ISSN 2096-0581
CN 10-1315/TP

ntelligent Manufacturing®

智能制造

I N E N G Z H I Z A O

智能制造全媒体平台 · 智造成就工业之美

4 /2022
www.idnovo.com.cn
2022 年第 4 期 8 月 17 日出版
总第 312 期

微信视频号　微信公众号

研究院主办 | 原《CAD/CAM 与制造业信息化》杂志

国家制造强国建设战略咨询委员会智能制造专家委员会指导

本期主题：典型行业数字化转型实践

IM Intelligent Manufacturing
智能制造
ZHINENG ZHIZAO
智能制造全媒体平台 · 智造成就工业之美
2022年第4期 总第312期
1994年创刊/双月刊 2022年8月17日出版

CONTENTS 目次

主题策划 THEME PLAN

新闻资讯 | Information

专家视点 | Expert View

特别报道 | Special Report

专栏 · 试点示范 | Special Column

智能装备 | Intelligent Equipment

软件应用 | Software Application

智能工厂 | Intelligent Factory

智慧物流 | Intelligent Logistics

新技术新应用 | New Technology &New Application

人才培养 | Talent Development

工业控制系统自动异常检测方法的应用综述

刘汝芳，姜亚光，王　端，林　昕，高慧芳

（中国软件评测中心（工业和信息化部软件与集成电路促进中心），北京 100084）

摘要：传统的工业控制系统不同于互联网开放的体系，而是个体封闭的。但是随着工业互联网平台的应用，越来越多的设备连接到企业网络，从而引发了越来越多的网络安全问题。传统采用网络流量的方法，出现了异常检测困难、难以检测APT等动态威胁、检测结果不准确等问题。本文列举了国内外众多厂商和研究学者在工业控制系统异常检测方法的研究和应用情况，并分析其优缺点，为工业控制系统自动异常检测方法的选择提供依据。

关键字：工业控制系统；异常检测；深度学习算法；综述

1　引言

典型工业控制系统（Industrial Control System，ICS）架构的Purdue模型[1-2]如图1所示。

该架构模型为工业互联网平台互连信息技术（Internet Technology，IT）和操作技术（Operation Transformation，OT）设备提供了六个级别：0级，传感器和执行器等现场设备；1级，可编程逻辑控制器（PLC）等本地控制器；2级，监控和数据采集（SCADA）组件和分布式控制系统（DCSs）；3级，控制中心和处理局域网；4级和5级，企业区。2级SCADA系统用于关键基础设施的高级监控和管理。DCS是分布式网络的控制设备，是一个或多个工业过程的一部分。PLC是与物理设备交互的早期控制系统，他们通过反馈控制设备（如传感器和执行器）对正在运行的过程进行本地管理。

随着工业互联网技术的发展，越来越多的ICS设备连接到公司传统信息网络中，便于用户来远程访问，统筹规划。然而，这将工业控制系统暴露在互联网之下，使其容易受到网络攻击。研究表明，近年来有记录的针对工业控制基础设施的攻击数量急剧增加[2]，导致用户对工业控制系统安全性的关注日益增长。高级工控系统攻击可能会危及工业基础设施，因此，工业设备的恶意活动可能会反映在不同的工控系统数据源中，如网络流量（从基于以太网的组件捕获）和设备日志。

