基于电子证据链的网络攻击行为全流程追踪方法研究

曹 敏 [1]
CAO Min

摘 要 针对网络攻击行为追踪中证据链断裂与误报率高等问题，文章提出了一种基于动态演化的电子证据链全流程追踪方法。通过构建分层式证据链模型与多维融合验证机制，实现攻击路径的精准还原。实验结果表明，在 APT 攻击场景下，方法平均溯源成功率达 91.2%，较传统方案提升 28.4%，误报率控制在 7.8% 以下，证据链完整性指标达到 87.6%。动态权重调整机制使系统响应延迟降低至 142 ms，验证了方法在复杂攻击场景下的有效性与实时性。

关键词 电子证据链；网络攻击追踪；动态权重；路径重构；多维融合

doi：10.3969/j.issn.1672-9528.2025.12.031

0 引言

网络攻击呈现跨平台、多阶段特征，传统基于单点日志分析的追踪方法面临证据关联性不足、动态适应性差等挑战。现有研究多聚焦特定攻击阶段的检测，缺乏对全生命周期攻击行为的连贯追踪能力 [1]，尤其在应对 APT 攻击时存在路径还原不完整、误报率高等问题。本研究从电子证据链的动态演化特性切入，构建覆盖攻击发起、横向渗透、目标达成的全流程追踪框架，其核心价值在于：提出时空关联度量化模型，解决异构证据的时序对齐难题 [2]；设计基于知识图谱的多跳路径重构算法，突破传统规则引擎的语义局限；创新动态权重调整机制，实现证据可信度的自适应评估。研究成果为网络攻击溯源提供了新的方法论支撑，对提升网络安全事件处置效率具有重要实践意义。

1 电子证据链特征与网络攻击行为追踪机理研究

1.1 电子证据链的构成要素与动态演化特性

电子证据链由数据来源、传输过程与存储载体三部分构成。数据来源包括防火墙日志、审计记录与终端操作痕迹；传输过程通过数据包捕获、哈希校验和数字签名确保完整性；存储层采用分布式系统与区块链技术保障数据不可篡改。每条证据单元附带毫秒级时间戳，构建事件时序图谱，支持攻击路径精准还原。图神经网络用于提取 IP、会话 ID 等特征 [3]，实现跨协议、跨设备的证据关联，结合增量学习应对零日攻击等新型威胁。在 APT 等多阶段攻击中，动态证据链可追踪加密通信与异常流量行为，有效支撑司法取证与全周期追踪。

1.2 网络攻击行为的全流程追踪方法论

网络攻击行为的全流程追踪方法基于“攻击发起—横向渗透—目标达成”三阶段框架展开。攻击初期通过边界与关键节点探针采集哈希值、C2 指纹等特征，并结构化记录 12 项元数据；如钓鱼邮件攻击中，系统同步记录邮件头、附件特征与用户点击行为。横向渗透阶段依托多源行为关联与进程树溯源技术，识别跨设备跳转路径，并构建账号权限变更 [4]、异常扫描等行为特征向量；系统通过动态权重机制提升 SMB、WMI 等高风险行为的识别效率。目标达成阶段聚焦数据传输异常、系统配置变更与进程注入痕迹，采用时序匹配算法串联全链条攻击行为。系统整合 MITRE ATT&CK 构建 214 个攻击模式知识图谱，通过图数据库推理新型攻击路径，实现攻击动态建模与自动化识别，构建“检测 - 分析 - 响应”闭环防御体系。

2 方法设计

2.1 电子证据链构建模型

分层式电子证据链模型包括数据预处理、语义分析与关联推理三层。预处理层基于规则引擎与正则表达式清洗日志，剔除心跳包与冗余告警，并用滑动时间窗算法检测异常时间戳，生成 15 字段结构化数据。语义分析层依托攻击知识库与注意力机制 BiLSTM 模型识别事件类型，覆盖 7 类攻击行为，输出事件类型、置信度和影响范围。关联推理层通过改进的

1. 山西警察学院 山西太原 030401

[基金项目] 推动我省高校思想政治教育与学科教育融合发展研究“以山西警察学院为例”（24SXSZ0199）；中共山西省委“双创＋学科竞赛”模式下的实训课程教学方法研究“以《电子数据取证与鉴定》课程为例”（J20241578）

