 DOI: https://doi.org/10.12349/iser.v7i3.9478

Research on Multi-source Threat Intelligence Fusion Based on Dynamic Credibility and Spatio-temporal Features

Ruili Li

Shanghai Digital Security Technology Co., Ltd., Shanghai, 200435, China

Abstract

To address the challenges of frequent APT attacks and 0day vulnerabilities, as well as the limitations of traditional static rule-based detection, this paper proposes a dynamic credibility-based multi-source threat intelligence fusion method. First, a unified framework is established to standardize the parsing of heterogeneous intelligence. Second, an innovative spatiotemporal dynamic evaluation model is introduced: the temporal dimension utilizes LSTM neural networks to analyze historical performance of intelligence sources and extract temporal features; the spatial dimension assesses the tactical coverage and logical coherence of attack behaviors based on the MITRE ATT&CK framework. Finally, by integrating spatiotemporal feature parameters, the method dynamically calculates real-time credibility weights for each intelligence source to generate a comprehensive threat score. Experiments demonstrate that this approach effectively adjusts intelligence source weights, significantly reduces false positive and false negative rates, and enhances the accuracy and reliability of threat response.

Keywords

Threat intelligence; Data fusion; Dynamic credibility; Long short-term memory network; MITRE ATT&CK; Network security

基于动态可信度与时空特征的多源威胁情报融合方法研究

李瑞丽

上海数字安全科技有限公司，中国 · 上海 200435

摘　要

针对APT攻击与0day漏洞频发、传统静态规则检测能力不足的问题，本文提出一种基于动态可信度的多源威胁情报融合方法。首先，构建统一框架实现异构情报的标准化解析。其次，创新引入时空动态评估模型：时间维度利用LSTM神经网络分析情报源历史表现以提取时序特征；空间维度基于MITRE ATT&CK框架评估攻击行为的战术覆盖度与逻辑连贯性。最后，融合时空特征参数，动态计算各情报源的实时可信度权重，生成综合威胁评分。实验证明，该方法能有效调整情报源权重，显著降低误报漏报率，提升威胁响应的准确性与可靠性。

关键词

威胁情报；数据融合；动态可信度；长短期记忆网络；MITRE ATT&CK；网络安全

1 引言

随着 APT 攻击、0day 漏洞等新型威胁的演进，传统依赖特征库的安全设备检测效率低下，响应滞后。安全运营平台虽整合多源威胁情报，但现有融合方法多采用静态权重，无法根据情报源实时可信度动态调整，导致误报漏报率居高不下。

针对此问题，本文提出一种基于动态可信度的多源威胁情报融合方法，核心创新包括：构建统一标准化处理框架、引入时空动态评估模型、基于时空特征动态计算可信度权重并生成融合评分。

【作者简介】李瑞丽（1983—），女，中国上海人，硕士，工程师，从事数字安全、网络威胁情报分析与多源数据融合技术研究。

2 相关工作

2.1 威胁情报标准化研究

威胁情报标准化是多源情报融合的基础。业界广泛采用STIX/TAXII标准格式[5]，STIX 2.1定义了18种领域对象，为情报结构化描述提供统一规范。

然而实际应用中，各情报源在 API 接口、数据格式、置信度表示等方面差异显著，部分采用 JSON、CSV、XML 格式，甚至包含大量非结构化 PDF 报告 [6]。现有适配器方案需为每个情报源定制解析逻辑，导致接入成本高、维护周期长。文献 [4] 提出基于模板映射的标准化方法，通过预定义映射规则实现异构数据转换，但对非结构化数据处理能力有限。

2.2 情报融合与可信度评估研究

多源情报融合的核心是整合异构情报形成一致威胁判

断。传统融合方法包括投票法、D-S 证据理论、贝叶斯网络等 [8]。

可信度评估研究分为两类：基于内容可信度（分析情报完整性、一致性等）[9] 和基于来源可信度（依据历史表现、声誉赋权）[10]。但两类方法通常分开考虑，未挖掘内在关联，且多采用静态权重，无法根据情报源实时表现动态调整。

文献 [5] 提出了基于可信度的多源网络安全数据融合方法，但主要关注静态权重分配，未考虑情报源可信度的动态变化。MITRE ATT&CK 框架 [6] 为分析攻击行为的战术阶段关联提供了有力工具，但将其应用于情报可信度动态评估的研究尚不多见。

