

2026 年度陕西省科学技术进步奖公示信息

项目名称		智能网联系统可信安全防护关键技术及应用		
提名者		中共陕西省委军民融合发展委员会办公室		
提名意见				
当前智能网联系统快速发展，广泛应用于智能网联汽车、新型电力系统、工业互联网等关键领域，其中的模型安全、网络安全、终端安全已成为产业升级的核心瓶颈，亟需自主可控的安全解决方案。陕西省是我国重要的能源化工基地和汽车产业基地，国家电网陕西省电力公司承担着全省电力供应与新型电力系统建设的核心任务，陕汽等龙头企业正加速布局智能网联汽车产业，智能网联系统的安全可控直接关系到本省能源安全与支柱产业的核心竞争力。该项目紧密围绕陕西省新型电力系统建设和智能网联汽车千亿级产业集群发展需求，聚焦智能网联系统模型安全、网络安全与终端安全展开研究，突破模型可信训练、流量可信利用以及终端可信评估等核心技术。项目主要发明点如下： 1. 原始创新：提出分布式模型训练中的投毒检测与鲁棒聚合方法，实现了智能模型的可信训练； 2. 原始创新：提出轻量级网络流量异常检测技术，确保了车联网中网络报文的可信利用； 3. 原始创新：提出智能网联终端的多维可信度评估技术，实现了异常终端的快速识别。 项目已授权发明专利 39 项，制定各类标准 4 项，获软著 10 项，核心指标显著优于国内外同类技术，整体技术成熟度高。成果已规模应用于工信部电子第五研究所、国家电网（含国家电网陕西省电力公司）等核心单位，以及奇瑞汽车、陕汽集团等头部车企，支撑多款量产车型与电网关键组件落地，直接服务于陕西省能源安全与智能网联汽车产业链安全。项目支撑多个国家级平台建设，获日内瓦国际发明展金奖、中国发明协会创新奖一等奖等重要奖项 10 余项，研究成果获得中国网等多家国内外权威媒体报道，经济与社会效应显著。 该项目原创性突出、先进性显著、应用效益巨大、行业贡献重大，成果材料齐全、规范、无知识产权纠纷，人员排序无争议，符合陕西省科学技术奖提名条件，特此提名该项目申报陕西省科学技术进步奖二等奖。				
主要完成人情况				
排名	姓名	技术职称	工作单位	完成单位
1	郭晶	教授	西安电子科技大学	西安电子科技大学
2	戴光	高级工程师	国网陕西省电力有限公司	国网陕西省电力有限公司
3	马菁	教授	长安大学	长安大学
4	刘志全	教授	暨南大学	暨南大学
5	马慧生	正高级工程师	中国电子科技集团公司第十五研究所	中国电子科技集团公司第十五研究所
6	周兵兵	高级工程师	陕西重型汽车有限公司	陕西重型汽车有限公司

7	牛永玺	工程师	中科数测固源科技（安徽）有限公司			中科数测固源科技（安徽）有限公司			
主要完成单位									
排名	单位名称								
1	西安电子科技大学								
2	国网陕西省电力有限公司								
3	长安大学								
4	暨南大学								
5	中国电子科技集团公司第十五研究所								
6	陕西重型汽车有限公司								
7	中科数测固源科技（安徽）有限公司								
主要知识产权和标准规范等目录									
序号	知识产权（标准）类别	知识产权（标准）具体名称	国家（地区）	授权号（标准编号）	授权（标准发布）日期	证书编号（标准批准发布部门）	权利人（标准起草单位）	发明人（标准起草人）	发明专利（标准）有效状态
1	发明专利	一种车载自组网环境下面向内容的信任评估系统及方法	中国	ZL201910735254.0	2021-07-27	4575594	西安电子科技大学	郭晶晶，马建峰，刘志全，杨腾飞，孟倩，侯高攀，张	有效
2	发明专利	一种横向联邦学习系统中拜占庭节点的检测方法	中国	ZL2021 10851735.5	2023-09-19	6341459	西安电子科技大学	郭晶晶，刘玖樽，魏林锋，黄斐然，刘志全	有效
3	发明专利	一种云辅助车联网中隐私保护的声誉更新系统及方法	中国	ZL202311672590.8	2024-07-23	7221888	暨南大学	刘志全，马森婷，万琳，郭晶晶，马勇，冯霞，王晓明	有效

