文章编号: 1001-0920(2019)11-2277-12 DOI: 10.13195/j.kzyjc.2019.1302

工业控制系统网络入侵检测方法综述

张文安[1,2], 洪 榛[1,2†], 朱俊威[1], 陈 博[1,2]

(1. 浙江工业大学 信息工程学院，杭州 310023；2. 浙江工业大学 网络空间安全研究院，杭州 310023)

摘 要: 随着工业控制系统(industrial control systems, ICS)的网络化,其原有的封闭性被打破, 各种病毒、木马等随着正常的信息流进入ICS,已严重威胁ICS的安全性,如何做好ICS安全防护已迫在眉睫. 入侵检测方法作为一种主动的信息安全防护技术可以有效弥补防火墙等传统安全防护技术的不足,被认为是ICS的第二道安全防线,可以实现对ICS外部和内部入侵的实时检测. 当前工控系统入侵检测的研究非常活跃,来自计算机、自动化以及通信等不同领域的研究人员从不同角度提出一系列ICS入侵检测方法,已成为ICS安全领域一个热点研究方向. 鉴于此,综述了ICS入侵检测的研究现状、存在的问题以及有待进一步解决的问题.

关键词: 工业控制系统；网络入侵检测；模式匹配；时域分析；频域分析；设备指纹

中图分类号: TP273 **文献标志码:** A

A survey of network intrusion detection methods for industrial control systems

ZHANG Wen-an[1,2], *HONG Zhen*[1,2†], *ZHU Jun-wei*[1], *CHEN Bo*[1,2]

(1. College of Information Engineering，Zhejiang University of Technology，Hangzhou 310023，China；2. Institute of Cyberspace Security，Zhejiang University of Technology，Hangzhou 310023，China)

Abstract: With the networking of industrial control systems (ICS), its original closeness has been broken. Various viruses and Trojans have entered ICS with normal information flow, which has seriously threatened the security of ICS. Then, how to protect ICS security becomes an issue of prior importance. Intrusion detection, as an active information security protection technology, can effectively remedy the shortcomings of traditional security protection technologies such as firewalls. It is often considered as the second security line of ICS, and can realize real-time detection of external and internal intrusions of ICS. At present, the research of intrusion detection in industrial control systems is very active. Researchers from different fields, such as computer, automation and communication, have proposed a series of ICS intrusion detection methods from different perspectives, which has become a hot research direction in the field of ICS security. This paper briefly reviews the state-of-art of the ICS intrusion detection, the existing problems and the problems to be further solved.

Keywords: industrial control systems；network intrusion detection；pattern matching；time-domain analysis；frequency-domain analysis；device fingerprinting

0 引 言

早期的工业控制系统(industrial control systems, ICS)是一个相对独立和隔离的系统,与外部互联网保持着分离的关系,ICS自身的功能性和可控性是其关注的主要问题. 然而,随着网络和信息技术的快速发展,ICS逐渐朝着网络化、开放式体系结构发展. 近年来,工业互联网的呼声日益高涨,ICS走向网络化已是大势所趋. 在这样的背景下,ICS原有的封闭性被打破,而ICS自身的安全意识和系统化的安全保护措施还远未跟上,各种病毒、木马等随着正常的信息流进入ICS,已严重威胁ICS的安全性. 近年来,ICS的安全事件与日俱增,如何做好ICS安全防护迫在眉睫.

ICS的安全防护问题已在产业界和学术界引起了广泛重视. 研究人员开始借鉴传统信息安全领域的防护技术解决ICS的安全防护问题,并针对ICS的特殊性进行改良,例如工业防火墙、ICS系统漏洞挖掘(如针对PLC等控制器的漏洞挖掘)、风险评估技术等. 然而,漏洞挖掘和风险评估不能提供实时的网

收稿日期: 2019-09-13；**修回日期:** 2019-10-07.

基金项目: 国家自然科学基金项目(61573319, 61803334, 61973277)；浙江省自然科学基金项目(LQ18F030012)；国家留学基金项目(201908330040).

†通讯作者. E-mail: zhong1983@zjut.edu.cn.

络安全防护. 防火墙是一种被动防御性的安全工具,高级攻击者可以找到防火墙漏洞,绕过防火墙进行攻击,且防火墙无法防御来自ICS的内部攻击.

入侵检测是一种通过安全监控和异常报警的方式确保系统安全的防护技术,通过采集ICS系统中的设备和网络相关信息,并对这些数据信息加以分析、识别,从而判断系统中是否存在异常行为. 因此,入侵检测方法作为一种主动的信息安全防护技术可以有效弥补防火墙等传统安全防护技术的不足,往往被认为是ICS的第二道安全防线,可以实现对ICS外部和内部入侵的实时检测. 近年来,针对ICS的入侵检测得到了产业界和学术界的广泛关注,并取得了一系列研究成果. 本文将对这些研究成果进行简要综述.

1 工业控制系统入侵检测方法

1.1 基于模式匹配的ICS入侵检测方法

研究人员借鉴传统信息安全领域的入侵检测方法和思路用于解决ICS的入侵检测问题,从检测手段上可将这些方法分为基于异常的检测方法和基于签名的检测方法. 基于异常的检测方法获取ICS系统处于正常运行状态下的信息,并对信息加以分析,从中提取正常活动的特征模型,将正常活动状态的系统特征模型与待检测的系统特征一一比较,如果不符合正常特征模型,则认为系统发生入侵. 基于签名的检测获取处于攻击状态下的系统信息,对攻击信息进行分析,从中提取入侵行为特征模型,并将该特征模型与待检测系统的特征进行比较,若特征匹配则认为系统发生入侵行为.

另一方面,ICS的系统信息来自主机(即ICS中的各种设备,如控制器、传感器)或网络(如网络流量),根据数据信息来源又可将入侵检测分为基于主机(设备)的入侵检测和基于网络的入侵检测. 不管是异常检测还是签名检测,都需要提取ICS系统中的主机或网络在正常工况和受攻击情况下的特征. 特征提取和分析是ICS异常检测和签名检测的关键环节,特征提取不准确、不全面将导致入侵漏报或误报. 例如,异常检测只提取正常工况特征,很难做到全面、最优,往往导致误报,而签名检测只能在一定程度上识别已知的网络攻击,对未知攻击无法做到有效检测,漏报频繁. 因此,可将这种基于特征分析与匹配的方法统称为基于模式匹配的入侵检测方法. 在该类模式匹配方法中,通常在提取完特征后采用机器学习中的分类方法对特征进行分类. 由此可见,机器学习方法也被大量应用于入侵检测方法中.

由于ICS中设备和通信协议种类繁多,如各种类型的控制器、传感器以及多种多样的工业以太网、现场总线,基于模式匹配的ICS入侵检测方法可以从不同的切入点进行特征提取和分析,检测方法多种多样. 以下将简要概述基于主机特征分析的入侵检测和基于网络特征分析的入侵检测的一些研究结果.

