# SDN 环境下基于 XGBoost-CNN-LSTM 的异常流量检测模型

谷瑞泽[1] 王小英[1] 崔方方[1] 李春辉[1] 杨国庆[2]
GU Ruize WANG Xiaoying CUI Fangfang LI Chunhui YANG Guoqing

**摘 要** 软件定义网络（software-defined networking, SDN）通过将控制层与数据层分离提供了更高的灵活性和可编程性，但控制器的集中化也为异常流量注入和流表篡改埋下隐患。因此，文章提出了一种基于 XGBoost-CNN-LSTM 的异常流量检测模型。该模型首先通过 XGBoost 筛选高判别性特征，然后利用 CNN（convolutional neural network）提取局部空间模式，最后结合长短期记忆网络（long short-term memory, LSTM）捕捉攻击行为的时序依赖关系，形成端到端的检测框架。在公开数据集 InSDN 上的实验结果表明，该模型检测准确率达到 99.32%，精确率达到 99.15%，召回率达到 99.02%，$F_1$ 得分达到 99.09%。

**关键词** SDN；CNN；特征提取；XGBoost；网络异常流量检测

doi：10.3969/j.issn.1672-9528.2025.10.033

## 0 引言

软件定义网络[1]（software-defined networking, SDN）是一种新型的网络体系结构。SDN 结构可分为三层[2]：转发平面、控制平面和应用平面。

在 SDN 架构中采用集中式的控制平面和分布式的转发平面，实现两个平面相互分离。利用控制平面的控制－转发通信接口（南向接口）对转发平面的网络设备进行集中控制，并通过应用－控制接口（北向接口）向应用平面提供灵活的可编程能力。虽然 SDN 提高了网络的可编程性，简化了配置操作，但也随之受到了许多网络攻击的威胁。比如对控制器的拒绝服务攻击（denial of service, DoS），对交换机流表、缓存及相关链路的分布式拒绝服务攻击（distributed denial of service, DDoS）[3]。

此外，还有针对网络上存在的漏洞的病毒等攻击。为了检测这些攻击，研究人员提出了许多方法。目前，大多数机器学习算法被用于 SDN 环境下的流量检测，常用的有随机森林算法[4]、GAN、GRU[5] 等。但其中大多数算法仅适用于二分类攻击检测，而不适合多分类的攻击检测。而且传统的 CNN 模型在处理网络流量时面临一些难题。一方面，存在网络流量数据维度高、时间序列特征难以有效捕获以及对不平衡数据的鲁棒性不足的问题；另一方面，在数据集方面，存在异常流量信息获取困难，公开数据集中的正常数据和攻击数据不平衡问题。

相关研究显示，在二分类检测中，使用传统机器学习模型，随机森林算法在 NSL-KDD 数据集上获得了超过 90% 的准确率，但当扩展到多分类问题时，准确率显著下降。与之相比，CNN 作为深度学习模型能够提取特征层面的高阶信息，但其在多分类检测任务中的性能往往受限于数据集的不平衡性，尤其是在少数类检测上的表现较差。此外，RNN 等序列模型在捕获时间相关性方面表现出色，但由于计算开销较大，无法适应实时检测需求。

因此，鉴于现有模型在多分类异常流量检测中存在的种种不足，本文提出 XGBoost-CNN-LSTM 模型，通过 XGBoost[6] 的高效特征选择能力、CNN[7] 的空间特征提取能力以及 LSTM[8] 的时间序列建模能力，解决现有模型在多分类异常流量检测中的不足，进一步提升检测准确率与鲁棒性，为 SDN 环境下的异常流量检测提供新的解决方案。实验验证表明，本文提出的方法在检测异常流量上取得了显著的效果提升。

