doi:10.19306/j.cnki.2095-8110.2023.04.004

基于区块链＋北斗的铁路装备可信数字身份服务方法

樊玉明[1,2]，刘　琦[2,3]，咸晓雨[2,4]，王　剑[1]

（1. 北京交通大学电子信息工程学院，北京 100044；
2. 中车工业研究院，北京 100160；
3. 北京交通大学软件学院，北京 100044；
4. 北京航空航天大学交通科学与工程学院，北京 100191）

摘　要：智能铁路装备是一个典型的分布式物联系统，具有大量复杂的数据交互共享的需求与场景，装备及其产生的数据信令在系统中的数字身份标识是其重要安全基础。应用基于区块链去中心化的分布式数字身份标识技术，结合北斗时空信息，设计了铁路装备身份标识（railway decentralized identifier，RDID）可信数字身份服务，包括服务架构、生成流程、流转流程和验证流程，并进行了应用模型实现与效能分析。服务可以有效提升装备及其产生的数据信令的规范安全性，保证标识身份全局唯一，可追溯认证，从而提高智能装备系统通信过程数据的完整性与可靠性。

关键词：可信数字身份；区块链；北斗；铁路装备；物联网；通信安全

中图分类号：TP393；V19　　**文献标志码**：A　　**文章编号**：2095-8110(2023)04-0048-10

Method of trusted digital identity service for railway equipment based on blockchain ＋ BeiDou

FAN Yuming[1,2], LIU Qi[2,3], XIAN Xiaoyu[2,4], WANG Jian[1]

(1. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
2. CRRC Academy, Beijing 100160, China;
3. School of Software Engineering, Beijing Jiaotong University, Beijing 100044, China;
4. School of Transportation Science and Engineering, Beihang University, Beijing 100191, China)

Abstract: As a typical distributed internet of things (IoT) system, intelligent railway equipment possesses a large amount of requirements and scenarios of data interaction and sharing. And the important security basis is the digital identity label of the equipment and the generated data/signals in the system. Hence, a railway decentralized identifier (RDID) is designed using the decentralized digital identity technology based on blockchain, combined with Beidou position-time information, including its service architecture, generation process, flow process and verification process. The implementation of application model and efficiency analysis are also carried out. The service can effectively improve the security of equipment and the generated data, and ensure the global uniqueness of identity and traceability authentication, so as to improve the integrity and reliability of data in the communication process of the intelligent equipment system.

收稿日期：2023-05-29；**修订日期**：2023-07-01

基金项目：国家重点研发计划(2022YFB4300600)；国家自然科学基金(T2222015)；国家自然科学基金委员会-中国国家铁路集团有限公司铁路基础研究联合基金(U2268206)；北京市自然科学基金(4232031)

作者简介：樊玉明(1986-)，男，博士研究生，工程师，主要从事物联网、边缘计算及智能硬件方向的研究。

通信作者：王剑(1978-)，男，博士，教授，主要从事卫星导航、组合导航、列车运行控制和工业信息安全方向的研究。

Key words: Trusted digital identity; Blockchain; BeiDou; Railway equipment; Internet of things; Communication security

0　引言

随着我国“一带一路”倡议以及“交通强国”“新基建”等国家战略的制定和实施，轨道交通作为核心基础设施得到了前所未有的巨大发展机遇，而信息化、智能化的铁路装备是铁路系统提升其运营效率和运营安全的核心载体。新兴技术如物联网、5G、大数据、人工智能及边缘计算等被逐步应用到铁路装备中，使“安全可靠、便捷舒适、经济高效、绿色节能”的智能化铁路有了实现基础。而铁路装备智能化落地应用带来大量复杂的数据交互共享的需求与场景，同时也带来很多安全隐患，亟需提供一套可信的身份服务体系来保障智能装备系统的通信安全[1-2]。智能铁路装备是一个典型的物联系统，其中的交互兼具集中式和分布式特征，大量数据与信令运行其中，装备及其产生的数据信令在系统中的可信数字身份标识是其重要安全基础[3]，也是要解决的一个关键问题，对此业界多有研究。

区块链技术作为一种新兴的分布式网络数据管理技术，在解决交互可信化问题方面有其独有的优势和应用空间。利用区块链机制进行安全交互设计、身份认证设计和授权机制设计，可以有效提升物联网安全管理能力。W3C 主导研制了一套通过去中心化的分布式身份标识(decentralized identifier，DID)来进行用户身份自主管理的方案[4]。Faísca 等[5]提出一种基于区块链的身份认证方案，进行去中心化身份管理，用区块链来实现用户的标识和权属。焦英楠等[6]从物联网的三层体系结构和系统整体架构入手，采用区块链去中心化、信任机制、数据加密和时间序列等特点解决物联网存在的数据安全、隐私泄露及中心化等问题。Rana[7]等针对应用区块链进行身份证明的安全化隐私化进行了研究。通过区块链技术提取装备或消息信令的独特特征构建身份标识，并纳入区块链管理，建立数字身份体系，可以应用于全链条可信追溯、信息信任流转及设备可信访问。

