工业物联网异常检测技术综述

孙海丽[1]，龙翔[1,2]，韩兰胜[1,3]，黄炎[4]，李清波[1]

（1. 华中科技大学网络空间安全学院，湖北 武汉 430074；2. 湖北生物科技职业学院，湖北 武汉 430070；
3. 鹏城实验室网络空间安全研究中心，广东 深圳 518000；4. 华中科技大学计算机科学与技术学院，湖北 武汉 430074）

摘 要：针对不同的异常检测方法的差异及应用于工业物联网（IIoT）安全防护的适用性问题，从技术原理出发，调研分析 2000—2021 年发表的关于网络异常检测的论文，总结了工业物联网面临的安全威胁，归纳了 9 种网络异常检测方法及其特点，通过纵向对比梳理了不同方法的优缺点和适用工业物联网场景。另外，对常用数据集做了统计分析和对比，并从 4 个方向对未来发展趋势进行展望。分析结果可以指导按应用场景选择适配方法，发现待解决关键问题并为后续研究指明方向。

关键词：工业物联网；异常检测；网络入侵；网络攻击

中图分类号：TN92

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022032

Overview of anomaly detection techniques for industrial Internet of things

SUN Haili[1], LONG Xiang[1,2], HAN Lansheng[1,3], HUANG Yan[4], LI Qingbo[1]

1. School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China
2. Hubei Vocational College of Bio-Technology, Wuhan 430070, China
3. Cyberspace Security Center, Peng Cheng Laboratory, Shenzhen 518000, China
4. School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

Abstract: In view of the differences of existing anomaly detection methods and the applicability when applied to security protection of the industrial Internet of things (IIoT), based on technical principles, the network anomaly detection papers published from 2000 to 2021 were investigated and the security threats faced by IIoT were summarized. Then, network anomaly detection methods were classified into 9 classes and the characteristics of each class was studied. Through longitudinal comparison, the merits and shortcomings of different methods and their applicability to IIoT scenarios were sorted out. In addition, statistical analysis and comparison of common data sets were made, and the development trend in the future was forecasted from 4 directions. The analysis results can guide the selection of adaptive methods according to application scenarios, identify key problems to be solved, and point out the direction for subsequent research.

Keywords: industrial Internet of things, anomaly detection, network intrusion, cyber attack

0 引言

随着 5G 通信技术的快速发展，以及传感器和处理器等嵌入式设备的计算和存储能力不断增加，这些网络通信和嵌入式设备在工业系统中的应用越来越普遍。工业物联网（IIoT, industrial Internet of things）是由应用程序、软件系统和物理设备三者组成的大型网络，这三者与外部环境以及人类之间进行通信和共享智能[1]。据埃森哲预测，到 2030 年，美国的工业物联网价值将出到

收稿日期：2021−11−01；**修回日期**：2022−01−24

通信作者：韩兰胜，hanlansheng@hust.edu.cn

基金项目：国家自然科学基金资助项目（No.61272033, No.62072200, No.6217071437, No.62127808）

Foundation Item: The National Natural Science Foundation of China (No.61272033, No.62072200, No.6217071437, No.62127808)

7.1 万亿美元，对欧洲而言价值将超过 1.2 万亿美元[2]。

在这波工业发展浪潮中，物联网安全是影响工业物联网广泛使用的重要因素之一。事实上，物联网设备的安全性通常很差，因此很容易成为攻击者的目标。攻击者利用这些设备可以进行毁灭性的网络攻击，如分布式拒绝服务（DDoS, distributed denial of service）[3-4]。传统的工业环境在过去一直遭受攻击，有的还造成了灾难性的后果（例如，震网病毒[5]或故障超驰/工业破坏者[6]）。因此，如果没有安全性，工业物联网将永远无法发挥其全部潜力。另外，工业系统对性能和可用性有严格的要求，即使系统受到网络攻击，维护系统不间断和安全地运行也常常是优先考虑的。

异常检测在防御系统和网络的恶意活动中是至关重要的。近年来，为了缓解网络攻击，工业物联网异常检测方面的研究迅速增多，许多检测机制被提出。另一方面，在异常检测方面研究者已经从技术手段、应用场景等方面做了一些调研工作，如文献[7-10]，但这些工作很少专门针对工业物联网的特性和适用性进行深入剖析。近两年，虽然出现了针对工业物联网异常检测的综述性文章，但介绍的都不够全面。例如，文献[2]只介绍了基于系统规则、建模系统物理状态的检测方法，文献[4]则只介绍了基于统计和机器学习的检测方法。除了文献[2,4]提到的检测方法之外，还存在许多新颖的检测技术。

因此，本文从技术原理的角度，梳理了基于系统不变性和物理状态的建模、基于统计学习、特征选择、机器学习、图、边缘/雾计算、指纹、生物免疫等算法的异常检测技术，并详细分析了各类技术的优缺点。由于用于工业异常检测研究的数据集繁杂且多样，本文详细归纳了常用数据集的特点及其使用频率，方便读者对比和选择。除此之外，本文针对工业物联网典型场景的网络威胁和异常检测方法进行调研和综述，介绍了边缘/雾计算方法在异常检测方面的应用，增加了对 2021 年最新论文的调研，对不同检测方法的特点和适用场景进行了深入分析。

1　工业物联网面临的安全威胁

工业 4.0 将信息通信技术应用于工业制造和自动化领域，极大地提高了生产力和效率。然而，这一进步的代价是扩大了工业系统的受攻击面。针对工业物联网的攻击，可以分为被动攻击和主动攻击。被动攻击是隐蔽的，通常无法检测到，如窃听和流量分析。主动攻击包括丢包、回注、干扰网络的正常运行等。恶意软件感染、拒绝服务（DoS, denial of service）、未授权访问和虚假数据包注入等主动攻击通常是可以检测到的[9]。下面简要总结几种主动攻击的特点和目标。

恶意包注入攻击。重放抓包，发送伪造或篡改的报文，以达到干扰或破坏系统操作的目的。

DoS 攻击。消耗系统或网络资源，导致资源不可用。

未授权访问攻击。探测计算机或网络以发现漏洞；对报文进行嗅探或拦截，用于收集信息。

除此之外，还涌现出了一些针对工业物联网典型场景的威胁。

物理攻击。例如针对交通运输物联网的物理攻击，对交通设备节点本身进行物理上的破坏，如断电、移动节点位置等，造成信息缺失、信息泄露等。

感知数据破坏。非授权地增删、修改或破坏感知数据，例如针对新能源发电厂的电力物联网生产数据篡改。

控制命令伪造攻击。发送伪造的控制命令，从而达到破坏系统或恶意利用系统的目的，例如针对数控机床设备物联网的控制命令伪造。

为了保护工业系统免受网络攻击，涌现出了各种安全措施，如加密通信数据、数据完整性校验和访问控制等方法，可以保护系统免受多种类型的攻击。然而，即使这些安全措施已经到位，攻击者仍然可以成功地对系统发起攻击，如恶意包注入和 DDoS 攻击等。因此，有必要对网络进行异常检测，以此来进一步保障工业系统的安全。

2　工业物联网异常检测

本节首先介绍了工业物联网中存在的异常种类，进而详细分析和梳理了现有的针对不同异常类别和不同应用场景的异常检测方法。

2.1　异常种类

网络攻击以损害系统信息的机密性、完整性和资源的可用性为目标，通常以某种方式造成网络运行偏离正常，表现出异常行为。因此，可以通过发现数据中不符合预期行为的模式来识别异常。现阶段 IIoT 中主要存在 3 种异常[8]。

点异常。即个别数据实例相对于其余数据是

异常的。例如，假设水温传感器值的预定义范围是 30℃～40℃，那么超出这个范围的值将是一个异常点。

上下文异常。仅在特定上下文中表现异常的数据实例称为上下文异常。这类异常多为空间数据或时序数据中的异常。

集合异常。如果相关数据实例的集合相对于整个数据集是异常的，则称为集合异常。集合异常中的单个数据实例本身可能不是异常，但它们一起作为一个集合出现就是异常。例如，单个 TCP 连接请求是正常的，但是连续从同一个源收到多个这种请求就有可能是 DoS 攻击，也就是异常。

网络异常检测是指检测网络流量数据中的异常，利用设备或软件应用程序对网络流量进行监控和分析，从而检测出恶意活动。现有工业物联网异常检测方法可以分为基于系统不变性、物理状态建模、统计学习、特征选择、机器学习、边缘/雾计算、图、指纹以及生物免疫等算法的检测方法。下面将针对每一种检测方法的技术原理、现有研究成果、优缺点及适用应用场景做介绍梳理和深入分析。

