

小样本下基于度量学习的僵尸网络检测方法

林宏刚^{1,2}, 朱竣菁^{1,2}, 陈麟³

(1. 成都信息工程大学网络空间安全学院, 四川 成都 610225; 2. 先进密码技术与系统安全四川省重点实验室, 四川 成都 610225;
3. 网络空间安全态势感知与评估安徽省重点实验室, 安徽 合肥 230037)

摘要: 僵尸网络给互联网带来了极大的威胁, 尽早有效地检测出僵尸网络对于维护网络空间安全具有重要的实践意义。然而在僵尸网络发现初期, 可获得带标记样本数量较少, 这使得目前大部分基于深度学习的检测方法无法得到充分训练, 导致检测结果不佳。因此, 提出了一种用于小样本下的基于度量学习的僵尸网络检测方法 BT-RN, 利用基于任务的元学习训练策略优化模型, 在任务中引入验证集并通过度量验证样本和训练样本特征表示之间的相似度来快速累积经验, 从而降低模型对标记样本空间的依赖; 引入了特征级注意力机制, 通过计算特征中各维度的注意力系数, 重新整合特征表示并分配重要度关注来优化特征表示, 从而减少深度神经网络在小样本中的特征稀疏问题; 引入了残差网络设计模式, 利用跳跃链接来规避增加特征级注意力机制模块后, 较深的网络所带来的模型退化和梯度消失风险。实验结果表明, 在小样本背景下, 所提僵尸网络检测方法的正确率和模型泛化能力优于其他小样本检测方法和深度学习检测方法。

关键词: 僵尸网络; 流量检测; 小样本检测; 度量学习

中图分类号: TP309.5

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023076

Metric-based learning approach to botnet detection with small samples

LIN Honggang^{1,2}, ZHU Junjing^{1,2}, CHEN Lin³

1.School of Cyberspace Security, Chengdu University of Information Technology, Chengdu 610225, China

2.Sichuan Key Laboratory of Advanced Cryptography and System Security, Chengdu 610225, China

3.Anhui Key Laboratory of Cyberspace Security Situational Awareness and Assessment, Hefei 230037, China

Abstract: Botnets pose a great threat to the Internet, and early detection is crucial for maintaining cybersecurity. However, in the early stages of botnet discovery, obtaining a small number of labeled samples restricts the training of current detection models based on deep learning, leading to poor detection results. To address this issue, a botnet

收稿日期: 2022-11-21; 修回日期: 2023-04-28

通信作者: 陈麟, linhg@cuit.edu.cn

基金项目: 国家 242 信息安全计划 (2021-037); 网络空间安全态势感知与评估安徽省重点实验室开放课题 (CSSAE-2021-002)

Foundation Items: The National 242 Information Security Plan(2021-037), Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation Open Project (CSSAE-2021-002)

引用格式: 林宏刚, 朱竣菁, 陈麟. 小样本下基于度量学习的僵尸网络检测方法[J]. 网络与信息安全学报, 2023, 9(5): 33-47.

Citation Format: LIN H G, ZHU J Q, CHEN L. Metric-based learning approach to botnet detection with small samples[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 33-47.

detection method called BT-RN, based on metric learning, was proposed for small sample backgrounds. The task-based meta-learning training strategy was used to optimize the model. The verification set was introduced into the task and the similarity between the verification sample and the training sample feature representation was measured to quickly accumulate experience, thereby reducing the model's dependence on the labeled sample space. The feature-level attention mechanism was introduced. By calculating the attention coefficients of each dimension in the feature, the feature representation was re-integrated and the importance attention was assigned to optimize the feature representation, thereby reducing the feature sparseness of the deep neural network in small samples. The residual network design pattern was introduced, and the skip link was used to avoid the risk of model degradation and gradient disappearance caused by the deeper network after increasing the feature-level attention mechanism module.

Keywords: botnet, traffic detection, few-shot detection, metric learning

0 引言

国家互联网应急中心发布的互联网安全报告^[1-2]显示,截至2022年5月,各僵尸网络家族的控制规模和实施攻击的活跃度依旧维持在较高水平,网络空间持续遭受着巨大的僵尸网络攻击威胁,有效检测僵尸网络对于维护网络空间安全具有实际意义。僵尸网络是由一群被攻击者恶意控制的僵尸主机所组成的网络,攻击者可以利用命令与控制(C&C, command and control)信道远程操控受控主机,并发起一系列的非法活动。大部分基于深度学习的僵尸网络检测模型需要足够多的已标记训练数据,当已标记样本数量较少时,模型容易学习到单个样本特点并认定为一般性规律,导致模型过拟合和泛化能力下降,进而检测准确率下降。

小样本下的僵尸网络检测方法主要存在以下问题。① 拟合问题。当新型僵尸网络攻击刚被发现时,往往很难在短时间内获得足够多的、分布良好的优质样本。在小样本背景下,避免产生拟合问题并且得到高检测准确率是挑战之一。② 特征提取问题。对于不同类型的僵尸网络,其流量特征往往是具有共性和差异的,如何在小样本背景下使特征提取模型保留共性、弱化差异、提高检测准确率的检测能力是挑战之一。

因此在样本数量较少背景下,有效训练模型并检测识别出僵尸网络攻击流量是值得研究的问题。为有效应对上述挑战,本文提出了基于度量学习的小样本僵尸网络检测方法——BT-RN (botnet relation network) 方法。为避免传统训练策略在小样本下产生严重的训练偏差导致拟合问题,本文使

用了元学习思想训练模型,解决样本空间依赖以及泛化能力差的问题;为了提升特征提取模块的特征提取能力,尽可能为下游分类器提供优质的特征表示,本文改进了混合注意力机制,并提出适用于僵尸网络的卷积块注意力机制(BT-CBAM, botnet convolutional block attention module)。为了避免BT-CBAM的引入造成网络加深,引发梯度消失问题,特征提取模块采用残差网络的设计模式。

综上所述,本文的主要贡献和创新如下。

1) 采用基于任务的元学习训练策略。每轮任务随机学习不同的僵尸网络类型,在每轮任务中通过对比验证集和训练集样本的特征表示,利用少量样本快速积累经验,提升模型的学习能力,快速优化模型的拟合能力和泛化能力。

2) 提出一种用于优化僵尸网络流量特征图的特征级注意力机制,提升模型的特征提取能力。BT-CBAM从空间和通道两个角度出发,通过计算不同维度上特征的注意力分数,优化特征表示,使模型更加关注与正常流量相比具有区分性的重要维度的特征信息,得到具有高共性的僵尸网络特征图表示。

1 相关工作

1.1 僵尸网络检测

基于异常分析检测^[3]僵尸网络的大部分解决方案是以海量已标记样本为检测背景的,如统计分析法^[4-5]、分布式方法^[6]、机器学习法^[7-10]、深度学习法^[11-16]等。

文献[4-5]提出了基于统计分析的检测方案,对攻击行为的统计属性进行建模,以检测僵尸网

络异常流量。Spathoulas 等^[6]提出了一种基于分布式方法的检测方案,即设计和部署多个检测器来处理多维的大数据集,以提高检测的灵活性。Wang 等^[7-9]提出了基于支持向量机、随机森林和聚类算法的检测方案,通过预先收集专业的先验知识,建立检测僵尸网络的模型。

Jung 等^[11]改进了 LeNet-5,提出了一种 8 层卷积神经网络(CNN, convolutional neural network)深度学习模型,用于自动检测数据中的功耗差异,识别僵尸网络攻击。但大数据集下的检测准确率为 84%,该模型特征提取能力尚有提升空间。Wang 等^[12]提出了将原始流量转为二维灰度图后,再结合 CNN 进行恶意流量分类工作,实验结果表明二维灰度化原始流量可有效利用 CNN 视觉识别优势,但识别未知类型流量的能力尚不足。尹传龙等^[13]将具备长期信息记忆能力的长短期记忆(LSTM, long short-term memory)网络应用于僵尸网络检测,解决了标准循环神经网络(RNN, recurrent neural network)存在的长序依赖问题。罗扶华等^[14]结合 CNN 的视觉识别优势和 LSTM 的记忆优势,进一步提升了模型特征提取能力,在 5.3 GB 的 ISCX2014 数据集上实验误报率为 1.2%,但离开大样本环境,检测能力未知。谭越等^[15]将双向长短期记忆(BiLSTM, bi-directional long short-term memory)网络和残差机制引入模型中,从时间和空间维度训练分类器,通过解决 LSTM 向后编码问题,有效提高了对已知僵尸网络的准确率,但对未知僵尸网络检测精确度不足 80%。Yerima 等^[16]串行堆积了 100 个隐藏层,建立了深度神经网络(DNN, deep neural network)检测模型,特征提取能力得到了提升,但模型忽略了深度网络存在梯度消失的风险。