北斗三号全球卫星导航系统(BDS-3)2020 年建成并投入使用，是我国完全自主可控的全球时空服务基础设施，也是国家综合定位导航与授时(positioning，navigation，and timing，PNT)体系的重要组成部分[8]，为不同物理域的各类用户提供满足需求的高精度时空信息服务。目前铁路装备正在逐步应用北斗替代 GPS 系统，可有效解决 PNT 系统自主可控问题，但是应用场景仍较单一，需要进一步释放“＋北斗”的赋能空间。BDS-3 可以提供的公共服务包括水平 10 m、高程 10 m、计时精度 20 ns 的高精度时空信息[9-10]，且具有如下特征：1)服务泛在，全球可用能够普及；2)基准统一，单点单次结果唯一；3)时空自洽，序贯逻辑可验证推理；4)秩序严谨，单向信息不可逆转[11-12]。利用此信息能够为铁路装备提供具有时空可信性的标签，将其作为装备主体或其产生及流转的消息信令当前时刻和生命周期流转过程的重要特征，结合区块链的去中心化安全存储、传输和加密功能与特性，可以生成更可靠的数字身份标识，具有自主性、规范性、时空关联性、唯一性及可认证性的特性优势。

本文结合北斗三号全球卫星导航系统 PNT 技术与基于区块链方案的 DID 技术，提出了基于区块链＋北斗的可信数字身份服务，并将其应用于铁路装备身份标识(railway DID，RDID)。该方法采用合理的设计架构，可以有效提升装备及其产生的数据信令的规范安全性，保证标识身份全局唯一、可追溯认证，从而提高智能装备系统通信与数据的完整性与可靠性。

1　基于区块链的 DID 技术

区块链技术基于分布式系统，是一种综合运用密码学、数据库和计算机技术的数据记录管理技术，其核心在于在不完全可信的环境中构建分布式账本解决现有中心化系统存在的许多问题[13]。区块链中的数据具有开放性、透明性，数据源的透明度解决了信息不对称的问题。通过密码学的方法确保交易无法抵赖和破坏，并尽量保护用户信息和记录的隐私性，在分布式系统中设计共识机制与链式数据管理体系，通过所有节点共同存储、管理和监督数据，参与到系统上的节点可能不属于同一组织，彼此互不信任但地位相当，系统运行不受单一节点约束，使得整个系统具有数据信息不可伪造篡改、信息操作可追溯的特点。

以太坊是第二代区块链的代表和基础，其引入

智能合约设计，可提供更灵活的合约功能，执行更为复杂的操作，从而超越了单纯数据记录的功能，实际上带有“普适计算”的功用[14]。智能合约通过具有图灵完备的语言编写代码，理论上可以解决任何可计算的问题。通过智能合约可以实现操作的去中心化可信，例如进行身份认证、协议签订等，降低分布式系统的信任成本。

简化的区块链基础模型如图 1 所示。

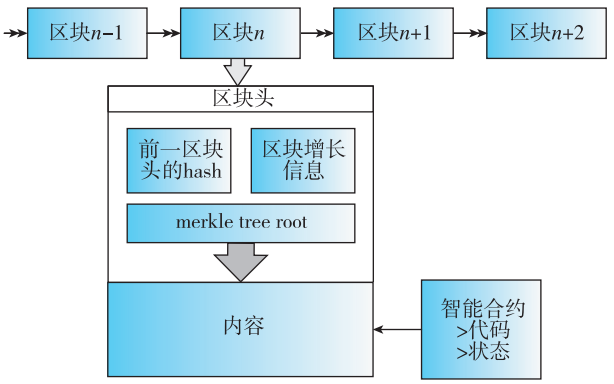

图 1 简化区块链基础模型

Fig. 1 Simplified blockchain foundation model

利用区块链技术进行数字身份设计，通过密码学加密、分布式存储等特性，可以对主体的隐私、数据安全进行全方位的保护，简化身份管理流程。分布式信任是数字身份的基础，其核心是基于区块链去中心化、不可篡改的特性而创建的 DID。然后，多方通过接入工具接入分布式信任网，以区块链为依据，建立不同身份标识之间的安全交互，为可验证声明（基于 DID 体系的一类证书）的流转建立前提，保证数字身份信息准确，防止伪造、冒用。DID 技术基于区块链及智能合约构建标识，能够实现标识的自动生成和自分配。相对于传统的基于公钥基础设施（public key infrastructure，PKI）的身份体系，基于区块链建立的分布式数字身份系统具有保证数据真实可信、保护主体隐私安全和可移植性强等特征[15]，其优势在于：1）去中心化，基于区块链，避免了身份数据被单一的中心化权威机构所控制；2）身份自主可控，基于分布式公钥基础设施（distributed public key infrastructure，DPKI），每个主体的身份不是由可信第三方控制，而是由其所有者控制，单元能自主管理拥有的身份；3）可信的数据交换，身份相关数据锚定在区块链上，认证的过程不需要依赖于提供身份的应用方。

主体的 DID 不是单一中心赋予的，而是主体根据规范的算法生成的且完全自主控制。生成 DID 的同时，也会生成对应的公私钥，公钥与 DID 的绑定关系会被发布在分布式存储上，私钥由主体保管，身份相关数据会被锚定在区块链上。应用方验证主体身份信息时，要根据分布式系统中形成共识的主体的公钥进行验证计算，验证用户的真实性。

