Advances in Applied Mathematics 应用数学进展, 2022, 11(11), 7719-7728
Published Online November 2022 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2022.1111816

Hans汉斯

面向物联网的僵尸网络流量检测与应用

杨　坤[1*]，陈杨芊芊[2]

[1]成都信息工程大学网络空间安全学院，四川　成都
[2]四川大学计算机学院，四川　成都

收稿日期：2022年10月7日；录用日期：2022年11月1日；发布日期：2022年11月10日

摘　要

物联网设备比个人主机更加容易遭受攻击，物联网设备的激增导致基于物联网的僵尸网络攻击的增加。为了减轻来自物联网设备僵尸网络的威胁，需要提高面向物联网的基于流量的僵尸网络流量检测效率和精度。实验出轻量级检测模型方法，应用到自适应的迁移学习策略中去，解决异构物联网中僵尸网络流量的概念漂移问题，进行恶意流量检测。经过Mirai和Gafgyt僵尸网络流量公开数据集的测试，证明检测方法能够精准的二分类识别僵尸网络流量。

关键词

物联网，僵尸网络，流量检测

Botnet Traffic Detection and Application for the Internet of Things

Kun Yang[1*], Yangqianqian Chen[2]

[1]School of Cybersecurity, Chengdu University of Information Technology, Chengdu Sichuan
[2]College of Computer Science, Sichuan University, Chengdu Sichuan

Received: Oct. 7th, 2022; accepted: Nov. 1st, 2022; published: Nov. 10th, 2022

Abstract

IoT devices are more vulnerable to attacks than personal hosts. The proliferation of IoT devices has led to an increase in botnet attacks based on the IoT. In order to mitigate the threat from the botnet of IoT devices, it is necessary to improve the efficiency and accuracy of traffic detection of the traffic based botnet for IoT. The lightweight detection model method is tested and applied to

*通讯作者。

文章引用: 杨坤, 陈杨芊芊. 面向物联网的僵尸网络流量检测与应用[J]. 应用数学进展, 2022, 11(11): 7719-7728.
DOI: 10.12677/aam.2022.1111816

the adaptive migration learning strategy to solve the concept drift problem of botnet traffic in the heterogeneous Internet of Things and detect malicious traffic. The test of Mirai and Gafgyt botnet traffic open data sets proves that the detection method can accurately identify botnet traffic by two classifications.

Keywords

Internet of Things, Botnet, Traffic Detection

1. 引言

近年来，物联网设备数量持续激增，由于缺乏网络安全的重视，物联网设备分散、权责不清，部分设备部署之后基本处于无人监管状态，导致物联网设备存在大量安全隐患，很容易被攻击者发现漏洞并利用，基于物联网的攻击流量呈现逐渐增加的趋势[1]。Mirai 僵尸网络是物联网分布式拒绝服务攻击僵尸网络中的典型代表，其在 2016 年末引发了一场互联网风暴，当时它通过分布式拒绝服务攻击摧毁了多个物联网集群。

与传统个人主机相比，物联网系统的安全风险更高，原因如下：1) PC 机的安全水平在提高，暴露的可利用的高危漏洞快速被修复。而 IoT 设备的生产厂商对漏洞修复效率低下[2]。2) 随着智能家电、智慧城市的普及，依附的 IoT 设备急剧扩张[3]。3) IoT 设备遇到问题不能够及时响应发现，监管不是实时性的，所以被僵尸网络接管后不易被发现。4) IoT 设备的系统通常都是 24 小时持续在线，更加稳定。5) IoT 设备大多具有真实 IP，在 DDoS 攻击中能造成更大伤害，有效对抗 DDoS 防御机制。6) 物联网系统在通信媒介、协议、平台和设备方面高度异构。物联网系统或其部分设备可能在物理上不受保护或由不同方控制[4]。

在物联网环境中，流量传输不停断。针对僵尸网络流量的检测在物联网环境中面临几个关键挑战：1) 物联网流量数据是流式的，可能是无限的；2) 存储一个经过训练的模型来预测即将到来的新数据是不可行的；3) 僵尸网络流量的模式可能会意外改变。僵尸网络流量是僵尸网络操作其组成的计算机设备集群对其他计算机设备发起攻击产生的网络流量，同时也包括僵尸网络感染新的计算机设备期间产生的网络流量。

