

## 基于国密的工控低算力设备身份认证与群组认证方案

孙建军<sup>1</sup>, 李昕泽<sup>2</sup>, 李伟<sup>1</sup>, 李焕<sup>1</sup>, 杨澜<sup>1</sup>, 曹进<sup>2</sup>

(1. 新疆油田公司数智技术公司, 新疆 克拉玛依 834000; 2. 西安电子科技大学, 陕西 西安 710126)

**摘要:** 工业控制网络系统是现代工业生产的重要组成部分, 具有高实时性、高可靠性和资源受限等特点, 广泛应用于制造业、能源、交通等关键领域。然而, 其安全性问题日益突显, 尤其是基于Modbus总线的通信系统, 该协议采用明文传输, 缺乏加密或认证机制, 导致攻击者一旦获得总线访问权限, 便能轻易实施数据窃取、篡改或重放攻击, 严重威胁通信设备的正常运行, 甚至危及产业及人员安全。针对工业控制网络中节点资源受限、总线带宽不足以及安全需求迫切等问题, 基于中国商用密码算法提出了一种轻量化的节点身份认证及群组认证方案, 充分利用了Modbus通信协议的广泛适用性, 通过哈希运算和对称加密等轻量化操作, 实现了基于节点ID的订阅群组身份认证和会话密钥协商。性能分析表明, 在计算开销和通信开销方面均优于现有方案, 并可基于现有Modbus总线硬件设备, 以较小的改动集成到现有工业控制系统中。此外, 通过形式化验证工具Scyther对方案的安全性进行了全面验证, 证明其能够满足双向认证、密钥协商和抗重放攻击等安全目标, 有效抵御多种网络攻击。

**关键词:** 身份认证; 群组认证; 工业控制网络; Modbus总线

**中图分类号:** TP393

**文献标志码:** A

**DOI:**10.11959/j.issn.2096-109x.AQ25225

## An identity and group authentication scheme for resource-constrained industrial control devices based on Chinese commercial cryptography

Sun Junjun<sup>1</sup>, Li Xinze<sup>2</sup>, Li Wei<sup>1</sup>, Li Huan<sup>1</sup>, Yang Lan<sup>1</sup>, Cao Jin<sup>2</sup>

1. Xinjiang Oilfield Company Digital Intelligence Technology Company, Karamay 834000, China

2. Xidian University, Xi'an 710126, China

**Abstract:** Industrial control network systems are regarded as critical components of modern industrial production, characterized by high real-time performance, high reliability, and resource constraints. They are widely used in key sectors such as manufacturing, energy, and transportation. However, their security issues have become increasingly prominent, especially in Modbus-based communication systems. In this protocol, data are transmitted in plaintext without encryption or authentication mechanisms. Once access to the bus is obtained by attackers, data theft, tampering, or replay attacks can be easily executed, seriously threatening the normal operation of communication devices and even endangering industrial operations and personnel safety. To address the issues of limited node resources, insufficient bus bandwidth, and urgent security requirements in industrial control networks, a lightweight node identity authentication and group authentication scheme based on Chinese commercial cryptographic algorithms was proposed. In this scheme, full advantage was taken of the widespread applicability of the Modbus communication protocol. By utilizing lightweight operations such as hash functions and symmetric encryption, subscrip-

收稿日期: 2025-08-26; 修回日期: 2026-03-19

通信作者: 李昕泽, 24151213813@stu.xidian.edu.cn

tion group identity authentication and session key negotiation based on node ID were implemented. Performance analysis showed that it outperformed existing solutions in terms of both computational and communication overhead. Moreover, it could be integrated into existing industrial control systems with minimal changes to the current Modbus bus hardware. Additionally, the security of the scheme was thoroughly verified using the formal verification tool Scyther, and it was demonstrated that the scheme met security objectives such as bidirectional authentication, key negotiation, and resistance to replay attacks, effectively defending against various network attacks.

**Key words:** identity authentication, group authentication, industrial control network, Modbus bus

## 0 引言

在现代石油和天然气工业中,工业控制(简称工控)系统(industrial control system, ICS)是保障生产安全、提高生产效率的核心基础设施,尤其是在新疆油田等重要能源生产基地,保障工业控制网络的稳定性和安全性对国家能源安全和经济发展具有重要意义。随着设备间互联互通的不断加深,工业控制系统暴露在更为开放的网络环境中,进而面临诸如非法访问、数据篡改、拒绝服务攻击等网络安全威胁。Modbus<sup>[1]</sup>是一种广泛应用于工业自动化领域的通信协议,主要用于工业设备之间的数据传输和控制。它采用主从架构,支持多种通信方式,包括串行通信(如 RS-232、RS-485)和以太网通信(如 Modbus TCP)。Modbus 结构简单、易于实现且成本低廉,因此在可编程逻辑控制器(programmable logic controller, PLC)、远程终端(remote terminal unit, RTU)、传感器等设备间的通信中被广泛使用,是确保工业控制系统和监控与数据采集(supervisory control and data acquisition, SCADA)系统稳定运行的关键。

然而,在以 Modbus 协议为核心的工业控制网络中,由于协议本身缺乏安全机制,且数据以明文形式传输,设备间的通信极易受到攻击,威胁系统的整体安全性。然而,安全防护措施大多依赖于设备的计算能力和网络设备的安全认证机制,对设备资源要求较高。在低算力设备(如传感器、执行器、PLC 等)广泛部署的工业环境中,带宽、存储和功耗受到限制,这使得许多主流的身份认证和加密技术无法在这些设备上应用。此外,现有研究主要集中在 Modbus 通信的加密与访问控制层面,但仍存在轻量级安全机制与实时性平衡、协议安全扩展的通用性,以及对攻击检测与溯源机制缺乏系

统性研究等关键科学问题。基于 Modbus 实现高效的身份认证和群组认证,以确保设备的可信性和通信的安全性,已成为保障油田生产安全的核心目标。

与传统的国际标准加密算法相比,中国商用密码算法(商用密码算法标识 SM 系列,包括 SM2、SM3、SM4 等)在安全性上具备等效性,具备自主可控的优势,能够有效规避对国外加密技术的依赖,适用于资源受限的设备和网络环境。SM3 是一个高效的哈希算法,适合用于数据完整性校验和数字签名;SM4 作为对称加密算法,能够为数据传输提供强有力的机密性保障。

基于上述背景,本文提出了一种基于中国商用密码算法的轻量化节点身份认证与群组认证方案,并将其应用于 Modbus 通信协议中,用于应对传统工业控制网络中低算力设备在身份认证和群组认证方面面临的挑战。本文利用 SM3 确保数据的完整性,利用 SM4 进行数据加密保护。通过这一方案,不仅能够保证设备身份认证的安全性和可靠性,还能大幅降低设备对计算资源的需求,从而满足传统工业控制系统对安全性和效率的双重需求。本文的主要研究工作如下。

1) 提出了一种基于 Modbus 总线的统一身份管理机制和功能码扩展设计。在统一身份管理机制中,通过对域 ID 和节点 ID 进行组合,实现了对单一从节点和群组节点的身份管理,为身份认证和密钥协商提供了基础支持。同时,通过对 Modbus 功能码的自定义扩展,满足了数据加密、完整性校验、跨域通信和身份认证等安全需求,在未改变原有协议架构和通信方式的基础上,通过在现有 Modbus 协议的功能码中添加扩展字段而不干扰原有 Modbus 协议的基本操作,并采用

可选的安全功能，避免了对现有设备硬件或固件的修改，确保了方案与现有Modbus硬件设备的兼容性。

2) 提出适用于Modbus TCP和Modbus RTU/ASCII的两节点及 $n$ 个节点间身份认证与会话密钥协商方案。该方案基于SM3以及SM4，通过预置密钥和随机数生成会话密钥，并利用基于哈希的消息认证码（Hash-based message authentication code, HMAC）实现双向认证。 $n$ 个节点间的群组认证通过广播机制实现，主节点与多个从节点协商群组密钥，确保群组内通信的安全性。

3) 仿真结果及安全分析表明，本文方案能够满足双向认证、密钥协商和抗重放攻击等安全目标，有效抵御多种网络攻击。与传统Modbus认证方案相比，本文方案在计算开销和通信开销方面具有明显优势，具有较高的适用性和可推广性。

