Postdoctoral Scholar
Network Security Lab
University of Washington, Seattle
+1 (508) 831 8983
luyaoniu@uw.edu
luyaoniu.github.io
Google Scholar

Luyao Niu

Curriculum Vitae

Research Interests

My research focuses on developing scalable algorithms with certifiable guarantees to ensure security and resilience of cyber-physical systems in the presence of attacks and faults. These solutions use an interplay of methodologies from machine learning, optimization and control, game theory, and formal methods. Potential application domains of the proposed solutions include power systems and smart transportation systems. My software implementations to guarantee system safety in the presence of faults and attacks have been transitioned to the community through open source code on Github, and awarded with a Badge of Reproducibility through independent third-party certification.

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.**, *Secure Cyber Physical Systems Lab, Electrical and Computer Engineering*, **Worcester Polytechnic Institute**, Worcester, MA
Dissertation Title: *Secure Control for Autonomous Cyber-Physical Systems Under Linear Temporal Logic Constraints*
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

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

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

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

Publications: Journal Articles

[J1] Z. Li, **L. Niu**, and A. Clark, "LQG reference tracking with safety and reachability guarantees under unknown false data injection attacks," *to appear in IEEE Transactions on Automatic Control*, 2022. DOI: 10.1109/TAC.2022.3153456.

[J2] **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.

[J4] **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.

[J5] **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: Articles under Review

[R1] 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*, Under Review at ACM Transactions on Cyber-Physical Systems. Original submission date: Aug. 30, 2022.

Publications: Peer-Reviewed Conference Publications

* indicates equal contribution

[C1] **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, 2022, arXiv preprint arXiv:2204.00514.

[C2] 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, arXiv preprint arXiv:2204.00512.

[C3] **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, arXiv preprint arXiv:2208.10060.

[C4] 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, arXiv preprint arXiv:2208.05944.

[C5] 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.

[C6] 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.

[C7] **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.

[C8] **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.

[C9] 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.

[C10] 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.

[C11] **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.

[C12] **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.

[C13] 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.

[C14] **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.

[C15] **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.

[C16] 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.

[C17] **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.

[C18] **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.

[C19] **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.

[C20] **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.

[C21] 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.

[C22] **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.

[C23] **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.

[C24] **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.

Teaching Experience

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

Professional Service – Review Activities

IEEETransactions on Automatic Control, Elsevier Automatica, IEEETransactions on Control Systems Technology, IEEETransactions on Vehicular Technology, IEEE Robotics and Automation Letters, IEEE Control Systems Letters, Elsevier Pervasive and Mobile Computing, Springer International Journal of Wireless Information Networks, IEEE Access, IEEE Conference on Decision and Control, IEEE American Control Conference