IP网络APT攻击检测及安全态势感知技术研究

Research on APT Attack Detection and Security Situation Awareness Technology in IP Networks

王　新，杨　飞，高存宇，郭翔乾，杨丽丽（中讯邮电咨询设计院有限公司，北京 100048）
Wang Xin，Yang Fei，Gao Cunyu，Guo Xiangqian，Yang Lili（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
在数字化浪潮的推动下，IP网络作为关键信息基础设施，正面临日益严峻的网络安全威胁。围绕IP网络中的APT攻击检测与安全态势感知展开研究，重点突破未知攻击监测、攻击链溯源与分析、安全编排与自动化响应等关键技术，构建了面向IP网络的安全态势感知量化模型。该模型能够实现对网络空间安全态势的实时、精准、全面感知，提升安全威胁的识别与响应效率，为IP网络实现全局协同防护提供有力支撑，助力构建更高水平的网络安全主动防御体系。

关键词：
IP网络；APT攻击检测；威胁情报；安全态势感知
doi：10.12045/j.issn.1007-3043.2025.09.013
文章编号：1007-3043（2025）09-0070-05
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Driven by the digital revolution，IP networks，as critical information infrastructure，are confronted with increasingly severe cybersecurity threats. It delves into APT attack detection and security situational awareness within IP networks，emphasizing breakthroughs in key technologies such as unknown attack monitoring，attack chain tracing and analysis，security orchestration and automated response. A quantitative model for IP network security situational awareness is introduced，which is designed to provide real-time，precise，and comprehensive perception of cyberspace security. By enhancing the efficiency of threat identification and response，this model supports global collaborative protection of IP networks and aids in establishing a robust，proactive defense system for advanced cybersecurity.

Keywords：
IP network；APT attack detection；Threat intelligence；Security situation awareness

引用格式：王新，杨飞，高存宇，等. IP网络APT攻击检测及安全态势感知技术研究[J]. 邮电设计技术，2025（9）：70-74.

1 概述

1.1 研究背景[1-3]

在当今数字化时代，IP网络作为信息传输的核心基础设施，已广泛服务于政府、金融、能源、通信等关键领域。然而，随着网络技术的迅猛发展，网络安全威胁日益加剧，尤其是高级持续性威胁（APT）攻击，因其隐蔽性强、攻击持久、目标高度精准，已成为网络安全领域面临的重大挑战。APT攻击通常由专业化的黑客组织发起，旨在窃取敏感数据、破坏关键系统或谋取非法利益。与传统网络攻击相比，APT攻击具有长期潜伏、多阶段协同、行为隐蔽和针对性极强等显著特征，给网络安全防御带来了更高的技术门槛和更严峻的实战考验。

1.2 研究现状

目前，网络安全研究领域已经提出了多种APT攻击检测与溯源技术，主要包括基于规则的检测、基于威胁情报（IOC）的检测、基于异常检测的检测以及单点检测等方法。而这些技术在应对IP网络APT攻击时仍存在诸多局限性，如基于规则的检测难以应对未知攻击，基于IOC的检测时效性有限，基于异常检测的检测误报率较高，单点检测难以还原完整攻击链路。

收稿日期：2025-07-18

1.3 研究意义与目标

鉴于传统APT攻击检测技术的局限性，本研究旨在提出一种基于IOC+TTP（即战术意图Tactic、技术能力Technique 和过程细节Procedure 等方面的特征）特征融合的综合检测模型，结合全流量分析与知识推理技术，实现对IP网络中APT攻击的高效检测与精准溯源。通过构建智能化攻击溯源知识图谱，深入分析攻击者的攻击路径、攻击工具和技术手段，为网络安全防护提供有力的技术支持。具体研究目标包括设计并实现一种基于IOC+TTP特征的APT攻击检测模型；研究多源数据融合与深度分析技术，构建智能化攻击溯源知识图谱；开发一套适用于IP网络的APT攻击检测与溯源系统。

