基于深度学习的 5G 网络入侵检测系统研究

黎恒光　曾杰祥　黄良浔　庞斯匀 *
南宁师范大学　南宁　530100

摘　要：目的：探讨 5G 网络在工业互联网与远程医疗等行业的应用场景，因架构复杂、终端多样、业务开放面临的架构、终端接入、数据传输、业务应用四类安全威胁，以及传统入侵检测方法（特征码检测、异常行为检测、协议分析）存在检测准确率低、实时性差、泛化能力弱的问题，构建响应 5G 网络安全挑战的入侵检测体系。方法：深入审视 5G 网络技术的特性及其潜在的安全挑战，指明传统方法的局限；再构建含数据采集、预处理、特征提取、深度学习检测、响应处置的系统架构，采用 CNN-LSTM-AE 模型实现多特征的整合，结合 HDFS 分布式存储、Spark 分布式计算及数据采样等实时性优化技术提升性能；对 UNSW-NB15 和 CSE-CIC-IDS2018 数据集进行分析，从准确率、实时性、泛化能力维度与传统及单一深度学习模型对比。结果：该系统在 UNSW-NB15 数据集准确率达 98.2%，CSE-CIC-IDS2018 数据集达 97.5%；该检测的平均时延值介于 0.8 到 1.2 毫秒，跨数据集准确率下降仅 1.8-2.3 个百分点，整体表现略胜一筹于对比模型，结论：该系统在 5G 网络安全威胁面前展现强大应对力，为 5G 网络安全稳定运行提供技术支撑。

关键词：5G 网络；网络安全；入侵检测系统；深度学习

1 引言

信息技术的迅猛进步，5G 网络以其卓越的带宽、极低的延迟和庞大的连接能力著称，逐渐成为支撑工业互联网、智慧城市、远程医疗等新兴领域的核心基础设施，5G 网络架构的复杂性、终端接入的多样性以及业务场景的开放性，网络安全所面临的挑战变得愈发严峻。传统的入侵检测方法在应对 5G 网络中新型、隐蔽且高速的攻击时，呈现出检测精度不高、响应速度迟缓、泛化能力较弱的问题，无法跟上 5G 网络安全防护的步伐，深度学习技术凭借其强大的特征提取和复杂模式识别能力，深度学习技术为 5G 网络入侵检测难题的破解注入了新的活力，实施深度学习驱动的 5G 网络安全防护系统研究，对于保障 5G 网络安全稳定运行、推动数字经济健康发展具有重要的理论意义和实际应用价值。

2 5G 网络的特点及面临的安全风险

2.1 5G 网络的主要特点

对比早期的 2G、3G、4G 技术，网络结构、技术特色与应用场景方面均显现出显著差异，就网络架构而言，5G 技术采用软件定义网络（SDN）与网络功能虚拟化（NFV）技术作为其核心技术，实现网络管控部分与数据传输部分的分割，实现了网络资源的灵活调度和网络功能的动态部署。即便该架构在提高网络灵活性及可扩展性方面取得了成效，此举也使网络的防御边界变得更广，成为攻击者的首要攻击对象，从技术特点层面考察，5G 网络展现出超凡的带宽、极低的延迟以及巨大的连接能力，超高带宽使得 5G 网络能够传输大量的高清视频、虚拟现实等大流量数据；极短的延迟满足了诸如工业控制、远程手术等对时间响应极为敏感的服务需求，海量连接则支持了大规模物联网设备的接入，这种技术特性对网络安全构成了新的挑战。

2.2 5G 网络面临的主要安全风险

2.2.1 终端接入安全风险

5G 网络支持海量物联网设备的接入，这些终端设备通常具有计算能力弱、存储资源有限、安全防护措施不足等特点，此类设备往往充当网络攻击的入侵门户，非法分子渗透终端设备，实现对设备的操控，继而展开对网络内其余设备与服务器的攻击行动。攻击者可以利用物联网设备发起大规模的分布式拒绝服务（DDoS）攻击，引发带宽资源的全面饱和，使网络陷入全面停滞，5G 网络所涉及的终端设备呈现出多样化的特点，接入途径多样化，各设备采用的安全防护及认证手段各异，此举也加剧了终端接入的安全风险。

2.2.2 数据传输安全风险

5G 网络中传输的数据量巨大，且储存了众多敏感数据，诸如用户隐私数据和公司机密信息等，在数据传输阶段，这

ISSN: 2661-3719(Print); 2661-3727(Online)

