doi:10.11959/j.issn.1000-436x.2017036

# 工业控制系统入侵检测研究综述

赖英旭[1]，刘增辉[2]，蔡晓田[1]，杨凯翔[1]
(1. 北京工业大学信息学部计算机学院，北京 100124；2. 北京电子科技职业学院自动化工程学院，北京 100176)

**摘 要**：工业控制系统是国家关键基础设施的重要组成部分，一旦遭受网络攻击，会造成财产损失、人员伤亡等严重后果。为向工控安全领域的研究人员提供理论支持，对工控系统攻击的特点和检测难点进行了分析，报告了工业系统中入侵检测技术的研究现状，并对不同检测技术的性能和特点进行了比较，最后生成了一份工业入侵检测研究综述。

**关键词**：工业控制系统；入侵检测；误用检测；异常检测
**中图分类号**：TP309 **文献标识码**：A

# Research on intrusion detection of industrial control system

LAI Ying-xu[1], LIU Zeng-hui[2], CAI Xiao-tian[1], YANG Kai-xiang[1]
(1. College of Computer Science, Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China;
2. Automation Engineering Institute, Beijing Polytechnic, Beijing 100176, China)

**Abstract:** Industrial control system was an important part of national critical infrastructure, once it was suffered from the cyber attack, it would cause property damage, casualties and other serious disasters. For providing theoretical supports to industrial security researchers, the features of attacks in an industrial control system and the difficulties of detection to these attacks were introduced. Then, a survey of intrusion detection technologies used by the industrial control systems was given. Also, the performance and characteristic were compared for the different types of detection technologies. Finally, an industrial intrusion detection research was generated.

**Key words:** industrial control system, intrusion detection, misuse detection, anomaly detection

## 1 引言

工业控制系统（ICS, industrial control system）是国家关键基础设施中的重要组成部分，全球每年会发生几百起针对 ICS 系统的攻击事件，虽然数量远低于互联网，但每一次事件都会使生产受到巨大影响，经济遭受重大损失。2010 年“震网”(stuxnet)病毒的爆发，让全球再一次明白，工业控制系统已成为黑客的主要目标[1]，随后“毒区”（duqu）和“火焰”（flame）病毒又相继出现，与“震网”共同形成“网络战”攻击群。2014 年，功能更为强大的 Havex 以不同工业领域为目标进行攻击，至 2016 年已发展到 88 个变种。2015 年底发生的乌克兰大面积停电事件又一次为工控安全拉响警报。

随着德国工业 4.0 战略进一步实施，工业控制系统的安全问题将更加严重。全球多数国家都将工业控制系统的网络攻击列为国家间战略制约手段，美国早在 20 世纪就开始关注此问题，由能源部和国土安全部成立了多个国家实验室，建立了关键基础设施测试靶场。2009 年，出台了国家基础设施保护计划（NIPP），2011 年，发布了“实现能源供应系统信息安全路线图”，2012 年，推动了 2 个国家级专项计划（国家 SCADA 测试床计划 NSTB 和控制系统安全计划 CSSP），为顺利开展工控系统信息安全问题的研究提供了坚实的基础平台。

虽然在中国尚未出现较大范围工业系统安全

**收稿日期**：2016-08-23；**修回日期**：2016-11-10
**基金项目**：国家智能制造专项基金资助项目（No.[2015]1170）
**Foundation Item:** The National Manufacturing Special Program (No.[2015]1170)

事件报道，但我国有高达 91%的 ICS 系统采用国外品牌，存在着极大感染工业病毒的潜在隐患。“十一五”期间，我国就将制定的 ICS 安全标准作为《信息化安全标准化“十一五”规划》的工作重点[2]。2011 年 9 月，工信部又发布了《关于加强工业控制系统信息安全管理的通知》，旨在强调加强工业信息安全的重要性、紧迫性，并明确了重点领域工业控制系统信息安全的管理要求[3]。随后，国务院又发布了《关于大力推进信息化发展和切实保障信息安全的若干意见》（国发[2012] 23 号），明确提出要保障工业控制系统安全[4]。国家发改委在 2011 年~2013 年间发布信息安全专项指南时，均将工业控制安全保障列为重要研究方向[5,6]。2016 年，科技部将“工业控制系统深度安全技术”列入“网络空间安全”重点专项计划[7]，这足以显示我国对工控安全发展的重视。

早期提出的多种 ICS 安全保障方案主要是移植传统的主动防御解决方案[8,9]，然而无法在高实时性与资源受限条件下进行有效预测与控制，因此，近年来，工业网络流量异常检测是这一领域的研究热点。本文对工业控制系统入侵检测技术进行了概述。首先，针对工控系统攻击的特点和检测难点，介绍了工控系统的特点；其次，分析了现有的工控系统 IDS 架构，讨论了它们的优缺点；最后，分析了工控系统 IDS 研究所面临的挑战，并对工业 IDS 的技术发展和应用实现进行了展望。

## 2 工业控制系统概述

当前的工业控制系统在具体部署时通常涉及如下几种网络：企业办公网络（简称办公网络）、过程控制与监控网络（简称监控网络）以及现场控制系统[10]，ICS 拓扑结构如图 1 所示。

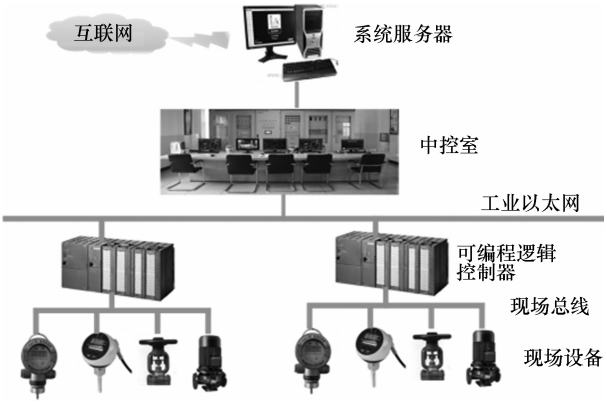



图 1 ICS 系统结构

办公网络中的管理者根据监控网络提供的数据对企业进行管理和决策，通过工厂信息管理系统（PIMS）等工控管理系统对企业的计划产排、仓储管理、生产调度等流程活动进行统一部署。监控网络中，操作员可使用数据采集与监控系统（SCADA）对现场运行的设备进行监测和控制，在调度控制方面有极高的可靠性。在现场控制层中，分布式控制系统（DCS）、可编程逻辑控制器（PLC）或远程终端单元（RTU）进行现场设备的逻辑控制、数据采样、指令执行等工业操作。

由此可见，传统计算机系统绝大多数都是由 PC 机、服务器通过 TCP/IP 协议通信，通用的操作系统有 Windows、Linux 等，系统兼容性好，软件升级频繁。而工业控制系统主要由 PLC、RTU、DCS、SCADA 和传感器等设备组成，通过 OPC、Modbus、DNP3 等专有协议信息通信，使用 WinCE 等嵌入式系统，系统兼容性差、软硬件升级困难。在性能特征等方面，传统计算机系统对实时性要求不高，运行有一定的延时，可停机或重启，需要高吞吐量，系统具有足够的资源支持。而工业控制系统实时性要求高，流量具有突发性和周期性，没有足够的升级资源和安保功能，并且必须具备容错功能，不能停机或重启[11]。

传统入侵检测在流量过滤和监测时存在细粒度过大、协议类型不兼容的问题，并且工业环境复杂，无法防御中间人或内部人攻击。因此，需要针对工控环境和协议类型制定基于工控环境的入侵检测技术，不能将传统入侵检测技术直接套用。

## 3 工业控制系统攻击分析

工业系统中的攻击按工业网络部署层次可分为 3 类：1) 监控网攻击，即来自信息空间的网络攻击，如篡改数据分组，破坏其完整性；2) 系统攻击，注入非法命令破坏现场设备，或违反总线协议中数据分组格式的定义，如篡改其中某些参数，令其超出范围而形成攻击；3) 过程攻击，命令是符合协议规范的，但违背了工控系统的生产逻辑过程，使系统处于危险状态（如反应釜的进料阀与一个出料阀不能同时打开）。其中，监控网攻击主要来自信息空间，其安全保障可借鉴传统安全技术。但现实中更多的攻击途径集中于系统攻击和过程攻击，且攻击方法已经转向慢渗透方式，仅统计网络流量特性已不能满足需求。目前，有学者提出在检测特征中

