文章编号：0253-374X(2024)02-0157-09 **DOI**：10.11908/j.issn.0253-374x.23361

面向城轨云平台边界安全防护的动态信任管理方法

张　雷[1,2]，徐　倩[1]，何积丰[1,2]，曾小清[1]，宁　正[1]
（1. 同济大学 交通运输工程学院，上海 201804；2. 同济大学 上海自主智能无人系统科学中心，上海 201810）

摘要：针对城轨云平台边界数量多、边界安全防护薄弱的问题，分析了城轨云与工业控制网络协同交互过程，提出了一种面向城轨云平台边界安全防护的动态信任管理方法，包括异常行为识别、信任评估、信任更新、基于信任值的动态访问控制。根据城轨云的综合监控系统网络拓扑，分析了未经授权控制指令、违规控制指令、干扰正常控制指令三类异常行为。结果表明，所提出的动态信任管理方法能够有效抵御恶意节点发起的异常行为；对于不同节点、不同异常行为的信任值变化不同；符合“缓升快降”的规则，能够保障城轨云平台细粒度的边界安全防护。

关键词：信任管理；城轨云；边界安全防护；异常控制指令
中图分类号：U285.8　　**文献标志码**：A

A Dynamic Trust Management Method for Border Security Protection of Metro Cloud Platform

ZHANG Lei[1,2], *XU Qian*[1], *HE Jifeng*[1,2], *ZENG Xiaoqing*[1], *NING Zheng*[1]
(1. College of Transportation Engineering, Tongji University, Shanghai 201804, China; 2. Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai 201810, China)

Abstract: To address the problem of numerous borders and weak border protection in metro cloud platform, the collaborative interaction between the cloud and the industrial control network is analyzed, and a dynamic trust management method for border security protection of metro cloud platform is proposed. The method consists of abnormal behavior recognition, trust evaluation, trust updating, and trust-based dynamic access control. Based on the network topology of metro cloud-based integrated supervisory control system, three kinds of abnormal control commands are simulated, i.e., unauthorized control commands, non-conforming control commands, and interference with normal control commands. The results show that the proposed method can effectively resist abnormal control commands initiated by malicious nodes. The changes in trust values vary for different nodes and different types of misbehaviors following the rule of “slow rise and fast fall”, thus ensuring fine-grained boundary protection for the metro cloud platform.

Keywords: trust management; metro cloud; border security protection; abnormal control commands

云平台从数据流、控制流和大数据交互三方面来满足交通信息物理融合系统中多应用支持、拥塞控制、资源配置、快速移动、无缝覆盖等需求[1]。城轨云是智慧城市轨道交通建设的支撑平台，城轨云将在便利大数据分析、打破信息孤岛、承载智慧城轨业务等方面带来变革。然而，引入城轨云后，外部服务网的业务会频繁与安全生产网、内部管理网进行交互，容易导致攻击的蔓延[2]。在传统静态边界安全防护措施下，城轨云平台面临着边界数量多、可扩展性弱、边界整体利用率低、边界安全性较弱等边界安全问题[3-4]。信任管理是计算及维护信任的一组步骤，包括定义信任、识别信任相关元素、信任计算、信任传播、信任聚合等环节[5]。研究城轨云平台的信任管理方法是实现细粒度、动态边界安全防护的有效措施之一[6-7]。

在对等网络(peer to peer，P2P)[8]、无线传感器网络(wireless sensor network，WSN)[9]、推荐系统[10]、车载移动自组织网络(vehicular Ad Hoc network，VANET)[11]等领域，已提出了一些信任管理方法，这些方法建立在概率论、贝叶斯推理、模糊理论、Dempster-Shafer证据理论、半环代数理论等理论基础上[12]。随

收稿日期：2023-10-24
基金项目：国家自然科学基金资助项目(52172329)；国家重点研发计划资助项目(2022YFB4300501)；上海市科委资助项目(23DZ2204900)
第一作者：张　雷，男，教授，工学博士，主要研究方向为AI+交通、可信计算在工业物联网中的技术开发等。E-mail：reizhg@tongji.edu.cn
通信作者：何积丰，男，教授，工学博士，主要研究方向为可信AI等。E-mail：19857@tongji.edu.cn

论文拓展介绍

着云计算的发展,许多研究工作围绕云服务提供商、云用户、身份提供者等各个参与方的信任进行评估和管理。为了适应云计算环境中多域的特点,文献[13]提出了一种基于动态用户信任值的访问控制模型。考虑不同用户和服务提供者的行为参数,例如错误请求、虚假请求、未经授权的请求和总请求数,文献[14]将模糊c-means聚类、Mamdani模糊方法分别应用于云用户及云服务提供商的信任评估上。为了解决传统静态联合身份管理在应用于云计算技术时可扩展性不足的问题,文献[15]提出了一种模糊认知图的动态信任管理模型,该模型能够使云服务提供商实时预测目标身份提供者的信任级别。

本文作者在前期研究中提出了一种基于诱导有序加权平均算子的轨道交通数据平台的信任管理方法[16]。通过对比文献,现有的信任管理在理论和方法已取得一定研究成果,如表1所示,现有的云计算信任管理方法集中在云计算层多个参与方之间的信任,但是对于将信任管理应用于城轨云与工控系统综合系统的研究还缺乏深入研究。

表1 与现有研究工作的比较

Tab. 1 Comparison with other current studies

文献	时间	对象	直接信任	间接信任	信任机制的抗攻击性	考虑能耗	边界安全防护措施
[8]	2015	P2P电子商务	未提及	基于余弦相似度的邻居信任	Sybil攻击	否	是
[9]	2018	并置式、分布式WSN	主观逻辑	欧氏距离	通过抗波动检测异常	是	是
[10]	2022	社交物联网推荐系统	矩阵中的计算	局部和全局加权中心性	恶意推荐(如串通攻击、坏话攻击)	否	否
[11]	2022	VANET	贝叶斯推理	考虑置信度的第三方推荐	否	否	是
[13]	2021	云计算	矩阵中的计算	余弦相似度	恶意推荐	否	是
[14]	2019	云计算	模糊认知图	无	无	否	是
[15]	2022	云计算	模糊逻辑	无	无	无	是
本文	2024	云计算与工控系统	主观逻辑	考虑惩罚、奖励的第三方推荐	是	是	是

