基于多传感器融合的通信网络异常流量监测方法

张 涛[1] 李倩倩[1] 罗理机[1]
ZHANG Tao LI Qianqian LUO Liji

摘 要 复杂工业通信网络中，存在大差异多传感器采集外部信息，导致异常流量监测的阈值存在多样性。当前方法以单一阈值完成异常流量检测，存在监测精度低、监测时效性差的问题。通过引入多传感器信息融合技术，设计一种工业通信网络异常流量监测方法。首先，应用多传感器融合技术，为改善局部滤波器的估计精度，选用丢失观测的预报值作为补偿，在此基础上，给出任意两个估计误差之间的互相协方差矩阵，利用该滤波方法实现对通信网络数据滤波处理。然后，基于矩阵模型的平面和 2D 坐标属性，将流量特征指纹库按一定的规律进行排序，因为特征经验库具有识别通信网络流量异常的作用，通过与位置特征相结合的方法，建立异常流量匹配模型，对网络中的异常流量进行监测，并确定异常流量产生位置。最后，实验结果表明，新的监测方法具备更高的监测精度，同时能够保证良好的监测时效性，实现对异常流量的快速监测反馈。

关键词 多传感器融合；通信网络；流量监测；数据融合；单一阈值

doi：10.3969/j.issn.1672-9528.2024.02.039

0 引言

在工业通信网络中，异常流量监测对于维护工业网络的安全和稳定至关重要。传统的异常流量监测方法往往依赖于单一的阈值，无法全面通过多传感器准确地掌握网络状况。工业通信网络中的异常流量通常指与正常流量分布规律不符的流量，如拒绝服务攻击、病毒传播、网络钓鱼等恶意行为产生的流量 [1]。这些异常流量不仅会影响网络的正常运行，还可能对用户的隐私和财产造成威胁。因此，对工业通信网络中的异常流量进行监测，有助于及时发现并处理这些问题，提高通信网络的质量和安全性。异常流量监测技术在通信网络中的应用已经越来越广泛。通过对异常流量的有效监测，网络运营商可以及时发现并处理各种网络安全问题，保障通信网络的稳定性和安全性 [2]。未来，随着人工智能技术的发展，基于机器学习和深度学习的监测方法将成为主流。同时，随着 5G、物联网等新技术的普及，异常流量监测技术也将面临更多的挑战和机遇。

近年来，学者们对通信网络异常流量监测方法进行了广泛的研究。以此为例，文献 [3] 中，王莎莎提出了一种基于深度学习的通信网络流量实时监测方法。它具有较高的准确性和实时性，能够自动学习复杂的流量模式。然而，该方法需要大量标记数据和计算资源，并且解释困难。文献 [4] 中，沈嘉慧提出了基于sFlow技术的通信网络流量实时监测方法。该方法具有实时监测和较低的存储需求的优势。然而，由于采样误差和监测精度的限制，其精确性相对较低。文献 [5] 中，张玲玲提出了一种基于 PSO 算法的通信网络流量异常智能监测方法，具有自适应性和较好的可解释性。然而，该方法存在较高的计算复杂性和参数调整可能较为困难的问题。

为解决上述方法中存在的问题，本文结合多传感融合技术，开展对通信网络异常流量监测方法的设计研究。

1 多传感器下的通信网络数据融合

在获取工业通信网络数据时，需要结合实际所需分不同情况，采用传感器进行采集。如果需要全面采集网络中的数据报文，可以考虑 Sniffer 嗅探法。这种方法可以捕获工业网络中的所有数据，并且可以完全复制网络中的数据，因此适用于需要详细分析网络流量数据的场景。

如果只需要采集特定类型的数据，可以考虑使用 SNMP。该方法能够定期地从路由器存储器中提取 IP 记账记录，并对对应的存储记录进行清理，以便下一步的数据收集。如果需要采集的数据量很大，但是不需要完全复制所有的数据报文，可以考虑使用 sFlow。该算法只需设定特定的抽样速率即可，且不会对网络设备的性能造成太大的影响。此外，在 sFlow 中还包含了诸如 MAC 地址、协议类型、TCP/UDP 端口号，以及应用层协议之类的信息。对于一些简单的网络流量分析任务来说是足够的。考虑到通信网络环境复杂，为