2 关键技术研究

2.1 信息汇聚与融合

全面收集并整合链路状态、网络拓扑结构、隧道配置、路由策略、准入控制规则、网络流量数据、安全日志记录以及内生安全事件等多维度信息，形成全面、详实的网络状态数据库。通过数据清洗、标准化、关联分析等手段，将这些离散的、异构的信息进行深度融合，构建起网络的全景视图，为安全态势感知提供丰富的数据基础。信息汇聚与融合是实现安全态势感知的前提和基础，只有全面、准确地掌握网络的各种信息，才能为后续的分析和决策提供有力支持。

2.2 网络APT攻击监测

2.2.1 分布式图连通求解的IOC关联挖掘[4-5]

现有通过威胁情报进行APT攻击检测，往往依赖于IP、域名、URL、样本Hash等的及时性和准确性。APT组织为躲避安全防护软件的检测，会不断变换攻击使用的威胁指标IOC，但APT攻击的技术手段、攻击习惯、攻击过程等，在一定时间段内与APT组织的IOC之间存在明显的关键数据特征交叉和相似的情况。因此，本项目采用分布式图联通求解算法，实现千亿级数据的快速联通，利用ConvNet模型的自动化特征提取、泛化能力、高精度分类等特点，经过充分训练，分析攻击端的证书信息，可深度挖掘并关联出更多未被威胁情报披露的IOC线索，基于这些拓展的IOC情报线索，能够高概率且及时、准确发现新的APT攻击。突破IP/域名等显式IOC依赖，利用证书序列号等隐式特征构建攻击资源关联图谱（见图1）。

通过服务指纹和关联样本分析等技术手段验证，

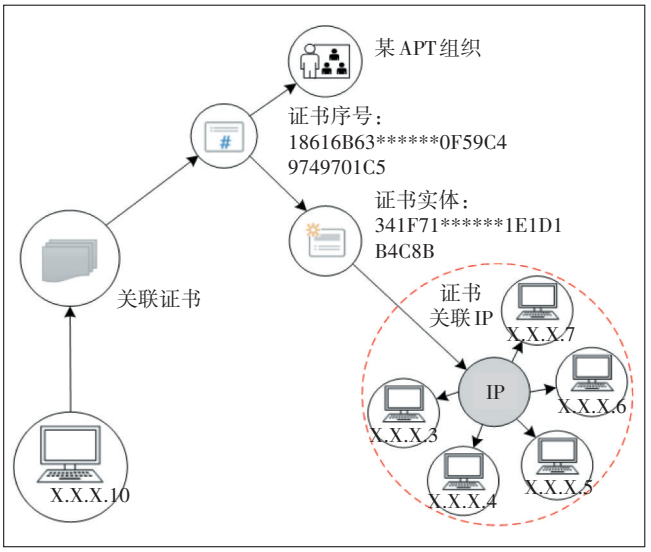

图1　攻击资源关联图谱

可确认这5个IP地址同样为某APT组织进行攻击使用的基础资源。由此可见，这5个IP地址是基于已披露的X.X.X.10地址拓展出的IOC，攻击者若持续发起攻击，则会使用这些未被披露的IP地址资源。因此通过关联挖掘拓展的IOC进行APT攻击检测，往往能够高概率发现新的APT攻击行为。

2.2.2 多模型会话TTP特征提取[6-8]

基于攻击过程中某个具体的通信数据包制定的规则进行APT攻击检测，存在特征偶合数据包多、误报率高的问题。但APT攻击过程中的TTP特征，即战术意图（Tactic）、技术能力（Technique）和过程细节（Procedure）等方面的特征，在短时间内不会轻易改变。因此，本项目通过在攻击的横向移动、命令与控制、信息渗漏等3个阶段，构造基于明文通信、标准加密通信、非标准加密通信等会话的TTP特征，并对可疑的会话数据包进行初筛过滤，形成疑似APT攻击的会话候选检测数据集。基于多模型的会话TTP特征提取方法，来实现对APT攻击的深度分析和发现（见图2）。

启动流量采集后，针对获取的工业网络流量，其中的各类元数据首先被抽取，计算IOC特征值，执行基于情报挖掘的关联检测分析。同时将所有的会话详单、全流量数据包进行留存，形成后续进行TTP特征分析的数据基础。

