 DOI: https://doi.org/10.12345/bdai.v7i1.35263

Research on Collaborative Optimization of AI Security Technology and Intelligent Defense System for Industrial Internet

Xinfei Dong

Hainan International College, Communication University of China, Lingshui, Hainan, 572400, China

Abstract

In recent years, the rapid development of industrial networks and the widespread application of artificial intelligence have led to the digitalization and intelligence of the manufacturing system in the manufacturing industry. This change has not only improved the productivity and flexibility of enterprises, but also brought unprecedented security issues to them. In view of the new problems faced by the current industrial Internet, such as massive equipment interconnection and real-time data interaction, the existing security protection methods have been difficult to effectively address. How to effectively integrate artificial intelligence and intelligent protection system is an important way to ensure the stable operation of industrial Internet.

Keywords

Industrial Internet; Artificial intelligence security technology; Intelligent Defense System

面向工业互联网的人工智能安全技术与智能防御系统协同优化研究

董欣菲

中国传媒大学海南国际学院，中国·海南 陵水 572400

摘　要

近年来，工业网络的迅猛发展与人工智能的广泛应用，使得制造业的制造体系正在向数字化和智能化方向发展。这种改变一方面提高了企业的生产率和柔性，另一方面也给企业带来了空前的安全性问题。针对当前工业互联网面临的海量设备互联和数据实时交互等新问题，现有的安全保护方法已很难有效应对。如何将人工智能与智能化防护体系进行有效融合，是保证工业互联网稳定运行的重要途径。

关键词

工业互联网；人工智能安全技术；智能防御系统

1 引言

在网络环境中，网络的安全性保护有着独特的特点和复杂的特点。首先，工控系统对实时、可靠的需求，决定了在保证安全性的前提下，不能以降低系统的性能为前提；同时，由于行业内的多源异构性和终端通信协议的多样化，使得一体化的安全保护面临着极大的困难。在实现安全保护的同时，AI 技术本身也存在着不可忽视的安全和可靠性问题。在保证其安全性和可靠性的前提下，通过人工智能手段提高其保护性能，并与已有的产业体系进行高效的协作，是目前工业互联网安全研究中急需突破的关键问题。

【作者简介】董欣菲（2005–），女，中国山东日照人，在读本科生，从事智能科学与技术研究。

2 工业互联网人工智能安全面临的关键挑战

2.1 据安全与隐私保护的脆弱性

在数据获取、传输和存储等整个流程中，数据的安全性和隐私保障都将受到极大的挑战。在数据获取方面，由于大量的传感和智能终端在生产中不断地生成多源异质的数据，且缺少对其进行密文防护和完整性认证的方法。其中，黑客可以利用中介式的攻击方式对传感数据进行修改，也可以利用旁路检测技术来获得关键的加工参数。目前，大多数行业的通信协议都具有一定的安全性问题，比如 Modbus TCP 缺少一个身份验证的方法，而 OPC UA 则具有密码能力，但是在应用时通常使用较弱的密码算法。在基于 IEEE802.15.4 标准的 WSN 中，通信链路极易被监听、被干扰，尤其是在基于 IEEE802.15.4 的 WSN 中，其安全性问题尤为突出。而在信息存储过程中，也存在着不可忽视的风险。

目前，行业普遍使用的是传统的关系式数据库结构，其存取控制方式较为粗糙，很难满足对用户进行精细的属性授权。在信息的分享与利用中，制造业企业的关键技术与运行数据存在着信息泄露的危险。已有的数据减敏方法对工业时间序列数据的影响不大，而且黑客可以通过数据相关性分析恢复其原有的信息。尤其在云计算 - 边缘协作框架下，数据在云端与云端之间的迁移，使得网络的安全性变得更加复杂，而跨域的数据更有可能违背行业规范 [1]。

2.2 智能算法模型的安全可靠性不足

在实际应用中，所采用的基于人工智能的算法模型将会受到来自各方面的威胁。而对抗式攻击则是网络攻击中最为重要的一类，它利用复杂的训练数据引导深度学习进行误判。在工业视觉测量中，由于人为干扰因素的存在，使得瑕疵识别系统可以将不合格的零件错误识别为合格零件。这些类型的网络安全漏洞给行业的质量管理体系带来了巨大的风险。而这种模式的秘密攻击也是如此，它是指在模型的学习过程中，通过在模型的学习过程中，植入一些特殊的触发机制，从而使系统产生预先设定的恶意动作。此类攻击非常隐蔽，通常情况下性能很好，只有在某些情况下才会启动。在实际应用中，其模型的稳定性也是一个非常重要的问题。但因其与现实工况之间的分布不一致，导致其在实际应用中极易发生性能退化。在多变的工况和设备老化等复杂多变的工况条件下，该方法的预报精度会急剧降低。另外，由于人工智能的“黑箱”特征，传统的人工智能建模方法不具有很好的解释性，导致用户对人工智能的依赖程度较低。在发现问题后，技术人员难以迅速找到问题的根本原因，从而降低了及时处理错误的能力。由于在建模和维护中存在版本管理混乱和测试不足等问题，使得智能算法在实际生产中面临着更加严峻的挑战 [2]。

