计算机科学
COMPUTER SCIENCE

面向物联网僵尸网络多阶段攻击的异常流量检测方法

陈亮, 李志华

引用本文

陈亮, 李志华. 面向物联网僵尸网络多阶段攻击的异常流量检测方法[J]. 计算机科学, 2024, 51(8): 379-386.

CHEN Liang, LI Zhihua. Abnormal Traffic Detection Method for Multi-stage Attacks of Internet of Things Botnets [J]. Computer Science, 2024, 51(8): 379-386.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

域名生成算法检测技术综述

Survey of Detection Techniques for Domain Generation Algorithm

计算机科学, 2024, 51(8): 371-378. https://doi.org/10.11896/jsjkx.230700189

面向物联网的分布式联邦学习加密验证研究

Study on Cryptographic Verification of Distributed Federated Learning for Internet of Things

计算机科学, 2024, 51(6A): 230700217-5. https://doi.org/10.11896/jsjkx.230700217

基于联盟链的细粒度安全访问控制机制

Fine Grained Security Access Control Mechanism Based on Blockchain

计算机科学, 2024, 51(6A): 230400080-7. https://doi.org/10.11896/jsjkx.230400080

基于快速傅里叶卷积与特征修剪坐标注意力的壁画修复

Mural Inpainting Based on Fast Fourier Convolution and Feature Pruning Coordinate Attention

计算机科学, 2024, 51(6A): 230400083-9. https://doi.org/10.11896/jsjkx.230400083

DRSTN:深度残差软阈值化网络

DRSTN:Deep Residual Soft Thresholding Network

计算机科学, 2024, 51(6A): 230400112-7. https://doi.org/10.11896/jsjkx.230400112

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700197

面向物联网僵尸网络多阶段攻击的异常流量检测方法

陈　亮　　李志华
江南大学人工智能与计算机学院　江苏 无锡 214112
(chenliang006@qq.com)

摘　要　针对如何从海量的网络流量数据中高效检测出物联网僵尸网络多阶段攻击行为,提出了一种基于多尺度混合残差网络(Multi-scale Hybrid Residual Network,MHRN)的物联网僵尸网络攻击检测(IoT Botnet Attack Detection based on MHRN,IBAD-MHRN)方法。首先,为了减少检测模型的计算参数,在数据预处理中提出基于方差阈值法的特征选择(Feature Selection based on Variance Threshold,FS-VT)算法;其次,采取一种将数据样本转换为图像样本的数据图像化处理策略,充分挖掘深度学习模型的潜能;然后,为了弥补传统僵尸网络检测模型表征能力有限的不足,提出了一种基于多尺度混合残差网络的物联网僵尸网络多阶段攻击检测模型,该模型通过混合方式融合了不同尺度深度提取的特征信息,再通过残差连接消除网络加深造成的网络退化影响;最后,集成上述模型和算法,进一步提出了一种物联网僵尸网络攻击检测方法 IBAD-MHRN。实验结果表明,IBAD-MHRN 方法的检测准确率和 F1 值均达到了 99.8%,与表现较好的卷积神经网络方法相比在准确率和 F1 值上分别有 0.14%和 0.36%的提升,能够有效且高效地检测物联网僵尸网络多阶段攻击。

关键词:物联网;僵尸网络;方差阈值法;残差网络;多阶段攻击
中图分类号　TP393.08

Abnormal Traffic Detection Method for Multi-stage Attacks of Internet of Things Botnets

CHEN Liang and LI Zhihua
School of Artificial Intelligence and Computer,Jiangnan University,Wuxi,Jiangsu 214122,China

Abstract　To address the problem of how to efficiently detect multi-stage attack behavior of IoT botnet from massive network traffic data,an IoT botnet attack detection method based on multi-scale hybrid residual network(IBAD-MHRN)is proposed. Firstly,in order to reduce the calculation parameters of the detection model,a feature selection algorithm based on variance threshold(FS-VT)method is proposed in data preprocessing. Secondly,a data image processing strategy that converts data samples into image samples is adopted to fully tap the potential of the deep learning model. Then,in order to solve the deficiency of the traditional botnet detection model with limited representation ability,a multi-stage attack detection model of IoT botnet based on multi-scale hybrid residual network is proposed. The model integrates the feature information extracted at different scales and depths in a hybrid way,and then eliminates the effect of network degradation caused by network deepening through residual connection. Finally,an IBAD-MHRN method for IoT botnet attack detection is proposed by integrating the above models and algorithms. Experimental results show that the detection accuracy and F1 value of the proposed IBAD-MHRN method reaches 99.8%,and the accuracy and F1 value is improved by 0.14% and 0.36% respectively compared with the better convolutional neural network method,which can effectively and efficiently detect multi-stage attacks of Internet of Things botnets.

Keywords　Internet of Things,Botnet,Variance threshold method,Residual network,Multi-stage attacks

1　引言

据 GSMA 预测,到 2025 年将会有 750 亿台物联网设备在线连接到互联网[1]。由于大多数物联网设备或装置具有应用广泛、生产成本低的特点,因此这些设备、装置通常先天性缺乏系统安全防护等方面的保护措施。一旦这些不安全的设备或装置被恶意软件感染,往往很容易构成庞大的僵尸网络[2]。近年来,由物联网僵尸网络发起的针对互联网的分布式拒绝服务(DDoS)攻击事件频发,并且规模和数量愈发庞大,这些攻击大多都会对整个网络造成严重的危害[3]。因此,对物联网僵尸网络发起面向互联网的僵尸网络攻击检测是当前比较有意义的研究话题之一。

到稿日期:2023-07-26　返修日期:2023-11-11
基金项目:工业和信息化部智能制造项目(ZH-XZ-180004);中央高校基本科研业务费专项资金(JUSRP211A41,JUSRP42003)
This work was supported by the Intelligent Manufacturing Project of the Ministry of Industry and Information Technology(ZH-XZ-180004)and Fundamental Research Funds for the Central Universities of Ministry of Education of China(JUSRP211A41,JUSRP42003).
通信作者:李志华(jswxzhli@aliyun.com)

