基于电力云边协同的非侵入式 Modbus TCP 协议安全增强方法

何涂哲秋[1]，徐子东[1]，车欣[2]，张镇勇[1]

(1. 省部共建公共大数据国家重点实验室（贵州大学 计算机科学与技术学院），贵州 贵阳 550025；
2. 浙江大学 控制科学与工程学院，浙江 杭州 310027)

摘　要：分布式电源（distributed resources，DR）中智能边缘设备数据传输的安全问题为电力系统带来了安全隐患。Modbus TCP（transmission control protocol）协议作为边缘设备采用的通信手段之一，其协议安全性的不足使得系统易遭到网络空间的攻击。为保障电力设备数据传输安全，对现有安全手段进行整理，分析现有安全手段在 DR 应用场景下的不足，提出一种非侵入式Modbus TCP协议安全增强方法。该方法采用云边协同的架构，利用电力控制中心云平台管理访问控制原则，将实际访问控制决策模块部署在边缘设备，并通过细粒度的访问控制组合限制恶意行为。依据 Modbus 协议参考指南，搭建 DR 应用场景进行渗透测试，验证该方法能有效防御重放攻击和中间人攻击，可将安全开销控制在百微秒以内，显著优于其他安全手段，满足 DR 对实时性的需求。

关键词：Modbus TCP 协议；协议安全；分布式电源；访问控制

DOI：10.11930/j.issn.1004-9649.202401006

0　引言

Modbus 协议是一种应用层信息交换协议，作为伴随着数据采集与监控系统（supervisory control and data acquisition，SCADA）而出现的串行通信标准之一[1]，因其易于实现和维护的特性，常被应用于电力控制系统现场层智能设备和 SCADA 系统之间的数据交换[2]。在分布式光伏发电系统中，Modbus TCP 协议用于从光伏逆变器中采集电压、电流和功率输出等关键参数，SCADA 系统对这些数据进行分析以优化电能管理和分配[3]。在分布式风力发电系统中，Modbus TCP 用于监控和控制风力发电机的状态，包括风速、叶片角度和发电量，从而提高能源捕获效率。在电力能源管理系统中，Modbus TCP 协议用于实现对可编程逻辑控制器（programmable logic controller，PLC）、变压器、断路器、智能电表等设备的控制和监控[4]。Modbus TCP 协议为分布式电源（distributed resources，DR）边缘设备、端设备的可靠实时通信提供支持，在云、边、端电力监控系统中起到重要作用[1]。

由于 Modbus TCP 协议在设计时以可用性为第一需要，并未充分考虑安全特性，导致其本身存在缺少访问控制、缺乏数据保护的漏洞[5]，而这些漏洞随着 DR 系统对信息技术的引入被暴露在更加开放的网络环境中，给系统带来了更大的安全风险[6]。例如，来自网络空间的攻击者先通过暴力枚举协议中的设备地址或单元标识符字段，发现和识别网络中的全部 Modbus 设备，再利用协议设计中缺少访问控制字段的特性，执行中间人攻击或者重放攻击，进行未授权访问[7]。攻击者会向电力设备发送错误指令，篡改 PLC 的控制逻辑，使得风力涡轮机或太阳能逆变器等电力设备过载；或是注入虚假指令[8]，修改智能电表的读

收稿日期：2024-01-02；**修回日期：**2024-05-27。

基金项目：国家自然科学基金资助项目（面向信息物理协同攻击的负载频率控制系统安全防御研究，62303126；基于多源密态数据的隐私保护神经网络模型，62362008）；贵州省基础研究计划（自然科学）一般项目（面向智能电网状态估计的信息物理攻防建模及防御成本优化研究，ZK〔2022〕149）；贵州省教育厅高等学校科学研究项目（青年项目）（面向大数据赋能的电网稳定性评估系统脆弱性研究，黔教技〔2022〕104 号）。

