【文件名】

Mixed\_Cloud\_Control\_Testbed\_Validating\_Vehicle-Road-Cloud\_Integration\_via\_Mixed\_Digital\_Twin\_[J]\_2023

【总结】

可靠、高效的验证技术是当前多车协同和车路云融合发展的关键。本文介绍了基于混合数字孪生(mixedDT)概念开发的微型实验平台——混合云控制试验台(MCCT)。mixedDT将混合现实与数字孪生相结合，将虚拟空间和物理空间融合为一个混合空间，物理实体共存，并通过数字实体与虚拟实体互动。在mixedDT框架下，MCCT分别包含物理空间、虚拟空间和混合空间三大实验平台，并为各种人机界面和驾驶模拟器等外部设备提供统一访问。云单元部署混合实验平台，负责融合多平台信息和分配控制指令，实现同步操作和实时跨平台交互。特别是，MCCT允许由不同的多源车辆(例如，物理车辆，虚拟车辆和人类驾驶的车辆)组成的多车辆协调。车辆队列的验证验证了MCCT的灵活性和可扩展性。

【参考文献】

Dong J, Xu Q, Wang J, et al. Mixed cloud control testbed: Validating vehicle-road-cloud integration via mixed digital twin[J]. IEEE Transactions on Intelligent Vehicles, 2023.

【文件名】

Evaluation\_Method\_of\_Vehicle-road-cloud\_Collaborative\_System\_with\_Grey\_System\_Theory\_[C]\_2022

【总结】

在自动驾驶时代，要真正实现高效安全的交通出行，单靠一辆车的智能化是远远不够的。随着5G、V2X、人工智能等一系列技术的发展，车路云协同越来越成为未来的主要应用方向。对车路云协同系统的安全性、有效性和服务能力进行有效评估势在必行。在此基础上，本研究首先选取执行能力、V2X能力、环境感知与定位精度、应用场景功能、综合驾驶能力五个一级评价指标，构建了车路云协同系统的评价指标体系。然后，在多级指标体系的基础上，确定了基于灰色系统的车辆-道路-云协同系统综合评价方法。最后，对车辆-道路-云协同系统的综合评价进行了实证研究。结果表明，本文提出的评价方法能够对车辆-道路-云协同系统进行有效、全面的评价。

【参考文献】

Wang H, Zhang Z, Li J, et al. Evaluation Method of Vehicle-road-cloud Collaborative System with Grey System Theory[C]//2022 8th Annual International Conference on Network and Information Systems for Computers (ICNISC). IEEE, 2022: 949-953.

【文件名】

An\_Evaluation\_Method\_of\_Vehicle-Road-Cloud\_Collaborative\_System\_Security\_Situation\_Based\_on\_CD2-A\_Elastic\_Computing\_Framework\_[C]\_2023

【总结】

随着智能网联汽车的蓬勃发展，车-路-云协同系统的网络安全备受关注，相应的，对其进行信息安全评估。该领域现有的信息安全评估研究主要集中在车联网(10V)，特别是智能车辆和特定车辆部件，而针对车-路-云协同系统安全状况的定量评估方法研究是空白。目前，层次分析法(AHP)是一种比较被认可的信息安全评估方法，但由于其断言标准的主观性和随意性，甚至在多个评估对象存在的情况下工作效率低下。针对这些问题，提出了一种基于(CD)2-A弹性计算框架的车辆-道路-云协同系统安全态势评估方法。该方法将车辆-道路-云协同系统划分为子系统级、组件级等层次模型。据此，采用c2r - dea法对CVSS和DREAD模型的得分进行弹性评价，采用AHP法对子系统的安全状况进行评价，最终确定整个系统的安全状况评价值。通过对行业报告中实际icv受攻击数据的计算，证明了本文方法的有效性，更适用于车路云协同系统的安全评估。

【参考文献】

Jia S, Zhang T, Lin W, et al. An Evaluation Method of Vehicle-Road-Cloud Collaborative System Security Situation Based on (CD) 2-A Elastic Computing Framework[C]//2023 8th International Conference on Data Science in Cyberspace (DSC). IEEE, 2023: 546-550.

【文件名】

A node trust evaluation method of vehicle-road-cloud collaborative system\_[J]\_2022

【总结】

随着车路云协同系统的快速发展，在解决数据传输问题的同时，也伴随着严重的信息安全问题。为了构建安全的数据传输，推荐将信任作为实现网络安全的相关方式;也就是说，开发一个传感器节点可以用来确定另一个节点可靠性的信任模型是至关重要的。然而，网络的异构性对信任评估有不同的功能要求，网络的开放性使节点更容易受到攻击。因此，车辆-道路-云协同系统中信任评估模型的研究面临着比传统网络更大的挑战。提出了一种基于联邦学习(FLT)的车辆-道路-云协同系统信任评估方案。设计了一个层次信任评估模型，利用层次分析法将复杂的模型简化为有序的层次结构。评估了不同层次的信任指标，综合考虑了不同节点之间的影响因素。结合联邦学习，解决了寻找最可靠路线的问题，实现了设备、数据、模型层面的个性化。为了减轻异构性，获得每个设备的高质量个性化模型，信任值可以随着网络拓扑的实时变化而自适应更新。仿真结果表明，该算法在保持信任稳定性的前提下，能耗降低35%，准确率提高45%。

【参考文献】

Wang D, Yi Y, Yan S, et al. A node trust evaluation method of vehicle-road-cloud collaborative system based on federated learning[J]. Ad Hoc Networks, 2023, 138: 103013.

