经验交流

基于改进 ADT 的综合能源系统信息安全风险分析

李朝阳[1]，彭道刚[1]，吕政权[2]，张　涵[1]，王丹豪[1]

（1. 上海电力大学　自动化工程学院，上海　200090；
2. 国网上海市电力公司培训中心，上海　200438）

摘　要：在电力系统向综合能源转型与网络攻击技术演进的双重影响下，电力信息安全和防护形势日益严峻。归纳面向电网的攻防分布体系，提出了一种基于决策实验室分析法和攻击防御树模型的综合能源系统信息安全风险分析方法。该方法根据决策实验室分析法确定更适用于综合能源的叶节点安全多属性权重，结合现有攻防对抗策略与 CVSS(通用漏洞评分体系)，计算攻防树模型中攻击序列风险程度与灵敏度指标。通过城市光–储–充–换一体化智能电站进行信息安全威胁实例分析，结果表明，该方法威胁因素赋权科学，能自由添加删除攻击行为，凸显一定的可拓展性，安全属性等级评价客观。

关键词：综合能源系统；攻击防御树；决策实验室分析法；信息安全

文章编号：1007–1881(2020)12–0122–07　　**DOI:** 10.19585/j.zjdl.202012018

中图分类号：TP393.08　　**文献标志码：**B　　**开放科学(资源服务)标识码(OSID)：**

Information Security Risk Analysis of Integrated Energy System Based on Improved ADT

LI Zhaoyang[1], *PENG Daogang*[1], *LYU Zhenquan*[2], *ZHANG Han*[1], *WANG Danhao*[1]

(1. School of Automation Engineering, Shanghai University of Electric Power, Shanghai 200090, China;
2. State Grid Shanghai Electric Power Training Center, Shanghai 200438, China)

Abstract: Under the dual influences of the transformation of power system to integrated energy and the evolution of cyberattack technology, electric power information security and protection is faced with a severe situation. The paper summarizes the distribution system of attack and defense for power grid and proposes an information security risk analysis method for an integrated energy system based on decision-making trial and evaluation laboratory (DEMATEL) and attack defense tree (ADT) model. According to the DEMATEL, the security multi-attribute weight of leaf node more suitable for integrated energy is determined, and the vulnerability of attack sequence and the sensitivity index of leaf node in the ADT model are calculated by combined existing attack defense strategy and CVSS (common vulnerability scoring system). This paper analyzes the information security threat of the intelligent integrated solar-storage-charging-swamping station, and the result shows that the method, featuring scientific weight determination, can freely add or delete attacks, show expansibility and objectively evaluate security attribute level.

Keywords: integrated energy system; ADT; DEMATEL; information security

0　引言

在化石燃料低效匮乏、环境污染持续严重的背景下，我国能源创新高度活跃，光伏、风机等新能源供能成本下降，各类储能技术不断改进，“云大物移智链”逐渐渗透，多种能源之间亟需整合设计规划、协调运行，以方便可再生能源的安全消纳[1–2]。因此，国家电网有限公司高度重视综合能源产业建设发展，努力实现可再生能源广域

基金项目：上海市“科技创新行动计划”高新技术领域项目(185111105700)；国网上海市电力公司科技项目(52097019001N)

互联、智能数字化采集和源网荷储友好互动[3]。但伴随着两化融合以及信息物理系统的高度集成，新兴业务被引入大量现场电力终端设备，网络信息安全将对能源供给带来更多的不稳定因素，这是综合能源系统发展必须解决的问题之一。而且网络空间形式日益复杂，网络攻击的针对性、持续性和隐蔽性显著增强，各种威胁源相互交织，呈现出多元复杂的局势。《2020 全球风险报告》指出，网络攻击发生的可能性和影响力分别排第七、第八位，仅次于若干非人为威胁。另外，据 2019 年报道统计(英国、印度核电站内网访问权限遭窃取以及委内瑞拉、南非大规模停电)表明，网络攻击国家化潜在趋势明显，电力企业面临前所未有的威胁。因此，有必要全面加强面向综合能源系统的网络安全风险管控，开展高危风险点的验证与分析工作，针对性部署安全防护措施。

