基于深度学习的工业互联网异常流量检测与入侵响应研究

韩 彬，杨晓雾

（武警保定支队勤务保障大队信息保障站，河北 保定 071000）

摘 要 从工业互联网安全防护实际需求出发，开展基于深度学习的异常流量检测与入侵响应对策研究，对遏制网络攻击、保障生产安全、维护产业链稳定具有重要意义。当前，工业互联网面临设备防护薄弱、攻击手段迭代等安全困境，传统检测方法已难以适配其“人、机、物”协同的开放特性。通过剖析深度学习技术在特征提取、模式识别上的优势，结合工业互联网流量特点，从检测框架构建、模型优化、响应机制完善等维度，提出系统化解决方案，以期为提升工业互联网安全防护的智能化与精准化水平提供借鉴。

关键词 深度学习；工业互联网；异常流量检测；入侵响应；网络安全

中图分类号：TP3 **文献标志码**：A **DOI**：10.3969/j.issn.2097-3365.2026.11.010

0 引言

工业互联网是将工业领域的设备、传感器、机器和系统通过互联网连接起来，实现数据交换、信息共享和智能化管理的应用生态，是未来全球制造业发展的重要基石。但与此同时，工业互联网遭到的网络攻击愈加严重[1]。深度学习技术凭借强大的自主学习与模式识别能力，为工业互联网安全防护提供了新路径。基于此，聚焦基于深度学习的工业互联网异常流量检测与入侵响应展开研究，可为工业互联网高质量发展提供安全支撑。

1 基于深度学习的工业互联网面临的安全挑战

1.1 工业互联网自身特性引入的安全挑战

工业互联网“人、机、物”协同的开放互联特性，是其安全挑战的主要来源，在提升生产效能的同时，也让安全风险显著增加。传统工业系统多处于封闭可信环境，攻击面有限，而工业互联网的开放性，使得大量制造资源直接暴露在网络空间，易被外部攻击者触达利用。其接入设备种类繁杂、规模庞大，多数工业控制终端计算资源不足，原生防护能力薄弱，部分设备甚至无基础防护，难以抵御恶意攻击[2]。工业互联网对实时性、可靠性要求极高，系统中断或控制指令篡改，不仅会导致生产停滞，还可能引发设备损坏、人员伤亡等严重后果。此外，平台连接海量系统、承载核心数据，针对关键节点的攻击会快速扩散至全产业链，进一步放大安全隐患，给企业带来不可估量的损失。

1.2 深度学习模型在训练阶段面临的安全威胁

深度学习模型训练阶段的安全威胁主要集中在数据和模型层面，其中投毒攻击与模型逆向攻击危害最为突出，直接影响模型可用性与安全性。投毒攻击通过恶意篡改训练数据，破坏模型决策逻辑或植入隐蔽后门。例如：攻击者操纵传感器测量值，导致设备故障检测器在特定场景下失效，造成生产异常漏报。后门攻击作为投毒攻击的特殊形式，会在训练数据中植入不易察觉的触发器，使模型正常输入时表现正常，遇到触发器则输出错误结果，隐蔽性强且常规测试难以发现。模型逆向攻击通过分析模型输出或获取参数，推断训练数据中的敏感信息，而工业互联网训练数据多包含商业机密，此类攻击会导致核心知识产权泄露，破坏企业竞争力。

1.3 深度学习模型在预测阶段面临的安全威胁

深度学习模型进入预测阶段后，安全威胁主要围绕输入干扰、模型窃取和物理欺骗展开，直接影响工业生产的准确性与安全性。对抗性攻击最为常见，通过向输入数据添加人眼难以察觉的微小扰动，诱导模型输出错误结果，如质量检测系统误判次品为合格品，或传感器读取异常触发错误控制指令，影响生产质量与安全。模型提取攻击针对模型知识产权，攻击者通过反复调用模型API，分析输入输出对应关系，复现功

作者简介：韩彬（1984-），男，本科，助理工程师，研究方向：网络安全。

能相近的替代模型，给企业投入大量资源训练的工业模型带来巨大的经济损失[3]。物理欺骗攻击操作简单、难以追踪，通过改变现实物体属性欺骗模型，如在工业产品上添加微小标记导致检测误判，对依赖视觉识别和传感器数据的工业自动化系统构成严峻挑战。

1.4 大模型等新技术应用带来的潜在风险

大模型为工业互联网安全赋能的同时，也从实时性、成本、可靠性等方面带来新型潜在风险，制约其实际应用价值。在实时性方面，大模型流量检测速度无法满足工业场景高实时要求，且误报率较高，影响威胁判断准确性，多数实时检测任务仍需依赖传统小模型或规则引擎。在成本层面，大模型训练与推理需消耗海量算力，如训练 650 亿参数的模型需上千块 GPU 连续运算数周，高昂成本让资源敏感型工业环境难以普及。同时，大模型“黑盒”特性导致决策过程不可解释，生成结果可信度不稳定，直接用于安全运营或控制决策，可能引发生产安全事故。