增加语义描述，如控制命令的相关参数、传感器的可信测量值等信息，可以检测出错误命令注入、篡改报文等系统攻击，取得了阶段性成果。但是由于未考虑控制命令之间的行为依赖关系，检测的准确性有待提高。

### 3.1　ICS 系统风险根源分析

造成 ICS 安全风险依然存在的原因主要有以下 4 个方面。

1) 工业网络运行环境复杂。为保证 ICS 系统向分布化、智能化方面发展，工业网络引入远程控制技术（如图 1 所示），其中，广泛采用通用 TCP/IP 技术、无线接入技术和 OPC 标准等，这些开放、透明的标准化技术为 ICS 系统开辟出广阔空间，却导致工业网络流量更加复杂，攻击者可以通过工控设备漏洞、TCP/IP 协议缺陷和工业软件漏洞等多种安全缺陷，构建更加隐蔽的攻击方法[12]。

2) 工业网络流量具有冲击特性。工业网络常常出现冲击性背景流量，即在很短时间段内，流量由各分支节点向控制中心节点或数据中心节点汇聚，此时，背景流量的主成分会急剧增大而后急剧减小，呈现冲击性特点，这种特性与攻击流量特性类似，导致无法有效识别攻击行为。

3) 传统解决方案无法移植。网络流量建模及其成因分析是检测异常流量的基础。工业网络流量包含实时流、非实时流和突发流，工业应用一般导致小数据量、高频率的循环数据交换，网络流量的平稳性、相关性、自相似性等特征与传统网络有着明显的不同，因此，无法简单移植传统网络的异常流量检测方案。

4) 硬件设计先天不足。应用于控制领域的很多微控制器没有提供硬件安全机制。Intel 的 X86 系列处理器从 80286 芯片开始就引入了保护模式机制，以后引入的页式存储技术也进行了保护机制的设计，所以通用 CPU 的保护机制是比较完善的。但是广泛应用于工业领域的 ARM7DMI 系列芯片，内核和应用程序共享相同的地址空间，这显然不能提供完整的安全保护。

### 3.2　工业网络攻击检测难点

企业办公网络与外部的互联网通信，存在来自互联网的安全威胁，这就需要具有较完备的安全边界防护措施，如防火墙、严格的身份认证及准入控制机制等。而监控网络通常采用 IP 或 UDP 协议，用于控制消息和操作消息的通信，由于协议未考虑安全性，因此极易受到攻击，如欺骗攻击、拒绝服务攻击、中间人攻击和端口扫描攻击等[13]。在设计异常检测方法时，需要结合每类攻击的特点，建立入侵检测系统模型。虽然现有方案分析了攻击的特点，充分利用样本信息，并考虑系统的实时性和可用性要求，为有效检测监控网攻击奠定了基础。但现实中更多的攻击者伪装成现场设备，在现场总线上监听和篡改监测数据，或进行隐蔽的过程攻击。所以，现有的工业入侵检测还存在以下 4 个难以满足实际应用需求的问题。

1) 如何正确理解控制命令的语义信息以检测变种攻击。

2) 如何获得控制命令之间的依赖关系以有效检测过程攻击。

3) 如何改进 IDS 检测算法以满足工控网络入侵检测准确性需求。

4) IDS 是纯滞后系统，如何保证 IDS 及时报警以满足工控系统的实时性需求。

总之，由于目前检测技术的局限性，仍存在一些过程攻击无法被有效检测，且未来的变种会更具欺骗性，成为攻击检测的重点和难点，关于准确性这一问题还需要进行更具创新性的研究和更多细致完善的工作。

## 4　工业 IDS 研究现状

根据现有的文献进行总结，工业 IDS 的检测方法主要有 2 种：变种攻击检测和隐蔽过程攻击检测。

### 4.1　变种攻击检测

攻击者为躲避检测，不断更新功能或在一些攻击特征上进行修改，制作出更多的变种攻击，导致检测手段失效。对于变种小的攻击，可采用误用入侵检测技术，利用攻击族的共性特征进行检测。对于变种大的攻击，采用异常入侵检测技术，进一步提高正常行为的建模准确度，凡与正常行为不一致的都归为入侵行为。下面将介绍检测变种攻击方面的工作。

#### 4.1.1　误用入侵检测技术

误用入侵检测技术又称基于特征的入侵检测，这一检测的前提是假设入侵者的活动可以用一种模式表示出来，入侵检测的目标是检测出主体活动是否符合这些模式。所以，误用入侵检测的关键是准确描述攻击行为的特征。

工控网的流量是具有鲜明特点的，工业现场设备通常采用轮询机制收集并上传数据[14]，因此，会呈现出高度周期性。许多攻击会引起网络流量频域范围内的变化，包括周期爆发频率的出现或消失、周期爆发持续时间的变化、噪声总量增加等。Liu 等[15]在爱尔兰都柏林国立大学（UCD）实验台上利用频率检测来检测网络攻击对智能电网的影响。测试电网模拟了 3 个水电站发电厂，当入侵者进入其中一个变电站局域网后，会控制 IED，断开输电线，使该发电厂断开，剩余 2 个发电厂必须满负荷发电，使发电厂正常运行，这就使变电站频率降低。所以针对该攻击应找出相应的策略，阻止网络攻击，断开入侵者连接，使其重新恢复到稳定值。Barbosa 等[16]对 SCADA 流量的特性进行研究分析，并根据常见的攻击类型的特点，得出基于网络流量的周期性检测方法，不仅可以成功检测出网络中的攻击，如拒绝服务（DoS）攻击、扫描信息攻击，还能在识别出攻击后，根据数据流量周期的变化来检测异常流量。实验中，Barbosa 利用快速傅里叶变换（FFT）和滑动窗口形成可视化的检测模型，其检测效率高，但在准确率上存在较大的问题。而工业网络的周期性存在不确定性，由于控制网络除了实时数据轮询功能，还有配置功能，在配置期间网络流量的周期性无法保证，容易引起误报。因此，单纯依靠周期性进行检测，将会产生很高的误报率。为此，侯重远等[17]提出了工业网络流量异常检测的概率主成分分析法（PPCA），分析了误报的原因是源于随机突发流量，建立了工业控制网络流量矩阵的概率主成分分析模型，并描述了随机突发流量对主成分分析法（PCA）的影响；接着利用变分贝叶斯理论对 PPCA 模型的秩进行推断，通过检测秩的变化判断异常流量，从而抑制随机突发流量对异常检测的干扰。实验中使用网络分析仪采集 ProfiBus 流量，使流量数据通过 OPC Tools 工具箱导入仿真软件，按照流量异常检测算法来进行异常检测，并模拟震网病毒在传播和攻击时的网络通信行为来实现对攻击流量的模拟，证实了基于 PPCA 模型的算法能有效降低误报率，平均下降率达到 32%，这种方法仅在攻击流量特征与正常业务类型差异比较大的情况下才有指导意义。

工业系统中的攻击方法已经转向慢渗透方式，仅统计网络流量特性已不能满足需求，研究者们开始采用基于行为的分析方法进行检测。Vollmer 等[18]应用一种多情感的遗传算法去自动提取异常行为的规则，可以为已知入侵行为建立规则。它与过去的网络入侵检测相似，但内容上有所不同。过去的工作是开发规则集，从未知行为中分离出已知行为。而此工作是通过使用遗传算法，为基于行为的系统检测到的特殊异常生成一组最优的 IDS 规则，此规则要满足完整性规则匹配、部分规则匹配和语法检查。通过输入数据流量分组，利用遗传算法，输出一组规则以及各自的适应值；然后利用 Nemesis、PackETH 和 ISIC 这 3 个工具创建 2 套测试网络数据，与生成的规则进行匹配，对 33 804 个测试分组进行测试，只误报了 3 个数据分组，说明此算法生成的规则的误报率很低，算法的精确度非常高。但是该方法对于每一种攻击至少生成 3 条检测规则，有些行为多达 8 条规则，影响了检测性能。Morris 等[19]针对 Modbus RTU/ASCII 协议，设计了一种基于 Snort 软件的入侵检测方法，利用 Snort 规则对上行数据和下行数据进行检测，该方法可以有效检测 Modbus 协议中出现的非法数据分组，但对检测规则的制定要求非常高。Morris 于 2013 年对其进行了改进，仔细分析了 Modbus 协议的漏洞，提出了 50 个基于入侵检测系统的签名规则，检测精度得到了很大的提升。

