Zhenyong Zhang

Contact Information	Guizhou University, Building Boxue, Room 513 Guiyang, China, 550025	+86 13291885709 zyzhangnew@gmail.com

Research Interests

Cyber-Physical System Security, Machine Learning Security, Mobile Computing

Education

Central South University, Changsha, Hunan province, China

Undergraduate,

Control Science and Engineering, Sept. 2011 — June 2015

- Thesis Topic: *Research on multi-robot formation modeling*
- Advisor: Hui Peng, Ph.D

Zhejiang University, Hangzhou, Zhejiang Province, China

Ph.D. Candidate,

Control Science and Engineering, Sept. 2015 — June 2020

- Topic: *Security of Cyber-physical Systems; Indoor Localization and Navigation System Design using Smartphones*
- Advisors: Sherman Shen, Ph.D., Jiming Chen, Ph.D., Peng Cheng, Ph.D.

Singapore University of Technology and Design, Singapore, Singapore

Visiting Ph.D. Student,

Information Systems Technology and Design, Oct. 2018 — Oct. 2019

- Topic: *Security Enhancement of Power Grids with Moving Target Defense*
- Advisor: David K. Y. Yau, Ph.D.

Work experience

Guizhou University, Guiyang, Guizhou Province, China

Professor,

CPS Security, July 2020 — Present

Zhejiang University, Hangzhou, Zhejiang Province, China

Research Fellow,

Cybersecurity, June 2020 — July 2021

- Topic: *Smart grid and machine learning security*
- Advisor: Peng Cheng, Ph.D.

Published J./Conf. Papers

1. **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.
2. **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.
3. **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.

4. **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.

5. **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.

6. **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*, July 2021.
DOI: 10.1109/TCNS.2021.3100411

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. **Zhenyong Zhang**, Ruilong Deng, David K. Y. Yau, Peng Cheng, and Jiming Chen. "Zero-Parameter-Information False Data Injection Attacks in Power Grid". *American Control Conference (ACC)*, July 2020.
DOI: 10.23919/ACC45564.2020.9147943.

10. 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.

11. 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.

12. 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.

13. 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*, accepted.

14. 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*, accepted.

Projects Experience

1. National Natural Science Foundation of China under Grant 61833015, Cyber-Physical Security Theory and Proactive Defense Technology for Smart Grid, Researcher
   - Write part of the project document: research on cyber-physical attack identification methods;
   - Propose an attack detection method based on moving target defense (MTD) strategy, and verify the effectiveness of this method using MATLAB simulations;
   - Analyze the shortcomings of MTD in detecting false data injection attacks, and propose a low cost, high detection performance MTD scheme.
2. National Key Research and Development Program under Grant 2018YFB0803501, Defense Strategy for the Industrial Control Systems, Researcher
   - Write part of the project document: vulnerability identification based on ICS threat model;
   - Analyze the vulnerability exposed in the state estimation of smart grids, and propose a zero-knowledge attack model;
3. National Key Research and Development Program under Grant 2016YFB0800204, Security Enhancement for the Industrial Control Systems, Researcher
   - Propose a secure state estimation algorithm based on hybrid homomorphic encryption scheme;

Awards

Student Awards — Central South University

- Outstanding Graduate Student Award — June 2015
- Outstanding Student Award — May 2014
- National Encouragement Scholarship — May 2013

Student Awards — Zhejiang University

- Outstanding Graduate PHD Student — Dec 2019
- National Scholarship — Dec 2019
- Outstanding Postgraduate Scholarship — Dec 2018/2019
- Second price of China graduate contest on application, design and innovative of mobile-terminal — Oct 2018
- Outstanding reviewer of Pervasive and Mobile Computing — Feb 2017
- Outstanding reviewer of Journal of the Franklin Institute — Aug 2018

Foreign Academic Experience

Visiting

- Centre for Research in Cyber Security-iTrust, Singapore — September 2017

Competition

- Microsoft Indoor Location Competition, Vienna, Austria — April 2016

Presentations

- The ACM International Conference on Embedded Networked Sensor Systems, Delft, Netherlands — Nov 2017
- ACM/IEEE International Conference on Cyber-Physical Systems, Porto (aka Oporto), Portugal — April 2018

Service

Editor of

- Frontiers In Communications And Networks

TPC member of

- Globecom2021 SAC SGC

Reviewer of

- IEEE Transactions on Power Systems
- IEEE Transactions on Smart Grid
- IEEE Transactions on Automatic Control
- IEEE Transactions on Vehicular Technology
- IEEE Transactions on Industrial Informatics
- ACM Transactions on Embedded Computing Systems
- IEEE Wireless Networks
- Elsevier Pervasive and Mobile Computing
- International Journal of Communication Systems
- Pervasive and Mobile Computing
- Journal of the Franklin Institute
- Globecom, SmartGridComm, ACC, INFOCOM