2.3 协同防御体系的实时性与适应性缺失

已有的工业互联网安全防护系统缺乏有效的协作手段。不同类型的安全装备之间缺少有效的数据分享与联动机制，防火墙、入侵检测系统、安全审计系统等都是各自为政，很难组成一个完整的保护合力。面对多个安全领域的攻击，单一的保护手段很难有效地阻止其蔓延。工控系统对实时性的需求导致了常规信息安全策略很难在实际中得到有效地解决，而深层数据包探测等精细化的分析方法则会带来较大的时延，从而降低了工业制造的可靠性。防卫体系的适应性迫切需要提高。在实际应用中，由于电网的拓扑及设施的布置常常会随产品的要求而发生改变，因此，对其进行的安全政策的修改通常会比系统的改变要晚。传统的特征提取技术在应对新的信息攻击时已变得十分困难，且难以有效地识别出潜在的威胁。当受到袭击时，该体系缺少自动的应对措施，仍然需要依靠人为的介入来应对，从而导致了袭击事件的持续时间较长。由于设备种类繁多、体系结构复杂，使得企业难以对其进行一体化的安全态势认知，使得企业的管理者很难对其整体的安全状况进行整体把握。

3 工业互联网智能安全防御协同优化策略

3.1 构建数据全生命周期安全防护体系

在数据采集、传输、存储、处理和销毁等各个阶段，都要建立起一套完整的数据保护系统。在获取过程中，通过配置具备安全性鉴别能力的边缘获取装置，利用电子凭证技术实现对访问终端的身份认证，保证了信息来源的真实性。在生成过程中，使用轻量化的密码技术，实现对收集到的信息的即时加密，并在生成的瞬间构建起一道安全壁垒。针对实际环境中的温度、压力和流量等传感器，研究基于异常行为的数据质量评价方法，实现对被篡改和篡改的信息的准确定位，从而在根源上保证数据的完整性。在数据传递方面，采用软件定义网络（Software Definition Network, SDN）技术，建立一种安全的数据传送信道。采用中央控制器，对网络中的重要服务进行专用的传送信道，并对其进行优先保护。针对网络中存在的问题，提出了一种基于多层次结构的密码学方法，并针对不同的信息进行了分析。针对跨地域传送的关键资料，采用基于区块链的方法，构建具有抗伪造性的传送记录，以达到对整个传送过程的追踪。在数据储存方面，采取一种基于分布式密文的方式，把数据块保存在多个物理空间的结点中，这样即便某个结点遭到攻击，也能保证整个信息的安全。根据用户角色、设备类型以及所处的不同情况，构建面向用户的访问控制策略，实现对不同用户的访问权限进行动态调节。在数据的存储过程中，通过构建一个安全的多方计算平台，保证在保证信息不泄露的前提下，以密文的形式进行运算。在数据删除过程中，通过构建自动的数据生存期管理体系，对已过期的数据进行不可修复的物理毁灭，以保证失效的数据不会产生新的安全隐患 [3]。

3.2 强化智能模型的安全性与鲁棒性

在工业互联网的背景下，网络的安全和健壮性是决定网络防护体系能否可靠运行的关键因素。为了保证该模型能够在受到恶意的攻击时保持良好的性能，必须在结构的设计中加入一个安全因子。在构建深层网络架构时，需要将对抗训练模块嵌入到隐含层中，并在正向传递中引入适当的干扰，从而在学习阶段逐渐培养出对对抗样本的辨识能力。该算法可以在人为构建的非正常输入下提高其稳定性。在实现过程中，首先要从各个训练批中抽取一定数量的样本，然后利用该样本的目前的梯度来产生一个新的对抗样本，然后把它们和普通样本进行融合，从而得到更好的特征表达。实际应用中，实际应用中的实际运行数据呈现出显著的非均衡特征，其运行过程中的常规运行数据数量远远超过了运行过程中的异常值，极易造成对稀有攻击的失效。为此，我们提出了一种新的基于产生式对抗网络的信息增强方法。研究内容包括：构造产生器网络对典型的异常样本进行综合，并使用判别网络对产生的数据进行识别，并在此基础上对生

