

DNS异常检测：大规模实验分析

侯榕浩¹, 贺明², 孔凯传¹, 陈勇², 左鹏²

(1. 暨南大学网络空间安全学院, 广东 广州 510000; 2. 中国互联网络信息中心, 北京 100190)

摘要: 域名系统 (domain name system, DNS) 是互联网实现互联互通的关键基础设施。域名系统的安全, 直接关系到互联网是否能够正常提供服务, 与人们的工作生活息息相关。围绕 DNS, 设计了3种常见的 DNS 服务器攻击场景, 并在这些场景下收集构建 DNS 主被动数据集供异常检测和预测。通过大量实验对比验证了15种机器学习算法, 包括机器学习算法、深度学习算法 (特别是面向 DNS 不间断服务特性的时间序列检测算法) 对于不同攻击场景异常检测的适用性, 并给出最优的算法模型, 为 DNS 安全态势感知和防护提供多样化模型选择。

关键词: 域名系统; 异常检测; 机器学习; 深度学习

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025067

Anomaly detection in DNS: an empirical study

HOU Ronghao¹, HE Ming², KONG Kaichuan¹, CHEN Yong², ZUO Peng²

1. School of Cyber Science and Engineering, Jinan University, Guangzhou 510000, China

2. China Internet Network Information Center, Beijing 100190, China

Abstract: Domain name system (DNS) is a critical infrastructure that enables connectivity on the internet. The security of the DNS is vital for the ability of Internet to provide services and is closely tied to people's daily work and lives. three DNS server attack scenarios are designed and data is collected to build both active and passive DNS datasets for attack detection, anomaly detection and prediction in these scenarios. Through experimental comparisons, the applicability of up to 15 machine learning algorithms, including both machine learning and deep learning algorithms (especially time-series detection algorithms tailored for the continuous service characteristics of DNS), is validated across various attack and anomaly scenarios. The best algorithm models are presented, providing a diverse set of model choices for DNS system security situational awareness and defense.

Keywords: domain name system, anomaly detection, machine learning, deep learning

0 引言

随着互联网的快速发展, 全球的信息交换、商业活动和社交互动日益依赖于网络基础设施。互联网已成为现代社会的核心组成部分, 支撑着

全球信息的流动。然而, 随着互联网的普及与技术的不断进步, 网络空间的复杂性和安全挑战也不断增加, 这使得如何保障网络的稳定性和安全性成为亟待解决的问题。互联网的稳定运行

收稿日期: 2025-03-21; 修回日期: 2025-06-23

通信作者: 左鹏, zuopeng@cnnic.cn

基金项目: 工业和信息化部工业互联网标识解析体系安全监测与防护项目 (TC220H078); 广东省自然科学基金 (2021A1515011314)

Foundation Items: MIIT Project Industrial Internet Identification Resolution System Security Monitoring and Protection (TC220H078), The Natural Science Foundation of Guangdong Province (2021A1515011314)

依赖于多种关键技术, 其中, 域名系统 (domain name system, DNS) 作为互联网基础架构中的一个核心组成部分, 起着至关重要的作用。

DNS 是互联网中一种分布式的命名系统, 用于将易记的域名映射为对应的 IP 地址。通过 DNS, 用户无须记住数字化的 IP 地址即可访问互联网资源, 极大地方便了互联网的使用。作为一种分层结构, DNS 由多个级别的域名服务器组成, 确保了全球范围内域名解析的高效性和可靠性。DNS 的工作机制涉及域名查询、缓存、递归解析等多个过程, 确保全球范围内的资源可以被迅速且准确地定位和访问。

DNS 自 1984 年诞生至今已有 40 多年的发展历程, 从最初的基于用户数据报协议的域名系统 (DNS over UDP) 只能通过明文传输数据, 到如今发展出了基于传输层安全协议的域名系统 (DNS over TLS, DoT)、超文本传输安全协议 (DNS over HTTPS, DoH)、域名系统安全扩展 (DNSSEC) 等技术来保护 DNS 服务的安全性。

尽管 DNS 的不断发展和优化确保了其高效和可靠的性能, 但在互联网日益复杂的背景下, DNS 仍然面临诸多安全威胁。特别是 DNS 体系存在复杂的授权依赖关系, 该体系遭受的很多攻击和异常会被急剧放大。相关威胁不仅影响到 DNS 服务器的稳定性和可靠性, 还可能对整个互联网生态系统带来深远的负面影响。

随着网络攻击的日益复杂化, 恶意域名、域名劫持和域名滥用等问题也开始浮现, 这些都为 DNS 的安全性带来了巨大挑战。因此, 针对 DNS 的异常检测和安全防护机制的研究显得尤为重要。

本文围绕 DNS 设计了 3 种典型的 DNS 服务器异常场景, 并在这些场景下构建了一个新的 DNS 异常检测数据集。通过一系列实验, 验证了传统机器学习算法、深度学习算法 (特别是时间序列检测算法) 在 DNS 异常检测中的有效性。实验结果表明, 机器学习和深度学习的异常检测方法能够有效识别 DNS 中的异常行为, 为解决 DNS 异常检测问题提供了可行的技术路径。

1 相关工作

1.1 DNS 攻击

DNS 是互联网的核心基础设施之一, 但由于其开放性和分布式结构, 容易受到多种网络攻击。

(1) 拒绝服务 (denial of service, DoS) 攻击
Alieyan 等^[1]对基于 DNS 服务的 DoS 攻击进行了梳理和分析。这些攻击利用 DNS 的基础服务作为工具对其他服务器进行攻击, 造成了广泛而严重的影响。Bushart 等^[2]提出了一种新型应用层 DoS 攻击 DNS UNCHAINED, 针对核心 DNS 基础设施, 将 CNAME 记录链式串联并强制解析器执行深度名称解析, 从而以有效请求使目标权威名称服务器超载。

(2) 缓存投毒攻击

Alharbi 等^[3]提出了新的 DNS 缓存投毒攻击, 该攻击通过对客户端缓存进行 DNS 投毒, 绕过了针对解析器的防御机制, 使得非路径攻击者能够与低权限恶意软件配合, 污染客户端操作系统上的 DNS 缓存。Man 等^[4]发现了如 BIND、Unbound 和 dnsmasq 等软件堆栈中存在的多个弱点, 使攻击者能够突破相关防御, DNS 缓存投毒再次出现。胡杨^[5]指出域名系统中存在恶意密钥生成中心、DNS 转发器缓存中毒攻击问题。

(3) DNS 放大攻击

Anagnostopoulos 等^[6]提出了一种隐蔽的基于 DNSSEC 的放大攻击方法。它利用大量 DNS 转发器来增加放大系数, 攻击者只利用支持 DNSSEC 相关资源记录的转发器, 转发较大的 DNS 数据包。

1.2 异常检测

异常检测是一种数据分析和机器学习技术, 旨在识别与正常模式不一致的观测或数据点。这些异常可能表示数据中的错误、欺诈、故障或其他异常行为。异常检测在许多领域都有广泛的应用, 包括网络安全、金融欺诈检测、工业制造、医疗保健、环境监测等。

传统的异常检测方法主要依赖基于规则匹配、统计分析及签名库的静态防御机制。其中, 基于规则的方法 (如黑名单过滤、查询模式正则匹配) 通过预定义恶意域名或查询语法特征实现

高准确率的已知威胁拦截,但依赖人工经验且难以应对动态生成的域名攻击^[7]。基于统计分析的阈值检测(如查询频率监测、响应类型分布分析)通过建模历史流量基线识别显著偏离正常行为的异常活动,但对低速率隐蔽攻击敏感度不足,且易受网络环境波动干扰^[8-9]。此外,传统方法普遍缺乏对加密 DNS (DoH/DoT) 流量的解析能力,且难以有效关联多维度上下文信息(如时序依赖、跨协议行为),导致其在复杂攻击场景下的泛化性能受限。