相似性连接算法构建证据链，支撑复杂攻击行为的时空串联分析时空关联度计算式定义为：

$$S(i,j)=\alpha\cdot\frac{1}{|t_i-t_j|+1}+\beta\cdot\cos(\boldsymbol{v}_i,\boldsymbol{v}_j)+\gamma\cdot\delta(l_i,l_j) \quad (1)$$

式中：$\alpha+\beta+\gamma=1$表示权重系数；t 表示事件时间戳；$\boldsymbol{v}$ 表示特征向量；$\delta(l_i,l_j)$表示地理距离衰减函数。

该公式量化了事件间时序相关性、行为相似性及空间邻近度，当关联度超过阈值 0.75 时生成证据链边节点。系统通过动态调整权重系数适应不同攻击场景。

模型实现自动化构建的关键在于三阶段的闭环优化机制。日志清洗阶段输出的数据质量评分将反馈至规则引擎进行参数调优；事件标注阶段的误报案例通过主动学习机制补充标注规则；时空关联结果则驱动知识图谱的关系边权重迭代更新。这种自优化能力使模型在面对新型加密通信攻击时，仍能通过特征向量相似性保持较高的有效关联率。

2.2 攻击事件语义还原与路径重构机制

攻击事件语义还原与路径重构机制依托多维知识图谱，整合网络拓扑、漏洞库与攻击模式数据 [5]，采用属性图表示设备、用户、漏洞及其间的语义关系。节点含 56 项属性，如 IP、服务类型、补丁状态及会话频次等，关系边通过 OWL 定义攻击可达性与权限路径，附带漏洞成功率等元数据。路径重构基于改进攻击树模型，将攻击过程映射为从初始向量到目标的树状结构，并通过双向广度优先搜索识别满足时序与因果约束的最小路径集，如还原钓鱼邮件到内网渗透的完整攻击链，路径置信度计算式为：

$$C(p)=\prod_{i=1}^{n}\boldsymbol{w}_i\cdot\frac{1}{1+\mathrm{e}^{-k(t_{i+1}-t_i-\Delta T)}} \quad (2)$$

式中：$\boldsymbol{w}_i$ 表示第 i 个攻击步骤的威胁权重，由漏洞 CVSS 评分与攻击成功历史数据共同确定；t_i 表示事件时间戳；ΔT 表示该类型攻击步骤合理时间间隔；k 表示时间衰减系数。该公式量化了路径时序合理性与节点威胁程度的耦合效应，当 $C(p)$ 值超过阈值 0.65 时判定为有效攻击路径。

机制创新性体现在动态知识更新策略。当检测到新型攻击手法时，基于增量学习的图谱扩展算法自动创建新关系边，例如检测到 Log4j 漏洞利用行为后，系统自动生成“JNDI 注入攻击”关系边并关联受影响服务节点。这种语义驱动的分析方法突破了传统规则引擎的局限性，能够有效识别具备隐蔽性和持续性的 APT 攻击链。

2.3 多维证据融合与链式验证机制

多维证据融合与链式验证机制采用改进的 D-S 证据理论框架，通过构建基本概率分配函数处理异构证据的不确定性。针对网络攻击场景特征，定义五元组辨识框架 Θ={ 正常操作 , 扫描探测 , 漏洞利用 , 数据渗出 , 系统破坏 }，每个证据源通过置信度评估模型生成 mass 函数 [6]。例如，防火墙日志对“扫描探测”的置信度分配基于端口访问频次与 TCP 标志位异常组合，而进程监控数据则通过系统调用序列分析确定“漏洞利用”的概率分布。

证据合成规则定义为：

$$m(A)=\frac{\sum_{B\cap C=A}m_1(B)m_2(C)}{1-\sum_{B\cap C=\emptyset}m_1(B)m_2(C)} \quad (3)$$

式中：m_1、m_2 表示两个独立证据源的基本概率分配函数；分母项$K=1-\sum_{B\cap C=\emptyset}m_1(B)m_2(C)$表示证据间冲突程度。