## 1 预备知识

### 1.1 Modbus 总线

在工业自动化和控制系统中，Modbus总线是一种广泛应用的串行通信协议，最初由Modicon公司于1979年开发，用于其PLC系统。Modbus的设计目的是简化工业设备间的数据交换，其通信架构灵活，适用于多种应用场景。Modbus主要有两种类型：Modbus RTU和Modbus TCP。Modbus RTU通过串行通信（如RS-232、RS-485）实现数据传输，而Modbus TCP则基于以太网协议，将Modbus的报文通过TCP/IP网络传输。

Modbus的核心思想是主从式通信模式，即在一个通信网络中，主设备（如控制系统或计算机）负责发起请求，而从设备（如传感器、执行器等）则响应主设备的请求。数据交换是通过功能码指定的操作命令实现的，功能码涵盖了读取、写入寄存器、读写离散输入输出等多种操作。

Modbus的简单性和开放性使其成为工业控制领域中被广泛采用的标准协议。然而，由于其早期设计缺乏安全机制，Modbus在现代网络环境中暴露了诸多安全漏洞。例如，在数据传输过程中缺乏加密和身份认证机制，易受到恶

意攻击，如数据篡改、重放攻击等的威胁。因此，尽管Modbus在工业控制系统中仍具有广泛应用，但其安全性问题已成为研究和改进的重点。

### 1.2 国家密码算法

国家密码算法（简称国密）是我国为保障信息安全而制定的自主可控的密码算法体系，旨在替代传统的国际密码算法，如高级加密标准（AES）、RSA等，并满足国内信息安全需求。国密涵盖了多种加密技术，包括对称加密、非对称加密、哈希算法及数字签名等多个领域，具有较高的安全性和适应性，已成为国家信息安全标准的重要组成部分。

SM3和SM4是国家密码算法体系中的核心算法，分别用于消息摘要和对称加密，广泛应用于中国的政府和企业信息安全领域。它们是根据GB/T 32905—2016开发的，旨在为国内信息安全提供自主可控的加密技术。

SM3是一种哈希算法，用于生成固定长度（256位）的消息摘要。SM3通过迭代处理输入消息，结合复杂的非线性函数和加密操作，确保其抗碰撞性和抗预映像攻击能力。SM3被广泛应用于数字签名、消息认证码（MAC），以及数据完整性校验等场景，作为一种高效且安全的哈希函数，其已被中国多个重要标准所采纳，并在金融、政府及通信领域中得到了广泛应用。

SM4是一种对称加密算法，采用128位密钥，支持数据的加解密操作。SM4的设计基于Feistel结构，类似于国际上广泛使用的AES，但其加密轮数和密钥长度等细节与AES有所不同。SM4使用固定的128位块大小和32轮的迭代加密结构，具有较高的抗攻击性。由于其简单且高效的实现，SM4在我国的无线通信、电子支付以及电子政务等领域中得到了广泛应用，成为我国自主可控的信息加密标准。

总体而言，SM3和SM4不仅提升了中国在密码学领域的自主创新能力，还在实际应用中发挥了重要的安全保障作用。随着信息安全需求的不断增加，SM3和SM4的应用范围逐步扩大，并逐渐成为国内外信息系统中的重要加密基础设施<sup>[2]</sup>。

## 2 相关工作

由于广泛部署的 Modbus 本身缺乏安全机制, Modbus 的安全性近年来一直备受关注<sup>[3]</sup>。现有研究提出了不同的方法解决与 Modbus 有关的安全问题, 并提出了各种身份认证方法, 以增强 Modbus 传输的安全性。Shahzad 等<sup>[4]</sup>的研究强调了加密技术在客户端/服务器架构中作为安全机制的重要性, 并针对 Modbus 提出了一种新的安全方案。Nardone 等<sup>[5]</sup>对 Modbus 进行了安全评估, 并证明了基于 Modbus 的系统中存在中间人攻击。Rajesh 等<sup>[6]</sup>提出了一种增强 Modbus 安全性的新方法, 主要聚焦于 ICS 中的数据采集服务器。You 等<sup>[7]</sup>提出了一种基于 Modbus 的智能建筑安全系统, 通过集成感知、控制和管理功能, 实现了高效的数据通信和资源管理, 并通过网页控制端实现了环境监测和安全检测。Martins 等<sup>[8]</sup>提出增强版 Modbus TCP 安全协议并新增认证、授权自定义功能, 针对工业 Modbus 协议缺乏基础安全机制、易受网络攻击且无法实现细粒度访问控制的问题, 给出了实现人员身份验证、权限管控的可行性。此外, Figueroa-Lorenzo 等<sup>[9]</sup>提出了一种基于 Hyperledger Fabric 区块链的去中心化身份管理解决方案, 以提升 Modbus 的安全性, 同时确保其简单性、兼容性和互操作性。此外, Gamess 等<sup>[10]</sup>评估了 Modbus TCP 在正常运行和分布式拒绝服务 (distributed denial of service, DDoS) 攻击下的性能。Phillips 等<sup>[11]</sup>的研究探讨了在使用 Modbus 的监控与数据采集 (SCADA) 系统中应用机器学习技术进行异常检测的重要性, 强调了检测针对 SCADA 系统的新型安全威胁的必要性。

针对 Modbus 缺乏认证的问题, Hayes 等<sup>[12]</sup>提出了一种新颖的 Modbus 替代方案, 该替代方案利用基于哈希的消息认证码 (HMAC) 和流传输控制协议来确保安全和向后兼容的 Modbus 消息传输。这种改进包括一种相互认证机制, 以确保 Modbus 消息的可用性和完整性。Keliris 等<sup>[13]</sup>提出了一种基于 Modbus 的工业设备指纹识别方法, 利用供应商实现差异和协议缺乏身份认证的特点, 成功识别了 308 个设备的品牌和型号。Pricop 等<sup>[14]</sup>专注于开发一种通过 Modbus TCP 进行身份认证传感器的创新方法, 强调了安全性在

工业控制系统中的重要性, 并强调了安全身份认证机制保护 Modbus 网络传输的敏感数据的必要性。Luo 等<sup>[15]</sup>引入了一个名为 Modbus-E 的安全协议, 以解决 Modbus TCP 的安全问题。通过白名单过滤方法, Modbus-E 确保指令的可控性, 而不需要增加通信过程的复杂性, 实现了安全通信。Figueroa-Lorenzo 等<sup>[16]</sup>为 Modbus SCADA 系统提出了一个基于角色的访问控制模型, 以解决安全认证的问题。这种集中的模型方法旨在授权客户、服务器, 以及 Modbus 框架, 以增强工业通信系统的整体安全性。Bernieri 等<sup>[17]</sup>提出了 Tambus 方法, 通过在 Modbus TCP 中利用基于存储和基于计时的秘密通道实现发射机身份认证和数据包完整性, 既保持了与旧设备的兼容性, 又能在低开销下检测攻击, 实验证明其在工业环境中具有高准确性和可行性。李环<sup>[18]</sup>通过优化祖冲之 256 算法, 设计出基于该算法的 Modbus TCP 安全数据传输模型, 实现数据加密、完整性验证等多项安全功能, 但模型仅在 OpenPLC 模拟环境中验证, 未在实际工业场景中测试。

Liao 等<sup>[19]</sup>提出基于哈希链和自定义压缩函数的密码学认证方案, 针对 Modbus 协议无安全机制、主设备易被伪造且从设备资源受限的问题, 通过初始化哈希链、指令签发验证及存储值刷新的流程, 实现了主设备身份认证且将从设备存储开销降至  $O(1)$ , 兼顾安全性与资源效率。Katulić 等<sup>[20]</sup>提出了一种利用 MAC 来保护基于 Modbus TCP 的工业自动化和控制系统方案。该方法通过基于 MAC 进行完整性保护增强了网络安全性, 且不需要对硬件或固件进行任何修改。Alsabbagh 等<sup>[21]</sup>揭示了 Modbus 在 SCADA 系统中的安全漏洞, 提出了一种错误命令注入的攻击方法, 通过嗅探和数据库重放掩盖攻击行为, 可能导致灾难性后果, 并提出了相应的安全措施建议以防止此类严重威胁。Guo 等<sup>[22]</sup>提出了一种基于可信密码模块 (trusted cryptography module, TCM) 和数字信封技术的可信 Modbus TCP, 通过实验证明该协议在满足工业控制系统高实时性要求的同时, 保障了消息完整性和机密性。王英州等<sup>[23]</sup>提出了一种结合报警时间与频率相关性量化、报警量分类的工控系统物理层报警关联算法, 实现

