809,T0814,T0878,T0838
信息泄露	32	T0802,T0811,T0852,T0801,T0861,T0845,T0877
未授权访问	15	T0817,T0865,T0819,T0833,T0866,T0847,T0864,T0891,T0812,T0859,T0863,T0869,T0885
内部人员	3	—

4.2 攻击路径发现实验

完成实验场景的威胁识别之后,攻击路径发现实验依照 PDDL 描述自动生成算法分 3 步进行,即威胁模型构建、PDDL 描述文件生成及攻击路径发现。

首先,利用自动化威胁实验结果构建威胁模型 G。设备与 ATT&CK 技术之间的映射关系,即 $g(f(device))$ 如表 7 所列。完成威胁模型构建后,利用 Neo4j 图数据库,以图数据结构存储威胁模型。

表 7 设备与攻击技术映射

Table 7 Device and attack technique mapping

设备与网络	MITRE ATT&CK 技术
攻击者(Attacker)	T0817,T0847,T0864,T1087
远程主机 1(Host1)	T0865,T0863,T0802
远程主机 2(Host2)	T0865,T0848,T0834,T0809,T0811,T1548.002
远程主机 3(Host3)	T0865, T1059, T1133, T1018, T1056, T1566, T0866,T0891
远程网络(Onet)	T1071,T1040,T0856
工程师站(Edevice)	T1059, T1136, T1570, T1112, T1055, T1070, T1562,T0874,T0843
服务器(Service)	T1059,T0881,T0885
人机接口(HMI)	T0823, T1059, T1136, T1570, T1112, T0871, T0816,T0852,T0859
站控层 PC(SPC)	T1059,T1133,T0822,T0884,T0812
站控层网络(Snet)	T1071, T0885, T1040, T0830, T0855, T0856, T0803,T0804
保护 IED(PCIED)	T0803, T0836, T0838, T0839, T0873, T0858, T0821,T0889,T0869
测量 IED(MIED)	T0804, T0838, T0856, T0878, T0845, T0877, T0869
断路器 IED(CBIED)	T0813,T0806,T0805
合并单元(MUIED)	T0813
间隔层网络(Bnet)	T0830,T0855,T0856,T0803,T0857

接着，以图数据库作为输入，自动生成 PDDL 描述文件。为了贴近实际生产场景，假设攻击者成功接入变电站远程监控网络的 IT 网络，选取图 10 的 3 条覆盖所有设备的数据流作为具体实验对象。场景一表示工程师在远程主机 1 通过远程主机 3 的 VPN 服务接入变电站网络站控层的工程师站，接着对 P&C IED 进行软件升级以及配置更新等操作。场景二表示维护人员远程接入站控层的 HMI，进而向 P&C IED 发送控制命令。场景三表示测量 IED 收集电流电压数据，并将诊断报告传输至服务器。

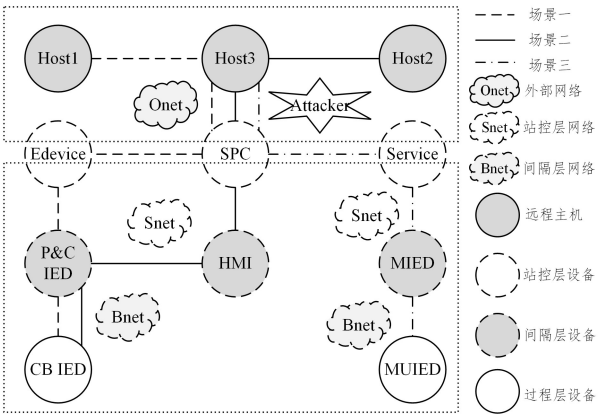

图 10 数据流选取

Fig. 10 Dataflow selection

在攻击路径规划阶段，将生成的所有 PDDL 描述文件输入路径规划工具 SGPlan 后，针对每条数据流生成所有可能的攻击路径。

4.3 实验结果与分析

攻击路径规划结果如图 11 所示。攻击者在妥协某个设备后，可以在该设备执行相关攻击技术达成攻击目标或进行进一步渗透。末端攻击路径指在攻击者妥协主机后，执行属于 Command and control 或 Actions on objectives 阶段的攻击技术序列。途径攻击路径指攻击者为妥协设备执行的攻击技术序列。规划结果表明，攻击者可采取的攻击技术组合众多，攻击路径组合数随着攻击深度呈倍数增长。