4	论文	ProAdvPromp t: A Two-Stage Journey to Effective Adversarial Prompting for LLMs	中国	/	2025 -04- 24	International Conference on Learning Representatio ns (ICLR)	西安 交通 大学, 国家 电网	Hao Di, Tong He, Haishan Ye, Yinghui Huang, Xiangyu	有效
5	发明 专利	一种联邦学习 中异常节点的 检测方法及系 统	中国	ZL202110020440.3	2022 -10- 04	5497208	西安 电子 科技 大学	郭晶晶, 李海洋, 刘玖樽, 熊良成, 田思怡, 马建峰,	有效
6	论文	Double Stochasticity Gazes Faster: Snap-Shot Decentralized Stochastic Gradient	中国	10.5555/3692070.3692498	2024 -07- 21	International Conference on Machine Learning (PMLR)	西安 交通 大学, 国家 电网	Hao Di, Haishan Ye, Xiangyu Chang, Guang Dai, Ivor	有效
7	发明 专利	一种横向联邦 学习系统用户 节点的激励方 法及系统	中国	ZL2021 10218159.0	2024 -05- 07	6975875	西安 电子 科技 大学	郭晶晶, 熊良成, 马建峰,	有效
8	发明 专利	一种车载网络 异常流量检测 方法、系统、设 备及介质	中国	ZL2025 10280532.3	2025 -11- 04	8437665	西安 电子 科技 大学	郭晶晶, 杜永超, 侯高攀, 许家源, 李晴仪, 赖笑莹,	有效
9	论文	基于模型水印 的联邦学习后 门攻击防御方 法	中国	10.11897/SP.J.1016.2024.00 662	2024 -01- 04	计算机学报	西安 电子 科技 大学	郭晶晶, 刘玖樽, 马勇, 刘 志全, 熊 宇鹏, 苗 可, 李佳	有效
1 0	论文	An incentive mechanism for horizontal federated learning based on principle of compound	中国	10.1016/j.phycom.2023.102 128	2023 -10- 01	Physical Communicati on	西安 电子 科技 大学	Jingjing Guo, Liangchen g Xiong, Jiaxing Li, Jiuzun Liu, Siyi	有效
客观评价									

Witold Pedrycz（波兰科学院外籍院士、加拿大皇家科学院院士、Information Sciences 前主编、IEEE Life Fellow）在 IEEE Communications Surveys & Tutorials 期刊（中科院一区、TOP）上发表的论文“A Survey on Trust Models in Heterogeneous Networks”中正面评价项目组论文“TROVE: A Context-Awareness Trust Model for VANETs Using Reinforcement Learning”，并将其作为车联网信任建模领域的代表性工作（“For example, in network scenarios, context can be channel conditions, networking requirements and location [78], [79].”）；正面评价项目组论文“PPTM: A Privacy-Preserving Trust Management Scheme for Emergency Message Dissemination in Space-Air-Ground-Integrated Vehicular Networks”，并将项目组提出的“隐私保护的信任建模”评价为异构网络信任建模领域最具研究价值的方向之一（“Future Research Directions: Privacy-preserving trust evaluation is a significant research topic, which deserves special efforts. ... For preserving identity privacy, fuzzification of reputation scores and trust thresholds is a common way, but it inevitably incurs false positives [213]. ... It is undeniable that trust plays a crucial role in future HetNets.”）。

中国科学院院士郭世泽等组成专家组对本项目的评价意见认为：该项目成果技术复杂度高，研制难度很大，有重大技术创新，拥有自主知识产权，项目总体达到国内领先、国际先进水平。

《面向智能汽车的自适应车载网络安全保护系统》获日内瓦国际发明展金奖（全球四大发明展），央媒对项目进行了专题报道。②《智能驾驶感知模型鲁棒性增强与对抗性防御系统》获全国人工智能应用场景挑战赛总决赛一等奖（参赛队伍总数 2300+），中央电视台、新华社等对赛事进行了专题报道。③《车联网“云-网-端”融合安全关键技术及产业化》获中国发明协会发明创业奖创新奖一等奖。④《RKEGuardian:自适应跳频技术增强的 RKE 安全通信系统》获 2024 年全国大学生信息安全竞赛一等奖。

项目简介

智能网联系统是支撑我国新质生产力发展、数字基础设施建设的国家战略级底座，它打通终端感知、边缘协同、云端调度，实现海量异构节点互联互通、跨域数据协同流转，是智慧交通、新型电网、工业互联网等国民经济关键领域数字化转型的共同技术载体。陕西省作为国家重要的能源基地和汽车产业基地，一方面，新型电力系统建设中分布式新能源、智能电表、配电终端等海量节点广泛接入，电网智能网联系统的安全防护直接关系到全省能源供应安全；另一方面，陕汽、比亚迪等龙头企业正加速推进智能网联汽车量产落地，车载智能网联系统的安全能力已成为产业竞争的核心制高点。在科技部、基金委等国家部委支持下，项目组面向智能网联系统，在“模型可信训练-流量可信利用-终端可信评估”三个方面取得关键技术创新，构建了智能网联系统可信安全防护体系。主要技术创新如下：

