doi:10.11959/j.issn.1000-436x.2017277

工业以太网协议脆弱性与安全防护技术综述

冯涛[1]，鲁晔[2,3,4]，方君丽[1]

（1. 兰州理工大学计算机与通信学院，甘肃 兰州 730050；2. 兰州理工大学电气工程与信息工程学院，甘肃 兰州 730050；
3. 甘肃省工业工程先进控制重点实验室，甘肃 兰州 730050；4. 兰州理工大学电气与控制工程国家级实验教学示范中心，甘肃 兰州 730050）

摘 要：为解决工业控制系统信息安全问题，对工业以太网协议安全进行深入研究，报告了协议安全防护的研究现状。首先论述了工业控制系统和工业以太网协议的体系结构，分析了 5 种主要协议的脆弱性。其次从外部主动防御技术、内部被动防御技术和协议安全改进三个方面，提出完善的工业以太网协议安全防护模型，并对主要防护技术进行论述，最后指出未来工业以太网协议信息安全改进的发展方向和研究方法。

关键词：工业控制系统；工业以太网协议；信息安全；防御技术

中图分类号：TP309 **文献标识码：**A

Research on vulnerability and security technology of industrial Ethernet protocol

FENG Tao[1], LU Ye[2,3,4], FANG Jun-li[1]

(1. College of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China;
2. College of Electrical and Information Engineering, Lanzhou University of Technology, Lanzhou 730050, China;
3. Key Laboratory of Gansu Advanced Control for Industrial Processes, Lanzhou University of Technology, Lanzhou 730050, China;
4. National Demonstration Center for Experimental Electrical and Control Engineering Education, Lanzhou University of Technology, Lanzhou 730050, China.)

Abstract: To solve the information security of industrial control system, the safety of industrial Ethernet protocol was studied deeply, the research status of protocol security protection was reported and the vulnerability of the five-major protocol was analyzed. Firstly, the architecture of industrial control system and industrial Ethernet protocol was discussed. Secondly, from the three aspects of external active defense technology, internal passive defense technology and protocol security improvement, a perfect industrial Ethernet protocol security protection model was put forward, and the main protection technology was discussed. Finally, the future development direction and research ideas of information security improvement of industrial Ethernet protocol were pointed out.

Key words: industrial control system, industrial Ethernet protocol, information security, defense technology

1 引言

伴随中国制造 2025 提出[1]，针对工业数据通信与控制网络的相关研究逐步成为研究热点。越来越多的通用协议被应用在工业控制系统（ICS）中，在拓展网络化控制的过程中也引入了信息安全威胁[2]。据国家信息安全漏洞共享平台针对工控系统行业漏洞统计，截至 2017 年 5 月共发现超过 1 031 条信息安全漏洞，涉及国内外大量工控设备厂商，其中高危漏洞更是占到 48.59%。另据权威工业安全事件信息数据库（RISI）统计截至 2017 年 5 月，全球共发生 242 起针对工业关键基础设施的网络攻击事件，每次攻击均造成巨大损失。

上述安全事件的主要攻击策略大都利用了工业以太网协议漏洞向控制系统发送恶意控制命令。由于工业控制系统设计之初是封闭隔离的，所以控

收稿日期：2017-09-03
基金项目：国家自然科学基金资助项目（No.61462060, No.61762060）；甘肃省科技计划青年科技基金计划（No.1610RJYA008）
Foundation Items: The National Natural Science Foundation of China (No.61462060, No.61762060), Gansu Science and Technology Plan Youth Science and Technology Fund Project (No.1610RJYA008)

制协议并没有采用加密认证等信息安全手段（如1979 年发布的 Modus 协议）。因此攻击者只需获得总线的访问权限，就能够对总线数据进行监听、篡改以达成对控制系统的破坏。随着控制系统网络化的发展，此类协议面临越来越多的安全威胁[3]。以2010 年震惊世界的 Stuxnet 蠕虫病毒为例，其首先利用 4 个零日漏洞感染装有西门子公司 WinCC 组态软件和装有 PCS7 程序的工控主机，然后利用 PROFIBUS 协议缺乏认证和加密，攻击者监听总线数据，寻找工作在 800~1 200 Hz 范围内的变频器并对其强制降频到 2 Hz，此次事件共造成伊朗核电站20%离心机损坏，约 3 万台终端被感染[4]。

本文首先建立工业控制系统及协议的体系结构，并对 5 个广泛应用的工业以太网协议进行脆弱性分析，然后从外部主动防御技术、内部被动防御技术和协议安全改进 3 个方面，提出完善的工业以太网协议安全防护模型，并对主要防护技术进行论述，最后指出未来工业以太网协议信息安全改进的发展方向和研究方法。