目前，对综合能源信息安全的研究主要集中于分布式能源、能源互联网和信息物理系统等领域。文献[4]基于身份安全机制、通信协议和智能能源管理系统构建了能源互联网信息安全框架。文献[5]针对能源区块链的私钥、隐私和协议等问题提出应对策略并构建防护体系。通过定位综合能源系统潜在危险点及风险因素分析，可以合理准确地判断攻击事件的影响及威胁被利用的难易程度[6]。目前，主流的安全风险分析形式有定性和定量 2 种。文献[7-8]应用层次分析法，结合粒子群算法/证据理论，分别讨论了工控系统中功能与信息安全两大问题。面对具体攻击行为特征提取困难、攻击渠道复杂、攻击空间模糊等问题，场景模型化分析提供了一种定量解决思路[9]，Petri 网[10]和攻击图[11]作为其常用建模方法已被电力行业广泛应用。文献[12]通过计算攻防博弈模型均衡解来识别某光热冷综合能源的系统危险点并预测其攻击行为。文献[13]在攻击树的基础上引入防御措施概念，计算数据采集与监控系统的威胁性指标。本文首先对当前综合能源系统信息安全防护建设情况进行梳理；其次提出一种基于 DEMATEL(决策实验室分析)法优化权重结合 ADT(攻防树模型)，即 DEMATEL-ADT 的综合能源系统信息安全风险分析方法；最后通过对某光-储-充-换一体化电站进行威胁分析，验证了所提方法的实用性并提出了相关安全建设意见。

1 综合能源系统结构安全

随着产业互联网的转型升级，信息安全问题与日俱增，在智慧综合能源时代下，任何无意识的安全漏洞，都有可能导致新能源电站故障或瘫痪。由此，电力企业开展安全等级划分，将信息系统划分为管理信息和生产控制大区，筑牢互联网边界、信息内外网边界和管理信息大区边界“三道防线”[14]，融入安全防护技术于系统采集、传输和控制等业务环节模块，并参考《国家电网公司管理信息系统安全防护技术要求》，满足物理、边界、网络、应用、数据、主机和终端 7 个层面的要求[15]，以此形成电力企业网络安全防护体系。其中生产控制大区普遍采取专网专用，辅以防病毒软件、工控安全设备、物理防护和电磁屏蔽底层防护措施；管理信息大区通过主动防御体系辅以无线安全管理、网络监控、信息加密和代码检测等防护措施进行全面布防。但在电力系统向综合能源转型过程中，光伏风机地热天然气等多种能源形式以及电热冷等多元化用能需求在产生、传输分配、转换存储、消费交易等过程可能存在安全威胁的环境下，网络攻击技术也逐步发生演进。传统网络扫描、信息收集、拒绝服务、入侵控制和实体检测五大类攻击又衍生出可持续威胁攻击、暗链攻击、移动终端病毒攻击等高级攻击形式[16]，有必要应用场景风险分析方法，实现安全拓展需求，做到采集、通信、数据、运维的多角度、全方位和立体化保护。面向电网综合能源系统的网络攻防分布如图 1 所示。

2 风险分析方法实现原理

2.1 攻击防御树模型

ADT 作为一种攻击场景模型化分析方法，由 Schneier 于 1999 年提出[17]，一般用来描述威胁攻击与防护措施二者之间的交互影响。作为综合能源服务业务的重要分支，同样面临互联网化所映射出的信息安全问题，电动汽车与综合能源系统的安全相关研究高度重合。攻击者根据其与电网双向电力交换的特性，往往利用无线通信从充电设施切入，进行中间人攻击、支付欺诈、隐私窃取、损坏电池和拒绝服务攻击，甚至在电网中传播恶意软件，造成严重后果[18]。以华东地区某城

