DOI:10.7544/issn1000-1239.2016.20150465
53(9):2039-2054,2016

工业控制系统入侵检测技术综述

杨 安[1,2] 孙利民[1] 王小山[1,2] 石志强[1]

[1](物联网信息安全技术北京市重点实验室(中国科学院信息工程研究所) 北京 100093)

[2](中国科学院大学 北京 100049)

(yangan@iie.ac.cn)

Intrusion Detection Techniques for Industrial Control Systems

Yang An[1,2], Sun Limin[1], Wang Xiaoshan[1,2], and Shi Zhiqiang[1]

[1](*Key Laboratory of IOT Information Security Technology* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)

[2](*University of Chinese Academy of Sciences*, *Beijing* 100049)

Abstract In recent decades, with the introduction of Ethernet and the more close connection with external network, an increasingly larger number of vulnerabilities have been found in the industrial control system (ICS), exposing its serious security problem. These security issues cannot be handled completely due to the variety of the vulnerability. Therefore, we must construct the defense-in-depth system for ICS. In particular, the intrusion detection system (IDS) is one of the most important parts in the defense-in-depth system of ICS. The IDS is able to discover the potential intrusion by misuse detection and anomaly detection. In this survey, we analyze the architecture and characteristics of ICS and provide the detailed descriptions of the security concept of ICS. Then, according to the characteristics of ICS, we put forward a clear requirement of ICS IDS and elaborate its connotation. Moreover, we categorize the existing IDS methods based on the detection strategy, including traffic detection, protocol detection and equipment state detection. In each category, we analyze the detection technique and discuss the detection algorithm. Finally, for future work, from the perspective of the disadvantages of current solutions and the constraints for ICS applications, we summarize some research trends of ICS IDS from the aspects of performance metric, detection technique and detection architecture.

Key words industrial control system (ICS); intrusion detection system (IDS); traffic detection; protocol detection; equipment state detection

摘 要 随着工业控制系统(industrial control systems, ICS)的逐渐开放,暴露出严重的脆弱性问题.入侵检测作为重要的安全防御措施,根据误用和行为检测,可及时发现可能或潜在的入侵行为.首先,介绍

收稿日期:2015-06-09;**修回日期**:2015-10-30

基金项目:国家自然科学基金项目(61472418);中国科学院国防科技创新基金重点基金项目(CXJJ-14-Z68);中国科学院战略性先导科技专项基金项目(XDA06040101);新疆维吾尔族自治区科技专项基金项目(201230122)

This work was supported by the National Natural Science Foundation of China (61472418), the Innovation Foundation of the Chinese Academy of Sciences (CXJJ-14-Z68), the State Priority Research Program of the Chinese Academy of Sciences (XDA06040101), and Xinjiang Uygur Autonomous Region Science and Technology Project (201230122).

通信作者:孙利民(sunlimin@iie.ac.cn)

了 ICS 的系统架构及特性,并对 ICS 的安全理念进行阐释;其次,依据 ICS 的特性,给出了对工业控制入侵检测系统(intrusion detection system, IDS)(简写为 ICS IDS)的需求和解释;再次,基于检测对象角度,从流量检测、协议检测、设备状态检测 3 个方面,对现有的 ICS IDS 技术、算法进行了分类及详细的分析;最后,从检测性能指标、检测技术、检测架构 3 个方面,对整个 ICS IDS 的研究趋势进行了展望.

关键词 工业控制系统;入侵检测系统;流量检测;协议检测;设备状态检测

中图法分类号 TP309

工业控制系统(industrial control system, ICS)是一类用于工业生产的控制系统的统称,它包含监视控制与数据采集系统(supervisory control and data acquisition, SCADA)、分布式控制系统和其他一些常见于工业部门与关键基础设施的小型控制系统(如可编程逻辑控制器)等[1]. 它是电力、交通、水利等传统国家关键基础设施的核心[2-3]. 美国政府把国家关键基础设施分为信息处理、通信系统、金融系统、政府系统、关键制造业、水利系统、核电系统、应急响应系统、能源系统、国防军工、交通运输、食品系统、化工系统、商业系统、卫生系统、供水系统共 16 个领域,ICS 涉及到其中绝大多数领域[4-5]. 当前,大国间军事对抗日益升级,恐怖主义活动和社会不稳定因素不断增加,ICS 安全与否已直接关系到国家关键基础设施的安危.

然而随着技术的发展及业务需求的增加,ICS 在近十多年间引入了工业以太网和 TCP/IP 等开放性通信协议,系统平台趋于开放化和标准化,与外部网络的连接变得更为紧密与频繁,特别是新近提出的工业 4.0 概念融合了智能工厂、智能生产、智能物流等思想. 这些现象使得 ICS 的系统固有漏洞和攻击面日益增加,互联网面临的安全攻击被引入到 ICS 中. 从 2010 年出现攻击 ICS 的超级病毒——“震网”病毒到“Duqu”病毒、“火焰”病毒、“Havex”病毒,以及俄罗斯输气管道爆炸、德国钢厂事故等,都显示出 ICS 面临着越来越多的复杂攻击. 据权威统计信息,仅在 2010—2013 年间,美国 ICS 网络应急响应小组(Industrial Control Systems Cyber Emergency Response Team, ICS-CERT)累计响应了 600 多起 ICS 安全事件,且年平均安全事件呈现急剧上升的趋势[6]. 传统 ICS 安全措施无法应对上述威胁,亟需加深对 ICS 安全的理解,从设备故障和信息数据安全 2 方面保障 ICS 安全.

针对受到的安全威胁,ICS 采用入侵检测技术监控系统运行状态,实时发现可疑行为,便于安全人员及时采取应对措施,抵御已知和未知攻击. 入侵检测是系统防御的核心技术,众多保护技术的实施依赖于入侵检测技术的效率,即是否能够实时发现入侵行为. 然而 ICS 具有实时性高、资源受限、更新困难等特殊性,导致传统入侵检测系统(intrusion detection system, IDS)无法直接应用于 ICS 中. 目前针对 ICS 的 IDS 技术受到研究人员的广泛关注. 然而由于不同研究人员自身研究背景等诸多原因,现有 ICS IDS 测技术参差不齐. 鉴于此,本文旨在对现有工业控制 IDS 技术进行总结、归纳与分析,以便于未来对工业控制防御措施的深入研究.

1 工业控制系统(ICS)

1.1 ICS 架构

ICS 与物理世界关系紧密,为监控真实设备的正常生产,人们建立了由企业网络、控制网络、现场网络 3 级网络组成的工业控制网络,如图 1 所示[7].

1) 企业网络包括以企业资源计划(enterprise resource planning, ERP)系统为代表的管理信息系统(management information system, MIS)以及制造执行系统(manufacturing execution system, MES). 管理信息系统融合信息服务、决策支持于一体;制造执行系统负责生产管理和调度执行. 管理者可及时掌握和了解生产工艺各流程的运行状况以及工艺参数的变化,实现对工艺的过程监视与控制.

2) 控制网络包括众多监控站、工程师站、OPC(OLE for process control)[8]服务器以及历史/实时数据库服务器等设备. 该网络的主要任务是监视底层现场网络的行为,并负责企业网络与现场网络之间信息的传递和存储.

3) 现场网络包括可编程逻辑控制器(programmable logic controller, PLC)、可编程自动化控制器(programmable automation controller, PAC)、远程终端单元(remote terminal unit, RTU)等现场设备. 它负责感知工业过程的现场信息,并根据实时性要求控制系统正确、高效地运行.

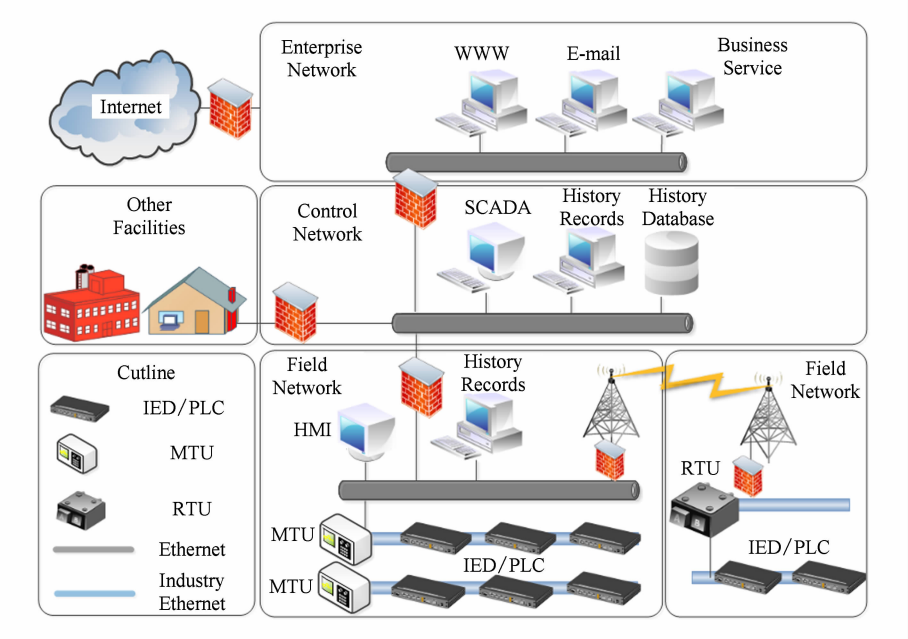


Fig. 1　Industrial control system.