## 1 基于 XGBoost-CNN-LSTM 的异常流量检测流程

本文提出的异常流量检测框架处理数据集流程分为数据集部分、数据预处理部分、异常流量检测模型部分以及评估指标部分，如图 1 所示。

1. 防灾科技学院 河北廊坊 065201
2. 廊坊市网络应急保障与网络安全重点实验室 河北三河 065201

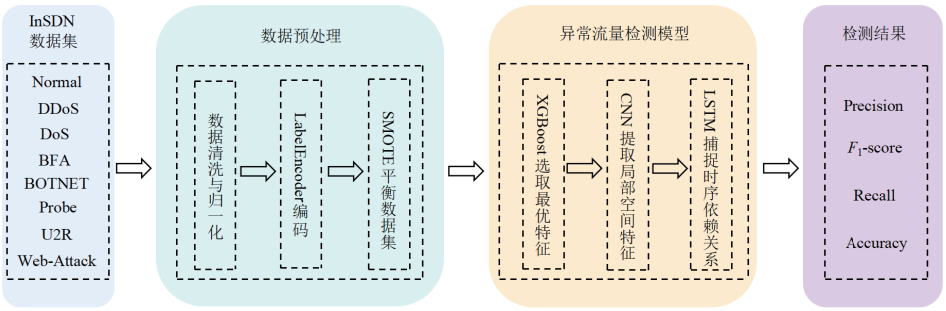


图 1 异常流量检测框架流程图

### 1.1 数据集介绍

本文使用的 InSDN[9] 数据集是在 SDN 环境下收集的公开网络数据集，该数据集包含多种攻击类型，如 DoS、DDoS、Web 攻击、密码猜测、僵尸网络、利用攻击和探测攻击等。InSDN 数据集与以往仅限于 DoS/DDoS 攻击的数据集相比，攻击类型更加多样和全面。同时该数据集不仅包含了攻击流量，还涵盖了各种流行应用服务产生的正常流量，这种结合使得数据集更加贴近实际 SDN 网络中的流量情况，有利于提高入侵检测模型的准确性和鲁棒性。详细信息如表 1 所示。

表 1 InSDN 数据集信息

| 序号 | 类型 | 含义 | 条数 |
|---|---|---|---|
| 1 | Normal | 正常流量 | 68 424 |
| 2 | DDoS | 分布式拒绝服务攻击 | 121 942 |
| 3 | DoS | 拒绝服务攻击 | 53 616 |
| 4 | BFA | 暴力破解攻击 | 1 405 |
| 5 | BOTNET | 僵尸网络 | 164 |
| 6 | Probe | 探测攻击 | 98 129 |
| 7 | U2R | 用户到根权限提升攻击 | 17 |
| 8 | Web-Attack | 网络攻击 | 192 |

### 1.2 数据预处理

为解决 InSDN 数据集中存在的缺失值和数据不平衡问题，首先进行数据清洗，移除无关的 ID 列和填补缺失值，此外，对诸如协议（Protocol）等分类特征实施了编码处理，以便于模型识别。对于标签列处理采用 LabelEncoder 编码，方便进行后续的模型训练与结果的标签映射。同时为了加快模型的读取和收敛速度，采用最大最小归一化来将数据映射到 [0,1] 之间，用公式表示为：

$$x_i^{'} = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \tag{1}$$

式中：$x_i$ 是数据集中某个样本的特征值；$x_{\min}$ 是该特征在整个数据集中的最小值；$x_{\max}$ 是该特征在整个数据集中的最大值。

最后应用 SMOTE[10] 过采样技术来平衡各类样本数量，增强模型对少数类样本的识别效果。经过平衡之后的样本数量达到 975 536 条。

### 1.3 基于 XGBoost-CNN-LSTM 的异常流量检测模型

为进一步提取特征，提升检测效果，本文提出基于 XGBoost-CNN-LSTM 的异常流量检测模型。在经由数据预处理之后，首先进入特征选择阶段，采用 XGBoost 嵌入式特征选择方法，其在训练过程中会计算每个特征在所有决策树节点分裂时带来的平均损失函数减少量（即增益），该指标直接反映特征对模型预测性能的提升程度。增益越高的特征，意味着其对目标变量的解释能力越强，因此在筛选中得到的重要性评分就越高。本文使用的 InSDN 数据集共包含 83 列特征，经由特征选择之后，最终选取 15 列特征用作训练，其具体得分排名如图 2 所示，其中横坐标是选取出的特征名称，纵坐标是对应的特征得分。这一方法不仅可以自动捕捉特征与目标之间的非线性关系和交互效应，还能通过正则化避免对噪声特征的过拟合，从而确保模型能聚焦在最优特征子集。