近年来,机器学习和深度学习方法通过自动化特征学习、动态适应、复杂场景建模及高维数据处理能力,解决了传统 DNS 异常检测方法在精度、研发效率和可扩展性上的核心瓶颈。

基于机器学习的异常检测, Liu 等^[10]提出了基于监督学习的异常检测 Opprentice。该系统通过并行应用多种现有的异常检测器,从性能数据中提取异常特征,然后使用这些特征和标注数据训练随机森林分类器,自动选择合适的检测器参数组合和阈值。Hasan 等^[11]在物联网攻击与异常检测数据集上比较了逻辑回归、支持向量机、决策树、随机森林和人工神经网络这几种机器学习模型的性能。

基于深度学习的异常检测, Kim 等^[12]引入了一种将一维数据转化为二维数据的编码技术,增强了卷积神经网络(convolutional neural network, CNN)结构识别异常事件的性能。Munir 等^[13]提出了基于深度学习的时间序列数据异常检测方法 DeepAnT,包括两个模块:时间序列预测模块和异常检测器模块。时间序列预测模块使用深度卷积神经网络来预测给定视界内的下一个时间戳。该模块接受一个时间序列窗口(用作上下文),并尝试预测下一个时间戳,然后将预测值传递给异常检测器模块,异常检测器模块负责将相应时间戳标记为正常或异常。江友华等^[14]对用户异常用电行为进行了研究,用 K-means 聚类算法提取负荷状态特征;采用深度学习算法中的 sequence to sequence 模型,将电力用户用电总数据分解成单个电器的功耗数据;结合支持向量机(support vector machine, SVM)算法对分解后的多种家用电器用

电数据进行异常检测。Geiger 等^[15]提出了基于生成对抗网络(generative adversarial network, GAN)的无监督异常检测方法 TadGAN,使用长短期记忆网络(long short term memory, LSTM)作为生成器和判别器的基础模型以捕捉时间序列分布的时间相关性,并采用循环一致性损失进行训练,以实现有效的时间序列数据重建。Li 等^[16]通过构建高置信度根区文件和异常判断规则来检测根服务器自身解析异常和非自身解析异常。Hu 等^[17]利用域名知识,识别并提取了异常递归 DNS 查询行为的 12 个关键特征,实现了一个基于 t-SNE 的密度聚类模型,定位了异常的 DNS 服务器。项思羽等^[18]提出了一种结合混合特征选择和 Transformer 的网络数据流异常检测模型,混合特征选择做数据预处理,以改进 Transformer 完成异常检测。然而,上述研究主要集中在医疗异常、日志异常、视频异常等场景,面向 DNS 服务器异常检测相关的研究较少。因此,本文针对 DNS 场景的异常检测,构建了新的数据集,并在这些数据集上比较了机器学习算法、深度学习算法和时间序列检测算法的效果。

2 实验方法

本文实验流程如图 1 所示:①设计 DNS 服务器异常场景,分别收集被动监测数据和主动探测数据;②数据预处理模块,对收集的数据进行预处理,处理后的数据将被划分为训练集、验证集和测试集;③算法库模块,使用机器学习模型和深度学习模型在收集的数据集中进行训练、验证和测试。

2.1 攻击方法

构建 DNS 服务器异常场景,需确保选择的异常场景是现实世界中频繁发生的,具有高度的可变性和复杂性,这样的场景才可以帮助评估检测方法在面对多样化和未见过的攻击类型时的泛化能力和鲁棒性。因此,本文基于最常见的网络攻击类型设计 DNS 攻击异常场景:DNS 洪泛攻击和 DNS 放大攻击。

DNS 洪泛攻击可以使目标 DNS 服务器不可用或性能下降。DNS 负责将域名解析为对应 IP 地址,是互联网关键基础设施。攻击者向目标

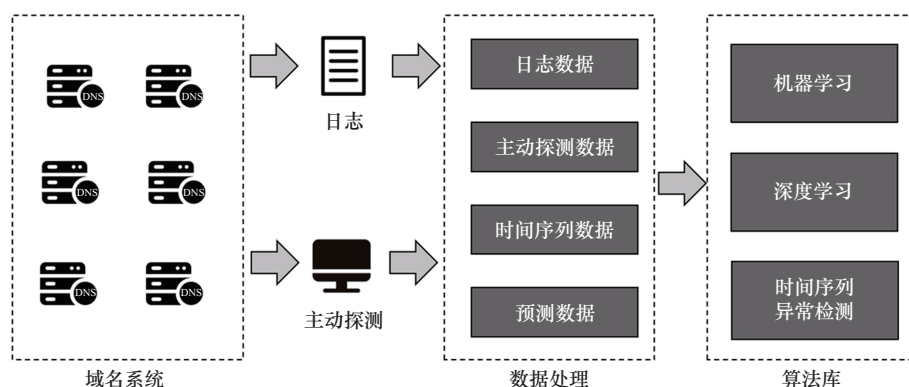


图1 实验流程

DNS服务器发送大量虚假请求，耗尽其资源，致其无法响应合法查询。

DNS洪泛攻击过程如图2所示，僵尸网络向递归DNS服务器发送大量不存在的域名解析请求，导致递归DNS服务器需要不停地向授权服务器发送这些不存在域名的解析请求，持续收发数据包加重服务器的负担，最终导致递归DNS服务器崩溃。

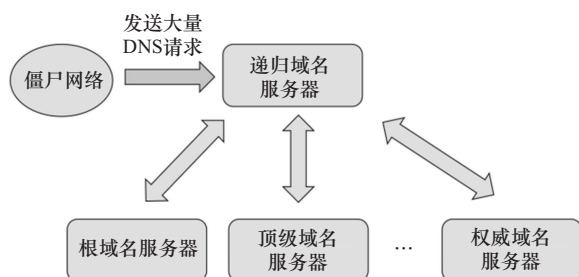


图2 DNS洪泛攻击过程

DNS放大攻击是一种常见的分布式拒绝服务（distributed denial of service, DDoS）攻击形式，它是许多反射放大攻击中的一种。攻击者利用DNS的弱点以及互联网上的僵尸网络或被黑客远程控制的计算机等资源，修改DNS报文的源地址为受攻击者的地址，并向大量互联网公共递归请求发送大量全记录类型的域名查询，以此消耗受攻击者网络带宽和服务器性能资源。

DNS放大攻击流程如图3所示，僵尸网络伪造受害者的源IP地址，向递归DNS服务器发送大量DNS查询请求。递归DNS服务器则会向DNS的各级服务器递归发起查询，最终获取指定域名的IP地址，并将响应包发送至受害者。

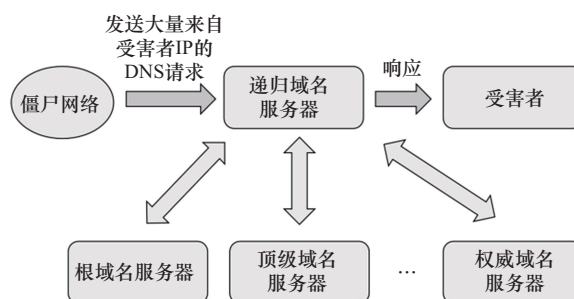


图3 DNS放大攻击流程

2.2 DNS服务器异常场景构建

BIND^[19]（berkeley internet name domain）是一款开源的DNS服务器软件，由加州大学伯克利分校开发和维护，它是目前使用最广泛的DNS服务器软件。

本文使用BIND 9搭建了基本的DNS，其网络结构如图4所示，包括根（Root）域名服务器、顶级（COM）域名服务器、二级（TEST_COM）域名服务器、递归（Recursive）服务器以及4台攻击机（Attack_1~Attack_4）和测试机。利用DNS原生日志和Dig^[20]收集服务数据，构建DNS异常检测数据集。