系统将适合作为流量检测的TTP特征，转换为TTP规则和TTP模型2个部分，经过TTP规则初筛和TTP模型检测后，输出APT攻击告警信息，该告警结果具有非常低的误报率。

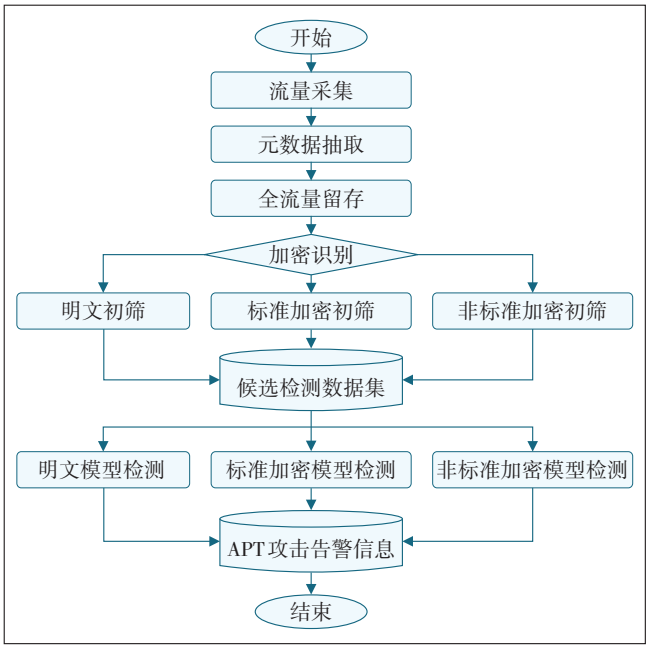

图2　APT攻击告警信息采集流程

TTP规则初筛：系统分别从明文特征、标准加密的密特征/密文特征、非标准加密的密特征/密文特征等3个维度对可疑通信会话的数据包进行初筛，具体的方法规则包括数据包结构模式、URI模式、DGA模式、SSL/SSH指纹模式等。经过初筛后，产生有待TTP模型进一步检测分析的候选会话数据集。

TTP模型检测：系统将根据不同模型的特点，将TTP规则初筛产生的会话数据集，以单/多会话的方式重组出分析所需的应用层数据，详细的分析逻辑和算法则通过具体的会话分析插件表达，同样从明文模型、标准加密模型、非标准加密模型等3个维度针对已经全流量落盘存储的可疑单个/多个会话的全流量，完成流程复杂和具有一定计算量的分析过程。具体模型分析方法包括密钥重协商特征分析、加解密运算分析、加解压运算分析、控制命令交互分析、心跳激活交互分析等。

2.2.3 网络设备异常行为检测[9-10]

基于采集的数据构建高精度、低误报的系统运行白名单和正常运行基线模型，利用AI驱动的设备运行基线偏离检测与高级异常行为识别技术，实现系统异常行为的精准识别。

数据预处理与多维度数据关联模型利用数据预处理技术，对采集的原始数据进行全面而细致的清洗、去噪、缺失值填充及归一化处理，确保数据质量和一致性。基于机器学习特征选择与表示学习方法，构建多维度智能数据关联模型，将文件系统、内存、进程活动、网络通信等异构数据进行深度融合，关联上下文语义，形成结构化且语义丰富的“数字足迹”智能视图。

网络设备自适应白名单与正常运行基线模型基于深度学习与图神经网络等先进AI技术，自动提取网络设备各层级（进程、文件、内容、用户账号等）的关键特征，构建静态白名单。然后利用无监督学习、半监督学习及增量学习方法，在动态行为数据（如进程行为、内存使用、文件访问、系统调用序列、网络连接等）上构建多层次、多粒度的正常运行基线模型，形成精准的“正常行为画像”。