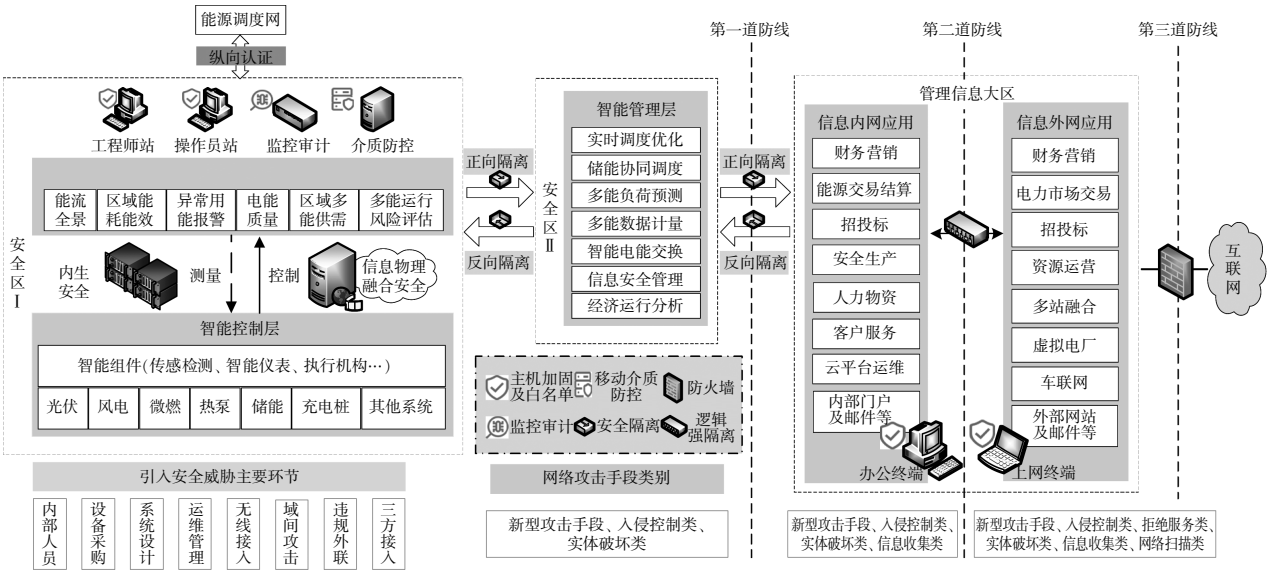

图 1　综合能源系统的网络攻防分布

市光–储–充–换一体化充换电工程为例，构建适应一般情况的安全威胁路径和防护策略攻防树模型，如图 2 所示，表 1 则给出各节点的含义。图 2 中，根节点 G 为内网渗透，即监视与控制能量生产管控、调度配网和交易中心等信息资产。

设三元组 ADT=$\{N, E, R\}$，其中 $N=(N_a, N_d)$ 为树的节点集合，包括攻击节点集合和防御节点集合。图 2 中节点 M，X 表示攻击；D 表示防御；$e=\{N_i, N_j\} \in E$ 表示节点 N_i 与节点 N_j 的边，节点之间的边有父子(即节点 X 与 M，M 与 G)和防护对

