# Luyao Niu he/him/his

*Curriculum Vitae*

*Postdoctoral Scholar*
*Network Security Lab*
*University of Washington, Seattle*
*luyaoniu@uw.edu*
*luyaoniu.github.io*
*Google Scholar*


## Professional Experience

My research aims to develop scalable algorithms and methodologies to establish trustworthy autonomy in adversarial environments by encompassing three major areas: (1) safe AI, (2) verification and robust control, and (3) resilience of cyber systems. These solutions use an interplay of methodologies from artificial intelligence, optimization and control, cybersecurity, game theory, formal methods, and mechanism design. Potential application domains of the proposed solutions include robotics, power systems, and smart transportation systems. I was the instructor of EE 241 (Programming for Signal and Information Processing Applications) in Spring 2023 and EE 342 (Signals, Systems, and Data II) in Winter 2024 at UW.

## Education & Training

2022–present **Postdoctoral Scholar**, *Network Security Lab, Electrical and Computer Engineering*, **University of Washington**, Seattle, WA
Advisor: Prof. Radha Poovendran

2016–2022 **Ph.D.**, *Electrical and Computer Engineering*, **Worcester Polytechnic Institute**, Worcester, MA
Advisor: Prof. Andrew Clark

2013–2015 **M.S.**, *Electrical and Computer Engineering*, **Worcester Polytechnic Institute**, Worcester, MA
Advisor: Prof. Kaveh Pahlavan

2009–2013 **B.S.E.**, *Electro-Mechanical Engineering*, **Xidian University**, Xi'an, China

## Awards and Honors

2023 **Outstanding Mentorship Award**
Department of Electrical and Computer Engineering, University of Washington

2022 **Certification of Reproducibility Badge**
ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)

2020 **Best Paper Session**
ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)

2018 **Outstanding Paper Award**
Springer Conference on Decision and Game Theory for Security (GameSec)

## Teaching Experience

Winter 2024 Instructor of EE 342 (Signals, Systems, and Data II), University of Washington. Responsibilities include preparing course materials, giving lectures weekly, and hosting office hours. **Evaluation Rating: 4.5 out of 5**

Spring 2023 Instructor of EE 241 (Programming For Signal And Information Processing Applications), University of Washington. Responsibilities include giving lectures weekly, grading assignments, and hosting office hours. **Evaluation Rating: 4.8 out of 5**

Fall 2020 Teaching assistant of ECE 2010 (Introduction to Electrical and Computer Engineering), Worcester Polytechnic Institute. Responsibilities include leading lab sessions weekly, grading assignments, and maintaining office hours.

## Mentoring Experience

2023–present **Anokhi Mehta**, *undergraduate student*
Dept. of Energy Science and Engineering,
Indian Institute of Technology Bombay

2022–present **Fengqing Jiang**, *doctoral student*
Network Security Lab, Dept. of Electrical and Computer Engineering,
University of Washington, Seattle, WA

2022–present **Zhangchen Xu**, *doctoral student*
Network Security Lab, Dept. of Electrical and Computer Engineering,
University of Washington, Seattle, WA

## Records of Innovation/ Patents

Dec. 9 2022 **Provisional Patent filed with CoMotion at the University of Washington, Seattle**
LDL: A Defense for Label-Based Membership Inference Attacks
A. Rajabi, D. Sahabandu, **L. Niu**, B. Ramasubramanian, R. Poovendran

## DEI Service

Fall 2023 **UW ECE Graduate Applicant Support Program (GASP)**
Provide mentorship and feedback on graduate school applications to underrepresented and marginalized applicants.