了贴合真实工艺流程的报警关联结构构建与报警源头追溯。王红敏等<sup>[24]</sup>量化工控系统风险传播速度、明确传播范围边界,结合最优控制理论提出防控策略,为风险精准管控提供理论支撑。综上,现有的研究突出了Modbus身份认证在保护工业控制系统和SCADA系统中的重要性,提出了各种身份认证方法,例如基于哈希的消息身份认证代码,基于角色的访问控制模型以及无证书的签名身份认证方案,以解决与Modbus相关的安全挑战,确保通过Modbus网络传输的数据的机密性、完整性和可用性。

### 3 系统模型和安全模型

#### 3.1 系统模型

本节描述本文的系统模型,模拟典型的工业自动化控制系统架构,如图1所示,主要包括以下实体。

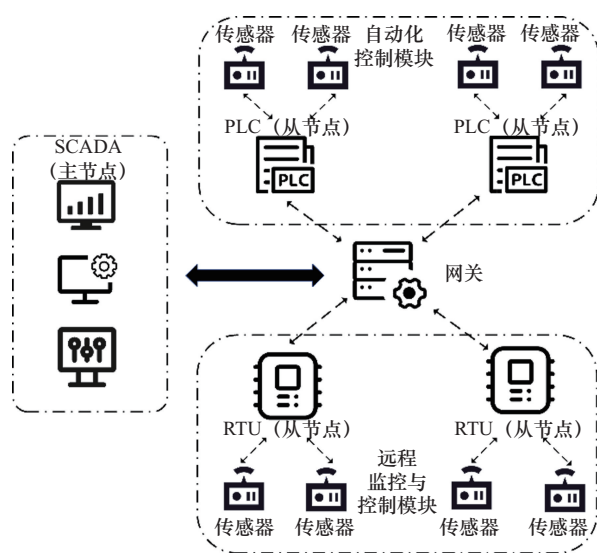


图1 工业控制网络场景

1) SCADA系统: SCADA系统用于监控和控制整个工业过程,负责从PLC/RTU和其他设备中收集数据,并提供用户界面供操作员进行监控和控制。

2) 自动化控制模块: 负责自动化的任务执行、数据采集与处理,在大型工业控制系统中,多个PLC和传感器组成分布式控制单元。每个分布式控制单元负责某个区域或某些设备的控制,通过网络连接协调全系统的工作。

3) 远程监控与控制模块: 此模块允许操作员从远程位置监控和控制整个系统,进行现场数据采集和控制任务,并通过通信网络与上层系统对接。

4) 网关: Modbus网关可以连接不同类型的Modbus网络,确保数据在不同协议之间的转换传输。

5) PLC: PLC是工业自动化中常用的控制设备,用于执行具体的控制逻辑和操作,通常与传感器和执行器连接,以实现对设备的精确控制。

6) RTU: RTU通常用于远程监控和控制,可以收集数据并将其传输到中央控制系统。

7) 传感器: 传感器用于收集环境或设备的数据,如温度、压力、湿度等。

基于上述实体,本节提出以下系统模型。

1) Modbus主节点是发起Modbus请求的设备。本文假设SCADA系统是信任的,并充当主节点。SCADA系统向Modbus从节点发送请求并等待响应。主节点具有与多个从节点通信的能力,并且可以向每个从节点请求不同类型的数据。

2) Modbus从节点是等待Modbus主节点请求的设备。本文假设PLC与RTU充当从节点,一旦收到请求,从节点将处理该请求并将响应发送回主节点。从节点不主动发起通信,仅响应来自主节点的请求。

3) PLC和RTU被视为不可信的设备。此外,Modbus通信信道是公开的,明文传输的通信过程中可能存在安全风险。

4) 本文主要聚焦于SCADA系统与PLC/RTU之间的通信和认证安全问题。网关主要负责消息的传递,因此不在本文的重点关注范围内。同时,PLC/RTU与传感器之间的数据采集过程也不在本文的研究范围内。

#### 3.2 敌手模型和安全目标

本文采用Dolev-Yao攻击模型。在典型的Dolev-Yao模型中,攻击者可以完全控制通信信道,具备以下攻击能力。

1) 窃听攻击: 敌手通过监听网络通信,非法获取系统中传输的数据或敏感信息。在传统工业控制网络中,窃听可以导致重要的控制指令、设

备状态、传输的数据甚至密钥被泄露，严重威胁到系统的机密性和完整性。

2) 伪造攻击：敌手伪装成合法设备或用户，通过伪造消息、身份或证书，试图欺骗系统接受恶意请求。在传统工业控制网络中，伪造攻击可能导致恶意设备被允许接入系统，从而破坏网络的安全性，甚至导致控制指令被非法修改或执行。

3) 重放攻击：攻击者通过捕获合法的通信报文，并在稍后某个时间点重新发送此报文，进而影响系统的正常运行。在 Modbus 中，攻击者可能通过监听和记录传输中的控制指令或状态更新信息，并在后续发送这些报文来干扰系统的操作。

4) 篡改攻击：攻击者通过修改或篡改传输中的通信报文，插入恶意指令或非法数据，破坏报文的完整性。在工业控制网络中，尤其是使用明文通信的 Modbus 系统，缺乏足够的加密和认证机制，这使得数据在传输过程中易受到篡改的威胁。

5) 中间人 (man-in-the-middle, MITM) 攻击：攻击者通过控制或监听通信网络，将自己伪装成通信双方中的一方，从而拦截、篡改或伪造数据传输。在工业控制网络中，MITM 攻击可能对 Modbus 等协议的安全性构成重大威胁，尤其是在没有加密保护的情况下，攻击者可以轻易地拦截和操控数据流。

因此，设计的安全方案需要有效抵御这些威胁，确保系统的可靠性与机密性。针对潜在的攻击威胁，本文需实现以下 6 个关键安全目标。

1) 个人计算机 (PC) 和 PLC/RTU 双向认证：应实现 PC 和 PLC/RTU 间的双向身份认证，抵抗伪造攻击，确保只有合法设备才能加入网络并进行通信。

2) 安全密钥分发：应实现 PC 和 PLC/RTU 之间的安全密钥分发，避免密钥泄露或遭到截获。

3) 抵御重放攻击：应能抵抗重放攻击，确保每一条消息都是唯一且在时效期内。

4) 消息机密性：应能保障消息机密性，抵抗窃听攻击。

5) 消息完整性：应保障消息完整性，抵抗篡

改攻击。

6) 抵御中间人攻击：应能抵抗中间人攻击，确保攻击者无法伪装成通信双方中的一方，从而拦截、篡改或伪造数据传输。

## 4 统一身份管理与认证机制方案设计

本文针对 Modbus 总线缺乏安全机制的问题，提出了一种 Modbus 总线节点的统一身份管理机制，为每个设备分配唯一标识符（唯一地址）。基于此机制，设计了一种适用于 Modbus TCP 和 Modbus RTU 的身份认证方法，通过引入自定义功能码，提出了两节点身份认证方案和  $n$  个节点群组身份认证方案，实现了上位机与 PLC、RTU 设备之间的双向认证与安全密钥协商。表 1 为系统参数符号对照。

表 1 系统参数符号对照

| 参数           | 含义            |
|--------------|---------------|
| $K_{pre,1}$  | 预置密钥          |
| $R_i$        | 节点 $i$ 生成的随机数 |
| MID          | 节点地址          |
| $F_{enc}()$  | 加密操作          |
| $F_{dec}()$  | 解密操作          |
| $K_{sess,1}$ | 会话密钥          |
| KDF()        | 密钥派生函数        |
| AUTH         | 消息认证码         |
| XAUTH        | 计算消息认证码操作     |
| $F_{mac}()$  | 计算 MAC 操作     |

### 4.1 统一身份管理机制

结合 Modbus 总线报文格式，参与工控网络数据传输的从节点在主节点的协助下完成工控网络安全通信控制的节点身份注册，具体步骤如下。每个设备的节点地址，由 1 字节共 8 bit 的数据表示，即由域 ID (3 bit) 和节点 ID (5 bit) 表示。