1. 湖北工业大学 信息技术中心 湖北武汉 430068
[基金项目] 湖北省教育厅科学研究计划指导性项目，项目编号：B2020043，项目名称：面向图像分类的深层网络优化算法研究

了避免通信干扰、观测丢失和乘性噪声对异常流量监测的影响，结合多传感器融合技术，对获取到的通信网络数据进行融合和滤波处理[6]。图 1 为基于多传感器融合的通信网络数据分布式融合结构图。

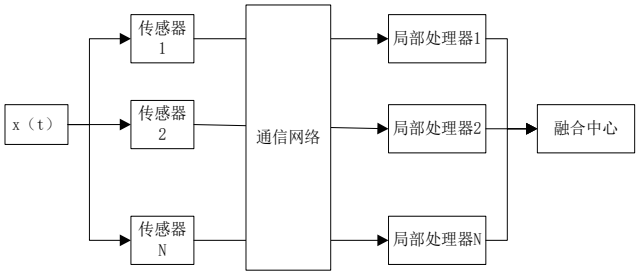

图 1 基于多传感器融合的通信网络数据分布式融合图

结合图 1 所示融合图，构建多传感器离散随机函数为：

$$x(t+1)=[\Phi_0(t)+\xi(t)\Phi_1(t)]x(t)+\Gamma(t)\omega(t) \quad (1)$$

式中：$x(t+1)$ 表示 $t+1$ 时刻多传感器状态矢量；$\Phi_0(t)$、$\Phi_1(t)$ 表示未知干扰信号；$x(t)$ 表示局部滤波器端接收观测值；$\Gamma(t)$ 表示传感器观测输出结果；$\omega(t)$ 表示噪声。在该多传感器离散随机函数中存在未知通信干扰、乘性噪声等不确定因素[7]。

因此，在融合的过程中，设置一个 Bernoulli 分布的随机变量序列 $g_i(t)$。当 $g_i(t)=1$ 时，此时多传感器观测数据没有丢失，传感器经由通信网络按时到达局部滤波器段；当 $g_i(t)=0$ 时，此时存在传感器观测数据丢失的情况[8]。为了改善局部滤波器的估计精度，选用丢失观测的预报值作为补偿，通过局部滤波器设计观测数据满足下述条件。

$$z_i(t)=g_i(t)y_i(t)+D_i(t)x(t+1) \quad (2)$$

式中：$z_i(t)$ 表示局部滤波器观测数据；$y_i(t)$ 表示丢失观测的预报器；$D_i(t)$ 表示转置信号。分布式融合滤波器因其并行化的特点，在容错性、可靠性和故障诊断方面都有很大的优势。在此基础上，给出任意两个估计误差之间的互相协方差矩阵，利用该滤波方法实现对通信网络数据滤波处理。

2 工业通信网络流量特征提取

针对通信网络中出现的各种异常情况，提出了一种多个终端间高效的通信连接方式。在采用这种方法进行通信时，借助互联网上的 TCP/IP 协议，使得多个终端间的通信能够消除网络中的低层差别，保证多个终端间的通信效率[9]。在完成对端的通信连接后，对上述通过多传感器融合和滤波处理的通信网络数据，提取通信网络流量特征[10]。为确保所提取的通信网络流量特征有足够的可信度，在特征提取完毕之后，应该设置一个有效的可信区间。用 N_c 来表示区间，那么 N_c 的表达式为：

$$N_c=1-z_i(t)^{\left(\frac{\ln(1-\alpha\%)}{\alpha}\right)} \quad (3)$$

式中：α 表示通信数据包占用网络通信流量比例。根据公式（3）进行运算，获得不同的 N_c 值，并以求出的极大值和最小值为可信区间的界限，从而提取出通信网络流量的特征。

通信网络流量特征提取是指从采集到的网络流量数据中提取出有用的信息，以供后续分析和应用。假定有多个分组要被共享并传送，则根据分组在通信网中所占的份额来抽取其特征，这个过程可以表达为：

$$\sigma^2=N_c{}^2\frac{\alpha(1-\frac{\alpha}{n})}{n(n-1)} \quad (4)$$

式中：σ 表示通信网络流量特征；n 表示特征提取行为的发生次数。

在掌握了其特点之后，进行规范化的建设[11]。为通信网络异常流量监测建立一个经验库。表 1 为通信网络流量特征经验库基本格式。

表 1 通信网络流量特征经验库基本格式

序号	流量类型	特征	最大值
（1）	TCP-SYN	直接通信	65
（2）	Worm.exe	常规通信	12
（3）	SQL	数据库通信	50
（4）	UPD	直接通信	15
（5）	ICMP	直接通信	25
（6）	UPD	UPD 通信	15
（7）	Opasoft	直接通信	2650

