基于数字孪生的工业互联网安全检测与响应研究

马佳利，郭渊博，方晨，陈庆礼，张琦
（信息工程大学密码工程学院，河南 郑州 450001）

摘　要：考虑传统网络安全防御方法不能够满足工业互联网对可靠性和稳定性的严格要求，基于数字孪生的思想研究了一种在数字空间中通过采集现场数据和使用孪生模型安全认知进行异常检测和响应的方法。首先，通过对数字孪生建模方案进行分析，总结出4类建模方法并集成到多模块数字孪生（DT）架构中；然后，通过引入信号时序逻辑技术将不同孪生模型认知转化为标准的信号时序逻辑（STL）规范集，根据规范集对系统行为的监测实现异常检测，多源认知增加了检测结果的可靠性；最后，通过对违反STL规范集情况的分析实现异常定位，并通过对已知设备故障的分析设计相应STL弱规范实现异常分类，对异常的两方面响应有利于帮助系统恢复正常运行。案例研究表明，所提方法在异常检测和响应方面非常有效。将所提方法与基于深度学习的入侵检测系统进行对比，实验结果表明，所提方法在对异常情况的检测时检出率提高了25%~40.9%。

关键词：工业互联网；数字孪生；异常检测；异常响应；信号时序逻辑
中图分类号：TP391
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2024091

Research on industrial Internet security detection and response based on digital twin

MA Jiali, GUO Yuanbo, FANG Chen, CHEN Qingli, ZHANG Qi
School of Cryptographic Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: Considering that traditional network security defense methods cannot meet the strict requirements of industrial Internet for reliability and stability, a method for anomaly detection and response in digital space was studied based on the idea of digital twins by collecting on-site data and using twin model security cognition. Firstly, four types of modeling methods were summarized and integrated into the multi module digital twin (DT) architecture by analyzing the digital twin modeling solutions. Secondly, the cognition of different twin models was transformed into a standard signal temporal logic (STL) specification set by introducing signal temporal logic technology, and anomaly detection was achieved by monitoring system behavior based on the specification set, by the reliability of detection results was increased. Finally, anomaly localization was achieved through the analysis of violations of the STL specification set, and corresponding STL weak specifications were designed through the analysis of known device faults to achieve anomaly classification. Two aspects of response to anomalies were beneficial for helping the system restore normal operation. The case study demonstrates that the effectiveness of the proposed method in anomaly detection and response. Comparing the proposed method with the intrusion detection system based on deep learning, the experimental results show that the detection rate of the proposed method increases by 25%~40.9% in detecting anomalies.

Keywords: industrial Internet, digital twin, anomaly detection, anomaly response, signal temporal logic

收稿日期：2023–11–13；**修回日期：**2024–04–08
通信作者：郭渊博，yuanbo_g@hotmail.com
基金项目：国家自然科学基金资助项目（No.62276091）；国家社科基金资助项目（No.2022-SKJJ-B-057）；河南省重大公益专项基金资助项目（No.201300311200）
Foundation Items：The National Natural Science Foundation of China (No.62276091), The National Social Science Fund of China (No.2022-SKJJ-B-057), The Major Public Welfare Project of Henan Province (No.201300311200)

0 引言

工业互联网是工业控制系统和互联网相结合的产物，通过信息技术（IT, information technology）和操作技术（OT, operational technology）的融合为工业控制系统提供灵活的控制能力，同时也不可避免地引入了网络安全风险[1]。近年来，工业互联网安全事件频发[2-4]，不仅给整个工业行业带来了严重的经济损失，还造成了极其恶劣的社会影响。由于网络组件与其物理对应物相关联，因此在网络域发起的攻击可能会对物理制造资源、产品，甚至人类造成伤害和损害。面对日益复杂的网络环境，工业互联网安全防御的研究受到了国内外学者们的广泛关注。

传统网络安全方法根据PDR（protection detection response）模型[5]可以划分为保护、检测和响应，工业互联网由于其OT部分组件的存在，主要依赖检测和响应的方法。工业互联网的OT部分对可靠性和稳定性有严格的要求，而在OT环境中部署传统IT网络保护技术，如防火墙、加密技术、访问控制等，有可能对系统OT部分的性能产生不利影响，而且工业环境中协议的特殊性进一步限制了传统IT网络保护方法的应用[6]。与之相对的是，检测和响应技术与工业互联网的架构更加适应，可以在不影响工业OT部分正常运行的前提下执行，通过及时发现和快速响应安全威胁保护系统免受损害。

在工业互联网检测方面，基于机器学习的入侵检测系统（IDS, intrusion detection system）是当前主流的检测方案[1]，机器学习技术具备出色的泛化能力和运算性能，以及处理大规模数据的能力，学者们已经探索了基于SVM（support vector machine）、CNN（convolutional neural network）、GAN（generative adversial network）等不同入侵检测方法[7-9]。然而，机器学习算法本身的黑盒特性导致其缺乏可解释性，用户难以信任检测结果，而且机器学习算法对数据高度敏感，在训练数据较少时不可使用。在工业互联网响应方面，主要方法包括异常报警和攻击溯源等[10-11]，但是对异常本身的研究分析较少，特别是异常定位和异常分类可以用于发现异常点和排除故障，对系统恢复正常运行十分重要。针对现有研究的不足之处，数字孪生（DT, digital twin）提供了一种有效的解决方案。

DT是一种将物理实体实时映射到数字空间的技术，由物理实体、孪生模型以及它们之间的数据交互组成[12]。DT在数字空间中以孪生模型的形式实时表示物理实体状态，为分析工业互联网安全提供了新的可能性。一方面，DT在数字空间中捕获工业互联网的实时动态信息，在数据层面支持异常检测和响应工作；另一方面，DT将物理资源孪生化提供额外的分析能力和对运行时系统的洞察力，在认知层面为执行检测和响应任务提供支撑。本文重点关注DT带来的强大的认知能力，提出一种基于DT的方法以实现对工业互联网的检测和响应。

为了全面建模工业互联网，需要使用多种孪生模型表示系统的不同方面。根据对现有工业互联网DT解决方案[13-16]的分析，本文按照建模对象和建模方法的不同提出了4种DT：基于语义技术的特征DT、基于机理模型的行为DT、基于神经网络的行为DT以及基于状态机的行为DT，其中特征DT对工业互联网中的异构信息进行建模，后3种行为DT使用不同方法对系统行为进行建模，它们涵盖了现有研究的大多数DT方案，代表了不同的认知能力。本文提出使用多模块DT的架构来集成这些不同类型的DT，可以实现对工业互联网全方位、多角度的数字化表示，为后续检测和响应任务提供充分的执行依据。

然而，不同类型的DT对系统的表示和表现形式均有所不同。为了从这些DT中提取关于系统安全的认知并将其应用于检测和响应任务，本文通过引入一种形式化语言信号时序逻辑（STL, signal temporal logic）[17]以实现对异构DT的标准化表示。具体来说，STL将不同DT的认知按照一定规则转化为标准的形式化规范描述，结合DT架构实时捕获的系统状态信号，使用STL规范集合对表示系统行为的信号开展全面监测，根据监测信号对STL规范的执行情况实现检测异常的功能，并根据STL规范违反情况的分析实现对异常的定位和分类。

综上所述，本文针对工业互联网安全的检测和响应问题，提出了一种基于DT的方法，研究不同类型的DT如何支撑工业互联网安全中的检测和响应任务，主要工作包括构建工业互联网多模块DT架构以及基于STL形式化方法提取不同DT的认知执行检测和响应任务。与传统基于机器学习的IDS相比，基于DT的方法融合了多方面的认知，不仅提高了异常检测结果的可靠性和准确度，即使在训练数据量较少的情况下也可以展现良好的检测性

能，而且在响应方面也提供了定位和分类的解释能力。本文的主要贡献包括以下 3 个方面。

1) 提出一种多模块 DT 的架构建模工业互联网，将多种孪生建模方案进行集成，实现对系统全方位、多角度的认知。

2) 使用 STL 形式化语言将不同 DT 的认知转化为标准的 STL 规范，并根据信号对 STL 规范的满足与否检测异常，提高检测的可靠性并且可以灵活适用于不同的场景。

