轨道交通移动边缘计算网络安全综述

谢人超[1,2]，文雯[1]，唐琴琴[1]，刘云龙[1]，谢高畅[1]，黄韬[1,2]
（1. 北京邮电大学网络与交换技术国家重点实验室，北京 100876；2. 紫金山实验室，江苏 南京 211111）

摘 要：在环境复杂、乘客密集、高速移动的轨道交通场景中引入移动边缘计算（MEC）技术可满足其对低时延、移动性和海量连接等的需求。然而，MEC 在改善轨道交通通信网络性能的同时也带来了安全挑战。首先对轨道交通通信网络和 MEC 进行了概述；然后讨论了 MEC 在轨道交通中的价值和轨道交通移动边缘计算网络的架构；接着分析了轨道交通移动边缘计算网络面临的安全威胁并提出了防护方案；最后提出了一些开放性问题，希望对后续的研究提供思路。

关键词：边缘计算；轨道交通；网络安全；防护
中图分类号：TP393
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023071

Survey on rail transit mobile edge computing network security

XIE Renchao[1,2], WEN Wen[1], TANG Qinqin[1], LIU Yunlong[1], XIE Gaochang[1], HUANG Tao[1,2]
1. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Purple Mountain Laboratories, Nanjing 211111, China

Abstract: The introduction of mobile edge computing (MEC) technology in rail transit which has the characteristics of complex environment, high densities of passengers, and high-speed mobility can meet the low latency, mobility, and massive connection requirements of rail transit. However, MEC not only improves the performance of rail transit communication network but also brings security challenges. Firstly, an overview of rail transit communication network and MEC was given. Then the value of introducing MEC into rail transit and the architecture of rail transit edge computing network were discussed. After that, the security threats faced by rail transit edge computing network was analyzed and protection scheme was proposed. Finally, some open questions were proposed, which was expected to provide ideas for future research.

Keywords: edge computing, rail transit, cybersecurity, protection

0 引言

城市轨道交通凭借其运量大、速度快、安全舒适、节能环保等优点，成为中国城市最主要的出行方式之一。随着城市轨道交通的运营不断转型升级，轨道交通运营产生的海量数据以及轨道交通系统的计算密集型业务和时延敏感型业务都使轨道交通系统对通信网络服务质量的要求越来越高。

为解决云计算面临的网络带宽消耗过多、远距离传输时延过长等问题，一种在网络边缘侧提供数据处理服务的新型计算模式——移动边缘计算（MEC, mobile edge computing）应运而生。MEC 在数据源头的网络边缘处完成任务，可以减轻网络传输压力并减少数据传输时延。此外，MEC 支持移动性且可以提供位置感知和低成本的服务以支持轨道交通的各种应用业务。因此，引入 MEC 后，轨道交通移动边缘

收稿日期：2022−10−24；**修回日期：**2023−01−31
通信作者：唐琴琴，qqtang@bupt.edu.cn
基金项目：北京市自然科学基金–丰台轨道交通前沿研究联合基金资助项目（No.L201002）
Foundation Item: Beijing Municipal Natural Science Foundation-Fengtai Rail Transit Frontier Research Joint Foundation (No.L201002)

计算网络能更有效率地处理终端产生的海量数据，提高行车安全性并改善轨道交通的服务质量。

在提高网络性能的同时，MEC 异构终端设备海量分布、终端和应用之间采用多样化但安全性不强的通信协议、多种安全域并存、依赖虚拟化、资源受限的 MEC 服务器防护能力相对薄弱等特点使 MEC 面临严重的安全威胁。除此之外，城市轨道交通所处的外部环境复杂多变，设备终端分布密集，而且铁路通信系统在网络安全研究领域起步较晚，尚未形成完善的安全保障体系。由于轨道交通移动边缘计算网络具有轨道交通和 MEC 两者的特点，因此它也综合了两者的弱点和面临的安全威胁，甚至当受到同一种攻击时，由于该网络防护能力弱、依赖虚拟化且所处环境动态复杂，攻击导致的后果可能会更加严重，轨道交通移动边缘计算网络的防护方案设计也更具挑战性。和别的场景不同，针对轨道交通移动边缘计算网络的安全攻击不仅会造成隐私泄露，还会影响行车决策，危及乘客生命安全，引发重大交通安全事故。因此，针对城市轨道交通移动边缘计算网络安全的研究至关重要，已成为学术界和工业界共同关注的课题之一。

本文主要综述了城市轨道交通移动边缘计算网络安全方面的相关研究，首先概述了轨道交通通信网络和 MEC 的基本情况，包括架构、业务、安全威胁和防护技术；然后探讨了在轨道交通中引入 MEC 的动机和轨道交通移动边缘计算网络架构；接着对轨道交通移动边缘计算网络面临的安全威胁和可行的防护方案进行了详细分析；最后提出了几点开放性研究问题，讨论了轨道交通移动边缘计算网络安全未来的研究方向。

1 轨道交通通信网络与 MEC 安全概述

本节对轨道交通通信网络架构、业务、安全威胁和防护技术以及 MEC 的部署方案、安全威胁和防护技术进行了简要概述，为轨道交通移动边缘计算网络安全威胁分析及防护技术提供理论基础。

1.1 轨道交通通信网络概述

轨道交通通信系统可实现轨道交通各要素的泛在互联和列车运行全过程的高度信息化，旨在为列车关键任务提供高可靠性和可用性的网络服务，高质量完成列车信号控制、视频监控、语音通信、运行维护[1]和乘客通信等任务，在保证行车安全和高效方面具有重要作用。

1.1.1 轨道交通通信网络架构

目前，业界普遍应用的是基于长期演进（LTE, long term evolution）技术的轨道交通通信网络架构，如图 1 所示[2]。该架构包括控制中心、无线通信网络、车站子系统和车辆子系统。LTE 核心网、基于通信的列车控制（CBTC, communication based train control）系统控制中心、闭路电视监控（CCTV, closed circuit television）服务器、乘客信息系统（PIS, passenger information system）服务器、无线电调度服务中心等都部署在控制中心。LTE 基站的室内基带处理单元（BBU, building base band unit）和射频拉远模块（RRU, radio remote unit）部署在车站。由于轨道交通无线通信需要沿轨道进行无线覆盖，泄漏电缆比较适合线状的覆盖场景。在车辆子系统中，列车两端驾驶室安装列车接入单元（TAU, train access unit），驾驶室顶部安装 TAU 天线，此外，还安装用来播放列车信息的液晶显示器（LCD, liquid crystal display）控制器和 LCD 屏以及控制列车运行的 CBTC 控制器。

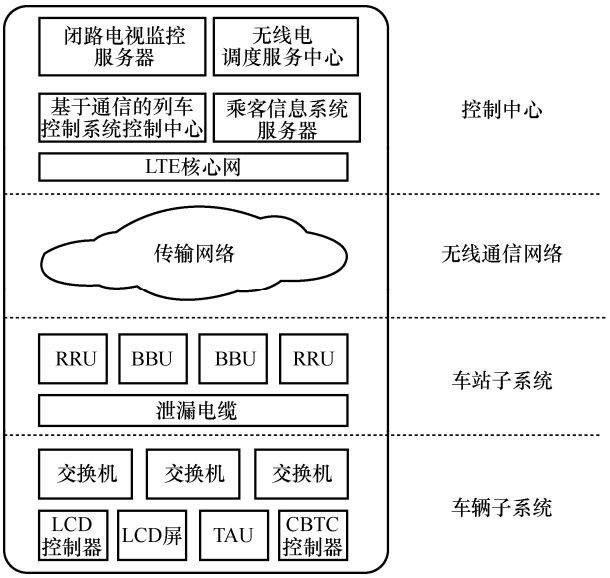

图 1 基于 LTE 技术的轨道交通通信网络架构

由轨道交通通信网络架构可知，核心网设备与控制中心的服务器相连，服务器将线路、轨旁设备状态等信息通过核心网、传输网络等一层一层地下发给车载设备。RRU 采用光纤与 BBU 直接连接，BBU 和 RRU 设备通过传输网提供的传输通道与核心网设备相连，在隧道区间布置 RRU 设备延伸无线覆盖，从而实现与车载设备的数据通信。在每列车的车头、车尾各设有一套 TAU，TAU 通过车载

交换机完成与列车各应用系统的通信[3]。

根据业务的重要性和传输性能要求，轨道交通通信网络把不同的业务划分成不同的优先级，以保证列车运行控制业务传输的高优先级。不同的业务经过不同的网元和接口，系统能根据 IP 地址、端口号等参数区分不同业务来分配服务保障策略。

1.1.2　轨道交通无线通信业务

1) CBTC 业务

CBTC 系统是列车综合运行控制的重要组成部分，可实现连续、大容量的车地双向通信，并执行安全功能[4]。CBTC 系统的主要功能包括列车自动保护（ATP, automatic train protection）系统、列车自动操作（ATO, automatic train operation）系统和列车自动监控（ATS, automatic train supervision）系统功能。ATP 功能应提供故障安全保护；ATO 功能用于实现列车调度指挥、间隔控制和安全防护等操作与功能的自动化；ATS 功能用于监测列控系统的状态信息，并发出一些控制命令来指挥交通。