1.2 元学习

元学习的提出是为了让模型从相关的任务上学习到经验,并应用到新的任务中。在小样本入侵检测方面,元学习思想发挥了重要的作用。

Olasehinde 等^[17]在 2020 年首次将元学习思想与入侵检测问题相结合,提出了一种基于三元级算法的入侵检测方法,在小样本检测中得到了高于原有检测方案的最高准确率。Xu 等^[18]将成熟的元学习框架应用在入侵检测的小样本检测中,

提出了 FC-Net。该网络从成对的流量样本中计算得出相应的特征图,然后度量样本相似度得出分类结果。这种深度神经网络和元学习思想的结合,很好地解决了样本缺失问题,并且该网络具有高泛化性。Tang 等^[19]将基于度量的原型网络应用在物联网入侵检测系统中,设计了 ConvProtoNet 模型,实验证明模型在小样本背景下通过元学习思想可获得好的学习能力,且取得比机器学习更高的检测准确率。Pan 等^[20]将卷积 LSTM 网络和一种时间序列原型网络相结合,解决了物联网在恶意网络行为方面的指纹推断问题。Hindy 等^[21]将基于度量的孪生网络应用在入侵检测系统中,上游并联两个深度网络,下游使用非固定的度量函数计算待测样本与支持集数据的相似度,以分类正常流量和攻击流量。在 1-shot 检测中,获得了 74.55% 的检测准确率,检测效果良好。

2 本文方法

本文提出了一种基于度量学习的检测方法 BT-RN 用于小样本僵尸网络检测。训练策略上,本文采用基于任务的元学习思想训练模型,元学习中验证集的概念使得模型能够在少量训练样本背景下快速积累经验,并迅速推广到新的任务中且继续提升模型学习能力。网络结构上,本文采用基于度量的思想设计模型。首先,本文在特征提取模块引入了用于僵尸网络流量特征优化的混合注意力机制 BT-CBAM,重点关注特征图中具有辨识性的部分(注意力分数较高的部分)及平衡样本中携带的共性和差异特征,以提取不同类型僵尸网络中更具共性、更高表达能力的特征,尽可能为下游分类器提供优质的特征表示。然后,特征提取模块设计上使用残差网络的设计模式,避免 BT-CBAM 的引入造成网络加深,引发梯度消失问题。最后,根据特征提取模块得到的特征表示,利用可学习度量模块计算并得出分类结果。BT-RN 检测流程如图 1 所示。将流量转为二维灰度图像作为特征提取模块的输入,通过特征级注意力机制 BT-CBAM 优化特征表示;利用可学习度量模块计算验证样本与训练样本的相似度分数,得出分类预测结果。

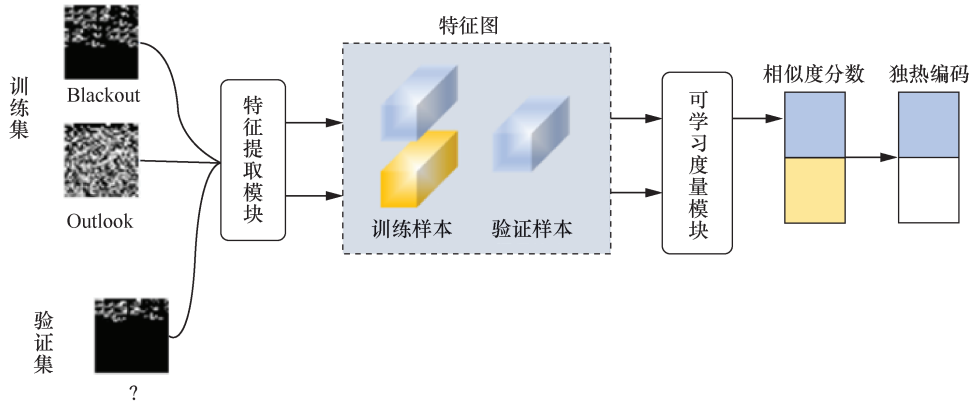


图 1 BT-RN 检测流程
Figure 1 BT-RN detection process

2.1 元学习训练策略

尽管深度学习模型的迭代训练模式在大规模已标记样本下效果良好,但当极少量带标签训练样本时,会出现严重的拟合问题。这种小样本下的僵尸网络流量检测是一种小样本学习^[18] (FSL, few-shot learning) 问题的现实应用。研究者使用了迁移学习思想微调预训练模型^[22],用于 FSL 检测,但在新任务上仍依赖大量带标签数据^[23]。而人类却能从少量示例中学习到高泛化性的知识表示。元学习提供了一种与人类学习方式类似的新的学习模式,即模型可以通过少量多次学习来获得经验,并利用这些经验来改进自身算法^[24]。因此,本文选择了在元任务空间上进行快速训练,避免模型过度依赖实例空间,通过基于任务的度量学习更快地应对一些未见过的僵尸网络样本或类型。

首先对问题进行定义:在任务上,将任务 T 定义为 $T = \{T_{\text{src}}, T_{\text{tar}}\}$, T_{src} 表示训练阶段使用的源任务集, T_{tar} 表示元测试阶段使用的目标任务集,两个集合相互独立。其中,若元训练阶段含有 M 个任务,记 $T_{\text{src}} = \{(T_{\text{src}}^{\text{train}}, T_{\text{src}}^{\text{val}})^{(i)}\}_{i=1}^M$; 若元测试阶段含有 N 个任务,记 $T_{\text{tar}} = \{(T_{\text{tar}}^{\text{train}}, T_{\text{tar}}^{\text{test}})^{(j)}\}_{j=1}^N$ 。在数据集上,将数据集 D 分为训练集、验证集和测试集 3 个部分,记 $D = \{D_{\text{train}}, D_{\text{val}}, D_{\text{test}}\}$ 。其中,若训练集 $T_{\text{src}}^{\text{train}}$ 含有 C 个不同类,且每类含有 K 个样本,验证集 $T_{\text{src}}^{\text{val}}$ 每类中含有 B 个样本,则该 FSL 问题称为 C -way K -shot。任务集与数据集关系如图 2 所示。

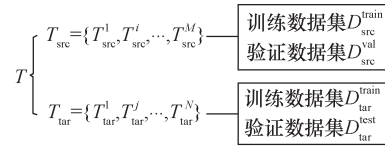


图 2 任务集与数据集的关系
Figure 2 The relationship between task sets and datasets

每一次学习时,从 T_{src} 中任意选择一个源任务 $T_{\text{src}}^{(i)}$ 作为本次学习目标,然后在 D_{train} 对应的 C 类中每类随机抽取 K 个样本作为样本集 $S = \{(x_i, y_i)\}_{i=1}^M$,在 D_{val} 对应的 C 类中每类随机抽取 B 个样本,作为验证集 $Q = \{(x_j, y_j)\}_{j=1}^N$,再将 S 和 Q 输入模型中得出分类结果。元训练的步骤如下。

$$\tau^* = \arg \max_{\tau} \log p(\tau | D_{\text{src}}) \quad (1)$$

经过 P 轮学习,逐步优化元知识 τ^* 。在元测试阶段,利用元训练阶段得到 τ^* ,在每一个新的目标任务 j 上进行测试^[25],元测试步骤如下。

$$\theta^* = \arg \max_{\theta} \log p(\theta | \tau^*, D_{\text{tar}}^{\text{train}}) \quad (2)$$

元测试阶段的计算受益于式(1)计算得到的元知识 τ^* ,在此基础上,结合新目标任务的训练样本的特征,获得更准确的预测分类结果。

以“2-way 1-shot $B=3$ ”问题为例,任务集和数据集分配如图 3 所示。元训练时,每次学习从 T_{src} 中随机选择一个源任务 $T_{\text{src}}^{(i)}$ 作为本次学习目标, $T_{\text{src}}^{(i)}$ 中含有一类僵尸网络流量和一类正常流量,从这 2 类流量中分别随机抽取 1 个样本

