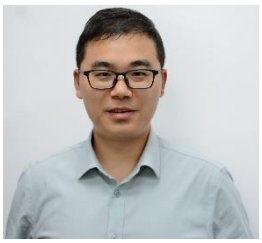
Zhenyong Zhang
Professor, School of Computer Science and Technology
Vice director, Department of Information Security
Guizhou University, Guiyang, China
Building Boxue, Room 513
E-mail: zyzhangnew@gmail.com
Phone: +86 13291885709
Homepage: https://zzyzhuiying.github.io/



Research Interests

Smart grid security
- Attack: False data injection attack, coordinated attack, physical attack
- Defense: Moving target defense, encryption-based control

Industrial control security
- Vulnerability: Exploit vulnerabilities of PLC, ICS network, authentication protocol

Metaverse security
- Attack and authentication enhancement

Mobile computing
- Indoor localization

Education

Central South University, Changsha, Hunan province, China
- Undergraduate,
- Control Science and Engineering, Sept. 2011 — June 2015

Zhejiang University, Hangzhou, Zhejiang Province, China
- Ph.D. Candidate,
- Control Science and Engineering, Sept. 2015 — June 2020
- Advisors: Sherman Shen, Jiming Chen, Peng Cheng

Singapore University of Technology and Design, Singapore, Singapore
- Visiting Ph.D. Student,
- Information Systems Technology and Design, Oct. 2018 — Oct. 2019
- Advisor: David K. Y. Yau

Work experience

Guizhou University, Guiyang, Guizhou Province, China
- Professor,
- July 2021 — Present

Zhejiang University, Hangzhou, Zhejiang Province, China
- Research Fellow,
- June 2020 — July 2021
- Advisor: Peng Cheng

Jornal Papers

1, Ke Zuo, Mingyang Sun, **Zhenyong Zhang**, Peng Cheng, Goran Strabac, and Chongqing Kang. Transferability-Oriented Adversarial Robust Security-Constrained Optimal Power Flow, IEEE Transactions on Smart Grid, Accept.

2, **Zhenyong Zhang**, Kedi Yang, Youliang Tian, Jianfeng Ma. An Anti-disguise Authentication System Using the First Impression of Avatar in Metaverse, IEEE Transactions on Information Forensics & Security, vol. 19, pp. 6393-6408, June 2024.

3, **Zhenyong Zhang**, Mengxiang Liu, Mingyang Sun, Ruilong Deng, Peng Cheng, Dusit Nyato, Moyuen Chow, and Jiming Chen. Vulnerability of Machine Learning Approaches Applied in IoT-based Smart Grid: A Review, IEEE IoT-J, 2024, vol. 11, no. 11, pp. 18951-18975, June 1, 2024.

4, **Zhenyong Zhang**, Bingdong Wang, Mengxiang Liu, Yan Qin, Jingpei Wang, Youliang Tian, and Jianfeng Ma. Limitation of Reactance Perturbation Strategy Against False Data Injection Attacks on IoT-based Smart Grid, IEEE IoT-J, vol. 11, no. 7, pp. 11619-11631, 2023.

5, Jie Meng, Zeyu Yang, **Zhenyong Zhang**, Yangyang Geng, Ruilong Deng, Peng Cheng, Jiming Chen, and Jianying Zhou.SePanner: Analyzing Semantics of Controller Variables in Industrial Control Systems based on Network Traffic, ACSAC 2024.Distinguished Paper Award

6, Lanting Zeng, Mingyang Sun, Xu Wan, **Zhenyong Zhang**, Ruilong Deng, and Yan Xu. Physics-Constrained Vulnerability Assessment of Deep Reinforcement Learning-based SCOPF, IEEE Transactions on Power Systems, vol. 38, no. 3, pp. 2690-2704, May 2023.

7, **Zhenyong Zhang**, Zhibo Yang, David K. Y. Yau, Youliang Tian, and Jianfeng Ma. Data Security of Machine Learning Applied in Low-carbon Smart Grid: A Formal Model for the Physics-constrained Robustness, Volume 347, 1 October 2023, 121405, Applied Energy.