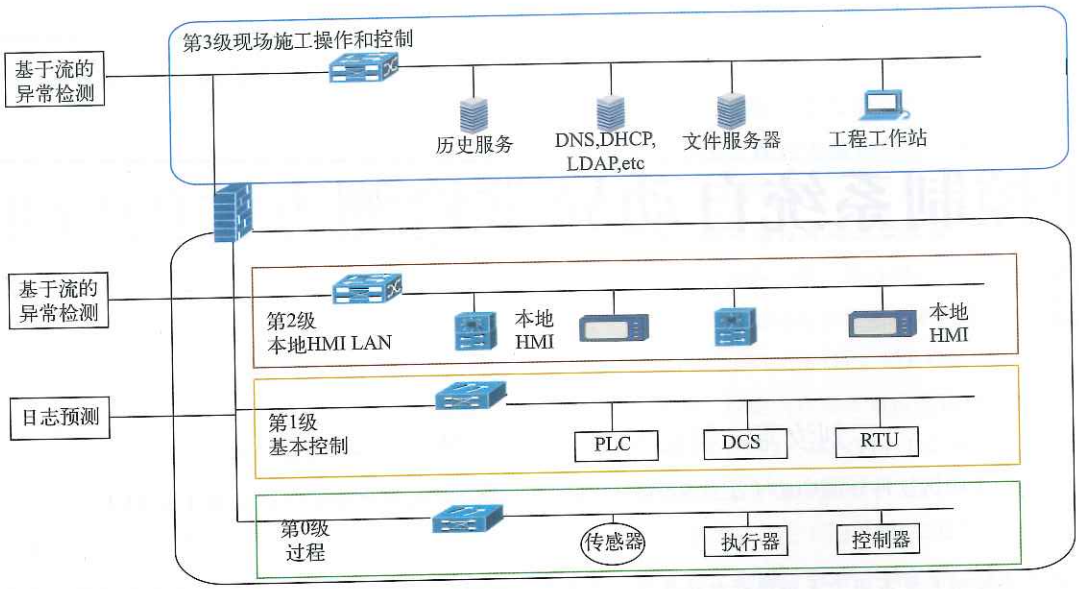

图 1 工业网络的安全 Purdue 模型

2 工控网络检测现状

监控 ICS 网络中的所有数据源有助于安全分析师尽早地检测到攻击，避免造成不可挽回的损失。然而，过去几年中提出的大多数异常检测方法都是基于工业控制系统结构局部分析的[5-7]，并且这类检测方法并不适用于具有不同类型数据源的大规模和多级工业控制网络。因此，许多学者和企业开始研究针对全局和多维度的工控网络的检测方法，如成分分析法[6]。然而，这类研究多是针对单一类型数据源进行异常检测，通过不同算法的优化，来提升工控设备异常检测的准确性[8-10]。

此外，针对 IT 和 ICS 网络中的 APT 攻击导致的异常检测也是工业控制系统自动异常检测方法的一个研究热点[11-13]。APT 攻击具有动态行为特征，具备一定的随机性，他们遵循不同的攻击技术和策略来达到他们的目标。基于攻击特征的异常检测方法是一种专门针对 APT 攻击的检测方法。但经验证，该检测方法对于 0-day 漏洞仍是无效的[14]。在这种情况下，采用一种耦合相关性分析和因果关系分析[12]的检测方法来进行异常检测。该方法要求对网络进行切片化处理，每层网络预先存入异常检测策略，虽然这些方法来检测 APT 攻击，但是大多数研究假设网络已经在每个层中预先存在入侵检测策略，以时间为函数进行关联安全和非安全日志来可视化攻击者的路径并预测未来的行动[11-14]。

3 工控安全异常检测中的常用方法

目前国内外在工业控制系统异常检测方法主要分为三种：第一种是基于深度学习算法的异常检测方法，结合工业控制网络自身的时序特性，其中最为常用的是无监督学习的非线性时间序列“ARIMA+GARCH”混合模型；第二种方法是基于多层网络流量的异常检测方法，其结合工业控制系统的工业过程进行分层，并基于有效负载的分析和基于报文头数据的分析；第三种是耦合深度学习算法的多层网络流量的异常检测方法。随着深度学习算法的不断优化，工业互联网促进工业控制数据多源融合，该类方法必将成为主要的工业控制系统异常检测的方法。

3.1 基于深度学习算法的异常检测方法

监督学习是深度学习算法中最为常见的一种，也是对应算法模型最多的。虽然异常检测中的监督学习方法可以提供更高的异常检测精度[14-15]，但该类方法的数据标记过程非常烦琐和耗时，因此，对于现实世界中的多源异构的复杂工业控制系统并不实用。因此，一般采用无监督的方法进行对工业控制系统实现自动异常检测。例如，在 Oliveira 等人的多层工业控制系统异常检测方法中，第一层是用于识别恶意网络流记录的无监督聚类方法；第二层是基于物理设备的行为模式分析。其采用的算法模型 ARIMA/GARCH，用于创建正常行为模型和预测未来值[11]。在其模型中实际值与预测值的任何偏差都

