Hui Lin

Mailing address:
2 East Alumni Avenue,
Fascitelli Center for Advanced Engineering 413
Kingston, RI 02881

Phone: 401.874.2643
Email: huilin@uri.edu
Web: https://web.uri.edu/decps/meet/hui-lin/

RESEARCH INTERESTS

- System/network security, intrusion detection, cyber-physical systems, Internet of things, software-defined networking, and cloud computing.
  - Minors in deep learning, formal methods, power system analysis, control theory, and hybrid systems
- Future work: deep/adversarial learning, blockchain, network virtualization, data-driven approach to improve the resilience of broad and dynamic cyber-physical systems

EDUCATION

Ph.D., June 2010 ~ August 2017, Electrical and Computer Engineering
University of Illinois at Urbana-Champaign (UIUC), GPA: 4.0/4.0
Thesis: Detecting Intrusions in Cyber-Physical Infrastructure of Power Systems
Advisor: Prof. Ravishankar K. Iyer and Prof. Zbigniew T. Kalbarczyk

M.S. August 2007 ~ May 2010, Electrical and Computer Engineering
University of Illinois at Chicago (UIC), GPA: 4.0/4.0

B.S. September 2002 ~ June 2006, Electronics and Information Engineering
Huazhong University of Science & Technology, Hubei, China, GPA: 91/100

ACADEMIC APPOINTMENTS

Assistant Professor, August 2020 ~ Present
Electrical, Computer, Biomedical Engineering Department, the University of Rhode Island

Assistant Professor, January 2018 ~ August 2020
Computer Science and Engineering Department, the University of Nevada at Reno

Lecturer, September 2017 ~ December 2017
Computer Science and Engineering Department, the University of Nevada at Reno

Research Assistant, June 2010 ~ August 2017
Coordinated Science Laboratory, the University of Illinois at Urbana-Champaign
Supervisor: Prof. Ravishankar K. Iyer and Prof. Zbigniew T. Kalbarczyk

Mentor for Graduate Intern, May 2016 ~ July 2016
Information Trust Institute, the University of Illinois at Urbana-Champaign

Researcher, June 2015 ~ August 2017

Cyber Resilient Energy Delivery Consortium (CREDC)
Principle Investigator: Prof. David M. Nicol

Researcher, June 2010 ~ August 2015
Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)
Principle Investigator: Prof. William H. Sanders and Prof. Peter W. Sauer

Research Aide, June 2015 ~ August 2015
Energy Division, Argonne National Laboratory
Supervisor: Jianhui Wang

Research Intern, January 2015 ~ March 2015
Advanced Digital Science Center, Singapore
Supervisor: Rui Tan

Research Assistant, June 2007 ~ May 2010
Department of Electrical and Computer Engineering, the University of Illinois at Chicago
Advisor: Prof. Gyungho Lee

Teaching Assistant, August 2007 ~ May 2008
Department of Electrical and Computer Engineering, the University of Illinois at Chicago

RESEARCH FUNDING

Current

"CAREER: PARP: Mislead Physical-Disruption Attacks by Preemptive Anti-Reconnaissance for Power Grids Cyber-Physical Infrastructures"
Amount: $499,996
Duration: 07/01/2022 – 06/30/2027
Investigators: Hui Lin [Single-PI]
Sponsor: National Science Foundation (award number 2144513)

Pending (recommended by NSF Program Director)

"SaTC: CORE: Small: Enabling Programmable In-Network Security for an Attack-Resilience Smart Grid"
Amount: $280,000
Duration: 06/01/2023 – 05/30/2026
Investigators: Hui Lin [PI at URI side]
Sponsor: National Science Foundation

Expired (made significant contribution during PhD)

"Preempting Physical Damage from Control-related Attacks on Smart Grids' Cyber-Physical Infrastructure" (*link*)
Amount: $148,66
Duration: 08/10/2020 – 05/31/2022
Investigators: Hui Lin [Single-PI]
Sponsor: National Science Foundation (award number 2041643)

"Semantic Security Monitoring for Industrial Control Systems" (*link*)
Amount: $898,299
Duration: 06/20/2013 – 05/31/2018
Investigators: Ravishankar K. Iyer, Adam Slagell
My role: contributed the key idea
Sponsor: National Science Foundation (award number 1314891)

PUBLICATIONS

Book Chapters

Hui Lin, "Domain-Specific Security Approaches for Cyber-Physical Systems," in System Dependability and Analytics, Editors: Long Wang, Karthik Pattabiraman, Arjun Athreya, Catello (Lelio) DiMartino, Saurabh Bagchi, Zbigniew Kalbarczyk, Springer, 2022.