2) 集群调度业务

集群调度系统是城市轨道交通专用无线电通信系统的关键组成部分，集群调度业务包含多个场景的调度，如列车调度负责满足列车行驶要求，综合维修调度负责满足日常维护维修要求，防灾调度负责满足事故救援和防灾要求。

3) PIS 业务

PIS 分为中心控制系统和网络系统，可使旅客通过列车显示终端及时、准确地了解列车运行信息和公共媒体信息。PIS 服务器在正常情况下可以发布运营服务信息或多媒体信息；在非正常情况下可以传送紧急文本信息，提供动态紧急疏散提示[5]。

4) CCTV 业务

CCTV 业务是列车监控服务，用来监控列车运行和及时处理紧急情况。每列列车有 30 个摄像头，高清格式每路速率是 2 Mbit/s，所有摄像头的图像需要实时上传来保障 CCTV 业务[6]。

1.1.3　轨道交通通信网络安全威胁和防护技术

1) 安全威胁

轨道交通通信网络因为身份认证机制、访问控制机制和入侵检测技术不完善以及列车自身固有的特性等面临安全威胁。轨道交通网络的身份认证机制粒度较粗，难以限制非授权设备接入列车网络，从而导致恶意用户获得权限入侵网络。攻击者还可以伪造节点与弱认证的通信设备连接，劫持流量，造成数据泄露[7]。不具备强身份认证和访问控制能力的车载设备容易被恶意代码植入，使攻击者可以修改、破坏、非法分析和损坏物理设备，造成其功能丧失，严重影响行车安全[7]。很多网络接口仅部署了初步的隔离保护措施，部分系统甚至根本未部署入侵检测设备，缺少对流量的实时监控和对异常模型的分析，导致网络异常无感知，且无法抵御有组织的网络攻击[8]，如攻击者可以通过中间人攻击（MitM, man-in-the-middle）操纵两列列车的通信数据。由于列车高速运行经常需要进行网络切换，乘客会在很短的时间内通过多个基站，这会导致信令风暴，甚至导致呼叫丢弃。

2) 防护技术

基于上述的安全威胁分析可知，因为身份认证机制、访问控制机制和入侵检测技术不完善以及列车高速移动导致的切换频繁，轨道交通通信网络面临一系列安全威胁。此外，如果没有加密技术，信息将会面临巨大的泄露风险。因此，本节从身份认证、数据加密、访问控制、入侵检测和高速切换 5 个方面介绍针对轨道交通的防护技术，如表 1 所示。

①身份认证。Wang 等[9]提出了一种基于椭圆曲

表 1　轨道交通安全防护技术

防护技术	文献	方案	技术方法	安全威胁
身份认证	文献[9]	提出了一种高效认证方案	椭圆曲线密码体制	非授权访问；非法基站；恶意代码植入
	文献[10]	提出了一种轻量级高效认证机制	混沌系统	
数据加密	文献[11]	提出了一种铁路无线通信领域的密钥协议	Diffie-Hellman 密钥协议算法	隐私泄露
	文献[12]	提出了一种改进协议以优化协议密钥服务流程	高级加密标准	
访问控制	文献[13]	提出了一种基于位置的安全访问控制方案	基于轨迹等的定位算法	非授权访问；非法基站；恶意代码植入
	文献[14]	提出了一种基于角色的安全访问控制方案	基于角色的访问控制	
入侵检测	文献[4]	提出了一种基于贝叶斯博弈的中间人攻击的检测方法	贝叶斯博弈	中间人攻击
高速切换	文献[15]	提出了一种新颖的车载架构	多个固定波束定向天线	信令风暴，呼叫丢弃
	文献[16]	提出了一种基于预测算法的高速铁路场景切换方案	灰色模型预测	

线密码系统的无证书代理签名（ECC-CLPS, elliptic curve cryptosystem based certificateless proxy signature）算法的认证方案，在不牺牲效率的情况下增强网络的安全性。Xu 等[10]提出了一种基于混沌系统和不可逆加密操作的高效认证机制，克服了现有轻量级身份验证的缺点。

②数据加密。在铁路信号系统中，需要对数据加密来保障安全通信。Hei 等[11]通过对铁路领域现有关键管理规范的安全分析，将密钥协议（经典的 Diffie-Hellman 密钥协议算法）的思想引入铁路无线通信领域。Wu 等[12]针对铁路信号安全通信协议 RSSP-II 中消息认证安全层的消息认证码（MAC, message authentication code）算法安全性低等问题，采用高级加密标准，优化了协议密钥服务流程。

③访问控制。Li 等[13]提出了基于轨迹、基于神经网络和基于光线追踪的定位算法，实现基于位置的安全访问控制。Cheng 等[14]将基于角色的访问控制（RBAC, role-based access control）模型应用于高速铁路 ATP，设计访问控制的物理数据模型，实现对系统关键资源的访问控制。

④入侵检测。入侵检测方法可针对多种攻击类型，这里以 MitM 为例介绍轨道交通网络的入侵检测技术。彭亚枫[4]采用贝叶斯博弈的方法对 MitM 攻击行为进行研究，构建包含被动攻防博弈和主动防御博弈的两层攻防博弈架构。

⑤高速切换。为实现高速场景下的无缝切换，Parichehreh 等[15]提出了一种车载架构用于列车到地面 LTE 回程，极大地优化了切换决策。Wang 等[16]设计了一种基于灰色模型预测的切换算法来避免切换滞后，大大提高了高速铁路场景下的切换性能。

1.2　MEC 概述

欧洲电信标准化协会提出了移动边缘计算的概念，将其定义为“在移动网络的边缘提供 IT 服务环境和云计算能力”[17]。MEC 通过将服务和功能从云数据中心转移到移动网络的边缘来降低服务交付时延，并降低回传网和核心网的传输压力[18]。

1.2.1　5G 架构下的 MEC 部署方案

MEC 在 5G 架构下的部署方案如图 2 所示[18]。MEC 通过网络开放功能（NEF, network exposure function）接入 5G 网络。用户发送的请求经用户平面功能（UPF, user plane function）到 MEC，在策略控制功能（PCF, policy control function）的控制下，MEC 为用户提供各类计算、存储和通信服务。MEC 的具体部署方式十分灵活，既可以集中部署，与用户面设备耦合，提供增强型网关功能，也可以分布式部署在不同位置，通过集中调度提供服务。

1.2.2　MEC 面临的安全威胁和防护技术

1) MEC 面临的安全威胁

在提高网络性能、改善用户体验的同时，MEC 由于自身固有的特性也面临诸多安全威胁。MEC 开放一系列接口与用户终端应用通信，但目前关于接口和 API 的管理并不完善，攻击者可以借此控制一部分网络，边缘设备之间也可以进行信息交换而不通过中央系统，在这种情况下，边缘设备间的网络也容易被攻击者劫持，攻击者通过控制网络来发

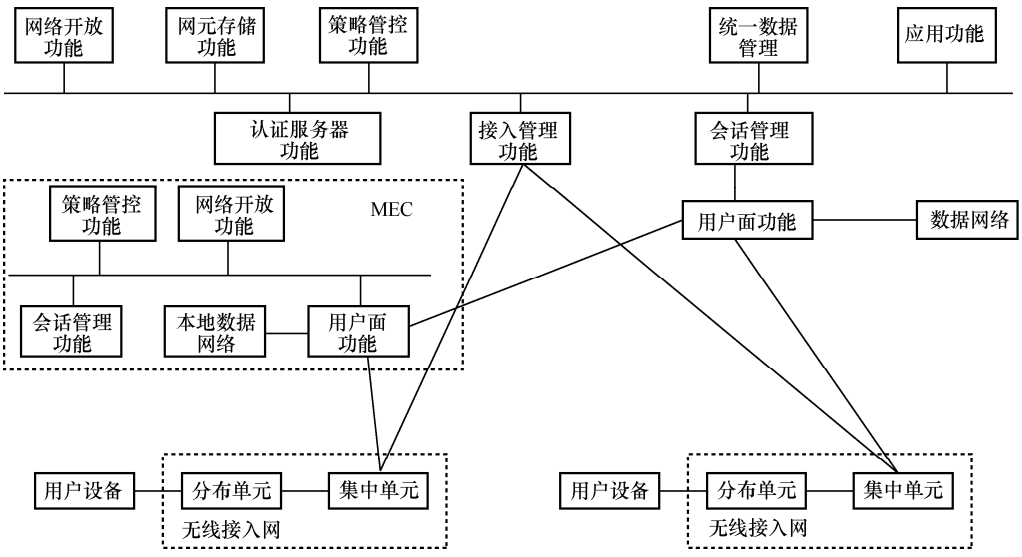

图 2　MEC 在 5G 架构下的部署方案

动 MitM 攻击以拦截数据通信，成功操纵从 MEC 服务器到用户或边缘设备之间的数据。与中心服务器相比，MEC 服务器的计算资源、存储资源等都比较受限，服务器性能较差，海量的终端设备可能会被攻击者操控向 MEC 服务器发动拒绝服务（DoS, denial of service）攻击，导致用户无法正常请求主机资源。MEC 服务器也可能被第三方 APP 侵入，面临非法接入等安全威胁。MEC 依赖虚拟化，如果一个虚拟机受到破坏，它可能会影响整个虚拟化基础架构。此外，终端设备和边缘节点之间以及分布式边缘节点和云中心之间的身份认证仍不够完善，攻击者可以把恶意的终端或边缘节点伪装成合法节点，由于终端设备和边缘节点泛在分布，定位恶意节点十分困难[19]。终端设备或 MEC 服务器如果连接到恶意节点，可能会面临机密数据泄露、恶意代码植入等风险，如终端设备被注入错误数据或恶意代码后，可以被重新配置并向网络发送虚假信息甚至在集群环境中更改和控制集群中的服务。随着 MEC 应用场景的扩展，MEC 网络面临的风险挑战不断升级，而安全是网络服务的底线，如何应对隐蔽的安全威胁已经成为边缘计算的重要研究方向。