由于物联网设备硬件资源有限，存储所有资源是不现实的[5]。在预测分析和机器学习中，概念漂移是指模型试图预测的目标变量的统计特性会随着时间以不可预测的方式发生变化。这会造成随着时间的推移，预测变得越来越不准确。

综上所述，由于物联网具有资源受限、数据量大、实时性要求高等特点，将传统技术应用于物联网比较困难，当今大多数大型机安全解决方案都需要大量计算和大内存需求。同时物联网系统高度异构，僵尸网络流量变种多样，造成检测方法的精确度会有大幅波动。

2. 相关研究

为了检测面向物联网的僵尸网络流量，相关工作者提出了不少方法技术。

Soe 等[6]开发了基于机器学习的物联网僵尸网络攻击检测模型。该模型由两个阶段组成：模型训练

阶段和攻击检测阶段。在模型训练阶段，逐步进行数据收集、数据分类、模型训练和特征选择。在攻击检测阶段，首先对数据包进行解码，然后以与模型构建阶段相同的方式提取特征。最后，这些特征被传递到攻击检测器引擎，其中人工神经网络、决策树和朴素贝叶斯机器学习模型被用于僵尸网络攻击检测。

Sriram 等[7]提出了一种基于深度学习的物联网僵尸网络攻击检测框架。提出的解决方案基于物联网流量，这些流量被进一步转换为特征记录，然后传递给深度神经网络模型，用于物联网僵尸网络攻击检测。Nugraha 等[8]通过进行几项实验，评估了僵尸网络攻击检测的四种深度学习模型的性能。实验结果表明，CNN-LSTM 在僵尸网络攻击检测方面优于其他三种深度学习模型。

Parra 等[9]提出了一个基于云计算的分布式深度学习框架来检测物联网僵尸网络攻击。深度学习框架包括递归神经网络和 LSTM 网络模型。

Maeda 等[10]提出了基于软件定义网络的深度学习的僵尸网络攻击检测方法。对于僵尸网络检测，使用从僵尸网络收集的基于流量的流量数据训练深度学习模型，然后评估检测精度。

Bovenzi 等[11]提出了一种用于物联网环境的混合两级入侵检测系统。他们提出的方法首先从网络流量中检测异常，而在第二阶段，他们将异常划分为攻击类别。使用多模态深度自动编码器进行异常检测，同时使用三个机器学习分类器对第一阶段检测到的异常进行分类。

综上，目前物联网僵尸网络流量检测方法倾向于实时检测和分布式异构检测，目的是解决物联网网络流量异构多变，流量内容不仅会产生概念漂移还有持续化产生，训练好的模型就不适用于未来变动的流量检测。本文着重于解决以上问题，提出了两个主要贡献：

1) 提出寻找轻量级检测模型方法，进行模型训练，为提供实时检测能力提供可能性。

2) 同时利用自适应迁移策略，探究异构物联网中僵尸网络流量产生的概念漂移问题，检测训练完成的旧模型是否适用新产生的流量，进而提出如何自适应的调整旧的训练完成的模型检测出时刻变化的恶意流量。

3. 流量检测方法模型

3.1. 机器学习模型

根据相关研究所使用的机器学习算法的表现，选取了两种有代表性的机器学习算法 DNN 和 CNN-LSTM，进行比较检测精准度和计算机资源占有量，选取在占用计算机资源少的情况下检测精确率高的算法模型，并将最优算法应用到自适应检测策略中去。

第一个模型是 DNN，也称之为多层感知机，其中隐藏层具有三层全连接层，每个全连接层设置了不同的维度，是在自编码器模型上删减而来。第一个模型的隐藏层结构见表 1 所示，基础公式见公式 1。