2.2 基于系统不变性的检测方法

系统不变性是指系统运行过程的“物理”或“化学”特性中的一个条件，每当系统处于给定状态时，必须满足该条件。通过分析物理不变性来检测异常已经被应用于许多网络信息物理系统（CPS, cyber-physical system）[11-14]。文献[11]将所有组件的稳定性和正确性约束以逻辑不变性的形式表示出来，系统动作只有在保证不违反这些不变性时才能执行。针对 CPS 各个模块的不变性，文献[12]提出了统一不变性，开发了跨越系统各个层面的公共语义。然而，文献[11-12]都是通过人工来产生物理不变性，开销很大，且很容易出错。为了解决这个问题，文献[13]提出利用关联规则挖掘算法自动识别系统不变性，该算法的优点是可以发现隐藏在设计布局中的不变性，避免了手动寻找的烦琐。但是，这项技术仅适用于成对出现的传感器和执行器，而在真实的 CPS 中，所有传感器和执行器都是跨多个过程协同工作的。也有一些使用机器学习算法来挖掘 CPS 物理不变性的研究。例如，Momtazpour 等[14]采用预先发现潜在变量的外源性输入自动回归模型，以发现多个时间步内无线传感器数据之间的不变性。Chen 等[15]利用代码变异程序生成异常数据轨迹，然后利用支持向量机（SVM, support vector machine）分类器和统计模型检验来发现安全水处理实验台传感器数据之间的不变性。文献[16]采用几种机器学习和数据挖掘技术的组合，系统地从工业控制系统（ICS, industrial control system）的操作日志以及执行器的状态信息生成不变性。

2.3 基于物理状态建模的检测方法

CPS 的底层过程一般由其工作原理控制，因此其过程状态是可预测的。基于物理模型的异常检测方法根据物理状态对正常的物理操作进行建模，从而能够从偏离物理操作模型的异常状态中检测到网络攻击。

文献[17]提出了一个 CPS 攻击弹性框架。该框架利用已知物理领域的数学描述，以及预测值和历史数据信息，验证预测值和测量值之间的相关性。文献[18]描述了如何使用流体动力学模型来检测供水网络的物理故障和网络攻击，并通过状态和测量方程以及未知输入来建模水系统。该模型能够反映传感器、执行器故障或漏水等异常事件对系统的影响，但仅依靠建模物理模型来检测网络攻击是不够的，如果传感器的测量值被破坏，则很难检测到攻击。为了识别攻击者利用系统漏洞，注入合法的恶意控制命令来破坏电网的行为，文献[19]提出结合电网物理基础设施知识和网络信息来检测攻击。该方法基于协议规范对数据包进行检测，提取其中的关键控制命令，并通过电力系统运行方程进行仿真运行。通过仿真，对执行控制命令所产生的系统状态进行估计，并与可信度量进行比较，从而识别攻击。文献[20]提出了一种针对电力领域的基于模型的异常检测算法。该算法验证了接收到的测量数据与控制底层物理系统运行的方程所获得的预测数据的一致性。文献[21]描述了一种基于模型的方法来保护智能电网。该方法基于系统状态动力学方程，评估系统状态，并与采集的测量值比较，检测出受损的测量值。文献[22]在一个水基础设施实验台上测试了基于控制理论建模的故障检测和基于网络安全的异常检测方法。结果表明，这 2 种方法都能有效地检测出故障和攻击，但存在一定的局限性。在物理故障和网络攻击同时进行的实验中，网络攻击者可以躲避控制理论建模方法的检测。因此，将物理动态建模方法中的状态估计与网络安全方法中的数据分析相结合，是提高 ICS 网络安全的关键。

2.4　基于统计学习的检测方法

基于统计的异常检测方法为数据集创建一个分布模型，并与目标数据对象相匹配。假设正常数据落在高概率区间，而异常数据相对落在低概率区间，根据目标数据集中数据落在模型中的概率来判断是否异常。Rajasegarar 等[23-24]建立了 2 种异常检测模型：统计检测模型和非参数检测模型。这 2 种模型可以应用于不同的场景，其中前者适用于数据类型和采样周期预先确定的应用；而后者在没有先验知识的情况下，通过比较当前数据和相邻数据的行为识别异常。费欢等[25]提出一种多源数据异常检测方法。该方法主要应用于平台空间，通过二维坐标的位置来确定 2 个节点之间的关系。类似地，文献[26]提出基于密度的模型，通过分析电数据来发现太阳能发电系统的异常行为。

另外，传感器数据的时间和频率属性能够为建立时频逻辑提供有价值的信息。时域信号（均值、标准差或方差等）可以描述有关系统行为的某些信息。例如，基于频率的信号特性（傅里叶变换、小波变换等）可以单独或结合时域特征来理解系统的行为[27]。工业系统复杂而广泛，大量的传感器被用于监控空间和物体，以为异常行为预测提供全面、多维度的运行数据。对于这种情况，基于相关性分析的方法[28]被证明可以更有效地识别异常。该方法能够反映系统的真实表现，因为这些相关性可以从物理上反映系统的运行机制和条件。表 1 列出了基于统计学习方法的异常检测在工业物联网中的应用。

2.5　基于特征选择的检测方法

异常检测处理的数据是人工从复杂的网络系统中提取出来的。这些数据一般具有高维、强冗余、低相关性等特点。直接使用原始数据，检测算法的性能会很差。而特征选择的作用是从原始数据中选择有用的特征，选出的特征具有更强的相关性、非冗余特性和更少的噪声。这些特征可以帮助相关算法更高效、快速地区分、检测和分类出不同的目标。因此许多研究者将其应用于入侵检测系统（IDS, intrusion detection system）的设计中，以提高检测精度，减少检测时间。

这些研究通常来自 2 种观点。一种是有效提取，如主成分分析（PCA, principal component analysis）。针对异常检测系统耗时长、性能下降等问题，文献[30]提出了一种混合的 PCA 神经网络算法。该算法利用 PCA 变换对特征降维，使训练时间减少约 40%，测试时间减少约 70%，同时还提高了检测精度。文献[31]基于核主成分分析和极限学习机（ELM, extreme learning machine）设计 IDS。其中，核主成分分析用于特征矩阵降维。实验结果表明，该系统比单纯基于 ELM 或者 SVM 算法的 IDS 效率更高，速度更快。类似地，文献[32]提出一种增量 ELM 与自适应 PCA 相结合的方法，该方法可以自适应地选择相关特征以获得更高的精度。然而，所有这些方法都没有减少原始数据的特征量，总的时间消耗仍然非常大。另一种是有效特征选择，如遗传算法和最大相关最小冗余算法。文献[33-34]将特征选择问题定义为组合优化问题，提出基于局部搜索最优解算法来选择有效的特征子集，用于检测“正常”和“DoS”攻击数据。虽然使用该算法选择出的有效特征子集在检测率和准确率方面都优于使用全部特征集，但也带来了较高的误报率。文献[35]提出了一种基于遗传算法的特征选择方法来设计 IDS 以选择最优特征，采用单点交叉而不是两点交叉优化该遗传算法的参数。总体而言，其给出了更好的结果，但在某些情况下分类率会下降。Feng 等[36]提出基于 K 近邻和树种子算法的 IDS 模型来选择特征，减少特征冗余，检测效率有所提升但准确率没有明显的改善。

表 1　　**基于统计学习方法的异常检测在工业物联网中的应用**

方法	数据性质	异常类型	可用的数据	传感器类型	应用领域	评价标准	被引用数
统计学习	连续型数据	点异常	温度、湿度、光照强度等数据	温度、湿度传感器等	野外监测	准确率和误报率	17
时序逻辑	连续型数据	点异常	在50个轨迹集合上进行监督学习	空压机电机转速	燃料电池车辆	误分类率	18
关联性分析	连续型数据	上下文异常	在 5 个机器数据上进行监督学习	发动机上的传感器	工厂里的发电机	相关性系数	36
密度函数模型	连续型数据	点异常	在24个太阳能面板数据上进行监督学习	电流数据	太阳能发电系统	ROC 曲线	6
马尔可夫链	连续型数据	点异常	在压力传感器数据上进行监督学习	压力传感器	石油管道	准确率	14

上述方法有一个共同的缺点，即选择的特征具有一定的随机性和不确定性，不能应用于下次选择。为了克服这个问题以及明确不同特征对异常检测的影响，文献[37]基于最大相关最小冗余特征选择算法和 SVM 分类方法进行了一系列实验。另外，为了进一步选取有效的特征，文献[38]结合群体智能算法和强化学习，提出了一个名叫 QBSO-FS 的特征选择模型，实验结果表明，该模型确实优于传统特征选择算法。工业系统中基于特征选择的异常检测方法对比如表 2 所示。

