

面向智慧矿山的设备通信协议设计

贺海涛

(神东煤炭集团有限责任公司, 陕西 神木 719300)

摘要:针对传统矿山感知层网络设备通信协议存在的开放性、实时性和安全性等问题,该文主要围绕智慧矿山通信协议展开研究,在架构层面改进了智慧矿山系统,设计了智慧矿山工业物联网的分层体系结构,并提出了智慧矿山设备通信协议改进方案。基于矿鸿通信协议和动态地址命名解析服务,研究了统一数据模型与通信协议的信息交互方案,提升了矿山系统的开放性,促进多体系、多设备的互联互通。在此基础上,结合分布式软总线技术与邻居发现协议、软总线组网技术和轻量化协议三种技术,提出了一种实时矿山数据传输方法,减少数据通信时延,提高数据传输的实时性;依据协议的加密技术、可信执行环境和全生命周期的数据保护,研究了如何在智慧矿山设备通信协议中建立完善的身份认证机制、构建安全的数据传输环境、形成可靠的全周期安全管理,保证了通信数据和通信协议的安全性。

关键词:智慧矿山;通信协议;数据模型;软总线;身份认证

中图分类号:TP393.0

文献标识码:A

文章编号:1673-629X(2023)10-0073-07

doi:10.3969/j.issn.1673-629X.2023.10.012

Design of Equipment Communication Protocol for Intelligent Mine

HE Hai-tao

(Shendong Coal Group Co., Ltd., Shenmu 719300, China)

Abstract: Aiming at the problems of openness, real-time and security of traditional mine perception layer network equipment communication protocols, we mainly focus on intelligent mine communication protocols, improve the intelligent mine system at the architectural level, design a layered architecture of intelligent mine industrial IoT, and propose an intelligent mine equipment communication protocol improvement scheme. Based on the mine Hong communication protocol and dynamic address naming resolution service, the information interaction scheme of unified data model and communication protocol is studied, which improves the openness of the mine system and promotes the interconnection of multiple systems and devices. On this basis, combining distributed soft bus technology with three technologies of neighbor discovery protocol, soft bus networking technology and lightweight protocol, a real-time mine data transmission method is proposed to reduce the data communication time delay and improve the real-time data transmission. Based on the protocol's encryption technology, trusted execution environment and whole life cycle data protection, it is studied how to establish a perfect identity in the intelligent mine equipment communication protocol. Based on the encryption technology of the protocol, the trusted execution environment and the whole-life data protection, we study how to establish a perfect authentication mechanism, build a secure data transmission environment and form a reliable full-cycle security management in the communication protocol of intelligent mining equipment, which ensures the security of communication data and communication protocol.

Key words: intelligent mine; communication protocol; data model; soft bus; identity authentication

0 引言

物联网、人工智能、大数据及新一代通信技术迅速发展,其在裁决系统、监控系统、运输系统等矿山系统深度应用,加快了矿山信息化、智能化的步伐。海量智能化仪器、设备、传感器也导致了智慧矿山网络数据传输的实时性和安全性面临巨大挑战。以数据加密、身份认证、访问控制、Switched Ethernet 技术为代表的智慧矿山通信技术可以抵御数据恶意窃取、保障数据实

时传输,是智慧矿山建设的关键与基础,对于矿山数据的安全性与实时性具有重要意义。智慧矿山通信技术也在矿山生产、调度、管理、救援等领域起到重要作用,实现矿山各设备之间的数据交互、智能化识别、定位、跟踪、监管等功能^[1-2]。

当前许多工作聚焦于矿山通信协议研究,解决了不同场景下智慧矿山数据的实时、安全传输问题。然而,现有矿山通信协议仍存在局限,在协议开放性、实

时性、安全性等方面有进一步的改进空间。以智慧矿山中常用的 EtherNet/IP^[3]、EtherCAT^[4]、Modbus^[5] 工控通信协议为例, EtherNet/IP 协议采用周期性轮询的方式, 时间或事件触发, 多波或简单的点对点连接的通信机制来适应矿山场景对实时性的要求, 但无法满足矿山系统的硬实时性要求^[6]; EtherCAT 协议具有较好的实时性能和拓扑的灵活性, 但由于私有化定制以及企业盈利的目的, 导致该协议在开放性方面有所欠缺^[7]; Modbus 协议规定通过一般的差分电路传输数据, 通信距离较远, 但是不支持加密传送, 传输数据的安全性无法得到有效保障^[8]。