Table 1. The first model hides the layer structure
表 1. 第一个模型隐藏层结构

Hidden Layer	Architecture	Param
1	32	3712
2	72	2376
3	32	2336

$$y = f\left(\sum_{i=1}^{n}\left(\omega_i X_i - \theta\right)\right) \tag{1}$$

其中 x_i 为样本的特征向量，是感知机模型的输入；ω_i，θ 是感知机模型的参数；ω_i 是权重、θ 是阈值。

DNN 采用的学习算法是随机梯度下降法，权重 ω_i 的更新公式如公式 2、3 所示：

$$\omega \to \omega + \Delta\omega \tag{2}$$

$$\Delta\omega = -\eta\left(\hat{y}_i - y_i\right)x_i \tag{3}$$

第二个模型是 CNN-LSTM，由两层卷积层连接长短期记忆神经网络组成，模型结构见表 2 所示。

Table 2. The structure diagram of the second model
表 2. 第二个模型的结构图

Layer	Outputshape	Param
Convld	(115, 64)	384
Convld_1	(115, 32)	10272
Lstm	(115, 32)	8320
Lstm_1	(115, 16)	3136

3.2. 自适应迁移学习策略

迁移学习即获取从一个问题中学习到的特征，然后将这些特征用于新的类似问题。具体操作是保留上一个模型的训练权重，在本次模型进行训练前提前载入权重并新的数据集上进行训练微调。将自适应策略应用到迁移学习的思想上来应对物联网流量突变型概念漂移。

概念漂移即机器学习的训练好的模型不再适用于新的待检测数据，从而导致检测精准度下降。

自适应思想即是指在新的环境适当地改变原系统的结构或参数以保持系统的良好运行特征。更确切的说自适应迁移学习是自适应的调整训练集并且根据数据集漂移程度判断进行重新模型重新微调训练，同时每种物联网设备对应一种拥有相同隐藏层的扩张多层感知机，来适应每种物联网设备的特点。

具体策略应用流程如图 1 所示。

输入： 训练集 D = $\{(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_N, y_N)\}$;
测试集 G = $\{(a_1, b_1), (a_2, b_2), (a_3, b_3), \ldots, (a_M, b_M)\}$;
学习算法 α_1 , α_2 , α_3 , … , α_T , β ;

过程：

for t = 1,2,3,...,T **do**
  h_t = α_t(D);
end for
E = ∅;
for m = 1,2,3,...,M **do**
  for t = 1,2,3,...,T **do**
    if (b_m != $h_t(a_m)$)
      break;
    E = E∪(a_m, b_m);
  end for
end for
wait one cycle
β = β (E)
end

Figure 1. Adaptive transfer learning policy flowchart
图 1. 自适应迁移学习策略流程图

其中学习算法 α_T 包含的 β 算法是由第一个模型或者第二个模型的其中之一构成，为了适应不同的物联网设备做出的模型扩展形成，由 β 模型加上一层不同的参数的隐藏层组成。

迁移学习从公式上解释就是在 ω 中的固定一部分分量 ω_i 进行微调，从而减少训练所花费的时间。

3.3. 整体方法检测

整体检测方法分为四个模块，分别是流量预处理特征提取、流量检测二分类检测、自适应生成调整训练集，自适应的微调训练模型。

整体方法检测结构图如图 2 所示，其中特征提取方法来自 Mirsky 等提出的方法[12]，将 PCAP 文件转换成 CSV 文件。学习算法经过初始训练集预训练完成，投入使用。在检测的过程中输出检测结果，同时在固定时间段内所有学习算法 α_T 共同检测为相同数据标签的数据加入到训练数据集中，在模型检测精度下降时重新进行迁移学习微调检测模型。