2 ICS 体系重构

2.1 工业控制系统的体系结构

工业控制系统是多种生产控制系统地统称。根据实现功能的不同，工业控制系统可划分为如图 1

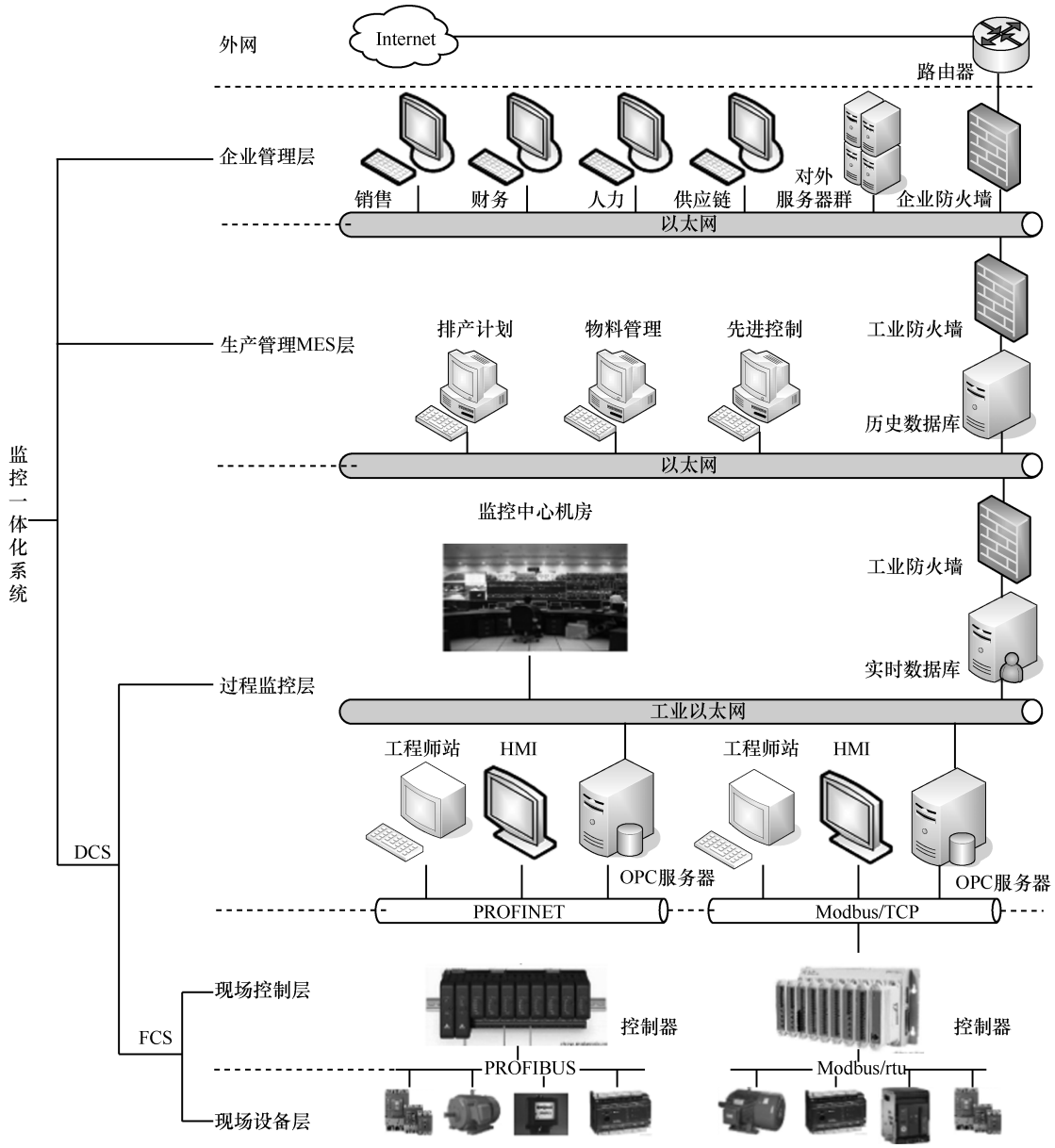

图 1 工业控制系统体系结构

所示的 5 个层次，即现场设备层（第 1 层）、现场控制层（第 2 层）、过程监控层（第 3 层）、生产管理 MES 层（第 4 层）、企业管理层（第 5 层）。现场设备层主要传输 I/O 信号，包括检测仪表、执行器等其他现场设备。现场控制层进行数据采集转换，包含 PLC 和 HMI 等设备。过程监控层执行过程操作、报表打印，信息处理等功能，包括工业 PC 机、HMI 等。生产管理层主要承担制造数据管理、物料管控、生产调度，通常采用 MES 系统。企业管理层主要实现市场订货销售统计等功能，包括企业 ERP 系统等。

随着通信技术、自动控制技术的进步及企业信息化的发展趋势，IT 技术开始大量在自动控制领域应用，推动了工业过程控制信息化发展[5]。工业控制系统历经了模拟仪表控制系统、直接数字控制系统、集散控制系统及现场总线控制系统 4 个发展阶段，从封闭向开放化、分布化、智能化发展[6]。控制网络逐渐由不可路由的现场总线发展到可路由的工业以太网，形成了以工业以太网为代表的新一代扁平化网络控制系统。如图 1 所示，当第一层与第二、三层合并时即构成了集散控制系统(DCS)。当第一层与第二层融合时即构成现场总线控制系统(FCS)，为不可路由网络。第三层和第四层由以太网组成，为可路由网络，主要完成生产经营管理即企业 ERP 和 MES 管理系统。当 DCS 或 FCS 系统与 ERP 和 MES 系统无缝集成时就形成了管控一体化系统。

2.2　工业以太网协议的体系结构

由于各大工控厂商的利益，现场总线未能形成统一的国际标准，不能完全实现真正意义上的开放互联。大量工业企业都希望将以太网应用在工业控制系统中，取代目前种类繁多的现场总线，使控制系统与管理系统无缝衔接，形成垂直方向的系统集成，同时降低不同厂商设备在水平面上的集成成本。因此工业以太网协议逐步成为了业界的研究热点，出现了 Modbus TCP、DNP3、PROFINET、Ethernet/IP、OPC、EPA 等多种工业以太网协议。

工业以太网在部分继承以太网原有核心技术的基础上，针对实时性、安全性、时间同步性、非确定性进行相应改进，以满足工业需求。图 2 给出了 3 种主要工业以太网协议的结构模型并与标准以太网协议模型相对照。

Modbus/TCP 协议将 Modbus 帧嵌入 TCP 帧中，是 OSI 通信参考模型第 7 层上的应用层报文传输协议，使用 502 端口，采用请求应答模式。能够兼容标准以太网设备，拥有超过 300 个 Modbus 兼容设备厂商，应用最为广泛，已经成为工业以太网标准的既定事实标准。

Ethernet/IP 协议在应用层采用 CIP 协议，控制部分实现实时 I/O 通信，信息部分采用非实时报文交换。CIP 协议也可以作为 ControlNet（链

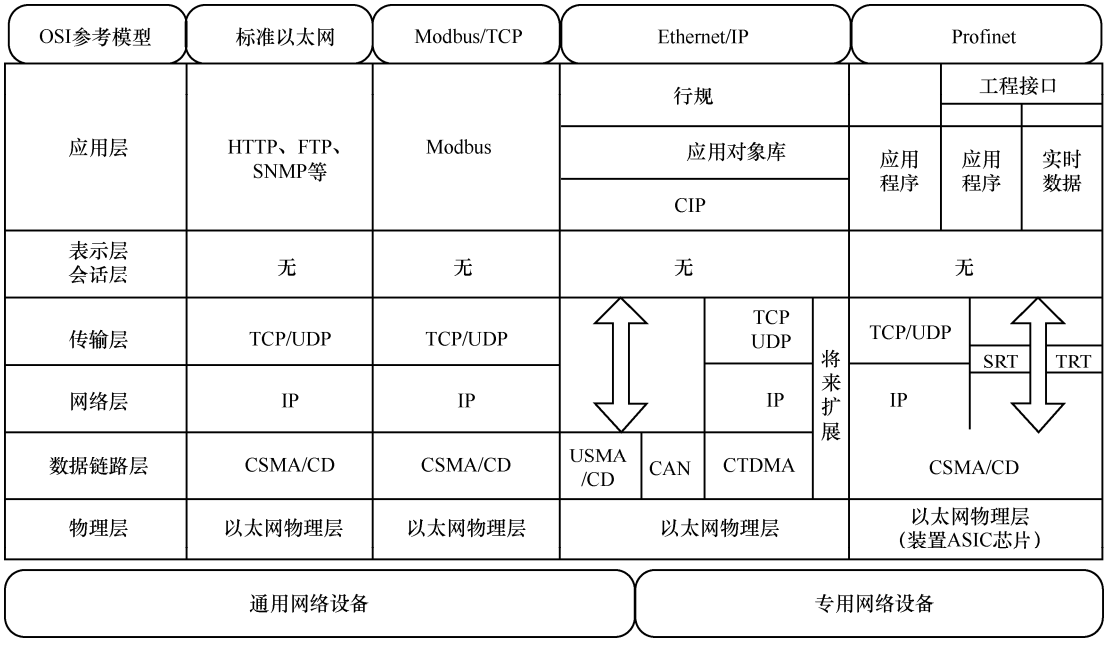

图 2　3 种主要工业以太网协议的体系结构

路层采用 CAN 协议）网络和 DeviceNet(链路层采用 CTDMA 协议)网络的应用层，3 种网络分享相同的应用对象库，可以在 3 类网络中实现即插即用。