Hong 等[20]综合基于特征检测和行为检测的优点，提出一种基于主机和网络的集成式异常检测系统，基于主机的异常检测通过分析日志信息以检测应用层攻击（如用户重复错误口令、非法拷贝文件等），基于网络的异常检测，检测多播信息，以检测网络层的异常行为攻击。在变电站 WSU 网络安全试验台上测试，使用试验台模拟重放攻击，通过篡改数据分组、中间人和 DoS 等不同类型的网络入侵，来验证提出的异常检测算法。测试结果表明基于主机的异常检测系统的误报率（*FPR*）和漏报率（*FNR*）分别为 0.013%和 0.02%，基于网络的异常检测系统的 *FPR* 和 *FNR* 分别为 0.013%和 0.016%。由于基于主机的异常检测取决于生成的日志，而基于网络的异常检测不能检测未知攻击，所以为了提高检测率，基于主机的异常检测需要分析更多的系统日志，基于网络的异常检测需要周期更新算法。

误用入侵检测性能的比较如表 1 所示。它的关键问题是入侵行为的获取和表示，这种检测方法的优点是检测正确率高，缺点是变种攻击行为的检测能力有限。但是这个缺点并未影响其实际应用价

**表 1**　　**误用入侵检测性能比较**

| 研究文献 | 支持工控协议 | 检测技术 | 检测攻击类型或检测规则数 | 是否检测未知攻击 | 局限性 | 检测效果 |
|---|---|---|---|---|---|---|
| 文献[16] | Modbus | 流量周期性 | DoS 攻击、扫描信息攻击 | 否 | 控制网络的周期性存在不确定性 | 检测效率高，但在准确率上存在较大的问题 |
| 文献[17] | Modbus | 概率主成分分析法 | 只针对震网攻击 | 否 | 仅对于攻击流量特征与正常业务类型差异比较大的情况 | 使 *FPR* 平均下降率达 32% |
| 文献[15] | SCADA | 频率检测 | 过程攻击 | 否 | 无 | 频率降低 |
| 文献[18] | Modbus | 多情感的基因算法去自动提取异常行为的规则 | 30 条规则 | 否 | 该方法对于每一种攻击至少生成 3 条检测规则，有些行为多达 8 条规则，影响了检测性能 | 算法精度非常高，对 33 804 个数据分组进行了测试，只误报了 3 个数据分组 |
| 文献[19] | Modbus | 特征检测 | 50 条规则 | 否 | 无 | 检测精度高 |
| 文献[20] | Modbus、IEC 60870-5 | 特征检测和行为检测 | 重放攻击、中间人攻击、DoS 攻击 | 否 | 只能检测已知攻击 | *FPR* 为 0.13%，*FNR* 为 0.16%~0.2% |

值，由于实际情况中有些变种攻击仍使用部分已知攻击方法，该技术还是可以有效检测大部分变种攻击行为的。

#### 4.1.2　异常入侵检测技术

异常入侵检测技术是检测变种攻击的另一重要途径，它能够建立用户或系统的正常行为轮廓，在早期的异常检测系统中通常用统计模型，通过统计模型计算出随机变量的观察值落在一定区间内的概率，并且根据经验规定一个阈值，超过阈值则认为发生了入侵。后来很多人工智能技术应用于异常检测，如神经元网络技术和数据挖掘技术等。

Vollmer 等[21]提出了基于 EBP 神经网络的规则学习算法，运用 EBP 神经网络作为训练网络，按照 Snort 规则向量的形式，从 ICMP 数据分组中提取数据特征（向量）作为输入提交给训练网络，让网络学习规则，实验中针对 ICMP 数据分组提取了 129 个 Snort 规则，并分为 7 类，此网络能够以 60%的正确率识别出 DoS、混合行为和企图探测的网络攻击行为。Linda[22]将此方法结合基于动态窗口的数据分组特征提取技术，并使用 LM 算法将反馈神经网络中的误差最小化。实验中使用标记的数据分组进行规则的学习，之后使用攻击分组进行探测，检测率达到 100%。但其并没有根据现实场景的攻击类型进行多样化测试来进一步说明检测的准确性，也使其成为今后的研究实验方向。2014 年，Vollmer 等[23]又使用了一种低交互式的蜜罐技术（Honeyd），其可以在一台简单的主机上模拟数千台主机而减少硬件成本，目的是在较短的时间内收集信息，确认攻击者和可能破坏的网络平台。使用主动扫描工具 Nmap 和被动扫描工具 Ettercap 收集信息进行蜜罐的配置；根据这些配置信息，Honeyd 可以对虚拟主机进行自动配置和更新。文献[23]使用基于异常的检测方法，用户定义的网络行为被认为是正常的，任何针对蜜罐的行为被认为是不正常的。Vollmer 用一个小型校园网络作为测试场景，所有虚拟的主机设备都能够被识别，并且模拟主机的 IP 都会进入到异常检测系统中。如果系统认为有新的 IP，则它的一切行为都是异常的，并会被记录下来。但是 Honeyd 建立的虚拟主机的响应数据分组只有 ICMP、TCP 和 UDP，如果是真实的设备响应，则种类会更多。而且，虚拟的主机对于 IP 中的选项字段也没有正确响应，这都容易暴露蜜罐系统的存在。

Tsang 等[24]提出多主体的 IDS 架构，用于大型交换网络中的分布式入侵检测和预防控制。采用蚁群算法和无监督特征提取的方法，重点讨论如何提高聚类算法的精度和如何针对高维数据进行降维，为 ICS 中的入侵检测提供了一种多主体的分布式控制检测机制。实验中采用 KDDCup99 IDS 数据集评估训练模型，共 311 029 个记录。表明提出的蚁群聚类模型 ACCM 能提高现有的基于蚁群聚类算法的整体性能，能自动确定聚类数；为了对高维数据进行降维，评估比较了 4 个无监督特征提取算法，即主成分分析算法、*K*-means 算法、E-M 算法和独立成分分析（ICA）算法。其中，应用 ICA 能从网络数据中提取潜在特征，能加强聚类结果。结果证明 ACCM 应用 ICA 算法能有效检测已知或未知入侵攻击，有着较高的检测率，在识别正常网络流量上，具有较低的 *FPR*。Gao 等[25]提出了一组命令和响应注入、DoS 攻击，让商业 SCADA 系统遭受攻击，

使用 SCADA 网络事务数据记录器，捕获与这些攻击相关的网络流量，然后让捕获的网络流量结合 SCADA 控制系统正常运行捕获的流量，验证基于 IDS 的神经网络，也就是采用设备地址、MTU 命令、RTU 响应频率和物理特性等作为特征，应用神经网络模型检测命令和响应注入攻击。Gao 等在密歇根州立大学的 SCADA 测试床上进行了攻击测试，在正常操作下，抓取的数据分组有 12 000 个，当遭受中间人攻击时，抓取的数据分组有 5 000 个，*FPR* 为 0~6.2%，*FNR* 为 0~8.9%；在 DoS 攻击情况下，*FPR* 为 0~8.2%，*FNR* 为 0~2.0%；重放攻击的 *FPR* 为 45.1%，*FNR* 为 42.7%；其中，中间人攻击和 DoS 攻击的检测率非常高，但重放攻击的检测率非常低，这说明特征的选取是建立异常入侵检测模型的难点。