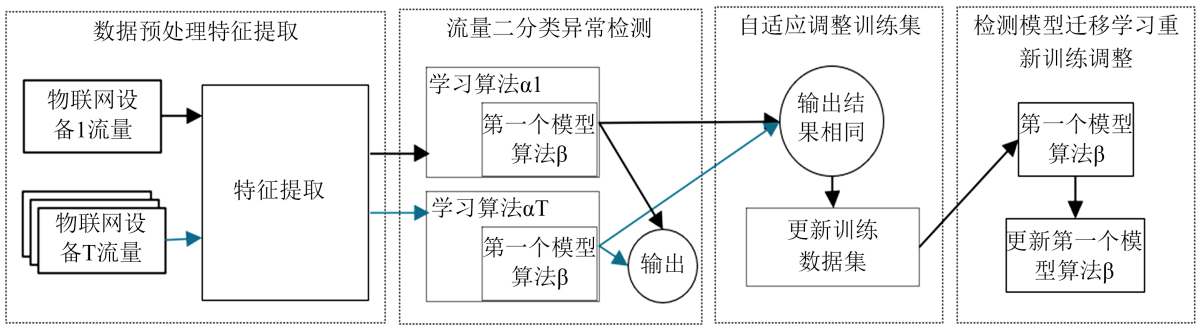

Figure 2. Overall detection method diagram
图 2. 整体检测方法图

4. 实验与分析

4.1. 数据集介绍

实验数据为公开数据集 N-BaIoT [13]，整体流量检测方法包括公开数据集所使用的流量抓取、数据包解析、特征提取方法，流量抓取调用 Wireshark 接口，数据包解析调用 Packet 接口，数据收集和预处理操作具体如下：

1) 数据收集，在交换机上捕获原始网络流量 PCAP 数据，捕获流量通常通过该交换机流。

2) 特征提取，特征提取。每当数据包到达时，对传送该数据包的主机和协议进行行为快照。快照通过提取五个时间窗口上 23 个特征共 115 个特征，流量统计信息来获取数据包的上下文，包括如下五个种类：

1) 来自特定 IP 地址的流量特征的统计值。

2) 来自同一 IP 和 MAC 的流量特征的统计值。

3) 特定主机之间流量的特征的统计值。

4) 包含端口的特定主机之间流量的统计值。

5) 流量包之间时间间隔相关的统计值。

对于每个种类，计算平均值、数据包大小、数据包计数和方差。对于 2)、3)种类，增加了补充统计信息，例如包大小相关系数、幅度、半径和协方差。

数据集具体收集自九种真实物联网设备，包含 Gafgyt 和 Mirai 两个僵尸网络家族各五种攻击流量，

同时包含了来自该物联网设备的良性流量。本文使用通过三种物联网设备的以上攻击以及正常流量数据进行实验，是从 Danmini_Doorbell、Ecobee_Thermostat、Provision_PT_737E 三种型号的物联网设备收集获得。其中被提取特征为流量包的包头信息为主，包括包内的数据流之间的通信情况，不包含包内负载信息。表 3 为型号名叫 Provision_PT_737E 的物联网设备上收集的网络流量样本分布示例表，其他两种物联网设备流量数据集包含同种类标签，只是标签数据分布不同。

Table 3. Provision_PT_737E sample table of sample distributions
表 3. Provision_PT_737E 的样本分布示例表

样本种类名称	样本数量
benign	15,538
mirai_udp	15,345
gafgyt_combo	15,449
gafgyt_junk	14,648
gafgyt_scan	15,676
gafgyt_tcp	15,602
gafgyt_udp	15,120
mirai_ack	14,517
mirai_scan	16,436
mirai_syn	15,625
mirai_udpplain	15,004

4.2. 评价标准

采用准确率(Accuracy)和精确率(PPV)作为分类性能评估，使用分类指标准确率(Accuracy)来评估模型整体标签识别能力，使用分类指标精确率(PPV)来评估模型正常流量和僵尸网络流量二分类识别能力。所涉及的名词缩写、计算公式定义解释如下：

混淆矩阵：混淆矩阵每一行之和是该样本的真实值，每一列之和是被预判为该样本的数量。多分类混淆矩阵横坐标是预测的种类，纵坐标是真实的种类，混淆矩阵如公式 4 所示。

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \tag{4}$$

Accuracy：准确率计算的是正确预测的概率有多少。分类的准确率为混淆矩阵中对角线上的元素之和除混淆矩阵上总的元素之和，是对整体分类的预测结果的准确率的评价，具体公式如公式 5 所示。PPV 是第 i 个类别的检测精确率，具体公式如公式 6 所示，精确率是恶意流量检测的重要指标。

$$\text{Accuracy} = \frac{\sum_{i=1}^{n} a_{ii}}{\sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}} \tag{5}$$