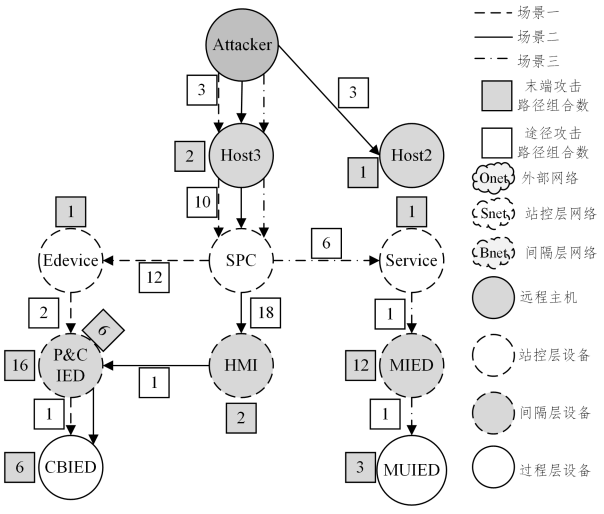

图 11 实验结果总图

Fig. 11 Overall diagram of experimental results

根据图 11 所示结果，可将途径攻击路径组合数看作边的权重，末端攻击组合数看作节点的权重。假设当前节点为 v，w 表示权重，当前节点带权出度为 $Out(v)=\sum_{(v,u)\in E} w(v,u)$，当前节点的带权入度为 $In(v)=\sum_{(v,u)\in E} w(u,v)$。带权出度越高，表明攻击者以此设备为跳板可执行更多的攻击操作；带权入度越高，表明该设备在攻击路径中越关键，节点权重越高，表明通过该设备实现最终攻击目标的方式越多。定义设备的威胁系数如下：

$$\theta(v)=\alpha\cdot Out(v)+\beta\cdot In(v)+\gamma\cdot w(v) \tag{1}$$

其中，α，β 和 γ 为权重系数，分别设置为 0.4，0.2 和 0.4，代表不同因素对威胁系数的影响程度，威胁系数越高，说明该设备面临的安全风险越高。

表 8 列出了各设备的威胁系数。

表 8 设备威胁系数

Table 8 Device threat factor

设备	出度	入度	节点权重	威胁系数
Attacker	6	0	0	2.4
Host2	0	3	1	1
Host3	10	3	2	5.4
SPC	36	10	0	16.4
Edevice	2	12	1	3.6
HMI	1	18	2	4.8
Service	1	6	1	2
P&C IED	1	3	22	9.8
MIED	1	1	12	5.4
CB IED	0	1	6	2.6
MUIED	0	1	3	1.4

实验结果表明，SPC 作为连接变电站网络与监控网络的枢纽，面临着最显著的安全风险。其次，P&C IED 由于与物理过程控制紧密关联，承担着关键的安全职责，因此也容易成为攻击的目标。HMI 的入度最高，表明其位于设备的关键交互路径上，是攻击者潜在的攻击入口。因此，HMI 应被重点关注并加强安全防护措施。

图 12 展示了场景一的攻击路径规划的详细结果。攻击者主要通过工程师站修改 P&C IED 的配置，如过载保护阈值，进而在电流电压正常情况下，使 P&C IED 向断路器发出断闸操作。

图 13 展示了场景二的攻击路径规划的详细结果。在这一场景中，攻击者首先通过对人机界面（HMI）的控制，直接向 P&C IED 发送恶意命令，这可能导致设备执行不当的操作，影响整个电力系统的安全性和稳定性。此外，攻击者还可能通过入侵站控层网络，篡改合法的控制命令，伪造系统指令或操控数据流，进而影响 P&C IED 的正常运行。