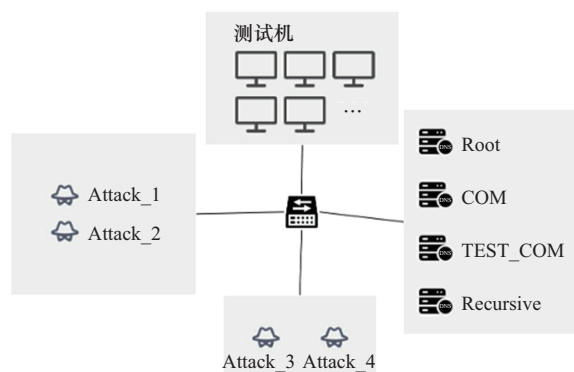


图4 DNS网络结构

本文设计了 3 种不同的 DNS 服务器异常场景,包括 DNS 放大攻击场景、DNS 洪泛攻击场景和混合攻击场景。具体的场景设计如下。

1) DNS 放大攻击场景:使用测试机群对被攻击机的递归 DNS 服务器进行持续的 DNS 查询请求,请求时间间隔 0.01 s,并使用随机生成的域名来模拟正常的 DNS 流量。同时,定期使用攻击机群以 Root 服务器作为跳板,对被攻击机的递归 DNS 服务器进行放大攻击。每次攻击持续 1 min,共进行 4 次攻击,每台机器峰值速率 1×10^5 QPS。每次攻击均造成正常查询的响应时间延长,并引发查询失败。

2) DNS 洪泛攻击场景:通过测试机群持续向目标递归 DNS 服务器发送 DNS 查询请求,请求时间间隔 0.01 s,并使用随机生成的域名来模拟正常的 DNS 流量。同时,定期使用攻击机群对目标递归 DNS 服务器进行洪泛攻击,每次攻击持续 1 min,共执行 4 次攻击,每台机器峰值速率 1×10^5 QPS。每次攻击均造成正常查询的响应时间延长,并引发查询失败。

3) 混合攻击场景:通过测试机群持续向目标递归 DNS 服务器发送 DNS 查询请求,查询时间间隔为 0.01 s,并通过随机生成的域名模拟正常的 DNS 流量。同时,定期使用 Attack_4 对目标递归 DNS 服务器进行洪泛攻击,同时使用 Attack_1、Attack_2 和 Attack_3 进行放大攻击。每次攻击持续 1 min,共执行 4 次,每台机器峰值速率 1×10^5 QPS。每次攻击均造成正常查询的响应时间延长,并引发查询失败。

在上述 3 种攻击场景下均收集以下两种异常数据:被动监测数据和主动探测数据。

1) 被动监测数据:DNS 查询日志记录了域名系统中的所有请求和响应信息,可用于诊断和解决 DNS 性能、安全及故障问题。日志数据包括时间、信息分类、源 IP 地址、端口、查询域名及类别等关键字段。通过分析递归 DNS 服务器上的 DNS 查询日志,可以检测异常的 DNS 查询流量。

2) 主动探测数据:主动探测可及早发现服务器异常,降低故障对业务的影响,提升系统可用性。探测数据包括探测时间、响应耗时和请求是

否成功等。通过分析主动探测返回数据,可以检测服务器是否发生异常。

2.3 数据预处理

数据预处理是机器学习和数据分析中重要的步骤,直接影响模型的性能和泛化能力。正确处理和提取特征可以使模型更容易学习数据的模式,提高模型的预测准确性,并降低过拟合的风险,同时缩短训练时间。

因此,本文对被动监测数据和主动探测数据进行了以下处理,并构建了时间序列数据和服务器异常预测数据。

1) 被动监测数据:由于 DNS 原生日志是非结构化的文本数据,本文通过正则匹配等技术将其转为结构化数据,从而提取关键的时间、信息分类、源 IP 地址、端口、查询域名以及类别等关键字段。然后,利用统计分析等特征工程方法从原始数据中提取更有效的特征,例如单位时间内各类请求数、同源 IP 请求数、同端口请求数等。

2) 主动探测数据:主动探测数据本身为结构化数据,因此本文利用统计分析等特征工程方法从原始数据中提取更有效的特征,例如单位时间内成功请求数、成功率及响应耗时方差等。

3) 时间序列数据:各场景数据按固定周期产生,因此可以将异常检测转化为时间序列分类任务。本文通过时序数据滑窗将原始数据转换成时间序列数据,并对窗口数据进行统计分析。

4) 服务器异常预测数据:为提前识别潜在异常并采取措施,需基于当前状态预测未来异常。通过预测异常,可以实施预防性维护,降低设备故障风险,减少停机时间,提高系统可用性。因此,在主动探测数据和被动监测数据的基础上,构建了预测数据。为使预测数据集能依据当前状态预测未来异常,保留了两类状态字段,即主动探测数据中的主动探测返回信息和被动监测数据集的请求信息,去除原先的异常标记,按预知时间与攻击时段重新标注异常。

2.4 算法库

对 DNS 服务器异常检测而言,算法库模块中包含的算法需要有效应对 DNS 环境中的各种复杂问题。一是主被动数据的多样性问题,不同

地域、时间和设备生成的DNS请求可能具有不同的流量模式,正常请求和异常请求界限往往模糊。例如,某些地区可能正常的查询频率较高,而其他地区较低,这种差异使得准确判断异常变得复杂。主动探测数据的多样性进一步增加了复杂性,攻击者可能伪造看似无害的DNS请求进行恶意行为,传统的检测方法难以区分这些伪装行为。二是不断变化的攻击手段带来的挑战,体现在多种高级攻击方式的出现,如DNS放大攻击、缓存投毒等,这些攻击可通过伪装成正常流量来绕过传统检测,增加了检测系统的难度。

因此,本文在设计算法库模块时,需要包含类型多样的算法以应对不同的场景。算法库模块中包含了以下算法。

1) 传统方法:参考开源的防火墙规则集^[21]和DDoS攻击检测研究^[8-9],构建了基于规则和频率统计的传统方法基线(仅用于被动监测任务)。指标主要包含:DNS请求是否符合DNS标准要求、DNS请求和响应大小差异、窗口时间内同源IP请求数量、窗口时间内同端口请求数量等。

2) 机器学习算法:K近邻(K-nearest neighbor, KNN)^[22]、SVM^[23]、逻辑回归(logistic regression, LR)^[24]、决策树(decision tree, DT)^[25]、随机森林(random forest, RF)^[26]、Adaboost^[27]。

3) 深度学习算法:深度神经网络(deep neural network, DNN)^[28]、CNN^[29]、循环神经网络(recurrent neural network, RNN)^[30]、门控循环单元(gated recurrent unit, GRU)^[31]、LSTM^[32]、时间卷积神经网络(temporal convolutional neural network, TCN)^[33]。

4) 时间序列异常检测算法:MC-LSTM(multiscale CNN-LSTM)、FC-GRU(frequency-CNN-GRU)、TCN-LSTM。

其中,机器学习算法和深度学习算法是近年来DNS异常检测相关研究的常用方法,能够自动从海量DNS流量中学习深层特征,通过模型捕捉非线性关系和动态模式,有效识别未知攻击类型,显著提升检测准确性和泛化能力,在实践中也取得了良好的效果。

然而,尽管机器学习模型和深度学习模型可以用于异常检测问题,但也存在局限性。一方

面,服务器异常检测场景中不同时间段的数据之间可能存在较大的差异(如服务器夜间CPU负载相对较小,而白天访问服务器的人数较多,CPU负载相应较大),难以根据单一时间点的数据来判断服务器在某一时段是否存在异常。另一方面,服务器数据的变化与时间存在较强的关联(如DoS攻击会突然增大服务器的内部压力,导致主动探测数据在某时段内响应明显迟缓),常常表现为数据在时间尺度上的波动。