数[9]，窃取系统运行状态[10]，导致电力控制中心做出错误的发电量估计和能源分配决策[11]，造成经济损失。

现有的解决方案大多通过运用加密技术[12-15]或引入中间设备[16-19]进行访问控制，以增强 Modbus TCP 协议的通信安全。这些安全防护手段在分布式电源场景下的应用存在以下困难。一是难以确保加密后的设备仍与原有系统兼容。由于电力 SCADA 系统中存在大量的老旧设备，使用协议加密方法改变 Modbus TCP 协议数据帧会使老设备无法解析报文，导致系统运行中断[20-21]。二是引入中间设备会带来额外的安全风险。用于信息交换的中间设备作为系统的通信枢纽，一旦瘫痪则可能导致相关设备无法通信，给系统带来新的安全漏洞。三是难以降低安全手段带来的时间开销。由于 Modbus TCP 协议主要用于电力控制系统现场层上位机与控制器、控制器与控制器、控制器与智能仪表之间，这些设备对实时性有很高的要求[20]，引入复杂的安全方案会带来更高响应时延，使协议不再适用于原场景。

为解决上述问题，本文提出一种非侵入式方法以增强 Modbus TCP 协议的安全。

1 电力 Modbus TCP 协议相关安全工作

1.1 侵入式方法

侵入式方法是指直接对系统或网络进行物理或逻辑上的更改以提升安全性的方法。文献 [12] 通过在 Modbus 数据帧中加入安全哈希算法 2（security hash algorithm 2，SHA-2）生成的数据摘要确保 Modbus 数据传输过程中的完整性，同时利用 RSA 签名验证数据来自正确的发送方。这种保护方法要求系统提供足够的计算资源，因此该方法难以部署到智能逆变器等计算资源有限的分布式电源设备中。文献 [13] 提出利用基于哈希的消息验证码算法生成数据认证码以保障数据完整性，同时利用 SM4 对称加密算法为传输过程中的数据加密，从理论上分析了该方法的算法执行次数，并认为对称加密手段在时间性能上优于非对称加密，但对其实际时间开销并未进行实验验证。文献 [14] 提出利用 IT 领域中常见的传输安全层（transport security layer，TLS）协议对 Modbus TCP 报文进一步封包，从而为协议提供加密、完整性和认证的保障。这种方法提高了 Modbus TCP 的安全能力，但 TLS 所支持的加密套件会带来 18%~86% 的额外响应延迟。文献 [15] 在此工作的基础上提出了一种中心化的访问控制方法，该方法延用 TLS 协议确保通信安全，使用 X.509v3 证书确认双方的身份，并要求 Modbus TCP 从机通过查询身份管理中心对主机的行为进行约束，这种三方交互的模型带来了 47%~79% 的额外响应延迟。

1.2 非侵入式方法

非侵入式方法是指在不改变现有系统或设备的基础上，通过附加方法来提升网络和系统的安全性。文献 [16] 提出了一种附加的硬件安全模块用于保障分布式电源系统中端到端的通信安全。该硬件通过 OpenSSL 实现数据的加密和解密，并且提供了基于角色的访问控制能力，但需要布置在每一个 Modbus TCP 通信节点上，这种通信方式给系统带来了 300%~500% 的额外响应时间。文献 [17] 提出对 Modbus TCP 通信双方添加安全代理，由代理使用 AES-256 进行报文加密，并使用 SHA-256 生成认证令牌。虽然该方案仍需要为每个通信实体添加中间模块，但其将时间开销控制在 2 ms 内。此外还有基于蜜罐诱导攻击的方法[18]、基于入侵检测系统[19]分析异常流量的方法等。

侵入式方法的弊端在于需要对系统进行大范围的改动，在实践中存在兼容性问题。而非侵入式方法在时间性能上弱于对协议进行修改的侵入式方法，这是由于引入大量的中间模块导致的。此外，从成本和部署难度来讲，非侵入式的方法也存在实现上的困难。基于上述分析，本文聚焦于对 Modbus TCP 协议中非法访问行为进行约束，基于电力云边协同管理的策略，在实现非侵入式协议安全增强的同时，满足分布式电源系统对实时性的需求。

2 电力 Modbus TCP 安全增强方法

2.1 安全增强框架

在分布式电源系统中，存在大量太阳能光伏面板、逆变器、电能质量监控传感器等智能设备，这些设备通过 Modbus TCP 协议实时传输电

压、电流、频率等关键数据。但由于这些设备地理位置分散、缺少清晰的网络边界，而传统的中心化访问控制和引入中间设备的防护手段很难部署在分布式电源场景。因此，本研究提出了一种基于电力云边端架构的安全增强框架。