2.6 基于机器学习的检测方法

在工业系统中，机器学习方法（如贝叶斯网络、k-means、ELM[39]、SVM、回归等）已经被成功用于识别和检测工业物联网中的异常行为[10]。除此之外，聚类[40-42]、随机森林[43]、孤立森林[44]和隐马尔可夫模型[45]等算法也取得了不错的成绩。表 3 总结了工业系统中基于机器学习的异常检测方法。

单分类支持向量机（OCSVM, one class support vector machine）是一种非常著名的异常检测算法，被应用于许多应用领域中，它能够学习可见数据的边界，并将边界之外的所有事件或数据点识别为系统异常行为[43,46-47]。为了进一步提升 OCSVM 的性能，文献[48]采用云灰狼优化算法对 OCSVM 参数进行优化。实验结果表明，该算法在一定程度上确实提高了模型的检测精度。与文献[48]的工作不同，文献[49]提出 2 种将 OCSVM 扩展到张量空间的异常检测算法，即单分类支持塔克机和基于张量塔克分解以及遗传算法的遗传单分类支持塔克机。两者都是针对传感器大数据的无监督异常检测，保留了数据结构信息的同时，提高了检测的准确率和效率。

聚类方法以无监督的方式将特征相似的对象归为一组，经过这种自动分组后，如果新的数据点不能被放入预定义的集群（组）中，则系统会将该数据点判为异常情况并生成警报[40,42]。梯度提升树是一种集成学习分类器，文献[50]用其检测风力机螺栓断裂问题的早期异常。该算法首先生成多棵决策树，然后综合所有树的结果从而做出最终决策。梯度提升树有个令人不容忽视的缺点，即不能处理海量数据。为了解决这个问题，文献[51]提出结合轻量级梯度提升机和贝叶斯优化来检测工业网络流量中的异常。该方法在提高检测效率和准确率的同时，减少了人工对模型训

表 2 工业系统中基于特征选择的异常检测方法

方法	文献	使用的数据集	性能指标	被引次数
PCA-神经网络	文献[30]	NSL-KDD 数据集	训练时间、检测时间、检测到的记录数	126
KPCA+ELM	文献[31]	KDD Cup 99 数据集	准确率为 0.98，误报率为 0.02，检测时间为 0.75 ms	2
IELM+APCA	文献[32]	NSL-KDD 数据集	准确率为 0.81，检测时间为 19.97，误报率为 0.30	20
		UNSW-NB15 数据集	准确率为 0.70，检测时间为 476.19，误报率为 0.35	20
元启发式算法+k-means	文献[34]	NSL-KDD 数据集	准确率为 0.97，检测率为 0.96，误报率为 0.02	60
TSA+KNN	文献[36]	KDD Cup 99 数据集	准确率为 0.873 4	16
MRMR + SVM	文献[37]	UNSW-NB15 数据集	准确率为 0.699 6	0
		MSU 数据集	准确率为 0.956 7	0
QBSO-FS+机器学习	文献[38]	NSL-KDD 数据集	准确率、召回率	0

表 3 工业系统中基于机器学习的异常检测方法

方法	异常类型	实验数据	传感器类型	评价标准
ELM	点异常	燃烧室排气数据	温度传感器	ROC 曲线
多元聚类	上下文异常	真实的感知数据	来自电力、水和天然气系统的传感器数据	误分类率
聚类	上下文异常	在五层建筑物的非监督学习	温度传感器	错误警报
GBDT	上下文异常	风力涡轮机数据的监督学习	150 个风力涡轮机的测量参数	准确率
双重孤立森林+主成分分析	集合异常	安全水处理实验台和水分配试验台数据	压力传感器、红外传感器等	分类精度、召回率
OCSTuM+GA-OCSTuM	点异常	蒙特斯传感器数据集等	54 个不同种类的传感器	准确率

练的参与度。

然而，机器学习方法有以下 3 个局限性：1) 性能很大程度上依赖所采用的特征工程技术的稳健性，限制了稳定性；2) 应用于大规模高维数据时，性能会严重恶化；3) 学习能力不够强，无法应对工业物联网环境中数据（网络攻击）的动态性。

2.6.1 深度学习方法

深度学习（DL, deep learning）是一种具有自动学习能力的智能算法，是机器学习的一个分支。由于 DL 对任何特征工程的独立性、对动态环境的适应性以及强大的学习能力（特别是从高维数据中），其很快成为解决上述局限性的新的学习范式。各种各样的 DL 方法已经成功应用于异常和入侵检测，如卷积神经网络（CNN, convolutional neural network）[52-53]、循环神经网络（RNN, recurrent neural network）[54-56]、生成对抗网络（GAN, generative adversarial network）[57-59]、脉冲神经网络[60]、粒子深框架[61]和长短期记忆（LSTM, long short-term memory）网络[56,62-66]。Ferrag 等[53]对 CNN、RNN 和深度神经网络（DNN, deep neural network）进行了入侵检测研究，并对它们在不同配置下的性能进行了对比分析。Bhuvaneswari 等[67]在基于雾的物联网中引入向量卷积构建入侵检测系统。但是，CNN 有一个让人无法忽视的缺点，即无法学习物联网流量的长时依赖特征，而这正是 LSTM 网络的优势。因此，Saharkhizan 等[68]提出使用 LSTM 来学习时序数据之间的依赖关系。该研究使用一个 LSTM 集合作为检测器，将该检验器的输出合并成决策树，最终进行分类。

然而，这些模型的计算成本很高。为了解决这个问题，Liaqat 等[69]提出了一个整合 CNN 和 Cuda DNN LSTM 的方案，该方案能够及时有效地检测出医疗物联网环境中的复杂恶意僵尸网络。

文献[70]提出了一种压缩卷积变分自动编码器，用于 IIoT 中时间序列数据的异常检测。该方法减少了模型的大小和推理的时间，但是分类性能基本上没有提升。研究了卷积神经网络在工业控制系统异常检测的应用后，文献[52]提出了一种基于测量预测值与观测值的统计偏差的异常检测方法，并指出一维卷积网络在工业控制系统的异常检测方面优于循环神经网络。从网络包内容分析的角度出发，文献[66]提出了签名+LSTM 的多层异常检测方法。其首先开发了一个数据包的基准签名数据库，并用布鲁姆过滤器存储该签名数据库同时检测包异常，然后将该签名数据库作为数据源输入 LSTM 中，来进行时间序列的异常检测。为了保护集成电路免受网络攻击，文献[71]采用 2 种异常检测算法来做异常检测，一个是传统机器学习算法 k-means，另一个是卷积自编码算法，并取 2 种算法结果的逻辑与来作为最终的检测结果。但是该方法在特征选择时，没有采用专有的特征选择算法，仅仅通过人工过滤掉了不产生影响的属性。另外，为了保护 IIoT 系统免受勒索软件攻击，文献[72]提出了一种基于堆叠变分自编码的检测模型，该模型具有一个全连接神经网络，能够学习系统活动的潜在结构，并揭示勒索软件的行为。为了提高检测的准确率和降低出错率，文献[73]利用深度学习自编码器结合编码层的系数惩罚和重构损失来提取高维数据特征，然后使用极限学习机（ELM, extreme learning machine）对提取的特征进行快速有效的分类。文献[59]提出一种基于双向生成对抗网络（BiGAN, bidirectional-GAN）的 ICS 入侵检测策略。为了提高 BiGAN 模型在 ICS 入侵检测中的适应性，该研究通过单变量原理和交叉验证得到了最优模型。针对循环 DL 模型不能并行化且难以处理长流量序列的问题，文献[74]设计了基于取证的深度学习模型，该模型使用局部门控制循环单元学习局部特征，并引入多头注意力机制来捕获和学习全局表示（即长期依赖）。文献[75]设计了一个双向多特征层的长短时记忆网络。文献[76]基于深度随机神经网络设计了入侵检测方案，在训练过程中，其选择了数据集的 41 个最显著的特征。文献[77]提出了基于孪生卷积神经网络的少样本学习模型，以缓解 ICPS 中的过拟合问题，同时提高了智能异常检测的准确率。表 4 展示了工业系统中的基于深度学习的异常检测研究成果。

2.6.2 联邦学习方法

联邦学习是一种机器学习框架，能有效帮助多个机构在满足用户隐私保护、数据安全等要求下，进行数据使用和机器学习建模。近年来，为了在异常检测的过程中不泄露用户的隐私，联邦学习在工业物联网中的应用引起了学术界和产业界的极大兴趣。

