

# Hoang Hai Nguyen (Frank)

<https://www.hoanghainguyen.com>

Email: [nhh311@gmail.com](mailto:nhh311@gmail.com)

LinkedIn: [nguyen-hoang-hai](#)

Mobile: (217) 751-2846

## EDUCATION

### University of Illinois at Urbana-Champaign (UIUC)

Ph.D., Electrical and Computer Engineering

M.Sc., Electrical and Computer Engineering

Urbana, IL

Dec 2018 - May 2022

Aug 2015 - Dec 2018

### National University of Singapore (NUS)

B.Comp. in Computer Engineering (with Honours), School of Computing

Singapore

Aug 2007 - May 2011

### High School for Gifted Student, Hanoi National University of Education

Specialized in Mathematics

Hanoi, Vietnam

Aug 2004 - May 2007

## WORK & RESEARCH EXPERIENCE

### University of Illinois at Urbana-Champaign (UIUC)

Research Assistant, Information Trust Institute

Urbana, IL

Aug 2015 - Present

Research funded by the National Security Agency's Science of Security project to solve hard problems in security. [network security, Monte Carlo methods, graph theory, probabilistic risk analysis, fault tree analysis, optimization]

- **Security risk assessment:** Developed probabilistic graphical model based on *uncertain graphs* to model information uncertainty in network security. Developed *probabilistic risk assessment* framework to quantify the impacts of cyber-attacks against computer networks. Designed *rare event simulation* techniques based on importance sampling to quantify the risks of low-probability high-impact cyber-security events. [Current project] Study the *dynamic risks* of ongoing cyber-attacks and develop *risk-informed decision framework* for incidence response.
- **Digital twin simulation:** Designed and developed Melody, a *cyber-physical system simulation* tool that synthesizes datasets that are used to train machine learning-based intrusion detection systems.

### Advanced Digital Sciences Center (ADSC)

Software Engineer, Smart Grid group

Singapore

Sept 2011 - May 2015

Research funded by Singapore's Agency for Science, Technology, and Research (A\*STAR) in collaboration with UIUC. [smart grid security, false data injection attack, building energy efficiency, demand response, load disaggregation, wireless sensor networks, compressed sensing]

- **Living lab testbed:** Designed, developed, and deployed *ADSC living lab testbed*, a 100-node heterogeneous wireless sensor network for studying building energy efficiency. Developed a monitoring and management system for the living lab network with automated and centralized control. Built a low-cost, high-sample rate (up to 3.9 kbps), and power-efficient *electricity current sensing platform* based on the Z1 mote and TinyOS operating system.
- **Smart grid security:** Proposed a discrete-time linear regression model to predict the impact of *false data injection* (FDI) attacks against the power grids. Designed an *active learning* method that allows an attacker to infer such a model. Designed algorithms to compute the *optimal FDI attacks*, detect the attack launch time, identify compromised sensor measurements, and monitor the grid's time-to-emergency. Successfully demonstrated the attack on a physical 16-bus power system testbed at the Nanyang Technological University (NTU), Singapore.

### Temasek Laboratories, National University of Singapore

Software Engineer Intern, Antenna group

Singapore

Oct 2010 - Mar 2011

Developed Python-based GUI for configuring the Universal Software Radio Peripheral (USRP) radio devices.

## Miscellaneous

Other research projects completed or participated in at UIUC:

- **ECE598 Dependable AI systems:** Developed rare-event simulation technique for *safety evaluation* of automated driving technology with machine-learning components. Evaluated the simulation technique using scenarios developed from Matlab's Automated Driving Toolbox.
- **CS598 Reliability of cloud-scale systems:** Proposed programmable network-based *resiliency testing* tool for data center networks.
- **Social simulation:** Participated in UIUC's team to compete in DARPA's SocialSim Challenge. Developed agent-based simulation framework for modeling *information propagation* over social networks.

## ★ HONORS & AWARDS

---

**EPRI Research Award, Aug 2019:** A \$75,000 research grant awarded by the Electric Power Research Institute for “*Synthesizing power grid datasets for the assessment of cyber incident detection tools*”.

**RSA Security Scholar, Aug 2018:** Awarded for 3 years by RSA Security (Dell Technologies).

**DSN Student Travel Grant, Jun 2018:** Awarded by the International Conference on Dependable Systems and Networks.

**Siebel Energy Institute Award, Aug 2016:** A \$50,000 research grant awarded for a year of research in “*Data-driven methods to thwart attacks on microgrids*”.

## ⚙ SKILLS

---

**Research topics:** • *Bayesian analysis* (Bayesian belief network & Bayesian inference) • *Monte Carlo methods* (rare event simulation, variance reduction) • *Risk analysis* (uncertainty modeling and quantification, probabilistic risk analysis) • *System reliability* (fault tree, event tree, network reliability, binary decision diagram) • *Applied probability and statistics* (random process, Markov decision process, hidden Markov model, queueing theory, hypothesis testing, dependence modeling with copulas) • *Graph theory* • *Optimization* (global and heuristic optimization) • *Machine learning* (neural networks, multi-armed bandit, regression analysis, reinforcement learning).

**Network security:** Attack graph, cyber kill-chain, lateral movement attack, false-data injection attack, industrial & control system security, incident response.

**Programming languages:** Python, C, nesC, Java, Matlab, SQL, Modbus, HTML, R, Linux Shell Scripting.

**Software tools:** Python’s numpy, scipy, & matplotlib, Emacs, LaTeX, PowerWorld simulator, Matlab Simulink and Automated Driving Toolbox, OpenBUGS, Wireshark, Git.

**Amateur radio:** General Class licence, call sign KD9RIZ.

## 📖 SELECTED PUBLICATIONS

---

**Exploiting monotonicity and symmetry for evaluation of highly dependable systems**, to appear in the 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2022).

**A model-based approach for quantitative decision-making in cybersecurity incident response**, to appear in the Hot Topics in Science of Security, Special Session on Works-in-Progress (HotSoS 2022).

**Estimating loss due to cyber-attack in the presence of uncertainty**, 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020).

**Extensions of network reliability analysis**, 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2019).

**Melody: synthesized datasets for evaluating intrusion detection systems for the smart grid**, 2017 Winter Simulation Conference (WSC 2017).

**An approach to incorporating uncertainty in network security analysis**, 2017 Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp (HotSoS 2017).

**A joint data compression and encryption approach for wireless energy auditing networks**, ACM Transactions on Sensor Networks (TOSN 2017).

**Modeling and mitigating impact of false data injection attacks on automatic generation control**, IEEE Transactions on Information Forensics and Security (TIFS 2017).

**Safety-assured collaborative load management in smart grids**, ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS 2014).

**Energytrack: Sensor-driven energy use analysis system**, Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings (BuildSys 2013).

Rest of the publications (citations=343, h-index=9, i10-index=9) can be found at:

<https://scholar.google.com/citations?user=VMc14jAAAAAJ&hl=en>