1) 编码长度 8 bit，前 3 bit 表示所在域（可以为单一从节点，或多个从节点组成的关键群组），后 5 bit 表示节点序号。

2) 采用十六进制表示，如 0x41——01000001 表示 010 域节点 ID 为 00001 的从节点。

3) 主节点作为特殊节点, 可使用特殊的节点地址进行标识, 由3位域ID (3 bit) 和5位0 (5 bit) 组成。

结合当前 Modbus 总线报文格式标准, 本文将 Modbus 总线报文的功能码域进一步自定义功能, 并根据不同协议进行介绍。

#### 4.1.1 Modbus TCP

Modbus TCP 中, 数据帧由3个部分组成: Modbus 应用协议报文头 (MBAP)、协议数据单元 (PDU) 和校验码。其中, MBAP 长度为7字节, 由事务处理标识、协议标识符、长度以及单元标识符组成; PDU 由功能码和数据字段组成, 功能码长度为1字节, 数据字段长度不定; 校验码负责对报文的数据进行校验, 长度为2字节。MBAP 格式见表2, Modbus TCP 报文格式如图2所示。

表2 MBAP 格式

| 字段名称   | 字段长度 | 字段含义                  |
|--------|------|-----------------------|
| 事务处理标识 | 2字节  | 报文的序列号                |
| 协议标识符  | 2字节  | 0x0000, 指代 Modbus TCP |
| 长度     | 2字节  | 表示接下来的报文的总长度, 单位为字节   |
| 单元标识符  | 1字节  | 接收报文的从节点地址            |

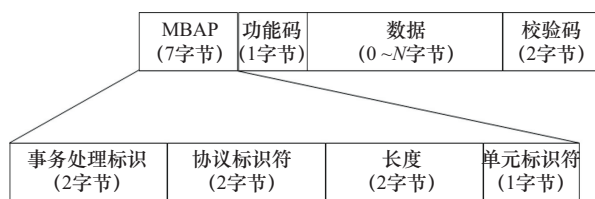


图2 Modbus TCP 报文格式

新的报文格式对功能码自定义后可满足系统全部需求, 具体如下。

1) 事务处理标识字段, 长度为2字节, 指示报文的序列号, 主设备发起的每次事务处理标识应该具有唯一性, 用于区分不同请求。

2) 协议标识符字段, 长度为2字节, 指示该报文所属的协议, 在 Modbus TCP 中, 该字段一般值为 0x0000, 指代 Modbus TCP。

3) 长度字段, 长度为2字节, 表示该字段后的剩余报文长度 (包括数据字段)。

4) 单元标识符字段, 长度为1字节, 表示该

报文的接收从节点的节点地址, 包括3 bit 的域ID和5 bit 的节点ID。

PDU 共包括两个部分: 功能码和数据。功能码长度为1字节, 指示该报文的操作类型, 例如读取保存寄存器、写入单个寄存器或者多个寄存器等。为了实现数据分级保护以及完整性保护等功能, 本文依托 Modbus 标准<sup>[1]</sup>预留了可自定义功能码的特性, 对协议中未被使用的功能码进行了自定义设计和功能扩展, 具体见表3。

表3 自定义功能码

| 功能码 | 十六进制 | 含义                              |
|-----|------|---------------------------------|
| 101 | 0x65 | 将数据以明文形式发送并读/写入寄存器              |
| 102 | 0x66 | 数据加密后发送, 经过解密后读/写入寄存器           |
| 103 | 0x67 | 数据通过完整性保护检验后读/写入寄存器             |
| 104 | 0x68 | 将数据加密传输, 并通过解密以及完整性校验后读/写入寄存器   |
| 105 | 0x69 | 跨域将数据以明文形式发送并读/写入寄存器            |
| 106 | 0x6a | 跨域将数据加密发送, 解密后读/写入寄存器           |
| 107 | 0x6b | 跨域将数据通过完整性校验后读/写入寄存器            |
| 108 | 0x6c | 跨域将数据加密传输, 并通过解密以及完整性校验后读/写入寄存器 |
| 109 | 0x6d | 身份认证以及密钥协商过程                    |
| 65  | 0x41 | 域内授权                            |
| 66  | 0x42 | 跨域授权                            |

#### 4.1.2 Modbus RTU/ASCII

Modbus RTU 和 Modbus ASCII 基本相同, 主要的差异在于校验、起始字段和数据表示。因此本文不将两种方案分别讨论, 以 Modbus RTU/ASCII 统称。

在 Modbus RTU/ASCII 中, 报文格式主要由设备地址、功能码、数据以及校验码4个部分组成。设备地址和功能码两个字段的长度都是1字节。其中设备地址字段与 Modbus TCP 中的单元标识符字段类似, 功能码字段的自定义部分同 Modbus TCP。数据字段长度不定。Modbus RTU

中, 校验码为循环冗余校验 (CRC) 码, 共 2 字节; Modbus ASCII 中, 校验码为纵向冗余校验 (LRC) 校验码, 也为 2 字节。具体格式如图 3 所示。

| 设备地址<br>(1 字节) | 功能码<br>(1 字节) | 数据<br>(0~N 字节) | 校验码<br>(2 字节) |
|----------------|---------------|----------------|---------------|
|----------------|---------------|----------------|---------------|

图 3 Modbus RTU/ASCII 报文格式

## 4.2 两节点间身份认证及密钥协商

两节点间身份认证及会话密钥协商过程如图 4 所示。

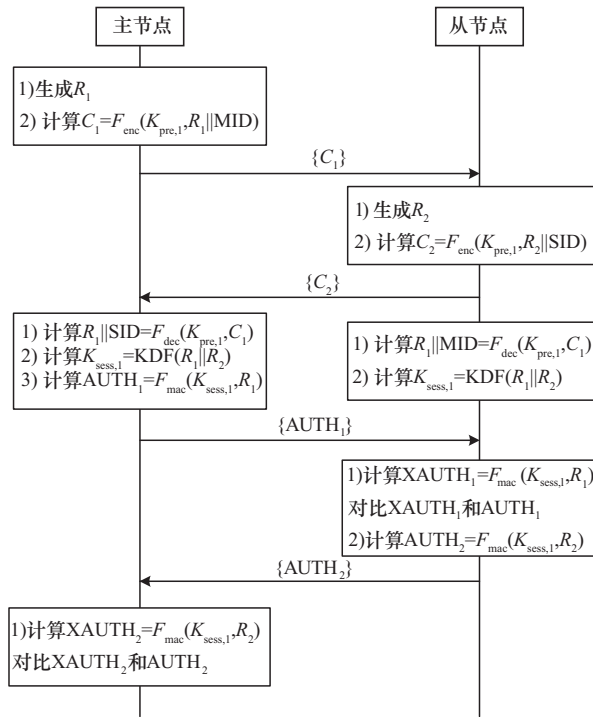


图 4 两节点间身份认证及会话密钥协商过程

### 4.2.1 两节点间的 Modbus TCP

记身份认证的两个节点为主节点与从节点。两节点间身份认证及密钥协商的步骤如下。

**步骤 1** 主节点生成随机数  $R_1$ , 并按照式(1), 使用预置密钥  $K_{pre,1}$  加密  $R_1$  和主节点的 MID 得到密文  $C_1$ , 将  $C_1$  放入 Modbus 报文数据帧中的数据域中, 发送给从节点。

$$C_1 = F_{enc}(K_{pre,1}, R_1 || MID) \quad (1)$$

**步骤 2** 从节点生成随机数  $R_2$ , 并按照式(2)使用预置密钥  $K_{pre,1}$  加密  $R_2$  和 SID 得到密文  $C_2$ , 将  $C_2$  放入 Modbus 报文数据帧中的数据域中, 返

回给主节点。

$$C_2 = F_{enc}(K_{pre,1}, R_2 || SID) \quad (2)$$

**步骤 3** 主节点收到  $C_2$  后, 按照式(3)使用预置密钥  $K_{pre,1}$  解密, 获得从节点的随机数  $R_2$ , 之后按照式(4)计算生成会话密钥  $K_{sess,1}$ 。从节点同理。

$$R_2 || SID = F_{dec}(K_{pre,1}, C_2) \quad (3)$$

$$K_{sess,1} = KDF(R_1 || R_2) \quad (4)$$

**步骤 4** 主节点使用会话密钥  $K_{sess,1}$  计算  $R_1$  的消息认证码  $AUTH_1$ , 如式(5)所示。之后, 将  $AUTH_1$  放入 Modbus 报文数据帧中的数据域中, 发送给从节点。

$$AUTH_1 = F_{mac}(K_{sess,1}, R_1) \quad (5)$$

**步骤 5** 从节点收到  $AUTH_1$  后, 计算  $XAUTH_1$ , 如式(6)所示, 并将  $XAUTH_1$  与  $AUTH_1$  进行比较, 相等则认证主节点身份,  $K_{sess,1}$  为协商的会话密钥。