为了保护用户的隐私数据，Liu 等[78]将联邦学习与深度异常检测相结合，建立具有 LSTM 的卷积

表 4　　**工业系统中的基于深度学习的异常检测研究成果**

方法	文献	使用的数据集	性能指标	被引用数
CNN	文献[52]	SWAT 数据集	精确率为 0.95，召回率为 0.79，F1 得分为 0.87	132
RNN+LSTM	文献[54]	网络流量包	均方差为 265.65，平均绝对误差为 3.23，R2 为 0.97	3
包签名+LSTM	文献[66]	Gas pipeline system 数据集	准确率为 0.92，精确率为 0.94，召回率为 0.78，F1 得分为 0.85	134
向量卷积深度学习	文献[67]	UNSW Bot-IoT 数据集	准确率为 0.99，精确率为 0.99，召回率为 0.99	11
LSTM	文献[68]	Modbus/TCP 网络流量数据集	准确率为 0.99，精确率为 0.99，召回率为 0.98，F1 得分为 0.99	16
CNN cuDNNLSTM	文献[69]	Bot-IoT 数据集	准确率为 0.99，精确率为 0.99，召回率为 0.99，F1 得分为 0.99，假阳率为 0.059	8
k-means + 卷积自动编码器	文献[71]	Gas pipeline system 数据集	准确率为 0.95，精确率为 0.95，召回率为 0.83，F1 得分为 0.89	5
		Water storage tank 数据集	准确率为 0.96，精确率为 0.93，召回率为 0.94，F1 得分为 0.93	5
堆叠变分神经网络	文献[72]	Windows 勒索软件数据集	准确率为 0.92，检测率为 0.99，假阳率为 0.139	7
自动编码器+极限学习机	文献[73]	Gas pipeline 数据集	准确率为 0.97，假阳率为 0.0035，ROC 为曲线	1
GRU+多头注意力	文献[74]	Bot-IoT 数据集	准确率为 0.98，F1 得分为 0.97，AUC 为 0.99	2
		UNSW_NB15 数据集	准确率为 0.99， F1 得分为 0.98，AUC 为 0.99	2
双向 LSTM	文献[75]	CTU-13 数据集	准确率为 0.95，检测率为 0.67，假阳率为 0.53，假阴率为 0.21	6
		AWID 数据集	准确率为 0.97，检测率为 0.83，假阳率为 0.20，假阴率为 0.602	6
深度随机神经网络	文献[76]	UNSW_NB15 数据集	准确率为 0.9954	4
孪生卷积神经网络	文献[77]	UNSW_NB15 数据集	精确率为 0.90，召回率为 0.96，F1 得分为 0.93，误报率为 0.047	21

神经网络模型，同时在联邦学习的过程中利用基于 Top-k 选择的梯度压缩机制降低通信代价以及提高通信质量。2021 年，Liu 等[79]在文献[78]的基础上引入注意力机制，进一步提高了异常检测的准确率。Li 等[80]基于卷积神经网络和门控递归单元设计了联邦深度学习方案。该方案允许多个工业 CPS 以隐私保护的方式共同构建一个综合性的入侵检测模型，并利用 Paillier 加密机制保护训练过程中模型参数的安全性和隐私性。值得一提的是，该模型仅适用于同域工业 CPS。文献[81]提出了一种联邦深度强化学习异常检测算法，即利用联邦学习技术，建立一个通用的异常检测模型，然后采用深度强化学习算法训练每个局部模型。由于联邦学习过程中不需要局部数据集，减少了隐私泄露的机会。此外，通过在异常检测设计中引入隐私泄露程度和动作关系，提高了检测精度。表 5 总结了联邦学习在工业异常检测中的研究成果。

2.7　基于边缘/雾计算的检测方法

深度神经网络的进展极大地支持异常物联网数据的实时检测。然而，由于计算能力和能源供应有限，物联网设备几乎负担不起复杂的深度神经网络模型。虽然可以将异常检测的任务转移到云上，但当数千个物联网设备同时将数据传到云上时，会导致时延和网络拥塞。

一种新兴架构——雾（边缘）计算的出现，解决了上述问题。该架构旨在通过将计算、通信、存储和分析等资源密集型功能转移到终端用户来减轻云和核心网络的网络负担。雾计算系统能够处理对时间要求严格的物联网的能源效率和时延敏感型应用，如工厂的火灾报警系统、地下采矿环境等，都需要快速检测出异常。因此，涌现出许多基于雾（边缘）计算的异常检测框架[82-84]。文献[85]针对数据异常检测的准确性和时效性，提出了一种基于层次边缘计算（HEC, hierarchical edge computing）模型的多源多维数据异常检测方案。该研究首先提出了 HEC 模型，来实现传感器端和基站端负载均衡和低时延数据处理；然后设计了一种基于模糊理论的单源数据异常检测算法，该算法能够综合分析多个连续时刻的异常检测结果。针对工业物联网终端设备中数据量大的问题，文献[86]先采用边缘计算对传感器数据进行压缩优化（即预处理），进而利用 k-means 聚类算法对处理后数据的离群值进行判断。

表 5　　联邦学习在工业异常检测中的研究成果

方法	文献	使用的数据集	性能指标	被引次数
联邦学习+CNN-LSTM	文献[78]	Power demand 数据集	准确率：约 0.94，均方根误差：约 3.8	6
		Statlog 数据集	准确率：约 0.93，均方根误差：约 4	6
联邦学习+注意力机制+CNN-LSTM	文献[79]	Power demand 数据集	准确率：约 0.97，均方根误差：约 3.7	32
		Statlog 数据集	准确率：约 0.95，均方根误差：约 3.75	32
联邦学习+CNN-GRU	文献[80]	Gas pipeline 数据集	精确率，召回率，F1 得分	26
联邦学习+深度强化学习	文献[81]	—	系统吞吐量，平均时延，准确率	4

然而，压缩技术会造成数据信息的损失，可能影响检测精度。因此，需要权衡好压缩率与检测精度的关系。

与文献[84-85]类似，文献[87]同样基于 HEC 提出了自适应异常检测方法。首先，构建了 3 个复杂度不断增加的 DNN 异常检测模型，并将其与 HEC 的三层（物联网设备、边缘服务器、云）自下而上关联。然后，根据输入数据的上下文信息自适应地选择合适的模型进行异常检测。表 6 展示了工业物联网中基于云计算、边缘计算和雾计算的异常检测方法。从表 6 中可以看出，虽然文献[87]的准确率和 F1 得分略低于文献[84]，但平均时延大幅度降低了。由此可知其必然是牺牲了部分的精度来获得较小的检测时延。

基于自适应图更新模型，文献[88]引入一种新的边缘计算环境中的异常检测方法。在云中心，利用深度学习模型对未知模式进行分类，根据分类结果定期更新特征图，不断地将分类结果传输到每个边缘节点，利用缓存暂时保存新出现的异常或正常模式，直到边缘节点接收到新的更新的特征图。

2.8　基于图的检测方法

基于图的异常检测在医疗保健、网络、金融和保险等各个领域都有应用。由于来自网络、电子邮件、电话等的数据相互依赖，使用图表检测异常变得越来越流行。文献[89]提出了一种基于知识图谱的工业物联网移动设备异常检测方法，并利用可视化技术对检测结果进行演示。具体地，作者使用优化后的基于频繁项集的数据挖掘算法对数据进行分析，使提出的方法能够准确地检测出不同类型的并发攻击。另外，作者还设计了可以将结果多维度可视化的异常告警模块，帮助非专业用户在工业领域充分了解网络安全情况。

文献[90-91]引入了一种新的基于图的异常检测方法，并将背景知识添加到传统图挖掘方法的评价指标中。背景知识以规则覆盖的形式添加，报告子结构实例覆盖了最终图的百分比。由于人们认为异常不会频繁出现，因此作者假定，通过为规则覆盖分配负权值，可以发现异常的子结构。该方法在不损失精度的同时，大大降低了检测时间。表 7 介绍了工业物联网中基于图的异常检测方法的研究成果。

2.9　基于指纹的检测方法

指纹识别技术被广泛应用在人们生活的方方面面，如企业考勤、智能小区等。另一方面，越来越多的无线智能设备被应用到 ICS 网络中，由于设备的计算和存储能力较弱，使用常规的加密方法和安全补丁来提高 ICS 网络中遗留设备的安全水平几乎是不可能的。因此，指纹识别技术的

