计算机与安全 116 (2022) 102675

ScienceDirect提供的目录列表

计算机与安全

期刊主页： www.elsevier.com/locate/cose

基于异常的网络入侵检测方法和数据集的系统文献综述

甄央嘎,刘晓东 , 童丽a, , 地哇 , 晋江万佳, 赵云伟_ , 韩寒布

[A] 北京工业大学信息技术学院,北京,中国
[b] 中国北京 CNCERT/CC

文章 信息

文章历史：
2021 年 9 月 27 日收到
2021 年 11 月 28 日修订
2022 年 2 月 27 日接受
2022 年 3 月 1 日在线发售

关键词：
入侵检测
系统的文献回顾
机器学习
数据集

抽象的

随着网络技术的快速发展,攻击变得越来越复杂和具有威胁性。
网络入侵检测作为应对网络威胁的有效手段已被广泛接受。已经提出了许多方法,探索不同的技术并针对不同类型的流量。基于异常的网络入侵检测是入侵检测的一个重要研究和发展方向。尽管对基于异常的网络入侵检测技术进行了广泛的调查,但缺乏对最新技术和数据集的系统文献综述。我们按照系统文献综述的方法,对 119 篇关于基于异常的入侵检测的高被引论文进行了调查和研究。我们的研究严格而全面地调查了该领域的技术前景,以促进该领域的后续研究。具体来说,我们从以下几个角度进行调查:应用领域、数据预处理和攻击检测技术、评估指标、合作者关系和数据集。根据研究结果,我们分别从各个角度确定了未解决的研究挑战和未研究的研究主题。

最后,我们提出了几个有前途的高影响未来研究方向。

一、简介

计算机和网络技术在我们的日常生活中发挥着越来越重要的作用,但近年来严重的网络攻击在一定程度上抵消了它们的好处。 2020 年 NTSC（美国国家技术安全联盟)安全报告指出,重大网络安全问题每个月都在加剧。1 2019 年,约有 6.2 亿个账户信息被黑客泄露并在暗网上出售。 COVID-19 大流行加剧了这种威胁情况,因为许多人不得不在家工作,导致网络流量显着增加。根据 2020 年 CIRA（加拿大互联网注册局)网络安全调查,由于 COVID-19.2,三分之二的 IT 工作者被要求在家工作。入侵检测系统 (IDS) 是一种有效的安全机制,可以监控网络流量并防止恶意要求。入侵检测研究发展迅速

机器学习的发展。传统的机器学习技术已经广泛应用于入侵检测,如决策树（DT） (Safavian and Landgrebe,1991)、随机森林（RF） (Zhang et al.,2008)、支持向量机（SVM）) (Hsu et al., 2003)。并且,随着深度学习的发展,卷积神经网络 (CNN) (Vinayakumar et al., 2017)、递归神经网络 (RNN) (Yin et al., 2017)和长短期记忆 (LSTM) (Roy et al., 2017)在入侵检测中越来越受欢迎。这些技术基于不同的原理,如何有效地利用它们的优势来解决特定领域的入侵检测任务仍然是一个悬而未决的研究问题。此外,由于数据的高维性和复杂性,一种常见的解决方案是使用数据预处理技术,这可能有助于降低维度,从而使研究人员能够处理这些高维空间。预处理方法会影响检测性能,在设计入侵检测方法时应仔细考虑。

鉴于上述研究问题,系统和全面的文献综述可以为社区的发展做出贡献。现有的 IDS 可以根据检测方法分为两类:基于异常的检测和基于误用的检测或签名检测

*通讯作者。
邮箱： litong@bjut.edu.cn （T.李）。 https://
[1] www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf https://
[2] www.cira.ca/cybersecurity-report-2020

https://doi.org/10.1016/j.cose.2022.102675

（Axelsson,2000 年;Ghorbani 等人,2009 年）。基于异常的网络入侵检测是入侵检测的一个重要研究和发展方向。我们按照系统文献综述 (SLR) 的方法对 119 篇关于基于异常的网络入侵检测的高引用论文进行了调查。我们从多个角度进行分析。首先,我们分析研究进展并确定特定应用场景中的潜在瓶颈,例如物联网（IoT)和工业控制网络。其次,我们研究了数据清洗、特征选择和特征转换等预处理技术,这些技术可以为数据准备提供建议。第三,我们讨论了入侵检测技术,并按技术类别分析了它们的原理和相关应用。第四,我们研究评估方法,包括指标和数据集,这可以帮助我们标准化它们。第五,为了研究社区的现状,我们计算贡献者并绘制协作网络。

最后,我们对网络安全数据集进行了系统调查,以更好地理解它们并评估它们的适用性。

总之,本文的贡献如下:

- 我们率先使用SLR 方法对网络安全入侵检测领域的119 篇高被引论文进行了调查研究,系统地从14,942 篇候选论文中筛选出这些论文。
- 我们从粗粒度和细粒度的角度对入侵检测领域进行了全面的技术概述。我们提供了 52 个网络安全数据集的全面概述,并根据它们的属性对其进行了标记。 · 方法分析揭示了未来的研究方向

系统。

本文的其余部分安排如下。
第 2 节总结了与入侵检测系统和数据集相关的现有文献综述工作,第 3 节介绍了我们的入侵检测系统方法的文献综述。

我们的研究结果在第4节中介绍。第 5 节总结本文并讨论未来的研究方向。

二、相关工作

大量文献涵盖了入侵检测的各个方面。在本节中,我们介绍现有的相关工作并将它们与我们的研究进行比较。

2.1.入侵检测方法综述

大多数相关研究都集中在入侵检测方法上。 Bhuyan 等人。 (2013)简要描述和比较了大量的网络异常检测方法和系统。艾哈迈德等人。 (2016)分析了异常检测方法和机器学习/数据挖掘 (ML/DM) 算法的复杂性。 Milenkoski 等人。 (2015)通过分析现有的标准评估参数（包括工作负载和指标)来评估入侵检测系统的常见做法。 Buczak 和 Guven (2015)讨论了用于网络分析以支持入侵检测的机器学习和数据挖掘方法。霍多等人。 (2017)提出了浅层和深层网络入侵检测系统的分类,调查了机器学习技术在检测异常方面的性能,并讨论了误报率和真报警率。 Wang 和 Jones (2017)回顾了数据挖掘、机器学习、深度学习和大数据在入侵检测中的应用。哈克等人。 (2015)对机器学习技术在入侵检测中的应用进行了广泛的研究。米什拉等。 (2018)讨论了机器学习方法在入侵检测中的应用,并为每种攻击提供了攻击分类和攻击特征映射。

Nisioti 等人。 (2018)全面概述了无监督和混合入侵检测方法,还介绍并强调了特征工程技术在入侵检测中的重要性。

这些研究根据技术原理对入侵检测技术进行分类,详细描述了它们的优缺点,但没有从可复现性的角度提供研究思路和方法。这削弱了它们的严格性,不利于进一步的研究。此外,此类论文在入侵检测方法的讨论上缺乏全面性。

我们对入侵检测的预处理方法、分析模型和评估方法等几个方面进行了较为充分的研究和讨论。

2.2. IDS不同领域的应用概况

Zarpelão 等人。 (2017)调查了物联网中的 IDS。在物联网设备的概述中,他们认为物联网范式具有收集阶段;传播;处理、管理和开发,并介绍了一系列可用于物联网设备的技术,重点是无线技术。 Hande 和 Mud dana (2021)概述了现有的 SDN 安全解决方案,并对基于深度学习模型和机器学习方法的各种 IDS 方法进行了比较研究。

这些研究讨论了特定目标网络下入侵检测的研究现状。与这些工作相比,我们的研究范围更广,涵盖互联网、物联网 (IoT)、软件定义网络 (SDN) 和工业控制网络 (ICN)。并且,我们还研究了来自不同领域的数据集,以供研究人员参考。

2.3.入侵检测数据集调查

环等。 (2019)确定了 34 个入侵检测数据集的 15 个特征,分为五组:一般信息、评估、记录环境、数据量和数据性质。

Thakkar 和 Lohiya (2020)调查了不同的 IDS 数据集和用于评估 IDS 模型的研究进展,重点关注 CIC-IDS-2017 和 CSE-CIC-IDS-2018 数据集。上述研究主要集中在数据集的特点和研究进展上。与这些研究相比,我们的研究还讨论了入侵检测的原理和相关方法。

此外,我们对上述相关研究进行了分类。
我们根据以下标准对这些研究进行了分类,结果见表1。

- 方法论:表明该研究是否基于SLR 方法论。 · 入侵检测技术:表明该研究是否讨论了入侵检测技术,并且可以具体到预处理方法、分析模型和评估方法。 · 多领域:表明该研究是否讨论了不同网络环境下入侵检测的研究现状

环境。
- 数据集:表明该研究是否涵盖了相关研究数据集的搜索。

如表1 所示,与其他研究相比,我们的研究遵循 SLR 方法论,全面涵盖入侵检测技术（包括预处理方法、分析模型和评估方法)和数据集,并探索多目标网络。

三、研究方法

已经提出了各种入侵检测系统。我们根据该方法制定了研究方案

表1网络
入侵检测调查的相关研究。

相关工作	年	基于单反	入侵检测方法			多领域	数据集
			预处理	模型	评估		
Bhuyan 等人。 (2013)	2014		√	√	√		√
Milenkoski 等人。 (2015)	2015				√		
哈克等人。 (2015)	2015		√	√	√		√
Buczak 和 Guven (2015)	2015			√	√		√
艾哈迈德等人。 (2016)	2016			√		√	√
霍多等人。 (2017)	2017			√			
王与琼斯 (2017)	2017			√			
Zarpelão 等人。 (2017)	2017			√	√ √		
Nisioti 等人。 (2018)	2018			√		√	
米什拉等。 (2018)	2019			√	√		√
环等。 (2019)	2019		√				
塔卡和洛希亚 (2020)	2020						
汉德与穆达那 (2021)	2021			√			√ √
我们的学习		√	√	√	√	√	√

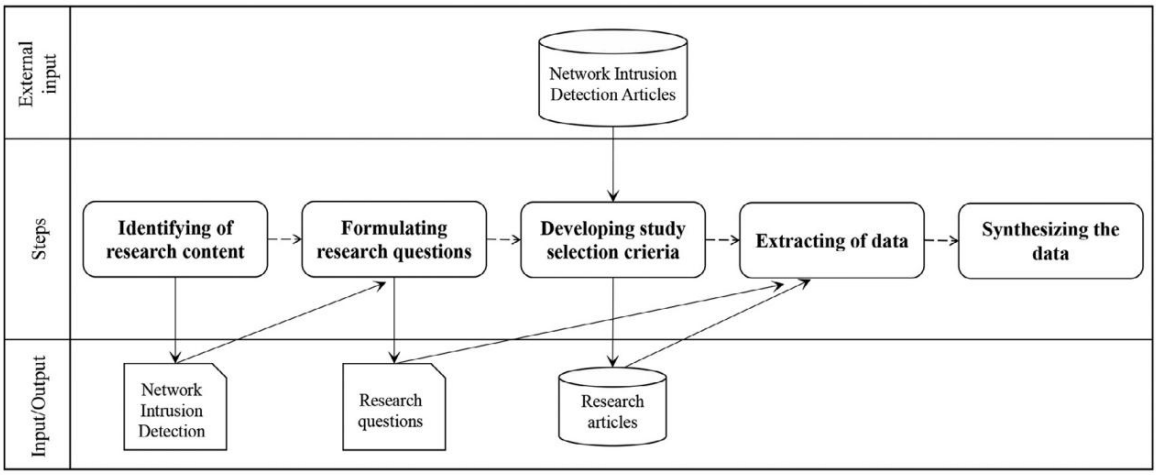

图 1. SLR 过程。

系统文献综述（SLR） （Keele et al., 2007），如图1所示。这包括研究的识别、研究问题、研究选择、数据提取和数据合成。该方法采用混合方法（定性和定量研究方法）来更直观地表示上述需求。

3.1.确定研究内容

要获得一套全面的论文，需要一种公正的搜索策略来找到与入侵检测系统相关的原始评论。搜索过程必须尽可能严格和明智，并且必须定义搜索词。我们发现一些基于异常的入侵检测文章以入侵检测命名。因此，为了全面涵盖基于异常的入侵检测文章，我们将搜索词定义为“网络入侵检测”。

在我们开始文献检索工作之前，我们评估了三个数据库，Scopus、Google Scholar 和 Web of Science。 Sco pus 涵盖了 RE（ACM、Springer、IEEE）的主要出版商，比 Web of Science 更具包容性，但不如 Google Scholar。然而，谷歌学术可能包含许多未经同行评审的论文，例如技术报告。出于这些原因，我们使用 Scopus 来执行出版物检索。

3.2.研究问题

我们提出了分析论文的想法，并阐明了具体的研究问题 (RQ)，如表2 所示，包括详细的子问题，以指导我们的研究。首先，我们总结了入侵检测技术应用的网络环境（RQ1），这有助于我们分析入侵检测技术发展和应用的特点。

其次，我们调查了入侵检测中常用的数据预处理技术（RQ2）和入侵检测数据集（RQ6），并根据调查结果对数据准备阶段提出了建议。第三，我们关注论文（RQ3）中提出的入侵检测技术，包括框架（RQ3（a））、学习方法（RQ3（b））和监督类型（RQ3（c））。此外，我们对模型（RQ3（d））的原理和应用非常感兴趣。第四，评估方法对于衡量入侵检测技术的能力很重要，因此我们想了解该领域的一般评估指标（RQ4）。最后，我们还对论文的作者 (RQ5) 感兴趣。

3.3.研究选择

以下研究原则可确保一致的评估并最大限度地减少主观性。

表 2研究
问题。

RQ1 应用领域	(a) 入侵检测技术涵盖哪些领域？ (b) 这些研究在不同领域之间的分布情况如何？ (c) 这种分布的原因是什么？ (d) 这些领域的研究因国家而异？
RQ2 数据预处理方法	(a) 网络入侵检测中常用的数据预处理技术有哪些？ (b) 预处理技术是如何实现的，其技术特点是什么？ (c) 它们在入侵检测中的应用分布情况如何？
RQ3 检测技术	(a) 哪些模型应用于入侵检测技术？ (b) 机器学习和深度学习如何应用于入侵检测？ (c) 监管类型的分布情况如何？ (d) 不同的入侵检测技术的原理和特点是什么？ (a) 如何评估入侵检测技术的性能？ (b) 在我们的研究文章中，这些评估方法是如何应用的？
RQ4 评估指标	(a) 谁是文章的主要贡献者？ (b) 合著者网络是什么样的？
RQ5 作者	(a) 可用的公共数据集有哪些？ (b) 哪些数据集常用于网络入侵检测？ (c) 为什么这些数据集被广泛使用？
RQ6 数据集	

