PLCBlockMon 的 PLC 逻辑. 该逻辑仅记录标识系统状态和影响物理过程的变量数据, 一方面简化日志记录的复杂性, 另一方面也提高了检测方法的安全性, 减小入侵检测系统的负载. 文献 [15] 则针对 PLCs 中来自受信任节点的拒绝服务 (Denial of Service, DoS) 攻击, 提出一个入侵防御系统 (Intrusion Prevention System, IPS). 该系统最大的贡献在于它的通用性, 可以在任何 PLC 系统使用而不受工业基础设施的功能限制. 该系统可以安装在 PLC 系统内部, 降低攻击者破坏 IPS 的可能性; 还可以安装在 PLC 外部, 为 PLC 系统增加一层安全层, 巩固深度防御方法. 最重要的是, IPS 检测到 DoS 攻击后会自动重启, 以彻底清除所有攻击流量数据, 确保系统正常运行, 而不受攻击影响.

(3) SCADA 系统架构安全解决方案

文献 [16] 考虑到 SCADA 系统组件中实现监控功能的数据完整性的重要性, 使用区块链技术提高系统组件中数据日志的完整性. 文章将以工作量证明 PoW (Proof of Work) 为基础的区块链技术集成到 CPS 系统中. 为了提高系统资源利用率, 不影响工业控制系统实时性的需求, 文章引入时间概念, 对消息到达时间进行预测. 该方案的贡献在于不仅对 SCADA 系统中数据的完整性提供了可靠保证, 优化验证计算以交付难以篡改的数据日志, 还充分考虑了工业控制系统的系统监控功能的实时性需求.

在安全研究中, 为了更好的验证安全解决方案的可行性, 需要在工业控制系统中直接运行, 但厂商不会允许在工业控制系统中部署不信任或未证实身份的设备, 因此在研究中使用真实的 SCADA 系统是不现实的. 文献 [17] 开发了一个新颖的开源框架, 用于新建、部署和管理 SCADA 系统仿真平台, 它可以在本地或远程自动部署大量虚拟机用来复制 SCADA 网络. 该框架包含多个虚拟主机模拟传感器和执行器, 使用 HMI 控制虚拟主机. 同时, 该框架提供一组自动化脚本, 可以根据用户需求自动部署可变数量的虚拟机. 文章指出该框架符合 IEC104 和 OPC-UA 标准, 并支持其他工业协议. 最重要的是该框架建立在开源代码库的基础上, 是一款免费开源的仿真平台软件.

(4) 智能电网系统架构安全解决方案

在我国工业领域的控制系统信息安全研究中, 电力行业一直处于领先地位, 但是电力行业安全的研究重心一直放在边界安全上, 没有对系统架构安全进行深入研究, 文献 [18] 和文献 [19] 分别对电力系统架构改进和重建两方面做出分析. 文献 [18] 针对电网系统中电力存储的检测与防护, 提出一种名为 PSP 的储能保护框架. 文献 [18] 认为当今电网的安全管理体系中, 系统安全人员面对攻击无法获悉攻击者的目标和攻击过程, 仅能够观察到部分设备的状态变化情况, 入侵检测工具的分析结果也具有不确定性. 为了应对攻击者对电力存储系统攻击, 电力设施的运营商必须以最小成本维持供电系统的稳定性. 针对上述问题, 文章设计一种名为 PSP 的框架, 它参考零和博弈问题, 利用部分可观察马尔可夫决策过程 (Partially Observable Markov Decision Process , POMDP) 为系统问题建模, 使用动态规划算法求得最优解并进行验证. 该方案一方面充分考虑工控系统可用性至上的特性, 从系统运行状态出发, 只要系统运行正常, 处于连续一致的状态, 就不采取任何防御行动. 另一方面充分考虑电力存储的 3 种形式, 以适应电力运营商的存储需求. 文献 [19] 指出, 智能电网的系统架构正在向分布式系统模型方向发展, 欧盟的 ELECTRA 项目提出关于未来智能电网可能的系统架构 WoC (Web of Cells) 概念模型, 如图 4 所示. 该模型最大的特点是“在当地解决当地问题”, 单个细胞的稳定性通过细胞内的设备控制, 系统整体的稳定性则由一个控制器控制. 针对该系统架构, 文章提出一种理论分析方法, 首先将一次攻击过程分解为多个攻击阶段, 然后分别对各个阶段进行建模评估, 实现多段攻击过程的安全分析. 该方法最大的贡献[20] 在于引入时间属性, 指出攻击成功的概率不仅是一个百分比, 而是一个包含攻击者攻击过程可用时间的函数, 以此对攻击结果进行定量分析.

