

AI 大模型在导览机器人个性化推荐中的应用研究

赵玉涛 顾欣 吴晓杰 范志龙

华电河北新能源有限公司, 河北 石家庄 050000

[摘要]伴随着 AI 技术的发展, AI 大模型应用于导览机器人个性化推荐系统的应用越来越受到重视。文章详细介绍了导览机器人的构成, 对目前 AI 大模型助力导览机器人进行个性化推荐时存在的用户数据获取不准确、个性化推荐程度不高、实时性差的问题以及网络和数据安全等问题进行了阐述。为解决以上问题, 从完善用户画像及分析、改进个性化推荐方法、提升系统的即时互动性、保障数据安全和个人隐私以及促进 AI 大模型与多模态相结合等方面提出了建议。

[关键词]AI 大模型; 导览机器人; 个性化推荐; 多模态融合; 数据安全

DOI: 10.33142/sca.v9i6.19808

中图分类号: TP18

文献标识码: A

Research on the Application of AI Large Models in Personalized Recommendation of Tour Robots

ZHAO Yutao, GU Xin, WU Xiaojie, FAN Zhilong

Huadian Hebei New Energy Co., Ltd., Shijiazhuang, Hebei, 050000, China

Abstract: With the development of AI technology, the application of AI big models in personalized recommendation systems for navigation robots is receiving increasing attention. The article provides a detailed introduction to the composition of navigation robots and elaborates on the issues of inaccurate user data acquisition, low degree of personalized recommendation, poor real-time performance, and network and data security that currently exist when AI models assist navigation robots in personalized recommendations. To solve the above problems, suggestions have been put forward from the aspects of improving user profiles and analysis, enhancing personalized recommendation methods, improving real-time interactivity of the system, ensuring data security and personal privacy, and promoting the combination of AI big models and multimodality.

Keywords: AI big model; guided robot; personalized recommendation; multimodal fusion; data security

引言

近些年来, 人工智能大模型在智能机器人个性化推荐方面有着很广阔的前景。华电河北新能源公司积极促进场站智能化升级, 相继在多个风光电站里安装了集巡检、导览、智能交互于一身的机器人系统, 探寻以 AI 大模型为引领的智慧运维新方式。但是, 在实际使用中, 现有的导览机器人对于用户数据获取的准确性、推荐结果个性化程度、实时响应速度以及网络和数据的安全性等还存在着明显的不足, 不能很好地适应新能源场站复杂的运行环境和运维人员多样化的需要。本文首先对导览机器人的系统构成和端云协同结构进行论述, 接着对目前 AI 大模型导览机器人所存在的主要问题进行分析, 最后从完善用户画像、改进推荐算法、加强实时交互、加强数据安全保护以及推进多模态技术融合这五个方面提出相应的优化策略, 希望给大模

型在导览机器人个性化推荐方面的深入应用提供一些借鉴。

1 导览机器人系统组成

导览机器人是由多种硬件以及软件组成的较为复杂的智能化设备, 在结构上一般分为四层, 即感知层、决策层、交互层以及执行层, 其中感知层用于获取环境信息以及用户交互数据, 主要由激光雷达、深度摄像头、麦克风阵列以及其他各种感知设备组成, 它们相互配合完成建图、避障、定位以及拾音等工作; 而决策层则是整个导览机器人的“大脑”, 负责所有的工作内容, 如数据处理、意图理解以及推荐生成等, 一般是以一个大的 AI 模型作为推理单元, 在此基础上再加上一个推荐器以及路径规划器, 对从感知层得到的数据进行分析后给出最终的服务决定。交互层为用户提供输出接口, 主要有触摸屏、语音合成人声、表情灯等, 以文字、语音、表情等多种方式进行交流;

执行层使机器人能够进行动作,有由伺服电机带动的自主导航系统、跟随人移动功能模块和充电等功能性部件。同时,导览机器人还要借助云上服务器完成对用户信息保存、模型更新和完善等内容管理工作,“端云协同”。