DID 技术框架如图 2 所示。

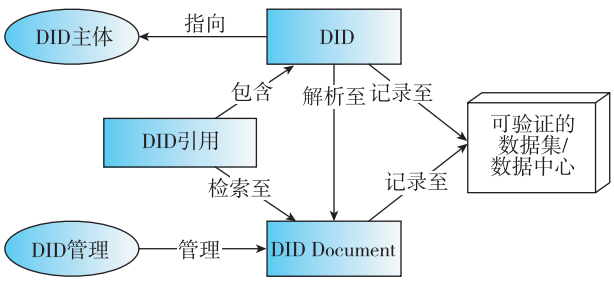

图 2 DID 技术框架

Fig. 2 DID architecture

2 可信数字身份服务架构

基于 DID 技术设计应用于铁路装备的可信数字身份服务 RDID，应着重管理两类主体的身份：设备数字身份和虚拟对象数字身份。其中，虚拟对象特指整个通信体系中流转执行的消息、信令与操作历史。对于每个主体，根据服务准则可以自己产生身份，并更新身份特征，请求身份验证。服务主要包括身份生成与解析、身份共识与上链、身份特征声明及身份验证应用 4 个模块。

2.1 铁路装备分布式物联网络组成与特点

当前的铁路装备适应智能化发展，应用了大量的感知通信技术，在智能铁路的总体技术框架中[16]，基础设施、智慧列车和智能运维三大系统建立了复杂的网络通信机制，构建成为铁路装备物联网（以下简称“铁路物联网”），用于进行数据交互与信息共享。每个大系统有自己的子系统，子系统后扩展终端节点，大系统和子系统均不是唯一孤立，而是呈分布式共存，同一类型系统存在多个地位对等的系统节点。

从通信网络总的对象划分来讲，主要有车车通信、车路通信和车管通信，从网络角色划分来讲，可以分为状态感知层、数据传输层、技术应用层、智能管理层，而基础设施、智慧列车及智能运维又各自有各自的子网，进行系统内通信，系统抽象如图 3。

总结来看，铁路物联网是一个完整的分布式应用环境，典型应用特点如下：

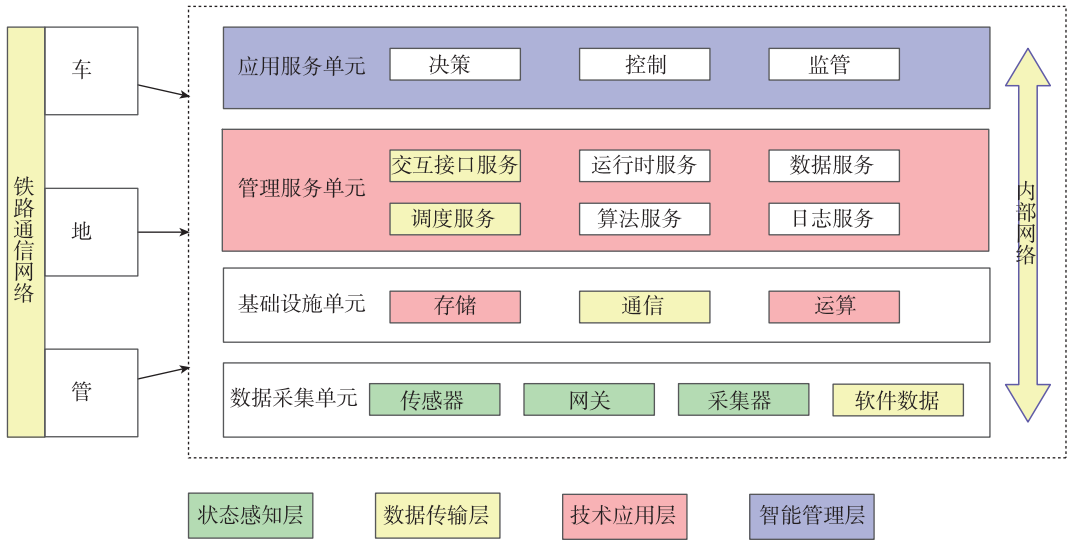

图 3　子系统结构示意

Fig. 3　Schematic of subsystem structure

1)网络连接拓扑复杂,终端设备海量异构,而且整个网络具有地理分布式、架构分布式及业务分布式的特性,适合应用部署区块链基础设施。

2)规模庞大,节点众多,场景广泛,物理设备节点角色丰富,数字对象模态内容丰富,作为物联网结合大数据高效应用与协同共享,需要进行全局身份管理,建立全局唯一的统一标识并进行数字化映射。

3)面临众多安全挑战,如设备缺乏物理安全控制、受限于资源的安全能力不足、恶意节点攻击、后门漏洞、不安全的组件或接口、难以监管的用户等,而安全防护对策中最基础的信任建立条件就是要提供鲁棒的可信身份与访问控制方法,包括不可篡改可认证的身份标识、安全高效的认证机制。

作为广域交通设施所用的物联网,地理位置信息是其中网络、设备、虚拟对象的关键属性,是分布式实体身份标识全局唯一的重要信息构成。对于网络中的实体,按照位置信息来源可以分为有独立个体位置信息源的实体、可以获取相关位置信息的实体、没有位置信息的实体;按照位置信息动态可以分为长期固定位置的实体、可移动位置的实体。精确时间信息也是分布式网络的关键属性和应用资源,而且对安全应用、实时应用、同步应用以及数据的共享、记录与追溯具有重要的价值。将时空信息结合,可以有效辅助铁路物联网的可信身份服务应用。

