基于模糊熵的无线网络流量异常检测数学模型构建

古兰君[1] 樊多妮[1]
GU Lanjun FAN Duoni

摘 要 无线网络流量时序数据的非平稳性与高噪声干扰使得传统特征提取方法鲁棒性差，难以获取判别力强的稳健特征；同时，攻击行为的动态演化特性导致基于静态模型的检测机制存在概念漂移问题，检测准确率随时间衰减。为解决上述问题，文章提出一种基于模糊熵的自适应异常检测模型。该方法构建基础时间序列，通过计算连续流量变动的相像系数捕捉异常流量点，提取对噪声不敏感的综合异常流量特征。融合模糊熵原理，以提取的特征为基础进行相空间重构，定义模糊相似度并计算模糊熵，构建能够刻画流量序列复杂性的动态检测数学模型，输出初步检测结果。为克服概念漂移，引入自适应动态更新机制，该机制依据历史输出与实时流量预测动态调整检测阈值与参考基线，实现多目标同步异常判定与模型参数在线更新，从而保障检测系统长期运行的精准性与稳定性。实验结果表明：该方法将异常流量误检率控制在 4% 以下，检测精度显著提升，具备优越性能。

关键词 模糊熵；无线网络；流量监测；异常识别；数学模型；流量变动

doi：10.3969/j.issn.1672-9528.2026.05.022

0 引言

无线网络流量异常诱因复杂，集中表现为流量激增导致的网络拥塞，篡改数据导致的服务缺失等。这些异常行为往往具备强关联性和随机性，短时间内难以辨别及预测，导致网络运行受阻，严重的甚至会造成网络瘫痪，无法保障运行安全。为解决上述问题，提升异常流量检测能力，部分专业人员提出了应对性的建议。田博宇设计的无线通信网络异常流量动态检测方法[1]。采用随机森林决策树，设计无线通信网络异常流量特征提取流程，在提取全面特征后，以特征作为引导，计算任务分配节点权重，构建异常流量动态检测判断机制，但随机森林作为静态模型，难以快速适应动态演化的攻击行为，易出现概念漂移，导致检测准确率随时间衰减。郝莉萍等结合深度学习技术设计的无线通信网络异常流量攻击检测方法[2]。对流量数据进行预处理，从噪声中逐一去除隐藏的异常行为。提取基础特征，以特征作为驱动目标，利用深度学习技术，确定无线通信网络异常流量的攻击位置，最终完成目标的快速检测，然而固定预处理方式无法及时适应新攻击模式产生的异常特征，影响检测准确率。杨静设计的 GRU 融合无线传感器网络汇聚层流量异常检测方法[3]。运用多级离散小波变换算法，将预处理数据分解为多尺度子序列，深入提取多尺度特征信息，利用设定的阈值和特征值展开综合检测，实现目标任务的检测，但该算法对噪声较为敏感，处理高噪声数据时会影响特征提取准确性和鲁棒性。张兵等融合 FW-PSO 设计的大区域无线传感网络流量异常检测算法[4]。采用时间滑动窗口处理大区域无线传感网络数据流，用正态 Grubbs 法则剔除粗大误差值，可固定窗口难以适应非平稳数据，且该法则基于正态分布假设，易误判真实异常数据、降低特征判别力。

为此，本文面向无线网络异常检测中噪声敏感、特征判别力不足及模型适应能力有限等问题，构建基于模糊熵的异常检测数学模型。该方法通过提取流量时序的模糊熵特征量化其复杂度变化，融合多测度策略实现异常流量的精准识别，为无线网络安全防护提供新的研究思路。

1 融合模糊熵的网络流量异常检测数学建模

1.1 时间序列内噪声不敏感的综合异常流量特征提取

无线网络运行时，由于多种因素的影响，异常流量增加，基于实时增强的流量，先构建时间序列[5]。用公式表示为：

$$X=\{x_1,x_2,\ldots,x_n\} \tag{1}$$

式中：X 表示流量时间序列，x_n 表示变动目标。当无线网络出现异常，对应的流量也会形成不同程度的波动[6]。此时针对序列内流量的变化计算出相像系数。用公式表示为：

$$F_x=\frac{\int h(x)\kappa^2\mathrm{d}x}{\sqrt{\int h(x)\mathrm{d}x}^2\cdot\lambda(\kappa-\kappa')} \tag{2}$$

