Hui Lin (Hugo)

Mailing address:
303 E White St, Apt 4
Champaign, IL, 61820

Phone: 773 495 5156
Email: hlin33@illinois.edu, hugolin615@gmail.com
Web: http://hlin33.web.engr.illinois.edu

RESEARCH INTERESTS

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

EDUCATION

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

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

ACADEMIC APPOINTMENTS

Research Assistant, June 2010 ~ Present
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 2010 ~ August 2015
TCIPG: Trustworthy Cyber Infrastructure for the Power Grid
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

PUBLICATIONS

Journals

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*, July 27th, 2016, doi: 10.1109/TSG.2016.2593021. (invited to present at INFORMS 2016 Annual Meeting) (*link*)

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*, March 28th, 2016, doi:10.1109/TSG.2016.2547742. (*link*)

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

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

Conference Papers

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), to appear.

Hui Lin, Xinshu Dong, Rui Tan, Ravishankar K. Iyer, 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, 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, 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, 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 '14*), September, 2015. (*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, 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.

In Submissions

Hui Lin, Ravishankar K. Iyer, Zbigniew Kalbarczyk, "RAINCOAT: RAndomized Network Communication in Power Grid Cyber INfrastructure to Mislead Cyber Attackers," *the 47th IEEE/IFIP International Conference on Dependable Systems and Networks* (*DSN '17*), in submission.

Abstract: In preparing attacks on power grids, attackers can use periodic data acquisitions performed by control centers. In this paper, we present Raincoat, which randomizes data acquisitions to disrupt and mislead attackers. We transform one data acquisition into multiple rounds. In each round, we dynamically manipulate network flows in the control networks so that randomly selected "online" devices respond with real measurements. Meanwhile, we intelligently spoof measurements for other "offline" devices to mislead attackers into designing ineffective strategies. Based on experiments using large-scale power systems and six real wide area networks, Raincoat is effective against false data injection and control-related attacks with small overhead. The probability of successful attacks can be reduced from 70% to 5%; attacks introduce little damage even if they are executed. When Raincoat is used, the differences of state estimation accuracy is within ±2%, and network latency of data acquisition increases on average by less than 5%.

Hui Lin, Zbigniew Kalbarczyk, and Ravishankar K. Iyer, "Impact of Malicious SCADA Commands on Power Grid Control Performance," in preparation.

Abstract: Our previous work uses steady state of power systems to estimate the consequence of malicious commands. However, the steady-state analysis fails to understand any anomalies happened during the transient period of power systems, during which physical components can experience oscillations. In this paper, we study the impacts of control-related attacks on transient activities. Specifically, we use the electromechanical models of generators to formulate a power system as a linear-time invariant system. We establish the mathematic relationship between control fields included in network communication and power system's underneath control functionality. We use control-theoretic approach to evaluate how attacks perturb system's transient and steady states. The experiments performed on IEEE 14 bus system validate the theoretic findings and reveal

that the proposed approach can help find an attack strategy.

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

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

PROPOSAL EXPERIENCES

"***Semantic Security Monitoring for Industrial Control Systems***"
National Science Foundation under award number 1314891 (PIs: Prof. Ravishankar K. Iyer) (*link*)
- Made a significant contribution

"Detecting Intrusions in Cyber-physical Infrastructure of Power Systems"
Department of Energy, DOE FOA 1441
- Contributed to concept development

"ARMIES: Attack Resilient Microgrid cyberInfrastructure for Energy System Security"
National Science Foundation
- "Pending"
- Contributed to concept development

TALKS & DEMOS

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

Involved in reviewing publications from the following conferences and journals:

- IEEE Transactions on Smart Grid
- Proceedings of the IEEE
- Computers & Security (COSE)
- International Workshop on Communication, Computing, and Networking in Cyber-Physical Systems (CCN-CPS 2016)
- IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012, 2015, and 2016)
- 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)
- 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)

MEDIA COVERAGE

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

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 IDS (included in Bro) that fully supports communication protocols used in power systems, e.g., DNP3 and Modbus
  - Can be freely downloaded with Bro
  - 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 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

Randomize Network Communication in CPSes (on-going)
- 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

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

REFERENCES

Ravishankar K. Iyer
George and Ann Fisher Distinguished Professor of Engineering,
Coordinated Science Lab, University of Illinois at Urbana-Champaign,
225 Coordinated Science Laboratory, 1308 West Main St, Urbana, IL 61801.
Tel: (217) 333-9732; Email: rkiyer@illinois.edu

Peter W. Sauer
W. W. Grainger Chair in Electrical Engineering,
Electrical and Computer Engineering Department,
University of Illinois at Urbana-Champaign,
4046 ECE Building, 306 North Wright Street, Urbana, IL 61801.
Tel: (217) 333-0394; Email: psauer@illinois.edu

Jianhui Wang
Section Lead - Advanced Power Grid Modeling, Center for Energy, Environmental, and Economic

Systems Analysis (CEEESA), Energy Systems Division.
Argonne National Laboratory, 9700 S. Cass Avenue, Bldg. 202, Argonne, IL 60439.
Tel: (630) 252-1474; Email: jianhui.wang@anl.gov
Interfolio Email: send.Wang.C0EB79C886@interfolio.com (please use this email address for confidential reference letter)

Zbigniew T. Kalbarczyk
Research Professor of Electrical and Computer Engineering,
Coordinated Science Lab, University of Illinois at Urbana-Champaign,
267 Coordinated Science Laboratory, 1308 West Main St, Urbana, IL 61801.
Tel: (217) 244-7110; Email: kalbarcz@illinois.edu

William H. Sanders
Electrical and Computer Engineering Department Head
Donald Biggar Willett Professor of Engineering
University of Illinois at Urbana-Champaign,
2090 ECE Building, 306 North Wright Street, Urbana, IL 61801.
Tel: (217) 333-2301; Email: whs@illinois.edu

Alfonso Valdes
Managing Director of Smart Grid Technologies,
Information Trust Institute,
457 Coordinated Science Laboratory, 1308 West Main St, Urbana, IL 61801.
Tel: (217) 244-5147; Email: avaldes@illinois.edu