综上,时间序列异常检测算法可结合服务器数据的时间规律,利用每个时间点数据多维度特征之间的关联,以及数据在时间上的前后关联,提升异常检测的精度。由此,提出了融合时间序列异常检测算法的DNS异常检测模型。

MC-LSTM模型由CNN、LSTM和DNN组成,网络结构如图5所示。在CNN层中采用多种不同大小的卷积核,增强空间特征提取能力,能够解决多维时间序列挑战中面临的各维度间的特征提取和单维度不同时间序间的特征提取问题。

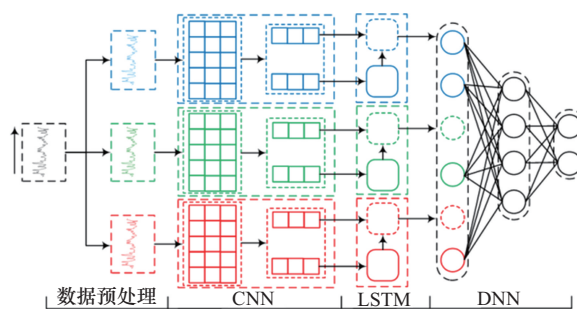


图5 MC-LSTM网络结构

FC-GRU模型包含傅里叶变换方法、卷积算法、GRU和DNN,网络结构如图6所示。通过快速傅里叶变换构建包含频率和时间特征的频率矩阵。利用CNN提取频率间关联特性。进一步使用GRU刻画频率间的整体关联性,以辅助CNN提取特征。从频域的视角,实现异常检测,解决异常序列在时域难辨,而在频域可辨的问题。

TCN-LSTM模型结合了TCN、LSTM和DNN,网络结构如图7所示。利用TCN可以并行计算所有时间步中的数据,兼具强大的长期依赖建模能力和更少的参数量,解决传统时序分析模型在处理长序列场景时,随着网络层数增加,可能出现的梯度消失或梯度爆炸的问题。

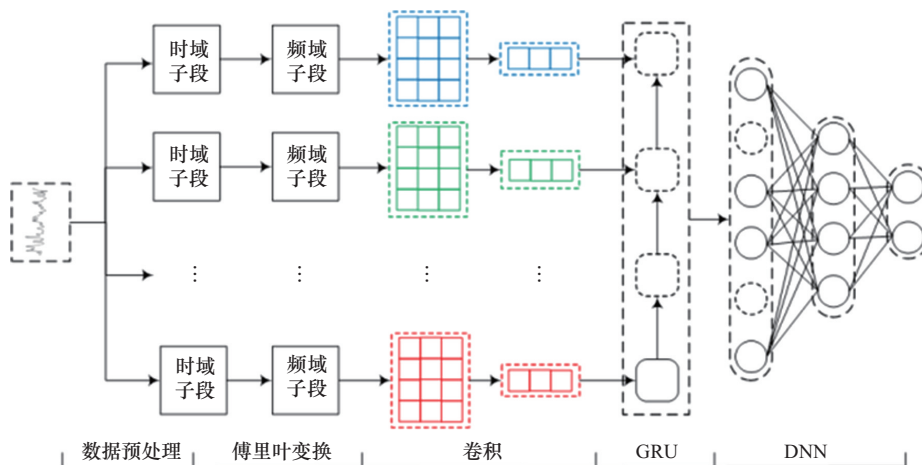


图6 FC-GRU网络结构

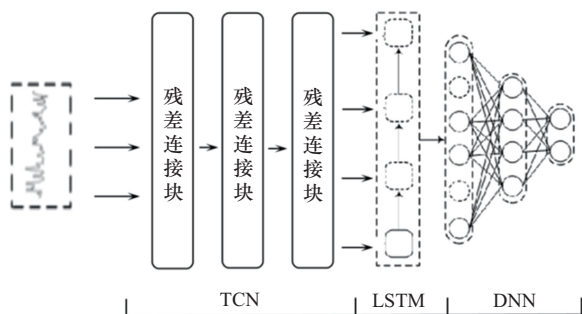


图7 TCN-LSTM网络结构

2.5 实验设置

递归DNS服务器：Intel Xeon W-2225、64 GB 内存、1 Gbit/s 网络接口；攻击机与测试机：Intel i7-10700K、32 GB 内存；算法库服务器：Intel Xeon W-2225、RTX 3080、64 GB 内存。

在DNS服务器异常场景中，本文收集了以下6类数据集：DNS洪泛攻击被动监测数据集、DNS洪泛攻击主动探测数据集、DNS放大攻击被动监测数据集、DNS放大攻击主动探测数据集、混合攻击被动监测数据集、混合攻击主动探测数据集。

被动监测数据集：在DNS洪泛攻击场景下，收集了50万条记录；在DNS放大攻击场景下，收集了超过90万条记录；在DNS混合攻击场景下，收集了超过80万条记录。

主动探测数据集：在DNS洪泛攻击场景下，收集18万条记录；在DNS放大攻击场景下，收集了超过18万条记录；在DNS混合攻击场景下，收集了18万条记录。

上述数据集用于实验训练和测试。实验过程

中，将数据集按照6:4的比例分为训练集和测试集，从训练集中取20%作为验证集，实验采用F1值、召回率（recall）、精确率（precision）、准确率（accuracy）作为评价指标。计算式如下：

$$F1 = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \quad (1)$$

$$\text{recall} = \frac{|\text{TP}|}{|\text{TP}| + |\text{FN}|} \quad (2)$$

$$\text{precision} = \frac{|\text{TP}|}{|\text{TP}| + |\text{FP}|} \quad (3)$$

$$\text{accuracy} = \frac{|\text{TP}| + |\text{TN}|}{|\text{TP}| + |\text{TN}| + |\text{FP}| + |\text{FN}|} \quad (4)$$

其中，TN表示正确预测的负例，FN表示错误预测的负例，FP表示错误预测的正例，TP表示正确预测的正例。

3 实验结果

3.1 DNS放大攻击场景

DNS放大攻击场景测试集实验结果见表1，其中加粗的是综合表现最好的模型的数值。在放大攻击场景的被动监测数据集中，算法库模块中的模型在测试集中的F1值、准确率、精确率、召回率的中位数（平均值）分别为91.67%（91.70%）、95.69%（95.72%）、91.67%（89.98%）、94.14%（93.95%），说明算法库模块中的大部分模型能够满足放大攻击场景的被动监测数据异常检测的精度要求，适用于从DNS服务器的被动监测日志中检测放大攻击。同时，测试集实验结果中的F1值、准确率、精确率、召回率的最高值分别为95.33%、97.57%、100.0%、99.31%，对应的模型