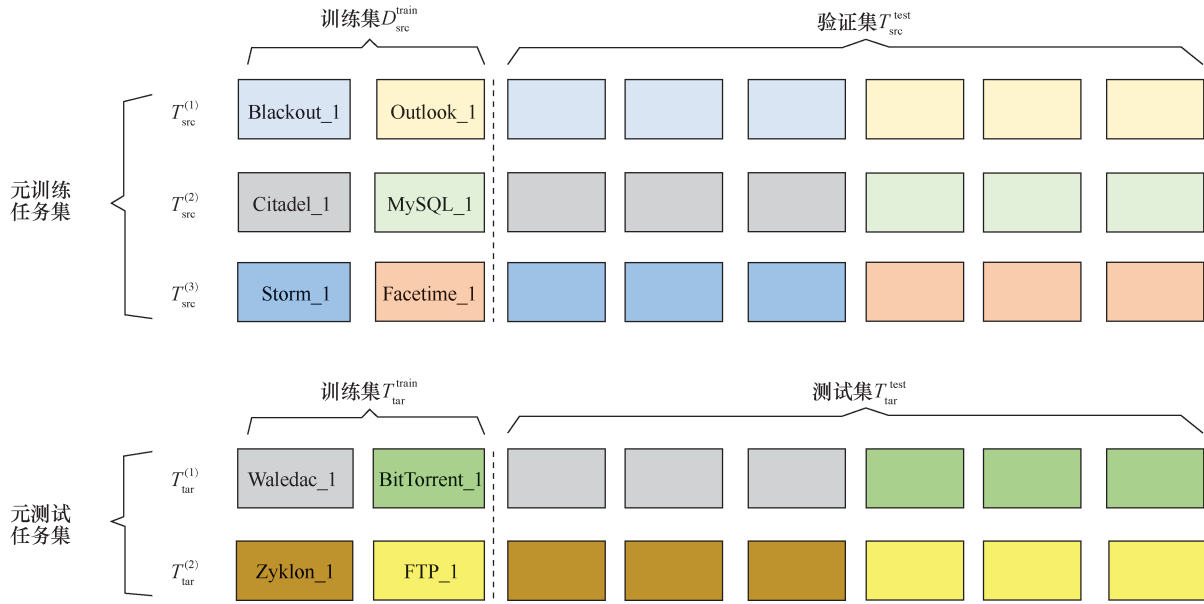


图 3 “2-way 1-shot $B=3$ ”问题下的任务集和数据集分配
Figure 3 Task sets and datasets allocation for “2-way 1-shot $B=3$ ” problem

作为本次任务的样本集 S , 然后在 D_{val} 对应类中随机抽取 3 个样本作为本次任务的验证集 Q 。经过 P 轮任务学习迭代, 模型得到元知识, 再应用到测试集中测试评估模型。

2.2 基于特征级注意力机制和残差网络的特征提取模块

2.2.1 特征级注意力机制 BT-CBAM

FSL 因各类流量样本量少, 且 CNN 以局部出发, 利用卷积核有限的感受视野去感受上一层的局部特征, 这种计算模式忽略了各个局部特征的整体相关性, 生成了稀疏的特征表示。这很容易受到小噪声的影响^[22]。事实上, 并非验证样本特征空间的所有维度就足以做出明确的分类, 并且带有噪声的提取结果可能会导致下游分类结果的巨大偏差。针对这些问题, 本文在文献[22]的基础上, 设计了一种用于僵尸网络流量特征优化的特征级注意力机制 BT-CBAM, 以缓解稀疏和小噪声的问题。通过计算特征空间中各维度的注意力系数, 对各维度特征进行整合并分配重要度关注, 使 CNN 能够注意到一系列的局部信息, 将注意力集中在注意力系数高的重要部分, 从而缓解特征稀疏问题, 增强模型特征提取的鲁棒性和有效性, 进而提高模型检测的准确性。

BT-CBAM 的结构如图 4 所示, 由通道注意

力 Att_c 和空间注意力 Att_s 两部分组成。从通道和空间的维度出发, 同时关注“是什么”“在哪里”两类重要信息。为了充分利用通道注意力的计算结果, 结构设计上, 舍去了原始混合注意力机制^[26] (CBAM, convolutional block attention module) 中的跳跃链接^[27], 采用了垂直布局模式。

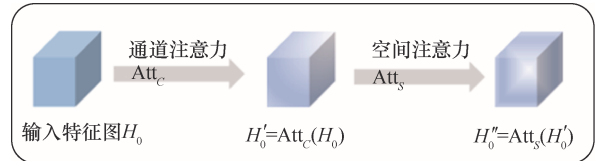


图 4 BT-CBAM 的结构
Figure 4 BT-CBAM structure

BT-CBAM 的通道注意力模块 Att_c (结构如图 5 所示) 由 Squeeze 模块、Excitation 模块两部分组成。Squeeze 模块在空间域上并行计算全局平均池化 (GAP_s , global average pooling) 和全局最大池化 (GMP_s , global max pooling), 整合了空间维度上的特征信息。Excitation 模块为避免降维对 Att_c 产生负面影响, 使用了共享一维卷积。利用 k 邻居模拟跨通道交互, 分别计算出两类特征图, 再对其逐元素相加后激活得到通道注意力图 H_0' 。

BT-CBAM 空间注意力模块 Att_s (结构如图 6

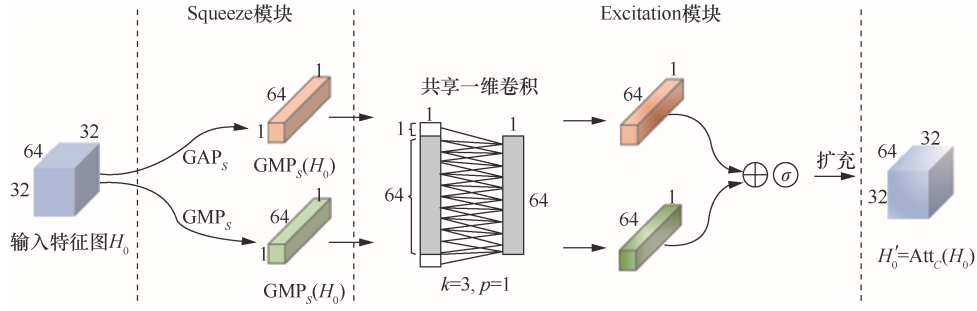


图 5 BT-CBAM 的通道注意力模块 Att_C
Figure 5 Channel attention module Att_C for BT-CBAM

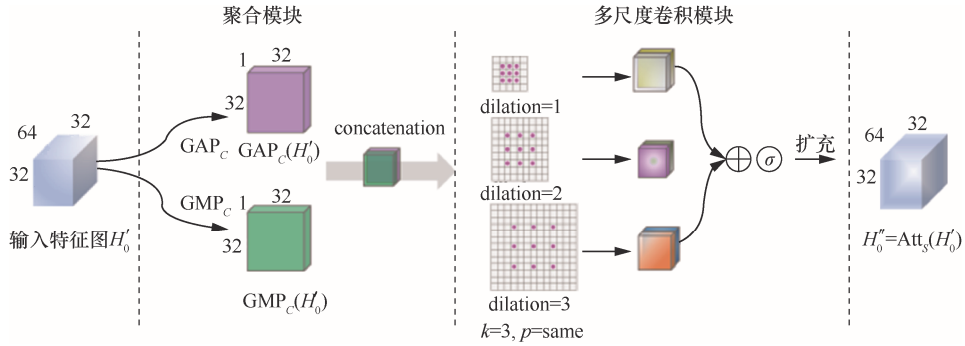


图 6 BT-CBAM 的空间注意力模块 Att_S
Figure 6 Spatial attention module Att_S for BT-CBAM

所示)由聚合模块和多尺度卷积模块两部分组成。聚合模块在通道域上计算 GAP_C 和 GMP_C 得到两个通道为 1 的空间特征图, 并将其在通道域上进行拼接得到有效表示, 以此突出重点信息区域。多尺度卷积模块中, 为避免大尺度卷积核和多卷积核引起计算量增加, 模块引入了 Inception V1^[28] 设计模式, 使用了扩张率为 1、2、3 的空洞卷积核来提取全局和局部等多个特征, 丰富感受野的同时, 尽量减轻计算量。最后对 3 个空洞卷积的计算结果进行逐元素相加并激活, 得到注意力图 H''_0 。

