doi:10.3772/j.issn.1002-0470.2020.09.005

工业物联网安全态势评估方法研究综述①

邵子豪② 王慧强③ 孟庆川 吕宏武 冯光升

(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要 安全问题已成为阻碍工业物联网(IIOT)发展的突出问题,而安全态势评估方法能够实时监测网络状态信息,是工业物联网安全保障的重要手段。本文对工业物联网现有安全态势评估的研究成果进行了综述。首先针对国内外工业物联网的发展战略和行业现状进行了分析;其次在理论上,从安全威胁分析和安全状态2个方面对现有工业物联网安全态势评估成果进行分类,并总结了各代表性评估方法的优缺点;然后,从实际应用层面上阐述了现有代表性物联网安全工具,并对比了它们的安全态势"可视性"水平;最后对工业物联网面临的挑战及未来研究方向进行了展望。

关键词 工业物联网(IIOT);安全态势评估;威胁分析;状态监测;网络靶场

0 引 言

在开篇之前,首先明确工业物联网(industrial Internet of things,IIoT)的定义。工业物联网(IIoT)是指将具有感知、监控能力的各类采集、控制传感器或控制器,以及移动通信、智能分析等技术不断融入到工业生产过程各个环节,从而大幅提高制造效率,改善产品质量,降低产品成本和资源消耗,最终实现将传统工业提升到智能化的新阶段[1]。

近年来,工业物联网在信息安全领域方面危机四伏,黑客可以通过系统的漏洞实现对工业物联网应用进行攻击,从而达到窃取数据、破坏系统和敲诈勒索等目的。相较于传统物联网,工业物联网的概念较新,其主要依托现代成熟的物联网和工业自动化通信技术,这就意味着黑客们只需通过对传统物联网攻击的手段稍加改变即可实现对工业物联网的有效攻击。另外,由于工业物联网系统中包含着大量有价值的商业机密、用户数据等,这都吸引着各方去攻击挑战。例如,2016 年 1 月,乌克兰电网遭黑客攻击,导致3个地区数百家用户供电遭到中断。据调查,此次攻击是利用应用软件的0day漏洞嵌入BlackEnergy木马实现远程入侵,最终达到破坏目的。当前工业物联网面临的安全隐患可以分为3大类,分别是工业物联网内部结构隐患、外部网络攻击隐患和基于社会工程学的非技术渗透隐患[2]。由此可以发现,工业物联网存在着较严重的信息安全隐患,其主要特点包括涵盖范围广、涉及层面多、攻击手段多样性。因此,信息安全的风险现已经成为制约工业物联网快速推广与发展的重要障碍。

目前,我国在发展工业物联网过程中,虽然引起了足够的重视,但仍缺少建立完善的工业物联网安全态势评估机制。现有研究主要集中在基础安全理论、单一应用场景和防御异常攻击上,而对实际应用中具体的物联网安全态势评估方法的研究则较少,尤其缺乏全面准确评估复杂应用场景中存在的安全漏洞或遭受具体攻击后网络态势的评估,具体体现在缺乏对威胁态势的评估、评估平台的可靠性与可信性、多源数据融合的处理和全方位安全综合态势的分析方法研究。同时,对工业物联网安全态势评

① 国家科技重大专项(2016ZX03001023-005)和国家自然科学基金(61872104)资助项目。

② 男,1992 年生,博士生;研究方向:群智感知,工业物联网安全;E-mail:shaozihao@hrbeu.edu.cn

③ 通信作者,E-mail:wanghuiqiang@hrbeu.edu.cn

(收稿日期:2019-10-25)

估的研究不应局限在如何防止异常攻击的发生,还应通过平台的构建实现对安全漏洞或异常攻击的预测,做到防患于未然。工业物联网安全态势评估不同于传统的物联网安全态势评估技术,其主要面临的挑战具有以下特点:(1)数据连锁性强;(2)数据维度大;(3)难以监督;(4)经济影响范围广。工业物联网系统中包含着大量的工业生产资料、商业机密等极具经济价值的数据,当工业物联网遭受到攻击时其产生的经济损失往往是灾难性的。

本文针对安全问题综述了工业物联网现有的安全态势评估方法,说明了安全态势评估方法的重要性,列举了其典型应用场景,并对该领域的研究成果进行了系统的梳理和总结。按照研究的侧重点将现有研究成果分为工业物联网安全威胁分析和工业物联网安全状态监测 2 类,阐述了代表性的安全态势评估方法,分析和对比了各评估方法的性能和主要优缺点;在实际应用层面,给出了现有 7 种强化物联网安全的可视化工具。最后,对未来工业物联网网络靶场建设的挑战进行了展望。

本文第 1 节介绍当前国内外工业物联网发展战略,包括德国工业 4.0、美国工业互联网和中国制造 2025,并对其进行对比分析;第 2 节分别对基于工业物联网安全威胁分析和安全状态监测的态势评估方法进行阐述,对比分析了各研究成果的特点;第 3 节介绍了 7 种安全可视化工具;第 4 节对未来工业物联网网络靶场建设进行展望;第 5 节对全文进行了总结。