电力云边协同架构的优势在于数据处理不仅发生在远程的电力控制中心云平台上，而且还发生在距离数据源更近的边缘节点上[22-24]。该架构将云平台的处理能力和边缘计算的低延迟优势相结合，从而减少边缘设备对中心服务器的依赖，降低系统带宽的占用率，从而减少系统的响应时间。这一特性可应用于增强基于 Modbus TCP 协议的通信安全，将控制行为发生节点由中心服务器迁移部署到边缘设备，借此实现更低的系统延迟。

本文提出的 Modbus TCP 协议安全增强架构如图 1 所示。该架构由电力控制中心云平台、边缘设备和端设备构成。在该架构中，电力控制中心云平台负责产生和管理针对边缘设备的访问控制原则。边缘设备依据访问控制原则对接收到的报文进行处理解析，当收到不合法的报文时，拒绝该访问行为，并将访问记录上传到电力控制中心云平台以供安全人员进行下一步的决策和分析。端设备是边缘设备的控制对象，用于实时采集环境数据，接收和处理来自边缘设备的指令。

在分布式电源的应用场景下，电力控制中心云平台可以限制对存储关键信息的线圈或寄存器

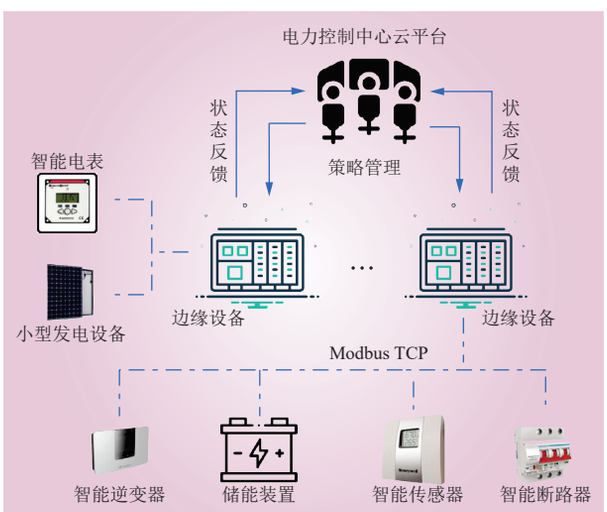

图 1　Modbus TCP 协议安全增强架构

Fig. 1　The security enhancement architecture of Modbus TCP protocol

的访问，边缘设备依据该原则，拒绝修改风力涡轮机的转速限制、断路器的触发机制等敏感参数。当电力控制中心云平台接收到报警信息后，可对系统进行安全检查或执行更加严格的访问控制策略。

2.2　访问控制设计

访问控制方案需要确保与系统老旧设备兼容并防范恶意攻击的发生。

为确保所提方案与系统中老旧实体通信，本方案设计了安全增强模块（security enhancement module，SEM）。该模块位于 Modbus TCP 协议的报文处理流中，其逻辑位置如图 2 所示。Modbus TCP 在接收到报文后，会解析并去除报文头部的事务标识符、协议标识符、长度字段等标识信息以提取协议数据单元（protocol data unit，PDU），随后 SEM 利用提取的 PDU 作为输入，获取报文详细信息，最后依据访问控制原则进行决策。该过程发生在接收端对报文的处理流中，并且通过调用原 Modbus TCP 协议的异常响应码拒绝非法操作，未对协议本身结构和数据进行修改，因此本方案与原 Modbus TCP 具有通信兼容性。

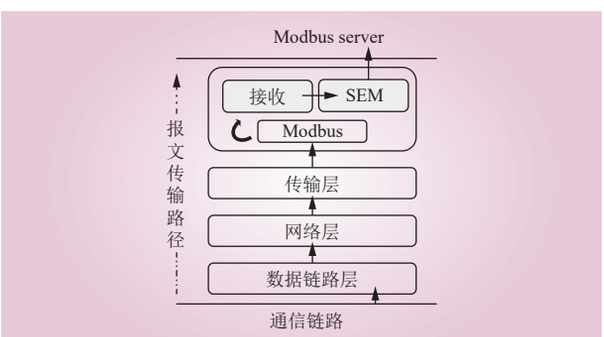

图 2　安全增强模块 SEM 逻辑位置

Fig. 2　The logical location of the security enhancement module

本方案的访问控制策略针对 Modbus TCP 协议在防重放攻击和防中间人攻击方面的脆弱性进行设计。Modbus TCP 协议的 PDU 中携带的最小粒度信息可分解为功能码和数据[25]，因此通过重放攻击和中间人攻击执行的恶意操作可以使用功能码进行约束。针对重放攻击分时段发生的特性，在访问控制中结合时间戳以拒绝运行时间以外的访问；针对中间人攻击的数据篡改特性，采用将功能码结合访问地址的方式，先通过功能码确定