8, Kedi Yang, **Zhenyong Zhang**, Youliang Tian, and Jianfeng Ma. A Secure Authentication Framework to Guarantee the Traceability of Avatars in Metaverse, IEEE Transactions on Information Forensics & Security, vol. 18, pp. 3817-3832, June 2023.

9, **Zhenyong Zhang**, Ruilong Deng, and David K. Y. Yau. Vulnerability of the Load Frequency Control Against the Network Parameter Attack, IEEE Transactions on Smart Grid, vol. 15, no. 1, pp. 921-933, Jan. 2024.

10, **Zhenyong Zhang**, Ke Zuo, Ruilong Deng, Fei Teng, and Mingyang Sun. Cybersecurity Analysis of Data-Driven Power System Stability Assessment, IEEE Internet of Things Journal, vol. 10, no. 17, pp. 15723-15735, Sept. 2023.

11, Sha Peng, **Zhenyong Zhang**, Ruilong Deng, and Peng Cheng. Localizing False Data Injection Attacks in Smart Grid: A Spectrum-based Neural Network Approach, IEEE Transactions on Smart Grid, DOI: 10.1109/TSG.2023.3261970, to appear.

12, Mengzhi Wang, Peng Cheng, **Zhenyong Zhang**, Mufeng Wang, and Jiming Chen. Periodic Event-triggered MPC for Continuous-time Nonlinear Systems with Bounded Disturbances, IEEE Transactions on Automatic Control, to appear.

13, **Zhenyong Zhang**, Ruilong Deng, Youliang Tian, Peng Cheng, and Jianfeng Ma. SPMA: Stealthy Physics-Manipulated Attack and Countermeasures in Cyber-Physical Smart Grid. IEEE Transactions on Information Forensics & Security, vol. 18, pp. 581-596, Dec. 2022.

14, **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, Peng Cheng, and Moyuen Chow. Security Enhancement of Power System State Estimation With An Effective and Low-cost Moving Target Defense. IEEE Transactions on Systems, Man and Cybernetics：Systems, vol. 53, no. 5, pp. 3066-3081, May 2023.

15, **Zhenyong Zhang*** and David K. Y. Yau. CoRE: Constrained Robustness Evaluation of Machine Learning-based Stability Assessment for Power Systems. IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 2, pp. 557–559, Feb. 2023.
16, **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, vol. 10, no. 2, pp. 550–553, Feb. 2023.
17, **Zhenyong Zhang** and Ruilong Deng. Impact Analysis of Moving Target Defense on the Frequency Stability in Smart Grid. IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 1, pp. 275–277, Jan. 2023.
18, Jingpei Wang, Mufeng Wang, **Zhenyong Zhang***, and Hengye Zhu. Towards A Trust Evaluation Framework against Malicious Behaviors of Industrial IoT. IEEE Internet of Things Journal, vol. 9, no. 21, pp. 21260-21277, Nov. 2022.
19, Jingpei Wang, **Zhenyong Zhang**, and Mufeng Wang. A Trust Management Method against Abnormal Behavior of Industrial Control Networks under Active Defense Architecture. IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2549-2572, Sept. 2022.
20, **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, vol. 38, no. 1, pp. 872-884, Jan. 2023.
21, **Zhenyong Zhang**, Youliang Tian, Ruilong Deng, and Jianfeng Ma. A Double-Benefit Moving Target Defense Against Cyber-Physical Attacks in Smart Grid. IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17912-17925, Sept. 2022.
22, Mengxiang Liu, Chengcheng Zhao,**Zhenyong Zhang**, Ruilong Deng, Peng Cheng and Jiming Chen. Converter-based Moving Target Defense Against Deception Attacks in DC Microgrids. IEEE Transactions on Smart Grid, DOI: 10.1109/TSG.2021.3129195, to appear.
23, Mengxiang Liu, Chengcheng Zhao, **Zhenyong Zhang**, and Ruilong Deng. Explicit Analysis on Effectiveness and Hiddenness of Moving Target Defense in AC Power Systems. IEEE Transactions on Power Systems, vol. 37, no. 6, pp. 4732-4746, Nov. 2022.
24, **Zhenyong Zhang**, Ruilong Deng, Peng Cheng, and 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.(中科院一区)
25, **Zhenyong Zhang**, Shibo He, Yuanchao Shu, and 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.
26, **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, Peng Cheng, and 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.
27, **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, Peng Cheng, and 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, pp. 1-29, March. 2020.
28, **Zhenyong Zhang**, Junfeng Wu, Peng Cheng, and 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.
29, **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, and 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.