2) MEC 安全防护技术

MEC 由于缺乏完善的身份认证技术以及本身的脆弱性，易受到 DoS 攻击、MitM 攻击等，并面临隐私泄露的风险。因此，本节从身份认证技术、入侵检测技术和隐私保护 3 个方面介绍针对 MEC 的安全防护技术，如表 2 所示。

①身份认证技术。Guo 等[20]提出了一种建立在 MEC 节点上的区块链网络，该网络采用区块链和数字签名算法对车辆进行身份认证，并将区块链网络划分为三层结构以提高身份认证速度。Ni 等[21]提出了面向服务的身份验证框架，该框架可用于物联网边缘计算系统，支持网络切片技术。

②入侵检测技术。本节以 DoS 攻击防护技术和 MitM 攻击防护技术为例介绍入侵检测技术。Jia 等[22]提出一种基于流量变化的分布式拒绝服务（DDoS, distributed DoS）攻击检测算法，并设计了 2 个机器学习模型：长短期记忆（LSTM, long short-term memory）和卷积神经网络（CNN, convolutional neural network）。Choi 等[23]提出一种基于区块链的中间人攻击检测方法，该方法能够检测在传输数据时发生的 MitM 攻击，为物联网系统提供零信任系统。

③隐私保护。Li 等[24]提出了一种在支持物联网 MEC 场景中保护隐私的模型，该模型包括 3 个实体：终端设备、MEC 服务器和公共云中心，3 个实体系统模型采用 Boneh-Goh-Nissim 密码系统。

2　轨道交通移动边缘计算网络

2.1　MEC 技术在轨道交通通信网络中的应用价值

本节从流量爆炸式增长场景、低时延高可靠场景和海量连接场景 3 个方面介绍 MEC 技术在轨道交通通信网络中的价值[25]。

1) 流量爆炸式增长场景

流量爆炸式增长场景主要包括娱乐和视频监控业务。为支持铁路沿线和车厢内的全面实时视频监控，可以在本地部署 MEC 服务器对监控视频数据进行处理，并将有变化的事件和视频片段传回，有效节省传输资源。对于大量价值较低的监控内容，可以直接存储在 MEC 服务器上来减轻核心网的负担和提高处理效率。

2) 低时延高可靠场景

低时延高可靠场景包括铁路通信、系统维护服务等。在高速运动过程中，列车的状态信息变化迅速，在边缘设备上进行处理和计算，可以有效地减少数据传输中的转发和处理时间。铁路通信网络中部署的 MEC 服务器对有价值的运行数据进行处理，并进一步将分析结果以超低时延传输到附近的联网列车上，使列车能够快速做出决策。

3) 海量连接场景

在物联网时代，各种传感设备与互联网结合形成一个巨大的网络，人、机、物可以在任何时间、

表 2　MEC 安全防护技术

防护技术	文献	方案	技术方法	安全威胁
身份认证技术	文献[20]	提出了一种建立在边缘节点上的区块链网络，为车载网络提供访问控制	区块链	恶意节点攻击
	文献[21]	提出了面向服务的身份验证框架并设计了一种保护隐私的切片选择机制	网络切片	
DoS 攻击防护技术	文献[22]	提出了一种基于流量变化的 DDoS 攻击检测算法	LSTM、CNN	DoS 攻击
MitM 攻击防护技术	文献[23]	提出一种基于区块链的 MitM 攻击检测方法，实现零信任系统	区块链	MitM 攻击
隐私保护	文献[24]	提出了一种在支持物联网 MEC 场景中保护隐私的模型	Boneh-Goh-Nissim	隐私泄露

任何地点连接在一起，轨道交通场景也不例外。轨道交通中的大量连接会不可避免地造成带宽压力，处理累积的数据也需要更多的计算和处理设备。此时，部署在网络边缘的服务器可以很好地缓解核心网的压力。

2.2 轨道交通移动边缘计算网络架构

本节设计了一个包含控制中心子系统、轨道交通线路主干网和边缘子系统三部分的轨道交通移动边缘计算网络架构[26]，如图 3 所示。

1) 控制中心子系统

控制中心子系统是轨道交通移动边缘计算网络的云核心，包括多种业务的服务器，负责处理分析列车运行的关键核心数据。根据权限的不同，控制中心子系统中的核心服务器可以管控单条线路或者多条线路。不同权限的服务器所处的位置也不同，负责单条线路的服务器位于该线路的控制单元中，而负责多条线路或全部线路的服务器则位于轨道交通公司中，同时这些服务器还可以选择运行在云计算平台上，使用云计算服务。

2) 轨道交通线路主干网

负责提供数据传输的轨道交通线路主干网连接控制中心子系统、各站点子系统以及车辆段子系统。MEC 节点在用户侧就近提供服务，但重要运行数据和相关状态需要通过线路主干网上传到控制中心。同时，控制中心子系统的各种服务器和控制中心通过主干网自顶向下地调控各边缘集群的工作。此外，由于轨道交通列车移动速度快，各 MEC 节点之间还要频繁地交互以控制列车安全运行。

3) 边缘子系统

边缘子系统由车辆段子系统、站点子系统和车载子系统组成。站点子系统和车辆段子系统中部署有 MEC 节点和小基站，通过无线阵列与轨道交通列车通信，与各类传感器、显示屏、摄像头和轨道信号灯等组成边缘子系统。车载子系统通过天线阵列与车辆段子系统和站点子系统通信，包括列车上的车载核心控制设备和边缘接入设备。

与轨道交通通信网络相比，轨道交通移动边缘计算网络增加了边缘层，是一个云–边缘的网络结构，需考虑控制中心子系统和边缘子系统如何协同工作来更好地处理任务。

2.3 轨道交通移动边缘计算网络架构优势

列车运行时，大量物联网设备以高采样频率连续工作，在短时间内产生大量数据，传统的轨道交通通信网络只依赖远程云数据中心处理，但列车和远程云数据中心之间的网络拥塞会导致较大的端到端时延，无法立即处理的数据将逐渐积累并失去时效性，影响列车运行[27]。2.2 节设计的轨道交通移动边缘计算网络架构通过将部分数据和计算密集型任务卸载到附近的边缘服务器来减少网络拥塞的风险，降低处理时延，使列车可以快速做出决策，提高行车安全性并改善用户体验。

3 轨道交通移动边缘计算网络安全威胁

本节基于四大基本攻击角度即网络基础设施、服务基础设施、虚拟化基础设施和终端设备[28]，结合轨道交通自身的特点来分析讨论轨道交通移动边缘计算网络面临的安全威胁，如表 3 所示。

3.1 网络基础设施

网络基础设施由所有能够传输数据或指令的组件组成，主要包括无线接入网、移动边缘网和核

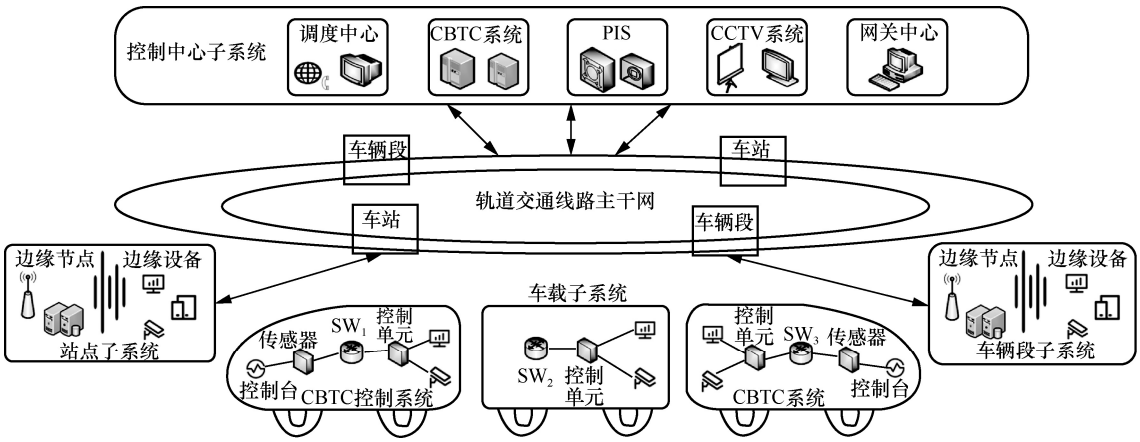

图 3 轨道交通移动边缘计算网络架构

心网，任一基础设施都可能被当成攻击目标。

1) 网络基础设施 DoS 攻击

DoS 攻击可以消耗系统和网络设备的数据处理能力，破坏数据的可用性，其主要特点是多个节点，甚至整个网络都无法响应来自系统的请求。为监测车辆的运输状况并自动化运行列车，轨道交通系统安装了大量的传感器和控制器，这些传感器和控制器分布在安全保护薄弱的边缘侧，而且列车为了保持稳定运行，难以经常更新设备，上述限制削弱了设备的安全性，为僵尸病毒提供了可乘之机。被感染的设备如果向无线网络接入点发出大量请求，网络接入点就无法处理其他合法用户的请求；如果向资源受限的边缘计算节点发送大规模的请求，边缘主机提供的服务就会被阻塞。在这种情况下，DoS 攻击会导致轨道交通移动边缘计算网络无法提供正常的网络服务，造成整个网络瘫痪。