针对 EtherNet/IP、EtherCAT、Modbus 协议的局限性, 文献[9-10]提出通过异常检测、优化轮询、构建新型网络架构等方式改善矿山协议。文献[9]对工业以太网通信协议提出栈结构优化方案, 但仅集中于实时性和安全性方面的提升, 未将多协议共存时设备互通互联的开放性问题的考量; 文献[10]立足于传统工业物联网智慧化过程中平台多协议统一化的趋势, 较好地解决了其开放性、实时性问题, 却忽略了对数据安全性的分析。尽管工业已有对通信协议从多方面进行改善的尝试, 但现有研究^[9-10]缺少对常见协议全方面、多角度的统筹分析, 没有形成统一的标准体系, 阻碍了矿山通信整体性能的提升。智慧矿山产业亟需构造一种满足三方面需求的新通信架构。

基于上述分析, 该文以智慧矿山工业通信的分层

体系结构为基础, 对矿山通信协议中存在的开放性、实时性和安全性三方面问题进行了深入研究并设计了解决方案。针对智慧矿山设备通信协议的开放性问题, 该文在矿鸿通信协议的基础上引入了动态地址命名解析服务, 提出了适用于异构网络的统一数据模型与通信协议的信息交互方案, 提高了矿山系统的开放性; 针对智慧矿山设备通信的实时性问题, 该文结合分布式软总线与邻居发现协议设备间信息的自动交换, 并通过软总线组网和轻量化协议分别解决了设备间不同协议交互和传统协议模型精简的问题, 构建了降低矿山数据传输时延的方案, 满足了矿山通信场景对实时性的需求; 针对智慧矿山设备通信的安全性问题, 该文通过完善身份认证机制、构建矿山设备传输安全环境、保障全生命周期的数据安全, 建立了集成身份认证、设备认证、数据通道认证的三重认证机制, 对矿山数据安全起到了强力保障。该研究有助于形成数据互联互通的标准化通信体系, 促进智慧矿山行业信息化改造的高效发展, 实现真正意义上的数字化、信息化、智慧化矿山。

1 智慧矿山通信系统模型

针对智慧矿山设备互联互通的数据交互需求, 设计了智慧矿山工业通信分层体系结构, 如图 1 所示。该体系结构由感知控制层、网络传输层、数据平台层及智能应用层四部分组成。