表1 DNS放大攻击场景测试集实验结果

模型	被动监测数据集				主动探测数据集				被动监测预测数据集				主动探测预测数据集			
	F1值	准确率	精确率	召回率	F1值	准确率	精确率	召回率	F1值	准确率	精确率	召回率	F1值	准确率	精确率	召回率
传统方法	72.86%	84.00%	64.69%	83.39%	—	—	—	—	—	—	—	—	—	—	—	—
KNN	87.80%	93.37%	81.23%	95.52%	73.85%	95.88%	67.29%	81.82%	81.03%	89.23%	72.36%	92.07%	78.26%	94.77%	70%	88.73%
SVM	90.36%	95.61%	100%	82.41%	81.33%	97.74%	98.39%	69.32%	87.71%	94.40%	97.07%	80.00%	88.19%	97.76%	100%	78.87%
LR	93.97%	97.07%	96.72%	91.38%	82.12%	97.82%	98.41%	70.45%	91.03%	95.52%	91.03%	91.03%	89.92%	98.06%	100%	81.69%
DT	89.69%	94.57%	85.36%	94.48%	60.56%	92.01%	46.63%	86.36%	82.57%	90.44%	75.79%	90.69%	71.58%	91.94%	57.14%	95.77%
RF	88.32%	93.71%	82.39%	95.17%	74.29%	95.64%	63.93%	88.64%	81.92%	89.92%	74.23%	91.38%	78.36%	94.48%	67%	94.37%
Adaboost	88.89%	94.06%	83.38%	95.17%	72.64%	95.32%	62.10%	87.50%	83.31%	90.78%	76.07%	92.07%	75.43%	93.58%	63.46%	92.96%
DNN	93.66%	96.90%	95.68%	91.72%	82.89%	97.90%	98.44%	71.59%	91.29%	95.69%	92.25%	90.34%	90.77%	98.21%	100%	83.10%
CNN	93.75%	96.90%	94.41%	93.10%	82.89%	97.90%	98.44%	71.59%	90.26%	95.09%	89.49%	91.03%	90.77%	98.21%	100%	83.10%
RNN	93.59%	96.81%	94.08%	93.10%	82.89%	97.90%	98.44%	71.59%	88.67%	94.14%	85.81%	91.72%	90.77%	98.21%	100%	83.10%
GRU	93.43%	96.73%	93.75%	93.10%	82.89%	97.90%	98.44%	71.59%	90.88%	95.43%	90.72%	91.03%	90.77%	98.21%	100%	83.10%
LSTM	93.26%	96.64%	93.43%	93.10%	82.89%	97.90%	98.44%	71.59%	86.55%	92.85%	81.65%	92.07%	90.77%	98.21%	100%	83.10%
TCN	91.61%	95.69%	89.22%	94.14%	85.71%	98.14%	94.52%	78.41%	92.11%	96.21%	95.89%	88.62%	90.77%	98.21%	100%	83.10%
MC-LSTM	95.33%	97.57%	91.67%	99.31%	91.57%	98.86%	96.03%	87.36%	87.85%	93.66%	84.35%	91.67%	97.84%	99.55%	98.55%	97.14%
FC-GRU	90.13%	94.62%	83.24%	98.26%	89.70%	98.62%	94.87%	85.06%	88.70%	94.36%	88.85%	88.54%	98.55%	99.70%	100%	97.14%
TCN-LSTM	91.67%	95.49%	85.12%	99.31%	91.67%	98.86%	95.06%	88.51%	88.64%	93.92%	83.23%	94.79%	97.84%	99.55%	98.55%	97.14%

依次为 MC-LSTM、MC-LSTM、SVM、MC-LSTM。说明相较于其他模型, MC-LSTM在 DNS 服务器的放大攻击检测上具有更强的检测能力。

在放大攻击场景的主动探测数据集中, 算法库模块中的模型在测试集中的 $F1$ 值、准确率、精确率、召回率的最高值分别为 91.67%、98.86%、98.44%、88.64%, 对应的模型依次为 TCN-LSTM、MC-LSTM、DNN、RF, 说明针对不同精度指标要求, 算法库模块中都存在能够适用的模型。在测试集中的 $F1$ 值、准确率、精确率、召回率的中位数依次为 82.89%、97.90%、98.39%、71.59%, 说明算法库模块中的大部分模型能够基本满足该场景下 $F1$ 值、准确率、精确率上的检测精度要求, 能够从对服务器的主动探测中检测放大攻击。但对于召回率要求高的情况, 则应该放弃传统基于机器学习和深度学习的模型, 尝试使用时间序列检测模型, 其中检测性能较好的是 TCN-LSTM 模型, 召回率达 88.51%。

在放大攻击场景的预测数据集中, TCN-LSTM 模型和 FC-GRU 模型取得了较好的效果, TCN-LSTM 模型在被动监测预测中 $F1$ 值、准确率、精确率、召回率 88.64%、93.92%、83.23%、94.79%, FC-GRU 模型在主动探测预测中则达 98.55%、99.70%、100%、97.14%。在被动监测预测中算法库在测试集中的中位数分别为

88.64%、94.14%、85.81%、91.03%, 而在主动探测预测中的中位数分别为 90.77%、98.21%、100.0%、83.10%, 说明算法库模块中的大部分模型能够满足该场景下的预测精度要求, 可用于预测服务器即将遭遇的放大攻击。

在放大攻击场景的任务中, MC-LSTM、FC-GRU、TCN-LSTM 3 类时间序列模型在各评价指标上均取得较好效果。DNS 放大攻击的突发性、周期性、多维关联特性与时间序列模型优势高度契合。结合 TCN 的并行计算能力、LSTM 的时序敏感性, 使时间序列模型能够更精准地捕捉攻击流量与正常流量的动态差异, 从而在检测精度、召回率和鲁棒性上显著优于其他方法。

综上, 在 DNS 放大攻击场景的实验中, 验证了 15 种机器学习算法, 包括传统机器学习算法和深度学习算法 (特别是面向 DNS 不间断服务特性的时间序列检测算法), 在 DNS 服务器遭遇放大攻击及其异常场景的适用性, 为 DNS 系统安全态势感知和防护提供多样化模型选择。另外, 传统方法基线表现不佳, 表明其灵活性不足, 难以应对日益复杂多样的攻击。

3.2 DNS 混合攻击场景

DNS 混合攻击场景测试集实验结果见表 2, 其中加粗的是综合表现最好的模型。在混合攻击场景收集的被动监测数据集中, 算法库模块中的

表2 DNS混合攻击场景测试集实验结果

模型	被动监测数据集				主动探测数据集				被动监测预测数据集				主动探测预测数据集			
	F1 值	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值	准确率	精确率	召回率	F1 值	准确率	精确率	召回率
传统方法	73.10%	84.26%	65.27%	83.06%	—	—	—	—	—	—	—	—	—	—	—	—
KNN	87.80%	93.37%	81.23%	95.52%	85.00%	97.14%	97.70%	75.22%	83.74%	90.87%	75.41%	94.14%	92.59%	97.93%	100%	86.20%
SVM	90.36%	95.61%	100%	82.41%	84.69%	97.14%	100%	73.45%	90.36%	95.61%	100%	82.41%	91.93%	97.77%	100%	85.06%
LR	93.97%	97.07%	96.72%	91.38%	84.69%	97.14%	100%	73.45%	93.75%	96.90%	94.41%	93.10%	91.93%	97.77%	100%	85.06%
DT	89.51%	94.49%	85.31%	94.14%	64.93%	91.03%	56.12%	76.99%	89%	94.23%	84.95%	93.45%	80.43%	93.81%	76.29%	85.06%
RF	88.89%	94.06%	83.38%	95.17%	84.31%	96.95%	94.51%	76.11%	87.74%	93.45%	82.42%	93.79%	89.82%	97.08%	93.75%	86.21%
Adaboost	88.89%	94.06%	83.38%	95.17%	76.85%	95.22%	80.58%	73.45%	88.21%	93.71%	82.98%	94.14%	82.76%	94.85%	82.76%	82.76%
DNN	94.14%	97.16%	97.07%	91.38%	84.69%	97.14%	100%	73.45%	93.50%	96.81%	95.34%	91.72%	89.87%	97.25%	100%	81.61%
CNN	93.13%	96.55%	92.81%	93.45%	84.69%	97.14%	100%	73.45%	93.59%	96.81%	94.08%	93.10%	91.93%	97.77%	100%	85.06%
RNN	92.33%	96.12%	91.25%	93.45%	84.69%	97.14%	100%	73.45%	91.92%	95.87%	89.80%	94.14%	89.87%	97.25%	100%	81.61%
GRU	93.52%	96.81%	95.02%	92.07%	84.69%	97.14%	100%	73.45%	92.97%	96.47%	92.49%	93.45%	89.87%	97.25%	100%	81.61%
LSTM	93.59%	96.81%	94.08%	93.10%	84.69%	97.14%	100%	73.45%	91.92%	95.87%	89.80%	94.14%	89.87%	97.25%	100%	81.61%
TCN	93.13%	96.55%	92.81%	93.45%	84.69%	97.14%	100%	73.45%	93.91%	96.99%	94.74%	93.10%	89.87%	97.25%	100%	81.61%
MC-LSTM	93.62%	96.61%	88.54%	99.31%	92.75%	98.56%	100%	86.49%	91.92%	95.83%	89.22%	94.79%	100%	100%	100%	100%
FC-GRU	89.84%	94.44%	82.75%	98.26%	92.23%	98.46%	100%	85.59%	91.22%	95.49%	88.82%	93.75%	99.42%	99.83%	98.84%	100%
TCN-LSTM	94.21%	96.96%	89.91%	98.96%	92.75%	98.56%	100%	86.49%	94.34%	97.14%	93.22%	95.49%	99.42%	99.83%	98.84%	100%