式中：F_x 表示无线网络变动环境下可控相像系数，$h(x)$ 表示正实函数，κ 和 κ' 分别表示连续、异常周期，λ 表示定义域。输出的相像系数一定程度上反映了无线网络的变动实况，采

1. 黄河交通学院通识教育学院 河南武陟 454950

用监测装置捕捉对应数据，展开归一化整合，锁定可能存在异常的目标点[7]。用公式表示为：

$$A=\sum_{i=1}h(x)^{i-1}\times F_x\cdot\left[\lambda\left(v\kappa-v\kappa'\right)\right] \tag{3}$$

$$p=F_x\sum_{o=1}vo+\frac{|\iota|}{|h(x)|} \tag{4}$$

式中：A 表示归一化处理目标，i 表示流量长度，v 表示最大长度，p 表示特征值，o 表示实时相像系数，ι 表示属性特征。不同于常规结果的是，归一化处理后的结果更为细化、多维，能够作为后续异常检测的参考依据[8]。

1.2 基于模糊熵原理的流量异常检测数学模型构建

完成时间序列内噪声不敏感的综合异常流量特征提取后，虽然已获得反映异常的综合特征，但仍存在难以直接观察和利用的隐藏模式与规律。为深入挖掘信息、提高异常流量判断的准确性与可靠性，需构建更精细的检测模型，模糊熵原理为此提供了有效途径。融合该原理构建流量异常检测数学模型，是对提取特征进一步挖掘分析的过程，通过相空间重构和定义模糊相似度计算模糊熵与异常阈值，模型能发现隐藏模式规律，且异常阈值可动态调整，提高对不同类型异常流量的适应能力。

基于无线网络的实际运行情况，首先开展相空间重构工作，该重构直接基于前述提取的异常流量特征序列，以挖掘其在高维空间中的动力学特性。同时，结合无线网络异常流量特征，定义目标的模糊相似度[9]。用公式表示为：

$$\begin{cases}Y_i=\{x_i,x_{i+1},\ldots,x_{i+n}\}\\ D_i^p=|\varpi|\times\dfrac{1}{N-h(x)}\displaystyle\sum_{l=1}\left(\lambda l-e^{h(x)^{i-1}}\right)\end{cases} \tag{5}$$

式中：Y_i 表示重构空间，x_{i+n} 表示叠加目标，D_i^p 表示相似度，ϖ 表示指数函数，N 表示相似容限，l 表示相似连续目标，$e^{h(x)^{i-1}}$ 表示分解对象。在相像系数和特征值的双向辅助下，明确测算出模糊熵和异常阈值，用公式表示为：

$$T_p=\ln\Phi^{\lambda}(x)-\ln\Phi^{\lambda+1}(x) \tag{6}$$

$$S_{T_p}=\frac{F_x}{\iota\cdot\int\left(A\kappa-A\kappa'\right)\mathrm{d}A}\times\Re h(x)^2 \tag{7}$$

式中：T_p 表示模糊熵，$\Phi^{\lambda}(x)$和$\Phi^{\lambda+1}(x)$分别表示不同维度异常流量特征变化，S_{T_p}表示异常阈值，$\Re$表示模糊熵均值。模糊熵值和异常阈值可以作为异常检测的约束条件及可参考相关标准，有助于检测结果的精准锁定。

1.3 基于模型输出的自适应动态更新与多目标异常判定

利用模糊熵值和异常阈值为判定参考，采用自适应动态更新的方式对多目标验证分析，输出最佳检测结果。先设计周期范围内的更新过程，用公式表示为：

$$J=\sqrt{v^{t+1}}\cdot\int\frac{1}{p}\times\varsigma\left(\kappa S_{T_p}-\kappa' S_{T_p}\right)\mathrm{d}p \tag{8}$$

式中：J 表示自适应更新结果，v^{t+1} 表示预测流量，ς表示更新阈值。无线网络更新后，不同环境下，受外部环境及特定因素的影响[10]，所出现的波动差异性较大，参考更新后的约束条件，对多目标同步判定，用公式表示为：

$$P=\left[\left(\frac{1}{J}\times\sum_{b=1}v^{t+1}b-\kappa' b\right)\cdot\aleph\right]\times\frac{F_x}{h(x)} \tag{9}$$