图 14 展示了场景三的攻击路径规划的详细结果。攻击者主要通过抑制测量 IED 的告警服务，阻碍站控层设备在故障发生时做出及时响应。此外，攻击者还可以通过入侵过程层网络，篡改原始的测量值，伪造数据流，间接影响后续控制命令的执行。

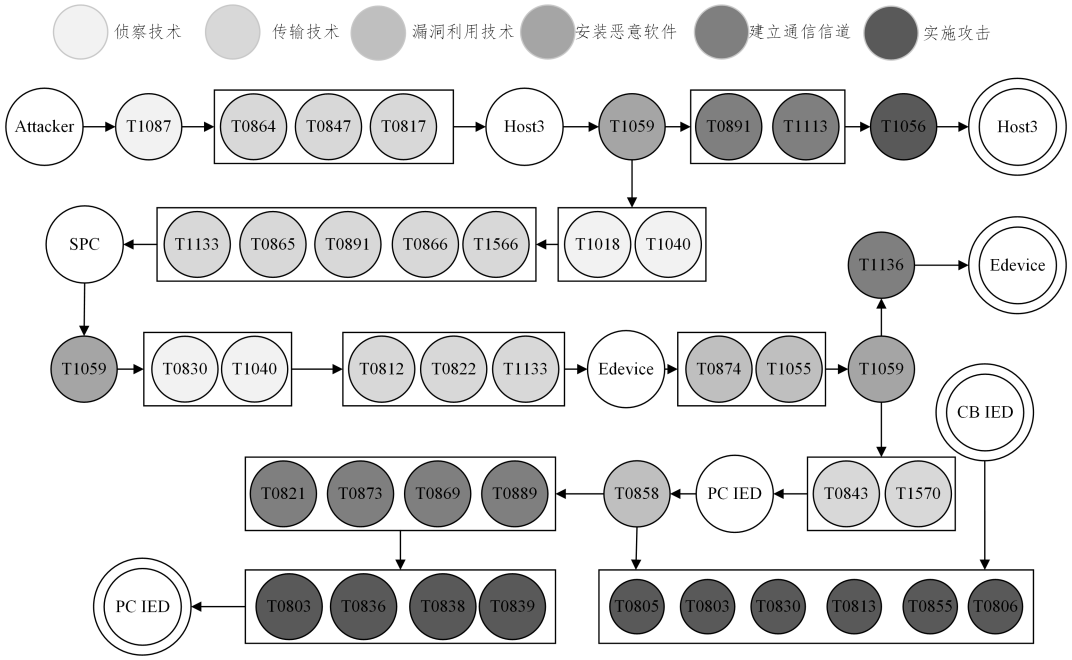

图 12 场景一攻击路径规划结果

Fig. 12 Attack path planning results for scenario 1

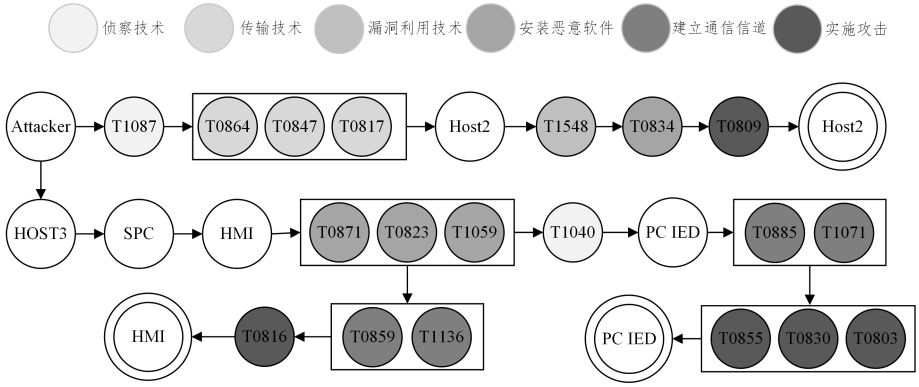

图 13 场景二攻击路径规划结果

Fig. 13 Attack path planning results for scenario 2

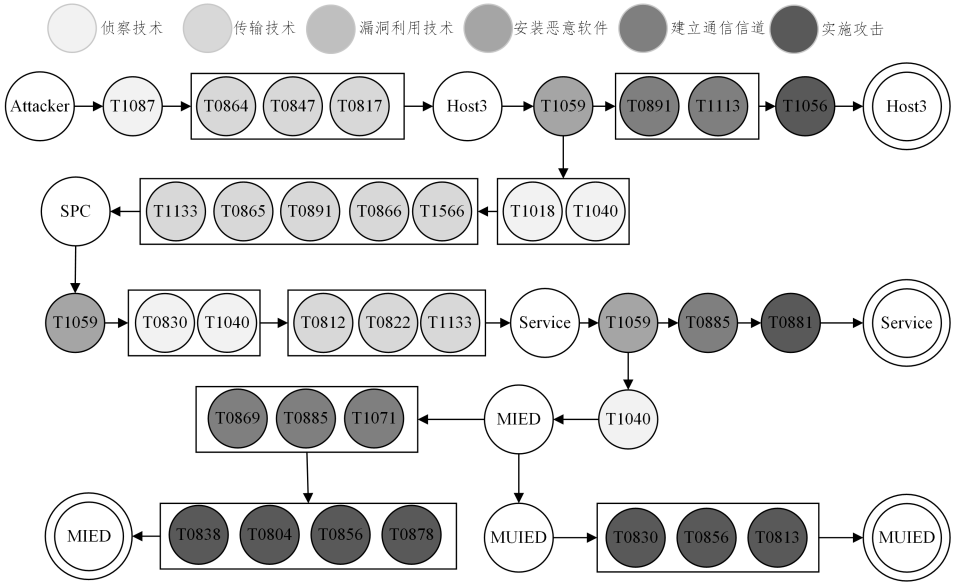

图 14 场景三攻击路径规划结果

Fig. 14 Attack path planning results for scenario 3