基线偏离检测与高级异常行为识别技术基于AI的监测与异常检测机制，利用高效的数据比对算法，将采集的路由器数据与白名单及正常基线模型进行动态匹配。结合行为图谱和多维度智能关联分析，深层解析基线偏离和异常行为特征。通过AI驱动和深度神经网络分析识别内存攻击代码植入、识别依赖库加载路径异常、检测恶意进程等异常行为。

2.2.4 流量异常检测

在运营商IP网络环境中，面对日益复杂的APT攻击手法，构建面向多维流量的异常检测体系已成为提升整体防护能力的关键一环。APT攻击通常具备“潜伏期长、活动隐蔽、通信稀疏”的特点，传统以签名为核心的检测机制难以应对。因此，必须从网络的不同维度出发，全面挖掘流量中的异常特征，实现对APT攻击路径中关键通信行为的主动识别与动态感知。本节从以下3个方向展开论述，系统地总结当前适用于运营商网络环境中的流量异常检测关键方法。

一是面向数据平面的基于NetFlow等流量元数据的异常检测机制，通过构建流量模型与行为基线，实现对异常连接模式、突发通信行为的快速识别。

二是面向数据平面的基于DNS协议流量的深度分析与识别机制，特别关注于APT常用的动态域名生成（DGA）、DNS隧道通信等隐蔽手段。

三是面向控制平面的设备登录与管理流量（如SSH、Telnet）监控机制，通过用户行为建模与异常行为溯源，识别攻击者可能渗透或控制网络设备的路径。

通过以上3类机制的协同部署与智能融合，能够显著提升运营商对APT攻击的早期发现能力与纵深防御能力。流量异常检测总体框架示意如图3所示。

2.3 溯源与攻击链分析[11-13]

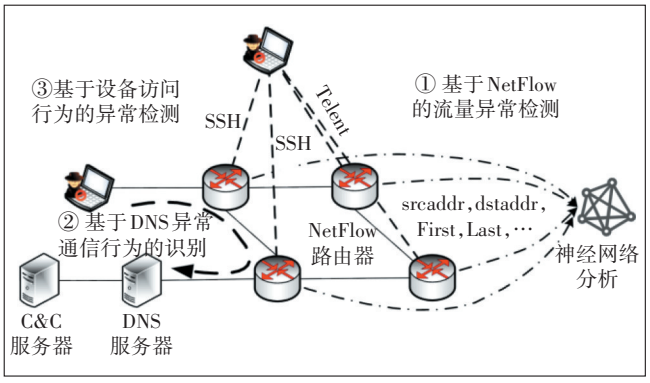

图3　流量异常监测

通过收集和分析各种安全事件的日志、系统记录等数据，获取关于攻击事件的信息；利用外部威胁情报和内部情报分析来揭示攻击者的行为模式、攻击工具和技术等信息；将收集到的数据和分析结果进行结构化建模，构建攻击事件和相关实体（如攻击者、受害者、漏洞、恶意软件等）之间的关系。然后基于实体关系建模的结果，构建一个知识图谱，将攻击事件和相关实体以及它们之间的关系进行连接和组织，发现隐藏的关联和模式，揭示攻击者的行为路径和攻击链。

2.3.1　自学习多威胁场景路径溯源技术

基于网元日志、NetFlow、DNS、网络拓扑、路由信息等数据，结合威胁情报库，实现多源异构数据融合，形成多种场景网络攻击事件溯源分析关系图，实现攻击源、受害者、攻击路径及代理池或肉鸡的画像绘制。

2.3.2　智能化攻击溯源知识图谱技术

基于图数据库算法、机器学习、深度学习等技术，形成网络攻击事件溯源关系图。通过知识图谱技术，实现攻击路径的精准溯源和攻击链的完整还原。

2.4　安全编排与自动化响应

研究并实现安全编排与自动化响应技术，根据智能决策引擎生成的安全态势评估结果，自动调整网络的安全策略，如调整路由规则、关闭风险链路、启动备份系统、隔离可疑设备等，实现对安全威胁的快速响应和有效处置。同时，安全编排与自动化响应技术应具备跨域协同、多层联动的能力，确保在网络全局范围内实现安全防护的统一指挥与协同作战。该技术能够显著提高网络安全运营的效率和效果，降低安全事件的响应时间和损失，增强网络的整体安全性。