Kwon 等[26]针对 IEC61850 协议，提出了基于行为的 IDS，它使用多个网络特性的统计分析，得到高精度的检测。采用从智能变电站环境中捕获的真实的网络数据流量，通过分析 IEC61850 网络流量，利用静态特征和动态特征，来检测异常流量。测试了 288 个场景，包括 261 个正常操作场景，以及 27 个已知攻击，如扫描攻击、DoS 攻击、GOOSE 攻击和 MMS 攻击等；结果表明，提出的算法不仅能检测到 24 个已知攻击，还能检测出未知攻击，即使漏报了 3 个攻击，但是并无误报，并且算法精确度很高，为 99.0%。所以，该基于行为的 IDS 能有效识别出给定的实验中所有异常数据，并且无误报，检测率高。但是实验缺乏开放的可用网络数据集，无法比较其性能和精确度。Hadziosmanovic 等[27]也比较了 4 种基于行为的 IDS 模型（PAYL、PSEIDON、Anagram 和 McPAD），使用 *n*-gram 方法提取特征，测试数据集包括 Modbus 协议数据和局域网协议数据，结果显示这 4 种 IDS 在 Modbus 协议数据集上有比较高的检测精度，但是在 LAN 数据集上的检测精度比较低，进一步说明工控网与传统网络的 IDS 特征选择方法有较大的区别。

此外，Barbosa 等[28]提出使用服务器的轮询方式来模拟 SCADA 周期性的网络流量，从而通过流量之间的关系建立正常的行为模型，并且可以依据此方法建立异常行为模型。Carcano 等[29]提出了基于状态的入侵检测系统，它能够检测复杂攻击，并为 SCADA 架构设计了一个 IDS 原型，采用单分组签名技术和状态分析技术 2 种检测方法来分析 Modbus 数据分组。其原型包括 3 个模块：负载系统（LS）、状态控制器（SC）和规则分析仪（RA）。还提出了一种规则语言来描述 Modbus 签名和现场设备状态。为验证 SCADA、IDS 的效率和有效性，实验执行了 2 种测试，即单分组签名检测和临界状态检测来进行检测比较，结果表明，提出的 IDS 能够检测所有的潜在威胁。但 Barbosa 等定义的系统临界状态过于简单，所以能够检测的入侵行为类型较少。Parvania 等[30]使用网络入侵检测系统来保护混合配电系统（ADS），通过其网络流量特征进行数据分组协议合法字段的规则定义（IP 地址，有效的功能码）。ADS 为减少出现故障的恢复时间，启用了自动化恢复过程（FLISR），此自动化过程拥有一套严格的行为过程特征，在研究其配电系统的业务逻辑以及 FLISR 的基础上，确定了配电系统的 FLISR 过程操作，以及自动化操作的周期性规则定义，并且在特定环境的基础上，提出了可通过观察配电系统的电流、电压、功率流的守恒值来建立正常的特征基线，从而判断异常。实验使用 2 个 PLC 来模拟系统控制器，并验证了 DoS 攻击和中间人攻击。但实验由于只观察了一个通信链路，并没有充分验证通过观察电流、电压等物理定律来判断是否为攻击，这也成为他们今后的研究工作。

Hong 等[31]建立了网络安全测试台，包括电力系统模拟、变电站自动化和 SCADA 系统，并在测试台上进行了评估；提出的网络安全框架的主要任务是实时监控、异常检测、影响分析和缓解策略。而且还定义了网络安全基准测试，提出了 2 种异常检测算法，这 2 种算法在爱尔兰都柏林国立大学（UCD）的试验床上得到检验，并且计划通过 ICCP 连接 UCD 和 ISU（爱荷华州立大学）2 个测试台。

Zhou 等[32]为工业过程自动化提出了基于多模式的异常检测系统，能够从时间和空间上检测到 PCS 中的异常，提出的异常检测包含基于通信的异常检测（CAD），用 *N*-gram 序列检测通信状态；基于节点的异常检测（NAD），使用 *n* 元序列和统计模型进行检测，通过检测时间来判断异常，以及基于应用的异常检测（ADD）。此外，还设计了一个基于智能的隐马尔可夫（HMM）模型，以识别连续异常警报的攻击。最后，在 OPNET 环境的仿真平台上，使用 TEP 控制系统对入侵检测系统的检测精度和实时性能进行评估，即通过对各类攻击设置不同的攻击频率，测试运行时间，来检测不同攻击频率下的精确度。实验采用了欺骗攻击、篡改攻击

和 DoS 攻击，为训练 HMM 模型，还设计了故障注入（物理故障、通信故障和计算故障），使系统正常运行、注入攻击、注入故障，得到的训练数据集包含 7 200 个观察值，测试数据集包含 3 600 个观察值。分析模拟结果，证实 PCS 中的攻击在宏周期内能被快速检测出，误判率（*FPR* 和 *FNR*）低于 1.61%，并且提出的 IDS 能检测到未知攻击，其对 TEP 控制系统的性能几乎无影响。

为解决工业控制系统中通信行为的异常检测问题，Shang 等[33]使用改进的单类 SVM 建立了正常的通信行为控制模型，设计了基于粒子群算法的 PSO-OCSVM 来优化参数。该方法建立的入侵检测模型，依据正常的 Modbus 功能码序列，能够识别异常的 Modbus TCP 流量。在模拟实验中，当系统运行时，操作员通过 WireShark 抓取 Modbus TCP 流量数据分组，丢弃无 Modbus 功能码的数据分组。使用 Modbus 功能码作为特征向量，在提取特征后，Shang 等挑选了 180 个 Modbus 功能码序列，其中的 140 个作为训练样本，剩余的 40 个为测试样本。在 PSO-OCSVM 中，选用的种群大小为 20，进化代数为 50，利用交叉验证方法可以得出 OCSVM 的精确度。模拟结果表明，PSO 优化过程效率很高。测试样本的分类精度达到 96%，训练样本的分类精度达到 100%，说明 OCSVM 有较强的学习能力和泛化能力。提出的 PSO-OCSVM 能满足工业控制系统的异常检测。

异常入侵检测技术的性能比较如表 2 所示。由表 2 可知，虽然研究人员在变种攻击检测方面进行了深入研究，取得了很多优秀成果，但是这些算法还存在许多问题，最大的缺点是会产生虚警率，且结果缺乏可解释性。这主要是由于单纯地分析监控特征，忽略了其中的形成机理，造成特征表达信息的缺失。因此，工业控制系统中的变种攻击检测技术还需要进一步地完善和发展。

### 4.2　隐蔽过程攻击检测

过程攻击是指违背了生产过程的攻击。命令虽

**表 2**　　**异常入侵检测性能比较**

| 研究文献 | 支持工控协议 | 检测技术 | 检测攻击类型或检测规则数 | 是否检测未知攻击 | 局限性 | 检测效果 |
|---|---|---|---|---|---|---|
| 文献[22] | SCADA | 神经网络和动态窗口特征提取技术 | 零日攻击 | 是 | 无 | 检测率达 100% |
| 文献[23] | SCADA | 蜜罐技术 | 无 | 是 | 建立的虚拟主机的响应数据分组只有 ICMP、TCP 和 UDP | 能识别所有虚拟主机设备，并记录异常行为的 IP |
| 文献[24] | SCADA | 蚁群聚类算法和无监督特征提取技术 | DoS 、 Remote-to-Local（ R2L ）、 User-to-Root（U2R）和 Probing 攻击 | 是 | 无 | 能检测已知和未知攻击，检测率高，误报率低 |
| 文献[25] | 密歇根州立大学 SCADA 测试床和 Modbus | 神经网络 | 重放攻击、中间人攻击和 DoS 攻击 | 否 | 中间人攻击和 DoS 攻击的检测率非常高，但重放攻击的检测率非常低 | 重放攻击：*FNR* 为 42.7%，*FPR* 为 45.1%<br>中间人攻击：*FNR* 为 0~8.9%，*FPR* 为 0~6.2%<br>DoS 攻击：*FNR* 为 0~2.0%，*FPR* 为 0~8.2% |
| 文献[26] | IEC 61850 | 基于网络特征的统计分析 | 27 个攻击 | 是 | 缺乏与开放的可用网络数据集的比较性能和精确度 | 检测率高，无误报 |
| 文献[27] | Modbus | *n*-gram 特征提取技术 | 数据注入攻击 | 是 | 无 | 检测精度较高 |
| 文献[29] | SCADA | 语义分析技术 | 水母攻击 | 是 | 系统临界状态过于简单 | 能检测所有潜在威胁 |
| 文献[30] | Modbus、DNP3、IEC 61850 | 流量特性和协议特性分析技术 | DoS 攻击、中间人攻击和内部人攻击 | 是 | 无 | 能检测到自动化网络可信周界内发起的各种攻击场景 |
| 文献[32] | SCADA | *n*-gram 序列状态分析，统计模型分析 | 欺骗攻击、篡改攻击、DoS 攻击，故障注入 | 是 | 只基于系统知识 | 能快速检测到攻击，误判率低于 1.61% |
| 文献[33] | Modbus TCP | 单类支持向量机 | PLC 上的恶意代码 | 是 | 在数据预处理上只对 Modbus 功能码进行基本的向量处理，并未对所获得的所有数据进行建模 | 精确度高，有较强的学习能力和泛化能力 |