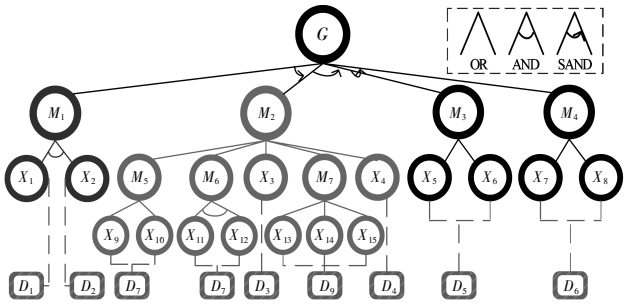

图 2　攻防树节点表示方法

表 1　攻防树节点符号含义

节点	含义	描述	子节点	含义	防御节点	内容
M_1	信息收集	涉及充电设施、运维主机、BMS、移动终端软件等多方面	X_1	扫描	D_1	防火墙、网络回溯、CDN 技术服务
			X_2	网络监听	D_2	VPN，SSL 加密网关、加密机
M_2	网络入侵	获取敏感信息/特权，中断服务	X_3	协议重放	D_3	时间戳、序列号、随机数
			X_4	高级攻击	D_4	沙箱、EDR，SIEM，SOC，MSS
M_3	权限提升	进一步查找破坏有价值的信息系统	X_5	水平	D_5	漏洞扫描、安全策略配置
			X_6	垂直		
M_4	后门安装	便于再次植入攻击代码	X_7	系统	D_6	网络回溯、EDR、防病毒软件
			X_8	网页		
M_5	口令攻击	破解用户/应用密码	X_9	密码破解	D_7	漏洞扫描、身份认证与单点登录、CA 数字证书、安全管理培训
			X_{10}	社会工程学		
M_6	拒绝服务攻击	通过发送大量非法无用请求，占用服务器全部资源	X_{11}	计算机消耗	D_8	抗 DDoS 设备、云端抗 DDoS 服务
			X_{12}	带宽消耗		
M_7	漏洞利用攻击	利用技术缺陷实施攻击	X_{13}	服务漏洞	D_9	IPS，IDS、渗透测试、WAF、源代码与数据库审计、Web 应用防火墙等
			X_{14}	操作系统		
			X_{15}	应用程序		

抗(即节点 D 与 X)2 种关系，以边的虚实区分，各攻击叶节点延伸出一个或一组防护措施；R={AND，OR，SAND}表示节点之间有“与、或、顺序”3 种逻辑关系，即判断子节点是否独立完成父节点的入侵过程。

攻击示意图中 X 代表具体的攻击方式，按照传统网络攻击步骤，从图 1 描述的六大类中衍生；相应的 D 被安全技术员普遍采用，一定程度上可以缓解特定类型安全风险压力。每一条从根节点出发到叶节点的分支都代表一个完整攻陷最终目标的攻击序列，中间节点 M 表示系统已经在一定程度上遭受入侵，多个序列汇集的根节点 G 表示各种攻击行为的最终安全事件。

2.2　DEMATEL 方法

DEMATEL 法作为一种运用图论与矩阵的系统分析方法，由 Gabus 于 1971 年提出，用来衡量决策指标相对重要程度与作用反馈。本文参考美国工业控制系统安全指南[19]，将综合能源系统中信息安全威胁指标分为攻击实施成本 c_i、难易程度 n_i、攻击隐蔽性 f_i 和收益影响 y_i 4 个因素，Z_c，Z_n，Z_f 和 Z_y 为 4 个因素对应的综合权重，其和为 1。在搭配 Delphi(专家调查)法的基础上，综合考虑因素间的逻辑关系，得到指标混合权重 Z。

为达到中断能源系统运行、窃取工作信息等的目的，攻击难易度往往被黑客优先考虑。因此，利用本节方法，确定更适应综合能源系统的威胁指标权重。组织 5 位网络安全工程师参与评估，采用五分度法判断二元关系，模糊数 0~4 表示相互关系的无、弱、一般、较强、很强。得到直接影响矩阵 $\boldsymbol{A}$。

为保证运算收敛归一化原始关系矩阵，得到规范直接影响矩阵记为 $\boldsymbol{A}_s$，其中 $\boldsymbol{I}$ 为单位矩阵；元素 a_{ij} 表示因素 i 对比因素 j 的重要等级：

$$\boldsymbol{A}_s=\frac{a_{ij}}{\max\left(\sum_{j=1}a_{ij}\right)} \quad . \qquad (1)$$

接着计算综合影响矩阵 $\boldsymbol{A}_o$：

$$\boldsymbol{A}_o=\boldsymbol{A}_s(\boldsymbol{I}-\boldsymbol{A}_s)^{-1} \quad . \qquad (2)$$

混合权重 $\boldsymbol{Z}$ 反映初始权重 w 大小的同时，也照顾到了各因素的影响程度，这样权重赋值显得科学合理。

$$\boldsymbol{Z}=w+\boldsymbol{A}_o\cdot w=(I+\boldsymbol{A}_o)\cdot w \quad . \qquad (3)$$