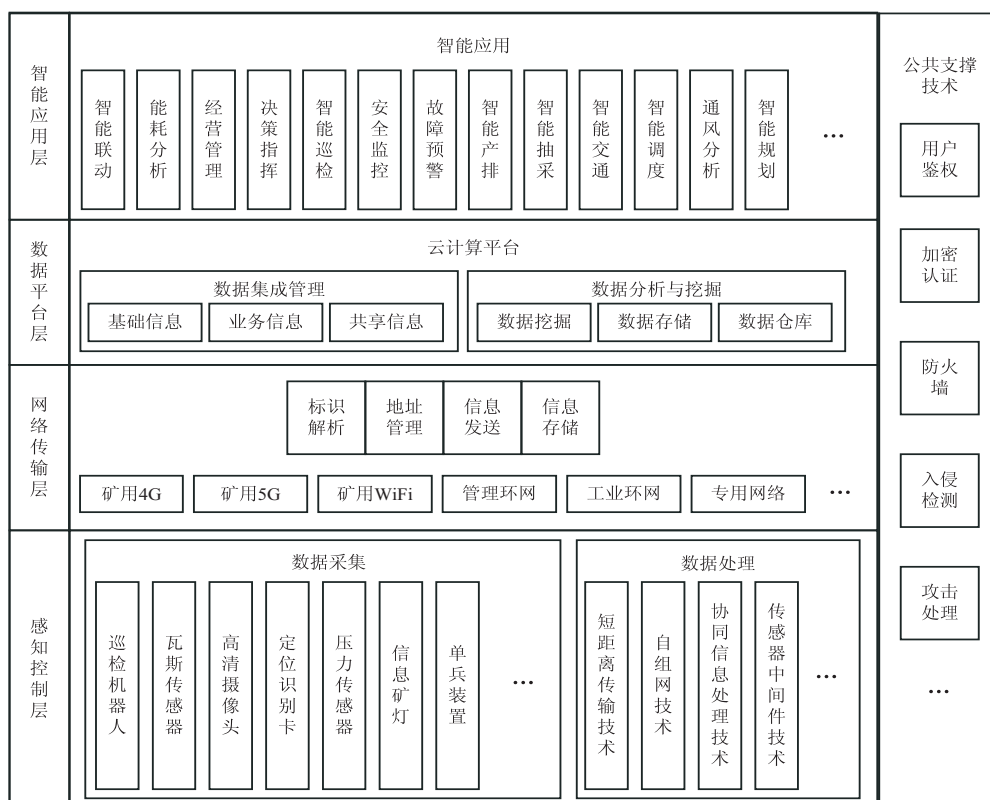


图 1 智慧矿山工业通信的分层体系结构

感知控制层负责智慧矿山工业通信的信息采集及传输^[11]。该层借助各类传感器、数码相机等智能终端设备对矿山环境和矿山生产资源相关数据进行采集,通过短距离传输技术、自组网技术、协同信息处理技术、传感器中间件技术等对采集数据进行初步处理。

网络传输层负责智慧矿山工业通信的信息交互。该层将感知层数据进行近距离接入和远距离传输,通过工业环网、管理环网等有线网络以及 4G、5G、WiFi6 等无线网络进行标识解析、地址管理、信息发送、信息存储等。

数据平台层负责智慧矿山工业通信海量数据管理。该层针对由感知控制层采集、网络传输层分发、多

物联网信息协同平台汇聚的多种类、大数量的矿山工业相关数据,通过云计算等手段实现数据分析、挖掘和利用^[12]。

智能应用层负责智慧矿山工业通信的用户交互。结合海量数据与行业需求,该层为用户提供丰富的矿山工业物联网应用,如智能巡检、安全监控、故障预警、智能产排等^[13]。

针对矿山设备通信系统中面临的开放性、实时性和安全性问题,该文基于智慧矿山工业物联网通信的分层体系结构,提出智慧矿山通信协议改进方案,如图 2 所示。

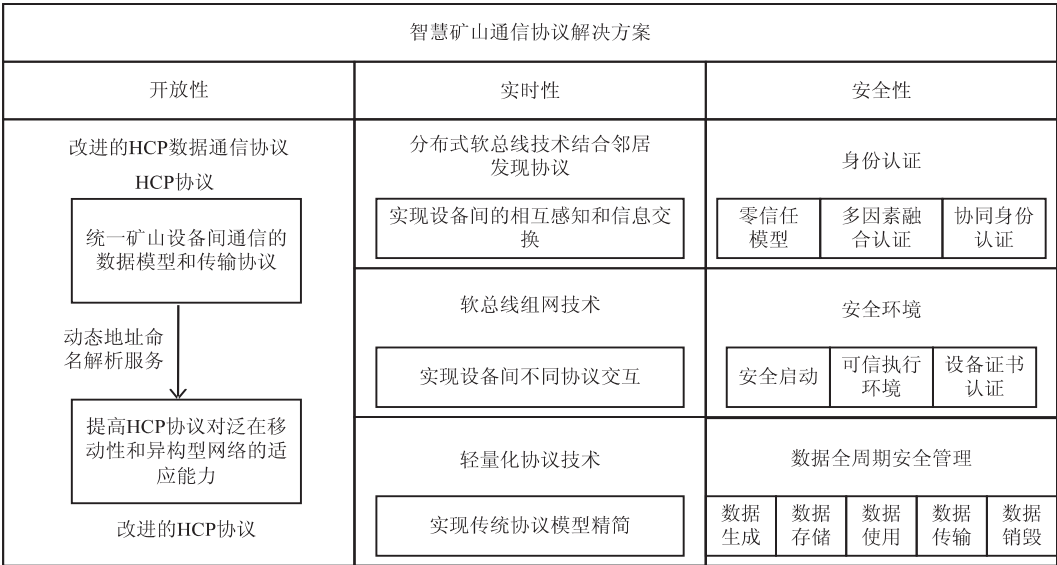


图 2 智慧矿山设备通信协议改进方案

通过动态地址命名解析服务对矿鸿通信协议 HCP 做出改进,提高其对泛在移动性和异构网络的适应能力以解决通信中的开放性问题,通过结合分布式软总线技术和邻居发现协议、软总线组网技术、轻量化协议技术提高通信实时性,通过身份认证、安全环境构建和数据全周期安全管理保障通信过程的安全进行。