2) MitM 攻击

MitM 攻击的特点是存在一个恶意的第三方，在 2 个或多个通信方之间插入，并秘密转发或拦截双方之间的通信。在轨道交通系统中，复杂多样的设备之间通信关系也十分复杂，如车载控制器、轨旁区域控制器（ZC）设备、ATS 系统等均需进行大量的交互数据通信，系统接口多且使用非安全的通信协议。攻击者可以利用这些漏洞获得网络接口的访问权进而控制一部分网络。攻击者通过在会话中间抓包，读取敏感隐私信息，并且将篡改后的数据转发给会话的另一方，这不仅导致终端设备和云中心的交互数据被窃听，而且可能会返回错误指令和结果，严重威胁乘客的生命安全。轨道交通系统引入 MEC 技术后，MitM 攻击会更加强大，因为 MEC 严重依赖于虚拟化，MitM 攻击会破坏边缘级的内部虚拟化基础设施实体，从而很容易地影响到更多元素。

3) 恶意网关攻击

MEC 的开放性原则使攻击者可以相对容易地将恶意网关加入系统中。攻击者通过部署未经授权的网关来访问网络设备、应用程序和边缘服务器等，使网络设备出现故障以致无法提供网络服务或窃取边缘服务器的行车数据。恶意网关也可以劫持通信信道，发动中间人攻击。乘客还可能被诱导连接到恶意网关，导致敏感信息泄露。恶意网关部署在列车上会比部署在轨旁有更大的杀伤力，因为部署在列车上的恶意网关可以与车载设备以及乘客保持更长时间的通信，攻击者可以长时间干扰车载控制器，同时更方便地窃取乘客隐私信息。

3.2 服务基础设施

在轨道交通移动边缘计算网络中，最主要的服务设施就是部署在网络边缘为用户提供计算、网络和存储服务的 MEC 节点。本节将介绍 MEC 主机层和 MEC 系统层易遭受的安全威胁。

表 3　　轨道交通移动边缘计算网络安全威胁

攻击角度	攻击模型	易感于攻击或加重影响的原因	造成影响
网络基础设施	DoS 攻击	防护能力弱；通信协议多样化；缺乏数据加密和消息验证机制	轨道交通移动边缘计算网络无法提供正常的网络服务，继而造成整个网络瘫痪
	MitM 攻击	通信关系复杂	隐私泄露、传达错误指令和结果影响行车决策
	恶意网关攻击	开放性	数据泄露、干扰网络设备提供服务
服务基础设施	DoS 攻击	依赖虚拟化、防护能力弱	MEC 主机无法提供服务、对整个轨道交通系统产生影响
	恶意注入攻击	身份认证机制和防护能力都比较薄弱	MEC 服务器做出错误的判断和指令影响列车业务、造成更多的服务器感染
	非授权访问攻击	身份认证、访问管理机制存在缺陷	隐私泄露、MEC 服务器对沿途列车的运行判断失误
	恶意节点攻击	身份认证、访问管理机制存在缺陷	破坏核心网络的稳定性、造成整个边缘计算网络的瘫痪
虚拟化基础设施	DoS 攻击	多租户	耗尽运行虚拟机的边缘服务器的资源、影响其他应用程序
	虚拟机逃逸	软件漏洞	在虚拟机管理器层或者管理域中安装后门、执行 DoS 攻击、窃取用户数据以及控制其他虚拟机等
	虚拟机复制	频繁的网络切换	发动从信息抽取到复制运算密集型任务等多种形式的攻击、损害其他服务器或数据中心的安全性
终端设备	侧信道攻击	具有丰富的信道信息	隐私泄露
	非授权访问攻击	身份认证、访问管理机制存在缺陷；频繁切换	影响行车决策、隐私泄露、导致更多的 MEC 服务器被感染

1) 服务基础设施 DoS 攻击

在轨道交通场景下，MEC 主机不仅可能受到海量终端设备发起的 DDoS 攻击，被感染的应用程序也可以控制 MEC 服务器的移动边缘平台管理器，为特定应用分配更多不必要的资源[29-30]。此外，MEC 高度依赖虚拟化的特性也使攻击者可以通过控制恶意虚拟机占用 MEC 主机的资源，导致用户无法正常请求 MEC 服务，而且缺少了外置硬件安全防护的虚拟机之间也更容易传播病毒，恶意虚拟机可以联合其他虚拟机发起大规模 DDoS 攻击。受 DoS 攻击的 MEC 主机无法提供服务，这会严重干扰列车监控视频分析等业务，考虑到 MEC 服务器的协作问题，单个边缘服务器遭受 DoS 攻击可能会对整个轨道交通系统产生影响。

2) 恶意注入攻击

将恶意软件、虚假数据等有效且隐蔽地注入计算机系统或通信链路的行为被称为恶意注入攻击。和云计算中心相比，轨道交通 MEC 服务器身份认证机制粒度较粗，服务器系统安全配置薄弱，很难支持高性能防火墙，这些缺陷使 MEC 服务器更容易受到恶意注入攻击。MEC 服务器受到攻击后，恶意代码能够通过主机之间的通信连接感染另一个主机。攻击者将恶意软件或数据注入 MEC 服务器后，就可以对计算机和基于计算机的系统和功能造成自主破坏并发布虚假数据，导致 MEC 服务器做出错误的判断和指令，对列车的控制和运行、乘客票务等产生恶劣的影响。

3) 服务基础设施非授权访问攻击

未授权访问是指身份认证、访问管理机制存在缺陷，导致攻击者在没有获取到登录权限或未授权的情况下可以直接访问，从而引发重要权限可被操作、敏感信息泄露等问题。MEC 平台会向某个边缘设备或其应用程序授予权限，如果攻击者打算直接访问受保护的 MEC 平台或边缘设备，则会被认证系统阻止，所以攻击者会利用 MEC 系统的认证和授权协议的弱点，绕过或欺骗认证过程以执行未经授权的访问[31]。通过非授权访问，攻击者盗取或修改铁路沿线 MEC 服务器数据，可导致乘客隐私泄露或使 MEC 服务器对沿途列车的运行判断失误。

4) 恶意节点攻击

攻击者一旦通过非授权访问攻击获得整个MEC服务器的控制权，这个节点就变成了恶意节点。攻击者获得了节点的所有权限，它可以对所有传入和传出节点的信息进行操作，这与中间人攻击类似。但由于 MEC 服务器的资源和可实施的功能比一般节点多而且可与列车控制中心和车载终端双方通信，借助这种“中介”身份，攻击者既可以向车载控制器发送错误指令，也可以向核心网络提供虚假信息，破坏核心网络的稳定性[32]，这种攻击的影响范围和破坏性都比普通的中间人攻击更大。除此之外，恶意 MEC 服务器还可以攻击邻近的 MEC 服务器，进而影响整个轨道交通移动边缘计算网络。

3.3 虚拟化基础设施

虚拟化基础设施是轨道交通边缘数据中心的核心之一，支持在网络边缘部署云服务。虚拟化基础设施可能通过多种方式被利用，而且攻击者还会控制虚拟机本身来利用可用的资源。

1) 虚拟化基础设施 DoS 攻击

当虚拟机本身被恶意对手控制成为恶意虚拟机时，它就尝试耗尽运行它的边缘服务器的资源（包括计算、网络和存储资源），与物理机不同，虚拟化环境下可能存在多租户的服务模型，即多个虚拟机共享同一台物理主机，所以同一台物理机的其他虚拟机也会因为资源耗尽而停止服务。

2) 虚拟机逃逸

虚拟机逃逸是指利用虚拟机软件或者虚拟机中运行的软件漏洞进行攻击，破坏系统的隔离性来操控虚拟机监控器或宿主操作系统。虚拟机逃逸会造成在虚拟机管理器层或者管理域中安装后门、执行 DoS 攻击、窃取用户数据以及控制其他虚拟机等后果[33]。

3) 虚拟机复制

一个被攻击者控制的主机能够对运行于其中的虚拟机发动从信息抽取到复制运算密集型任务等多种形式的攻击。此外，攻击者也能够通过恶意代码或是其他含有害因素的虚拟机在不同节点之间的迁移对其他的节点造成损害[28]。轨道交通高速移动的特性和地理环境的复杂性会造成频繁的网络切换，为保证用户服务的可靠性，需要进行虚拟机的任务迁移，一旦恶意虚拟机迁移到其他物理位置，将会损害其他服务器或数据中心的安全性。