表 3排除
标准及其解释。

标准		标准解释
包容	IC1	研究工作明确且专门致力于入侵检测系统。
	IC2	基于机器学习的入侵检测方法研究 未达到平均每年10次引用。
排除EC1		
	EC2	少于 6 页的论文包含的研究内容不足。
	EC3	不是基于异常的入侵检测论文。
	EC4	只是一篇评论文章。

·明确的纳入和排除标准。这些应该明确概述;参见表3。我们筛选了论文的质量、长度和类型，以获得可有效用于研究和分析的集合。 ·客观审查策略。论文应由至少两名具有该领域知识的审稿人审阅以纳入或排除。数据集的信息确定应由至少两名审查员审查其适用性。如果存在分歧，则由第三位审阅者做出最终决定。

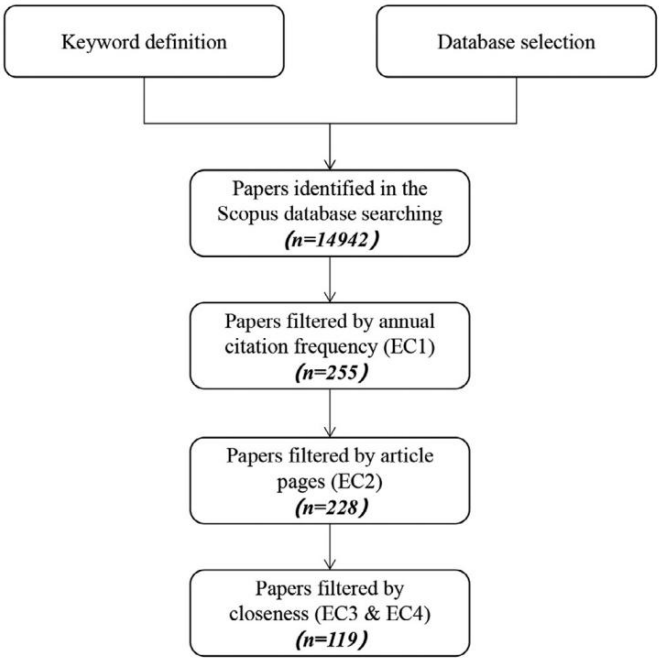

图 2.论文选择过程。

3.4.数据提取

从数据库中收集的论文使用我们定义的标准进行过滤，如图 2所示。过滤后，我们有 119 篇与入侵检测相关的论文。

每篇论文的相关信息被提取并标记以供分析。有两类标签。第一个可以从论文的内容中获得:发表年份、作者、引用次数、领域、模型、评估指标和数据集。二是基于学习方法和监督类型。

没有必要仔细阅读论文的全文。
我们阅读了标题、摘要和介绍，其中包含大部分信息，并在必要时检查了文本。

3.5.数据综合

对于学习方法和监督类型，我们通过分析所采用的模型进行了注释。我们通过对传统互联网 (Web)、IoT、工业控制网络 (ICN) 和软件定义网络 (SDN) 的研究对领域进行了分类。由于缺乏特定的应用场景，我们将论文这样分类。 IoT 是一个对象网络，其中嵌入了传感器、软件和其他技术，可通过 Internet 与其他设备和系统连接并交换数据。十种物联网技术中的大部分都与“智能家居”概念相关。 ICN 是使用以太网标准连接的数字控制系统网络。工业网络在现场设备、数字控制器、各种软件套件和外部系统之间实施通信协议。 SDN 通过编程增强网络控制。

这种功能组合可以带来增强配置、改进性能和新架构的好处。

还需要标记数据集。出于隐私原因，商业产品中用于网络数据包分析的数据集并不容易获得。 DARPA、KDD 和 UNSW-NB15 等公开可用的数据集被广泛用作基准。我们定义了标签，包括“年份”，“真实性”，“计数”，“标签”，

表 4入侵
检测方法领域的论文数量。

领域	数字
互联网	88
物联网 (IoT)	20
工业控制网络（ICN）	9 2
软件定义网络 (SDN)	

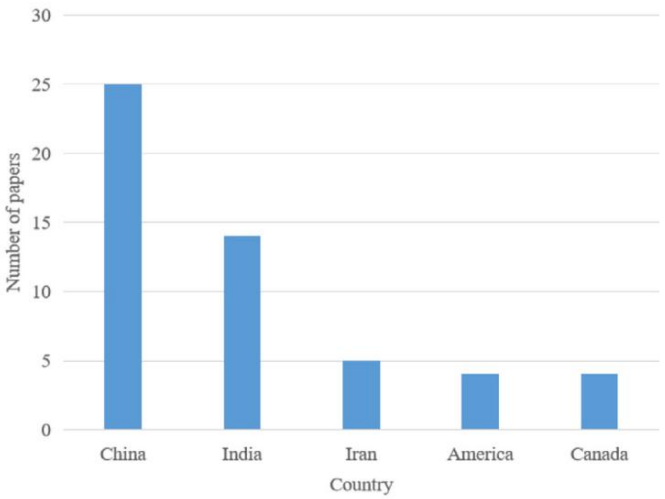

图 3.发表论文最多的五个国家。

“标签数量”反映数据集的可用性、新颖性、真实性和数据量。

4. 入侵检测文献综述分析

在本节中,我们将介绍并分析我们的发现。我们从方法应用领域、数据预处理方法、检测技术、评估指标、数据集和作者等多个角度对网络入侵检测领域进行了深入分析并提出了我们的建议。

4.1.应用领域

从应用领域来看,119篇文章可归类为互联网、物联网、ICN和SDN （RQ1(a)）。值得注意的是,我们将所有没有指定特定应用领域的文章都归类为 Internet。我们在表4中总结了基于不同应用领域分类的 119 篇文章的数量,回答了 RQ1(b)。超过70%的论文应用于互联网,这表明传统网络的安全是一个重要的研究课题。这种分布一方面是由于传统网络领域的入侵检测研究相对成熟,许多论文致力于对现有方法的改进或细化（RQ1（c））。另一方面,该领域使用的公共数据集较多,如KDD99、UNSW-NB15等,便于研究人员进行分析和实验。 ICN和SDN领域的研究文章较少,分别只有9篇和2篇。通过我们的研究,我们发现ICN领域的文章由于工业网络数据的保密性而没有公开他们的数据集,这也限制了他们在安全研究方面的发展。缺乏数据集也是限制SDN领域研究的关键因素。研究人员在进行安全研究之前,往往需要搭建SDN网络环境来模拟数据。

不同的国家或地区在不同的应用领域也呈现出不同的趋势。从图3可以看出,中国和印度在发表的文章数量上处于明显领先地位。

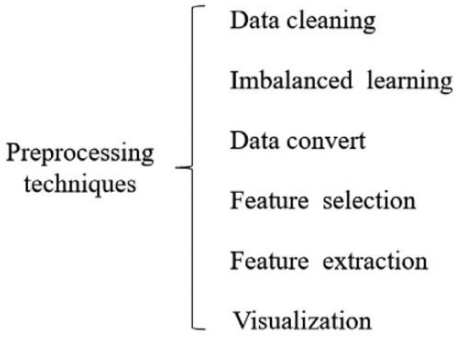

图 4.入侵检测中常用的数据预处理技术。

网络入侵检测领域（RQ1（d））。这表明当前中印两个发展中大国对网络安全的重视程度和重视程度很高。随着物联网技术的快速发展,物联网安全也成为近年来的研究热点,近三年发表的研究文章占一半。与传统网络环境一样,中国在物联网领域的文章发表数量领先,占总数的1/5。基于5G技术的快速发展和物联网的赋能,未来物联网将处于持续发展的状态,安全问题及相关研究也将成为安全领域的研究热点。

4.2.数据预处理方法

数据的表示和质量在任何数据分析过程中都是最重要的（Pyle,1999）。原始数据通常包含会影响训练和分析的噪声和不可靠数据。此外,用于入侵检测的数据集具有高维度的特点,这使得在训练过程中更难发现知识。构建高性能检测器需要高效的预处理。图4总结了入侵检测中常用的数据预处理方法,包括数据清洗、不平衡学习、数据变换、特征选择、特征提取和可视化（RQ2(a)）。

上述方法从不同的角度对数据进行预处理,使分析模型能够更好地从数据中学习到有用的信息。为了研究不同方法的技术特点,我们总结了它们的实现原理和应用来回答RQ2(b)。 a) 数据清理数据清理纠正损坏或不准确的记录。质量标准

teria 可能包括以下内容。

·有效性。数据可能必须是某种类型,例如布尔值或数字。 ·准确性。数据必须符合情况。例如,由于记录过程可能存在异常值。通过数据清洗很难保证准确性,因为需要真实的数据源进行验证。

·完整性。一些数据可能有未知值或缺失值。完整性问题通常通过默认值、设置零或删除来解决。

·均匀性。当数据集中存在冲突时,就会出现不一致。例如,两个接收器之间的源 IP 可能不同。解决此类问题需要确定哪个数据最可靠。

基于均值、标准差或聚类算法的数据分析可以揭示错误,其值有时可以设置为均值或其他统计度量。

b) 不平衡学习一个样本中正例

和负例的比例不同,会导致学习过程偏向于较高比例。例如,在具有 95% 正例和 5% 负例的数据集的极端情况下,该模型将没有实际意义。由于攻击往往是稀疏的,因此入侵检测中的数据集通常是不平衡的。以下方法可能会提高性能。

·抽样方法。平衡的数据集通常提供更好的整体分类性能（Estabrooks et al., 2004; Weiss and Provost, 2001），获得相同比例的正例和负例是最常见的不平衡学习方法。最简单的方法,对多数类进行欠采样,显然会导致信息丢失。

刘等人。 (2008)引入了 EasyEnsemble 和 BalanceCas cade 算法,将多数类的子集与少数类相结合,并对分类器执行集成学习。 NearMiss 使用 KNN 分类器选择与少数类平均距离最小的主要类（Mani 和 Zhang,2003）。少数样本的过采样通常通过合成采样来完成。合成少数过采样技术 (SMOTE) 根据少数示例之间的特征空间相似性来合成数据(Chawla et al., 2002)。已经提出修改和扩展的采样算法（Fernández 等人,2018 年)来解决 SMOTE 中的过度泛化问题（Wang 和 Japkowicz,2004 年）。自适应集成采样方法（ADASYN） （He et al., 2008)根据少数样本的分布自适应地创建合成数据,解决了类之间重叠的问题。 ·成本敏感的方法。这种方法将成本视为与错误分类相关,并在对数据进行错误分类时使用不同的成本矩阵来描述它们(Ting, 2002)。它已被证明是抽样方法的可行替代方法（McCarthy 等人,2005 年）。 ·其他方法。许多算法从其他角度获得了良好的性能。基于内核方法和主动学习,Ertekin 等人。提出了一种基于 SVM 的主动学习方法(Ertekin et al., 2007) ,该方法将主动学习的每次迭代中的查询过程限制在数据池而不是整个数据集。 SVM 在这个过程中得到训练,从超平面中提取出信息量最大的实例,形成新的训练集。一类学习主要或仅使用单类样本进行识别,将其与传统的基于区分的归纳区分开来,在极度不平衡的数据（特别是高特征空间维度)下具有良好的结果（Raskutti 和 Kowal czyk,2004）。

c) 数据转换训练数据在输

入模型之前必须经常进行转换和映射以满足要求,并提高检测速度和准确性。这会影响 IDS 数据集中的两种类型的数据。

·非数字数据。以UNSW-NB15数据集为例,标称形式的特征包括传输协议类型、状态、服务类型和攻击类型,以字符串形式存储,这是大多数机器学习算法不支持的。最直接的方法是将特征下的值编号并映射,但这会导致错误。例如,在均方误差的计算中,

$$\text{均方误差} = \frac{1}{m}\sum_{i=1}^{m} (y_i - \hat{y}_i)^2, \quad (1)$$

将标记为 0 的类错误分类为标记为 9 的类的 MSE 将是错误分类为 1 的类的 81 倍,这是不合理的。单热编码是处理这种情况的常用方法。该算法使用 n 位状态寄存器来编码 n 个状态。当给定状态有效时,只有一个相应的寄存器位有效。

·数字数据。值的范围因功能而异。深度学习框架通过引入偏差来避免其对模型准确性的影响,但当两个特征的取值范围相差太大时,模型学习所花费的时间仍可能受到影响。例如,在使用梯度下降的 ML 优化中， {XT X}的特征值（即特征的尺度)决定了收敛到全局或局部最小值的速度。因此,特征的取值范围通常在训练前通过数据缩放统一,例如通过最小-最大归一化。

特征的每个值都映射到 0 和 1 之间， $x = \frac{x - \min(x)}{\max(x) - \min(x)}$. (2)

但是,此方法无法处理异常值。例如,对于 0 到 1 之间的九个值和一个等于 100 的离群值,九个较小的值将映射到 0 到 0.01 之间的值。这可以通过 z-score 标准化来避免,

$$x = \frac{x - \mu}{\sigma}, \quad (3)$$

其中μ和σ分别是特征的均值和标准差。这可以在保持特征分布的同时将值缩放到接近 0,但特征可能不在完全相同的比例上。

d) 特征选择特征选择是选

择原始数据集的一个子集作为模型输入。这可以避免维度灾难并增强泛化能力(Bermingham et al., 2015)。进行特征选择要求数据包含冗余或不相关的特征,以避免过多的信息丢失。特征选择可以通过多种方式完成。

·手动选择。是否删除特征是手动确定的。参见,例如， Zhang 等人。 (2018)。 ·详尽搜索。测试每个可能的特征子集以找到错误率最低的子集可能需要大量计算（Guyon 和 Elisseeff,2003 年）。 ·嵌入式方法。特征选择是在模型构建期间执行的。 Bolasso算法（Bach, 2008)通过构建线性模型,结合岭回归的L1惩罚和L2惩罚,将很多回归系数降为零。 FeaLect (Zare et al., 2013)基于回归系数的组合分析对特征进行评分和选择。

·包装方法。使用每个子集训练预测模型并在保留集上进行测试。从模型测试的错误率中获得子集的分数。这是计算密集型的,通常只用于寻找最好的特征子集。

·过滤方法。互信息(Guyon and Elisseeff, 2003)、 Pearson 相关系数和显着性得分（例如类间或类内距离)(Yang and Pedersen, 1997) 等方法可用于对特征子集进行评分,它可以对特征进行排序但不会产生最佳子集。

e) 特征提取与特征选择

(Sarangi et al., 2020) 不同,特征提取,即创建新特征以促进学习,被认为是构建模型的关键因素。这可以通过以下算法来执行。

·主成分分析(PCA)。 PCA 是最常用的线性降维方法之一,它根据主成分改变数据的基础,主成分本质上是数据协方差矩阵的特征向量。

德拉霍兹等人。 (2015),使用 PCA 进行特征提取,而Xiao 等人。 (2019)将 PCA 与自动编码器相结合,压缩高维特征以输入到 CNN。变体包括概率 PCA (PPCA),它利用概率分布； kernel PCA,在使用 PCA 降维之前,使用核函数将低维空间映射到高维空间;和独立成分分析（ICA）,它不需要隐藏变量服从高斯分布。