2.2.2 残差网络

CNN 和 BT-CBAM 的结合加深了检测模型网络, 这可能导致模型退化或梯度消失等问题。为

此, 本文引入了残差网络^[27] (ResNet, residual network), 利用跳跃链接的“短路”机制缓解深度网络中的梯度消失和模型退化问题^[29]; 设计了专用于特征提取模块的残差块 FeatureAttResNet。FeatureAttResNet 结构示意图如图 7 所示, 模块内部将跳跃链接设置在了两个卷积层和注意力模块的前后, 完成残差学习后再使用激活函数激活。计算上, 将输入记为 x , 经过中间 3 层网络的表示学习得到 $F(x)$, 再将输入 x 和 $F(x)$ 逐元素相加进行信息融合, 最终学习得到特征表示, 具体公式如下。

$$F'(x) = x + F(x) \quad (3)$$

$F'(x)$ 表示 x 经过一个残差块的计算过程。最后利用 LeakyReLU 函数对计算结果进行激活,

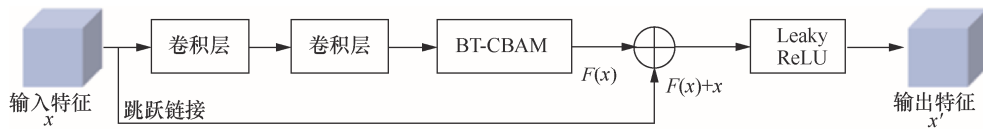


图 7 FeatureAttResNet 结构示意图
Figure 7 Schematic of FeatureAttResNet structure

得到完整特征表示 x' 作为 FeatureAttResNet 的输出。

$$x' = \text{LeakyReLU}(F'(x)) \quad (4)$$

为得到更强的特征表示,使用3个相似的 FeatureAttResNet 残差块提取样本流量的特征,具体设置如下。残差块 I: 卷积层使用 64 个 3×3 卷积核;残差块 II: 使用 128 个 3×3 卷积核;残差块 III: 使用 256 个 3×3 卷积核。输入样本经过 3 个基本残差块的维度变换如图 8 所示。

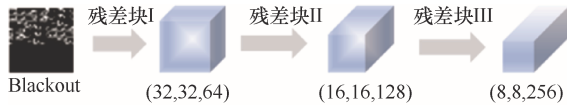


图 8 经 FeatureAttResNet 的维度变换
Figure 8 The dimensional transformation via FeatureAttResNet

2.3 可学习的度量模块

由于度量函数的选择会对模型分类结果产生重大影响^[22],为了提高模型对不同僵尸网络流量的分类能力,本文使用了关系网络^[30]的度量概念:可学习的深度度量网络。相较于匹配网络^[31]和原型网络^[32]的固定度量方式,这种深度度量网络可以随训练任务数量的增加,优化调整其参数,以达到更好的分类效果。优化后的特征表示被输入度量网络中,先与验证样本进行依次拼接组合,再利用深度度量网络计算出相似度分数,进而做出分类预测。

1) 为便于度量计算,训练样本的特征图与验证样本的特征图逐一拼接。前一模块输出的训练集和验证集的两种特征图,维度均为 $(8, 8, 256)$,每轮有 $C(K+B)$ 个特征图。图 9 为“2-way 1-shot $B=1$ ”问题下的预处理,即对输出的 2 个训练样本特征图和 1 个验证样本特征图的处理结果。

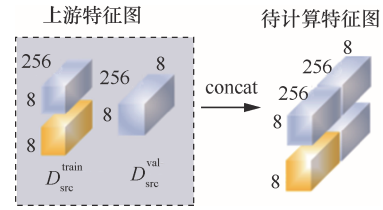


图 9 “2-way 1-shot $B=1$ ”问题下的预处理
Figure 9 Pre-processing under "2-way 1-shot $B=1$ " problem

2) 利用深度网络模型计算训练样本与验证样本的相似度分数。深度度量网络结构如图 10 所示。在设计思路,使用两层卷积残差块以达到更充分提取特征和避免模型退化的目的,使用 GAP_s 以达到在空间域上压缩且同时可抑制过拟合的目的。网络结构上,拼接好的特征图先经过两层卷积残差块,再使用 GAP_s 在空间域上进行维度压缩得到附带全局信息的相似度向量,接着利用两个全连接层对所有信息进行整合特征信息,最后采用 Sigmoid 激活函数得到相似性计算结果。

3 实验评估

3.1 数据集

本文实验使用了 ISOT、CTU-13 和 USTC-TFC2016 这 3 个数据集。表 1 列出了 3 种数据集的基本情况与抽样情况。

ISOT 数据集是由维多利亚大学的 ISOT 组织在虚拟机中收集的一组恶意流量数据,属于仿真数据集。本文选择了 5 类僵尸网络流量,再从每类中各随机抽样 400 个样本作为训练集,随机抽样 900 个样本作为测试集。

CTU-13 数据集是捷克理工大学在内部实验室捕获的一组僵尸网络流量数据,属于真实流量数据。本文选取了 4 类僵尸网络流量,再从每类中各随机抽取 500 个样本作为训练集,随机抽取

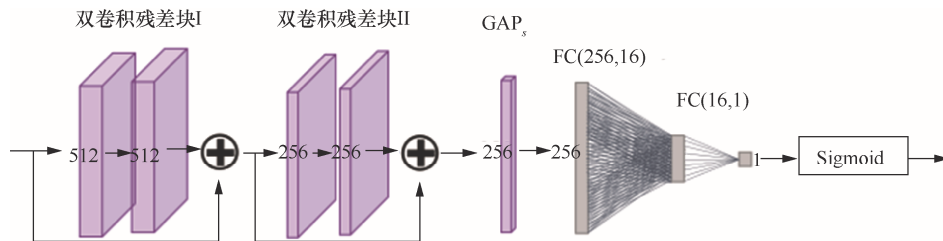


图 10 深度度量网络结构
Figure 10 Deep metric network structure

表 1 数据集的基本情况及抽样
Table 1 Dataset basics and sampling

数据集	流量类型	是否真实	流量协议类型	僵尸网络类型	训练样本/个	测试样本/个
ISOT	Botnet	否	P2P	Waledac、Strom	2 000	4 500
			HTTP	Blackout、Citadel、Zyklon		
CTU-13	Botnet	是	IRC	Neris、Rbot	2 000	2 000
			P2P	Zeus		
			HTTP	Virus		
USTC-TFC2016	Benign	是		9 种应用流量	2 700	2 700

500 个样本作为测试集。

USTC-TFC2016 数据集是由 Wang 等^[12]整理的正常通信流量数据。本文从中选择了 9 种应用流量作为阴性数据样本，并从每类中各随机抽取 300 个样本作为训练集，随机抽取 300 个样本作为测试集。

3.2 预处理

为便于模型统一化处理，本文选择了尺寸为 32×32 的二维灰度图作为模型输入格式。整个预处理包含 3 个部分：流量筛选、数据清洗、格式转换。

第一步：流量筛选。本文选择了含有更多交互数据和标记信息的“会话+所有层”流量数据。第二步：数据清洗。考虑原流量样本集可能存在受污染数据，先对截取后数据进行重复或相似文件清洗，再随机化处理 IP 和 MAC 信息。第三步：格式转换。首先将所有数据处理为 1 024 byte，文件过小则末尾填充 0，文件过大则末尾舍弃。预处理后的流量二维灰度图示意如图 11 所示。

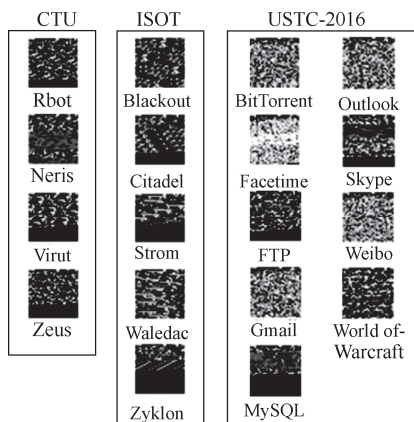


图 11 预处理后的流量二维灰度图示意
Figure 11 Illustrative two-dimensional grey scale diagram of the pre-processed flow

3.3 实验设置

3.3.1 实验环境

本文针对小样本背景下的僵尸网络流量检测，对计算资源没有较高要求。本文配置如下：硬件处理器使用 Intel Core i7-8550U CPU @ 1.80 GHz，内存 16 GB，显卡为 NVIDIA GTX 940MX，Windows10 家庭版 64 位操作系统。