$$\text{PPV} = \frac{a_{ii}}{\sum_{j=1}^{n} a_{ji}} \tag{6}$$

4.3. 实验结果分析

实验都是使用 CPU 资源运行完成，考虑到物联网硬件资源限制，在实验中没有使用 GPU 资源，实验所用处理器型号为 Inteli5-6300HQ。

第一组实验是第一个模型和第二个模型进行比较对于三个数据集的训练时间和多分类 Accuracy，为了实现自适应学习的实时检测，需要模型的训练时间和模型准确率综合考量，寻找最适合的模型当作自适应迁移学习策略的应用算法，如图 3、图 4、图 5 所示，对于 Danmini_Doorbell、Ecobee_Thermostat、Provision_PT_737E 三个数据集，第一个模型在训练时间和多分类整体 Accuracy 都有很好的表现，训练时间所占用的计算机资源存在的差距较大，第一个模型在计算机硬件资源占有量小的情况下达到了 90%左右的准确率。

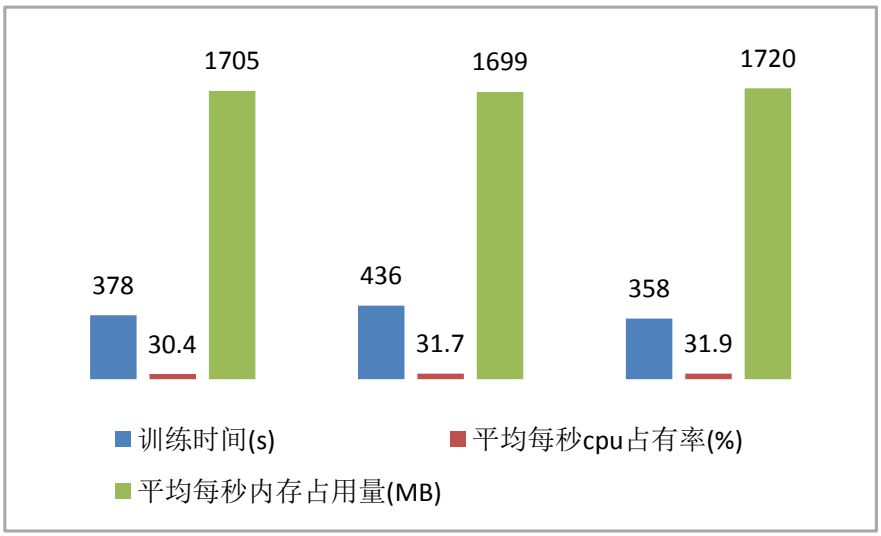

Figure 3. DNN model training time and computer resource consumption
图 3. DNN 模型训练时间和计算机资源占用量

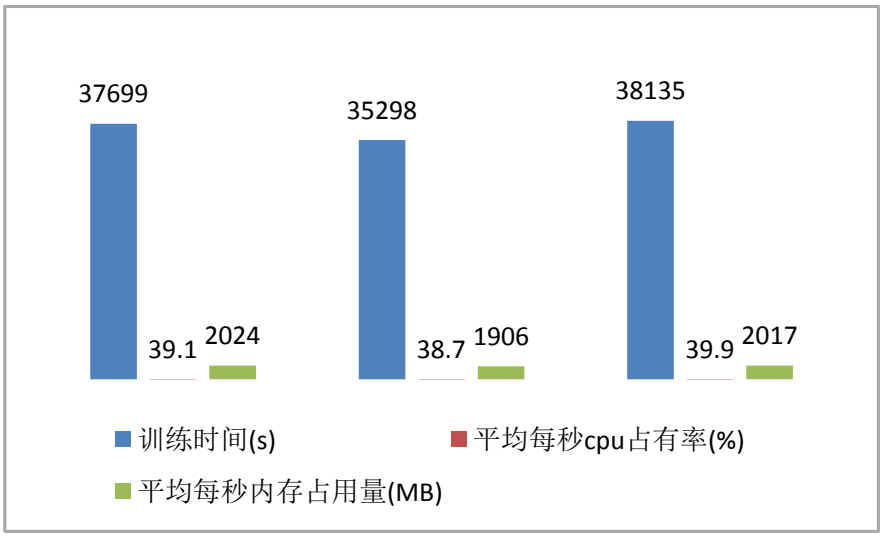

Figure 4. CNN-LSTM model training time and computer resource consumption
图 4. CNN-LSTM 模型训练时间和计算机资源占用量