信息源来自于网络的入侵检测方法主要通过获取网络信息流中的内容,从中提取关键字段特征值、频率、阈值、时间等特征,对网络中的数据包、流量、协议、拓扑结构等进行实时检测,从而判别网络入侵行为. 文献[1]以ICS中的网络通信协议为特征,所采用的具体协议信息包括通信类型、IP地址、MAC地址、端口号、modbus功能码、时间戳等,并以这些特征建立异常检测规则. 文献[2]提取通信模式、网络拓扑结构、静态应用功能等为特征,建立多模型的工业过程异常检测规则,采用隐马尔可夫模型进行异常分类. 文献[3-4]提取系统状态和通信协议为特征,具体包括网络通信类型、IP地址、MAC地址、端口号、modbus功能码、时间戳、系统中的事件等,其中文献[3]基于上述特征建立时间序列模型,采用隐马尔可夫模型进行异常判别,文献[4]利用系统知识采用状态检测方法进行异常检测. 文献[5]以通信协议为特征,所提取的特征包括数据包大小、协议类型、端口号、序列号、长度、校验等,采用半监督K均值(K-means)聚类算法对网络流量数据进行建模和异常判别. 文献[6]以网络流量为特征,所提取的特征包括网络连接及其内容的基本统计特征、基于时间的网络流量统计特征,采用支持向量机(support vector machine, SVM)算法进行分类和异常检测. 文献[7]以通信协议为特征,提取的特征包括数据包源/目的MAC地址、IP地址、端口号、协议标识符、长度和单元标识符,采用SVM和神经网络进行分类和异常判别. 文献[8]以网络流量为特征,即网络上流量源节点和目的节点间的流量,采用概率主成分分析(probabilistic principal component analysis, PPCA)方法进行异常流量检测. 文献[9]以网络流量为特征,包括人机界面(human machine interface, HMI)可编程逻辑控制器(programmable logic controller, PLC)之间的通信流量,HMI线程传输数据采集与监视控制系统(supervisory control and data acquisition, SCADA)命令的循环模式,采用有限自动机和离散马尔科夫链方法进行异常判别. 文献[10]提出了一种针对分布式网络协议3(distributed network protocol 3, DNP3)

的自动网络保护框架,采用基于规则的异常检测技术判别网络流量异常情况. 文献[11]提出了一种通过测量网络会话的时间特性来判别ICS网络是否遭受入侵. 文献[12]采用非平稳时间序列的随机分析方法对正常ICS网络流量序列进行建模和预测,从而实现对电网系统的异常检测. 文献[13]以网络流量为特征,采用基于熵的动态半监督K-means算法和单分类SVM进行流量异常检测. 文献[14]对常用的DNP3、传输控制协议(transmission control protocol, modbus TCP)和OPC(OLE for process control)协议进行解析,提取相关特征后采用神经网络进行分类和异常判别. 文献[15]对modbus TCP协议进行解析,采用SVM进行异常检测. 文献[16]研究了汽车CAN(controller area network)总线的入侵检测问题,提取CAN总线数据包格式特征,采用布隆过滤器(bloom filter)判别是否有入侵行为. 文献[17]研究了DoS(denial of service)攻击下的ICS入侵检测问题,提取网络流量为特征,采用K-近邻(K-nearest neighbor, KNN)等机器学习方法进行入侵判别.

上述基于网络的入侵检测方法其优点在于从网络数据包中分析入侵行为,与主机设备的配置等信息无关,可以部署在外部设备上进行检测,具有较好的移植性,能够对一个区域内所有设备的网关进行监控,降低入侵检测成本. 但是,当网络流量较高时,基于网络的入侵检测方法可能会在监控所有数据包时错过正在发起的攻击. 另一方面,被监测的ICS的操作行为和意图并不能完全从网络信息(如IP地址、端口等)推断出来. 在一些情况下,若网络攻击行为不违反ICS所使用的协议或设备之间的通信模式,则基于网络的入侵检测系统将无法检测这类攻击行为. 1998年,Martin Roesch用C语言开发了开放源代码的入侵检测系统Snort,可以认为是一种基于网络的入侵检测系统. 如今,Snort已发展成为一个具有多平台、实时流量分析、网络IP数据包记录等特性的强大的网络入侵检测系统. Snort有数据包嗅探、数据包分析、数据包检测、响应处理等多种功能,每个模块实现不同的功能. Snort部署比较灵活,适用于多种平台、操作系统,支持开源,是一种轻量级的入侵检测系统,但其功能还有待完善.

信息源来自于主机设备的入侵检测方法,主要检测主机设备的审计、设备的进程状态、日志内容及属性,如查看和监测设备登录状态、操作人员对设备和文件的操作权限、操作人员进行的敏感操作、设备的操作变量及输出变量、设备的运行状态(如开关状态、功耗)等信息. 基于这些信息提取特征,对其中的异常行为进行识别,并在尽可能短的时间内作出决策,中止攻击行为. 文献[18]通过PLC控制器、传感器等设备获取ICS输入输出数据,进而建立系统的状态特征模型,采用固定宽度聚类方法进行入侵判别. 文献[19]提取了热风炉拱顶温度,基于改进的CUSUM(cumulative sum)方法比较温度的预测值和实际值,依此识别攻击行为. 文献[20]使用自动关联核回归模型对ICS测量输出的正常行为进行建模,根据当前测量输出和模型输出计算残差,采用概率比测试判别异常. 文献[21]提取代表内核统计和I/O吞吐量的变量,包括服务器审计记录中的变量、CPU相关变量、内存利用率等,采用迭代数据挖掘方法进行异常判别. 文献[22]提取过程控制系统中各类变量的值,包括输入寄存器变量、保持寄存器变量、离散输入变量、线圈变量等,采用概率模型估计多变量过程参数值的演变情况并进行异常判别. 文献[23]提取发电机的运行数据以及一些相对数据,包括转子转速、变速箱温度、发电机功率、发电机与周围环境温度差以及发电机与发动机舱的环境温度差,通过主成分分析法寻找原始数据集中最能表征系统状态的属性,然后利用偏最小二乘法预测系统状态并检测异常行为. 文献[24]通过获取ICS输入输出数据建立系统行为模型,通过比较实际系统输入输出与模型输入输出进行异常判别. 文献[25]通过SCADA系统输入输出信号的时间序列建立系统行为模型,采用隐马尔可夫模型和神经网络进行异常行为判别. 文献[26]研究水处理控制系统的入侵检测问题,提取了控制器、传感器等各个关键设备中的输入输出数据,并建立正常行为模型,基于该模型设计分布式入侵检测算法. 文献[27]提出了基于相位测量单元(phasor measurement unit, PMU)数据的入侵检测方法,通过深度自动编码器学习PMU在正常工况下的数据模型,基于该模型输出与实际PMU输出值判别是否有入侵行为. 文献[28]研究了大规模系统的分布式入侵检测问题,提取系统的输入输出数据,并采用图论和数据时空相关性提出分布式入侵检测算法. 文献[29]提取一类计算机数控(computerized numerical control, CNC)加工系统的输入输出数据,通过分析数据的时序和相关性,采用诸如KNN等分类方法实现异常检测. 文献[30]同时提取ICS系统参数、过程数据以及网络流量数据,建立系统正常工

况检测模型,实现了基于数据的ICS多层次入侵检测. 文献[31]通过分析CAN总线的时钟偏移实现异常检测. 文献[32]通过提取智能电网中的运行数据,采用非监督学习方法实现了隐蔽性入侵检测. 上述基于主机设备的入侵检测方法主要通过提取设备或整个系统的参数、运行数据、控制逻辑等建立ICS系统特征模型,进而基于特征模型状态和输出与实际系统运行状态和输出之间的差异进行异常判别.