3) 针对发现异常后如何响应的问题，提出一种基于 STL 执行情况定位异常的方法，并根据对已知故障行为模式的了解区分网络攻击和设备故障，从两方面对异常做出解释。

1　相关工作

1.1　工业互联网检测和响应研究

检测和响应是支撑工业互联网安全的关键技术，学者们已经提出使用不同方法的检测和响应方案。

常用的检测方法主要包括基于规则的方法和基于数据的方法[18]。其中，基于规则的方法基于事先定义的规则来确定异常，但是规则的定义和维护需要领域专家参与，而且对于未知的、新型的异常无法有效检测。基于数据的方法是通过对数据进行统计建模和分析，发现与已有数据模式不一致的数据点，根据所采用的数据建模机器学习方法不同可以分为：基于传统机器学习的算法，如罗耀锋[7]提出基于多分类 SVM 的入侵检测方法用于检测多类攻击；基于神经网络的算法，如 Song 等[8]提出使用 CNN 算法将数据流转化为图像进行检测，根据与正常行为下构建图像的不同检测出异常；基于对抗学习的算法，如 Liu 等[9]提出使用 BiGAN（bidirectional GAN）用于入侵检测，并通过交叉验证得到最优的模型以提高其适应度。然而基于数据的方法的缺点是需要大量的训练数据来建立模型，在数据量较少时无法进行检测，而且模型的黑盒特性导致了无法对异常进行进一步的解释分析。

在异常响应方面的研究目前仍较少，除了常见的根据异常检测结果进行报警外，学者们探索了攻击溯源的响应方法，如张玫等[11]提出通过对工业协议、系统运行日志和安全日志的解析发现网络攻击的源头，确认攻击者的 IP 地址、攻击技术等信息。目前，工业互联网异常响应机制仍不完善，需要重点研究如何帮助系统迅速恢复正常运行的方法。

1.2　DT 与工业系统

DT 的概念起源于 2003 年的信息镜像模型，意为与物理产品等价的虚拟数字化表达[19]，其后直到 2011 年美国空军在对战斗机机身维护的研究中首次提出了机身数字孪生体，DT 才被正式提出[20]。目前对于 DT 的定义仍存在一些分歧，但一般认为 DT 包含如下特征：高保真的孪生模型以及物理空间与虚拟空间之间的信息交互。

工业系统是 DT 应用最为广泛的领域，学者们探索了 DT 的不同应用模式，包括系统流程优化、故障诊断、智能决策、生命周期管理等。Samir 等[21]提出利用 DT 实现资产的可追溯性和可见性，有助于更好地控制、计划和调度决策。Tao 等[22]探索了数字孪生车间的新概念，根据实时状态变化更改生产计划以实现生产优化。Xie 等[23]提出了一种基于 DT 的液压支架虚拟监控方法，采用信息融合算法对液压支架的姿态进行监测。Guivarch 等[24]提出利用 DT 进行虚拟调试，计算动力系统机械部件所承受的负荷，而不会引入大量维护负担和传感器连接。DT 在工业系统中已经得到了广泛的应用，为工业系统提供了强大的工具和平台，可以用于提高系统的效率、可靠性和可持续性，辅助传统制造业向智能制造业迈进。

1.3　基于 DT 的安全应用研究

DT 技术的灵活性和潜力同时也促进了其在工业互联网网络安全方面的应用，学者们探索利用 DT 加强系统安全性的不同方法。

Eckhart 等[25]提出在数字孪生中使用状态复制的方法进行入侵检测，将信息重播到数字孪生模型中进行预测，并将预测结果与实际系统运行结果之间的偏差定义为系统异常。Dietz 等[26]提出在安全运营中心（SOC, security operation center）中使用数字孪生进行安全仿真，仿真定义了攻击事件和安全规则，只有检测到攻击事件的规则才会被部署到实际系统中，检测能力来源于数字孪生中探索的安全规则。Dietz 等[27]提出可以使用数字孪生进行安全测试，提供有价值的安全分析来检测未来系统的漏洞并使系统在设计上更安全。Vielberth 等[28]提出基于数字孪生构建 SOC 分析师的网络靶场，学员在数字孪生中学习如何与安全信息和事件管理

（SIEM, security information and event management）系统交互，并创建关联事件的规则以检测安全事件，用户研究表明参与者的安全知识显著增加。Xu等[29]使用时间自动机模型构建数字孪生，基于历史数据进行训练并使用实时数据进行改进，将正在运行的系统行为与模型的预测进行比较，产生差异说明发生异常。基于DT的安全主要关注其模拟推演能力，通过离线仿真的方式产生新的安全防御知识和策略来促进网络安全，仅有少部分研究认识到DT在针对系统的在线监测方面的潜力，这2种方法代表了基于DT安全研究的不同方面。

本文主要关注DT技术在在线监测方面的应用，针对现有工业互联网检测和响应的研究中认知来源单一、对训练数据量要求高、检测结果缺乏进一步解释分析等问题，提出一种多模块DT架构用于工业互联网安全，旨在将不同类型的DT集成以适应各种工业互联网环境，并利用一种通用的方法提取来自不同DT的认知用于异常检测和响应。

2 工业互联网多维度DT建模

为了实现对工业互联网的全面建模，首先对其系统组成结构进行概述与分析，然后总结已有研究提出的适合工业系统的多种DT建模方法，构建由不同类型的DT组成的多模块架构，最后对各类型DT的实现细节和应用模式进行说明。

2.1 多模块工业互联网DT架构

工业互联网将原本封闭的工业控制系统接入互联网中，利用云计算、深度学习、大数据分析等技术帮助工厂实现智能化，工业互联网架构[30]如图1所示。

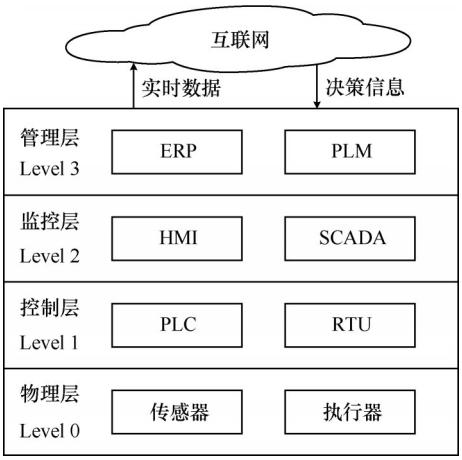


图1 工业互联网架构

物理层主要包括传感器和执行器等工业现场的物理设备。

控制层主要包括程序逻辑控制器（PLC）、远程终端单元（RTU）在内的现场控制设备，用于对生产过程的设备进行感知和操作。

监控层主要包括人机接口（HMI, human machine interface）和数据采集与监控系统（SCADA, supervisory control and data acquisition），其中，HMI用于系统和用户之间进行信息交互，向现场控制设备发送控制命令和查询请求，SCADA可以对现场运行的设备的监视和控制，实现对现场设备的数据采集、设备控制、测量、信号报警以及参数调节等功能。

管理层主要包括企业资源计划（ERP, enterprise resource planning）和产品生命周期管理（PLM, product lifecycle management），用于使企业管理者了解和掌握整个系统的运行状况和设备状态变化，实现对工艺的过程监视与控制。

上述各部分组成了传统工业控制系统，形成了一个封闭的工厂局域网，工业互联网在其基础之上将系统数据接入互联网中，通过云计算、人工智能、大数据分析等智能技术为系统提供增值服务。

云计算平台具有丰富的计算和存储资源，结合连续采集的工业现场实时数据，为构建工业互联网DT提供了适宜的环境，因此工业互联网DT构建于云平台中并以孪生模型的形式实现对工业数据的处理，形成有价值的信息，这些信息将反馈到工业环境中提供智能服务，本文的研究关注基于DT的安全监测和响应。

图2展示了用于工业互联网安全监测的多模块DT架构，支持不同建模策略来创建工业互联网的模型，建模策略来源于对已有工业系统DT的研究。根据建模对象和建模方法的不同，划分为对系统中海量异构的数据和信息使用基于语义技术的特征DT进行建模及对系统内在运行规律分别使用基于机理方程、数据驱动、基于状态机的行为DT进行建模。这些DT使用不同的建模方法表示建模工业互联网的不同方面，涵盖了现有研究的绝大多数DT类型，提供了对工业互联网多角度的认知。