式中：P 表示异常流量判定结果，b 表示异常分类，$\aleph$表示同步目标。多周期时段内，异常流量的波动反映了网络的运行状态。针对异常流量的计算和目标点锁定，为管理人员提供维护依据，具有重要价值。

2 实验

为确保测试结果的真实可靠，对基于模糊熵的无线网络流量异常检测数学模型应用效果展开分析研究。在测试环境中，以 L 无线网络为目标测试对象，选取无线通信网络异常流量动态检测方法及深度学习下无线通信网络异常流量攻击检测方法作为对照组，按照实际的测试需求，部署实验环境及测试条件。

2.1 实验准备

为验证所提模型在非平稳与高噪声干扰环境下的有效性，布设了对应的测试环境。搭建 NS-2 WSNs 应用平台，设置实时处理能力在 10~12 Gbit/s，网络接口为 10 Gbit/s Ethernet，通过 ST-Visualizer 进行实时检测和目标辨识处理。为模拟真实无线网络中的信道噪声与背景干扰，在实验平台中注入了高斯白噪声，信噪比（SNR）设定为 10~15 dB 的动态范围，构建高噪声干扰的测试背景。实验过程中，为保证控制稳定性，还需增设 SSD 系统辅助操作，增加同步控制的协同性。调整无线网络流量的检测应用参数及标准，如表 1 所示。

表 1 无线网络流量检测应用参数

检测应用指标	参数标准值
带宽利用率 /(Mbit/s)	900~1 000
抖动 /ms	10~18
丢包率 /%	4.5~5.5
设备连接数 / 台	12~24
覆盖监测节点数量 / 个	6~8
单目标识别耗时 /s	0.2~0.5
参与测试单项攻击总次数 / 次	20

表 1 中参数的设置可以统一控制条件，但是无线网络异常流程的变动不具有规律性，为避免检测遗漏，需要接入实时的监测系统，实现关联辅助，如图 1 所示。

将图 1 捕捉的数据以及流量信息按照周期汇总，存储在数据库内作为后续检测的参考。测试时为强化实验环境的多变性和随机性，需要导入辅助测试的攻击条件，拟定复杂环境，生成不同类型的异常流量，如表 2 所示。

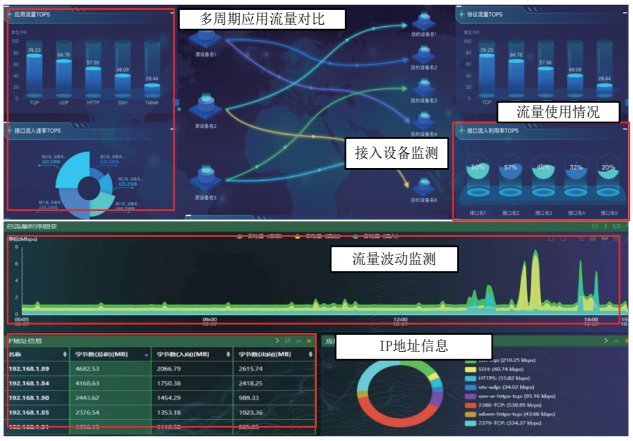

图 1 网络流量实时变动监测平台

表 2 不同类型辅助测试攻击条件

攻击类型	缩写	说明
拒绝服务攻击	DoS	以耗尽目标资源的方式，导致系统无法服务
中间人攻击	MITM	窃取篡改通信数据，造成 ARP Spoofing 的欺骗
恶意软件	Worm	自我复制传播，恶意破坏网络
应用层攻击	HTTP	发送大量 HTTP 请求，导致无法服务
持续性威胁	APT（Zero-Day Exploit）	长期潜伏，窃取敏感数据，阻止系统持续运行