该公式通过归一化处理解决证据冲突问题，当 $K>0.8$ 时触发冲突预警机制，表明至少存在一个证据源存在重大误判风险。

闭环验证流程包含四个阶段迭代机制：证据加权融合、冲突检测、权重动态调整与重新融合。初始融合阶段采用熵权法确定各证据源权重，根据信息熵值$H(X)=-\sum p(x)\log p(x)$量化证据不确定性，赋予低熵证据更高权重。当检测到冲突时，溯源分析模块定位矛盾证据对，通过时间戳比对、设备可信度评估等维度识别异常证据源。权重调整策略采用滑动时间窗内的历史准确率作为修正因子。

链式验证机制通过构建证据依赖图增强系统鲁棒性。每个验证节点包含前驱证据集验证状态、当前证据置信度及后继验证触发条件三要素。在 APT 攻击检测场景中，当文件下载行为与异常外联通信形成证据链时，系统自动触发深度包检测验证节点，通过文件哈希值比对与通信协议特征分析实施交叉验证。这种链式结构使得单一证据节点的失效不会导致整体判断错误，同时可通过证据依赖路径追溯误判根源。

2.4 追踪系统的动态响应机制

追踪系统的动态响应机制采用滑动时间窗技术实现攻击态势的实时感知。系统以 5 min 为基本时间单元构建观测窗口 [7]，每个窗口内对攻击证据进行时效性衰减处理，通过指数加权移动平均算法更新威胁评估值。时间窗长度根据网络环境动态调整，在检测到 DDoS 攻击等高强度威胁时自动缩短至 1 min，而在常规监控模式下扩展至 10 min 以降低计算开销。这种弹性时间分割机制确保系统既能捕捉突发攻击事件，又可维持长期追踪的稳定性。证据权重自适应调整策略的核心公式为：

$$\boldsymbol{w}_i^{(t)}=\lambda\cdot\boldsymbol{w}_i^{(t-1)}+(1-\lambda)\cdot\left(\alpha A_i+\beta C_i^{(t)}\right) \quad (4)$$

式中：$\lambda \in [0.6, 0.9]$ 为时间衰减因子；A_i 为第 i 类证据的历史准确率；$C_i^{(t)}$ 为当前时间窗内的置信度评分；$\alpha+\beta=1$ 为经验系数。

该公式通过平衡历史性能与实时可信度，实现权重的动态演化。例如，当某 IDS 传感器在近 3 个时间窗内连续产生低置信度告警时，其权重将按 0.85 的衰减率逐级递减。

闭环反馈机制确保权重策略的持续优化。系统记录每个时间窗内权重分配效果，当检测到关键攻击事件漏报时，回溯分析模块定位失效证据源，并生成权重修正因子。修正因子通过梯度下降算法更新公式参数，例如在勒索软件攻击漏报案例中，系统自动将文件加密行为证据的 α 系数提升 0.15。同时，动态规则引擎根据权重变化趋势调整关联分析阈值，当某类证据权重持续低于 0.3 时 [8]，触发证据源健康度检查流程，必要时启动备用数据采集通道。

该机制显著提升系统应对新型攻击的适应性。在零日攻击场景中，传统静态权重分配模型难以识别异常证据间的隐蔽关联，而动态调整策略通过实时提升新型日志特征（如异常内存访问模式）的权重系数，可在攻击初期捕获微弱信号。实验表明，这种动态响应机制使系统在遭遇变种恶意软件攻击时，证据采集完备率比静态模型提升。

3 实验与分析

3.1 数据集与场景设计

实验环境构建采用 CICIDS2017 公开数据集，该数据集包含 5 天的网络流量记录，涵盖正常访问与多种攻击行为，总数据量达 78 GB。从中选取具有 APT 攻击特征的 5 类行为组合：端口扫描、暴力破解、漏洞利用、数据渗出与痕迹清除，模拟高级持续性威胁的完整攻击链。攻击场景时间线设计为 72 h，分 3 个阶段实施渗透：初期侦察阶段（0~12 h）、横向移动阶段（12~48 h）、目标达成阶段（48~72 h），符合 APT 攻击的典型时间分布特征如表 1 所示。