2.3　攻击序列风险计算

由 ADT 可以看出整体过程呈现顺序关系，如攻击者通过前期收集工作确定潜在入侵对象，诱导对象下载病毒 APP，进而攻陷不安全的通信协议，致使用户恶意缴费。这一流程来看，该案例中各步骤既从自身获益，也为后续铺垫了道路。由此引入局部信息抗攻击能力评价指标 F，描述 SAND 节点条件概率，反映攻击者后续继续入侵意愿。

$$F=\frac{J'}{J} \quad , \qquad (4)$$

式中：J'，J 表示综合能源系统网络攻击当前所属阶段与所有阶段统计数值。

根据 2.1 和 2.2 小节内容结合多属性效用理论，将以下属性转换为效用值并给出叶节点风险分析公式：

$$T(X_i)=Z_c\cdot U(c_i)+Z_n\cdot U(n_i)+Z_f\cdot U(f_i)+Z_y\cdot U(y_i) \quad , \qquad (5)$$

$$T'(X_i)=T(X_i)\cdot\left(1-\frac{d}{d_{max}}\right) \quad , \qquad (6)$$

式中：i 为任意攻击方式即叶节点；$T(X_i)$和 $T'(X_i)$为引入防护措施前、后叶节点的风险威胁指标；U 为系统风险因素效用值，$U(x)=1/x$；d，d_{max} 分别为该节点防护实施效果与系统最佳防护效果加 1。

综合能源系统面临的各类信息安全威胁小到边缘资产泄密，大到电网主站监控中心数据的篡改，需要根据属性的不同对各因素量化。本文参照 CVSS(通用漏洞评分体系)3.0 版本给出攻击难度与收益影响标准(见表 2)量化公式，全因素风险分析等级标准见表 3。充电站的可用性由充电服务的激活时间与停止时间决定。

$$n_i=8.22\mathrm{AV}\cdot C\cdot R\cdot U \quad , \qquad (7)$$

$$y_i=6.42[1-(1-O)\cdot(1-N)\cdot(1-K)] \quad . \qquad (8)$$

表 2　攻击难度与收益影响标准

标度	指标	取值范围	等级系数
攻击难度评价	攻击途径 AV	远程/相邻/本地/物理	0.85/0.62/0.5/0.2
	攻击复杂度 C	低/高	0.77/0.44
	权限要求 R	无/低/高	0.85/0.62/0.2
	用户交互 U	无/有需求	0.85/0.62
影响度评价	机密性影响 O	高/低/无	0.56/0.22/0
	完整性影响 N	高/低/无	0.56/0.22/0
	可用性影响 K	高/低/无	0.56/0.22/0

表 3 全因素风险分析等级标准

攻击成本/万元	难易程度系数	被发现可能	收益影响	防护效果	等级
≥10	0.1~0.8	极易	0.1~1.2	极高	5
5~10	0.8~1.6	易	1.3~2.4	高	4
3~5	1.6~2.4	一般	2.4~3.6	中	3
1~3	2.4~3.2	难	3.6~4.8	低	2
<1	3.2~3.9	极难	4.8~5.9	极低	1

按照逻辑规则自上而下计算攻击序列风险值，整棵攻防树的风险指标用其中每条攻击序列风险属性最大值来表示。

$$S(E)=\begin{bmatrix} S(e_1)=\prod_{i\in S_1}T(X_i) \\ S(e_2)=\prod_{i\in S_2}T(X_i) \\ S(e_3)=\prod_{i\in S_3}T(X_i) \end{bmatrix}, \quad (9)$$

$$S_r=\max\{S(e_1),\ S(e_2),\ \cdots,\ S(e_i)\}, \quad (10)$$

式中：j 为若干攻击序列之和；E 为攻防树模型中攻击序列集合；$S(e_i)$为一条序列中所有节点风险值的乘积；S_r 为整株树的攻防风险指标。

最后给出引入防御措施前、后攻击序列相比于模型整体风险的灵敏度 $L(X_i)$。根据数值结果找出威胁系统安全的关键叶子节点，检测目标系统安全状态与防御能力，后续对其暴露问题着手改善。

$$L(X_i)=\frac{[S(k_i)-S'(k_i)]/S(k_i)}{(S_r-S_r')/S_r}, \quad (11)$$

式中：$S'(k_i)$和 S_r'分别为采取防护措施后序列与系统的风险指标。

3 算例分析

本文对华东地区某城市光–储–充–换一体化电站进行安全风险分析，该电站利用夜间低谷电价进行储能，在充电高峰通过储能和电网一起为充电站供电。装配 120 kW，60 kW，30 kW 直流电桩各 3台，7 kW 交流电桩 51 台；换电站为单通道双工位换电站，装配有 156 个充电机；换电站电池有 156 块，每块 15 kWh；光伏车棚约 15 kW 薄膜组件。通过对电动汽车行业充电设备、运营平台、移动智能终端及信息交换接口攻防现状进行调研，充分考虑数据和控制命令的机密性、完整性以及充电站、充电站管理接口、能源管理系统 EMS 和电网的可用性，其具体风险威胁分析步骤为：

