

Kacper Wardega

🏠 kwardega.com ✉️
📱 in kacper-wardega 📍 USA

INTERESTS

multi-agent systems · multi-robot systems · cyber-physical systems · design automation
AI safety · formal methods

EDUCATION

- | | | |
|-----------|--------------------------------------|--|
| 2017–2023 | Ph.D. | BOSTON UNIVERSITY ELECTRICAL & COMPUTER ENGINEERING DEPT.
Computer Engineering
Thesis title: “Securing Multi-Robot Systems with Inter-robot Observations and Accusations”
Dependable Computing Laboratory – Advised by Prof. Wenchao Li |
| 2013–2016 | B.Sc. (cum laude with honors) | THE OHIO STATE UNIVERSITY COLLEGE OF ENGINEERING
Major in Computer Science & Engineering |
| 2013–2016 | B.Sc. (cum laude) | THE OHIO STATE UNIVERSITY COLLEGE OF ARTS AND SCIENCES
Major in Mathematics, Minor in German
Specialization in Theoretical Mathematics |

PUBLICATIONS

- Kacper Wardega**, Max von Hippel, Roberto Tron, Cristina Nita-Rotaru, and Wenchao Li. “Byzantine Resilience at Swarm Scale: A Decentralized Blocklist from Inter-robot Accusations”. In: *The 22nd International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. May 2023 (to appear).
- Kacper Wardega**, Max von Hippel, Roberto Tron, Cristina Nita-Rotaru, and Wenchao Li. “HoLA Robots: Mitigating Plan-Deviation Attacks in Multi-Robot Systems with Co-Observations and Horizon-Limiting Announcements”. In: *The 22nd International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. May 2023 (to appear).
- Kacper Wardega**, Wenchao Li, Hyoseung Kim, Yawen Wu, Zhenge Jia, and Jingtong Hu. “Opportunistic Communication with Latency Guarantees for Intermittently-Powered Devices”. In: *Design, Automation and Test in Europe (DATE)*. Mar. 2022.
- Qi Zhu, Wenchao Li, Hyoseung Kim, Yecheng Xiang, **Kacper Wardega**, Zhilu Wang, Yixuan Wang, Hengyi Liang, Chao Huang, Jiameng Fan, and Hyunjong Choi. “Know the Unknowns: Addressing Disturbances and Uncertainties in Autonomous Systems”. In: *International Conference on Computer Aided Design (ICCAD)*. Nov. 2020.
- Panagiota Kiourti, **Kacper Wardega**, Susmit Jha, and Wenchao Li. “Evaluation of Backdoor Attacks on Deep Reinforcement Learning”. In: *Design Automation Conference (DAC)*. June 2020.
- Kacper Wardega** and Wenchao Li. “Application-Aware Scheduling of Networked Applications over the Low-Power Wireless Bus”. In: *Design, Automation and Test in Europe (DATE)*. Mar. 2020.
- Kacper Wardega**, Roberto Tron, and Wenchao Li. “Resilience of Multi-Robot Systems to Physical Masquerade Attacks”. In: *IEEE Workshop on the Internet of Safe Things (SafeThings)*. May 2019.
- Kacper Wardega**, Roberto Tron, and Wenchao Li. “Masquerade Attack Detection Through Observation Planning for Multi-Robot Systems”. In: *The 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. May 2019.

Chao Huang, **Kacper Wardega**, Wenchao Li, and Qi Zhu. “Exploring Weakly-hard Paradigm for Networked Systems”. In: *The 1st Workshop on Design Automation for CPS and IoT (DESTION)*. Apr. 2019.

WORK EXPERIENCE

Summer 2021	Applied Scientist Intern AMAZON ROBOTICS Conducted research on the performance of fully-automated robotic floors. Project culminated in a whitepaper, all-hands talk, and software artifacts.
-------------	--

HONORS

2021	Graduate Teaching Assistant of the Year Award	BU ECE DEPT.
2019	Travel Grant IEEE S&P 2019	IEEE S&P 2019 AWARD COMMITTEE
2019	Travel Grant CPS-IoTWeek 2019	CPS-IoTWEEK 2019 AWARD COMMITTEE
2017	Hariri Graduate Student Fellowship	BU HARIRI INSTITUTE FOR COMPUTING

CORE GRADUATE COURSEWORK

Fall 2017	EC504: Advanced Data Structures
Fall 2017	EC700: Computer Aided Verification & Synthesis
Spring 2018	EC700: Advanced Computer Systems
Fall 2018	EC505: Stochastic Processes
Fall 2019	EC541: Computer Communication Networks
Spring 2021	EC724: Advanced Optimization Theory & Methods

ACADEMIC SERVICE

Peer Reviewing	Reviewer for Conference Articles <ol style="list-style-type: none"> 1. Design Automation Conference (DAC), 2018, 2019, 2020. 2. Design, Automation and Test in Europe (DATE), 2020, 2021, 2022. 3. Dependable Systems and Networks (DSN), 2021, 2022. 4. International Conference on Embedded Software (EMSOFT), 2018. 5. ACM International Conference on Hybrid Systems: Computation and Control (HSCC), 2020. 6. International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2020, 2023. 7. International Conference On Computer Aided Design (ICCAD), 2018, 2021, 2022. 8. ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2022. 9. Asia and South Pacific Design Automation Conference (ASP-DAC) 2023. 10. IEEE International Conference on Robotics and Automation (ICRA) 2023.
Teaching Assistant	EC330: Applied Algorithms for Engineers FALL 2019, SPRING 2020 Undergraduate course on algorithms. Topics covered include the general concept of algorithms, efficiency and run-time of algorithms, graph algorithms, priority queues, search trees, various approaches to design of algorithms and data structures, together with their applications to numerical and non-numerical problems.

Grading Assistant	EC545: Cyber-Physical Systems	FALL 2019-2022
	Graduate course on building high-assurance systems with real-time and concurrent behaviors. Topics covered include modeling of dynamical behavior and the design, specification, and analysis of CPS.	
Mentoring	RISE Mentor	SUMMER 2018, 2019
	Mentored high school students during six-week summer research internships.	