1 工业物联网发展战略

工业物联网这一概念最早起源于德国提出的工业 4.0 计划,后逐渐向世界发展,被各个国家所重视。美国通用电气公司(General Electric Company,GE)提出了工业互联网概念。中国于 2015 年提出《中国制造 2025》,旨在全面推动中国制造业及工业物联网的发展。

1.1 战略特点

(1)德国工业 4.0

所谓工业 4.0 是针对工业发展的不同阶段进行的划分。根据目前的共识,工业 1.0 是蒸汽机时代,其特点主要是通过水力和蒸汽机实现工厂机械化;工业 2.0 是电气化时代,其特点主要是在劳动分工基础上采用电力驱动产品的大规模生产;工业 3.0 是信息化时代,其特点是在升级工业 2.0 的基础上,广泛应用电子与信息技术,使制造过程自动化控制程度再进一步大幅度提高;工业 4.0 则是利用信息化技术促进产业变革的时代,也就是智能化时代。德国政府率先提出“工业 4.0”战略[3],并在 2013 年的汉诺威工业博览会上正式推出,其项目主要分为 3 大主题,分别是“智能工厂”、“智能生产”和“智能物流”。

(2)美国工业互联网

2012 年 11 月,美国通用电气公司(GE)提出了工业互联网的概念。2013 年 6 月,GE 公司整合了智能机器、传感器和高级分析的功能,推出了第 1 个大数据与分析平台,夯实了资产性能管理系统高效运行的基础,明确了美国工业互联网的具体目标。根据美国工业互联网的定义,其主要包含 3 大要素:“智能机器”、“高级分析”和“工作人员”[4]。

(3)中国制造 2025

2015 年 5 月 19 日,国务院正式印发《中国制造 2025》,“中国制造 2025”是中国政府实施制造强国战略的第 1 个 10 年行动纲领,其根本目标是为了改变中国制造业“大而不强”的局面。从布局上看,“中国制造 2025”战略搭建了“一二三四五五十”的总体结构:即 1 个目标、2 化融合发展(信息化和工业化)、“3 步走”战略、4 项原则、5 条方针与 5 大工程和 10 大领域[5]。

1.2 战略对比

表 1 分别从概念提出时间、目标、侧重点、核心和意义这 5 个方面对比了德国工业 4.0、美国工业互联网和中国制造 2025。

综上,无论“中国制造 2025”、“德国工业 4.0”或是“美国工业互联网”,都是根据当前国内、国外产业形势研判后作出的决策,其核心方向都是面向新时代新方向,面向第 4 次工业革命的国家制造业转型升级战略,都是为了在新时代的背景下占据全球智能制造的先机,成为新时代的智造强国。未来

各国在工业制造业的背景下还会存在着大量的竞争与合作。

表 1 三者对比

国家	德国	美国	中国
概念	德国工业 4.0	工业互联网	中国制造 2025
时间	2013 年 4 月	2012 年 11 月	2014 年 12 月
目标	保证制造业的领先地位	实现在未来新的制造业中的领导地位	跻身世界制造强国行列
侧重点	建立信息物理系统(CPS),实现虚拟网络与现实物理世界的高度融合。将所有资源与人紧密联系在一起,从而创造物联网及相关服务,将生产工厂转变为一个智能环境。	以政府战略为主推进器,通过产业联盟打通技术壁垒。希望借助网络和数据的力量提升整个工业的价值创造能力。更好地促进物理世界和数字世界的融合。	提高国家制造业创新能力、推进信息化与工业化深度融合、强化工业基础能力、加强质量品牌建设、全面推行绿色制造、大力推动重点领域突破发展、深入推进制造业结构调整、积极发展服务型制造和生产性服务业、提高制造业国际化发展水平等。
核心	产业集成	鼓励创新	实现中国制造强国
意义	使德国成为新一代工业生产技术的供应国和主导市场,在继续保持国内制造业发展的前提下再次提升它的全球竞争力。	通过美国在信息产业与先进制造业的优势,通过信息技术的改进重塑世界工业格局。	使中国迈入制造强国行列,为到 2045 年将中国建成具有全球引领和影响力的制造强国奠定坚实基础。
共同点	注重 CPS 技术在未来工业发展中的核心地位,在信息化、智能化、网络化、全球化等方面投入了大量的物力、人力、财力进行创新研究。		

2 工业物联网安全态势评估

近年来,随着工业物联网的高速发展,安全问题日益突出,对工业安全态势评估技术已得到了高度的重视,工业物联网安全态势评估作为构筑工业物联网网络安全体系中的关键环节,有着不可替代的重要作用和意义。工业物联网安全态势评估技术的应用可以综合分析各个方面的安全因素,实现对不同层次、规模、适用范围的网络或系统进行分析。同时,还可以从整体上动态反映现阶段的工业网络安全实际状况。对当前网络的评估结果一般具有实时性、综合性、多角度性、多粒度性等特点。