将表 2 不提供类型的攻击条件转换为统一的格式，导入实验网络之中，完成实验环境的有效部署，进行测试验证。

2.2 网络流量异常捕捉结果

无线网络运行过程中，当出现 10~15 dB 噪声且同时受到隐藏攻击，会形成异常流量。捕捉对应时段的异常流量目标，输出结果如图 2 所示。

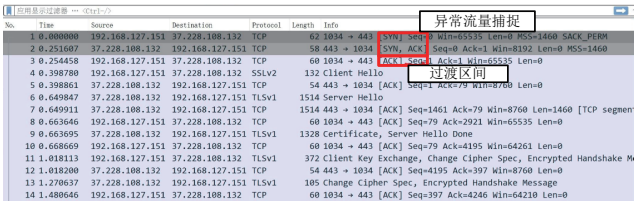

图 2 网络流量异常捕捉结果

根据图 2 结果分析可知：复杂环境下，该方法可以快速、精准地识别无线网络中的异常流量点，并在相对位置上设置标记。而过渡区间的锁定一定程度上也有助于与前后流量展开对比，输出更为精准的检测结果。通过测算无线网络流量变动相像系数，快速区分、确定异常流量的各个区间，根据提取的特征值展开搜索，标记并汇总相似性较强的目标，完成多目标同步捕捉任务，在实践过程中针对性提升，为后续异常判定提供了基础依据。

2.3 复杂环境下异常流量漏检结果

为增加测试环境的多变性和对比性，在当前网络环境内，随机选择恶意软件、拒绝服务攻击以及中间人攻击三种辅助测试条件，在随机触发机制进行异常流量漏检结果的分析，具体如图 3 所示。

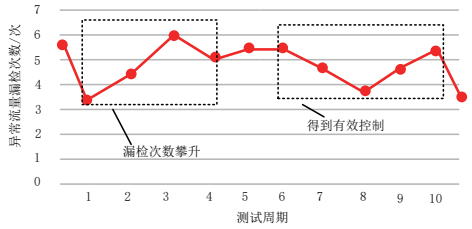

图 3 异常流量漏检次数结果

根据图 3 结果研究可知：1~4 周期内，网络流量在短时间内剧增，漏检次数也随之出现攀升的情况，但是均在可控的范围内，即为 10 次以下，灵活性与调整性较好。6~10 周期中，相较于前 4 个周期，漏检次数得到了进一步控制，降低为 3 次左右，这也表明针对异常流量的综合检测能力得到提升。以网络流量异常捕捉结果作为参考，基于设计的数学模型以及模糊熵、阈值等约束条件，对图 3 输出的结果细化，精准锁定异常流量的位置，漏检频次被有效控制，具有实际的应用价值。

2.4 性能结果对比分析

设定表 2 中所有攻击方式为可触发条件，利用选择的三种方法验证异常流量的误检率，误检率结果如图 4 所示。

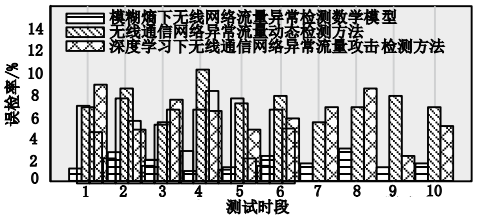

图 4 异常流量误检率结果对比

根据图 4 结果分析可知：模糊熵无线网络流量异常检测数学模型所输出的误检率均低于 4%；无线通信网络异常流量动态检测方法应用下的误检率分布在 0%~10% 之间；深度学习下无线通信网络异常流量攻击检测方法处于 0%~8% 以内。融合模糊熵检测结果，采用自适应动态更新的方式对该结果持续训练、对比、筛选，降低错误检测的概率，确保最终结果的精准性，具有优越的性能。

3 结语

本文针对无线网络流量时序数据存在的非平稳性与高噪声干扰问题，以及因攻击行为动态演化导致的静态检测模型概念漂移现象，提出一种基于模糊熵的自适应异常检测模型。该方法首先通过计算流量变动相像系数提取噪声不敏感的综合特征，随后融合模糊熵原理，在相空间重构基础上构建能