Profinet 在应用层使用.COM、OPC、XML 等技术。网络拓扑形式有星型、总线型、环形等。传输非实时数据时采用标以太网交换机即可，但是在传输实时数据时需要使用装备 ASIC 芯片的交换机设备，该芯片对实时应用提供预定义时间槽，来传输实时数据。实时通道分为软实时通道 SRT 和等时同步通道 IRT。IRT 通道用以解决比 SRT 通道实时性要求更高的运动控制数据的传输。

3 工业以太网协议脆弱性分析

目前，对于工业控制系统的安全防护，主要依据 IEC62443 标准中提出的纵深防御安全策略[7]。然而该种策略侧重于系统级的防御，无法抵御工业控制协议自身脆弱性带来的安全问题。ICS 系统所使用的协议并非传统 IT 系统的网络协议，而是 Modbus/Tcp、DNP3、Profinet、Ethernet/IP、HSE、EPA 等工业以太网协议及若干现场总线型协议。两者之间在信息安全需求上存在着较大差异，所面临的威胁也不尽相同[8]。ICS 协议面临的主要安全风险有：大量协议数据明文传输，缺乏认证和加密，存在被窃听、伪装、篡改、抵赖和重放的攻击风险。以下本文将针对目前应用最为广泛的 5 种工业以太网协议进行脆弱性分析。

3.1 Modbus 协议脆弱性分析

Modbus 协议目前衍生出 Modbus/RTU、Modbus/ASC II、Modbus +和 Modbus/TCP 4 个变种。图 3 所示为一典型 Modbus 协议通信结构示意图。在过程监控层和现场控制层使用 Modbus/TCP，而在各个 PLC 控制器与现场设备间综合使用多种串行 Modbus 协议。

文献[9]指出 Modbus/TCP 协议缺乏加密机制，攻击者可以识别通信设备，篡改数据分组，使服务器宕机。文献[10]指出 Modbus/TCP 协议缺乏安全属性，容易受到欺骗、洪泛、重放等攻击威胁。文献[11]在 Modbus/TCP 通信系统中注入恶意流量，导致 Modbus/TCP 通信延迟。文献[12]描述了针对 Modbus 串行协议和 Modbus /TCP 的主要攻击，并给出了相应的攻击分类。根据上述文献对各类攻击进行总结，表 1 归纳出 Modbus 协议主要存在以下安全漏洞。

表 1 Modbus/TCP 协议主要漏洞

漏洞	文献
加密	文献[9,10]
认证	文献[10]
校验	文献[12]
可编程	文献[11,12]
溢出	文献[11,12]
广播风暴	文献[10,11]

3.2 Ethernet/IP 协议脆弱性分析

Ethernet/IP 是实时以太网协议，其应用层包括 CIP 协议，容易受以太网漏洞影响。文献[13]利用 Ethernet/IP 协议缺乏时间戳和加密操作，成功对 Ethernet/IP 协议发起拒绝服务攻击。文献[14]通过 SNORT 入侵检测软件，检测到 Ethernet/IP 存在数据篡改和中间人攻击，此外，由于 UDP 之上的

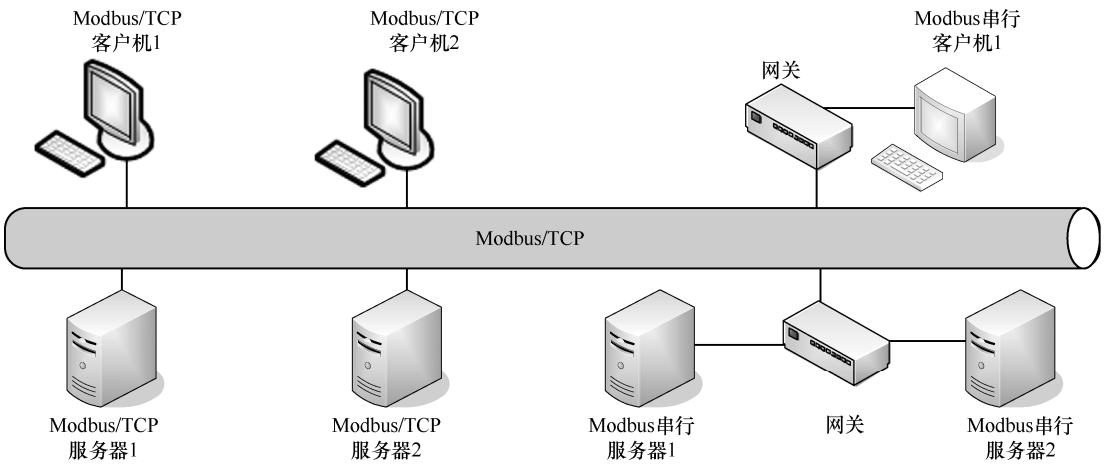

图 3 典型 Modbus 协议通信结构示意

Ethernet/IP 是无连接的，因此没有内在的网络层机制来保证可靠性、顺序性或进行数据完整性检查。最新的 CIP 协议安全版本 CIP safety[15]，通过加入时间戳机制来遏制重放攻击，增加应用层校验遏制数据篡改，但数据明文传输不加密、缺乏认证，同样存在伪造数据攻击、中间人攻击等安全威胁，Ethernet/IP 协议的主要漏洞如表 2 所示。

表 2　Ethernet/IP 协议主要漏洞

漏洞	文献
加密	文献[13, 15]
认证	文献[14, 15]
重放	文献[15]
拒绝服务	文献[11, 15]

3.3　Profinet 协议脆弱性分析

Profinet 主从协议通过共享令牌支持多个主节点，是 Profibus 协议在以太网上的扩展。文献[16]使用 Peach 模糊测试器，发送伪造的数据分组，使终端设备执行错误指令，指出 Profinet 协议存在大量安全威胁。文献[17]证明了对 Profinetio 节点进行攻击和获得控制是可能的，对共享和分组交换网络中的攻击的分析表明，攻击者可以控制进程数据，从而控制连接到输入/输出模块的机器状态。Profinet 协议主要存在缺乏授权、加密、认证三类安全漏洞，此外 Profinet 是实时以太网协议，同样容易受以太网协议漏洞影响。

3.4　OPC 协议脆弱性分析

OPC(OLE for process control)协议实际属于一种中间件技术，采用 C/S 架构将现场信号按照统一标准与组态软件无缝连接。客户端程序采用统一的方式对各个硬件设备进行通信，无须重复开发驱动。

最新的 OPC 规范为 OPC-UA[18]，该规范提出了标准安全模型，底层通信技术提供加密功能和标记技术以确保消息的完整性和秘密性。文献[19]研究了 OPC-UA 的安全性。通过使用加密协议验证工具，发现了一些针对协议机密性和身份验证属性的攻击。文献[20]从 OPC-UA 应用的网络环境安全与通信协议安全角度出发，研究了 OPC 联合安全问题，指出 OPC 服务器和客户端存在拒绝服务攻击和中间人攻击。文献[21]在深入分析 Windows 系统、.COM、MTS/COM+安全机制的基础上，指出 OPC 基于 Windows 系统，主机安全问题也会影响 OPC 安全，此外由于使用 DCOM 与 RPC 技术，OPC 同样受到组件漏洞的影响。因此 OPC 与其他工业以太网协议安全性存在较大差异。OPC 协议主要存在以下安全漏洞，如表 3 所示。