Journals & Magazines

Bibek Shrestha, **Hui Lin**, "Data-Centric Edge Computing to Defend Power Grids Against IoT-Based Attacks," *IEEE Computer Special Issues on Cybersecurity for the Smart Grid*, May 2020.

Hui Lin*, Homa Alemzadeh*, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Challenges and Opportunities in the Detection of Safety-Critical Cyberphysical Attacks," in Computer, vol. 53, no. 3, pp. 26-37, March 2020, doi: 10.1109/MC.2019.2915045 (*co-first authors).

Hui Lin, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "RAINCOAT: RAndomization of Network Communication in Power Grid Cyber INfrastructure to Mislead Attackers," in *IEEE Transactions on Smart Grid,* September 14, 2019, doi: 10.1109/TSG.2018.2870362 (impact factor 10.486).

Hui Lin, Chen Chen, Jianhui Wang, Junjian Qi, Dong Jin, Zbigniew Kalbarczyk, Ravishankar K. Iyer, "Self-Healing Attack-Resilient PMU Network for Power System Operation," in *IEEE Transactions on Smart Grid*, May, 2018, doi: 10.1109/TSG.2016.2593021 (impact factor 10.486). (invited to present at INFORMS 2016 Annual Meeting)

Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter W. Sauer, and Ravishankar K. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids," in *IEEE Transactions on Smart Grid*, January, 2018, doi:10.1109/TSG.2016.2547742 (impact factor 10.486).

Hui Lin and Gyungho Lee, "Micro-architecture support for integrity measurement on dynamic instruction trace," *Journal of Information Security* 1, no. 01 (2010): 1.

Gyungho Lee, Yixin Shi, and **Hui Lin**, "Indirect Branch Validation Unit," *Microprocessors and Microsystems* 33, no. 7 (2009): 461-468. (*link*)

Conference Papers

Jennifer Rogers, William Danilczyk, **Hui Lin**, Yan (Lindsay) Sun, "Learning from Future: Prediction-based Data Augmentation to Enhance Power Grids Fault Detection," 54th North American Power Symposium (NAPS), 2022, accepted.

Hui Lin, Yan (Lindsay) Sun, "EleGNN: Electrical-Model-Guided Graph Neural Networks for Power Distribution System State Estimation," The 2022 IEEE Global Communications Conference, accepted.

Hui Lin, Bibek Shrestha, Yih-Chun Hu, "Cyber-Physical Testbed: Case Study to Evaluate Anti-

Reconnaissance Approaches on Power Grids' Cyber-Physical Infrastructures," in *Proceedings of Learning from Authoritative Security Experiment Results (LASER) Workshop*, Feb 24th, 2020.

Hui Lin, Jianing Zhuang, Yih-Chun Hu, Huayu Zhou, "DefRec: Establishing Physical Function Virtualization to Disrupt Reconnaissance of Power Grids' Cyber-Physical Infrastructures," in *Proceedings of Network and Distributed System Security (NDSS) Symposium*, Feb 24th-26th, 2020.

Ye Niu, Abdullah Al-Mamun, **Hui Lin**, Tonglin Li, Yi Zhao, Dongfang Zhao, "Toward Scalable Analysis of Multidimensional Scientific Data: A Case Study of Electrode Arrays," in *Proceedings of the 2018 IEEE International Conference on Big Data (BigData)*, December 10th-13th, 2018.

Hui Lin, Zbigniew Kalbarczyk, and Ravishankar K. Iyer "Impact of Malicious SCADA Commands on Power Grids' Dynamic Responses," in *Proceedings of the 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids* (*SmartGridComm*), October 29th, 2018.

Hui Lin, "SDN-based In-network Honeypot: Preemptively Disrupt and Mislead Attacks in IoT Networks," in *Proceedings of the first International Workshop on Security and Privacy for the Internet-of-Things* (*IoTSec '18*), April 17th, 2018.