根据实际网络的拓扑特性、实体在网络中的角色及信息数据地位对等性,结合可信数字身份应用环境需求,将铁路装备分布式物联网实体抽象见图 4。

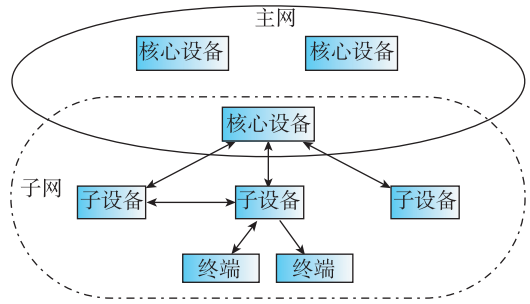

图 4　铁路装备分布式物联网实体抽象

Fig. 4　Railway equipment distributed IoT entity abstraction

如图 4 所示,网络呈树状扩展,其中核心设备指在网络中处于关键信息交换位置的设备,运算与业务处理能力较强;子设备指核心设备的下属设备,负责单一业务,具有简单运算处理能力;终端特指最末端的设备,不具有运算处理能力,是信息的来源;主网指由核心设备组成的网络,系统间信息交互需要通过主网进行;子网指核心设备与其辖下的子设备共同组建的子系统内部网络,子系统内信息主要在子网内交互。核心设备既可以作为身份信息的生产者也可以作为身份信息的消费者,子设备主要作为身份的生产者,也可以作为消费者,终端通过子设备链接身份信息。需要注意的是,在不同的网络和业务层面,一个设备既可以是核心设备也可以是子设备。

2.2　服务架构设计

根据 2.1 节所述的网络拓扑抽象,RDID 的服务架构如图 5 设计所示。

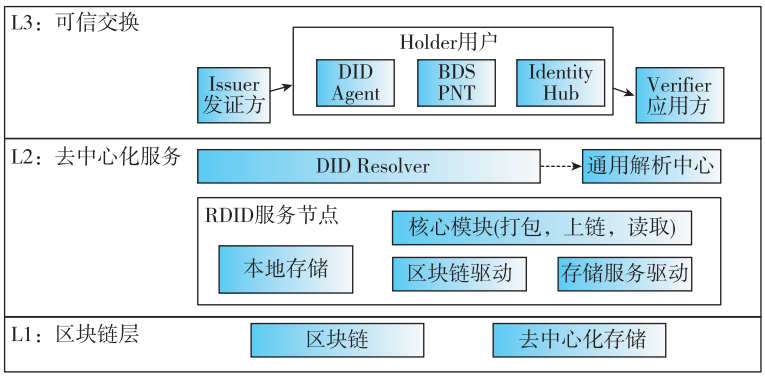

图 5 RDID 服务架构

Fig. 5 Service architecture of RDID

其中，服务共分为 3 层：

L1 区块链层是 RDID 方案的基础设施，包括区块链和去中心化的分布式存储。其可以部署在现有的主网核心设备中，也可以作为独立业务与服务系统部署。分布式存储中保存的是整个系统完整的数字身份信息，即 DID 文档(DID Document)。在区块链上则锚定着这些数字身份信息的对应关系。

L2 是去中心化的二层网络，是由物理网络与设备构成，主要由网络中的核心设备和运行于其上的 RDID 节点(R-S)组织而成。由于 RDID 服务只是这些设备的一部分业务，且不是其主体目标业务，所以 R-S 设计为轻量化服务单元，节点间依赖底层区块链共识机制来保证其一致性。节点主要业务是处理其负责的子网主体 RDID 操作请求，并将操作数据同步至 L1 的分布式存储，并将同步信息、引用信息在 LI 创建交易上链，这一操作可以通过区块链的智能合约接口完成。通过加入 RDID 节点分开主网与子网业务，提升系统业务的整体处理性能。同时在 L2 上还提供统一的 DID 解析业务(DID Resolver)，与 W3C 定义的 DID Resolver 兼容，能够根据 RDID 查询其对应的 DID Document。

L3 是可信交换层，是 RDID 系统中各个主体互相建立安全数字身份认证与数字身份信息的数据交换层。Holder 是 RDID 的主体，其中 RDID Agent 是 Holder 使用的 DID 客户端，能够处理主体的 RDID 相关的业务，包括但不限于创建 DID、提交可验证声明请求等。Identity Hub 用于保存和管理用户的数据，严格在本地使用并使用安全加密机制。基于 BDS－3 的位置应用在 L3 会被 RDID Agent 调用，经过处理注入 RDID 中。Issuer 是发证方，在 L3 中负责为主体签发可验证声明，为主体 DID 所包含的具体身份属性与信息背书；Verifier 应用方是使用 DID 的第三方主体，如应用、数据中心等。

2.3 基于 BDS-PNT 信息的数字身份及生成方法

RDID 是主体的数字身份表达，遵从 W3C 的 DIDs V1.0 标准。主体(Holder)分类中的设备指铁路物联网中存在的实体主体，虚拟对象是指铁路物联网中流转的数据主体，RDID 由上文所述运行于设备本体、上一级设备或虚拟对象生产主体中的 R-S 服务调用 DID Agent 和 BDS-PNT Service 生成并赋予，其生成方法如下所述：