·线性判别分析(LDA)。作为一种经典的降维方法,LDA 寻找特征的线性组合来描述多类对象。作为一种监督学习算法,它在低维空间中搜索最能区分数据类别的向量（Martinez 和 Kak,2001）,在低维中投影数据以最小化类内距离并最大化类间距离。

苏巴等人。 (2015)使用具有逻辑回归的 LDA 建立了入侵检测模型,在计算效率方面具有显着优势。

·自动编码器。该方法使用隐藏层进行无监督学习,通过非线性变换映射高维特征(Goodfellow et al., 2016)以生成尽可能接近原始输入的表示。正则化自动编码器（稀疏、去噪和收缩)通常用于学习表示（An 和 Cho,2015）。

张等。 (2018)使用去噪自动编码器 (DAE) 在 UNSW NB15 数据集上实现了 98.80% 的准确率。

f) Visualization数据

可视化是数据的图形表示,用于更好地帮助研究人员理解数据分布等特征。在入侵检测中,可视化通过提炼数据属性和特征,帮助我们进一步了解攻击的特征。并且,由于机器学习算法的不可理解性,我们往往无法分析分类器误分类的原因。使用可视化技术,我们可以更好地识别攻击行为以进行更深入的分析。数据降维通过提取原始特征的子集或将原始数据转换到较低维空间来工作。在入侵检测中,经常使用t-SNE和PCA来实现网络流量可视化。

· t 分布随机邻域嵌入(t-SNE)。 t SNE (Van Der Maaten, 2014)技术是一种降维技术,用于通过在二维或三维的低维空间中表示高维数据集来可视化它们。它基于分布式随机邻域嵌入（SNE） （Hinton and Roweis, 2002)的改进,解决了可视化后SNE样本分布拥挤、边界不明显的缺点。可视化可以帮助研究人员了解数据分布、样本重叠等信息。例如,图5显示了可视化后正常样本（绿点)和攻击样本（灰点)的分布。可视化方法已实际应用于入侵检测。 Hamid 和 Sugumaran（2020)在他们的研究中基于 t-SNE 并结合支持向量机进行数据降维和可视化进行分类。

结果表明,几乎所有攻击组的检测率都有所提高。姚等。 (2020)提出了一种新的基于 t-SNE 和分层神经网络的无监督入侵检测算法。在这项研究中,作者使用了两个

表 5特征
工程方法统计。

方法	数数
群体智能算法 12	
手动定义的规则	8
主成分分析	6
深度学习	5
聚类	4
支持向量机	2
决策树	1

维度可视化技术,以直观地确定降维效果。

·主成分分析(PCA)。上一节我们讲到,PCA常用于高维数据的降维,可以用来提取数据的主要特征。它也经常用于可视化数据。图 6显示了基于 PCA 可视化后的数据分布。绿色点是正常样本,灰色点是攻击样本。在与入侵检测相关的研究中， Ruan 等人。 (2017)基于 PCA 对 KDD99 数据集进行可视化,并提出了一种新的采样方法,可以直观地识别正常类,因为它具有内部类的紧凑性和唯一性。在 Bulavas 等人的研究Bulavas (2018) 中，作者提出了一种基于数据可视化的 PCA 方法结合决策树的入侵检测方法。实验表明,该方法在检测多种攻击方面表现出良好的性能。

与其他预处理方法相比,特征选择和特征提取是很多文章的研究重点。

在我们调查的所有论文中,有 38 篇专注于改进特征工程算法（包括特征选择、特征提取）,而其他论文则专注于改进分类算法。总的来说,可以认为目前对 IDS 的研究更侧重于提高分类算法的性能。我们认为这种趋势是由于每个数据集的格式差异太大造成的,这个问题意味着与特征相关的算法的泛化通常更差,进一步导致特征工程算法的应用效率低下。我们总结了这 38 篇文章中使用的算法,见表5。在表5 所示的结果中,可以发现群体智能算法相对更受欢迎,我们认为这又与数据集有关（RQ2（c））.鉴于 IDS 数据集通常具有太多特征,研究人员通常更关注执行特征选择。由于难以确定特征的重要性,具有一定随机性的群体智能算法成为首选。

与特征工程相比,研究人员倾向于改进基于集成学习和深度学习的分类算法,这些算法具有更高的能力,以获得更准确的分类结果。值得一提的是,深度学习本身还可以进行特征工程,这也是深度学习被广泛应用于IDS研究的原因之一。在未来的工作中,我们还建议将特征工程与可视化相结合,这将有助于我们了解数据分布等特征,从而进一步了解攻击的特征。

4.3.检测技术

我们总结了文章中使用的分类模型
表 6和7,回答RQ3(a)。入侵检测最常用的机器学习算法是SVM,一种判别式

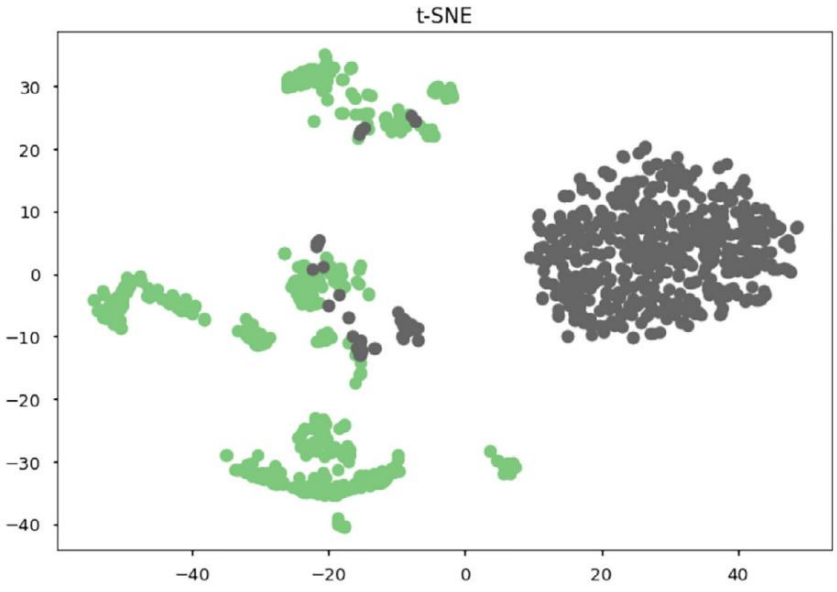

图 5.基于 t-SNE 的可视化图。

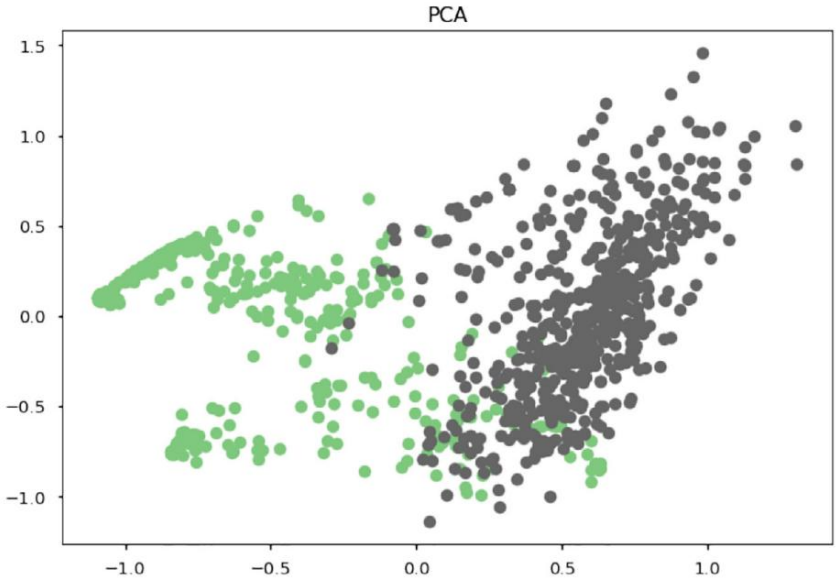

图 6.基于 PCA 的可视化图。

表 6提出的
方法中最常用的机器学习算法。

类型	方法	数数
监督学习	支持向量机 21	
	决策树 11	
	朴素贝叶斯 8	
	K-最近邻	7
	随机森林	5个
	AdaBoost	2个
	隐马尔可夫模型	
无监督学习 K-means		1
	数据库扫描	4 1

表 7提出的
方法中最常用的深度学习算法。

类型	方法	数数
监督学习	神经网络	7
	循环神经网络	7
	[illegible]	7
	长短期记忆网络	4个
	数据库编号	2个
	深度神经网络	2个
	神经网络 1	
	榆树 1	
无监督学习自动编码器 5		
	自学学习3	
	成果管理制 1	

由使用核函数将训练数据映射到高维空间以对入侵进行线性分类的分裂超平面定义的原始分类器。入侵检测中使用的数据通常具有高维性，SVM具有高生成eralization能力和表现良好。决策树由于其高效率和可解释性而被广泛使用。

深度学习正在迅速发展，并正在成为更多入侵检测方法的基础。为了回答RQ3(b)，我们绘制了

图 7.发表论文数量随时间的变化。

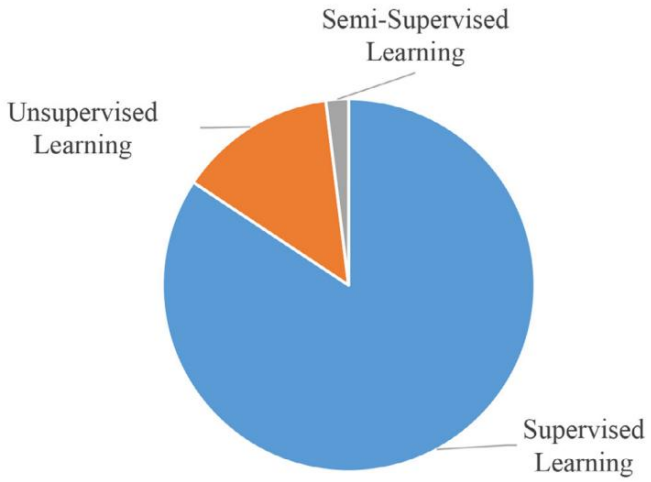

图 8.随时间变化的发表论文数量。

每年基于 ML 和 DL 的入侵检测文章数量,见图7。基于我们研究对象的特殊性,20192020 年的研究数量较往年有所下降。但是,搜索条件可能过滤掉了一些引用次数较少的优质论文。年度论文数量呈上升趋势,是因为网络攻击越来越频繁,人们对网络安全的关注度越来越高。随着 Internet 携带越来越多的信息,它已成为攻击者有利可图的目标。此外,黑客工具和技术也很容易获得。

我们可以看到,传统的机器学习方法仍然是主流技术。这些比深度学习方法更容易部署和实施,不受计算能力的限制,并且更具可解释性。不过,机器学习论文数量的变化趋势与深度学习相似。深度学习的快速发展为入侵检测的研究添砖加瓦。 SVM 和 DT 都是有监督的学习方法,在训练时都需要标签。标注对于大型数据集来说既费时又繁琐,聚类算法可能是更好的选择。 K-means和DBSCAN是常用的聚类算法,如表6所示。我们按监督类型对方法进行分类,如图8所示,从中可以看出监督学习应用最广泛（RQ3（c））.

这是因为许多公开可用的数据集已经被标记,并且研究人员更喜欢监督学习。如前面提到的,

注释费时费力。因此,unsu 监督和半监督学习也应该引起人们的兴趣。

在四个目标网络中,SVM和DT是“互联网”中使用最广泛的机器学习算法,并取得了优异的性能。无监督学习方法在“IoT”和“ICN”中比较流行。对于“SDN”,我们的工作中只包含两项研究,它们分别使用 RNN 和 RF 算法。

尽管机器学习和深度学习越来越多地用于网络入侵检测,但这些方法的有效性在对抗性环境中可能会显着降低。对抗性环境是敌对的环境

saries 通过某种方式有意识地限制或阻止准确的表现。例如,对手设计对抗性示例并将它们添加到训练集中以诱使模型产生正确的输出。 Alhajjar 等人。 (2021)使用进化计算（粒子群优化和遗传算法)和深度学习（生成对抗网络)生成对抗样本。他们的对抗样本生成技术在 11 种不同的机器学习模型和投票分类器中导致了高误分类率。为了提高入侵检测算法在对抗环境中的鲁棒性,研究人员也进行了相关研究。卡米内罗等人。 (2019)提出了一种用于入侵检测的对抗环境强化学习算法。他们在训练中加入了对抗代理策略,以增加分类器的错误预测并迫使其学习最困难的案例,最终获得更好的结果。然而,总的来说,需要更多的努力来研究对抗环境中的入侵检测算法。

为了研究不同入侵检测模型的原理和特点,我们将在下面进行介绍,并分析它们的原理和相关应用,以回答RQ3(d)。

- DT通过由决策及其结果组成的树状模型来支持决策,广泛用于分类任务（通常称为分类树）,因此IDS中有一种常见的监督学习分类方法。训练有素的 DT 对数据包的特征进行多项选择以确定其类别。最佳 DT 以最少的级别保存最多的数据(Quinlan, 1983)。已经提出了几种算法来生成最优树,例如 ID3 (Quinlan, 1986)、 C4.5 (Quinlan, 2014)和分类和回归树 (CART) (Loh, 2011)。有不同的指标来衡量 DT 性能。 ID3使用信息增益（熵）,通过选择信息增益最高的属性进行决策,但不支持特征中的缺失值和连续值,这限制了它的适用性。 C4.5 使用信息

基于 ID3 的增益比,并通过替换对叶节点没有帮助的分支来修剪树。 CART 使用 Gini impurity（一种对应于 Tsallis 熵的信息论度量)作为度量,解决了 ID3 无法处理回归任务的问题。

DT 具有直观的分类策略,可解释且易于实现,并且通常允许通过构建后剪枝进行更好的泛化,使其成为入侵检测中的常用模型。安西等人。 (2019)提出了一种三层入侵检测系统 (IDS),可根据 MAC 地址识别物联网设备,将消息分类为善意或恶意,并使用 DT 对攻击进行分类。阿贝斯等。 (2010)通过分析应用程序协议,对每个记录使用单独且不同的自适应 DT,将记录分类为良性或异常。该系统在识别DoS攻击、扫描攻击和僵尸网络方面取得了良好的效果。 Muniyandi 等人。 (2012)提出了一种异常检测方法,该方法使用 k-means 基于欧氏距离相似性形成 k 个训练实例集群,并在每个集群上使用 C4.5 构建正常和异常实例密度区域的 DT。

DT的缺点是鲁棒性弱;训练数据的微小变化可能会导致完全不同的 DT。此外,信息增益偏向于具有更多级别的属性(Deng et al., 2011),因此较大的 DT 可能需要手动修剪。