Esther Amullen*, **Hui Lin***, Zbigniew Kalbarczyk, and Lee Keel, "Multi-agent System for Detecting False Data Injection Attacks Against the Power Grid," in *Proceedings of the Second Annual Industrial Control System Security Workshop* (*ICSS '16*) (*co-first authors), December 6th, 2016, pp 38-44.

Hui Lin, Xinshu Dong, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk, "Software Defined Networking for Smart Grid Resilience," poster at the *Workshop on Science of Security through Software-Defined Networking* (*SoSSDN*), June 16-17th, 2016. (*link)*

Dong (Kevin) Jin, Jiaqi Yan, Xin Liu, Christopher Hannon, **Hui Lin**, Zbigniew Kalbarczyk, Ravishankar Iyer, Chen Chen, Jianhui Wang, and Cheol Won Lee, "Towards a Secure and Resilient Industrial Control System with Software-Defined Networking," poster at the *Workshop on Science of Security through Software-Defined Networking* (*SoSSDN*), June 16-17th, 2016 (best poster award).

Hui Lin, Homa Alemzadeh, Daniel Chen, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Safety-critical Cyber-physical Attacks: Analysis, Detection, and Mitigation," in *Proceedings of the Symposium and Bootcamp on the Science of Security (HotSos '16),* doi: http://dx.doi.org/10.1145/2898375.2898391. (*link*)

Xinshu Dong, **Hui Lin**, Rui Tan, Ravishankar K. Iyer, and Zbigniew T. Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," in *Proceedings of ACM AsiaCCS Workshop on Cyber-Physical System Security*, April 2015. (*link*)

Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids (Poster)," in *Proceedings of the 7th International Conference on Security of Information and Networks* (*SIN '1*4), September, 2014. (*link*)

Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter Sauer, and Ravishankar K. Iyer, "Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids," in *Proceeding of ACM CCS Smart Energy Grid Security Workshop*, Berlin, Germany, Nov., 2013. (*link*)

Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol," In *Proceeding of 8th Cyber Security & Information Intelligence Research Workshop* (*CSIIRW '12*)*,* Oak Ridge National Lab, Jan., 2013. (Third Place, Best Paper Award). (*link*)

Hui Lin, Md. Sajjad Rahaman, and Masud H Chowdhury, "Microarchitecture Support for Interconnect Power-aware Instruction Permutation," in *Proceeding of The IEEE International Symposium on Circuits and Systems (ISCAS) 2010*. (*link*)

Jing Jin and **Hui Lin**, "License Management Scheme for Learning Resources Delivery in P2P Networks," in the *Proceeding of 2006 International Conference on Parallel & Distributed Processing Techniques & Applications (PDPTA'06)*, June 26~29, 2006, Nevada, USA.

Technical Reports

Xinshu Dong, **Hui Lin**, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," *Coordinated Science Laboratory technical report UILU-ENG-15-2203*, University of Illinois at Urbana-Champaign, February 2015. (*link*)

Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Using a Specification-based Intrusion Detection System to Extend the DNP3 Protocol with Security Functionalities," *Coordinated Science Laboratory technical report UILU-ENG-12-2207*, University of Illinois at Urbana-Champaign, November 2012. (*link*)

AWARDS, HONORS, & CERTIFICATES

Member of Tau Beta Pi - The Engineering Honor Society

Best poster award, Workshop on Science of Security through Software-Defined Networking (SoSSDN)

Student Travel Grant, ACM Conference on Computer and Communications Security (CCS), November 2013

Third Place, Best Paper Award at 8th Cyber Security & Information Intelligence Research Workshop, 2013

The certificate of Neural Networks and Deep Learning, an online non-credit course authorized by deeplearning.ai and offered through Coursera

The certificate of Improving Deep Neural Networks: Hyperparameter tuning, Regularization and

Optimization, an online non-credit course authorized by deeplearning.ai and offered through Coursera

The certificate of Structuring Machine Learning Projects, an online non-credit course authorized by deeplearning.ai and offered through Coursera

The certificate of Convolutional Neural Networks, an online non-credit course authorized by deeplearning.ai and offered through Coursera

TALKS & DEMOS

Hui Lin, "Preempting Physical Damage from Control-Related Attacks on Smart Grids' Cyber-Physical Infrastructure," the fourth biennial NSF Secure and Trustworthy CyberSpace Principal Investigators' Meeting, 2019.