(1)根据目标信息系统的体系结构、主要资产和防护措施部署情况，构建系统攻防树模型。

(2)利用 DEMATEL 优化风险因素权重赋值。

(3)评估各叶节点风险因素等级。

(4)分析攻击序列、攻防树安全风险，计算风险灵敏度，重点提升薄弱环节防护水平。

应用 2.2 小节中的 DEMATEL 法优化文献[20]中德尔菲法 c_i，n_i，f_i 和 y_i 4 个因素权重，结果如下：

$$\boldsymbol{Z}=(I+A_o)\cdot w=\begin{bmatrix} 1.070\,1 & 0.137\,4 & 0.481\,1 & 0.078\,5 \\ 0.572\,8 & 1.122\,5 & 0.428\,7 & 0.641\,4 \\ 0.163\,6 & 0.320\,7 & 1.122\,5 & 0.183\,2 \\ 0.199\,7 & 0.111\,3 & 0.389\,4 & 1.063\,6 \end{bmatrix}\begin{bmatrix} 0.15 \\ 0.2 \\ 0.35 \\ 0.3 \end{bmatrix}=\begin{bmatrix} 0.182\,9 & 0.314\,4 & 0.258\,3 & 0.244\,4 \end{bmatrix}$$

即攻击实施成本、难易程度、被发现可能性和收益影响 4 因素权重分别为 0.182 9，0.314 4，0.258 3 和 0.144 4。根据表 4 对各个叶子节点进行风险测评得到属性值，并将其代入式(4)—式(8)，得到引入防护措施前、后各攻击事件的风险威胁值。另添加未经 DETEMATEL 优化的攻击

表 4 攻击事件的风险威胁值

项目	$T_0(X_1)$	$T_0(X_2)$	$T_0(X_3)$	$T_0(X_4)$	$T_0(X_5)$	$T_0(X_6)$	$T_0(X_7)$	$T_0(X_8)$	$T_0(X_9)$	$T_0(X_{10})$	$T_0(X_{11})$	$T_0(X_{12})$	$T_0(X_{13})$	$T_0(X_{14})$	$T_0(X_{15})$
未经 DEMATEL 优化	0.437 5	0.69 17	0.525 0	0.730 0	0.61 67	0.665 0	0.616 7	0.691 7	0.591 7	0.600 0	0.737 5	0.587 5	0.691 7	0.606 7	0.675 0
引入防护措施前	0.486 1	0.661 3	0.512 9	0.617 9	0.592 0	0.619 3	0.592 0	0.661 3	0.539 3	0.543 6	0.806 3	0.684 1	0.661 3	0.576 3	0.635 1
引入防护措施后	0.121 5	0.496 0	0.256 5	0.463 4	0.444 0	0.464 5	0.444 0	0.496 0	0.404 5	0.407 7	0.604 7	0.342 1	0.496 0	0.432 2	0.476 3

表 5　攻击序列风险值

项目	$S(k_1)$	$S(k_2)$	$S(k_3)$	$S(k_4)$	$S(k_5)$	$S(k_6)$	$S(k_7)$	$S(k_8)$	$S(k_9)$	$S(k_{10})$	$S(k_{11})$	$S(k_{12})$	$S(k_{13})$	$S(k_{14})$	$S(k_{15})$	$S(k_{16})$
引入前	0.321 5	0.043 7	0.044 3	0.041 2	0.053 2	0.049 7	0.013 5	0.013 7	0.012 8	0.016 5	0.015 4	0.006 7	0.006 8	0.006 3	0.008 2	0.007 6
引入后 /10^{-2}	2.01	0.136 6	0.069 3	0.128 9	0.166 2	0.232 9	0.021 1	0.010 7	0.019 6	0.025 7	0.036 1	0.005 2	0.002 7	0.004 9	0.006 4	0.008 9

