基于安全事件关联分析的电力监控系统网络攻击识别技术研究

童加斌[1]
TONG Jiabin

摘 要 针对电力监控系统多源告警分散、攻击关系难以连续表达及攻击执行时间不一致的问题，文章提出一种基于安全事件关联分析的电力监控系统网络攻击识别技术。该技术对防火墙、入侵检测、主机审计、监控操作和工控流量进行统一编码，以 FP-Growth 关联结果生成事件图边先验，通过关系注意图神经网络提取账户、资产、会话和控制业务之间的传播特征，再利用阶段约束动态时间规整校正攻击序列的时间伸缩性。实验结果表明，所提技术的准确率、召回率和 F_1 值分别为 96.4%、95.1% 和 95.4%，误报率为 2.4%，攻击链完整率为 94.2%，在日志缺失和攻击时间变化条件下仍具有较稳定的识别效果。

关键词 电力监控系统；安全事件关联；图神经网络；动态时间规整；攻击链；网络攻击识别

doi：10.3969/j.issn.1672-9528.2026.07.021

0 引言

电力监控系统连接调度主站、厂站设备、远动终端和安全防护装置，网络攻击往往经历资产探测、身份获取、横向移动和控制操纵等阶段，分散告警难以呈现完整传播路径。现有研究主要采用 CNN-LSTM、LSTM-SVM 等模型检测异常流量[1-2]，并通过告警关联、攻击图、FP-Growth 及灰色关联分析恢复攻击场景[3-5]；相关研究还从 APT 特征分析、审计业务检测、安全态势评估和虚假数据攻击识别等角度增强了电力网络安全分析能力[6-9]。但流量模型难以描述账户、主机和控制对象之间的跨域联系，规则及攻击图又易受集中检修、批量登录等正常行为干扰，普通图卷积对不同关系类型的语义差异刻画不足，同类攻击在执行速度变化时还会产生阶段错位[10]。据此，本文采用关联规则生成事件图先验，通过关系注意图神经网络提取网络可达、账户继承、进程派生和控制业务关系特征，并利用阶段约束动态时间规整校正攻击序列的时间伸缩，实现多源安全事件关联、攻击类型判定及攻击链恢复。

1 电力监控系统安全事件关联机理

1.1 多源安全事件语义统一

防火墙、入侵检测、主机审计、SCADA 业务日志和工控协议流量分别记录通信、身份、执行和控制行为，其字段结构、时间精度及实体名称存在差异。同一工程师站在不同数据源中可能表示为 IP 地址、主机名、设备编号或工作站角色。本文依据资产台账、账户目录和业务对象编码完成实体对齐，将第 i 条事件表示为：

$$x_i=\phi_t(t_i-\delta_i)\|\phi_a(s_i,d_i,z_i)\|\phi_u(u_i,r_i)\|\phi_p(p_i,c_i,o_i)\|\phi_b(b_i,q_i)\|\phi_l(l_i) \quad (1)$$

式中：t_i 为事件时间戳，δ_i 为设备时钟偏差，s_i 和 d_i 分别为源实体和目的实体，z_i 为所属安全区域，u_i 为操作账户，r_i 为账户角色，p_i 为通信协议，c_i 为协议类型标识或功能码，o_i 为操作对象，b_i 为行为类别，q_i 为执行结果，l_i 为风险等级，$\phi(\cdot)$ 为相应属性的编码函数，$\|$ 表示向量拼接。

实体对齐后，异常登录、远程进程启动、控制服务调用和设备状态变化能够围绕同一账户、资产和业务对象形成连续证据。节点语义由结构化字段和行为类别共同构成，避免仅以风险等级或告警名称表达事件，从而为多关系边构建提供一致输入。

1.2 攻击链关联约束

事件进入同一攻击链需同时满足时间方向、网络可达、身份连续和业务顺序约束。资产探测位于攻击前端，认证失败和异常登录反映初始访问，权限变化及远程服务调用对应权限提升和横向移动，异常控制功能码、遥控操作和设备状态变化表明攻击进入控制环节。相邻事件若在时间上接近但不存在通信路径或共享身份，其关联缺少传播基础。