3　IP网络安全态势感知量化模型构建[14-15]

3.1　模型构建目标

构建IP网络安全态势感知量化模型，旨在实现对网络整体安全状况的实时、准确、全面感知，为网络安全防护决策提供量化依据。该模型能够综合评估网络中各类安全要素的状态和变化趋势，将网络安全态势以量化指标的形式直观呈现，便于安全管理人员快速了解网络的安全状况，及时发现潜在的安全威胁，并制定相应的防护策略。

3.2　模型构建方法

量化模型构建基于层次分析法与模糊综合评价法。首先，明确安全态势要素，如网络设备运行状态、流量异常程度、系统漏洞数量、安全事件响应效率等，构建层次化目标体系。然后，结合专家经验与历史数据分析确定各要素权重，运用模糊综合评价法对网络安全态势进行量化评估，得出量化结果，直观反映网络整体安全态势的严重程度。

3.2.1　确定量化指标

依据网络安全特性，从网络设备、流量、系统、安全事件等维度选取多项量化指标，包括设备故障率、流量异常占比、漏洞修复率、安全事件响应时长等。各指标能从不同侧面反映网络安全态势，如设备故障率体现设备可靠性与稳定性，流量异常占比反映网络通信异常情况，漏洞修复率衡量系统漏洞管理与修复能力，安全事件响应时长体现安全事件响应效率。

3.2.2　收集数据并标准化处理

收集量化指标历史和实时数据，经清洗、去噪和标准化处理，消除量纲与数量级差异，统一数据格式与范围。采用Z-score标准化方法，将数据转换为无量纲、可比性强的形式，确保量化评估准确性与可靠性。

3.2.3　权重确定与量化评估

通过专家经验与层次分析法确定各量化指标在网络安全态势评估中的权重，构建判断矩阵，经一致性检验后计算权重向量。然后，采用模糊综合评价法结合权重向量与标准化数据，得出网络安全态势量化结果，为安全防护决策提供直观依据。

3.3　模型应用与优势

将量化模型应用于IP网络安全防护决策中，实时采集计算量化指标值，依据权重公式和量化模型计算网络安全态势量化结果，并将结果实时更新在安全态势展示界面上。同时，设置量化结果阈值，当超过阈值时，自动触发预警机制，及时提醒安全管理人员关注网络异常。该模型能全面量化网络安全状况，辅助科学决策，有效规避风险，因其直观性、系统性和及时

性，为IP网络安全防护决策提供有力支持，提升网络安全性与稳定性。

4 结论

4.1 研究成果总结

本文提出了一种基于IOC+TTP特征融合的检测模型和智能化攻击溯源知识图谱构建方法，并开发了相应的系统应用。通过深入研究和实验验证，主要取得了以下研究成果：设计并实现了一种融合IOC和TTP特征的APT攻击检测模型，该模型能够综合利用威胁情报和攻击者的行为特征，提高APT攻击检测的准确性和时效性，有效降低了误报率。提出了一种基于多源数据融合和深度分析的攻击溯源技术，构建了智能化攻击溯源知识图谱，该知识图谱能够全面、直观地展示攻击事件的全貌，包括攻击路径、攻击工具、攻击者与受害者之间的关系等，为安全人员进行攻击溯源和事件调查提供了有力支持。开发了一套适用于IP网络的APT攻击检测与溯源系统，该系统具有良好的可扩展性和易用性，能够与现有的网络安全防护体系进行有效集成，提供了丰富的功能模块和可视化展示界面，帮助安全人员快速响应和处置APT攻击事件，提升了网络安全防护的整体效能。

本文创新性地融合了IOC和TTP特征，打破了传统检测方法单一依赖IOC或TTP的局限，充分发挥了两者的优势互补作用，实现了对已知和未知APT攻击的全面检测，提高了检测的准确性和适应性。