30, **Zhenyong Zhang**, Ruilong Deng, Peng Cheng, and 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.

31, Shisheng Fu, **Zhenyong Zhang***, Yang Jiang, Jing Chen, Xiaoxiao Peng, and Weiguo Zhao. "An Automatic RF-EMF Radiated Immunity Test System for Electricity Meters in Power Monitoring Sensor Network", Ad Hoc & Sensor Wireless Networks, vol. 50, pp. 173-192, 2021.

32, Rongkuan Ma, Peng Cheng, **Zhenyong Zhang**, Wenwen Liu, Qingxian Wang, and 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, June 2019.

33, Ke Liu, Mufeng Wang, Rongkuan Ma,**Zhenyong Zhang**, and Qiang Wei. "Detection and Localization of Cyber Attacks on Water Treatment System: An Entropy-Based Approach". Frontiers of Information Technology and Electronic Engineering, Available: http://www.jzus.zju.edu.cn/iparticle.php?doi=10.1631/FITEE.2000546.

34, Ke Liu, Jing-Yi Wang, Qiang Wei, **Zhenyong Zhang**, Jun Sun, Rong-Kuan Ma, Rui-Long Deng. HRPDF: A Software-Based Heterogeneous Redundant Proactive Defense Framework for Programmable Logic Controller. Journal of Computer Science and Technology, 36(6): 1307-1324, Nov. 2021.

35, Senjie Zhang, Jinbo Wang, Shan Zhou, Jingpei Wang,**Zhenyong Zhang***, and Ruixue Wang. Identification of Important FPGA Modules Based on Complex Network, Computers, Materials & Continua, vol. 78, no. 1, pp. 1027-1047, Jan. 2024.

36, Ruobing Zuo, Xiaohan Huang, Xuguo Jiao, and **Zhenyong Zhang***. An Improved YOLOv5s-Based Smoke Detection System for Outdoor Parking Lots, Computers, Materials & Continua, accepted, Jan. 2024.

37, Zhibo Yang, Xiaohan Huang, Bingdong Wang, Bin Hu, and **Zhenyong Zhang***. Physics-Constrained Robustness Enhancement for Tree Ensembles Applied in Smart Grid, Computers, Materials & Continua, accepted, July 2024.

38, Xuguo Jiao, Guozhong Wang, Xin Wang, **Zhenyong Zhang***, Yanbing Tian, and Xiwen Fan. Anti-Windup Pitch Angle Control for Wind Turbines Based on Bounded Uncertainty and Disturbance Estimator, Journal of Marine Science and Engineering, vol. 12, no. 473, pp. 1-16, May 2024.

Conference Papers

1, Ze Yang, **Zhenyong Zhang**, Youliang Tian. "Experimental Validation of Encrypted Quadratic Optimization Implemented on Raspberry Pi", 2022 13th Asian Control Conference (ASCC), May 2022.

2, Xuguo Jiao, Xiaowen Zhou, Qinmin Yang, **Zhenyong Zhang**, Wenfeng Liu, and Jingbo Zhao. "An Improved Optimal Torque Control Based on Estimated Wind Speed for Wind Turbines", 2022 13th Asian Control Conference (ASCC), May 2022.

3, **Zhenyong Zhang**, Xin Che, Xuguo Jiao, Wanke Yu, and Liang Wan. "Quadratic Optimization Using Additive Homomorphic Encryption in CPS", 2022 13th Asian Control Conference (ASCC), May 2022.

