 DOI: https://doi.org/10.12349/iser.v6i2.4802

Construction of TDCS/CTC network security protection system based on blockchain technology

Feng Wang Xiaotong Du

China Railway Hohhot Group Co., Ltd. Hohhot Electric Power Section, Hohhot, Inner Mongolia, 010000, China

Abstract

With the rapid development of Internet technology and the deepening of digital transformation, TDCS and CTC play a crucial role in railway transportation. However, these systems are also facing increasing cybersecurity threats. Blockchain technology, with its decentralization, data immutability and transparency, provides a new solution for TDCS/CTC network security protection. As a phased result of network development, blockchain adopts leading technologies such as consensus mechanism, point-to-point transmission, distributed data storage and encryption algorithms, which can establish a new network security defense system based on blockchain and greatly improve the defense performance of network security. This paper aims to explore the construction of TDCS/CTC network security protection system based on blockchain technology, analyze how blockchain technology enhances the security of TDCS/CTC system, and propose specific implementation strategies and advantages.

Keywords

blockchain technology; TDCS/CTC; Network security; Protection system

基于区块链技术的 TDCS/CTC 网络安全防护体系构建

王峰 杜晓桐

中国铁路呼和浩特局集团有限公司呼和浩特电务段，中国 · 内蒙古 呼和浩特 010000

摘 要

随着互联网技术的飞速发展和数字化转型的深入，TDCS与CTC在铁路运输中扮演着至关重要的角色。然而，这些系统也面临着日益严峻的网络安全威胁。区块链技术，以其去中心化、数据不可篡改和透明性等特点，为TDCS/CTC网络安全防护提供了新的解决方案，区块链作为网络发展的阶段性成果，其采用共识机制、点对点传输、分布式数据存储和加密算法等领先技术，可以建立一个全新的基于区块链的网络安全防御体系，大大提高网络安全的防御性能。本文旨在探讨基于区块链技术的TDCS/CTC网络安全防护体系的构建，分析区块链技术如何增强TDCS/CTC系统的安全性，并提出具体的实施策略和优势。

关键词

区块链技术；TDCS/CTC；网络安全；防护体系

1 引言

铁路运输作为国家重要的基础设施，其安全性和可靠性直接关系到国民经济的稳定和发展。近年来，随着信息技术的广泛应用，TDCS/CTC 系统已成为铁路运输中不可或缺的一部分然而，随着网络技术的不断发展，这些系统也面临着越来越多的网络安全威胁，如数据篡改、非法访问和恶意攻击等。这些威胁不仅可能导致系统瘫痪，还可能引发严重的交通事故，对人民生命财产安全构成严重威胁。因此，加强 TDCS/CTC 系统的网络安全防护显得尤为重要。

【作者简介】王峰（1988–），男，中国内蒙古土默特右旗人，本科，从事铁道通信信号研究。

2 TDCS/CTC 系统架构与功能

2.1 系统架构

TDCS/CTC 系统是铁路信息化建设的关键成果，其架构复杂且功能强大，涵盖了多个层次和组成部分，以实现对铁路运输的高效调度指挥。从整体架构来看，TDCS/CTC 系统主要由调度中心子系统、车站子系统以及网络通信子系统三大部分构成。

调度中心子系统是整个 TDCS/CTC 系统的核心大脑，负责对全路列车运行的宏观调控和管理。它主要包括数据库服务器、应用服务器、调度员工作站、助理调度员工作站、值班主任工作站等关键设备。车站子系统是 TDCS/CTC 系统的基层执行单元，分布在各个车站，负责实现对本站列车进路的控制、信号设备的监控以及与调度中心的信息交互。车站子系统主要包括车站自律机、车务终端、综合维修终端、

电务维护终端等设备。网络通信子系统是连接调度中心子系统和车站子系统的桥梁，负责实现数据的快速、可靠传输，采用了 2Mb/s 光通道及电缆回线构成的专用广域网，信息传输按 TCP/IP 协议进行，确保了系统的通信稳定性和兼容性。网络通信子系统还包括网络设备、电源设备、防雷设备等，以保障网络的正常运行和数据的安全传输。

2.2 功能

在功能方面，TDCS 主要实现了列车调度指挥信息的记录、分析、车次号校核、自动报点、正晚点统计、运行图自动绘制、调度命令及计划的下达、行车日志自动生成等功能。例如，通过对列车运行数据的实时采集和分析，系统能够自动生成准确的列车运行图，为调度员提供直观的列车运行信息，帮助其合理安排列车运行计划；同时，通过车次号校核和自动报点功能，能够实时掌握列车的位置和运行状态，及时发现列车晚点等异常情况，并采取相应的措施进行调整 [1]。