3.3.2 实验方法

为了验证本文方法可用于小样本僵尸网络检测，将 BT-RN 与以下 3 种小样本方法进行了对比：基于 FC-Net 的方法^[18]、基于原型网络的方法^[20]、基于孪生网络的方法^[21]。为增强可信度，小样本方法的度量模块与本文保持一致。

为了验证基于任务的元学习训练策略优于传统的深度学习训练策略，将 BT-RN 与以下基于深度神经网络的方法进行了对比：基于 CNN 的方法^[12]、基于 LSTM 的方法^[13]、基于 LSTM_CNN 的方法^[14]、基于 BiLSTM_CNN 的方法^[15]、基于 ViT 的方法^[33]、基于 CoAtNet 的方法^[34]。为增强可信度，基于深度神经网络的方法在卷积层设置上与本文方法保持一致。

为了证实本文方法具有良好的鲁棒性和泛化能力，本文在未知类型僵尸网络上进行了验证：同源实验和异源实验。同源实验是指实验中所有的数据均来自同一数据集，异源实验是指实验中训练阶段和测试阶段使用的数据来自不同数据集。

实验设置如表 2 所示。

3.3.3 参数设置

本文方法主要针对僵尸网络检测中的二元分类问题，故设置 $C=2$ ，即将网络流量分为正常流量和僵尸网络流量两个类别。为模拟小样本场景，本文设置了 $K=1$ 和 $K=5$ 两种场景，两种场景中查

询样本每类均为 15 个。其中, $K=1$ 场景中, 每次学习任务的正常和僵尸网络样本分别为 1 个; $K=5$ 场景中, 每个学习任务的正常和僵尸网络样本分别为 5 个。考虑到僵尸网络的类型多样, 故训练时每个 episode (episode 为一次选择训练集和验证集类型的过程) 选取 1 种僵尸网络类型和 1 种正常流量类型进行学习。episode 设置为 400。此外, 还引入数据扩增避免过拟合, 对输入样本随机进行旋转, 如旋转 90° 、 180° 、 270° 。

表 2 实验设置
Table 2 Experimental setups

实验分类	检测类型	具体设置
小样本方法对比	已知类型样本	基于 FC-Net 的方法 ^[18]
		基于原型网络的方法 ^[20]
		基于孪生网络的方法 ^[21]
BT-RN		
深度学习方法对比	已知类型样本	基于 CNN 的方法 ^[12]
		基于 LSTM 的方法 ^[13]
		基于 LSTM_CNN 的方法 ^[14]
		基于 BiLSTM_CNN 的方法 ^[15]
		基于 ViT 的方法 ^[33]
		基于 CoAtNet 的方法 ^[34]
BT-RN		
泛化能力检测	同源未知类型样本	1) 样本均来自 ISOT 数据集 2) 样本均来自 CTU 数据集
	异源未知类型样本	1) 使用 ISOT 数据集训练,使用 CTU 数据集测试
		2) 使用 CTU 数据集训练,使用 ISOT 数据集测试

实验其他参数设置如下。损失函数使用均方误差 (MSE, mean squared error), 这是因为模型输出值为查询样本与阳性实例的近似度分数。采用 L2 正则化避免过拟合。使用结合动量与均方根传递 (RMSprop, root mean square prop) 的 Adam (Adam, adaptive moment estimation) 优化器, 提升学习效率和增强超参数鲁棒性。betas 和 eps 采用默认值 (0.9, 0.999) 和 1×10^{-8} , 对权重增加了 L2 正则化。学习率初始值设置为 0.001, 并设置了每 50 个 episode 衰减一半的优化策略。

3.3.4 评估指标

本文使用 5 个评估指标: 准确率 (ACC,

accuracy)、精确率 (Precision)、召回率 (Recall)、F1 值、平均准确率 (MACC, average accuracy)。其

$$\text{ACC} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}, \quad \text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}},$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \quad F1 = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}.$$

其中, TP 表示样本的预测结果且实际标签同为僵尸网络流量, TN 表示样本的预测结果且实际标签为正常流量, FN 表示样本的预测结果为正常流量但实际标签为僵尸网络流量, FP 表示样本的预测结果为僵尸网络流量但实际标签为正常流量。

为减少小样本背景下一次实验结果的偶然性影响, 本文引入了 MACC 指标, 对所有实验做 n 次重复实验并计算其平均准确率, 计算公式如下。

$$\text{MACC} = \frac{\sum_{i=1}^n \text{ACC}_i}{n} \quad (5)$$

其中, n 表示一次实验的重复次数, 对 n 次重复实验的准确率 ACC_i 进行求和再求平均。利用 MACC 指标用于小样本模型的准确率评估, 使得评估结果更具有客观性。

3.4 实验结果及分析

根据 3.3 节中的实验设置, 所有使用元学习训练策略方法的实验均在 1-shot 和 5-shot 的设定下学习 400 轮任务。为避免小样本学习的偶然性因素影响评估准确性, 所有实验均进行 20 次独立实验。

3.4.1 小样本方法对比实验

对比实验选择了 3 种基于度量学习的小样本方法 (基于 FC-Net 的方法^[18]、基于原型网络的方法^[20]、基于孪生网络的方法^[21]), 这些方法都通过度量训练样本和验证样本间的相似度对异常和正常流量进行分类, 以实现小样本下僵尸网络的检测。实验中, 每次独立实验随机选取 3 类僵尸网络作为学习任务集, 学习结束后对每类进行单独检测并评估准确率。本文通过僵尸网络检测并计算 MACC 值来评估实验结果。小样本方法对比实验结果如表 3 所示。

由表 3 中数据可以得出以下结论。① BT-RN 适用于小样本僵尸网络检测, 并且优于其他小样本方法。这种通过度量查询样本和训练样本之间距离对查询样本进行预测分类的学习模式, 使得

表 3 小样本方法对比实验结果
Table 3 Results of comparison experiments on small sample approaches

样本来源	数据类型	2-way 1-shot (MACC)				2-way 5-shot (MACC)			
		FC-net ^[18]	孪生网络 ^[21]	原型网络 ^[20]	BT-RN	FC-net ^[18]	孪生网络 ^[21]	原型网络 ^[20]	BT-RN
CTU 数据集	Neris	86.67%	76.13%	88.21%	91.81%	89.16%	94.39%	95.82%	96.09%
	Zeus	89.23%	78.34%	91.69%	94.47%	96.37%	88.28%	98.46%	99.63%
	Rbot	97.90%	91.61%	99.02%	99.25%	98.74%	98.40%	99.53%	99.74%
	Virut	92.95%	75.73%	85.21%	90.26%	98.28%	97.77%	96.14%	97.22%
	Avg	93.36%	80.45%	91.03%	93.95%	95.64%	94.71%	97.49%	98.20%
ISOT 数据集	Citadel	93.50%	92.78%	87.92%	95.03%	97.30%	97.24%	97.86%	98.61%
	Blackout	91.87%	88.70%	84.16%	92.44%	93.55%	93.17%	98.02%	98.50%
	Storm	78.65%	80.22%	78.81%	85.01%	82.32%	97.00%	98.96%	99.46%
	Walecdac	82.88%	79.21%	94.13%	94.77%	93.66%	95.78%	98.79%	98.12%
	Zyklon	94.93%	94.41%	97.43%	98.74%	97.60%	91.45%	99.31%	99.64%
	Avg	88.37%	87.07%	88.49%	93.20%	92.89%	94.93%	98.59%	98.87%

模型在少量训练样本下得到良好的学习。即使在 400 个训练样本的极限环境下, BT-RN 和其他 3 种基于度量学习的小样本方法在两种数据集上都取得了较好的 MACC, 均高于 80% 的检测准确率, BT-RN 的大部分准确率在 90% 以上。② BT-RN 的特征提取模块优于其他小样本方法的特征提取模块。根据 3.3 节的实验方法设置, 其他小样本方法仅特征提取模块设置与 BT-RN 不同, 这可以有效验证 BT-RN 的特征提取模块是否具有更强的特征提取能力。实验结果显示, BT-RN 的 MACC 均高于其他小样本方法, 在 2-way 1-shot 检测中, 基于孪生网络的方法相较于 BT-RN 平均准确率落后了 8.82%。在实验结果中, BT-RN 检测 Storm 僵尸网络的 MACC 较低, 可能是在 ISOT 数据集中选择的僵尸网络协议类型不均衡以及任务抽样的随机偶然性因素, 但数据显示 BT-RN 对 Storm 的检测 MACC 均高于其他小样本学习方法的检测结果, 这表明 BT-RN 的表现依旧良好。