设事件 e_i 与 e_j 的候选关联条件为：

$$\Gamma_{ij}=I(t_j>t_i)I(\Delta t_{ij}\le W_i)I(\chi_{ij}^{N}=1)I(\chi_{ij}^{U}=1)I(\chi_{ij}^{B}=1) \quad (2)$$

式中：Δt_{ij} 为时间差，W_i 为事件关联窗口，χ_{ij}^{N}、χ_{ij}^{U}和χ_{ij}^{B}分别为网络可达、身份连续和业务顺序是否成立，I 为示性函数。任一硬约束不成立时，两事件之间不建立传播边。

另外，不同攻击阶段采用差异化关联窗口：扫描和口令

1. 龙岩开放大学 福建龙岩 364000

试探使用较短窗口，横向移动允许较长间隔，控制命令和设备状态变化采用紧密时序约束。候选条件仅排除明显无关事件，实际关联强度由图模型结合上下文确定。

2 基于安全事件关联分析的网络攻击识别技术

本文以统一事件向量和关联约束为基础，构建多关系有向事件图，经过阶段感知关系传播后解码攻击链，整体过程如图 1 所示。

2.1 多关系安全事件图构建

将标准化事件作为节点，构建有向属性图 $G=(V,E,\boldsymbol{X},R)$，其中，V为事件节点集合，E为有向边集合，$\boldsymbol{X}$为节点特征矩阵，R 为关系类型集合。关系类型包括时间邻接、地址继承、账户继承、进程派生、会话响应、拓扑可达、规则关联和业务操作关联。边类型直接对应攻击传播条件，避免把不同语义的连接压缩为单一邻接关系。

候选边的初始关联强度表示为：

$$a_{ij}^{r}=\Gamma_{ij}\exp(-\Delta t_{ij}/\tau_r)\frac{(1+\cos(x_i,x_j))}{2}(1+\xi_r m_{ij}) \quad (3)$$

式中：a_{ij}^{r}为关系 r 下的初始强度，τ_r 为关系时间衰减尺度，$\cos(x_i, x_j)$ 为事件语义相似度，m_{ij} 为共享账户、资产、会话、进程或业务对象的数量，ξ_r 为共享实体调节系数。不同关系类型在边权计算中的侧重点并不相同：时间关系主要反映事件发生间隔，账户关系强调身份继承，业务关系则同时考察控制对象、操作顺序和执行结果。基于这一差异化关系表达，IEC 60870-5-104 报文中的类型标识、传送原因和信息体地址被进一步引入业务边构建，使控制选择、执行确认和设备变位能够形成连续业务链，同时将登录、进程启动和远程服务调用组织为身份传播链和进程执行链。

2.2 阶段感知关系图学习

普通图卷积对不同边采用相同传播形式，容易削弱账户继承、进程派生和业务控制关系之间的差异。本文为每类关系设置独立参数，并将攻击阶段转移概率写入注意力计算。

第 l 层由节点 u 向节点 v 传递的信息权重为：

$$\alpha_{uv}^{r,l}=\mathrm{softmax}_{u\in\mathcal{N}_r(v)}\left\{\mathrm{LeakyReLU}\left[\left(a_r^{l}\right)^{\mathrm{T}}\left(\boldsymbol{W}_r^{l}\boldsymbol{h}_u^{l}\|\,\boldsymbol{W}_r^{l}\boldsymbol{h}_v^{l}\|\,a_{uv}^{r}\|\,p_{c_uc_v}\right)\right]\right\} \quad (4)$$

式中：$\boldsymbol{W}_r^{l}$ 和 a_r^{l} 为关系 r 的映射矩阵及注意参数，$\boldsymbol{h}_u^{l}$ 和 $\boldsymbol{h}_v^{l}$ 为节点隐藏状态，$p_{c_uc_v}$为阶段 c_u 向 c_v 的转移概率。探测向初始访问、初始访问向权限提升、权限提升向横向移动或控制操纵具有较高转移概率，违反阶段方向的连接在传播时受到抑制。

节点更新采用关系聚合和残差门控：

$$\boldsymbol{h}_v^{l+1}=g_v^{l}\sigma\left(\sum_{r\in R}\sum_{u\in\mathcal{N}_r(v)}\alpha_{uv}^{r,l}\boldsymbol{W}_r^{l}\boldsymbol{h}_u^{l}\right)+\left(1-g_v^{l}\right)\boldsymbol{h}_v^{l} \quad (5)$$