## Professional Development

Winter 2024 **MS Admissions Triage Committee**
Department of Electrical and Computer Engineering, UW

Winter 2023 **FERPA 101**
Office of the University Registrar, UW

Winter 2023 **NETI-1 Course Design and Student Engagement**
National Effective Teaching Institute

Winter 2022 **Using Student Evaluations and Feedback to Improve Teaching and Learning**
Center for Teaching and Learning, UW

Fall 2022 **Teaching Workshop on Well-being for Life and Learning: Designing Learning Environments that Support the Whole Student**
Center for Teaching and Learning, UW

Summer 2022 **Pronouns Training Program**
Diversity, Equity, and Inclusion, UW Human Resources

## Publications: Journal Articles

[J8] **L. Niu**, D. Sahabandu, A. Clark, and R. Poovendran, "A hybrid submodular optimization approach to controlled islanding with post-disturbance stability guarantees," *IEEE Transactions on Power Systems*, pp. 1–12, 2023. DOI: 10.1109/TPWRS.2023.3299280.

[J7] A. A. Maruf, **L. Niu**, A. Clark, J. S. Mertoguno, and R. Poovendran, "A timing-based framework for designing resilient cyber-physical systems under safety constraint," *ACM Transactions on Cyber-Physical Systems*, vol. 7, no. 3, 2023. DOI: 10.1145/3594638.

[J6] **L. Niu**, B. Ramasubramanian, A. Clark, and R. Poovendran, "Robust satisfaction of metric interval temporal logic objectives in adversarial environments," *Games*, vol. 14, no. 2, 2023. DOI: 10.3390/g14020030.

[J5] Z. Li, **L. Niu**, and A. Clark, "LQG reference tracking with safety and reachability guarantees under unknown false data injection attacks," *IEEE Transactions on Automatic Control*, vol. 68, no. 2, pp. 1245–1252, 2023. DOI: 10.1109/TAC.2022.3153456.

[J4] **L. Niu** and A. Clark, "A differentially private incentive design for traffic offload to public transportation," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 2, pp. 1–27, 2021. DOI: 10.1145/3430847.

[J3] B. Ramasubramanian, **L. Niu**, A. Clark, L. Bushnell, and R. Poovendran, "Secure control in partially observable environments to satisfy LTL specifications," *IEEE Transactions on Automatic Control*, vol. 66, no. 12, pp. 5665–5679, 2021. DOI: 10.1109/TAC.2020.3039484.

[J2] **L. Niu**, J. Fu, and A. Clark, "Optimal minimum violation control synthesis of cyber-physical systems under attacks," *IEEE Transactions on Automatic Control*, vol. 66, no. 3, pp. 995–1008, 2021. DOI: 10.1109/TAC.2020.2989268.

[J1] **L. Niu** and A. Clark, "Optimal secure control with linear temporal logic constraints," *IEEE Transactions on Automatic Control*, vol. 65, no. 6, pp. 2434–2449, 2020. DOI: 10.1109/TAC.2019.2930039.

## Publications: Peer-Reviewed Conference Publications

*indicates equal contribution, †indicates undergraduate mentee, and ‡indicates graduate mentee

[C41] F. Jiang‡*, Z. Xu‡*, **L.Niu***, Z. Xiang, B. Li, and R. Poovendran, "Artprompt: Ascii art-based jailbreak attacks against aligned llms," in *62nd Annual Meeting of the Association for Computational Linguistics (ACL)*, 2024.

[C40] Z. Xu[‡], F. Jiang[‡], **L.Niu**, J. Jia, B. Y. Lin, and R. Poovendran, "Safedecoding: Defending against jailbreak attacks via safety-aware decoding," in *62nd Annual Meeting of the Association for Computational Linguistics (ACL)*, 2024.

[C39] Z. Xu[‡], F. Jiang[‡], **L.Niu**, J. Jia, B. Li, and R. Poovendran, "ACE: A model poisoning attack on contribution evaluation methods in federated learning," in *USENIX Security*, 2024.

[C38] A. Mehta[†], **L.Niu**, D. Sahabandu, J. Lukuyu, and R. Poovendran, "A principled incentive mechanism to promote economic viability of mini-grids," in *IEEE PES General Meeting*, 2024.