树分析结果作为对比，结果见表 4。

由图 2 可知，整棵防御树共计 16 条攻击序列，分别为：k_1={M_1}，k_2={M_1，M_5}，k_3={M_1，M_6}，k_4={M_1，X_3}，k_5={M_1，M_7}，k_6={M_1，X_4}，k_7={M_1，M_5，M_3}，k_8={M_1，M_6，M_3}，k_9={M_1，X_3，M_3}，k_{10}={M_1，M_7，M_3}，k_{11}={M_1，X_4，M_3}，k_{12}={M_1，M_5，M_3，M_4}，k_{13}={M_1，M_6，M_3，M_4}，k_{14}={M_1，X3，M_3，M_4}，k_{15}={M_1，M_7，M_3，M_4}，k_{16}={M_1，X_4，M_3，M_4}。引入防护措施前、后各攻击序列的风险威胁值，结果见表 5。

根据式(10)得到整棵攻防树的风险指标 S_r，无设防情况下系统整体风险指标值为 0.321 5，引入图 2 中各项针对性防护手段后，系统整体风险指标值为 0.020 1。根据式(11)计算各序列风险灵敏度指标，如图 3 所示。M_1 与涉及到 M_6 的攻击序列风险灵敏度较高，表明网络入侵过程中，攻击者有较大可能利用 UDP 或 TCP/IP 洪水、低速、ping/ICMP 洪水等 DOS 攻击变体入侵充电设施或充电站生态中其他节点。根据文献[20–21]所提方法计算，对于节点 M_2，其子节点风险灵敏度由大到小依次为 X_4，M_7，M_5，X_3 和 M_6，与本文方法计算结果存在出入，究其原因，一方面未考虑防护措施实施效果的影响；另一方面威胁权重因环境对象差异而应有不同取值。

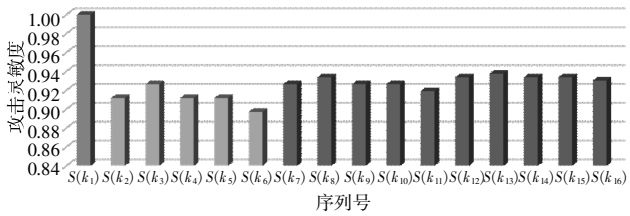

图 3　序列风险灵敏度

分析攻击防御树结果，随着攻击阶段的演进，攻击者或因达成预期计划或因成本、难度、被发现可能性增大而中止入侵，序列的风险程度逐渐降低。后续应多关注中风险漏洞修补，考虑上游开发链安全问题，对非技术部门人员进行培训，加大在容易忽视问题上的关注力度，提高基础信息安全攻击免疫力。此外在保证传统防护手段如防火墙、入侵检测和安全审计等落实到位的前提下，需融合可信计算、协议过滤、移动终端管理和安全态势感知等技术，及时监测存在的攻击威胁，立即做出相应的防护动作以减少损失。

4　结语

本文采用基于改进 ADT 的综合能源系统信息安全风险分析，旨在促进信息系统与能源网络的安全规划建设。首先根据现有网络攻防分布情况建立攻击防御树模型，在树中模拟攻击者可能利用的路径，以及入侵过程攻守对抗的相互影响。其次根据 DEMATEL 法结合 CVSS 确定风险分析因素，定义相关参数评估等级，实现了对系统风险值的定量与防护程度定性评估，计算得到不同攻击序列组合后整体系统风险值与灵敏度。从具有综合能源系统典型特征的电动汽车服务实例着手论证，结果表明，提出的 DEMATEL–ADT 综合能源系统信息安全风险分析方法威胁因素赋权科学，能自由添加删除攻防行为，凸显一定的可拓展性，安全属性等级评价客观。本方法便于电网企业安全技术人员针对性配置安全策略，确保多种能源在源–输–储–荷各环节稳定运行。在指标因素选取方面，应随着智慧综合能源系统建设的推进，及时改善完备评估指标体系，在不同时间攻防双方不断变化发展的基础上进行动态深入研究，全方位分析电网内部安全防御能力。

参考文献：

[1] 葛少云，曹雨晨，刘洪，等.考虑可靠性约束的综合能源微网供能能力评估[J].电力系统自动化，2020，44(7)：31–41.

