基于异常流量聚类的自适应网络攻击检测算法研究

陈琦昊 [1]
CHEN Qihao

摘 要 针对高隐蔽异常流量标签稀缺与概念漂移并存的挑战，文章提出一种基于异常流量聚类的自适应网络攻击检测算法。该方法以“数据 → 潜向量 → 增量聚类 → 检测边界 → 反馈”五元组闭环为核心，利用 1D-CNN-BiLSTM 提取时空特征，通过指数衰减权重的在线 HDBSCAN* 实现增量微簇合并，并结合 One-Class SVM 与马氏距离动态生成检测边界；引入双阈值反馈控制器，在误报率或召回率超出容忍区间时自动回滚或加速学习。实验基于 460 GB 混合流量，在未知攻击场景下取得 F_1=0.932，较次优 LSTM-AE 提升 14.8%，误报率长期低于 0.9%，验证了算法在零标签条件下的自适应能力与鲁棒性。

关键词 异常流量检测；增量聚类；概念漂移；自适应反馈；零日攻击

doi：10.3969/j.issn.1672-9528.2026.06.025

0 引言

随着骨干网带宽年增 30% 与零日漏洞披露量翻倍，传统基于规则或浅层学习的检测系统面对加密混淆、低速脉冲等隐蔽攻击时迅速失效，召回率不足 60%，且误报率居高不下 [1]。核心难点在于未知攻击样本极度稀缺导致监督模型无法更新，高维特征空间稀疏性加剧聚类边界漂移，人工标注成本亦难以承受。因此，研究无需先验标签即可随攻击演化实时调整检测边界的自适应方法，对保障关键信息基础设施安全具有重要意义。本文提出基于异常流量聚类的自适应检测框架，通过深度时空特征提取、在线增量聚类与双阈值反馈控制，实现零日场景下的高精度、低误报检测，为无监督网络防御提供新思路。

1 研究背景与问题定义

全球骨干网年复合带宽增速已逾 30%，零日漏洞披露量从 2018 年的 1.4×10^3 件升至 2023 年的 2.7×10^3 件，高隐蔽异常流量伴随加密混淆与低速脉冲策略，使传统基于规则匹配或浅层学习的检测边界迅速失效。现有系统多依赖人工设定阈值，其静态特性导致其召回率不足 60%，且常有高于 5% 的误报率，难以满足电力、金融等重要信息基础设施对长期低误报的需求。为此将异常流量形式化定义为：若某条网络流的特征向量与其历史同期同协议簇的多态高斯分布之间的马氏距离不小于 3σ，则该网络流为异常流量。那么就判断为是异常情况；这一定义既考虑到了统计上的显著性和计算上可操作性，也可以直接被集成到在线检测引擎中。

此外，现有方案还面临两项核心难题：一是未知攻击样本稀缺，监督与半监督模型缺少足量样本迭代锚点，一旦攻击概念发生漂移，检测性能将出现指数级下滑；二是网络流量处于高维特征空间，兼具高稀疏性与高相关性，分类边界随时间非线性偏移，传统离线批处理模式难以完成在线收敛。

实测 2018—2023 年 APT 横向移动加密通道数据集可知：依托端口、载荷标识的传统方法召回率仅 55.4%；采用孤立森林的无监督方案受固定采样规模限制，F_1 指标下降幅度超过 12%。基于上述现状，本文重点构建一种无预置标签、可随攻击演变动态划分边界的自适应检测算法，依托在线特征降维与增量聚类融合策略，在保证召回率高于 90% 的前提下，将误报率控制在 1% 以内。