些数据可能面临被窃取、篡改、伪造等安全风险，5G 网络采用的无线传输技术容易受到无线信号干扰和窃听，攻击者可以通过搭建伪基站或使用无线监听设备，非法手段捕获用户数据。5G 网络中的数据传输路径复杂，由多个网络节点及众多传输链路构成，每个节点和链路都可能成为数据安全的薄弱环节，攻击者得以对数据传输路径上的节点或链路实施攻击行动，对数据进行非法篡改或伪造，破坏数据的完整性及可用性结构。

3 传统网络入侵检测方法的局限性

3.1 基于特征码的检测方法

基于特征码的检测方法是目前应用最为广泛的入侵检测方法之一，该技术以建立一个收录已知攻击特征码的数据库为核心理念，一旦网络流量内出现与特征库中存储的特征码相匹配的数据包，则认定存在攻击迹象，该技术凸显出检测精度高、误报率低的显著效果，但也存在明显的局限性。技术仅能辨识已知类型的攻击，应对那些尚未收录在特征库中的新型攻击及变异攻击，未在特征库中发现相应的特征码，无法进行有效检测，在 5G 通信时代背景之下，网络攻击者对攻击手段的探索和创新从未停歇，不断涌现的新攻击形式层出不穷，特征库的更新速度难以跟上攻击技术的发展，此检测手段的效果不断降低，5G 网络的演进带动了数据量的急剧扩张，需对每一数据包实施特征匹配检测，执行这一操作需要消耗不少的计算和时长资源，与 5G 网络的实时性能标准不匹配。

3.2 基于异常行为的检测方法

基于异常行为的检测方法通过建立正常网络行为的模型，网络行为若与正常行为模式不一致，即认定为异常或攻击性活动，无需预先掌握攻击特征要素，具备对新出现的攻击手段的探测能力，展现出出色的适应性与良好的泛化性能，但此法仍存在不足之处。构建正常网络行为模型是一项极具挑战性的工作，必须搜集海量的常态网络数据以支撑训练过程，且伴随着网络生态的演变，该模型须持续跟进网络环境的变化进行更新，否则会导致误报率升高，在 5G 通信技术普及的今天，网络行为复杂多变，构建并更新模型的工作在 5G 网络环境中显得尤为挑战。确定该方法对异常行为识别的阈值显得复杂，阈值设置过低会导致误报率升高，阈值设置过高则会导致漏报率升高，基于异常行为的检测方法通常需要对网络流量进行深度分析，处理难度不低，难以跟上 5G 网络在实时性方面的快速响应要求。

3.3 基于协议分析的检测方法

依托对网络协议格式及含义的分析，辨别出违背协议规范的数据包，进而识别攻击行为的蛛丝马迹，该方法展现出高效检测、低误报率的双重优势，本方法适用于网络安全中对网络协议的检测工作，该方法也存在一定的局限性，本方法仅能对协议漏洞相关的攻击进行检测，此类攻击不针对协议层面的漏洞，诸如应用层这一层面的攻击，检测效果欠佳。面对 5G 技术时代的网络环境，应用层攻击的案例不断涌现，协议基础上的检测技术其检测覆盖面有限，5G 网络中采用了多种新型协议，诸如网络切片、边缘计算等协议，这些协议的结构与含义相对繁杂，分析此类协议存在一定的复杂性，需不断优化调整协议分析的规则体系，否则会影响检测效果。

4 采用深度学习方法的 5G 网络安全检测系统设计方案

4.1 系统总体架构

4.1.1 数据采集模块

数据采集模块的核心工作即搜集 5G 网络中的不同类型数据，涵盖网络流量、设备日志及用户行为等数据类别，力求全面把握网络安全态势，数据采集模块需要覆盖 5G 网络的核心网、接入网和终端设备等各个层面，在数据搜集阶段，需要考虑数据的完整性、准确性和实时性。就网络流量而言，在节点部署流量采集器，涉及交换机镜像端口及网络探针等工具，对网络传输过程中的数据包进行采集；就设备日志而言，可远程接入设备或利用日志搜集工具，获取设备运行及安全监控日志内容；用户行为数据采集的途径，依托用户端设置的代理软件及网络管理体系，获取用户行为轨迹及操作记录等数据资料。

4.1.2 数据预处理模块

由于采集到的原始数据通常包含大量的噪声、冗余信息和缺失值，这些数据会影响后续特征提取和检测模型的性能，因此需要对原始数据进行预处理，数据预处理阶段涉及数据清洗、整合、格式转换及标准化等关键环节，主要目标为移除数据中原有的杂音及异常值，实现数据空缺的填充，例如可以采用均值填充、中位数填充或基于机器学习的方法进行缺失值填补；将来自不同数据库的数据进行聚合，去除数据间的冗余与差异，数据转换的目标是将数据调整为适合特征提取及模型训练的格式。