为了解决上述问题,提出一种用于城轨云平台异常控制指令分析的信任管理方法。该方法以时间窗内的交互记录作为数据源,提出一种直接信任值、间接信任值和综合信任值的信任计算方法。同时,考虑奖励因子和惩罚因子的信任更新方法,最终实施基于信任决策的动态访问控制,以实现细粒度的边界安全防护目标。选择城轨云下的综合监控系统作为分析示例系统,这是率先进行单专业云改造的工控系统。

1 城轨云平台两级三网结构及边界防护需求

城轨云平台按服务范围划分为中心云平台、站段云两级结构,按网络类型划分为外部服务网、内部管理网、安全生产网三类网络,如图1所示。中心云平台与轨道交通运营商、设备供应商企业及相关科研单位合作,利用支撑平台提供的实时数据和从终端传递的列车运行信息,提供宏观的数据分析与决策。而站段云平台实现列车调度、运行控制、监控运维等功能,为用户提供统计、可靠性分析等非实时要求的服务[17]。城轨云网络安全防护的总体策略遵循“系统自保、平台统保、等保达标、边界安全防护”[2]。其中,边界安全防护的目标分为接入层安全及区域边界安全两部分。接入层安全主要关注外部网络或终端设备接入的数据和用户的安全,而区域边界安全主要关注不同功能区域之间的安全。边界安全防护方法包括边界访问控制、边界完整性检查、边界入侵防御、边界安全审计、边界恶意代码防范,本文提出的信任管理方法是一种创新的边界访问控制方法,有效应对边界安全威胁。

2 城轨云平台动态信任管理方法的实施过程

将城轨云平台的信任管理组件分为三个部分:信任管理核心组件、信任管理调整组件、数据库,如图2所示。对于计算能力、存储能力充足的设备,可选择运行在可信平台模块(trusted platform module, TPM)上。TPM是一种内置于主板上的硬件安全模块,能够存储密钥、数字证书和其他机密信息,实现安全启动、数据加密和数字签名等功能[18]。对于计算能力、存储能力较小的设备,只需配置信任管理核心组件。

2.1 信任评估

在时间窗T,实施一个控制指令,在节点i部署的信任收集组件收集与目标节点j的记录,包括节点i与节点j的直接历史交互序列及相邻节点与节点j的历史交互序列,分别用于直接信任的计算、间接信任的计算。为了缓解“冷启动”问题,一些关键节点

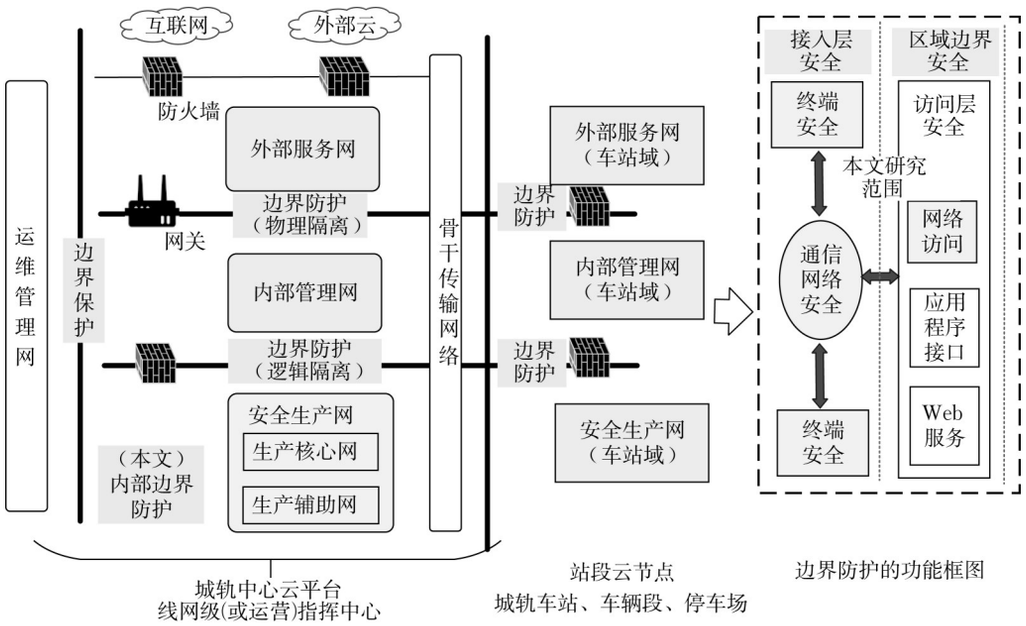


图1　城轨云平台的两级结构及三网隔离示意图

Fig. 1　Two-tier structure and three-network isolation diagram of metro cloud platform