1)获取 Holder 的特征信息 K，通过 BDS-PNT Service 得到 BDS 时空信息 tp。

2)DID Agent 生成私钥与对应的 RDID，并将其注入 Holder。

私钥通过改进的哈希函数 H 计算生成，函数基础算法为 SM3，基于 BDS 时空信息进行优化。哈希函数的输入为特征信息 K，将 BDS 时空信息 tp 进行如式(1)的处理，得到 16 个 8 位二进制串，按照图 6 的流程作为 SM3 消息扩展过程的添加因子，计算 $H(K, tp)$ 得到第一私钥串，计算 $H(H(K, tp), tp)$ 得到第二私钥串，进一步通过 Secp256k1 算法派生计算得到两个私钥对应的公钥 key1 与 key2，应对不同的应用场景。

$$bin\_str = [MD5(tp)[i:i+8]\ for\ i\ in\ range(0, 128, 8)] \tag{1}$$

RDID 格式定义为 $did:rdid: < method\text{-}specific\text{-}id >$，其中

$$< method\text{-}specific\text{-}id >= ripemd160(MainID):SubID \tag{2}$$

MainID 定义为主体的出生 ID，生成式为

$$base58(sha256(<base\ DID\ Document>)) \tag{3}$$

在 base DID Document 中需要包含 key1，key2；SubID 定义为主体的生命周期 ID，包含其生命周期状态信息 *st* 和流转的 BDS 时空信息 *tp-update* 的摘要。

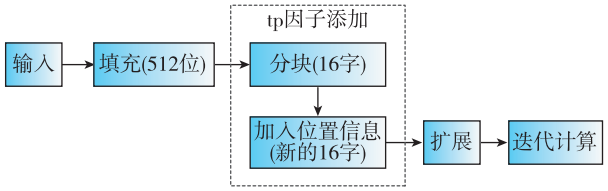

图 6　SM3 消息扩展因子添加流程

Fig. 6　SM3 message extension factor addition process

3）生成 DID Document 并上链。

结合初始和流转节点的 BDS 时空信息做摘要生成 MD5(tp)，MD5(tp-update)，与 RDID 一起扩展 base DID Document 得到 DID Document，并通过合约进行上链操作，将 DID Document 置入分布式存储。

4）适时更新 RDID 与 DID Document。

在流转过程中如果有生命周期状态变化或者流转节点变更，需要更新 RDID 中的 SubID 和对应的 DID Document。

RDID 生成流程如图 7 所示，所有的生成过程都在主体框架内完成。实体的 DID 由 Holder 自主生成，虚拟对象的 DID 由虚拟对象的生产节点（子设备以上层级）生成，流转节点更新。主体采用北斗提供的 PNT 时空信息，在初始化和适时更新两个层面保障 RDID 的唯一性、追溯性。

2.4　身份验证流程

RDID的流转由用户、发证方和应用方共同参

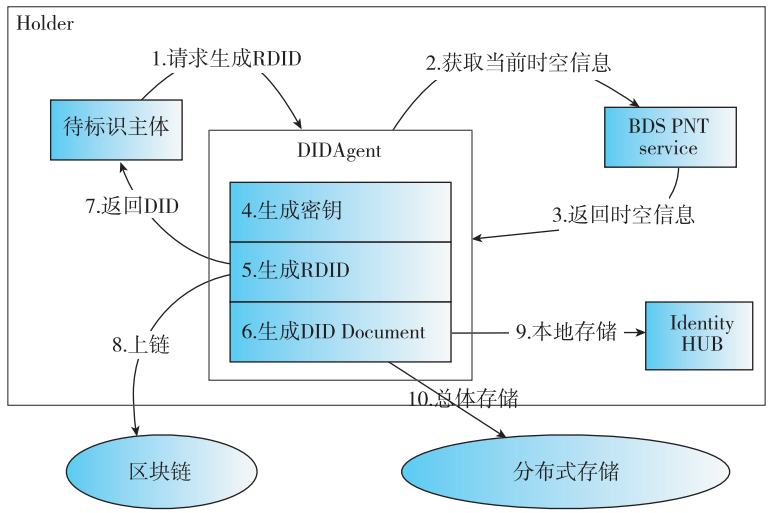

图 7　RDID 生成流程

Fig. 7　Service architecture of RDID

与，映射到实体系统，就是拥有标识的主体（即所有铁路物联网中的设备与设备产生的需要标识的信息流）、给主体的标识签发可验证声明的可信主体（铁路物联网系统内的核心设备，可以是主网设备，也可以是子网设备）、需要检验主体身份的环节（数据信息的应用设备，需要验证所收到的信息来源可信，需要验证接入的设备是合法设备）。

