doi: 10.3969/j.issn.1672-6073.2024.04.003

面向城市轨道交通典型应用场景的高级持续性威胁检测技术

张洪军，吕　默，高　阳
（中车长春轨道客车股份有限公司，长春 130062）

摘　要：为解决城市轨道交通场景下如何有效应对高级持续性威胁(advanced persistent threat，APT)这一难题，提出将攻击溯源图与深度流量学习相结合的方法，集成攻击重构与流量监控，实现对 APT 攻击的判断和检测。通过实验结果可知，该模型能够实现对 APT 攻击的有效溯源。与传统的基于机器学习的 APT 攻击检测模型比较，这种组合模型在检测准确率、精确度、召回率等指标方面具有明显的优势。

关键词：轨道交通；网络安全；APT 攻击；攻击溯源图；深度学习
中图分类号：U231　　**文献标志码：**A　　**文章编号：**1672-6073(2024)04-0016-08

Advanced Persistent Threat (APT) Detection Technology for Typical Application Scenarios in Urban Rail Transit

ZHANG Hongjun, LYU Mo, GAO Yang
(CRRC Changchun Rail Transit Co., Ltd., Changchun 130062)

Abstract: To address the challenge of effectively managing APT in urban rail transit scenarios, this paper proposes a method that combines attack source graphs with deep traffic learning. This integrated approach merges attack reconstruction with traffic monitoring to facilitate identifying and detecting APT attacks. Experimental results demonstrate that this model can effectively trace the sources of APT attacks. Compared to traditional APT attack detection models based on sandboxes or abnormal characteristics, this combined model significantly improves detection accuracy, precision, recall rate, and other performance indicators.

Keywords: rail transit; cybersecurity; APT attack; attack source map; deep learning

近年来，高级持续性威胁(advanced persistent threat，APT)以其目标针对性强、攻击链隐蔽性高、技术手段多样化和策略变化性强等特点，成为未来网络安全的首要威胁之一。随着我国城市轨道交通系统智能化水平的提高，网络安全问题日益突出[1]。轨道交通作为重大民生工程，近年来数次遭受黑客攻击。2022 年 4 月，央视焦点访谈曝光，上海某公司非法窃取我国高铁运行数据并提供给境外公司，两年间平均每月泄露 500 GB 数据。这些数据包括物联网、对讲通话和城铁信号专用网 GSM-R 的通信数据[2]。2020 年 7 月，“网络复仇者”组织针对以色列城铁 150 多台工业服务器发起了一系列网络攻击，影响了 28 座火车站和地铁站的运

收稿日期：2023-12-25　修回日期：2024-05-16
第一作者：张洪军，男，硕士，高级工程师，从事轨道交通车辆网络信息安全研究，013200020808@crrcgc.cc
通信作者：吕默，男，博士，高级工程师，从事轨道交通车辆网络信息安全研究，lvmo.ck@crrcgc.cc
基金项目：中国中车科技研究开发计划(2023CKA362-1)
引用格式：张洪军，吕默，高阳. 面向城市轨道交通典型应用场景的高级持续性威胁检测技术[J]. 都市快轨交通，2024，37(4)：16-23.
ZHANG Hongjun, LYU Mo, GAO Yang. Advanced persistent threat (APT) detection technology for typical application scenarios in urban rail transit[J]. Urban rapid rail transit, 2024, 37(4): 16-23.

营，包括耶路撒冷、特拉维夫大学和本古里安，且在攻击行动结束 6 d 后，由于设备和基础设施受到严重破坏，车站仍然无法正常运行[3]。2018 年 5 月，旅行网站欧洲铁路(Rail Europe)公司向客户发布通告，有黑客入侵了该公司的机票预订网站，窃取了大量敏感数据，对城铁信息服务系统造成了严重破坏[4]。如何对 APT 攻击事件进行有效防护已经成为全球范围内的一个热点而又棘手的问题。

城市轨道交通领域针对 APT 攻击检测的研究是一个相对较新的研究领域。通过借鉴已有研究提供的基本方法和策略，一些模型可以被应用于对城市轨道交通 APT 攻击的检测与防御。KOUR 等[5]使用扩展网络杀伤链(CKC)模型和工业控制系统(ICS)网络杀伤链进行 APT 行为建模，帮助轨道交通系统预测网络攻击并从中恢复。田小芳[6]开展了基于路径追踪的轨道交通系统 APT 攻击检测研究。该研究利用机器学习和深度学习技术，对轨道交通控制系统进行数据采集、特征提取、模型训练和预测等操作，实现了基于攻击路径追踪的 APT 攻击检测和防御算法。

本文在上述研究的基础上，针对城市轨道交通系统主要组成部分，如乘客信息服务数据、信号数据、车辆段、供电段和数据中心等信息安全防护问题，结合城市轨道交通系统网络业务场景，开展面向高级持续性威胁(APT)攻击的溯源及检测技术研究。在城市轨道交通领域首次提出基于组合模型的 APT 攻击检测技术路线、实施路径和 APT 整体防御方案。

