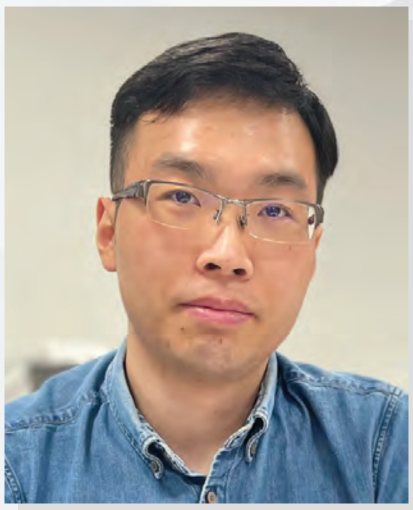
Department of
Systems Engineering
香港城市大學
City University of Hong Kong

Towards Agent-Based Autonomous Security and Resilience in Cyber-Physical-Human Networks



Mr Tao LI
PhD candidate,
Electrical Engineering,
New York University (NYU), USA

29 November 2024 (Fri) | 10:30 am

Seminar Link: https://cityu.zoom.us/j/82566382018

Abstract

Security of cyber-physical-human network (CPHN) systems, such as 5G/6G communication networks, vehicular networks, and the Internet of Things, has become increasingly critical nowadays. Traditional security mechanisms rely primarily on manual operations, which can be slow, expensive, and ineffective in the face of the dynamic landscape of adversarial threats. This problem will only be exacerbated as attackers leverage artificial intelligence (AI) to automate their workflows. As a countermeasure, safeguarding critical network systems also calls for autonomous defensive operations that delegate security decisions to AI agents. This talk presents our agentic framework for autonomous attack detection and response based on reinforcement learning (RL) and large language models (LLM). To address conventional RL's reactive nature, we propose a new RL paradigm, conjectural online RL (coRL), to equip the security agent with predictive power when dealing with the agent's epistemic uncertainty over the attacker's presence and actions. The intuition of coRL is to endogenize the epistemic uncertainty as part of the RL process: the agent maintains an internal world model as a conjecture of the uncertainty, and the learned conjecture produces valid predictions consistent with environment feedback induced by epistemic uncertainty. To mitigate the RL agent's reliance on stylized modeling and textual data pre-processing, we incorporate LLMs into the agentic framework to deliver end-to-end autonomous cyber operations. We finally conclude the talk by discussing the path ahead to building fully autonomous security agents.

About the Speaker

Tao Li is a Ph.D. candidate in Electrical Engineering at New York University (NYU), affiliating with the NYU Center for Cybersecurity. He received his B.S. in mathematics from Xiamen University in 2018. His research focuses on game theory and multi-agent learning theory, which advances novel methodologies and frameworks on predictive reinforcement learning, non-equilibrium analysis, and meta-learning control for secure and resilient cyber-physical-human system design, defense, and management. His continued enthusiasm and efforts have won him the Dante Youla Award for research excellence at NYU. The IEEE Technical Committee on Cognitive Networks has recently recognized him as a rising star in AI and machine learning in security. His research led to more than 20 publications in control, robotics, and security conferences, such as ICRA, CDC, and INFOCOM, as well as journals, including IEEE TIFS, TSPN, TITS, and TRC.

Enquiry: 3442 8422 | All are welcome

Seminar 2024-2025, SYE11