2.2 特征DT建模异构信息

在工业互联网中，实时数据和专业知识表示了系统的动态和静态信息，特征DT通过数据预处理

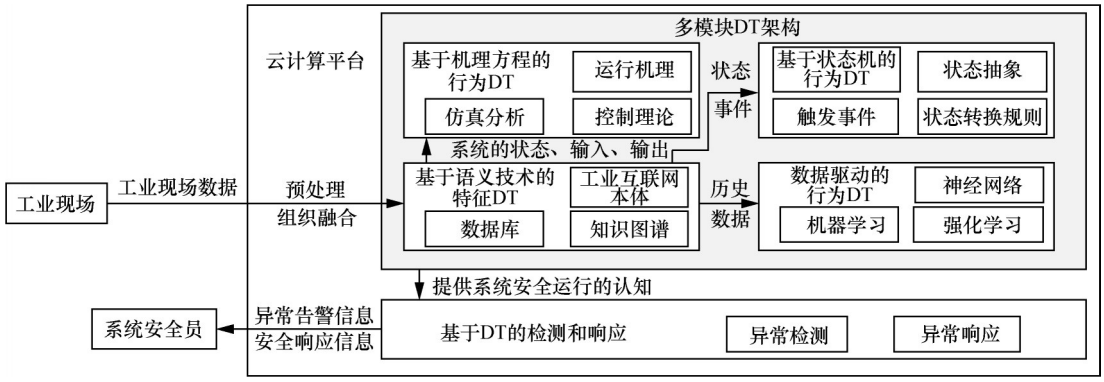


图2　多模块DT架构

和关联的方法对异构信息进行数据建模，实现对数据资产的统一表示。一方面，实时数据包括生产过程中传感器和执行器产生的数据、控制器输入以及操作员输入等，这些原始数据由于存在噪声、数据不稳定等原因不能直接使用，需要使用数据平滑、离散化、特征提取、数据缩减和估算缺失值等方法进行数据预处理；另一方面，工业互联网中专业知识包括设备规格信息、操作手册、安全运行区间以及由专家定义的其他专业知识等，这些信息具有多样性、非同质性、时效性的特点，难以进行统一的管理，本文使用语义技术组织和关联这些异构信息。

知识图谱作为一种先进的语义技术，能够以实体和关系的形式展现系统信息，提供简洁、统一的描述，实现异构数据和信息的语义互操作性，知识图谱技术成为工业互联网中组织复杂信息有效的解决方案。因此，在特征DT中使用知识图谱建模工业互联网，建立工业互联网特征本体并用于领域概念的形式化表达，工业互联网特征本体与知识图谱实例化如图3所示。

特征DT基于语义技术，使用少量计算存储资源将工业互联网中各类信息资产关联起来实现知识聚合，代表一种轻量级的系统建模方案，可以辅助工业互联网完成优化调度、资源分配等管理任务，也可以用于语义搜索、智能问答、可视化以及知识推理等功能。

然而，特征DT只是对可观测、可获取的信息数据进行整合，无法了解数据所代表的实际含义，在要求深入了解系统运行状况的场景下需要构建描述其内部逻辑的行为DT。

2.3　行为DT建模运行逻辑

工业系统的运行遵循预先定义控制策略和现实物理法则，行为DT对这种内在运行逻辑进行建模，帮助理解系统内部规律。根据对系统运行逻辑的认知程度不同，行为DT可以采用不同的建模方法，包括基于机理方程的行为DT、数据驱动的行为DT以及基于状态机表示的行为DT。

基于机理方程的行为DT。该方法通过对系统内在运行逻辑进行建模，帮助理解系统内部规律，使用严格的数学物理方程描述系统具有的明确物理

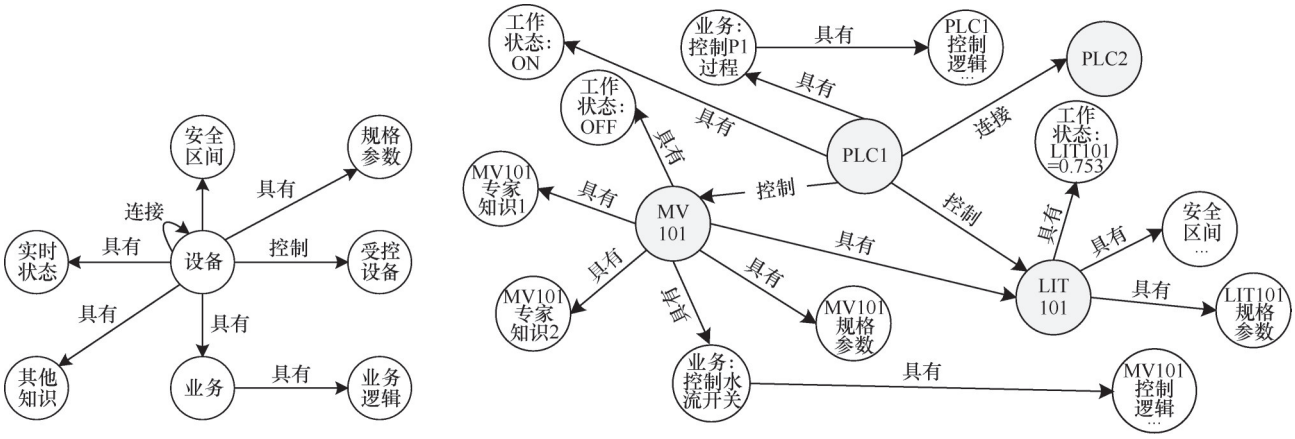


图3　工业互联网特征本体与知识图谱实例化

意义，在理想状况下可以准确表征系统行为，是一种“白盒模型”。以离散过程工业为例，使用状态转换方程表示其运行机理，如式(1)和式(2)所示。

$$x(t+1)=f(x(t),u(t),w(t)) \tag{1}$$

$$y(t)=g(x(t),v(t)) \tag{2}$$

其中，$x(t)$是过程状态，$u(t)$是过程输入，$y(t)$是测量值，$w(t)$和$v(t)$分别是过程和测量噪声，t是离散时间指数，$f(\cdot)$和$g(\cdot)$分别是过程模型和测量模型。

基于机理方程的行为DT在系统运行阶段不断更新状态和输入数据实现与实际系统的同步，甚至还可以进行超前模拟以预测系统行为和评估决策方法：在不影响实际系统运行的条件下，可以用于评估不同操作和配置对系统功能或性能的影响，对不同状态和输入产生的结果进行预测，以及评估不同控制策略的效果并选择合适的控制算法和参数以满足控制要求，例如采用各种控制方法和逻辑将过程测量值$y(t)$调节至决策者提供的参考设定点，要求偏差在合适的范围且尽可能小。

数据驱动的行为DT。由于工业系统的复杂性存在无法理解其工作原理的情况，难以建立准确的数学方程，而在DT的架构中采集运行数据是容易的，数据驱动的行为DT旨在对这些数据进行观察和分析，从中挖掘出系统的隐含规律和模式用于推断系统的行为。数据驱动的行为DT表现为根据过去一段时间的观测数据对下一时刻数据进行预测，即

$$\boldsymbol{x}(t+1)=M(\boldsymbol{x}(t),\boldsymbol{x}(t-1),\cdots,\boldsymbol{x}(t-w+1)) \tag{3}$$

其中，w为观测窗口大小，$M(\cdot)$为所使用的预测模型，一般选择使用泛化性好的深度学习模型。采用数据驱动的方法建模系统行为可以减少专业知识的使用，在训练数据充足的情况下可以真实地反映实际系统的规律，是一种“黑盒模型”。

基于状态机的行为DT。除了上述建模方法外，还存在对系统行为部分已知的情况，使用时间自动机、Petri网等状态机形式表示系统运行规律，这些方法将系统建模为特定状态的集合，并定义了状态跳转的触发条件。基于状态机的行为DT描述系统在不同状态之间转换的规则，一般情况下由以下步骤组成。

1) 定义状态：标识系统可能处于的不同状态。状态应该是相互独立且彼此排斥的，以确保状态转换的一致性。

2) 定义事件：识别可能触发状态转换的输入或条件。事件可以是外部事件（例如用户输入、传感器信号等）或内部事件（例如定时器超时、条件满足等）。

3) 建立状态转换规则：根据系统需求和行为定义转换规则。确定每个状态下特定事件的响应，以及由此导致的状态转换。

基于状态机的行为DT将系统行为进行抽象，在认知层面，该方法处于基于机理方程的行为DT和数据驱动的行为DT之间，可以看作一种“灰盒模型”。

上述DT类型涵盖了现有研究绝大多数DT建模方法，将这些不同类型的DT集成到一起建模工业互联网可以实现一种灵活检测机制，即使在对系统只有部分认知的情况下也可以使用多模块DT架构中的一种或者多种DT表示，因此该架构可以灵活适用于不同场景的工业互联网。