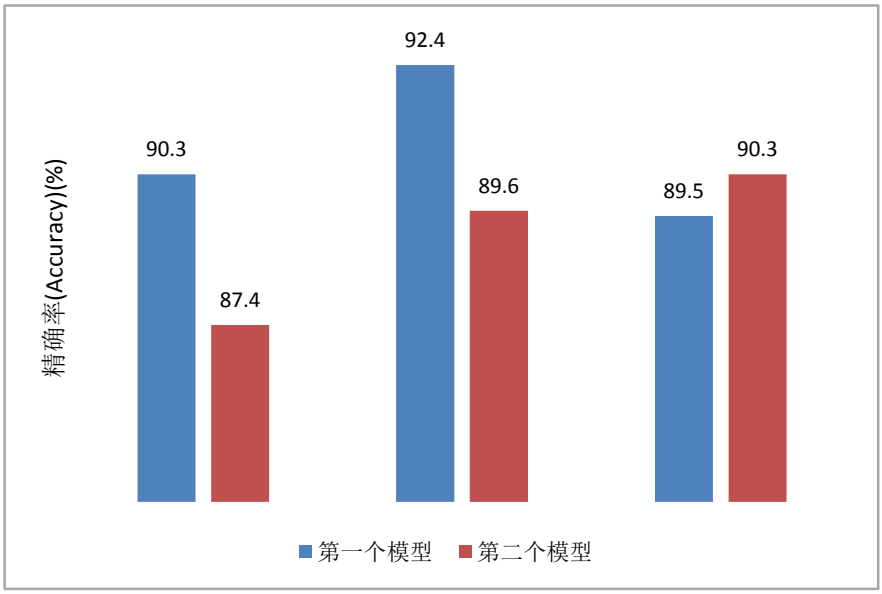

Figure 5. The first set of experimental models detects the accuracy
图 5. 第一组实验模型检测准确率

第二组实验是在第一组实验结果的基础上，选取了第一个模型作为 β 算法模型，即自适应迁移学习策略的应用算法。同时选取 β 模型在 Provision_PT_737E 数据集上的训练权重作为α_T算法模型的初始训练权重。第二组实验结果是良性数据和僵尸网络流量二分类结果精确率，如图 6 所示。

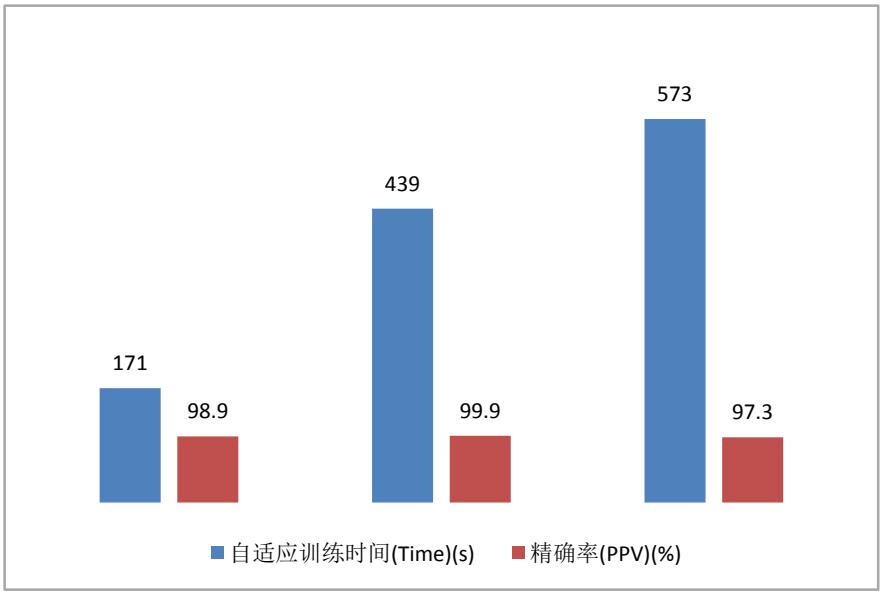

Figure 6. Second set of experiments model detection ppv
图 6. 第二组实验模型检测精确率

针对第二组实验中，检测 Danmini_Doorbell 数据集的算法多分类检测混淆矩阵如图 7 所示。对应的二分类良性流量和僵尸网络流量精确率达到了 99.6%，与 Meidan 等[13]的实验结果精确率相当，且占用的计算机硬件资源更少、训练时间更短，说明自适应迁移学习策略有明显效果。