防护对象，再对可访问的地址区间进行约束，从而对数据单元实施细粒度防护。

因此，访问控制原则由 2 个五元组构建，描述为：rulesFC (rid, fc, default, timeStart, timeEnd) 和 rulesAD (rid, type, default, adrStart, adrEnd)。rulesFC 和 rulesAD 分别表示以功能码为核心和以数据为核心的策略，元组的属性含义和取值空间如表 1 所示。其中，rid 字段用于标识策略的类型；fc 用于表示受约束的功能码；type 用于确定防护的对象；default 用于设置策略的开关状态；timeStart 和 timeEnd 用于划分策略生效的时间范围，adrStart 和 adrEnd 用于设定策略作用的地址空间。

表 1 访问控制要素

Table 1 The elements of access control

控制属性	属性描述	取值空间
rid	访问策略标识符	整型
fc	防护功能码	0x01~0x08 0x0 F、0x5 A
type	防护数据对象	Discretes Input Coils Input Registers Holding Registers
default	策略状态	开启/关闭
timeStart	策略生效时间	用户自定义
timeEnd	策略失效时间	用户自定义
adrStart	地址约束起点地址	用户自定义
adrEnd	地址约束终点地址	用户自定义

2.3 安全增强模块 SEM

为了确保访问控制方案的时间性能满足分布式电源系统要求，本文设计并优化了 SEM 对报文的处理算法。一是对访问控制策略的维护，确保与当前安全需求保持一致；二是基于这些策略对传入报文进行有效处理，确保每项操作都符合预定的安全规范。

对于计算设备而言，输入输出（input/output，I/O）延迟通常被视为性能瓶颈之一，因此 SEM 算法时间上的优化重心在于读取和维护访问控制策略的阶段。本文对 SEM 的算法做如下设计。首先，SEM 将 Modbus TCP 协议的 PDU 作为输入，获取 PDU 后，算法进入初始化流程。然后，程序检查访问策略文件的更新，其判断依据是获取读取文件的更改时间。仅当策略文件更新或内存中的访问控制策略为空时，才会调用系统 I/O 加载文件，以此减少 I/O 过程的发生次数，降低 SEM 的时间开销。

读取到访问控制信息后，SEM 优先对功能码策略进行验证。首先，从请求中提取功能码，调用功能码验证函数验证其合法性。这一设计能够快速确定操作的合法性。如果某个功能码已被禁用或不被支持，那么无需进一步分析访问的数据单元，借此进一步提高处理效率。如果功能码不合法，SEM 则会向控制台输出报警信息并记录在日志中，返回 False 表示未通过功能码验证，使用 Modbus TCP 协议原生异常码响应非法请求。然后进行时间范围的验证，完成 rulesFC 规则检验。

针对访问地址的检验，SEM 会首先读取 type 字段的内容，确定受约束的地址类型，依据地址类型对报文访问的地址空间进行解析，然后利用偏移量将其转化为 adrStart、adrEnd 表达的空间，最终进行比对。当报文访问空间与策略禁止的空间存在交集时，则表明地址验证失败。完成检验后，算法最终会返回一个布尔类型的值，以表明验证是否通过。

3 方法性能验证与分析

3.1 验证环境搭建

本文基于 LibModbus 进行模拟以验证本文设计的安全增强方法。LibModbus 是一个用于实现 Modbus TCP 协议的函数库，库中所实现的通信方式依赖 Modbus 组织发布的 Modicon Modbus 协议参考指南[26] 构建。

为近似模拟分布式电源应用场景，测试床的构建如图 3 所示。位于云端的电力控制中心通过网络服务提供商路由访问分布式电源系统路由，后者将广域网与分布式电源系统局域网相连。安全策略通过路由转发到分布式电源基础设施。数据采集终端 1 和 2 用于模拟上位应用程序向分布式电源基础设施发起请求，配置设备运行状态，采集设备中存储的数据。分布式电源基础设施 1 和 2 用于模拟受控的 Modbus 从设备，其中的数据单元中存储着控制设备运行的关键变量，例如风机的风速、叶片角度、发电量，或光伏逆变器中的电压、电流和功率参数。这些数据是攻击和防护的主要目标。