按照表 1 中记录的数据，针对不同的流量类型对应 N_c 取值进行判断，为后续通信网络异常流量监测提供参考。在实际应用中，需要进行进一步寻找并剔除可信度较小的特征，以此提高监测方法的运行速率[12]。对于提取到的通信网络流量大小的特征，可用 $B=\{B\}$ 表示，B 为通信网络流量大小。针对提取到的流量协议数据内容，结合 SV 报文协议内容，选取数据包长度、源地址、目的地址等信息，得到协议内容特征。

3 流量异常判定规则设计与异常监测

在完成对通信网络流量特征的提取后，对通信网络流量异常判定规则进行设计。通过流量异常判定规则的制定可以实现对异常流量特征的量化，在上述构建的通信网络流量特征经验库中包含了流量的大小特征、协议特征以及协议内特征等内容[13]。利用流量特征经验库的流量大小特征可以实现对流量是否存在异常的判定。通过协议类型特征可实现对异常流量是否存在规则外通信链路的判定。通过协议数据内容特征可以实现对通信网络所连接设备是否产生异常流量的判定[14]。基于矩阵模型的平面和 2D 坐标属性，将流量特征指纹库按一定的规律进行排序，因为特征经验库具有识别通信网络流量异常的作用。通过与位置特征相结合的方法，建立异常流量匹配模型，对网络中的异常流量进行监测，并确定异常流量产生位置[15]。通信网络异常流量矩阵可表示为：

$$\Delta=\begin{bmatrix}\sigma_{11} & \cdots & \sigma_{1m}\\ \sigma_{21} & \cdots & \sigma_{2m}\\ \sigma_{31} & \cdots & \sigma_{3m}\end{bmatrix} \quad (5)$$

式中：Δ 表示通信网络异常流量矩阵；$\sigma_{11}...\sigma_{1m}$ 表示流量特征；$\sigma_{21}...\sigma_{2m}$ 表示数据特征；$\sigma_{31}...\sigma_{3m}$ 表示类型特征。对上述构建的矩阵中每一个矢量长度进行统计，并将得到的统计结构存储在矢量 $\boldsymbol{\mu}$ 当中。结合表 1 中记录的内容，建立一个标准参照矩阵 Δ'，对 Δ 和 Δ' 作差，得到新的矩阵 $\boldsymbol{\rho}$，对 $\boldsymbol{\rho}$ 当中每一行中的 0 元素数量进行统计，并将其标记为 $zero(\rho_i)$，将统计结果存储在矢量 $\boldsymbol{v}$ 当中，将矢量 $\boldsymbol{\mu}$ 与矢量 $\boldsymbol{v}$ 作差，得到新的矢量 $\boldsymbol{\lambda}$。若矢量 $\boldsymbol{\lambda}$ 当中所有的元素数据均不超过设定的阈值，则说明该行位置上形成了匹配。并且，此时在异常监测输出中既包含了通信网络流量特征的异常信息，又包含了异常流量信息相关的网络位置信息。根据上述内容，完成对通信网络流量异常判定规则的设计。基于该判定规则，对通信网络流量进行实时监测，并对通信网络环境中是否存在异常流量进行判定。在监测过程中可以按照时间序列方法，这种方法将网络流量数据看作时间序列数据，通过时间序列分析提取出网络流量的周期性和趋势性等特征，并设定正常流量的阈值，当流量数据超过阈值时，判定为流量异常。例如，可以设定每天的流量峰值和谷值的阈值，当流量数据超过这些阈值时，就认为出现了流量异常。

4 对比实验

4.1 实验准备

通过实验验证本文上述基于多传感器融合监测方法与现有监测方法相比在实际应用中的可行性和有效性。为了提高实验的真实性，选择某企业内部运营专网作为研究对象。据公司的工作人员反映，这一通信网络在使用过程中，常常会出现中断、卡顿等异常情况，因此，本文选取这一通信网络进行研究是很有可行性的。在选定了被监测对象之后，将实验中的终端和监测装置进行对接，将这次的监控模式设置为在线监控。