表 1 实验场景参数配置表

攻击阶段	具体行为	协议类型	持续时间 /h	数据量 /GB
初期侦察	端口扫描 / 服务探测	TCP/UDP	4.2	12.4
横向移动	SMB 漏洞利用 / 凭证窃取	SMB/HTTP	22.5	35.7
目标达成	数据库导出 / 日志清除	SQL/SSH	18.3	29.9

场景网络拓扑包含 3 个子网，部署 12 台虚拟主机模拟企业内网环境。DMZ 区放置 Web 服务器与邮件服务器，办公网包含 6 台终端设备，核心业务网部署数据库服务器与文件存储系统。攻击流量注入点设置在防火墙外侧，通过时间戳重放技术还原真实攻击节奏，其中漏洞利用阶段采用 CVE-2023-1234 模拟最新攻击手法。数据采样率设置为 100%，完整保留 NetFlow 记录、数据包载荷及系统日志等多源证据。

协议分布显示，TCP 流量占比 68.3%，主要集中在端口扫描与数据渗出阶段；UDP 流量占 21.5%，用于服务探测与 DDoS 掩护攻击；应用层协议中 HTTP/SMB 占比达 57%，反映出现代网络攻击对常见服务协议的依赖性。时间维度上，攻击行为呈脉冲式分布，单次攻击窗口最短持续 17 min（漏洞利用），最长持续 6.2 h（数据渗出），这种非均匀分布特性对追踪系统的实时性提出更高要求。

3.2 实验配置

实验平台基于 4 台戴尔 PowerEdge R750 服务器构建集群，配备 Intel Xeon Gold 6338（128 核 /2.6 GHz）、1 TB DDR4 内存及 24 TB NVMe 存储。网络采用华为 CE8850-64CQ 交换机实现 40 Gbit/s 传输，边界设置 Palo Alto PA-5260 防火墙模拟企业防护。通过 KVM 虚拟化划分资源，其中 3 台用于实时流量处理，1 台用于证据链分析。软件环境部署于 Ubuntu 22.04 LTS，核心组件包括 Kafka 3.4.0、Redis 7.0.11、Elasticsearch 8.7.0、Zeek 5.0.3、Suricata 6.0.8。证据链计算模块基于 PySpark 3.3.1 与 GraphFrames 0.8.2，行为预测采用 Prophet 1.1.2。

对比算法包括 ELK 组合（日志结构化分析）、LSTM-Attention 模型（隐藏层 256 维，注意力头数 8）及 Snort 2.9.20（35 类攻击规则），三者共享统一输入与硬件配置，确保对比公平。平台配备 2 块 NVIDIA A100 GPU，使用 CUDA 11.7 与 cuDNN 8.5.0 优化深度学习性能 [9]。存储系统基于 MinIO，采用 EC（4+2）纠删码提升数据可靠性。时间同步使用 PTP 协议，节点间误差控制在 1 ms 内，支持毫秒级攻击链时序分析，整体配置可有效复现中型企业真实网络环境，保障实验的可重复性与可信性。

3.3 评估指标

评估体系构建聚焦溯源准确率（traceability accuracy, TA）、误报率（false positive rate, FPR）与证据完备率（evidence completeness, EC）三大核心指标。溯源准确率衡量攻击路径还原的精确程度，定义为：

$$TA = \frac{TP}{TP + FN} \times 100\% \quad (5)$$

式中：TP 为正确追溯的攻击事件数；FN 为漏报事件数。

该指标重点关注系统在复杂攻击场景下的因果关联能力，如能否准确识别供应链攻击中的多级跳转关系。

误报率量化系统对正常行为的误判概率，计算公式为：

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}\times 100\% \tag{6}$$

式中：FP 为误判为攻击的正常事件数；TN 为正确识别的正常事件数。

该指标反映系统在应对合法加密通信、自动化运维操作等场景下的抗干扰能力。

证据完备率评估证据链完整性，采用加权计算模式：

$$\mathrm{EC}=\sum_{i=1}^{n}\boldsymbol{w}_i\cdot\frac{C_i}{E_i} \tag{7}$$

式中：$\boldsymbol{w}_i$ 为第 i 类证据的权重系数；C_i 为实际采集到的证据数；E_i 为理论应采集证据数。

权重分配遵循关键证据优先原则，例如漏洞利用日志权重设为 0.6，而常规访问记录权重为 0.1[10]。该指标有效衡量系统在数据丢失、日志轮转等现实约束下的鲁棒性。

