ISCAS 中国科学院软件研究所学术年会’2024
暨重点实验室科技活动周

关键技术

基于多类型特征融合的僵尸网络流量智能检测方法

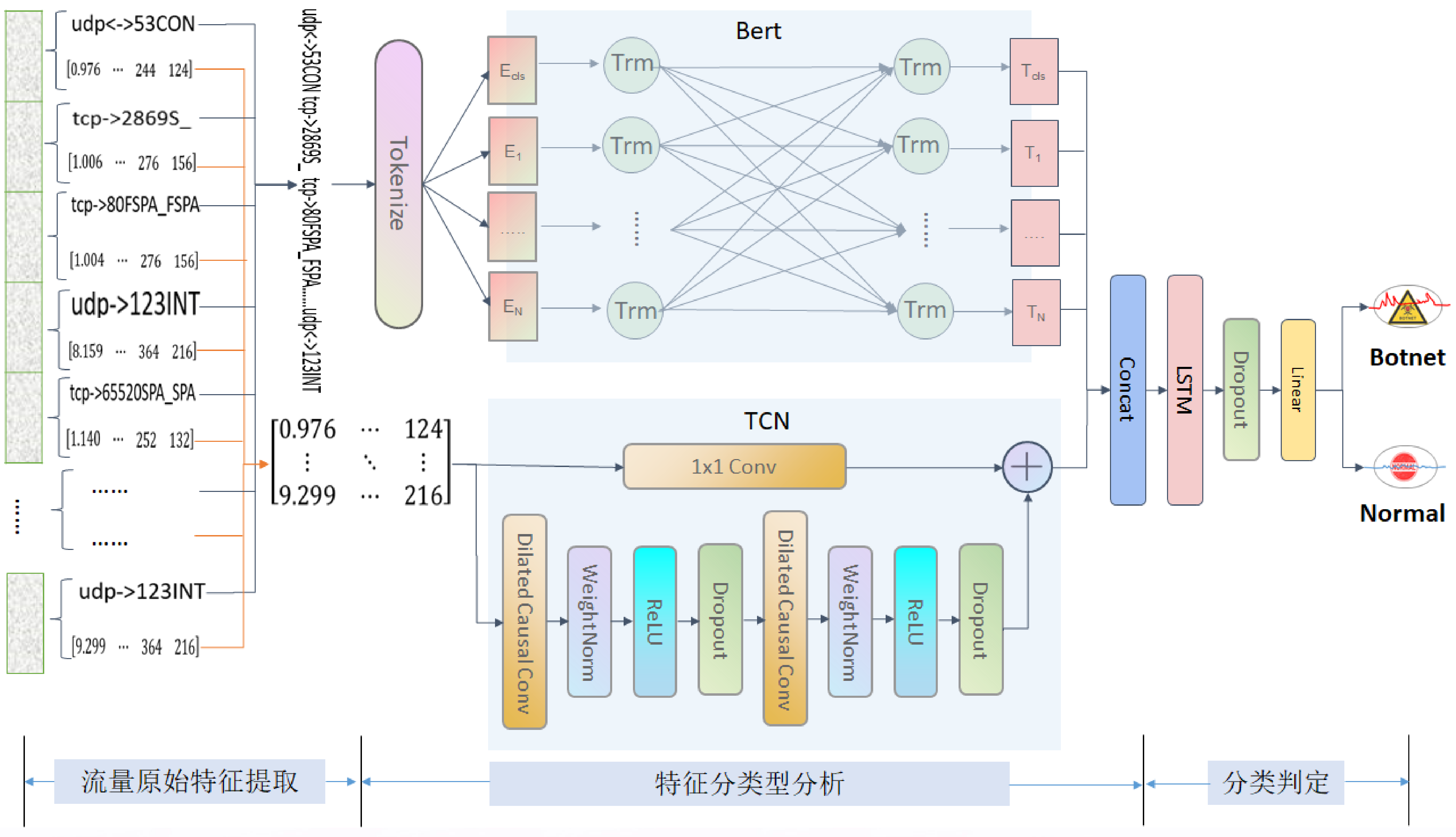
黄克振，连一峰，张海霞

联系方式：黄克振，15201067285，kezhen@iscas.ac.cn

工作介绍

随着信息技术的飞速发展，僵尸网络攻击已逐渐成为具有高危害程度的网络安全威胁，僵尸网络流量检测是识别发现僵尸网络的有效手段之一。当前已有的僵尸网络流量检测方法存在误报率高、人工特征工程等局限性，针对这些局限性，本工作提出一种基于多类型特征融合的僵尸网络流量智能检测方法。首先，该方法对某主机发出的网络流量按照时序关系进行排列，进而对滚动窗口内的网络流量利用B-TCN（Bert and Temporal Convolutional Network）模型挖掘网络流量间通信协议、通信状态、通信方向、通信端口等非数值型特征间共存模式以及通信时长、通信数据包数量、通信数据字节数等数值型特征间潜在的局部及全局统计特性，最后，基于网络流量在非数值型特征共存模式、数值型特征的统计特性方面存在的差异进行分类检测。