表 3　OPC 协议主要漏洞

漏洞	文献
加密	文献[10, 19]
认证	文献[19]
完整性	文献[10, 19]
DOS	文献[20]
主机	文献[21]

3.5　DNP3 协议脆弱性分析

DNP3 是由美国 IEEE 电力工程协会(PES)制定的美国国家工业通信标准[22]。DNP3 目前存在两种安全版本 DNP3-Sec[23]和 DNP3-SAv5[24]。前者侧重链路层安全加固，后者侧重应用层安全加固。尽管两种安全协议中使用了认证、加密、授权、完整性校验等安全机制，它们仍然面临一些安全威胁。文献[25]使用 SCAPY 向 DNP3 通信链路发送大量伪造的数据分组，验证了 DNP3 协议存在数据篡改、重放和欺骗等安全漏洞。文献[26]在包含 DNP3 协议的模拟环境中使用各种攻击场景进行渗透测试。漏洞分析和渗透测试表明存在中间人(MITM)攻击。文献[27]通过发送大量错误信息，引起协议栈缓冲区溢出，最终导致服务奔溃。通过上述文献可以归纳 DNP3 协议主要存在以下攻击向量：中间人、重放、窃听、数据篡改、拒绝服务、缓冲区溢出。

上述 5 种工业以太网协议的安全性能对比如表 4 所示。由表 4 可知，首先所有协议都满足可用性和可靠性的设计要求，这也进一步说明，工业系统信息安全相较传统 IT 系统信息安全更加注重可用性和可靠性。其次对于有安全性版本的协议，安全改进主要侧重于完整性。只有 DNP3 协议针对信息安全的 5 项基本属性都做出了安全改进，但是一些研究[25~27]表明 DNP3 协议的安全版本仍然存在漏洞，此外 OPC 协议安全性高度依赖主机系统安全。表 4 中，“○”表示满足，“×”表示不满足。

4　工业以太网协议安全防护技术

现代工业控制系统大量地采用工业以太网协

表 4 **5 种工业以太网协议的安全性能对比**

协议	可用性	可靠性	完整性	保密性	不可抵赖性	安全版本	系统关联度
Modbus/TCP	○	○	×	×	×	×	×
Ethernet/IP	○	○	○	×	×	○	×
Profinet	○	○	×	×	×	×	×
OPC	○	○	○	×	×	○	○
DNP3	○	○	○	○	○	○	×

议与互联网对接。工业以太网继承了传统以太网的脆弱性，同时又具有上文讨论的特有安全漏洞，因此仅仅借助传统的以太网安全策略，如采用 VPN 技术将控制网划分为逻辑独立的非实时子网和实时子网；采用 QoS 技术保证实时数据的质量；采用证书分级登录验证功能等，已经无法满足现代工业控制系统的安全需求。

本文针对工业以太网协议的脆弱性，从外部主动防御技术、内部被动防御技术和协议安全改进 3 个方面，提出完善的工业以太网协议安全防护模型，如图 4 所示，该安全防护模型具备 3 个层次功能：1）阻挡外部网络入侵；2）检测内部协议数据异常；3）加固协议自身安全。下面将依据该防护模型，总结工业以太网协议防护技术的研究进展。

4.1 基于协议的外部主动防护技术

主动防护技术特指部署在系统外部的，主动探测协议脆弱性的安全技术。包括纵深防御技术、IDS 与 IPS、协议蜜罐、协议漏洞管理等。

4.1.1 协议纵深防御技术

构建工业控制系统“纵深防御”体系[7]，是目前学术界与工业界普遍公认的保证工业控制系统物理安全和信息安全最有效的方法。建立协议的纵深防御体系，需要列出使用该协议的所有设备的完整清单，并将设备资产划分为若干安全域：外部区域、内网区域、非军事区、生产区域（含各控制单元）、安全隔离区等。文献[28]从工业通信协议深度解析的角度出发，指出构建工控 SCADA 系统的纵深防御体系主要分为 2 个核心环节，分别是区域划分和安全策略设计，并构建了基于 Modbus/TCP 协议的纵深安全防御模型。文献[29]在分析协议网络分区变化基础上，建立基于协议行为感知的动态分区技术。基于协议的纵深防御体系能够针对特定协议进行安全防护，对于控制系统整体或功能域内的单一协议数据安全防御会事半功倍。

基于协议的纵深防御技术涵盖了协议防火墙、网络隔离、端口过滤、白名单、数据二极管等安全技术。文献[30]提出一种跨区域的单向传输数据二极管技术,有效保证协议数据安全。文献[4]总结了当前国内外领先的工业协议防火墙和网络隔离产品包括：三零卫士“30Trust FWS”，海天炜业“Guard”，力控华康“HC-ISG”，加拿大 Tofino 防火墙。文献[31]

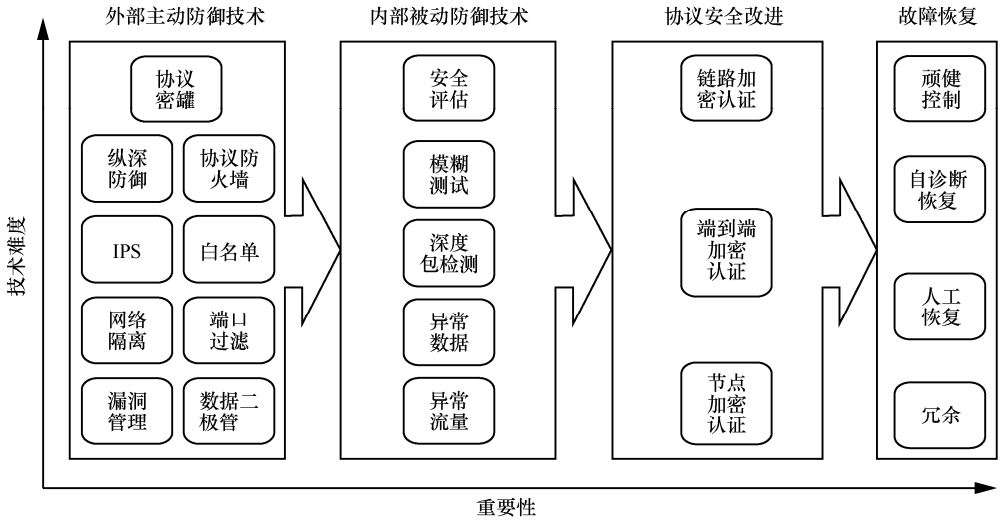

图 4 工业以太网协议安全防护模型

建议工控企业使用白名单机制，通过允许特定协议的特定数据和指令，降低安全风险。

4.1.2 协议 IDS 与 IPS

入侵检测系统 IDS 与入侵防御系统 IPS 主要采用模式匹配的方法，对符合特征的数据分组进行操作。IDS 并联在系统中，旁路监听系统流量，IPS 串联在系统中，数据需要经由 IPS 才能到达接收端，能够拦截违法消息。文献[32]建立了基于 Modbus 协议和 DNP3 协议恶意数据分组的入侵检测系统，能够抵御针对 2 种协议的数据伪造攻击。文献[33]提出了一种用于 Snort 的 Modbus/TCP 协议入侵检测方法，能够检测协议异常数据。文献[34]综述了工业控制系统的入侵检测方法，并对攻击方法、变种攻击检测、隐蔽过程攻击检测技术的性能进行分析对比。需要注意入侵检测技术仅可以检测异常，不能够帮助工控系统恢复正常。