相比于基于网络的入侵检测方法,基于主机设备的入侵检测不需要监听网络数据流中的信息,减少了由于数据监听带来的带宽消耗. 但是,由于ICS系统之间的结构、功能等都存在较大的差异性,基于主机设备的入侵检测方法可移植性较低. 本节基于模式匹配的入侵检测算法,需要获取、分析网络中的数据包或者系统参数、配置、输入输出数据,计算量和系统资源消耗大,算法如何做到轻量型以适合于快速实时检测有待进一步研究.

1.2 基于ICS信号时域分析的入侵检测方法

对于ICS系统,无论是传感器和控制器等设备被攻击还是网络传输被破坏、篡改,最终都会导致被控对象的输入输出信号偏离正常工况值,从这一点看,其结果与系统发生故障(如传感器故障)很相似. 因此,很多研究人员借鉴故障诊断和坏数据检测的理论和方法以解决ICS的入侵检测问题,如贝叶斯框架下的二元假设检测方法[33-34]、最小二乘检测方法[35],基于新息(innovation)统计特性分析的χ^2检测器[36]以及基于残差生成原理的入侵检测方法[37-39].

文献[40]讨论了一般攻击信号的可检测性问题,给出了攻击不可检测的充要条件;文献[41]进一步讨论了能观性冗余度与攻击可检测性的关系. 受计算机数据安全原理启发,一些研究者尝试通过在ICS中主动加入特定激励信号以破坏攻击的隐蔽性. 文献[42]提出一种低成本数据加密方法,即设计时变编码矩阵对测量数据进行数值变换,在不需要改变χ^2检测器结构条件下实现了隐蔽攻击检测. 文献[43]针对单输入单输出ICS提出一种“动态水印”坏数据检测方法,在控制输入中附加一个随机激励信号,重新检验闭环系统状态的统计特性以确认传感器数据是否被恶意篡改.

另一些研究者着眼于通过保护部分测量数据的可靠性来保证有效的攻击检测. 文献[44]为了躲避常规χ^2检测器报警,设计了一类与无攻击模式下具有相同新息统计特性的攻击序列,在多传感器融合框架下通过利用部分安全可靠数据改变自身新息统计特性实现坏数据检测. 文献[45]研究了电网负载频率控制系统的入侵检测问题,设计了带随机未知输入的观测器,并通过残差分析判别是否发生入侵. 文献[46]通过噪声控制的方式设计一种新型的χ^2检测器,可有效检测出常规χ^2检测器无法检测的隐蔽性攻击. 文献[47]采用极大似然估计方法同时进行系统状态和攻击参数估计,从而实现隐蔽性攻击的检测. 文献[48]利用ICS系统的历史数据设计了一种summation入侵检测器,可以有效识别常规χ^2检测器无法检测的隐蔽性攻击. 文献[49]通过设置冗余传感器方法设计了一类动态观测器,通过残差分析方法实现了对非线性系统在假数据注入攻击下的入侵检测. 文献[50]通过利用ICS的历史状态统计信息设计了一种新型χ^2检测器,能有效识别常规χ^2检测器无法识别的智能电网隐蔽性攻击. 文献[51]结合状态估计方法和强化学习方法设计了隐蔽性入侵检测器. 文献[52]结合状态估计和相对熵方法对智能电网中的隐蔽性入侵进行检测. 文献[53]研究了基于传感器网络的目标定位系统中的传感器攻击检测问题,通过设计极大似然估计器获得传感器与目标之间的距离,进而分析传感器与目标之间的位置几何关系,实现了传感器入侵检测. 文献[54]将攻击信号视为系统未知输入,通过设计未知输入观测器和残差分析实现了电网的隐蔽性入侵检测.

类似地,文献[55]通过设计一类非线性未知输入观测器和残差分析实现了电网的隐蔽性入侵检测. 文献[56]通过设计离散时间动态观测器和残差分析的方法实现了无线网络化控制系统的入侵检测. 文献[57]提出了一种新的基于ICS系统状态估计的入侵检测方法,即将存在于“传感器-控制器”通道的入侵检测和存在于“控制器-执行器”通道的入侵检测分开处理,利用系统模型预测两个通道的输入输出信号,通过检验预测值与真实值是否存在重叠判断系统是否存在入侵行为.

上述入侵检测方法的基本思想是通过系统状态估计的方法获得ICS系统状态或输出,并通过信号差异性分析(如残差分析、坏数据与正常数据的距离)进行入侵判别. 一种更加直观的处理方法是直接将攻击信号估计出来,即将攻击信号重构和可视化,从而可以更加全面地获得攻击信号的各个特征,包括攻击信号的发生时刻、类型和大小等,更有利于系统管理者开展迅速的攻击溯源以及针对性防御. 有些研究

结果也将这种方法称为攻击辨识.

文献[58-60]将攻击信号视为未知时变输入信号,通过设计滑模观测器对攻击信号进行在线重构. 滑模观测器方法的辨识准确性较高,然而需要攻击分布矩阵已知并且满足严格的观测器匹配条件,即防御者已预知攻击目标,显然,攻击者意图是无法预先获知的. 在要求系统具备足够的测量信息冗余度的情况下,文献[61]基于扩维观测器研究了固定攻击目标下的龙伯格攻击估计器设计,并利用攻击辨识信息构造了基于补偿机制的安全控制策略. 通过在观测器设计中引入切换策略,该方法被进一步推广至更一般的切换攻击辨识问题的处理[62]. 文献[63]将传感器攻击描述为一个马尔科夫过程,通过一种无偏最小方差估计器得到攻击的最优估计值.

上述入侵辨识方法均为传统故障估计方法,仅将攻击作为普通未知输入处理,并且假设攻击分布矩阵已知,而忽略了攻击策略随时可能发生变化,因此无法保证获得可靠的攻击辨识性能. 需要强调的是,攻击能被准确辨识的基本前提是系统需同时满足充分的冗余能观性(或称稀疏能观性). 近年来,一些学者从信号稀疏性角度分析了攻击可检测性与系统冗余能观性之间的定量关系,对于攻击辨识理论具有重要意义. 攻击向量的S-稀疏性定性刻画了攻击者所能施加的攻击行为的复杂度,它表示攻击向量的最大非零元素个数为S. 文献[64-68]指出S-稀疏攻击能被检测的充分条件是系统满足S-稀疏能观性. 文献[69]针对静态电网给出了如何在多项式时间内找到具有最小稀疏性的不可检测攻击集合的优化搜索算法. 文献[70-71]证明在攻击者能任意操控超过一半传感器数据的情况下,估计器无法得到准确的状态估计值. 文献[72]进一步指出在此情况下攻击辨识准确性也无法保证,并证明S-稀疏传感器攻击存在最优估计值的充要条件是系统满足$2S$-稀疏能观性,并给出了梯度下降攻击估计算法的标称设计. 这些结论揭示了攻击辨识精度与系统传感器测量信息冗余度的内在联系. 在文献[72]的基础上,文献[73]通过引入正交互补矩阵,给出了同时存在执行器和传感器攻击下系统状态能观的充要条件. 文献[74]采用切换梯度下降方法大幅减少了文献[72]中标称梯度下降算法的计算量.