物联网的快速发展对不同行业的发展及其全球经济起到了重要推进作用,如 Alharam 等人[6]将物联网应用于医疗行业中,分析了现有医疗行业中物联网的网络安全体系结构的复杂性并对其进行优化,提升了现有医疗行业的办公效率。然而,安全问题的频发引起了社会各界对工业物联网安全态势评估方法的广泛关注,工业物联网安全威胁分析和工业物联网安全状态监测研究是工业物联网安全态势评估的 2 大关键技术。

2.1 安全威胁分析

现阶段对工业物联网安全威胁的研究取得了大量的研究成果,Samaila 等人[7]总结了现有物联网在不同领域的充分应用,而现有的工业物联网体系结构中存在的安全威胁将严重制约工业物联网安全态势评估的准确性,因此该研究针对不安全的 Web 接口和网络服务威胁、路由协议威胁、传输信息威胁、环境威胁、GPS 干扰威胁、标签跟踪和克隆威胁及不适当的网络配置威胁这 6 种威胁提出了不同的安全对策,保障了工业物联网安全态势评估的顺利执行,但对威胁预测机制的构建并未提及。Shahzad 等人[8]总结了当前物联网体系结构及工业物联网态势监测解决方案的必要设计要求,认为对工业物联网安全态势评估需具有实时性、健壮性和控制成本的特点。同时,还列举了当前态势监测存在的设计

挑战并尝试着给出一些解决方案。但是该团队从终端设备的角度出发,对状态监测系统进行设计,缺少相关安全漏洞或异常攻击预测的研究。在具体的安全威胁分析中,Condry 等人[9]针对物联网端点使用智能物联网设备进行用户访问控制时容易受到重播、中间人和拒绝服务攻击的问题,提出了一种将智能物联网设备功能与控制系统网关相结合的模型,该模型使用实时响应来实现安全控制的操作。他们所提出的解决方案混合使用了计算、加密、信号/图像处理以及用于身份验证和授权功能的通信功能,并将其模型部署在现有工业物联网环境中,实现了对其设备的控制、制造、运输和零售的跟踪。但目前的模型部署仍处于小范围的使用,其实用性有待考证。

针对中国工业物联网的特殊性,中国工程院院士倪光南[10]以工业控制系统为切入点,详细分析了当前工业物联网面临的安全问题和国家网络安全战略,阐述了核心技术即桌面计算机技术国产化的重要性,给出了替代现有体系的途径和关键技术,并对我国网络安全和信息技术的未来发展提出了建设性的建议。倪光南认为“自主可控不等于一定安全,但不自主可控一定不安全”。因此,只有将自主可控作为网络安全的必然要求,才能构建真正意义上的工业物联网安全态势评估体系。其给出的安全态势评估技术主要侧重于如何进行攻击的防御,但对威胁的预测并未提及。杨悦梅等人[11]对工业物联网的安全防护体系做了层次化的研究,详细分析了工业物联网感知层、传输层、处理层、综合应用层及控制系统的安全架构,并对工业物联网安全防护产品的开发提出了建议,说明了基于工业物联网安全防护的设备开发与软件开发的重要性与必要性,该研究侧重于对安全防护体系的构建,但对相关威胁检测技术的研究并未提及。王展鹏等人[12]先对当前的工业物联网安全威胁进行分析,接着引出入侵检测技术对工业物联网安全态势评估的重要性,采用了多种基于机器学习算法的入侵检测技术,通过实验对每种算法的应用效果进行了展示,为工业物联网态势感知入侵检测技术的研究提供了宝贵建议。但他们多使用现有的机器学习算法进行,对已知攻击的检测效果较好,但对未知攻击的检测效果并未提及。

在实际场景的应用中,McNeil[13]针对工厂自动化系统的可用性与安全性展开研究,针对系统安全设计、系统性能保证、固件升级、不安全协议、大量设备和供应商管理这 6 个问题,分别给出了解决意见,旨在帮助管理者确保工业物联网部署的安全。虽然该研究保证了工厂自动化系统的可用性与安全性,但缺乏建立一种基于当前态势对未来威胁进行预测的防范机制。Vishal 等人[14]针对现有无人机工业物联网缺乏提供无人机的状态验证,识别行为异常及准确评估漏洞的安全策略,提出一种基于 Petri 网的 N 层分层上下文感知模型,该模型不仅可以评估无人机的行为,还可以利用安全策略来评估其潜在的漏洞。但目前该方法只适用于无人机工业物联网安全态势的评估中,缺少更广泛的应用范围。孟光磊等人[15]针对无人机的空战态势,提出一种基于混合动态贝叶斯网络的评估模型,并通过实验证明了该模型具有快速性、有效性和容错性的特点。但随着系统的日益复杂化,未来无人机空战决策系统对安全态势评估的实时性和准确性会提出更高的要求,文中所提方法的参数学习效率将是未来研究的一个难点。