表 6　　工业物联网中基于云计算、边缘计算和雾计算的异常检测方法

方法	文献	使用的数据集	性能指标	被引次数
HEC-自动编码器+LSTM	文献[84]	Power consumption 数据集	准确率为 0.99，F1 得分为 0.87，时延为 144.5 ms	2
		mHealth 数据集	准确率为 0.98，F1 得分为 0.97，时延为 674.87 ms	2
HEC-深度神经网络	文献[87]	Power consumption 数据集	准确率为 0.98，F1 得分为 0.83，时延为 16.28 ms	9
HEC-模糊理论	文献[85]	单个/多个传感器数据	准确率，算法执行时间，平均时延	11
边缘计算−深度学习	文献[88]	BaIoT、EI Nino 数据集	真阳率，假阳率，时耗	0

表 7　　工业物联网中基于图的异常检测方法的研究成果

方法	文献	使用的数据集	性能指标	被引次数
知识图谱−数据挖掘	文献[89]	UCSD 数据集	—	0
图−背景知识规则	文献[90]	KDD Cup 99 数据集	运行时间，内存占用	10
图−机器学习	文献[91]	SWAT 数据集	精确率为 0.86，召回率为 0.78，F1 得分为 0.82	64

高度成功吸引了许多安全领域研究者的目光。已经有许多人将指纹技术的思想运用到检测 ICS 网络的异常工作中。文献[92]提出 2 种设备类型指纹方法，来增强现有 ICS 环境下的入侵检测方法。方法 1 利用 ICS 网络的静态和低时延等特征建立设备指纹，方法 2 采用物理操作时间为每个设备类型开发一个唯一的签名。文献[93]提出了一种混合增强设备指纹的方法，利用程序流程的简单性和硬件配置的稳定性，通过过滤掉异常数据包，来实现 ICS 网络中的异常检测。为了消除对信号周期性的依赖，文献[94]设计了一种不考虑周期性的异构工业物联网设备指纹识别算法。该算法从信号传输的时间序列中提取模式，然后通过聚类得到的模式来学习设备的指纹。文献[95]提出一种称为过程倾斜的技术，该技术利用 ICS 过程中的小偏差（称为工艺（process）指纹）进行异常检测。表 8 展示了工业物联网中基于指纹的异常检测的研究成果。

2.10 基于生物免疫的检测方法

基于异常的入侵检测技术通常假阳性很高，这使一些学者将目光转向其他领域以寻求突破。人工免疫系统（AIS, artificial immune system）是一类生物启发计算方法，出现在 20 世纪 90 年代，连接了不同的领域，如免疫学、计算机科学和工程。

基于 AIS 的 IDS 通常被用作异常检测系统。文献[96]在生物免疫系统的启发下，提出了一种基于多智能体系统的入侵检测新模型，该模型集成在网络上的分布式代理行为中，以确保良好的入侵检测性能。文献[97]基于确定性树突细胞算法（DDCA, deterministic dendritic cell algorithm）设计了用于工业场景的入侵检测算法，该算法利用上下文与抗原之间的相关性作为异常检测的基础。DDCA 的分类性能很大程度上依赖于特征选择过程，高度相关的特征导致近似完美的分类，反之，相关性较差的特征在 DDCA 分类过程中会带来非常负面的影响。为了能够实时检测异常，文献[98]基于分层时间记忆网络，构建了在线序列记忆算法。该分层时间记忆网络不断学习和建模输入数据的时空特性，通过预测输入和实际输入之间的差异来更新其突触连接。学习发生在每个时间步，但由于表示非常稀疏，因此只有小部分突触被更新，大大节省了训练时间。

上文详细介绍了工业物联网领域的 9 种异常检测方法。为了更加直观地比较各种的算法，本文进而介绍了每种检测方法的优缺点以及现有研究成果，如表 9 所示。

3 公开的数据集

表 1～表 8 列举了对应技术下工业物联网中具有代表性的异常检测技术的研究，包括使用的数据集以及被引次数。统计表 1~表 8 中数据集出现的频率可以发现，研究者比较常用的数据集有 4 个，即 SWAT、NSL-KDD、UNSW-NB15 以及 KDD Cup 99 数据集。除此之外，还有许多优秀的数据集可用于异常检测的研究，这些数据集的详细信息如表 10 所示。

4 未来展望

工业物联网的安全是大趋势，随着终端设备存储和计算能力的增加，终端设备将来必然拥有独立的操作系统，安全问题随之而来。未来，终端的智能性、自主性、互联的依赖性都会增加，工业物联网的安全问题会越来越严重。这些安全问题之间也存在依赖性以及相互影响的问题，同时，工业物联网也可能作为危险的翘板，蔓延到其他领域，如互联网。因此，对工业物联网的异常检测势在必行。

从上文的分析中可以发现，针对工业物联网异常检测，机器学习和深度学习等算法应用较广泛；而基于雾计算、知识图谱、生物免疫、联邦学习等的研究则略显不足。

表 8 工业物联网中基于指纹的异常检测的研究成果

方法	文献	使用的数据集	性能指标	被引次数
指纹识别-贝叶斯算法	文献[92]	真实世界的变电站数据集	准确率为 0.92，精确率为 0.89，召回率为 0.95	135
指纹识别-机器学习	文献[93]	TCP/Modbus 流量	准确率	37
指纹识别	文献[94]	CAN 总线原型	准确率为 0.93，精确率为 0.92，召回率为 0.94，F1 得分为 0.92	2
指纹识别-CUSUM	文献[95]	SWAT 数据集	真阳率，假阳率	5

表 9　每种检测方法的优缺点以及现有研究成果

方法	优点	缺点	研究成果
系统不变性	一旦挖掘出系统不变性，只要是违反这些不变性的动作，都被认为是异常的；能够应对工业系统数据的动态性	不能发掘系统所有的不变性；适用性较差；不适合处理高维传感器数据	文献[11-16]
物理状态建模	一旦完成物理模型的构建，只要是偏离物理模型的操作，都被识别为异常；计算量小，时间复杂度低；为特定系统量身定做	不适合处理高维传感器数据；网络攻击者可以躲避控制理论建模方法的检测；构建模型需要专家知识；适用性较差	文献[17-22]
统计学习	一旦获得合适的概率分布模型，就能够有效识别异常；利用时间相关性可以检测出传感器的故障和异常值	由于通常没有以前的传感器数据分布知识，参数统计方法是没有好处的，而非参数统计模型不适用于数据密集的物联网在实时环境下的工作。通常，管理产生的多变量数据的计算成本很高	文献[23-29]
特征选择	筛选出强相关性的特征，降低数据的噪声和冗余性；能够处理高维传感器数据	需要通过人工选择或自动提取方式找到合适的特征，人工特征选择依赖专家经验，自动提取方式模型可解释性较差	文献[30-38]
机器学习	适用于物联网系统中不同传感器产生的各种类型的数据，有监督、半监督和无监督等多种学习方式	性能很大程度上依赖所采用的特征工程技术的稳健性；应用于大规模高维数据时，性能会严重恶化；学习能力不够强，无法应对工业物联网环境中数据（网络攻击）的动态性	文献[39-51]
深度学习	具有自动学习能力，且学习能力强大，可处理高维传感器数据；可应对物联网环境中数据（网络攻击）的动态性；不需要特征工程；实时检测异常	模型需要进行多次微调和模拟，才能在现实生活中投入使用；模型计算成本高，不适合资源不足的传感器；依赖大量标注数据	文献[52-73]
联邦学习	在多方数据源聚合的场景下协同训练全局最优模型，同时能够保护数据隐私，支持样本数量不足的情况	通信效率短板明显、隐私安全仍有缺陷、缺乏信任与激励机制	文献[78-81]
边缘/雾计算	减轻云和核心网络的网络负担；能够处理对时间要求严格的物联网的能源效率和时延敏感型应用	依赖网络传输、存在通信时延和隐私问题	文献[82-88]
图	能够学习多传感器数据之间的相互依赖；检测并发攻击	依赖图结构数据，需要构建数据之间的复杂关联，并且可能存在数据稀疏情况下的学习不平衡问题	文献[89-91]
指纹	通过建模 ICS 网络的静态和低时延特征或者信号传输的模式来建立设备的指纹，不符合该指纹模式的数据皆被识别为异常	不能应对工业网络数据的动态性；若系统特征少，则无法建立指纹	文献[92-95]
生物免疫	建立在精确数据模型或进化计算的基础上；数学模型简单，易于实现	功能不强，容易失真	文献[96-98]