1.3　基于ICS信号频域分析方法的入侵检测方法

上述两种基于系统状态估计或攻击信号估计的方法均从系统输入输出信号的时域角度进行分析,对于一些低幅值高频率的攻击信号,时域分析方法并不一定适用. 尽管这些低幅值高频率的攻击信号不会瞬时产生很大的破坏,但会对ICS的一些节点(如执行器)产生长期劳损,从而起到潜伏式隐蔽性攻击的破坏作用. 针对这类攻击信号,研究者们提出了基于频域分析方法(如傅立叶分析)和时频分析方法(如短时傅立叶分析和小波分析),即将系统输入输出信号变换到频域,通过观察频谱可以发现异常频率的信号,从而实现入侵检测.

文献[75]基于小波的攻击检测签名方法(wavelet based attack detection signatures, WADeS)检测网络流量中的分布式拒绝服务(distributed denial of service attack, DDoS)攻击. 由于DDoS攻击会引起小波方差的变化,通过与阈值方法相结合,可以实现攻击检测. 文献[76]基于小波分析的能量分布检测DDoS攻击流量. 其中,正常时网络流量会表现出稳定的能量分布;当发生DDoS攻击时,会引起能量分布显著变化,其波形出现“尖峰”群. 此外,能量分布方差的峰值还可以在攻击的早期阶段被捕获,使基于小波分析的能量分布分析方法成为有效的攻击检测工具. 文献[77]利用离散小波变换分解网络流量信号,并提出偏差分数的概念来综合考虑高频段和中频段的信号变化. 偏差分数可以有效区分异常,并且适用于生成基于阈值的警报. 文献[78]应用小波分析来检测由于中间人攻击导致的异常情况. 文献[79]从频域的角度对DDoS攻击进行检测,通过离散小波变换(discrete wavelet transform, DWT)和离散傅立叶变换(discrete fourier transform, DFT)提取攻击特征,并比较了朴素贝叶斯分类器与常规阈值分类器的攻击检测效果. 文献[80]基于谱能量分布概率模型的信号处理技术,提出了一种检测低速率DoS攻击的方法. 文献[81]基于时频分析提出了两级攻击检测方法,首先将小波分析用于检测潜在的攻击,然后使用自相关分析提取攻击特征. 文献[82]结合常规自适应阈值设计和连续小波变换,实现了对DoS攻击的有效检测,并量化分析了攻击持续时间对检测性能的影响. 文献[83]设计了一种推荐系统攻击检测机制,通过组合离散小波变换提取特征,基于提取的特征和支持向量机对虚假文件进行分类. 文献[84]针对协作推荐系统,提出了一种使用Hilbert-Huang变换和SVM的虚假数据注入攻击检测方法. 文献[85]结合小波分析和决策树方法研究了智能电网的异常检测问题. 文献[86]结合小波分析和神经网络研究了智

能电网在假数据注入攻击下的入侵检测问题. 文献[87]结合小波分析和多尺度主成分分析方法研究了ICS的正弦入侵检测问题.

1.4 基于设备指纹技术的入侵检测方法

近年来,相关学者从提取ICS系统特征入手,借助机器学习等人工智能算法识别、检测攻击行为,其中ICS系统特征形象地被称为ICS系统“指纹”. 针对ICS入侵检测系统存在误报、漏报现象,无法组织起面向内部攻击的有效防范体系,设备指纹技术成为另一种解决入侵检测的有效方法. 设备指纹技术源自生物学中人体的指纹,它是生物体中表征唯一性的特征值,可用于快速区分与识别. 一般而言,设备指纹可以从设备物理特性、运行机理、网络特征中挖掘,如设备运行的数据采样周期、执行的物理模型、网络同步时间戳等,但也绝不是简单的表面特征,如设备的体积、种类、网络的MAC或者IP地址等,因为这些特征极易被截取、篡改和伪装. 因此,设备指纹技术主要是通过收集设备的各种隐性特征实现对其硬件身份的唯一识别[88],进而帮助系统快速、精确识别与检测出隐藏的攻击行为.

根据设备指纹技术入侵检测特点,一些文献虽未明确提出设备指纹,但在实际实施过程隐含了指纹特征挖掘. 如文献[89]提出了一种进程感知入侵检测方法,通过训练SVM模型实时检测环境中的入侵行为. 文献[90]提出了一种基于时序的边信道异常检测方法,该方法建立唯一的设备特征以识别未经授权的操作行为. 文献[91]针对网络化控制系统,从过程控制和数据采集的角度出发,将工业网络通信特性与时间序列联系起来,提取出两种不同行为,即功能控制行为和过程数据行为,基于这些行为特征,采用单分类方法进行入侵检测,此外还提出了加权混合核函数和参数优化方法,以提高分类性能. 文献[92]基于SCADA系统状态数据设计了两种新的入侵检测方法,一是自动识别任何给定系统的SCADA数据的一致和不一致状态,二是从识别状态中自动提取邻近检测规则. 文献[93]利用电网同步相量(synchrophasor)单元测量数据的时空相关性设计了入侵检测方法. 该方法能够检测正常和异常工况下的数据完整性攻击,适用于实时应用. 文献[94]利用智能电表的原始数据检测电力系统动态负荷变化攻击. 通过分析电表数据的频域特性建立攻击模型并实现入侵检测,是一种基于签名的入侵检测方法. 文献[95]同时利用电网PMU数据、负载预测值、电网状态估计值等信息建立电网系统特征,并基于这些特征设计了隐蔽性入侵检测算法.

然而,需要注意的是,一旦出现设备指纹提取不准确、不全面的情况,也将导致入侵检测结果的漏报、误报. 在ICS中,除了系统运行数据外,还需进一步挖掘隐藏信息以作为设备指纹. 一些隐藏于设备自身中,没有通过网络传输也不易被攻击者修改的参数也可以作为系统指纹信息而用于入侵检测,如PLC控制器的功耗. 通常将这种入侵检测方法称为旁路分析方法. 例如,文献[96-97]认为,当加工程序被攻击者修改后,PLC控制器在执行加工程序的过程中功耗会相应发生改变,通过在线测量PLC功耗变化情况,采用神经网络学习功耗变化规律实现入侵检测. 如何做到“非侵入式”的分析,即不影响设备自身正常运行以及如何有效地获取设备的这些隐蔽的运行参数是旁路分析方法需要关注的问题.