2.2 基于通信协议的安全解决方案

工业控制系统的协议众多, 早先工业控制系统为封闭系统, 为了保证自己的核心竞争力和机密性, 多采用不对外开放的专有协议. 随着 TCP/IP 等通用协议在工业领域的应用, 专有协议的安全缺陷开始被攻击者利用, 大部分专有协议的安全机制无鉴别、无加密、无审计, 设备可通过扫描工业协议漏洞被发现, 如表 2[2].

文献 [21] 以“Stuxnet”事件为引, 针对 PLC 系统面临的严重的安全威胁, 对西门子最新的 S7-1211C 控制器协议和 TIA (Totally Integrated Automation) 软件漏洞进行研究, 为 PLC 的安全研究做出极大贡献. 文章指出, 首先, 文中发现的漏洞并不复杂, 复杂的是使用通

讯协议本身的合法功能时产生的安全威胁; 其次, 通讯协议的身份认证机制和数据完整性检查机制并不可靠; 最后, 现有的入侵检测防御软件的功能是有限的, 对系统自身合法行为引起的安全威胁的检测并不完善. 文献 [22] 更进一步, 分析通用的西门子 S7 通讯协议, 其分析方法有更好的实用性. 该方法使用神经网络训练系统模型, 利用系统模型当前的网络流量对系统异常进行监测. 文章针对 S7 通讯协议不需要身份验证即可与 PLC 建立连接并获取数据的漏洞, 开发 S7 通讯协议客户端用于攻击测试. 结果表明, 该方法以 97% 的成功率检测异常网络数据包. 这样的结果为人们分析不同 IDS 中的 S7 通讯协议提供更加具体、可靠的依据, 同时为配合其他检测技术, 建立检测能力更高的入侵检测系统提供帮助.

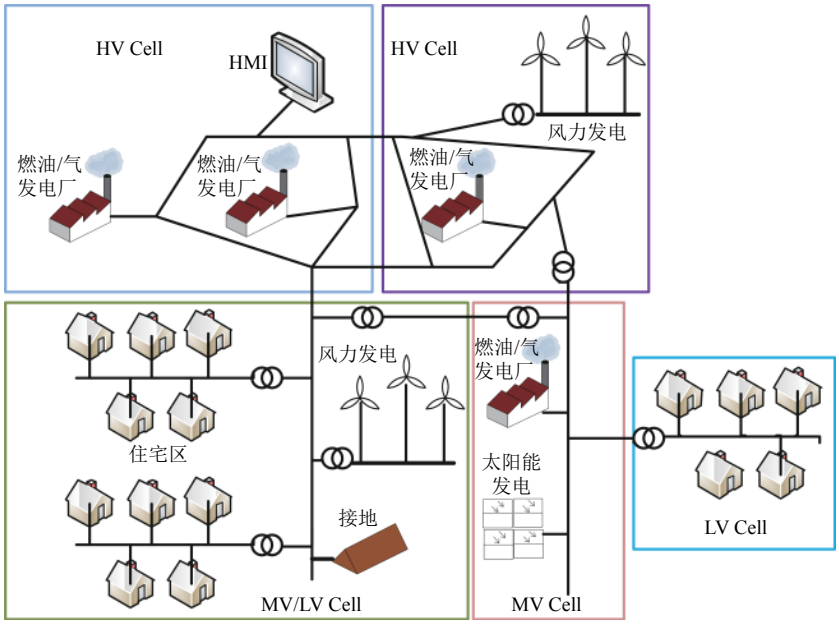

图 4 文献 [19] 涉及的 WoC 概念模型

表 2 2018 年不同协议可探测设备数量

工业协议	设备数量
Modbus	30065
IEC	1451
DNPS	953
S7	243

同样, 用于监视和控制底层物理系统, 满足其更好的功能性和可用性需求的 SCADA 系统也不能保证过程数据的机密性. 文献 [23] 针对 IEC-104 协议开发一个解析器, 对协议包解析后直接反馈到系统模型中, 然后利用 Bro 自适应性策略制定的物理约束和安全需求对 SCADA 流量进行实时检查. 该方法可以在现场使用, 探测到可疑和错误的命令或传感器读数时会自动生成警报, 因此, 该方法可以全面提高本地入侵检测系统的安全性能.