然符合协议规范，但违背了工控系统的生产逻辑，使系统处于危险状态。检测隐蔽的过程攻击方法可分为 2 种，一方面需要提取更多的上下文信息，如果信息量不充分，那么就可能存在漏报现象；另一方面，要获取工业控制系统中的领域约束逻辑，这是检测隐蔽过程攻击的关键，同时，也是一个非常耗时的过程。

Carcano 等[29]考虑到配置命令必须通过现场总线传递给 PLC，被动地监测总线流量可以发现异常，提出了基于状态的 SCADA 入侵检测系统，该系统包含 3 个模块：负载系统、状态控制器和规则分析器。设计了一种描述语言表达的智能电网，收集 PLC 和 RTU 的内部寄存器值、数字量及模拟量的输入和输出，为检测特征增加了语义描述，通过关键状态距离度量值能够检测隐蔽攻击（也称水母攻击），这种攻击由合法的 SCADA 命令组合形成，但组合后的命令能导致系统进入危险状态。

与 Carcano 提出的语义检测类似，Lin[34]提出了分布式网络入侵检测语义分析框架，通过评估执行控制命令时系统的状态，以此揭露攻击者的恶意意图。语义分析框架包括：1) 从 SCADA 网络数据分组中提取控制命令；2) 从变电站中的传感器获取测量值；3) 触发故障分析软件去估计可能的执行命令结果。在 IEEE 30 总线系统上对此方法进行评估，实验证明通过打开 3 个传输线路，即恶意地手动控制命令，攻击者可以通过传统的故障分析避免检测，立即使测试的 IEEE 30 总线系统处于不安全状态；语义分析能花费很少的时间提供可靠的恶意命令监控和检测。然后对其进行性能评估，主要是测量分析关键命令的执行时间和网络吞吐量，在测量执行时间中进行了网络监控和触发故障分析，其中故障分析导致了 IDS 性能下降，而提出的语义分析主要依靠 2 个特点来保证实时性：1) 电网中许多设备的关键执行命令是手动执行的，因此，控制命令的间隔是分钟级的；2) 关键命令的类型和数量有限，因此，IDS 语义分析计算量小。

Hadziosmanovic 等[35]开发了一种基于语义的网络 IDS。采用了 3 个步骤确定特征及语义信息。1) 确定了 24 个关键特征变量；2) 基于对话提取告警、控制命令等信息，增加特征变量的语义信息；3) 确定变量间的相关性，即一组变量可以从不同角度描述一个设备，以此增加语义关联信息。作者的模型可以有效检测部分过程攻击，但对于特征的语义描述还不充分，下一步的工作将是获得更多的上下文信息，包括更多的结构协议和更多的工程配置文件。

文献[36~39]一直致力于航空、医疗、电网等工业网络中的 IDS 研究。文献[40]为医疗领域中的 IDS 系统增加了丰富的领域语义信息，为医疗网络物理系统（MCPS）的医疗设备中嵌入的入侵检测提出了一种基于行为规则规范技术。在医疗系统中，将医疗的行为规则转换为状态机，并基于此，去检查行为偏差。以生命体征观察器（VSM）医疗设备为例，首先规定行为规则集；接着，将行为规则转化成状态机；然后，基于攻击原型，如鲁莽攻击、随机攻击和伺机攻击，收集合规度数据，确定合规度分布参数，从 IDS 性能评估生成的 ROC 曲线中估算 *FNR* 和 *FPR*。实验证明，所提出的方法能检测出低于 5%的鲁莽攻击者，以及低于 25%的随机攻击者和伺机攻击者。通过比较分析，证实了提出的基于行为规范的 IDS 技术要优于现有的 2 项基于异常的用于检测异常病人行为的技术。

隐藏式过程攻击检测方法如表 3 所示，从表 3 可以看出，检测隐蔽的过程攻击已经成为近年来工业 IDS 的研究热点，避免漏报和语义分析是关键。如何设计新的算法，提升过程攻击的检测精度是需要进一步研究的内容。

**表 3** **隐藏式过程攻击检测方法对比**

| 研究文献 | 支持工控协议 | 检测技术 | 检测攻击类型或检测规则数 | 是否检测未知攻击 | 局限性 | 检测效果 |
|---|---|---|---|---|---|---|
| 文献[29] | SCADA | 语义分析 | 水母攻击 | 是 | 系统临界状态过于简单 | 能检测所有潜在威胁 |
| 文献[34] | DNP3 | 语义分析 | 恶意控制命令 | 是 | 无 | 分析时间短 |
| 文献[35] | IEC 60870-5-104 | 自回归模型 | 直接控制攻击，间接控制攻击 | 是 | 延时较长 | 误报率为 4.5% |
| 文献[36~40] | Modbus | 状态机模型 | 错误命令注入，灰洞攻击 | 否 | 无 | 可检测出低于 5%的鲁莽攻击，低于 25%的鲁莽和随机混合攻击 |

## 5　工业 IDS 的研究趋势

准确性和实时性是 IDS 追求的 2 个目标，但是这 2 个目标又是相互矛盾的。

### 5.1　工业 IDS 的准确性保证

提高攻击检出率、降低 *FPR* 和 *FNR* 是工控系统攻击检测准确性与完备性需求的重要保证。目前，处理该问题的方法分为 2 类，一类方法是进一步提高检测规则的质量；另一类方法是应用更精确的检测算法，如采用神经元网络技术和数据挖掘技术等人工智能技术，以更大的内存消耗或更多的检测时间来换取检测精度。

提高检测精度的一类方法是建立高质量的检测规则。由于监控网络对实时性要求高，加之受限于资源等因素，需要采用轻量级的入侵检测系统。如 Oman 等[41]提出了基于 SCADA 网络的入侵检测和事件监控系统，能帮助操作员识别 SCADA 设备上错误或恶意的设置。SCADA 传感器系统测试床由通信系统、传感器系统、数字故障模拟器和消息系统组成。Oman 等使用 XML 图记录系统中的所有设备信息，如 IP 地址、Telnet 端口号、设备命令码等，使用 Perl 程序解析 XML 文件并由此产生 Snort IDS 特征，用以监测 RTU 的运行情况。该方法的优点在于自动收集并比较现场设备的配置，对关键信息的修改将产生报警信号，可以有效避免依靠人工识别所产生的漏报。基于 Snort 的网络监控可以有效阻止已知攻击，但无法对未知攻击进行检测。Linda[42]在上述研究结果的基础上，于 2011 年提出了一个低成本的基于模糊逻辑的异常检测算法，该算法能快速学习及快速分类，构建了一个基于模糊逻辑的规则库来建模正常的网络行为，使用在线最近邻聚类算法来对数据分组流提取模糊规则。在实验过程中记录了 2 组数据集，一组是由 60 661 个正常行为的数据分组组成的 6 个数据集，用于算法训练，训练共用时 11.946 s，使最大处理速度超过 5 000 个/秒，总共提取了 71 个模糊规则。另一组是由 11 个数据集组成的一组测试集，由 200 000 多个异常网络行为的数据分组组成，最后在该数据集上进行系统的性能评估，测试结果表明产生的正确分类率为 99.36%，*FPR* 为 0，*FNR* 为 0.9%。