在分布式信任的铁路物联网中，需要使用 RDID 验证授权的操作有两种（见图 8）：1）无需可验证声明即可承认授权的操作，例如一般状态信息流转；2）需要指定可验证声明才能承认授权的操作，例如进行安全相关的控制操作。在第一种情况中，应用方只需验证主体是 RDID 的拥有者即可。在第二种情况中，主体首先需要去向发证方比如数据中心，申请一个证明自己的操作有授权的声明，然后向应用方出示此声明才能完成 RDID 的验证。这里的可验证声明（verifiable claim）是一个 RDID 给另一个 RDID 的某些属性做背书而发出的描述性声明，并附加自己的数字签名，用以证明这些属性的真实性，可以认为是一种数字证书。可签发 Claim 的 RDID 必须具有公信力。因为可验证声明是 RDID 签发出来的，所以应用方只需要去链上获得此

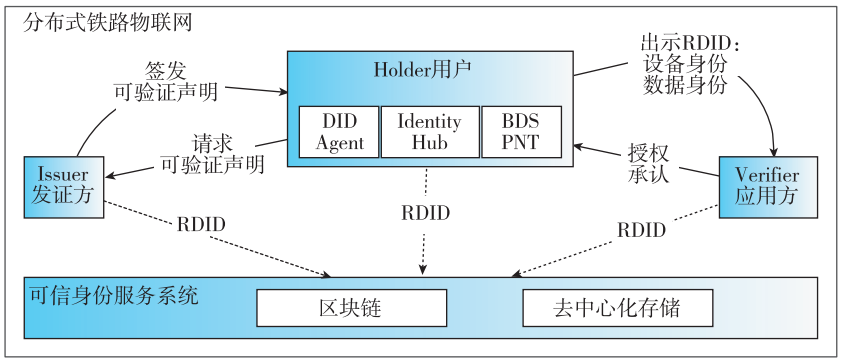

图 8 RDID 流转

Fig. 8 RDID flow

RDID 的公钥即可验证声明的真伪。

身份验证过程中使用基于北斗时空信息的公私钥，执行挑战——响应机制，数据发送方或者身份验证方获取到接收方或者被验证方的 RDID，在区块链检索获取到其 DID Document，即可得到对应的公钥 key 和北斗时空信息的摘要 MD5(tp-update)，同时可通过北斗系统获取到当前时空信息的摘要 MD5(tp-now)，用公钥对 MD5(tp-update) ⊕ MD5(tp-now)进行加密，发送给接收方或者被验证方。接收方需要有正确的私钥与 tp-update 才能进行解密，并将解得的信息返回与 MD5(tp-now) 比对，如果返回值正确，则表明接收方或者被验证方是 RDID 的合法持有者，实现身份的安全认证。时空信息是可以定时更新的，而且更新连续有规律，非法的第三方由于无法获取正确的时空信息和私钥，不能进行正确解密，也不能冒用身份。

3 应用模型与效能评估

以列车故障预测与健康管理（prognostic and health management，PHM）系统为例，系统由列车子系统、地面子系统构成。列车子系统包括列车网控与车载 PHM 系统，负责收集车辆运行状态信息；地面子系统包括 1)地面感知系统，负责收集地面数据；2)地面 PHM 系统，负责统筹 PHM 信息，进行数据分析，调度各系统；3)管理系统，根据获取到的车路态势提供决策功能。整个系统通过收集列车、地面设备等铁路装备的大量运行状态数据，结合模型分析，提出设备故障预测和全生命周期管理策略，所以数据的来源和安全性对于决策来说至关重要。系统如图 9 所示[17]。

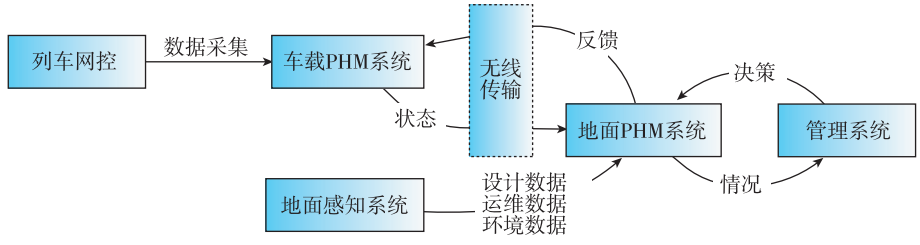

图 9 列车 PHM 系统

Fig. 9 PHM system of train

系统各部分的角色和获取时空信息的方式如下：

1)车载 PHM 系统、地面感知系统、地面 PHM 系统及管理系统是核心设备，构成主网，在主网上搭建区块链网络，分布式数据存储，负责管理存储 RDID 与 DID Document，在核心设备上部署 2.2 节所定义的 R-S 节点，主网单元各自的北斗时空信息是其关键信息，会随区块链在网间同步；

2)配置地面 PHM 系统为发证方，地面 PHM 系统的时空信息从地面站系统的北斗接收机或等效信源获取，属于自主定位信源；

3)列车网控与车载 PHM 系统构成子网，列车网控角色为终端，配置车载 PHM 系统为应用方，子网的时空信息引用列车的车载北斗接收机的时空信息，

属于共享定位信源，全车共享车辆的 BDS 信息；

4)地面感知系统构成子网，子网的时空信息引用地面感知系统北斗接收机或等效信源的时空信息，属于自主定位信源。

在此系统中：

1)各设备单元 RDID 依照 2.3 节定义的规则自主生成，且定期更新，由于列车为移动装备，其 SubID 对应的＜DID Document＞项会有随动变化。

2)消息的 RDID 由其生产者生成，例如由车载 PHM 系统收集而来的状态信息需要打包传送给地面 PHM 系统时，车载 PHM 系统负责利用当前时空信息生成消息包的 RDID 及 DID Document，将消息的 RDID 与自身的 RDID 作为消息头一并打包发送，在数据流和数据存储中，此 RDID 就包含消息的追溯信息。