2 智慧矿山设备通信协议设计

2.1 智慧矿山设备通信协议开放性设计

协议的开放性对于设备的互联互通尤为重要,协议的开放能够提高数据的流通性,增强设备之间的通信能力。要实现智慧矿山系统的开放性,必须要解决两个关键问题:①数据模型和表示方式,即发送方如何表示自己提供的信息和服务,需确定信息内容、组织方式、信息格式等。②交互协议问题,即发送方与接收方之间如何实现通信,需确定通信步骤、通信接口、消息格式等。

该文提出通过矿鸿通信协议 HCP 和动态地址命名解析服务来解决矿山系统的开放性问题。HCP 协

议栈被细分五层,分别为接口层、模型层、服务层、安全层、传输层。接口层负责协议栈对上层业务应用的总体能力呈现,模型层负责支撑配置管理、设备控制等子模块的逻辑实现,服务层负责协议栈的对上接口能力实现,安全层负责提供协议栈进行各类设备间业务交互过程中的安全保障能力,传输层负责设备之间业务会话可达性、各类业务操作指令、模型抽象编码的消息报文格式定义、逻辑通道的连接管理及服务质量的优先级调度。通过各层之间的相互作用,HCP 统一了矿山设备的数据模型和传输协议,解决了智慧矿山系统的开放性问题。

HCP 有效解决了矿山系统在传输层、会话层、表示层以及应用层的开放性需求,然而传统的基于 IP 地址的静态命名解析服务缺少对泛在移动性和异构性的适应能力,难以实现对异构地址类型和新型映射机制的兼容,导致矿山系统网络核心机制难以拓展,无法满足矿山在网络层开放性的发展需求。

针对此问题,在 HCP 的基础上,该文提出通过动态地址命名解析服务,进一步实现矿山系统在网络层

的开放性,如图 3 所示。该命名服务基于 xml,通过网络对象的元素属性,如:addr_name 表示地址类型名称,用以实现网络对象命名空间的标识,addr_struct 表示地址结构,addr_blocks 表示地址块数目,cons_method 表示地址构造方法,实现对地址模型的详细描述。该命名服务不仅可以实现对现有模型的描述,同时还可以根据矿山设备业务需求自定义或扩展引入其他类型的地址模型,使得所有的地址模型之间相互理解,提高网络层的拓展性^[14]。针对动态地址解析服务,该文提出构造一张存储网络对象间绑定关系的动态解析关系表,通过该表的逆向遍历实现动态解析。具体过程如下:在动态解析关系表中查找对象索引,获得对象索引对应的解析位置及解析机制,再以解析得到的对象为索引继续查找动态解析关系表,以此形成完整的动态解析链,实现从名字到转发端口的映射。如在应用层与网络层之间增加新的协议层,则可查找动态解析关系表,通过对应的解析协议将域名解析为新协议层对象,继续查找动态解析关系表将新协议层对象解析为 IP,再利用 ARP 将 IP 解析为对应的 MAC 地址。该方法在保证原有体系结构兼容性的同时实现了传统体系结构中新协议层和解析机制的透明引入^[15],满足了矿山系统在网络层的开放性需求。

改进的 HCP 协议	HCP 协议	接口层	对矿山智能应用的总体呈现
		模型层	矿山设备控制等子模块的逻辑实现
		服务层	协议栈对上接口能力实现
		安全层	矿山设备交互过程的安全进行
		传输层	实现矿山中的可靠传输服务
	网络层	动态地址命名解析服务	
		地址类型名称	地址结构
		地址块数目	地址构造方法
		IPv4 协议/IPv6 协议	
		数据链路层	IEEE802.1 标准
	物理层	100Mbps/s-1Gbps/s 传输速度	

图 3 设备通信开放性实现结构

2.2 智慧矿山设备通信协议实时性设计

2.1 节对智慧矿山通信协议做了开放性的研究,改进后的协议保证了原有协议的兼容性,实现了矿山系统在网络层的开放性的需求,增强了矿山系统设备间的通信能力。但在实时性上仍存在设备发现效率低、协议层复杂等问题,无法满足矿山系统对实时性高的设备的需求。该文提出采用分布式软总线技术结合邻居发现的协议、异构网络组网和轻量化协议的方式,能够减少矿山系统设备发现所需的时延,提高数据的带宽,提升数据传输能力,满足矿山系统设备对实时性的需求。