3 基于DT认知的检测与响应方法

多模块DT架构集成了对系统多方面的认知，但由于不同类型的DT使用的建模方法不同，其表现形式也有所不同，需要从这些异构DT中提取有关系统的安全认知用于检测和响应任务。本节通过引入STL形式化方法将不同DT的安全认知转化为统一的STL规范，根据系统行为信号对STL规范的执行情况检测异常，然后利用STL的违反情况判断异常发生的位置，最后根据已知故障类型增加STL弱规范描述分别作为网络攻击和设备故障的依据。

3.1 预备知识

形式化方法是使用严格的数学方法来构建软件和硬件系统以表现系统性质和属性的建模方法，它使用数学证明作为系统验证的补充，可以在系统运行期间监视正式规范，以检测违反要求的情况并采取纠正措施[31]。近年来提出的STL等新一代形式化规范能够有效地监控系统中的信号，以逻辑谓词的形式规定了预先定义的时间窗口内的测量信号的预期行为，STL的语法如式(4)所示。

$$\pi \triangleq \top \mid f(x)\sim\mu \mid \neg\pi \mid \pi_i \wedge \pi_j \mid \pi_i U_{[a,b)} \pi_j \tag{4}$$

其中，$\top$为逻辑真；$f(x)\sim\mu$为原子谓词，由函数、实数值和顺序关系表示；$\neg\pi$表示命题π的否定；$\wedge$

表示 2 个命题的逻辑与；$U_{[a,b)}$ 为直到运算符；$\pi_i U_{[a,b)} \pi_j$ 表示命题 π_i 至少在命题 π_j 为真的区间 $[t+a,t+b)$ 为真，其中 t 为当前时间。此外，STL 还定义了最终运算符 $\Diamond$ 和总是运算符 $\Box$，$\Diamond_{[a,b)}\pi$ 表示命题 π 至少在区间 $[t+a,t+b)$ 的某一时间点为真，$\Box_{[a,b)}\pi$ 表示命题 π 在区间 $[t+a,t+b)$ 一直为真。

STL 的语义在信号 S 中的表示为

$$\begin{gathered} s[t] \vDash \top \leftrightarrow \top \\ s[t] \vDash f(x) \sim \mu \leftrightarrow f(s(t)) \sim \mu \\ s[t] \vDash \neg \pi \leftrightarrow \neg (s[t] \vDash \pi) \\ s[t] \vDash (\pi_1 \wedge \pi_2) \leftrightarrow (s[t] \vDash \pi_1) \wedge (s[t] \vDash \pi_2) \\ s[t] \vDash \pi_1 U_{[a,b)} \pi_2 \leftrightarrow \exists t' \in [t+a,t+b), \text{s.t.} f(s(t')) \sim \mu \end{gathered} \tag{5}$$

对于一个信号 $s \in S$，当且仅当 $s(t) \vDash \pi$ 时，称为满足一条 STL 规范 π，这里 $\vDash$ 符号用于表示左边的条件满足右边的条件。例如，如果要求系统中部分信号满足如下性质：当信号 a 的值大于 1，要求至少在 2 s 的时间内收敛到小于 1 的值，且至少保持 5 s，则这种性质可以使用 STL 规范进行形式化声明，即

$$\pi: a[t] > 1 \rightarrow \Diamond_{[0,2)} (\Box_{[0,5)} (a[t] < 1)) \tag{6}$$

3.2　基于 STL 规范的异常检测

异常检测问题需要相应的检测规则，在本文的架构中这种规则从各种 DT 中获取并以 STL 规范的形式表现，然后使用 STL 规范集合来监测工业互联网行为识别异常状况，工业互联网行为以其连续实时动态的时间序列信号为代表。异常检测方法如图 4 所示。

基于 STL 规范的异常检测方法的核心是对运行时信号的监控，令 $\Pi = \{\pi_1, \pi_2, \cdots, \pi_n\}$ 表示一系列 STL 规范集合，$\boldsymbol{x}(t)$ 表示运行时的监控信号，则系统正常运行情况下应该满足

$$\boldsymbol{x}(t) \vDash \pi_1 \wedge \pi_2 \wedge \cdots \wedge \pi_n \tag{7}$$

当 STL 规范集合 Π 中的任意一条规范不满足时，工业互联网检测出异常并发出警告。使用 STL 规范建模网络安全的关键在于通过深入了解系统需求和属性，并使用 STL 语言形式化地表达出来，但是这一工作往往依赖于大量的专业知识和经验，需要寻求专业人士的指导和支持。为了实现 STL 规范的快速获取，在所提出的多模块 DT 架构下，提取来自特征 DT 和行为 DT 的有关系统安全运行的认知构造相应的 STL 规范。

特征 DT 对数据信息进行建模，其系统安全的认知主要来源于专业知识，如关于设备规格说明及其执行业务流程，前者描述了系统的安全工作范围，后者描述了系统的条件触发状况，均可以使用 STL 语言进行形式化描述。以信号 a 和信号 b 为例，特征 DT 根据这些专业知识构建的 STL 规范为

$$\pi: \Box((a[t] > 0.2) \wedge (a[t] > 0.8)) \tag{8}$$

$$\pi: a[t] > 0.5 \rightarrow b[t] = 0 \tag{9}$$

基于机理方程的行为 DT 描述了系统运行逻辑，其系统安全认知主要来源于系统正常运行时对下一时刻状态的预测，在理想化状态下的预测值应该等于下一时刻的观测值。以残差信号 ε 为例（残差信号是通过可观测信号计算得到的），ϵ 表示系统可以容忍的最大偏差，基于机理方程的行为 DT 利用预测残差生成的 STL 规范为

$$\pi: \varepsilon[t] < \epsilon \tag{10}$$

基于状态机的行为 DT 描述了系统可能的状态跳转，其系统安全认知主要来源于可能跳转到的系统状态，状态纠缠导致状态空间中存在禁止状态子集。以状态信号对 (s_1, s_2) 为例，基于状态机的行为 DT 根据可达状态构建的 STL 规范为

$$\pi: (s_1, s_2) = ((0,0),(0,1),(1,0)) \tag{11}$$

基于数据驱动的行为 DT 的系统安全认知主要来源于根据过去一段区间的数据对下一时刻数据的预测，基于数据驱动的行为 DT 构建的 STL 规范为

$$\pi_M: |M(\boldsymbol{x}(t)) - \boldsymbol{x}(t+1)| < \epsilon \tag{12}$$

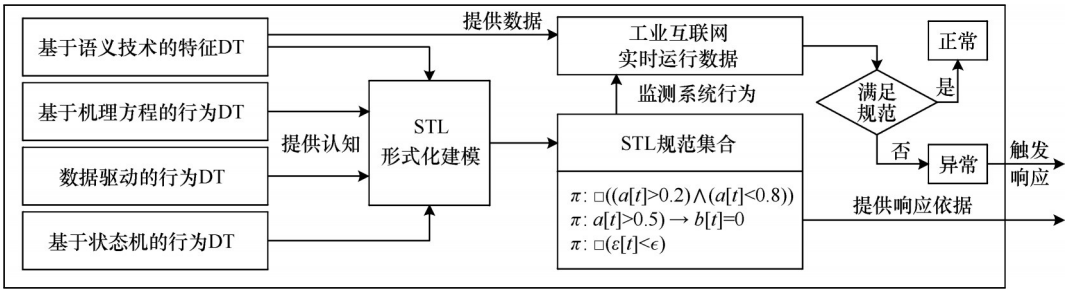


图4　异常检测方法

其中，$M(\cdot)$表示所使用的算法模型，可根据过去时间区间的行为对下一时刻的行为进行预测。

实际上，数据驱动的行为DT转化为STL规范用于异常检测任务代表了一种IDS的方法，而使用IDS在工业互联网异常检测任务中是必不可少的，特别是由于不可能挖掘所有系统的STL安全规范，使用其他类型的STL规范只能检测出已知安全问题，这种IDS的方法弥补了检测未知异常的问题。此外，只依赖IDS进行异常检测也存在一些问题，例如IDS需要使用大量数据进行训练，在工业互联网运行初期难以有效地检测异常，而且IDS的黑盒特性导致其难以执行进一步的响应分析。