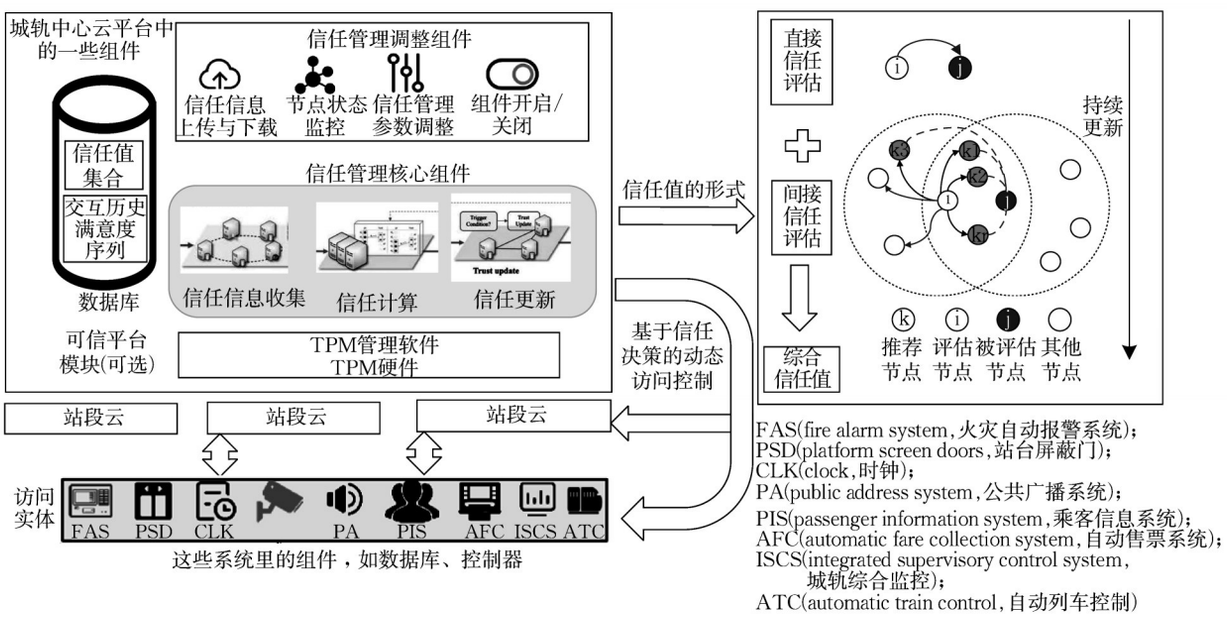


图2　面向城轨云平台的动态信任管理方法的结构图

Fig. 2　Structural diagram of dynamic trust management method for metro cloud platform

的历史信任值存储在数据库中，以历史信任值作为起点，从而加快信任评估。

(1)直接信任评估：主观逻辑是一种处理不确定性的逻辑框架，被广泛应用于信任管理[19-20]。该框架包含了三个核心概念，即belief(信任)、disbelief(不信任)和uncertainty(不确定性)，表示为$\{b,d,u\}$。直接信任值的计算式如下：

$$\mathrm{T\_Dir}_{ij}=\frac{2b+u}{2} \tag{1}$$

式中：b,u分别指信任、不确定性，计算公式分别为$b=\dfrac{N_s}{N_s+N_f+1}$，$u=\dfrac{1}{N_s+N_f+1}$；N_s，N_f分别是指一段时间内成功交互的次数、失败交互的次数。

(2)间接信任评估：当节点i和节点j之间没有直接交互时，执行下述迭代计算。获取节点j在同一时间窗T与其他节点的历史交互序列，通过加权平均，得到间接信任值RT_{ij}，如式(2)所示：

$$\mathrm{T\_Rec}_{ij}=\frac{\sum t_{ik}t_{kj}}{\sum t_{ik}},\ k\in Q_1 \tag{2}$$

式中:t_{ik}为节点i和k之间的信任值;t_{kj}为节点k和j之间的信任值。

在计算间接信任时,需要考虑节点之间的通信跳数。由于交互概率低,考虑距离i或j过远的节点给出的间接信任值可能不具有实际意义;相反,会增加计算量。因此,本文仅考虑2跳以内的节点。

2.2 信任更新

基于奖励因子、惩罚因子、交互次数因素,根据直接信任和间接信任的加权值计算综合信任值。节点i在当前时间t对节点j的综合信任值,如式(3)所示。

$$T_{ij}=\begin{cases}w_1\cdot\mathrm{T\_Dir}_{ij}+w_2\cdot\mathrm{T\_Rec}_{ij}+\mathrm{RW}(t), & N_{\mathrm{d}}(t)<\theta_n\\ \mathrm{T\_Dir}_{ij}+\mathrm{RW}(t), & N_{\mathrm{d}}(t)\geqslant\theta_n\end{cases} \tag{3}$$

式中:w_1和w_2分别表示当前节点在时间点t的直接信任值和推荐信任值的权重;$N_{\mathrm{d}}(t)$表示直接交互次数。当$N_{\mathrm{d}}(t)$在一个时间窗T内达到θ_n时,即$N_{\mathrm{d}}(t)\geqslant\theta_n$,即双方完全建立了信任关系,此时只考虑直接信任。

(1)同一个时间窗内,w_1和w_2不变;不同时间窗内,w_1和w_2可以动态调整。权重设置考虑两类情况:① 空闲阶段:当节点之间的连接较少或处于空闲时间时,信任收集组件将收集更多的间接信任信息,从而需要增加w_2。② 频繁交互阶段:信任收集组件会接受更直接的交互信息,从而需要增加w_1。具体地,将w_1和w_2分别定义为$w_1=1-\alpha^{N_{\mathrm{d}}(t)}$,$w_2=\alpha^{N_{\mathrm{d}}(t)}$。通过这种动态调整,提出的方法能够适应不同时间段的交互特征和信任需求。

(2)奖励因子$\mathrm{RW}(t)$用于调节奖励程度。本文根据节点的稳定性指标确定$\mathrm{RW}(t)$,即在一段时间内持续提供良好服务的能力。持续提供良好服务的节点应当具有较高的信任值,未能持续提供良好服务的节点的信任值则应降低。此外,信任值的增幅过大可能导致"On-Off(开-关)攻击",即攻击者通过反复增加和降低信任值而干扰系统的正常运行。因此在设计$\mathrm{RW}(t)$时,需要限制信任值的增幅。综上需求,$\mathrm{RW}(t)$计算如下:

$$\mathrm{RW}(t)=0.1N_{\mathrm{suc}}(t)/N(t) \tag{4}$$

式中:$N_{\mathrm{suc}}(t)$指连续成功交互的次数;$N(t)$是总交互次数;常数0.1用于缩放结果,限制信任值的增幅。

2.3 基于信任决策的动态访问控制

在每个时间窗结束后,对获取的信任值进行分级,再设置访问实体的权限。每个信任级别对应不同的阈值,较高信任值的节点可以执行更重要的操作。如果访问实体的信任指标值小于当前信任级别的阈值,则该访问实体将降级,同时云平台将执行控制措施以约束其权限。相反,如果访问实体的信任值超过较高信任级别的阈值,则需要增加其访问权限。