$$XAUTH_1 = F_{mac}(K_{sess,1}, R_1) \quad (6)$$

**步骤 6** 从节点使用会话密钥  $K_{sess,1}$  计算  $R_2$  的消息认证码  $AUTH_2$ , 如式(7)所示。之后, 将  $AUTH_2$  放入 Modbus 报文数据帧的数据域中发送给主节点。

$$AUTH_2 = F_{mac}(K_{sess,1}, R_2) \quad (7)$$

**步骤 7** 主节点收到  $AUTH_2$  后, 计算  $XAUTH_2$ , 如式(8)所示。并与  $AUTH_2$  进行比较, 相等则认证从节点身份,  $K_{sess,1}$  为协商的会话密钥。

$$XAUTH_2 = F_{mac}(K_{sess,1}, R_2) \quad (8)$$

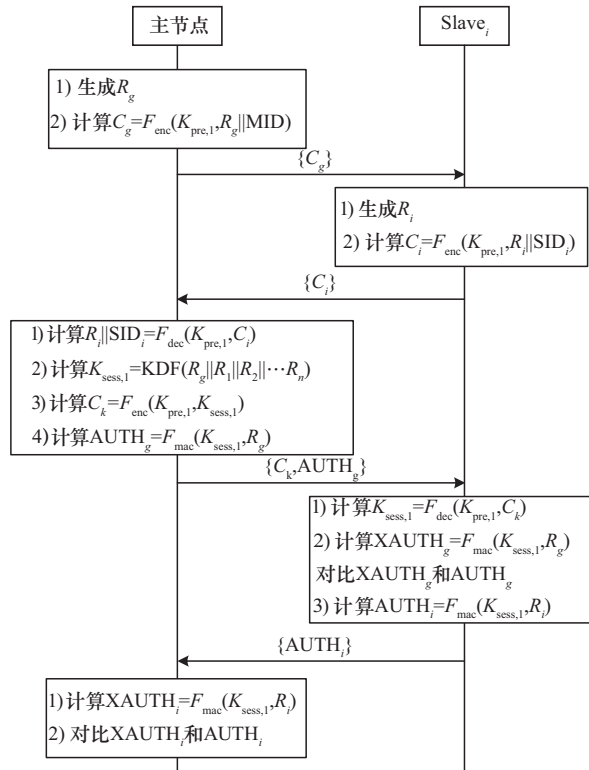
其中, Modbus TCP 安全认证协议基于对称密码算法实现, 使用 SM4 加密或解密, SM3 生成或验证消息认证码。

### 4.2.2 两节点间的 Modbus RTU/ASCII

Modbus RTU/ASCII 的两节点间安全认证流程与 Modbus TCP 类似, 尽管通信协议和传输方式有所不同, 但两者的身份认证及会话密钥协商过程基本一致, 确保了通信的安全性和可靠性。

## 4.3 n 个节点间身份认证及密钥协商

n 个节点间身份认证及会话密钥协商过程如图 5 所示。

图5  $n$  个节点间身份认证及会话密钥协商过程

#### 4.3.1 $n$ 个节点下的 Modbus TCP

主节点 Master 与域内  $n$  个从节点 Slave <sub>$i$</sub>  进行认证,  $i \in [1, n]$ ,  $n \geq 3$ 。  $n$  个节点间身份认证及密钥协商的步骤如下。

**步骤1** 主节点生成随机数  $R_g$  (变量索引  $g \geq 1$ ), 并按照式(9)使用预置密钥  $K_{pre,1}$  加密  $R_g$  和 MID, 得到  $C_g$ , 并将  $C_g$  放入 Modbus 报文数据帧中的数据域中, 广播发送给其他从节点。

$$C_g = F_{enc}(K_{pre,1}, R_g || MID) \quad (9)$$

**步骤2** 域内其他所有从节点收到  $C_g$ , 并按照式(10)进行解密, 之后生成随机数  $R_i$ 。使用预置密钥  $K_{pre,1}$  按照式(11)加密  $R_i$  和  $SID_i$ , 得到  $C_i$ , 并将  $C_i$  放入 Modbus 报文数据帧中的数据域中, 发送给主节点。

$$R_g || MID = F_{dec}(K_{pre,1}, C_g) \quad (10)$$

$$C_i = F_{enc}(K_{pre,1}, R_i || SID_i) \quad (11)$$

**步骤3** 主节点收到  $C_i$  后, 按照式(12)进行解密, 之后计算会话密钥  $K_{sess,1}$ , 如式(13)所示。

$$R_i || SID_i = F_{dec}(K_{pre,1}, C_i) \quad (12)$$

$$K_{sess,1} = KDF(R_g || R_1 || R_2 || \dots || R_n) \quad (13)$$

**步骤4** 主节点使用预置密钥  $K_{pre,1}$  按照式(14), 将会话密钥  $K_{sess,1}$  加密得到  $C_k$  (变量索引  $k \geq 1$ ), 将  $C_k$  放入 Modbus 报文数据帧中的数据域中, 并将该报文进行广播发送。

$$C_k = F_{enc}(K_{pre,1}, K_{sess,1}) \quad (14)$$

**步骤5** 主节点使用会话密钥  $K_{sess,1}$  计算  $R_g$  的消息认证码, 得到  $AUTH_g$ , 如式(15)所示。之后将  $AUTH_g$  进行广播发送。

$$AUTH_g = F_{mac}(K_{sess,1}, R_g) \quad (15)$$

**步骤6** 其他节点 Slave <sub>$i$</sub>  收到  $C_k$  和  $AUTH_g$  后, 按照式(16)解密  $C_k$ , 得到会话密钥  $K_{sess,1}$ , 并使用会话密钥  $K_{sess,1}$  计算  $XAUTH_g$ , 如式(17)所示。之后将  $XAUTH_g$  与  $AUTH_g$  进行对比, 相等则认证主节点身份,  $K_{sess,1}$  为协商的会话密钥。

$$K_{sess,1} = F_{dec}(K_{pre,1}, C_k) \quad (16)$$

$$XAUTH_g = F_{mac}(K_{sess,1}, R_g) \quad (17)$$

**步骤7** 各从节点 Slave <sub>$i$</sub>  使用会话密钥  $K_{sess,1}$  计算  $R_i$  的消息认证码  $AUTH_i$ , 如式(18)所示。之后将  $AUTH_i$  放入 Modbus 报文数据帧中的数据域中, 发送给主节点。

$$AUTH_i = F_{mac}(K_{sess,1}, R_i) \quad (18)$$

**步骤8** 主节点收到各从节点的  $AUTH_i$  后, 分别计算各从节点的  $XAUTH_i$ , 如式(19)所示。之后将  $XAUTH_i$  与  $AUTH_i$  进行对比, 相等则认证从节点 Slave <sub>$i$</sub>  身份。

$$XAUTH_i = F_{mac}(K_{sess,1}, R_i) \quad (19)$$

其中, 主节点与多个从节点可以构成群组, 进行群组认证并协商群组密钥。

#### 4.3.2 $n$ 个节点下的 Modbus RTU/ASCII

Modbus RTU/ASCII 的两节点间安全认证流程与 Modbus TCP 类似, 两者的群组身份认证及会话密钥协商过程基本一致。

## 5 安全性分析

本节分析两点间认证以及群组认证的安全性, 包括基于 Scyther 的安全性分析和实验验证。

### 5.1 非形式化安全性分析

(1) PC 和 PLC/RTU 双向认证: 本文 PC (主节点) 和 PLC/RTU (从节点) 通过双向身份认证建立相互信任。认证过程采用挑战-响应机制,

利用其功能码可自定义的特性,在不改变现有系统架构的情况下,选择了未被占用的功能码 0x6D (十进制 109) 来定义身份认证和密钥协商过程的报文,通过使用功能码 0x6D,标识用于身份认证和密钥协商过程的报文传输,实现了通信双方的身份认证和安全密钥的协商。

(2) 安全密钥分发:本文会话密钥是基于主节点和从节点各自使用对方发送的随机数以及预置密钥按照公式计算出相同的会话密钥,保证每次密钥的新鲜性,从而确保密钥的安全协商。由于会话密钥是基于每次认证生成的新随机数计算得出的,每次通信会话都使用不同的密钥,即使某次会话密钥被泄露,也不会影响未来的通信,保证了前向保密性。