总体框架



检测效果

CTU-13是混杂正常网络流量及Neris、Rbot、Virut、Menti、Sogou、Murlo、NSIS.ay等7种恶意软件产生的僵尸网络流量的大规模数据集。基于该数据集，本方法在准确率、精确率、召回率和F1值等各项指标上均超过了99%。

表1 CTU-13数据集数据分布

Id	Duration(hrs)	# Packets	#NetFlows	Size	Bot	#Bots
1	6.15	71,971,482	2,824,637	52GB	Neris	1
2	4.21	71,851,300	1,808,123	60GB	Neris	1
3	66.85	167,730,395	4,710,639	121GB	Rbot	1
4	4.21	62,089,135	1,121,077	53GB	Rbot	1
5	11.63	4,481,167	129,833	37.6GB	Virut	1
6	2.18	38,764,357	558,920	30GB	Menti	1
7	0.38	7,467,139	114,078	5.8GB	Sogou	1
8	19.5	155,207,799	2,954,231	123GB	Murlo	1
9	5.18	115,415,321	2,753,885	94GB	Neris	10
10	4.75	90,389,782	1,309,792	73GB	Rbot	10
11	0.26	6,337,202	107,252	5.2GB	Rbot	3
12	1.21	13,212,268	325,472	8.3GB	NSIS.ay	3
13	16.36	50,888,256	1,925,150	34GB	Virut	1

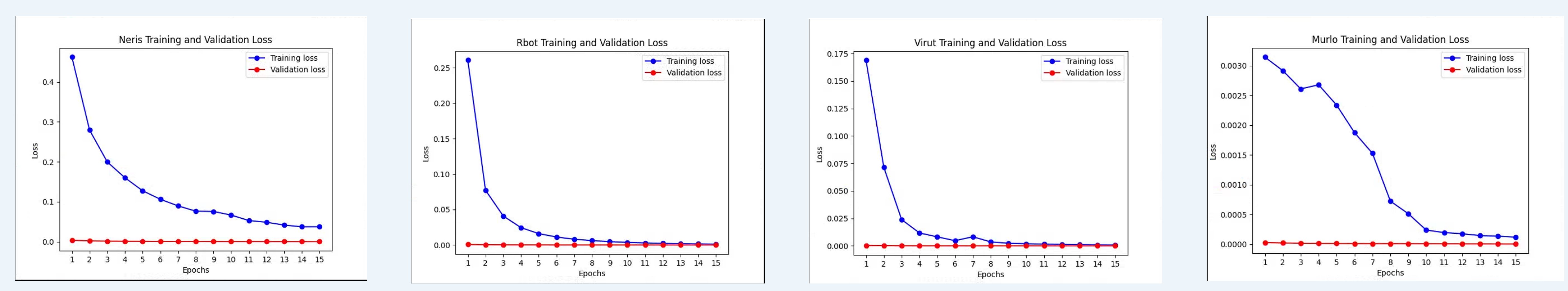


图1 训练损失率及验证损失率曲线

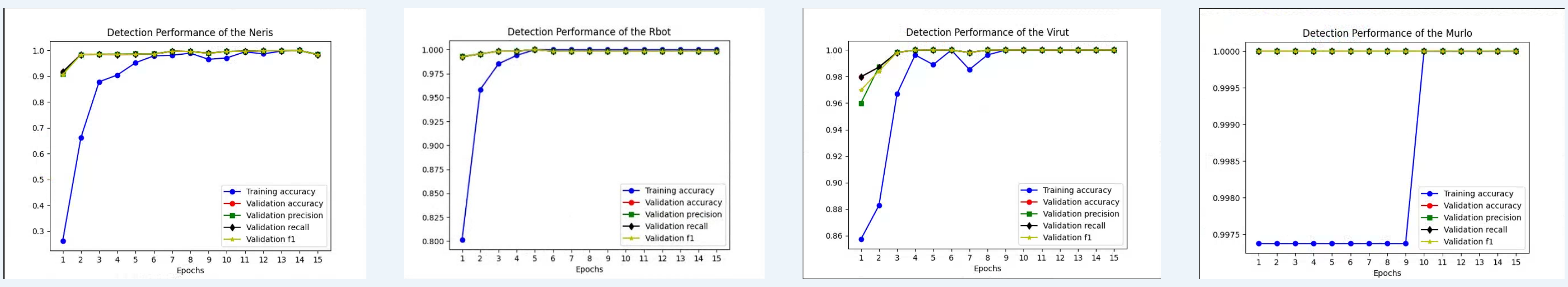


图2 检测效果评价指标曲线