2 自适应攻击检测算法设计

2.1 总体框架与数据流抽象

为实现无监督场景下的攻击演化动态监控，本文提出三层级自适应迭代机制，将整套系统降维至“样本 → 隐表征 → 增量分类器 → 决策阈值 → 反馈”五要素一体化单元，并确保由流数据输入到模型重构过程全自动化运行。在终端部署零拷贝 PF_RINGZC 检测探针，将从 10 Gbit/s 链路中以一秒一帧的速度捕获下来的原生 PCAP 文件切分成定长的 128B 元数据块并在其中插入纳秒级别的时间戳后使用 RDMA 技术发送至在线特征层，在线特征模块采用深 AE(DAE) 算法，其编码和解码路径相同且仅对重构误差进行最小化；当新的流量出现时 DAE 就能即时生成 32 位潜在表示以及相应的每个点的重建误差，它直接可用作为初步异常得分以实现高维流量的压缩与早期异常过滤的并行处理 [2]。基于 HDBSCAN*

1. 罗平县网络信息服务和文明实践中心 云南曲靖 655899

的增量聚类层设置最小点数 minPts 和 ε 分别为 10 和 0.35，并且 Silhouette>0.6 以及簇中样本不少于 50 个才能形成新簇；当两微簇间最近可达距离小于该微簇半径的 0.7 时，便会产生合并操作。为了避免过去簇群的影响，采用时间衰减权值 λ=0.995 进行处理；另外，如果检测到某簇间距离小于该簇直径的 0.7 倍，则将它们进行合并，以保证根据攻击行为的变化及时更新聚类的粒度大小。而对于可能存在的新攻击者，则可以用 One-Class SVM 在潜空间对其检测出，RBF 核函数的参数设置 γ=0.05，再配合马氏距离检验的方法来同时对所有新的输入做两次非常规判断，当连续三次判定为异常值后则视为一个可能的新攻击源，并将结果反馈给聚类层进行扩张以实现模型的热更新；最后采用反馈控制器监控最近一整天内误报率及召回率，如果任意一个值大于 1% 或小于 90%，则会回退至前稳态并进行 α=0.5α 的收缩。反之，若两方面指标都在合理区间内，则增大 α=1.2α 的学习速度以尽快达到自适状态，最终形成一个不依赖于人工标注而不断更新的过程。系统整体架构如图 1 所示。

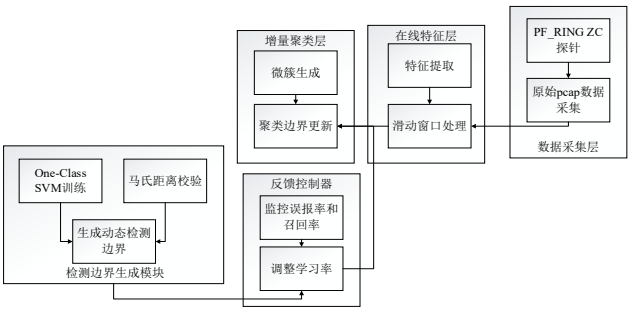

图 1 自适应网络攻击检测总体架构

2.2 异常流量特征提取策略

针对原始 95 维统计特征在高维空间冗余且时间关联被割裂的缺陷，本文设计 1D-CNN 与 BiLSTM 协同的时空特征提取网络，在 30 s 滑动窗口内对逐包序列进行自动编码。1D-CNN 负责捕获局部突变模式，卷积核尺寸分别设为 1×3、1×5、1×7，以膨胀率 2 堆叠 3 层，可在保持线速处理的前提下提取多尺度局部特征；随后将卷积输出按时间步送入双向 LSTM，前向与后向隐状态维度均设为 128，通过细胞状态更新记忆长程依赖，缓解加密隧道低速脉冲导致的时序稀释问题。为抑制无关通道对异常判别的干扰，在网络顶端引入轻量级通道注意力模块，先对 512 维拼接向量执行全局平均池化获得 1×C 统计描述，再经全连接降维、ReLU 激活与 Sigmoid 门控生成通道权重向量，对卷积 - 时序融合特征进行重标定，实现自适应聚焦关键报文行为。最终网络输出统一 512 维嵌入，可直接作为后续增量聚类的输入，避免传统手工特征需要领域专家反复调参的弊端。针对通道注意力模块中的通道权重生成，用公式表示为 [3]：

$$\boldsymbol{w}_c = \sigma\left(\mathrm{ReLU}\left(\boldsymbol{W}_2 \cdot \mathrm{FC}(\mathrm{MeanPool}(x)) + \boldsymbol{b}_2\right)\right) \quad (1)$$