1　APT 检测技术内涵

对 APT 攻击的检测主要面临三类挑战[7-8]：第一类是传统用于入侵检测的工具在收紧策略检测 APT 类型攻击时，会产生大量的超额误报，确认告警真实性往往需要进行人工核查，工作量巨大导致任务积压，最终造成告警风暴问题；第二类是攻击者可能利用 0day 漏洞发动攻击，0day 漏洞是指此前未被披露的漏洞，这种攻击行为难以被工具检测出来；第三类是在海量流量数据中观测 APT 攻击流量犹如大海捞针，业务流量与背景流量往往会淹没攻击流量。

对 APT 攻击的检测要克服上述三类挑战，需要深度结合轨道交通业务场景进行 APT 攻击建模，在典型场景的约束下展开攻击溯源分析和异常流量分析。轨道交通领域中应用 APT 攻击检测技术主要包括以下 3 个方面：①实时 APT 检测系统，适用于实时监测和快速响应的环境；②流量分析与时空关联算法，适用于处理轨道交通系统中复杂的网络流量，能够有效地从多种类型的流量中检测隐藏的 APT 攻击；③图形结构数据分析，图形结构数据的全局特征和灵活性有助于更精准地判断威胁和重构 APT 攻击。以下将详细描述基于城轨典型应用场景的 APT 检测平台构成与核心功能。

2　基于城轨典型应用场景的 APT 检测平台

基于城轨典型应用场景的 APT 检测平台由 4 部分组成，如图 1 所示。在典型场景模型中根据实际运营情况定义每个场景之间的业务接口，这些接口之间传递的可能是通信信息、设备实体或者人员信息。模型结合运营、检修规范对这些实际传递的要素进行规范性建模，为后续攻击溯源图的生成打下基础。

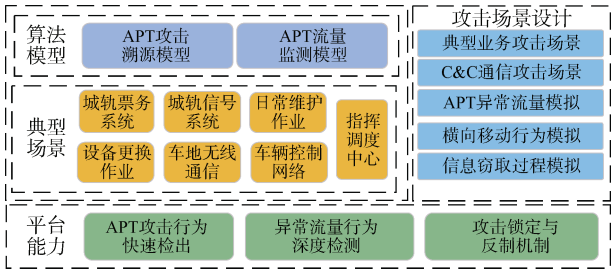

图 1　高级持续性威胁检测平台

Figure 1　APT Detection Platform

APT 检测平台设计了 4 类典型业务攻击场景：针对信号系统的信息窃取和瘫痪攻击；针对轨道车辆控制网络的信息窃取和瘫痪攻击；内部人员长期潜伏的信息窃取攻击；控制系统的供应链劫持攻击。

在这些场景中，通过模拟 APT 攻击的各种行为，结合攻击溯源图模型和流量检测模型预测攻击路径、进行攻击重构并且对异常流量进行判断和取证。

平台能力模块的主要功能是综合展示 APT 攻击态势，对 APT 攻击行为实现快速、准确的告警，以及通过预设的事件响应机制对攻击行为进行锁定和遏制。

平台核心算法模型为 APT 攻击溯源模型与 APT 流量检测模型。

3　城轨 APT 攻击溯源模型构建

基于攻击图的 APT 溯源技术在 APT 检测和分析中发挥着关键作用。APT 攻击溯源框架能够对恶意方进行归因，涵盖数据收集、威胁画像、入侵特征取证以及基于博弈论的动态响应等功能。通过图形化的攻击路径展示，帮助防御方揭示 APT 攻击的意图和目的；紧密结合场景，从管理、物理和技术三个层次理