实际上,现有文献对设备指纹技术的讨论主要从网络层面与物理层面两个方面进行阐述. 从网络层面分析,文献[98]提出一个指纹识别架构,该架构使用轻量级签名在路由器级别对垃圾邮件发送者应用垃圾邮件检测过滤,可进一步扩展至ICS的消息传递. 此类设备指纹技术主要提取TCP/IP协议包头信息,如初始包大小、初始TTL、窗口大小、最大段大小、窗口缩放值、“不分段”标志、“sackok”标志和“nop”标志等. 通过对这些字段的标识识别特定的操作系统及版本号,从而确定垃圾邮件主机(或恶意攻击者). 另一方面,一些研究工作以网络中的硬件属性定义ICS合适的指纹特征. 文献[99]表明使用多达25个以太网帧可以唯一地识别和跟踪以太网设备,文献[100]提出在设备硬件中记录称为时钟偏差的小偏差,并以此偏差作为设备指纹检测攻击者的行为. 文献[101]详细阐述了如何基于数据包有效负载检查构建高度可靠的分类技术.

上述设备指纹识别方法主要通过观察网络流量的异常检测攻击,这对于网络攻击而言是有效的,但是针对物理攻击,需要从物理层面分析基于物理特征的指纹识别方法来进行检测与防御. 文献[102]研究基于物理模型的攻击检测方法,提出了将多种检测方法进行组合和配置可以有效提高攻击检测的成功率. 文献[103]提出挖掘无线电信号的开/闭瞬时特征,通过采集的实时信号消除其中的干扰因素,利用信号分析技术抽取相关特征,并利用有效特征实现设备精确匹配. 文献[104]结合Kalman滤波,以超高

频传感器设备信号长度、振幅方差、载波信号峰值、瞬时功率差值等关键特征生成指纹向量,并实行分类,获得70%左右的识别准确率. 这种方式虽然已经结合了滤波技术,但仍然在处理弱干扰信号时发生失效,进而导致设备指纹认证失败. 文献[105]针对GSM设备提取突发信号中的射频作为唯一指纹,利用最大似然估计与多重判定机制实现设备指纹认证,有效提高了攻击检测效率. 文献[106]从调制信号入手,针对模数信号的差异只对其中一个物理帧进行特征提取,从而实现物理网卡的准确识别. 文献[107]将基于调制信号的设备指纹生成技术扩展应用于物联网RFID(radio frequency identification)设备上,通过波形分析及频谱特征提取,最后利用KNN和SVM方法分类与识别,将检测错误率降至5%以下. 文献[108]给出了基于频谱特征约束下的物理层识别的理论建模和实验验证,采用无线物理层识别技术,利用无线信号物理波形的独特功能实现分类和识别合法设备.

近年来,也有研究人员将传统IT系统中的指纹生成机制应用到ICS系统中,进而有效实现了入侵检测. 文献[109]考虑设备指纹识别技术在ICS中的可行性应用研究,建立了一个参考模型,并利用该模型提取ICS的重要特性生成指纹. 文献[110]首次提出利用设备物理操作时间作为设备指纹来进行攻击检测,结合一定的力学分析,从整体上保障ICS的系统安全性. 在此基础上,文献[111]继续探讨了基于操作时间戳的物理指纹识别系统,并搭建了实验平台模拟化工生产验证了指纹的存在. 文献[112]提出“跨层响应”的方法,以层间的数据响应时间作为设备指纹,其攻击检测依据为攻击者的入侵会导致层间数据响应时间与正常运行时间不同,进而能够快速感应攻击者的攻击行为. 文献[113]建立系统的动态方程,并提出了一种将系统物理过程噪声作为设备指纹的攻击检测方法. 文献[114]研究了低功耗蓝牙信号的独特性,进一步探讨了指纹在具有蓝牙信标的环境中定位器件的应用,通过搭建物理实验平台对基于指纹识别的蓝牙定位进行验证,并详细分析了无线电信号及精确室内定位的关键参数对设备指纹生成的影响.

2 总结与展望

工业控制系统的网络化已经是一种发展趋势,网络化控制系统面临着前所未有的安全威胁. 作为一种重要的防御手段,入侵检测技术已成为网络化工业控制系统安全问题的一个重要研究方向,近几年已引起工业界和学术界的广泛关注. 主要的解决思路可以分为两大类:一是采用计算机信息安全领域的入侵检测方法,即基于网络或主机行为分析、坏数据检测的方法,在移植的过程中根据工业控制系统的特点进行改进;二是采用自动化领域的信号与系统的分析方法,将攻击视为输入系统的未知信号,借鉴故障诊断、状态估计、信号时域和频域分析的思路.

与计算机系统不同,工业控制系统之间的个体差异性较大,即使同类型的控制系统,由于不同的生产要求、生产规模、工艺参数等,也会导致工控系统会有不同的选型,从而表现出不同的特征. 因此,需要针对工控系统的入侵检测实行个性化定制. 此时,如何综合工控系统的生产过程、设备以及所采用的工控网络的特征,提取出能表征某个工控系统自身特点的DNA是实现精准入侵检测的关键. 其次,由于工控系统自身的脆弱性和复杂性,如多种多样的工控网络协议、接口标准,各种型号的控制器、传感器,使得工控系统受到入侵的部位和渠道也多种多样,极大地增加了入侵检测的难度. 另外,在工控系统中,信息的传输不仅有数据包的形式,还有其他形式,如电磁波等,这种多域空间的信息传输也使得工控系统受到入侵的渠道变得更加丰富,入侵检测的困难性也急剧增加. 目前,针对这些方面的入侵检测问题的研究还远远不够,网络化工控入侵检测依旧任重道远.

参考文献(References)

[1] Morris T, Vaughn R, Dandass Y. A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems[C]. Proceedings of the 45th Hawaii International Conference on System Science. Hawaii: IEEE, 2012: 2338-2345.

[2] Zhou C J, Huang S, Xiong N X, et al. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2015, 45(10): 2168-2216.

[3] Caselli M, Zambon E, Kargl F. Sequence-aware intrusion detection in industrial control systems[C]. Proceedings of the 1st ACM Workshop on Cyber-Physical System Security. Singapore: ACM, 2015: 13-24.

[4] Fovino I N, Carcano A, Murel T D L, et al. Modbus/dnp3 state-based intrusion detection system[C]. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications. Sydney: IEEE, 2010: 729-736.

[5] 王海凤. 工业控制系统的异常检测与防御资源分配研究[D]. 杭州: 浙江大学控制科学与工程学院, 2014.
(Wang H F. On anomaly detection and defense resource

allocation of industrial control networks[D]. Hangzhou: School of Control Science and Engineering, Zhejiang University, 2014.)

[6] 罗耀锋. 面向工业控制系统脆的入侵检测方法的研究与设计[D]. 杭州: 浙江大学控制科学与工程学院, 2013.
(Luo Y F. Research and design on intrusion detection methods for industrial control system[D]. Hangzhou: School of Control Science and Engineering, Zhejiang University, 2013.)

[7] 程超. 工业控制网络Modbus TCP协议深度包检测技术研究与实现[D]. 成都: 电子科技大学自动化工程学院, 2016.
(Cheng C. Research and implementation of deep packet inspection of Modbus TCP on industrial control network[D]. Chengdu: School of Automation Engineering, University of Electronic Science and Technology of China, 2016.)

[8] 侯重远, 江汉红, 芮万智, 等. 工业网络流量异常检测的概率主成分分析法[J]. 西安交通大学学报, 2012, 46(2): 70-75.
(Hou C Y, Jiang H H, Rui W Z, et al. A probabilistic principal component analysis approach for detecting traffic anomaly in industrial networks[J]. Journal of Xi'an Jiaotong University, 2012, 46(2): 70-75.)