2.2 安全状态监测

在工业物联网安全状态监测研究中,现有研究多是从数据流的角度出发,通过监测数据的状态实现对工业物联网安全状态的监测。Emilia 等人[16]讨论了一个基于传感器的自动化系统状态监测应用实例,针对复杂大数据流的处理问题,提出一种验证技术,以此增强分类算法对特征提取的准确性,提升了对工业物联网安全状态的监测准确性,但对验证技术带来的额外开销并未进行分析。Raptis 等人[17]从数据保障的角度出发,提出了一种分布式路径重配置和数据转发方法,通过改善工业物联网网络中的数据转发的能耗和数据传输成功率,保障了工业物联网网络的高效传输,从而保障了工业物联网安全状态,但并没有考虑到数据转发过程中隐私泄露的问题。Jiang 等人[18]在可靠性竞争的背景下,提出了一种新的基于 BIERTE 的路由协议,旨在

通过有损无线介质提供确定性的网络，从而保证工业物联网的安全状态。同样，该协议对增加路径产生的额外开销及复杂环境对数据传输的影响并未进行考虑。Pinto 等人[19]认为现有解决工业物联网安全态势的评估都忽略了实时性的问题，该研究提出了一种信任区的体系结构，将可信执行环境的基本构建块作为实时操作系统的低优先级线程来实现，修改实时操作系统的线程以支持受信任的应用程序，并仅在空闲期间进行执行环境的调度。实验表明，在系统实时性几乎保持不变的情况下，安全性得到了保证。但在智能工业环境中，如何保证边缘设备的可信性仍是一个急需解决的问题。

针对工业物联网安全状态监测中存在大量多源数据的问题，文圳[20]设计了一种基于工业物联网的数据监测和质量回溯系统，并使用新一代的界面框架实现对生产线的实时监测，保障对生产质量的监测，提升了对工业物联网安全态势的感知准确性，但生产数据采集系统中的数据量问题将是一个亟需解决的问题。王春媚[21]提出一种自适应无迹卡尔曼滤波算法，提升了实测数据的精度，减少了数据冗余与测量误差，为工业物联网态势评估的顺利进行提供了数据保障，但如何调整相应数学模型的系数将决定着算法对数据融合处理的准确度。沙乐天等人[22]针对工业物联网安全态势评估中的后门隐私问题进行研究，提出了一种基于工业物联网环境下后门隐私泄露的感知方法。该方法首先给出后门隐私的基本定义，在此基础上根据数据特征定义若干基本属性，并根据静态及动态数据流安全威胁抽取上层语义，提出了一种泄露度的概念，以此计算安全级别和安全阈值，实现后门隐私信息在静态二进制结构及动态数据流向中的泄露场景感知，达到对工业物联网安全态势评估的目的。但感知方法的实时性和预测性功能并未提及。余雪晨[23]针对当前工业物联网控制系统存在的安全问题，提出一种可信系统平台的整体架构。从评估用户行为的角度出发，对用户行为的可信性与行为异常检测进行评估，通过计算用户行为的可信属性和用户异常行为检测的分类，为提高工业物联网模式下工业控制系统的用户行为可信度提供方法与技术上的支持，从而为实现对工业物联网安全态势的评估提供了用户可信保障，但缺乏对数据的高效处理及保障数据的安全。龚淑蕾等人[24]以提升工厂整体效益为目标，利用窄带物联网低功耗等特性，灵活部署传感设备，建设基于蜂窝工业物联网的制造执行系统，实现“人、机、料、法、环”信息的闭环处理，并对整个生产流程的工业大数据进行建模、分析和处理。通过工业大数据流的分析实现对当前安全态势的感知。但在面临攻击时应采取怎样的措施并未提及。

在实际场景的应用中，Signoretti 等人[25]将工业物联网应用于汽车行业，提出了一种边缘 OBD-II 装置的性能评估方法，通过改善服务器请求的响应时间，实现客户反馈车辆应用程式数据的高效处理，但在实验中只是在较小的实际场景中进行了验证，对设备的可靠性也并没有进行考虑。马亚楠[26]针对煤矿生产作业环境中的复杂危险环境，提出了一种对煤矿井下环境监测的设计方案，该方案不仅包含一种适合安全监测的物联网节点部署方法，还形成了一种基于模糊粗糙-灰色关联的决策级融合算法，实现了对复杂多源信息的高效处理，保障了对煤矿生产环境的安全态势评估。但在系统的可靠性分析中，只分析了关键节点和数据传输的可靠性，缺乏对系统整体可靠性的分析。张涛等人[27]在经典工业物联网结构基础上，提出了一种基于安全云的工业物联网分析监控系统，重点解决了传感信号接收问题、工业云网络的利用和工业网络安全保障技术，并将其应用于电力调度物联网系统中，取得了较好的性能。