图 1　工业控制系统

1.2　ICS 的特点

ICS 的目标及体系架构与传统信息技术有着根本的不同,导致其具有特殊性. ICS 的特点可归纳为“明确的工作人员按照确定的业务逻辑操作特定的设备”,具体可从参与人员、操作对象与工作流程等多个方面进行阐述.

1) 处理真实设备. 传统信息技术管理的是系统中的数据信息;而 ICS 处理的是直接面对人员和生态环境、能对物理世界产生重大影响的真实设备.

2) 设备种类繁多. 传统信息技术处理的是虚拟数据,对设备本身没有过多需求,因此设备种类少,以计算机、路由器、服务器等为主;而 ICS 面对物理环境中各种过程控制,针对不同的物理环境和业务需求,需要种类众多的工业控制设备.

3) 业务流程固定. 由于信息技术系统的开放性等原因,存在大量突发情况,需采用触发式机制处理相关信息;而 ICS 相对封闭,针对某个特定目标,具有固定的业务流程,采用自动、时间驱动的闭环处理方式.

4) 安全理念不同. 传统信息技术系统遵循 CIA (confidentiality,integrity,availability)原则,其首要目标是保证信息的机密性;而 ICS 与物理世界紧密联系,其首要目标是保障系统的稳定运行,即遵循 AIC(availability,integrity,confidentiality)原则.

5) 私有协议众多. 由于互联网的开放性,其绝大多数协议为公有协议;而 ICS 最初是个封闭系统,各企业依靠自身开发的私有协议进行竞争,导致工业控制网络私有协议众多.

1.3　ICS 安全与传统信息技术安全的差异

ICS 中对安全的理解与信息技术系统有本质的区别. ANSI/ISA-99 (American National Standards Institute/International Society of Automation) 和 IEC62443(International Electrotechnical Commission)等早期国际 ICS 标准对安全的理解是 safety,即主要考虑由于随机硬件故障所导致的组件或系统失效对健康、安全或环境(health,safety,environment, HSE)的影响. 而传统信息技术系统中认为安全是 security,即一系列包含敏感和有价值的信息和服务的进程和机制,不被未得到授权和不被信任的个人、团体或事件公开、修改或损坏[9]. 现有 ICS 安全对上述 2 个方面都有需求,具体来说,ICS 的安全特征如下:

1) 高实时性

在 ICS 中各个设备需按照业务逻辑在固定时间完成特定动作,不能有丝毫差错,否则将威胁设备、系统的正常运行,甚至对物理世界产生破坏. 由于 ICS 处理流程固定,一旦产生延迟则会产生突发情况,难以处理,易导致业务逻辑的断裂;且 ICS 处理的是真实物理世界,业务逻辑断裂会导致设备毁坏,造成资源、时间消耗巨大以及严重的生态环境破坏.

2) 工业控制设备资源受限

ICS 包含大量执行特定操作的传感器和执行器,为降低成本,其拥有的计算、存储资源通常十分有限. 当 ICS 运行时,空闲资源所剩无几,难以支持审计、安全等其他程序的运行.

3) 业务逻辑固定

ICS 具有特定的生产目标,为达到此目标制定了明确的生产逻辑,并在实际运行中严格遵守. 修改相应的操作流程可导致设备状态超过设计的安全运行参数,造成关键服务(如电力供应等)失效,甚至导致威胁生命的事故(如有害物质泄漏等)或直接威胁国家安全.

4) 运行时间长、遗留系统多

在 ICS 发展过程中,稳定是首要任务. 由于成本昂贵,ICS 通常数月甚至数年不间断运行,其生命周期可能长达数十年. 因此,目前运行的 ICS 中存在大量遗留设备(legacy device),即陈旧的设备,这些设备本身存在众多安全问题且对目前的检测技术造成严重的阻碍。例如遗留设备大多不存在日志文件,当系统异常时,安全系统无法根据日志对设备进行分析,进而无法判断出导致系统异常的原因.

5) 工业控制设备难以更新、重启

在 ICS 中,所有设备均需持续运行且与物理世界联系紧密. 为保持系统物理参数的稳定,ICS 无法暂停工作,否则会对整个工业控制系统、人员、环境造成严重的危害. 因此,设备无法暂停运行以进行软件版本更新或漏洞修补,导致系统中存在众多系统漏洞. 如在 2010 年,Red Tiger Security 对北美近 100 个电厂进行渗透测试,发现超过 38000 个安全警告和漏洞[10].

6) 私有协议安全措施差

原有 ICS 采用隔离形式,并大量采用私有协议保证机密性. 根据控制领域人员的理念,私有协议完全能保证自身数据的机密性,无需其他安全措施. 然而随着 ICS 开放性的提升以及协议逆向技术的发展,原有安全的私有协议逐渐变成无安全保护机制、极易受到攻击的公有协议,使整个系统及其机密信息直接暴露在网络上.

2 ICS IDS 概述

2.1 ICS IDS 定义

从“震网”病毒发现后,ICS 的安全问题受到全球研究人员的关注. 随着研究人员对该领域的探索,大量安全问题被披露出来. 针对目前 ICS 出现的众多安全问题,为保障 ICS 稳定运行,需采取入侵检测机制发现入侵行为. 入侵是任何危害或可能危害资源完整性、保密性或可用性的行为;而入侵检测是为通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象[11].

上述通用的 IDS 定义并未考虑 ICS 的特殊性,不适应于 ICS. 虽然国际上对制定 ICS IDS 的呼声急剧增加,然而目前仍未有明确的 ICS IDS 定义. 考虑到 ICS 高实时性等特性,经对大量的文献解读、分析后,本文将 ICS IDS 理解为针对种类众多的工业控制设备,在不影响实时性的前提下,充分利用有限的设备资源收集设备、系统、物理世界的信息,依据数据完整性以及业务逻辑等对上述信息进行分析,从中发现是否存在违反数据安全策略或物理操作流程的行为和被攻击的迹象. 其核心目标是在保证自身不影响物理世界正常、稳定生产的前提下,发现数据或系统生产逻辑的异常.

2.2 ICS IDS 分类

ICS IDS 没有统一明确的分类方法,目前仍主要采用传统分类方法进行分类,如 Chen 等人[12]将 ICS IDS 从检测技术和数据源 2 个维度进行划分,如图 2 所示:

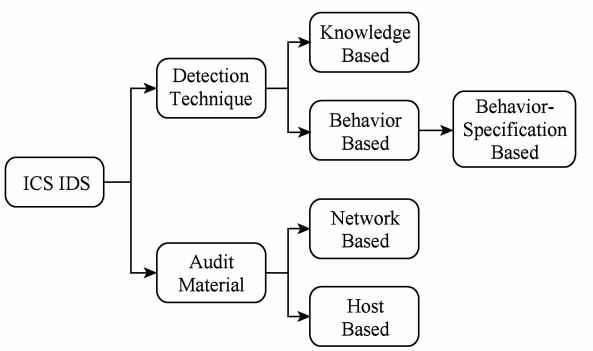


Fig. 2 A classification tree for ICS IDS by Chen et al.

图 2 Chen 等人[12]的 ICS IDS 分类方法

具体来说,根据数据来源的不同,ICS IDS 可分成网络和主机 2 种类型. 网络 IDS 通过网络不同区域设置的检测点,获取全局网络流量并进行挖掘、分析,发现网络异常现象,实现全局信息检测,缺点是无法对特定节点的数据进行检测;主机 IDS 主要监控系统设置、配置文件、应用程序和敏感文件,发现系统异常情况,但缺乏对 ICS 全局信息的检测.

同时,根据检测技术的不同,ICS IDS 可分成误用检测和异常检测 2 类. 误用检测采用特征匹配技术,将检测数据与已知攻击行为特征库进行比对,发现入侵行为,其缺点在于无法检测未知攻击;异常检测将实时行为与正常行为模型进行匹配,发现违反该模型的行为即判定为入侵行为,缺点在于无法对攻击进行精确识别、划分. 此外,根据 ICS 业务流程固定的特性,Chen 在异常检测中又进一步划分出新的子类——基于行为规范的检测方法. 该检测方法依据特定工业控制环境、行为规范,对系统行为进行更加精准的检测.

上述 ICS IDS 分类仍是采用传统 IDS 分类方法,没有充分考虑 ICS 的特点,未能体现 ICS 与真实物理世界联系紧密等特性,如未考虑 ICS 的报文乱序除造成逻辑混乱外可对物理设备造成损害.

基于对大量 ICS IDS 文献的分析和理解,本文考虑 ICS 的特点,尝试从检测对象角度提出新的分类方法,将现有 ICS IDS 技术划分成基于流量检测、协议检测、设备状态检测 3 大类. 首先,针对 ICS 中特定的业务流量特征,从宏观上对流量信息进行分析与控制;其次,在流量分析基础上,对每个报文分组进行协议方面的深度解析;再次,针对真实的物理设备,分析协议报文在设备、系统中的具体执行,根据系统、物理世界反馈的执行结果发现异常行为. 综合来看,该分类方法对流量信息逐步深入分析,且在每类检测中均对应多个 ICS 特性. 因此,该分类方法充分考虑了 ICS 的特性.