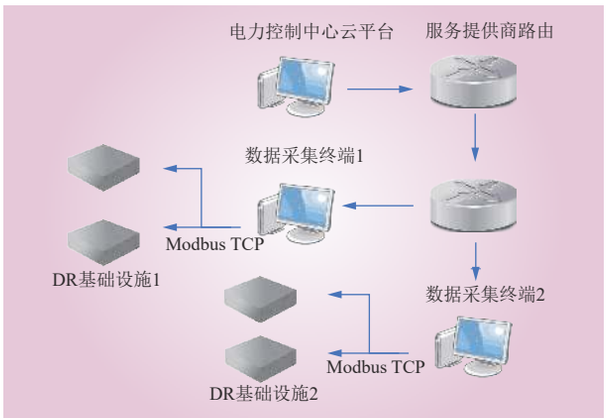

图 3　分布式电源场景下的测试网络拓扑结构

Fig. 3　Topology for testing over a DR network

3.2　安全性分析

基于上述测试网络拓扑结构，对 Modbus 从机实施如表 2 所示的重放和中间人 2 种攻击进行安全性验证和分析。表 2 中拦截因子是指对应攻击模式下会触发的访问控制策略。

表 2　攻击模式设计

Table 2　Patterns of attacks

手段	攻击模式	拦截因子
重放攻击	恶意第三方截获数据，并在某一时刻再次发送	时间约束
中间人攻击	恶意第三方截获数据，执行恶意操作	功能码
	恶意第三方截获数据，访问敏感信息	访问地址

表 2 结果表明，所提方案在假设的攻击模式下，对于中间人攻击和重放攻击均实现拦截，其效果如图 4 所示，Wireshark 将设备响应的报文解析为 Illegal function，即该恶意访问行为被设备拒绝。

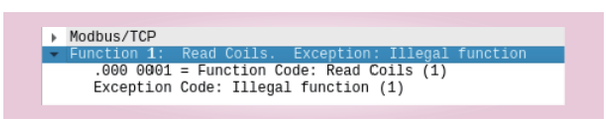

图 4　设备拒绝非法访问

Fig. 4　Rejection of illegal access

通过访问控制策略中的功能码约束和时间约束能够禁止约束时间之外的重放攻击，通过功能码约束和访问地址约束能够拒绝存在恶意读写的中间人攻击。因此，该访问控制方案具有抵抗相应攻击的能力。

3.3　性能评估

通信延迟是判断 Modbus TCP 协议性能和可用性的主要考量因素。为评估所提方案的可用性，排除网络因素和系统复杂程度对实验的干扰，本文提出将报文处理函数的时间开销 L 作为判断延迟的量，其计算方式为

$$L = t_{\text{end}} - t_{\text{start}} \tag{1}$$

$$t = \text{gettime}(t) \tag{2}$$

gettime()函数用于获取精确到微秒级的系统时间，由此记录进入报文处理流程的起点时间 t_{start} 和终止时间 t_{end}，继而利用式（1）计算时间开销 L。

本方案所提访问控制将功能码限制和访问地址限制作为控制元素，因此在性能验证环节分别针对这 2 种元素进行验证。图 5 显示的是读写线圈功能码访问验证的时间开销。图 5 中，横轴表示单位时间内 Modbus 主机发送的报文数量，纵轴表示监测程序所记录的时间开销 L。实验选择 0x01 和 0x05 功能码对应的线圈读取和线圈强制写入作为对象，分别测试了在处理线圈读取和处理线圈写入操作下的时间开销，并将禁止的线圈读取和线圈操作混合其允许的操作，测试访问控制方法的时间开销。

实验产生的箱体和分布图说明，在单位时间 100 次的流量压力下时间开销在 40 μs 处分布较多，上四分位数和下四分位数在 37~55 μs，异常情况导致的波动低于 100 μs。流量压力上升至 1000 次后没有给系统时间开销带来可见扰动。

图 6 呈现的是将访问地址作为要素进行的时间开销验证结果。该实验选择 0x03 功能码和 0x04 功能码对应的读取保持寄存器和读取输入寄存器作为对象。通过地址约束限制使用 0x03 功能