综合以上分析，针对图 9 所示实验场景，以破坏断路器正常开断进而引起电力故障为攻击目标，可构建如图 15 所示的攻击树。

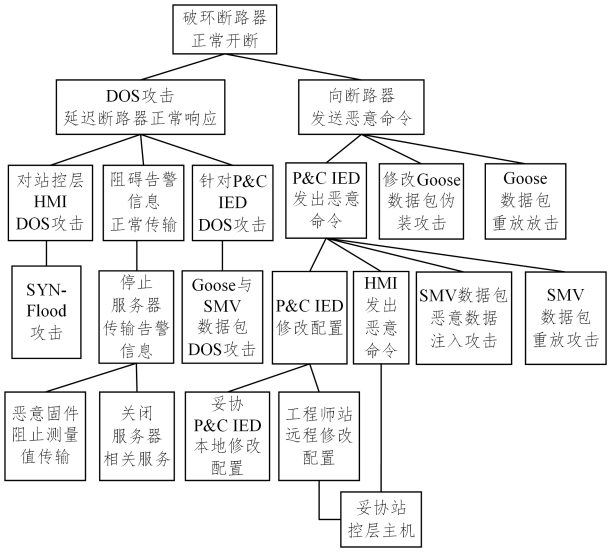

图 15　针对断路器的攻击树

Fig. 15　Attack tree for circuit breaker

本实验针对 3 个具体场景规划出了符合实际情况的多阶段攻击路径，并基于整个系统攻击路径的整体视图计算每个设备的威胁系数，从而明确了安全防护的重点区域。本文采用了 MITRE ATT&CK 框架对企业和工控网络的攻击行为进行统一建模，这种方法具备跨层分析能力，能够有效识别如智能变电站远程监控网络等 IT 与 OT 融合场景中的潜在攻击路径。实验结果表明，本文方法不仅能够覆盖传统 HMI、间隔层及过程层设备等 OT 层核心设备，还能扩展至远程主机等 IT 层相关组件。这种全面性为实际系统的安全防护提供了有力支持，并为未来更复杂的跨层攻击分析奠定了基础。