3.4.2 深度学习方法对比实验

为证明本文方法优于采用传统训练策略的深度学习方法, 对比实验选择了目前已用于僵尸网络检测的 CNN^[12]、LSTM^[13]、LSTM_CNN^[14]、BiLSTM^[15] 和目前在图像分类领域更加先进的 ViT^[33]、CoAtNet^[34] 两种模型, 将基于这些模型的检测方法与 BT-RN 进行对比。在以往基于深度学习模型提出的检测方法中, 通常是需要利用海量标记样本训练模型, 再用于僵尸网络检测。这种

端对端的训练策略与基于任务的元训练策略不一致。因此在本文实验中, 将基于任务训练策略的 2-way 1-shot 和 2-way 5-shot 下的 400 轮学习转换为随机抽样 400 个僵尸网络样本和 2 000 个僵尸网络样本作为训练样本用于基于深度学习的检测方法, 并分别在 ISOT 数据集和 CTU 数据集上进行了 20 次独立的已知类型检测。类型分配上, 每次实验都分别对 ISOT 数据集和 CTU 数据集中所有类型的带标记样本进行训练, 然后使用测试样本对方法进行检测评估, 实验结果如表 4 所示。

由表 4 中数据可以得出以下结论。① BT-RN 能够通过学习少量样本获得很强的学习能力。当训练阶段只有 400 个样本时, BT-RN 可以达到 93.20% 的平均准确率, 而原有基于深度学习的僵尸网络检测方法在同样条件下, 检测平均准确率低于 80%。在可用于灰度图分类的最新模型中, ViT 和 CoAtNet 模型应用在小样本僵尸网络检测上准确率更是低于 65%, 可以看出基于深度学习的检测方法在样本量极少的情况下无法得到充分学习。BT-RN 受到了 2.1 节基于任务的元训练策略的影响, 使得模型尽管在训练阶段使用了极少的训练样本 (400 轮 1-shot 下仅 400 个), 但也可以充分利用到验证集中的样本, 及时利用未知样本评估衡量网络的元泛化能力和分类能力, 并对自身算法的超参数进行反馈调整, 提升自身学习能力^[35], 加速模型分辨数据类别的能力。这种元训练策略下, 验证集的设定在一定程度上弥补了训

表 4 深度学习模型在小样本下的对比实验结果
Table 4 Result of comparison experiments on deep learning models with small samples

样本来源	样本数量/个	MACC						
		ViT ^[33]	CoAtNet ^[34]	LSTM ^[13]	CNN ^[12]	LSTM_CNN ^[14]	BiLSTM_CNN ^[15]	BT-RN
ISOT 数据集	400	64.63%	56.49%	64.86%	63.52%	60.15%	67.48%	93.20%(1-shot)
	2000	65.27%	62.63%	65.63%	76.82%	70.92%	68.82%	98.87%(5-shot)
CTU 数据集	400	57.37%	58.02%	68.63%	77.45%	76.92%	72.31%	93.95%(1-shot)
	2000	59.18%	68.65%	62.63%	79.75%	79.85%	75.20%	98.20%(5-shot)

训练样本量不足, 并加快了 BT-RN 的学习。② BT-RN 解决了深度神经网络模型在小样本背景下的拟合问题。表 4 中数据显示: 基于 LSTM 的方法在样本量较小时(400 个训练样本)平均准确率更高, 反而在样本量大时(2 000 个训练样本)表现很差, 表明基于 LSTM 的方法对小样本的拟合程度过强, 而 BT-RN 可随样本增多正向提高准确率, 这是 BT-RN 优于这些基于深度学习方法的原因; 大多数基于深度学习方法在面对少量样本时检测准确率低于 70%, 说明了深度学习模型与大量的训练样本脱钩后, 模型训练不足导致检测效果不佳。

3.4.3 泛化能力检测

为进一步检测 BT-RN 的性能, 在未知类型僵尸网络上进行了实验以验证本文方法的泛化能力, 具体设置详见 3.3 节, 有同源检测(同数据集未知类测试)和异源检测(跨数据集未知类测试)两类。

(1) 同源检测实验

在同源实验(a)中, 训练和测试样本均来自仿真数据集 ISOT, 即优越的实验结果可能会受到仿真数据影响。数据分配上, 从 ISOT 中随机抽

样 3 类作为元训练的阳性样本, 余下 2 类作为元测试的阳性样本。其他设置与 3.3 节保持一致。

泛化能力检测实验中在 ISOT 数据集上进行未知类型检测的结果如表 5 显示。① BT-RN 对仿真数据集中未知类型检测效果良好。模型在元任务空间进行学习的策略, 以及训练集验证集内外合作优化自身超参的方式^[35], 使得模型在不断优化自身经验的同时, 快速获得了更强的元泛化能力。在小样本的环境下, BT-RN 对未知类型僵尸网络的检测结果准确率较高, 2-way 1-shot 条件下准确率可达 95.79%, 2-way 5-shot 条件下准确率可达 99.02%, 这得益于基于任务的学习方式和大量验证样本的反馈。② 泛化能力强。尽管本文实验的测试集使用了在训练阶段未见过的僵尸网络类型, 但本文实验结果与已知类型检测结果相近, 这表明训练好的模型对未知类型样本无须重新训练或进行微调, 可直接将训练好的模型用于未知样本检测, 其检测准确率基本一致, 具有很好的泛化能力。对于 Storm 的较低检测结果, 考虑是训练过程中 P2P 协议类的僵尸网络样本量低于

表 5 泛化能力检测实验中在 ISOT 数据集上进行未知类型检测的结果
Table 5 Results of unknown type detection on the ISOT dataset in generalization ability detection experiments

问题设置	ISOT 数据类型	准确率	精确率	召回率	F1
2-way 1-shot	Blackout	95.79%	96.37%	95.17%	95.77%
	Citadel	97.50%	96.61%	98.44%	97.52%
	Storm	90.97%	92.28%	89.42%	90.83%
	Walecdac	96.71%	96.89%	96.52%	96.70%
	Zyklon	97.71%	96.98%	98.49%	97.73%
2-way 5-shot	Blackout	98.23%	97.11%	99.41%	98.25%
	Citadel	99.06%	99.22%	98.89%	99.05%
	Storm	99.24%	99.48%	99.01%	99.24%
	Walecdac	99.32%	99.07%	99.58%	99.32%
	Zyklon	98.06%	97.61%	98.53%	98.07%

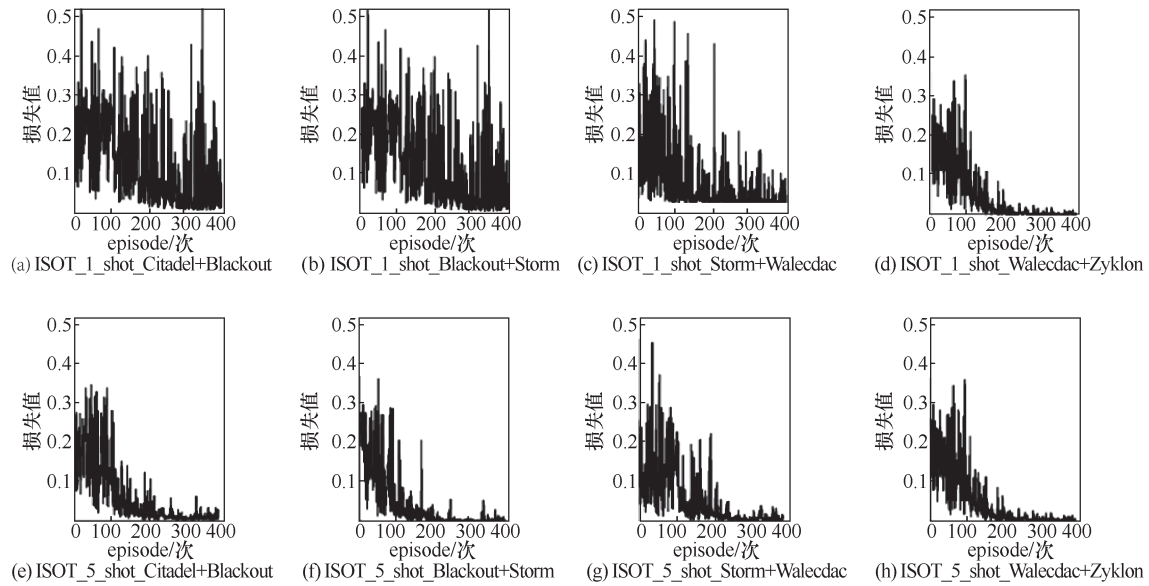


图 12 ISOT 数据集上的训练损失曲线
Figure 12 Training loss curve on the ISOT dataset

HTTP 类的样本量, 但 90.97% 检测效果在小样本检测来看, 依旧良好。③ 学习速度快。由图 12 ISOT 数据集上的训练损失曲线可以看出, 尽管僵尸网络类型不同, 但在 180 轮左右模型基本完成了学习, 后期损失基本持平。这种效果在深度神经网络中基本不能实现。