4.2 实验环境与参数设置

在实验开始之前，为防止实验中发生异常现象，必须在监控终端上设置监控装置的额定工作参数。具体参数设置如表 2 所示。

表 2 监控装置额定参数

参数	数值
工作电压	1 300.0 V
额定电流	280.0 ～ 500.0 A
终端对监控结构的反馈	1.0 次 /s
工作频率	300.0 ～ 1 250.0 Hz

将该方案与 MTU 的工作环境相连接，其具体的工作环境如表 3 所示。

表 3 工作环境设置

项目	数值
网络流量监测器	10 台
数据包捕获设备	5 台
路由器和交换机	20 台
服务器和计算机	3 台
异常流量监测管理软件	1 个
数据处理和分析软件	1 个
存储系统容量	1 TB
数据处理平台	高性能计算服务器

选取网络峰值时间，在该时间段的前 250.0 s 内，进行通信业务异常监控，并用折线形式画出该通信网络在运行过程中的实际流量变化结果，如图 2 所示。

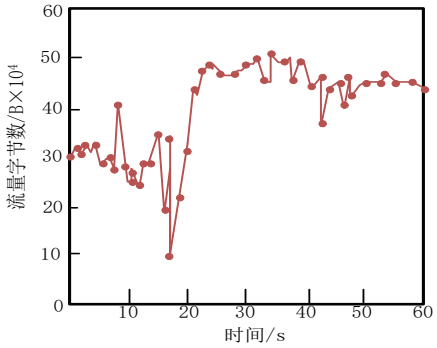

图 2 通信网络运行中流量变化情况图

从图 2 可以看出，在实验过程中，该通信网络流量呈现出逐渐增加的趋势，从 40 s 开始逐渐平稳，保持最高流量变化水平。

4.3 实验结果分析

分别利用本文提出的基于多传感融合的监测方法（实验组）、文献 [4] 基于 PSO 算法的监测方法（对照 A 组）、文献 [5] 基于 Socket 的监测方法对上述所选择的通信网络流量进行监测。在利用本文提出的监测方法进行对异常流量的监测时，准备多种类型的传感器，如网络流量传感器、防火墙传感器、入侵检测系统（IDS）传感器等，用于采集通信网络中的流量数据和安全事件数据。将图 2 所示流量变化作为依据，对比三种监测方法的检测结果，得到如图 3 所示的结果。

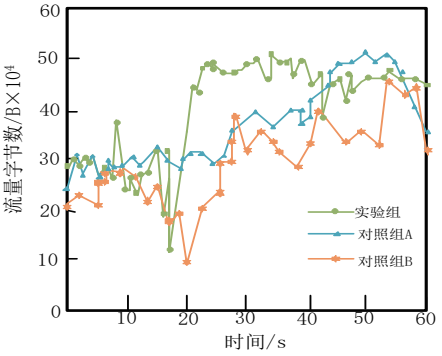

图 3 不同方法作用下的监测效果对比结果

通过对比图 2 和图 3 得到的监测结果可以看出，实验组监测方法得到的结果与该通信网络流量实际变化更加接近，而对照 A 组和对照 B 组监测结果均与实际情况存在较大出入，由此可以看出，实验组监测方法具备更高的监测精度。

为进一步验证三种监测方法对异常流量监测的性能，对三种方法监测到异常流量的反馈时间进行对比，反馈时间越长，说明对应的监测方法监测时效性越差，反之，反馈时间越短，说明对应的监测方法监测时效性越强。根据上述分析，针对随机的五个流量异常点（分别编号为 I 点、II 点、III 点、IV 点和 V 点），将三种监测方法的监测反馈时间记录如表 4 所示。

表 4 三种监测方法监测反馈时间记录表

序号	流量异常点	反馈时间 /s		
		实验组	对照 A 组	对照 B 组
（1）	I 点	0.42	1.25	1.85
（2）	II 点	0.41	1.52	1.95
（3）	III 点	0.46	1.56	1.84
（4）	IV 点	0.48	1.54	1.86
（5）	V 点	0.41	1.52	1.84