在介绍分布式软总线结合邻居发现、异构网络组网和轻量化协议的实时性方案前,先简要介绍方案背景。在计算机系统中,各部件之间传送信息的数据通路就是总线,设备间通过总线传输数据前需要先发现并建立网络连接,传统的设备发现需要用户手动配置或动态寻址的方式,但是由于矿山环境天然的复杂性,传感器设备众多,环境对于网络的干扰性强,传感器设备加入网络并建立连接的过程也占用了大量时间,通过传统设备发现方式对智慧矿山影响设备通信系统的实时性影响较大^[16]。传统的设备互联方面,不同的设备厂商需要适配不同的网络协议和标准规范,设备间组网和解耦较为复杂。矿山系统中大量的设备和传感器间组网和解耦的过程,造成大量的时间开支,影响矿山系统的实时性^[17]。

该文提出采用分布式软总线技术结合邻居发现协议,提升智慧矿山设备通信系统的实时性。分布式软总线技术支持设备间自发现,近场同账号的设备可以相互感知,并交换彼此的设备信息,在用户需要触发业务时,周边设备可直接出现,达到“零等待”的体验。除了加快设备的发现和传输,在数据传输速率上也获得了极大提升,最高 160 MB/s 的速度使得矿山系统在传输 4K 视频文件时,也依然能够做到“秒传”。对于传感器设备而言,由于传感器本身具有体积小特点,因此传感器节点往往采用电池供电,这决定了传感器网络节点应尽可能节省能耗^[18]。为了减少能耗并缩短传感器节点的发现时间,在矿山系统中,采用多信道邻居发现的方式。在 IEEE802.15.4 标准中明确定义了 16 个互不干扰的信道,在邻居发现过程中,主动发现节点和被动待发现节点采用相同的唤醒调度模式,当主动发现节点和被动待发现节点扫描至相同信道时,两者便实现了网络发现并建立连接。这种连接方式既能够较好地适应矿山的复杂环境,又能够适应矿山系统传感器设备动态加入和退出网络连接的需求,满足矿山系统对实时性的要求。

除了上述的方式提升实时性外,该文还提出了异构网络组网和轻量化协议的技术方案。异构网络组网可以自动构建一个逻辑全连接网络,以解决设备间不同协议交互的问题。设备上线后会向网络层注册,同时网络层会与设备建立通道连接,实时检测设备的变换。网络层负责管理设备的上线、下线变换,设备间可以监听自己感兴趣的设备,设备上线后可以立即与其建立连接,实现零等待体验。传统的通信协议主要分为基于以太网的通信协议与非基于以太网的通信协议。基于以太网的通信协议,一般以双绞线为通信介质。通信协议的实时性与网络的拓扑、带宽等因素密切相关。由于当前矿山网络软硬件设备种类繁多、制

式复杂、网络升级改造困难,上下行传输带宽受限,导致基于传统网络通信协议的矿山系统的数据传输速率差异非常大,时延也难以得到保证。该文提出的轻量化协议技术则是在传统网络协议的基础上进行的增强,改变传统的 OSI 七层模型,将表示层、会话层、传输层、网络层精简为一层。摒弃传统滑动窗口机制,丢包快速恢复,避免阻塞;颠覆传统 TCP 每包确认机制,减少包头开销;智能感知网络变化,自适应流量控制和拥塞控制,有效提高实时性和可靠性,获得高带宽、低时延、高可靠的传输能力。

设备通信实时性实现结构如图 4 所示。

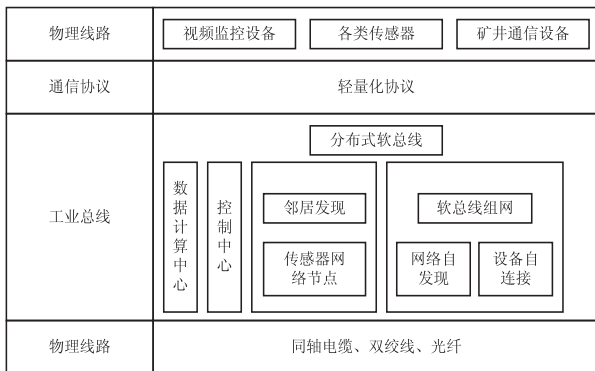


图 4 设备通信实时性实现结构

2.3 智慧矿山设备通信协议安全性设计

通过前文对智慧矿山通信协议开放性、实时性的研究,改进后的协议已具备扩展性良好的数据模型和高效可靠的数据传输能力。为进一步完善协议的安全性构建,解决身份认证不足、传输环境不可靠、数据保护不完整等问题,该文从建立完善的身份认证机制、构建安全的数据传输环境、形成可靠的数据全周期安全管理三方面入手,提出了结合联邦学习和 DID 分布式数字身份的身份认证机制,基于国产自主操作系统及安全芯片的可信计算环境,以及对数据进行预先分级分类管理后的数据全周期安全保护机制,形成了全方位保障数据的安全性和完整性的方案。