3 区块链技术在 TDCS/CTC 网络安全防护中的应用优势

3.1 防止数据篡改与伪造

区块链技术的分布式存储和共识机制特性，为有效防止 TDCS/CTC 系统中的数据被篡改和伪造提供了坚实保障。在传统的 TDCS/CTC 系统中，数据通常集中存储在中心服务器上，这种集中式存储方式存在单点故障和易受攻击的风险。一旦中心服务器被攻击，数据就可能被恶意篡改或伪造，从而对铁路运输安全造成严重威胁。而区块链技术采用分布式存储方式，将数据分散存储在网络中的多个节点上。每个节点都保存着完整的数据副本，并且可以独立地对数据进行验证和记录。当有新的数据产生时，这些数据会被广播到整个网络中的各个节点，每个节点都会对数据进行验证和共识。只有当大多数节点都认可数据的有效性时，数据才会被添加到区块链中。

3.2 数据加密与隐私保护

在数据加密存储和传输方面，区块链技术发挥着重要作用，为 TDCS/CTC 系统的数据安全提供了多维度的保障。区块链采用非对称加密算法，为每个用户生成一对公私钥。公钥用于加密数据，私钥则由用户自行保管，用于解密数据和对交易进行签名。在 TDCS/CTC 系统中，当列车运行数据、调度命令等关键信息需要存储或传输时，首先会使用接收方的公钥对数据进行加密。加密后的数据在网络中传输或存储在节点上，即使数据被第三方截获，由于没有对应的私钥，也无法解密获取原始数据，从而确保了数据的机密性 [2]。

3.3 基于区块链的数字身份认证

在 TDCS/CTC 系统中，利用区块链技术构建数字身份认证体系，能够显著提升用户身份认证的安全性和可靠性。传统的身份认证方式，如用户名密码、数字证书等，存在着诸多安全隐患。用户名密码容易被猜测、窃取或泄露，一旦密码泄露，用户身份就可能被冒用，导致系统权限被非法获取，进而对列车调度指挥等关键业务造成严重影响。数字证书认证虽然相对较为安全，但依赖于中心化的证书颁发机构（CA），CA 一旦遭受攻击，整个认证体系将面临信任危机。

在具体实现过程中，用户在注册时，将自己的身份信息，如姓名、身份证号、工号等，经过加密处理后存储在区块链上，形成一个独一无二的数字身份。同时，系统为用户生成一对公私钥，私钥由用户自行妥善保管，公钥则存储在区块链上。当用户登录 TDCS/CTC 系统时，用户使用私钥对登录请求进行签名，系统通过区块链上存储的公钥验证签名的真实性。如果签名验证通过，则证明用户身份合法，允许用户登录系统。

3.4 防范 DDoS 攻击

在基于区块链的 TDCS/CTC 网络中，数据存储和处理被分散到众多的节点上，不存在单一的中心控制点。每个节点都具有相同的地位和功能，它们共同参与数据的验证、存储和传输。当面对 DDoS 攻击时，攻击者需要同时攻击大量的节点才能对整个网络造成实质性影响。然而，由于区块链网络中的节点数量众多且分布广泛，攻击者很难控制足够数量的节点来实施有效的攻击。以比特币区块链网络为例，它拥有全球范围内数以万计的节点，这些节点共同维护着区块链的运行。即使遭受大规模的 DDoS 攻击，部分节点被攻击或瘫痪，其他节点仍然能够继续工作，确保区块链网络的正常运行。

4 关键技术实现

4.1 共识算法选择与优化

在 TDCS/CTC 网络安全防护体系中，共识算法的选择与优化至关重要，它直接影响着系统的性能、安全性和可靠性。目前，常见的区块链共识算法包括工作量证明（PoW）、权益证明（PoS）、股份授权证明（DPoS）等，每种算法都有其独特的特点和适用场景。

PoW 算法通过让节点进行复杂的数学运算来竞争记账权，只有率先完成运算的节点才有资格将新的交易记录打包成区块，并添加到区块链中。这种算法的优点是具有较高的安全性和去中心化程度，因为攻击者需要控制超过一半的节点算力才能篡改区块链数据，这在实际操作中难度极大。

PoS 算法则根据节点持有的权益来分配记账权，持有权益越多的节点获得记账权的概率越大。与 PoW 算法相比，PoS 算法具有能耗低、交易处理速度快等优点。在 TDCS/CTC 系统中，采用 PoS 算法可以减少节点的计算负担，提高系统的运行效率。但是，PoS 算法也存在一些问题，如可能出现权益集中的情况，导致少数节点掌握过多的记账权，从而影响系统地去中心化特性和安全性。

DPoS 算法是一种基于选举的共识算法，它通过节点投票选举出一定数量的代表节点来进行记账和验证。代表节点

按照一定的规则轮流记账，其他节点对代表节点的记账结果进行验证。DPoS 算法具有高效、低能耗、可扩展性强等优点，能够快速处理大量交易，适用于对实时性要求较高的场景。在 TDCS/CTC 系统中，DPoS 算法可以确保系统能够及时处理列车运行数据和调度命令，保障铁路运输的高效运行。同时，通过合理的选举机制和监督机制，可以有效避免代表节点的权力滥用，保证系统的安全性和公正性。