目前，针对变电站监控网络进行攻击路径发现的研究较为稀缺，现有方法集中于网络物理系统的攻击路径发现，研究侧重点不尽相同。智能变电站作为关键基础设施，对其开展系统全面的攻击路径发现，对于提前识别安全威胁、预防安全事件具有重要意义。本文方法致力于以低成本发现尽可能全面的攻击路径。攻击路径数量受网络拓扑结构和组件脆弱性影响，在不同网络环境中可能有显著差异。因此，本文选取各相关文献实验场景中两个设备间的平均攻击步骤数与路径数进行对比分析。依据 Cyber Kill Chain 中除 Weaponization 的 6 个攻击阶段，确定了设备间的平均攻击步骤数，并通过计算图 9 中途径攻击路径组合数的平均值，得出了设备间的平均攻击路径数，如图 16 所示。结果表明，本文方法在攻击路径发现的全面性方面具有明显优势。

为进一步评估本文方法的优势，从使用成本、规划粒度和规划广度 3 个维度将其与相关文献进行对比，对比结果如表 9 所列。

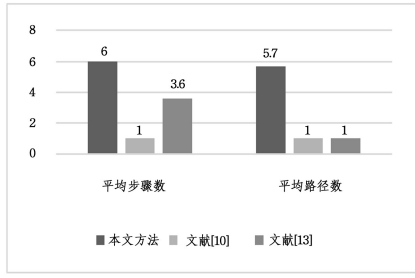

图 16　设备间的平均攻击步骤数与路径数

Fig. 16　Average number of attack steps and paths between devices

表 9　相关工作的比较

Table 9　Comparison of related work

方法	使用前准备	成本	粒度	广度
本文方法	宏观脆弱性分析	低	细粒度	多路径
文献[10]方法	详细脆弱性分析	中	粗粒度	多路径
文献[13]方法	构建知识图谱	高	细粒度	单路径

从表 9 可以看出，本文方法在控制使用成本的前提下实现了细粒度的攻击路径规划和多路径覆盖，兼具全面性和实用性。通过“设备-脆弱性-ATT&CK 攻击技术”的 3 层解耦架构与 Neo4j 图数据库的拓扑存储特性，系统可灵活应对新型攻击。具体而言，当新的攻击技术出现时，只需在数据库中新增相应的攻击技术节点，并将其与已知或新发现的脆弱性关联，同时建立其与目标设备的联系，而无需修改核心算法。这种模块化的设计机制不仅保证了系统的可扩展性，也显著降低了系统的迭代维护成本。

在实际应用中，本文方法可直接部署在规模较小的变电站远程监控网络拓扑中。随着网络规模的扩大，可能出现路径爆炸等问题。针对此问题，可选择更高效的规划器或对大规模网络进行分区分析并整合结果来解决。此外，实际部署中可能存在脆弱性分析不足等问题，可结合公开漏洞数据库、安全分析报告及历史攻击数据，构建针对各类设备的脆弱性自查手册。使用者仅需对照手册，检查如弱密码等常见脆弱性即可。

结束语　本文针对变电站远程监控网络，提出了一种基于 ATT&CK 框架与 PDDL 的攻击路径自动规划方法。该方法能够根据具体网络拓扑生成包含 Cyber Kill Chain 攻击阶段的具备可操作性的攻击路径。在实验中，通过 Microsoft Threat Modeling Tool 模拟对实际场景的脆弱性分析，基于 Neo4j 构建图数据库，利用本文方法自动生成 PDDL 描述文件，并使用路径规划器 SGPlan 输出可能的攻击路径，证明了与现有的针对网络物理系统攻击路径规划方法相比，本文方法在降低对专业人员技能要求的同时，提供了更细粒度和全面的攻击规划结果。下一步拟结合 CVE 和 CNVD 等已知漏洞数据库以及安全事件分析报告，以提高对系统的脆弱性分析效果。

参 考 文 献

[1] ALOMARI M A, AL-ANDOLI M N, GHALEB M, et al. Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions [J]. Energies, 2025,