(3) 抗重放攻击:为了有效抵御重放攻击,本文在认证和密钥协商过程中引入了随机数机制。每次认证都会生成新的随机数,确保每次会话的唯一性,防止攻击者利用先前截获的认证数据进行重放攻击。在身份认证完成后,主节点和从节点使用会话密钥生成消息认证码,即使攻击者成功重放之前的认证信息,也无法伪造有效的消息认证码。

(4) 消息机密性:本文方案使用会话密钥保护后续报文数据的机密性,防止攻击者通过监听通信链路窃取敏感信息。通过身份认证和会话密钥协商,确保只有合法设备才能获取用于加密通信的密钥,攻击者即使窃听了整个通信过程,也无法解密数据。

(5) 消息完整性:在身份认证后,采用会话密钥生成的消息认证码(MAC)来保证数据的完整性,即主节点和从节点计算MAC,并在收到对方的数据后进行验证,以确保数据在传输过程中未被篡改。

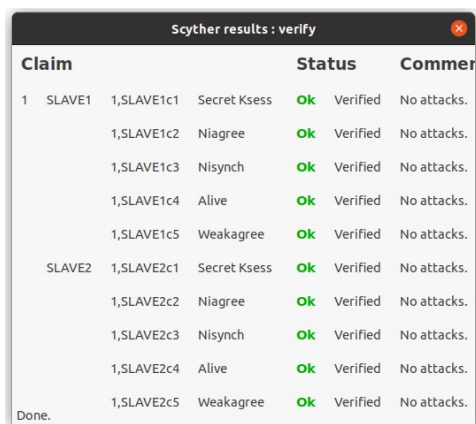
(6) 抗中间人攻击:为了防止中间人攻击,本文方案在双向认证过程中使用了随机数和预置密钥机制。预置密钥通过离线配置仅为合法节点持有,攻击者无法非法获取,进而无法伪造符合加密规则的身份凭证与通信数据。每次认证过程中,主从节点均生成全新随机数,经加密信道交换后,结合预置密钥通过密钥派生函数动态生成会话密钥,随机数的唯一性确保认证流程不可重复。攻击者即便拦截通信数据,因缺乏预置密钥

无法解密获取随机数,无法生成合法会话密钥与消息认证码,既无法伪装成通信双方介入交互,也无法篡改或伪造传输数据,从而从身份验证、密钥协商与数据传输环节阻断攻击路径。

## 5.2 形式化安全性分析

本节使用形式化安全验证工具 **Scyther** 验证所提协议的安全性。**Scyther** 是一个已被证明有效的安全协议分析工具,支持多个敌手模型,包括 **Dolev-Yao** 模型、**CK** 模型、**eCK** 模型等,基于安全协议描述语言对协议进行描述,并提供一组认证声明来建模安全属性。使用 **Scyther** 可以检测协议在密钥机密性、抗伪装攻击、抗重放攻击、抗中间人攻击等方面的潜在风险。

本节选择 **Dolev-Yao** 模型作为工控场景下的威胁模型,以验证节点间身份认证以及群组认证过程中的安全性。图 6 为两节点间身份认证流程 **Scyther** 形式化验证结果,图 7 为  $n$  个节点间身份认证流程 **Scyther** 形式化验证结果。图 6 和图 7 中 **Secret** 表示相关信息在不安全的网络环境中不会泄漏,确保信息的机密性。**Alive** 表示该实体是活跃的,验证该实体确实参与了协议的过程,且行为符合协议规定。**Weakagree** 表示协议的参与者在某些属性上有一个基本的一致性,可防止假冒攻击。**Niagree** 表示非单射一致性,意味着协议的参与者可能同意了相同的值,但这个值在协议的不同实例之间可能不是唯一的。**Nisynch** 表示非单射同步,确保了参与者对协议中的重要事件发生的顺序有共同的理解,保证了消息的完整性。**Scyther** 验证的结果表明,本节所提出的工控场景下节点身份认证及分级安全传输方案是安全的。



| Claim                            | Status      | Commer      |
|----------------------------------|-------------|-------------|
| 1 SLAVE1 1,SLAVE1c1 Secret Ksess | Ok Verified | No attacks. |
| 1,SLAVE1c2 Niagree               | Ok Verified | No attacks. |
| 1,SLAVE1c3 Nisynch               | Ok Verified | No attacks. |
| 1,SLAVE1c4 Alive                 | Ok Verified | No attacks. |
| 1,SLAVE1c5 Weakagree             | Ok Verified | No attacks. |
| SLAVE2 1,SLAVE2c1 Secret Ksess   | Ok Verified | No attacks. |
| 1,SLAVE2c2 Niagree               | Ok Verified | No attacks. |
| 1,SLAVE2c3 Nisynch               | Ok Verified | No attacks. |
| 1,SLAVE2c4 Alive                 | Ok Verified | No attacks. |
| 1,SLAVE2c5 Weakagree             | Ok Verified | No attacks. |
| Done.                            |             |             |

图6 两节点间身份认证流程 **Scyther** 形式化验证结果

| Claim                                                  | Status      | Comment     |
|--------------------------------------------------------|-------------|-------------|
| SLAVE2MASTER SLAVE SLAVE2MASTER,SLAVE1 Secret MESSAGE1 | OK Verified | No attacks. |
| SLAVE2MASTER,SLAVE2 Secret MESSAGE2                    | OK Verified | No attacks. |
| SLAVE2MASTER,SLAVE3 Secret SK                          | OK Verified | No attacks. |
| SLAVE2MASTER,SLAVE4 Alive                              | OK Verified | No attacks. |
| SLAVE2MASTER,SLAVE5 Weakagree                          | OK Verified | No attacks. |
| SLAVE2MASTER,SLAVE6 Niagree                            | OK Verified | No attacks. |
| SLAVE2MASTER,SLAVE7 Nisynch                            | OK Verified | No attacks. |
| MASTER SLAVE2MASTER,MASTER1 Secret MESSAGE1            | OK Verified | No attacks. |
| SLAVE2MASTER,MASTER2 Secret MESSAGE2                   | OK Verified | No attacks. |
| SLAVE2MASTER,MASTER3 Secret SK                         | OK Verified | No attacks. |
| SLAVE2MASTER,MASTER4 Alive                             | OK Verified | No attacks. |
| SLAVE2MASTER,MASTER5 Weakagree                         | OK Verified | No attacks. |
| SLAVE2MASTER,MASTER6 Niagree                           | OK Verified | No attacks. |
| SLAVE2MASTER,MASTER7 Nisynch                           | OK Verified | No attacks. |

图7  $n$ 个节点间身份认证流程Scyther形式化验证结果

### 5.3 安全性对比

表4列举了本文方案与其他相关方案的安全性对比。文献[25,27-28]支持双向认证、消息机密性、消息完整性和防重放攻击,但不支持群组认证,且缺乏形式化验证。文献[26]仅支持消息机密性、防重放攻击和消息完整性,缺乏双向认证、群组认证和形式化验证,且无法验证方案的正确性。

表4 安全性对比

| 方案     | 双向认证 | 群组认证 | 消息机密性 | 消息完整性 | 防重放攻击 | 形式化验证 |
|--------|------|------|-------|-------|-------|-------|
| 文献[25] | √    | ×    | √     | √     | √     | ×     |
| 文献[26] | ×    | ×    | √     | √     | √     | ×     |
| 文献[27] | √    | ×    | √     | √     | √     | ×     |
| 文献[28] | √    | ×    | √     | √     | √     | ×     |
| 本文方案   | √    | √    | √     | √     | √     | √     |

本文方案支持群组认证,且有效解决了群组通信中的安全问题。此外,本文方案还引入了形式化验证,进一步增强了方案的可靠性和可信度。

通过对比可以看出,本文方案在多个安全维度上具有明显优势,具有更高的综合安全性和实用性。

## 6 性能分析

### 6.1 计算开销

本节对本文方案的计算开销进行了评估。首先在Arduino Mega开发板(微处理器为ATmega328,时钟频率为16 MHz,SRAM为8 kB)上对方案的主要计算操作进行测试。为使测试结果更具参考价值,本节对每种计算资源进行20次测试,每次测试中,运行500次获得平均运算时间,取20次运算时间的平均值作为计算时间。典型的计算所需执行时间见表5。表6为 $n$ 个节点间身份认证过程中主节点和从节点计算开销对比。