基于访问权限粒度及实际需求,划分了四级访问级别。将节点默认信任值设置为0.5,因此低于0.5时权限为"拒绝访问"。此外,为了提供更细粒度的访问控制,将信任值范围在[0.5,1]划分了三个级别,由低级别到高级别分别是"暂时拒绝访问"、"受监控的访问"、"完全访问"。在实际场景中,可信设备的信任值通常分布在[0.8,1]范围内。因此,将"完全访问"权限所对应的信任值范围划分为[0.8,1],以确保在较高的信任度下获得访问权限。当前划分为四级访问级别,如表2所示。然而,在更加严苛的安全需求下,需要设置更细粒度的访问级别,需要进一步划分。

表2 访问权限分级表

Tab. 2 Hierarchy of access permissions

级别	信任值	控制措施	权限
I	[0.8,1]	N/A(不需要)	完全访问
II	[0.6,0.8)	降级权限受限访问	受监控的访问
III	[0.5,0.6)	重新验证访问	暂时拒绝访问
IV	[0,0.5)	阻断连接访问	拒绝访问

3 城轨云边界安全防护实验及结果

3.1 实验场景及仿真参数设置

3.1.1 城轨云综合监控系统的真实网络拓扑

在传统的城轨综合监控系统中,每个车站、车辆段均各自设置服务器来处理和存储本站数据;最终,所有站段级综合监控系统的数据会传输到中央级综合监控系统。然而,这种架构存在一些问题,如高成本和资源利用效率低下,无法进行灵活的资源调配。为了解决这些问题,引入城轨云的概念可以改善综合监控系统的结构。在城轨云中,中央级和站段级的服务器被虚拟化为位于中央服务器群组中的虚拟服务器。通过全线的主干网络,各个站段监控网的监控信息直接传输到控制中心的服务器群组,从而实现本线内多个系统的综合监控管理。本文提出的方法以基于温州市域铁路S1线应用的城轨云综合监控系统[21]作为案例分析,其网络拓扑如图3所示。除了图2中设备英文缩写解释外,其他设备解释如下:FEP(front end processor,前

端处理器）、BAS（building automation system，环境与设备监控系统）、SCADA（supervisory control and data acquisition，数据采集与监视控制系统）、FG（fieldbus gateway，现场总线）；ACS（access control system，门禁系统）；CCTV（closed-circuit television，闭路电视监控系统）、SIG（signal，信号机）。

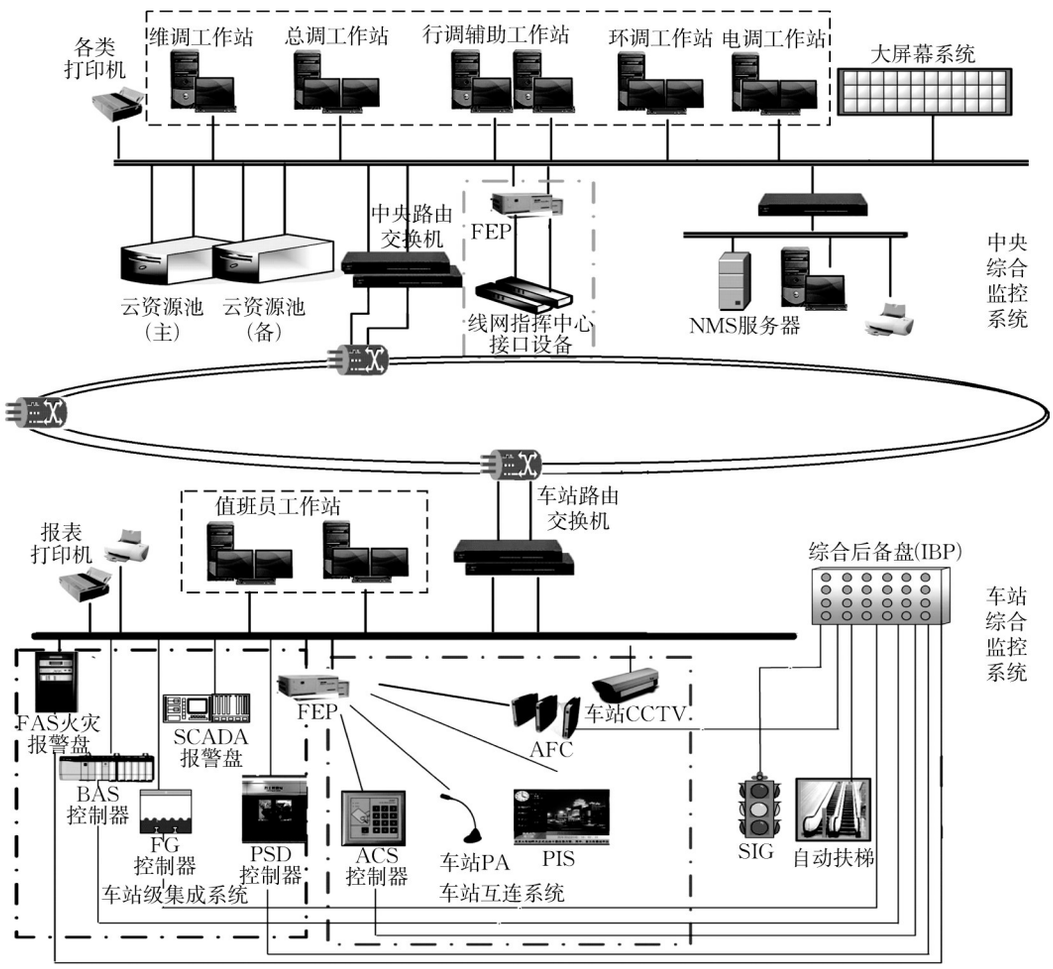


图3　基于城轨云的综合监控系统的网络拓扑图（部分）[21]