模型在测试集中的 $F1$ 值、准确率、精确率、召回率的中位数（平均值）分别为 93.13%（91.8%）、96.55%（95.78%）、91.25%（90.28%）、93.45%（93.81%），说明算法库模块中的大部分模型能够满足 DNS 混合攻击场景的被动监测数据异常检测的精度要求，能够适用于从服务器的被动监测日志中检测混合攻击。在测试集中的 $F1$ 值、准确率、精确率、召回率的最高值分别为 94.21%、97.16%、100%、99.31%，对应的模型依次为 TCN-LSTM、DNN、SVM、MC-LSTM，说明针对不同精度指标要求，算法库模块中存在适用的模型。

在混合攻击场景的主动探测数据集中，算法库模块中的模型，在测试集中的 $F1$ 值、准确率、精确率、召回率的最高值达 92.75%、98.56%、100%、86.49%，对应的模型依次为 TCN-GRU、MC-LSTM、SVM、MC-LSTM，说明针对不同精度指标要求，算法库模块中存在适用的模型。在测试集中的 $F1$ 值、准确率、精确率、召回率的中位数（平均值）分别为 84.69%（84.52%）、97.14%（96.87%）、100%（95.26%）、73.45%（76.53%），

说明算法库模块中的大部分模型基本满足 $F1$ 值、准确率、精确率要求，可从服务器主动探测中检测混合攻击，而对于召回率要求高的情况，则最好使用时间序列检测模型，其中检测性能较高的是 MC-LSTM 和 TCN-LSTM 模型，召回率均达 88.51%。

在混合攻击场景的预测数据集中，TCN-LSTM 模型和 MC-LSTM 模型取得了较好的效果，TCN-LSTM 模型在被动监测预测中 $F1$ 值、准确率、精确率、召回率分别为 94.34%、97.14%、93.22%、95.49%，MC-LSTM 模型在主动探测预测中均为 100%。在被动监测预测中，算法库在测试集中 $F1$ 值、准确率、精确率、召回率的中位数分别为 91.92%、95.87%、89.8%、93.75%，而在主动探测预测中的中位数分别为 89.87%、97.25%、100.00%、85.06%，说明算法库模块中的大部分模型能够满足该场景下的预测精度要求，可用于预测服务器即将遭遇的混合攻击。

在混合攻击场景的任务中，MC-LSTM、FC-GRU、TCN-LSTM 3 类时间序列模型在各评价指

标中均取得较好的效果。混合攻击结合了DNS洪泛攻击(流量突增)和放大攻击(反射放大)的双重特性,复杂性显著高于单一攻击场景。时间序列模型通过多尺度特征提取的特性,可捕获两类攻击特征。

综上,在DNS混合攻击场景的实验中,对比了15种算法的性能,包括传统机器学习算法和深度学习算法(尤其是面向DNS不间断服务特性的时间序列检测算法)。实验评估各类算法在DNS服务器面临混合攻击及异常场景中的适用性,为DNS系统安全态势感知与防护提供多样化模型选择。另外,传统方法基线的表现不佳,表明面对日益复杂多样的攻击,无法仅依赖人工规则与黑名单防御。

3.3 DNS洪泛攻击场景

DNS洪泛攻击场景测试集实验结果见表3,其中加粗的是综合表现最好的模型的数值。在洪泛攻击场景的被动监测数据集中算法库模块中的模型在测试集中的 $F1$ 值、准确率、精确率、召回率的中位数(平均值)分别为97.22%(97.30%)、99.42%

(99.43%)、98.6%(98.13%)、95.89%(96.34%),说明算法库模块中的大部分模型能够满足洪泛攻击场景的被动监测数据异常检测的精度要求,可用于从DNS服务器被动监测日志中检测洪泛攻击。在测试集中的 $F1$ 值、准确率、精确率、召回率的最高值分别为99.31%、99.85%、100%、99.31%,对应的模型依次为TCN-LSTM、TCN-LSTM、SVM、TCN-LSTM,说明相较其他模型,TCN-LSTM在DNS服务器的洪泛攻击检测上具有更强的检测能力。总体而言,算法库满足洪泛攻击场景下的检测精度要求,能够从服务器的被动监测日志中检测洪泛攻击。

在洪泛攻击场景的主动探测数据集中,算法库模块中的模型的 $F1$ 值、准确率、精确率、召回率的最高值分别为99.29%、99.85%、100.0%、98.59%,对应的模型依次为MC-LSTM、MC-LSTM、LR、MC-LSTM,说明对于不同类型的精度要求,算法库模块中存在适用的模型。各模型的 $F1$ 值、准确率、精确率、召回率的中位数为94.96%、98.99%、98.51%、91.67%,说明算

表3 DNS洪泛攻击场景测试集实验结果

模型	被动监测数据集				主动探测数据集				被动监测预测数据集				主动探测预测数据集			
	$F1$ 值	准确率	精确率	召回率	$F1$ 值	准确率	精确率	召回率	$F1$ 值	准确率	精确率	召回率	$F1$ 值	准确率	精确率	召回率
传统方法	83.69%	94%	100%	71.96%	—	—	—	—	—	—	—	—	—	—	—	—
KNN	97.22%	99.42%	95.89%	95.89%	92.62%	98.41%	89.61%	95.83%	95.04%	98.98%	98.53%	91.78%	92.37%	99.05%	96.64%	88.46%
SVM	96.45%	99.27%	100%	93.15%	94.96%	98.99%	98.51%	91.67%	95.04%	98.98%	98.53%	91.78%	93.88%	99.25%	100%	88.46%
LR	97.22%	99.42%	98.59%	95.89%	95.65%	99.14%	100%	91.67%	95%	98.98%	99.25%	91.10%	93.88%	99.25%	100%	88.46%
DT	95.62%	99.06%	94.04%	97.26%	63.26%	88.62%	47.55%	94.44%	83.81%	96.30%	78.11%	90.41%	58%	91.64%	42.96%	89.23%
RF	96.59%	99.27%	95.95%	97.26%	86.79%	96.97%	79.31%	95.83%	91.10%	98.11%	91.10%	91.10%	83.94%	97.81%	79.86%	88.46%
Adaboost	96.93%	99.35%	96.60%	97.26%	82.42%	95.82%	73.12%	94.44%	92.63%	98.48%	94.96%	90.41%	81.85%	97.46%	76.16%	88.46%
DNN	96.45%	99.27%	100%	93.15%	94.96%	98.99%	98.51%	91.67%	95.04%	98.98%	98.53%	91.78%	93.88%	99.25%	100%	88.46%
CNN	97.56%	99.49%	99.29%	95.89%	94.96%	98.99%	98.51%	91.67%	94.66%	98.91%	98.52%	91.10%	93.88%	99.25%	100%	88.46%
RNN	97.22%	99.42%	98.59%	95.89%	94.96%	98.99%	98.51%	91.67%	95.04%	98.98%	98.53%	91.78%	88.72%	98.56%	89.76%	87.69%
GRU	97.56%	99.49%	99.29%	95.89%	95.65%	99.14%	100%	91.67%	95.04%	98.98%	98.53%	91.78%	93.44%	99.20%	100%	87.69%
LSTM	97.56%	99.49%	99.29%	95.89%	95.65%	99.14%	100%	91.67%	95.04%	98.98%	98.53%	91.78%	93.88%	99.25%	100%	88.46%
TCN	97.93%	99.56%	98.61%	97.26%	94.96%	98.99%	98.50%	91.67%	94.96%	98.98%	100%	90.41%	86.69%	98.26%	85.71%	87.69%
MC-LSTM	97.92%	99.56%	98.60%	97.24%	99.29%	99.85%	100.00%	98.59%	97.53%	99.49%	100%	95.17%	96.80%	99.60%	100%	93.80%
FC-GRU	97.93%	99.56%	97.93%	97.93%	97.84%	99.56%	100.00%	95.77%	95.17%	98.98%	95.17%	95.17%	96.41%	99.55%	99.18%	93.80%
TCN-LSTM	99.31%	99.85%	99.31%	99.31%	98.59%	99.71%	98.59%	98.59%	97.53%	99.49%	100%	95.17%	96.80%	99.60%	100%	93.80%