在同源实验 (b) 中, 数据使用了真实捕获的流量数据集 CTU, 即实验结果更为真实。数据分配上, 从 CTU 中随机抽取 3 类作为训练阳性样本, 余下 1 类作为测试样本。结合 CTU 数据的分布, 元训练阶段共使用 400 个 episode 进行学习, 2-way 1-shot 和 2-way 5-shot 设置下的元测试均使用 600 个 episode 进行测试。其他设置与 3.3 节保持一致。泛化能力检测实验中在 CTU 数据集上进行未知

类型检测的结果如表 6 所示, CTU 数据集上的训练损失曲线如图 13 所示。① 该实验结果与在 ISOT 数据集上的实验结果一致, 模型在未知僵尸网络的检测效果良好, 具有很强的泛化能力、学习能力。Zeus 作为一种在训练阶段未见过的 P2P 协议类型僵尸网络, 在实验结果上检测准确率低于其他类型流量, 但其结果对于小样本检测来说, 依旧良好。② 真实数据集上的测试结果与仿真数据集测试结果基本一致, 表明在小样本背景下, 可以对僵尸网络流量有效检测。

(2) 异源检测实验

异源检测实验是在不重复训练或微调的情况下, 直接将训练好的模型应用于其他数据集的未知僵尸网络样本上进行检测, 利用其检测结果验

表 6 泛化能力检测实验中在 CTU 数据集上进行未知类型检测的结果

Table 6 Results of unknown type detection on the CTU dataset in generalization ability detection experiments

问题设置	CTU 数据类型	准确率	精确率	召回率	F1 值
2-way 1-shot	Neris	93.92%	92.90%	95.10%	93.99%
	Zeus	89.16%	90.99%	86.93%	88.91%
	Rbot	94.03%	92.01%	96.44%	94.17%
	Virus	95.68%	95.10%	96.33%	95.71%
2-way 5-shot	Neris	97.16%	98.04%	96.24%	97.13%
	Zeus	93.45%	96.76%	89.90%	93.21%
	Rbot	99.13%	99.19%	99.07%	99.13%
	Virus	97.46%	96.97%	97.99%	97.47%

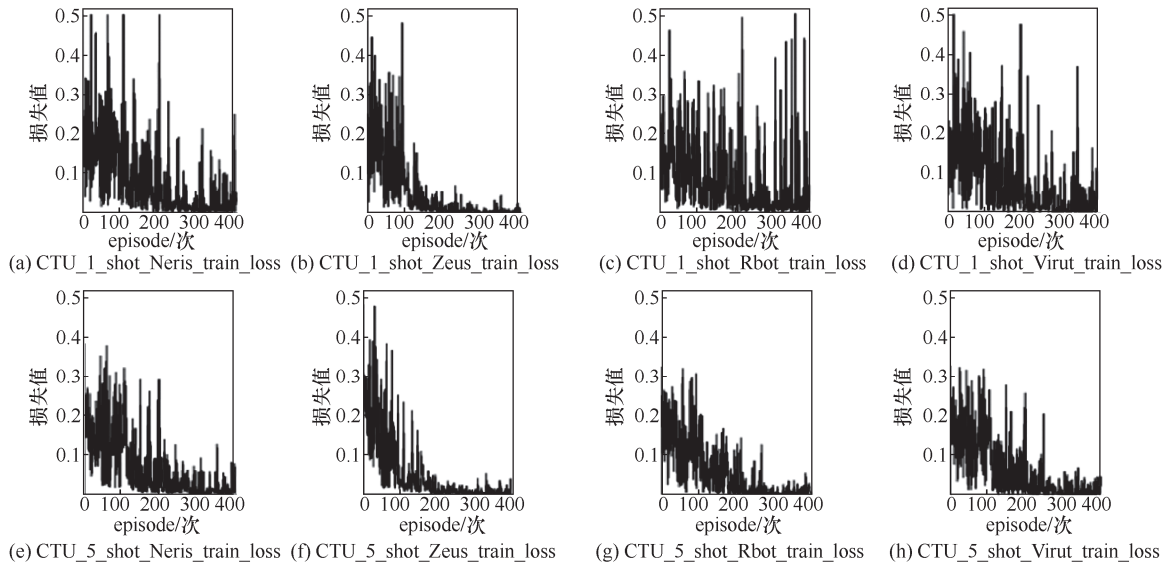


图 13 CTU 数据集上的训练损失曲线
Figure 13 Training loss curve on the CTU dataset

证模型是否具有更高的泛化性。

异源实验 (a) 中, 使用仿真数据集 ISOT 进行模型训练, 使用真实捕获数据集 CTU 进行模型评估。不同于之前实验设置的是, 元训练训练了 700 轮。泛化能力检测实验中在 ISOT 数据集和 CTU 数据集上进行跨数据的未知类型检测结果如表 7 所示。① BT-RN 对跨数据集的未知僵尸网络检测效果良好。结果显示, BT-RN 在 1-shot 设置下准确率为 90.85%, 5-shot 设置下准确率为 94.73%。尽管实验中训练集与测试集的数据样本来源不同, 但检测效果良好。② BT-RN 在跨数据集测试上也具有很强的泛化能力。在训练阶段, 训练集中未含有基于 P2P 协议的 Zeus 僵尸网络流量样本, 但在测试阶段引入了另一数据集的 P2P 协议 Zeus 僵尸网络流量样本, 其 MACC 值较高, 2-way 1-shot 设置下的准确率高达 86.40%, 2-way

5-shot 设置下的准确率高达 96.62%, 表明模型在未知协议类型的僵尸网络检测上具有很高的泛化能力。

异源实验 (b) 中, 训练和测试样本来自不同数据集。元训练的阳性样本来自 CTU 中的 4 种僵尸网络流量, 元测试的阳性样本来自 ISOT 中的 5 种僵尸网络流量。元训练阶段使用 700 个 episode 进行学习, 元测试使用 140 个 episode 进行测试评估模型。泛化能力检测实验中在 CTU 数据集和 ISOT 数据集上进行跨数据的未知类型检测结果如表 8 所示, 该实验的评估结果与前一实验结论相似:

① BT-RN 对未知僵尸网络检测效果良好; ② BT-RN 具有良好的泛化能力。

4 结束语

本文提出了一种将深度神经网络与元学习理论相结合的小样本检测方法 BT-RN, 为僵尸网络

表 7 泛化能力检测实验中在 ISOT 数据集和 CTU 数据集上进行跨数据的未知类型检测结果
Table 7 Results of unknown type detection across data on ISOT and CTU in generalization ability detection experiments

CTU 数据类型	2-way 1-shot				2-way 5-shot			
	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值
Zeus	91.33%	91.81%	90.77%	91.28%	96.62%	97.98%	95.20%	96.57%
Neris	86.40%	87.63%	84.77%	86.17%	95.57%	94.14%	88.37%	91.16%
Virut	90.85%	91.90%	89.60%	90.73%	95.30%	96.13%	94.40%	95.26%
Rbot	94.83%	93.95%	95.83%	94.88%	91.43%	94.70%	96.53%	95.61%

表 8 泛化能力检测实验中在 CTU 数据集和 ISOT 数据集上进行跨数据的未知类型检测结果
Table 8 Results of unknown type detection across data on CTU and ISOT in generalization ability detection experiments

ISOT 数据类型	2-way 1-shot				2-way 5-shot			
	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值
Storm	84.43%	85.93%	82.33%	84.09%	89.26%	87.67%	91.38%	89.48%
Walecdac	84.36%	86.17%	81.86%	83.96%	88.33%	88.96%	87.52%	88.24%
Zyklon	87.69%	86.90%	88.76%	87.82%	92.79%	90.60%	95.48%	92.97%
Blackout	90.76%	90.04%	91.67%	90.84%	95.12%	94.88%	95.38%	95.13%
Citadel	90.36%	91.16%	89.38%	90.26%	95.07%	95.40%	94.71%	95.05%