解 APT 攻击与目标系统的整体互动行为，对后续攻击取证与网络安全配置调整提供整体策略图景[9-10]，APT 攻击溯源图模型构建如图 2 所示。

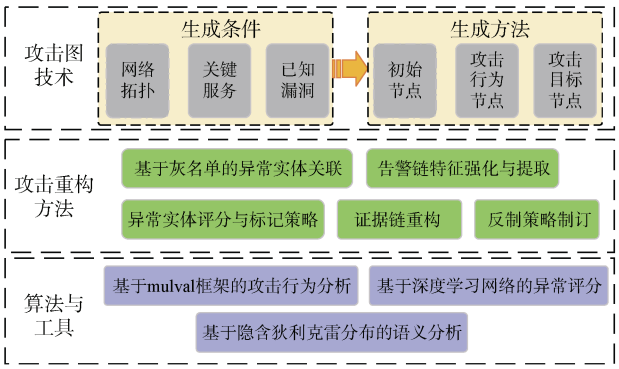

图 2 APT 攻击溯源图模型构建

Figure 2 Construction of APT attack source tracing graph model

3.1 基于典型攻击场景的攻击图

攻击图初始化分析包括轨道车辆目标网络的边界接口配置信息、内部拓扑信息、关键业务服务以及系统中的已知和潜在漏洞。这也涉及系统管理员和关键人员的账户信息，因为这些账户可能成为攻击者的主要攻击目标。此外，数据访问策略的详细信息，包括哪些用户和服务有权限访问关键系统组件，这也是至关重要的。这些信息节点还应包含对可能的攻击者特征的分析，例如他们可能利用的特定漏洞或针对城市轨道交通系统的已知攻击模式。攻击行为节点描述攻击者可能采取的具体技术和行动，包括但不限于钓鱼、社会工程学、漏洞利用，或通过物理接入点的入侵。这些节点还需要具体化攻击者在轨道交通各系统中可能采取的行动，如获得控制权、窃取敏感数据、破坏系统功能或造成系统瘫痪。攻击目标节点则集中在攻击者的最终目的，例如控制信号系统、获取敏感信息或造成城轨业务系统的功能障碍。生成 APT 攻击图的过程首先利用规则推理引擎分析攻击者可能的攻击行为，特别是在信号系统的具体环境中；然后根据攻击技术和阶段之间的关系，分析攻击行动的 APT 阶段。攻击行为分析主要基于 MulVAL 框架[11]的二次开发和规则编写进行，重点关注操作系统行为和城轨专用网络中各种组件的可能交互。

通过这种自顶向下的方法，APT 攻击图能够全面反映城市轨道交通系统面临的整体威胁，为网络信息安全保障提供了易于理解、业务聚焦的安全分析工具，帮助更好地理解和预防这类复杂和隐蔽的攻击。

3.2 攻击重构方法

本文应用基于攻击实体关联灰名单的攻击重构方法，排除正常或无关的实体，确保重点分析可能与攻击相关的实体。这种方法的核心在于两方面的实体筛选策略：首先，根据系统事件的频率异常程度，识别并排除在证据链分析中被判定为正常的系统实体；其次，依赖灰名单机制对出现在多次攻击中的实体进行关联分析，从而持续监控系统实体的安全状况。在这个过程中，通过应用隐含狄利克雷分布语义分析方法[12]，关联各个灰名单实体的 APT 告警序列与溯源框架提供的异常告警模型库进行深度遍历，提取最具价值的核心告警链。在此基础上结合目标网络边界、系统拓扑信息、数据收集偏好、告警语义特征等信息采用深度学习技术，确定从系统入口到出口的全部攻击链路分布特征，完成对轨道车辆网络目标系统 APT 攻击场景和攻击证据链的重建。

在这些证据链中，每个节点代表一个系统实体，而边则表示这些实体之间的系统调用关系。

此外，本研究从典型场景还原出发，通过评估事件的频率异常程度辨识良性系统实体，并将它们从证据链中剔除。这一筛选过程，收集每个攻击场景在特定时间窗口内的系统事件，并将这些信息存储在关系型数据库中。通过计算事件的发生频率得出每个事件的异常得分。这种方法可以减少由于实体筛选错误而对攻击影响范围评估不准确的情况发生，从而提高整个 APT 攻击重构过程的准确性和效率。通过这种综合的分析和筛选机制，能够更加准确地还原攻击过程，为网络安全团队提供关键的信息，从而制定更有效的防御策略和应急响应计划。

4 城轨 APT 攻击流量检测模型构建

轨道交通系统的复杂通信网络，负责控制信号、车辆调度以及提供乘客信息服务，成为 APT 攻击的潜在目标。APT 攻击者可能尝试窃取关键信息，如乘客数据和运营策略，或者企图干扰车辆调度和信号系统，从而导致严重的安全隐患和运营中断。APT 组织越来越倾向于使用无文件攻击技术，以规避基于样本的安全检测手段，这意味着在受控主机和目标网络中避免留下可识别的完整攻击武器样本。这导致传统安全检测手段，如端点检测与响应(EDR)和沙箱检测，在识别 APT 攻击时的有效性大幅降低。

在实际应用中，用户面临的主要问题是如何从海量误报中筛选出真正有分析价值的攻击线索。基于通

信数据包规则的检测方法也面临着误报率过高的问题。这是因为这种方法是基于特定通信数据包制定的规则，而在大流量环境中，很可能出现许多与制定规则一致的数据包，从而产生大量误报。同时，实时流量检测必须在通信会话活跃的短时间内生成告警结果，限制了其进行复杂和计算量大的分析，进而降低了这种基于通信数据包规则的检测方法的效果。