在物联网领域，比较典型的僵尸网络攻击有 Mirai，Mozi，Hajime 和 Torii 等[4]。这些攻击的共同特征是多阶段攻击，包括侦察、入侵、恶意软件注入、指挥与控制通信，最后对目标发起攻击，所发起攻击的类型有 TCP/SYN 洪泛、基于 HTTP 的 DDoS 攻击、垃圾数据包等[5]。在物联网僵尸网络攻击中，最具代表性的攻击是 Mirai。随着 Mirai 源码于 2016 年公开，物联网僵尸网络攻击近年来演化出了更多的变种和形式[6]。并且，其网络攻击模式的不断迭代和更新使得攻击方式愈加隐蔽化、持久化[7]，进而从另一个方面增加了物联网僵尸网络攻击检测的难度。

在传统的计算机网络领域，入侵检测的模型和算法相对较多，技术也相对成熟[8-10]。而在物联网安全领域，如何构建精确、高效的物联网僵尸网络攻击检测模型具有一定的挑战性。由于物联网的异构性和协议多样性，物联网流量不同于传统遵循固定格式的计算机网络流量，当试图从包含有物联网网络流量的互联网网络流量中进行物联网僵尸网络攻击检测时，需要研究并设计更加复杂的物联网僵尸网络攻击检测模型，以弥补传统的检测模型表征能力有限、泛化能力较弱的不足。通常，深度学习算法在面向高维度、海量数据挖掘时，具有更强的特征抽取能力，特别是具有时空差异性和能表征对象细节的特征[11]。针对物联网僵尸网络攻击检测的需要，本文对物联网僵尸网络攻击流量进行分析，对经典的深度学习算法进行改进，使其适用于多阶段性和协议多样性的物联网僵尸网络攻击场景。基于这些研究，本文提出一种基于多尺度混合残差网络（MHRN）的物联网僵尸网络攻击检测（IBAD-MHRN）方法。IBAD-MHRN 方法包含：用于特征降维的基于方差阈值法的特征选择（FS-VT）算法和基于 MHRN 的物联网僵尸网络攻击类型识别（IoT Botnet Attack Category Identification base on MHRN，IBACI-MHRN）算法。实验结果表明，所提出的方法具有较高的检测精度和较快的收敛速度，可以实现有效且高效的物联网僵尸网络多阶段攻击检测。

2 相关工作

为了抵御物联网僵尸网络攻击这类比较复杂的网络威胁，需要探索性能更强、检测精度更高的物联网网络入侵检测技术。近年来，机器学习和深度学习已被广泛用于构建物联网僵尸网络攻击检测模型和系统。

基于机器学习的物联网僵尸网络攻击检测方法通常能够以较少的特征维数实现较好的检测效果。文献[12]通过基于 Fisher 评分法的特征选择算法筛选出相关特征，再通过基于遗传算法的梯度提升（GXGBoost）模型对物联网僵尸网络攻击进行检测。该方法能够实现对攻击样本的快速检测，但其局限性在于无法确认模型的参数值是否达到全局最优值。文献[13]对 4 种机器学习算法进行僵尸网络攻击检测的性能进行了比较，包括朴素贝叶斯、支持向量机、决策树和 K 近邻算法。其中决策树取得了最好的结果。但是，由于这些方法无法完成更多未知攻击的检测，因此限制了方法的实用性。文献[14]结合了贝叶斯优化高斯过程算法和决策树分类器，能够高效地检测物联网僵尸网络攻击。虽然该方法在物联网海量数据场景下展现出较好的鲁棒性，但是能否满足物联网僵尸网络攻击其他阶段产生的低速率攻击类型检测仍需验证。

相比基于机器学习的方法，基于深度学习的方法能够提取更多的特征信息，适应性更强。文献[15]通过迁移学习对卷积神经网络（CNN）进行改进，实现对物联网僵尸网络流量的分类，并且将该方法与长短期记忆网络（LSTM）和递归神经网络（RNN）进行对比，证明了 CNN 方法在海量数据场景下对物联网僵尸网络流量有着较好的分类效果，但是在小数据量场景下检测精度不足。文献[16]提出基于门控递归单元（GRU）的轻量级模型执行僵尸网络攻击检测方法，能够进行实时流量检测，极大地减少了攻击对软件定义网络的影响，但依旧存在误检率较高的不足。文献[17]分析了递归神经网络（RNN）方法检测物联网僵尸网络攻击的可行性，将其建模为随时间变化的状态序列，以此检测物联网流量中的恶意攻击行为。该方法能够以较低的误报率实现对流量的分类，但是不易区分具有相同攻击行为模式的恶意流量。文献[18]评估了 4 种不同的深度学习模型在僵尸网络攻击检测上的性能。实验结果表明 CNN 与 LSTM 相结合的模型在准确度上优于其他模型。但该模型没有针对物联网海量流量数据场景进行优化，能否满足复杂的网络攻击模式亟需验证。文献[19]使用长短期自动编码器 LAE 降低了数据的特征维数，通过双向长短期记忆网络（Bi-directional Long-Short Term Memory，BiLSTM）实现了僵尸网络流量的准确分类，在过拟合方面该方法表现出稳健性，并且占用的内存资源较少。但是该方法只验证了僵尸网络攻击阶段产生的流量，是否满足僵尸网络多阶段检测场景亟需验证。

综上所述，目前大多数物联网僵尸网络攻击检测模型存在表征能力有限以及海量数据场景适应性较差的不足。为此，本文通过对残差网络进行改进，提出了一种多尺度混合残差网络，并在此基础上提出了一种物联网僵尸网络攻击检测模型和方法。