- SVM （Özgür 和 Erdem,2016 年)构造一个 N 维超平面以对数据进行最佳分类。 SVM 可以是线性的也可以是非线性的。线性SVM用于线性可分的数据,即可以被一条直线分为两类的数据集。非线性 SVM 用于非线性可分离数据。为此,我们使用了一个内核技巧,将数据点设置在更高的维度中,可以使用平面或其他函数将它们分开。

SVM 可以简化高维问题的求解。它基于小样本统计理论,具有良好的泛化能力,常用于入侵检测。简等人。 (2019)开发了一种轻量级攻击检测策略,使用基于监督机器学习的 SVM 来检测将不需要的数据注入物联网网络的尝试。它从样本中获取特征池,并将其与标签向量一起使用来训练 SVM。该方法具有良好的分类精度和检测次数。

腾等。 (2017)提出了一种基于SVM的入侵检测方法,该方法基于DT的结构构造了四个两阶段SVM。 SVM1、SVM2、SVM3、SVM4分别检测正常数据、DoS/DDoS攻击、探测攻击、R2L或U2R攻击。实验表明,该方法在检出率和召回率方面优于单一SVM的方法。

德拉霍兹等人。 (2015)提出了一种用于网络异常检测和分类的混合统计技术和自组织图 (SOM)。该方法使用 PCA 和 Fisher 判别比 (FDR) 进行特征选择和噪声去除,并使用基于概率自组织映射 (PSOM) 的特征空间建模来区分正常和恶意流量。

- 聚类将彼此比其他组中的对象更相似的对象分组。一般理解为要解决的任务而不是算法。由于无法精确描述聚类的概念（即对象之间的相似性）,因此聚类算法存在很大差异。根据对象和簇之间的匹配规则,可以将聚类视为硬聚类或软聚类。硬聚类严格地将对象分配给类。最具代表性的算法是k-means cluster ing和k-nearest neighbor (KNN),它们计算对象之间的欧氏距离来对簇进行分类。软（或模糊)聚类计算每个对象对一个聚类的渴望程度（例如,概率）。数据往往不能划分为明确分离的簇,软分类用于获得更灵活的结果。模糊聚类是一种应用广泛的软聚类算法,计算每个对象的隶属系数在每个集群中基于它们之间的距离,这证明了复杂数据的聚类。

聚类算法可以分类,例如基于连通性（例如,分层）、基于质心（k 均值、模糊 c 均值）、基于分布 (GMM)、基于密度 (DBSCAN) 或基于网格 (STING) .聚类通常实现简单,易于解释,但对异常值敏感,参数的初始值对结果的影响太大。

彭等。 (2018)提出了一种使用小批量 k 均值进行聚类和 PCA 来降低数据维数的入侵检测系统方法。实验结果和时间复杂度分析表明该方法是有效的。

卡萨斯等。 (2012)提出了 UIDS,这是一种无监督网络入侵检测系统,能够在不使用 q 签名、标记流量或训练的情况下检测未知网络攻击。

UIDS采用基于子空间聚类的无监督异常值检测方法和多种证据积累技术来识别攻击类型。

- 朴素贝叶斯 (NB)是基于贝叶斯定理 [44] 的概率分类器。所有朴素贝叶斯分类器都基于特征值独立于任何其他特征值的原则,即

$$\hat{y} = \underset{k\in\{1,\ldots,K\}}{\operatorname{argmax}}\, p(C_k) \prod_{i=1}^{n} p(x_i \mid C_k), \tag{4}$$

其中y^是数据属于每一类的条件概率， k是类数， Ck是第k类,n是特征数， p(Ck)是Ck的先验概率， p (xi | Ck)是给定类别Ck的特征xi的条件概率。必须假定从训练集中生成的特征分布（即事件模型)或非参数模型才能计算先验类别。多重分布和伯努利分布通常用于离散特征,高斯分布用于连续特征。贝叶斯分类器可以通过某些半监督训练算法 [15] 在标记和未标记的数据集上进行训练。

科克等。 (2012)提出了一种基于隐藏贝叶斯 (HNB) 模型的方法,可应用于受维度、天真 高度相关特征和高网络数据流容量影响的入侵检测问题。 HNB 是一种数据挖掘模型,它放宽了 NB 方法的条件独立性假设。实验结果表明,HNB 模型在准确率、错误率和误分类成本方面均优于传统 NB 模型。为了解决物联网中 DDoS 攻击的潜在威胁， Mehmood 等人。 (2018)提出了一种基于多代理的 IDS (NB-MAIDS) 的 NB 算法,并在整个网络中实现了多代理。

虽然NB的独立性假设在实践中经常被违反,但它仍然具有较高的准确性。另外,NB作为一种线性算法,训练效率高。这些特性导致其作为分类问题的基线得到广泛应用。

- 集成学习通过算法结合多个分类器,以在混合的多重假设空间中找到（希望)更好的假设。应该注意的是,多个分类器的组合并不能保证比最好的单个分类器更好的性能,但它可以降低选择特别差的风险。

最早和最直观的基于集成的算法之一,装袋（bootstrap aggregating）（Breiman,1996)通过随机抽取整个训练的子集来训练相同类型的分类器来获得分类器的多样性,并允许每个分类器在集合中以相同的权重投票以在单独的分类器中组合。随机森林分类器(Breiman, 2001)是一种常见的机器学习方法,它结合了 bagging 和

DT。 boosting 方法通过训练一个新的分类器来递归地构建一个集成,以强调被其先前的分类器错误分类的训练数据。基于该算法,已经提出了几种著名的机器学习算法,例如自适应提升（AdaBoost） （Freund 等人,1996）、梯度提升决策树（GBDT)和极端梯度提升（XGBoost）。

集成学习通过集成多个分类器来提高最终模型的泛化性和准确性,并且不太可能过拟合。它的训练和预测速度自然低于单个分类器,并且模型的可解释性在一些复杂的集成中很大程度上丢失了（Madeh Piryonesi 和 El-Diraby,2021）。辛格等。 (2014)开发了一种基于 RF 的 DT 模型,用于准实时对等僵尸网络检测问题。李等。 (2018)提出了一种使用软件定义技术的基于人工智能的两阶段入侵检测方法。它使用蝙蝠算法的群划分和二进制差分变体来选择典型特征,并使用 RF 通过使用加权投票机制自适应地改变样本的权重来对流进行分类。

胡等。 (2013)提出了一种在线入侵检测算法,该算法使用在线 AdaBoost 算法在每个节点处构建局部参数化检测模型。使用节点中的少量样本,结合局部参数模型,在每个节点中构建全局检测模型。实验结果表明,改进后的在线AdaBoost具有更高的检测率和更低的误报率。

- 进化算法是受生物进化启发的全局优化算法,通常是种群的试错问题。初始候选解决方案反复更新和迭代,在每一代中删除性能不佳的解决方案并引入随机变化,与自然选择和变异的概念一致。

最广泛使用的是遗传算法、遗传编程、进化算法、粒子群优化 (PSO) 和人工免疫系统,它们的主要区别在于迭代的执行方式。遗传算法和遗传编程计算种群中每个个体的适应度值,通过个体间遗传物质的交换和突变,选择适应度值高的个体作为交配池产生下一代的概率高。遗传算法把比特串看作一个个体,而遗传编程把程序看作一个个体。进化算法通常模拟自然界中的生物学习过程。例如,人工蜂群（ABC)算法模拟了蜜蜂寻找食物来源的过程。人工免疫系统通过克隆和变异与“病毒”（即待检测样本)具有高亲和力的抗体来模拟免疫系统功能,从而进行迭代。

进化计算的特点是有多种迭代方法。迭代方法通常需要为要解决的问题手动定义多个参数和评估函数。因此,该算法具有与问题无关的快速搜索能力和广泛的适用性,基于种群的原理带来并行性,提高了搜索最优解的速度。然而,进化计算的性能在很大程度上取决于评估函数和参数（通常是凭经验设置的),这会影响解决方案的效率。有些算法太容易收敛到局部最优,甚至是任意点,而其他算法则很难找到局部最优问题。虽然这可以通过更换评估函数和参数来缓解（Taherdangkoo et al., 2013),但“没有免费的午餐”定理（Wolpert and Macready, 1997)已经证明这个问题没有通用的解决方案。

Khammassi 和 Krichen (2017)提出了一种用于网络入侵检测中特征选择的 GA-LR 打包方法,使用基于遗传算法的打包方法作为搜索策略,逻辑回归作为学习算法来选择最佳特征子集。该方法有效地提高了入侵检测性能。 Hajisalem 和 Babaie (2018)提出了一种基于 ABC 和人工鱼群 (AFS) 算法的混合分类方法,使用模糊 C-均值 (FCM) 聚类和基于相关性的特征选择 (CFS) 对训练数据集进行划分并去除不相关的特征.基于选定的特征,通过 CART 技术生成 if-then 规则以区分正常和异常记录。生成的规则用于将方法训练到检测模型。在NSL-KDD和UNSW-NB15数据集上的仿真中,该方法实现了99%的检测率和0.01%的误报率。

- DNN是一种人工神经网络 (ANN),在输入层和输出层之间有多个层(Bengio, 2009)。
从狭义上讲,它是一个结构类似于多层感知器（MLP)的全连接神经网络。全连接 DNN 的下层神经元可以与所有上层神经元形成连接。 DNN 使用反向传播来执行具有非线性激活函数的监督学习任务。

Vinayakumar 等人。 (2019)为实时处理和分析超大规模数据的入侵检测框架构建了基于 DNN 的分布式深度学习模型。

许等。 (2018)提出了一种 IDS,由具有门控循环单元 (GRU)、MLP 和 softmax 模块的 RNN 组成。 DNN 理论上可以逼近任何函数（Cybenko,1989）。

- CNN是一种人工神经网络,具有基于卷积核或过滤器的共享权重结构。受生物过程的启发（Hubel 和 Wiesel,1968）， CNN 沿着输入特征滑动卷积核以提取称为特征图的平移等变响应。

CNN 及其相关架构因其在计算机视觉方面的出色性能而受到相当多的关注（He et al., 2016）。从 LeNet-5 (LeCun et al., 1998) 开始,已经提出了许多 CNN 架构,包括 AlexNet (Krizhevsky et al., 2012)和 ResNet (He et al., 2016) 。尽管 CNN 架构通常应用于 CV 问题,但它们在 IDS 中也显示出良好的结果（Dong 等人,2019 年; Vinayakumar 等人,2017 年）。李等。 (2017)提出了一种 NSL-KDD 数据的图像转换方法,其中 CNN 自动学习图形 NSL-KDD 转换的特征。

与DNN相比,CNN对局部特征的提取减少了权重的数量,以及计算复杂度,从而提高了训练和预测速度。然而,这可能会导致问题;一些训练有素的 CNN 模型会提取图像中车轮的特征,并立即将图像判断为卡车。

- RNN是一类可以暂时表现出记忆行为的人工神经网络。这种动态行为是通过节点之间的连接来实现的,以沿着时间序列形成有向图（Dupond,2019）。 RNN 的内部状态允许它处理可变长度的输入序列。

根据构建的图是否有循环,RNN 可以进一步分为有限脉冲或无限脉冲(Miljanovic, 2012)。有限脉冲网络可以展开并用严格的前馈神经网络 (FNN) 替换,而无限脉冲循环网络则不能。此外,在 RNN 中可以有额外的存储状态,从而将其改进为可以用时间延迟或反馈循环实现的网络（例如,长期和短期记忆网络）。

RNN 的提出是为了解决 DNN 难以拟合随时间变化的数据的问题。因此,RNN 在自然语言处理和动作识别等领域发挥了重要作用(Tang et al., 2018)。 RNN 越来越多地应用于 IDS,其数据主要由时间上连续的数据流组成

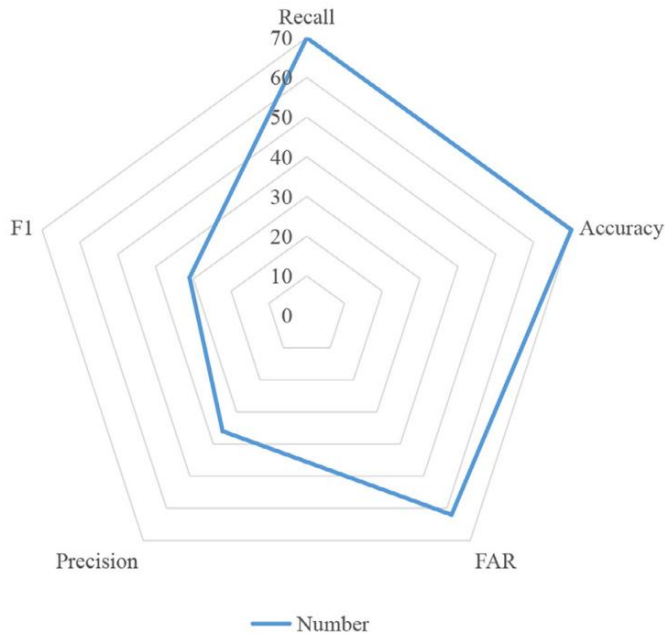

图 9.论文中使用的评估指标。

（Hochreiter 和 Schmidhuber,1997 年;Yin 等人,2017 年）。然而,由于RNNs没有对激活函数进行特殊处理,当网络层数较高时,其偏导数的连续乘积很容易导致梯度消失甚至梯度爆炸。

- LSTM通过引入额外的存储状态解决了经典 RNN 的梯度消失问题(Gers et al., 2000)。
LSTM通过使用一个门函数作为激活函数,选择性地让一部分信息通过,有效地控制了梯度消失的程度。

基于原始的 LSTM 架构， Gers 等人。 (2000)引入了遗忘门,使 LSTM 能够重置其状态,模拟记忆的遗忘过程。由于其出色的性能（Capes et al., 2017; Wu et al., 2016），它被认为是最经典的 LSTM 架构。基于此， Cho 等人。 (2014)提出了一种由重置门和更新门组成的门循环单元 GRU,它以更少的参数尽可能保持 LSTM 的性能。

LSTM 已成为最常用的 RNN 变体之一,因为它解决了传统 RNN 的梯度消失问题。

许多 IDS 研究使用 LSTM 网络(Bontemps et al., 2016; Roy et al., 2017),因为它们非常适合基于时间序列数据的分类和预测,遗忘机制更适合检测的数据流。然而,由于 RNN 的固有特性,经典的 LSTM 架构无法并行训练（Bai 等人,2018 年）,这使得基于 LSTM 的模型有时运行成本太高而无法运行。

4.4.评价指标

我们介绍了入侵检测论文中常用的评估标准。为了回答RQ4(a),图 9显示了评估指标及其使用次数。

如图 9 所示,准确度、精确度、召回率、F1 值和误报率 (FAR) 是最常用的(RQ4(b))。大多数论文都使用召回率和准确率。召回率,也称为检测率或真阳性率 (TPR),是正确分类的攻击占所有攻击的比例。召回率可以衡量分类器识别攻击的准确性。准确率是正确预测的样本数与预预测样本总数的比值