2.3　ICS IDS 性能

在 ICS 中,误报率、漏报率和检测率等传统 IDS 性能指标仍适用. 其中,误报率是将正常行为误判断为异常行为的概率;漏报率是将异常行为误判断为正常行为的概率;检测率是检测出真实异常行为的概率. 传统信息技术领域对这 3 个指标均没有特定的限制条件,也没有考虑检测率、漏报率、误报率之间的关系. 然而,由于 ICS 具有高实时性、难暂停更新等特点,不能因误报导致系统停滞,否则会给系统、资源等带来巨大的损害. 因此对 ICS IDS 的误报率提出更严格的要求,即宁可漏报也不允许误报.

同时,研究人员针对 ICS 的高实时性和资源受限等特点,对 ICS IDS 提出新的性能指标. 如 Striki 等人[13]提出了“检测时延”评价指标,即入侵行为从开始攻击到被 IDS 识别的时间间隔;Misra 等人[14]提出了系统功耗、通信开销和处理器负载等指标.

3　ICS IDS 检测技术

目前研究人员基于神经网络、支持向量机、模式匹配、虚拟仿真,提出了众多 ICS IDS 技术,涵盖了设备生产车间、智能电网、国家基础设施等众多领域. 本节将对现有的 ICS IDS 技术,按照本文提出的基于检测对象的分类方法进行分类,并对各检测方法及其关键技术进行分析.

3.1　基于流量的 IDS

基于流量的 IDS 依据 ICS 不同安全区域的流量特征,针对外部攻击和内部攻击的流量特征,通过多检测点间协同合作,在不解析具体协议格式的情况下,发现网络的异常流量,实现 IDS.

传统基于流量的检测方法是通过提取 5 元组(源 IP、目的 IP、传输层协议、源 port、目的 port)、IP 选项域、流量持续时间、平均包间隔等指标,从时间、空间分布上构造“正常模式”;将“正常模式”作为检测基准,将实时通信数据与检测基准进行比较,实现对未授权访问、中间人攻击、拒绝服务(denial of service, DOS)攻击等入侵行为的检测. 然而经过几十年的发展,信息技术系统变得极为复杂,开放性导致系统拓扑变化剧烈,多应用支持使系统中充斥种类繁多的应用程序和协议,需采用复杂方法获取全面的数据信息协同进行检测.

由于各设备所处的位置、功能以及人员所处的部门、职能不同,将设备和人员划分成多个不同的安全区域. 在各安全区域中,应考虑内部或外部攻击,需对安全区域进行全方位的保护. ICS 的参与人员、操作对象与工作流程相对固定,致使 ICS 具有明显的流量特征;同时 ICS 业务固定,采用静态拓扑且所使用的应用程序及协议数量较少,导致流量模式稳定不变. 因此,基于流量的检测适用于 ICS 安全区域,可精确检测出大流量攻击或误用特征明显的攻击.

3.1.1　流量检测内容的选取

研究人员在对流量信息检测之初,必须确定在工业控制网络中提取何种数据进行分析. 为此,Stavroulakis 等人[15]详细讨论了流量分析在 ICS IDS 方面的应用,分析比较了主动式和被动式测量方法,把 ICS 流量划分为:由独立的源 IP、目的 IP、TCP/UDP 端口等信息组成的流量矩阵(traffic matrix),表示网络中各个会话的流量信息;由所有流量、字节数组成的总流量(traffic volume),表示一定时间内网络发送、接收的流量总和;由报文延迟变化、可用带

宽变化等组成的流量变化(traffic dynamics),表示网络流量随时间的变化.

3.1.2 基于数学模型的检测方法

目前针对上述流量信息,在业务固定的 ICS 中通常采用大量计算资源,利用数学模型构造"正常模式",对流量进行实时检测来识别出异常流量.

神经网络具有非线性适应性信息处理能力,可通过对大量训练样本进行分析,获得对未知异常行为的识别.在流量检测中,神经网络可通过学习/训练过程建立 ICS 特定流量模式与系统安全状态之间的映射关系,以此对实时数据进行分析,检测出异常行为.

例如 Vollmer 等人[16]利用单个分组流量进行入侵检测,提取网络流量负载,ICMP 协议的 ID 域、序列号、代码域,以及 IP 协议 ID 域、IP 选项域等特征量,并采用误差反向传播(back propagation,BP)算法训练神经网络,使神经网络的总误差最小;在检测时实时提取特征量并导入该神经网络中进行分析,以实现对 attempted-dos,attempted-recon,bad-unknown,attempted-user,misc-activity 等多种网络入侵的检测.在此基础上,Vollmer 等人[17]又采用滑动窗口技术,动态、精确地提取真实包序列中的 IP 地址数目、单 IP 地址包数、平均包间隔、标识码数目、数据长度置 0 的包数目等 16 种网络特征,利用 BP 和 LM(Levenberg-Marquardt)算法训练神经网络,检测异常流量事件.

为克服神经网络训练开销大的缺点,Manic 等人[18-20]采用模糊逻辑实现了一系列入侵检测机制.模糊逻辑采用模糊隶属度来描述不精确、不确定的事件和现象,并通过近似推理技术提升检测系统的容错性.

文献[18]针对由滑动窗口技术在线提取的真实报文特征,将其中正常行为模式通过最近邻聚类算法聚合成多个簇,再通过非对称高斯模糊关系函数将簇转化成模糊逻辑规则集,形成正常的网络流量模式.在检测时,该方案根据模糊逻辑输出的最大触发强度取值与合法阈值之间的比较,判断入侵行为.

文献[19]针对训练数据的不确定导致检测性能下降的问题,采用 TYPE-2 模糊逻辑,先将输入数据进行模糊化后,再通过文献[18]的思路形成正常网络流量模式.该方案与文献[18]的区别在于其输出的触发强度是一个范围$[y_{\min}(\boldsymbol{x}),y_{\max}(\boldsymbol{x})]$.在检测时,该方案根据实时数据生成的触发强度取值范围与合法阈值之间的比较,若该范围在阈值之上则认为异常;在阈值之下则认为正常;包含该阈值则认为存疑.

文献[20]则提出了基于模糊逻辑的异常检测架构.该架构利用 TYPE-2 模糊逻辑分析具体工业场景和网络环境下的潜在知识,并根据分析结果动态调节后续异常检测算法的阈值,提升异常检测的精度.

此外,研究人员还采用支持向量机(support vector machine, SVM)技术,将原本线性不可分的流量特征向量借助核函数映射到高维空间,并构造 1 个分类面以区分正常流量与入侵流量.Maglaras 等人[21]采用单类支持向量机(one-class support vector machine, OCSVM)为 DNS,FTP,MDNS,Modbus,TCP,UDP 等协议建立流量模型,无需攻击相关的先验知识和异常数据,可检测中间人攻击、同步洪泛等入侵行为.然而,普通 SVM 仅能区分出异常,无法精确地识别出异常的类别,为此文献[22]采用多个 SVM 二值分类器,将其结合起来,构建层次 SVMs,先检测出异常数据,再依次采用特定攻击 SVM 以实现对入侵行为的类别划分,如图 3 所示:

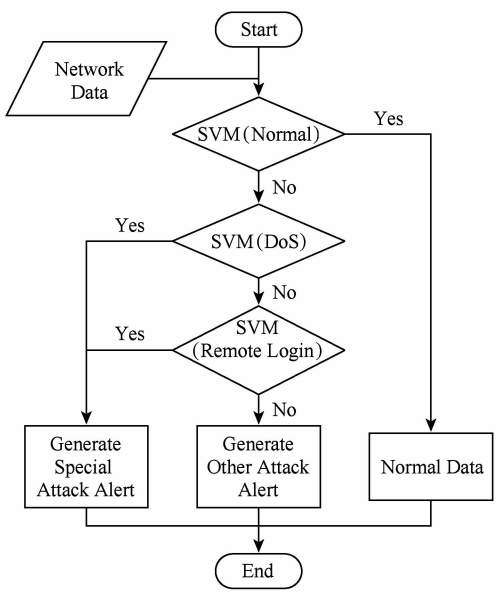


Fig. 3 The hierarchical SVM IDS (take the detection of 2 attacks for example).

图 3 层次 SVM 入侵检测流程(以检测 2 种特定攻击为例)

3.2 基于协议的 IDS

基于协议的 IDS 依靠工业控制通信协议规范,采用成熟的协议格式分析和状态协议分析技术,对报文中协议格式及协议状态的变化进行检测,发现异常行为.

3.2.1　常用工业控制通信协议的安全性

工业控制通信协议是为了提高效率与可靠性而设计的,以便满足 ICS 的经济性和运作需求.早期大多数工业控制通信协议为提升效率,很少考虑所有非必需的特性与功能,如要求额外开销的认证和加密等安全措施.常用的开放工业控制通信协议包括 Modbus, ICCP/TASE. 2 (inter-control center communications protocol/telecontrol application service element 2), DNP3 (distributed network protocol)等,均存在诸多安全性问题.