3 多尺度混合残差网络

3.1 网络结构

本节讨论所提出的多尺度混合残差网络（MHRN），其结构如图 1 所示。

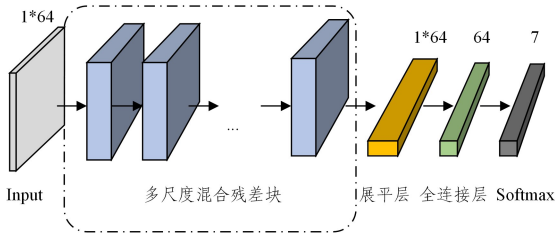


图 1 多尺度混合残差网络结构

Fig. 1 Structure of multiscale hybrid residual network

MHRN 由若干多尺度混合残差块、展平层和全连接层组成。其中，多尺度混合残差块用以提取多个尺度的特征信息；展平层将特征信息序列输出并且向全连接层过渡；全连接层对全局特征进行整合处理，最后通过 Softmax 函数输出结果。MHRN 的优势在于，通过堆叠多个多尺度混合残差块来增加

网络深度，通过加深网络深度来提高网络的表示能力以及避免欠拟合的发生。MHRN 中最重要的是多尺度混合残差块，下文将对多尺度混合残差块进行详细讨论。

3.2　多尺度混合残差块

多尺度混合残差块是 MHRN 的核心，其结构如图 2 所示。首先，通过多尺度混合设计对不同尺度提取的局部特征信息进行放大与聚合，以便增强模型的特征提取能力；然后，借助文献[20]中采取恒等映射方式的做法，消除随着网络深度加深造成的网络退化影响；最后，为了提升 MHRN 的泛化性能，借助文献[21]在多尺度混合残差块上设计 Dropout 层，通过 Dropout 的随机失活特性保证网络的稀疏性。

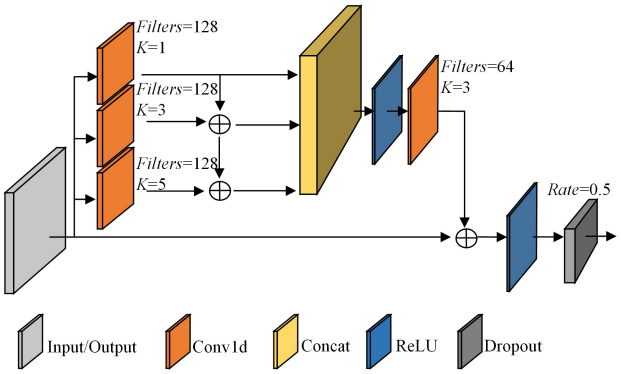


图 2　多尺度混合残差块结构

Fig. 2　Structure of multi-scale hybrid residual block

3.2.1　多尺度混合

通常，小尺度的卷积核能够捕获到图像的细节特征，而大尺度的卷积核能够捕捉图像的全局特征。由于物联网僵尸网络攻击具有多阶段性和协议多样性，因此其检测不能仅仅依赖于流量中的局部特征，更要兼顾流量中的全局特征[22]。为了能够提取流量数据中更多的局部空间特征，本文通过不同大小的卷积核提取特征图，再通过混合设计对提取不同尺度的特征信息进行叠加与聚合，以期增强 MHRN 的特征提取能力。下文将对多尺度混合的计算方式进行讨论。

线性激活函数 $f_i(x)$ 如式(1)所示：

$$f_i(x)=\sigma(\boldsymbol{W}_i\times x+\boldsymbol{b}_i) \tag{1}$$

其中，x 为激活值。$\boldsymbol{W}_i\in P^k$ 为扩展卷积第 i 列的权重矩阵，k 为卷积核数，$\boldsymbol{b}_i$ 为扩展卷积第 i 列的偏差因子，σ 为激活函数。

本文提出的多尺度混合是对不同尺度的卷积核进行特征融合，即在叠加阶段使用 Add 函数对特征信息进行逐通道相加，在聚合阶段使用 Concatenate 函数进行逐通道拼接。混合过程分别按式(2)－式(4)计算：

$$f_{s1}=f_1+f_2 \tag{2}$$

$$f_{s2}=f_{s1}+f_3 \tag{3}$$

$$f_h=concat(f_1,f_{s1},f_{s2}) \tag{4}$$

其中，f_h 为混合叠加结果。

由此可见，本文通过混合设计，先对不同尺度的卷积核提取的特征信息进行叠加，再以聚合方式提取更丰富的信息量，从而提升 MHRN 的表征能力。

3.2.2　残差结构

残差结构能够解决深层网络优化时引起的梯度消失和网络退化问题[23]。MHRN 中的多尺度混合残差块使用恒等映射作为短路连接，将残差量和原始输入量相叠加，得到最终的目标映射函数。恒等映射结构不仅能够加快网络收敛，而且能够有效地解决网络加深过程中出现的网络退化问题。其计算过程如下。

假设输入变量为 x，按文献[24]计算残差模块输出结果 $F(x_l)$，其计算式如式(5)所示：

$$F(x_l)=x_l+H(x_l,\boldsymbol{W}_i) \tag{5}$$

其中，x_l 为 l 层输入量；$H(x_l)$ 为 l 层残差映射量；$\boldsymbol{W}_i$ 为在处理输入数据时，传递信息到第 i 卷积层所设计的权重矩阵。$H(x)$ 为多尺度混合后再次进行深度卷积，其计算式如式(6)所示：

$$H(x)=\boldsymbol{W}_2\times f_h(x)+\boldsymbol{b}_2 \tag{6}$$

其中，$\boldsymbol{W}_2$ 为第二层卷积的权重，$\boldsymbol{b}_2$ 为第二层卷积的偏差因子。对于 MHRN，残差结构的引入并未增加网络参数和计算复杂度。另外，由于 MHRN 通过堆叠多个多尺度混合残差块来增加网络深度，而残差连接的设计将来自输入层的信息传播到残差块的输出层，这种方式不仅有效地减小了网络退化可能产生的影响，而且有助于加快模型的收敛速度。

4　IBAD-MHRN 方法

IBAD-MHRN 方法旨在针对物联网环境下僵尸网络多阶段产生的恶意流量准确识别出攻击类型，其过程如图 3 所示，主要包括数据预处理、数据图像化以及检测模型 3 个部分。首先，通过数据预处理将原始流量数据处理成实验所需的标准数据样本集；然后，为了发挥深度学习模型的性能，采用数据图像化的方式将标准样本集转化成灰度图像格式样本集；最后，提出基于 MHRN 的物联网僵尸网络攻击类别检测模型，实现对物联网僵尸网络多阶段产生的恶意流量样本的攻击类型的分类和识别。下文将分别对各个部分进行详细讨论。