文献 [24] 则针对 Modbus 协议提出新的入侵检测方法. 该文献为基于软件定义网络 (Software Defined Networking, SDN) 的工业控制系统建立基于网络的两层入侵检测系统. 第一层由运行在交换机上的协议白名单组成, 利用基于 P4 (Programming Protocol-independent Packet Processors) 的数据包处理器实时监控, 将可疑数据包直接转移到第二层进行深入检测; 第二层则由一个深度包探测器和 Bro 组成, 目的是更新第一层中的白名单. 该文献的主要贡献有:首先, 该两层入侵检测系统使用 P4 编写包处理器, 为以后扩展其他工业协议奠定了基础, 且数据包处理器直接运行在交换机上, 不需要额外添加设备, 降低运营成本; 其次, 两层的设计理念解决现有的白名单方法的缺点, 系统不再直接拒绝可疑包, 而是将其转发到第二层做深入检测, 减小负载; 最后, 仿真实验证明, 该入侵检测系统对工控系统的通讯仅有极小的通讯延迟, 基本不影响系统的实时性要求.

以上 4 篇文章的贡献在于从工控系统中使用的专

用通讯协议出发, 针对通讯协议的安全漏洞提出相应的入侵检测方法, 不仅填补了工业协议相关研究方面的空白, 还为后续 ICS 信息安全研究提出新思路.

3 ICS 信息安全未来发展方向

本文对会议论文中提出的安全解决方案进行研究与分析, 针对其中采用的技术与方法, 对未来 ICS 信息安全研究方向提出以下建议.

(1) 网络攻击模型的应用

网络攻击模型的应用可以加深研究人员对网络攻击的认识和描述, 通过网络攻击模型可以对整个攻击过程进行结构化建模和形式化描述, 帮助研究人员利用已有的攻击行为背景对网络攻击进行深入分析. 随着 IT 技术的发展和网上共享资源的增加, 攻击手段越来越多样化, 攻击过程越来越复杂, 想把攻击完全隔离在系统之外是不可能的, 只能根据已知攻击行为的关联性找出攻击规律, 进一步确定攻击目标, 从而针对攻击过程采取阶段性的防御策略来阻止攻击. 这足以可见网络攻击模型在当前背景下的重要作用. 当前我国研究人员对网络攻击模型研究的实际应用还不完善, 更加需要深入研究网络攻击模型的实际应用和理论创新, 积极在入侵检测和防御系统中应用网络攻击模型.

(2) 开源的工业控制系统仿真平台

由于工业控制系统的封闭性, 厂商对不信任或未经身份验证设备连接的拒绝, ICS 仿真平台一直是研究的热点, 随着仿真和虚拟技术的发展, 工业控制系统系统仿真技术已得到广泛应用. 但是已有的仿真平台聚焦于特定的工业协议和控制系统, 通用性差, 不具备扩展能力. 更重要的是, 大部分仿真平台不开源, 使用成本高, 使得部分学术研究试验不可再现, 阻碍学术研究进展. 随着工业控制系统信息安全受重视程度的提高, 迫切需要开发更多免费、开源的仿真平台, 以便其在信息安全研究进程中发挥重要作用.

(3) 非技术型人机界面的研究

人机界面可以把系统中涉及和产生的数据信息转为直观的图形化界面, 方便系统和用户之间的信息交互, 但已有的人机界面多用于与技术人员进行沟通, 专业性过强, 非技术型研究人员不能简单易懂的获取相关信息, 阻碍研究进程. 工业控制系统信息安全研究中, 不仅涉及以信息安全为背景的研究人员, 还会涉及工业背景的研究人员, 以及不具有任何安全知识背景管理层和用户. 为了更明确的表示安全结果, 可视化人机界面要多者兼顾, 提供技术型和非技术型人机界面, 促进不同研究背景下安全技术的融合.