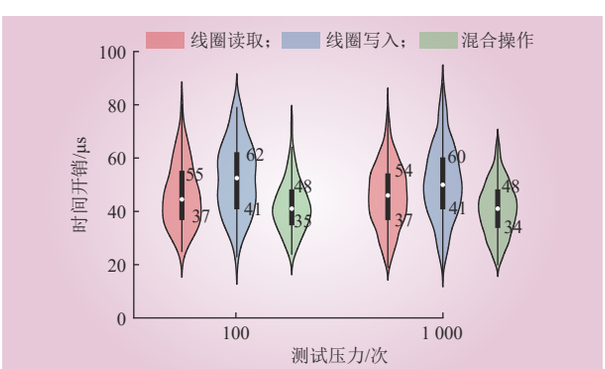

图 5　功能码访问控制时间开销

Fig. 5　Time consumption of function-code-based access control scheme

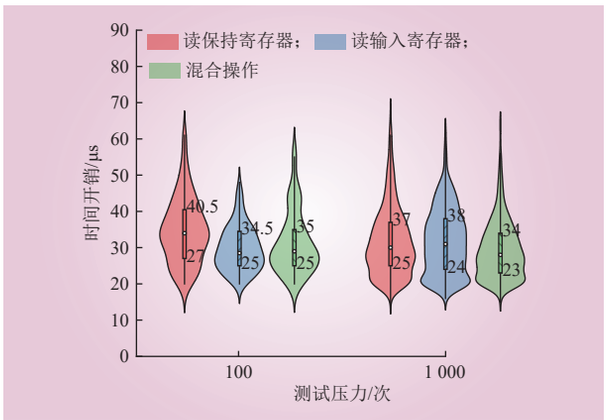

图 6 地址访问控制时间开销

Fig. 6 Time cost of address-based access control scheme

码访问 01 至 03 地址的保持寄存器，以及 0x04 功能码访问 00 至 01 地址的输入寄存器。

图 6 的实验结果表明，将访问地址作为因子其时间开销仍低于 100 μs。因此，2 种访问控制因子皆不会对 Modbus 设备的响应时间造成较大影响。与现有 Modbus TCP 安全方案中考虑时间开销的 2 种方案对比测试结果如表 3 所示，其中，文献 [12] 使用 SHA-2 算法生成数据摘要以保障消息完整性，并结合 RSA 签名算法确保消息来源于正确的发送方；文献 [15] 基于身份的访问控制技术（role based acess control，RBAC）和消息加密以确保身份安全和消息机密性及完整性。测试结果表明，本方案具有更低的时间开销。

表 3 安全方案时间开销对比

Table 3 Time consumption comparison

方案名	测试对象	平均时间开销/ms	标准差
SEM	0x01	0.045	0.012
RBAC[15]	0x01	0.440	0.230
Modbus TLS[12]	0x01	0.170	—

4 结语

本文针对分布式电源设备存在的通信安全问题，提出了一种非侵入式的电力 Modbus TCP 通信协议安全增强方法。为解决非侵入方法中间设备冗余的问题，提出基于电力云边协同的访问控制架构，由电力控制中心云平台管理访问控制策略，将实际的访问控制部署在边缘设备中，并利用 Modbus TCP 协议中的功能码组合时间因素以及访问的数据单元实现细粒度的访问控制。本文通过实验验证了所提方案的性能，实验结果表明，部署 SEM 的设备具有与老旧通信实体对等通信的能力，在时间开销上相较于现有方案有显著提升。总体而言，本方法在解决分布式电源应用场景下边缘设备通信安全问题有显著优势，且满足场景的实时性要求。本方法的不足之处在于，安全能力依赖于访问控制策略的优劣，未来将考虑如何基于历史行为等环境信息，最优化访问控制原则，实现访问权限动态调整。

参考文献：

[1] ORTIZ N, CARDENAS A A, WOOL A. A taxonomy of industrial control protocols and networks in the power grid[J]. IEEE Communications Magazine, 2023, 61(6): 21–27.

[2] OCHIAI H, HOSSAIN M D, CHIRUPPHAPA P, *et al*. Modbus/RS-485 attack detection on communication signals with machine learning[J]. IEEE Communications Magazine, 2023, 61(6): 43–49.

[3] SRIDHAR S, HAHN A, GOVINDARASU M. Cyber–physical system security for the electric power grid[J]. Proceedings of the IEEE, 2012, 100(1): 210–224.