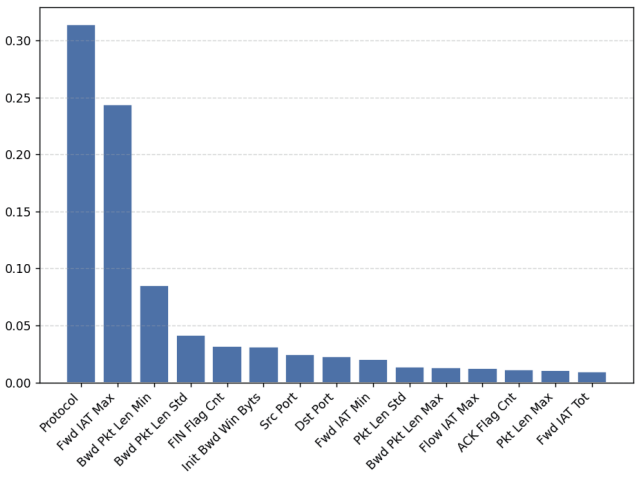


图 2 特征重要性得分排名图

随后输入至 CNN 特征提取模块：该模块包含由 64 个尺寸为 3 的一维卷积核构成的卷积层，通过局部特征感知提取空间特征；继而通过步长为 2 的池化层进行特征维度压缩。经处理的特征序列传递至 LSTM 单元构成的时间序列建模层，捕捉数据中的时间依赖关系。为防止模型过拟合，在模型后端设置概率为 0.3 的 Dropout 正则化层。最终特征经展平层向量化处理后，通过具有 Softmax 激活函数的全连接层输出多分类概率。检测模型具体架构如图 3 所示。

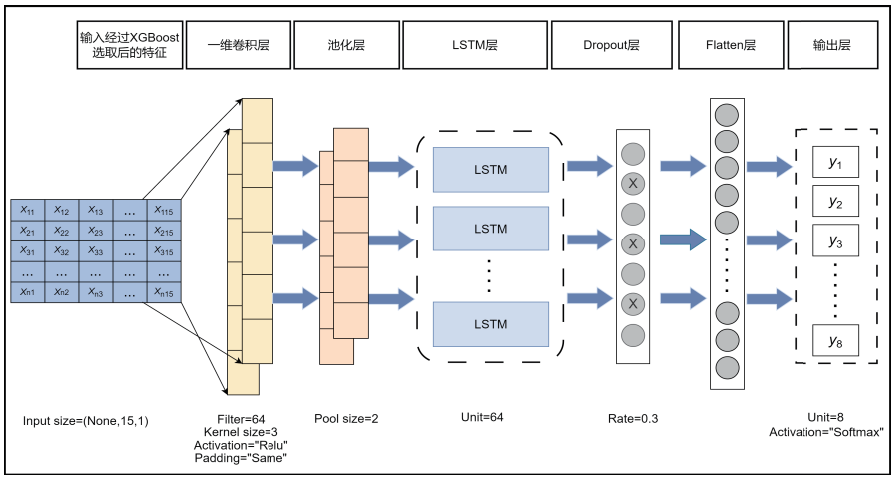


图 3 检测模型架构图

### 1.4 评估指标

对于分类问题，本文使用 Accuracy（准确率）、Precision（精确率）、Recall（召回率）和 $F_1$-score（$F_1$ 得分）来评价模型分类性能。计算公式分别为：

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{2}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

$$F_1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5}$$

式中：真正例（TP）指真实类别就是该类流量，被预测的结果也是该类流量的数量；假正例（FP）指真实类别为其他类型的流量，但是却被预测为该类流量的数量；假负例（FN）指真实类别本该是该类流量，但是却被预测为另一类流量的数量；真负例（TN）指真实类别为其他类型的流量，被预测为其他类型流量的数量。