被视为异常，即当前工业控制系统遭受攻击。

实际上，基于深度学习算法的异常检测方法中，多数都采用非线性时间序列“ARIMA+GARCH”模型用于从相关变量预测 PLC 日志的预期未来值。因为该模型很好地耦合了 ARIMA 模型的线性特征和 GARCH 模型的非线性特征 [11,17]。当不同时间段的值之间存在相关性时，ARIMA 模型可用于时间序列预测。GARCH 模型更好地描述了时间序列的非线性特征，包括更多的波动前信息，并允许条件方差依赖于以前的值。“ARIMA+GARCH”混合模型是 ARIMA 模型和 GARCH 模型的结合，可以显著提高异常检测的预测精度。

实际检测过程中，ICS 设备日志遵循预期行为的可预测模型。一般使用手动调参来发现该行为模型，并且该过程需要耦合 ICS 及其相关的工业过程。因此，它可以检测与预期行为模型的偏差，并发送异常行为警报。PLC 日志可以存储在设备上或通过 HMI 存储，HMI 根据命令和日志与 PLC 通信 [12]。Wireshark 是一种常见的网络流量分析器，安装在工厂自动化数据集 [12] 的 HMI 上可以用来捕捉 PLC 日志。

3.2 基于多层网络流量的异常检测方法

网络流量分析分为基于有效负载的分析和基于报文头的分析。ICS 环境中基于有效载荷的异常检测是一个研究得很好的领域。基于网络流量的分析可用于检测影响网络流量的网络攻击。这种方法能够检测端口扫描、DNS 中毒、DoS 和 DDoS 攻击等攻击 [6-7,19-20]。有效载荷分析的缺乏使得基于 NetFlow 的方法对于异常检测来说是可扩展的、快速的和具有成本效益的。因此，基于 NetFlow 的分析可以在泛洪攻击影响整个网络之前的最早阶段检测到他们。该方法可以作为基于有效载荷的异常检测方法的补充方法。

NetFlow 是 Cisco 的专有协议，可在路由器设备上启用，以提供 NetFlow 日志。网络流记录被定义为一组具有一些共同特征的数据包，这些数据包在特定的时间间隔内通过一个监控点 [6-9]。与基于有效负载的方法相比，基于网络流的分析方法显著减少了要处理的流量。例如，在 Twente 大学的 IT 网络中，NetFlow 输出的流量与网络上的数据包之比为 0.1 [10-11]。Dong 等人 [4] 已经使用了这种基于网络流量的异常检测，提出了一种基于使用离散余弦变换和奇异值分解将周期性流量特征映射到散列摘要的入侵检测方法，其检测效果更优。Markman 等人提出了基于代理的流量模型 [15]，其中 PLC 和 HMI/ 工程工作站之间的通信周期可以建模为确定性有限自动机模式建模，提升了网络流量检测方法的精确性。

3.3 耦合深度学习算法的多层网络流量的异常检测方法

常规的基于网络流量的异常检测方法，能够监控包括 NetFlow 数据在内的分布式 ICS 数据源 [7-8]。由于基于网络流的检测方法只是基于报文头数据，大大减少了数据分析的工作量，同时有效载荷的加密不影响其结果。此外，网络设备（如路由器和交换机）可以轻松生成和收集网络流数据，较容易的产生大量的可分析检测的数据。使用网络流分析和日志分析，耦合深度学习的网络流量的异常检测方法的性能明显优于仅基于网络数据包或设备日志的异常检测。

传统信息系统和工业控制系统的主要区别在于后者集成到工控物理设备中。由于这种集成，工业控制系统引入了新类型的漏洞，增加了异常检测的复杂性 [15-16]，例如，对于多层集成电路网络，就需要采用耦合深度学习算法的多层网络流量的异常检测方法。

虽然基于网络流量的方法可用于 ICS 网络中的异常检测 [8-9,12]，但基于网络流量的异常检测算法的固有问题是，他们无法在监督控制层识别受损工作站的异常行为。例如，攻击者可以访问操作员的凭据，并使用他们发送命令来中断物理过程。为了应对这一挑战，研究人员提出了基于物理过程的异常检测算法 [12,16-17]。这种方法可以识别来自受损工作站的攻击。然而，这种算法在检测影响 ICS 网络顶层的网络流量的 DoS 和分布式拒绝服务（DDoS）攻击时效率不高。在 ICS 上的 DDoS 或 DoS 攻击影响物理过程之前，可以在网络层有效地检测出来。