Fig. 3　Network topology diagram of integrated supervisory control system based on metro cloud(partial)

3.1.2　城轨云综合监控系统的实验拓扑图与仿真参数设置

基于网络拓扑图，提出了一个实施异常控制指令的实验拓扑图，如图4所示。该图在网络拓扑图的基础上补充了人机界面（human machine interface，HMI）、控制服务器和控制器，用于模拟控制指令在城轨中心云平台、站段云平台的组件之间的传输过程。为便于说明，为节点从上往下编号。

结合图3及相关工程经验，制定了以下假设以进行拓扑图的设计：① 中心控制服务器、总调工作站、行调辅助工作站和HMI1通常通过以太网或其他协议连接在同一局域网上。② 云资源池是硬件设施、虚拟化软件和管理软件的分布式计算资源集合，可被视为云计算的基础设施。云资源池是基于互联网的，通常通过网络管理系统连接到工业现场的局域网或广域网，并与其他设备通信。③ 在逻辑连接关系方面，前端处理器和线网指挥接口设备通常是通过现场总线或者其他工业网络协议来实现的。④ 中央路由交换机连接到中央综合监控系统的局域网上。不同的站段综合监控系统可以直接连接到中央路由交换机的不同端口上，通过交换机的路由功能可以实现跨网段通信；或者通过虚拟专用网络来连接不同的综合监控系统，使它们能够通过中央路由交换机进行通信。基于以上假设，对设备及设备间的连接关系进行抽取，获得了用于实施信任管理方法的节点链接关系图，如图5所示。

异常行为识别分为三类，按重要性由高到低，依次为干扰正常控制指令的操作、节点违规的控制指令、未授权的控制指令。此外，仿真参数的设置如表3所示。可部署完整信任管理功能的节点是中央监控所属节点

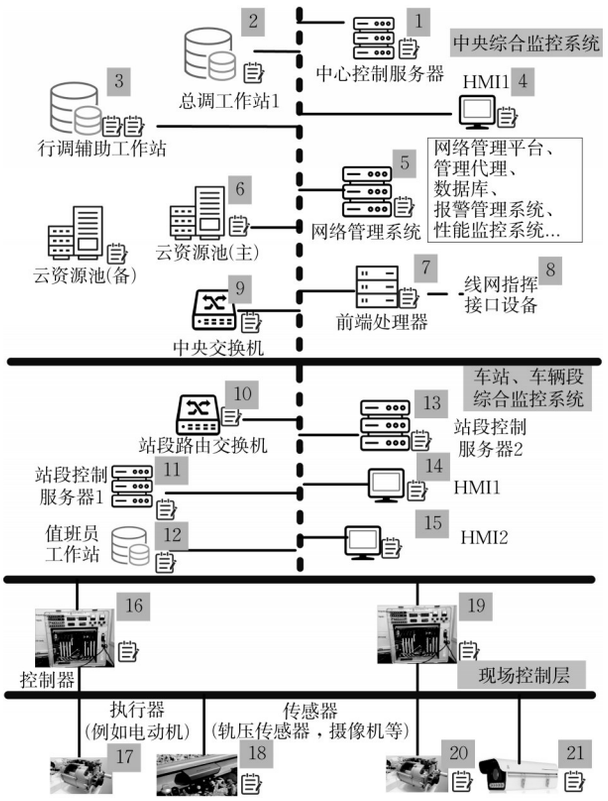


图4 用于实施异常控制指令的实验拓扑图

Fig. 4 Experimental topology diagram for implementing abnormal control commands

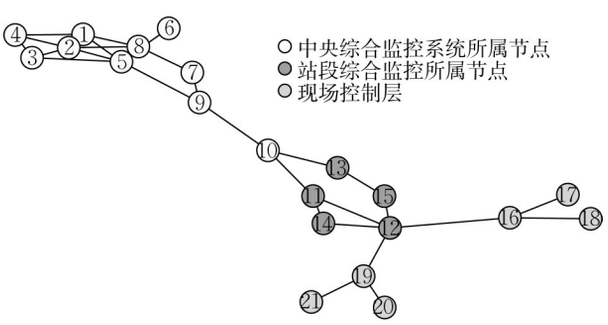


图5 城轨云综合监控系统下节点链接关系图

Fig. 5 Node linkage diagram of tintegrated supervisory control system based on metro cloud

和站段综合监控所属节点，其余节点只部署信任管理核心组件。本文仿真工具为Matlab 2022b。

表3 仿真参数的设置

Tab. 3 Setting of simulation parameters

参数描述	参数值
总节点数N_1	21
可部署完整信任管理的节点N_2	15
初始信任值Trust_0	0.5
直接交互次数的阈值θ_n	15
用于计算直接信任、间接信任权重参数α	0.9

3.2 仿真结果

3.2.1 正常控制指令操作下信任值的变化

选取了三个关键节点，如云资源池(节点6)、HMI1(节点4)和行调辅助工作站(节点3)，观察了随时间变化这些节点的信任值变化情况。结果如图6所示，横坐标是以时间窗次数表示时间，每个时间间隔即1次时间窗，纵坐标表示节点的信任值。随着时间推移和交互次数增加，在正常控制指令的运行下，成功交互次数逐渐增加，从而导致信任值逐渐增加，并最终趋于一个较高的信任值范围。根据表2中规定的访问权限分级，当信任值处于[0.8,1]范围，节点的信任值可达到信任I级，管理员可获得完全访问的权限。综上，这些信任变化符合预期的目标。