[4] SALODKAR P, NANDANWAR S, SAWARKAR S. Communication between energy meters and PLC based on modbus protocol[C]//2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). Delhi, India. IEEE, 2023: 1–7.

[5] MOHAMMED A S, SAXENA N, RANA O. Wheels on the modbus - attacking ModbusTCP communications[C]//Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks. San Antonio TX USA. ACM, 2022: 288–289.

[6] 杨国泰, 王宇飞, 罗剑波, 等. 电力 CPS 信息网络脆弱性及其评估方法 [J]. 中国电力, 2018, 51(1): 83–89.
YANG Guotai, WANG Yufei, LUO Jianbo, *et al*. Electric CPS information network vulnerability and assessment method[J]. Electric Power, 2018, 51(1): 83–89.

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

[8] ZHANG Z Y, DENG R L, YAU D K Y, *et al*. Analysis of moving target defense against false data injection attacks on power grid[J].

IEEE Transactions on Information Forensics and Security, 2020, 15: 2320–2335.

[9] 何金栋, 王宇, 赵志超, 等. 智能变电站嵌入式终端的网络攻击类型研究及验证 [J]. 中国电力, 2020, 53(1): 81–91.
HE Jindong, WANG Yu, ZHAO Zhichao, *et al*. Type and verification of network attacks on embedded terminals of intelligent substation[J]. Electric Power, 2020, 53(1): 81–91.

[10] ZHANG Z Y, DENG R L, YAU D K Y, *et al*. Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid[J]. IEEE Internet of Things Journal, 2021, 8(8): 6608–6623.

[11] DENG R L, XIAO G X, LU R X, *et al*. False data injection on state estimation in power systems —attacks, impacts, and defense: a survey[J]. IEEE Transactions on Industrial Informatics, 2017, 13(2): 411–423.

[12] FOVINO I N, CARCANO A, MASERA M, *et al*. Design and implementation of a secure modbus protocol[M]//IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 83–96.

[13] YI F M, ZHANG L, YANG S M, *et al*. A security-enhanced modbus TCP protocol and authorized access mechanism[C]//2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). Shenzhen, China. IEEE, 2021: 61–67.

[14] FERST M K, DE FIGUEIREDO H F M, DENARDIN G, *et al*. Implementation of secure communication with modbus and transport layer security protocols[C]//2018 13th IEEE International Conference on Industry Applications (INDUSCON). São Paulo, Brazil. IEEE, 2018: 155–162.

[15] FIGUEROA-LORENZO S, AÑORGA J, ARRIZABALAGA S. A role-based access control model in modbus SCADA systems. A centralized model approach[J]. Sensors (Basel), 2019, 19(20): E4455.

[16] HUPP W, HASANDKA A, DE CARVALHO R S, *et al*. Module-OT: a hardware security module for operational technology[C]//2020 IEEE Texas Power and Energy Conference (TPEC). College Station, TX, USA. IEEE, 2020: 1–6.

[17] LIN Y C, LIN C F, CHEN K H. Security enhancement of industrial Modbus message transmission with proxy approach[C]//2021 IEEE 3rd Eurasia Conference on IOT, Communication and Engineering (ECICE). Yunlin, Taiwan, China. IEEE, 2021: 90-95.

[18] 高魏轩. 基于 Modbus 协议的工业控制系统信息安全主动防御系统设计与实现 [D]. 西安: 西安电子科技大学, 2018: 1–81.
GAO Weixuan. Design and implementation of industrial control system information security active defense system based on Modbus protocol[D]. Xi'an: Xidian University, 2018: 1–81.

[19] KATULIC F, SUMINA D, ERCEG I, *et al*. Enhancing modbus/TCP-based industrial automation and control systems cybersecurity using a misuse-based intrusion detection system[C]//2022 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM). Sorrento, Italy. IEEE, 2022: 964–969.

[20] 王林浩, 吴桂初, 戴翀, 等. 智能断路器中 Modbus/TCP 协议的实时性能测试 [J]. 中国电力, 2015, 48(12): 6–11.
WANG Linhao, WU Guichu, DAI Chong, *et al*. Research and testing of real-time performance of modbus/TCP protocol[J]. Electric Power, 2015, 48(12): 6–11.