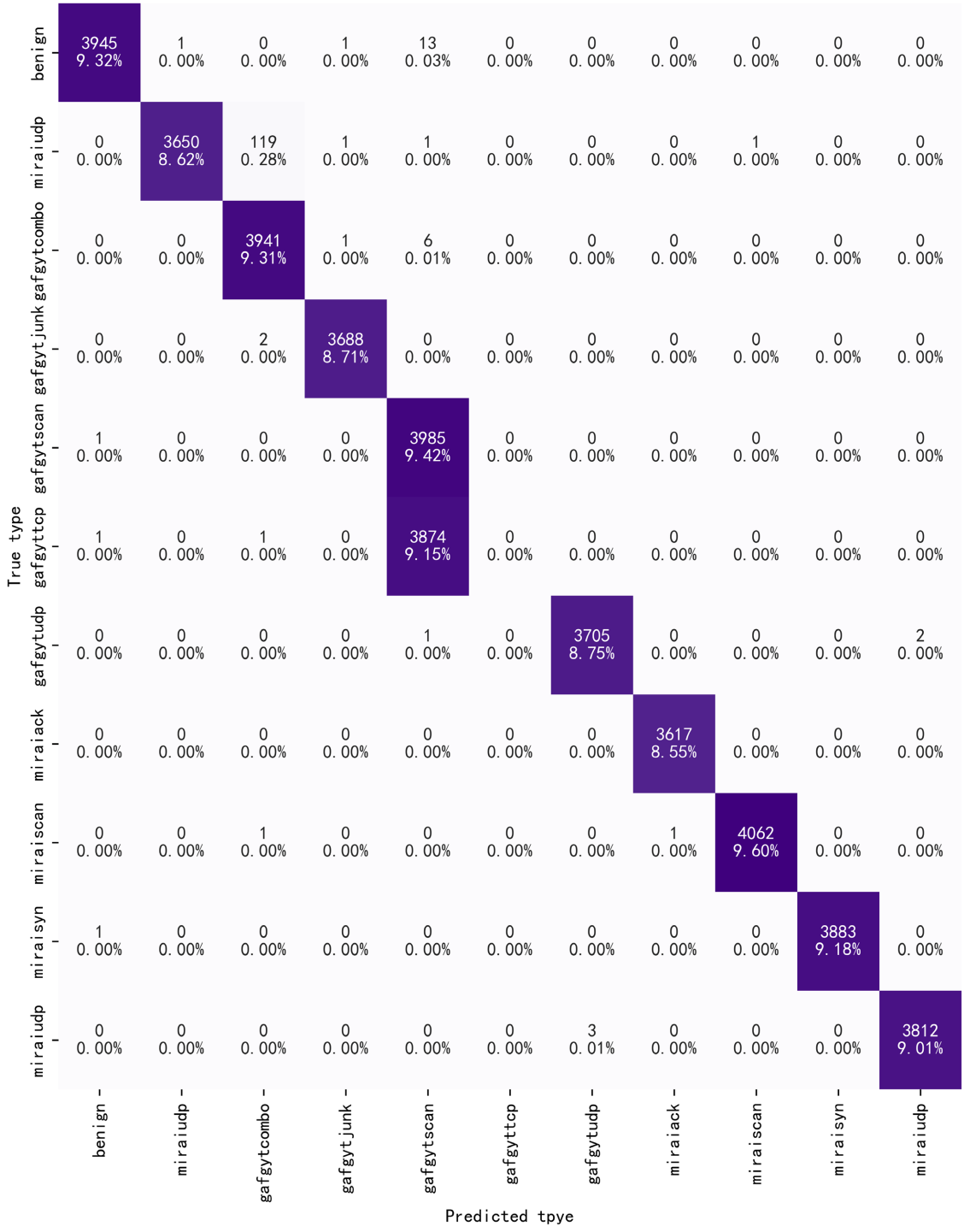

Figure7. Multi-classification detection confusion matrix
图 7. 多分类检测混淆矩阵

5. 结束语

本文我们探索了将检测恶意流量的机器学习轻量化，为未来下沉部署到更接近物联网设备的检测设备上提供可能性。在实现实时检测的同时适应物联网设备异构性高、硬件资源有限的环境，在更接近数