4.1.3 协议蜜罐

蜜罐通过模拟各种工业以太网协议在公网上的运行，为真实系统提供防护参考。ICS Security Work Space 发布仿真西门子 S7-300PLC 与工控系统最常见的 Modbus 协议运行在公网的情况，记录扫描攻击该系统过程以及相应 IP，用以研究工控系统的防御[4]。文献[35]采用蜜罐技术研究针对工业控制系统协议的攻击过程。文献[36]结合 Honeyd 蜜罐和 Matlab/Simulink，模拟了田纳西—伊斯曼化工过程控制系统的通信过程，并使用 Python 脚本对协议发起攻击测试。文献[37]基于 Conpot 蜜罐提出适用于各种协议的远程数据入侵检测方法。

4.1.4 协议漏洞管理

科学的检测工业以太网协议漏洞，并及时更新补丁是协议防护技术的重要组成部分。CNVD、CVE、ICS-CERT、中国国家信息安全漏洞共享平台等权威机构会实时发布最新漏洞，包括针对协议的攻击漏洞。工控企业可以配置工业协议漏洞扫描设备来检测协议漏洞。国内外成熟的漏洞扫描器有绿盟科技的 ICSScan、启明星辰的天镜工控漏洞挖掘系统、Scada Strange Love 黑客开发的 PLCScan。文献[38]开发出基于模糊测试的工控系统漏洞挖掘机，成功找出零日漏洞；文献[39]研究一种层次化漏洞扫描方法，并对西门子 PLC 系统进行扫描，并验证了该方法的有效性。文献[40]基于 Peach 以 Modbus/TCP 为例，进行模糊安全测试，实验结果表明研究的安全分析方法可以高效挖掘协议漏洞。

基于协议的外部主动防护技术性能比较如表 5 所示，其中蜜罐技术与漏洞管理技术主要从威胁探测的角度和漏洞挖掘的角度对攻击溯源和漏洞防护，并不直接保护工业系统，而纵深防御和入侵检测技术虽然能够直接保护系统协议数据，但是存在误报率高和维护难度大的缺点。

4.2 基于协议的内部被动防护技术

被动防护技术指当攻击向量已经进入系统内部时，需要采取的防御技术，包括深度分组检测、异常流量、异常数据、模糊测试及协议安全评估等技术。

4.2.1 深度分组检测

深度分组检测技术广泛应用于流量管理、协议安全分析中，也是主要的异常流量及异常数据

表 5　外部主动防护技术性能比较

文献	支持协议	防御策略	防御技术	防御效果	局限性
文献[28]	Modbus TCP	纵深防御	数据匹配	中	难以防范具备专业知识的攻击
文献[29]	ICS	纵深防御	行为感知	中	仅针对单一协议数据
文献[30]	ICS	纵深防御	数据二极管	中	数据单向传输
文献[31]	ICS	纵深防御	白名单	中	需制定大量规则，维护难度大，易误操作
文献[32]	DNP3/ Modbus	入侵检测	数据匹配	中	难以防范具备专业知识的攻击
文献[33]	Modbus TCP	入侵检测	数据匹配	中	需制定大量规则，维护难度大，易误操作
文献[35]	ICS	蜜罐	Conpot	低	
文献[36]	ICS	蜜罐	Honeyd	低	无法实际防御，仅对攻击行为进行收集
文献[37]	ICS	蜜罐	Conpot	低	
文献[38]	Modbus TCP	漏洞挖掘	Fuzzing	低	
文献[39]	Modbus TCP	漏洞挖掘	Fuzzing	低	不能直接防御攻击、存在误报
文献[40]	Modbus TCP	漏洞挖掘	Fuzzing	低	

检测方法。深度分组检测技术可分为 3 类：基于特征字的识别技术；应用层网关识别技术；行为模式识别技术。

4.2.2 安全评估

安全评估是 ICS 系统的网络安全防御中关键的组成部分，对于 ICS 系统来讲，安全评估是通过收集和分析 ICS 系统的协议行为，以检测是否存在针对 ICS 系统的可疑的攻击。安全评估又包含了面向不同具体对象的安全评估方法，如图 5 所示。

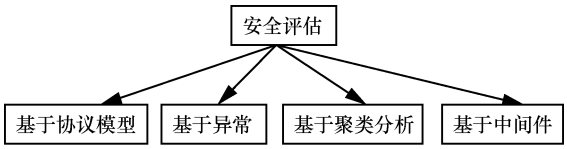

图 5 安全评估方法分类

文献[41]提出了一种基于协议模型的面向现场总线协议的安全评估方法，根据现场总线规范，建立现场总线协议行为模型，从而检测不符合该行为模型的潜在攻击。但是它的缺陷在于，当行为模型不够精确的时候，容易导致较高的误报率。文献[42]通过语言模型对系统关键状态进行建模，能够检测针对 DNP3 协议发起的复杂攻击。文献[43]通过对比 ICS 协议在正常情况下和异常情况下的网络参数，建立状态矩阵，当状态矩阵关键参数偏离正常状态达到设定阀值时，触发报警，能够检测 DOS、泛洪等恶意攻击，但是它的缺陷在于漏报率和误报率取决于阀值的设定。文献[44]基于蚁群聚类算法和无监督特征提取的方法，设计出一种针对工业协议安全评估的多代理分布式检测机制。文献[45]提出了一种适用于工业嵌入式系统中间件的安全评估方案,将协议安全评估感知器和探测器都集成到中间件层，适用于对 OPC 类协议的安全评估。但是，该方法可能会因为不适当的策略配置，导致系统的不确定行为。表 6 对上述文献所采用的安全评估方法进行对比分析。

4.3 协议的安全改进

目前，针对协议安全性的改进主要基于加密技术实现，一种是针对协议自身的改进，优点是可以兼容主流的工业设备。另一种是借助其他安全设备或安全协议实现协议传输安全。主要有 3 种方法：链路加密、节点加密和端到端加密。如图 6 所示。

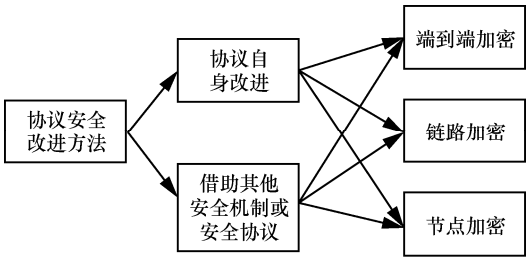

图 6 协议安全改进方法分类

4.3.1 链路加密

链路加密方式，数据在源节点处进行加密处理，到达目的节点后进行解密，分组在链路上以密文传输,能够隐藏传输源点与终点,防止攻击者对通信地址进行分析。但是链路加密的缺陷是会导致链路负荷增加。文献[46]提出一种低开销的工业无线网安全机制，通过实施基于散列链的 μTESLA 安全广播方法,建立了轻量化的安全体系结构和层次化的密钥体系。文献[47]针对不同通信服务和性能需求，提出一种 MAC-SEC 的安全机制，实现了 hop-by-hop 的安全通信。文献[48]提出基于 ECC 加密体制的认证授权机制，实现用户与变电站智能设备的双向认证和访问控制