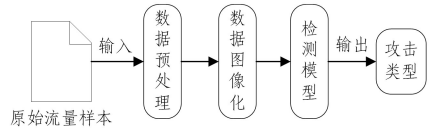


图 3　IBAD-MHRN 方法

Fig. 3　Method of IBAD-MHRN

4.1　数据预处理

如图 4 所示，数据预处理包含数据表示、数据过滤和特征降维 3 个步骤。数据表示主要借助 CICFlowerMeter[25] 工具将原始流量表示成格式统一的数据样本集，该数据样本集共含有 83 个特征；数据过滤的目的是丢弃特征不完全或格式错误的数据样本，如剔除数据样本集中包含 nan，-inf，+inf 等无效特征值的样本；特征降维借助方差阈值法[26]对数据样本进行特征过滤。选择方差阈值法的主要原因是其计算开销相对较小，有利于提高模型的检出效率。

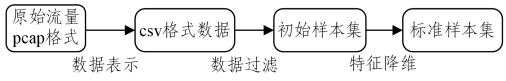


图 4　数据预处理方法

Fig. 4　Method of data preprocessing

基于方差阈值法的特征降维方法[27]简介如下：初始样本用 X_0 表示，特征降维后的标准样本用 X_{vt} 表示。首先，按式(7)计算 X_0 中所有特征的方差，并用特征方差集 F 表示。

$$var(x^j)=\frac{1}{n}\sum_{i=1}^{n}(x_i^j-\bar{x}^j)^2 \tag{7}$$

其中，样本 x_i 表示初始样本集 X_0 中第 i 个数据样本，x^j 表示初始样本集 X_0 中第 j 维特征，x_i^j 表示样本 x_i 中第 j 维的特征值，$\bar{x}^j$ 表示第 j 维的特征均值。然后，计算过滤阈值 τ，阈值 τ 的计算通常选择方差在[0,1]范围内产生最大间隙值的方差。最后，过滤掉方差小于阈值 τ 的特征，生成标准样本集。综合上述过程，本文提出基于方差阈值法的特征选择算法(FS-VT)，其伪代码描述如算法 1 所示。

算法 1 FS-VT 算法

```
Input: X0
Output: Xvt
1. for each x^j in X0 do
2.    use equation(7) to calculate variance
3.    F←var(x^j) // * 获取特征方差集
4.    while each Ft in F do
5.       if Ft∈[0,1] Then
6.          τ←Ft max gap value // * 最大间隙值
7.       end
8.    end
9. end
10. for each x^j in X0 do
11.   if var(x^j)≤ τ Then
12.      drop x^j from X0 // * 过滤特征
13.   end
14. end
15. Xvt←X0
16. Return Xvt
```

算法 1 的计算开销主要由计算方差和计算阈值产生，即算法的第 2 行和第 6 行。计算方差对样本中的特征依次计算，每一特征的时间复杂度为 $O(n)$；计算阈值是对阈值区间进行差值计算来判断，共产生 n^2 次计算。因此算法的时间复杂度为 $O(n^2)$。

4.2 数据图像化

由于网络流量数据集是以非图像格式捕获的，并且最终以文本格式(.txt,.csv 或者.pcap)存储，为了发挥模型的检测性能，借鉴文献[28]的数据图像化方法，将 csv 格式的数据样本转换为灰度图像，并根据数据预处理后得到的特征个数确定图像化后的样本尺寸。为了能够将数据转化成灰度图像，先按式(8)对数据预处理后所得标准数据样本集 X_{vt} 进行标准化处理。

$$x_i^j=\frac{x_i^j-\mathrm{Min}(x_i)}{\mathrm{Max}(x_i)-\mathrm{Min}(x_i)}\times 255 \tag{8}$$

其中，x_i 表示样本中序号为 i 的样本，x_i^j 表示该样本中第 j 维特征值，$\mathrm{Min}(x_i)$ 表示该样本中最小值，$\mathrm{Max}(x_i)$ 表示该样本中最大值。然后遍历所有的样本，使用 OpenCV 库将其转换为灰度图像，并保存至对应类别的文件夹中，生成的图像样本集用 P 表示。

4.3 模型检测

本文借鉴文献[29]中的检测模型设计提出了基于 MHRN 的物联网僵尸网络攻击检测模型，模型结构如图 5 所示。将经过数据图像化处理后的图片样本集 P 作为模型的输入，样本的攻击类型检测结果 $\hat{Y}$ 作为模型的输出。检测过程描述如下：首先，模型初始输入用 x_{in} 表示，经过若干多尺度混合残差块深度特征提取获得输出 x_{out}；经过展平层将多维输出一维化获得输出 z_f；再经过全连接层对提取出的特征进行综合处理获得输出 z_d；并且在全连接层中选择激活函数 Softmax 实现对输入样本的类别预测。Softmax 激活函数的计算式如式(9)所示：

$$\hat{Y}=\mathrm{softmax}(z_d)=\boldsymbol{W}_d\times z_f+\boldsymbol{b}_d \tag{9}$$

其中，$\boldsymbol{W}_d$ 和 $\boldsymbol{b}_d$ 分别表示权重矩阵和偏置项；$\hat{Y}$ 表示输出[0,1]范围内不同类别预测的概率值，其最大概率所对应的类别即输入样本的检测结果。