从表 4 中记录的数据可以看出，实验组对异常流量监测反馈的时间能够始终控制在 0.50 s 以下，而对照 A 组和对照 B 组监测方法反馈时间均超过 1.00 s。由此可以看出，实验组监测方法的监测反馈时效性更强。

综合上述实验得到的结果可以证明，基于多传感融合技术的监测方法在实际应用中可以实现对流量的高精度监测，同时保证监测反馈的时效性，具有极高的应用价值，值得广泛应用和推广。本文实验结果和分析结论，为通信网络异常流量监测提供参考和建议。例如，可以根据实验结果选择适合特定场景的异常监测方法，或者提出综合使用多种方法的建议，以提高通信网络异常流量监测的准确性和鲁棒性。

需要注意的是，对比实验需要充分考虑实验的设计和实施细节，确保实验结果的准确性和可重复性。同时，还需要根据实际需求选择合适的方法进行实验和分析，以获得最佳的实验效果和应用价值。

5 结语

通信网络异常流量监测是保障网络稳定性和安全性的重要手段。本文提出的基于多传感器融合的通信网络异常流量监测方法能够有效地提高异常流量的识别准确率和实时性。通过多个传感器的数据融合，能够更全面、准确地反映通信网络的流量状况，及时发现异常流量，为企业的网络安全和稳定运营提供了有力保障。在实际应用中，该方法表现出了良好的效果和潜力，值得进一步研究和推广。

参考文献：

[1] 张耀雷 , 白洋 , 隋鹏 . 一种通信网络性能监测及综合分析技术研究 [J]. 通信管理与技术 ,2023(3):47-50.

[2] 蒋志颀 , 范雷 . 基于机器学习的无线通信网络安全漏洞智能监测系统 [J]. 电子设计工程 ,2021,29(15):115-119.

[3] 王莎莎 . 基于深度学习的通信网络流量实时监测方法 [J]. 长江信息通信 ,2023,36(8):161-163.

[4] 沈嘉慧 . 基于 sFlow 技术的通信网络流量实时监测方法 [J]. 长江信息通信 ,2023,36(1):178-179+182.

[5] 张玲玲 . 基于 PSO 算法的通信网络流量异常智能监测方法 [J]. 信息与电脑 (理论版),2023,35(10):88-90.

[6] 伍坪 . 基于 ZigBee 通信网络的农机作业监测系统设计 [J]. 农机化研究 ,2024,46(1):146-150.

[7] 高文林 , 马永超 . 卫星通信网络信号智能监测系统设计 [J]. 无线互联科技 , 2023,20(7):14-16.

[8] 王维维 . 基于嵌入式以太网的智能变电站通信网络状态监测 [J]. 北京石油化工学院学报 ,2023,31(2):49-53.

[9] 郭天一 . 基于 ZigBee 通信网络公园生态园林维护机械监测系统 [J]. 农机化研究 , 2023,45(9):201-204+208.

[10] 赵志俊 . 基于机器学习的通信网络安全漏洞监测系统设计 [J]. 长江信息通信 ,2022,35(12):175-177.

[11] 温圣军 , 韩春晓 , 袁刚 , 等 . 主动式通信网络性能自动监测方法 [J]. 自动化技术与应用 ,2022,41(10):142-145.

[12] 李秋月 , 孙俊 . 基于卷积神经网络的通信网络漏洞监测系统设计 [J]. 长江信息通信 ,2022,35(8):71-73.

[13] 王珂 . 高速公路通信网络全流量安全及威胁监测平台研究 [J]. 中国信息化 ,2022(6):63-64.

[14] 孙学波 , 李志福 , 王元杰 , 等 . 基于 5G 通信网络的高精度无线微震监测技术研究 [J]. 矿业安全与环保 , 2022, 49(2): 83-90.

[15] 熊水平 . 基于 NetFlow 技术的造纸生产通信网络在线监测系统 [J]. 造纸科学与技术 ,2022,41(2): 55-61.

【作者简介】

张涛（1979—），男，湖北汉川人，硕士研究生，高级工程师，研究方向：计算机网络。

李倩倩（1986—），女，湖北宜城人，硕士研究生，工程师，研究方向：网络工程、人工智能。

罗理机（1990—），男，湖北武汉人，硕士研究生，工程师，研究方向：网络工程、云计算。

（收稿日期：2023-11-27）