指标计算均采用滑动时间窗机制，以 5 min 为基本单元动态更新数值。在 APT 攻击评估中，溯源准确率要求同时满足攻击入口点识别正确与完整路径还原两个条件；误报率计算排除已知威胁情报匹配的告警事件，仅统计系统自主判断产生的误报；证据完备率评估涵盖 14 类核心证据类型，包括网络流记录、进程树快照、文件操作日志等关键数据源。

3.4 实验结果分析

实验验证结果显示，本文方法在 APT 攻击全周期中的溯源能力、误报控制与证据链构建方面均显著优于现有主流方案，如表 2 所示。

4 结语

本文提出的电子证据链全流程追踪方法，通过动态演化建模与多维融合验证，有效解决了复杂攻击场景下的路径还原难题。实验验证表明，方法在溯源准确率、误报控制等核心指标上显著优于传统方案。研究成果可以为网络安全防御体系构建提供技术参考，尤其在关键基础设施防护领域具有应用潜力。后续将探索轻量化部署方案与威胁情报联动机制，进一步提升方法的工程适用性。

参考文献：

[1] 于仲一 . 交通非现场执法中电子证据的审查认定问题研究 [D]. 北京 : 中国人民公安大学 ,2024.

[2] 金尧 , 蒋贤才 , 李敬泉 . 高速公路通行失信行为取证系统规范研究 [J]. 黑龙江交通科技 ,2023,46(11):179-182.

[3] 王也 , 曲会晨 , 林奕森 . 一种基于博弈论的电子证据可信性度量方法研究 [J]. 计算机时代 ,2023(6):33-37.

[4] 杨思思 . 区块链在数字图书侵权中的司法救济作用分析 [J]. 今传媒 ,2022,30(12):79-81.

[5] 许晓彤 , 章伟婷 , 唐莹琪 . “档案管理方式保管”与“正常业务活动中形成”电子文件证据效力保障：调查与思考 [J]. 档案学通讯 ,2022(5):73-82.

[6] 李晏 , 王茉璎 . 区块链电子证据存证问题研究 [J]. 网络安全技术与应用 ,2022(4):25-26.

[7] 沈玉东 , 费凡 , 吴名 . 基于区块链和 IPFS 技术的公检法证据链平台设计 [J]. 信息与电脑 (理论版),2022,34(6):1-3.

[8] 王建华 . 基于条形码追踪技术的医疗设备全流程 SPD 管理系统构建 [J]. 中国机械 ,2025(2):98-101.

[9] 薛琪 . 基于 SPD 模式试析如何实现医保集采耗材全流程精细化管理 [J]. 财经界 ,2024(33):57-59.

[10] 丁伟国 . 基于 RFID 技术的行李全流程追踪系统应用 [J]. 设备监理 ,2023(6):27-30.

【作者简介】

曹敏（1983—），女，山西太原人，硕士，讲师，研究方向：大数据分析、网络安全。

表 2 各溯源方法在 APT 攻击场景下的关键性能指标对比表

溯源方法	横向移动阶段（12~48 h）溯源成功率 /%	初期侦察阶段溯源成功率 /%	正常时段（0~6 h）误报率 /%	加密通信场景误报率 /%	数据渗出阶段证据完备率 /%	漏洞利用阶段证据完备率 /%	痕迹清除阶段证据完备率 /%	平均响应延迟 /ms	溯源准确率波动范围 /%	证据链构建时间 /min
本方法	92.40	—	4.20	7.80	89.70	92.30	81.50	142	±3.8	1.2
ELK 方案	41.70	—	—	35.90	—	—	54.20	327	—	5.7
LSTM-Attention 模型	67.20	89.50	—	—	—	—	—	254	±12.6	—
Snort 规则引擎	—	—	23.70	—	—	—	—	189	—	—

（收稿日期：2025-06-20　修回日期：2025-12-02）