## 2 结果分析与仿真实验

### 2.1 结果分析

在对比实验中，本文评估了 5 种不同的模型：CNN、XGBoost-CNN、XGBoost-LSTM、GRU 以及本文使用的模型。其结果如表 2 所示。

表 2 不同模型的性能比较

| 模型 | 准确率 /% | 精准率 /% | 召回率 /% | $F_1$ 分数 /% |
|---|---|---|---|---|
| CNN | 95.04 | 95.31 | 95.04 | 95.03 |
| XGBoost-CNN | 95.17 | 95.33 | 95.17 | 95.19 |
| XGBoost-LSTM | 98.34 | 98.54 | 98.43 | 98.45 |
| GRU | 98.47 | 98.57 | 98.47 | 98.46 |
| 本文模型 | 99.32 | 99.15 | 99.02 | 99.09 |

本文提出的模型在检测准确率上高达 99.32%，与之对比 XGBoost-LSTM 与 GRU 在准确率上分别为 98.34% 与 98.47%，两者性能接近，但都未能超越本文模型。本文模型的精确率同样达到了 99.15%，表明其在预测正类样本时具有很高的准确性。同时本文模型的召回率也达到了 99.02%，显示出其在识别正类样本方面的强大能力。最后就是 $F_1$ 分数，其综合考虑了模型的精确性和召回能力，而本文模型的 $F_1$ 分数为 99.09%，进一步证明了其在分类任务中的优越性能。

### 2.2 仿真实验

为进一步检验模型效果，本文在 Ubantu18.04 系统中使用虚拟化网络仿真工具 Mininet 构建网络拓扑，如图 4 所示。控制器选择使用 Ryu 控制器，拓扑中划分两个不同的网段，每个网段出入口放置交换机，分别为 S1 交换机和 S2 交换机。两个网段分别为：10.0.0.X、10.0.1.X。在不同网段内各有 4 台主机，IP 地址分别为：10.0.0.1~10.0.0.4 和 10.0.1.1~10.0.1.4。使用虚拟机中各种工具来模拟入侵流量，例如：使用网络数据包处理工具 Scapy 来模拟正常流量、使用 Hping3 工具模拟 DDoS 攻击、使用 Nmap 模拟刺探攻击、使用 SQLMap 自动注入工具来模拟 Web 攻击等。

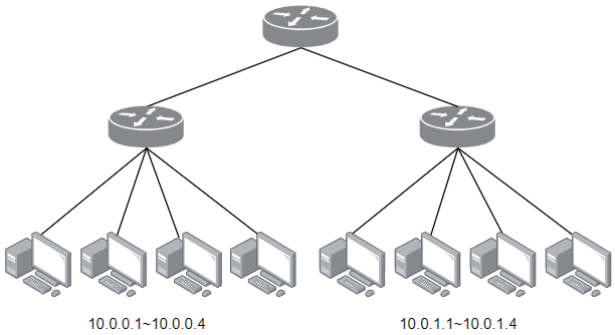


图 4 搭建 SDN 网络拓扑图

### 2.3 仿真实验结果

在 Ryu 控制器上部署训练好的 XGBoost-CNN-LSTM 模型作为检测模型，使用上文提到的工具分别在 IP 为：10.0.0.1 的主机上对拓扑中其余随机的 IP 模拟不同的攻击，取正常流量为 1，其余攻击依次为 2~8，检测结果中会显示检测结果是否正确、源 IP 和目的 IP，得到的部分检测结果如图 5~6 所示。