Modbus[23]是历史最悠久、应用最广泛的工业控制通信协议.该协议直接使用无认证等额外开销的原始消息通信,是一种开放标准.基于请求/应答方式,该协议仅采用 Modbus 请求、应答和异常应答 3 种不同的协议数据单元,实现互连设备间的高效通信.由于处理开销非常小,Modbus 适合作为 PLC 和 RTU 与 SCADA 间传递监控数据的协议.然而正是由于开销小的特点,导致其存在严重的安全问题:缺乏认证,仅通过有效 Modbus 地址和功能码进行验证,易遭受泛洪等攻击;明文传输,易于窃取、篡改、伪造报文数据;Modbus/TCP 无消息验证机制,易于篡改、伪造数据;具有可编程性,易被利用向 RTU 和 PLC 注入恶意代码.

ICCP[24]是用于电力等能源工业中控制中心间通信的协议,它采用客户端/服务器模式,通过构造客户端可访问数据元素的访问控制类表——双边表,实现可靠的标准化数据交换.该协议相对于 Modbus 有部分安全改进:双边表显示定义 ICCP 客户端和服务器的通信权限,提供了对通信路径的基本控制.但是 ICCP 的安全机制十分有限,仍存在重大安全隐患:缺少认证与加密,易受假冒、会话劫持等攻击;双边表未进行隐藏,易被利用来直接破坏 ICCP 服务器和客户端的安全性.

DNP3[25]最初用于主控站和从设备(或子站)间,以及控制站内部 RTU 与 IED(intelligent electronic device)间的串行通信.该协议支持模拟数据、2 进制数据等多种数据对象,并通过双向通信实现实时数据传输.与上述 2 种协议相比,DNP3 具有更高的可靠性:支持数据时间戳,提高实时传输的可靠性;频繁使用 CRC 校验,单个 DNP3 帧中最多包含 17 个 CRC.然而,在引入安全机制的同时协议复杂度增加,提升了在协议实现上出现漏洞的可能.目前 ICS-CERT 已报告多个 DNP3 漏洞.此外该协议仍未采用授权或加密机制,易受中间人攻击.

通过对上述 3 种工业控制通信协议的分析可知,由于设计之初未考虑安全性,公开/私有工业控制通信协议存在大量的安全隐患,易遭受如包篡改、伪装等攻击,这些攻击无法通过流量进行检测,因此需要通过对流量中的报文分组进行深度解析,根据协议格式、协议状态机以及协议分组生成的事件/事件序列,检测入侵行为.

3.2.2　基于协议的检测方法

1) 针对通用开放工业控制通信协议的检测机制

在 ICS 中,少量协议是公开的,研究人员可以直接获得这些协议的规范.在规范中详细定义了其自身的报文格式以及通信模式.因此研究人员可依据规范制定检测规则,对协议进行检测.

早在 2007 年,Cheung 等人[26]针对工业控制通信协议提出了一种基于模型的 IDS.该方案针对 Modbus/TCP 等基于 TCP/IP 的现场总线协议,根据公开的协议规范及业务逻辑,对报文中功能码等特定域的取值范围、多域间的数值关系构造基于协议格式的模型;根据 ICS 划分的安全区域,对通信对象构造传输方向、端口等通信模式模型;根据系统需求,对如检测到新 Modbus ID 等特定事件构造基于服务的模型.依靠上述 3 个模型,该方案可检测出潜在攻击,但易导致较高的误报率.

工业控制现场网络采用现场总线结构实现数据交换,无法采用传统、基于信息技术的入侵检测方法.为适应现场总线数据的入侵检测需求,Morris

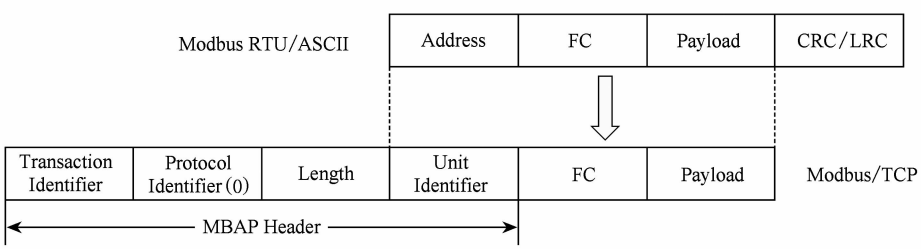


Fig. 4　The transformation between Modbus RTU/ASCII and Modbus/TCP.

图 4　Modbus RTU/ASCII 与 Modbus/TCP 的转换

等人[27]将 Modbus RTU/ASCII 等现场总线数据转化成 Modbus/TCP 等 TCP/IP 报文,并依靠协议规范白名单、业务逻辑白名单构造内联/旁路检测模式,可识别出 DoS、命令注入、响应注入等入侵行为.

该方案主要针对具有串行、以太网 2 种传输方式且报文结构相似的工业控制通信协议.如图 4 所示,依据报文结构的相似性生成 2 种报文格式的对应关系(如 Modbus/TCP 报文中的 Unit Identifier,FC,Payload 域分别与 Modbus RTU/ASCII 的 Address,FC,Payload 域一一对应),研究人员可快速、直接地将串行报文(Modbus RTU/ASCII)转换成 TCP/IP 报文(Modbus/TCP),便于传统 IDS 检测.

为节省设计、开发时的资源消耗,研究人员对传统 IDS 进行改进以适应工业控制环境.Bro 是五大免费企业网络 IDS 之一,它以旁路模式捕获所有数据包,依赖协议解析器对网络层、传输层乃至应用层协议进行深度解析,并根据数据包的内容形成相应的事件,最后根据策略脚本对事件做详细的分析,检测出异常、入侵行为.

Lin 等人[28]针对 Bro 进行改进,如图 5 所示,构建支持 DNP3 等工业控制通信协议的报文解析器模块,并根据工业控制通信协议分组各域的含义、取值范围以及请求/应答操作序列等信息制定对应协议的安全策略,使其增添对 SCADA 私有协议的支持.

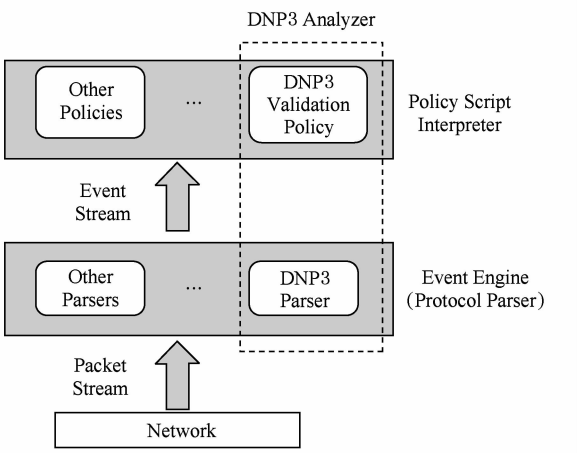


Fig. 5 The ICS IDS based on Bro.

图 5 基于 Bro 的 ICS IDS

2) 其他工业控制通信协议检测机制

除对公有工业控制通信协议的检测技术进行研究外,研究人员还针对特定行业、私有协议进行分析,研制特定的入侵检测机制.比如 Hong 等人[29]对智能电网中的子站自动化系统进行分析,通过对 IEC 61850 标准下的 GOOSE(generic object oriented substation event)和 SV(sampled value)多播协议包进行深度解析,并根据由协议规范和设备状态之间的关系制定的白名单规则,实现对包篡改、重放、DoS 等入侵行为的检测.

3) 工业控制通信协议检测优化机制

上述 2 类协议检测方案均是采用白名单的形式,在检测时需要对所有报文进行深度包检测,影响 IDS 的检测效率.因此研究人员提出了误用与异常相结合的入侵检测机制[30-31].该机制首先依靠误用检测技术,根据入侵行为特征库,快速识别出未授权访问、伪装、缓冲区溢出等已知攻击;然后对剩余数据结合协议规范生成的协议模型、通信模型,采用基于异常的检测机制(如 SVM、神经网络等),实现对未知攻击的入侵检测.经分析,该方案可大幅度地提升整体 IDS 检测效率.

此外,流量检测往往只处理传输层(含)以下的数据信息,而工业控制通信协议往往是应用层协议且在规范中规定了报文的传输周期等时间信息.因此,协议检测也可和流量检测进行联动,依据工业控制通信协议规范中指定的会话通信标准以及具体的业务逻辑,制定相应的规则并交给流量检测机制进行检测,提升流量检测的精度.Hadeli 等人[32]针对电力系统,提出了基于协议的流量检测方案.该方案根据 IEC61850 标准,从协议规范以及各节点的 ICS 配置文件中提取合法的通信数据、传输时间间隔等信息(如 IEC61850 中规定每 200 ms 发送一条 MMS (manufacturing message specification)协议报文),构造正常流量模型并将其转化成 Snort 规则库(如图 6 所示),依赖 Snort 开源软件对流量进行检测,准确判断出系统流量是否发生异常.

```
Required 172.16.80.101 tcp 102→172.16.80.22
any 20 second
```

Fig. 6 An Snort traffic rule based on protocol.