残差门控在聚合邻域信息的同时保留节点原始表征，使扫描、登录和控制等不同事件在多层传播后仍保持语义区分。为同时约束节点所处攻击阶段、事件边是否属于真实传播路径以及相邻阶段的演化顺序，进一步构建由阶段分类损失、边关联损失和阶段连续性损失组成的联合训练目标：

$$\mathcal{L}=\mathcal{L}_{\mathrm{stage}}+\lambda\mathcal{L}_{\mathrm{edge}}+\mu\mathcal{L}_{\mathrm{cons}} \quad (6)$$

式中：$\mathcal{L}_{\mathrm{stage}}$ 为衡量节点攻击阶段预测误差，$\mathcal{L}_{\mathrm{edge}}$ 为衡量事件边是否属于同一攻击链，$\mathcal{L}_{\mathrm{cons}}$ 为约束相邻节点的阶段顺序。三个损失围绕同一事件图优化，阶段识别结果反向修正边注意力，边关联结果又为阶段传播提供结构依据。

2.3 攻击链解码及类型判定

模型输出节点攻击阶段概率和边传播概率，并从高概率入口事件开始，沿时间方向搜索满足阶段连续性的候选路径。候选路径Π的评分为：

$$S(\Pi)=\frac{1}{|\Pi|}\sum_{(i,j)\in\Pi}\ln P\left(e_{ij}=1\right)+\frac{\beta}{|\Pi|}\sum_{i\in\Pi}\ln P(c_i)+\gamma C(\Pi)-\eta Q(\Pi) \quad (7)$$

式中：路径边关联概率的平均对数项用于衡量传播关系可信度，节点阶段概率的平均对数项用于衡量阶段识别可靠性；$C(\Pi)$为阶段覆盖率，$Q(\Pi)$为账户、拓扑或业务结果冲突数量，β、γ和 η 为调节参数。

路径评分综合边关联可信度、节点阶段概率、阶段覆盖

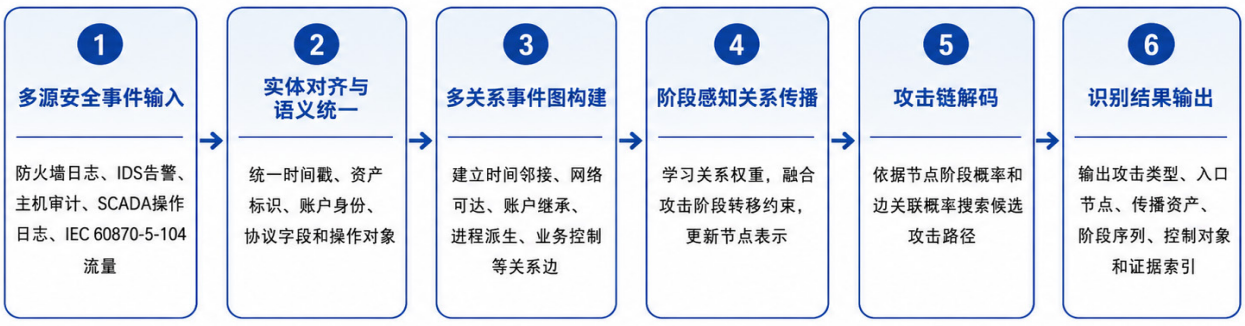

图 1 基于安全事件关联分析的网络攻击识别流程

率和冲突数量。仅包含探测、认证和权限获取的路径判定为入侵尝试或横向移动风险；连接异常控制命令、量测偏移或设备状态变化的路径判定为控制域攻击。具有相同入口账户、恶意进程或攻击源的路径进一步归并为完整攻击实例，输出攻击类型、入口节点、传播资产、阶段序列、控制对象和证据索引。

3 实验设计与结果分析

3.1 实验场景及数据集构建

实验采用某省级电力调度系统脱敏日志和隔离环境攻击注入数据，数据源包括防火墙、纵向认证装置、入侵检测系统、主机审计、SCADA 操作日志和 IEC 60870-5-104 流量。正常样本覆盖计划检修、批量登录、主备切换、总召唤、通信重传和紧急遥控，攻击样本包括扫描探测、口令攻击、横向移动、控制指令篡改、虚假数据注入和拒绝服务攻击。