口述样本,它衡量分类器的整体识别度。 FAR 是评估入侵检测方法的关键指标。误报是误报的一种表现形式,其数量多会增加系统和人力资源的负担。

经过分类,数据可以分为四类:真阳性（TP）、假阳性（FP）、真阴性（TN)和假阴性（FN）。计算公式如下：

$$\text{精度} = \frac{TP + TN}{TP + TP + FP + FN} \quad (5)$$

$$\text{精度} = \frac{TP}{TP + FP} \quad (6)$$

$$\text{回忆} = \frac{TP}{TP + FN} \quad (7)$$

$$\text{远} = \frac{\text{计划生育}}{TN + FP} \quad (8)$$

$$F\text{－测量} = 2 \times \frac{\text{准确率} \times \text{召回率 准确率}}{+\text{召回率}} \quad (9)$$

检测时间也是入侵检测领域常用的评价指标。我们的研究中有 74 篇文章讨论了时间表现。检测时间是指用训练好的模型对样本进行分类所花费的时间。由于网络流量的复杂性,即使采用特征选择等方法进行降维,IDS研究也常常面临维数灾难的问题,最终体现为检测时间长。现有的众多入侵检测算法中的一些算法在工程实现中几乎无法实现,一个重要原因是它们的检测时间长。从应用的角度来看,入侵检测的主要目标是在资源消耗最小的情况下达到合适的检测率,这就需要一个理想的IDS模型结构和参数设置。一个模型的高检测时间通常意味着它的算法复杂度太高。回顾之前的研究,可以发现模型的性能和复杂性之间存在明显的权衡。

虽然基于深度学习的方法通常在检测能力方面比其他方法表现更好,但它们的检测时间太长,使得这些方法难以在大数据等场景中使用。虽然计算复杂度是对检测时间最直接的影响,但考虑到某些算法的计算复杂度在不同假设下难以计算或存在争议,因此大多数论文仅提供其算法在指定数据集上的训练和测试时间。由于获得每个结果所使用的平台和对数据集的预处理方法不同,因此仅从运行时间来判断算法在时间复杂度方面的优越性仍然很困难。综上所述,我们认为目前的IDS研究仍然需要一个统一的复杂度评价标准,而不仅仅是检测时间。

4.5.作者

我们通过 Scopus 检查包含的出版物的引用总数来评估入侵检测的主要贡献作者,回答RQ5(a)。如图10 所示， The (Ambusaidi et al., 2016; Tan et al., 2014; Yin et al., 2017)对该领域的贡献最大。我们发现除了前几位作者外,其他人的引用率都不是很高。这表明很少有研究人员被引用。

我们研究的文章中引用最多的三篇文章如表8 所示。文章“A Deep Learning Approach for

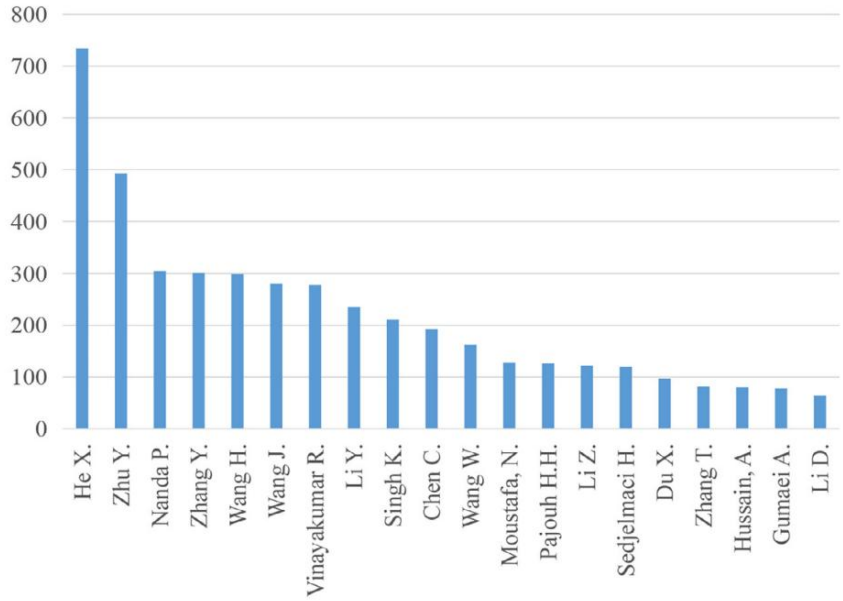

图 10. Scopus 引用总数排名靠前的作者。

表 8被引用
次数最多的三篇文章。

纸	年	引用次数 平均引用次数
一种使用递归神经网络进行入侵检测的深度学习方法 2018 430		143
网络入侵检测的深度学习方法 2017 313		78
基于模糊的入侵检测系统半监督学习方法	2017 286	71

表 9论文中
使用的数据集。

数据集	数数
KDD99	47
NSL-KDD	35
UNSW-NB15	8 6
2012年ISCX	2
京都 2006+	
僵尸网络	2个

Intrusion Detection Using Recurrent Neural Networks”发表于2018年,总引用次数超过430次,年均引用86次。在这篇文章中,作者提出了一种使用Recurrent Neural Networks进行入侵检测的深度学习方法（RNN-IDS）。此外,作者还研究了模型在二分类和多分类中的性能,以及神经元数量和不同学习率对模型性能的影响。在论文《A Deep Learning Approach to Network Intrusion Detection》中,作者也提出了一种基于深度学习的入侵检测模型。该模型基于堆叠的 NDAE 构建,并取得了优异的结果。从这两篇被高引用的文章中,我们可以看到深度学习在入侵检测领域的巨大影响和潜力。在另一篇论文“Fuzziness based semi-Supervised learning approach for intrusion detection system”中,作者提出了一种基于模糊的半监督学习方法,该方法使用未标记样本辅助监督学习算法来提高分类器的性能。与前两篇论文不同,本文以数据标注的复杂性为痛点,旨在降低数据标注过程中的人工消耗。

为了回答RQ5(b),我们绘制了作者网络,如图11所示。如图 11 所示,作者网络作品的分布是分散的。请注意,这些高亮作者的圆圈大小是根据他们的论文数量缩放的,而所有其他作者的圆圈大小是固定的且较小,以便于阅读。该图包括 82 个未连接的集群,有 451 位作者。如图 12所示,两个最大的集群均包含 32 位作者,仅占所有作者的 14%。

这表明社区中作者之间的合作水平较低。

4.6.数据集

为了回答RQ6(a),我们调查了现有的网络入侵检测数据集。如表 10 所示,我们通过调查共收集了 52 个数据集。并且,根据数据集发布者提供的信息和额外的搜索,我们提取了每个数据集的创建年份、创建方法、数据量、注释状态、标签数量和链接。从时间上看,从 DARPA 1998 年的数据集开始,新的数据集不断出现在社区中。以2009年为节点,网络入侵检测数据集相关研究开始增多。从表10第四列可以看出,超过一半的数据集是通过模拟实验得到的。这从侧面反映了网络入侵检测领域数据的敏感性。然而,此类数据集的准确性和真实性一直受到质疑(Mahoney et al., 2003),基于此类数据集构建的入侵检测模型的有效性较差。

此外,我们在表 9 (RQ6(b)) 中总结了数据集的使用频率。从表中可以看出,KDD99和NSL KDD是最常用的两个数据集,虽然都是模拟实验数据。这主要是因为

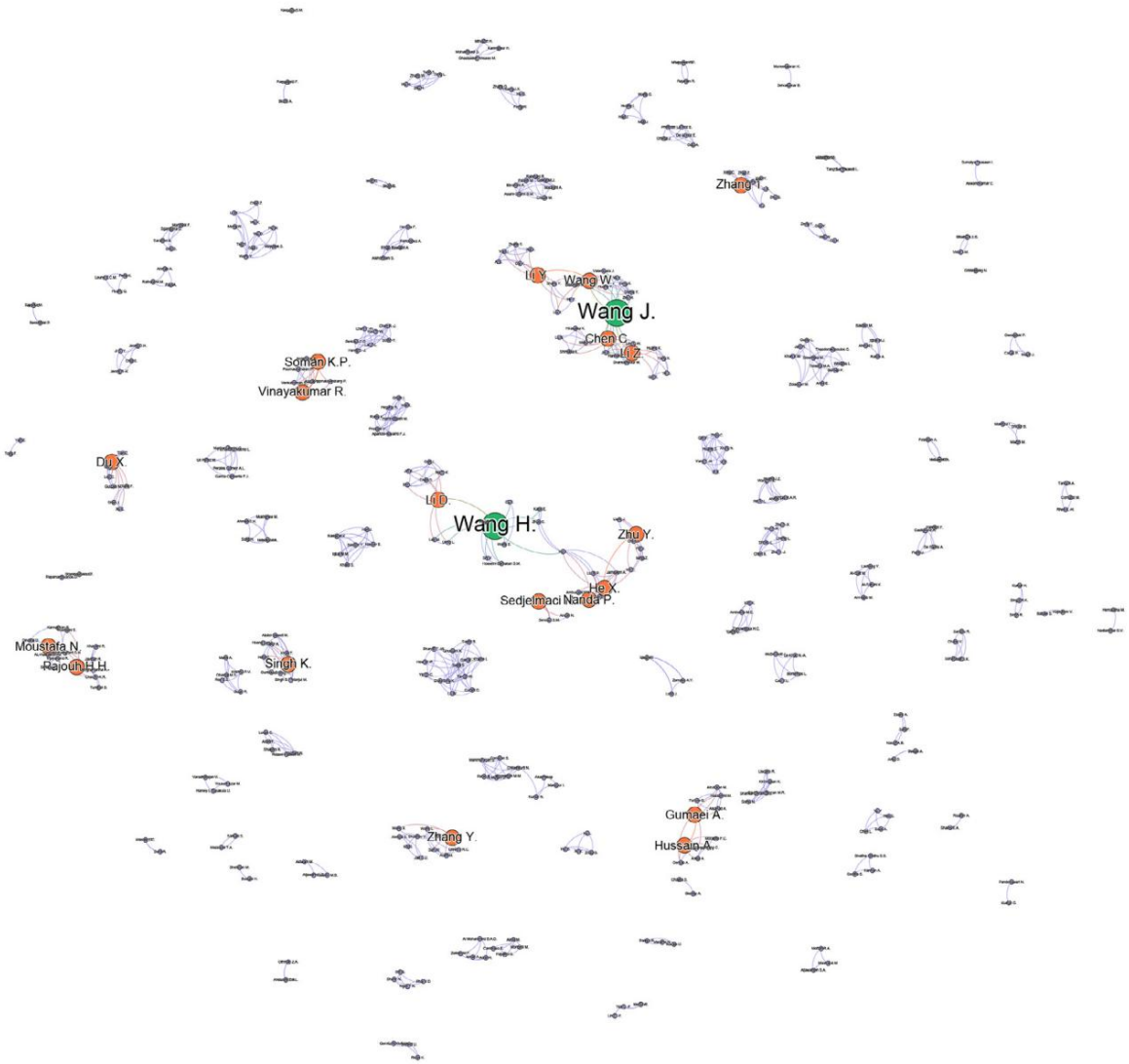

图 11.完整的合作者网络。

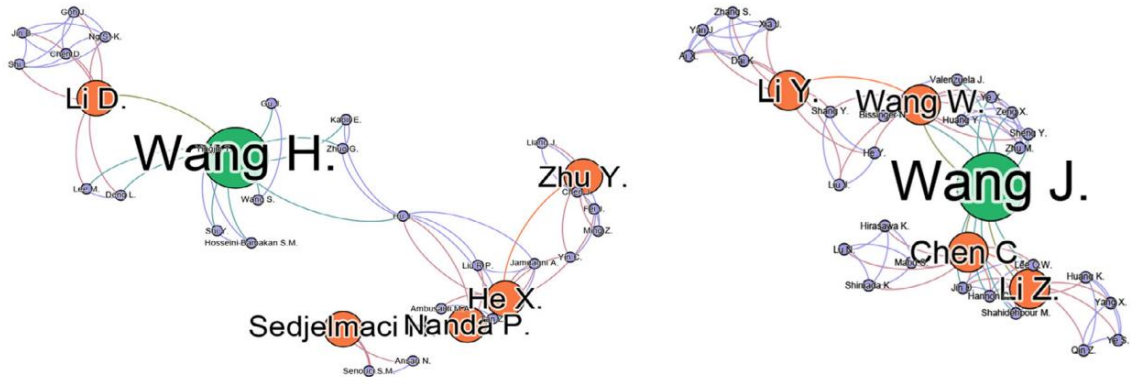

图 12.作者网络子图。

KDD99 和 NSL-KDD 是已经公开了很长时间的数据集。研究人员基于这两个数据集发表了许多文章。当一种新的入侵检测技术被提出时,往往需要与之前的技术进行比较,这导致了KDD99和NSL-KDD （RQ6（c））的不断使用。

然而,KDD99 和 NSL-KDD 数据集的内容已经过时。在未来的研究中,我们建议研究人员使用更新的方法评估入侵检测方法的性能入侵检测数据集,例如 CIRA-CIC-DoHBrw 2020 数据集,参考我们表格中的信息。此外,研究人员应尝试使用一些真实的数据集进行实验,例如 ISOT CID 数据集,以确保其方法的有效性。