的发现初期高效利用少量样本识别检测僵尸网络而设计，并能有效检测未知僵尸网络。BT-RN 由特征提取模块和相似性度量模块等构成；引入了特征级混合注意力机制 BT-CBAM 和残差网络增强模型提取能力；使用下游的深度可学习度量网络提升模型分类准确率；基于任务的元学习训练策略利用少量样本快速积累优化经验提升学习能力和检测能力。实验结果表明，本文方法在小样本环境下，通过元学习思想能够得到更高的检测准确率，并且具有较好的泛化能力，同时可用于检测未知僵尸网络。

参考文献:

- [1] 国家计算机网络应急技术处理协调中心(CNCERT/CC). CNCERT 互联网安全威胁报告[R]. 2021-8. National Computer Network Emergency Response Technology Processing Coordination Center (CNCERT/CC). CNCERT Internet security threat report[R]. 2021-8.
- [2] 国家计算机网络应急技术处理协调中心(CNCERT/CC). 2020 年中国互联网络网络安全报告[R]. 2021-7. National Computer Network Emergency Response Technology Processing Coordination Center (CNCERT/CC). 2020 China Internet network security report[R]. 2021-7.
- [3] XING Y, SHU H, ZHAO H, et al. Survey on botnet detection techniques: classification, methods, and evaluation[J]. Mathematical Problems in Engineering, 2021, 2021: 1-24.
- [4] GARG S, GUIZANI M, GUO S, et al. Guest editorial: special section on ai-driven developments in 5g-envisioned industrial automation: big data perspective[J]. IEEE Transactions on Industrial Informatics, 2019, PP (99): 1.
- [5] WANG X, YANG Q, JIN X. Periodic communication detection algorithm of botnet based on quantum computing[J]. Chinese Journal of Quantum Electronics, 2016, 33 (2): 182-187.
- [6] SPATHOULAS G, GIACHOUDIS N, DAMIRIS G-P, et al. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets[J]. Future Internet, 2019, 11 (11): 226.
- [7] LASHKARI A H, GIL G D, KEENAN J E, et al. A survey leading to a new evaluation framework for network-based botnet detection[C]//International Conference. 2017: 59-66.
- [8] WANG J, CHEN Y. Botnet detection method based on permutation entropy and clustering variance[C]//The 2017 3rd International Symposium on Mechatronics and Industrial Informatics(ISMII 2017). 2017: 161-166.
- [9] BILGE L, BALZAROTTI D, ROBERTSON W, et al. Disclosure: detecting botnet command and control servers through large-scale NetFlow analysis[C]//Proceedings of the 28th Annual Computer Security Applications Conference. 2012: 129-138.
- [10] 金渝笙, 谢彬, 朱毅. 基于通信相似度的僵尸网络节点检测方法[J]. 网络与信息安全学报, 2018, 4 (10): 31-38. JIN Y Q, XIE B, ZHU Y. Method of botnet network nodes detection base on communication similarity[J]. Chinese Journal of Network and Information Security, 2018, 4(10): 31-38.
- [11] JUNG W, ZHAO H, SUN M, et al. IoT botnet detection via power consumption modeling[J]. Smart Health, 2020, 15: 100103.
- [12] WANG W, ZHU M, ZENG X, et al. Malware traffic classification using convolutional neural network for representation learning[C]//2017 International Conference on Information Networking (ICOIN). 2017: 712-717.
- [13] 尹传龙, 祝跃飞, 张鹤童. 基于 LSTM 深度学习的僵尸网络检测模型[J]. 信息工程大学学报, 2018, 19(94): 76-82. YIN C L, ZHU Y F, ZHANG H T. Deep learning approach for botnet detection using LSTM[J]. Journal of Information Engineering University, 2018, 19(94): 76-82.
- [14] 罗扶华, 张爱新. 基于深度学习的僵尸网络检测技术研究[J]. 通信技术, 2020, 53 (1): 174-179. LUO F H, ZHANG A X. Botnet detection technology based on deep learning[J]. Communications Technology, 2020, 53 (1): 174-179.
- [15] 谭越, 邹福泰. 基于 ResNet 和 BiLSTM 的僵尸网络检测方法[J]. 通信技术, 2019, 52 (12): 7. TAN Y, ZOU F T. Botnet detection method based on BiLSTM and ResNet[J]. Communications Technology, 2019, 52 (12): 7.
- [16] YERIMA S Y, ALZAYLAEE M K, SHAJAN A. Deep learning techniques for android botnet detection[J]. Electronics, 2021, 10(4): 519.
- [17] OLASEHINDE O, JOHNSON O V, CATHERINE O O. Evaluation of selected meta learning algorithms for the prediction improvement of network intrusion detection system[C]//2020 International Conference in Mathematics, Computer Engineering and Computer

- Science (ICMCECS). 2020.
- [18] XU C, SHEN J, DU X. A method of few-shot network intrusion detection based on meta-learning framework[J]. IEEE Transactions on Information Forensics and Security, 2020, (99): 1.
- [19] TANG Z, WANG P, WANG J. ConvProtoNet: deep prototype induction towards better class representation for few-shot malware classification[J]. Applied Sciences, 2020, 10 (8): 2847.
- [20] PAN J. Iot network behavioral fingerprint inference with limited network traces for cyber investigation[C]//2021 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC). 2021: 263-268.
- [21] HINDY H, TACHTATZIS C, ATKINSON R, et al. Developing a siamese network for intrusion detection systems[C]//Proceedings of the 1st Workshop on Machine Learning and Systems. 2021: 120-126.
- [22] TIANYU G, ZHIYUAN L, MAOSONG S, et al. Hybrid attention-based prototypical networks for noisy few-shot relation classification[C]//The AAAI Conference on Artificial Intelligence, 2019: 6407-6414.
- [23] AMIR E, DAVID E, MASSOUD P, et al. A meta-learning approach for custom model training[C]//The AAAI Conference on Artificial Intelligence. 2019: 9937-9938.
- [24] YANG A, LU C, LI J, et al. Application of meta-learning in cyberspace security: a survey[J]. Digital Communications and Networks, 2022, 9 (1): 67-78.
- [25] HOSPEDALES T M, ANTONIOU A, MICAELLI P, et al. Meta-learning in neural networks: a survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 44(9): 5149-5169.
- [26] WOO S, PARK J, LEE J Y, et al. Cbam: convolutional block attention module[C]//Proceedings of the European Conference on Computer vision (ECCV). 2018: 3-19.
- [27] HE K, ZHANG X, REN S, et al. Deep residual learning for image recognition[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2016: 770-778.
- [28] SZEGEDY C, LIU W, JIA Y, et al. Going deeper with Convolutions[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2015: 1-9.
- [29] ZOU Y, ZHANG L, LIU C, et al. Super-resolution reconstruction of infrared images based on a convolutional neural network with skip connections[J]. Optics and Lasers in Engineering, 2021, 146: 106717.
- [30] SUNG F, YANG Y, ZHANG L, et al. Learning to compare: Relation network for few-shot learning[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018: 1199-1208.
- [31] VINYALS O, BLUNDELL C, LILLICRAP T, et al. Matching networks for one shot learning[J]. Advances in Neural Information Processing Systems, 2016: 3637-3645.
- [32] SNELL J, SWERSKY K, ZEMEL R. Prototypical networks for few-shot learning[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017: 4080-4090.
- [33] DOSOVITSKIY A, BEYER L, KOLESNIKOV A, et al. An image is worth 16×16 words: transformers for image recognition at scale[C]//International Conference on Learning Representations. 2021.
- [34] DAI Z, LIU H, LE Q V, et al. CoAtNet: marrying convolution and attention for all data sizes[J]. 2021: arXiv.2016.04803.
- [35] HUISMAN M, VAN RIJN J N, PLAAT A. A survey of deep meta-learning[J]. 2020: arXiv: 2010. 03522.

[作者简介]



林宏刚(1976-), 男, 四川资阳人, 成都信息工程大学教授, 主要研究方向为物联网安全、网络与系统安全。



朱竣菁(1998-), 女, 四川达州人, 成都信息工程大学硕士生, 主要研究方向为网络空间安全。



陈麟(1973-), 男, 重庆忠县人, 网络空间安全态势感知与评估安徽省重点实验室教授, 主要研究方向为网络空间安全。