4, **Zhenyong Zhang**, Xin Che, Xuguo Jiao, and Jingpei Wang. "Enhance Smart Grid Security With

A Coordinated Cyber-Physical Defensive Mechanism", 2022 41st Chinese Control Conference (CCC), July 2022.

5, Bingdong Wang, Junjie Song, Liang Wan, Youliang Tian, Xin Wang, **Zhenyong Zhang**. "Impact Analysis of Moving Target Defense on the Small-Signal Stability in Power Systems", IEEE IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), May 2023.

6, **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, Peng Cheng, and Jiming Chen. "Zero-Parameter-Information FDI Attacks Against Power System State Estimation", IEEE America Control Conference (ACC), July 2020. Invited Paper

7, **Zhenyong Zhang**, Junfeng Wu, David K. Y. Yau, Peng Cheng, and Jiming Chen. "Secure Kalman Filter State Estimation by Partially Homomorphic Encryption", in ACM/IEEE Int. Conf. Cyber-Physical Syst. (ICCPS), Apr. 2018. DOI: 10.1109/ICCPS.2018.00046.

8, **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, Peng Cheng, and Jiming Chen. "On Effectiveness of Detecting FDI Attacks on Power Grid using Moving Target Defense", in IEEE-PES Int. Conf. Innovative Smart Grid Technologies (ISGT NA 2019), Feb. 2019. DOI: 10.1109/ISGT.2019.8791651

9, Zhuoying Shi, **Zhenyong Zhang**, Yuanchao Shu, Shibo He, and Jiming Chen. "Indoor Navigation Leveraging Gradient WiFi Signals", in ACM Int. Conf. Embeded Netw. Sensor Syst. (Sensys), Demo, Nov. 2017. https://doi.org/10.1145/3131672.3136993.

10, Mengxiang Liu, Zheyuang Cheng, **Zhenyong Zhang**, Mingyang Sun, Ruilong Deng, Peng Cheng, and Mo-Yuen Chow. "A Multi-Agent System Based Hierarchical Control Framework for Microgrids". The IEEE Power and Energy Society General Meeting 2021.

11, Mengxiang Liu, Chengcheng Zhao, **Zhenyong Zhang**, Ruilong Deng, Peng Cheng, and Mo-Yuen Chow. "Analysis of Moving Target Defense in Unbalanced and Multiphase Distribution Systems Considering Voltage Stability". IEEE SmartGridComm'21.

Awards

Outstanding Graduate Student Award
Outstanding Student Award
National Encouragement Scholarship
Outstanding Graduate PHD Student
National Scholarship
Outstanding Postgraduate Scholarship
Second price of China graduate contest on application, design and innovative of mobile-terminal
Outstanding reviewer of Pervasive and Mobile Computing
Outstanding reviewer of Journal of the Franklin Institute
Distinguised paper award of ACSAC

Professional Service

Editor of CMC-Computers Materials & Continua, Springer Nature Computer Science, Frontiers In Communications And Networks, Computer Networks and Communications, Mechatronics Technology

Workshop Organizer and Chair of IEEE SmartGridComm, 2022, “Intelligence and Security for Smart Energy Systems”, 6th International Conference of Industrial Cyber-physical Systems, “Cybersecurity of the Future DER-Based Power Grid”, 13th Asia Control Conference, “Security, Privacy, and Optimization of Industrial Intelligent System”

Workshop Organizer of 2022 CCF China National Computer Congress, “ICS security”, 2023 CCF China National Computer Congress, “Smart grid security”

TPC member of ICPADS 2023、iSCI 2022/2024、Globecom 2021/2022 SAC SGC、ASCC 2022

Reviewer of IEEE Transactions on Information Forensics & Security、IEEE Transactions on Power Systems、 IEEE Transactions on Smart Grid、IEEE Transactions on Automatic Control、Automatica、IEEE Transactions on Industrial Informatics、IEEE Transactions on Vehicular Technology、ACM Transactions on Embedded Computing Systems、IEEE Wireless Networks、INFOCOM