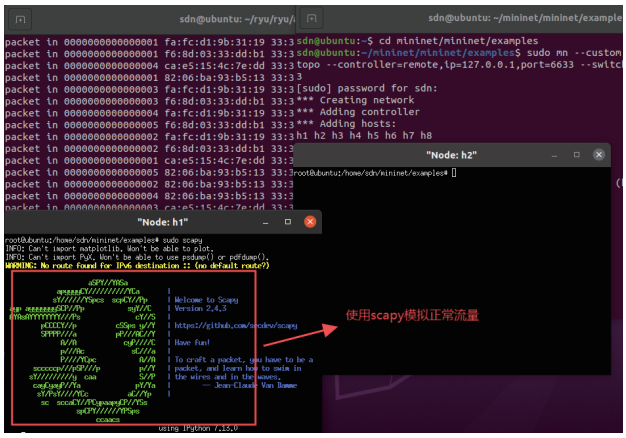


图 5 模拟正常流量结果图

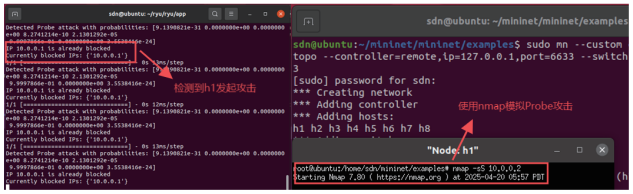


图 6 异常流量检测结果图

通过记录检测记录，计算得到如表 3 所示的检测准确率，其中多种攻击的检测平均准确率达到了 95% 以上。

表 3 各类攻击检测准确率

| 类型 | 准确率 /% |
|---|---|
| Normal | 95.31 |
| DDoS | 95.20 |
| DoS | 96.12 |
| BFA | 94.12 |
| BOTNET | 94.13 |
| Probe | 96.65 |
| U2R | 95.05 |
| Web-Attack | 96.23 |

## 3 结语

本文提出一种基于 XGBoost-CNN-LSTM 的网络异常流量的检测模型，同时进行了对比实验用以评估在不同模型上的检测性能。在对比实验中证明了本文提出的模型对于 SDN 下采集的 InSDN 数据集中的各种攻击的检测的精准度，召回率和 $F_1$ 得分要优于其他几类模型。同时仿真实验结果表明，该方法可以检测到本文提出的多种攻击，且平均检测准确率达到了 95% 以上。后续需要实现处理策略即发现攻击后的处理，以及进一步提高模型的检测准确率。

**参考文献：**

[1] 董道远，贾晖，徐晨．软件定义技术发展与未来影响研究 [J]. 工业信息安全，2024(5): 68-73.

[2] 翟亚红，崔峻玮．软件定义网络安全研究进展 [J]. 科技导报，2023, 41(13): 76-88.

[3] 靳燕．基于 SDN 架构的 DDoS 攻击检测研究 [J]. 电脑与电信，2024(6): 26-30.

[4] 傅友，邹东升．SDN 中基于条件熵和决策树的 DDoS 攻击检测方法 [J]. 重庆大学学报，2023, 46(7): 1-8.

[5] 杨亚红，王海瑞．基于 Renyi 熵和 BiGRU 算法实现 SDN 环境下的 DDoS 攻击检测方法 [J]. 计算机科学，2022, 49(S1): 555-561.

[6] CHEN T Q, GUESTRIN C. XGBoost: a scalable tree boosting system[C]//Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining. NewYork:ACM,2016: 785-794.

[7] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[8] VAN HOUDT G, MOSQUERA C, NÁPOLES G. A review on the long short-term memory model[J]. Artificial intelligence review, 2020, 53(8): 5929-5955.

[9] ELSAYED M S, LE-KHAC N A, JURCUT A D. InSDN: a novel SDN intrusion dataset[J]. IEEE access, 2020, 8: 165263-165284.

[10] CHAWLA N V, BOWYER K W, HALL L O, et al. SMOTE: synthetic minority over-sampling technique[J]. Journal of artificial intelligence research, 2002, 16: 321-357.

**【作者简介】**

谷瑞泽（2003—），男，河南周口人，硕士研究生，研究方向：异常流量检测，email: 24661605@st.cidp.edu.cn。

王小英（1979—），女，陕西咸阳人，硕士，教授，研究方向：无线通信、WSN 技术、网络安全，email:wangxiaoying@cidp.edu.cn。

崔方方（2001—），女，山东济宁人，硕士研究生，研究方向：灾害信息处理技术，email: 24661604@st.cidp.edu.cn。

李春辉（1999—），女，山东青岛人，硕士研究生，研究方向：数据与网络安全，email: chunhuili2023@163.com。

杨国庆（2000—），男，河北张家口人，硕士研究生，研究方向：DDoS 攻击检测，email: 1583015769@qq.com。

（收稿日期：2025-05-23 修回日期：2025-10-14）