因此，在多模块DT架构下使用STL规范方法检测异常弥补了单一检测方法的不足，基于STL语言将来自多种DT的认知进行统一集成，可以直接作用于DT捕获的系统行为信号进行异常检测，这种方法的优点在于可以使用对系统的多方面认知检测异常，不仅可以增加异常检测的准确性和可靠性，而且可以应用于对工业互联网不同认知的场景，以灵活的方式支撑系统安全。

3.3　基于STL规范的异常定位与分类

当异常检测模块检测出系统异常状况后，需要对异常进行响应，以帮助系统安全员排除或者缓解异常带来的影响。对于工业互联网的异常响应问题，本文重点关注2种任务：异常定位和异常分类。前者用于在系统中迅速找到引起异常的设备，后者用于区分异常来源是网络攻击还是设备故障，它们可以帮助系统安全员迅速准确地处理异常，降低异常带来的损失。使用已经构建的STL模型执行上述2种任务，异常定位和异常分类方法如图5所示。

当工业互联网检测到发生异常状况后，异常定位是首要任务，系统的复杂性导致了手动发现异常位置是不可行的，为此本文提出一种基于已构建STL规范的定位方法。

具体来说，触发异常定位任务的条件是系统的行为信号违反STL规范集合中的一条或几条，而单条STL规范π_i一般与特定信号集合s_i关联，这些信号表示相关设备的状态，因此当某条STL规范被违反时，其对应信号表示的设备发生故障，根据STL规范的执行情况进行异常定位表示为

$$\text{Location} = \{\, s_i \mid \exists \neg\pi_i, \pi_i \in \Pi \,\} \tag{13}$$

上述方法存在例外的情况，即STL规范对所有信号进行定义，在这种状况下难以定位异常产生的位置，需要结合相关知识进行进一步的分析，这部分内容超出了本文研究范围，因此不再赘述。

工业互联网中发生异常的原因主要有2种：网络攻击和设备故障。为了分析异常产生的原因，本文对已知设备故障模式设计了新的STL规范，根据已知设备故障对系统的影响设计一种条件更弱的规范，定义为STL弱规范，其在执行监测的过程中降低了对信号的约束条件。以通信故障导致响应时延为例，对式(9)中的STL规范π检测条件通过延迟响应时间进行弱化并表示为π^{-}，即

$$\pi^{-}: a[t] > 0.5 \rightarrow \Diamond_{[t+1,\, t+t_d]}(b[t] = 0) \tag{14}$$

本文研究中主要考虑对系统正常运行不会产生严重影响的设备故障，将它们与网络攻击区分开，可以减少因为系统停机带来的资产损失。当监控信号不满足原始STL规范而满足相应的弱规范时，认为系统发生故障；当原始STL规范和对应的弱规范都不被满足时，认为系统是遭到网络攻击。值得注意的是，由于系统中故障产生的原因有很多种，难以全部枚举出来，因此在面对未知故障时所提方法会将其识别为网络攻击。

对于多模块DT中各种DT带来的不同形式的认知，使用STL形式化语言将它们转化为标准的STL规范，并将这些STL规范集合应用到检测系统行为信号上，实现了异常检测和响应的功能。

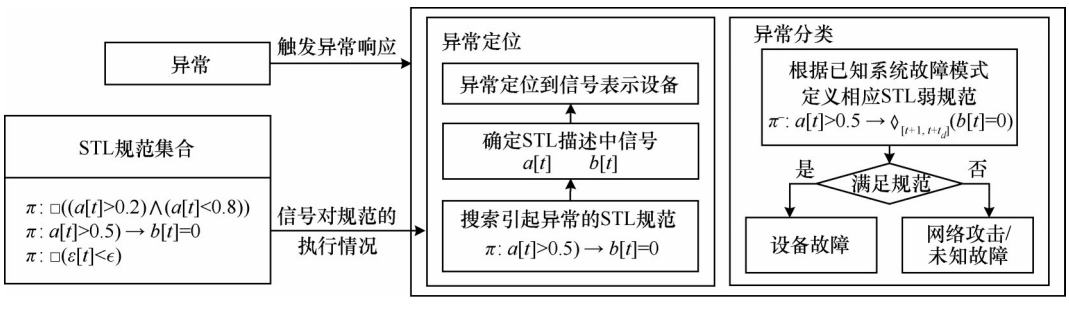


图5　异常定位和异常分类方法

4　案例研究

为了评估本文所提出的基于DT的检测和响应方法的有效性，使用SWaT[32]水处理厂的案例进行验证，首先介绍系统组成以及针对它的攻击设计，然后说明不同类型DT认知如何转化为形式化的STL规范来监测系统，最后展示这些STL规范在异常检测和异常响应方面的结果。

4.1　系统概述和攻击设计

SWaT的工业现场由6个子过程组成，每个子过程由一个PLC设备控制，本文对其中的P1~P3阶段过程进行研究，设计针对该过程的多种攻击类型，并展示使用基于DT的方法实现异常检测和响应。

水处理厂P1~P3阶段过程完成来自水箱T101中的水经过氯化处理移动至水箱T301进行超滤，SWaT工业过程如图6所示。

系统运行过程中需要保证2个水箱中有足够的水，因此与之相关的运行逻辑遵循以下规则：水箱T101有4个液位标记HH、H、L和LL，当T101中的水位低于L标记时，阀门MV101打开，水流入，流量由流量计FIT101测量并传送至PLC1；当水位高于H标记时，阀门MV101关闭。水箱T301也有4个液位标记HH、H、L和LL，当T301中的水位低于L标记且T101中的水位高于LL标记时，水泵P101启动。当水箱T301中的水位等于或高于H标记、MV201关闭、水箱T101中的水位等于或低于LL标记等任意条件成立时，P101关闭。

SWaT中潜在的攻击面很大，根据每个阶段的攻击点攻击分为以下4类。

1) 单阶段单点（SSSP）。单阶段单点攻击集中于系统中的一个点。

2) 单阶段多点（SSMP）。单阶段多点攻击集中于系统中的2个或多个攻击点，但仅针对一个阶段。

3) 多阶段单点（MSSP）。多阶段单点攻击与SSMP攻击类似，只不过SSMP攻击是在多个阶段执行的。

4) 多阶段多点（MSMP）。多阶段多点攻击是执行2个或多个阶段的SSMP攻击。

使用4个攻击案例对这些方法进行说明，针对SWaT的攻击如表1所示。

研究人员在数据收集过程中共发起了36种类型的攻击，每次攻击将会持续一段时间，其中与P1~P3阶段相关的攻击有16种，在后续的研究中，只要在攻击持续过程中识别出异常则认为检测到该类攻击。

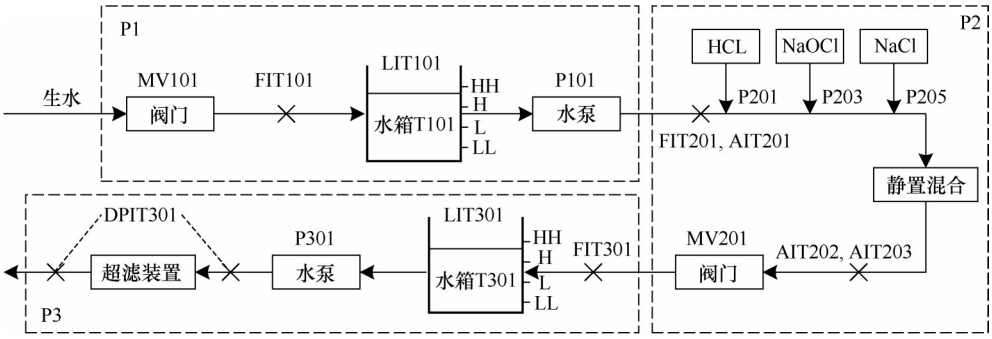


图6　SWaT工业过程

表1　针对SWaT的攻击

攻击类型	受损节点	攻击描述	攻击结果
SSSP	MV101	初始时，阀门MV101处于关闭状态；打开MV101	T101溢出
SSMP	P203 P205	初始时，P203和P205均处于开启状态；关闭P203和P205	改变水质
MSSP	P101 LIT301	初始时，P101和P102分别处于关闭和开启状态，LIT301处于L和H之间；持续打开P101并设置LIT301为H	T101下溢 T301溢出
MSMP	LIT101 P101 MV201	初始时，P101、MV101和MV201均处于关闭状态，LIT101处于L和H之间，LIT301处于L和H之间；持续打开P101和MV101，设置LIT101为H，P102由于LIT301下降而启动	T101下溢 T301溢出