在这种背景下，识别轨道交通系统中的关键入口节点成为提高检测效率和准确性的先决条件。通过对这些已辨识的关键入口节点进行重点监控，可以集中资源对特定的通信数据包进行更深入的分析，从而有效降低误报率，并及时发现和阻止 APT 攻击。这种针对性的方法不仅提高了检测的准确性，也增强了系统的整体安全性。基于深度流量学习的 APT 攻击检测技术框架如图 3 所示。

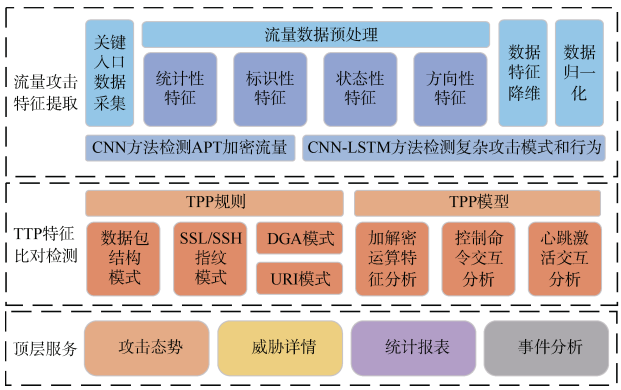

图 3　基于深度流量学习的 APT 攻击检测技术框架

Figure 3　APT detection technology framework based on deep traffic learning

4.1　针对攻击溯源图关键入口点的流量特征提取

在确定了这些关键入口节点之后，APT 流量特征分析的重点将转移到这些节点上。通过监控这些节点的网络流量，可以识别出与 APT 攻击相关的异常流量模式。例如，可能会发现在非运营时间内信号控制系统出现了异常的数据交换活动，或者车辆调度系统的网络流量出现了不寻常的增加。这些都是可能的 APT 攻击迹象。

基于网络流量进行 APT 攻击行为的描述，首先需要完成对目标网络全域的实时流量重建工作。这一工作需要依赖网络各个节点的镜像流量汇总和数据库层面的范式化处理。在轨道交通系统中，实时流量包括控制信号、车辆调度和乘客信息服务等关键数据。之后，可基于一些基本的流量特征，诸如预先定义的业务数据绝对流向、网络会话建立和连接时间、数据包计数与载荷长度的变化情况等进行特征提取。这些流量统计性特征作为关键的背景特征，是识别 APT 攻击的先决条件。尤其是在轨道交通系统中，由于其特定的数据交换模式和通信行为，这些特征更加明显。

对于本文所关注的 4 个 APT 攻击场景，可以通过判断信号控制命令的异常模式，如频繁的状态更改请求或非典型的远程操作命令判断城市轨道交通信号系统是否遭到了 APT 信息窃取攻击，这些攻击在流量上通常表现为非授权访问、异常信号指令传输或不寻常的数据包频率。针对轨道车辆控制网络的信息窃取攻击，通常会伴随非常规的控制数据包和非授权 IP 地址的访问尝试。利用流量标识性特征，如 PSH 值的分析，可以区分绝大部分正常业务流量与 APT 攻击流量。针对内部运维人员长期潜伏的信息窃取攻击和控制系统的供应链劫持攻击，这两种攻击模式仅在网络流量层面进行攻击，勘察能起到的效果非常有限，需要基于攻击溯源图技术完成威胁画像和攻击链重构后，再配合有针对性的异常流量勘察和取证判断 APT 攻击行为。

综上所述，流量背景特征的提取，有助于发现 APT 攻击进行中出现的与背景相冲突的传输方向或流量大小的异常波动。可利用卷积神经网络(CNN)检测 APT 加密流量[13]。CNN 通过图像识别方法对网络流量进行分析，能够有效识别出 APT 攻击的加密流量。这对于轨道交通系统尤其重要，因为攻击者可能会使用加密流量隐藏其恶意行为，从而绕过传统的安全监控机制。APT 攻击者通常应用 C&C 指令确认内部攻击链路存活，其指令潜伏模式多为低频短时连接模式，具有传输内容少的特点。与此相对的是，支持正常业务的信号控制和车辆运行流量的会话连接相对稳定，且流量整体的潮汐规律会根据具体应用场景产生变化，而 APT 攻击过程通常会因为与业务不存在共生关系而暴露在流量潮汐特征中。

针对 APT 攻击中内网横向移动与渗透攻击，可以提取东西向流量特征，在区分内部流量和外部流量后，采用混合深度学习方法，结合卷积神经网络和长短期记忆网络(CNN-LSTM)[14]方法检测复杂的攻击模式和行为。

4.2　基于 ATP 组织指纹特征的流量比对检测

TTP 特征是指 APT 组织在实施攻击过程中所展示的战术意图、技术能力和过程细节方面的特征。由

于攻击者很难在短时间内彻底更新攻击武器库和攻击人员，因此对特定的 APT 组织而言，TTP 特征的稳定性远远高于 IOC(indicators of compromise)特征，这意味着使用 TTP 特征作为检测依据将具有更高的成功率。