3)车载 PHM 系统收到地面感知系统来源的数据时，可向地面 PHM 系统申请身份验证，地面感知系统也可向地面 PHM 系统申请可验证声明附加在其数据包中，供车载 PHM 系统验证。

在实验室环境采用 3 台服务器(Ubuntu 环境，16vCPU，32GB 内存)，1 台工控机(Ubuntu 环境，4vARM64CPU，8GB 内存)，6 台 RaspberryPi-CM4(Debian 环境，4vARM64CPU，2GB 内存)搭建了模拟验证环境如图 10，其中服务器模拟管理系统、地面 PHM 系统和地面感知系统，工控机模拟车载 PHM 系统，树莓派模拟终端。采用以太坊 Ethereum 部署底层区块链网络，采用 IPFS 作为底层的分布式持久化存储文件系统，开发智能合约完成打包上链功能。BDS 系统采用移远 RM500Q 提供的定位消息，部署在一台服务器和一台工控机上，从 $GBGGA 报文提取时空信息并以 100ms 周期间隔进行更新，由此产生和更新设备和消息的 RDID。实测由于采用了 L2 分布式信任网络机制，RDID 服务独立于业务运行，摘要上链的方法，系统开销较小，与不采用 RDID 的数据生成与传输模式没有可见的性能下降，如表 1。

表 1　RDID 服务工作效率

Tab. 1　RDID service efficiency

主体	平均生成时间	上链时间	平均验证响应时间
服务器	＜10 ms	10 s	＜30 ms
工控机	＜30 ms	10 s	＜80 ms
CM4	＜50 ms	10 s	＜100 ms

图 10　测试环境实景

Fig. 10　Test environment

在 Ubuntu 环境下基于 Python 编写模拟程序，引入基于声誉的信任度计算模型[18-19]构建仿真测试环境，对比具有 BDS PNT 信息的节点和没有该信息的节点。BDS PNT 信息可以用于数据一致性校验和时空逻辑校验，从而增加直接信任值的信息维度和计算参数复杂度；推荐节点可基于 BDS PNT 信息生成相关系数作为推荐权重，动态调整推荐信任因子，以提高推荐信任值的可靠性。添加 50 个模拟节点，其中 25 个没有 BDS 信源、25 个有 BDS 信源，并且两类节点中各有5个节点被设置为恶意节点，恶意节点会随机伪造 BDS PNT 信息，生成恶意随机数据。设定所有节点的初始信任值为 0.5，按照每秒 2 次信息交互的速率，进行信任值迭代。统计如图 11，可见加入 BDS PNT 信息的节点相对于没有此信息的节点，信任度能够更加迅速地响应调整，信任评估更加敏感，系统整体可信度提高。

由模拟试验和仿真可见，采用 RDID 服务的系统整体加解密机制运行良好，使用方可以通过 RDID 服务验证所收到的信息的所有者，验证响应的系统用时在 100 ms 以内，保障系统可信安全。

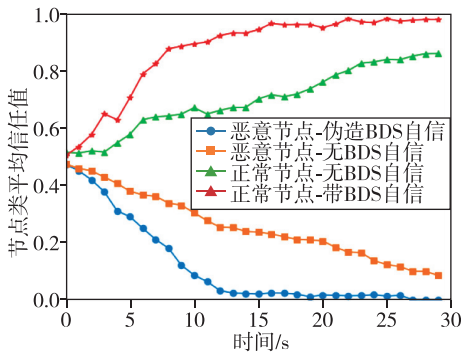

图 11 节点类平均信任值仿真

Fig. 11 Node average trust value simulation

4 结论

1)本文创新性地利用区块链去中心化身份管理、信息不可篡改、可追溯和不可抵赖等特性结合 DID 技术设计了用于铁路物联网的可信数字身份服务 RDID,以期利用铁路物联网本身的分布式特性为其信息安全防护提供重要工具。

2)本文根据 W3C 标准,结合实际应用需求设计了 RDID 的服务架构、生成流程、流转流程和验证流程,并结合 BDS 提供的时空信息优化了 DID 组成和验证方法,提高了 RDID 的可验证性和安全性。

3)后续研究会进一步优化拓展 BDS 的 PNT 时空信息在整个身份标识安全系统中的应用,包括短报文机制、精确授时和差分定位的应用。

面向铁路物联网应用对大体量设备进行分布式自主管理的需求,区块链具有的分布式计算和群体可信协作机制可以为物联网安全挑战提供有效解决方案,也可为在网设备和主体的身份认证与访问控制、全生命周期全链条的数据安全可信追溯等提供有效技术手段。

参考文献

[1] 张彦. 智能铁路时代网络安全问题探讨[J]. 铁路计算机应用, 2019, 28(3): 51-56.
ZHANG Y. Discussion on cybersecurity security of intelligent railway[J]. Railway Computer Application, 2019, 28(3): 51-56(in Chinese).