综上，目前国内、外对工业物联网安全态势理论评估方法的研究主要集中在工业物联网安全威胁分析和工业物联网安全状态监测研究上，相关研究成果在车辆、工厂和医疗中都得到了广泛的应用。工业物联网安全的威胁分析主要针对的是如何识别威胁的研究，但缺乏对相关漏洞与威胁的预测的研究。对工业物联网安全状态的监测多以数据流为基础，缺乏对状态监测的可靠性与可信性进行研究。总体来看，当前工业环境下的工业物联网安全态势评估方法的研究多为防御手段，主要是问题发生后针对漏洞进行有效的控制和解决。网络安全态势评估的

挑战和突破口是研究主动实施防护新模型、新技术和新方法,通过风险评估手段对当前安全态势进行判断,并依据判断结果实施主动预测防御的安全防护体系。

2.3 安全态势评估方法对比

表2根据各研究者对现有工业物联网安全态势评估方法的主要研究点及针对领域进行了总结,表3则对现有研究技术进行进一步细分,分别从文章所属类别、主要优点和主要缺点3个方面进行了汇总对比。

表2 安全态势评估方法分类

方法分类	文献	研究点	针对领域
安全威胁分析	[7]	总结现有物联网在不同领域的应用,针对6种威胁提出了不同的安全对策。	智能环境监测、智能医疗、智能消防、智能制造、智能可穿戴设备、智能玩具
	[8]	总结当前物联网体系结构及工业物联网态势监测解决方案的必要设计要求。	工业物联网态势监测
	[9]	提出一种将智能物联网设备功能与控制系统网关相结合的模型。	智能物联网设备访问安全
	[10]	详细分析当前工业物联网面临的安全问题和国家网络安全战略,阐述核心技术——桌面计算机技术国产化的重要性,给出了替代现有体系的途径和关键技术。	工业控制系统——桌面计算机技术
	[11]	对工业物联网的安全防护体系做了层次化的研究,阐明基于工业物联网安全防护的设备开发与软件开发的重要性与必要性。	工业物联网安全防护设备与软件
	[12]	在工业物联网态势感知中,引入多种基于机器学习的入侵检测技术,保障安全态势评估准确性。	工业物联网入侵检测技术
	[13]	针对工厂自动化系统的可用性与安全性展开研究,对不同问题分别给出了解决意见。	工厂自动化系统安全性
	[14]	提出一种基于Petri网的N层分层上下文感知模型。	无人机状态验证
	[15]	提出一种基于混合动态贝叶斯网络的评估模型。	无人机空战态势决策
安全状态监测	[16]	讨论一个基于传感器的自动化系统状态监测应用实例,针对复杂大数据流的处理问题,提出一种验证技术,增强分类算法对特征提取的准确性。	自动化系统验证技术
	[17]	提出一种分布式路径重配置和数据转发方法,保障工业物联网网络的高效传输。	工业物联网网络数据转发与传输
	[18]	提出一种新的基于BIERTE的路由协议,旨在通过有损无线介质提供确定性的网络。	工业物联网网络安全协议
	[19]	考虑工业物联网安全态势的评估的实时性问题,提出一种信任区的体系结构。	工业物联网安全体系结构保障
	[20]	设计一种基于工业物联网的数据监测和质量回溯系统。	工业物联网生产质量监测
	[21]	提出一种自适应无迹卡尔曼滤波算法,提升了实测数据的精度,减少了数据冗余与测量误差。	工业物联网数据融合
	[22]	提出一种基于工业物联网环境下后门隐私泄露的感知方法。	工业物联网后门隐私安全
	[23]	提出一种可信系统平台的整体架构。	工业物联网用户行为可信评估
	[24]	提出一种基于蜂窝工业物联网的智能工厂解决方案。	工厂传感设备部署
	[25]	提出一种边缘OBD-II装置的性能评估方法。	车联网
	[26]	针对煤矿生产作业环境中的复杂危险环境,提出了一种对煤矿井下环境监测的设计方案。	煤矿井下环境监测
	[27]	提出一种基于安全云的工业物联网分析监控系统。	工业物联网结构设计