根据 MITRE 的 ATT&CK 模型，在攻击战术的“横向移动”“命令与控制”“信息渗漏”阶段，攻击者无法避免地产生大量网络通信数据。这三个战术阶段的 TTP 特征非常适合构造流量侧检测方法。

具体的技术路线包括将适合作为流量检测的 TTP 特征转换为 TTP 规则和 TTP 模型两部分。TTP 规则用于可疑通信会话的初筛，具体规则例如数据包结构模式、URI 模式、DGA(domain generation algorithm)模式、SSL/SSH 指纹模式等。例如，通过分析 SSL/SSH 通信中的加密模式和密钥交换协议，可以揭示潜在的 APT 活动。DGA 模式分析则有助于识别攻击者为绕过防御系统而生成的随机域名。

TTP 模型通过具体的会话分析插件，针对已经落盘的可疑单个或多个会话的全流量，完成流程复杂和具有一定计算量的分析过程。这些模型包括数据加密特征分析、加解密运算、控制命令交互分析、心跳激活交互分析等。

经过 TTP 规则初筛和 TTP 模型验证产生的告警，其具有非常低的误报率。这种方法的应用，特别是在全流量溯源系统的支持下，使得对 APT 攻击的复杂网络通信进行深入分析成为可能，从而有效提升了对 APT 攻击的检测能力和准确性。