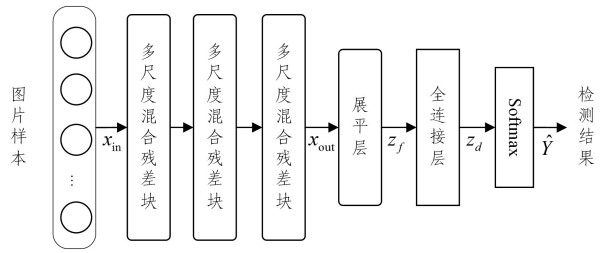


图 5 基于 MHRN 的物联网僵尸网络攻击检测模型

Fig. 5 IoT botnet attack detection model based on MHRN

综合上述过程，提出一种基于 MHRN 的物联网僵尸网络攻击类型识别(IBACI-MHRN)算法。输入样本集 $P=(p_1,p_2,\cdots,p_n)$、迭代次数 *epoch* 和多尺度混合残差块的数量 N，输出样本的攻击类型检测结果 $\hat{Y}$。在多次迭代训练过程中，依次按照式(1)—式(6)计算多尺度混合残差块的多尺度卷积层、混合层与残差层。经过若干多尺度混合残差块后，使用 *Flatten* 进行输出一维化与 *Dense* 完成全连接层输出。最后使用式(9)计算出分类结果。IBACI-MHRN 算法的伪代码描述如算法 2 所示。

算法 2 IBACI-MHRN 算法

```
Input: P=(p1,p2,…,pn); epoch; N
Output: Ŷ
1. xin←P=(p1,p2,…,pn) // * 输入图片样本
2. xin←xin/255 // * 对 xin 进行归一化
3. for epoch=1,2,3,…,m do
4.    for i=1; i≤N do
5.       使用式(1)计算卷积层输出
6.       使用式(2)—式(4)计算混合输出
7.       使用式(5)和式(6)计算残差层输出
8.       xout←Dropout(xout) // * 随机失活
9.    end
10.   zf←Flatten(xout) // * 输出一维化
11.   zd←Dense(zf) // * 全连接层输出
12.   使用式(9)计算输出 Ŷ
13. end
```

14. save model // * 保存训练好的模型

15. return $\hat{Y}$

算法 2 的时间开销主要来自于多尺度混合残差块的计算，即算法的第 5－8 行。设每个卷积核输出维度为 m，则一维卷积输出特征图的面积为 $1\times m$，第一层卷积核边长为 k_1，第二层卷积核边长为 k_2，输入输出的通道数均为 n。由卷积时间复杂度计算 $O(mkn^2)$可得，多尺度混合残差网络的时间复杂度为 $O(6mk_1n^2+mk_2n^2)$，即 $O(n^2)$。

4.4 IBAD-MHRN 方法

联合上述 FS-VT 算法和 IBACI-MHRN 算法，本文进一步提出物联网僵尸网络攻击检测方法 IBAD-MHRN。其具体步骤如下：首先，在数据预处理阶段，将原始流量样本 T_0 通过数据表示、数据过滤和特征降维后，生成标准数据样本集 X_{vt}；然后，对 X_{vt} 做数据图像化处理，生成图像样本集 P；最后，使用检测模型对样本集 P 进行深度特征提取，实现从待检测流量中识别出具体僵尸网络攻击类型。IBAD-MHRN 算法的伪代码描述如算法 3 所示。

算法 3　IBAD-MHRN 算法

Input：T_0

Output：$\hat{Y}$

1. $X_0\leftarrow T_0$ use CICFlowerMeter // * 数据表示
2. for each x_i in X_0 do
3.　　if x_i contains Infinity value then
4.　　drop x_i from X_0 // * 数据过滤
5.　　end
6. end
7. $X_{vt}\leftarrow X_0$ call FS-VT // * 调用算法 1
8. for each x_i in X_{vt} do
9.　　for each x_i^j in x_i do
10.　　use equation(8) to standardization
11.　　end
12.　　$p_i\leftarrow x_i$ use OpenCV // * 生成图像
13.　　$P^n\leftarrow p_i$ // * 获取图像数据集
14. end
15. $\hat{Y}\leftarrow P$ call IBACI-MHRN // * 调用算法 2
16. return $\hat{Y}$

IBAD-MHRN 算法的计算开销主要来自算法 1 特征降维、数据图像化和算法 2 检测模型 3 部分。最终时间复杂度为 $O(n^2)$。

5　实验结果与分析

5.1　数据集介绍

实验采用物联网僵尸网络数据集 Bot-IoT 进行验证[30]，该数据集包含物联网僵尸网络在侦查阶段和攻击阶段产生的恶意流量样本。实验从数据集中随机抽取了 5 种不同类型的原始恶意流量样本，样本类型分别是 OSScan，ServiceScan，DDoS-HTTP，DDoS-TCP 和 DDoS-UDP，并且通过搭建 Mirai 仿真环境抓取正常网络流量样本（BENIGN）和指挥与控制阶段（C&C）流量作为补充，构成新的实验用原始流量样本集。经过数据预处理，采集的流量样本被处理成统一格式的标准数据集。实验数据集的统计如表 1 所列。

表 1　实验数据集

Table 1　Experiment datasets

Label	Stage	Sample size
BENIGN	正常流量	53435
C&C	指挥与控制	5509
OSScan	侦查/扫描	35547
ServiceScan	侦查/扫描	4305
DDoS-HTTP	攻击	17788
DDoS-TCP	攻击	399811
DDoS-UDP	攻击	262153

通过方差阈值法计算测得样本特征的方差在[0，1]内共有 12 个特征，其余特征方差数值均大于 100。因此，选择 1 作为方差阈值法的过滤值。最后，通过 FS-VT 算法共去除样本中的 12 个特征，分别是：Fwd PSH Flags，Bwd PSH Flags，Fwd URG Flags，Bwd URG Flags，RST Flag Count，ECE Flag Count，FIN Flag Count，CWR Flag Count，Fwd Bulk Rate Avg，Fwd Packet/Bulk Avg，Fwd Bytes/Bulk Avg，Down/Up Ratio。为了避免样本数量不平衡对检测效果的影响，对每个类型的数据样本均采用相同数量的样本数，并且按照 6∶2∶2 的比例将标准数据集切分成训练集、验证集和测试集进行实验。

5.2　实验设置

实验环境如下：操作系统为 Windows11，CPU 为 Inter Core i7-9700，GPU 为 NVIDIA 1660s，采用 python3.9 实现模型的构建，深度学习框架采用 Tensorflow2.10。

另外，实验超参数设置如表 2 所列。Optimizer 采用 Adam 优化器；Learning rate 表示学习率，其决定了模型的更新步长；Batch size 设置为 128，表示每批次训练样本数为 128；Epochs 设置为 50，表示训练 50 轮次。