在身份认证方面,结合智慧矿山广泛存在的数据孤岛问题,提出采用具备高安全性的分布式架构联邦学习框架结合 DID 分布式数字身份的机制,对用户身份进行高效可靠的认证。当前部分常用的通信协议存在着缺乏身份认证机制和数据加密机制等问题,如 Modbus 及 EthernetIP 作为最常用的设备间通信协议,在网络上采取明文传输,易受欺骗、洪泛、重放等攻击威胁,存在着用户数据被非法访问、泄露隐私的风险^[19-20]。为此,需建立一种机制,在多设备终端场景下对包括数据访问者、业务操作者在内的用户进行协同身份认证^[21]。该机制的实现基于以下三个部分:零信任模型、多因素融合认证、协同互助认证。

该文采用基于零信任模型的持续验证、动态授权机制,以实现用户的认证和对数据的访问控制。当用户需要跨设备访问数据资源或者发起高安全等级的业务操作(例如,对安防设备的操作)时,机制会对用户进行身份认证,确保其身份的可靠性。不同于当前智慧矿山实践常用的易受社会工程学攻击的双因素认证^[22],提出采用多因素融合认证方法。考虑到智慧矿山传输过程的参与者有网关节点、链路节点、外部用户三类,三者需要的安全等级有所区别,该文提出对网关节点增设安全芯片,对传输链路节点布置独立证书与密钥对,对于外部用户将不同设备上标识同一用户的认证凭据关联起来,用于标识一个用户,以提高认证的准确度。此外,针对智慧矿山业务重合率高、用户重合率低、大量设备在短时间内产生海量数据的特征,选用横向联邦学习模型对传输进行加密,并采用基于区块链技术的 DID 分布式数字身份系统进行协同互助认证,通过将硬件和认证能力解耦(即信息采集和认证可以在不同的设备上完成),来实现不同设备的资源池化以及能力的互助与共享。高安全等级设备作为验证者,结合区块链上的 DID 注册系统验证低安全等级设备证书的完整性及来源,以协助低安全等级的设备完成用户身份认证。通过以上三种方式,建立起完善的用户身份认证机制,增强矿山数据安全的第一道防线,从而确保用户身份的真实性和合法性,规避了数据泄露等风险。

从发展的必然趋势出发,国内可信计算将朝着国产化、自主可控的规模化应用方向发展。对此,该文提出基于国产研发的鸿蒙 OS 进行安全环境的构筑。智慧矿山传统传输协议忽视了检验设备可靠性,如在矿山智慧化中作为标准使用的 OPC 协议,其基于 Windows 系统开发的特性导致了数据传输安全受主机安全环境的限制,且由于配置了 DCOM 与 RPC 接口,组件漏洞对 OPC 同样存在一定的影响。这使得用户数据无法在虚拟终端得到有效保护,面临着泄露隐私的危险。为此,需对传输的设备进行安全环境构建,机制的实现基于以下三个部分:安全启动、构筑可信的执行环境、设备证书认证。

为确保源头每个虚拟设备运行的系统固件和应用程序是完整的、未经篡改的,该文提出将鸿蒙操作系统搭载的自研芯片(如麒麟、龙芯等)作为信任根来设计设备的开机启动信任链,以实现安全启动,保证数据能够安全产生。此外,为保护用户的个人敏感数据的存储、传输和处理,建立可信执行环境(Trusted Execution Environment, TEE)是必要的。考虑到传统智慧矿山采用的可信执行环境往往受外国芯片所制,该文提出基于支持 TCM/TPCM、TPM2.0 等可信计算规范且支持