4.2 多维度DT建模

对于上述工业过程，使用多模块DT来建模它的不同方面。

为了构建特征DT，引入文献[33]中关于P101和P102控制逻辑的专业知识，这些信息通过知识图谱表示在专业知识节点中，并以规则的形式表示，特征DT引入专业知识如表2所示。

表2 特征DT引入专业知识

规则	专业知识描述
规则1	当LIT101水位低于LL时，P101和P102均关闭
规则2	当LIT301水位低于L时，P101和P102均打开
规则3	当LIT301水位高于H时，P101和P102均关闭

为了构建基于机理方程的行为DT，将2个水箱中水位的行为建模为离散过程。以传感器LIT101为例，令$x(k)$表示采样时刻t_k时水箱T101中的水位，$x(k)$由传感器LIT101测量，传感器FIT101和FIT201分别测量流入和流出T101的水流量，流速表示为流入的$u_i(k)$和流出的$u_o(k)$，则在采样时刻t_{k+1}，T101中的水位取决于时刻t_k的水位、流入和流出。假设在完美传感器的情况下，忽视测量噪声和过程噪声，该过程的机理可建模为

$$x(k+1)=x(k)+\alpha(u_i(k)-u_o(k)) \tag{15}$$

$$y(k)=x(k) \tag{16}$$

其中，α是根据水箱的物理尺寸和流量计算得出的常数。

为了构建基于状态机的行为DT，参考Adepu等[34]提出的状态机模型，将MV101和P101的行为建模为状态条件图（SCG, state condition graph）。SCG表示水泵P101处于关闭状态以及MV101处于关闭状态时必须满足的条件。其中，P101的SCG包含来自P2的MV201和FIT201以及来自P3的T301的条件。基于状态机的行为DT如图7所示。

为了构建数据驱动的行为DT，本文使用Deng等[35]提出的GDN模型根据时间窗口内行为来预测下一时刻行为，单个信号在时间窗口w中的行为数据表示为$\boldsymbol{s}_i^t=[x_i^{t-w},x_i^{t-w+1},\cdots,x_i^{t-1}]\in\boldsymbol{R}^w$，对于窗口数据分别捕捉时序特征$\boldsymbol{a}_i^t$和空间特征$\boldsymbol{b}_i^t$，然后通过一个全连接网络进行预测。

$$\hat{\boldsymbol{x}}^t=f_\theta([\boldsymbol{a}_1^t\odot\boldsymbol{b}_1^t,\cdots,\boldsymbol{a}_m^t\odot\boldsymbol{b}_m^t]) \tag{17}$$

其中，m表示信号数。使用均方误差来优化该神经网络模型

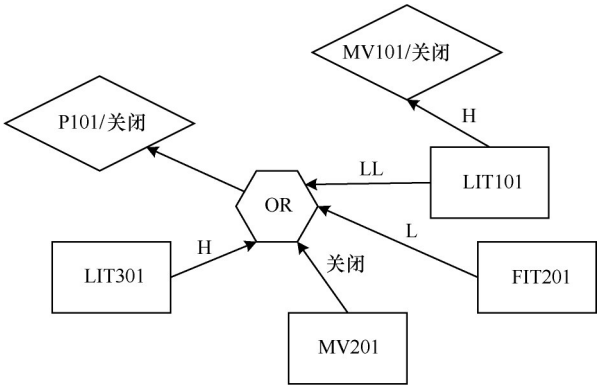


图7 基于状态机的行为DT

$$\text{Loss}=\sum_{\text{history}}\left\|\hat{\boldsymbol{x}}^t-\boldsymbol{x}^t\right\|_2^2 \tag{18}$$

4.3 检测与响应结果

与过程相关的全部信号表示为$\boldsymbol{x}(t)$，其包括全部过程共计51个信号，这里将其中与前面DT建模相关的信号MV101、FIT101、LIT101、P101、P102、FIT201、MV201、FIT301、LIT301和FIT401表示为$a(t)\sim j(t)$。

根据第3节STL规范构建方法，将上述多个DT模块转化为STL语言进行形式化描述，得到监控逻辑为

$$\begin{gathered}\boldsymbol{x}(t)\vDash\pi_1\wedge\cdots\wedge\pi_7\wedge\pi_M\\ \pi_1{:}c(t)<\text{LL}\rightarrow d(t)=0\wedge e(t)=0\\ \pi_2{:}i(t)<\text{L}\rightarrow d(t)=1\wedge e(t)=1\\ \pi_3{:}i(t)<\text{H}\rightarrow d(t)=0\wedge e(t)=0\\ \pi_4{:}|c(t)+\alpha(b(t)-f(t))-c(t+1)|<\varepsilon_1\\ \pi_5{:}|i(t)+\alpha(h(t)-j(t))-i(t+1)|<\varepsilon_2\\ \pi_6{:}c(t)>\text{H}\rightarrow a(t)=0\\ \pi_7{:}d(t)=0\rightarrow(c(t)<\text{LL}\vee f(t)=0\vee\\ g(t)=0\vee i(t)>\text{H})\\ \pi_M{:}|M(\boldsymbol{x}(t))-\boldsymbol{x}(t+1)|<\varepsilon_3\end{gathered} \tag{19}$$

其中，ε_1、ε_2和ε_3是根据正常行为数据学习到的阈值。

为了验证基于STL规范的异常检测方法的有效性，本文比较了所提方法与数据驱动的深度学习方法在不同攻击场景中的检测性能，其中，数据驱动方法使用GDN模型进行异常检测，基于STL规范的方法则使用上述监控逻辑进行异常检测，在攻击持续阶段检测异常就认为检测到该攻击。使用GDN模型进行异常检测实际上与π_M的监控逻辑一致，为了验证π_M对STL规范方法的影响，本文还比较了非数据驱动方法的检测性能，即仅使用

$\pi_1 \sim \pi_7$ 的监控逻辑进行异常检测。此外，在总计36种类型的攻击中，与数字孪生建模的P1~P3阶段相关的攻击只有22种，异常检测性能对比如表3所示。

从表3可以看到，对22种与过程相关的攻击，非数据驱动方法可以检测到其中的14种，未被检测到的攻击主要包括以下2类。

1) 对手改变阀门MV301的状态，在正常情况下MV301在反冲洗过程中打开，然而攻击者在没有反冲的情况下打开，这与P6相关。

2) 对手的攻击在化学品计量泵P203上进行，同时另一个泵P204正在运行，在正常情况下这2个泵中只有一个运行，而另一个在一个泵故障的情况下保持备用，攻击者关闭泵P204，由于DT没有建模水的化学性质，因此没有检测出这种攻击。

数据驱动方法则对这2类攻击具有一定的检测能力，甚至可以检测出对于未知过程部分的攻击，而使用混合方法比只使用单一方法在检测性能上更具有优势。因此融合多种认知可以提升监测异常的性能。

本文不采用传统的F1分数、精确度和召回率的检测指标，这是因为虽然数据驱动方法在上述指标中达到了优异的结果：F1 = 0.788，精确度为0.995，召回率为0.652，具有较低的误报率，但在检测到的攻击数目上只能检测出少数几种。上述问题出现的原因是攻击数据集中存在一类容易检测的攻击，而且该攻击持续时间较长，因此在计算上述指标时显示出良好的效果。

由于深度学习对训练数据具有很高的要求，训练数据量也是影响异常检测性能的重要因素。上述实验主要对比了在训练数据充足情况下各种方法的检测结果，为了验证所提方法在训练数据不足条件下依然具有较好的检测效果，本文还比较了在训练数据量较少的情况下不同数据量下的异常检测性能，如表4所示。

在数据量较少的时候，数据驱动方法检测性能几乎不可以使用，而非数据驱动方法用于异常检测则对数据量没有要求，即使在缺乏数据的时候也可以实现较好的检测结果。因此，基于STL的异常检测方法可以灵活适应于工业互联网安全的全生命周期。