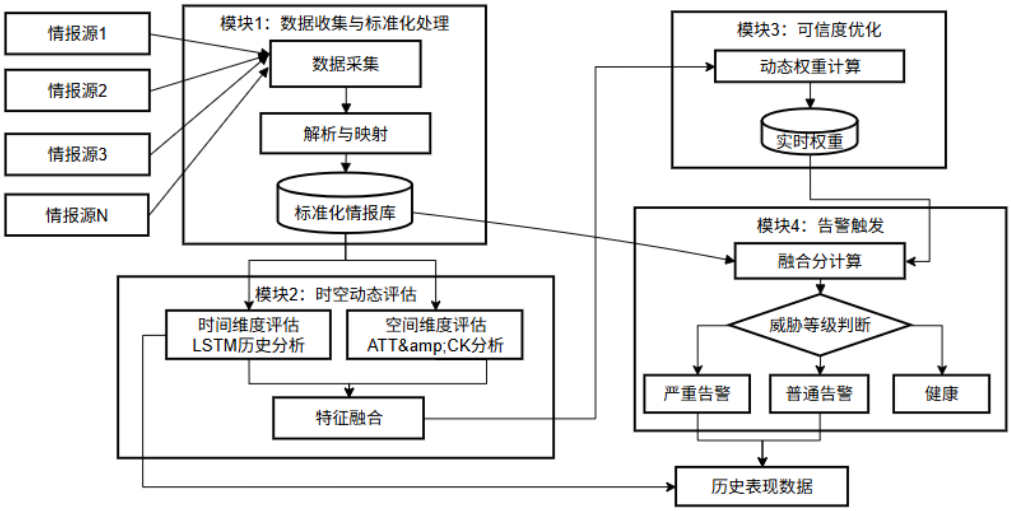
综上，现有研究在融合时间维度历史表现与空间维度攻击行为完整性进行综合评估方面存在空白，本文旨在填补这一空白。

3 系统模型与方法

3.1 总体框架

本文提出的基于动态可信度的多源威胁情报融合方法总体框架如图 1 所示，主要包括四个核心模块：数据收集与标准化处理模块、时空动态评估模块、可信度优化模块以及告警触发模块。

数据收集模块负责针对特定安全产品，实时采集其配置的多个情报源所产生的威胁情报，并记录各情报源的历史表现数据。标准化处理模块对异构情报进行统一格式转换与特征提取。时空动态评估模块分别从时间维度（利用 LSTM 分析历史表现）和空间维度（基于 ATT&CK 框架分析攻击行为）评估威胁情报的特征参数。可信度优化模块根据时空特征参数动态计算各情报源的实时权重。告警触发模块基于多源情报的融合分进行最终决策。系统总体框架图如下：



3.2 多源威胁情报标准化处理

考虑到各情报源在数据格式、字段定义、置信度量纲等方面存在显著差异，本文设计了一套统一的多源威胁情报标准化处理流程，该流程首先对原始情报进行语法级解析，将其转换为统一的 JSON 格式；随后通过语义映射机制，将异构的字段定义对齐至预设的标准数据模型；最后对置信度等数值量纲进行归一化处理，从而形成结构一致、语义明确的高质量情报数据集，为后续的动态可信度评估奠定基础。

3.2.1 字段类型识别与映射

首先，识别威胁情报原始数据的字段类型。本文将字段划分为基础字段类型和复合字段类型两类：

将威胁情报字段划分为两类：

基础字段：唯一标识符、类型、创建时间等基本属性，直接映射至标准模板

复合字段：攻击阶段（kill_chain_phases）、置信度（confidence）等，需结构化解析提取关键信息

3.2.2 攻击阶段的 TTP 编码转换

对于攻击阶段字段，本文将其转换为 MITRE ATT&CK 标准编码。具体地，将字段值中的攻击阶段名称映射为对应的 ATT&CK 战术标识符（TA 代码）。例如，将 "phase_name": "initial-access" 转换为 "ttp_stages": ["TA0001"]；将 "execution" 转换为 "TA0002"。这一转换使得后续可以基于 ATT&CK 框架进行空间维度的评估分析。

3.2.3 置信度归一化处理

不同情报源对置信度的表示方式各不相同，有的采用 0-100 的整数，有的采用 0-10 的整数，还有的采用高、中、低等定性描述。为统一量纲，本文将所有置信度值归一化到 0-1 区间。例如，原始数据中 "confidence": 75 转换为 "confidence_score": 0.75；原始数据中 "confidence": "high" 可根据预设规则转换为 0.9。