Hui Lin, "Detection and Prevention of Intrusions in Power Systems' Cyber-Physical Infrastructure," invited talks at Link Lab at the University of Virginia, April 10th, 2018.

Hui Lin, "SDN-based In-network Honeypot: Preemptively Disrupt and Mislead Attacks in IoT Networks," in *Proceedings of the first International Workshop on Security and Privacy for the Internet-of-Things* (*IoTSec '18*), April 17th, 2018.

Hui Lin, Ravishankar K. Iyer, Zbigniew Kalbarczyk, "RAINCOAT: Randomization of Network

Connectivity in Industrial COnTrol Systems to Mitigate Cyber-Attacks," *Workshop on Science of Security through Software-Defined Networking* (*SoSSDN*), June 16-17th, 2016 (invited presentation).

Hui Lin, Homa Alemzadeh, Daniel Chen, Zbigniew Kalbarczyk, Ravishankar K. Iyer, "Safety-critical Cyber-physical Attacks: Analysis, Detection, and Mitigation," *Symposium and Bootcamp on the Science of Security (HotSos '16).*

Hui Lin, "Specification-Based IDS for the DNP3 Protocol," 2014 TCIPG Industry Workshop, November 12-13th, 2014 (One of four selected student presentation). (*video recording*, *slides*)

Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Specification-based IDS for the DNP3 Protocol," 2013 TCIPG Industry Workshop, November 2013. (*poster*)

Hui Lin, "Semantic Security Analysis of SCADA Networks to Detect Malicious Control Commands in Power Grids," *ACM CCS Smart Energy Grid Security Workshop*, Berlin, Germany, November 2013.

Hui Lin, "Detection of a Man-in-the-middle Attack in SCADA Network**,**" 2012 TCIPG Industry Workshop, October 2012 (Selected research demo). (*video recording*)

Hui Lin, "Adapting Bro into SCADA: Building a Specification-based Intrusion Detection System for the DNP3 Protocol," *8th Cyber Security & Information Intelligence Research Workshop,* Oak Ridge National Lab, January 2013.

Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer "Adapting Bro into SCADA: Building a Specification-based IDS for the DNP3," 2012 TCIPG Industry Workshop, October 2012. (*poster*)

ACADEMIC SERVICE

Publication Peering Review

- IEEE Transactions on Smart Grid
- Proceedings of the IEEE
- IEEE Access
- Computers & Security (COSE)
- IEEE/ACM Transactions on Networking
- IEEE Internet Computing
- ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS 2019)
- IEEE Control Systems Society Conference (CDC 2018)
- IEEE PES-Letter (2018)
- International Workshop on Communication, Computing, and Networking in Cyber-Physical Systems (CCN-CPS 2016, 2017, 2018)
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012, 2015, 2016, and 2018)
- Network and Distributed System Security Symposium (NDSS 2014)
- IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2015)
- IEEE International Conference on Smart Grid Communication (SmartGridComm 2015 and 2018)
- IEEE Global Communication Conference (Globecom 2015)
- IEEE International on-Line Testing Symposium (IOLTS 2013)
- International Conference on Computer Safety, Reliability & Security (SafeComp 2012)
- Cyber Security and Information Intelligence Research Workshop (CSIIRW 2012)

Grant Peering Review

- 2021 National Science Foundation, Smart and Connected Communities (S&CC)
- 2019-2020 Undergraduate Scholarship Program, Nevada NASA Space Grant Consortium
- Cyber security: Digital Security and Privacy, Dutch Research Council, NWO

TEACHING

- ***Special Topics on Cyber-Physical System Security (I created)***
  The focus of this course is to discuss and understand the fundamental constructions and the emerging challenges unique to today's cyber-physical systems. On top of these understanding, we will explore the possible solutions from the perspectives of systems specification, system modeling, network programming, and formal verification.

- ***Reliability and Security of Computing Systems (I redesigned)***
  Security in computing systems has gained paramount significance as an increasing amount of sensitive and private data is being stored in computers (embedded or desktop or server). Furthermore, many computing systems need to operate reliably and dependably to meet application requirements. The course elaborates essential reliability and security primitives in computing systems and motivate students for considering security and reliability in the design of computing systems.