选择高效的检测算法是提升检测精度的另一种方法。Ponomarev 等[43]提出了基于网络遥测技术的 IDS，利用网络服务器—客户端会话流模型，监控所有通过 ICS 网络的数据分组，主要依赖于服务器与客户端间的跳数，通过分析网络遥测数据的特征，识别不同机器设备上的通信来检测入侵。其 IDS 检测精度高，为 94.3%，无漏报；*FPR* 为 5.7%。Narsingyani[44]使用基因算法来优化异常入侵检测中的 *FPR*。利用带有 DoS 攻击的 KDDCup99 入侵检测数据集来实现该算法。从训练数据中随机选择创建初始化种群，生成一组分类规则，计算其适应值，从中选择具有较高适应值的规则。结果表明，通过增加规则数，可降低 *FPR*。所以，使用带有 KDDCup99 数据集的特征选择方法，可降低 *FPR*。

Linda 等[22]采用神经元网络模型构建了 IDS 系统并应用于电网中。由于数据流可以看成一个时间序列，现有的神经元网络模型是不适合处理时间序列的，Linda 等提出了一个基于特征提取方法的滑动窗模型，采集监控网络流量，通过滑动窗选取 IP 地址数、分组平均间隔、协议数量等参数作为模型的特征向量。实验结果表明，该模型在没有 *FPR* 的情况下具有非常高的检测精度，不仅能检测长报文的入侵攻击，还能检测出多个分组组合成的攻击。虽然这种方法可以在一定程度上检测未知攻击，但是必须首先进行模型离线学习，而嵌入式设备的学习能力十分有限，不利于模型及时更新。Dussel 等[45]提出了一种快速有效的基于负载的异常检测，能够检测未知攻击。该方法能够计算传输层数据分组的负载嵌入几何空间的相似性，包含网络数据采集、特征提取、计算相似性、异常检测 4 个阶段。通过对现代工业控制系统上出现的网络流量进行实验，用 2 组数据集进行测试，第一个数据集捕获的是 HTTP 流量，包含 1 000 000 个 TCP 数据分组，有 42 种相应的攻击集，11 种漏洞；第二个数据集是捕获 RPC 流量，包含 2 组数据，一组包含 57 100 个 TCP 数据分组，另一组包含 765 103 个 TCP 数据分组，共 19 种攻击，8 种漏洞。其 *FPR* 为 0.2%，模型的检测率为 88%~92%，表明该方法能用于检测网络流量的未知攻击，但是还不能完全满足工业需求。王海凤[46]针对工业控制系统易受到攻击，设计了面向工业控制网络的异常检测模型，能提高检测精度、降低 *FPR*，具有学习能力，能够检测出未知攻击；模型分为数据预处理、网络建模和异常检测模块。在数据预处理模块，设计了基于时间窗口的特

征提取方法；网络建模模块，针对工业控制网络的已知攻击和正常流量，提出了基于不完备信息的半监督 *K*-means 网络异常检测算法。根据已知的部分攻击类型，充分挖掘有效信息，结合半监督思想，提出了基于不完备信息的 *K*-means 算法，该算法选择标记样本作为训练集，将半监督技术与异常检测算法有机的结合，从而使系统在保持较高的检测率的同时具有较强的学习能力，能有效检测未知攻击，并模拟了工业网络常见攻击，如欺骗攻击、DoS 攻击、中间人攻击和端口扫描攻击，使用获取的 2 种训练数据进行测试，其中，用工业现场数据作为样本集，来验证设计方法的实时性、检测精度和 *FPR*；用 KDDCup99 数据集样本，验证对未知攻击的检测能力。结果表明该算法可以避免半监督 *K*-means 的缺点，适用于工业网络的异常检测。

Shang 等[33]使用改进的单类 SVM 建立了正常的通信行为控制模型，设计了基于粒子群算法的 PSO-OCSVM 来优化参数，并模拟实验证明粒子群算法的优化效率很高，提出的 OCSVM 有较强的学习能力和泛化能力，PSO-OCSVM 能满足工业控制系统的异常检测。Ambusaidi 等[47]于 2016 年提出了基于交互信息的特征选择算法（FMIFS），来为分类器选择最优特征。提出的基于最小二乘支持向量机（LSSVM）的入侵检测框架分为收集数据、数据预处理、分类器训练和攻击识别 4 个阶段，并利用 KDDCup99、NSL-KDD 和 Kyoto 2006+这 3 个入侵检测评估数据集来评估其性能。在实验中，LSSVM-IDS 结合 FMIFS 的检测模型，与结合其他算法的检测模型进行比较，表明该检测模型具有较高的检测率和较低的 *FPR*。

准确率提升技术的研究进展如表 4 所示。从表 4 中可以看出，入侵检测技术的准确率仍不尽人意，无论是在学术领域还是在工业界，高效的工控系统入侵检测算法是一个关键课题。

### 5.2 工业 IDS 的实时性保证

及时准确报警是工业系统安全实时性需求的重要保证，但由于采用了基于语义的分析方法，会增加入侵检测系统的滞后时间。解决此问题的有效方法包括 2 类，一类是提升硬件设备的计算能力；另一类方法是进行预估报警，提取预测系统的行为趋势，根据预测值进行预警。

Premaratneu 等[48]以模拟攻击智能电子设备（IED）为基础，为自动化变电站使用基于规则的 IDS 来应对威胁，与其他研究者方案的不同之处在于他设计的 IDS 是部署在一台独立主机上的，提升了 IDS 的计算能力，而大部分研究者的 IDS 是部署在现有设备上。同时，为了能够快速响应，Premratneu 等讨论了部署 IDS 的位置。IDS 是在真实场景（如 FTP 会话、远程登录会话、HTTP 浏览、ICMP pings 和 ARP 流量）上，模拟恶意攻击（如密码破解攻击、DoS 攻击、ARP 分组嗅探攻击），测试系统的检测能力，证实系统能检测到恶意攻击，对于攻击能做出快速报警响应，并为基于已知攻击的统计分析，提出了入侵时间风险评估方法。

Lin[34]提出了一种新的基于语义的检测方法。

**表 4 准确率提升技术对比**

| 研究文献 | 支持的工控协议 | 检测技术（算法） | 检测攻击类型或检测规则数 | 是否检测未知攻击 | 局限性 | 检测效果 |
|---|---|---|---|---|---|---|
| 文献[41] | SCADA | 事件监控、特征提取 | 电力有关攻击 | 否 | 无 | 可避免人工识别情况下产生的漏报 |
| 文献[42] | Modbus | 模糊集 | Probing 攻击 | 是 | 必须首先进行模型离线学习，而嵌入式设备的学习能力十分有限，不利于模型及时更新 | 正确分类率为 99.36%，*FPR* 为 0，*FNR* 为 0.9% |
| 文献[43] | Modbus | 网络遥测技术 | 中间人攻击、DoS 攻击、欺骗攻击、分组注入攻击 | 是 | 无 | 精确度为 94.3%，*FPR* 为 5.7%，无漏报 |
| 文献[44] | 无 | 基因算法、特征选择 | DoS 攻击 | 否 | 无 | 规则数增加，降低 *FPR* |
| 文献[45] | Modbus | 基于载荷的异常检测 | 19 种攻击及 8 种漏洞 | 是 | 无 | *FPR* 为 0.2%，检测率为 88%~92% |
| 文献[46] | 无 | 不完备信息的半监督 *K*-means 技术、 | 欺骗攻击、DoS 攻击、中间人攻击、端口扫描攻击 | 是 | 无 | 能提高检测精度，降低 *FPR* |
| 文献[47] | 无 | 基于交互信息的特征选择 | DoS、U2R、R2L、Probing 攻击 | 是 | 无 | 检测率高，*FPR* 低 |

依靠以下 2 个特点来保证其实时性：1) 电网中许多设备的关键执行命令是手动执行的，因此，控制命令的间隔是分钟级的；2) 关键命令的类型和数量有限，因此，IDS 语义分析计算量小。