表 10　工业物联网中用于异常检测的公共数据集

数据集	数据类型	正常实例数	异常实例数	特征数	通信协议	详情	被引次数
Bot-IoT 数据集	物联网网络流量	9 543	73 360 900	—	—	文献[56]	284
Smart grid 数据集	网络流量	470	391	14	DNP3	文献[98]	22
UNSW_NB15 数据集	网络流量	2 218 761	321 283	49	TCP,UDP,ICMP	文献[99]	992
SWAT 数据集	CPS 网络流量	15 000 000（未区分）		19	MODBUS	文献[101]	193
	物理属性	946 722（未区分）		51	—	—	—
NSL-KDD 数据集	网络流量	训练集：125 973，测试集：22 544（未区分）		41	TCP/IP	文献[102]	3 085
KDD Cup 99 数据集	网络流量	训练集：4 900 000，测试集：2 000 000（未区分）		41	TCP/IP	文献[102]	3 085
CTU-13 数据集	网络流量	59 190	21 760	11	HTTP	文献[103]	493
mHealth 数据集	多元时间序列	120（未区分）		23	—	文献[104]	227

在工业系统中，稳健的、性能良好的异常检测方法对于降低系统宕机的可能性至关重要。虽然当前已经存在许多研究成果，但是，仍然有许多值得研究的方向。

1) 可视化检测结果。当前的研究只关注异常检测方案本身，检测结果需要专业人士解读，不方便非专业人士阅读；另外，可视化结果还能帮助非专业人士在工业领域充分了解网络安全情况。

2) 混合架构。由于工业物联网数据具有大量、高维、强冗余、低相关性、环境噪声等复杂性，直接使用原始数据，模型的训练时间和检测性能都不容乐观。因此，将特征选择、知识图谱和深度学习等知识结合是一个趋势。一方面，特征选择算法能够选择强相关的特征，降低数据的冗余和噪声；另

一方面，深度学习由于其强大的自学习能力，能够精准地识别出异常。

3) 深度学习方法尚未涵盖多个领域，因此有必要重新审视不同领域异常检测的问题，如 SCADA、智能电网、5G 和众多物联网平台，这些平台已经存在传统机器学习等异常检测方法。对不同领域的可扩展性需要真正反映目标环境的数据集，才能取得更好的效果。

4) 一旦工业系统遭受攻击，将会造成严重的损失。因此，有必要在异常行为损害工业系统前，对可能发生的异常进行预测和警告，并提供预防性解决方案。

5　结束语

多年来，异常检测一直是一个活跃的研究领域，得到了各个应用领域研究者的广泛关注。识别异常行为可以降低功能风险，避免系统宕机和其他难以预料的问题。本文尽可能全面地搜集了现有工业物联网中异常检测的研究工作，按照实现原理的角度，对现有工业物联网中的异常检测方法进行了归类分析。这些信息可以帮助研究者对最新提出的异常检测算法及其概要信息产生宏观认知。另外，还需要进一步研究新的智能检测和预测技术，来实时处理复杂工业系统产生的各种数据流，做到实时健康态势感知、异常检测、风险预警和及时预防。

参考文献：

[1] DAUGHERTY P, BERTHON B. Winning with the industrial Internet of things: how to accelerate the journey to productivity and growth[R]. 2015.

[2] TANGE K, DONNO M D, FAFOUTIS X, et al. A systematic survey of industrial Internet of things security: requirements and fog computing opportunities[J]. IEEE Communications Surveys & Tutorials, 2020, 22(4): 2489-2520.

[3] SPOGNARDI A, DONNO M D, DRAGONI N, et al. Analysis of DDoS-capable IoT malwares[C]//Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, Annals of Computer Science and Information Systems. Piscataway: IEEE Press, 2017: 807-816.

[4] ZHOU L Y, GUO H Q. Anomaly detection methods for IIoT networks[C]//Proceedings of 2018 IEEE International Conference on Service Operations and Logistics, and Informatics. Piscataway: IEEE Press, 2018: 214-219.

[5] LANGNER R. Stuxnet: dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[6] LEE R. CRASHOVERRIDE: analysis of the threat to electric grid operations[R]. 2017.

[7] BUCZAK A L, GUVEN E. A survey of data mining and machine learning methods for cyber security intrusion detection[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2): 1153-1176.

[8] CHANDOLA V, BANERJEE A, KUMAR V. Anomaly detection[J]. ACM Computing Surveys, 2009, 41(3): 1-58.

[9] BHUYAN M H, BHATTACHARYYA D K, KALITA J K. Network anomaly detection: methods, systems and tools[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 303-336.

[10] GARCÍA-TEODORO P, DÍAZ-VERDEJO J, MACIÁ-FERNÁNDEZ G, et al. Anomaly-based network intrusion detection: techniques, systems and challenges[J]. Computers & Security, 2009, 28(1/2): 18-28.

[11] CHOUDHARI A, RAMAPRASAD H, PAUL T, et al. Stability of a cyber-physical smart grid system using cooperating invariants[C]// Proceedings of 2013 IEEE 37th Annual Computer Software and Applications Conference. Piscataway: IEEE Press, 2013: 760-769.

[12] PAUL T, KIMBALL J W, ZAWODNIOK M, et al. Unified invariants for cyber-physical switched system stability[J]. IEEE Transactions on Smart Grid, 2014, 5(1): 112-120.

[13] PAL K, ADEPU S, GOH J. Effectiveness of association rules mining for invariants generation in cyber-physical systems[C]//Proceedings of 2017 IEEE 18th International Symposium on High Assurance Systems Engineering. Piscataway: IEEE Press, 2017: 124-127.

[14] MOMTAZPOUR M, ZHANG J H, RAHMAN S, et al. Analyzing invariants in cyber-physical systems using latent factor regression[C]//Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2015: 2009-2018.

[15] CHEN Y Q, POSKITT C M, SUN J. Learning from mutants: using code mutation to learn and monitor invariants of a cyber-physical system[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2018: 648-660.

[16] FENG C, PALLETI V R, MATHUR A, et al. A systematic framework to generate invariants for anomaly detection in industrial control systems[C]//Proceedings of 2019 Network and Distributed System Security Symposium. Reston: Internet Society, 2019: 1-15.

[17] ASHOK A, GOVINDARASU M, WANG J H. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid[J]. Proceedings of the IEEE, 2017, 105(7): 1389-1407.

[18] AMIN S, LITRICO X, SASTRY S S, et al. Cyber security of water SCADA systems—part II: attack detection using enhanced hydrodynamic models[J]. IEEE Transactions on Control Systems Technology, 2013, 21(5): 1679-1693.

[19] LIN H, SLAGELL A, KALBARCZYK Z, et al. Semantic security analysis of SCADA networks to detect malicious control commands in power grids[C]//Proceedings of the First ACM Workshop on Smart Energy Grid Security. New York: ACM Press, 2013: 29-34.

[20] SRIDHAR S, GOVINDARASU M. Model-based attack detection and mitigation for automatic generation control[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 580-591.

[21] MO Y L, KIM T H J, BRANCIK K, et al. Cyber–physical security of a

smart grid infrastructure[J]. Proceedings of the IEEE, 2012, 100(1): 195-209.

[22] ETCHEVÉS M E, SETOLA R, BERNIERI G, et al. Fault diagnosis and network anomaly detection in water infrastructures[J]. IEEE Design & Test, 2017, 34(4): 44-51.

[23] RAJASEGARAR S, LECKIE C, PALANISWAMI M. Anomaly detection in wireless sensor networks[J]. IEEE Wireless Communications, 2008, 15(4): 34-40.

[24] RAJASEGARAR S, LECKIE C, PALANISWAMI M. Detecting data anomalies in wireless sensor networks[M]. Singapore: World Scientific, 2009.

[25] 费欢, 肖甫, 李光辉, 等. 基于多模态数据流的无线传感器网络异常检测方法[J]. 计算机学报, 2017, 40(8): 1829-1842.
FEI H, XIAO F, LI G H, et al. An anomaly detection method of wireless sensor network based on multi-modals data stream[J]. Chinese Journal of Computers, 2017, 40(8): 1829-1842.

[26] AKIYAMA Y, KASAI Y J, IWATA M, et al. Anomaly detection of solar power generation systems based on the normalization of the amount of generated electricity[C]//Proceedings of 2015 IEEE 29th International Conference on Advanced Information Networking and Applications. Piscataway: IEEE Press, 2015: 294-301.

[27] NGUYEN L V, KAPINSKI J, JIN X Q, et al. Abnormal data classification using time-frequency temporal logic[C]//Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control. New York: ACM Press, 2017: 237-242.

[28] ZHAO P S, KURIHARA M, TANAKA J, et al. Advanced correlation-based anomaly detection method for predictive maintenance[C]//Proceedings of 2017 IEEE International Conference on Prognostics and Health Management. Piscataway: IEEE Press, 2017: 78-83.

[29] ZANG D, LIU J H, WANG H Z. Markov chain-based feature extraction for anomaly detection in time series and its industrial application[C]//Proceedings of 2018 Chinese Control and Decision Conference (CCDC). Piscataway: IEEE Press, 2018: 1059-1063.