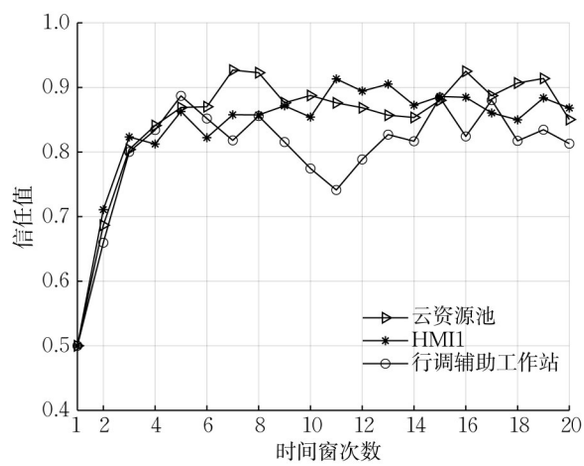


图6 正常控制指令运行下信任值的变化图

Fig. 6 Trust value variation diagram under normal control instruction operation

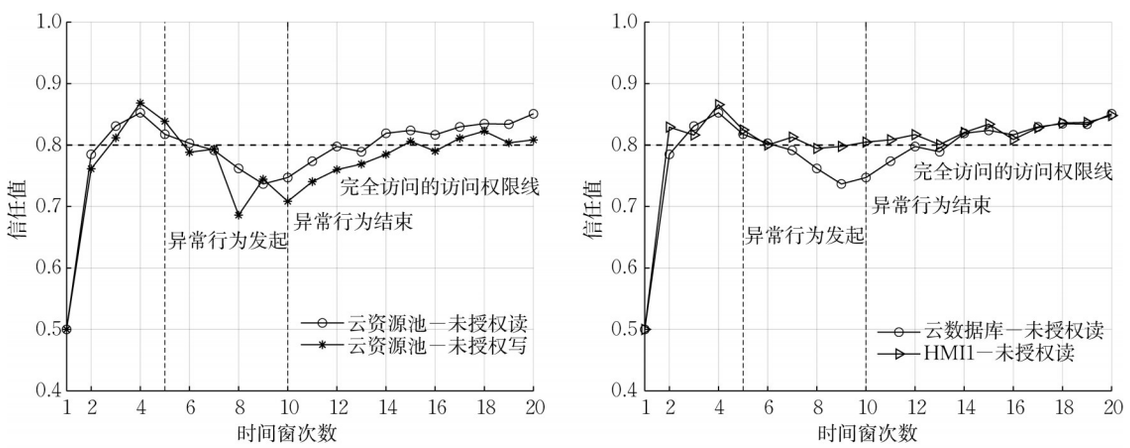
3.2.2 异常控制指令操作下信任值的变化

(1)节点在未经授权控制指令操作下的信任值变化

攻击的最终目标是修改城轨云平台发出的控制指令。针对未经授权的控制指令发起攻击，恶意攻击者可能通过对城轨云的设备和网络链路进行以下方式的攻击：越权访问、篡改控制指令和泄露控制指令。①越权访问：指某个用户或设备在未经授权的情况下，对数据或资源越权访问。②篡改控制指令：攻击者通过篡改控制指令，改变系统的控制参数或控制逻辑。③泄露控制指令：指攻击者获取控制指令，使其能够获取系统的控制参数、运行状态和控制策略等敏感信息。在仿真过程，假设云资源池(节点6)和HMI1(节点4)为非授权节点，并模拟了这些节点对执行请求、读取、写入控制指令的服务。同时，部署在节点中的信任管理核心组件能够检测到这些异常行为，并追踪具有异常行为的邻居节点的上一跳或下一跳。周期性地将这

些记录反馈给信任管理数据库。

在第5次交互时发起异常行为，并在第10次交互时恢复正常运行。如图7所示，在异常行为发生期间，两个节点的信任值均迅速下降，且下降至低于0.8的水平。异常行为结束后，信任值缓慢增加。在云资源池的未授权写操作中，从第5次交互到第8次交互，信任值下降率为5.3 %；而第10次交互到第15次交互，信任值增长率为2.2 %，如图7 a 所示。这种信任值变化的趋势表现为“缓升快降”，避免了节点表现时好时坏的“开–关攻击”。此外，根据预先假设，未授权写操作的惩罚要大于未授权读操作，因而写操作的信任值下降速度高于读操作，如图7 a 所示。实验结果与预期目标一致。在相同未授权读控制指令下，从第5次交互到第9次交互，云资源池的信任值降低率为2.0 %，高于HMI的信任值降低率0.67 %，如图7 b 所示。该结果也符合预先假设，即云资源池的重要性高于HMI1。



a 同一节点在不同未经授权控制指令下　　b 不同节点在相同未经授权控制指令下

图7　未经授权控制指令下不同节点及不同操作的信任值变化图

Fig. 7　Trust value variation diagram of different nodes and operations under unauthorized control commands

（2）节点在违规控制指令操作下的信任值变化

在考虑由内部异常或攻击引发的行为时，合法节点可能进行违规操作，具体如下：① 已授权的合法节点进行违规交互、修改、拦截、欺骗、丢弃控制指令；② 合法操作者的误操作：合法操作者由于操作失误或者其他原因导致控制系统产生错误或者失效。针对上述情况，模拟了云资源池（节点6）和HMI1（节点4）为已授权但发起了违规操作的节点。信任管理核心组件能够检测所部署的节点或其邻居节点这些异常行为，并定期将记录反馈给信任管理数据库。

在第5次交互时发起异常行为，并在第10次交互时恢复正常运行。如图8所示，在异常行为发生期间，两个节点的信任值迅速下降，降至低于完全访问权限的水平，而某些交互次数下的信任值低于拒绝访问权限线。具体地，在预先设定的情况下，实施违规控制指令的惩罚力度大于未经授权控制指令。因而，从第5次交互到第7次交互，云资源池违规写操作的信任值下降率30.13 %，高于未授权写操作的5.3 %，如图8 a所示。此外，预先假定了写操作的惩罚大于读操作，因而写操作的信任值比读操作下降得更快且更低。在云资源池比HMI1更重要的预先假设下，云资源池的信任值比HMI1下降得更快，如图8 b 所示。HMI1 节点的信任变化遵循了“缓升快降”规则。但在某些交互次数下，其信任值低于拒绝访问权限线时，该节点将被屏蔽，不再响应任何交互。例如在云资源池恢复正常运行后，其信任值不再增加，需要管理员检查后恢复。