4 结论

传统的工业控制系统不同于互联网开放的体系，而是个体封闭的。但是随着工业互联网平台的应用，越来越多的设备连接到企业网络，从而引发了越来越多的网络安全问题。工业控制网络本身具有分布式特性，同时随着工业互联网等政策的落地实施，工业控制网络本身的边界逐渐模糊，其与工业过程工艺流程具备更高的关联性，工业过程的强时序性也越发显现。传统采用网络流量的方法，出现了异常检测困难，难以检测 APT 等动态威胁，检测结果不准确等问题。

本文列举了国内外众多厂商和研究学者在工业控制系统异常检测方法的研究和应用情况，并分析其优缺点，

为工业控制系统自动异常检测在选择方法时提供依据。并指出，随着深度学习算法的不断优化，工业互联网促进工业控制数据多源融合，耦合深度学习算法的多层网络流量的异常检测方法必将成为主要的工业控制系统异常检测的方法。

参考文献

[1] JADIDI Z, MUTHUKKUMARASAMY V, SITHIRASENAN E, et al. Flow-based anomaly detection using semisupervised learning[C]// International Conference on Signal Processing and Communication Systems. IEEE, 2016.

[2] HOFSTEDE R, JONKER M, SPEROTTO A, et al. Flow-based web application brute-force attack and compromise detection[J]. Journal of network and systems management, 2017, 25 (4): 735–758.

[3] 郭肖旺，闵晓霜，韩庆敏. 基于自适应深度检测的工控安全防护系统设计 [J]. 电子技术应用，2019, 45 (1): 85-87, 91.

[4] COLELLI R, PANZIERI S, PASCUCCI F. Exploiting system model for securing CPS: the anomaly based IDS perspective[C]//2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2018.

[5] ZHANG F, KODITUWAKKU H, HINES W, et al. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data[J]. IEEE Transactions on Industrial Informatics, 2019.

[6] 张玫，曾彬，朱成威. 工控系统安全监测及溯源系统的设计与实现 [J]. 信息技术与网络安全，2019, 38 (1): 14-19.

[7] SESTITO G S, TURCATO A C, DIAS A L, et al. A method for anomalies detection in real-time ethernet data traffic applied to profinet[J]. IEEE Transactions on Industrial Informatics 2018, 14 (5): 2171-2180.

[8] HADELI H, SCHIERHOLZ R, BRAENDLE M, et al. Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration[C]//Proceedings of 12th IEEE International Conference on Emerging Technologies and Factory Automation, Palma de Mallorca, Spain: IEEE, 2009.

[9] OLIVEIRA L, RODRIGUES J, SOUSA A, et al. Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms[J]. IEEE Transactions on Industrial Informatics, 2017, 12 (6): 2186-2195.

[10] LI B, SPRINGER J, BEBIS G, et al. A survey of network flow applications[J]. Journal of Network and Computer Applications, 2013, 36 (2): 567–581.

[11] OLIVEIRA L, RODRIGUES J, SOUSA A, et al. Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms[J]. IEEE Transactions on Industrial Informatics, 2017, 12(6): 2186-2195.

[12] 刘庆华，赵雪寒. 融合自编码降维的改进 DNN 水利工控网入侵检测算法 [J]. 计算机与数字工程，2021, 49 (11): 2287-2291, 2401.

[13] 刘庆华，吴昊天. 融合 PCA 降维的改进深度神经网络工控安全算法 [J]. 计算机与数字工程，2019, 47 (7): 1688-1693.

[14] WANG Q, CHEN H, LI Y, et al. Recent advances in machine learning-based anomaly detection for industrial control networks[C]// 2019 1st International Conference on Industrial Artificial Intelligence (IAI). IEEE, 2019.

[15] 陈思，吴秋新，张铭坤，等. 基于边云协同的智能工控系统入侵检测技术 [J]. 计算机应用与软件，2020, 37 (11): 280-285, 333.

[16] 张晔. 异常检测技术在工控系统安全中的成功应用 [J]. 自动化博览，2019 (4): 46-48.

[17] 朱亮，李东波，吴崇友，等. 基于数据挖掘的电子皮带秤皮带跑偏检测 [J]. 农业工程学报，2017, 33 (1): 102-109.

[18] CALINSKI T, HARABASZ J. A dendrite method for cluster analysis[J]. Communications in Statistics, 1974, 3(1): 1–27.

[19] DAVID J, THOMAS C. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic[J]. Computers & Security, 2019, 82 (5): 284–295.

收稿日期：2022-05-26