成的数据进行持续的优化。该方法可以对训练样本进行有效的互补，在保证检测率的前提下，减少虚警率。在实际应用中，还需构建对模型进行连续监控的方法，通过对其预报置信度的动态变化进行实时检测，以实现对其性能衰退的早期预警。

在实际应用中，模型的可理解性是非常重要的。在防卫体系进行非正常行为的判定时，必须有明确的判断根据，使安全分析人员可以对此作出正确的判断。因此，将注意机理与分层解译技术相结合，通过视觉化建模中的注意范围，实现对模型的判断。比如，在探测工控系统中出现的不正常运行时，该模型应该可以清楚地指出引发报警的是哪一系列的参量或运行命令及其与以往的攻击方式之间的相关性。该方法的良好可理解性，既提高了网络系统的安全性，又为网络系统的安全性决策制定提供了重要的依据。为应对网络环境下普遍存在的数据泄露、数据泄露等问题，提出了一种有效的建模防护方法。在模式的服务界面上，采用严密的接入控制机制，通过对接入次数的限定以及对接入行为的解析，来发现可能存在的恶意检测。在建模过程中加入可控的随机噪音，能够在保持其正确利用率的情况下，有效地避免了通过大规模的搜索对模型进行重建。针对基于边缘计算的轻量化建模方法，在建模过程中必须对建模参数进行加密，并保证其在执行过程中不受影响 [4]。

3.3 建立动态自适应的协同防御机制

以情景认知技术为基础，通过在工业互联网中的各个节点上配置的监控探头，实时获取业务数据、系统日志以及用户的行为等数据。在对采集到的数据进行预处理之后，将其送入解析机中，利用流式运算进行实时的处理，并利用批运算对其进行深度解析。在此基础上，构建了基于模式匹配、基于统计的异常行为检测以及基于机器学习的分类方法，从而实现对多维威胁的有效辨识。在应对威胁的层次上，提出了一种分层的决策方法。一旦发现有可能存在的安全隐患，就会立即开始认证过程，利用多源数据对威胁进行交互验证。识别出的危险按照危险程度分为若干个处理水平：危险程度较小的会发出警报，中危险的会自动进行检疫，而对于危险性较大的危险，会进行封锁作业，并开始紧急应对计划。对处理流程进行了详细地记载，建立了一个完备的处理流程，为下一步的优化工作奠定了基础。

构建闭环学习机制，以达到对防卫措施的适应性调节。不断地搜集防卫效能资料，并与防卫智能资讯相配合，对现行防卫措施之效能进行周期性的评价。将评价的评价信息反馈给决策产生器，并采用再励学习方法对识别规则及反应参数进行优化。与此同时，还将对现有的防护政策进行分级公布，首先在本地的网络上对其进行实验和检验，并对其进行进一步的扩展，以保证整个防御体系在不断的变化和变化中的稳定性和可靠性。同时，该系统也强调了人 - 机协同的设计。该系统能自动应对常见的威胁，减轻安保人员的负担；针对较复杂的袭击情景，给出具体的应对方案，并给出具体的应对方案，以帮助系统管理者做出正确的判断。通过定期开展的攻防演习，对体系的协作防护性能进行持续的检验与优化，以保证应对各种新的威胁。

4 结语

综上所述，针对工业互联网环境下的人工智能安全与智能防卫体系的协调优化问题，对保证我国重大基础设施安全，推动产业智能化进程，有着重大的现实意义。构建安全可靠、智能自适应的工业互联网安全防御系统，既能有效地解决现有安全问题，又能为我国工业互联网的创新发展奠定安全保障。在人工智能和工业互联网的深入发展下，物联网的智能安全保护将更加自主和协作，从而为建立一个更加安全、更加可靠的工业互联网的生态系统奠定坚实的基础。

参考文献

[1] 董耀聪等.基于生成式人工智能的工业互联网安全技术与应用研究[J].信息通信技术与政策, 2024, 50 (08): 32-37.

[2] 柴天佑.工业人工智能与工业互联网协同实现生产过程智能化及其未来展望[J]. 控制工程, 2023, 30 (08): 1378-1388.

[3] 唐辉荣. 基于工业互联网的白酒智慧工厂体系架构与应用[J].数字技术与应用, 2023, 41 (03): 196-199.

[4] 李伯虎等.一种新型工业互联网——智慧工业互联网[J].中国工业和信息化, 2021, (06): 54-61.