[30] LAKHINA M, SINI J, BHUPENDRA V. Feature reduction using principal component analysis for effective anomaly–based intrusion detection on NSL-KDD[J]. International Journal of Engineering Science and Technology, 2010, 2(6): 1790-1799.

[31] ZHOU Y, YU L, LIU M S, et al. Network intrusion detection based on Kernel principal component analysis and extreme learning machine[C]//Proceedings of 2018 IEEE 18th International Conference on Communication Technology. Piscataway: IEEE Press, 2018: 860-864.

[32] GAO J L, CHAI S C, ZHANG B H, et al. Research on network intrusion detection based on incremental extreme learning machine and adaptive principal component analysis[J]. Energies, 2019, 12(7): 1223.

[33] KANG S H. A feature selection algorithm to find optimal feature subsets for detecting DoS attacks[C]//Proceedings of 2015 5th International Conference on IT Convergence and Security (ICITCS). Piscataway: IEEE Press, 2015: 1-3.

[34] KANG S H, KIM K J. A feature selection approach to find optimal feature subsets for the network intrusion detection system[J]. Cluster Computing, 2016, 19(1): 325-333.

[35] FERRIYAN A, THAMRIN A H, TAKEDA K, et al. Feature selection using genetic algorithm to improve classification in network intrusion detection system[C]//Proceedings of 2017 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC). Piscataway: IEEE Press, 2017: 46-49.

[36] CHEN F, YE Z W, WANG C Z, et al. A feature selection approach for network intrusion detection based on tree-seed algorithm and K-nearest neighbor[C]//Proceedings of 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems. Piscataway: IEEE Press, 2018: 68-72.

[37] ZHANG X Y, LI J, ZHANG D J, et al. Research on feature selection for cyber attack detection in industrial Internet of things[C]// Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies. New York: ACM Press, 2020: 256-262.

[38] CHENG X X, LI W, XIAO Z, et al. Intrusion detection system based on QBSO-FS[C]//Proceedings of 2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE). Piscataway: IEEE Press, 2020: 372-377.

[39] YAN W Z. One-class extreme learning machines for gas turbine combustor anomaly detection[C]//Proceedings of 2016 International Joint Conference on Neural Networks (IJCNN). Piscataway: IEEE Press, 2016: 2909-2914.

[40] NARAYANASWAMY B, BALAJI B, GUPTA R, et al. Data driven investigation of faults in HVAC systems with model, cluster and compare (MCC)[C]//Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings. New York: ACM Press, 2014: 50-59.

[41] HAYES M A, CAPRETZ M A M. Contextual anomaly detection in big sensor data[C]//Proceedings of 2014 IEEE International Congress on Big Data. Piscataway: IEEE Press, 2014: 64-71.

[42] FU L D, ZHANG W B, TAN X B, et al. An algorithm for detection of traffic attribute exceptions based on cluster algorithm in industrial Internet of things[J]. IEEE Access, 2021, 9: 53370-53378.

[43] TAMY S, BELHADAOUI H, RABBAH M A, et al. An evaluation of machine learning algorithms to detect attacks in SCADA network[C]//Proceedings of 2019 7th Mediterranean Congress of Telecommunications (CMT). Piscataway: IEEE Press, 2019: 1-5.

[44] ELNOUR M, MESKIN N, KHAN K, et al. A dual-isolation- forests-based attack detection framework for industrial control systems[J]. IEEE Access, 2020, 8: 36639-36651.

[45] ALSHAMMARI A, ZOHDY M A. Internet of things attacks detection and classification using tiered hidden Markov model[C]//Proceedings of the 2019 8th International Conference on Software and Computer Applications. New York: ACM Press, 2019: 550-554.

[46] CARINO J A, ZURITA D, PICOT A, et al. Novelty detection methodology based on multi-modal one-class support vector machine[C]//Proceedings of 2015 IEEE 10th International Symposium on Diagnostics for Electrical Machines, Power Electronics and Drives. Piscataway: IEEE Press, 2015: 184-190.

[47] LEE S, YOO H, SEO J, et al. Packet diversity-based anomaly detection system with OCSVM and representative model[C]//Proceedings of 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data. Piscataway: IEEE Press, 2016: 498-503.

[48] YANG H H, ZHOU Z P. A novel intrusion detection scheme using cloud grey wolf optimizer[C]//Proceedings of 2018 37th Chinese Control Conference (CCC). Piscataway: IEEE Press, 2018: 8297-8302.

[49] DENG X W, JIANG P, PENG X N, et al. An intelligent outlier detection method with one class support tucker machine and genetic algorithm toward big sensor data in Internet of things[J]. IEEE Transactions on Industrial Electronics, 2019, 66(6): 4672-4683.

[50] WU C W, CHEN M. Early anomaly detection in wind turbine bolts breaking problem—methodology and application[C]//Proceedings of 2018 IEEE 3rd International Conference on Big Data Analysis. Piscataway: IEEE Press, 2018: 402-406.

[51] WANG B, LI M X, SHU F, et al. Bayesian-based industrial Internet service abnormal detection algorithm[C]//Proceedings of the 2nd International Conference on Information Technologies and Electrical Engineering. New York: ACM Press, 2019: 1-4.

[52] KRAVCHIK M, SHABTAI A. Detecting cyber attacks in industrial control systems using convolutional neural networks[C]//Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy. New York: ACM Press, 2018: 72-83.

[53] FERRAG M A, MAGLARAS L, MOSCHOYIANNIS S, et al. Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study[J]. Journal of Information Security and Applications, 2020, 50: 102419.

[54] PARK S H, PARK H J, CHOI Y J. RNN-based prediction for network intrusion detection[C]//Proceedings of 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Piscataway: IEEE Press, 2020: 572-574.

[55] GOH J, ADEPU S, TAN M, et al. Anomaly detection in cyber physical systems using recurrent neural networks[C]//Proceedings of 2017 IEEE 18th International Symposium on High Assurance Systems Engineering. Piscataway: IEEE Press, 2017: 140-145.

[56] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E, et al. Towards the development of realistic botnet dataset in the Internet of things for network forensic analytics: Bot-IoT dataset[J]. Future Generation Computer Systems, 2019, 100: 779-796.

[57] FREITAS D A P, KADDOUM G, CAMPELO D R, et al. Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment[J]. IEEE Internet of Things Journal, 2021, 8(8): 6247-6256.

[58] ZHOU P. Payload-based anomaly detection for industrial Internet using encoder assisted GAN[C]//Proceedings of 2020 IEEE 6th International Conference on Computer and Communications. Piscataway: IEEE Press, 2020: 669-673.

[59] LIU H P, ZHOU Z P, ZHANG M. Application of optimized bidirectional generative adversarial network in ICS intrusion detection[C]//Proceedings of 2020 Chinese Control and Decision Conference (CCDC). Piscataway: IEEE Press, 2020: 3009-3014.

[60] IBITOYE O, SHAFIQ O, MATRAWY A. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks[C]//Proceedings of 2019 IEEE Global Communications Conference. Piscataway: IEEE Press, 2019: 1-6.

[61] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E. A new network forensic framework based on deep learning for Internet of things networks: a particle deep framework[J]. Future Generation Computer Systems, 2020, 110: 91-106.

[62] ZHOU X K, HU Y Y, LIANG W, et al. Variational LSTM enhanced anomaly detection for industrial big data[J]. IEEE Transactions on Industrial Informatics, 2020, 17(5): 3469-3477.

[63] KONG F H, LI J Q, JIANG B, et al. Integrated generative model for industrial anomaly detection via Bi-directional LSTM and attention mechanism[J]. IEEE Transactions on Industrial Informatics, 2021, PP(99): 1.

[64] WU D, JIANG Z K, XIE X F, et al. LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2020, 16(8): 5244-5253.

[65] ROY B, CHEUNG H. A deep learning approach for intrusion detection in Internet of things using Bi-directional long short-term memory recurrent neural network[C]//Proceedings of 2018 28th International Telecommunication Networks and Applications Conference (ITNAC). Piscataway: IEEE Press, 2018: 1-6.

[66] FENG C, LI T T, CHANA D. Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks[C]//Proceedings of 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2017: 261-272.

[67] BHUVANESWARI A, SELVAKUMAR S. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment[J]. Future Generation Computer Systems, 2020, 113: 255-265.

[68] SAHARKHIZAN M, AZMOODEH A, DEHGHANTANHA A, et al. An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic[J]. IEEE Internet of Things Journal, 2020, 7(9): 8852-8859.

[69] LIAQAT S, AKHUNZADA A, SHAIKH F S, et al. SDN orchestration to combat evolving cyber threats in Internet of medical things (IoMT)[J]. Computer Communications, 2020, 160: 697-705.