表 3 安全态势评估方法的优缺点

类别分类	文献	主要优点	主要缺点
综述型	[7]	涵盖领域广,针对不同威胁提出了不同安全对策,针对性强。	缺乏对威胁预测机制的关注。
	[8]	从终端设备的角度出发,对状态监测系统进行设计,确定了态势评估需具备实时性、健壮性和控制成本的特点。	缺少相关安全漏洞或异常攻击预测的研究。
	[11]	从工业物联网 5 层架构体系进行分析,具有全面性。	缺乏对相关威胁检测技术的介绍。
	[12]	已知攻击的检测效果较好,将入侵检测技术与机器学习算法相结合。	但对未知攻击的检测效果并未提及。
	[13]	针对 6 个问题,分别给出了不同的解决意见,针对性强。	缺乏对未来威胁进行预测。
技术型	[9]	实时性好,安全性高。	模型部署处于一个小范围的使用,实用性有待考证。
	[10]	为我国网络安全与信息技术发展指明道路。	关键技术重防御,轻预测。
	[14]	可识别行为异常并准确评估安全漏洞。	应用领域单一。
	[15]	提升无人机空战决策的准确性。	参数学习方法的高效性问题难以解决。
	[16]	增强数据特征提取的准确性。	缺乏对验证技术引入后额外开销的考虑。
	[17]	改善数据转发能耗,提升传输成功率。	缺乏考虑数据转发过程中隐私泄露的问题。
	[18]	保障网络的确定性。	缺少对增加路径产生的额外开销及复杂环境对数据传输影响的考虑。
	[19]	提升工业物联网的安全性。	缺乏对边缘设备可信性的研究,难以保障数据质量。
	[20]	实现对生产线实时监测,保障生产质量。	数据量膨胀问题。
	[21]	去除数据冗余,提升数据精度。	数学模型系数调整困难。
	[22]	保障了工业物联网后门隐私的安全。	缺乏感知实时性与预测性。
	[23]	对用户异常行为及可信性检测准确率高。	缺乏数据预处理与数据安全性的保护。
	[24]	提升了工厂整体效益。	未提及面临攻击时应采取怎样的措施。
	[25]	实现车联网数据的高效处理。	实验只是在较小的实际场景中进行了验证,缺乏对设备的可靠性考虑。
	[26]	提升了多源信息融合效率,分析了关键节点和数据传输的可靠性。	缺乏对系统整体可靠性的分析。
	[27]	解决了电力调度物联网的信号接收问题。	应用场景单一。

3 安全可视化工具

由于物联网设备的快速增长,未知领域的逐渐扩大,对安全的“可视性”显得日益重要,可视性意味着连接到网络的所有设备及运行在所有这些设备上的软件可能使用的云服务等等都可以直观地呈现。然而传统的网络可视性工具(tap 或 span 端口)可以提供对网络的访问,但缺乏分析功能,难以满足物联网可视化的需求。因此,表 4 列出了增强可视性的物联网安全性工具,并对其功能、特点与不足进行了分析。

4 未来前景展望

工业物联网给用户带来便利的同时也为安全态势评估方法提出了新的要求,很多具有挑战性的问题有待进一步研究。其中,工业物联网网络靶场的建设将是国家工业物联网网络信息安全战略的迫切需要,是实现工业物联网安全态势准确评估的必备

平台,是提供我国工业物联网网络安全能力的重要战略措施,是建设工业强国的安全保障。

表4 可视化工具对比

工具名称	功能	特点	不足
AppDynamics[28]	应用性能管理;最终用户监控;基础设施可视性;业务监控。	代码级监控	难以分析网络中不活跃的设备状态。
ForeScout CounterACT[29]	准确发现,严格控制;全面协调;集中管理;掌握详情。	即时监测连接至网络的设备	服务范围较小,普适性低。
Fortinet[30]	远程控制访问;多源信息融合;追踪设备及其数据流量。	高性能安全保护;顶级工业控制保护;具有工业物联网版本的Fortigate。	费用较高。
LogRhythm Netmon[31]	强大的网络可视性;灵活部署的网络监控	针对不同企业规模提供不同的可视化工具;兼容性高。	分为收费版本与不收费版本,不收费版本的宽带和存储容量低。
PwnieExpress[32]	识别周围设备;评估潜在的安全威胁;智能保护。	设备适用范围广;设备识别方法具有多样性。	对无线网及其设备保护性好,缺乏对工业物联网的具体应用。
Trustwave[33]	资产识别;弱点识别;易于部署;降低设备受损风险。	托管服务;提供个性化服务。	缺乏专门针对工业物联网安全的检测工具。
Zingbox[34]	安全保障;智能管理;优化处理。	第一个通过自动识别、保护、管理和优化工业网络设备来确保面对网络风险的运营连续性。	缺乏对安全威胁的预测模块。

网络靶场一般是针对网络攻防演练和网络新技术评测的重要基础设施,主要供政府、军队、企业等使用,用来提高网络和信息系统的稳定性、安全性等性能[35]。针对工业物联网的相关特点,建设工业物联网网络靶场,可以为金融、交通、电信、电力、能源等国家工业关键基础设施安全体系建设提供基础分析、架构设计、系统测试、安全评估、运行维护等全生命周期的保障服务,解决难以在真实环境中对复杂大规模异构网络和用户进行逼真的模拟和测试以及风险评估等问题,实现国家工业物联网安全能力的整体跃升。未来,需对靶场建设和运行过程中涉及到的网络情景实时复现、多维度多部门测试、靶场资源动态管理等一系列关键支撑技术进行研究和突破,具体如下:

(1)复杂异构网络快速复现及重构技术

工业物联网网络靶场相对传统的网络靶场而言具有领域专业性高、部门差异性大、利润驱动性强、参与者负担小等特征。与此同时,参与测试的平台通常需要具备灵活重组和快速重构的能力,这最终会导致复现目标类型复杂、异构多样。因此,为避免"烟囱式"的目标复现提供一种统一共享的物理网络设施构建和开展大规模复杂网络快速可重构复现技术是十分紧迫的。