MEDIA COVERAGE

Nikki Moylan, "Two recently-hired engineering faculty win National Science Foundation awards," April 1st, 2019 (*Link*)

Christine Des Garennes, "NCSA shares $1.6 million cybersecurity grant," The News-Gazette, September 1st, 2013 (*Link*)

INDUSTRIAL EXPERIENCES

Interim Engineering Intern, May 2013 ~ August 2013
The Office of the Chief Scientist, Qualcomm®
Manager: Anand Palanigounder, *Supervisor*: Olivier Benoit
- Researched on the vulnerabilities of the package installation procedure in Android operating system
- Replaced an existing user application with a Trojan

Graduate Intern, May 2011 ~ August 2011
Security and Cryptography Research Lab, Intel®
Manager: David Durham, *Supervisor*: Ravi Sahita
- Exploited a hypervisor based on Intel® Virtual Technology for X86 to monitor user-level processes and prevent them from being compromised by malware or Trojan

RESEARCH EXPERIENCES

Randomize Network Communication in CPSes

- Randomize network connectivity of control devices deployed at remote field sites
  - Increase the unpredictability in control networks
  - Expose attackers when accessing to "off-line" devices
  - Limit information collected by attackers to design attack strategies
- Intelligent spoofing of responses for "off-line" devices
  - Prevent attackers from learning the randomized connectivity
  - Include decoy measurements to mislead attackers
- Implementation
  - Used "Onos" SDN controller to dynamically control connectivity, e.g., allowing/dropping traffic to devices in substations
  - Implemented communication networks with real SDN-enabled hardware switches in Geni testbed (nation-wide network experiment platform)
  - Designed HoneyGrid prototype based on AC state estimations to issue decoy measurements on behalf of "off-line" devices

Detect Intrusions in Cyber-Physical Infrastructure of Power Systems

- Used control theoretic approaches and numeric simulations to evaluate the impact of attacks on power systems' transient and steady state
- Developed first instrusion detection systems (included in Zeek) that fully supports communication protocols used in power systems, e.g., DNP3 and Modbus
  - Can be freely downloaded with Zeek
  - Presented its usage in a demo of man-in-the-middle attacks on SEL RTAC (Real-Time Automation Controller) device
- Extended the proposed IDS with a power flow analysis algorithm to estimate the physical consequence of malicious commands
- Proposed a new power flow analysis algorithm which adapts its parameters, e.g., number of iterations of computations, based on observed network communications
  - Reduce the computation time by fifty percent compared with AC power flow analysis
  - Increase the accuracy by two orders of magnitudes compared with DC power flow analysis

Self-healing Mechanism for PMU Network

- Restored PMU (Phasor Measurement Units) measurements due to isolated or disconnected PDCs (Phasor data concentrators)
- Used an integer linear programming (ILP) model to solve the PMU-reconnection problem
  - Jointly reduce the performance overhead of reconfiguring communication networks and increase the redundancy of measurements
  - Consider the resource constraints in both communication networks and physical infrastructures
  - Proposed a heuristic algorithm to reduce the computation complexity

Multi-agent Communications to Detect False Data Injection Attacks

- Proposed multi-agent communications among substations to share measurements
- Built a virtual grid for each substation based on measurements from its neighbors
  - When no attacks happen, state estimation in the virtual grids is consistent with state estimation in the whole grid
  - False data injection attacks can bypass the state estimation in the whole grid, but fail to bypass the state estimation in the virtual grids

Cyber-Physical Testbed

- Developed a cyber-physical test-bed which simulates both communication network and transmission network of power grids.

- Used PowerWorld's transient analysis toolbox to simulate physical operations of power grids
- Used Mininet to simulate an SDN-enabled communication network
- Simulated the interactions between events occurred in both of these simulation environments

Analyze Attack Incidents on Supercomputing Environment

- Analyzed more than 150 real incidents detected and collected by NCSA (National Center of Supercomputing Association)
  - Understand methods, logics, and habits of attackers that penetrate into systems through stolen credentials

Adapt Computer Architecture to Secure Program's Execution

- Use the information of indirect branch instructions to detect anomalies in programs' executions
  - Extended the branch prediction units in Intel® X86 architecture to profile the information of indirect branch instructions
  - Detected the anomaly based on the deviation from the profile
  - Implemented in Bochs, X86 emulator