[21] 席禹, 林冬, 于力, 等. 一种基于生物特征的电力系统安全认证协议 [J]. 广东电力, 2022, 35(10): 83–90.
XI Yu, LIN Dong, YU Li, *et al*. Biometric based security authentication protocol for power system[J]. Guangdong Electric Power, 2022, 35(10): 83–90.

[22] 杨晋祥, 彭勇刚, 蔡田田, 等. 面向边缘计算的电力终端轻量级认证协议 [J]. 中国电力, 2023, 56(4): 88–94.
YANG Jinxiang, PENG Yonggang, CAI Tiantian, *et al*. Power terminal lightweight authentication protocol for edge computing[J]. Electric Power, 2023, 56(4): 88–94.

[23] 程钎, 陈羽, 孙伶雁. 考虑服务配置的细粒度电力任务云边协同优化调度策略 [J]. 电力系统保护与控制, 2023, 51(7): 53–62.
CHENG Qian, CHEN Yu, SUN Lingyan. Cloud-edge collaborative optimization scheduling strategy for fine-grained power tasks considering service configuration[J]. Power System Protection and Control, 2023, 51(7): 53–62.

[24] 彭鹏, 薛东. 基于边缘代理的云边协同物联网框架设计及其应用研究 [J]. 广东电力, 2023, 36(5): 18–26.
PENG Peng, XUE Dong. Research on design of cloud side collaborative IOT framework based on edge agent and its application[J]. Guangdong Electric Power, 2023, 36(5): 18–26.

[25] 刘林彬, 苗泉强, 李俊娥. 基于模糊测试的 GOOSE 协议解析漏洞挖掘方法 [J]. 中国电力, 2022, 55(4): 33–43.
LIU Linbin, MIAO Quanqiang, LI June. A method for mining GOOSE protocol parsing vulnerabilities based on fuzzing[J]. Electric Power, 2022, 55(4): 33–43.

[26] The Modbus Organization. Modicon modbus protocol reference

guide[EB/OL]. (1996-06)[2023-10-25]. https://modbus.org/docs/PI_MBUS_300.pdf.

作者简介：

何涂哲秋（1999—），男，硕士研究生，从事控制系统协议安全分析与逆向工程研究，E-mail：auyuwhale@gmail.com；

张镇勇（1991—），男，通信作者，博士，教授，从事信息物理系统安全、工控系统安全、智能电网安全、人工智能安全等科研工作，E-mail：zyzhangnew@-gmail.com。

（责任编辑　李博）

A Non-intrusive Method for Enhancing the Security of Modbus TCP Protocol Based on Cloud-Edge Collaboration in Distributed Resources

HETU Zheqiu[1], XU Zidong[1], CHE Xin[2], ZHANG Zhenyong[1]

(1. State Key Laboratory of Public Big Data (College of Computer Science and Technology, Guizhou University), Guiyang 550025, China;
2. State Key Laboratory of Industrial Control Technology and College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: The security problem of data transmission from smart edge devices in distributed resources (DR) brings hidden risks for power system. The Modbus TCP (transmission control protocol) is a commonly used communication method for edge devices, but its flawed security design makes the system vulnerable to cyber-attacks. In this paper, based on a review of the existing security methods, we analyzed their shortcomings under DR application scenarios, and proposed a non-intrusive Modbus TCP security enhancement method. The method adopts an architecture of cloud-edge collaboration, and uses the cloud platform of the power control center to manage access control principles, and deploys the actual access control module in the edge devices to restrict malicious behaviours through fine-grained access control combinations. Finally, based on the Modbus protocol reference guide, a DR application scenario was built for penetration testing. It was proved that the proposed method can effectively defend against the replay attacks and man-in-the-middle attacks in this scenario, and the time cost is within a hundred microseconds.

This work is supported by National Natural Science Foundation of China (A Defense Framework Against the Coordinated Cyber-physical Attack on Load Frequency Control, No.62303126，A Privacy Preserving Neural Network with Multi-source Encrypted Data, No.62362008)，Guizhou Provincial Science and Technology Projects (Research on Cyber-Physical Attack and Defense of State Estimation in Smart Grid, No.ZK[2022]149), Guizhou Provincial Research Project (Youth) for Universities under grant (Research on the Vulnerability of Power Grid Stability Assessment System Empowered by Big Data, No.[2022]104).

Keywords: Modbus TCP protocol; protocol security; distributed resources; access control