(2)网络空间安全自动化多维度测试技术

在工业物联网网络靶场建设中,不同的用户部门对安全的需求往往是具有差异性的,未来的一个关键挑战是如何更好地利用现有技术实现对不同用户的测试需求。因此,未来的研究方向可包含:①将人工智能、决策论等相关理论方法和技术手段引入平台的测试评估过程,构建科学合理的测试评估模型;②构建自动化调用平台的计算、存储资源和漏洞库、知识库等资源,以及各类测试工具,自动从效果、效率、成本、难易程度等多个维度综合衡量,实现对设备级、子系统级、系统级、体系级各个级别的网络空间安全性试验验证,提高测试评估的客观性、准确性与效率。

(3)靶场资源动态配置与擦除相结合的资源管理技术

在工业物联网网络靶场资源管理中,平台提供的存储、信息、计算等资源具有数据量大、异构性和高度复杂的特点,因此,未来的研究方向可包含:①共用资源的集中处理与灵活调用。资源管控具有高复杂度与高度集中化的特点,因此,可通过对异构资源进行抽象描述并进行统一标识,形成资源目录,同时建立靶场资源管理平台,实现对靶场资源的发现与自动推送、实时监视、动态调度、智能控制;②数据冗余擦除。针对工业物联网网络靶场资源管理中存在大量的冗余数据,为防止试验参数和信息外泄,形成封闭与隔离测试的安全保障,需为试验中非易失性存储数据提供一种可以自动擦除数据、拆除测试平台、回收所用资源的安全擦除技术。

(4)网络靶场安全度量和评估基准

现有研究中很少采用统一的度量标准来实现工业物联网网络靶场的安全评估,这使得很难对工业物联网网络靶场的有效性进行客观性评价。如何形成一个统一的度量方案来量化工业物联网网络靶场的有效性,将是一个长期的研究目标。为了获得这样的度量标准,目前使用的靶场安全度量需要进行校验,以确定一种规范化的评价指标和输入参数。此外,可以借鉴具有普适性的物联网领域或者具有特殊性的军事网络的靶场安全评估方法。未来,针对工业物联网领域通用的安全度量指标框架将进一步被研究。

5 结 论

随着工业物联网技术在各个领域的广泛应用,其面临的安全问题将成为工业物联网发展过程中的核心问题与重大挑战。本文对现有工业物联网安全态势评估技术的研究成果进行了综述,主要工作包括:(1)介绍了德国、美国和中国工业物联网发展战略并对三者的战略进行了对比分析;(2)针对现有工业物联网安全态势评估方法按照基于安全威胁分析和安全状态监测 2 种方法进行分类,详细阐述了代表性的安全态势评估方法,并总结了各方法的主要优缺点;(3)列举了现有 7 种强化物联网安全的可视化工具,总结了其功能、特点与不足;(4)分析了工业物联网网络靶场的必要性,并针对未来工业物联网领域网络靶场建设中的关键技术进行了展望。

参考文献

[1] Dorsemaine B, Gaulier J P, Wary J P, et al. Internet of things: a definition & taxonomy[C]//International Conference on Next Generation Mobile Applications, Cambridge, UK, 2016:72-77

[2] 张猛. 工业物联网安全风险分析及对策研究[J]. 中国工业评论, 2017(4):42-50

[3] Christian F. Industry 4.0: the digital german ideology [J]. *Triple C: Communication, Capitalism and Critique*. 2018, 16(1):280-289

[4] Li J Q, Yu F R, Deng G, et al. Industrial internet: a survey on the enabling technologies, applications, and challenges[J]. *IEEE Communications Surveys and Tutorials*, 2017, 19(3):1504-1526

[5] 李金华. 德国"工业 4.0"与"中国制造 2025"的比较及启示[J]. 中国地质大学学报(社会科学版), 2015, 15(5):71-79

[6] Alharam A K, Elmadany W. Complexity of cyber security architecture for IoT healthcare industry: a comparative study[C]//IEEE International Conference on Future Internet of Things & Cloud: Workshops, Prague, Czech, 2017: 246-250

[7] Samaila M G, Jo SequeirosB F, Freire M M, et al. Security threats and possible countermeasures in IoT applications covering different industry domains[C]//Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 2018: 1-9

[8] Shahzad K, Nils M O. Condition monitoring in industry 4.0-design challenges and possibilities: a case study[C]//2018 Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy, 2018: 101-106

[9] Condry M W, Nelson C B. Using smart edge IoT devices for safer, rapid response with industry IoT control operations[J]. *Proceedings of the IEEE*, 2016, 104(5):938-946

[10] 倪光南. 工业物联网安全与核心技术国产化[J]. 物联网学报, 2018, 2(2):5-11

[11] 杨悦梅, 宋执环. 工业物联网安全防护体系研究[J]. 淮海工学院学报(自然科学版), 2015, 24(2):36-39

[12] 王展鹏, 吴红光, 马蓓娇, 等. 基于机器学习的工业物联网入侵检测技术研究[J]. 智能物联技术, 2018, 1(2):17-21

[13] McNeil P. Secure IoT deployment in the cement industry [C]//2017 IEEE-IAS/PCA Cement Industry Technical Conference, Calgary, Canada, 2017: 1-12