[C37] H. Zhang, **L.Niu**, A. Clark, and R. Poovendran, "Fault tolerant neural control barrier functions for robotic systems under sensor faults and attacks," in *IEEE International Conference on Robotics and Automation (ICRA)*, 2024.

[C36] A. A. Maruf, **L.Niu**, B. Ramasubramanian, A. Clark, and R. Poovendran, "Risk-aware distributed multi-agent reinforcement learning," in *American Control Conference (ACC)*, 2024.

[C35] Z. Xu[‡], F. Jiang[‡], **L.Niu**, J. Jia, B. Li, and R. Poovendran, "Brave: Byzantine-resilient and privacy-preserving peer-to-peer federated learning," in *5th AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI)*, 2024. [Online]. Available: `https://arxiv.org/abs/2401.05562`.

[C34] F. Jiang[‡], Z. Xu[‡], **L.Niu**, B. Wang, J. Jia, B. Li, and R. Poovendran, "Identifying and mitigating vulnerabilities in LLM-integrated applications," in *NeurIPS 2023 Workshop on Instruction Tuning and Instruction Following*, 2023. [Online]. Available: `https://openreview.net/forum?id=V09d7AMh15`.

[C33] J. Jia, Z. Yuan, D. Sahabandu, **L.Niu**, A. Rajabi, R. Bhaskar, B. Li, and R. Poovendran, "FedGame: A game-theoretic defense against backdoor attacks in federated learning," in *Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS)*, 2023.

[C32] A. Rajabi, S. Asokraj, F. Jiang[‡], **L.Niu**, R. Bhaskar, and R. Poovendran, "MDTD: A multi-domain Trojan detector for deep neural networks," in *ACM Conference on Computer and Communications Security (CCS)*, 2023.

[C31] **L.Niu**, A. A. Maruf, J. S. Mertoguno, A. Clark, and R. Poovendran, "A compositional resilience index for computationally efficient safety analysis of interconnected systems," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2023.

[C30] S. Cheng, **L.Niu**, A. Clark, and R. Poovendran, "A submodular energy function approach to controlled islanding with provable stability," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2023.

[C29] **L.Niu**, A. Clark, and R. Poovendran, "Necessary and sufficient conditions for satisfying linear temporal logic constraints using control barrier certificates," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2023.

[C28] A. A. Maruf, **L.Niu**, B. Ramasubramanian, A. Clark, and R. Poovendran, "Learning dissemination strategies for external sources in opinion dynamic models with cognitive biases," in *International Joint Conferences on Artificial Intelligence (IJCAI)*, 2023, pp. 3–11. DOI: `10.24963/ijcai.2023/1`.

[C27] **L.Niu***, A. A. Maruf*, J. S. Mertoguno, A. Clark, and R. Poovendran, "POSTER: A common framework for resilient and safe cyber-physical system design," in *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, ACM, 2023, pp. 1025–1027. DOI: 10.1145/3579856.3592826.

[C26] A. A. Maruf, **L.Niu**, B. Ramasubramanian, A. Clark, and R. Poovendran, "Cognitive bias-aware dissemination strategies for opinion dynamics with external information sources," in *ACM International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, ACM, 2023, pp. 2769–2771.

[C25] A. Rajabi, D. Sahabandu, **L.Niu**, B. Ramasubramanian, and R. Poovendran, "LDL: A defense for label-based membership inference attacks," in *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, ACM, 2023, pp. 95–108. DOI: 10.1145/3579856.3582821.

[C24] **L.Niu***, A. A. Maruf*, J. S. Mertoguno, A. Clark, and R. Poovendran, "An analytical framework for control synthesis of cyber-physical systems with safety guarantee," in *IEEE Conference on Decision and Control (CDC)*, IEEE, pp. 1533–1540. DOI: 10.1109/CDC51059.2022.9993062.

