Announcement of New Graduate Research Assistantship Position for CS and ECE PhD or MS (Thesis) Students

Topic: Secure Distributed Protocols for Autonomous Systems

Saurabh Bagchi
School of Electrical and Computer Engineering
Department of Computer Science (By Courtesy)
Purdue University
Contact: sbagchi@purdue.edu

Posted: August 19, 2020

We are looking for multiple Graduate Research Assistants on a newly funded project from the **Army Research Lab (ARL)** on secure distributed protocols for autonomous systems. The project involves a total of 5 faculty members, spread across Purdue and Princeton. The project is open to a PhD student in ECE or CS, in the 1st or 2nd year of his/her study. We may also hire an exceptional Masters (thesis) student in ECE or CS in the student's 1st semester. The positions will be filled on a rolling basis.

Characteristics of applicants: Some expertise in distributed system security, fundamental machine learning building blocks. Good system building skills and experience with any ML framework (PyTorch, MXNet, TensorFlow, etc.).

Project team: The project PI is Prof. Saurabh Bagchi and co-PIs are Profs. David Inouye, Mung Chiang, Somali Chaterji, and Prateek Mittal (Princeton). When fully staffed, the project team will have 5 Graduate Researchers and 1 Research Scientist along with several undergraduate research assistants to work closely with the graduate researchers.

Citizenship requirement: None

Problem Statement

Civilian rescue and relief in the future will involve autonomous operations among multiple cyber, physical, and kinetic assets, together with interactions with humans. Such autonomous operation will rely on a pipeline of machine learning (ML) algorithms executing in real-time on a distributed set of heterogeneous platforms, both stationary and maneuverable. The algorithms will have to deal with both adversarial control and data planes. The former means that some of the nodes on which the algorithms will execute cannot be trusted and have been compromised for leaking information or

violating the integrity of the results. An adversarial data plane means that the algorithms will have to operate with uncertain, incomplete, and potentially, maliciously manipulated data sources. This project will design secure algorithms that can provide probabilistic guarantees on security and latency, under powerful, rigorously quantified adversary models, moving away from the trend of one-off security solutions for specific attack vectors. The project will provide a robust, scalable, and usable software suite that can execute on today's standard and custom execution platforms plus on ARL CISD's (Computational and Information Sciences Directorate) autonomous battlefield testbed.

The project will make fundamental research contributions under three pillars—robust adversarial algorithms, interpretable algorithms aiding the trust of the warfighter on the results of the autonomous algorithms, and secure, distributed execution of the autonomy pipeline among multiple platforms.

Two representative papers that give a flavor of this kind of work are:

1. Bagchi, Saurabh, Vaneet Aggarwal, Somali Chaterji, Fred Douglis, Aly El Gamal, Jiawei Han, Brian Henz et al. "Vision Paper: Grand Challenges in Resilience: Autonomous System Resilience through Design and Runtime Measures." IEEE Open Journal of the Computer Society (OJCS), pp. 1-15, 2020, doi: 10.1109/OJCS.2020.3006807.
2. Minghong Fang, Xiaoyu Cao, Jinyuan Jia, and Neil Zhenqiang Gong. "Local Model Poisoning Attacks to Byzantine-Robust Federated Learning". In USENIX Security Symposium, 2020.

Application procedure

Send an email note to Prof. Bagchi with your CV (in pdf) and answers to the following specific questions in the body of the email. Qualified candidates will be invited for interviews.

1. When did you start your Masters/PhD?
2. What are your grades in courses at Purdue?
3. What was your rank in your undergraduate department (e.g., 3rd among 50 students in Computer Science)?
4. What are your grades in programming courses in your undergraduate?
5. Is there a Purdue person (professor, supervisor, etc.) who can speak about your qualifications?