4 结束语

工业 4.0 时代的到来, ICS 在国家关键基础建设中的重要地位得到极大提高. 同时, 信息化与工业化的深度融合使工业控制系统继承 IT 系统的网络安全威胁, 但是工业控制系统 ICS 与 IT 系统之间存在巨大差异, 不能直接将传统 IT 安全技术应用于 ICS 中, 需要根据实际需求研究适用于 ICS 的安全技术, 这使我国起步较晚的工业控制系统信息安全面临着严峻的挑战. 本文对 2018 年 ICS-CSR 会议涉及的先进的 ICS 信息安全解决方案做出阐述与分析, 并根据实际需求对研究方向提出针对性建议. 总之, ICS 信息安全行业刚刚步入正轨, 成长空间广阔, 仍需要研究人员对工业控制系统信息安全技术做出新的研究.

参考文献

1 王昱镔, 陈思, 程楠. 工业控制系统信息安全防护研究. 信息网络安全, 2016, (9): 35–39. [doi: 10.3969/j.issn.1671-1122.2016.09.007]

2 北京神州绿盟信息安全科技股份有限公司. 2019 工业控制系统信息安全保障框架. http://www.nsfocus.com.cn/html/2019/134_0924/38.html. [2019-09-24].

3 彭勇, 江常青, 谢丰, 等. 工业控制系统信息安全研究进展. 清华大学学报 (自然科学版), 2012, 52(10): 1396–1408.

4 区和坚. 工业控制系统信息安全研究综述. 自动化仪表, 2017, 38(7): 4–8.

5 王小山, 杨安, 石志强, 等. 工业控制系统信息安全新趋势. 信息网络安全, 2015, (1): 6–11. [doi: 10.3969/j.issn.1671-1122.2015.01.002]

6 李鸿培, 忽朝俭, 王晓鹏. 2014 工业控制系统的安全研究与实践. 计算机安全, 2014, (5): 36–59, 62. [doi: 10.3969/j.issn.1671-0428.2014.05.011]

7 杨安, 孙利民, 王小山, 等. 工业控制系统入侵检测技术综述. 计算机研究与发展, 2016, 53(9): 2039–2054. [doi: 10.7544/issn1000-1239.2016.20150465]

8 IEC. IEC/TS 62443-1-1 Industrial communication networks. Network and system security. Part 1-1: Terminology, concepts and models. Geneva: IEC, 2009.

9 张文安, 洪榛, 朱俊威, 等. 工业控制系统网络入侵检测方法综述. 控制与决策, 2019, 34(11): 2277–2288.

10 熊琦, 彭勇, 戴忠华, 等. 工业控制系统的安全风险评估. 中

国信息安全, 2012, (3): 57–59. [doi: 10.3969/j.issn.1674-7844.2012.03.017]

11 Niedermaier M, Hanka T, Plaga S, *et al*. Efficient passive ICS device discovery and identification by MAC address correlation. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 21–30.

12 Hassanzadeh A, Burkett R. SAMIIT: Spiral attack model in IIoT mapping security alerts to attack life cycle phases. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 11–20.

13 Depamelaere W, Lemaire L, Vossaert J, *et al*. CPS security assessment using automatically generated attack trees. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 1–10.

14 Findrik M, Smith P, Quill K, *et al*. PLCBlockMon: Data logging and extraction on PLCs for cyber intrusion detection. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 102–111.

15 Das R, Menon V, Morris TH. On the edge Realtime intrusion prevention system for DoS attack. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 84–91.

16 Koumidis K, Kolios P, Panayiotou C. Optimizing Blockchain for data integrity in Cyber physical systems. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 74–83.

17 Maynard P, McLaughlin K, Sezer S. An open framework for deploying experimental SCADA Testbed networks. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 92–101.

18 Wadhawan Y, Neuman C, Anas A. PSP: A framework to allocate resources to power storage systems under cyber-physical attacks. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 57–66.

19 Terruggia T, Dondossola G, Ekstedt M. Cyber security analysis of Web-of-Cells energy architectures. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 41–50.

20 宋蕙慧, 于国星, 曲延滨. Web of Cell 体系——适应未来智能电网发展的新理念. 电力系统自动化, 2017, 41(15): 1–9.

21 Hui H, McLaughlin K. Investigating current PLC security issues regarding Siemens S7 communications and TIA portal. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 67–73.

22 Eigner O, Kreimel P, Tavolato P. Identifying S7comm protocol data injection attacks in cyber-physical systems. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 51–56.

23 Chromik JJ, Remke A, Haverkort BR. Bro in SCADA: Dynamic intrusion detection policies based on a system model. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 112–121.

24 Ndonda GK, Sadre R. A two-level intrusion detection system for industrial control system networks using P4. Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research. Hamburg, Germany. 2018. 31–40.