最后,为了方便研究人员的工作,我们提供了表中数据集的链接,并更详细地展示了一些数据集。

表 10现有网
络入侵检测数据集。

编号数据集	年	真实性计数		标签数量		关联
[illegible]	1998 DARPA	1998模拟1999模拟1999	7,000,000 巨	是的	[illegible]	美国国防部高级研究计划局 (1998,1999)
[illegible]	1999 DARPA	模拟2000年仿真2000	大 5,000,000	是的	[illegible]	美国国防部高级研究计划局 (1998,1999)
	KDD99 2000	REAL 2006 REAL 2009	巨大 未知 未	是的	4	KDD99 (1999)
3 4	DARPA DEFCON	REAL 2009模拟2009	知	是	4	美国国防部高级研究计划局 (1998,1999)
[illegible]	京都 2006+Song	2009 2009 REAL 2009		的	未知 未知	防卫大会 (2000)
[illegible]	等。 (2006)	REAL 2009仿真2009		是		京都-2006+ (2006)
7	NSL-KDD Tavallaee 等人。 (2009)	REAL 2010 REAL 2010	148,517 巨	的	[illegible]	NSL-KDD (2009)未知
8	LDID	ARE 2010 REAL 2011	大	是的 没有	未知	
9	ICML-09 Ma 等人。 (2009)	REAL 2011 REAL 2012	2,400,000 未	是的	[illegible]	ICML-09 (2009)
10	Twente Sperotto 等人。 (2009)	REAL 2013 REAL 2014	知 5771	是的	未知 2 未知	特温特 (2009)
11 CDX 12 13		REAL 2014 REAL 2014	1,675,424	是的		CDX (2009)
	ISOT僵尸网络	REAL 2014 REAL 2014	223,585 未	是的		ISOT-僵尸网络 (2010)
	中船重工 HTTP 2010	REAL 2014 REAL 2014	知 2,450,324	是的	[illegible]	CSIC-HTTP-2010 (2010)未知
14 SSENet-2011		REAL 2014 REAL 2014	5266	是的	[illegible]	
15	ISCX-IDS 2012 Shiravi 等人。 (2012)	REAL 2014 REAL 2014		是的	未知	ISCX-IDS-2012 (2012)
16 ADFA-LD Creech 和 Hu (2013) 17 CTU-13 18 僵尸		REAL 2015 REAL 2015		是的	[illegible]	ADFA-LD (2013)
网络 2014 Beigi 等。 (2014)		ARE 2015 AMUALD 2015	huge	是的	7	CTU-13 (2014)
		AMULATE 2015	283,770	是的	16	Botnet-2014 (2014)未知
19 圣诞老人 20		AMULATE 2015	unknown	是的	6 3	
MAWILab		AMULATE 2015仿真2015	unknown	是		MAWILab (2014)未知
21	SSENet-2014 Bhattacharya 和 Selvakumar (2014) 22 SSHCure	2015仿真2015 REAL	201,707	的	[illegible]	
Hofstede 等。 (2014)		2016仿真2016模拟2016	unknown	是	未知	SSHCure (2014)
23 UNSW-NB15穆斯塔法和斯莱 (2015)		仿真2016 REAL 2016	2,540,044	的	9	新南威尔士大学-NB15 (2015)
24 ISTS-12 25		REAL 2016 REAL 2016	huge huge	是的 没有	未知 16 1	ISTS-12 (2015)
AWID Kolias 等。 (2015)		REAL 2016 REAL 2016	unknown	是的		疯狂 (2015)
26 UCSD Jonker 等人。 (2017) 27 IRSC		REAL 2016 REAL 2016	unknown	是的		加州大学圣地亚哥分
NDSec-1啤酒等。 (2017)		REAL 2017 REAT 2017仿	huge 734,627	是的	未知	校 (2015)未知
28		真2017 REAL 2017 REAL	unknown	是的	[illegible]	NDSec-1 (2016)
29 DDoS 2016 Alkasassbeh 等。 (2016)		2017仿真2017 REAL	unknown	是的	[illegible]	DDos-2016 (2016)
30 NGIDS-DS Haider 等。 (2017) 31 UGR 16		2017 REAL 2017 REAL	huge	是的	[illegible]	NGIDS-DS (2016)
Cermak 等。 (2016) 32 CIC-IDS-2017 Sharafaldin 等人。 (2018) 33 练习主机		2017 REAL 2017仿真	unknown	是的		UGR 16 (2016)未
等。 (2016)		2017仿真2017仿真2017	61,730 yes	是的	5 未知 未知	知
		仿真45 PUF 2018	55,733 yes	是的		主机和网络 (2016)未知
		EMULATION 45 PUF	31,959,267 yes			
		2018 REAL 46 REAL 46	16,161,183 yes huge no		1	卡伦 (2016)
36 CIDDS-001环等。 (2017)		ISOT CID 47 CID 47	2,830,743 unknown		19 6	中毒 (2017)
Jonker 等CIDDS-002环等。 (2017) 37 38 CAIDA		CICDDOS 2019沙拉法尔	32,925 yes huge yes		[illegible]	中毒 (2017)
		丁等。 (2019) 2019 模拟	19,301,217 yes huge yes		未知 7 未知	彩达 (2017)
NCCDC 41 CICIDS2017Jazi等人。 (2017) 42 TRABID 43		了 48 个 BoT-IoT	6,000,000 yes 36,936,985	是的	8 2 3	CICIDS-2017（2017)未知
SUEE 2017		Koroniotis 等人。 (2019)	yes huge 73,360,900	是的		
		2019 真实 49 IoT-23	yes unknown yes			CICDDoS-2019 (2019)
		2020 真实 50 InSDN	343,939 yes 1,185,296	yes		TRAbID (2017)未知
		2020 模拟 CIRA-CIC-	107,634 是			
44 ISOT HTTP 僵尸网络		DoHBrw 2020			9	ISOT HTTP 僵尸网络 (2017)未知
MontazeriShatoori 等。 (2020) 2020 仿真 52 OPCUA 2020 仿真					4	
					18	国际标准化组织 (2018)
				是的	11	CICDDoS-2019 (2019)
					2	机器人物联网 (2019)
					20	IoT-23 (2020)
					7	InSDN (2020)
51					[illegible]	CIRA-CIC-DoHBrw-2020 (2020)
					[illegible]	OPCUA, 2020

- DARPA数据集最常用于入侵检测,是在麻省理工学院林肯实验室在模拟网络环境中创建的。 DARPA 1998 和 DARPA 1999 数据集分别包含七周和五周的基于数据包格式的网络流量,包括 DoS、缓冲区溢出、端口扫描和 Rootkit 等攻击。尽管（或由于)它们分布广泛,但数据集经常因人为攻击注入或大量冗余而受到批评。

- KDD99数据集由Lee 和 Stolfo (2000) 根据 DARPA 网络数据集文件创建。通过数据挖掘构建数据集,分析DARPA数据集的特征并对数据进行预处理。该数据集包含七周的网络流量,大约有 490 万个向量。攻击分为： (1) user-to-root (U2R)； (2) 远程到本地 (R2L)； (3) 探测； (4) 拒绝服务。每个实例由三个类别的 41 个特征表示：(1)基本； (2) 交通； (3) 内容。基本特征是从 TCP/IP 连接中提取的。流量特征被分组为具有相同主机特征或相同服务的流量特征
特征。内容特征与数据部分的可疑行为有关。这是用于评估入侵检测模型的最广泛的数据集。

- NSL-KDD是一个建议用于解决 KDD99 数据集的一些固有问题的数据集。虽然,这个新版本的 KDD 数据集仍然存在Tavallaee 等人讨论的一些问题。 (2009) 并且可能不是现有真实网络的完美代表,因为缺乏基于网络的 IDS 的公共数据集,我们相信它仍然可以作为一个有效的基准数据集来帮助研究人员比较不同的入侵检测方法。此外,NSL-KDD 训练集和测试集中的记录数量是合理的。这一优势使得在整个集合上运行实验而无需随机选择一小部分成为负担得起的。因此,不同研究工作的评价结果将具有一致性和可比性。

- UNSW-NB15由澳大利亚网络安全中心的网络靶场实验室创建。由于其用途广泛

各种新颖的攻击。攻击类型包括模糊器、分析、后门、DoS、漏洞利用、通用、侦察、Shellcode 和蠕虫。它有一个包含 82,332 条记录的训练集和一个包含 175,341 条记录的测试集。

- CICIDS2017包含良性和常见攻击,包括基于时间戳、源和目标 IP、源和目标端口、协议和攻击令牌流的源数据 (PCAP) 和网络流量分析结果（CSV 文件）。研究人员使用 B-Profile 系统（Sharafaldin 等人,2016 年)来分析人类交互的抽象行为并生成良性背景流量。该数据集包括基于 HTTP、HTTPS、FTP、SSH 和电子邮件协议的 25 个用户的抽象行为。暴力破解攻击包括FTP、SSH、DoS、Heartbleed、web攻击、渗透、僵尸网络和DDoS。

- CICDoS2017是一个公开可用的入侵检测数据集,包含来自加拿大网络安全研究所的应用层 DoS 攻击。作者在应用层执行了八次 DoS 攻击。通过将生成的跟踪与来自 ISCX 2012 数据集的无攻击流量相结合,生成了正常的用户行为。该数据集以基于数据包的格式提供,包含 24 小时的网络流量。

- CICDDoS2019包含最新的 DDoS 攻击,与真实世界的数据相似。它包括使用 CICFLOWMeter-V3 的网络流量分析结果,其中包含基于时间戳源的令牌流,以及目标 IPS 源和端口协议和攻击。

- Kyoto 2006+是一个公开可用的真实网络流量蜜罐数据集,仅包括少量和小范围的真实、正常的用户行为。研究人员将基于数据包的流量转换为一种称为会话的新格式。每个会话有 24 个属性,其中 14 个是受 KDD CUP 99 数据集启发的统计信息特征,其余 10 个属性是典型的基于流量的属性,例如 IP 地址（匿名）、端口和持续时间。这些数据是在三年内收集的,包括大约 9300 万次会话。

- NDSec-1包含网络设施研究人员合成的网络攻击跟踪和日志文件。它是公开可用的,并于 2016 年以基于数据包的格式捕获。它包含额外的系统日志和 Windows 事件日志信息。攻击组合位置包括僵尸网络、暴力破解（针对 FTP、HTTP 和 SSH）、DoS（HTTP、SYN 和 UDP 泛洪）、漏洞利用、端口扫描、欺骗和 XSS/SQL 注入。

- CTU-13于 2013 年捕获,可用于数据包、单向流和双向流格式。在大学网络中捕获,其 13 个场景包括不同的僵尸网络攻击。网站上提供了有关受感染主机的其他信息。3流量分三个阶段进行标记:1) 进出受感染主机的所有流量都被标记为僵尸网络； 2)匹配特定过滤器的流量被标记为正常； 3)剩余流量被标记为背景。因此,后台流量可能是正常的也可能是恶意的。

- BoT-IoT包含超过 7200 万条记录,包括 DDoS、DoS、操作系统、服务扫描、键盘记录和数据泄露攻击。 Node-red 工具用于模拟物联网设备的网络行为。 MQTT 是一种轻量级通信协议,可链接机器对机器 (M2M) 通信。测试平台物联网场景包括气象站、智能冰箱、运动激活灯、远程激活车库门和智能恒温器。

- IoT-23由 23 个物联网流量网络捕获（称为场景)组成,包括来自受感染物联网设备的 20 个（PCAP 文件)和三个真实物联网网络流量。 Raspberry Pi 恶意软件在每个恶意场景中使用多个协议和每个形成不同的动作。良性场景的网络流量捕获是从三个真实物联网设备的网络流量中获得的:飞利浦 HUE 智能 LED 灯、亚马逊 Echo 家庭智能个人助理和尚飞智能门锁。恶意和良性场景都在受控网络环境中运行,网络连接不受限制,就像任何真实的物联网设备一样。

- PUF是在三天内从校园网络捕获的,仅包含 DNS 连接,其中 298,463 个单向流中有 38,120 个是恶意的。所有流都使用入侵防御系统的日志进行标记。出于隐私原因删除了 IP 地址。

- LBNL的创建是为了分析企业网络中的网络流量特征。该数据集可用作安全研究的背景流量,因为它包含几乎完全正常的用户行为。数据集未标记,是匿名的,并且包含超过 100 小时的基于数据包格式的网络流量。该数据集可在网站上下载。4 - IEEE 300 总线电源测试系统提供电网的拓扑和电气结构,用于检测智能电网中的虚假数据注入攻击。该系统有411个分支,平均度为2.74。有关此标准测试系统的详细信息,我们建议读者参考Hines 等人的工作。 （2010）。 IEEE 300 总线电源测试系统已用于许多与网络攻击分类相关的工作。

- ICS网络攻击数据集包括：(1)电力系统数据集； (2) 输气管道数据集； (3) 能源管理系统数据集； (4) 新的天然气管道数据集； (5) 输气管道和储水罐数据集。电力系统数据集包含 37 个场景,分为 8 个自然事件、1 个非事件和 28 个攻击。攻击分为：(1)继电器设置改变； (2)远程跳闸指令注入； (3) 数据注入。这些数据集可用于工业控制系统中的网络安全入侵检测。

5.结论

我们对网络安全中入侵检测的研究工作进行了全面的概述和分析。该调查涵盖了网络安全入侵检测领域中被引用次数最多的论文中的 119 篇,包括预处理和入侵检测技术,并从多个角度对社区进行了分析。我们分析了不同场景下的研究进展和瓶颈。我们研究了预处理和入侵检测技术。我们检查了评估方法,包括指标和数据集,以便将性能标准化为评估。我们统计了社区中的贡献者并绘制了他们的协作网络。我们的出版物数据和类别描述是公开的,以促进可重复性和进一步研究。

我们的结果表明,在不同的目标网络下,网络异常检测的研究是不平衡的。在 ICN 领域,由于工业网络数据的敏感性和机密性,研究人员通常不会公开他们的数据集。可用数据集的缺乏限制了 ICN 领域的网络安全研究。缺乏数据集也是限制SDN领域研究的关键因素。在进行安全研究之前,研究人员往往需要搭建SDN网络环境来模拟数据。就目前入侵检测技术使用的手段而言,监督学习仍然是主流方向。然而,这些研究需要建立在已经标记的数据之上。在实际应用时,我们获得的数据是未标记的。拉

[17] http://mcfp.weebly.com/the-ctu-13-dataset-a-labeled-dataset-with-botnet normal-and-background-traffic.html。

[18] http://icir.org/enterprise-tracing/download.html。

对数据进行建模是一项耗时且乏味的任务。我们相信无监督学习和半监督学习是网络异常检测的前进方向。同样，我们认为网络数据的自动化标注也是一个值得深入研究的方向。此外，对抗性环境已被证明会影响基于机器学习的网络异常检测算法。因此，对抗环境中的抗扰动异常检测也需要更多的研究。

竞争利益声明

作者声明，他们没有已知的可能影响本文报告的工作的竞争经济利益或个人关系。

致谢

本工作得到国家自然科学基金（No.61902010）、国家自然科学基金重大研究计划（92167102）、北京市教委项目的部分支持（不。KM202110005025）。

参考

Abbes, T., Bouhoula, A., Rusinowitch, M., 2010。入侵检测中用于协议分析的高效决策树。诠释。 J. 安全。网络。 5 (4), 220–235。

ADFA-LD，2013 年。https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-IDS-Datasets/。

Ahmed, M.、 Mahmood, AN、 Hu, J.， 2016 年。网络异常检测调查技巧。 J. 网络。电脑。申请60、19–31。

Alhajjar, E.、 Maxwell, P.、 Bastian, N.， 2021 年。网络入侵检测系统中的对抗性机器学习。专家系统申请 186, 115782。

Alkasassbeh, M.、 Al-Naymat, G.、 Hassanat, A.、 Almseidin, M.， 2016 年。使用数据挖掘技术检测分布式拒绝服务攻击。诠释。 J. Adv。计算机。科学。申请7 (1), 436–445。

Ambusaidi, MA, He, X., Nanda, P., Tan, Z., 2016。使用基于过滤器的特征选择算法构建入侵检测系统。 IEEE 跨。电脑。 65 (10), 2986–2998。