图 6 基于协议的流量检测规则

3.3 基于设备状态的 IDS

基于设备状态的 IDS 根据业务逻辑和设备操作规程,通过定义设备正常状态或异常状态、判断状态转移趋势、监控操作序列等方法检测入侵行为.在 ICS 中,读取或操作的设备往往是与物理环境或生产过程相关的物理设备,对其攻击会导致工业控制设备毁坏,甚至出现重大安全事故,这是 ICS 不同于现有互联网的显著之处.经分析,除盗取信息外,

对 ICS 实施攻击的核心是通过非法篡改设备配置、非法控制设备的操作、修改业务流程等入侵行为,使设备进入不合理状态、停机状态或损坏.因此检测设备的状态/操作能够有效地检测入侵行为.

3.3.1　自动化领域设备状态检测技术

在自动化领域为保障系统的正常运作,在发生元件故障时能将其隔离,保证剩余系统的正常运行,提出了故障检测与诊断(fault detection and diagnosis, FDD)技术.FDD 从 1971 年诞生到现在已成为自控界的重要研究方向之一,取得了大量的研究成果[33].

FDD 是一种相对独立发展的技术,同时又是一门应用型边缘学科,其理论基础涉及现代控制理论、可靠性理论、数理统计、信号处理、模式识别、人工智能等多门学科,与容错控制、鲁棒控制、自适应控制、智能控制等具有密切的联系[34].

国际上通用将故障检测划分为基于信号处理的检测、基于解析模型的检测、基于知识的检测和基于离散事件的检测 4 大类.

1) 基于信号处理的检测

基于信号处理的检测是直接对可测信号进行处理,采用频谱、自回归滑动平均等信号模型,提取方差、幅度、频率等特征值,从而检测故障的发生.

最初的检测方法是设定正常数值范围(阈值)进行检测[35].为解决噪声污染以及增强通用性,学术界提出了归一化滑动窗口协方差格形滤波器.该滤波器采用滑动窗口提取系统输入和输出,采用自适应格形滤波器计算残差序列,判断该序列是否为零均值固定方差的高斯过程,是则处于正常状态,否则发生了故障[36].

小波变换是一种有前途的故障诊断方法,它无需构建数学模型,计算量较低,可实时检测且灵敏度高.该方法的基本思路是对被诊断对象的输入输出信号进行小波变换,计算出输入输出信号的所有奇异点,再剔除由于输入突变引起的极值点,剩下的极值点即表示被诊断对象存在故障并分别对应了相应的故障状态.

此外基于信号处理的检测方法还存在基于信息融合的检测方法、基于 Kullback 信息准则的检测方法、基于信息校核的检测方法等.这些方法实现简单,但只能当故障发生到相当程度并影响到外部特征时才有效,且难以直接定位故障.

2) 基于解析模型的检测

基于解析模型的检测即将被测对象的可测信息和系统先验信息模型进行比较,生成残差并对其进行分析以实现故障检测的技术.残差是与正常运行状态无关、由输入输出信息构成的线性/非线性函数.正常状态下,残差应等于或近似为零;一旦发生故障,残差应显著偏离零点[37].

根据残差产生形式的不同,基于解析模型的检测又可细分为状态估计方法、等价空间方法和参数估计方法.

状态估计方法是根据解析模型和可测信息设计检测滤波器,选取某个可测变量,由该滤波器的输出与真实系统输出的差值作为残差,并根据残差的取值实现系统的故障检测.例如,文献[38]通过构造与原系统系统相似的线性时不变系统及对应的检测滤波器,实现对部分线性时变系统的故障检测.

又如,Sridhar 等人[39]针对智能电网,根据电力系统相关知识预测发电负载,并通过对区域控制误差的预测值和实时值比较来判断异常,最后通过控制策略切换机制消除攻击影响,实现对变尺度攻击和渐变攻击的检测和防御.

等价空间法是构造被检测对象的输入、输出之间的数学关系,再根据系统的实际输入、输出值判断这些数值是否符合上述数学关系来实现故障检测.例如,文献[40]采用等价方程方法构造基本残差,再对基本残差进行线性变换以消除干扰因素,提高检测准确性.

参数估计方法是根据系统模型参数及故障参数变化的统计特性来检测故障.该方法主要有滤波器方法和最小二乘法.例如文献[41]提出了一种非线性系统偏差型故障检测算法.该算法首先根据卡尔曼滤波器计算出残差序列并用残差加权平方和算法实现故障的快速检测;然后,根据强跟踪滤波器取得系统状态与非线性时变参数的联合估计;最后,采用贝叶斯分类算法检验各参数估计值,实现对故障的检测.

3) 基于知识的检测

基于知识的检测是引入如人类专家的经验知识及被检测对象的模型知识等相关信息,通过推理来获取诊断结果,使其能对某个征兆集合的产生原因做最佳解释.

随着人工智能的快速发展,众多先进技术被用在故障检测中,如专家系统、神经网络和模糊数学等.

专家系统是根据专家的经验、知识进行推理判断,模拟专家决策过程的智能程序.专家系统在故障检测领域应用较早,是定性故障检测技术中的一个重要方向.典型的故障检测应用技术可归纳为:首先

将专家经验和设备参数用规则表示,建立故障信息知识库、规则库和推理机;然后在检测时将信息输入到推理机进行推理,检测系统故障.例如 Tan 等人[42]将断路器的动作逻辑和操作员的检测经验用规则表示并形成知识库,通过正向推理将实时数据与知识库中的规则进行匹配,检测出故障信息.

神经网络在故障检测中具有广泛的应用,例如直接作为分类器进行故障检测或与其他检测方法相结合进行复合故障检测.具体来说,神经网络在故障检测中主要有 4 种形式[43]:

① 用神经网络产生残差

该方法是将神经网络用于替代描述系统正常运行时的解析模型,通过采用真实测量的输入、输出对其进行训练;在故障检测时输入实时数据后,计算生成相应的残差供后续处理.

② 用神经网络评价残差

该方法是采用残差和故障库的数据对神经网络进行训练;在检测时将实时生成的残差作为输入并进行处理,根据神经网络的输出判断是否产生故障.

③ 用神经网络做进一步检测

该方法是将故障征兆和检测结果分别作为神经网络的输入和输出进行训练,获取它们之间的对应关系;在检测时,以真实数据为输入,根据输出的检测结果确定具体故障.

④ 用神经网络作自适应误差补偿

该方法针对检测时出现的误差,采用神经网络技术消除模型误差对检测准确度的影响,如可通过神经网络自适应补偿方法消除误差对残差的影响.

虽然神经网络具有自学习、鲁棒性好等特点,但其仍存在训练样本需求量大且获取困难等严重缺陷.

上述故障检测方法较少考虑信息的不确定性,影响检测的精确性.当难以获得精确模型时,可采用模糊理论进行故障检测.例如 Monsef 等人[44]针对电网系统,将所有输入信息模糊化,再通过神经网络/专家系统计算输出模糊数,最后采用反模糊系统对此模糊数进行解释以生成最终的检测结果.

此外基于知识的检测方法还存在基于贝叶斯网络的检测方法、基于优化技术的检测方法、基于支持向量机的检测方法、基于 Petri 网技术的检测方法、基于信息融合技术的检测方法、基于多智能体技术的检测方法等.这些方法弥补数学模型检测方法的不足,实现检测智能化,但它们各有优缺点和应用限制,有些仍处于理论状态.

4) 基于离散事件的检测

基于离散事件的检测将正常状态和故障(异常)状态共同形成一个集合并互为补集,通过构造的离散事件模型判断系统是否处于故障状态来实现对故障的检测.

3.3.2 计算机领域设备状态检测技术

随着“震网”病毒的发现,传统计算机领域逐渐关注对工业控制设备的检测并逐步提出多个检测方法,根据具体的检测思路,该检测技术可分为以下 3 类:

1) 基于配置的设备状态检测方法

每个设备为保证系统的正常运行,会保存一个配置文件,包含明确定义、授权的 IP 地址、端口、工业控制通信协议功能代码/命令、用户等信息.配置文件设定后基本不改变,若发生改变则视为发生入侵行为.

基于配置的设备状态检测通过配置,构造相应的白名单,并实时将程序行为与白名单进行比较,发现入侵行为.Paul 等人[45]根据设备自身的 XML (extensible markup language)文件构造设备配置信息,获取设备允许的 IP 地址、协议端口号和命令等信息,形成合法配置列表;系统运行时,实时收集设备的配置信息与已形成的合法配置列表进行比对,及时发现重要信息的异常变动,并视该变动为发生入侵行为,然后依据后台分析(关联分析等方法)识别具体的入侵行为.

除实时检测自身状态变化外,设备之间还可以相互协作进行检测.在正常的通信中,通信双方的数据应该是一致的(忽略传输延迟).然而中间人攻击可伪造发布控制指令或截断反馈信息,导致通信双方的状态、控制命令列表不同,即通信双方的数据不一致.然而单看通信一方,无法发现状态、控制命令列表的缺失,难以检测中间人攻击.

因此,文献[46]从系统全局进行检测,监控系统中的所有设备,实时获取各设备节点的状态信息和控制命令列表,并按照通信列表划分成多个通信集合;然后在每个通信集合中对获取的数据进行比对,若发现不一致的地方,则认为发生了中间人攻击.