对比方法包括静态规则、LSTM、普通 GCN 和本文技术。评价指标包括准确率、F_1 值、误报率和攻击链完整率。攻击链完整率按照正确恢复阶段数占真实阶段数的比例计算。

3.2 综合识别结果分析

在相同训练集、测试集和参数条件下，对静态规则、LSTM、普通 GCN 及本文技术进行对比，综合识别结果如表 1 所示。

表 1 不同网络攻击识别技术性能对比

单位：%

方法	准确率	F_1 值	误报率	攻击链完整率
静态规则	83.6	80.9	10.7	68.8
LSTM	91.5	89.9	5.9	80.7
普通 GCN	93.8	92.5	4.3	88.1
本文技术	96.6	95.7	2.2	94.5

由表 1 可知，本文技术在准确率、F_1 值和攻击链完整率方面分别达到 96.6%、95.7% 和 94.5%，误报率降至 2.2%，整体性能优于静态规则、LSTM 和普通 GCN。静态规则依赖固定阈值，容易将批量登录和集中检修识别为攻击行为，误报率达到 10.7%；LSTM 能够提取事件时序特征，但缺少账户、资产和控制对象之间的关系表达，攻击链完整率仅为 80.7%；普通 GCN 引入事件图后提升了跨主机事件关联能力，但不同关系采用统一传播方式，正常业务连接与攻击传播连接区分不足。本文技术通过关系专属参数刻画账户继承、进程派生、网络可达和业务控制关系，并利用阶段转移约束限制不合理传播路径，使 F_1 值较普通 GCN 提高 3.2 个百分点，攻击链完整率提高 6.4 个百分点，表明该技术能够提高多源安全事件关联和跨设备攻击链恢复的稳定性。

3.3 消融实验及鲁棒性分析

综合对比结果证明了本文技术的整体性能，但尚不能区分各组成部分的独立贡献。为此，实验依次移除关联规则先验、关系注意机制、阶段转移约束和动态时间规整，结果如表 2 所示。

表 2 本文技术消融实验结果

单位：%

模型设置	F_1 值	误报率	攻击链完整率
移除关系类型	92.7	4.4	88.0
移除阶段约束	93.5	3.7	89.6
移除边关联损失	94.1	3.2	90.8
完整技术	95.7	2.2	94.5

移除关系类型后，各类边采用相同传播参数，正常运维路径中的账户和业务连接获得过高权重，F_1 值下降 3.0 个百分点。移除阶段约束后，模型仍能学习事件结构，但跨阶段错误连接增多，攻击链完整率下降 4.9 个百分点。移除边关联损失后，节点分类仍保持较高准确率，路径边缺少直接监督，攻击链完整率下降至 90.8%。

4 结论

本文提出一种基于阶段感知多关系事件图的电力监控系统网络攻击识别技术，将多源事件统一表征、关系传播、阶段识别和攻击链解码纳入同一模型。实验结果表明，本文技术的识别准确率、F_1 值和攻击链完整率分别达到 96.6%、95.7% 和 94.5%，误报率降至 2.2%。消融结果验证了关系类型、阶段约束和边关联监督对跨设备攻击链恢复的作用。后续研究将引入操作票、检修计划和人员授权上下文，增强非常规合法操作与恶意控制行为的区分能力。

参考文献：

[1] 杜浩良，孔飘红，金学奇，等．基于深度学习的电力信息网络流量异常检测 [J]. 浙江电力，2021,40(12):117-123.

[2] 刘栋，蒋正威，朱英伟，等．基于 LDSAD 的电力监控系统网络流量异常检测 [J]. 浙江电力，2022,41(3):87-92.

[3] 雷轩，程光，张玉健，等．基于电力网络态势感知平台的告警信息关联分析 [J]. 计算机工程与科学，2023,45(7):1197-1208.

[4] 叶卫，王文，董科，等．面向变电站网络的虚假数据注入攻击定位与溯源技术研究 [J]. 浙江电力，2022,41(7):101-106.

[5] 许训炜，沈希澄，周霞，等．基于数据驱动的源网荷储协同控制系统网络攻击关联性分析 [J]. 浙江电力，2023, 42(2): 76-82.