2 AI 大模型导览机器人存在的问题

2.1 用户数据获取准确性不足问题

用户的数据获取是个性化推荐的前提条件,但是目前的导览机器人在这一方面存在很大的不足。导览机器人主要收集用户的地理位置信息、语音交流以及触控等数据,但是这些数据都比较单一而且收集的方法相对简单,不能很好地反映用户的实际行为及喜好,在人声鼎沸的公共场所,通过语音获得的信息容易受到外界环境的影响造成对用户意图的判断失误,另外由于数据来源复杂,没有统一的标准使得信息更新滞后并且质量较差,降低了导览的效果^[1]。游客在游览过程中所表现出的停留时间、注视方向以及表情的变化等行为信息很少被记录下来,因此导致导览机器人对游客了解不够全面。而在数据收集时样本偏差也是需要考虑的问题,在一些情况下某些特定的人群(例如老人或者小孩)他们的行为方式可能会不同于一般人群,在这种情况下如果采样不合理就会加重推荐系统中的“马太效应”,让一些人喜欢的东西越来越受欢迎而另外一部分人的需求却被忽略。而导览机器人的数据采集也存在着隐私安全以及授权机制不完备的情况,在一些游客眼里,被机器人的摄像头、拾音器捕捉到,可能会产生一定的反感之情,进而产生拒绝对方的要求,造成数据空白或者拒绝配合等问题,进而影响到数据完整性的程度;另外,导览机器人对各方面的信息并没有一个整合处理的能力,不能够做到把空间位置坐标同行为路径以及消费习惯等进行综合建模来绘制出完整的人物肖像。

2.2 推荐结果个性化程度不足问题

虽然 AI 大模型可以产生大量高质量的内容,但是在导览场景下生成真正个性化的建议仍然有较大困难。目前大多数导览机器人所使用的推荐方法都只是简单地基于标签进行匹配,例如用户选择了某种类型的展品或者倾向于某种语言,则向用户展示相关的内容,但是不能了解用户的真正兴趣并且不断更新。在电力行业,导览机器人需面向不同角色的参观者(如运维人员、管理人员、学生等)推荐差异化的电力设备知识或安全培训内容,同样面临个性化不足的问题。传统的推荐系统使用抽象 ID 来表示数据,这使得它无法很好地理解语义也无法结合上下文信息,而由大模型驱动推荐方法虽然可以较好地解决冷启动

的问题,但是对于导览机器人的应用来说,由于用户通常只有一两次访问而且每次停留时间较短并且没有任何行为,因此模型很难通过少量的信息建立出一个正确的用户兴趣模型。对于电力变电站或营业厅的导览场景,用户可能仅短暂停留,机器人难以在短时间内获取其专业背景 and 兴趣点,导致推荐内容无法满足实际需求。导览系统个性化推荐以及动态内容更新能力不足,不能很好地适应观众多样化的需求和个人爱好。推荐的内容单一化严重,在相同展品前不同的人所得到的信息几乎一样,“个性化”只是表象,并未做到真正的个性化和定制化。

2.3 实时响应性能不足问题

实时响应能力是评价导览机器人用户体验好坏的重要标准,也是目前大模型落地应用面临的主要问题之一。由于大模型推理所需资源较大,如果全部使用云端推理,则由于网络传输以及模型计算带来的延迟会大大降低人机自然交流效率,在某主流云服务商测试中,一般机器人控制链路端到端延迟为 200~300ms,在行走过程中这么大的延迟会导致机器人重心偏离正常范围而摔倒。对于导览机器人来说,虽然延迟带来的物理风险较小,但是响应延迟过高会使对话中断,导致用户认为“机器人反应迟钝”,这是一般人不能接受的问题。大模型以及机器人操作系统对降低交互延迟起到了一定的作用,相关研究显示可以降低约 7.01% 的通信延迟,但在复杂的交互情况下,多轮对话以及实时导航所需要的大量运算会导致系统竞争资源从而让响应变得更加缓慢。