异常检测定位过程如图8所示，检测过程通过检查STL的执行情况实现。对于SSSP攻击，在①处观察到系统行为不满足规范 π_6 的要求，根据其STL规范描述可以将故障定位到MV101和LIT101处；对于SSMP攻击，系统行为不满足规范 π_M 的要求，但是根据其STL规范描述无法定位故障；对于MSSP攻击，在②处观察到系统行为同时

表3　异常检测性能对比

场景	方法	检测攻击数/种	检出率
与P1~P3相关的22种攻击场景	数据驱动	9	40.9%
	非数据驱动	14	63.6%
	混合	18	81.8%
全部36种攻击场景	数据驱动	16	44.4%
	非数据驱动	14	38.9%
	混合	25	69.4%

表4　不同数据量下的异常检测性能

场景	方法	5%训练数据量		10%训练数据量	
		检测攻击数/种	检出率	检测攻击数/种	检出率
与P1~P3相关的22种攻击场景	数据驱动	2	9.00%	7	31.80%
	非数据驱动	14	63.60%	14	63.60%
	混合	16	72.70%	17	77.30%
全部36种攻击场景	数据驱动	6	16.70%	11	30.60%
	非数据驱动	14	38.90%	14	38.90%
	混合	20	55.60%	21	28.30%

不满足规范π_1和π_5的要求，根据其STL规范描述可以将故障定位到LIT101、P101和P102处，以及LIT301、FIT301和LIT401处；对于MSSP攻击，在③处观察到系统行为不满足规范π_4的要求，根据其STL规范描述可以将故障定位到LIT101、FIT101和LIT201处。

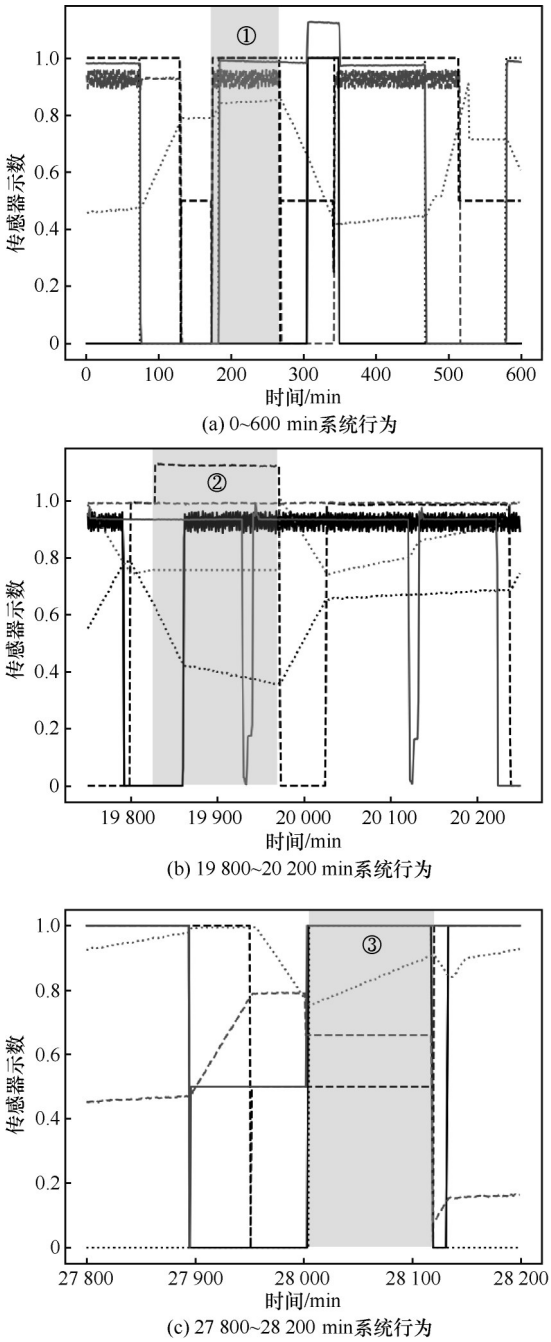


图8　异常检测定位过程

从图8可以看到，通过对STL规范的检查，对于一些简单的攻击，可以明确找到异常发生的位置；对于系统中的多个点进行攻击时，定位结果一般为部分受攻击节点或者与受攻击节点相关联的其他节点，定位过程主要是缩小检查的区域，加速系统安全员寻找异常点。然而，对于使用数据驱动方法预测的异常情况，无法对异常进行定位，需要相关领域专家的分析。

异常分类问题是根据已知故障模式来检查系统行为实现的。由于SWaT数据集中缺少设备故障的行为，以传感器故障为例，由于老化磨损和电磁干扰等因素，传感器测量值不准确，构造响应的行为数据。考虑设备故障对FIT201的影响，当LIT301显示的液位为H时控制P101关闭，传感器故障和水流的存在导致FIT201产生一段时间不稳定的流量读数。

上述故障将被STL规范π_4识别为异常，由于该故障对于系统的运行不会产生实际损失，为了与网络攻击进行区分，构造相应的STL弱规范为

$$\pi_4^-:\neg\pi_4 = \top \rightarrow \Diamond_{[1,10]}(\Box_{[1,20]}(\pi_4 = \top)) \quad (20)$$

式(20)所示规范要求当π_4不满足时，至少在10个时间步长内恢复正常，且至少需要保持20个时间步长。同时使用STL规范集合以及弱规范对系统行为进行监控，系统行为和异常分类结果如图9所示。

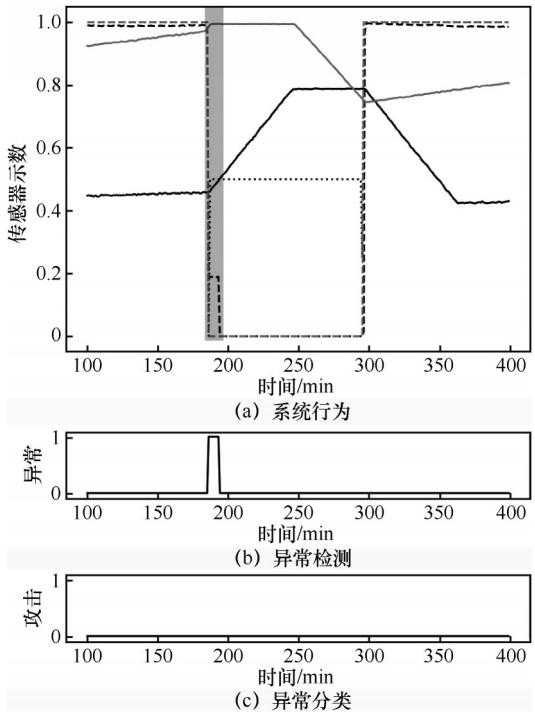


图9　系统行为和异常分类结果

图 9 中，阴影部分的系统行为显示其违反了 STL 规范 π_4，但是 π_4^- 的要求仍然满足，因此在异常检测中将其识别为异常，在异常分类中显示没有遭到恶意的网络攻击。基于 STL 弱规范的方法可以将设备故障从网络攻击中分离出来，在这种状况下仅需更换传感器而非系统停机，节约了运行维护的成本。

综上所述，基于 DT 的检测与响应方法可以有效地应用于工业互联网方面。通过实验表明，与传统基于深度学习的 IDS 相比，基于 DT 的检测与响应方法不仅在检测结果上显示出更加良好的效果，弥补了其在训练数据量较少时的缺陷，而且具备对异常的解释能力，通过异常定位和异常分类实现对异常的响应工作。

5　结束语

工业互联网面临着日益严重的安全风险，而由于工业现场对可靠性和稳定性有严格要求，其主要依赖于检测和响应技术来保证其安全性，为此本文提出了一种基于数字孪生的工业互联网检测和响应方法。首先，提出一种多模块 DT 的架构，从状态数据、专家知识、运行原理、数据预测等多角度建模工业互联网，包含系统安全运行的多方面认知；然后，引入信号时序逻辑技术将不同孪生模型的安全认知转化为标准的 STL 规范集，根据规范集对系统行为的监测实现异常检测；最后，基于 STL 形式化模型提出了相应的异常定位和异常分类的方法，帮助系统安全员迅速排除故障恢复生产。实例表明，所提方法在异常检测和响应方面非常有效。将所提方法与基于深度学习的入侵检测系统进行对比，实验结果表明，所提方法在对网络攻击的检测时检出率提高了 9.1%。

未来工作将进一步研究所提方法实用化的问题，深化其在高度异构的工业互联网场景下本文方法的实用性。拟结合工业互联网中网络日志提取与攻击链技术相关的信息进行安全监测，以在网络攻击实施之前发现问题。

参考文献：

[1] 刘奇旭, 陈艳辉, 尼杰硕, 等. 基于机器学习的工业互联网入侵检测综述[J]. 计算机研究与发展, 2022, 59(5): 994-1014.
LIU Q X, CHEN Y H, NI J S, et al. Survey on machine learning-based anomaly detection for industrial Internet[J]. Journal of Computer Research and Development, 2022, 59(5): 994-1014.