[14] Vishal S, Gaurav C, Yongho K, et al. Behaviour and Vulnerability Assessment of Drones-enabled Industrial Internet of Things (IIoT)[J]. *IEEE Access*, 2018, 6: 43368-43383

[15] 孟光磊, 马晓玉, 刘昕, 等. 基于混合动态贝叶斯网的无人机空战态势评估[J]. 指挥控制与仿真, 2017,

39(4):1-6, 39
[16] Emilia G D, Gaspari A. Data validation techniques for measurements systems operating in a industry 4.0 scenario a condition monitoring application[C]//2018 Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy, 2018:112-116
[17] Raptis T P, Passarella A, Conti M. Distributed path reconfiguration and data forwarding in industrial IoT networks[C]//International Conference on Wired/Wireless Internet Communication, Boston, USA, 2018:29-41
[18] Jiang H, Brodard Z, Chang T, et al. Competition: controlled replication for higher reliability and predictability in industrial IoT networks[C]//International Conference on Embedded Wireless Systems and Networks, Uppsala, Sweden, 2017: 282-283
[19] Pinto S, Gomes T, Pereira J, et al. IIoTEED: an enhanced, trusted execution environment for industrial IoT edge devices[J]. *IEEE Internet Computing*, 2017, 21(1):40-47
[20] 文圳. 基于工业物联网的数据监测和质量回溯系统的设计与应用[D]. 成都:电子科技大学机械与电气工程学院, 2017: 1-22
[21] 王春媚. 基于自适应无迹卡尔曼算法的工业物联网数据融合处理[J]. 电气传动自动化, 2016,38(4):43-47
[22] 沙乐天, 肖甫, 陈伟, 等. 面向工业物联网环境下后门隐私泄露感知方法[J]. 软件学报, 2018, 29(7): 41-57
[23] 余雪晨. 基于可信评估的工业物联网用户行为异常检测方法研究[D]. 广州:广东工业大学信息工程学院, 2014: 8-17
[24] 龚淑蕾,李堃,童恩,等. 基于蜂窝工业物联网的智能工厂解决方案[J]. 物联网学报, 2019,3(2):108-114
[25] Signoretti G, Silva M, Dias A, et al. Performance evaluation of an edge OBD-II device for industry 4.0[C]//2019 Workshop on Metrology for Industry 4.0 and IoT, Naples, Italy, 2019: 432-437
[26] 马亚楠. 物联网安全监测系统的设计优化与关键技术的研究与应用[D]. 北京:华北科技学院安全工程学院, 2017: 12-20
[27] 张涛, 庄严, 秦志军, 等. 基于安全云的工业物联网分析监控系统[J]. 自动化技术与应用, 2018, 37(11):86-90
[28] Appdynamics I. AppDynamics opens its application management platform with AppDyamics exchange ecosystem and AppSphere user community[J]. *Insurance Broadcasting*, 2013: 1-2
[29] ForeScout CounterACT. ForeScout Technologies[EB/OL]. https://zh.forescout.com/products/: ForeScout, 2019
[30] Tam K, Mcalpine K, Basile R, et al. UTM Security with Fortinet: Mastering FortiOS[M]. Syngress Publishing, 2012: 1-2
[31] LogRhythm. LogRhythm[EB/OL]. https://logrhythm.com/: LogRhythm, 2019
[32] Hamid H R H, Abdullah N Y. Portable toolkit for penetration testing and firewall configuration[C]//2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic, Jakarata, Indonesia, 2015: 90-94
[33] Trustwave. Trustwave global Security Report retrieved from[EB/OL]. https://www.trustwave.com/en-us/capabilities/by-topic/securing-the-iot-landscape/: Trustwave, 2016
[34] Zingbox. Zingbox[EB/OL]. https://www.zingbox.com/: Zingbox, 2019
[35] 盛威. 国外网络靶场现状与趋势分析[J]. 网信军民融合, 2017, 4(4):71-75

A survey on security situation evaluation method for industrial Internet of things

Shao Zihao, Wang Huiqiang, Meng Qingchuan, Lv Hongwu, Feng Guangsheng
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)

Abstract

Security issue has become a prominent problem hindering the development of the industrial Internet of things (IIoT). Through the applications of security situation evaluation methods, real-time monitoring of network status information can be realized, which is an important approach to ensure the security of IIoT. This paper surveys state-of-the-art security situation evaluation methods in IIoT. First, the paper analyzes the development strategy and industry status of IIoT in China and overseas. Second, existing works are classified into two categories from a theoretical perspective, including security threat analysis and security status monitoring, and the advantages and shortcomings of each representative evaluation method are summarized. Then, from a practical application perspective, the paper describes the existing representative visualization tools, and compares the 'visibility' of security situations. Finally, the challenges of IIoT development and promising future research directions are prospected.

Key words: industrial Internet of things (IIoT), security situation evaluation, threat analysis, status monitoring, cyber range