张镇勇

手机：132-9188-5709　　**E-mail：**zhangzy@gzu.edu.cn
地址：贵州省贵阳市花溪区贵州大学东校区博学楼 513　**邮编：**550025
出生年月：1991 年 3 月　**民族：**汉　**政治面貌：**中共党员

工作经历

2021.07-至今	**贵州大学**	计算机科学与技术学院	信息安全	**特聘教授**
2020.07-2021.06	**浙江大学**	控制科学与工程学院	网络空间安全	**博士后**
	合作导师：程鹏（教育部长江学者）			

教育背景

2018.10-2019.09	**新加坡科技设计大学**	信息系统科技与设计学院	电力系统安全	**访问学者**
2015.09-2020.06	**浙江大学（保送）**	控制科学与工程学院	控制科学与工程	**博士**
	孙优贤院士课题组、无线传感网络与控制研究组			
	导师：沈学民（外籍院士）、陈积明（教育部长江学者）、程鹏（教育部长江学者）			
2011.09-2015.06	**中南大学**	自动化学院	自动化	**本科**

研究方向

- 信息物理系统安全、人工智能安全、密态计算

项目经历

● 2022.1-2023.1	工业控制技术国家重点实验室开放课题	主持
● 2022.4-2025.3	贵州省基础研究计划（自然科学）一般项目	主持
● 2022.1-2024.9	贵州大学自然科学专项（特岗）科研基金项目	主持
● 2021.9-2024.9	贵州大学青年教师国家自然科学基金培育项目	主持
● 2022.6-2023.6	上海市大数据管理系统工程研究中心开放基金课题	主持
● 2018.07-2021.12	国家重点研发项目子课题：工控系统安全主动防御机制及体系研究	主参
● 2016.9-2019.6	国家重点研发项目子课题：可信增强的主动防御技术	主参
● 2021.12-2024.11	国家重点研发项目子课题: 全流程可追溯的数据滥用监管技术	主参
● 2022.1-2025.12	国家自然科学基金委员会, 联合基金项目	主参
● 2021.1-2024.12	国家自然科学基金委员会, 面上项目	主参
● 2020.1-2023.12	国家自然科学基金委员会, 面上项目	主参
● 2019.1-2023.12	国家自然科学基金委员会, 重点项目	主参

荣誉奖励

- 2020 年　浙江大学优秀毕业生，优秀研究生，国家奖学金
- 2018 年　Journal of the Franklin Institute 期刊审稿杰出贡献奖（前 10%）
- 2017 年　Pervasive and Mobile Computing 期刊审稿杰出贡献奖

海外交流

- 2018 年　葡萄牙波尔图 ACM/IEEE 国际会议 CPS week,
- 2018 年　新加坡 iTrust 信息物理系统安全实验室，合作交流
- 2017 年　荷兰代尔夫特 ACM 国际会议 Embedded Networked Sensor Systems (Sensys’17)
- 2016 年　奥地利维也纳微软全球室内定位大赛，团队核心成员
- 2018.10-2019.02　新加坡科技设计大学访问学者
- 2019.02-2019.08　南洋理工大学访问学者

社会工作

- 担任审稿人：控制领域汇刊 TAC，电力系统领域汇刊 TPS、TSG，信息领域汇刊 TII、TVT ACM TECS, IEEE Wireless Networks, IEEE TCNS, INFOCOM, ACC, 自动化学报，VTC, Journal of Modern Power Systems and Clean Energy, IEEE TGCN, IEEE Consumer Electronics Magazine, ASCC,IEEE

TNSE, 控制工程, IEEE IOT-J

- TPC member：iSCI 2022, Globecom 2021/2022, ASCC 2022
- 担任主席: ASCC 2022 special session chair, SmartGridComm 2022 workshop chair
- 担任编委：Frontiers In Communications And Networks，Computer Networks and Communications
- 中国自动化学会青工委委员
- 贵州省高等学校密码学与区块链技术重点实验室 副主任
- CCF YOCSEF (杭州) 特邀讲者
- 中国计算机大会 CNCC 2022 技术论坛“护卫国之重器——探索工业控制系统安全防护新路径”负责人