表 2　超参数设置

Table 2　Hyperparameter settings

Param name	Param value
Optimizer	Adam
Learning rate	0.0001
Batch_size	128
Epochs	50

5.3　评价指标

实验采用准确率（Accuracy，ACC）、精准率（Precision，P）、召回率（Recall，R）和 F1 值（F1-score，F1）作为评价指标。ACC 表示识别正确的样本占总样本的比值；P 表示预测正确样本占实际样本的比值；R 表示预测为正的样本和所有真实样本的比值；F1 值表示准确率和召回率的调和平均值，可评估方法的综合性能。计算式分别如下：

$$ACC=\frac{TP+TN}{TP+TN+FP+FN} \tag{10}$$

$$P=\frac{TP}{TP+FP} \tag{11}$$

$$R=\frac{TP}{TP+FN} \tag{12}$$

$$F1=\frac{2\times P\times R}{P+R} \tag{13}$$

其中，TN 是正确分类的负样本数，TP 是正确分类的正样本数，FN 是错误分类的负样本数，FP 是错误分类的正样本数。

5.4 实验结果与分析

5.4.1 MHRN模型的有效性

1)不同深度时MHRN模型的准确率

为了检验网络深度对模型检测效果的影响,本文设置不同数量的多尺度混合残差块堆积来增加MHRN的深度,比较多尺度混合残差块数量、F1值和测试花费时间三者之间的关系。多尺度混合残差块数量从2逐步递增至6,不同深度时F1值和测试花费时间的实验结果如表3所列。

表3 不同深度时MHRN的准确率与测试时间比较

Table 3 Comparison of accuracy and time spent on MHRN at different depths

Index	2	3	4	5	6
F1/%	98.73	99.81	99.63	99.62	99.57
Time/s	0.36	0.42	0.55	0.68	0.76

不难看出,混合残差块数量少于3时,随着多尺度混合残差块数量的增加,F1值有所提高,这说明多尺度混合残差块的堆积,网络深度加深,有利于提升模型的综合检测性能。然而,混合残差块数量大于3时,模型的F1值开始下降,原因是随着更多的多尺度混合残差块堆积,多个Dropout层会造成有用特征信息的丢失,进而对检测效果造成影响。通过分析,在混合残差块数量为3时,模型可达到较好的检测性能,并且保持较短的检测时间。因此,所提MHRN模型选择多尺度混合残差块的数量为3。

2)MHRN模型中多尺度混合计算的有效性

为了验证所提出的MHRN利用多尺度混合计算能加快模型的收敛速度,本文设计了训练过程中丢失率随训练轮数变化的实验。在多尺度混合残差块结构上取消多尺度混合计算,并通过3层残差块堆积构建出无多尺度混合计算的残差网络模型,记作RN。实验定义两种模型:MHRN和RN。MHRN由3个多尺度混合残差块堆叠、1个展平层和1个全连接层组成;RN由3个普通残差块堆叠、1个展平层和1个全连接层组成。

图6给出了MHRN与RN在训练及验证过程中丢失率的变化情况。

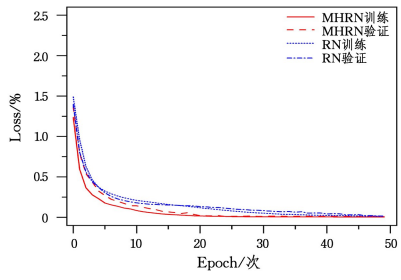


图6 MHRN与RN的丢失率对比

Fig. 6 Comparison of loss rates between MHRN and RN

随着Epoch迭代次数增加,MHRN与RN在训练及验证过程中丢失率均能达到最佳值。但是,与RN相比,MHRN在训练过程中始终保持更低的丢失率,并且在15次迭代后便能够保持非常低的丢失率。原因是多尺度混合计算聚合了不同尺度提取的特征信息,使得模型在面向多阶段性与协议多样化的僵尸网络流量时能够提取更丰富的细节特征,从而加快收敛速度。这一结果证明,本文提出的多尺度混合计算方式可有效加快模型的收敛速度,并且模型也展现出较强的泛化能力。

5.4.2 IBAD-MHRN方法的有效性

为了验证IBAD-MHRN方法在面向物联网环境下僵尸网络多阶段产生的恶意流量有较好的检测效果,本文将僵尸网络不同阶段产生的6种不同类型的恶意流量与正常流量进行流量分类实验。实验将7种不同类型的流量进行混合,分别计算出其准确率、精准率、召回率和F1值的多次实验平均值,实验结果如图7所示。

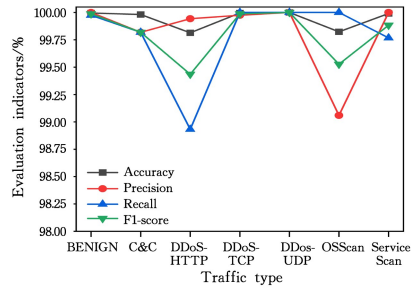


图7 不同阶段僵尸网络流量检测的多个评价指标

Fig. 7 Multiple evaluation indexes of botnet traffic detection at different stages

由图7可知,所提出的IBAD-MHRN方法对僵尸网络不同阶段的恶意流量均有较好的检出效果。其中,对于攻击阶段产生的DDoS-HTTP攻击流量的检测召回率略低于其他流量的检测,这是因为DDoS-HTTP攻击流量在攻击行为模式上与DDoS-TCP相似,造成了一定的误检,但召回率依然能达到98.75%以上。扫描阶段OSScan流量的检测精准率远远低于其他流量,这是因为扫描阶段OSScan流量样本远远多于ServiceScan流量样本,因此造成了一定的误判。物联网僵尸网络多阶段产生的恶意流量均能够被IBAD-MHRN方法准确识别,这一结果说明该方法能够有效地适用于多阶段性与协议多样化的物联网僵尸网络攻击检测场景。