4.3.2 节点加密

节点加密采用一个与节点相连的密码设备，密文在该设备中被解密并用另一个不同的密钥重新加密。文献[49]提出了 BITW(bump in the wire)解决方案—YASIR(yet another security retrofit)，将随机误差检测转化为数据认证和新鲜性校验并利用安全等级为 80 bit 的 HMAC 方法，防止更高威胁等级的选择—明文—密文攻击。文献[50]提出了基于计

表 6 协议安全评估方法性能比较

文献	支持协议	评估技术	评估效果	局限性
文献[41]	Modbus TCP	攻击图	中	行为摸型不够精确时，导致较高的误报率
文献[42]	DNP3	HLPSL 语言	中	仅模拟关键状态
文献[30]	ICS	状态矩阵	中	漏报率和误报率取决于阈值的设定
文献[31]	ICS	蚁群聚类算法	中	聚类尺度标准的划定影响检测精度
文献[45]	Modbus TCP	中间件	低	不适当的策略配置，导致系统的不确定行为

数器和消息校验的 Predictive YASIR 机制，确保传统工业控制网络的安全操作，利用广义消息模式减少消息认证延迟。文献[51]提出一种改进的 BITW 加密方案。通过在每个节点附加加密装置，实现通信安全。但是节点加密要求分组和路由信息以明文形式传输，以便中间节点能得到如何处理消息的信息，因此这种方法对于防止攻击者分析通信业务是脆弱的。

4.3.3 端到端加密

端到端加密方式，传输过程中消息始终以密文形式存在，不会导致信息泄露。文献[52]提出了一种快速、轻量级的基于 NTRU 公钥加密算法，实现了 SCADA 系统端到端的安全传输。文献[53]提出了 2 种方法保护 SCADA 通信安全：1) 利用 SSL、TLS 及 IPsec 等外部加密协议保护 SCADA 协议，但是这种方法只能保证部分链路的安全；2) 利用认证、加密等操作提供端到端的安全，保证信道安全。

端到端加密与节点加密、链路加密相比，实现和维护更加容易。但是该方法需要在端节点添加新的加解密设备来实现安全功能，降低了实时性和可靠性，增加了硬件成本。详细的性能比较见表 7。

5 结束语

伴随智慧城市、智能制造的蓬勃发展，及工业大数据、云平台的建设推进，工业控制系统的信息安全问题还将进一步扩大升级。特别是涉及国家关键基础设施领域的能源系统。文献[54~61]总结智能电网信息安全面临的威胁包括：设备安全、网络安全和数据安全，并指出智能电网的发、输、配、用电数据窃取难以发现，长期发展将不利于电网健康运行。文献[62]对智能电网面临的信息威胁进一步分类评估,包括网络可用性、数据完整性和隐私信息窃取 3 种。文献[63~68]利用同态加密、差分隐私等技术保护用户电表数据的隐私性和完整性。上述研究表明在工业领域，信息安全正在变的与物理安全、功能安全同等重要。

1) 未来基于协议的外部主动防御和内部被动防御技术仍然是工业控制系统信息安全保障的主要手段。工业以太网协议的自身安全改进，将是今后工业网络信息安全的根本保证。

2) 在发展方向上，基于端到端的轻量高效的加密认证方案，将是协议安全性改进的主要发展方向，另外工业协议设计和改进后的安全性、可靠性验证理论也是一个发展方向。最后基于工控协议的大数据分析也是未来工控安全研究的必然趋势。

3) 在研究方法上，可信计算已经取得了一定的研究进展，大量基于可信计算的工业以太网协议改进方案[69~71]值得研究人员借鉴。利用工控设备指纹[8, 35]改进系统的安全性，也是一类有效的研究思路。此外区块链技术[72]是目前的研究热点，通过将物联网设备信息交换类比于虚拟网络交易，利用智能合约模拟各类工业以太网协议，充分利用区块链的先天安全优势，确保工业控制系统安全将是有待尝试的新研究方法。

参考文献：

[1] 袁胜. 中国制造 2025, 工控安全不容忽视——工业控制系统被谁“反控”[J]. 中国信息安全, 2016(4):44-47.
YUAN S. Made in China 2025, industrial safety can not be ignored - industrial control system who "anti-control" [J]. China Information Security, 2016(4):44-47.

[2] 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.

表 7　　协议安全改进方法性能比较

文献	支持协议	改进策略	改进技术	改进效率	局限性
文献[46]	WLAN	链路加密	Hash-Chain	低	
文献[47]	ICS	链路加密	Mac	低	链路负荷增加，实时性降低
文献[30]	ICS	链路加密	ECC	低	
文献[31]	Modbus TCP	节点加密	BITW	中	
文献[32]	ICS	节点加密	YASIR	中	每一个节点都需要绑定加解密设备，成本高，实时性低
文献[33]	Modbus TCP	节点加密	BITW	中	
文献[52]	ICS	端到端加密	NTRU	高	端节点需要绑定加解密设备，成本高，实时性低
文献[53]	ICS	端到端加密	SSL、TLS、IPsec	高	

LUO J Z, YANG M, LIN Z, et al. Cyberspace security system and key technologies [J]. Scientia Sinica Information. 2016, 46(8):939.

[3] 屈婉莹, 魏为民, 朱苏榕. 工业控制系统通信协议安全研究[C]//全国智能电网用户端能源管理学术年会. 2015.
QU W Y, WEI W M, ZHU S R. Research on communication protocol security of industrial control system[C]//Clients nationwide smart grid energy management Annual Conference.2015.

[4] 陶耀东, 李宁, 曾广圣. 工业控制系统安全综述[J]. 计算机工程与应用, 2016, 52(13): 8-18.
TAO Y D, LI N, ZENG G S. Review of industrial control systems security. Computer Engineering and Applications[J]. Computer Engineering and Applications, 2016, 52(13):8-18.

[5] 柴天佑. 工业过程控制系统研究现状与发展方向[J]. 中国科学:信息科学, 2016, 46(8):1003.
CHAI T Y. Research status and development direction of industrial process control system[J]. Scientia Sinica Information, 2016, 46(8): 1003.

[6] 夏春明, 刘涛, 王华忠, 等. 工业控制系统信息安全现状及发展趋势[J]. 信息安全与技术, 2013, 4(2):13-18.
XIA C M, LIU T, WANG Z H, et al. Industrial control system security analysis[J]. Information Security and Technology.2013, 4(2):13-18.

[7] PIGGIN R S H. Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security[C]// Control and Automation 2013: Uniting Problems and Solutions, IET, 2013:1-6.

[8] 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(10):1396-1408.
PENG Y, JIANG C Q, XIE F, et al. Industrial control system cyber security research[J]. Tsinghua Univ (Sci&Tech), 2012(10):1396-1408.