预估报警是保证入侵检测实时性的新趋势。文献[39]讨论了信息物理系统（CPS, cyber physical system)中的 IDS 与传统 IDS 的区别，并指出传统 IDS 监控主机和用户的行为，而工控网中监测的是物理设备的行为，这些行为大部分是周期的，或是条件触发的，具有可预测性。Samdarshi 等[49]对 SCADA 系统提出了集成的 3 层 IDS 模型，其中，包含一个假设模块层，能够预测恶意的命令信号。这 3 层分别是通信网络保护层、命令和状态认证层、现场数据验证层。对这 3 层分别进行攻击测试，验证了 3 层 IDS 模型的有效性。Singh 等[50]针对 SCADA 网络安全和入侵检测，提出了一个带有比较器模块的测试台。比较器模块包括 SCADA 应用程序数据解析器、PSAT 模拟器和比较器，用于检查 RTU 上的入侵。当入侵时，比较器模块中的状态估计器会计算当前真实的响应状态，与以 PSAT 模拟结果为基础计算出的正常理想值比较，如果偏差较高，系统就会发生警报。Sridhar 等[51]从电力系统频率和电力市场运营方面分析了数据完整性攻击对自动化发电站控制（AGC）的影响，对此提出了基于模型的异常检测和攻击缓解算法，并通过模拟研究对提出的异常检测算法进行性能评估。依据网络攻击的环境，为 AGC 提出一种结合智能攻击检测和缓解的攻击弹性控制机制，它能够检测出存在的恶意测量值，并阻止控制器执行错误的 ACE（区域控制误差）计算；对于不可信测量值，使用基于模型的方法保持生产和需求间的平衡。当发现传输网络和控制中心被攻击时，传感器的测量值将不再可信，控制中心进入了盲区。提出的算法使用实时负载预测方法来预测 AGC 性能，并获得 ACE 预测值，采用 ACE 统计特征和时间特征 2 个规则来检测异常，如果预测值超过了阈值则进行报警，结果表明，该方法能有效缓解攻击，在攻击期间能有效维持系统频率，改善了 IDS 的滞后性。但完全按照预估理论进行报警，会有比较高的 *FPR*。

IDS 实时性的研究进展如表 5 所示，从表 5 中可以看出，工业 IDS 准确性与实时性之间的矛盾将会一直存在，矛盾的逐步解决也将促进工业 IDS 检测技术的进步。

## 6　结束语

针对上述问题的分析，目前的检测技术仍有局限性，还存在一些过程攻击无法被有效检测，且未来的变种会更具欺骗性。本文针对工业控制系统入侵检测技术本身存在的问题，从攻击方法、变种攻击检测、隐蔽过程攻击检测技术等几个方面进行了深入研究。首先讨论了工业控制系统的特点和攻击途径，主要有针对监控网的攻击、系统攻击和过程攻击，并对工业控制网络中攻击检测的根源和难点进行了深入分析；然后阐述了异常检测和误用检测技术的研究现状，分析了已有算法的优缺点；最后对隐蔽过程攻击的检测技术难度以及对基于语义的检测技术现状进行了分析。

工业控制系统入侵检测技术的研究是一个发展迅速的领域。虽然学术界已经获得相当的研究进展和积累，但是随着攻击方法的不断升级，工业领域还在不断地提出更高的新要求，带来新的课题和挑战。

入侵检测就是在追求准确性和实时性这 2 个目标及不断平衡的过程中发展深入的。基于语义的检测分析准确性好，但计算量大、耗时长，且随着语义描述信息的增加，计算量还在不断增长。为了满足工业控制系统的报警实时性需求，人们在进行及时报警时总是要牺牲一定程度的语义计算。对该方面的研究将有助于跨越传统安全防御技术无法简单移植到工业控制领域的鸿沟，解决工业控制系统安全问题，也可为物联网、云计算、移动互联网等网络安全研究提供新思路。

**表 5　　实时性提升技术对比**

| 研究文献 | 支持工控协议 | 检测技术（算法） | 检测攻击类型或检测规则数 | 是否检测未知攻击 | 局限性 | 检测效果 |
|---|---|---|---|---|---|---|
| 文献[48] | IEC 61850 | 特征提取 | 密码破解攻击、DoS 攻击、ARP 欺骗 | 否 | 仅限于已知攻击的统计分析 | 能对攻击做出快速报警响应 |
| 文献[34] | DNP3 | 语义分析 | 恶意控制命令 | 是 | 无 | 分析时间短 |

## 参考文献：


[1] DONALD P C. The application of autonomic computing for the protection of industrial control systems[M]. Tucson: The University of Arizona, 2011.

[2] 《国家信息安全标准化"十一五"规划》(摘登)[EB/OL]. http://wenku.baidu.com/view/71b8206eb84ae45c3b358cb4.html, 2007.
National information security standardization of 11th five-year planning (act) [EB/OL]. http://wenku.baidu.com/view/71b8206eb84ae45c3b358cb4.html, 2007.

[3] 《关于加强工业控制系统信息安全管理的通知》工信部协[2011] 451 号[EB/OL]. http://wenku.baidu.com/view/53681f4fe45c3b3567ec8b08.html, 2011.
The notice to strengthen information security management of industrial control system[EB/OL], http://wenku.baidu.com/view/53681f4fe45c3b3567ec8b08.html, 2011.

[4] 中华人民共和国国务院. 国务院关于大力推进信息化发展和切实保障信息安全的若干意见[EB/OL].http://www.gov.cn/ zwgk/2012-07/17/content_2184979. htm, 2012.
The State Council of the People's Republic of China. The State Council on vigorously promote the development of information technology and ensure the several opinions of the information security[EB/OL]. http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm,2012.

[5] 国家发展和改革委员会高技术产业司. 国家发展改革委办公厅关于组织实施 2012 年国家信息安全专项有关事项的通知(发改办高技[2012]2019 号) [EB/OL]. http://www.bjpc.gov.cn/tztg/201208/P020120828415567913703.pdf, 2012.
The National Development and Reform Commission, the High Technology Industry Company. General Office of the National Development and Reform. Commission about the notice to organizing the implementation of the national information security 2012 special matters (The National Development and Reform Commission and The High Technology Industry Company [2012] No.2019) [EB/OL]. http://www.bjpc.gov.cn/tztg/201208/P020120828415567913703.pdf, 2012.

[6] 国家发展和改革委员会高技术产业司. 国家发展改革委办公厅关于组织实施 2013 年国家信息安全专项有关事项的通知(发改办高技[2013]1965 号) [EB/OL].http://www.ndrc.gov.cn/zcfb/zcfbtz/ 2013tz/t20130822_554528.htm, 2013.
The National Development and Reform Commission, the High Technology Industry Company. General Office of the National Development and Reform. Commission about the notice to organizing the implementation of the national information security 2013 special matters (The National Development and Reform Commission and the High Technology Industry Company [2013] No.1965) [EB/OL]. http://www.ndrc.gov.cn/zcfb/zcfbtz/2013tz/t20130822_554528.htm, 2013.

[7] “工业控制系统深度安全技术”列入科技部发布的“网络空间安全”重点专项 2016 年度项目申报指南[EB/OL]. http://www.kongzhi.net/news/detail_156575.html, 2016.
"Industrial control system profound security technology" included in "cyberspace security" 2016 special project application guide the science and technology ministry published[EB/OL]. http://www. kongzhi.net/news/detail_156575.html, 2016.

[8] SHIN S, KWON T, JO G Y, et al. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks[J]. IEEE Transactions on Industrial Informatics, 2010, 6(4): 744-757.

[9] JONES R A, HOROWITZ B. A system-aware cyber security architecture[J].Systems Engineering, 2012, 15(2): 225-240.

[10] 胡毅, 于东, 刘明烈. 工业控制网络的研究现状及发展趋势[J]. 计算机科学, 2010, 37(1): 23-28.
HU Y, YU D, LIU M L. Present research and developing trends on industrial control network[J].Computer Science, 2010, 37(1): 23-28.

[11] 王玉敏, 丁露. 工业控制系统(ICS)概述和与 IT 系统的比较[J].中国仪器仪表, 2012, (2): 37-43.
WANG Y M, DING L. Industry control system (ICS) overview and comparison with the IT system[J]. China Instrumentation, 2012, (2): 37-43.

[12] 张帅. 工业控制系统安全风险分析[J]. 信息安全与通信保密, 2012(3): 15-19.
ZHANG S. The security risk analysis of the industrial control system [J]. Information Security and Communications Privacy, 2012(3): 15-19.

[13] 王玉敏. 工业控制系统的常见攻击[J].中国仪器仪表, 2012(3): 60-65.
WANG Y M. The general attacks and how to protect the ICS[J]. China Instrumentation, 2012(3): 60-65.