基于组合深度学习的 APT 攻击识别架构如图 4 所示。

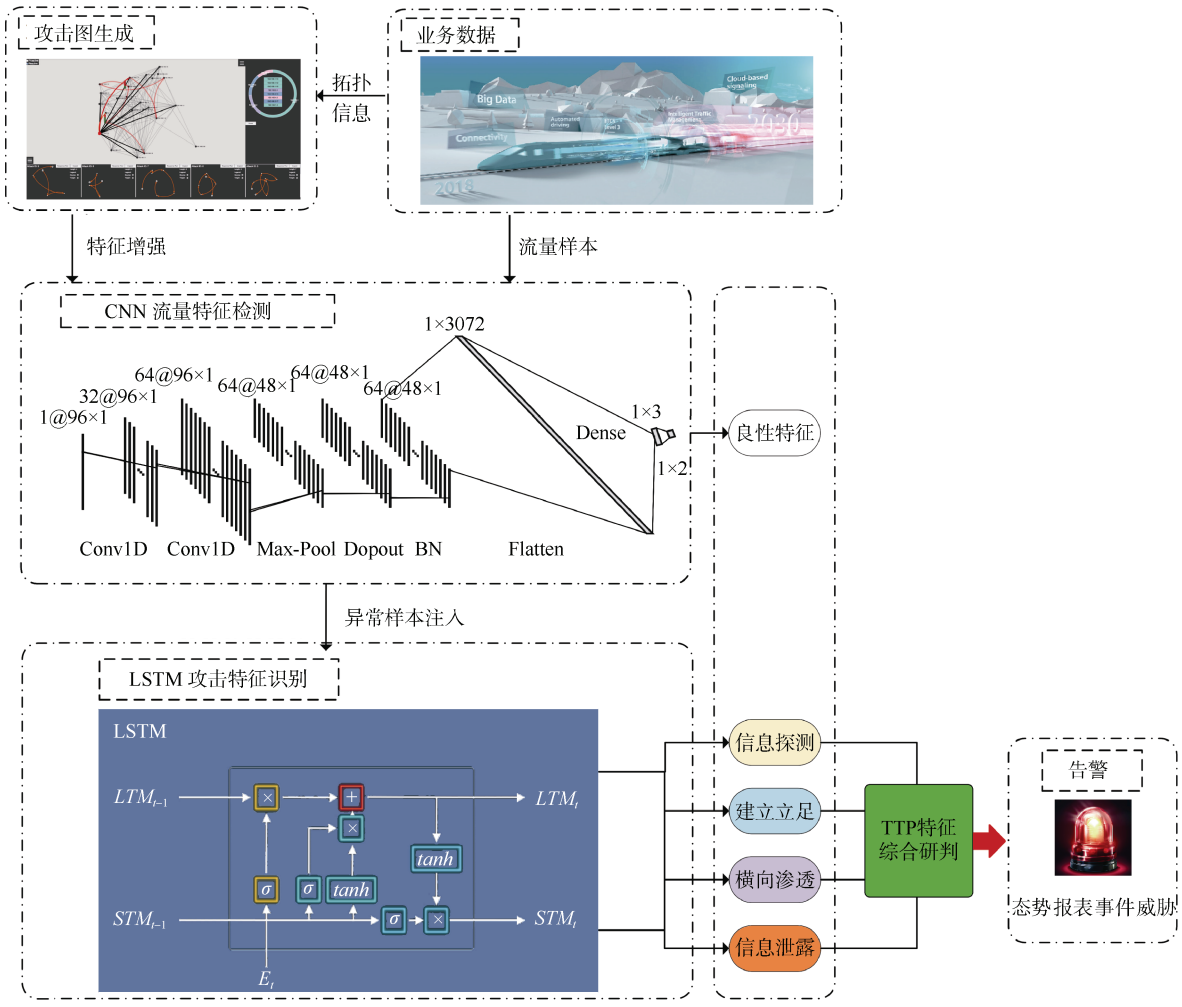

图 4　基于组合深度学习的 APT 攻击识别架构

Figure 4　APT detection framework based on hybrid deep learning

输入模型的数据需经过数据预处理，对相似流量进行合并与归一化。经过预处理后的流量数据集将作为 CNN 检测模型的训练输入。同时将攻击图作为特征强化参数与流量数据一同进行学习，极大地缩减 APT 攻击特征的发散性，一定程度上解决了数据集存在的异常不平衡问题。CNN 一维卷积包括 48 个卷积核，具有最大池化层用于增加泛化性，防止出现过拟合的 Dropout 层与用于加速收敛的批数据标准化(BN)层，使用 Sigmoid 非线性激活函数预测正常与异常类别。

模型第二阶段的 APT 攻击识别将用于从威胁流量数据中区分属于不同攻击阶段的攻击流量。本文采用基于长短期记忆网络 LSTM 模型作为识别模型。在模型完成攻击阶段分类后，再通过 TTP 特征对比检测，进一步确认 APT 攻击的真实性以及威胁性，减少误报率。

5 实例分析

本实验采用的 DAPT 2020[15]网络流量数据集是最新的用于检测 APT 攻击的开源数据集，可以在目标模拟环境中收集的流量标记为业务流量或各个 APT 攻击阶段的特征流量。

模拟持续 7 d 的 APT 攻击过程整体流量作为测试数据。具体过程为：首先模拟目标网络的正常行为流量数据和行为日志(第 1～3 d)，然后模拟在第 4～7 d 时间内收集到的包含 APT 攻击流量和信息的数据。为了便于后续实验对 APT 攻击的溯源和重构，模拟攻击行为涵盖针对城市轨道交通信号系统的信息窃取和瘫痪攻击；针对轨道车辆控制网络的信息窃取和瘫痪攻击；内部人员长期潜伏的信息窃取攻击以及控制系统的供应链劫持攻击 4 个攻击场景。每个场景的 APT 攻击数据都包含了所有的攻击步骤。来自各个网络控制终端的系统日志中混合了 APT 攻击行为与正常行为日志，并且模拟了真实情况下 APT 攻击日志的占比[16]。

表 1　数据集信息表

Table 1　Data set information table

序号	数据集描述
1	针对场景一的 DAPT 2020 系统日志与目标网络模拟流量(第 1～3 d、第 4 d)
2	针对场景二的 DAPT 2020 系统日志与目标网络模拟流量(第 1～3 d、第 5 d)
3	针对场景三的 DAPT 2020 系统日志与目标网络模拟流量(第 1～3 d、第 6 d)
4	针对场景四的 DAPT 2020 系统日志与目标网络模拟流量(第 1～3 d、第 7 d)

本文对原始数据进行了有条件的数据流合并降低其复杂度，避免其干扰对攻击路径的判断。合并的条件是如果在一个时间窗口内(20 s)，一个会话进行了多次数据交换，则将该时间内的同类型流量数据做合并。合并的原则是源地址、目的地址以及标签是相同的。数据经过重组与去重后可以得到一个新的适合实验的数据集，如表 2 所示。DAPT 2020 数据集经过合并与去重后总计有 8 112 条记录。其中与 APT 攻击相关的记录共计 1 117 条，最小类别为数据泄露阶段记录，为 28 条，约占 0.34%。

表 2　数据集概况

Table 2　Data set overview

数据标签	数量	占比/%
良性(benign)	6 995	86.20
侦察(reconnaissance)	758	9.34
建立立足点(establish foothold)	201	2.47
横向渗透(lateral movement)	130	1.60
数据泄露(data breach)	28	0.34
总计	8 112	100

采用 7∶2∶1 的比例对重组后的数据集进行分割，并且通过随机打乱确保 APT 攻击各阶段平均分布在训练、验证与测试集中。

实验测试环境为 HDP2.6.5 版本的大数据处理平台，提供 6 节点，16 核 2.4 GHz 处理能力，内存为 16 GB/node，存储空间为 2 TB。采用 Python 编程工具实现对网络抓包并对数据包进行上述的网络行为检测。

为了验证本文模型对于 APT 攻击威胁检测的准确率与高效性，本文采用 MLP、LSTM、随机森林等主流机器学习模型进行对比实验，基于正负样本评价指标，以准确度(Accuracy rate)、精确度(Precision rate)、召回率(Recall rate)和 F1 评分(F1-Score)衡量 APT 攻击检测模型的整体性能。