（3）节点在干扰正常控制指令操作的异常行为下的信任变化

一些恶意节点可能实施干扰正常控制指令，例如实施拒绝服务攻击（denial of service，DoS）。DoS攻击指的是某些设备可能会阻塞信息传输或恶意节点向同一地址发送大量数据包，扰乱正常业务运营并导致无法可靠地提供服务。将城轨云中央综合监控系统中的中心控制服务器（节点1）和前端处理器（节点7）设定为已授权但受到了DoS攻击的节点。信任管理核心组件能够监测到这种控制指令被拦截且数据包持续发往特定节点的行为。

在第5次交互时设置异常行为，并在第10次交互结束。观察到如下行为，两个节点的信任值均迅速下降，低于完全访问的访问权限线，如图9所示。中心控制服务器的信任值低于拒绝访问的访问权限线，导致节点被屏蔽且不再响应任何交互。当异常行为结束后，其信任值未增加，需要管理员进行检查和恢复。而前端处理器的信任值在恢复正常后缓慢增加。

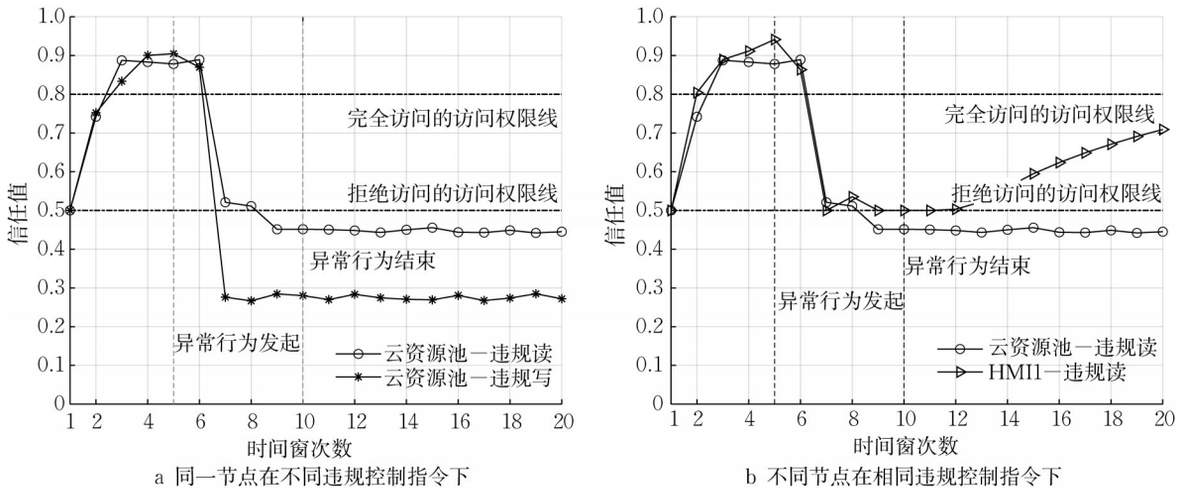


图8 违规控制指令下不同节点及不同操作的信任值变化图

Fig. 8 Trust value variation diagram of different nodes and operations under non-conforming control commands

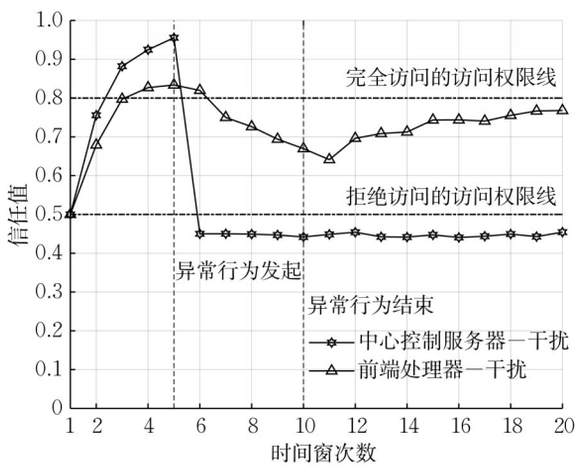


图9 干扰正常控制指令运行的异常行为下的信任变化图

Fig. 9 Trust value variation diagram of abnormal behavior interfering with normal control command operation

本文以温州S1线城轨云综合监控系统作为案例,计算结果能够指导实际应用。在实际应用时,偏差的影响因素有以下三点:① 将网络设备抽象为节点并简化了节点间连接关系,而实际节点连接关系更加复杂,可能会对授权结果造成影响;② 当前动态信任管理方法是基于主观逻辑方法,只考虑了成功与失败的交互次数,未考虑具体消息内容及网络设备可能会面临不同的负载和流量情况。

4 结语

(1) 提出了一种面向城轨云边界安全防护的动态信任管理方法。在异常行为识别上,信任管理组件能够监测多种异常控制指令行为,及时发现并应对潜在的安全威胁。在信任评估上,提出了基于主观逻辑的直接信任评估和基于第三方推荐的间接信任评估的综合信任值评估方法,且考虑了奖励及惩罚的影响。在动态访问控制的基础上,基于节点的信任值,将访问权限划分为四级,实现了细粒度的访问控制,以确保保证系统的安全性。

(2) 以城轨云综合监控系统为案例,根据真实的网络拓扑图,获得了节点间的链接关系图。在正常控制指令运行实验中,结果表明随着交互次数增加,信任值能够逐渐达到[0.8,1]范围,管理员能够获得完全访问权限。在异常控制指令运行实验中,结果表明在异常行为发生期间,节点的信任值能够迅速下降,降至低于[0.8,1]的范围,并且一旦节点的信任值降为[0,0.5)范围,节点将被屏蔽。