【文件名】

车路云一体化车联网系统\_[J]\_2022

【总结】

随着智能化网联化汽车的发展，车联网系统无时无刻不在产生着海量的交通数据，车路终端自身的计算能力已难以处理复杂任务，传统的集中式云计算技术已无法应对智能车联网应用中数据量大、传输延迟高、实时处理性低等瓶颈问题。车路云一体化系统以车载、路侧、云端等多源数据融合为基础，依赖车路云协同组网传输的可靠性和效率，借助云端计算和边缘计算对系统整体资源进行联合调度优化，共同实现车联网系统安全和效率的最大化。

【参考文献】

刘阳,张颂歌,田大新.车路云一体化车联网系统[J].建设科技,2022,(01):77-80.DOI:10.16116/j.cnki.jskj.2022.01.011.

【文件名】

车载无线网络安全关键技术研究\_[硕]\_2023

【总结】

本文基于下一代列车控制与监视系统中的WLCN架构，结合无线OSI七层模型和WLAN设备连接过程可能受到的攻击及风险，分析列车WLAN网络的脆弱性；同时，根据列车实时数据协议中的过程数据和消息数据的通信原理与机制，分析列车通信协议的脆弱性，发现列车无线通信网络中存在的安全问题。 使用 Qt 研发一款无线网络攻击软件，该软件包括：信息收集类攻击模块；身份欺骗类攻击模块；拒绝服务类攻击模块。 并利用设计的攻击软件对列车无线网络实验平台进行攻击测试。

【参考文献】

范晓龙. 车载无线网络安全关键技术研究[D].大连交通大学,2023.DOI:10.26990/d.cnki.gsltc.2023.000767.

【文件名】

列车网络系统的网络安全分析与安全防护\_[J]\_2020

【总结】

针对基于工业以太网的列车网络系统的安全问题，分析了列车网络系统面临的威胁，在此基础上，给出了列车网络系统终端设备、网络设备、维护设备、远程数据传输设备的安全防护措施，可为列车网络安全设计提供参考。

【参考文献】

周淑辉,常振臣,张尧,等.列车网络系统的网络安全分析与安全防护[J].城市轨道交通研究,2020,23(02):84-87.DOI:10.16037/j.1007-869x.2020.02.019.

【文件名】

智慧城轨车载网络安全防护解决方案\_[J]\_2022

【总结】

随着城市轨道交通向网络化、自动化、智慧化高速发展，城轨车载网络的安全防护问题不容忽视。本文从国家标准、行业发展、行业实践三个维度展开分析，提出一套智慧城轨车载网络安全防护机制和方法，探讨车载防护设备未来发展趋势。

【参考文献】

张雄杰,曹旭,周金鹏.智慧城轨车载网络安全防护解决方案[J].工业信息安全,2022,(06):65-72.

【文件名】

铁路网络数据安全风险分析及应对措施\_[J]\_2022

【总结】

随着信息技术在铁路领域的应用不断深化，铁路业务系统中产生和积累了海量的网络数据，

成为铁路企业重要的生产要素之一。网络数据在收集、存储、传输、应用、销毁等各个环节面临着被泄

露、窃取、非法使用的安全风险。通过分析铁路网络数据面临的主要安全风险，结合铁路企业网络数据

应用场景，研究提出网络数据安全风险应对措施，可为铁路企业网络数据安全管理工作提供借鉴和参考。

【参考文献】

魏长水,杨轶杰,李琪.铁路网络数据安全风险分析及应对措施[J].铁路计算机应用,2022,31(11):33-36.

【文件名】

基于深度包检测的列车通信网络入侵检测系统的设计与实现\_[硕]\_2019

【总结】

随着工业以太网在列车通信网络中的应用,其开放性越来越强,所面临的安全问题也越来越突出。以太列车通信网络是服务网络和控制网络的融合,两者需要通过网关来交换数据。本文分析了列车通信网络的脆弱性,以及列车控制网络中用来传递过程数据和消息数据的TRDP协议,并结合当前工业控制系统网络安全入侵检测技术的研究,设计了一种基于深度包检测的入侵检测系统。本文设计的入侵检测系统从网络中抓取实时通信数据,利用深度包检测技术对它进行从链路层到应用层的深度解析,提取出网络通信的特征,基于OCSVM的异常检测模型进行更深层次的异常行为检测。本文最后介绍了入侵检测系统各个模块的实现,通过实验验证了对TRDP协议的解析功能、数据包合法性检查功能和包过滤功能,将静态防护功能和基于PSOOCSVM的异常检测模型相结合,能够提高入侵检测的准确率。

【参考文献】

费力. 基于深度包检测的列车通信网络入侵检测系统的设计与实现[D].华中科技大学,2019.