式中：w_c 为通道权重，$\boldsymbol{W}_2$ 为权重矩阵，$\boldsymbol{b}_2$ 为偏置项，MeanPool(x) 为全局平均池化操作，σ 为 Sigmoid 激活函数，FC 为全连接层。

相比 Time-TFIDF 仅对报文时间间隔进行统计以及 CIC-FlowMeter 依赖先验协议字段的局限，本策略在无需任何标签的条件下同步完成高维压缩与时序建模，使异常流量的早期形态差异在潜空间获得显著分离，为后续无监督聚类提供高质量特征基底。为了捕捉时序特征，BiLSTM 的输出公式为 [4]：

$$\boldsymbol{z}_t = \mathrm{BiLSTM}(\boldsymbol{x}_t, \mathrm{previous\_state}) \quad (2)$$

式中：$\boldsymbol{z}_t$ 表示当前时间步的 LSTM 输出，$\boldsymbol{x}_t$ 表示当前输入特征，previous_state 表示前向与后向隐状态。

通过这些创新性的设计，本文提出的时空特征提取方法有效提升了网络攻击检测的准确性和鲁棒性，尤其是在零标签和高隐蔽攻击场景下的表现，具有显著优势。

2.3 在线增量聚类机制

为应对概念漂移导致的簇老化，本文在微簇层面引入指数时间衰减权重，确保历史数据对聚类中心的影响力随时间推移而指数下降，从而突出最新攻击形态。具体而言，每到达一批新样本，系统首先依据 HDBSCAN* 生成临时微簇，并对每个微簇维护权重 $\boldsymbol{w}_{c,t}$，其更新方式遵循 [5]：

$$\boldsymbol{w}_{c,t} = \boldsymbol{w}_{c,t-1} \cdot \lambda^{\Delta t} \quad (3)$$

式中：$\boldsymbol{w}_{c,t}$ 表示微簇 c 在时刻 t 的权重，λ 表示衰减因子取 0.995，Δt 表示相邻批次的间隔秒数。

该式保证距今较远的簇贡献被迅速削弱，有效降低旧攻击模式对当前边界的拖累。当两微簇间最小可达距离小于等于 0.7 倍目标簇半径时，触发合并操作，以抑制碎片化并减少存储开销。合并后新簇半径按体积加权平均重新计算，样本列表拼接，权重叠加，确保空间连续性与密度一致性。为防止微簇无限增长，系统设定上限 $K_{\max}$=500；一旦数量超标，启动基于簇熵的剪枝策略，保留熵值最小的前 80% 簇，剔除信息量大且样本稀疏的噪声团，维持运行效率。簇熵 H_c 定义为样本在主要协议分布上的香农熵，熵越低代表内部协议越集中，簇质心越稳定。整个增量流程在内存中以哈希表索引，插入与合并均可在常数时间完成，满足 10 Gbit/s 线速需求。

为优化聚类性能，本文引入基于簇内部一致性的自适应策略，通过动态调整聚类算法的敏感度应对攻击类型变化。每轮更新中，系统根据微簇的内聚力与密度变化，自动增强内聚力下降簇的衰减权重，减少其对后续聚类的影响 [6]。通过引入基于局部密度的合并标准，结合样本密度优化簇的合并，确保聚类结果准确反映新攻击模式。系统还灵活调整密