法库模块中的大部分模型可对服务器即将遭遇的洪泛攻击进行预测。

在洪泛攻击场景的预测数据集中, MC-LSTM模型取得了较好的效果。算法库模块中的模型在被动监测预测中的 $F1$ 值、准确率、精确率、召回率的中位数(最大值)分别为 95.04% (97.53%)、98.98% (99.49%)、98.53% (100%)、91.78% (95.17%), 在主动探测预测中的 $F1$ 值、准确率、精确率、召回率中位数(平均值)分别为 93.88% (96.8%)、99.25% (99.6%)、100% (100%)、88.46% (93.80%)。说明算法库模块中的大部分模型能够满足洪泛攻击场景下的预测精度要求, 可对服务器遭遇的洪泛攻击进行预测。

在洪泛攻击场景的任务中, MC-LSTM、FC-GRU、TCN-LSTM 3 类时间序列模型在各评价指标上均取得较好效果。DNS 洪泛攻击的突发性、多维关联性、阶段复杂性与模型动态建模、多尺度提取、长期依赖捕捉能力高度匹配。时间序列模型能够精准识别瞬时流量突增, 区分攻击阶段与正常波动。因此, 在需要实时检测高爆发流量的 DNS 洪泛攻击场景中, 时间序列模型(如 TCN-LSTM、MC-LSTM)成为最优选择。

通过 DNS 洪泛攻击场景的实验, 对比分析 15 种算法的性能, 包括传统机器学习算法和深度学习算法(尤其是面向 DNS 不间断服务特性的

时间序列检测算法)。实验结果验证各算法在 DNS 服务器遭遇洪泛攻击及相关异常场景中的适用性, 为 DNS 系统的安全态势感知与防护提供多样化的模型选择依据。另外, 传统方法基线需要根据攻击流量, 人工增加规则, 灵活性不足, 面对新的攻击表现不佳。

3.4 训练与测试效率

各算法测试耗时如图 8 所示, 由低到高排序为 DT、LR、DNN、RNN、CNN、KNN、GRU、LSTM、SVM、FC-GRU、RF、Adaboost、TCN、TCN-LSTM、MC-LSTM。其中, 机器学习算法 LR 和时间序列异常检测算法 FC-GRU 在耗时较短的同时, 能取得较优的性能。

各算法训练耗时如图 9 所示, 由低到高排序为 DT、LR、SVM、KNN、RF、Adaboost、DNN、CNN、FC-GRU、GRU、RNN、LSTM、MC-LSTM、TCN、TCN-LSTM。其中, 时间序列异常检测算法 FC-GRU 在具有较优性能的基础上, 有更快的训练效率。

4 结束语

后续研究将聚焦时间序列异常检测模型在高负载 DNS 环境的应用, 探索模型轻量化与边缘计算部署以提升实时性, 并探索新深度学习架构以提高准确性。研究其与传统防御机制的融合,

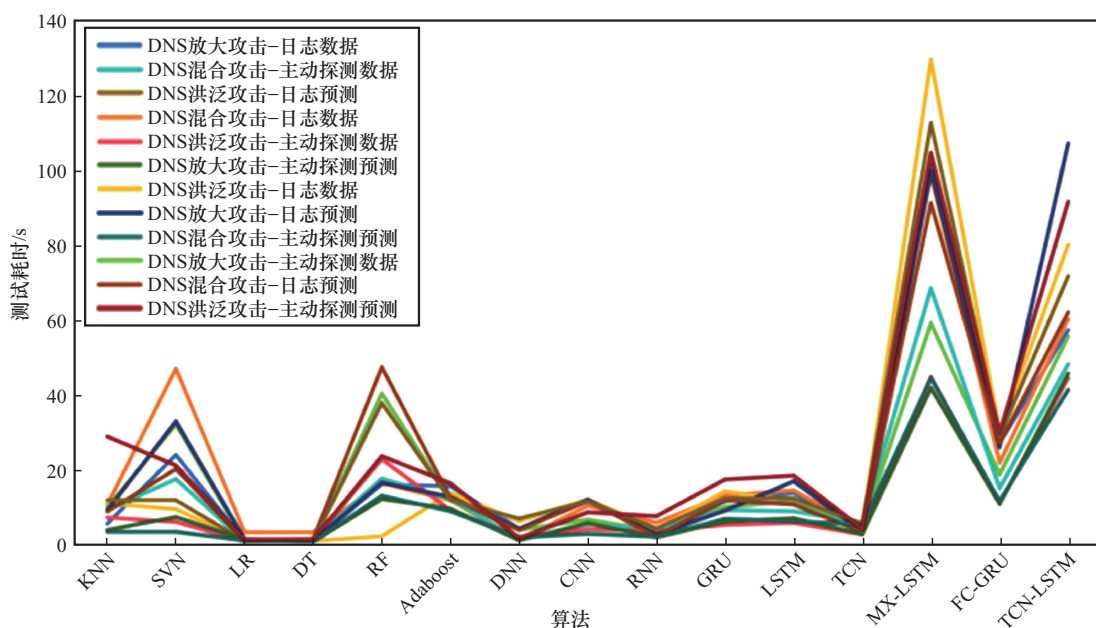


图8 各算法测试耗时

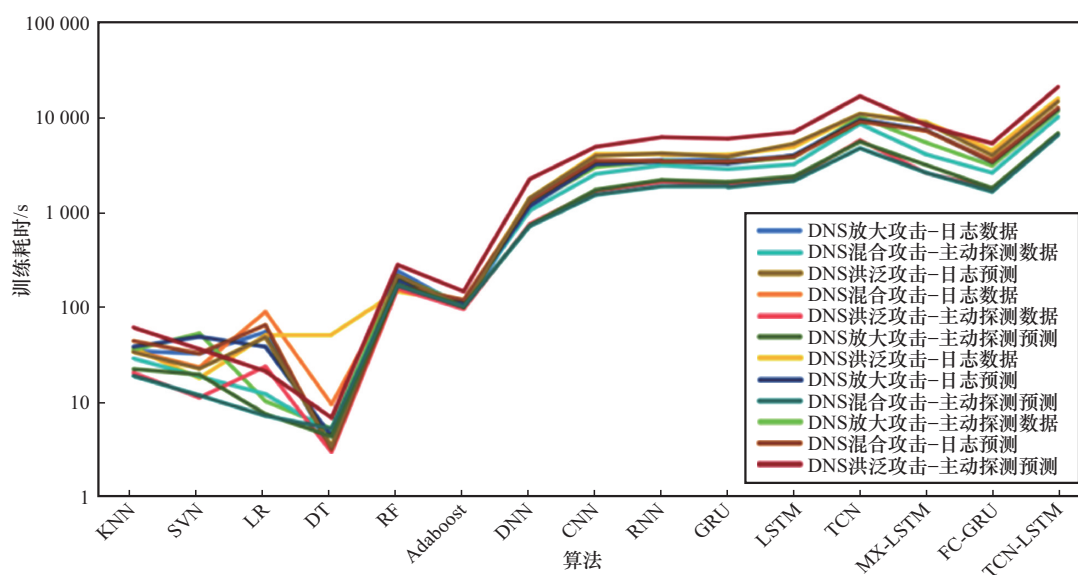


图9 各算法训练耗时

如AI-规则引擎新架构,并构建检测-响应端到端系统以实现自动化威胁处置与威胁情报共享,推动DNS安全从理论检测向动态免疫演进。同时拓展更多异常场景,如缓存投毒检测、DDoS攻击后服务器崩溃时间预测等。