An, J., Cho, S., 2015. 基于变分自动编码器的异常检测使用侦察构造概率。规格莱克特。即 2 (1), 1-18。

Anthi, E.、 Williams, L.、 S owinska, M.、 Theodorakopoulos, G.、 Burnap, P.， 2019 年。用于智能家居物联网设备的监控入侵检测系统。 IEEE Internet Things J. 6 (5), 9042–9053。

AWID，2015 年。http: //icsdweb.aegean.gr/awid/download.html。

Axelsson, S., 2000。入侵检测系统：调查和分类。技术的报告。

Bach, FR, 2008。Bolasso：通过 boot strap 模型一致的 Lasso 估计。在：第 25 届国际机器学习会议论文集，第 33-40 页。

Bai, S., Kolter, JZ, Koltun, V.，2018。序列建模的通用卷积和循环网络的实证评估。 arXiv 预印本 arXiv:1803.01271。

Beer, F.、 Hofer, T.、 Karimi, D.、 Bühler, U.， 2017 年。一种新的网络攻击组合安全。 10. DFN-Forum Kommunikationstechnologien。

Beigi, EB, Jazi , HH, Stakhanova, N., Ghorbani, AA， 2014 年。在基于机器学习的僵尸网络检测方法中实现有效特征选择。在：2014 年 IEEE 通信和网络安全会议，第 247-255 页。

Bengio, Y., 2009。学习人工智能的深度架构。现在出版商公司

Bermingham, ML, Pong-Wong, R., Spiliopoulou, A., Hayward, C., Rudan, I., Camp bell, H., Wright, AF, Wilson, JF, Agakov, F., Navarro, P., et al., 2015. 高维特征选择的应用：人类基因组预测的评估。科学。众议员 5 (1), 1–12。

Bhattacharya, S., Selvakumar, S., 2014。SSENet-2014 数据集：用于检测多连接攻击的数据集。在：2014 年第三届环保计算和通信系统国际会议，第 121-126 页。

Bhuyan, MH, Bhattacharyya, DK, Kalita, JK, 2013。网络异常检测：方法、系统和工具。 IEEE 通讯。生存。导师。 16 (1), 303–336。

Bontemps, L., McDermott, J., Le-Khac, N.-A., et al., 2016. 基于长短期记忆递归神经网络的集体异常检测。在：未来数据和安全工程国际会议，第 141-152 页。

BoT -IoT，2019年。https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php。

Botnet-2014，2014 年。https://www.unb.ca/cic/datasets/botnet.html。

Breiman, L., 1996。装袋预测器。马赫。学习。 24 (2), 123–140。

Breiman, L., 2001。随机森林。马赫。学习。 45 (1), 5–32。

Buczak, AL, Guven, E.， 2015 年。用于网络安全入侵检测的数据挖掘和机器学习方法调查。 IEEE 通讯。生存。导师。 18 (2), 1153–1176。

Bulavas, V., 2018. 使用数据可视化进行网络入侵检测的调查化方法，1-6。

CAIDA，2017 年。https://www.impactcybertrust.org/dataset_view?idDataset=834。

Caminero, G.、 Lopez-Martin, M.、 Carro, B.， 2019 年。用于入侵检测的对抗性环境强化学习算法。电脑。网络。 159、96–109.

Capes, T., Coles, P., Conkie, A., Golipour, L., Hadjitarkhani, A., Hu, Q., Huddleston, N., Hunt, M., Li, J., Neeracher, M.，等人， 2017 年。Siri 设备上深度学习引导的单元选择文本到语音系统。在：INTERSPEECH，第 4011-4015 页。

Casas, P.、 Mazel, J.、 Owezarski, P.， 2012 年。无监督网络入侵检测系统：检测未知的知识。电脑。公社。 35 (7), 772–783。

CDX，2009 年。https://www.usma.edu/centers-and-research/cyber-research-center/数据集。

Cermak, M.、 Jirsik, T.、Velan, P.、Komarkova, J.、Spacek, S.、Drasar, M.、Plesnik, T.，2018 年。通过半标记跟踪数据集实现可证明的网络流量测量和分析。在：2018 年网络流量测量和分析会议 (TMA)，第 1-8 页。

Chawla, NV, Bowyer, KW, Hall, LO, Kegelmeyer, WP, 2002。Smote：合成少数过采样技术。 J. Artif。智能。水库。 16, 321–357。

Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., Bengio, Y., 2014。使用 RNN 编码器-解码器学习短语表示以进行统计机器翻译. arXiv 预印本 arXiv:1406.1078。

CICDDoS-2019，2019。https://www.unb.ca/cic/datasets/ddos-2019.html 。

CICIDS-2017，2017 年。https://www.unb.ca/cic/datasets/ids-2017.html 。

CIDDS，2017 年。http://www.hs-coburg.de/cidds。

CIRA-CIC-DoHBrw-2020，2020 年。https://www.unb.ca/cic/datasets/dohbrw-2020.html 。

Creech, G., Hu, J., 2013。生成新的 IDS 测试数据集：是时候淘汰 KDD 集合了。在：2013 年 IEEE 无线通信和网络会议 (WCNC)，第 4487–4492 页。

CSIC-HTTP-2010，2010。https ://petescully.co.uk/research/csic-2010-http-dataset-in csv-format-for-weka-analysis/。

CTU-13，2014 年。http: //mcfp.weebly.com/。

Cybenko, G., 1989。S形函数的叠加逼近。数学。控制信号系统2 (4), 303–314。

美国国防部高级研究计划局，1998 年，1999 年。 http://www.tp-ontrol.hu/index.php/_DDos-2016，2016年。 TP_Toolbox。 www.researchgate.net/publication/292967044_Dataset-Detecting_Distributed_Denial_of_Service_Attacks_Using_Data_Mining_Techniques。

DEFCON，2000 年。https://defcon.org/html/links/dc-ctf.html。

Deng, H.、 Runger, G.、 Tuv, E.， 2011 年。多值属性和解决方案的重要性度量偏差。在：国际人工神经网络会议作品，第 293-300 页。

Dong, Y., Wang, R., He, J., 2019. 基于深度学习的实时网络入侵检测系统。在：2019 年 IEEE 第 10 届软件工程与服务科学国际会议 (ICSESS)，第 1-4 页。

Dupond, S., 2019. 对神经网络当前进展的全面回顾结构。安奴。修订版控制 14, 200–230。

Ertekin, S., Huang, J., Bottou, L., Giles, L., 2007。边界学习：不平衡数据分类中的主动学习。在：关于信息和知识管理会议的第十六届 ACM 会议论文集，第 127-136 页。

Estabrooks, A., Jo, T., Japkowicz, N., 2004。学习的多重重采样方法来自不平衡的数据集。电脑。智能。 20 (1), 18–36。

Fernández, A.、 Garcia, S.、 Herrera, F.、 Chawla, NV， 2018 年。Smote for learning from imbalanced data: progress and challenges，纪念 15 周年。 J. 神器。智能。水库。 61、863–905。

Freund, Y., Schapire, RE, et al., 1996。使用新的增强算法进行实验。在：国际机器学习会议，卷。 96，第 148-156 页。

Gers, FA, Schmidhuber, J., Cummins, F., 2000。学会遗忘：连续预测与 LSTM 结合。神经计算。 12 (10), 2451–2471。

Ghorbani, AA、 Lu, W.、 Tavallaee, M.， 2009 年。网络入侵检测和预防：概念和技术，第一卷。 47. 斯普林格科学与商业媒体。

Goodfellow, I.、 Bengio, Y.、Courville, A.、Bengio, Y.，2016 年。深度学习，卷。 1. 麻省理工学院剑桥出版社。

Guyon, I., Elisseeff, A., 2003。变量和特征选择介绍。 J. 马赫。学习。水库。 3（三月），1157–1182。

Haider, W., Hu, J., Slay, J., Turnbull, BP, Xie, Y., 2017。基于模糊定性建模生成逼真的入侵检测系统数据集。 J. 网络。电脑。申请87、185–192。

Hajisalem, V., Babaie, S., 2018。一种基于 ABC-AFS 算法的混合入侵检测系统，用于误用和异常检测。电脑。网络。 136、37–50。

Hamid, Y., Sugumaran, M., 2020. 基于 t-SNE 的非线性降维网络入侵检测。诠释。 J. Inf。技术。 12 (1), 125–134。

Hande, Y., Muddana, A.， 2021 年。软件定义网络 (SDN) 入侵检测系统调查。在：人工智能在安全中的应用研究选集。 IGI 全球，第 467–489 页。

Haq, NF, Onik, AR, Hridoy, MAK, Rafni, M., Shah, FM, Farid, DM, 2015。机器学习方法在入侵检测系统中的应用：一项调查。 IJARAI-诠释。 J. Adv。水库。神器。智能。 4 (3), 9–18。

He, H., Bai, Y., Garcia, EA, Li, S., 2008。ADASYN：用于不平衡学习的自适应合成采样方法。在：2008 年 IEEE 神经网络国际联合会议（IEEE 世界计算智能大会），第 1322–1328 页。

He, K., Zhang, X., Ren, S., Sun, J., 2016。用于图像识别的深度残差学习。在:IEEE 计算机视觉和模式识别会议论文集,第 770-778 页。

Hines, P.、 Blumsack, S.、 Sanchez, EC、 Barrows, C.， 2010 年。电网的拓扑结构和电气结构。在:2010 年第 43 届夏威夷系统科学国际会议,第 1-10 页。

Hinton, G., Roweis, ST, 2002。随机邻域嵌入。在:NIPS,卷。 15. Cite seer,第 833–840 页。

Hochreiter, S., Schmidhuber, J., 1997。长短期记忆。神经计算。 9 (8),1735–1780。

Hodo, E.、Bellekens, X.、Hamilton, A.、Tachtatzis, C.、Atkinson, R.,2017 年。Shal low and deep networks intrusion detection system: a taxonomy and survey。 arXiv 预印本 arXiv:1701.02145。

Hofstede, R.、 Hendriks, L.、 Sperotto, A.、 Pras, A.， 2014 年。使用 NetFlow/IPFIX 进行 SSH 危害检测。 ACM SIGCOMM 计算机。公社。修订版 44 (5), 20–26。

Host, U., Network, 2016. https://csr.lanl.gov/data/cyber1/。

De la Hoz, E.、 De La Hoz, E.、 Ortiz, A.、 Ortega, J.、 Prieto, B.， 2015 年。用于网络入侵检测的 PCA 过滤和概率 SOM。神经计算 164, 71–81。

Hsu, C.-W., Chang, C.-C., Lin, C.-J., et al., 2003. 支持向量实用指南
分类。

Hu, W., Gao, J., Wang, Y., Wu, O., Maybank, S., 2013。用于动态分布式网络入侵检测的基于 adaboost 的在线参数化方法。 IEEE 跨。赛伯恩。 44 (1), 66–82。

Hubel, DH, Wiesel, TN, 1968. 感受野和功能架构
关键纹皮质。 J.生理学。 195 (1), 215–243。

ICML-09, 2009. http://www.sysnet.ucsd.edu/projects/url/。

InSDN， 2020 年。http://aseados.ucd.ie/?p=177 。

IoT-23,2020 年。https://mcfp.felk.cvut.cz/publicDatasets/IoT-23-Dataset/iot_23_datasets_small.tar.gz。

ISCX-IDS-2012, 2012. https://www.unb.ca/cic/datasets/ids.html。

ISOT-僵尸网络,2010 年。https://www.uvic.ca/engineering/ece/isot/datasets/botnet ransomware/index.php。

ISOT-CID,2018 年。https: //www.uvic.ca/engineering/ece/isot/datasets/cloud-security/索引.php。

ISTS-12,2015 年。http://ists.sparsa.org/ 。

ISOT,2017 年。https: //www.uvic.ca/engineering/ece/isot/datasets/botnet-ransomware/索引.php。

Jan, SU, Ahmed, S., Shakhov, V., Koo, I., 2019。面向物联网的轻量级入侵检测系统。 IEEE 访问 7, 42450–42471。

Jazi, HH, Gonzalez, H., Stakhanova, N., Ghorbani, AA， 2017 年。在存在采样的情况下检测对 Web 服务器的基于 http 的应用层 DOS 攻击。计算机。网络。 121、25-36。

Jonker, M.、 King, A.、 Krupp, J.、 Rossow, C.、 Sperotto, A.、 Dainotti, A.， 2017 年。数百万受到攻击的目标:剂量生态系统的宏观特征。在:2017 年互联网测量会议论文集,第 100-113 页。

KDD99, 1999. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html。

Keele, S., et al., 2007。在软件工程中执行系统文献审查指南。技术报告。引用者。

Khammmassi, C., Krichen, S., 2017。一种用于网络入侵检测中特征选择的 GA-LR 包装器方法。电脑。安全。 70、255–277。

卡伦,2016 年。http://kharon.gforge.inria.fr/dataset/index.html 。

Kiss, N.、 Lalande, J.-F.、 Leslous, M.、 Tong, VVT， 2016 年。Kharon 数据集:显微镜下的安卓恶意软件。在： {LASER}研讨会:从权威安全实验结果中学习（{LASER} 2016），第 1-12 页。

Koc, L.、 Mazzuchi, TA、 Sarkani, S.， 2012 年。基于隐藏朴素贝叶斯多类分类器的网络入侵检测系统。专家系统申请39 (18), 13492–13500。

Kolias, C.、Kambourakis, G.、Stavrou, A.、Gritzalis, S.,2015 年。802.11网络中的入侵检测:威胁的实证评估和公共数据集。 IEEE 通讯。生存。导师。 18 (1), 184–208。

Koroniotis, N.、 Moustafa, N.、 Sitnikova, E.、 Turnbull, B.， 2019 年。在物联网中开发用于网络取证分析的真实僵尸网络数据集:机器人物联网数据集。未来的一代。电脑。系统。 100、779–796。

Krizhevsky, A.、 Sutskever, I.、 Hinton, GE， 2012 年。使用深度卷积神经网络进行 ImageNet 分类。进阶神经信息过程。系统。 25, 1097–1105。

Kyoto-2006+, 2006. http://www.takakura.com/Kyoto_data/。

LeCun, Y.、 Bottou, L.、 Bengio, Y.、 Haffner, P.， 1998。基于梯度的学习应用于
文件识别。过程。 IEEE 86 (11), 2278–2324。

Lee, W., Stolfo, SJ, 2000。构建入侵检测系统特征和模型的框架。 ACM 跨。信息。系统。安全 (TiSSEC) 3 (4), 227–
261.