SM2、SM3、SM4 等国密算法的自研安全芯片架构设计可信计算平台。由于多设备终端硬件的安全能力不同,对于用户的敏感个人数据,需要使用高安全等级的设备进行存储和处理。对于具备 TEE 的设备,将向其预置 PKI(Public Key Infrastructure)设备证书给设备身份提供证明,确保设备是合法制造生产的。设备证书在产线进行预置,设备证书的私钥写入并安全保存在设备的 TEE 环境中,且只在 TEE 内进行使用。在必须传输用户的敏感数据(例如密钥、加密的生物特征等信息)时,会在使用设备证书进行安全环境验证后,建立从一个设备的 TEE 到另一设备的 TEE 之间的安全通道,实现安全传输。此外,由于现场设备算力有限,智慧矿山系统往往借助云计算进行数据处理,因此常处于复杂的多域环境,而传统的 PKI 模型和基于身份的密码体系存在着跨域认证低效等问题^[23]。对此,该文提出采用区块链 CA(Blockchain Certificate Authority, BCCA)信任模型,有跨域需求的各个域的信任锚根加入联盟链,构成验证节点并自生成区块链证书及哈希值,实现高可扩展性的认证系统。通过上述三种方式为矿山数据构建起安全可靠的传输环境,保证了数据仅能被可信的设备产生、传输、接收,对通信网络起到有效的保护作用。

考虑到传统矿山协议缺少完整的数据审计方案,无法在多设备终端场景下保证对数据进行全生命周期的全方位保护(例如, EtherCAT 协议使用的 FSoE 机制^[24]),该文提出对数据进行全生命周期的安全管理,基于数据的生成、存储、使用、传输、销毁五个阶段设计全方位的安全策略。在数据生成阶段,根据数据所在

的国家或组织的法律法规与标准规范,对数据进行分类分级,并且根据分类设置相应的保护等级。每个保护等级的数据从生成开始,在其存储、使用、传输的整个生命周期都需要根据对应的安全策略提供不同强度的安全防护。虚拟超级终端的访问控制系统支持依据标签的访问控制策略,保证数据只能在可以提供足够安全防护的虚拟终端之间存储、使用和传输。在数据存储阶段,机制通过区分数据的安全等级,存储到不同安全防护能力的分区,对数据进行安全保护,并提供密钥全生命周期的跨设备无缝流动和跨设备密钥访问控制能力,支撑分布式身份认证协同、分布式数据共享等业务。在数据使用阶段,机制通过硬件为设备提供可信执行环境。用户的个人敏感数据仅在分布式虚拟终端的可信执行环境中使用,确保用户数据的安全和隐私不泄露。在数据传输阶段,为了保证数据在虚拟超级终端之间安全流转,需要各设备是正确可信的,建立了信任关系(多个设备通过华为账号建立配对关系),并能够在验证信任关系后,建立安全的连接通道,按照数据流动的规则,安全地传输数据。当设备之间进行通信时,需要基于设备的身份凭据对设备进行身份认证,并在此基础上,建立安全的加密传输通道。在数据销毁阶段,数据销毁即密钥销毁,数据在虚拟终端的存储都建立在密钥的基础上。当销毁数据时,只需要销毁对应的密钥即完成了数据的销毁。从数据全周期分别进行安全性设计,以求保证个人数据与隐私、以及系统的机密数据(如密钥)不泄漏^[25]。

设备通信安全性实现结构如图 5 所示。

身份认证	应用层	零信任模型	持续验证结合动态授权 对传输链路节点布置独立证书与密钥对,关键设备节点认证 加设安全芯片 引入区块链横向联邦学习模型与分布式数字身份系统
		多因素认证	
		协同互助认证	
安全环境	表示层		
	会话层		
	传输层	安全启动 可信执行环境 设备证书认证	设计针对自研操作系统的设备启动信任链 设计基于自研安全芯片架构的可信计算平台 采用基于区块链信任模型及区块链证书
数据全周期安全管理	网络层	数据生成	对数据预先分级分类,施行不同的访问控制策略
		数据存储	
	数据链路层	数据使用	限制数据在分布式虚拟终端的可信执行环境中使用 依托于账号建立多设备信任关系,跨设备传输时建立加密传输通道
		数据传输	
	物理层	数据销毁	销毁存储于虚拟终端的对应密钥

图 5 设备通信安全性实现结构

3 结束语

为促进矿山智慧化建设,在智慧矿山工业物联网

的分层体系结构的基础上,分析了当前矿山通信协议中面临的开放性、实时性和安全性三大问题并提出了针对性的解决方案。首先,通过应用改进的 HCP 通信

协议,提出了适应性更强的统一数据模型与通信协议的信息交互方案;其次,通过应用分布式软总线、邻居发现协议、软总线组网和轻量化协议等技术,构建了降低矿山数据传输时延的实时性方案;最后,通过对身份认证机制的完善、设备安全通信环境的构建、数据全周期的安全管理,建立了包含身份认证、设备认证、数据通道认证在内的三重认证机制。该研究有助于解决矿山通信协议中存在的开放性、实时性和安全性问题,形成数据互联互通的标准化通信体系。该体系不仅能够提升矿山系统运营效率,助推国内能源行业加速智能化转型,产生巨大的经济效益,而且能够促进数字化的技术顺畅落地,实现自主知识产权的智慧矿山技术,避免技术依赖造成的“卡脖子”问题和网络安全问题,带来深远的社会影响。