[9] Kleinmann A, Wool A. Automatic construction of statechart-based anomaly detection models for multi-threaded industrial control systems[DB/OL]. ACM Transactions on Intelligent Systems and Technology, 2017, 8(4): 55.

[10] Bai J, Hariri S, Nashif Y A. A network protection framework for DNP3 over TCP/IP protocol[C]. IEEE/ACIS 11th International Conference on Computer Systems and Applications (AICCSA). Doha: IEEE, 2014: 9-15.

[11] Ponomarev S, Atkison T. Industrial control system network intrusion detection by telemetry analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 252-260.

[12] 高春梅. 基于工业控制网络的流量异常检测[D]. 北京: 北京工业大学计算机学院, 2014.
(Gao C M. Network traffic anomaly detection based on industrial control network[D]. Beijing: School of Computer Science & Technology, Beijing University of Technology, 2014.)

[13] 刘亚丽. 电网工控系统安全防护中流量异常检测的研究与应用[D]. 北京: 中国科学院大学沈阳计算技术研究所, 2018.
(Liu Y L. Research and application of traffic anormal detection in smart grid industrial control system[D]. Beijing: Shenyang Institute of Computing Technology, University of Chinese Academy of Sciences, 2018.)

[14] 刘灿成. 工业控制系统入侵检测技术研究[D]. 成都: 电子科技大学自动化工程学院, 2017.
(Liu C C. Research on intrusion detection technology of industrial control system[D]. Chengdu: School of Automation Engineering, University of Electronic Science and Technology of China, 2017.)

[15] 尚文利, 张盛山, 万明, 等. 基于PSO-SVM的Modbus TCP通讯的异常检测方法[J]. 电子学报, 2014, 42(11): 2314-2320.
(Shang W L, Zhang S S, Wan M, et al. Modbus/TCP communication anomaly detection algorithm based on PSO-SVM[J]. Acta Electronica Sinica, 2014, 42(11): 2314-2320.)

[16] Groza B, Murvay P. Efficient intrusion detection with bloom filtering in controller area networks[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(4): 1037-1051.

[17] Hosseini S, Azizi M. The hybrid technique for DDoS detection with supervised learning algorithms[J]. Computer Networks, 2019, 158: 35-45.

[18] Almalawi A, Yu X, Tari Z, et al. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems[J]. Computers & Security, 2014, 46: 94-110.

[19] 赵华. 工业控制系统异常检测算法研究[D]. 北京: 冶金自动化研究设计院, 2013.
(Zhao H. Research on anomaly detection algorithm for industrial control systems[D]. Beijing: Automation Research and Design Institute of Metallurgical Industry, 2013.)

[20] Yang D, Usynin A, Hines J W. Anomaly-based intrusion detection for SCADA systems[C]. Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation, Control And Human Machine Interface Technology. Albuquerque: American Nuclear Society, 2006: 12-16.

[21] Khalili A, Sami A. SysDetect: A systematic approach to critical state determination for industrial intrusion detection systems using Apriori algorithm[J]. Journal of Process Control, 2015, 32: 154-160.

[22] Erez N, Wool A. Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems[J]. International Journal of Critical Infrastructure Protection, 2015, 10(10): 59-70.

[23] Marton I, Sánchez A, Carlos S, et al. Application of data driven methods for condition monitoring maintenance[J]. Chemical Engineering Transactions, 2013, 33: 301-306.

[24] Zhanwei S, Zenghui L. Abnormal detection method of

industrial control system based on behavior model[J]. Computers & Security, 2019, 84: 166-178.

[25] Kalech M. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques[J]. Computers & Security, 2019, 84: 225-238.

[26] Adepu S, Mathur A P. Distributed attack detection in a water treatment plant: Method and case study[J]. IEEE Transactions on Dependable and Secure Computing, 2018: 1-14.

[27] Wang J, Shi D, Li Y, et al. Distributed framework for detecting PMU data manipulation attacks with deep autoencoders[J]. IEEE Transactions on Smart Grid, 2019, 10(4): 4401-4410.

[28] Chen P, Yang S, Mccann J A, et al. Distributed real-time anomaly detection in networked industrial sensing systems[J]. IEEE Transactions on Industrial Electronics, 2015, 62(6): 3832-3842.

[29] Wu M, Moon Y B. Intrusion detection system for cyber-manufacturing system[J]. Journal of Manufacturing Science and Engineering-transactions of the Asme, 2019, 141(3): 031007.

[30] Zhang F, Kodituwakku H A, Hines J W, et al. Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data[J]. IEEE Transactions on Industrial Informatics, 2019, 15(7): 4362-4369.

[31] Ying X, Sagong S U, Clark A, et al. Shape of the cloak: Formal analysis of clock skew-based intrusion detection system in controller area networks[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(9): 2300-2314.

[32] Ahmed S, Lee Y, Hyun S, et al. Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(10): 2765-2777.

[33] Kailkhura B, Han Y S, Brahma S, et al. Distributed bayesian detection in the presence of byzantine data[J]. IEEE Transactions on Signal Processing, 2015, 63(19): 5250-5263.

[34] Kailkhura B, Han Y S, Brahma S, et al. Asymptotic analysis of distributed bayesian detection with byzantine data[J]. IEEE Signal Processing Letters, 2015, 22(5): 608-612.

[35] Huang Y, Tang J, Cheng Y, et al. Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis[J]. IEEE Systems Journal, 2016, 10(2): 532-543.

[36] Manandhar K, Cao X, Hu F, et al. Detection of faults and attacks including false data injection attack in smart grid using kalman filter[J]. IEEE Transactions on Control of Network Systems, 2014, 1(4): 370-379.

[37] Guan Y, Ge X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks[J]. IEEE Transactions on Signal and Information Processing Over Networks, 2018, 4(1): 48-59.

[38] Amin S, Litrico X, Sastry S S, et al. Cyber security of water SCADA systems, part I: Analysis and experimentation of stealthy deception attacks[J]. IEEE Transactions on Control Systems and Technology, 2013, 21(5): 1963-1970.

[39] Amin S, Litrico X, Sastry S S, et al. Cyber security of water SCADA systems, part II: Attack detection using enhanced hydrodynamic models[J]. IEEE Transactions on Control Systems and Technology, 2013, 21(5): 1679-1693.

[40] Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2013, 58(11): 2715-2729.

[41] Lee C, Shim H, Eun Y. On redundant observability: From security index to attack detection and resilient state estimation[J]. IEEE Transactions on Automatic Control, 2019, 64(2): 775-782.

[42] Miao F, Zhu Q, Pajic M, et al. Coding schemes for securing cyber-physical systems against stealthy data injection attacks[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 106-117.

[43] Satchidanandan B, Kumar P R. Dynamic watermarking: active defense of networked cyber-physical systems[J]. Proceedings of the IEEE, 2016, 105(2): 219-240.

[44] Li Y, Shi L, Chen T. Detection against linear deception attacks on multi-sensor remote state estimation[J]. IEEE Transactions on Control of Network Systems, 2018, 5(3): 846-856.