学术成果

收录论文：

- **Zhenyong Zhang,** Ruilong Deng, David K. Y. Yau, Peng Cheng, Jiming Chen. “Analysis of Moving Target Defense Against False Data Injection Attacks on Power Grid”. *IEEE Transactions on Information Forensics & Security*, vol.15, no. 1, pp. 2320-2335, Feb. 2020. CCF A 类，中科院 1 区, JCR 1 区, IF: 7.231 (top)
- **Zhenyong Zhang,** Mingyang Sun, Ruilong Deng, Chongqing Kang, and Mo-Yuen Chow. “Physics-Constrained Robustness Evaluation of Intelligent Security Assessment for Power Systems”. *IEEE Transactions on Power Systems*, DOI: 10.1109/TPWRS.2022.3169139, to appear. IF: 7.236，中科院 1 区
- **Zhenyong Zhang,** Shibo He, Yuanchao Shu, Zhiguo Shi. “A Self-Evolving WiFi-based Indoor Navigation System Using Smartphones”. *IEEE Transactions on Mobile Computing,* vol. 19, no. 8, pp. 1760-1774, Aug. 2020. CCF A 类, 中科院 2 区, JCR 1 区，IF: 6.075
- **Zhenyong Zhang,** Ruilong Deng, David K. Y. Yau, Peng Cheng. “Zero-Parameter-Information Data Integrity Attacks and Countermeasures in IoT-based Smart Grid”. *IEEE Internet of Things Journal,* vol. 8, no. 8, pp. 6608-6623, Apr. 2021. 中科院 1 区, JCR 1 区，IF: 10.238 (top)
- **Zhenyong Zhang,** Junfeng Wu, Peng Cheng, Jiming Chen. “Secure State Estimation using Hybrid Homomorphic Encryption Scheme”. *IEEE Transactions on Control Systems Technology*, vol. 29, no. 4, pp. 1704-1720, July 2021. JCR 1 区，中科院 2 区，IF: 5.418
- **Zhenyong Zhang,** Ruilong Deng, Peng Cheng, Moyuen Chow. “Strategic Protection against FDI Attacks with Moving Target Defense in Power Grids”. *IEEE Transactions on Control of Network Systems,* vol. 9, no. 1, pp. 245-256, March 2022. DOI: 10.1109/TCNS.2021.3100411, 中科院 3 区, JCR 1 区，IF: 4.347
- **Zhenyong Zhang,** Ruilong Deng, Peng Cheng, Qiang Wei. “On Feasibility of Coordinated Time-Delay and False Data Injection Attacks on Cyber-Physical Systems”. *IEEE Internet of Things Journal,* vol. 9, no. 11, pp. 8720-8736, June 2022. DOI: 10.1109/JIOT.2021.3118065,中科院 1 区, JCR 1 区，IF: 10.238
- **Zhenyong Zhang,** Youliang Tian, Ruilong Deng, Jianfeng Ma. “A Double-Benefit Moving Target Defense Against Cyber-Physical Attacks in Smart Grid”. *IEEE Internet of Things Journal,* 接收，2022.03. DOI: 10.1109/JIOT.2022.3161790,中科院 1 区, JCR 1 区，IF: 10.238
- **Zhenyong Zhang,** Ruilong Deng, David K. Y. Yau, Peng Cheng, Jiming Chen. “On Hiddenness of Moving Target Defense against False Data Injection Attacks on Power Grid”. *ACM Transactions on Cyber-physical Systems*, vol. 4, no. 3, article 25, Feb. 2020. CPS 领域顶刊，接受率＜10% (引用排名前 25%)
- **Zhenyong Zhang**, David K. Y. Yau. “CoRE: Constrained Robustness Evaluation of Machine Learning-based Stability Assessment for Power Systems”. IEEE/CAA Journal of Automatica Sinica, to appear. 中科院 1 区
- **Zhenyong Zhang**, Yan Qin, Jingpei Wang, Hui Li, and Ruilong Deng, “Detecting the One-shot Dummy Attack on the Power Industrial Control Processes with An Unsupervised Data-Driven Approach”. IEEE/CAA Journal of Automatica Sinica, to appear. 中科院 1 区
- **Zhenyong Zhang**, Ruilong Deng, “Impact Analysis of Moving Target Defense on the Frequency Stability in Smart Grid”. IEEE/CAA Journal of Automatica Sinica, to appear. 中科院 1 区