4.2 研究展望

尽管本研究在APT攻击检测与溯源方面取得了一定的成果，但仍存在一些值得进一步研究和改进的方向。

a）检测模型的优化，随着APT攻击技术的不断演进和变化，需要持续优化检测模型，引入更多的先进算法和分析方法，提高对新型攻击技术和未知攻击变种的检测能力。

b）知识图谱的完善与扩展，攻击溯源知识图谱的构建还需要不断丰富和完善，增加更多的实体类型和关系类型，提高知识图谱的覆盖率和准确性。

c）性能优化与大数据处理，在面对大规模IP网络和海量安全数据时，系统的性能和处理效率仍然是一个关键问题，未来需要进一步研究大数据处理技术和分布式计算架构，优化系统的存储、计算和查询性能，以满足实时检测和快速溯源的要求。

在研究IP网络安全态势感知关键技术的漫漫长路上，虽已取得阶段性成果，但前方挑战重重。我们深知，网络安全领域的发展日新月异，攻击手段不断翻新，防护技术也需持续进阶。未来，我们将砥砺前行，深入探索未知，攻克技术难关，为守护IP网络的安全贡献力量，筑牢数字世界坚实防线，保障信息社会的稳定运行。

参考文献：

[1] 亚历山大·科特，罗伯特·F. 厄巴彻，克利夫·王. 网络空间安全防御与态势感知[M]. 北京：机械工业出版社，2019.
[2] 赵金龙，王海晋，张磊. 基于云计算安全的APT防御[J]. 数字技术与应用，2013(11)：177-177，179.
[3] 杨铭，王静，刘冰洁. 新形势下APT防御：挑战与策略研究[J]. 通信技术，2025，58(4)：448-456.
[4] 宋国宝. 面向APT的网络威胁情报知识图谱构建研究[J]. 软件导刊，2025，24(5)：179-185.
[5] 何厚翰，芦天亮，张岚泽，等. 多维度边优化溯源图改进的APT攻击检测方法[J]. 计算机科学与探索，2025，19(6)：1640-1655.
[6] 王岗，王韫皓，李伟. 基于SIEM的APT攻击防御体系建设实践[J]. 网络安全和信息化，2025(4)：117-119.
[7] 季一木，张嘉铭，杨倩，等. 高级持续性威胁检测与分析方法研究进展[J]. 南京邮电大学学报(自然科学版)，2025，45(1)：1-11.
[8] 张涛. 深度学习对抗网络攻击的应用策略研究[J]. 信息记录材料，2025，26(5)：211-213.
[9] 李海芳，路晓亚. 基于深度学习的计算机通信网络APT攻击检测方法[J]. 信息技术与信息化，2025(2)：3-6.
[10] 汪一帆，徐正国，陆路希. 采用双塔Transformer模型的APT攻击序列检测方法[J]. 信息工程大学学报，2025，26(2)：231-237.
[11] 杨秀璋，彭国军，刘思德，等. 面向APT攻击的溯源和推理研究综述[J]. 软件学报，2025，36(1)：203-252.
[12] 陈浩，方诗虹，马丹东，等. 基于溯源图的APT攻击检测[J]. 西南民族大学学报(自然科学版)，2025，51(1)：77-84.
[13] 宋恒嘉，胡志锋，郑轶，等. 基于网络安全的威胁情报系统设计与实现[J]. 网络安全技术与应用，2025(2)：1-2.
[14] 卯升团. 端点检测与响应技术在企业网络安全中的应用研究[J]. 网络安全和信息化，2025(4)：141-143.
[15] 王海晓. APT攻击环境下医院网络安全预警方法的优化研究[J]. 电脑知识与技术，2025，21(10)：86-88.

作者简介：
王新，毕业于北京航空航天大学，硕士，主要从事网络安全技术方向的研究工作；杨飞，毕业于合肥学院，高级工程师，学士，主要从事网络安全技术的研究工作；高存宇，毕业于黑龙江大学，学士，主要从事通信网络技术相关工作；郭翔乾，毕业于西安邮电大学，学士，主要从事网络安全规划和总师支撑工作；杨丽丽，毕业于合肥工业大学，学士，主要从事网络安全技术方向的研究工作。