综合考虑 TDCS/CTC 系统的特点和需求，选择 DPoS 算法作为共识算法较为合适。为了进一步优化 DPoS 算法在 TDCS/CTC 系统中的性能，可以从以下几个方面进行改进：一是优化选举机制，通过引入信誉度评估等因素，确保选举出的代表节点具有较高的可靠性和稳定性，避免因代表节点故障或恶意行为导致系统出现问题；二是加强对代表节点的监督和管理，建立实时监测代表节点运行状态的机制，及时发现并处理异常情况；三是提高通信效率，通过优化通信协议和数据处理流程，减少节点之间的通信开销和数据处理时间，进一步提升系统的响应速度和处理能力 [3]。

4.2 智能合约开发部署

智能合约的开发与部署是基于区块链技术的 TDCS/CTC 网络安全防护体系的关键环节，它能够实现身份认证、访问控制、数据管理等重要功能，为系统的安全稳定运行提供有力支持。

在开发基于区块链的身份认证智能合约时，首先需要明确合约的功能和逻辑。合约应具备用户身份信息的存储、验证和更新功能，确保只有合法用户能够通过身份认证。合约还应支持多种身份认证方式，如密码认证、指纹认证、面部识别认证等，以满足不同用户的需求。在具体实现过程中，可以使用 Solidity 等智能合约开发语言，结合区块链平台提供的开发工具和接口，编写身份认证智能合约代码。例如，使用 Solidity 编写的身份认证智能合约可以包含以下主要函数：注册函数，用于用户注册身份信息，将用户的身份信息（如用户名、密码、公钥等）存储在区块链上；登录函数，用于用户登录系统，验证用户输入的身份信息是否与区块链上存储的信息一致，如果一致则允许用户登录；更新函数，用于用户更新身份信息，如修改密码、添加新的认证方式等。

在开发访问控制智能合约时，需要根据 TDCS/CTC 系统的业务需求和安全策略，制定详细的访问控制规则。这些规则应明确不同用户角色（如调度员、车站值班员、维护人员等）对系统资源（如列车运行数据、调度命令、设备状态信息等）的访问权限。合约应具备权限管理功能，能够根据用户的角色和权限，自动判断用户是否有权访问特定的资源。使用 Solidity 编写的访问控制智能合约可以包含以下关键函数：权限设置函数，用于管理员设置不同用户角色的访问权限，将权限信息存储在区块链上；访问验证函数，用于在用户访问系统资源时，验证用户的权限是否符合访问要求，如果符合则允许访问，否则拒绝访问。

4.3 加密算法应用

在 TDCS/CTC 网络安全防护体系中，加密算法的应用是保障数据安全的关键手段。通过采用对称加密、非对称加密等多种加密算法，能够有效保护数据在存储和传输过程中的机密性、完整性和真实性。

对称加密算法是指加密和解密使用相同密钥的加密算法，如 AES（高级加密标准）算法。AES 算法具有加密速度快、效率高的特点，适用于对大量数据进行加密处理。在 TDCS/CTC 系统中，当需要对列车运行数据、调度命令等大量数据进行存储时，可以使用 AES 算法对数据进行加密。具体过程为，首先生成一个随机的 AES 密钥，然后使用该密钥对数据进行加密，将加密后的数据存储在区块链节点或其他存储设备中。在需要读取数据时，使用相同的 AES 密钥对加密数据进行解密，恢复原始数据。AES 算法的加密强度较高，能够有效防止数据被窃取和篡改。

非对称加密算法则使用一对密钥，即公钥和私钥，公钥用于加密数据，私钥用于解密数据。常见的非对称加密算法有 RSA 算法、椭圆曲线加密（ECC）算法等。RSA 算法是一种广泛应用的非对称加密算法，它基于大整数分解的困难性原理，具有较高的安全性。在 TDCS/CTC 系统中，非对称加密算法主要用于身份认证和数字签名。例如，在用户登录系统时，用户使用自己的私钥对登录信息进行签名，系统通过用户的公钥验证签名的真实性，从而确认用户的身份。在数据传输过程中，发送方使用接收方的公钥对数据进行加密，接收方使用自己的私钥对加密数据进行解密，确保数据的机密性。

5 结语

综上所述，区块链技术以其去中心化、数据不可篡改和透明性等特点，为 TDCS/CTC 系统提供了强有力的网络安全保障。通过构建基于区块链的网络安全防护体系，可以有效抵御数据篡改、非法访问和恶意攻击等网络安全威胁，确保铁路运输的安全和稳定。展望未来，随着区块链技术的不断发展和完善，其在 TDCS/CTC 网络安全防护领域的应用前景将更加广阔。

参考文献

[1] 苗义烽,宋毅,张芸鹏.基于国密算法的TDCS/CTC系统通信加密技术应用方案研究[J].铁道通信信号,2024,60(10):58-64.

[2] 郝俊丽.基于铁路通信承载网TDCS保障策略的研究[D].内蒙古科技大学,2023.

[3] 陶然,陈洪雨,毛家明.基于TDCS/CTC的分路不良统计分析系统设计与实现[J].铁道通信信号,2023,59(06):86-90.