3.2.4 非结构化数据处理

针对非结构化数据（PDF 报告、安全公告等），进行多模态特征提取：

数据拆分：将原始数据拆分为文本、图像、元数据三组

文本处理：清洗、分词、实体识别、关键信息抽取

图像处理：OCR 技术提取图像文字

元数据处理：可信度验证与时间合理性检查

最终将多模态特征融合为结构化文本，供后续标准化处理使用。

3.2.5 低置信度特征标记

在完成标准化处理后，对置信度低于预设标准的特征数据进行标记。这些被标记的特征数据在后续的时空动态评估中将被剔除，仅利用置信度较高的特征数据进行评估，以确保评估结果的可靠性。

3.3 基于时空特征的动态可信度评估模型

本文提出基于 ATT&CK-LSTM 的时空动态评估模型，分别从时间维度和空间维度对威胁情报的可信度进行综合评估。

3.3.1 时间维度评估

时间维度评估的核心思想是利用情报源的历史表现预测当前威胁情报的时序特征。本文选取两个关键指标表征情报源的历史表现：

命中率：表示情报源产生的威胁情报的正确告警次数与总告警次数的比值，反映了情报源的准确性。

响应时间：表示从威胁发生到情报源产生告警的时间间隔，反映了情报源的时效性。

对于每个情报源，收集其在预设时间窗口（本文选取 30 天）内的每日命中率和响应时间数据。基于这些历史数据，计算两个统计特征：

准确率：时间窗口内命中率的平均值。

P99 延迟指标：时间窗口内响应时间的 99 分位值，用于衡量响应时间的分布情况。

将情报源的准确率和 P99 延迟指标作为输入，利用长短期记忆神经网络（LSTM）模型进行时序预测。LSTM 因其在处理时间序列数据方面的优势而被选为本模型的时序分析工具，它能够有效捕捉历史表现中的长期依赖关系。LSTM 模型的输出即为当前威胁情报的第一特征参数 T_time，表征其时间维度的可信度。

当情报源的准确率低于预设第一阈值时，相应调小当前威胁情报的第一特征参数，以避免低质量情报源对融合结果产生过大影响。

3.3.2 空间维度评估

空间维度评估的核心思想是利用 MITRE ATT&CK 框架分析威胁情报中攻击行为的逻辑完整性。本文从覆盖度和共现概率两个维度进行评估。

覆盖度（Coverage）：表示威胁情报所包含的攻击行为覆盖 MITRE ATT&CK 模型中记录的攻击行为的占比。计算公式为：C=N_ttp/N_total

其中，N_{ttp} 表示威胁情报中包含的 ATT&CK 技术数量，N_{total} 表示 ATT&CK 模型中记录的总技术数量（当前版本约为 200 余种）。覆盖度反映了威胁情报的信息丰富程度。

共现概率（Co-occurrence Probability）：用于量化攻击行为中战术之间的关联强度。通过分析历史数据中不同战术阶段同时出现的频率，计算当前威胁情报中战术阶段的共现概率。计算公式为：P=(Count_(co-occur))/(Count_total)

其中，Count_(co-occur) 表示当前威胁情报中涉及的战术组合在历史数据中的共现次数，Count_total 表示该战术组合中主导战术在历史数据中出现的总次数。共现概率反映了威胁情报中攻击行为的逻辑连贯性。

综合覆盖度和共现概率，计算第二特征参数 T_space：T_space=α·C+(1-α)·P

其中，α 为预设系数，本文取默认值 0.6，可根据实验优化调整。

此外，考虑到威胁情报的连续性，当连续多个关于同一情报源计算的第二特征参数均低于预设第二阈值时，说明该情报源在当前阶段匹配度持续较低，相应调小当前威胁情报的第二特征参数。

3.4 动态可信度权重计算与融合决策

3.4.1 可信度权重计算

基于时空动态评估得到的两个特征参数，计算情报源实时的可信度权重。权重计算公式如下：W=β·T_time+(1-β)·T_space

其中，W 表示情报源的可信度权重，β 为预设系数，用于平衡时间维度和空间维度的贡献。本文通过网格搜索方法确定β的取值，实验证明在0.55-0.65区间内的值表现最优，本文取默认值 0.6。