[2] 孙鹏, 张惟皎. 铁路物联网系统的安全挑战与对策研究[J]. 铁路计算机应用, 2022, 31(10): 62-67.
SUN Peng, ZHANG Weijiao. Security challenges and countermeasures of railway internet of things system [J]. Railway Computer Application, 2022, 31(10): 62-67(in Chinese).

[3] BUTUN I, ÖSTERBERG P, SONG H. Security of the internet of things: vulnerabilities, attacks, and countermeasures[J]. IEEE Communications Surveys & Tutorials, 2019, 22(1): 616-644.

[4] REED D, SPORNY M, LONGLEY D, et al. Decentralized identifiers (DIDs) v1.0[Z]. World Wide Web Consortium (W3C), 2019.

[5] FAíSCA J G, ROGADO J Q. Decentralized semantic identity[C]//Proceedings of the 12th International Conference on Semantic Systems. 2016: 177-180.

[6] 焦英楠, 陈英华. 基于区块链技术的物联网安全研究[J]. 软件, 2018, 39(2): 88-92.
JIAO Y N, CHEN Y H. Research on blockchain technology in the security field of IoT[J]. Computer Engineering & Software, 2018, 39(2): 88-92(in Chinese).

[7] RANA R, ZAEEM R N, BARBER K S. An assessment of blockchain identity solutions: minimizing risk and liability of authentication[C]//2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI). IEEE, 2019: 26-33.

[8] 蔚保国, 鲍亚川, 杨梦焕, 等. 通导一体化概念框架与关键技术研究进展[J]. 导航定位与授时, 2022, 9(2): 1-14.
YU Baoguo, BAO Yachuan, YANG Menghuan, et al. Conceptual framework and research progress on communication and navigation intergration[J]. Navigation Positioning and Timing, 2022, 9(2): 1-14(in Chinese).

[9] 高为广, 隋叶叶, 李敏, 等. 北斗系统 RNSS 服务下行导航信号应用模式及使用建议[J/OL]. 武汉大学学报(信息科学版): 1-13[2023-03-11]. https://doi.org/10.13203/j.whugis20220691.
GAO Weiguang, SUI Yeye, LI Min, et al. Application mode and usage suggestion of BDS downlink navigation signals for RNSS service[J/OL]. Geomatics and Information Science of Wuhan University: 1-13[2023-03-11]. https://doi.org/10.13203/j.whugis20220691(in Chinese).

[10] YANG Y, XU Y, LI J, et al. Progress and performance evaluation of BeiDou global navigation satellite system: data analysis based on BDS-3 demonstration system[J]. Science China Earth Sciences, 2018, 61(5): 614-24.

[11] 洪学敏, 周洋, 许雪婷, 等. 基于 5G 的通导融合位置认证系统性能分析[J]. 导航定位与授时, 2022, 9(2): 65-72.
HONG Xuemin, ZHOU Yang, XU Xueting, et al.

Performance analysis of positing verification system in 5G-based intergrated communiction and navigation networks[J]. Navigation Positioning and Timing, 2022, 9(2): 65-72(in Chinese).

[12] 刘娅,李孝辉,赵志雄,等. 基于北斗卫星的纳秒级全球授时系统[J]. 导航定位与授时,2022,9(3):14-22.
LIU Ya, LI Xiaohui, ZHAO Zhixiong, et al. Nanoseconds deviation timing service system for global user based on BDS[J]. Navigation Positioning and Timing, 2022, 9(3): 14-22(in Chinese).

[13] 邵奇峰, 金澈清, 张召, 等. 区块链技术:架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAQ Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988(in Chinese).

[14] CHRIS D. Introducing ethereum and solidity foundations of cryptocurrency and blockchain programming for beginners[M]. Apress, 2017.

[15] 宋智明,余益民,王贵文,等. 基于区块链智能合约的数字身份可验证凭证零知识认证和管理架构[J]. 信息安全学报, 2023, 8(1):55-77.
SONG Zhiming, YU Yimin, WANG Guiwen, et al. Zero-knowledge authentication and management architecture of verifiable certificate of digital identity based on smart contracts of blockchain[J]. Journal of Cyber Security, 2023, 8(1):55-77(in Chinese).

[16] Camilo L,W. J B,Julian Z, et al. Industry 4.0 technologies applied to the rail transportation industry: a systematic review[J]. Sensors,2022,22(7).

[17] 梁建英. 高速列车智能诊断与故障预测技术研究[J]. 北京交通大学学报, 2019, 43(1):63-70.
LIANG Jianying. Research on intelligent diagnosis and fault prediction technology for highspeed trains [J]. Journal of Beijing Jiaotong University, 2019, 43(1):63-70(in Chinese).

[18] TAN Z, WANG X, WANG X. A novel iterative and dynamic trust computing model for large scaled P2P networks [J]. Mobile Information Systems, 2016: 1-12.

[19] 朱子豪, 刘光杰. 一种面向物联网节点的动态信任评估模型[J]. 重庆理工大学学报(自然科学), 2022, 36(7): 188-196.
ZHU Zihao, LIU Guangjie. Dynamic trust assessment model for internet of things node[J]. Journal of Chongqing University of Technology(Natural Science), 2022, 36(7): 188-196(in Chinese).

(编辑:孟彬)