[70] KIM D, YANG H, CHUNG M, et al. Squeezed convolutional variational autoencoder for unsupervised anomaly detection in edge device industrial Internet of things[C]//Proceedings of 2018 International Conference on Information and Computer Technologies (ICICT). Piscataway: IEEE Press, 2018: 67-71.

[71] CHANG C P, HSU W C, LIAO I. Anomaly detection for industrial control systems using k-means and convolutional autoencoder[C]//Proceedings of 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). Piscataway: IEEE Press, 2019: 1-6.

[72] AL-HAWAWREH M, SITNIKOVA E. Industrial Internet of things based ransomware detection using stacked variational neural network[C]//Proceedings of the 3rd International Conference on Big Data and Internet of Things. New York: ACM Press, 2019: 126-130.

[73] LI Y Z, LI Y, ZHANG S P. Intrusion detection algorithm based on deep learning for industrial control networks[C]//Proceedings of the 2019 2nd International Conference on Robotics, Control and Automation Engineering. New York: ACM Press, 2019: 40-44.

[74] ABDEL-BASSET M, CHANG V, HAWASH H, et al. Deep-IFS: intrusion detection approach for industrial Internet of things traffic in fog environment[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7704-7715.

[75] LI X H, XU M F, VIJAYAKUMAR P, et al. Detection of low-frequency and multi-stage attacks in industrial Internet of things[J]. IEEE Transactions on Vehicular Technology, 2020, 69(8): 8820-8831.

[76] LATIF S, IDREES Z, ZOU Z, et al. DRaNN: a deep random neural network model for intrusion detection in industrial IoT[C]//Proceedings of 2020 International Conference on UK-China Emerging Technologies (UCET). Piscataway: IEEE Press, 2020: 1-4.

[77] ZHOU X K, LIANG W, SHIMIZU S, et al. Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2020, 17(8): 5790-5798.

[78] LIU Y, KUMAR N, XIONG Z H, et al. Communication-efficient federated learning for anomaly detection in industrial Internet of things[C]//Proceedings of 2020 IEEE Global Communications Conference. Piscataway: IEEE Press, 2020: 1-6.

[79] LIU Y, GARG S, NIE J T, et al. Deep anomaly detection for time-series data in industrial IoT: a communication-efficient on-device federated learning approach[J]. IEEE Internet of Things Journal, 2021, 8(8): 6348-6358.

[80] LI B B, WU Y H, SONG J R, et al. DeepFed: federated deep learning for intrusion detection in industrial cyber–physical systems[J]. IEEE Transactions on Industrial Informatics, 2021, 17(8): 5615-5624.

[81] WANG X D, GARG S, LIN H, et al. Towards accurate anomaly detection in industrial Internet-of-things using hierarchical federated learning[J]. IEEE Internet of Things Journal, 2021, PP(99): 1.

[82] LA Q D, NGO M V, DINH T Q, et al. Enabling intelligence in fog computing to achieve energy and latency reduction[J]. Digital Communications and Networks, 2019, 5(1): 3-9.

[83] CHEN Z, HU W L, WANG J J, et al. An empirical study of latency in an emerging class of edge computing applications for wearable cognitive assistance[C]//Proceedings of the Second ACM/IEEE Symposium on Edge Computing. New York: ACM Press, 2017: 1-14.

[84] NGO M V, LUO T, CHAOUCHI H, et al. Contextual-bandit anomaly detection for IoT data in distributed hierarchical edge computing[C]//Proceedings of 2020 IEEE 40th International Conference on Distributed Computing Systems. Piscataway: IEEE Press, 2020: 1227-1230.

[85] PENG Y H, TAN A P, WU J J, et al. Hierarchical edge computing: a novel multi-source multi-dimensional data anomaly detection scheme for industrial Internet of things[J]. IEEE Access, 2019, 7: 111257-111270.

[86] KONG D Q, LIU D S, ZHANG L, et al. Sensor anomaly detection in the industrial Internet of things based on edge computing[J]. Turkish Journal of Electrical Engineering & Computer Sciences, 2020, 28(1): 331-346.

[87] NGO M V, CHAOUCHI H, LUO T, et al. Adaptive anomaly detection for IoT data in hierarchical edge computing[J]. arXiv Preprint, arXiv: 2001.03314, 2020.

[88] YU X, SHAN C, BIAN J L, et al. AdaGUM: an adaptive graph updating model-based anomaly detection method for edge computing environment[J]. Security and Communication Networks, 2021, 2021: 9954951.

[89] MA G, GU W X, HUANG Q Y, et al. Anomaly detection for mobile devices in industrial Internet[C]//Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers. New York: ACM Press, 2020: 75-77.

[90] VELAMPALLI S, EBERLE W. Novel graph based anomaly detection using background knowledge[C]//Proceedings of the Thirtieth International Florida Artificial Intelligence Research Society Conference(FLAIRS). New York: ACM Press, 2017: 538-543.

[91] LIN Q, ADEPU S, VERWER S, et al. TABOR: a graphical model-based approach for anomaly detection in industrial control systems[C]//Proceedings of the 2018 on Asia Conference on Computer and Communications Security. New York: ACM Press, 2018: 525-536.

[92] FORMBY D, SRINIVASAN P, LEONARD A, et al. Who's in control of your control system? device fingerprinting for cyber-physical systems[C]//Proceedings of 2016 Network and Distributed System Security Symposium. Reston: Internet Society, 2016: 1-15.

[93] SHEN C, LIU C, TAN H L, et al. Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks[J]. IEEE Wireless Communications, 2018, 25(6): 26-31.

[94] CHEN Y F, HU W T, ALAM M, et al. Fiden: intelligent fingerprint learning for attacker identification in the industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2021, 17(2): 882-890.

[95] AHMED C M, PRAKASH J, QADEER R, et al. Process skew: fingerprinting the process for anomaly detection in industrial control systems[C]//Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. New York: ACM Press, 2020: 219-230.

[96] BENYETTOU N, BENYETTOU A, RODIN V. The cooperation of immune agents for intrusion detection system[C]//Proceedings of the 2017 International Conference on Industrial Design Engineering. New York: ACM Press, 2017: 133-137.

[97] PINTO R, GONCALVES G, TOVAR E, et al. Attack detection in cyber-physical production systems using the deterministic dendritic cell algorithm[C]//Proceedings of 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). Piscataway: IEEE Press, 2020: 1-8.

[98] AHMAD S, LAVIN A, PURDY S, et al. Unsupervised real-time anomaly detection for streaming data[J]. Neurocomputing, 2017, 262: 134-147.

[99] IGBE O, DARWISH I, SAADAWI T. Deterministic dendritic cell algorithm application to smart grid cyber-attack detection[C]//Proceedings of 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). Piscataway: IEEE Press, 2017: 199-204.

[100] MOUSTAFA N, SLAY J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)[C]//Proceedings of 2015 Military Communications and Information Systems Conference (MilCIS). Piscataway: IEEE Press, 2015: 1-6.

[101] GOH J, ADEPU S, JUNEJO K N, et al. A dataset to support research in the design of secure water treatment systems[C]//International Conference on Critical Information Infrastructures Security. Berlin: Springer, 2016: 88-99.

[102] TAVALLAEE M, BAGHERI E, LU W, et al. A detailed analysis of the KDD Cup 99 data set[C]//Proceedings of 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. Piscataway: IEEE Press, 2009: 1-6.

[103] GARCÍA S, GRILL M, STIBOREK J, et al. An empirical comparison of botnet detection methods[J]. Computers & Security, 2014, 45: 100-123.

[104] BANOS O, GARCIA R, HOLGADO-TERRIZA J A, et al. mHealthDroid: a novel framework for agile development of mobile health applications[C]//International Workshop on Ambient Assisted Living. Berlin: Springer, 2014: 91-98.

[作者简介]

孙海丽（1991− ），女，湖北武汉人，华中科技大学博士生，主要研究方向为工业物联网安全、入侵检测与预防、隐私保护、恶意行为识别等。

龙翔（1973− ），男，湖北武汉人，华中科技大学博士生，湖北生物科技职业学院副教授，主要研究方向为网络空间安全、网络虚拟化、网络空间安全仿真等。

韩兰胜（1972− ），男，湖北武汉人，华中科技大学教授、博士生导师，主要研究方向为网络安全、大数据安全、软件安全、恶意代码、移动终端安全等。

黄炎（1988− ），男，湖北武汉人，华中科技大学博士生，主要研究方向为网络功能虚拟化、人工智能安全、知识图谱等。

李清波（1998− ），女，江西宜春人，华中科技大学硕士生，主要研究方向为移动终端安全、隐私保护等。