2.4 网络与数据安全问题

基于 AI 大模型的导览机器人需收集及传输大量用户个人数据,从而造成较大的网络安全及数据安全隐患。用户与导览机器人交流时所说的话、所做的动作甚至是面部照片等都属于敏感信息,如果被泄漏,会危害用户的隐私安全。基于大规模语言模型(LLM)的方法被提出解决传统推荐系统冷启动用户或者新物品的问题,但是这些方法也容易遭受重建攻击,在攻击者试图根据模型的输出恢复包含个人喜好、交互记录以及人口学特征等原始提示时,实验显示这种方法可以恢复约 65% 的用户的交互物品并且在 87% 的情况下能够推测出其年龄及性别^[2]。这说明大模型推荐系统的隐私问题不容忽视。而边缘部署虽然可以在一定程度上减少数据泄露的可能性,但由于设备本身的计算能力有限且缺少有效的安全保障机制,也无法做到完全防止数据泄露。导览机器人部署在公共场合,设备丢失、远程入侵、恶意篡改等问题不容小觑。

表 1 AI 大模型导览机器人网络与数据安全问题总结

问题类别	具体表现	潜在风险	影响范围
用户数据泄露	语音指令、行为轨迹、面部图像等敏感信息遭窃取	用户隐私被侵犯、个人信息被滥用	所有使用导览机器人的用户
模型攻击风险	通过重建攻击恢复用户偏好和人口属性信息	用户画像泄露、年龄性别等敏感信息暴露	使用大模型推荐系统的导览服务
传输加密不足	数据在云端与终端之间传输时未充分加密	中间人攻击、数据被截获与篡改	依赖云端推理的导览机器人系统
边缘设备安全薄弱	设备遗失后数据可被直接读取，缺乏远程擦除机制	设备物理安全失控后的数据外泄	部署于公共场所的导览机器人

3 AI 大模型导览机器人优化对策

3.1 完善用户画像与数据分析体系

建立准确用户画像为个性化推荐奠定基础，在导览机器人中需要从多个来源、多种类型的数据中获取用户的声音交互信息、行为轨迹、展品停留时间、点击次数等来构建多维用户画像，在数据方面要有一致性要求以及质量保证，在收集到原始数据后对其进行清理、降噪、标准化，以减少由于样本不足造成的影响。针对新用户冷启动问题，可以利用大模型零样本推理能力，利用预训练大语言模型对用户行为的理解，通过对多个方面的用户喜好进行零样本推荐，如时间、地点以及个人属性等，在实验中发现这种方法比目前最好的方法有更高的准确率^[3]。同时，用户画像还需要有学习能力，不断根据用户和智能体互动过程中给出的意见改进用户的喜好模型，让推荐系统能更及时地捕捉到用户的兴趣变化。

3.2 优化个性化推荐算法

个性化的推荐算法的改进，可以提高导览机器人智能服务的水平。由于华电河北新能源场站运维人员设备关注点不同、巡检流程有差异，所以传统的依靠标签匹配的推荐方法不能很好地满足个性化的需求。可以利用大语言模型的零样本推理能力合成上下文感知的用户表示，有效地解决了冷启动的问题，不需要大量的交互数据就可以生成有针对性的推荐。同时用检索增强生成（RAG）架构把用户过去的交互和现在的会话行为利用向量检索、外部知识库索引，从而达到具有上下文相关性的精准推荐的效果。对于导览场景交互时间短、样本少的情况，应该采用在线学习的方式，在每次人机交互之后就立刻得到运维人员的反馈，并且会及时更新用户设备喜好以及任务习惯。借助记忆检索和增强推理框架，使大模型自主地依靠历史交互记忆来开展细致的推理工作，从而加强推荐的精确度以及上下文的敏感程度。另外还要采用多样化的推荐方式，主动推送和运维任务有关的运行趋势、安全风险等信息来防止出现信息茧房现象。经过以上算法的改进，导览机器人

由原来的只进行标签匹配变成了可以进行深层次的理解，给华电河北新能源提供了一种准确高效的服务。

3.3 提高系统实时交互能力

提高实时性需从系统结构以及算法上同时进行改进，在结构方面可以采取“以边缘端推理为主、云端补算为辅”的方式，将轻量化的大模型部署到导览机器人本身，用于日常交互中即时反馈及一般性建议工作，而将较为复杂的推理交给云端处理，边缘计算结构的应用可以有效减少从感知到决策再到执行的时间，使整个循环的时间保持在一个合理的区间内^[3]。在电力巡检或变电站导览场景中，机器人需对设备异常、人员闯入等事件做出毫秒级响应，边缘端实时处理尤为关键。在算法方面还可以对大模型进行量化、知识蒸馏或者模型剪枝，在不影响推荐质量的基础上减少模型所需的运算量以及所占的存储空间。电力行业对机器人功耗和散热有严格要求（尤其在密闭开关柜室或电缆沟内），模型轻量化更具实际意义。另外，应对导览机器人所处具体情况进行异步并发处理，在语音识别、推荐生成以及路径规划等工作可以同时进行而不是一个接一个地做，这样可以极大地提高整个系统效率。