2) 基于虚拟执行的设备状态检测方法

与传统信息技术网络不同,ICS 的指令数据(尤其是控制命令)对物理设备的影响重大,如一条简单控制命令即可导致物理设备损毁.为此需对所有的控制指令进行检测,判断其是否对物理设备造成破坏.然而为检测系统搭建、维护与现实相同的物理

环境,所耗人力、物力巨大.为降低成本,可构建高仿真的虚拟环境,以较为经济的方法实现控制指令的多次检测.

首先,可通过对系统收到的单个控制命令进行虚拟执行,分析命令执行后虚拟环境的状态变化,检测入侵行为.Fovino 等人[47]提出了基于设备临界状态的 SCADA 系统入侵检测机制.该机制将 ICS 或设备进入的停机、损毁等状态称为临界状态,并按照当前系统构建一个高仿真的虚拟镜像.在运行过程中,检测机制实时提取控制命令并将其放入到虚拟镜像中进行执行,然后周期性地将虚拟镜像与实际设备进行同步,以获取该控制命令在虚拟镜像中的执行结果.最后根据执行结果判断此控制命令是否正常,实现对导致系统或设备进入临界状态的复杂攻击的检测.

为提早发现入侵行为,Carcano 等人[48]提出了基于设备状态变化趋势的入侵检测机制.该机制定义了用于描述 SCADA 系统基本信息、临界状态的 ISML 语言,并通过设定多个状态参数的阈值来表示系统的临界状态.在检测时,该机制首先实时捕获当前状态,计算当前状态与临界状态的曼哈顿距离,并以此确定当前状态的危险等级;其次根据该距离的变化趋势来判断系统是否正向临界状态演变;最后根据虚拟镜像的输入日志判别是入侵还是故障导致系统向临界状态的转变,并以此发出警报.

通过虚拟执行进行入侵判别,需构造与真实系统高度相似的仿真系统,开发难度大,所需资源多.考虑到自动控制领域发展了几十年,拥有众多成熟的故障检测工具.因此可改造这些检测工具以发现入侵行为,节约开发成本.如图 7 所示,Lin 等人[49]在控制中心和子站分别部署检测代理,针对能影响现场设备状态的写、执行等重要命令,首先利用检测代理之间的专用通道,获取现场设备与控制中心之间传输的控制命令或状态数据,通过完整性检测保障数据传输的正确性;其次将这些控制命令发往传统电力系统的故障分析软件,由该软件对命令进行评估,判断该命令对设备产生的影响及影响程度;最后根据软件分析结果识别出针对设备、系统状态的攻击行为.

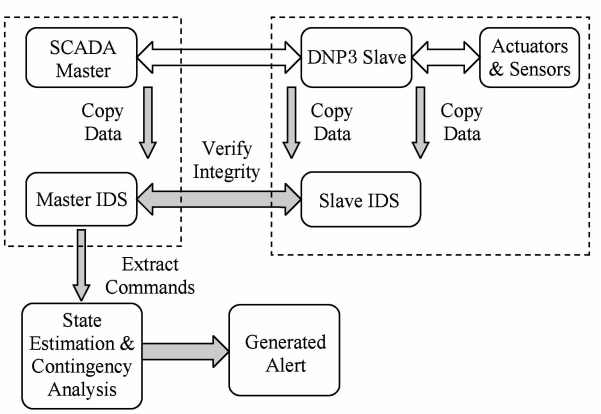


Fig. 7　The ICS IDS based on contingency analysis.

图 7　基于故障分析软件的 ICS IDS

3) 基于数学模型的设备状态检测方法

针对虚拟执行实时性差、成本高等问题,对现有系统进行分析,依靠数学模型构造“行为白/黑名单”,可实时、低成本地检测出入侵行为.

Mitchell 等人[50-51]分别以智能电网和无人飞行器为研究对象,以合取范式等数学理论、方法构建行为规则状态机,并利用监测器周期性地检查邻居节点状态来检测入侵行为,实现对复杂、隐藏攻击的高效检测.

该方案的核心是将行为规范转换成行为规则状态机.首先根据设备的行为规范,将违背行为规范的行为认定为攻击行为;其次,将每条攻击行为分解成合取范式,并将所有合取范式聚合成 1 条析取范式形式的布尔表达式;再次,根据布尔表达式提取状态机的状态参数并设置其对应的取值范围;最后通过合并、压缩状态参数及其取值范围解决状态爆炸问题,形成行为规则状态机.

Pan 等人[52]针对电力传输系统面临的 DoS、数据注入、控制命令注入攻击,改进贝叶斯网络,形成用于表示工业控制设备、网络行为的因果图,并筛选出所有异常场景形成攻击签名用于检测入侵行为.该因果图是将贝叶斯网络中的图节点表示为可观测事件,边表示事件之间的传递,则图中每条唯一路径对应某个特定真实场景,进而导致一张完整的因果图穷举了系统中所有可能出现的场景、事件.然而该方案检测精度严重依赖开发人员对 ICS 的理解程度,需与其他检测方法结合以减少漏报率.Yang 等人[53]提取网络流量、表示硬件操作统计信息的内核数据等 62 种特性,建立状态矩阵并实时监控,根据状态矩阵的偏移值发现系统变化,以极低的误报率识别出 jolt2,bubonic 等多种 DoS 攻击.

4　ICS IDS 检测技术的未来发展

本文第 2,3 节叙述了 ICS IDS 的研究现状,从

中可看出研究人员为保障 ICS 的正常运行,从多角度开发出多种不同的 IDS 技术,但存在准确性差等诸多问题.通过对这些问题进行细致的分析,本文可从检测性能指标、检测技术、检测架构 3 个方面归纳出未来的研究趋势.

4.1 检测性能指标

全面准确地检测性能指标有利于 IDS 的深入研究和产品推广.然而由于缺乏对 ICS 特性的考虑以及对性能研究的重视程度不足,目前仍采用传统 IDS 的性能指标评价 ICS IDS 的性能,缺乏准确性和全面性.虽然部分研究人员提出了新的性能指标,但这些指标缺乏科学的论证.因此,针对特定的 ICS 环境,制定精准、全面评价 ICS IDS 性能的指标必将是未来的一大研究重点.

4.2 检测技术

检测技术是为发现异常现象所采用的技术方法,其研究趋势可分为提升准确性和降低能耗 2 个方面.

4.2.1 准确性方面

1) 基于稀疏流量的异常检测机制

目前针对 SCADA 等 ICS 的攻击手段越来越高明,缓慢渗透的入侵攻击流量稀少,相对于高维度的检测模型训练向量,攻击样本呈现稀疏性.传统机器学习方法处理的数据维度较小,在训练检测模型时缺乏对参数本身的限制与优化机制,不利于从稀疏样本中提取与入侵行为紧密相关的流量特征,从而导致检测失效.因此,研究人员需要对检测模型进行优化,提高检测效率和精度,实现在大流量中检测出流量稀疏的攻击.

2) 可扩展的工业控制通信协议 IDS 机制

目前基于协议的 ICS IDS 检测技术对工业控制通信协议格式的检测进行了大量的研究.然而,此类检测技术的前提是必须获得某特定私有协议的规范,无法进行扩展,缺乏普遍性.

因此,如何提升协议检测的可扩展性是目前研究人员正在思考的问题,如可采用机器学习中的迁移学习[54]技术.迁移学习是在新环境中大量训练数据难以获得的情况下,从现有的数据中迁移知识,用来帮助新环境下的学习.在 ICS 领域,我们可以将在 Modbus,DNP3 等通用协议下构造的检测规则和方法,依靠自学习聚类算法等基于特征的无监督迁移学习技术,构造私有协议的检测规则,以实现协议检测的可扩展性.

3) 准确的设备状态 IDS 机制

① 准确的设备状态定义

简单的设备或系统易于定义设备状态,但复杂设备或系统往往有诸多观察量,难以将这些观察量与设备状态准确关联.因此,如何依赖诸多观察量准确判断出设备(系统)是否处于异常状态、状态转移趋势,吸引了众多研究人员去进一步挖掘、分析.比如可采用常用于标注或分析序列资料的条件随机场技术,通过判别式概率模型,在 ICS 中精确地确定复杂设备观测值与真实状态之间的关系,实现设备状态的精确判断.

② 精确的设备状态检测

ICS 现场设备成本昂贵、种类繁多、资源受限,需要考虑 MTU(master terminal unit)/RTU/控制主机与现场设备的协作.现通常考虑利用镜像技术来模拟现场设备,然而如何高效地实现设备模拟进而达到系统状态模拟,还需研究人员深入地分析、研究.比如可采用仿真和物理相结合的方法,在核心节点采用仿真技术,而边缘执行器部分采用真实物理设备,构建高仿真的工业控制设备环境.

③ 异常行为的成因分析

ICS 发生异常的原因可分为遭受入侵或故障 2 种情况.然而根据目前的研究进展,IDS 无法直接判断异常产生的具体原因,需要依靠其他信息进行判定且准确性差.为此,如何精准地区分异常产生原因是未来的重要研究方向.