正负样本评价指标具有如下定义：

1) 真阳性数据(TP)：也称检出样本，意为被正确归类为攻击样本的样本。

2) 假阳性数据(FP)：也称误报样本，意为被错误归类为攻击样本的正常样本。

3) 真阴性数据(TN)：也称正常样本，意为被正确归类为正常样本的样本。

4) 假阴性数据(FN)：也称漏报样本，意为被错误归类为正常样本的攻击样本。

根据正负样本评价指标得出的评价公式分别为

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{1}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{2}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{3}$$

$$\text{F1-Score}=2\cdot\frac{\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}} \tag{4}$$

本文模型同 MLP、LSTM、随机森林等主流机器学习模型进行识别结果横向对比如图 5 所示。APT 攻击各阶段各个模型横向对比如表 3 所示。

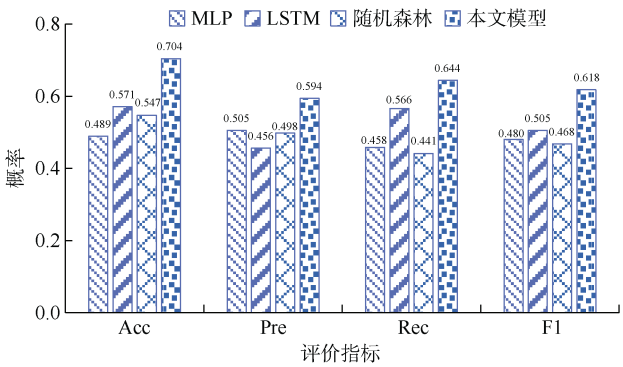

图 5　不同模型与 CNN_LSTM 性能对比

Figure 5　Performance comparison chart of different models and CNN_LSTM

表 3　APT 攻击各阶段横向对比

Table 3　Comparison of model performance at each stage of the APT attack

类别	模型	准确度/%	精确度/%	召回率/%	F1 评分
良性	CNN_LSTM	98	98	99	0.98
	MLP	98	98	99	0.98
	LSTM	98	98	99	0.98
	随机森林	97	98	99	0.98
侦察	CNN_LSTM	98	97	99	0.98
	MLP	98	94	94	0.94
	LSTM	98	96	95	0.95
	随机森林	98	97	92	0.94
建立立足点	CNN_LSTM	98	99	99	0.99
	MLP	97	98	98	0.98
	LSTM	98	99	99	0.99
	随机森林	97	99	98	0.98
横向渗透	CNN_LSTM	88	81	83	0.82
	MLP	73	80	68	0.74
	LSTM	82	71	78	0.74
	随机森林	90	79	66	0.72

续表

类别	模型	准确度/%	精确度/%	召回率/%	F1 评分
数据泄露	CNN_LSTM	85	78	8	0.79
	MLP	72	70	74	0.72
	LSTM	74	69	78	0.73
	随机森林	66	67	75	0.71

实验结果表明，由 CNN 与 LSTM 组成的模型在改造的 DAPT 2020 数据集上进行的 APT 攻击检测能力整体优于其他模型。在针对未知威胁的异常检测中总体召回率为 64%，相较其他机器学习方法提升了约 20%。即使数据集中的正常样本和攻击样本之间存在严重的不平衡的问题，本文提出的模型也可以实现对 APT 攻击的有效侦测。这说明深度学习组合模型对于提取 APT 攻击流量特征方面是有效的。从 APT 攻击各阶段横向对比表中可以观察到，本文提出的模型对数据泄露判断相较于其他模型有较大的优势，而对横向渗透的检测能力与其他模型相比并无明显的优势。

6　结论

本文在深度结合城市轨道交通典型业务场景的前提下，提出将攻击溯源图与深度流量学习相结合的方法，集成攻击重构与流量监控，实现对城市轨道交通 APT 攻击的判断和检测。该方法首先依据威胁画像、系统日志和业务风险评级策略构建攻击溯源图，在此基础上使用深度流量学习网络提取时间和业务跨度较大的关键节点异常流量。

通过实验结果分析可知，该模型能够实现对 APT 攻击的溯源、重构、检测与取证。并且，该模型在综合检测能力方面比单一的机器学习模型在准确度、精确度、召回率和 F1 评分方面都具有全面优势。

针对 APT 攻击的行为检测与重构在未来有着巨大的发展潜力，需要紧跟攻击技术的最新发展，持续投入资源对检测机制和方法进行深入的研究。

近年来，随着云存储技术和基于特征的数据实时压缩技术的出现，未来 APT 的攻击行为将更加贴近正常业务模式。需要具备更细粒度的信息收集能力才能够提高检测的精度，从系统级深入到应用级，降低误判率。基于图的结构化描述方法在保留了数据全局特征的同时，具备扩展和解释能力强、场景贴合度高、模型灵活度高等特点，这有助于预测 APT 威胁并对 APT 攻击态势作出更符合业务全局的判断。然而，这种方