据产生的物联网设备的设备上部署轻量级机器学习检测系统，或者在未来更近一步在交换机网关上部署机器学习恶意流量检测系统。在接下来的工作中，我们将尝试在嵌入式设备中应用 Tensor Flow Lite 框架运行机器学习检测恶意僵尸网络流量。同时进一步优化自适应的迁移学习策略，来适应物联网流量异构多变的特点，进一步提高僵尸网络流量的检测精确率。

致　谢

在此感谢在实验中和文章写作中给与帮助的老师及同学，是他们的鼓励与帮助让本文能够顺利的进行下去。

参考文献

[1] 汤辉. 物联网 DDoS 僵尸网络恶意程序监测分析研究[J]. 计算机学报, 2017(2): 317-336.

[2] 李柏松. 物联网僵尸网络严重威胁网络[J]. 计算机应用与软件, 2011, 28(9): 222-224.

[3] Hallman, R., Bryan, J., Palavicini Jr., G., Divita, J. and Romero-Mariona, J. (2017) IoDDoS—The Internet of Distributed Denial of Service Attacks: A Case Study of the Mirai Malware and IoT-Based Botnets. *Proceedings of the 2nd International Conference on Internet of Things*, *Big Data and Security—IoTBDS*, Porto, 2017, 47-58. https://doi.org/10.5220/0006246600470058

[4] Bertino, E. and Islam, N. (2017) Botnets and Internet of Things Security. *Computer*, **50**, 76-79. https://doi.org/10.1109/MC.2017.62

[5] Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J. (2017) DDoS in the IoT: Mirai and Other Botnets. *Computer*, **50**, 80-84. https://doi.org/10.1109/MC.2017.201

[6] Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R. and Sakurai, K. (2020) Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture. *Sensors*, **20**, 4372. https://doi.org/10.3390/s20164372

[7] Sriram, S., Vinayakumar, R., Alazab, M. and Soman, K. (2020) Network Flow Based IoT Botnet Attack Detection Using Deep Learning. *IEEE INFOCOM* 2020—*IEEE Conference on Computer Communications Workshops* (*INFOCOM WKSHPS*), Toronto, 6-9 July 2020, 189-194. https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162668

[8] Nugraha, B., Nambiar, A. and Bauschert, T. (2020) Performance Evaluation of Botnet Detection Using Deep Learning Techniques. 2020 11*th International Conference on Network of the Future* (*NoF*), Bordeaux, 12-14 October 2020, 141-149. https://doi.org/10.1109/NoF50125.2020.9249198

[9] De La Torre Parra, G., Rad, P., Choo, K.-K.-R. and Beebe, N. (2020) Detecting Internet of Things Attacks Using Distributed Deep Learning. *Journal of Network and Computer Applications*, **163**, 102662. https://doi.org/10.1016/j.jnca.2020.102662

[10] Maeda, S., Kanai, A., Tanimoto, S., Hatashima, T. and Ohkubo, K. (2019) A Botnet Detection Method on SDN Using Deep Learning. 2019 *IEEE International Conference on Consumer Electronics* (*ICCE*), Las Vegas, 11-13 January 2019, 1-6. https://doi.org/10.1109/ICCE.2019.8662080

[11] Bovenzi, G., Aceto, G., Ciuonzo, D., Persico, V. and Pescapé, A. (2020) A Hierarchical Hybrid Intrusion Detection Approach in IoT Scenarios. *GLOBECOM* 2020—2020 *IEEE Global Communications Conference*, Taiwan, 7-11 December 2020, 1-7. https://doi.org/10.1109/GLOBECOM42002.2020.9348167

[12] Mirsky, Y., Doitshman, T., Elovici, Y. and Shabtai, A. (2018) Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. *Proceedings of the 25th Annual Network and Distributed System Security Symposium*, *NDSS* 2018, San Diego, 18-21 February 2018.

[13] Meidan, Y., et al. (2018) N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Computing*, **17**, 12-22. https://doi.org/10.1109/MPRV.2018.03367731