3.4 终端设备

由于海量的终端设备分布分散，终端设备暴露的攻击面较大，同时，它们使用面向功能的多样化通信协议且缺乏数据加密和消息验证机制，而且碍于终端在操作系统、内存管理、通信、物理设计和

结构方面的各种技术，很难部署完善的防护机制。

1) 侧信道攻击

侧信道攻击是指使用任何对隐私不敏感的、可公开访问的信息，探索隐藏的相关性，最终从侧信道推断出敏感数据如密码、登录凭证、电子邮件和位置信息[34]。以轨道交通 PIS 业务为例，乘客通过手机终端可完成地铁网络购票、车辆到发站信息查询以及车站拥挤情况查询等，数据交互行为较多，需要频繁发送信号，具有丰富的信道信息。在这种情况下，攻击者不一定是边缘设备或边缘服务器，它可以是任何恶意节点，攻击者会不断地嗅探网络信号并从中提取敏感信息[31]。

2) 终端设备非授权访问攻击

轨道交通终端设备普遍存在安全配置弱等问题，易暴露在威胁下。终端受到的非授权访问攻击方式与 MEC 服务器基本一样。攻击者访问终端设备后，可以向车载控制器报告错误数据影响行车决策，也可以获取和篡改终端设备数据导致敏感数据泄露。如果攻击者向终端设备注入恶意代码，由于车载终端设备在高速移动状态时需要切换 MEC 服务器，则可能导致更多的 MEC 服务器被感染。

3.5 安全威胁对比分析

和轨道交通通信网络相比，轨道交通移动边缘计算网络引入了 MEC。MEC 服务器的防护能力相对较弱，所以轨道交通移动边缘计算网络更容易受到恶意注入攻击等，MEC 的开放性原则也使恶意网关加入系统的难度降低。当受到 DoS 攻击时，某些性能不强的 MEC 服务器更容易瘫痪，由于依赖虚拟化技术，DoS 攻击会导致同一物理机上的其他虚拟机也因为资源耗尽而停止服务，多个任务都会受到影响；受到 MitM 攻击时，攻击会破坏边缘级的内部虚拟化基础设施实体，影响范围更广。虚拟化技术还引入了轨道交通通信网络所没有的攻击模式，即虚拟机逃逸等虚拟机特有的安全威胁。

和移动边缘计算网络相比，轨道交通移动边缘计算网络设备之间通信关系复杂，系统接口多且使用非安全的通信协议，所以网络容易被攻击者控制而受到 MitM 攻击。乘客通过手机终端可完成各类地铁业务，需要频繁发送信号，数据交互量较大，具有丰富的信道信息，易受到侧信道攻击。如果终端被注入恶意代码，随着车载终端设备的高速移动，终端会与不同的 MEC 服务器交互，相比于移动边缘计算网络，轨道交通移动边缘计算网络的高速移动特性会导致更多的 MEC 服务器被感染，后果更加严重。

4 轨道交通边缘计算安全防护

本节基于业界的相关研究，从身份认证机制、入侵检测技术、隐私保护、虚拟化安全和基于 SDN 的安全防护架构等方面总结分析了适用于轨道交通移动边缘计算网络的安全防护方案。

4.1 身份认证机制

身份认证是安全入口点，完善的身份认证系统能屏蔽各类非法访问，有效抵御 DDoS、恶意网关、权限升级等攻击，其重要性也使大多数攻击者在准备摧毁网络时首先会破坏认证系统，因此，在研究城市轨道交通移动边缘计算网络防护方案时，第一步便是身份认证。轨道交通作为时延敏感型业务，不希望通过距离较远的中央服务器完成认证，而且 MEC 节点本身就是分布式部署，所以应设计一种能满足低时延、高带宽的分布式身份认证机制；任何安全机制的设计都应防止数据被篡改，身份认证机制同样需要具备不可篡改性。身份认证机制可以借助区块链技术实现分布式和不可篡改的要求，因为区块链是分布式系统，而且区块体内采用默克尔树结构，这种结构使区块链具有不可篡改性。为契合轨道交通的特点，轨道交通移动边缘计算网络的身份认证机制将以区块链为核心，并满足跨域、快速切换、轻量化和匿名性认证要求。

1) 跨域认证

轨道交通移动边缘计算网络中存在多种功能的 MEC 服务器，这些服务器来自不同的服务提供商，所以在设计身份认证时需要考虑跨多信任域的问题。联盟链作为一种准入型区块链，能够更好地保护数据隐私，因此，可以借助联盟链来解决跨域认证中的域间信任问题。Sun 等[35]利用通道技术通过许可区块链、基于属性的访问控制和基于身份的签名构建了一个跨域访问控制系统。受到通道技术的启发，轨道交通移动边缘计算网络在进行跨域认证时，可以基于联盟链利用共识机制、智能合约和通道技术，保持各个域数据的一致性，并通过不同信任域节点的相互背书实现跨域认证。

2) 快速切换认证

列车的高速移动使终端需要频繁地与不同的 MEC 服务器进行认证，轨道交通场景下的身份认证应实现快速切换认证，提高认证效率。认证 Ticket

可用于终端的切换重认证，在切换重认证时，车载终端和用户向 MEC 节点发送认证 Ticket，MEC 节点只需利用认证 Ticket 即可快速完成认证。

3) 轻量化认证

车载控制器、车载传感器、用户设备等终端资源有限，认证过程要减少资源消耗，具备低能耗性。ECC 和 RSA 具有相同安全性，但 ECC 的密钥较短，计算量更小，使用基于 ECC 的签名算法可以构造轻量化的认证方案。

4) 匿名性认证

终端在身份认证时面临着被第三方窃听的风险，所以应在正确进行身份认证的前提下避免暴露身份信息。零知识证明可以不让验证方得到任何有用的信息而证明合法性，从而有效保护身份隐私。除了零知识证明，椭圆曲线也可用来保护身份隐私，彭维平等[36]提出一种基于椭圆曲线双线性对性质的身份隐私保护方案，该方案通过选取某个 MEC 节点作为可信中心，使可信中心分配系统参数且对车载终端进行匿名化处理，实现终端用户身份隐私保护。

除了以上方案，为提高身份认证机制抵御攻击的能力，双因素身份认证以及结合深度学习、生物特征和物理特征的认证方案也可成为选择。

4.2 入侵检测技术

入侵检测系统能够实现主动检测异常和网络入侵告警，具有消耗资源少和便于部署的特点，适合资源和成本受限的轨道交通移动边缘计算网络。本节将从基于信息理论的检测方法和基于机器学习的检测方法 2 个方面分析轨道交通边缘计算场景下的入侵检测技术。

1) 基于信息理论的检测方法

沿着轨道行驶的列车的通信链路、运行模式和业务模型大多比较固定，通信往往是有规律的，所以轨道交通系统的信息熵相对稳定，当大量的恶意消息注入正常的通信中时会影响网络的稳定性（如 DoS 攻击），信息熵会显著降低，因此利用信息熵可以反映网络的异常情况。

目前，基于信息熵的检测方法大多只适用于高强度的攻击类型，低速率的恶意信息注入攻击比较隐蔽，难以检测。为了检测轨道交通面临的低速率攻击，可借鉴 Xiang 等[37]提到的基于广义熵和信息距离的检测方法，由于低速率攻击流量和正常流量的信息熵差值较小，可选择受阶数影响的广义熵和信息距离作为信息度量，通过选取合适的阶数值来放大正常流量和异常流量的差值从而提高检测精度。

虽然城市轨道交通业务整体比较固定，但受时间段、社会活动和突发事件影响比较大的 CCTV 和 PIS 业务会存在非周期性的消息和不同传输速率的情况。为了解决该情况带来的信息熵抖动问题，可以参考 Wu 等[38]提出的一种基于固定消息数量的滑动窗口策略，该策略利用模拟退火算法获得最佳滑动窗口大小和决策条件，实现高精度、低时延的入侵检测设计。

在以上提出的 2 种入侵检测系统中，如果系统测出的结果大于阈值，就会发出入侵告警。因此可以设置若干管理 MEC 节点的控制器，控制器根据列车行驶的速度、MEC 节点相隔的距离等因素将 MEC 节点划分为不同的物理区域，同一区域的 MEC 节点会协同跟踪异常设备，并拒绝其接入网络的请求。

现有的入侵检测系统没有考虑自身的安全性和可信性问题，一旦入侵检测系统被网络攻击者捕获，就会产生大量的恶意告警，严重影响基于通信的列车控制系统的运行，因此需要研究入侵检测系统的可信度。Hu 等[39]提出的方案可以移植到轨道交通边缘计算场景：选择分散的 MEC 节点作为入侵检测器构建分布式可信网络，每个 MEC 节点都具有检测攻击、评估其他 MEC 节点的可信性和管理可信性数据的能力。在该架构的基础上，采用相对熵方法实现入侵检测并建立基于模糊理论的信任评估模型，对入侵检测系统的可信度进行量化。