[9] SHAHZAD A, LEE M, LEE Y K, et al. Real time MODBUS transmissions and cryptography security designs and enhancements of protocol sensitive information[J]. Symmetry, 2015, 7(3):1176-1210.

[10] NARDONE R, RODRÍGUEZ R J, MARRONE S. Formal security assessment of Modbus protocol[C]//Internet Technology and Secured Transactions. 2017.

[11] KOBAYASHI T H, JR A B B, MEDEIROS J P S, et al. Analysis of malicious Traffic in Modbus/TCP Communications[C]//International Workshop on Critical Information Infrastructures Security. Springer Berlin Heidelberg, 2008:200-210.

[12] HUITSING P, CHANDIA R, PAPA M, et al. Attack taxonomies for the Modbus protocols[J]. International Journal of Critical Infrastructure Protection, 2008, 1(1):37-44.

[13] GRANDGENETT R, GANDHI R, MAHDNEY W. Exploitation of Allen Bradley's implementation of Ethernet/IP for denial of service against industrial control systems[C]//9th International Conference on Cyber Warfare and Security 2014:58-65.

[14] LAUGHTER S A, WILLIAMS R D. An Ethernet/IP security review with intrusion detection applications[J]. Science, 2006, 105(2731):475-6.

[15] 孙溪. CIP Safety 网络协议通信层协议关键技术的分析[J]. 仪器仪表标准化与计量, 2014(4):28-30.
SUN X, Analysis of the key technology for communication layer protocol in CIP safety and Metrology, 2014(4): 28-30.

[16] ZHANG D, WANG J, ZHANG H. Peach improvement on PROFINET-DCP for industrial control system vulnerability detection[C]// International Conference on Electrical, Computer Engineering and Electronics. 2015.

[17] ÅKERBERG J, BJÖRKMAN M. Exploring security in PROFINET IO[C]//Computer Software and Applications Conference, 2009. COMPSAC '09. IEEE International. 2009:406-412.

[18] LEHNHOFF S, ROHJANS S, USLAR M, et al. OPC unified architecture: a service-oriented architecture for smart grids[C]// International Workshop on Software Engineering for the Smart Grid. 2012: 1-7.

[19] PUYS M, POTET M L, LAFOURCADE P. Formal analysis of security properties on the OPC-UA SCADA protocol[C]//International Conference on Computer Safety, Reliability, and Security. Springer International Publishing, 2016:67-75.

[20] HUANG R, FENG L, PAN D. Research on OPC UA security[C]// Industrial Electronics and Applications. 2010:1439-1444.

[21] QIAO J X. Research on OPC security mechanism based on MTS/COM+[J]. Computer Technology & Development, 2007.

[22] BAGARIA S, PRABHAKAR S B, SAQUIB Z. Flexi-DNP3: flexible distributed network protocol version 3 (DNP3) for SCADA security[C]//International Conference on Recent Trends in Information Systems. 2012:293-296.

[23] MAJDALAWIEH M, PARISIPRESICCE F, WIJESEKERA D. DNPSec: distributed network protocol version 3 (DNP3) security framework[M]. Advances in Computer, Information, and Systems Sciences, and Engineering. 2007:227-234.

[24] CRAIN J A, BRATUS S. Bolt-on security extensions for industrial control system protocols: A case study of DNP3 SAv5[J]. IEEE Security & Privacy Magazine, 2015, 13(3):74-79.

[25] IAN Y X. Real-time and interactive attacks on DNP3 critical infrastructure using Scapy[C]//Australasian Information Security Conference (ACSW-AISC). 2015.

[26] DARWISH I, IGBE O, SAADAWI T. Vulnerability assessment and experimentation of Smart Grid DNP3[J]. Journal of Cyber Security, 2016, 5(1):23-54.

[27] JIN D, NICOL D M, YAN G. An event buffer flooding attack in DNP3 controlled SCADA systems[C]//Simulation Conference. 2011: 2619-2631.

[28] 张盛山, 尚文利, 万明,等. 基于区域/边界规则的 Modbus TCP 通讯安全防御模型[J]. 计算机工程与设计, 2014, 35(11):3701-3707.
ZHANG S S, SHANG W L, WAN M, et al. Security defense module of Modbus TCP communication based on region/enclave rules[J]. Computer Engineering and Design, 2014, 35(11):3701-3707.

[29] KATO W M I, KOIKE M, MATTA M. Dynamic zoning based on situational activities for ICS security[C]//The 10th Asian Control Conference(ASCC). 2015:1-5.

[30] JEON B S, NA J C.A study of cyber security policy in industrial control system using data diodes[C]//The 18th International Conference on Advanced Communication Technology (ICACT). 2016: 314-317.

[31] ICS-CERT. Targeted cyber intrusion detection and mitigation strategies[R]. Washington: DHS, 2013-02.

[32] FOVINO I N, CARCANO A, MUREL T D L, et al. Modbus/DNP3 State-Based Intrusion Detection System[C]//IEEE International Conference on Advanced Information NETWORKING and Applications. 2010:729-736.

[33] 姜伟伟, 刘光杰, 戴跃伟. 基于 Snort 的 Modbus TCP 工控协议异常数据检测规则设计[J]. 计算机科学, 2015,42(11):212-216.
JIANG W W, LIU G J, DAI Y W. Design of Modbus TCP industrial control network protocol abnormal data detection rules based on snort[J]. Computer Science, 2015,42(11):212-216.

[34] 赖英旭, 刘增辉, 蔡晓田,等. 工业控制系统入侵检测研究综述[J]. 通信学报, 2017, 38(2):143-156.
LAI Y X, LIU Z H, CAI X T, et al. Research on intrusion detection of industrial control system[J]. Journal on Communications,2017, 38(2): 143-156.

[35] WILHIOT K. Who's really attacking your ICS equipment [R].Silicon Valley：Trend Micro Incorporated, 2013.

[36] 周昆, 一种基于 Honeyd 的过程控制蜜罐系统的平台搭建研究[D]. 上海:华东理工大学, 2014.
ZHOU K. A honeypot process control system platform based on honeyd[D]. Shanghai: East China University of Science and Technology, 2014.

[37] 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.

[38] 于长奇. 工控设备漏洞挖掘技术研究[D]. 北京: 北京邮电大学, 2015.
YU C Q. The Study of Industrial Control System Device Vulnerability Discovery[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[39] 王欢欢. 工控系统漏洞扫描技术的研究[D]. 北京:北京邮电大学, 2015.
WANG H H. Research on vulnerability scanning technology of industrial control system[D]. Beijing University of Posts and Telecommunications, 2015.

[40] 伊胜伟, 张翀斌, 谢丰,等. 基于 Peach 的工业控制网络协议安全分析研究[J]. 清华大学学报自然科学版. 2017,57(1): 50-54.
YI S W, ZHANG C B, XIE F, et al. Security analysis of industrial control network protocols based on Peach[J]. J Tsinghua Univ (Sci & Technol), 2017, 57(1):50-54.

[41] CHEUNG S, DUTERTRE B, FONG M, et al. Using model-based intrusion detection for SCADA networks[C]//The Scada Security Scientific Symposium.2016.