[45] Ameli A, Hooshyar A, Yazdavar A H, et al. Attack eetection for load frequency control systems using stochastic unknown input estimators[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2575-2590.

[46] Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on SCADA systems[J]. IEEE Transactions on Control Systems and Technology, 2014, 22(4): 1396-1407.

[47] Kurt M N, Yilmaz Y, Wang X. Real-time detection of hybrid and stealthy cyber-attacks in smart grid[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 498-513.

[48] Ye D, Zhang T. Summation detector for false

data-injection attack in cyber-physical systems[J]. IEEE Transactions on Cybernetics, 2019: 1-8.

[49] Kim J, Lee C, Shim H, et al. Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors[J]. IEEE Transactions on Automatic Control, 2019, 64(3): 1162-1169.

[50] Chen R, Li X, Zhong H, et al. A novel online detection method of data injection attack against dynamic state estimation in smart grid[J]. Neurocomputing, 2019, 344: 73-81.

[51] Kurt M N, Ogundijo O E, Li C, et al. Online cyber-attack detection in smart grid: A reinforcement learning approach[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5174-5185.

[52] Singh S, Khanna K, Bose R, et al. Joint-transformation-based detection of false data injection attacks in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(1): 89-97.

[53] Zhang J, Wang X, Blum R S, et al. Attack detection in sensor network target localization systems with quantized data[J]. IEEE Transactions on Signal Processing, 2018, 66(8): 2070-2085.

[54] Ameli A, Hooshyar A, Elsaadany E F, et al. Attack detection and identification for automatic generation control systems[J]. IEEE Transactions on Power Systems, 2018, 33(5): 4760-4774.

[55] Wang X, Luo X, Zhang M, et al. Distributed detection and isolation of false data injection attacks in smart grids via nonlinear unknown input observers[J]. International Journal of Electrical Power & Energy Systems, 2019, 110: 208-222.

[56] Aldabbagh A W, Li Y, Chen T. An intrusion detection system for cyber attacks in wireless networked control systems[J]. IEEE Transactions on Circuits and Systems Ii-express Briefs, 2018, 65(8): 1049-1053.

[57] Mousavinejad E, Yang F, Han Q, et al. A novel cyber attack detection method in networked control systems[J]. IEEE Transactions on Systems, Man, and Cybernetics, 2018, 48(11): 3254-3264.

[58] Corradini M L, Cristofaro A. A sliding-mode scheme for monitoring malicious attacks in cyber-physical systems[J]. IFAC-PapersOnLine, 2017, 50(1): 2702-2707.

[59] Corradini M L, Cristofaro A. Robust detection and reconstruction of state and sensor attacks for cyber-physical systems using sliding modes[J]. IET Control Theory and Applications, 2017, 11(11): 1756-1766.

[60] Ao W, Song Y, Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory and Applications, 2016, 10(12): 1458-1468.

[61] Lu A, Yang G. Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks[J]. Information Sciences, 2017, 420: 96-109.

[62] Lu A, Yang G. Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer[J]. Information Sciences, 2017, 417: 454-464.

[63] Shi D, Elliott R J, Chen T, et al. On finite-state stochastic modeling and secure estimation of cyber-physical systems[J]. IEEE Transactions on Automatic Control, 2017, 62(1): 65-80.

[64] Chong M S, Wakaiki M, Hespanha J P. Observability of linear systems under adversarial attacks[C]. 2015 American Control Conference (ACC). Chicago: IEEE, 2015: 2439-2444.

[65] Fawzi H, Tabuada P, Diggavi S N. Secure estimation and control for cyber-physical systems under adversarial attacks[J]. IEEE Transactions on Automatic Control, 2014, 59(6): 1454-1467.

[66] Liu C, Wu J, Long C, et al. Dynamic state recovery for cyber-physical systems under switching location attacks[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 14-22.

[67] Chang Y H, Hu Q, Tomlin C J. Secure estimation based kalman filter for cyber-physical systems against sensor attacks[J]. Automatica, 2018, 95: 399-412.

[68] Shoukry Y, Nuzzo P, Puggelli A, et al. Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach[J]. IEEE Transactions on Automatic Control, 2017, 62(10): 4917-4932.

[69] Zhao Y, Goldsmith A J, Poor H V. Minimum sparsity of unobservable power network attacks[J]. IEEE Transactions on Automatic Control, 2017, 62(7): 3354-3368.

[70] Mo Y, Hespanha J P, Sinopoli B. Resilient detection in the presence of integrity attacks[J]. IEEE Transactions on Signal Processing, 2014, 62(1): 31-43.

[71] Mo Y, Sinopoli B. Robust estimation in the presence of integrity attacks[J]. Conference on Decision and Control, 2013, 60(4): 1145-1151.

[72] Shoukry Y, Tabuada P. Event-triggered state observers for sparse sensor noise/attacks[J]. IEEE Transactions on Automatic Control, 2016, 61(8): 2079-2091.

[73] Lu A, Yang G. Secure luenberger-like observers for cyber−physical systems under sparse actuator and sensor attacks[J]. Automatica, 2018, 98: 124-129.

[74] Lu A, Yang G. Switched projected gradient descent algorithms for secure state estimation under sparse sensor attacks[J]. Automatica, 2019, 103: 503-514.

[75] Ramanathan A. WADeS: A tool for distributed denial of service attack detection[D]. Calgary: College of Engineering, Texas A&M University, 2002.

[76] Li L, Lee G. DDoS attack detection and wavelets[J]. Telecommunication Systems, 2005, 28(3): 435-451.

[77] Barford P, Kline J, Plonka D, et al. A signal analysis of network traffic anomalies[C]. Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment. Marseille: ACM, 2002: 71-82.

[78] Dorsaneo J, Tummala M, Mceachen J C, et al. Analysis of traffic signals on an SDN for detection and classification of a man-in-the-middle attack[C]. The 12th International Conference on Signal Processing and Communication Systems (ICSPCS). Cairns: IEEE, 2018: 1-9.

[79] Fouladi R F, Kayatas C E, Anarim E. Frequency based DDoS attack detection approach using naive Bayes classification[C]. The 39th International Conference on Telecommunications and Signal Processing (TSP). Vienna: IEEE, 2016: 104-107.

[80] Wu Z, Yue M, Li D, et al. SEDP-based detection of low-rate DoS attacks[J]. International Journal of Communication Systems, 2015, 28(11): 1772-1788.

[81] Wen K, Yang J, Cheng F, et al. Two-stage detection algorithm for RoQ attack based on localized periodicity analysis of traffic anomaly[C]. The 23rd International Conference on Computer Communication and Networks (ICCCN). Shanghai: IEEE, 2014: 1-6.

[82] Dainotti A, Pescape A, Ventre G. NIS04-1: Wavelet-based detection of DoS attacks[C]. Global Communications Conference. San Francisco: IEEE, 2006: 1-6.

[83] Karthikeyan P, Selvi S T, Neeraja G, et al. Prevention of shilling attack in recommender systems using discrete wavelet transform and support vector machine[C]. The 8th International Conference on Advanced Computing (ICoAC). Chennai: IEEE, 2017: 99-104.

[84] Zhang F, Zhou Q. HHT-SVM: An online method for detecting profile injection attacks in collaborative recommender systems[J]. Knowledge Based Systems, 2014, 65(1): 96-105.