[14] 张风登, 谢力, 应启戛. 噪声环境中采用探询机制的局域网性能分析[J]. 通信学报, 2002, 23(6): 7-13.
ZHANG F D, XIE L, YING Q J. Performance analysis of LAN using polling mechanism in a noisy environment[J]. Journal of China Institute of Communications, 2002, 23(6): 7-13.

[15] LIU C C, STEFANOW A. Cyber–power system security in a smart grid environment[C]//IEEE PES Innovative Smart Grid Technologies. 2012: 1-3.

[16] BARBOSA R, SADRE R, PRAS A. Towards periodicity based anomaly detection in SCADA networks[C]//The 17th International Conference on Emerging Technologies & Factory Automation. 2012: 1-4.

[17] 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]. Academic Journal of Xi’an Jiaotong University, 2012, 46(2): 70-75.

[18] VOLLMER T, ALVES-FOSS J, MANIC M. Autonomous rule creation for intrusion detection[C]//IEEE Symposium on Computational Intelligence in Cyber Security. 2011: 1-8.

[19] MORRIS T, VAUGHN R, DANDASS Y. A retrofit network intrusion detection system for modbus RTU and ASCII industrial control systems[C]//The 45th Hawaii International Conference on System Sci-

ence. 2012: 2338-2345.

[20] HONG J, LIU C C, GOVINDARASU M. Integrated anomaly detection for cyber security of the substations[J]. IEEE Transactions on Smart Grid, 2014, 5(4): 1643-1653.

[21] VOLLMER T, MANIC M. Computationally efficient neural network intrusion security awareness[C]//The 2nd International Symposium on Resilient Control Systems. 2009: 25-30.

[22] LINDA O, VOLLMER T, MANIC M. Neural network based intrusion detection system for critical infrastructures[C]//International Joint Conference on Neural Networks. 2009: 1827-1834.

[23] VOLLMER T, MANIC M. Cyber-physical system security with deceptive virtual hosts for industrial control networks[J]. IEEE Transactions on Industrial Informatics, 2014, 10(2): 1337-1347.

[24] TSANG C H, KWONG S. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction[C]//International Conference on Industrial Technology. 2005: 115-120.

[25] GAO W, MORRIS T, REAVES B, et al. On SCADA control system command and response injection and intrusion detection[C]//The 5th Annual Anti-Phishing Working Group eCrime Researchers Summit. 2010: 1-9.

[26] KWON Y J, KIM H K, LIM Y H, et al. A behavior-based intrusion detection technique for smart grid infrastructure[C]//PowerTech Conference. 2015: 1-6.

[27] HADZIOSMANOVIC D, SIMIONATO L, BOLZONI D, et al. *N*-gram against the machine: on the feasibility of the n-gram network analysis for binary protocols[C]//The 15th International Symposium on Research in Attacks, Intrusions, and Defenses. 2012: 354-373.

[28] BARBOSA R, PRAS A. Intrusion detection in SCADA networks[C]// The 4th International Conference on Autonomous Infrastructure, Management and Security, 2010: 163-166.

[29] CARCANO A, FOVINO I N, MASERA M, et al. State-based network intrusion detection systems for SCADA protocols: a proof of concept[C]//The 4th International Workshop on Critical Information Infrastructures Security. 2010: 138-150.

[30] PARVANIA M, KOUTSANDRIA G, MUTHUKUMARY V, et al. Hybrid control network intrusion detection systems for automated power distribution systems[C]//The 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. 2014: 774-779.

[31] HONG J H, WU S S, STEFANOV A. An intrusion and defense testbed in a cyber-power system environment[C]//IEEE Power and Energy Society General Meeting. 2011: 1-5.

[32] ZHOU C, HUANG S, XIONG N, et al. Design and analysis of multi-model-based anomaly intrusion detection systems in industrial process automation[J]. IEEE Transactions on System, Man and Cybernetics-Systems, 2015, 45(10): 1345-1360.

[33] SHANG W L, LI L, WAN M, et al. Industrial communication intrusion detection algorithm based on improved one-class SVM[C]//2015 World Congress on Industrial Control System Security. 2015: 21-25.

[34] LIN H, SLAGELL A, KALLBARCZYK Z, et al. Semantic security analysis of SCADA networks to detect malicious control commands in power grids[C]//The First ACM Workshop on Smart Energy Grid Security. 2013: 29-34.

[35] HADZIOSMANOVIC D, SOMMER R, ZAMBON E, et al. Through the eye of the PLC: semantic security monitoring for industrial processes[C]//The 30th Annual Computer Security Applications Conference. 2014: 126-135.

[36] MITCHELL R, CHEN I R. Behavior rule based intrusion detection for supporting secure medical cyber physical systems[C]//The 21st International Conference on Computer Communication and Networks. 2012: 1-7.

[37] MITCHELL R, CHEN I R. Specification based intrusion detection for unmanned aircraft systems[C]//The first ACM MobiHoc Workshop on Airborne Networks and Communications. 2012: 31-36.

[38] MITCHELL R, CHEN I R. Behavior rule based intrusion detection systems for safety critical smart grid applications[J]. IEEE Transactions on Smart Grid, 2013, 4(3): 1254-1263.

[39] MITCHELL R, CHEN I R. A survey of intrusion detection techniques for cyber physical systems[J]. ACM Computing Surveys, 2014, 46(4): 1-27.

[40] MITCHELL R, CHEN I R. Behavior rule specification-based intrusion detection for safety critical medical cyber physical system[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(1): 16-30.

[41] OMAN P, PHILIPS M. Intrusion detection and event monitoring in SCADA networks[C]//The 1st Annual IFIP International Conference on Critical Infrastructure Protection. 2008: 161-173.

[42] LINDA O, MANIC M, VOLLMER T, et al. Fuzzy logic based anomaly detection for embedded network security cyber sensor[C]//IEEE Symposium on Computational Intelligence in Cyber Security. 2011: 202-209.

[43] 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.

[44] NARSINGYANI D, KALE O. Optimizing false positive in anomaly based intrusion detection using genetic algorithm[C]//The 3rd International Conference on MOOCs, Innovation and Technology in Education. 2015: 72-77.

[45] DUSSEL P, GEHL C, LASKOV P. Cyber-critical infrastructure protection using real-time payload-based anomaly detection[C]//The 4th International Workshop on Critical Information Infrastructure Security. 2010:85-97.

[46] 王海凤. 工业控制网络的异常检测与防御资源分配研究[D]. 浙江大学, 2014.

WANG H F. On anomaly detection and defense resource allocation of industrial control networks[D]. Zhejiang University, 2014.

[47] AMBUSAIDI M, HE X J, NANDA P. Building an intrusion detection

system using a filter-based feature selection algorithm[J]. IEEE Transactions on Computers, 2016(99): 1.

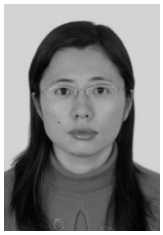
[48] PREARATNEU K, SAMARABANDU J, SIDHU T S. An intrusion detection system for IEC61850 automated substations[J]. IEEE Transactions on Power Delivery, 2010, 25(4): 2376-2383.

[49] SAMDARSHI R, SINHA N, TRIPATHI P. A triple layer intrusion detection system for SCADA security of electric utility[C]//India Conference. 2015: 1-5.

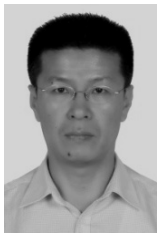
[50] SINGH P, GARG S, KUMAR V. A testbed for SCADA cyber security and intrusion detection[C]//International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications. 2015: 1-6.

[51] SRIDHAR S, GOVINDARASU M. Model-based attack detection and mitigation for automatic generation control[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 580-591.

作者简介：



**赖英旭**（1973-），女，辽宁抚顺人，北京工业大学教授，主要研究方向为工业控制网络安全和软件定义网络安全。



**刘增辉**（1963-），男，北京人，北京电子科技职业学院教授，主要研究方向为机电一体化技术和工业控制网络安全。

**蔡晓田**（1994-），女，山西运城人，北京工业大学硕士生，主要研究方向为工控网络安全和入侵检测。

**杨凯翔**（1992-），男，甘肃兰州人，北京工业大学硕士生，主要研究方向为工控网络安全、入侵检测和漏洞挖掘。