(3) 实验结果符合信任变化规律。首先,信任值的变化过程符合“缓升快降”的规则。例如在未授权写操作下,云资源池信任降低率为5.3 %,而信任增长率为2.2 %。其次,在执行不同控制指令时,信任值变化存在显著差异。例如在违规写操作下,云资源池和HMI的信任值降低率分别为30.13 %和5.3 %。最后,在不同节点下,信任值变化存在差异。例如在未授权读控制指令下,云资源池和HMI的信任值降低率分别为2.0 %和0.67 %。这些结果表明本文提出的动态信任管理方法能够根据节点的重要性,对信任值进行差异化的评估和管理,实现了动态、细粒度的边界安全防护。

(4) 为进一步研究提供了基础,未来的工作可以考虑处理多维度信任指标数据的信任管理,并探索采用机器学习方法来进一步提升系统的性能。此外,未来的工作需要利用真实的访问次数、流量等数据,并与

实际访问控制情况进行比较。

作者贡献声明:

张　雷:提供研究思路、技术指导以及论文完善工作。
徐　倩:提供研究思路,实施仿真实验,撰写论文。
何积丰:提供研究思路、技术指导以及论文完善工作。
曾小清:论文校对。
宁　正:协助文献整理及校对。

参考文献:

[1] 张雷,沈国琛,秦晓洁,等.智能网联交通系统中的信息物理映射与系统构建[J].同济大学学报(自然科学版),2022,50(1):79.
ZHANG Lei, SHEN Guochen, QIN Xiaojie, *et al*. Information physical mapping and system construction of intelligent network transportation [J]. Journal of Tongji University(Natural Science), 2022, 50(1): 79.

[2] 中国城市轨道交通协会.城市轨道交通云平台网络安全技术规范: T/CAMET 11005—2020[S].北京: 中国城市轨道交通协会, 2020.
China Association of Metros. Urban rail transit-technical specification for cloud cyber security: T/CAMET 11005—2020 [S]. Beijing: China Association of Metros, 2020.

[3] 中国城市轨道交通协会.中国城市轨道交通智慧城轨发展纲要[R].北京: 中国城市轨道交通协会, 2020.
China Association of Metros. Development outline for China intelligent urban rail transit[R]. Beijing: China Association of Metros, 2020.

[4] 国家标准化管理委员会.信息安全技术网络安全等级保护基本要求: GB/T 22239—2019[S].北京: 中国标准出版社, 2019.
National Standardization Administration Committee. Information security technology — Baseline for classified protection of cybersecurity: GB/T 22239—2019[S]. Beijing: Standard Press of China, 2019.

[5] WEI L J, YANG Y H, WU J, *et al*. Trust management for internet of things: A comprehensive study[J]. IEEE Internet of Things Journal, 2022, 9(10): 7664.

[6] 史永飞.云内云外融合网络安全纵深防御体系研究[J].都市快轨交通, 2022, 35(6): 59.
SHI Yongfei, Research on the defense-in-depth system of integrated network security inside and outside the cloud [J]. Urban Rapid Rail Transit, 2022, 35(6): 59.

[7] HUANG H X, ZHANG J B, HUN J, *et al*. Research on distributed dynamic trusted access control based on security subsystem [J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3306.

[8] WANG G J, MUSAU F, GUO S, *et al*. Neighbor similarity trust against Sybil attack in P2P e-commerce [J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26 (3): 824.

[9] FIROOZI F, ZADOROZHNY I V, LI Y F. Subjective logic-based in-network data processing for trust management in collocated and distributed wireless sensor networks[J]. IEEE Sensors Journal, 2018, 18(15): 6446.

[10] CAI B S, LI X Y, KONG W P, *et al*. A reliable and lightweight trust inference model for service recommendation in SIoT [J]. IEEE Internet of Things Journal, 2022, 9 (13): 10988.

[11] GAO H H, LIU C, YIN Y Y, *et al*. A hybrid approach to trust node assessment and management for VANETs cooperative data communication: Historical interaction perspective [J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 16504.

[12] WANG J, YAN Z, WANG H G, *et al*. A survey on trust models in heterogeneous networks[J]. IEEE Communications Surveys & Tutorials, 2022, 24(4): 2127.

[13] 潘瑞杰,王高才,黄珩逸.云计算下基于动态用户信任度的属性访问控制[J].计算机科学, 2021, 48(5): 313.
PAN Ruijie, WANG Gaocai, HUANG Hengyi. Attribute access control based on dynamic user trust in cloud computing [J]. Computer Science, 2021, 48(5): 313.

[14] BENDIAB G, SHIAELES S, BOUCHERKHA S, *et al.*, FCMDT: A novel fuzzy cognitive maps dynamic trust model for cloud federated identity management [J]. Computers & Security, 2019, 86: 270.

[15] KESARWANI A, KHILAR P. Development of trust based access control models using fuzzy logic in cloud computing[J]. Journal of King Saud University — Computer and Information Sciences, 2022, 34(5): 1958.

[16] YU W J, ZHANG L, XU Q. Real-time reliability access control based on rail traffic data platform[J]. Electronics, 2023, 12(5): 1105.

[17] 中国城市轨道交通协会.城市轨道交通云计算应用指南[R].北京: 中国铁道出版社, 2020.
China Association of Metros. Application guidelines for urban rail transit cloud computing[R]. Beijing: China Railway Publishing House, 2020.

[18] YU Z L, DAI H J, XI X M. A trust verification architecture with hardware root for secure clouds [J]. IEEE Transactions on Sustainable Computing, 2020, 5(3): 353.

[19] JIANG J F, HAN G J, WANG F, *et al*. An efficient distributed trust model for wireless sensor networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(5): 1228.

[20] XIA Y Z, DENG X J, YI L Z, *et al*. A trust-based reliable confident information coverage model of wireless sensor networks for intelligent transportation[J]. IEEE Transactions on Vehicular Technology, 2023, 72(7): 9542.

[21] 杨承东,徐余明.基于云计算技术的城市轨道交通综合监控系统架构方案[J].城市轨道交通研究, 2020, 23(5):6.
YANG Chengdong, XU Yuming. ISCS architecture scheme for urban rail transit based on cloud computing technology[J]. Urban Mass Transit, 2020, 23(5): 6.