基于信息理论的入侵检测方法可识别的威胁类型少，并且不同的轨道交通移动边缘计算网络的状态并不完全相同，从而使信息熵有所抖动，这类方法难以应对复杂多变的攻击。针对以上缺陷，基于机器学习的入侵检测技术有望解决这些问题。

2) 基于机器学习的检测方法

环境的复杂性和攻击的多样性使传统的入侵检测技术力不从心，研究者发现基于机器学习的入侵检测系统能提高检测效率和决策能力。

根据 Li 等[40]提出的一种通过引入边缘智能来解决 CBTC 受到 MitM 攻击的方案，可以得到适用于轨道交通边缘计算的入侵检测方法。在检测阶段，设计一种基于 LSTM 和支持向量机（SVM, support vector machine）的先验概率检测方案，结合列车的位置、

速度、日志文件等信息来进行 MitM 攻击检测。在防御阶段，构建一个基于贝叶斯博弈的防御模型，推导出针对 MitM 攻击的最优防御策略，考虑到车载计算机计算能力较差，将 MEC 节点当作边缘智能服务器，并将提出的防御方案在 MEC 节点上实现。

通过借鉴 Gao 等[41]提出的一种基于 AdaBoost 多分类算法，可以提出在轨道交通移动边缘计算网络中防 DoS 攻击的检测方法：首先建立数据的 n 元模型，通过学习得到典型正常行为集和典型异常行为集；然后设计一种用相似度度量算法构造的 AdaBoost 弱分类器，提高 AdaBoost 算法的分类效果；最后得到一种 AdaBoost 多分类算法来检测攻击。不过，轨道交通通信系统中环境复杂，隧道环境、列车高速运动等导致的随机延迟和丢包可认为是数据的噪声，由于噪声好像攻击，因此在数据集中应弱化对噪声的关注。每个 MEC 节点负责在本特征范围类选择出最好的特征，MEC 节点通过协同进行分布式的 AdaBoost 训练来提高训练速度。

对于未知攻击模型的入侵检测，机器学习的准确率较高，然而在资源受限的轨道交通移动边缘计算网络中，基于机器学习的入侵检测方法如何实现轻量化且不影响检测准确率还有待进一步解决。

4.3　隐私保护

用户与 MEC 节点涉及较多的数据交互，各类隐私都面临着泄露的风险。隐私保护是防止敏感数据泄露的技术，能为信息的隐私提供严格的可量化的保护[42]。鉴于在身份认证机制中已经提到身份隐私保护问题，本节将从位置隐私保护和数据隐私保护两方面介绍。

1) 位置隐私保护

由于列车的运行轨迹比较固定，而且乘客为了获得基于位置的服务（LBS, location based service）需要汇报自己的位置，因此攻击者可以很容易地定位和预估乘客的位置信息来分析用户的行为模式和习惯。为了更好地推动 LBS 的发展，保护位置隐私至关重要。Liang 等[43]提出了一种保护移动用户位置信息的方案，该方案采用马尔可夫链分布式缓存推送代理，可以将位置信息分成组并单独存储。位置信息通过从缓存代理接收基于位置的数据来保存，而不向服务提供者透露它们的真实位置。Ma 等[44]提出了一种 LBS 边缘计算增强隐私保护框架。MEC 节点负责通过 K 匿名计算任何进行 LBS 查询的用户的虚拟位置，在密文计算的基础上，通过 MEC 节点与 LBS 服务器的交互构造服务响应。其基本思想是将加密后的位置存储在 MEC 节点中，LBS 只能得到虚拟位置与服务目标之间距离的秩。

2) 数据隐私保护

在联邦学习中，数据不出本地的思想可以有效地保护数据隐私。针对轨道交通边缘计算中终端处理大量数据效率低且存在隐私泄露风险的问题，可参考刘庆祥等[45]提出的基于联邦学习的边缘计算方法，架构如图 4 所示。该方法从参与者选择、本地更新和全局聚合 3 个方面改进了联邦学习算法：在每一轮次的更新开始时，MEC 节点会确定参与终端并将模型参数传递至这些终端，然后生成参与者密钥。本轮次的参与者利用本地数据进行学习并将更新的模型参数加密后上传至 MEC 节点。MEC 节点采用 q-FedSGD 算法来聚合参与终端上传的数据，生成新的模型参数，直至达到全局更新轮数或者整个模型收敛。该方案可以使终端在保证目标精度的前提下大幅降低联邦学习的开销，符合轨道交通低时延和终端低能耗的要求。

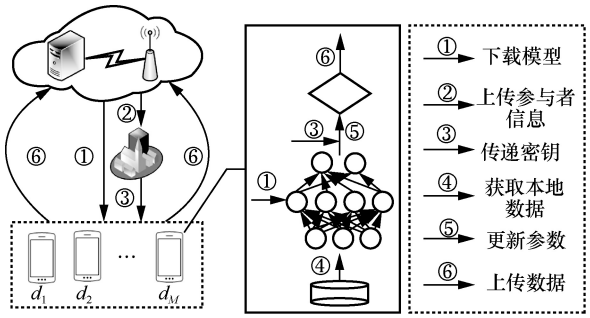

图 4　基于联邦学习的轨道交通边缘计算隐私保护架构

隐私保护方案会给边缘节点带来负载问题，如何设计轻量级的隐私保护方案，避免 MEC 节点花费过多的资源来保护用户的隐私成为未来研究的方向之一。

4.4　虚拟化安全

虚拟化基础设施是边缘范式的核心元素之一，因此必须通过在所有边缘数据中心中设计和部署安全机制来保护它。

虚拟机自省（VMI, virtual machine introspection）或虚拟机监视器自省可用于检测虚拟机或虚拟机监视器行为中的异常模式。VMI 根据处理器和内存利用率监视虚拟机的活动。文献[46]提出功能扩展 VMI，该 VMI 能够中断虚拟机的执行，或者在虚拟

机状态偏离正常的操作标准时隔离正在运行的程序。VMI 可以在边缘和核心级别启动，以检查移动边缘平台管理器、移动边缘计算编排器等行为。

虚拟机的隔离机制可以保障各虚拟机独立运行、互不干扰，防止因一个虚拟机出现错误影响其他虚拟机应用程序的运行。文献[47]基于硬件协助的隔离机制，提出一种基于 Intel VT-d 技术的虚拟机安全隔离架构，该架构通过安全内存管理和安全 I/O 管理 2 种手段进行保护。

4.5 基于 SDN 的安全防护架构

软件定义网络（SDN, software defined network）可以以安全为中心，简化安全基础设施来提高网络的灵活性，从而更好地整合多种安全设备和解决方案，并将多种安全解决方案编排为统一的防御层。文献[48-49]设计了一种基于 SDN 的安全轨道交通架构，此安全架构由终端设备、SDN 交换机、集群 SDN 控制器和主 SDN 控制器四部分组成，其中，集群 SDN 控制器根据其安全角色分为身份加密控制器、密钥管理控制器和入侵检测控制器，通过将不同的控制器与不同的安全角色相关联，可以大大提高整个架构的安全性能，架构如图 5 所示。

1) 终端设备

在轨道交通场景下，无论是车辆段子系统还是站点子系统，都有众多的终端设备。这些设备可能包括手机、监控摄像头、智能照明系统以及各种传感器设备等，这些设备连接到 SDN 交换机上。

2) SDN 交换机

在此安全架构中，假设为每个终端设备都分配一个与之兼容的 SDN 交换机，该 SDN 交换机可以实施各种安全策略和规则，这些交换机是服务提供商网络的端点。

3) 集群 SDN 控制器

终端设备的地理位置形成一个由少数终端设备组成的集群，车辆段子系统和站点子系统都可以作为一个集群，整个集群的交换机由集群 SDN 控制器控制。根据安全功能可分为以下控制器。

入侵检测控制器。此控制器负责监视网络流量并管理每个流的规则，由学习模块、分类模块和流量管理模块 3 个模块组成。前 2 个模块用于检测网络流量的异常情况，最后一个模块负责根据需要调整网络流量规则。