申威平台安全启动机制设计与实现

李之健[1] 苏卫强[1] 赵翊含[1]
LI Zhijian SU Weiqiang ZHAO Yihan

摘 要 当前，信息系统广泛依赖国外软硬件产品，存在严重安全隐患，如恶意后门、远程操控等潜在风险。申威处理器虽具备完全自主知识产权，但其安全启动能力仍有待加强。针对现有 UEFI 安全启动方案在申威架构下兼容性差、依赖国际密码算法等局限，文章结合我国在可信计算技术与 SM2/SM3/SM4 等国密算法体系，提出一种基于国产可信密码模块（TCM）为硬件可信根的多级安全启动方案。构建了从固件到操作系统的逐级验证信任链，支持启动过程的主动度量与完整性验证，具备抵御固件篡改、引导器劫持等攻击能力。在申威平台的实验结果表明，该启动机制能有效阻断多种启动阶段攻击，显著提高了申威平台的主动防御能力，为国产化信息系统的安全启动提供了可行的技术路径。

关键词 申威；安全启动；信任链

doi：10.3969/j.issn.1672-9528.2026.05.023

0 引言

随着我国信息化建设的高速发展，信息系统已经在军事、金融、能源、交通等各个行业领域得到了广泛应用，推动社会发展。然而，发展的进程始终与安全挑战相伴而生。计算机病毒、网络攻击与窃密事件频发，信息安全问题愈发严峻[1]。我国各类信息系统对国外产品的依赖也会带来潜在的安全风险。如英伟达对华出售的 H20 芯片被爆出存在“追踪定位”“远程关闭”技术，已被国家互联网信息办公室约谈[2]。由此可见，对国外软硬件的普遍依赖已成为信息系统的潜在风险源，可能导致泄密或影响信息系统正常运行。要从根本上解决此类

1. 无锡先进技术研究院 江苏无锡 214083

够刻画流量复杂性的检测模型，并引入自适应动态更新机制以持续优化检测阈值与参考基线。实验结果表明，在信噪比为 10~15 dB 的高噪声模拟环境下，该方法对 DoS、MITM、Worm 等多类攻击均能实现有效识别与精准标记，异常区间划分清晰，无明显重叠或漏标。漏检次数随系统运行逐步收敛，最终稳定在较低水平。与基于随机森林和深度学习的对照方法相比，本文方法在各攻击场景下的误检率均稳定控制在 4% 以下，展现出更优的鲁棒性与检测一致性。

参考文献：

[1] 田博宇 . 无线通信网络异常流量动态检测方法研究 [J]. 无线互联科技 ,2025,22(10):106-110.
[2] 郝莉萍 , 马迎辉 , 邬迎 . 基于深度学习的无线通信网络异常流量攻击检测方法 [J]. 长江信息通信 ,2025,38(4):172-175.
[3] 杨静 . 基于 GRU 的无线传感器网络汇聚层流量异常检测方法 [J]. 宁夏师范大学学报 ,2025,46(1):81-90.
[4] 张兵 , 卞利 . 基于 FW-PSO 的大区域无线传感网络流量异常检测算法 [J]. 传感技术学报 ,2023,36(7):1116-1121.
[5] 赵伟娜 , 马凯 . 多模态无线传感网络节点流量异常自调节研究 [J]. 传感技术学报 , 2025, 38(4):711-716..
[6] 王洁 , 吕奕飞 . 基于流量异常特征的无线网络攻击行为检测方法 [J]. 电脑知识与技术 ,2024,20(11):78-80.
[7] 吕广旭 , 王小英 , 冯燕茹 , 等 . 基于 VAE-GMM 的高级持续威胁攻击异常流量检测 [J]. 计算机应用与软件 , 2025, 42(11): 325-330.
[8] 安义帅 , 付钰 , 俞艺涵 , 等 . 基于数据增强与特征挖掘的异常流量检测方法 [J]. 通信学报 ,2025,46(8):16-30.
[9] 陈涛 , 薛皓铭 , 马宇翔 , 等 . 基于自适应联邦学习的边端协同网络异常流量检测模型 [J]. 计算机应用研究 , 2025, 42(11): 3461-3467.
[10] 卢庆武 , 赖坤宁 . 网络动态入侵多层特征最优检测方法仿真 [J]. 计算机仿真 , 2025,42(6):379-383.

【作者简介】

古兰君（1996—），女，河南郑州人，硕士，助教，研究方向：数学教学。

樊多妮（1986—），女，河南焦作人，硕士，讲师，研究方向：主题网络爬虫技术。

（收稿日期：2026-01-08 修回日期：2026-05-20）