参考文献:

- [1] 孙继平,陈晖升. 智慧矿山与 5G 和 WiFi6[J]. 工矿自动化,2019,45(10):1-4.
- [2] 郭 锐,冯志杰,高宗宁. 一种新型网络通信协议的设计与研究[J]. 计算机技术与发展,2017,27(1):75-79.
- [3] 吴爱国,李长滨. 工业以太网协议 EtherNet/IP[J]. 计算机应用,2003,23(11):9-11.
- [4] 单春荣,刘艳强,郇 极. 工业以太网现场总线 EtherCAT 及驱动程序设计[J]. 制造业自动化,2007,29(11):79-82.
- [5] 朱小襄. ModBus 通信协议及编程[J]. 电子工程师,2005(7):42-44.
- [6] 李武杰,郑 晟,陈文辉. Ethernet/IP 工业以太网的研究及应用[J]. 电子设计工程,2011,19(9):26-29.
- [7] 李 享,何 方,韩文泽. EtherCAT 时钟同步技术的研究[J]. 组合机床与自动化加工技术,2018(5):69-72.
- [8] 刘 鑫,王学华,白志城,等. 基于 Modbus 协议的终端通讯系统的开发[J]. 计算机技术与发展,2021,31(1):182-186.
- [9] 张宏科,程煜钧,杨 冬. 工业网络技术现状与展望[J]. 物联网学报,2017,1(1):13-20.
- [10] 杨章勇,李 欢. 工业以太网通信协议关键方法的优化与仿真[J]. 计算机仿真,2022,39(3):377-380.
- [11] 沙乐天,肖 甫,陈 伟,等. 面向工业物联网环境下后门隐私泄露感知方法[J]. 软件学报,2018,29(7):1863-1879.
- [12] UR REHMAN M H, AHMED E, YAQOOB I, et al. Big data analytics in industrial IoT using a concentric computing model[J]. IEEE Communications Magazine, 2018, 56(2):37-43.
- [13] 边 寒,陈小红,金 芝,等. 基于环境建模的物联网系统 TAP 规则生成方法[J]. 软件学报,2021,32(4):934-952.
- [14] 朱 亮,徐 恪,冯 梅. 互联网动态地址命名与解析服务[J]. 电子学报,2018,46(5):1089-1094.
- [15] 朱 亮,徐 恪. 互联网通用地址体系框架[J]. 西安交通大学学报,2017,51(2):6-12.
- [16] LORETI P, BRACCIALE L. Optimized neighbor discovery for opportunistic networks of energy constrained IoT devices[J]. IEEE Transactions on Mobile Computing, 2019, 19(6):1387-1400.
- [17] 车 楠,李治军,姜守旭. 异构无线网络中 Relay 节点部署算法[J]. 计算机学报,2016,39(5):905-918.
- [18] 裘 莹,李士宁,徐相森,等. 传感器网络邻居发现协议综述[J]. 计算机学报,2016,39(5):973-992.
- [19] 胡向东,李之涵. 基于胶囊网络的工业互联网入侵检测方法[J]. 电子学报,2022,50(6):1457-1465.
- [20] HE Y, MENDIS G J, WEI J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism[J]. IEEE Transactions on Smart Grid, 2017, 8(5):2505-2516.
- [21] 李文婷,汪 定,王 平. 无线传感器网络下多因素身份认证协议的内部人员攻击[J]. 软件学报,2019,30(8):2375-2391.
- [22] WU F, XU L, KUMARI S, et al. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment[J]. Journal of Network and Computer Applications, 2017, 89:72-85.
- [23] SARKAR S, CHATTERJEE S, MISRA S. Assessment of the suitability of fog computing in the context of internet of things[J]. IEEE Transactions on Cloud Computing, 2015, 6(1):46-59.
- [24] 冯 涛,王帅帅,龚 翔,等. 工业以太网 EtherCAT 协议形式化安全评估及改进[J]. 计算机研究与发展,2020,57(11):2312-2327.
- [25] 张玉清,周 威,彭安妮. 物联网安全综述[J]. 计算机研究与发展,2017,54(10):2130-2143.