表5 典型的计算所需执行时间

| 运算类型         | 符号                     | 计算开销/ms |
|--------------|------------------------|---------|
| 消息认证码        | $T_{SM3_{mac}}$        | 13.672  |
| 密钥派生         | $T_{kdf}$              | 18.068  |
| SM4加密        | $T_{SM4_{enc}}$        | 5.564   |
| SM4解密        | $T_{SM4_{dec}}$        | 5.438   |
| Ed25519签名生成  | $T_{Ed25519_{sg}}$     | 5 148   |
| Ed25519签名验证  | $T_{Ed25519_{sv}}$     | 8 196   |
| Curve25519加密 | $T_{Curve25519_{enc}}$ | 2 716   |
| Curve25519解密 | $T_{Curve25519_{dec}}$ | 2 718   |
| 主节点注册        | $T_{Rm}$               | 23.9    |
| 主节点安全信道建立    | $T_{CSm}$              | 28.7    |
| 从节点注册        | $T_{Rs}$               | 12.1    |
| 从节点安全信道建立    | $T_{CSs}$              | 26.2    |
| 从节点验证        | $T_{Vs}$               | 14.6    |

表6  $n$ 个节点间身份认证过程中主节点和从节点计算开销对比

| 方案     | 主节点计算开销/ms                                                                          | 从节点计算开销/ms                                                           |
|--------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| 文献[25] | $n(2T_{SM4_{enc}} + T_{SM4_{dec}} + 2T_{SM3_{mac}} + T_{kdf}) = 61.978n$            | $T_{SM4_{enc}} + T_{SM4_{dec}} + 2T_{SM3_{mac}} = 38.346$            |
| 文献[26] | $n(2T_{Ed25519_{sg}} + 3T_{SM3_{mac}} + 2T_{kdf}) = 10\,373.152n$                   | $T_{Ed25519_{sv}} + 3T_{SM3_{mac}} = 8\,237.016$                     |
| 文献[27] | $n(2T_{SM4_{enc}} + T_{SM4_{dec}} + 4T_{SM3_{mac}} + T_{kdf}) = 89.322n$            | $T_{SM4_{enc}} + 2T_{SM4_{dec}} + 4T_{SM3_{mac}} = 71.128$           |
| 文献[28] | $n(T_{SM4_{enc}} + T_{Curve25519_{enc}} + 2T_{SM3_{mac}} + T_{kdf}) = 2\,766.976n$  | $T_{SM4_{dec}} + T_{Curve25519_{dec}} + 2T_{SM3_{mac}} = 2\,750.782$ |
| 本文方案   | $2T_{SM4_{enc}} + nT_{SM4_{dec}} + (n+1)T_{SM3_{mac}} + T_{kdf} = 19.110n + 42.868$ | $T_{SM4_{enc}} + T_{SM4_{dec}} + 2T_{SM3_{mac}} = 38.346$            |

$n$  个节点间身份认证过程中主节点计算开销对比如图 8 所示。从图 8 可以看出, 本文方案主节点的计算开销显著小于其他方案。其中, 本文方案虽然在从节点的计算开销上与文献[25]相同, 但是主节点的计算开销远小于文献[25], 尤其是节点数较多时。文献[26, 28]采用的公钥技术在计算和通信开销上显著高于本文方案, 而本文方案通过高效的密码学机制和优化设计, 在计算效率、通信负载方面更具优势。本文方案在主节点计算开销方面低于其他方案, 主要原因是其他方案中, 会话密钥是通过主节点依次进行密钥分发的方式实现的, 这需要传输大量密钥信息, 占用大量总线资源。综合考虑, 本文方案更适用于工业控制网络环境。图 9 为节点身份认证过程中从节点功耗开销对比, 从图 9 可以看出, 本文方案在功耗开销方面具有优势。其中文献[25]与本文方案功率消耗相同, 二者结果一致, 因此在图 9 中两者为一条重合曲线。

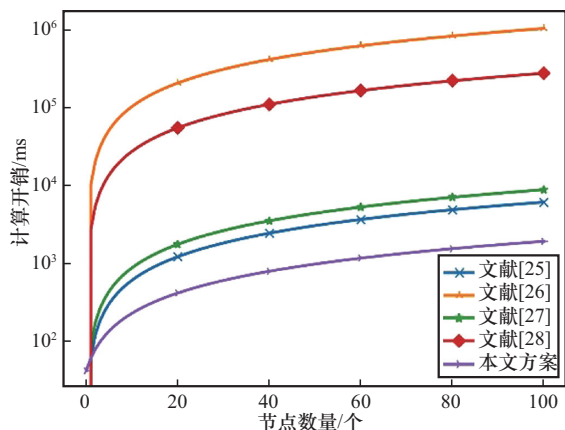
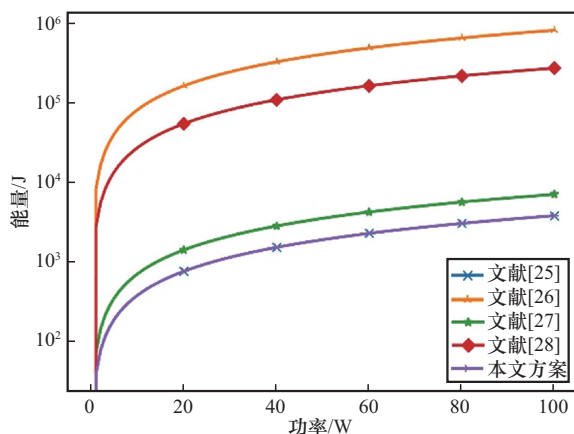
图 8  $n$  个节点间身份认证过程中主节点计算开销对比

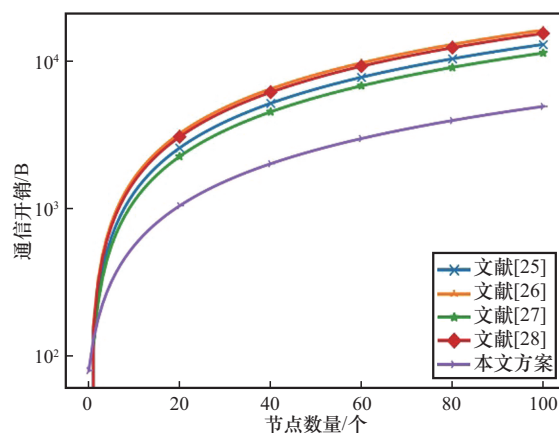
图 9 节点身份认证过程中从节点功耗开销对比

## 6.2 通信开销

在通信开销评估方面, 本节重点分析了协议的信令数量和信令交互过程中的带宽消耗。表 7 详细对比了本文方案与其他方案的主节点与从节点间的带宽开销。图 10 为  $n$  个节点间身份认证过程中主节点带宽开销对比。从表 7 和图 10 可以看出, 本文方案在信令数量上具有显著优势。尽管本文方案与文献[26]在信令数量上相近, 但文献[26]仅实现了主节点到从节点的单向认证, 而本文方案则实现了主节点与从节点的双向认证, 安全性更高。此外, 本文方案的带宽开销明显低于其他对比方案, 尤其在节点数量较多时, 从节点的通信开销远小于其他方案。综上所述, 本文方案在通信开销方面具有明显优势, 特别适合资源受限的工业控制网络场景。

表 7  $n$  个节点间身份认证带宽开销

| 方案     | 主节点带宽开销/B | 从节点带宽开销/B |
|--------|-----------|-----------|
| 文献[25] | $128n$    | 128       |
| 文献[26] | $160n$    | 128       |
| 文献[27] | $112n$    | 112       |
| 文献[28] | $152n$    | 152       |
| 本文方案   | $48n+80$  | 128       |

图 10  $n$  个节点间身份认证过程中主节点带宽开销对比

## 6.3 存储开销

本节对所提方案进行存储开销分析。假设每个对称密钥为 256 bit, 公钥为 1 024 bit, 私钥为 1 024 bit, 密钥种子为 256 bit, 白名单为 1 024 bit。

节点间身份认证存储开销见表 8, 从表 8 可以看出, 本文方案的存储开销为 256 bit, 与文

献[25, 27]相同, 具有较低的存储需求。总体来看, 本文方案在存储开销方面表现优异, 远低于文献[26, 28], 存储开销低。

表8 节点间身份认证存储开销

| 方案     | 存储开销/bit |
|--------|----------|
| 文献[25] | 256      |
| 文献[26] | 2 048    |
| 文献[27] | 256      |
| 文献[28] | 4 608    |
| 本文方案   | 256      |