[85] Mishra D P, Samantaray S R, Joos G. A combined wavelet and data-mining based intelligent protection scheme for microgrid[J]. IEEE Transactions on Smart Grid, 2016, 7(5): 2295-2304.

[86] Yu J J, Hou Y, Li V O. Online false data injection attack detection with wavelet transform and deep neural networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(7): 3271-3280.

[87] 刘大龙, 冯冬芹. 采用多尺度主成分分析的控制系统欺骗攻击检测[J]. 浙江大学学报, 2018, 52(9): 1738-1746.
(Liu D L, Feng D Q. Deceptive attack detection of control system using multi-scale principal component analysis[J]. Journal of Zhejiang University, 2018, 52(9): 1738-1746.)

[88] 罗军舟, 杨明, 凌振, 等. 网络空间安全体系与关键技术[J]. 中国科学: 信息科学, 2016, 46(8): 939-968.
(Luo J Z, Yang M, Ling Z, et al. Architecture and key technologies of cyberspace security[J]. Scientia Sinica: Informationis, 2016, 46(8): 939-968.)

[89] Keliris A, Salehghaffari H, Cairl B R, et al. Machine learning-based defense against process-aware attacks on industrial control systems[C]. 2016 IEEE International Test Conference. Fort Worth: IEEE, 2016: 1-10.

[90] Dunlap S, Butts J, Lopez J, et al. Using timing-based side channels for anomaly detection in industrial control systems[J]. International Journal of Critical Infrastructure Protection, 2016, 15: 12-26.

[91] Wan M, Shang W, Zeng P. Double behavior characteristics for one-class classification anomaly detection in networked control systems[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(12): 3011-3023.

[92] Almalawi A, Yu X, Tari Z, et al. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems[J]. Computers & Security, 2014, 46: 94-110.

[93] Iqbal T, Banna H U, Riaz M H. Cyber intrusion detection through spatio-temporal correlation in optimal power flow problem[C]. Proceedings in 2018 International Conference on Engineering and Emerging Technologies (ICEET). Lahore: IEEE, 2018: 1-5.

[94] Amini S, Pasqualetti F, Mohsenian-Rad H. Detecting dynamic load altering attacks: A data-driven time-frequency analysis[C]. Proceedings in 2015 IEEE International Conference on Smart Grid Communications. Miami: IEEE, 2015: 503-508.

[95] Ashok A, Govindarasu M, Ajjarapu V. Online detection of stealthy false data injection attacks in power system state estimation[J]. IEEE Transactions on Smart Grid, 2018, 9(3): 1636-1646.

[96] 肖玉珺. 非侵入式的基于功耗的PLC异常监测系统[D]. 杭州: 浙江大学电气工程学院, 2017.
(Xiao Y J. Non - Invasive PLC anomaly detection system based on power consumption[D]. Hangzhou: School of Electrical Engineering, Zhejiang University, 2017.)

[97] Xiao Y, Xu Wenyuan, Jia Z, et al. NIPAD: A non-invasive power-based anomaly detection scheme for

programmable logic controllers[J]. Journal of Zhejiang University, 2017, 18(4): 519-534.

[98] Esquivel H, Mori T, Akella A. Router-level spam filtering using TCP fingerprints: Architecture and measurement-based evaluation[C]. The 6th Conference on Email and Anti-Spam (CEAS). Mountain View: IEEE, 2009: 1-10.

[99] Gerdes R M, Daniels T E, Mina M, et al. Device identification via analog signal fingerprinting: A matched filter approach[C]. Network and Distributed System Security Symposium (NDSS2006). San Diego: ISOC, 2006: 1-11.

[100] Kohno T, Broido A, Claffy K C. Remote physical device fingerprinting[J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(2): 93-108.

[101] Endi M, Elhalwagy Y Z. Three-layer PLC/SCADA system architecture in process automation and data monitoring[C]. The 2nd International Conference on Computer and Automation Engineering (ICCAE). Singapore: IEEE, 2010: 774-779.

[102] Urbina D I, Giraldo J A, Cardenas A A, et al. Limiting the impact of stealthy attacks on industrial control systems[C]. 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS2016). Vienna: ACM, 2016: 1092-1105.

[103] Danev B, Zanetti D, Capkun S. On physical-layer identification of wireless devices[J]. ACM Computing Surveys (CSUR), 2012, 45(1): 1-29.

[104] Rasmussen K B, Capkun S. Implications of radio fingerprinting on the security of sensor networks[C]. The 3rd International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007). Nice: IEEE, 2007: 331-340.

[105] Reising D R, Temple M A, Mendenhall M J. Improved wireless security for GMSK-based devices using RF fingerprinting[J]. International Journal of Electronic Security and Digital Forensics, 2010, 3(1): 41-59.

[106] Gerdes R M, Mina M, Russell S F, et al. Physical-layer identification of wired ethernet devices[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(4): 1339-1353.

[107] Danev B, Heydt-Benjamin T S, Capkun S. Physical-layer identification of RFID devices[C]. The 18th Conference on USENIX Security Symposium. Montreal: USENIX Association, 2009: 199-214.

[108] Wang W, Sun Z, Piao S, et al. Wireless physical-layer identification: Modeling and validation[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(9): 2091-2106.

[109] Caselli M, Hadžiosmanović D, Zambon E, et al. On the feasibility of device fingerprinting in industrial control systems[C]. International Workshop on Critical Information Infrastructures Security. Cham: Springer, 2013: 155-166.

[110] Formby D, Srinivasan P, Leonard A, et al. Who's in control of your control system? Device fingerprinting for cyber-physical systems[C]. Network and Distributed System Security Symposium (NDSS2016). San Diego: ISOC, 2016: 1-15.

[111] Gu Q, Formby D, Ji S, et al. Fingerprinting for cyber-physical system security: Device physics matters too[J]. IEEE Security & Privacy, 2018, 16(5): 49-59.

[112] Shen C, Liu C, Tan H, et al. Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks[J]. IEEE Wireless Communications, 2018, 25(6): 26-31.

[113] Ahmed C M, Mathur A P. Hardware identification via sensor fingerprinting in a cyber physical system[C]. 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). Prague: IEEE, 2017: 517-524.

[114] Faragher R, Harle R. Location fingerprinting with bluetooth low energy beacons[J]. IEEE Journal on Selected Areas in Communications, 2015, 33(11): 2418-2428.

作者简介

张文安 (1982−), 男, 教授, 博士生导师, 从事网络化系统融合估计与控制的理论及应用等研究, E-mail: wazhang@zjut.edu.cn;

洪榛 (1983−), 男, 副教授, 博士, 从事信息物理系统/物联网、工控安全、物联网安全与数据安全等研究, E-mail: zhong1983@zjut.edu.cn;

朱俊威 (1985−), 男, 副教授, 博士, 从事信息物理系统安全等研究, E-mail: junweizhu1001@zjut.edu.cn;

陈博 (1984−), 男, 教授, 博士, 从事信息融合、信息物理系统安全、分布式估计与控制等研究, E-mail: bchen@zjut.edu.cn.

(责任编辑：郑晓蕾)