4.2.2 检测效率方面

1) 智能化、自适应的 IDS 机制

目前的检测机制大多数采用黑/白名单的方式进行检测,但二者相互独立且无法灵活适应外部情况的变化.因此,随着人工智能等智能化技术的发展,加强自身的学习能力和协作能力以提高检测精确度及实现智能化,是极吸引人的研究方向.比如,可构造自适应模型,利用增强式、类比学习等机器学习方法,对规则库进行补充和修正,以提升检测精度;又比如可以采用“智能列表”的理念加强它们之间的联系,将行为白名单的概念与一定的演绎智能相结合,以白名单动态定义黑名单,从而阻止新出现的威胁.

2) 高效节能的数学模型检测机制

目前在 ICS 中采用的如神经网络等数学模型,需消耗大量的存储资源和计算资源,同时随着检测精度的提升所需资源成倍数乃至指数增长.因此,越来越多的研究工作专注于节能数学模型的构建.如

Schmidt 等人[55]提出采用仿生学算法对流量进行检测,即通过人工免疫算法,以低成本的能耗对网络流量进行分类,发现异常流量信息.

4.3　检测架构

4.3.1　多源融合 IDS 架构

目前对架构的研究仅在部署和检测技术 2 个方面进行了简单的考虑,如文献[56]给出的架构只提及在企业网、控制网和现场网边界及控制网内部进行部署,以及采用访问控制白名单等进行异常检测.

这些方案未考虑复杂的工业控制环境,因此如何针对工业控制环境构建合理的检测架构是值得思考的问题.本文认为检测架构需从多方面进行思考、分析.比如在检测方法上,应构建更紧密的综合误用和异常这 2 种基本方法的机制;在检测对象方面,需考虑操作流程,并与系统的业务逻辑和设备操作规范密切结合;在现场设备、RTU、和服务器等设备上,针对有限的资源,部署不同量级的设备状态/操作的检测机制.

此外,单点、单类检测机制检测能力有限,无法进行全方位的检测,为此应开始研究多源融合的 IDS 框架.在该框架中需定义不同源之间传递的数据结构,并在后台构建数据标准化、关联分析等数据融合技术,以实现节点之间信息的交互.

4.3.2　并行 ICS 检测机制

在 ICS 中,为了提升 IDS 的检测效率,需采用多线程、流水线等并行优化技术来提升检测性能.然而大多数工业控制设备拥有的资源十分有限,无法采用普通的并行技术.为此,如何利用 ICS 资源实现并行检测是未来的重要研究方向.比如可依靠 CUDA(compute unified device architecture)技术[57]将检测数据按会话进行分配,在 GPU 中实现并行处理,有效地提升效率[58-59].又如可根据报文对应的网络事件,将数据分配到不同的 GPU 进行并行检测,规避了会话间的关系,实现对扫描等入侵行为的识别并提高了检测效率[60].

5　结束语

ICS 在国家基础设施中占据重要地位,但由于 ICS 与互联网的逐步融合,暴露出众多安全问题.IDS 作为主要的安全检测技术,可实时发现系统异常,进而确定可能的入侵行为.然而由于 ICS 的特殊性,传统 IDS 不能很好适用于工业控制领域,需要研究新的 IDS 技术.本文根据 ICS 的基本架构及其特性,给出了 ICS IDS 的解释、分类以及性能指标.同时,本文根据检测对象逐步递进的思想,从基于流量的 IDS、基于协议的 IDS、基于设备状态的 IDS 这 3 个方面,全面分析了 IDS 关键技术.最后,本文给出了 ICS IDS 未来的发展趋势.由于工业控制安全引起人们的关注较晚,学术界对 ICS IDS 的研究刚起步,还存在广阔的空间供研究人员探索.

参　考　文　献

[1] Stouffer K, Falco J, Scarfone K. SP 800—82 Guide to Industrial Control Systems (ICS) Security [S]. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2011

[2] Peng Yong, Jiang Changqing, Xie Feng, et al. Industrial control system cybersecurity research [J]. Journal of Tsinghua University: Science and Technology, 2012, 52(10): 1396-1408 (in Chinese)
(彭勇, 江常青, 谢丰, 等. 工业控制系统信息安全研究进展[J]. 清华大学学报: 自然科学版, 2012, 52(10): 1396-1408)

[3] Knapp E. Industrial Network Security—Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems [M]. Translated by Zhou Qin, Guo Bingyi, He Huimin, et al. Beijing: National Defense Industry Press, 2014 (in Chinese)
(Eric D. Knapp. 工业网络安全: 智能电网, SCADA 和其他工业控制系统等关键基础设施的安全[M]. 周秦, 郭冰逸, 贺惠民, 等译. 北京: 国防工业出版社, 2014)

[4] US Department of Homeland Security. Executive Order 13636—Improving Critical Infrastructure Cybersecurity [EB/OL]. [2015-05-31]. http://www.dhs.gov/publication/eo-13636-improving-ci-cybersecurity

[5] Office of the Press Secretary, The White House. Presidential Policy Directive—Critical Infrastructure Security and Resilience [EB/OL]. [2015-05-31]. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[6] Industrial Control Systems Cyber Emergency Response Team. ICS-CERT year in review 2013, 13-50369 [R/OL]. Arlington County, Virginia, USA: National Cybersecurity and Communications Integration Center, 2013 [2015-05-31]. https://ics-cert.us-cert.gov/ICS-CERT-Year-Review-2013

[7] Cheminod M, Durante L, Valenzano A. Review of security issues in industrial networks [J]. IEEE Trans on Industrial Informatics, 2013, 9(1): 277-293

[8] OPC Foundation. OPC unified architecture specification [S]. Scottsdale, Arizona, USA: OPC Foundation, 2006

[9] Computer security [EB/OL]. [2015-05-31]. http://en.wikipedia.org/wiki/Computer_security

[10] Pollet J, Tiger R. Electricity for free? The dirty underbelly of SCADA and smart meters [C/OL] //Proc of BlackHat Technical Conf. 2010 [2015-05-31]. https://media.blackhat.com/bh-ad-10/Pollet/BlackHat-AD-2010-Pollet-RTS-Electricity-for-Free-wp.pdf

[11] National Information Security Standardization Technical Committee. GB/T 20275—2006 Information Security Technology Techniques Requirements and Testing and Evaluation Approaches for Intrusion Detection System [S]. Beijing: Standards Press of China, 2006 (in Chinese)
(全国信息安全标准化技术委员会. GB/T 20275—2006 信息安全技术入侵检测系统技术要求和测试评价方法[S]. 北京: 中国标准出版社, 2006)

[12] Mitchell R, Chen I R. A survey of intrusion detection techniques for cyber physical systems [J]. ACM Computing Survey, 2014, 46(4): 55-84

[13] Striki M, Manousakis K, Kindred D, et al. Quantifying resiliency and detection latency of intrusion detection structure [C] //Proc of Military Communication Conf. Piscataway, NJ: IEEE, 2009: 1-8

[14] Misra S, Krishna P V, Abraham K I. Energy efficient learning solution for intrusion detection in wireless sensor networks [C] //Proc of the 2nd Communication Systems and Networks. Piscataway, NJ: IEEE, 2010: 1-6

[15] Stavroulakis P, Stamp M. Handbook of Information and Communication Security [M]. Berlin: Springer, 2010: 383-405

[16] Vollmer T, Manic M. Computationally efficient neural network intrusion security awareness [C] //Proc of the 2nd Int Symp on Resilient Control Systems. Piscataway, NJ: IEEE, 2009: 25-30

[17] Linda O, Vollmer T, Manic M. Neural network based intrusion detection system for critical infrastructures [C] //Proc of Int Joint Conf on Neural Networks. Piscataway, NJ: IEEE, 2009: 1827-1834

[18] Linda O, Manic M, Vollmer T, et al. Fuzzy logic based anomaly detection for embedded network security cyber sensor [C] //Proc of IEEE Symp on Computational Intelligence in Cyber Security. Piscataway, NJ: IEEE, 2011: 202-209

[19] Linda O, Manic M, Vollmer T, et al. Towards resilient critical infrastructures application of type-2 fuzzy logic in embedded network security cyber sensor [C] //Proc of the 4th Int Symp on Resilient Control Systems. Piscataway, NJ: IEEE, 2011: 26-32

[20] Linda O, Manic M, Vollmer T. Improving cyber-security of smart grid systems via anomaly detection and linguistic domain knowledge [C] //Proc of the 5th Int Symp on Resilient Control Systems. Piscataway, NJ: IEEE, 2012: 48-54

[21] Maglaras L A, Jiang Jianmin. Intrusion detection in SCADA systems using machine learning techniques [C] //Proc of 2014 Science and Information Conf. Piscataway, NJ: IEEE, 2014: 626-631

[22] Luo Yaofeng. Research and design on intrusion detection methods for industrial control system [D]. Hangzhou: Zhejiang University, 2013 (in Chinese)
(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)

[23] Modbus Application Protocol Specification [S]. Hopkinton, MA: The Modbus Organization, 2006

[24] TC 57—Power systems management and associated information exchange. IEC 60870-6-501 Telecontrol equipment and systems—Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations—Section 501: TASE. 1 Service definitions [S]. Geneva, Switzerland: IEC Central Office, 2005

[25] Curtis K. A DNP3 protocol primer [R/OL]. Raleigh, North Carolina: The DNP User Group, 2005 [2015-05-31]. http://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf

[26] Cheung S, Dutertre B, Fong M, et al. Using model-based intrusion detection for SCADA networks [C/OL] //Proc of SCADA Security Scientific Symp, 2007 [2015-05-31]. http://www.csl.sri.com/papers/scadaIDS07/SCADA-IDS-S4-2007.pdf

[27] Morris T, Vaughn R, Dandass Y. A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems [C] //Proc of the 45th Hawaii Int Conf on System Sciences. Piscataway, NJ: IEEE, 2012: 2338-2345

[28] Lin Hui, Slagell A, Martino C D, et al. Adapting Bro into SCADA: Building a specification-based intrusion detection system for the DNP3 protocol [C] //Proc of the 8th Annual Cyber Security and Information Intelligence Research Workshop. New York: ACM, 2013: 5

[29] Hong Junho, Liu Chen-Ching, Govindarasu M. Detection of cyber intrusions using network-based multicast messages for substation automation [C] //Proc of IEEE PES Innovative Smart Grid Technologies Conf. Piscataway, NJ: IEEE, 2014: 1-5

[30] Yang Yi, McLaughlin K, Littler T, et al. Rule-based intrusion detection system for SCADA networks [C] //Proc of IET Renewable Power Generation Conf. London: The Institution of Engineering and Technology (IET), 2013: 1-4

[31] Yang Yi, McLaughlin K, Littler T, et al. Intrusion detection system for IEC 60870-5-104 based SCADA networks [C] //Proc of Power and Energy Society General Meeting (PES). Piscataway, NJ: IEEE, 2013: 1-5

[32] Hadeli H, Schierholz R, Braendle M, et al. Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration [C] //Proc of the Conf on Emerging Technologies Factory Automation. Piscataway, NJ: IEEE, 2009: 1-8

[33] Zhang Dengfeng, Wang Zhiquan, Sun Jinsheng. Fault diagnosis technology in control systems [J]. Journal of Data Acquisition and Processing, 2002, 17(3): 293-299 (in Chinese)
(张登峰,王执铨,孙金生. 控制系统故障诊断的理论与技术[J]. 数据采集与处理,2002,17(3):293-299)

[34] Zhou Donghua, Ye Yinzhong. Modern Fault Diagnosis and Fault-Tolerant Control Technology [M]. Beijing: Tsinghua University Press, 2000 (in Chinese)
(周东华,叶银忠. 现代故障诊断与容错控制[M]. 北京:清华大学出版社,2000)

[35] Wen Xin, Zhang Hongyue, Zhou Lu. Fault Diagnosis and Fault Tolerant Control in Control System [M]. Beijing: China Machine Press, 1998 (in Chinese)
(闻新,张洪钺,周露. 控制系统的故障诊断和容错控制[M]. 北京:机械工业出版社,1998)

[36] Li Weihua, Xiao Deyun, Fang Chongzhi. An adaptive sliding window lattice filtering algorithms-based fault detector [J]. Acta Automatica Sinica, 1996, 22(2): 251-253 (in Chinese)
(李渭华,萧德云,方崇智. 一种基于自适应滑动窗格形滤波算法的故障检测器[J]. 自动化学报,1996,22(2):251-253)

[37] Patton R J. Robustness in model-based fault diagnosis: 1995 situation [J]. Annual Reviews in Control, 1997, 21: 103-123

[38] Edelmayer A, Bokor J, Szigeti F, et al. Robust detection filter design in the presence of time-varying system perturbations [J]. Automatica, 1997, 33(3): 471-475

[39] Sridhar S, Govindarasu M. Model-based attack detection and mitigation for automatic generation control [J]. Smart Grid, 2014, 5(2): 580-591

[40] Gertler J, Kunwer M. Optimal residual decoupling for robust fault diagnosis [J]. International Journal of Control, 1995, 61(2): 395-421

[41] Zhou Donghua, Sun Youxian, Xi Yugeng, et al. Real-time detection and diagnosis of "parameter bias" faults for nonlinear system [J]. Acta Automatica Sinica, 1993, 19(2): 184-189 (in Chinese)
(周东华,孙优贤,席裕庚,等. 一类非线性系统参数偏差型故障的实时检测与诊断[J]. 自动化学报,1993,19(2):184-189)

[42] Tan J C, Crssley P A, Goody J. Fault section identification on a transmission network using action factors and expert system technology [C/OL] //Proc of the 13th Power System Computation Conf (PSCC'99). 1999: 820-826 [2015-05-31]. http://www.pscc-central.org/uploads/tx_ethpublications/pscc1999_104.pdf

[43] Koppen S B, Frank P M. Neural networks in model-based fault diagnosis [C] //Proc of 1996 IFAC World Congress. Laxenburg, Wien: Int Federation of Automatic Control (IFAC), 1996: 67-72

[44] Monsef H, Ranjbar A M, Jadid S. Fuzzy rule-based expert system for power system fault diagnosis [J]. IEE Proc—Generation, Transmission and Distribution, 1997, 144(2): 186-192

[45] Goetz E, Shenoi S. Critical Infrastructure Protection [M]. Berlin: Springer, 2008: 161-173

[46] Verba J, Milvich M. Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS) [C] //Proc of Conf on Technologies for Homeland Security. Piscataway, NJ: IEEE, 2008: 469-473

[47] Fovino I N, Carcano A, Trombetta A, et al. Modbus/DNP3 state-based intrusion detection system advanced information networking and applications (AINA) [C] //Proc of the 24th IEEE Int Conf on Advanced Information Networking and Applications. Piscataway, NJ: IEEE, 2010: 729-736

[48] Carcano A, Coletta A, Guglielmi M, et al. A multidimensional critical state analysis for detecting intrusions in SCADA systems [J]. Industrial Informatics, 2011, 7(2): 179-186

[49] Lin Hui, Slagell A, Kalbarczyk Z, et al. Semantic security analysis of SCADA networks to detect malicious control commands in power grids [C] //Proc of Security of Information and Networks. New York: ACM, 2014: 29-34

[50] Mitchell R, Chen I-R. Behavior-rule based intrusion detection systems for safety critical smart grid applications [J]. Smart Grid, 2013, 4(3): 1254-1263

[51] Mitchell R, Chen I-R. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications [J]. Systems, Man, and Cybernetics: Systems, 2013, 44(5): 593-604

[52] Pan Shengyi, Morris T H, Adhikari U, et al. Causal event graphs cyber-physical system intrusion detection system [C] //Proc of the 8th Annual Cyber Security and Information Intelligence Research Workshop. New York: ACM, 2013: 40

[53] Yang Dayu, Usynin A, Hines J W. Anomaly-based intrusion detection for SCADA systems [C/OL] //Proc of the 5th Int Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies. 2005: 12-16 [2015-05-31]. http://wenku.baidu.com/link?url=t_Tt4k6YHPFkGcmWaDHGd6f3wu_9tY8Ky4e3Ey56Cdq5Dt1Cy63HsIC7FNCjatb9YlYNDmDKW1gc-GF-YGWX9zpKd8pIM4HRzp9GBS5jz7S

[54] Pan S J, Yang Qiang. A survey on transfer learning [J]. Knowledge and Data Engineering, 2010, 22(10): 1345-1357

[55] Schmidt B, Kountanis D, Al-Fuqaha A. A biologically-inspired approach to network traffic classification for resource-constrained systems [C] //Proc of IEEE/ACM Int Symp on Big Data Computing. Piscataway, NJ: IEEE, 2014: 113-118

[56] Yang Yi, McLaughlin K, Sezer S, et al. Multiattribute SCADA-specific intrusion detection system for power networks [J]. IEEE Trans on Power Delivery, 2014, 29(3): 1092-1102

[57] Wikimedia Foundation. CUDA [EB/OL]. [2015-05-31]. http://en.wikipedia.org/wiki/CUDA

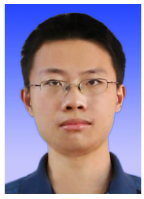
[58] Vasiliadis G, Polychronakis M, Ioannidis S. MIDeA: A multi-parallel intrusion detection architecture [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2011: 297-308

[59] Jamshed M, Lee J, Moon S, et al. Kargus: A Highly-scalable software-based intrusion detection system [C] //Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2012: 317-328

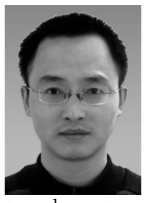
[60] De Carli L, Sommer R, Jha S. Beyond pattern matching: A concurrency model for stateful deep packet inspection [C] // Proc of ACM Conf on Computer and Communications Security. New York: ACM, 2014: 1378-1390

Yang An, born in 1988. PhD candidate. Student member of China Computer Federation. His main research interests include intrusion detection and industry control systems security.

Sun Limin, born in 1966. PhD supervisor in the Institute of Information Engineering, Chinese Academy of Sciences. Member of China Computer Federation. His main research interests include IOT and IOT security.



Wang Xiaoshan, born in 1986. PhD candidate. Student member of China Computer Federation. His main research interests include industry control systems security and wireless security (wangxiaoshan@iie.ac.cn).



Shi Zhiqiang, born in 1970. PhD supervisor in the Institute of Information Engineering, Chinese Academy of Sciences. Member of China Computer Federation. His main research interests include network system security and industry control systems security (shizhiqiang@iie.ac.cn).