密钥管理控制器。此控制器作为对称和非对称密钥的存储库，负责处理共享密钥的密钥分发。此外，此控制器可以充当第三方提供密钥管理服务。

身份加密控制器。此控制器负责用户的身份验证和身份管理，在轨道交通动态、异构和可扩展特征的环境下，通过多种加密算法实现完整性、机密性、隐私性的身份加密控制。

4) 主 SDN 控制器

作为整个安全架构的最高层，主 SDN 控制器位于轨道交通通信网络的控制中心子系统，所有的集群 SDN 控制器都由此主 SDN 控制器控制。

4.6 防护方案对比分析

和轨道交通通信网络相比，轨道交通移动边缘计算网络引入了来自不同服务提供商的 MEC 服务器，设计身份认证机制时需考虑跨域问题。由于 MEC

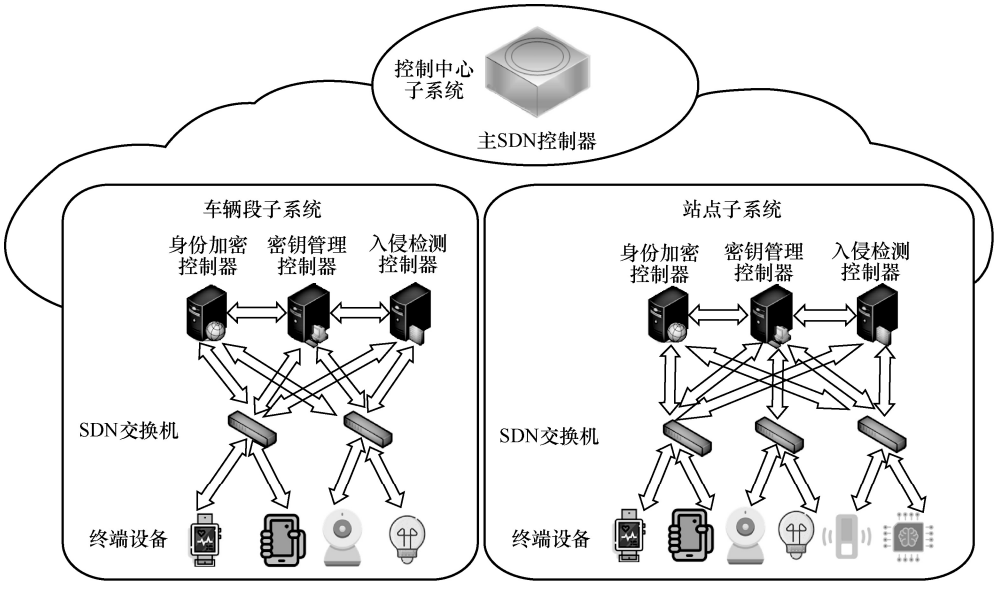

图 5 基于 SDN 的安全防护架构

服务器分布式部署且资源受限，设计入侵检测方案时需考虑多服务器协作检测且应减少服务器的计算量。由于该网络面临着针对虚拟机的攻击模式，因此应部署新的安全机制来保障虚拟机的安全。

和移动边缘计算网络相比，列车的高速移动使终端需要频繁与不同 MEC 服务器进行认证，所以在设计身份认证机制时需考虑如何实现高效的切换认证。入侵检测方案的设计与列车的运行环境、运行模式等紧密相关，如轨道交通系统的信息熵相对稳定，所以可利用信息熵进行检测。此外，隧道环境存在噪声，所以在数据集中应弱化对噪声数据的关注。由于轨道交通系统特有的业务类型和结构，4.5 节提出的安全防护架构只适用于轨道交通场景，不能对通用的移动边缘计算网络进行防护。

5　开放性问题

5.1　动态场景下的有限资源使用

轨道交通的地形和通信环境复杂，MEC 节点的通信和计算资源有限，一旦攻击发生，通信和计算资源就会面临枯竭，而现有的防护方案如基于机器学习的入侵检测方法也会消耗大量的计算和带宽资源。为应对资源受限问题，可以考虑利用分组压缩来减少传输的比特量，提高无线通信的效率。但这个方法无法从根本上解决资源不足问题，下一步还需要优化防护方案，在保证准确性的基础上降低算法复杂度和运算量，并设计合适的卸载和调度策略以充分高效利用 MEC 节点的通信和计算资源。

5.2　轨道交通通信网络和 MEC 的兼容性

列车电子零部件由不同供应商单独提供，不同供应商开发不同的分布式子系统，所以轨道交通的设备制式和协议标准等都存在一定的差异，而且轨道交通内部使用了大量私有协议，难以匹配现有 MEC 网络固有的网络接口和协议标准。研究人员以及服务供应商需要建立严格的测试、审查、验证体系，推进体系标准化工作，进行相关兼容性分析，解决系统之间的协调问题，制定针对轨道交通和 MEC 的统一安全方案。

5.3　针对新型攻击的防御

网络攻击手段层出不穷，未来会有更多的新型网络攻击威胁轨道交通移动边缘计算网络。由于未知攻击种类繁多，特征不明确，只针对特定的攻击类型而且检测效果稳健性不强的检测方法难以识别并应对未知攻击。因此，需要解决如何通过入侵检测模型和算法的优化研究来提高防护方案的通用性问题。目前可供参考的思路有：构建已知攻击和未知攻击之间的关联关系或对未知攻击进行聚类分析，分类后利用数据挖掘等方法提取未知攻击的特征规则[50]，但如何准确提取攻击行为中一些出现次数不多的特征值还需思考。

5.4　隐私机制和政策的标准化

轨道交通移动边缘计算网络集成了 NFV、SDN、5G 等技术，这些技术由不同的机构和公司操作并制定标准，隐私的概念没有标准定义，不同的机构和公司对隐私信息分类、隐私保护范围等都有不同的标准，这将直接影响整体隐私保护方案的设计。因此，政府和标准化组织等监管实体需要与该行业合作，根据新技术定义和更新隐私法规，同时，与信息安全相关的委员会可以完善轨道交通移动边缘计算网络的安全指南。在法规和指南的规范和指导下，这些技术组织之间可以建立一个关于轨道交通移动边缘计算网络隐私机制和政策的共同行为准则，在明确隐私信息分类、隐私保护范围、隐私保护原则及处理规范的基础上确定隐私保护框架以减轻利益冲突，建立统一的可互操作的隐私保护机制。

5.5　安全测试评估

为验证所提防护方案的准确性，需要模拟列车在真实环境中所受的攻击。然而，列车内部系统异构复杂，高速移动时外在的环境动态多变，这种复杂性不仅使列车易受多种攻击，也给实验测试带来巨大挑战。列车受到攻击时，数据会如何变化、外部的环境又会造成什么影响等都是在实验时需要考虑的，如何使测试数据更接近真实场景并保证安全测试的精度和效果是亟须解决的问题之一。

6　结束语

融合了 MEC 技术的城市轨道交通通信网络在提供更好的服务质量的同时也面临着不可忽视的安全威胁问题，由于轨道交通这一场景具有特殊性，对轨道交通移动边缘计算网络安全的研究不仅有学术价值，还有重要的社会意义。在此背景下，本文首先介绍了轨道交通和 MEC 的基本情况；其次对轨道交通移动边缘计算网络的架构和面临的安全威胁进行了分析和探讨，并针对安全威胁提出了对应的安全防护方案；最后讨论了该领域的开放性研究问题。

参考文献：

[1] LIEM M, MENDIRATTA V B. Mission critical communication networks for railways[J]. Bell Labs Technical Journal, 2011, 16(3): 29-46.

[2] WU H, LI F, DU C X, et al. City urban rail transit train-ground wireless communication network research based on LTE technology[C]//Proceedings of 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA). Piscataway: IEEE Press, 2020: 217-220.

[3] 纪艺勇. LTE 技术在地铁专用通信系统中的应用方案[J]. 中国科技纵横, 2016(21): 21-22.
JI Y Y. Application research on LTE technology in subway dedicated communication system[J]. China Science & Technology Overview, 2016(21): 21-22.

[4] 彭亚枫. 城轨 CBTC 系统中间人攻击检测与防御方法研究[D]. 北京: 北京交通大学, 2018.
PENG Y F. Research on detection and defense method of man-in-the-middle attack in CBTC system of urban rail transit[D]. Beijing: Beijing Jiaotong University, 2018.

[5] 熊桢. 轨道交通无线通信系统业务类型及技术方案探析[J]. 智能城市, 2020, 6(12): 172-173.
XIONG Z. Analysis on the service type and technical scheme of rail transit wireless communication system[J]. Intelligent City, 2020, 6(12): 172-173.

[6] 毛磊, 翟浩杰, 尹尚国. 5G 在轨道交通行业的应用探讨[J]. 移动通信, 2020, 44(1): 63-70.
MAO L, ZHAI H J, YIN S G. Discussion on the application of 5G in the rail transportation industry[J]. Mobile Communications, 2020, 44(1): 63-70.

[7] 丁超, 陈英, 鉴纪凯, 等. 城市轨道交通列车网络安全研究[J]. 现代城市轨道交通, 2022(9): 81-86.
DING C, CHEN Y, JIAN J K, et al. Research on network security of urban rail transit trains[J]. Modern Urban Transit, 2022(9): 81-86.

[8] 刘魁. 城市轨道交通网络安全集中管控防护方案[J]. 都市快轨交通, 2022, 35(2): 85-90.
LIU K. Centralized control and protection scheme for urban rail transit network security[J]. Urban Rapid Rail Transit, 2022, 35(2): 85-90.

[9] WANG Y, ZHANG W F, WANG X M, et al. Improving the security of LTE-R for high-speed railway: from the access authentication view[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(2): 1332-1346.

[10] XU T, GAO D Y, DONG P, et al. Improving the security of wireless communications on high-speed trains by efficient authentication in SCN-R[J]. IEEE Transactions on Vehicular Technology, 2019, 68(8): 7283-7295.

[11] HEI X H, GAO W, WANG Y C, et al. Railway key exchange scheme for improving communication efficiency of RSSP-II protocol[C]//Proceedings of 2019 IEEE Globecom Workshops (GC Wkshps). Piscataway: IEEE Press, 2020: 1-6.

[12] WU P W, WU Z D, LI L Y. Research on MAC verification code of railway signal security communication protocol[J]. Journal of Physics: Conference Series, 2021: doi.org/10.1088/1742-6596/1757/1/012166.