5.4.3 IBAD-MHRN方法的高效性

为了验证本文方法能够高效地检测物联网僵尸网络多阶段产生的恶意流量,实验将IBAD-MHRN方法在不同的指标、相同数据集上与其他几种表现优异的深度学习方法进行比较。参与比较的方法有CNN[15],GRU[16],RNN[17],CNN-LSTM[18]和BiLSTM[19],分别从精准率、召回率和F1值三大指标进行比较。

实验结果的精准率如图8所示。

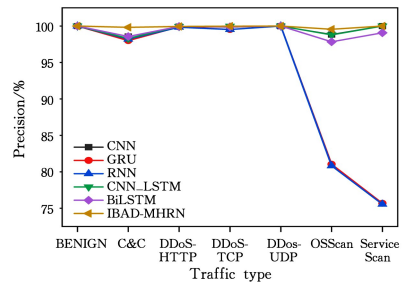


图8 不同方法的精准率对比

Fig. 8 Accuracy comparison of different methods

面向扫描阶段产生的 OSScan 和 ServiceScan 恶意流量检测时，GRU 和 RNN 方法的精准率低于其他方法。CNN 与 CNN_LSTM 方法由于具有出色的空间特征提取能力，在精准率上优于除本文方法以外其他方法，但在面向 C&C 恶意流量检测时，其精准率低于本文提出的 IBAD-MHRN 方法。

图 9 给出了不同方法之间的召回率比较结果。在面向 C&C 与 ServiceScan 检测时，GRU 和 RNN 方法的召回率相对较低，并且在面向扫描阶段流量检测时，本文提出的 IBAD-MHRN 方法相较于其他深度学习方法有着较优的召回率。这一结果说明，本文方法能够更高效地检测出扫描阶段产生的攻击行为。

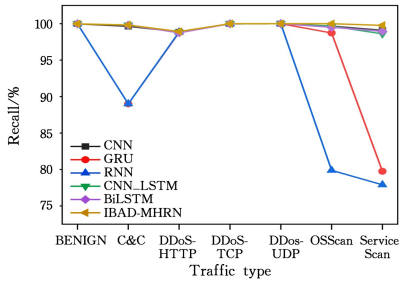


图 9　不同方法的召回率对比

Fig. 9　Recall comparison of different methods

由图 10 可知，GRU 和 RNN 方法在面向 ServiceScan 恶意流量检测时 F1 值不到 80%，并且对 OSScan 恶意流量检测时 F1 值也仅为 88%左右。然而本文提出的 IBAD-MHRN 方法在面向 C&C，OSScan 和 ServiceScan 恶意流量检测时均能保持较高的 F1 值，并且优于其他方法。

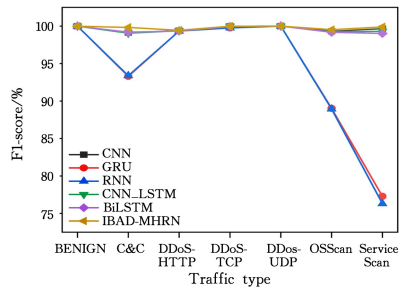


图 10　不同方法的 F1 值对比

Fig. 10　F1-score comparison of different methods

从图 8－图 10 的实验结果可以看出，对正常流量和 DDoS 攻击流量检测时，不同的深度学习方法均能达到较好的检测效果，但在面向僵尸网络的指挥与控制阶段和扫描阶段产生恶意流量检测时，不同方法之间检测效果差异较大。IBAD-MHRN 方法不仅利用多尺度混合计算提高了模型的表征能力，从而有较好的检测效果；而且通过若干多尺度混合残差块的堆积加深了网络，在面向物联网僵尸网络多阶段产生的恶意流量检测时具有更稳定、更高效的检测效果。

表 4 列出了不同深度学习方法的综合评估结果。本文提出的 IBAD-MHRN 方法达到了 99.94%的准确率与 99.80%的 F1 值，相较于其他深度学习方法中较优的 CNN 方法，准确率和 F1 值分别提高了 0.14%，0.36%。因此，本文方法能够有效且高效地适用于面向多阶段性与协议多样化的物联网僵尸网络攻击检测场景。

表 4　不同方法的评估结果

Table 4　Evaluation results of different methods

(%)

Methods	*ACC*	*P*	*R*	*F*1
CNN[15]	99.80	99.52	99.39	99.45
GRU[16]	98.70	94.25	85.42	85.94
RNN[17]	98.68	93.86	85.21	85.55
CNN_LSTM[18]	99.70	99.52	99.54	99.53
BiLSTM[19]	99.72	99.32	99.22	99.25
IBAD-MHRN	99.94	99.82	99.80	99.81

虽然本文提出的 IBAD-MHRN 方法与传统方法相比表现出了一定的优势，但是，随着物联网规模的扩大，设备类型和网络拓扑的多样性可能会导致该方法的适应性不足；并且不同设备之间存在多协议通信模式，这需要对方法进行进一步调整和优化，以满足不同应用场景。

结束语　本文提出了一种物联网僵尸网络多阶段攻击检测方法 IBAD-MHRN。首先，在数据预处理阶段通过方差阈值法进行特征降维，减少模型的计算参数；其次，为了发挥模型的检测性能，提出了一种数据图像化的策略；然后，为了充分提取样本的特征信息，提出了多尺度混合残差网络；最后，提出了一种基于多尺度混合残差网络的物联网僵尸网络攻击类型识别模型和 IBAD-MHRN 方法。IBAD-MHRN 方法能够对物联网僵尸网络不同阶段产生的 C&C 流量、侦查/扫描流量与 DDoS 攻击流量进行检测，在智能家居、工业自动化和智慧城市等多个领域中具有实际应用价值，通过监测异常流量模式，能够及时发现物联网环境中僵尸网络的感染和攻击等恶意活动。

但是，当前的模型和算法局限于具有多阶段性的传统物联网僵尸网络。下一步的研究工作将继续调整和优化方法，以期适应更广泛的物联网僵尸网络攻击检测场景。

参 考 文 献

[1] GSM ASSOCIATION. IoT Connections Forecast: The Rise of Enterprise[OL]. https://www.gsma.com/iot/resources/iot-connections-forecast-the-riseof-enterprise.