当某一威胁情报的第一特征参数与第二特征参数的差值超过预设第三阈值时，表明时间维度评估与空间维度评估存在较大分歧，可能存在异常情况。此时，系统不自动调整权重，而是直接触发告警并等待人工介入，以确保决策的可靠性。

3.4.2 融合评分与告警决策

基于安全产品实时产生的多源威胁情报，以及对应情报源实时计算得到的可信度权重，计算所有威胁情报的融合分：Score=\sum_{i=1}^{n} (I_i \times W_i)

其中，n 表示情报源数量，I_i 表示第 i 个情报源产生的威胁情报的指示值（通常为 0 或 1，表示是否存在威胁），W_i 表示第 i 个情报源的实时可信度权重。

根据融合分进行告警决策。本文将威胁判断标准划分为三个等级：

严重：90 ＜ Score ⩽ 100

警告：60 ＜ Score ⩽ 90

健康：0 ⩽ Score ⩽ 60

当融合分超过 60 时，系统触发相应级别的告警，通知运维人员进行处理。

4 实验与分析

4.1 实验设置

为验证本文方法的有效性，搭建模拟实验平台。数据来源包括：（1）5 个模拟商业情报源，具有不同初始可信度；（2）基于 MITRE ATT&CK 的开源情报；（3）200 个攻击场景测试数据集，涵盖 APT、勒索软件、Web 攻击等类型。

选取三种对比方法：

(1) 静态等权法：所有情报源等权，多数投票决策

(2) 静态加权法：基于初始可信度分配固定权重

(3) 单一维度动态法：仅基于时间维度动态调整权重

评价指标：准确率、召回率、F1 分数、误报率。

4.2 结果分析

4.2.1 整体性能对比

实验结果表明：本文方法在各项指标上均优于对比方法。与静态等权法相比，准确率提升 12.9 个百分点（78.3% → 91.2%），召回率提升 14.2 个百分点（75.6% → 89.8%），F1 分数提升 17.7%，误报率降低 12.9 个百分点（21.4% → 8.5%）。与静态加权法相比，F1 分数提升 11.5%；与单一维度动态法相比，F1 分数提升 5.7%。误报率降至 8.5%，显著优于其他方法，验证了时空联合动态评估的有效性。

4.2.2 动态权重调整效果验证

设计特殊测试场景：第 10-20 天人为降低情报源准确率，模拟情报源被污染。实验结果显示：

本文方法：2-3 个时间周期内将权重从 0.25 调整至 0.08，快速响应可信度下降

静态加权法：始终维持 0.25 权重，导致误报率上升 12.3%

单一维度动态法：调整幅度不足，误报率仍上升 5.7%

结果表明，本文方法能有效降低低质量情报源的负面影响。

4.2.3 参数敏感性分析

对关键参数进行网格搜索分析：

时间窗口：30 天时性能最优，过小易受短期波动影响，过大则反应迟钝

系数 α：0.6 附近表现最佳，覆盖度与共现概率保持平衡

系数 β：0.55-0.65 区间内 F1 分数稳定在 0.90 以上，验证模型鲁棒性

4.3 讨论

本文方法的核心优势在于：

（1）多维融合：同时考虑时间维度历史表现与空间维度攻击行为完整性；

（2）快速自适应：及时感知情报源可信度变化并动态调整权重；

（3）异常检测：通过时空特征参数分歧监测，触发人工介入，提高系统可靠性。

5 结语

本文提出一种基于动态可信度的多源威胁情报融合方法，主要贡献包括：构建标准化处理框架，解决异构情报接入问题；引入 LSTM 时间评估与 ATT&CK 空间评估，实现可信度综合度量；设计动态权重计算与融合评分机制，提升告警准确性。实验证明，该方法有效降低误报漏报率，提高威胁检测性能。

未来研究方向：引入更细粒度的情报上下文；探索 Transformer、图神经网络等先进模型；扩展至终端检测响应、网络流量分析等场景；研究基于联邦学习的跨组织协同防御等。

参考文献

[1] 张尼, 刘锳, 张静等. 网络安全威胁情报关键技术研究综述[J]. 计算机研究与发展, 2020, 57(10): 2035-2049.

[2] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks[J]. Computers & Security, 2018, 72: 212-233.

[3] 方滨兴, 贾焰, 李爱平等. 网络空间威胁情报共享与分析技术综述[J]. 信息安全学报, 2018, 3(5): 1-16.