- Shisheng Fu, **Zhenyong Zhang(通讯作者)**, Yang Jiang, Jing Chen, Xiaoxiao Peng, Weiguo Zhao. “An Automatic RF-EMF Radiated Immunity Test System for Electricity Meters in Power Monitoring Sensor Network”. *Ad Hoc & Sensor Wireless Networks*, 已接收, Aug. 2021.中科院4区，JCR 2区，IF:1.013
- Jingpei Wang, Mufeng Wang, **Zhenyong Zhang (通讯作者)**, Hengye Zhu. “Towards A Trust Evaluation Framework against Malicious Behaviors of Industrial IoT”. *IEEE Internet of Things Journal,* DOI: 10.1109/JIOT.2022.3179428, to appear. 中科院1区, JCR 1区，IF: 10.238
- **Zhenyong Zhang,** Junfeng Wu, David K. Y. Yau, Peng Cheng, Jiming Chen. “Secure Kalman Filter State Estimation by Partially Homomorphic Encryption”. *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, 2018. EI
- **Zhenyong Zhang,** Ruilong Deng, David K. Y. Yau, Peng Cheng, Jiming Chen. “On Effectiveness of Detecting FDI Attacks on Power Grid using Moving Target Defense”. *IEEE-PES International Conference on Innovative Smart Grid Technologies (ISGT NA)*, pp.1-5, Feb. 2019. EI
- **Zhenyong Zhang,** Ruilong Deng, David K. Y. Yau, Peng Cheng, Jiming Chen. “Zero-Parameter-Information FDI Attacks Against Power System State Estimation”. *IEEE America Control Conference (ACC),* July 2020. (顶级会议)
- **Zhenyong Zhang,** Xin Che, Xuguo Jiao, Wanke Yu, Liang Wan. “Quadratic Optimization Using Additive Homomorphic Encryption in CPS”. *Asian Control Conference (ASCC),* pp. 1995-2000, June 2022.
- Zhuoying Shi, **Zhenyong Zhang,** Yuanchao Shu, Shibo He, Jiming Chen. “Indoor Navigation Leveraging Gradient WiFi Signals”. *ACM International Conference on Embeded Networked Sensor Systems (Sensys)*, 2017. CCF B类，EI
- Rongkuan Ma, Peng Cheng, **Zhenyong Zhang,** Wenwen Liu, Qingxian Wang, Qiang Wei. “Stealthy Attack against Redundant Controller Architecture of Industrial Cyber-Physical System”. *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9783-9793, 2019. 中科院1区, JCR 1区, IF: 9.936
- Ke Liu, Mufeng Wang, Rongkuan Ma, **Zhenyong Zhang**, Qiang Wei. “Detection and Localization of Cyber Attacks on Water Treatment System: An Entropy-Based Approach”. *Frontiers of Information Technology & Electronic Engineering*, DOI: http://doi.org/10.1631/FITEE.2000546.已接收. 中科院3区，JCR 2区，IF: 1.604
- Mengxiang Liu, Zheyuang Cheng, **Zhenyong Zhang**, Mingyang Sun, Ruilong Deng, Peng Cheng, Mo-Yuen Chow. “A Multi-Agent System Based Hierarchical Control Framework for Microgrids”. *The IEEE Power & Energy Society General Meeting 2021,* 已接收. DOI: 10.1109/PESGM46819.2021.9638070
- Mengxiang Liu, Chengcheng Zhao, **Zhenyong Zhang**, Ruilong Deng, Peng Cheng. “Analysis of Moving Target Defense in Unbalanced and Multiphase Distribution Systems Considering Voltage Stability”. *The SmartGridComm 2021,* 已接收. DOI: 10.1109/SmartGridComm51999.2021.9632320
- Mengxiang Liu, Chengcheng Zhao, **Zhenyong Zhang**, Ruilong Deng, Peng Cheng, Jiming Chen. “Converter-based Moving Target Defense Against Deception Attacks in DC Microgrids”. *IEEE Transactions on Smart Grid*, Accepted, Early Access, 2021. DOI: 10.1109/TSG.2021.3129195, JCR 1区，中科院1区，IF: 8.96
- Mengxiang Liu, Chengcheng Zhao, **Zhenyong Zhang**, Ruilong Deng. “Explicit Analysis on Effectiveness and Hiddenness of Moving Target Defense in AC Power Systems”. *IEEE Transactions on Power Systems*, DOI: 10.1109/TPWRS.2022.3152801, to appear.
- Lanting Zeng, Mingyang Sun, Xu Wan, **Zhenyong Zhang**, Ruilong Deng, Yan Xu. “Physics-Constrained Vulnerability Assessment of Deep Reinforcement Learning-based SCOPF”. *IEEE Transactions on Power Systems*, DOI: 10.1109/TPWRS.2022.3192558, to appear.
- Ke Liu, Jingyi Wang, Qiang Wei, **Zhenyong Zhang**, Jun Sun, Rongkuan Ma, Ruilong Deng. “HRPDF: A Software-Based Heterogeneous Redundant Proactive Defense Framework for Programmable Logic Controller”. *Journal of Computer Science and Technology*, vol. 36, no. 6, pp. 1307-1324, Nov. 2021. JCR 2区，中科院2