1、隐私保护的分布式学习投毒防护（原始创新）

传统联邦学习投毒防御方案普遍受投毒比例约束，且隐私保护机制与模型精度存在固有矛盾，难以同时满足高鲁棒性与高精度要求；现有隐私窃取防御方案多依赖模型参数可见假设，无法适用于密文域训练场景。在电网负荷预测、车载驾驶行为分析等分布式建模场景中，上述瓶颈尤为突出。针对上述瓶颈，项目组提出密文域下基于挑战-应答的异常模型参数检测方法，通过在密文空间构造随机挑战向量并验证应答一致性，实现了对投毒节点的精准识别；构建了不受投毒比例约束的后门攻击防御方法，基于参数聚类与异常剪枝实现鲁棒聚合；设计了模型隐私泄露审计方案，通过梯度敏感度分析量化隐私泄露风险。在模型参数不可见的前提下实现了模型的可靠训练与推理，使全局模型精度不受攻击者比例的影响。已应用于电网分布式负荷预测与车载协同感知模型训练。

2、轻量化智能网联系统异常网络流量检测（原始创新）

智能网联系统中，车载总线与车云通信链路每秒产生数万条报文，电力通信网与配电自动化系统中同样存在海量实时数据流；传统基于深度包检测（DPI）的异常检测方案计算复杂度高（秒级），无法满足车载实时控制和电网继电保护的严苛需求；此外，现有轻量化检测模型在高噪声环境（恶意消息比例>50%）下准确率急剧下降。针对大规模流量数据的异常检测精度与实时传输之间的矛盾，项目组提出了基于强化学习的流量数据可信度评估方法；设计了轻量化异常流量检测模型。在恶意消息比例超过90%的极端场景下可实现98%的评估准确率，平均单条报文的检测时间仅为0.0108毫秒，远优于SOTA方案的0.9毫秒，可同时满足车载以太网/CAN总线与电力通信网的实时安全防护需求。

3、隐私保护的智能网联终端可靠性评估（原始创新）

智能网联系统中终端节点数量庞大、行为模式高度动态，既包括车载ECU、T-Box等车端终端，也包括智能电表、配电终端、新能源并网逆变器等电网终端；传统基于固定规则的信任评估机制难以适应终端行为的不确定性；现有信任计算方案需收集终端原始行为数据，存在严重隐私泄露风险；且信任更新过程中计算与通信开销随节点数呈指数增长，难以支撑大规模部署。针对智能网联系统中终端行为的不确定性和关键设施参与节点可靠性之间的矛盾，项目组建立了终端节点的多维信任画像模型，融合行为历史、交互反馈、环境上下文等多维度特征；设计了基于复利原理的终端行为激励机制，引导终端持续提供可信服务；提出了保护终端隐私的终端可信度计算与更新方法。在保证终端隐私不泄露的前提下实现了不同行为模式终端的准确评估，与SOTA方案相比，计算与通信复杂度分别降低88.36%和83.88%。

项目取得显著成果：

1、授权发明专利39项，制定各类标准4项，获软著10项，获日内瓦国际发明展金奖2项（央媒对本项目进行了专题报道），全国人工智能应用场景创新挑战赛总决赛一等奖1项。指导学生获2024年全国大学生信息安全竞赛一等奖、2025年“挑战杯”陕西省竞赛一等奖。

2、发表ESI热点论文2篇、高被引论文7篇，2篇论文入选IEEE年度100篇最受关注Popular论文（IEEE旗下700万+全领域学术论文中遴选）。获国际权威评价：首个（first）、表现更优（performed better）等。

3、成果已规模应用于陕西重型汽车有限公司、奇瑞汽车等头部车企，支撑多款量产车型与关键组件落地。

4、项目成果有力支撑了西安电子科技大学学科建设，学校2017年排名第一入选国家一流网络安全学院建设示范项目，获评首届网络安全先进集体，连续4年（2023-2026）软科排名全国第1。一大批优秀硕博生入职工信部电子第五研究所等行业领军研究机构以及华为车BU等头部企业。

应用情况
项目研究成果在陕西重型汽车有限公司、中汽智联、奇瑞汽车、中科数测固源科技（安徽）有限公司等单位推广应用，服务于智能网联相关的多个领域。大幅提升了我国智能网联系统安全自主可控水平，社会和经济效益显著。
完成人合作关系说明
郭晶晶与戴光、马菁、马慧生共同参与制定标准《公共基础服务业云边协同技术要求 第二部分：安全协同》。 郭晶晶与刘志全共同获得发明专利《一种车载自组网环境下面向内容的信任评估系统及方法》授权，共同发表学术论文《TROVE: A Context Awareness Trust Model for VANETs Using Reinforcement Learning》。 郭晶晶与牛永玺共同出版专著《网络通信协议模糊测试与漏洞挖掘技术》。 马菁与周兵兵共同参与陕汽集团产业项目技术攻关。