[2] ROHIT M H, FAHIM S M, KHAN A H A. Mitigating and detecting ddos attack on iot environment[C]// 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things(RAAICON). IEEE, 2019: 5-8.

[3] DANGE S, CHATTERJEE M. IoT botnet: The largest threat to the IoT network[M]//Data Communication and Networks: Proceedings of GUCON 2019. Singapore: Springer Singapore, 2019: 137-157.

[4] WAZZAN M, ALGAZZAWI D, ALBESHRI A, et al. Cross Deep Learning Method for Effectively Detecting the Propagation of IoT Botnet[J]. Sensors, 2022, 22(10): 3895.

[5] HUSSAIN F, ABBAS S G, PIRES I M, et al. A two-fold machine learning approach to prevent and detect IoT botnet attacks [J]. IEEE Access, 2021, 9: 163412-163430.

[6] BORYS A, KAMRUZZAMAN A, THAKUR H N, et al. An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet[C]// 2022 IEEE World AI IoT Congress(AIIoT). IEEE, 2022: 725-729.

[7] ZHENG J, LI Q, GU G, et al. Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(7): 1838-1853.

[8] ZAINUDIN A, AHAKONYE L A C, AKTER R, et al. An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks[J]. IEEE Internet of Things Journal, 2023, 10(10): 8491-8504.

[9] AYDIN H, ORMAN Z, AYDIN M A. A long short-term memory(LSTM)-based distributed denial of service(DDoS) detection and defense system design in public cloud network environment [J]. Computers & Security, 2022, 118: 102725.

[10] DONG S, SAREM M. DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks[J]. IEEE Access, 2019, 8: 5039-5048.

[11] JIAN S J, LU Z G, DU D, et al. Review on network intrusion detection technology [J]. Journal of Information Security, 2020, 5(4): 96-122.

[12] ALQAHTANI M, MATHKOUR H, BEN ISMAIL M M. IoT botnet attack detection based on optimized extreme gradient boosting and feature selection[J]. Sensors, 2020, 20(21): 6336.

[13] ALSHAMKHANY M, ALSHAMKHANY W, MANSOUR M, et al. Botnet attack detection using machine learning[C]// 2020 14th International Conference on Innovations in Information Technology(IIT). IEEE, 2020: 203-208.

[14] WU Z J, XU Q, WANG J J, et al. Low-rate DDoS attack detection based on factorization machine in software defined network [J]. IEEE Access, 2020, 8: 17404-17418.

[15] IDRISSI I, BOUKABOUS M, AZIZI M, et al. Toward a deep learning-based intrusion detection system for IoT against botnet attacks[J]. IAES International Journal of Artificial Intelligence, 2021, 10(1): 110-120.

[16] RA W, UK S. Detection of IoT Botnet using Machine learning and Deep Learning Techniques [J/OL]. https://doi. org/10. 21203/rs. 3. rs-2630988/v1.

[17] TORRES P, CATANIA C, GARCIA S, et al. An analysis of recurrent neural networks for botnet detection behavior[C]// 2016 IEEE Biennial Congress of Argentina (ARGENCON). IEEE, 2016: 1-6.

[18] ALKAHTANI H, ALDHYANI T H H. Botnet attack detection by using CNN-LSTM model for Internet of Things applications [J]. Security and Communication Networks, 2021, 2021: 1-23.

[19] CHAMOU D, TOUPAS P, KETZAKI E, et al. Intrusion detection system based on network traffic using deep neural networks [C]// 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks(CAMAD). IEEE, 2019: 1-6.

[20] HE K, ZHANG X, REN S, et al. Identity mappings in deep residual networks[C]// Computer Vision—ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part IV 14. Springer International Publishing, 2016: 630-645.

[21] POERNOMO A, KANG D K. Biased dropout and crossmap dropout: learning towards effective dropout regularization in convolutional neural network[J]. Neural Networks, 2018, 104: 60-67.

[22] WANG X, YIN S, LI H, et al. A network intrusion detection method based on deep multi-scale convolutional neural network [J]. International Journal of Wireless Information Networks, 2020, 27: 503-517.

[23] 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.

[24] MA W G, ZHANG Y D, GUO J. Abnormal traffic detection method based on LSTM and Improved residual network optimization [J]. Journal of Communications, 2021, 42(5): 23-40.

[25] LASHKARI A H, ZANG Y, OWHUO G, et al. CICFlowMeter [EB/OL]. https://github. com/ahlashkari/CICFlowMeter/blob/master/ReadMe. txt, 2017.

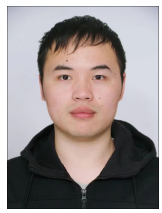
[26] FIDA M A F A, AHMAD T, NTAHOBARI M. Variance Threshold as Early Screening to Boruta Feature Selection for Intrusion Detection System[C]// 2021 13th International Conference on Information & Communication Technology and System (ICTS). IEEE, 2021: 46-50.

[27] LUCKY G, JJUNJU F, MARSHALL A. A lightweight decision-tree algorithm for detecting DDoS flooding attacks[C]// 2020 IEEE 20th International Conferenceon Software Quality, Reliability and Security Companion(QRS-C). IEEE, 2020: 382-389.

[28] HUSSAIN F, ABBAS S G, HUSNAIN M, et al. IoT DoS and DDoS attack detection using ResNet[C]// 2020 IEEE 23rd International Multitopic Conference(INMIC). IEEE, 2020: 1-6.

[29] WANG X T, WANG X, SUN Z X. Network Traffic Anomaly Detection Method Based on Multi-scale Memory Residual Network[J]. Computer Science, 2022, 49(8): 314-322.

[30] PETERSON J M, LEEVY J L, KHOSHGOFTAAR T M. A review and analysis of the bot-iot dataset[C]// 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE). IEEE, 2021: 20-27.



CHEN Liang, born in 1994, postgraduate. His main research interests include network security and information security.

LI Zhihua, born in 1969, Ph. D, professor, master supervisor. His main research interests include key technologies and information security of the end edge cloud, and its intersection with cutting-edge disciplines such as artificial intelligence.

(责任编辑:杨雪敏)