参考文献:

- [1] ALIEYAN K, KADHUM M M, ANBAR M, et al. An overview of DDoS attacks based on DNS[C]//Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC). Piscataway: IEEE Press, 2016: 276-280.
- [2] BUSHART J, ROSSOW C. DNS unchained: amplified application-layer DoS attacks against DNS authoritatives[C]//Proceedings of Research in Attacks, Intrusions, and Defenses (RAID 2018). Cham: Springer, 2018: 139-160.
- [3] ALHARBI F, CHANG J, ZHOU Y C, et al. Collaborative client-side DNS cache poisoning attack[C]//Proceedings of the IEEE Infocom 2019-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2019: 1153-1161.
- [4] MAN K Y, QIAN Z Y, WANG Z J, et al. DNS cache poisoning attack reloaded: revolutions with side channels[C]//Proceedings of the 2020 ACM Sigsac Conference on Computer and Communications Security. New York: ACM, 2020: 1337-1350.
- [5] 胡杨. 基于无证书签名的抗DNS中间人攻击方案研究[D]. 福州: 福建师范大学, 2022.
- [6] ANAGNOSTOPOULOS M, KAMBOURAKIS G, KOPANOS P, et al. DNS amplification attack revisited[J]. Computers & Security, 2013, 39: 475-485.
- [7] DNS amplification attacks observer[EB]. 2025.
- [8] 胡蓓蓓. 异常DNS行为检测[D]. 武汉: 武汉邮电科学研究院, 2012.
- [9] HU B B. Detection of abnormal DNS behavior[D]. Wuhan: Wuhan Research Institute of Posts and Telecommunications, 2012.
- [9] FICHERA S, GALLUCCIO L, GRANCAGNOLO S C, et al. OPERETTA: an OPENflow-based REMedy to mitigate TCP synflood attacks against web servers[J]. Computer Networks, 2015, 92: 89-100.
- [10] LIU D P, ZHAO Y J, XU H W, et al. Opprentice: towards practical and automatic anomaly detection through machine learning[C]//Proceedings of the 2015 Internet Measurement Conference. New York: ACM, 2015: 211-224.
- [11] HASAN M, ISLAM M M, ZARIF M I I, et al. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches[J]. Internet of Things, 2019, 7: 100059.
- [12] KIM T, SUH S C, KIM H, et al. An encoding technique for CNN-based network anomaly detection[C]//Proceedings of the 2018 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2018: 2960-2965.
- [13] MUNIR M, SIDDIQUI S A, DENGELA, et al. DeepAnT: a deep learning approach for unsupervised anomaly detection in time series[J]. IEEE Access, 2018, 7: 1991-2005.
- [14] 江友华, 叶梦豆, 赵乐, 等. 基于seq2seq和SVM双层融合的非侵入式用户异常行为检测[J]. 计算机应用与软件, 2024, 41(9): 97-105.
- [14] JIANG Y H, YE M D, ZHAO L, et al. Non-intrusive abnormal user behavior detection based on double-layer fusion of seq2seq and SVM[J]. Computer Applications and Software, 2024, 41(9): 97-105.
- [15] GEIGER A, LIU D Y, ALNEGHEIMISH S, et al. TadGAN: time series anomaly detection using generative adversarial networks[C]//Proceedings of the 2020 IEEE International Conference on Big Data. Piscataway: IEEE Press, 2020: 33-43.
- [16] LI C, CHEN J, ZHANG Z X, et al. DNS root server resolution anomaly detection[J]. Computers & Security, 2024, 144: 103946.

- [17] HU A L, GONG L Y, XIE J L, et al. A large-scale study of abnormal recursive DNS[C]//Proceedings of Network and Parallel Computing. Singapore: Springer, 2025: 351-362.
- [18] 向思羽, 刘才铭. 结合混合特征选择和Transformer的网络数据流异常检测[J]. 电子科技大学学报, 2025, 54(3): 442-454.
- XIANG S Y, LIU C M. Network data anomaly detection combined with hybrid feature selection and Transformer[J]. Journal of University of Electronic Science and Technology of China, 2025, 54(3): 442-454.
- [19] LIU C, ALBITZ P. DNS and Bind[M]. O'Reilly Media Inc, 2006.
- [20] AITCHISON R. DNS diagnostics and tools[M]. Berkeley, CA: Apress, 2011.
- [21] DNS-iptables-rules[EB]. 2025.
- [22] YING S, WANG B M, WANG L, et al. An improved KNN-based efficient log anomaly detection method with automatically labeled samples[J]. ACM Transactions on Knowledge Discovery from Data, 2021, 15(3): 1-22.
- [23] HOSSEINZADEH M, RAHMANI A M, VO B, et al. Improving security using SVM-based anomaly detection: issues and challenges[J]. Soft Computing, 2021, 25(4): 3195-3223.
- [24] SALEM O, GUERASSIMOV A, MEHAOUA A, et al. Anomaly detection in medical wireless sensor networks using SVM and linear regression models[J]. International Journal of E-Health and Medical Communications, 2014, 5(1): 20-45.
- [25] MUNIYANDI A P, RAJESWARI R, RAJARAM R. Network anomaly detection by cascading K-means clustering and C4.5 decision tree algorithm[J]. Procedia Engineering, 2012, 30: 174-182.
- [26] PRIMARTHA R, TAMA B A. Anomaly detection using random forest: a performance revisited[C]//Proceedings of the 2017 International Conference on Data and Software Engineering (ICoDSE). Piscataway: IEEE Press, 2017: 1-6.
- [27] QU Z J, LIU H X, WANG Z X, et al. A combined genetic optimization with AdaBoost ensemble model for anomaly detection in buildings electricity consumption[J]. Energy and Buildings, 2021, 248: 111193.
- [28] BENGIO Y. Learning deep architectures for AI[EB]. 2009.
- [29] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278-2324.
- [30] ELMAN J L. Finding structure in time[J]. Cognitive Science, 1990, 14(2): 179-211.
- [31] DEY R, SALEM F M. Gate-variants of gated recurrent unit (GRU) neural networks[C]//Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). Piscataway: IEEE Press, 2017: 1597-1600.
- [32] GRAVES A. Long short-term memory[M]. Supervised Sequence Labelling with Recurrent Neural Networks. Berlin: Springer, 2012.

- [33] HEWAGE P, BEHERA A, TROVATI M, et al. Temporal convolutional neural (TCN) network for an effective weather forecasting using time-series data from the local weather station[J]. Soft Computing, 2020, 24(21): 16453-16482.

[作者简介]



侯榕浩 (2000-), 男, 广东梅州人, 暨南大学硕士生, 主要研究方向为恶意软件检测、深度学习。



贺明 (1985-), 男, 北京人, 中国互联网络信息中心工程师, 主要研究方向为域名安全技术。



孔凯传 (1992-), 男, 广西柳州人, 暨南大学博士生, 主要研究方向为内部威胁检测、大型语言模型与异常检测。



陈勇 (1977-), 男, 湖南涟源人, 中国互联网络信息中心高级工程师, 主要研究方向为DNS安全。



左鹏 (1985-), 男, 安徽青阳人, 中国互联网络信息中心高级工程师, 主要研究方向为网络安全、互联网基础资源关键技术。