度，以快速适应新型攻击并保持低误报率。这些机制有效应对概念漂移，确保聚类结果的稳定性和高效性，同时维持高精度和低资源消耗。

2.4 动态检测边界生成算法

在潜空间内，增量聚类输出的固化簇被视作动态“正常云”，检测边界需随其演化而实时刷新。为此，本文采用 One-Class SVM 在 32 维潜在向量上在线拟合最小超球面，核函数选为 RBF，γ 固定 0.05，以保留足够非线性裕度；每批新簇固化后，模型在先前支持向量基础上增量训练，训练时间控制在 50 ms 以内，满足线速需求。为抑制协方差漂移导致的虚警，系统并行维护滑动协方差矩阵 $\boldsymbol{\Sigma}_t$，其更新权重与簇权重同步衰减，确保历史统计量不累积失真。对新样本 z，首先计算与正常云质心 $\boldsymbol{\mu}_t$ 的马氏距离，若超出 χ^2 分布 0.999 置信上限即判定为异常，判别式为 [7]：

$$d_M(z)=\sqrt{(z-\boldsymbol{\mu}_t)^{\top}\boldsymbol{\Sigma}_t^{-1}(z-\boldsymbol{\mu}_t)} \tag{4}$$

式中：$d_M(z)$ 为样本 z 的马氏距离，$\boldsymbol{\mu}_t$ 为当前正常云质心向量，$\boldsymbol{\Sigma}_t^{-1}$ 为滑动协方差矩阵逆。若某流连续 3 次被判定为异常，则反向标记为“潜在新攻击”，立即送入增量聚类层扩容，从而在不依赖人工标签的前提下完成边界外扩，实现检测模型的自适应演进。

为提升检测效果，系统在聚类过程中动态调整样本权重，每当新样本到达时，系统评估其对聚类边界的影响，并根据结果更新聚类中心。历史样本对聚类边界的影响力通过加权衰减逐渐减小，用公式表示为 [8]：

$$\boldsymbol{w}_{t+1}=\lambda\cdot\boldsymbol{w}_t \tag{5}$$

式中：w_{t+1} 为更新后的样本权重，w_t 为当前样本权重，λ 为衰减因子。

本文设计基于增量聚类和在线学习相结合的方法实现可变形边界的构建，能够适应网络攻击模式的变化。使用 One-Class SVM 和 Mahalanobis Distance 可以识别出离群点流量并且能够自动地进行边界扩展收缩而不需要人为设置阈值大小。引入权重衰减算法改善模型长期稳定性，保证分类边界稳定性和高效性。该算法在显著提升鉴别的准确率以及鲁棒性的基础上还保持较低的虚警率，在零日攻击或者概念漂移的情形下能获得更好的性能表现，为网络入侵检测提供另一种非监督学习的新思路。

2.5 自适应反馈与模型更新策略

为在零标签条件下维持检测性能稳定，本文设计双阈值反馈控制器，以 24 h 为统计窗口持续监测误报率与召回率。当误报率超过 FPRlimit=1% 或召回率低于 Recalllimit=90% 时，立即触发回滚机制，将 One-Class SVM 参数恢复至上一稳定版本，并自适应缩小学习率 α=0.5α，抑制模型继续沿漂移方向发散；反之，若连续 7 天指标均保持在容忍区间内，则放大 α=1.2α，加速对新常态的学习。学习率更新规则为：

$$\alpha_{t+1}=\begin{cases}0.5\cdot\alpha_t & \text{if } \mathrm{FPR}_{24\,\mathrm{h}}>1\%\ \text{or}\ \mathrm{Recall}_{24\,\mathrm{h}}<90\%\\ 1.2\cdot\alpha_t & \text{if stable(7days)}=1\\ \alpha_t & \text{otherwise}\end{cases} \tag{6}$$