[C23] A. A. Maruf*, **L. Niu***, A. Clark, J. S. Mertoguno, and R. Poovendran, "A compositional approach to safety-critical resilient control for systems with coupled dynamics," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2022, pp. 910–917. DOI: 10.1109/CDC51059.2022.9992810.

[C22] **L. Niu**, Z. Li, and A. Clark, "Abstraction-free control synthesis to satisfy temporal logic constraints under sensor faults and attacks," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2022, pp. 1568–1575. DOI: 10.1109/CDC51059.2022.9992935.

[C21] H. Zhang, S. Cheng, **L. Niu**, and A. Clark, "Barrier certificate based safe control for LiDAR-based systems under sensor faults and attacks," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2022, pp. 2256–2263. DOI: 10.1109/CDC51059.2022.9992432.

[C20] D. Sahabandu*, **L. Niu***, A. Clark, and R. Poovendran, "A hybrid submodular optimization approach to controlled islanding with heterogeneous loads," in *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2022, pp. 252–258. DOI: 10.1109/SmartGridComm52983.2022.9960986.

[C19] D. Sahabandu*, **L. Niu***, A. Clark, and R. Poovendran, "A submodular optimization approach to stable and minimally disruptive controlled islanding in power systems," in *IEEE American Control Conference (ACC)*, IEEE, 2022, pp. 4587–4594. DOI: 10.23919/ACC53348.2022.9867317.

[C18] **L. Niu**, D. Sahabandu, A. Clark, and R. Poovendran, "Verifying safety for resilient cyber-physical systems via reactive software restart," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, ACM, 2022, pp. 104–115. DOI: 10.1109/ICCPS54341.2022.00016, Certification Badge of Reproducibility.

[C17] **L. Niu**, H. Zhang, and A. Clark, "Safety-critical control synthesis for unknown sampled-data systems via control barrier functions," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2021, pp. 6806–6813. DOI: 10.1109/CDC45484.2021.9683019.

[C16] B. Ramasubramanian, **L. Niu**, A. Clark, and R. Poovendran, "Reinforcement learning beyond expectation," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2021, pp. 1528–1535. DOI: 10.1109/CDC45484.2021.9683261.

[C15] D. Sahabandu*, **L. Niu***, A. Clark, and R. Poovendran, "Scalable planning in multi-agent MDPs," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2021, pp. 5932–5939. DOI: 10.1109/CDC45484.2021.9683385.

[C14] **L. Niu**, D. Sahabandu, A. Clark, and R. Poovendran, "A game-theoretic framework for controlled islanding in the presence of adversaries," in *International Conference on Decision and Game Theory for Security (GameSec)*, Springer, 2021, pp. 231–250. DOI: 10.1007/978-3-030-90370-1_13.

[C13] **L. Niu** and A. Clark, "Control barrier functions for abstraction-free control synthesis under temporal logic constraints," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2020, pp. 816–823. DOI: 10.1109/CDC42340.2020.9304255.

[C12] B. Ramasubramanian, **L. Niu**, A. Clark, L. Bushnell, and R. Poovendran, "Privacy-preserving resilience of cyber-physical systems to adversaries," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2020, pp. 3785–3792. DOI: 10.1109/CDC42340.2020.9304080.

[C11] **L. Niu**, B. Ramasubramanian, A. Clark, L. Bushnell, and R. Poovendran, "Control synthesis for cyber-physical systems to satisfy metric interval temporal logic objectives under timing and actuator attacks," in *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, IEEE, 2020, pp. 162–173. DOI: 10.1109/ICCPS48487.2020.00023, Best Paper Session.

[C10] **L. Niu** and A. Clark, "A framework for joint attack detection and control under false data injection," in *International Conference on Decision and Game Theory for Security (GameSec)*, Springer, 2019, pp. 352–363. DOI: 10.1007/978-3-030-32430-8_21.