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

[3] LEE R M. Analysis of the cyber attack on the Ukrainian power grid[J]. Electricity Information Sharing and Analysis Center, 2016, 388(1-29): 3.

[4] PINTO A D, DRAGONI Y, CARCANO A. TRITON: The first ICS cyber attack on safety instrument systems[C]//Proceedings of the Black Hat USA. Piscataway: IEEE Press, 2018: 1-26.

[5] 戴翔, 倪浩杰. 基于 PPDRR 模型可攻击溯源的新型安全管理平台的设计[J]. 网络安全技术与应用, 2021(6): 42-43.
DAI X, NI H J. Design of a new security management platform based on PPDRR model and traceable attack[J]. Network Security Technology & Application, 2021(6): 42-43.

[6] DIBAJI S M, PIRANI M, FLAMHOLZ D, et al. A systems and control perspective of CPS security[J]. Annual Reviews in Control, 2019, 47: 394-411.

[7] 罗耀锋. 面向工业控制系统的入侵检测方法的研究与设计[D]. 杭州: 浙江大学, 2013.
LUO Y F. Research and design on intrusion detection methods for industry control system[D]. Hangzhou: Zhejiang University, 2013.

[8] SONG J Y, PAUL R, YUN J H, et al. CNN-based anomaly detection for packet payloads of industrial control system[J]. International Journal of Sensor Networks, 2021, 36(1): 36-49.

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

[10] 徐丽娟, 王佰玲, 杨美红, 等. 工业控制网络多模式攻击检测及异常状态评估方法[J]. 计算机研究与发展, 2021, 58(11): 2333-2349.
XU L J, WANG B L, YANG M H, et al. Multi-mode attack detection and evaluation of abnormal states for industrial control network[J]. Journal of Computer Research and Development, 2021, 58(11): 2333-2349.

[11] 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.
ZHANG M, ZENG B, ZHU C W. Design and implementation of safety monitoring and traceability system for industrial control system[J]. Cyber Security and Data Governance, 2019, 38(1): 14-19.

[12] ERIC V, SANKARAN M. Digital twin: generalization, characterization and implementation[J]. Decision Support Systems, 2021, 145: 113524.

[13] ABBURU S, BERRE A J, JACOBY M, et al. COGNITWIN – hybrid and cognitive digital twins for the process industry[C]//Proceedings of the 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). Piscataway: IEEE Press, 2020: 1-8.

[14] KUBOTA T, HAMZEH R, XU X. STEP-NC enabled machine tool digital twin[J]. Procedia CIRP, 2020, 93: 1460-1465.

[15] SNIJDERS R, PILEGGI P, BROEKHUIJSEN J, et al. Machine learning for digital twins to predict responsiveness of cyber-physical energy systems[C]//Proceedings of the 2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems. Piscataway: IEEE Press, 2020: 1-6.

[16] FRIEDERICH J, FRANCIS D P, LAZAROVA-MOLNAR S, et al. A framework for data-driven digital twins of smart manufacturing systems[J]. Computers in Industry, 2022, 136: 103586.

[17] MALER O, NICKOVIC D. Monitoring temporal properties of continuous signals[C]//International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems. Berlin: Springer, 2004: 152-166.

[18] GAUTHAMA RAMAN M R, MUJEEB A C, ADITYA M. Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation[J]. Cybersecurity, 2021, 4(1): 1-12.

[19] GRIEVES M W. Product lifecycle management: the new paradigm for enterprises[J]. International Journal of Product Development, 2005, 2: 71-84.

[20] TUEGEL E, INGRAFFEA A, EASON T, et al. Reengineering aircraft structural life prediction using a digital twin[J]. International Journal of Aerospace Engineering, 2011, 2011: 1-14.

[21] SAMIR K, MAFFEI A, ONORI M A. Real-Time asset tracking; a starting point for digital twin implementation in Manufacturing[J]. Procedia CIRP, 2019, 81: 719-723.

[22] TAO F, ZHANG M. Digital twin shop-floor: a new shop-floor paradigm towards smart manufacturing[J]. IEEE Access, 2017, 5: 20418-20427.

[23] XIE J, WANG X, YANG Z, et al. Virtual monitoring method for hydraulic supports based on digital twin theory[J]. Mining Technology, 2019, 128(2): 77-87.

[24] GUIVARCH D, MERMOZ E, MARINO Y, et al. Creation of helicopter dynamic systems digital twin using multibody simulations[J]. CIRP Annals, 2019, 68(1): 133-136.

[25] ECKHART M, EKELHART A, WEIPPL E. Enhancing cyber situational awareness for cyber-physical systems through digital twins[C]// Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). Piscataway: IEEE Press, 2019: 1222-1225.

[26] DIETZ M, VIELBERTH M, PERNUL G. Integrating digital twin security simulations in the security operations center[C]//Proceedings of the 15th International Conference on Availability, Reliability and Security. New York: ACM Press, 2020: 1-9.

[27] DIETZ M, SCHLETTE D, PERNUL G. Harnessing Digital Twin Security Simulations for systematic Cyber Threat Intelligence[C]//Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC). Piscataway: IEEE Press, 2022: 789-797.

[28] VIELBERTH M, GLAS M, DIETZ M, et al. A digital twin-based cyber range for SOC analysts[C]//Data and Applications Security and Privacy XXXV. Berlin: Springer, 2021: 293-311.

[29] XU Q H, ALI S, YUE T. Digital twin-based anomaly detection in cyber-physical systems[C]//Proceedings of the 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST). Piscataway: IEEE Press, 2021: 205-216.

[30] BIN M A, AMMAR H, VASOS V, et al. A blockchain-based data-driven fault-tolerant control system for smart factories in industry 4.0[J]. Computer Communications, 2023, 204: 158-171.

[31] 覃姜. 基于信号时序逻辑的运行时验证技术研究[D]. 广州: 华南理工大学, 2022.
QIN J. Research on runtime verification based on signal temporal logic[D]. Guangzhou: South China University of Technology, 2022.

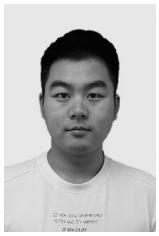
[32] GOH J, ADEPU S, JUNEJO K N, et al. A dataset to support research in the design of secure water treatment systems[C]//Critical Information Infrastructures Security: 11th International Conference. Berlin: Springer, 2017: 88-99.

[33] ADEPU S, MATHUR A. An investigation into the response of a water treatment system to cyber attacks[C]//Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE). Piscataway: IEEE Press, 2016: 141-148.

[34] ADEPU S, MATHUR A. Distributed attack detection in a water treatment plant: method and case study[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(1): 86-99.

[35] DENG A L, HOOI B. Graph neural network-based anomaly detection in multivariate time series[J]. arXiv Preprint, arXiv: 2106.06947, 2021.

[作者简介]



马佳利（1996– ），男，福建福清人，信息工程大学博士生，主要研究方向为数字孪生、网络安全、工业互联网等。

郭渊博（1975– ），男，陕西周至人，博士，信息工程大学教授、博士生导师，主要研究方向为网络安全、数据挖掘、机器学习和人工智能安全等。

方晨（1993– ），男，安徽宿松人，博士，信息工程大学讲师，主要研究方向为机器学习、隐私安全等。

陈庆礼（1998– ），男，河南新乡人，信息工程大学硕士生，主要研究方向为人工智能安全等。

张琦（1983– ），男，河南新乡人，信息工程大学副教授，主要研究方向为人工智能安全等。