[2] 贾宏杰，穆云飞，余晓丹.对我国综合能源系统发展的思考[J].电力建设，2015，36(1)：16–25.

[3] 曾鸣，杨雍琦，刘敦楠，等.能源互联网“源–网–荷–储”协调优化运营模式及关键技术[J].电网技术，2016，40(1)：114–124.

[4] SANI,ABUBAKAR SADIQ,YUAN,et al.Cyber security framework for internet of things-based energy internet[J]. Future generation computer systems,2019,93(21):849-859.
[5] 丁伟,王国成,许爱东,等.能源区块链的关键技术及信息安全问题研究[J].中国电机工程学报,2018,38(4):1026-1034.
[6] 费禹,蒋文保.一种基于层次分析法的攻防树模型[J].中国科技论文,2018,13(14):1644-1648.
[7] 段旭晨,彭道刚,姚峻,等.基于 SA-PSO-AHP 的火电厂控制系统信息安全威胁评估[J].中国电力,2019,52(5):29-35.
[8] 彭道刚,卫涛,赵慧荣,等.基于 D-AHP 和 TOPSIS 的火电厂控制系统信息安全风险评估[J].控制与决策,2019,34(11):2445-2451.
[9] 张小松,牛伟纳,杨国武,等.基于树型结构的 APT 攻击预测方法[J].电子科技大学学报,2016,45(4):582-588.
[10] 王永光.基于 Petri 网的网络安全防御体系评估模型的研究[D].长沙:湖南大学,2014.
[11] 陈德成,付蓉,宋少群,等.基于攻击图的电网信息物理融合系统风险定量评估[J].电测与仪表,2020,57(2):62-68.
[12] 张心洁,葛少云,刘洪,等.智能配电网综合评估体系与方法[J].电网技术,2014,38(1):40-46.
[13] 黄慧萍,肖世德,梁红琴.基于 AHP 和攻防树的 SCADA 系统安全脆弱性评估[J].控制工程,2018,25(6):1091-1097.
[14] 孙力.电力企业信息安全管理研究[D].南京:南京邮电大学,2014.
[15] 国家电网公司.国家电网公司管理信息系统安全防护技术要求:Q/GDW 1594—2014[S].北京:中国电力出版社,2015.
[16] SCHNEIER B.Attack trees:modeling security threats[J].Dr. Dobb's Journal,1999,24(12):21-29.
[17] GOTTUMUKKALA,MERCHANT,TAUZIN,et al.Cyber-physical system security of vehicle charging stations: 2019 IEEE Green Technologies Conference[C].Lafayette: IEEE,2019.
[18] NIST.Guide to industrial control system (ICS) security: SP 800-82[S].Gaithersburg: National Institute of Standards and Technology,2011.
[19] 孙卓,刘东,肖安洪,等.基于攻击树模型的数字化控制系统信息安全分析[J].上海交通大学学报,2019,53(增刊 1):68-73.
[20] 周飞,吴金城,郑东亚,等.考虑盲目攻击因子的电力 SCADA 系统安全脆弱性评估[J].浙江电力,2020,39(3):36-42.
[21] 郭仁超,徐玉韬.内外网数据安全交换技术在电网企业的应用研究[J].电力大数据 2018,20(2):61-66.
[22] 靳斌,汪德军.基于本质安全理论的供电企业安全管理探索[J].电力大数据,2018,20(3):61-64.
[23] 刘珊,杨华,岳克明.大数据在电力信息安全的研究[J].山西电力,2018(4):45-47.
[24] 杨嘉湜,杨帆.面向四川电力业务运行的信息安全保障体系构建研究[J].四川电力技术,2018,41(3):88-91.

收稿日期：2020-09-17

作者简介：李朝阳(1996)，男，硕士研究生，研究方向为电力信息安全。

彭道刚(1977)，男，博士后，教授，主要研究方向为智能发电、综合智慧能源与能源互联网等。(通讯作者)

(本文编辑：徐　晗)