[13] LI J, WU H. Localisation algorithm for security access control in railway communications[J]. IET Intelligent Transport Systems, 2020, 14(14): 2151-2159.

[14] CHENG J F, KANG R W, ZHAO X Q. Role based access control and its application in high speed railway[C]//Proceedings of 2013 Sixth International Conference on Advanced Computational Intelligence (ICACI). Piscataway: IEEE Press, 2014: 362-364.

[15] PARICHEHREH A, SPAGNOLINI U. Seamless LTE connectivity in high speed trains[C]//Proceedings of 2014 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2014: 2067-2072.

[16] WANG J R, YANG X J, ZHAO S Y, et al. Handover performance improvement for ultra dense network of high-speed railway[C]//Proceedings of 2017 IEEE 85th Vehicular Technology Conference (VTC Spring). Piscataway: IEEE Press, 2017: 1-5.

[17] ETSI. Mobile-edge computing: introductory technical white paper[R]. 2014.

[18] 谢人超, 廉晓飞, 贾庆民, 等. 移动边缘计算卸载技术综述[J]. 通信学报, 2018, 39(11): 138-155.
XIE R C, LIAN X F, JIA Q M, et al. Survey on computation offloading in mobile edge computing[J]. Journal on Communications, 2018, 39(11): 138-155.

[19] 边缘计算产业联盟和工业互联网产业联盟. 边缘计算安全白皮书[R]. 2019.
Edge Computing Consortium and Alliance of Industrial Internet. White paper on edge computing security[R]. 2019.

[20] GUO S Y, HU X, ZHOU Z Q, et al. Trust access authentication in vehicular network based on blockchain[J]. China Communications, 2019, 16(6): 18-30.

[21] NI J B, LIN X D, SHEN X S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 644-657.

[22] JIA Y Z, ZHONG F T, ALRAWAIS A, et al. FlowGuard: an intelligent edge defense mechanism against IoT DDoS attacks[J]. IEEE Internet of Things Journal, 2020, 7(10): 9552-9562.

[23] CHOI J, AHN B, BERE G, et al. Blockchain-based man-in-the-middle (MITM) attack detection for photovoltaic systems[C]//Proceedings of 2021 IEEE Design Methodologies Conference (DMC). Piscataway: IEEE Press, 2021: 1-6.

[24] LI X, LIU S P, WU F, et al. Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications[J]. IEEE Internet of Things Journal, 2019, 6(3): 4755-4763.

[25] ZHAO J H, LIU J, YANG L H, et al. Future 5G-oriented system for urban rail transit: opportunities and challenges[J]. China Communications, 2021, 18(2): 1-12.

[26] 谢高畅, 卢华, 唐琴琴, 等. 区块链在轨道交通移动边缘计算网络中的应用[J]. 电信科学, 2021, 37(10): 117-125.
XIE G C, LU H, TANG Q Q, et al. Application of blockchain in rail transit edge computing network[J]. Telecommunications Science, 2021, 37(10): 117-125.

[27] LIU X, ZHANG M J, ZOU C M, et al. Edge intelligence for smart metro systems: architecture and enabling technologies[J]. IEEE Network, 2022, 36(1): 136-143.

[28] ROMAN R, LOPEZ J, MAMBO M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges[J]. Future Generation Computer Systems, 2018, 78(2): 680-698.

[29] ALI B, GREGORY M A, LI S. Multi-access edge computing architecture, data security and privacy: a review[J]. IEEE Access, 2021, 9:

18706-18721.

[30] RANAWEERA P, JURCUT A, LIYANAGE M. MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures[J]. ACM Computing Surveys, 2022, 54(9): 1-37.

[31] XIAO Y H, JIA Y Z, LIU C C, et al. Edge computing security: state of the art and challenges[J]. Proceedings of the IEEE, 2019, 107(8): 1608-1631.

[32] RANAWEERA P, JURCUT A D, LIYANAGE M. Survey on multi-access edge computing security and privacy[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1078-1124.

[33] 叶润国, 蔡磊, 栾尚聪. 虚拟机逃逸漏洞分析和安全对策研究[J]. 信息技术与标准化, 2015(12): 30-34.
YE R G, CAI L, LUAN S C. Analysis and research on VM escaping and associated countermeasures[J]. Information Technology & Standardization, 2015(12): 30-34.

[34] LIYANAGE M, PORAMBAGE P, DING A Y. Five driving forces of multi-access edge computing[J]. arXiv Preprint, arXiv: 1810.00827, 2018.

[35] SUN S, DU R, CHEN S D, et al. Blockchain-based IoT access control system: towards security, lightweight, and cross-domain[J]. IEEE Access, 2021, 9: 36868-36878.

[36] 彭维平, 熊长可, 贺军义, 等. 边缘计算场景下车联网身份隐私保护方案研究[J]. 小型微型计算机系统, 2020, 41(11): 2399-2406.
PENG W P, XIONG C K, HE J Y, et al. Research on the identity privacy protection scheme of Internet of vehicles in edge computing scenario[J]. Journal of Chinese Computer Systems, 2020, 41(11): 2399-2406.

[37] XIANG Y, LI K, ZHOU W L. Low-rate DDoS attacks detection and traceback by using new information metrics[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(2): 426-437.

[38] WU W F, HUANG Y Z, KURACHI R, et al. Sliding window optimized information entropy analysis method for intrusion detection on In-vehicle networks[J]. IEEE Access, 2018, 6: 45233-45245.

[39] HU L R, BU B. Intrusion detection methods in communication-based train control systems based on relative entropy and trust evaluation[C]//Proceedings of 2021 IEEE International Intelligent Transportation Systems Conference (ITSC). Piscataway: IEEE Press, 2021: 3939-3944.

[40] LI Y, ZHU L, WANG H W, et al. A cross-layer defense scheme for edge intelligence-enabled CBTC systems against MitM attacks[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(4): 2286-2298.

[41] GAO B, BU B. A novel intrusion detection method in train-ground communication system[J]. IEEE Access, 2019, 7: 178726-178743.

[42] 刘艺璇, 陈红, 刘宇涵, 等. 联邦学习中的隐私保护技术[J]. 软件学报, 2022, 33(3): 1057-1092.
LIU Y X, CHEN H, LIU Y H, et al. Privacy-preserving techniques in federated learning[J]. Journal of Software, 2022, 33(3): 1057-1092.

[43] LIANG K, AU M H, LIU J K, et al. A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing[J]. Future Generation Computer Systems, 2015, 52: 95-108.

[44] MA L, PEI Q, XIAO H, et al. Edge computing enhanced privacy preserving for location based services[C]//Proceedings of IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Piscataway: IEEE Press, 2019: 1-6.

[45] 刘庆祥, 许小龙, 张旭云, 等. 基于联邦学习的边缘智能协同计算与隐私保护方法[J]. 计算机集成制造系统, 2021, 27(9): 2604-2610.
LIU Q X, XU X L, ZHANG X Y, et al. Federated learning based method for intelligent computing with privacy preserving in edge computing[J]. Computer Integrated Manufacturing Systems, 2021, 27(9): 2604-2610.

[46] GARFINKEL T, ROSENBLUM M. A virtual machine introspection based architecture for intrusion detection[C]//Proceedings of Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2003: 191-206.

[47] 林昆, 黄征. 基于 Intel VT-d 技术的虚拟机安全隔离研究[J]. 信息安全与通信保密, 2011, 9(5): 101-103.
LIN K, HUANG Z. Study on virtual machine security isolation based on Intel VT-d[J]. Information Security and Communications Privacy, 2011, 9(5): 101-103.

[48] KALKAN K, ZEADALLY S. Securing Internet of things with software defined networking[J]. IEEE Communications Magazine, 2018, 56(9): 186-192.

[49] BHUNIA S S, GURUSAMY M. Dynamic attack detection and mitigation in IoT using SDN[C]//Proceedings of 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). Piscataway: IEEE Press, 2017: 1-6.

[50] 曹扬晨, 朱国胜, 孙文和, 等. 未知网络攻击识别关键技术研究[J]. 计算机科学, 2022, 49(S1): 581-587.
CAO Y C, ZHU G S, SUN W H, et al. Study on key technologies of unknown network attack identification[J]. Computer Science, 2022, 49(S1): 581-587.

[作者简介]

谢人超（1984− ），男，福建南平人，博士，北京邮电大学教授、博士生导师，主要研究方向为算力网络、工业互联网和移动边缘计算等。

文雯（2001− ），女，安徽宿州人，北京邮电大学博士生，主要研究方向为算力网络、边缘计算、区块链等。

唐琴琴（1994− ），女，广西桂林人，博士，北京邮电大学在站博士后，主要研究方向为边缘计算、星地协同网络等。

刘云龙（2000− ），男，河南郑州人，北京邮电大学硕士生，主要研究方向为边缘计算、算力网络、任务调度等。

谢高畅（1997− ），男，山东泰安人，北京邮电大学博士生，主要研究方向为边缘计算、算力网络等。

黄韬（1980− ），男，重庆人，博士，北京邮电大学教授，主要研究方向为路由与交换、软件定义网络。