4.1.3 特征提取模块

提取关键特征是入侵检测系统的核心步骤，目的是从处理过的数据中筛选出能体现网络攻击特点的关键特征，处于 5G 通信网络的语境中，网络数据展现出高维、非线性及动态化的特点，传统的特征提取方法难以有效提取数据中的潜在特征，该系统采用深度学习策略以实现特征提取，深度学习模型的非线性逼近能力与特征学习能力得到充分利用，自动从原始数据中提取高层次、抽象的特征。常用的用于特征提取的深度学习模型包括卷积神经网络（CNN）、循环神经网络（RNN）和自编码器（AE）等，采用卷积与池化技术，辨识并提取数据内的局部及空间层面的特性，可对网络流量数据中数据包的结构进行解析；RNN 及其变体（如长短期记忆网络 LSTM、门控循环单元 GRU）可以处理序列数据，洞察数据序列中的时间关联，尤其擅长解析网络流量的时序模式及用户行为序列的规律性，自编码器可以通过无监督学习的方式，揭示并反映数据中的深层含义，自编码器能处理那些未标记的网络数据。

4.2 关键技术选型

4.2.1 深度学习模型选择

CNN 在图像识别及语音识别等前沿领域实现了重大突破，CNN 在特征提取领域展现出独有的优势，在 5G 网络环境下进行的安全防御工作中，网络流量数据可以看作是一种二维数据（如数据包的字节序列可以构成一个二维矩阵），CNN 可以通过卷积操作提取数据包中的局部特征，涉及的特征有协议标识符、端口号、有效载荷属性等，提取这些特征对识别网络层与传输层的安全威胁极为关键。LSTM 是一种特殊的 RNN，成功消除了循环神经网络在处理长序列数据时产生的梯度消失与梯度爆炸现象，针对第五代无线网络环境，网络流量的时间序列属性明显，DDoS 攻击通常表现为在一段时间内大量数据包的连续发送，LSTM 擅长发掘网络流量中的时序关联性，精准辨识并有效地捕捉呈现时间序列特性的恶意攻击活动，诸如 DDoS 攻击、端口扫描等攻击形式。AE 是一种无监督学习模型，由编码与解码两大要素组成，编码器将输入数据归纳为低维特征空间，解码器执行将低维特征空间的数据转换回原始数据空间的操作，实施 5G 网络的入侵检测措施，自动编码器借助对常规网络数据的训练，构建正常数据的特征映射，遇到异常数据输入情形，AE 的重构误差会显著增大，进而识别出异常行为的模式，本系统能有效辨识未知的网络安全威胁，适应性方面表现强劲。

4.2.2 数据存储与处理技术

5G 网络中产生的海量数据需要高效的存储和处理技术支持，本系统采用分布式存储技术，采用 Hadoop 的分布式文件系统技术，实现了对大量网络数据的存储支持，HDFS 以其高可靠性、可扩展性及高效的数据处理吞吐量见长，完全契合 5G 网络数据存储的特定需求，论及数据处理的层面，采取分布式计算途径，实现海量数据的并行化分析，内存计算技术为 Spark 所采用，极大地促进了数据处理的速率，适用于实时应对 5G 网络中大量数据处理的挑战。

结论

本篇论文针对采用深度学习的 5G 网络入侵检测系统进行深入探讨，开篇即对 5G 网络的属性及其所面临的安全挑战进行了系统研究，探讨了传统网络入侵检测技术在 5G 网络背景下的限制性，然后设计了基于深度学习的 5G 网络入侵检测系统，系统架构及关键技术的选用细节得到了深入的分析；实验最终揭示了系统的性能特性，测试结果显现，本系统在检测的准确性、实时性以及普遍适用性方面均超越了传统检测技术及独立深度学习模型，有效抵御 5G 网络的安全挑战。

参考文献：

[1] 汪琰 . 基于图神经网络的 5G-A 网络切片与资源动态分配 [J]. 信息记录材料 ,2025,26(08):202-204.

[2] 唐冬来 , 李玉 , 张强 , 欧渊 , 尚忠玉 , 唐吉忠 . 基于时空特征的 5G 通信基站短时流量预测方法 [J]. 信息技术 ,2025,(07):14-19.

[3] 张聪然 , 李震领 , 许浒 . 基于深度强化学习的海上风电场 5G 传感网络动态资源分配方法 [J]. 传感器世界 ,2025,31(06):21-25+31.

[4] 吴雨峰 . 基于深度学习的 5G-A 网络流量预测方法研究 [J]. 电子产品世界 ,2025,32(06):22-26.

[5] 张梦宇 .5G 通信环境下雷达信号处理技术的研究 [J]. 中国宽带 ,2025,21(05):91-93.