区, IF：1.571

- Mengzhi Wang, Peng Cheng, **Zhenyong Zhang**, Mufeng Wang, Jiming Chen. “Periodic Event-triggered MPC for Continuous-time Nonlinear Systems with Bounded Disturbance”. *IEEE Transactions on Automatic Control*, Accepted, 2021. JCR 1 区，中科院 2 区，IF: 5.792
- 彭莎，孙铭阳，**张镇勇**，邓瑞龙，程鹏，“机器学习在电力信息物理系统网络安全中的应用”．*电力系统自动化，*接收，中国科技期刊卓越行动计划梯队期刊，EI 核心期刊。北大核心 EICSCD :1-16[2022-01-13].http://kns.cnki.net/kcms/detail/32.1180.TP.20211224.2018.012.html.
- Xuguo Jiao, Xiaowen Zhou, Qinmin Yang, **Zhenyong Zhang**, Wenfeng Liu, Jingbo Zhao. “An Improved Optimal Torque Control Based on Estimated Wind Speed for Wind Turbines”. *Asian Control Conference (ASCC),* June 2022.
- Ze Yang, **Zhenyong Zhang**, Youliang Tian. “Experimental Validation of Encrypted Quadratic Optimization Implemented on Raspberry Pi”. *Asian Control Conference (ASCC),* June 2022.

发明专利：

- **张镇勇**，程鹏，潘骏，陈积明等. 基于混合同态加密的错误数据注入攻击防御方法. 专利号：ZL201910917532.4, 授权日：2021.01.01, 授权公告号：CN110545289B

编撰论著：

- 程鹏，**张镇勇**. 冶金工控系统主动防御技术体系白皮书. 网址：http://nesc.zju.edu.cn/#/res/whitebook，入选工业安全产业联盟“2021 年度国内工业控制系统网络安全最受关注榜单”