2 基于深度学习的工业互联网异常流量检测的必要性

2.1 应对工业互联网安全态势的现实需求

工业互联网高速发展的同时，早已成为网络攻击的核心目标，勒索软件、供应链攻击、挖矿攻击等新型安全威胁持续高发，再加上人工智能技术推动攻击手段不断迭代升级，工业互联网安全防御的难度陡增。在此背景下，基于深度学习的工业互联网异常流量检测技术成为应对当前安全态势的关键。它能深度分析海量网络流量数据，自动识别异常攻击模式，及时挖出潜在安全隐患，有效防范数据泄露、生产中断等风险，而构建高效的异常流量检测机制，既是提升工业互联网整体防护水平、保障其稳定运行的现实刚需，更是维护关键基础设施安全、筑牢国家经济安全防线的必然要求。

2.2 弥补传统检测方法应对新型威胁的局限性

传统工业互联网入侵检测系统大多依靠预定义规则库或浅层机器学习模型开展工作，场景适配性差，难以有效识别未知攻击与变种威胁，尤其是在加密流量解析、低频攻击捕捉、跨域渗透监测这些复杂场景中，其短板愈发明显，识别精度低、误报率高，严重影响实际检测效果[4]。基于深度学习的异常流量检测技术恰好能弥补这些不足，破解传统方法应对新型安全威胁的技术瓶颈，它具备强大的自动特征提取能力，不用依赖专家知识进行人工特征工程，可直接从原始流量数据中自主学习复杂的时空特征，大幅提升对新型威胁的识别能力。

2.3 深度学习适配异常流量检测的技术优势

相较于传统检测技术，深度学习处理工业互联网异常流量数据的优势十分突出。其一，支持无监督或半监督学习模式，能直接从非结构化流量数据中提取高维特征，有效解决工业场景中标记样本稀缺、数据分布不平衡的行业痛点；其二，大幅降低对专家经验的依赖，如变分自编码器与 Transformer 相结合的检测方法，不用人工标注样本，就能精准识别加密流量中的异常模式；其三，泛化能力强，能灵活适配不同工业场景的流量特征，依托端到端学习框架，捕捉人工分析难以察觉的细微流量异常，实现对网络攻击的精准前置预警。

2.4 契合智能化安全运营与合规性建设要求

基于深度学习的异常流量检测技术，是工业互联网实现智能化安全运营、满足行业合规性要求的必由之路。它能推动网络安全防护实现实时威胁发现、动态信任评估、自动响应处置的全流程闭环管理，助力企业构建主动防御体系，如融合零信任架构的深度学习检测方案，可通过动态信任分级与持续行为监测，实现对跨域流量的精细化管控，有效阻断网络攻击的横向渗透路径，而深度学习驱动的异常流量检测，不仅能大幅提升企业安全运营的效率与水平，还能为企业合规性建设提供坚实的技术支撑。

3 基于深度学习的工业互联网异常流量检测与入侵响应对策

3.1 构建融合时空特征与工业协议解析的智能检测技术框架

传统检测方法在协议理解、时空特征提取上存在明显不足，核心对策是构建智能检测框架，实现从流量统计到行为分析的升级，让检测更贴合工业场景需求。该框架核心为 CNN 与 GRU 异构神经网络模型，CNN 专注提取数据包字节序列、协议字段中的局部空间特征，GRU 则捕捉流量时间维度的依赖关系，一静一动间既能识别周期性通信异常与指令偏离，又能兼顾局部特征与动态变化，让特征提取更全面[5]。

为赋予模型工业场景上下文理解能力，可内嵌多种主流工业协议解析模块，吃透功能码语义、寻址逻辑与正常交互模式，避免仅靠流量表象判断，大幅减少误判。针对异常样本稀缺的数据不平衡问题，需引入动态焦点损失函数让模型重点关注难分类异常样本，采用 GAN 过采样技术合成代表性少数类样本，提升低频攻击识别灵敏度。同时，采用无监督学习与有监督微调的混合范式，先在大量未标注流量中学习正常行为，再针对特定异常优化，这种方式能增强模型在复

杂工业场景下的泛化性与鲁棒性，适配不同工业领域的差异化流量特征，为后续入侵响应奠定坚实的基础。

3.2 设计数据预处理与模型优化方案以提升检测效能

高效检测离不开高质量数据与轻量化模型，针对性设计数据预处理流程与模型优化方案，在检测精度与实时性之间找到最佳平衡点。工业互联网流量来源复杂，易掺杂各类无效信息，数据质量直接影响检测效果，因此数据预处理环节必须全面细致。预处理过程中，先利用 DPI 技术还原会话上下文，提取源 / 目的 IP、工业协议功能码、通信时序等关键元数据，筛选剔除无关冗余信息，再通过标准化消除量纲影响，将离散协议字段转化为神经网络可处理的嵌入向量，彻底清理噪声、缺失值与非标准化数据，确保输入模型的数据规范、有效，为精准检测筑牢数据根基。