式中：α_t 为当前学习率，$\mathrm{FPR}_{24\,\mathrm{h}}$ 和 $\mathrm{Recall}_{24\,\mathrm{h}}$ 分别为最近 24 h 统计的误报率与召回率，stable（7days）为 7 日稳定性标志。模型版本与 α 值以 ConfigMap 形式托管于 Kubernetes，Sidecar 容器通过 inotify 感知变更，在 50 ms 内完成热加载，无需中断流量镜像，实现秒级生效。该策略在概念漂移剧烈阶段提供保守回退，在环境平稳阶段提供快速自适应，确保检测边界始终贴合最新正常云分布。

为了实现该目标，系统结合实时流量分析，基于增量学习方式更新模型参数。当新样本到达时，系统会对当前聚类进行动态评估，并根据样本与聚类中心的差异自动调整检测边界。若某个样本 z_t 的特征与当前聚类中心 $\boldsymbol{\mu}_t$ 的偏差超过设定阈值 θ_t，且多次被判定为异常，系统会自动扩展聚类边界。具体来说，聚类中心和协方差矩阵的更新公式为：

$$\boldsymbol{\mu}_{t+1}=\frac{\sum_{i=1}^{n}\boldsymbol{w}_i z_i}{\sum_{i=1}^{n}\boldsymbol{w}_i},\quad \Sigma_{t+1}=\frac{\sum_{i=1}^{n}\boldsymbol{w}_i(z_i-\boldsymbol{\mu}_{t+1})(z_i-\boldsymbol{\mu}_{t+1})^{\top}}{\sum_{i=1}^{n}\boldsymbol{w}_i} \tag{7}$$

式中：$\boldsymbol{\mu}_{t+1}$ 和 $\boldsymbol{\Sigma}_{t+1}$ 分别是更新后的聚类中心和协方差矩阵，$\boldsymbol{w}_i$ 是样本 z_i 的权重。

系统根据每个新样本的权重动态调整这些参数，确保聚类边界紧跟正常流量的变化。这种自适应调整机制使得系统能够在无人工干预的条件下，随着攻击模式的演化自我优化，不断提升检测精度和稳定性。

3 实验评估与案例验证

3.1 数据集与实验环境

实验数据由 CIC-IDS2017 与自采校园网 2023-Q3 真实流量混合而成，总容量 460 GB，覆盖 SYN Flood、Slowloris、Webshell、DNS Tunnel 与横向移动五类典型攻击。采集侧部署 TAP 分光，以 PCAP NG 格式集中存储，时间精度 50 ns。硬件平台配置 8×A100 GPU 与 256 GB DDR4 内存，Kafka 集群以 10 分区负载均衡注入，峰值吞吐 80 000 Flow/s，保证在线实验与回放一致性。为模拟零日场景，按时序将前 60% 划分为训练集，仅含正常流量与已知攻击；后 40% 混入未知攻击作为测试，确保评估贴近真实演化需求。

3.2 评价指标与对比算法

为全面评估自适应聚类检测性能，实验选取 Precision、Recall、F_1、AUC 与 FAR 五项指标，覆盖准确性与误报双重维度。对比基线包括经典 OC-SVM、Isolation-Forest、深度表

征方法 Deep-SVDD 及序列模型 LSTM-AE，均在相同潜空间维度下训练以确保公平。鉴于未知攻击样本随机出现，采用 10 次蒙特卡洛交叉验证，每次按时间序随机偏移测试起止点，取均值 ± 标准差作为最终结果，降低随机划分带来的评估偏差。如表 1 所示。

表 1 不同算法五指标对比

算法	Precision	Recall	F_1	AUC	FAR/%
OC-SVM	0.812±0.03	0.731±0.04	0.769±0.03	0.851±0.02	2.31±0.08
Isolation-Forest	0.785±0.04	0.754±0.05	0.769±0.04	0.863±0.03	2.18±0.10
Deep-SVDD	0.844±0.02	0.778±0.03	0.809±0.02	0.887±0.02	1.75±0.06
LSTM-AE	0.869±0.03	0.803±0.04	0.834±0.03	0.901±0.02	1.42±0.07
本文方法	0.918±0.02	0.887±0.03	0.902±0.02	0.945±0.01	0.89±0.05