3.4 加强数据安全与隐私保护

数据安全、隐私保护是做好新能源场站安全运行的保障，也是做好导览机器人的基础。华电河北新能源下属的风光电站存在无线传输风险高、敏感数据易被截获、设备分散难统一管理等情况，因此要创建起由数据采集到存储的全部环节纵深防护体系。按照电力监控系统“安全分区、网络专用、横向隔离、纵向认证”的十六字原则，导览机器人采集到的运维指令、设备关注偏好、场站运行数据等，必须经过正向隔离装置从生产控制区单向传输到管理信息区，再经过国密算法加密后上送到云平台，保证生产控制区外的攻击指令不能进入内网。根据 GB/T 45502-2025 中服务机器人信息安全通用要求的规定，对机器人身份认证、访问控制、USB 外设接口进行白名单控制，并采用

工业防火墙、审计系统对病毒查杀、日志保存等操作进行管控。就大语言模型推荐系统而言,对于可能会遭遇的重建攻击(约65%的用户交互物品可以被恢复),可以采用联邦学习的方式,在场站本地保存用户的交互行为数据,只上传加密后的模型梯度参数,防止原始数据泄露;检索增强生成(RAG)架构依靠外部知识库检索来产生推荐,不需要直接存储备用用户行为,有利于创建更为安全的推荐系统。目前河北华电冀北新能源对下属的19个风光电场已经完成了等保测评和安全防护评估工作,并部署了恶意代码防护系统、网络安全就地监视终端、堡垒机等设备,为导览机器人合规接入做好了良好的准备。

3.5 推进 AI 大模型与多模态技术融合

多模态融合是提高导览机器人个性化推荐智能化的有效途径,用户的参观感受包括视觉、听觉、触觉等各个方面,单凭文字或者声音交流无法完全了解观众需求及意见,而基于 AI 大模型及多模态的技术可以进行文本、图片、音频、视频等多种类型的数据理解和生成,利用多模态推荐方式加入文本、图片等形式增强物品描述,大幅优化推荐效果,由于大语言模型拥有广泛的知识以及强大的逻辑思维能力,在推荐方面有广阔的应用前景^[4]。导览机器人能够利用计算机视觉识别人的目光以及人脸表情,了解观众对于当前所展示作品的关注度,从而改变讲解内容的难度以及速度;同时也可以借助语音情绪分析来及时察觉观众的情绪并做出相应反应。而多模态大模型的应用也

会让导览机器人拥有图像或者文字生成以及问答等更多功能上的提升,给观众带来更好的参观感受。

4 结语

AI 大模型给导览机器人个性化推荐带来很大的进步,但是它在实际使用过程中也存在着数据获取不准、推荐个性化不足、实时响应慢和数据安全风险等状况。本文就华电河北新能源场站场景给出完善的用户画像、改进推荐算法、提升实时交互、加强数据安全、推进多模态融合等策略。经过以上优化之后,导览机器人可以更好地理解运维人员的需求,给运维人员提供准确、安全的智能服务,助力新能源场站智慧化运行。

[参考文献]

- [1]李婷.具身智能机器人导览员“历小博”上岗[N].文汇报,2026-1-7(2).
- [2]贾淑琰,张文希,张立巍.民革广州大学党员之家导览机器人的创新设计[J].丝网印刷,2025(18):133-135.
- [3]徐萨.智能导览机器人问答系统的研究与实现[D].北京:北京邮电大学,2023.
- [4]梅术龙,朱林峰,潘小芳,等.智慧导览机器人的研究与应用[J].新型工业化,2021,11(11):90-93.

作者简介:赵玉涛(1990—),男,河北石家庄人,工程师,华北电力大学科技学院自动化专业毕业,现就职于华电河北新能源有限公司,从事新能源发电企业集控中心生产管理工作。