模型优化聚焦实时性提升，采用剪枝技术移除冗余连接降低计算复杂度，通过量化操作将浮点权重转化为低精度定点数减少内存占用与能耗，实现边缘节点轻量化部署，完美适配工业现场边缘设备资源有限的场景。此外，建立模型动态更新机制，通过增量学习融入新流量模式，适应设备入退网、工艺调整带来的分布漂移，及时适配场景变化，确保持续稳定的检测效能，满足工业生产对安全检测的实时性与可靠性需求。

3.3 建立基于威胁情报的智能入侵响应与闭环管理机制

异常检测只是安全防护的起点，关键在于构建与威胁情报联动的智能响应体系，形成闭环管理，真正实现主动防御。可建立“检测、响应、评估、优化”的自治循环机制，打破检测与响应脱节的困境，让安全防护更具主动性与连贯性。当深度学习模型识别出可疑流量，会立即自动关联内外部威胁情报库，核查恶意 IP 信誉、漏洞利用特征，精准评估事件严重等级，再结合工业生产优先级明确处置顺序，避免因盲目响应影响正常生产，实现安全与生产的协同推进。

针对不同等级威胁，建议触发差异化响应，高危攻击实时阻断连接、隔离失陷设备以快速遏制攻击扩散，潜在渗透行为则启动攻击链路还原，利用知识图谱关联多源日志，可视化展示攻击路径与影响范围，为工作人员精准处置提供有力支撑。同时，定义响应时长、误阻断率、业务恢复时间等量化指标，全面评估响应效果，借助强化学习算法，根据历史处置经验动态优化响应策略、完善响应流程，通过闭环管理，系统既能提升事件处置效率，又能持续学习新型威胁特征、积累处置经验，增强自适应能力，适配不断变化的安全态势。

3.4 构建协同防护体系并强化模型自身安全

单一检测节点易被绕过，且深度学习模型自身存在安全隐患，这两大短板需通过构建协同防护体系、强化模型自身安全来补齐，筑牢工业互联网安全最后一道防线。工业互联网涉及云、管、边、端多个层面，单一节点防护存在明显漏洞，各类攻击可通过跨域渗透突破防护，因此协同防护至关重要。对策主要分为两方面：一方面，构建“云、管、边、端”协同纵深防御体系，在工厂现场层、监控层等不同区域部署差异化检测模型，边缘侧重实时轻量检测以快速处置现场突发威胁，云端聚合多分支数据开展深度分析与威胁狩猎，挖掘潜在跨域威胁，同时融入零信任理念，对所有跨域流量进行动态信任评估与强制访问控制，遏制横向渗透，形成多层级、全方位的防护格局；另一方面，强化模型自身安全，深度学习模型易遭受对抗攻击、数据投毒等威胁，直接影响检测可靠性，对此采用多种技术手段加固，通过对抗训练引入扰动样本提升模型抗干扰能力，利用差分隐私技术添加噪声防止数据泄露，定期开展安全审计排查隐蔽攻击、修复安全漏洞，最终通过融合零信任架构与模型加固技术，有效免疫对抗性样本，降低模型误判率，确保检测系统可靠运行，守护工业互联网安全。

4 结束语

深度学习技术能够有效突破传统检测方法的局限，精准识别工业互联网中的异常流量与恶意入侵，提升安全防护的智能化水平。在复杂工业环境下，其自适应学习能力可大幅降低误报率，增强对未知威胁的感知与响应能力。未来，可进一步优化模型轻量化部署效果，提升极端场景下的检测实时性，同时探索大模型与工业互联网安全防护的深度融合，持续完善智能防护体系，为工业互联网安全稳定运行提供更坚实的技术保障。

参考文献：

[1] 王阳,谭振江.生成对抗网络赋能工业互联网入侵检测研究 [J].福建电脑,2025,41(12):1-8.
[2] 何承润,闫皓楠,侯志青,等.面向工业互联网的恶意流量智能检测模型 [J].移动通信,2025,49(05):49-56.
[3] 支祖利.深度学习算法在工业互联网入侵检测中的应用研究 [J].现代工业经济和信息化,2024,14(07):77-79.
[4] 胡向东,张婷.基于时空融合深度学习的工业互联网异常流量检测方法 [J].重庆邮电大学学报(自然科学版),2022,34(06):1056-1064.
[5] 邓华伟,李喜旺.基于深度学习的网络流量异常识别与检测 [J].计算机系统应用,2023,32(02):274-280.