案会带来较高的性能要求和系统开销，如何克服这一问题仍需不断探索。最后，APT 威胁检测模型需要对相当长时间跨度内的数据进行采集、清洗、存储和特征分析。这种分析模式可能带来判断滞后和事件响应能力不足的问题。并且，系统每天生产的海量关键数据和关联特征，如何在保证长期记录准确的基础上，引入多阶段感知注意力机制，提升系统敏感性是一个需要持续研究的课题。

参考文献

[1] 周淑辉，常振臣，张尧，等. 列车网络系统的网络安全分析与安全防护[J]. 城市轨道交通研究，2020，23(2)：84-87.
ZHOU Shuhui, CHANG Zhenchen, ZHANG Yao, et al. Safety analysis and protection of railway train network system[J]. Urban mass transit, 2020, 23(2): 84-87.

[2] 央广网. 上海一公司向境外出售高铁数据：一个月采集信号数据达 500 个 G[EB/OL]. (2022-04-15)[2023-02-25]. http://www.takungpao.com/news/232108/2022/0415/709032.html.

[3] 安全内参. 盘点：2020 年轨道交通典型网络攻击事件. [EB/OL]. (2020-12-21)[2023-02-25]. https://www.secrss.com/articles/28099.

[4] 全球多行业重大网络安全事件大盘点. [EB/OL]. (2022-01-01)[2023-02-25]. https://zhuanlan.zhihu.com/p/334990851.

[5] KOUR R, THADURI A, KARIM R. Railway defender kill chain to predict and detect cyber-attacks[J]. Journal of cyber security and mobility, 2020, 9(1): 47-90.

[6] 田小芳. 基于路径追踪的轨道交通系统 APT 攻击检测研究[J]. 网络空间安全，2023，14(3)：85-90.
TIAN Xiaofang. Research on APT attack detection in railway transportation systems based on path tracking[J]. Cyberspace security, 2023, 14(3): 85-90.

[7] HASSAN W U, BATES A, MARINO D. Tactical provenance analysis for endpoint detection and response systems[C]// 2020 IEEE Symposium on Security and Privacy (SP). San Francisco: IEEE, 2020.

[8] BODSTRÖM T, HÄMÄLÄINEN T. A novel deep learning stack for APT detection[J]. Applied sciences, 2019, 9(6): 1055.

[9] LUO Zhiyong, YANG Xu, LIU Jiahui, et al. Network Intrusion Intention Analysis Model Based on Bayesian Attack Graph[J]. Journal on communications, 2020, 41(9): 160-169.

[10] LI Heng, WANG Yongjun, CAO Yuan. Searching forward complete attack graph generation algorithm based on hypergraph partitioning[J]. Procedia computer science, 2017, 107: 27-38.

[11] 李红娇，何文豪，李晋国. 基于MulVAL改进的漏洞风险评估框架[J]. 上海电力大学学报，2021，37(6)：557-562.
LI Hongjiao, HE Wenhao, LI Jinguo. An improved vulnerability assessment framework based on MulVAL[J]. Journal of Shanghai University of Electric Power, 2021, 37(6): 557-562.

[12] CHAUHAN U, SHAH A. Topic modeling using latent dirichlet allocation: a survey[J]. ACM computing surveys, 2021, 54(7): 145.

[13] XU Junfeng, LIN Weiguo, FAN Wenqing. APT encrypted traffic detection method based on two-parties and multi-session for IoT[EB/OL]. http://arxiv.org/abs/2302.13234.

[14] ALREHAILI M, ALSHAMRANI A, ESHMAWI A. A hybrid deep learning approach for advanced persistent threat attack detection: Proceedings of the 5th international conference on future networks and distributed systems[C]. Dubai, United Arab Emirates, 2021.

[15] MYNENI S, CHOWDHARY A, SABUR A, et al. DAPT 2020-constructing a benchmark dataset for advanced persistent threats: International Workshop on Deployable Machine Learning for Security Defense. [C]. Cham: Springer, 2020.

[16] 刘扬. 高级持续性威胁攻击检测关键技术研究[D]. 哈尔滨：哈尔滨工程大学，2022.
LIU Yang. Research on key technologies of advanced persistent threat attack detection[D]. Harbin: Harbin Engineering University, 2022.

[17] 刘嘉，谢冰，杨传旭，等. 基于网络行为自学习的高级持续性威胁检测技术研究[J]. 计算技术与自动化，2019，38(2)：108-113.
LIU Jia, XIE Bing, YANG Chuanxu, et al. Research on advanced continuous threat detection technology based on network self-learning behaviors[J]. Computing technology and automation, 2019, 38(2): 108-113.

（编辑：王艳菊）