[42] FOVINO I N, CARCANO A, MUREL T D L, et al. Modbus/DNP3 state-based intrusion detection system[J]. Advanced Information Networking and Applications.2010:729-736.

[43] YANG D Y, USYNIN A, HINES J W, Anomaly-based intrusion detection for SCADA systems[J]. International Atomic Energy Agency (IAEA), Technical Meeting on Cyber Security, Idaho, 2016

[44] TSANG C H, KWONG S. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction[M]. 2016.

[45] NSS E, FRINCKE D A, MCKINNON A D, et al. Configurable Middleware-Level Intrusion Detection for Embedded Systems[C]/International Workshop on Security in Distributed Computing Systems. IEEE Computer Society, 2015:144-151.

[46] 罗新强. 低开销工业无线网络安全机制研究[D]. 北京:北京科技大学, 2015.
LUO X Q. Research on Low-Cost Security Mechanism of Industrial Wireless Network[D]. Beijing: University of Science and Technology Beijing, 2015.

[47] MOREIRA N, MOLINA E, LÁZARO J, et al. Cyber-security in substation automation systems[J]. Renewable & Sustainable Energy Reviews, 2016, 54:1552-1562.

[48] BINOD V, DIMITRIOS M, HUSSEIN T M. Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network[J]. IEEE Network, 2013(1):5-11.

[49] TSANG P P, SMITH S W. YASIR: a low-latency, high-integrity security retrofit for legacy SCADA systems[C]//The 23rd International Axiomatic Security Conference. Springer US, 2008: 445-459.

[50] SOLOMAKHIN R, TSANG P, SMITH S. High security with low latency in legacy SCADA systems[J]. Advances in Information & Communication Technology, 2010, 342:63-79.

[51] WEI D, LU Y, JAFARI M, et al. Protecting smart grid automation systems against cyberattacks[J]. IEEE Transactions on Smart Grid, 2011,2(4):782-795.

[52] PREMNATH A P, JO J Y, KIM Y. Application of NTRU cryptographic algorithm for SCADA security[C]//International Conference on Information Technology. 2014: 341-346.

[53] PATEL S C, BHATT G D, GRAHAM J H. Improving the cyber security of SCADA communication networks[J]. Communications of the ACM, 2009,52(7):139-142.

[54] SABALIAUSKAITE G, MATHUR A P.Design of intelligent checkers to enhance the security and safety of cyber physical systems[C]//The 38th Annual International Computers, Software and Applications Conference Workshops, 2014:7-12.

[55] HAO J P, PIECHOCKI R J, KALESHI D, et al.Sparse malicious false data injection attacks and defense mechanisms in smart grids[J]. IEEE Transactions on Industrial Informatics, 2015, 11(5):1198-1209.

[56] 辛耀中, 石俊杰, 周京阳, 等. 智能电网调度控制系统现状与技术展望[J]. 电力系统自动化, 2015, 39(1):2-8.
XIN Y Z, SHI J J, ZHOU J Y, et al. Technology development trends of smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1):2-8.

[57] 陈来军, 梅生伟, 陈颖. 智能电网信息安全及其对电力系统生存性的影响[J]. 控制理论与应用, 2012, 29(2):240-244.
CHEN L J, MEI S W, CHEN Y. Smart grid information security and its influence on power system survivability[J]. Control Theory & Applications, 2012, 29(2):240-244.

[58] 曾鸣, 李红林, 薛松, 等. 系统安全背景下未来智能电网建设关键技术发展方向—印度大停电事故深层次原因分析及对中国电力工业的启示[J]. 中国电机工程学报, 2012, 32(25):175-181.
ZENG M, LI H L, XUE S, et al. Key technologies of future smart grid construction based on power system security: a view of blackout in

India and experience and enlightment to power industry in China[J]. Proceedings of the CSEE, 2012, 32(25):175-181.

[59] 丁冠军, 樊邦奎, 兰海滨, 等. 智能电网信息安全威胁及防御策略研究[J]. 电力信息与通信技术, 2014, 12(5):58-63.
DING G J, FAN B K, LAN H B, et al. Research on information security threats and defense strategies for smart grid[J]. Electric Power ICT, 2014, 12(5):58-63.

[60] 刘雪艳, 张强, 李战明. 智能电网信息安全研究综述[J]. 智能电网,2014, 12(4):56-60.
LIU X Y, ZHANG Q, LI Z M. A Survey on information security for smart grid[J]. Electric Power ICT, 2014, 12(4):56-60.

[61] 张海鹏. 智能电网信息安全威胁及防御技术研究[D]. 石家庄：河北科技大学, 2014.
ZHANG H P. Smart grid information security threats and defense technology research[D]. Shijiazhuang: Hebei University of Science and Technology, 2014.

[62] LU Z, LU X, WANG W, et al. Review and evaluation of security threats on the communication networks in the smart grid[C]//Proceedings of IEEE Military Communications Conference, San Jose, 2010. 1830-1835.

[63] LI H, MAO R, LAI L, et al. Compressed meter reading for delay-sensitive and secure load report in smart grid[C]//Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg. 2010: 114-119.

[64] RIAL A, DANEZIS G. Privacy-preserving smart metering[C]//In: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society. 2011: 49-60.

[65] RUJ S, NAYAK A. A decentralized security framework for data aggregation and access control in smart grids[J]. IEEE Trans Ind Electron, 2013, 4: 196-205

[66] ROTTONDI C, VERTICALE G, CAPONE A. Privacy-preserving smart metering with multiple data consumers[J]. Computer Network, 2013, 57: 1699-1713

[67] BIRMAN K, JELASITY M, KLEINBERG R, et al. Building a secure and privacy-preserving smart grid[J]. ACM Special Interest Group Operating Syst Rev, 2015, 49: 131-136

[68] LI H, LAI L, QIU R C. Communication capacity requirement for reliable and secure state estimation in smart grid[C]//Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg. 2010: 191-196

[69] 张彤. 电力可信网络体系及关键技术的研究[D]. 北京: 华北电力大学, 2013.
ZHANG T. Research on theory and key technologies of trusted network in electric power industry control system[D]. Beijing: North China Electric Power University,2013.

[70] 詹静, 杨静. 基于远程证明的可信 Modbus/TCP 协议研究[J]. 四川大学学报(工程科学版), 2017, 49(1):197-205.
ZHAN J, YANG J. Research on remote attestation-based trusted Modbus/TCP protocol[J]. Advanced Engineering Sciences, 2017, 49(1): 197-205.

[71] 邵诚, 钟梁高. 一种基于可信计算的工业控制系统信息安全解决方案[J]. 信息与控制, 2015, 44(5):628-633.
SHAO C, ZHONG L G. Research of information security solutions of industrial control system based on trusted computing[J]. Information and Control,2015, 44(5):628-633.

[72] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4):481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4):481-494.

作者简介：

冯涛（1970-），男，甘肃临洮人，博士，兰州理工大学研究员、博士生导师，主要研究方向为网络与信息安全、密码学。

鲁晔（1986-），男，陕西宝鸡人，兰州理工大学博士生，主要研究方向为工业控制网络安全与协议安全。

方君丽（1985-），女，甘肃天水人，兰州理工大学讲师，主要研究方向为网络与信息安全。