18(1):141.
[2] CHAIJ W, LIU S M. Cyber security vulnerability assessment for Smart substations[C]// 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC). IEEE, 2016: 1368-1373.
[3] KOLOSOK I, KORKINA E. Problems of Cyber Security of Digital Substations[C]// International Workshop Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing And Cyber Security (IWCI 2019). Atlantis Press, 2019: 75-78.
[4] KHODABAKHSH A, YAYILGAN S Y, HOUMB S H, et al. Cyber-security gaps in a digital substation: From sensors to SCADA[C]// 2020 9th Mediterranean Conference on Embedded Computing (MECO). IEEE, 2020: 1-4.
[5] GASPAR J, CRUZ T, LAM C T, et al. Smart substation communications and cybersecurity: A comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2456-2493.
[6] JBAIR M, AHMAD B, MAPLE C, et al. Threat modelling for industrial cyber physical systems in the era of smart manufacturing[J]. Computers in Industry, 2022, 137: 103611.
[7] KALOROUMAKIS P E, SMITH M J. Toward a knowledge graph of cybersecurity countermeasures[J]. The MITRE Corporation, 2021, 11: 2021.
[8] CHEN Z, KANG F, XIONG X, et al. A Survey on Penetration Path Planning in Automated Penetration Testing[J]. Applied Sciences, 2024, 14(18): 8355.
[9] BODDY M S, GOHDE J, HAIGH T, et al. Course of Action Generation for Cyber Security Using Classical Planning[C]// ICAPS. 2005: 12-21.
[10] WANG Z, ZHANG Y, LIU Z, et al. An Automatic Planning-Based Attack Path Discovery Approach from IT to OT Networks[J]. Security and Communication Networks, 2021, 2021(1): 1444182.
[11] FOX M, LONG D. PDDL2.1: An extension to PDDL for expressing temporal planning domains[J]. Journal of Artificial Intelligence Research, 2003, 20: 61-124.
[12] WANG Y, LI Y, XIONG X, et al. DQfD-AIPT: An Intelligent Penetration Testing Framework Incorporating Expert Demonstration Data[J]. Security and Communication Networks, 2023, 2023(1): 5834434.
[13] LIU C, WANG B, LI F, et al. Optimal Attack Path Planning based on Reinforcement Learning and Cyber Threat Knowledge Graph Combining the ATT&CK for Air Traffic Management System[J/OL]. IEEE Transactions on Transportation Electrification, 2024. https://doi.org/10.1109/TTE.2024.3377687.
[14] HAPPE A, CITO J. Getting pwn'd by ai: Penetration testing with large language models[C]// Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering. 2023: 2082-2086.
[15] DENG G, LIU Y, MAYORAL-VILCHES V, et al. {PentestGPT}: Evaluating and harnessing large language models for automated penetration testing[C]// 33rd USENIX Security Symposium (USENIX Security 24). 2024: 847-864.
[16] ASSANTE M J, LEE R M. The industrial control system cyber kill chain[J]. SANS Institute InfoSec Reading Room, 2015, 1(1): 2.
[17] ZHANG Z, HUANG X, KEUNE B, et al. Modeling and simulation of data flow for VLAN-based communication in substations[J]. IEEE Systems Journal, 2015, 11(4): 2467-2478.
[18] ABDEEN B, AL-SHAER E, SINGHAL A, et al. Smet: Semantic mapping of cve to att&ck and its application to cybersecurity[C]// IFIP Annual Conference on Data and Applications Security and Privacy. Cham: Springer, 2023: 243-260.
[19] FLÅ L H, BORGAONKAR R, TØNDEL I A, et al. Tool-assisted threat modeling for smart grid cyber security[C]// 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, 2021: 1-8.
[20] UMAN O, GHAFOURI M, KASSOUF M, et al. Modeling supply chain attacks in IEC 61850 substations[C]// 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2019: 1-6.
[21] CHATTOPADHYAY A, UKIL A, JAP D, et al. Toward threat of implementation attacks on substation security: Case study on fault detection and isolation[J]. IEEE Transactions on Industrial Informatics, 2017, 14(6): 2442-2451.

SHI Junnan, born in 2000, postgraduate. His main research interest is industrial control system cybersecurity.

CHEN Zemao, born in 1975, Ph.D, professor. His main research interests include information system security, trusted computing and equipment information security.

(责任编辑:柯颖)