Li, J., Zhao, Z., Li, R., Zhang, H., 2018。基于人工智能的软件定义物联网网络两阶段入侵检测。 IEEE Internet Things J. 6 (2), 2093–2102。

Li, Z., Qin, Z., Huang, K., Yang, X., Ye, S., 2017。使用卷积神经网络进行表示学习的入侵检测。在:国际神经信息处理会议,第 858-866 页。

Liu, X.-Y., Wu, J., Zhou, Z.-H., 2008。类不平衡学习的探索性欠采样。 IEEE 跨。系统。人塞伯恩。 B 部分 39 (2), 539–550。

Loh, W.-Y., 2011。分类和回归树。威利跨学科。牧师数据最小知识。发现。 1 (1), 14–23。

Ma, J.、 Saul, LK、 Savage, S.、 Voelker, GM， 2009 年。超越黑名单:学习从可疑 URL 检测恶意网站。在:第 15 届 ACM SIGKDD 知识发现和数据挖掘国际会议论文集,第 1245-1254 页。

Madeh Piryonesi, S., El-Diraby, TE,2021 年。使用机器学习检查性能指标类型对柔性路面劣化建模的影响。J. 基础设施。系统。 27 (2), 04021005。

Mahoney, Matthew, V., Philip, K., Chan, 2003。对 1999 年 DARPA/林肯实验室网络异常检测评估数据的分析。在:关于入侵检测最新进展的国际研讨会。 Springer,柏林,海德尔堡,第 220-237 页。

Mani, I., Zhang, I., 2003。kNN 处理不平衡数据分布的方法:涉及信息提取的案例研究。在:从不平衡数据集中学习的研讨会论文集,卷。 126.

Martinez, AM, Kak, AC, 2001。PCA 与 LDA。 IEEE 跨。模式肛门。马赫。
智能。 23 (2), 228–233。

MAWILab,2014 年。http://www.fukuda-lab.org/mawilab/documentation.html。

McCarthy, K.、 Zabar, B.、 Weiss, G.， 2005 年。成本敏感型学习在对稀有类别进行分类时是否胜过抽样?在:第一届基于效用的数据挖掘国际研讨会论文集,第 69-77 页。

Mehmood, A.、 Mukherjee, M.、 Ahmed, SH、 Song, H.、 Malik, KM， 2018 年。NBC-MAIDS:多代理系统增强型 IDS 中的朴素贝叶斯分类技术,用于保护物联网免受 DDoS 攻击。 J. 超级计算机。 74 (10), 5156–5170。

Milenkoski, A.、 Vieira, M.、 Kounev, S.、 Avritzer, A.、 Payne, BD， 2015 年。评估计算机入侵检测系统:常见做法调查。 ACM 计算机。
生存。 (CSUR) 48 (1), 1–41。

Miljanovic, M., 2012。时间序列预测中递归和有限脉冲响应神经网络的比较分析。印度 J. Comput。科学。工程。 3 (1), 180–191。

Mishra, P.、 Varadharajan, V.、Tupakula, U.、Pilli, ES,2018 年。使用机器学习技术进行入侵检测的详细调查和分析。 IEEE 通讯。生存。导师。 21 (1), 686–728。

MontazeriShatoori, M., Davidson, L., Kaur, G., Lashkari, AH, 2020。使用加密流量的时间序列分类检测 DoH 隧道。在:2020 IEEE 国际。会议。关于可靠、自主和安全的计算,国际。会议。关于普适智能和计算,国际。会议。关于云计算和大数据计算,国际。会议。关于网络科学技术大会(DASC/PiCom/CBDCom/CyberSciTech),第 63–70 页。

Moustafa, N., Slay, J., 2015. UNSW-NB15:网络入侵检测系统综合数据集（UNSW-NB15 网络数据集）。在:2015 年军事通信和信息系统会议 (MilCIS),第 1-6 页。

Muniyandi, AP, Rajeswari, R., Rajaram, R., 2012。通过级联 k 均值聚类和 C4 进行网络异常检测。 5 决策树算法。 Procedia 工程。 30,
174–182。

NDSec-1,2016 年。https://www2.hs-fulda.de/NDSec/NDSec-1/Files/ 。

NGIDS-DS,2016 年。research.unsw.edu.au/people/professor-jiankun-hu 。

Nisioti, A.、 Mylonas, A.、 Yoo, PD、 Katos, V.， 2018 年。从入侵检测到攻击者归因:无监督方法的综合调查。 IEEE 通讯社。生存。导师。 20 (4), 3369–3388。

NSL-KDD,2009 年。https://www.unb.ca/cic/datasets/nsl.html。

OPCUA,2020 年。https://digi2-feup.github.io/OPCUADataset/。

Özgür, A., Erdem, H., 2016。2010 年至 2015 年间 KDD99 数据集在入侵检测和机器学习中的使用回顾。PeerJ Preprints 4, e1954v1。

Peng, K., Leung, VC, Huang, Q., 2018。基于小批量 Kmeans 的大数据入侵检测系统聚类方法。 IEEE 访问 6,11897–11906。

Pyle, D., 1999。数据挖掘的数据准备。摩根考夫曼。

Quinlan, JR, 1983。学习高效分类程序及其应用
下棋结束游戏。马赫。学习。 463–482。

Quinlan, JR, 1986。决策树的归纳。马赫。学习。 1 (1), 81–106。

昆兰,JR， 2014 年。C4。 5:机器学习程序。爱思唯尔。

Raskutti, B.， Kowalczyk, A.， 2004 年。SVM 的极端再平衡:案例研究。 ACM Sigkdd 浏览器。新闻6 (1), 60–69。

Ring, M.、 Wunderlich, S.、 Grüdl, D.、 Landes, D.、 Hotho, A.， 2017 年。用于入侵检测的基于流的基准数据集。在:第 16 届欧洲网络战与安全会议论文集。 ACPI,第 361–369 页。

Ring, M.、 Wunderlich, S.、 Scheuring, D.、 Landes, D.、 Hotho, A.， 2019 年。基于网络的入侵检测数据集调查。电脑。安全。 86, 147–167。

Roy, SS、 Mallik, A.、 Gulati, R.、 Obaidat, MS、 Krishna, PV， 2017 年。一种基于深度学习的人工神经网络入侵检测方法。见:国际数学与计算会议,第 44-53 页。

Ruan, Z., Miao, Y., Pan, L., Patterson, N., Zhang, J., 2017。大数据安全可视化:以 KDD99 杯数据集为例。数字。公社。网络。 3 (4), 250–259。

Safavian, SR, Landgrebe, D., 1991。决策树分类器方法的调查。
IEEE 跨。系统。人塞伯恩。 21 (3), 660–674。

Sarangi, S.、 Sahidullah, M.、 Saha, G.， 2020 年。用于自动说话人验证的数据驱动滤波器组优化。数字。信号处理。 104,102795。

Sharafaldin, I.、 Lashkari, AH、 Ghorbani, AA， 2018 年。生成新的入侵检测数据集和入侵流量特征。在:ICISSp,第 108-116 页。

Sharafaldin, I.、 Lashkari, AH、 Hakak, S.、 Ghorbani, AA， 2019 年。开发真实的分布式拒绝服务(DDoS) 攻击数据集和分类法。在:2019 年国际卡纳汉安全技术会议 (ICCST),第1-8 页。

Shiravi, A.、 Shiravi, H.、 Tavallaee, M.、 Ghorbani, AA， 2012 年。开发一种系统方法来生成用于入侵检测的基准数据集。计算机。安全。 31 (3), 357–374。

Singh, K.、 Guntuku, SC、 Thakur, A.、 Hota, C.， 2014 年。使用随机森林检测点对点僵尸网络的大数据分析框架。信息。科学。 278、488–497。

Song, J., Takakura, H., Okabe, Y., 2006。京都大学基准数据说明。链接： http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf [2016 年 3 月 15 日访问]。

Sperotto, A.、 Sadre, R.、 Van Vliet, F.、 Pras, A.， 2009 年。用于基于流的入侵检测的标记数据集。载于：知识产权运营和管理国际研讨会，第 39-50 页。

SSHCure，2014 年。www.simpleweb.org/wiki/index.php 。
Subba, B.、 Biswas, S.、 Karmakar, S.， 2015 年。使用线性判别分析和逻辑回归的入侵检测系统。在：2015 年度 IEEE 印度会议 (INDICON)，第 1-6 页。

Taherdangkoo, M., Paziresh, M., Yazdi, M., Bagheri, MH, 2013。功能优化的有效算法：改进的干细胞算法。分。欧元。 J. Eng。 3 (1), 36–50。

Tan, Z., Jamdagni, A., He, X., Nanda, P., Liu, RP, Hu, J., 2014。基于计算机视觉技术的拒绝服务攻击检测。 IEEE 跨。计算机。 64 (9), 2519–2533。

Tang, TA, Mhamdi, L., McLernon, D., Zaidi, SAR, Ghogho, M., 2018。基于 SDN 的网络中用于入侵检测的深度神经网络。在：2018 年第四届 IEEE 网络软件化和研讨会会议 (NetSoft)，第 202-206 页。

Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, AA, 2009。KDD CUP 99 数据集的详细分析。在：2009 年 IEEE 安全和国防应用计算智能研讨会，第 1-6 页。

Teng, S., Wu, N., Zhu, H., Teng, L., Zhang, W., 2017。基于 SVM-DT 的自适应和协同入侵检测。 IEEE/CAA J. Autom。罪。 5 (1), 108–118。
Thakkar, A.、 Lohiya, R.， 2020 年。入侵检测进展回顾
数据集。 Procedia 计算机。科学。 167、636–645。
Ting, KM, 2002。一种诱导成本敏感树的实例加权方法。 IEEE
反式。知识数据工程师。 14 (3), 659–665。
TRAbID，2017 年。https://secplab.ppgia.pucpr.br/?q=trabid。
特温特，2009 年。www.simpleweb.org/wiki/index.php。
加州大学圣地亚哥分校，2015 年。https://www.impactcybertrust.org/dataset_view?idDataset=915。
UGR 16，2016 年。https ://nesg.ugr.es/nesg-ugr16/index.php 。
UNSW-NB15，2015 年。 https://cloudstor.aarnet.edu.au/plus/index.php/s/2DhnLGDdEECo4ys?path=2FUNSW-NB1520-20CSV20 文件。
Van Der Maaten, L., 2014。使用基于树的算法加速 t-SNE。 J.马赫。
学习。水库。 15 (1), 3221–3245。
Vinayakumar, R.、 Alazab, M.、 Soman, K.、 Poornachandran, P.、 Al-Nemrat, A.、 Venkatra man, S.，2019 年。智能入侵检测系统的深度学习方法。
IEEE 访问 7, 41525–41550。
Vinayakumar, R.、 Soman, K.、 Poornachandran, P.， 2017 年。将卷积神经网络应用于网络入侵检测。在：2017 年计算、通信和信息学进展国际会议 (ICACCI)，第 1222–1228 页。

Wang, BX, Japkowicz, N., 2004。使用合成 sam 的不平衡数据集学习
请。在：过程。 IRIS 机器学习研讨会，卷。 19.
Wang, L., Jones, R.， 2017 年。用于网络入侵检测的大数据分析：一项调查。
诠释。 J. Netw.Commun。 7 (1), 24–31。
Weiss, GM, Provost, F., 2001。班级分布对分类器学习的影响：
一项实证研究。
Wolpert, DH, Macready, WG, 1997。优化没有免费的午餐定理。 IEEE 跨。进化。电脑。 1 (1), 67–82。

Wu, Y., Schuster, M., Chen, Z., Le, QV, Norouzi, M., Macherey, W., Krikun, M., Cao, Y., Gao, Q., Macherey, K., et al., 2016. Google 的神经机器翻译系统：弥合人类与机器翻译之间的差距。 arXiv 预印本 arXiv:1609.08144。

Xiao, Y., Xing, C., Zhang, T., Zhao, Z., 2019。一种基于特征缩减和卷积神经网络的入侵检测模型。 IEEE 访问 7, 42210–42219。

Xu, C.、Shen, J.、Du, X.、Zhang, F.，2018 年。使用带有门控循环单元的深度神经网络的入侵检测系统。 IEEE 访问 6, 48697–48707。
Yang, Y., Pedersen, JO, 1997。文本分类中特征选择的比较研究。 Icml 97 (412–420), 35。

Yao, H., Li, C., Sun, P., 2020。使用参数 t 分布随机邻域嵌入结合分层神经网络进行网络入侵检测。诠释。 J.网络。安全。 22 (2), 265–274。

Yin, C.、 Zhu, Y.、 Fei, J.、 He, X.， 2017 年。一种使用递归神经网络进行入侵检测的深度学习方法。 IEEE 访问 5, 21954–21961。
Zare, H.、 Haffari, G.、 Gupta, A.、 Brinkman, RR， 2013 年。基于 Lasso 组合分析的特征相关性评分及其在淋巴瘤诊断中的应用。 BMC 基因组学 14 (1), 1–9。

Zarpelão, BB, Miani, RS, Kawakani, CT, de Alvarenga, SC, 2017。物联网入侵检测调查。 J. 网络。电脑。申请84、25–37。
Zhang, H., Wu, CQ, Gao, S., Wang, Z., Xu, Y., Liu, Y., 2018。一种有效的基于深度学习的网络入侵检测方案。在：2018 年第 24 届模式识别国际会议 (ICPR)，第 682–687 页。

Zhang, J.、 Zulkernine, M.、 Haque, A.， 2008 年。基于随机森林的网络入侵检测系统。 IEEE 跨。系统。 Man Cybern.C 部分 38 (5), 649–659。

杨振现任北京工业大学计算机科学与工程学院教授。

他获得了北京邮电大学信号处理专业的博士学位。他的研究兴趣包括数据挖掘、机器学习、可信计算和内容安全。他已在高排名期刊和顶级会议论文集上发表了 30 多篇论文。中国电子学会高级会员，IEEE会员。

刘晓东目前在北京工业大学计算机科学与技术学院攻读硕士学位。研究领域：网络安全、入侵检测、机器学习。

Tong Li在中国北京工业大学信息技术学院担任讲师。他于 2016 年获得特伦托大学计算机科学博士学位。他在需求工程、安全工程、和概念建模。他目前专注于分析社会工程攻击的安全需求。现主持国家自然科学基金一项、国家重点研发计划子课题一项、北京市教育科学规划基金一项。 ISO/IEC JTC专家
1/ SC 27/ WG 4，并担任 ISO/IEC 24392 的共同编辑。

吴迪目前正在中国北京的北京工业大学计算机科学与技术学院攻读博士学位。她的研究兴趣包括多目标优化算法和知识图嵌入。

Jinjiang Wang是中国北京市北京工业大学信息安全专业的在读本科生。他的研究兴趣包括基于机器学习的网络入侵检测算法和强化学习。

赵云薇2015年获得清华大学博士学位,后在南洋理工大学从事博士后研究工作。她于2017年加入CNCERT/CC.她的研究兴趣是数据分析、网络安全、数据相互依赖、行为建模和社交媒体分析。她的出版物出现在顶级场所,包括 IJCAI、IJCNN、WI-IAT 等。

韩寒,CNCERT/CC工程师。他擅长软件工程、人工智能和网络安全。他的研究弥合了 AI 辅助软件系统的理论与实际时代之间的差距,以提供更好的质量保证和安全性。