基于多模态融合与动态对抗训练的智能网络安全检测系统研究

罗 彩[1] 王 勇[1]
LUO Cai WANG Yong

摘 要 针对传统网络入侵检测模型在复杂场景下的检测精度较低、鲁棒性不足等问题，文章提出了一种多模态融合 + 动态对抗检测系统，系统采用轻量化的四层架构，依托改进 VDBERT 垂域模型实现流量时序与日志语义特征深度融合，搭配 GAN 对抗训练提升模型抗变异攻击鲁棒性。实验选取 CIC-IDS2017 与 CERNET-Log 混合数据集开展多组测试，并进一步对 DDoS、SQL 注入、端口扫描等典型攻击类别的分类结果进行对比分析。实验结果表明，多模态融合动态对抗检测系统在混合数据集上的准确率、精确率、召回率、F_1-score 等指标均有不同程度的提升，误报率得到有效降低，综合性能优于各类基准模型，能够有效满足公开与真实网络场景的入侵检测需求，为复杂网络环境下的安全防护提供技术支撑。

关键词 人工智能；网络安全检测；多模态融合；动态对抗训练；生成对抗网络

doi：10.3969/j.issn.1672-9528.2026.07.022

0 引言

随着互联网技术的快速普及，网络已成为社会生产生活的核心基础设施，与此同时，DDoS 攻击、SQL 注入、端口扫描等各类网络攻击行为频发，严重威胁网络安全、数据隐私与系统稳定 [1]。网络入侵检测作为网络安全防护体系的核心环节，其核心任务是实时识别网络中的异常行为，及时预警攻击风险，为网络安全防护提供决策依据。

目前，网络入侵检测模型主要分为传统机器学习模型与深度学习模型两大类。传统机器学习模型如随机森林（RF）、支持向量机（SVM）等，优点是训练速度快、可解释性强，但在处理高维网络流量、复杂攻击场景时，容易出现特征提取不充分、检测精度较低的问题。深度学习模型，比如 CNN、VDBERT 等，能通过深层网络结构实现特征的自动提取，在入侵检测中展现出较好的性能，但单一模态的深度学习模型很难同时融合网络流量、系统日志等多源数据的特征，面对新型隐蔽攻击时鲁棒性不足。

针对上述问题，本文提出了一种多模态融合 + 动态对抗检测系统，整合网络流量与系统日志多源数据特征，通过动态对抗训练提升模型对新型攻击、隐蔽攻击的识别能力。为了验证模型的有效性与优越性，本文采用公开标准数据集与真实场景数据相结合的实验方案，以 CIC-IDS2017 数据集为基准，以 CERNET-Log 教育网真实日志数据集为真实场景验证，并与主流检测模型展开对照实验，全面评估所提模型的检测性能，为网络入侵检测技术的优化与应用提供一些实验依据与理论参考。

1. 广西国际商务职业技术学院 广西南宁 530007

[基金项目] 广西国际商务职业技术学院 2024 年度校级科研项目“基于机器学习的网络安全攻击检测系统研究”（GSB2024020）

[6] 杨航 , 樊凯 , 梁段 . 基于蚁群算法的电力数据网络 APT 攻击特征分析及防御技术 [J]. 微型电脑应用 , 2023, 39(7): 101-104.

[7] 孙勇 , 刘高原 . 针对电网审计业务应用的网络攻击检测 [J]. 微型电脑应用 ,2024,40(3):89-92.

[8] 高国庆 , 徐天竹 , 屈巍 , 等 . 电力信息系统网络安全态势智能评估方法 [J]. 微型电脑应用 ,2024,40(11):145-148.

[9] 吴莉艳 , 孙开元 , 陈坤 , 等 . 基于 CNN-LSSVM 的电力系统虚假数据攻击检测 [J]. 浙江电力 ,2024,43(11):90-96.

[10] 钟睿 , 冯文英 , 李若南 , 等 . 基于 ATT&CK 框架的技术关联分析方法综述 [J]. 网络空间安全科学学报 , 2025, 3(5): 2-13.

【作者简介】

童加斌（1986—），男，福建长汀人，硕士，讲师，研究方向：计算机技术、教育技术。

（收稿日期：2026-06-17 修回日期：2026-07-16）