## 7 结束语

本文针对工业控制网络环境下PLC/RTU节点计算资源受限以及Modbus总线报文缺乏安全防护机制等问题, 提出了一种轻量化的节点身份认证与群组认证方案。该方案基于哈希运算和对称加密等轻量级操作, 有效降低了认证过程和数据传输中的计算开销与通信开销。同时, 本文方案不改变Modbus原始报文结构, 仅需进行较小的改动(如自定义功能码), 即可适配到现有网络系统中, 展现了良好的适配性和可扩展性。为验证本文方案的安全性, 采用形式化验证工具Scyther对方案进行了安全性分析, 结果表明本文方案能够满足双向认证、密钥协商以及抗重放攻击等安全需求。此外, 通过与现有工业控制网络认证及会话密钥协商方案进行对比, 本文方案在认证及会话密钥协商过程中表现出显著的计算开销和通信开销优势, 极大地缓解了工业控制网络中引入安全机制的资源压力。因此, 本文方案特别适用于资源受限的工业控制网络环境, 为工控系统的安全防护提供了一种高效、可行的解决方案。

未来的研究将聚焦于进一步优化本文提出的轻量化认证方案, 主要包括算法优化以提高在资源受限设备上的执行效率、增强方案的安全性设计以应对新型攻击威胁, 以及扩大方案在大规模工业控制网络中的应用测试范围, 确保其在高并发和复杂网络拓扑下的稳定性和可靠性。同时, 将探索方案在跨域通信中的适用性, 增强不同安全域间的身份认证和密钥协商能力。此外, 未来还将推动本文方案的标准化与产业化应用, 与工

业设备制造商合作, 将方案推广至更广泛的工业控制系统中, 以满足日益严峻的网络安全需求。

## 参考文献:

- [1] Modbus Organization. MODBUS Application protocol specification v1.163[S].
- [2] 梁涛. 基于国密的工业物联网安全通信协议研究[D]. 哈尔滨: 哈尔滨工程大学, 2024.  
Liang T. Research on security communication protocol of industrial IoT based on national encryption standards[D]. Harbin: Harbin Engineering University, 2024.
- [3] 吴毅, 冯涛, 柳春岩, 等. 基于工业物联网的分层多设备认证密钥协商协议[J]. 网络与信息安全学报, 2025, 11(4): 86-106.  
Wu Y, Feng T, Liu C Y, et al. Hierarchical multi-device authentication and key agreement protocol for industrial IoT[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 86-106.
- [4] 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.
- [5] Nardone R, Rodríguez R J, Marrone S. Formal security assessment of Modbus protocol[C]//Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). Piscataway: IEEE Press, 2016: 142-147.
- [6] Rajesh L, Satyanarayana P. Vulnerability analysis and enhancement of security of communication protocol in industrial control systems[J]. Helix, 2019, 9(4): 5122-5127.
- [7] You W Z, Ge H B. Design and implementation of modbus protocol for intelligent building security[C]//Proceedings of the 2019 IEEE 19th International Conference on Communication Technology (ICCT). Piscataway: IEEE Press, 2019: 420-423.
- [8] Martins T, Oliveira S V G. Enhanced Modbus/TCP security protocol: Authentication and authorization functions supported[J]. Sensors, 2022, 22(20): 8024.
- [9] Figueroa-Lorenzo S, Añorga Benito J, Arrizabalaga S. Modbus access control system based on SSI over hyperledger fabric blockchain[J]. Sensors, 2021, 21(16): 5438.
- [10] Gamess E, Smith B, Francia G. Performance evaluation of modbus TCP in normal operation and under a distributed denial of service attack[J]. International Journal of Computer Networks & Communications, 2020, 12(2): 1-21.
- [11] Phillips B, Gamess E, Krishnaprasad S. An evaluation of machine learning-based anomaly detection in a SCADA system using the modbus protocol[C]//Proceedings of the 2020 ACM Southeast Conference. New York: ACM Press, 2020: 188-196.
- [12] Hayes G, El-Khatib K. Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol[C]//Proceedings of the 2013 Third International Conference on Communications and Information Technology (ICCIT). Piscataway: IEEE Press, 2013: 179-184.
- [13] Keliris A, Maniatakis M. Remote field device fingerprinting using device-specific modbus information[C]//Proceedings of the 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS). Piscataway: IEEE Press, 2016: 1-4.
- [14] Pricop E, Fattahi J, Parashiv N, et al. Method for authentication of

- sensors connected on Modbus TCP[C]//Proceedings of the 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT). Piscataway: IEEE Press, 2017: 679-683.
- [15] Luo X, Li Y. Security enhancement mechanism of Modbus TCP protocol[J]. DEStech Transactions on Computer Science and Engineering, 2019: 10.
- [16] Figueroa-Lorenzo S, Añorga J, Arrizabalaga S. A role-based access control model in modbus SCADA systems. a centralized model approach[J]. Sensors, 2019, 19(20): 4455.
- [17] Bernieri G, Cecconello S, Conti M, et al. TAMBUS: a novel authentication method through covert channels for securing industrial networks[J]. Computer Networks, 2020, 183: 107583.
- [18] 李环. 基于祖冲之算法的 Modbus TCP 协议安全通信研究[D]. 武汉: 华中科技大学, 2024.
- Li H. Security communication research on Modbus TCP protocol based on Zu Chongzhi algorithm[D]. Wuhan: Huazhong University of Science and Technology, 2024.
- [19] Liao G Y, Chen Y J, Lu W C, et al. Toward authenticating the master in the modbus protocol[J]. IEEE Transactions on Power Delivery, 2008, 23(4): 2628-2629.
- [20] Katulić F, Sumina D, Groš S, et al. Protecting modbus/TCP-based industrial automation and control systems using message authentication codes[J]. IEEE Access, 2023, 11: 47007-47023.
- [21] Alsabbagh W, Amogbonjaye S, Urrego D, et al. A stealthy false command injection attack on modbus based SCADA systems[C]//Proceedings of the 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC). Piscataway: IEEE Press, 2023: 1-9.
- [22] Guo C X, Cui Y B, Wang C. Research on trusted Modbus/TCP protocol of SCADA system based on digital envelope technology[C]//Proc SPIE 12641, International Conference on Cryptography, Network Security, and Communication Technology (CNSCT 2023). Bellingham: SPIE, 2023, 12641: 206-217.
- [23] 王英州, 张耀方, 徐有方, 等. 工业控制系统物理层报警量关联算法[J]. 网络与信息安全学报, 2025, 11(1): 178-188.
- Wang Y Z, Zhang Y F, Xu Y F, et al. Physical layer alarm correlation algorithm for industrial control system[J]. Chinese Journal of Network and Information Security, 2025, 11(1): 178-188.
- [24] 王红敏, 魏强, 王兰敏. 工业控制系统安全风险传播机理研究[J]. 网络与信息安全学报, 2025, 11(4): 107-116.
- Wang H M, Wei Q, Wang L M. Research on the mechanism of industrial control system security risk propagation[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 107-116.
- [25] Yi F M, Zhang L, Yang S M, et al. A security-enhanced modbus TCP protocol and authorized access mechanism[C]//Proceedings of the 2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2021: 61-67.
- [26] Wang Y, Wang L, Song N N, et al. Certificateless authentication application of the Modbus protocol in industrial control systems[C]//Proceedings of the 2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA). Piscataway: IEEE Press, 2022: 1308-1314.
- [27] Liu Z C, Liang T, Wang W S, et al. Design and implementation of a lightweight security-enhanced scheme for modbus TCP protocol[J]. Security and Communication Networks, 2023, 2023: 5486566.
- [28] Luo X, Li Y Z. Research and implementation of modbus TCP secu-

urity enhancement protocol[J]. Journal of Physics: Conference Series, 2019, 1213(5): 052058.

## [作者简介]



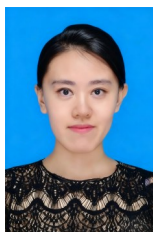
孙军军 (1968-), 男, 博士, 新疆油田公司数智技术公司高级工程师, 主要研究方向为网络与信息安全。



李昕泽 (2004-), 男, 西安电子科技大学博士生, 主要研究方向为网络与信息安全。



李伟 (1987-), 男, 硕士, 新疆油田公司数智技术公司高级工程师, 主要研究方向为网络安全、工控安全。



李焕 (1992-), 女, 新疆油田公司数智技术公司工程师, 主要研究方向为网络安全。



杨澜 (1999-), 女, 新疆油田公司数智技术公司助理工程师, 主要研究方向为工控安全与网络安全。



曹进 (1985-), 男, 博士, 西安电子科技大学教授, 主要研究方向为网络与信息安全。