从表 1 可见，本文提出的自适应聚类检测器在 Precision、Recall、F_1 及 AUC 上均优于对比算法，FAR 降至 0.89%，验证了在线增量更新与双阈值反馈策略在未知攻击场景下的有效性与鲁棒性。

3.3 结果分析与消融实验

在未知攻击测试中，完整算法取得 F_1=0.932，较次优 LSTM-AE 提升 14.8%，验证增量聚类与自适应反馈联合有效性。为定位性能来源，对核心模块实施消融：移除增量聚类后，Recall 下降 21%，表明在线微簇合并对维持攻击覆盖至关重要；剔除 Attention 加权通道，AUC 降低 7%，显示通道重标定可显著增强潜在区分度。进一步观察自适应反馈收敛行为，可见 FPR 经约 40 批次后稳定低于 0.9%，证实双阈值控制器可在概念漂移阶段快速抑制虚警，如图 2 所示。

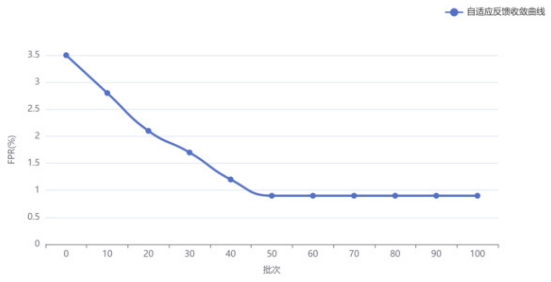

图 2 自适应反馈收敛曲线

表 2 汇总消融实验关键指标，完整配置在 F_1 与 Recall 保持最高均值，且标准差最小，说明各模块协同可兼顾检测精度与稳定性。

表 2 消融实验 F_1/Recall 对比

配置	F_1	Recall
完整算法	0.932±0.02	0.910±0.03
无增量聚类	0.785±0.04	0.700±0.05
无 Attention	0.872±0.03	0.841±0.04

4 结语

本文围绕零标签场景下的网络攻击检测难题，构建了以增量聚类与自适应反馈为核心的闭环框架，在真实大规模流量上验证了其对未知攻击的高检测率与长期稳定性。消融实验表明，各模块协同可显著缓解概念漂移带来的性能衰退。未来工作将探索跨域迁移机制，进一步提升算法在多云环境下的通用性与可扩展性。

参考文献：

[1] 周德坤，胡莉娜，叶露．基于相似度聚类的光纤通信网络流量异常检测方法 [J]. 微型电脑应用 ,2025,41(9):84-87.

[2] 尤刚，徐蕾，李美鹏，等．基于机器学习和规则的网络异常流量检测研究 [J]. 网络安全与数据治理 ,2025,44(2):1-9.

[3] 陈长松．基于均值聚类算法的网络链路安全监测系统设计 [J]. 现代计算机 ,2024,30(22):160-163.

[4] 税明星．基于模糊聚类的电力通信网络信息异常值挖掘方法研究 [J]. 数字通信世界 ,2024(11):62-64.

[5] 莫文中．基于 KNN 算法的电子通信网络节点异常流量告警方法 [J]. 佳木斯大学学报 (自然科学版),2024,42(10):21-23.

[6] 张仁飞，曾成．基于决策树挖掘的移动通信网络异常流量识别 [J]. 电信快报 ,2024(10):36-39.

[7] 关梅，冯宝珠，胡超．基于信息挖掘的计算机通信网络异常流量节点检测算法 [J]. 新乡学院学报 ,2024,41(9):46-51.

[8] 郭春．多聚类网络异常流量检测方法及应用研究 [J]. 软件，2024, 45(3): 122-125.

【作者简介】

陈琦昊（1990—），男，云南罗平人，本科，中级工程师，研究方向：网络舆情监测与分析。

（收稿日期：2025-11-12　修回日期：2026-06-09）