[C9] B. Ramasubramanian, **L. Niu**, A. Clark, L. Bushnell, and R. Poovendran, "Linear temporal logic satisfaction in adversarial environments using secure control barrier certificates," in *International Conference on Decision and Game Theory for Security (GameSec)*, Springer, 2019, pp. 385–403. DOI: 10.1007/978-3-030-32430-8_23.

[C8] **L. Niu**, Z. Li, and A. Clark, "LQG reference tracking with safety and reachability guarantees under false data injection attacks," in *IEEE American Control Conference (ACC)*, IEEE, 2019, pp. 2950–2957. DOI: 10.23919/ACC.2019.8814821.

[C7] **L. Niu**, J. Fu, and A. Clark, "Minimum violation control synthesis on cyber-physical systems under attacks," in *IEEE Conference on Decision and Control (CDC)*, IEEE, 2018, pp. 262–269. DOI: 10.1109/CDC.2018.8619174.

[C6] **L. Niu** and A. Clark, "A differentially private and truthful incentive mechanism for traffic offload to public transportation," in *International Conference on Decision and Game Theory for Security (GameSec)*, Springer, 2018, pp. 366–385. DOI: 10.1007/978-3-030-01554-1_21, Outstanding Paper Award.

[C5] **L. Niu** and A. Clark, "Secure control under linear temporal logic constraints," in *IEEE American Control Conference (ACC)*, IEEE, 2018, pp. 3544–3551. DOI: 10.23919/ACC.2018.8431595.

[C4] A. Clark and **L. Niu**, "Linear quadratic Gaussian control under false data injection attacks," in *IEEE American Control Conference (ACC)*, IEEE, 2018, pp. 5737–5743. DOI: 10.23919/ACC.2018.8431459.

[C3] **L. Niu**, Y. Guo, H. Li, and M. Pan, "A Nash bargaining approach to emergency demand response in colocation data centers," in *IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2016, pp. 1–6. DOI: 10.1109/GLOCOM.2016.7841520.

[C2] **L. Niu** and Y. Guo, "Enabling reliable data center demand response via aggregation," in *ACM International Conference on Future Energy Systems (e-Energy)*, ACM, 2016, pp. 1–11. DOI: 10.1145/2934328.2934350.

[C1] **L. Niu**, Y. Fan, K. Pahlavan, G. Liu, and Y. Geng, "On the accuracy of Wi-Fi localization using robot and human collected signatures," in *IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, 2016, pp. 375–378. DOI: 10.1109/ICCE.2016.7430654.

## Professional Service – Review Activities

| | |
|---|---|
| IEEE | Transactions on Automatic Control |
| IEEE | Transactions on Control Systems Technology |
| IEEE | Transactions on Information Forensics & Security |
| IEEE | Transactions on Vehicular Technology |
| IEEE | Robotics and Automation Letters |
| IEEE | Control Systems Letters |
| IEEE | Conference on Decision and Control |
| IEEE | Conference on Robotics and Automation |
| IEEE | American Control Conference |
| Elsevier | Automatica |
| Elsevier | Pervasive and Mobile Computing |
| Springer | International Journal of Wireless Information Networks |

## Professional References

**Radha Poovendran**, *Professor*
Electrical and Computer Engineering,
University of Washington, Seattle, WA,
*Contact: rp3@uw.edu*

**Andrew Clark**, *Associate Professor*
Electrical and Systems Engineering,
Washington University in St. Louis, St. Louis, MO,
*Contact: andrewclark@wustl.edu*

**Sukarno Mertoguno**, *Research Professor*
School of Cybersecurity and Privacy,
Georgia Institute of Technology, Atlanta, GA,
*Contact: karno@gatech.edu*

**Bo Li**, *Neubauer Associate Professor*
Computer Science Department and Data Science Institute,
University of Chicago, Chicago, IL,
*Contact: bol@uchicago.edu*