IEEE SMC 2022
PRAGUE • CZECH REPUBLIC

IEEE SMC 2022
International Conference on Systems, Man, and Cybernetics
Clarion Congress Hotel Prague, Czech Republic
October 9-12, 2022

Special Session

Code: 1waes

Title

Adversarial Machine Learning for Safety and Security in Cyber Physical Systems

Proposer / Main Organizer

Dr. Apurva Narayan, Assistant Professor, The University of British Columbia
Department of Computer Science, Mathematics, Physics, Statistics
1177 Research Rd, Kelowna, BC V1V 1V7
Email: apurva.narayan@uwaterloo.ca

Dr. Sandeep Paul, Professor, Dayalbagh Educational Institute,
Department of Physics and Computer Science,
Dayalbagh, Agra – 282 005
Email: spaul@dei.ac.in

Dr. Beiyu Lin, Assistant Professor, Department of Computer Science,
University of Nevada, - Las Vegas, Las Vegas, USA
Email: beiyu.lin@unlv.edu

IEEE Member or SMC Society Member

Yes

Category

Please select one of the following categories:

- *Cybernetics*

Number of Expected Paper Submissions:

6 or more

Keywords

See list of topics in the Call for Papers

- Deep Learning
- Image Processing and Pattern Recognition
- Information Assurance and Intelligent

- Machine Learning
- Neural Networks and their applications
- Quantum Machine Learning

Brief Description and Justification (200-250 words):

Adversarial machine learning is a new gamut of technologies that aim to study vulnerabilities of ML approaches and detect the malicious behaviors in adversarial settings. The adversarial agents can deceive an ML classifier by significantly altering its response with imperceptible perturbations to the inputs. Although it is not to be alarmist, researchers in machine learning have a responsibility to preempt attacks and build safeguards especially when the task is critical for information security, and human lives. We need to deepen our understanding of machine learning in adversarial environments.

While the negative implications of this nascent technology have been widely discussed, researchers in machine learning are yet to explore their positive opportunities in numerous aspects. The positive impacts of adversarial machine learning are not limited to boost the robustness of ML models, but cut across several other domains including privacy protection, reliability and safety test, model understanding, improving generalization performance on different tasks, etc.

Since there are both positive and negative applications of adversarial machine learning, tackling adversarial learning to their use in the right direction requires a framework to embrace the positives. This workshop aims to bring together researchers and practitioners from a variety of communities (e.g., machine learning, computer security, data privacy and ethics) in an effort to synthesize promising ideas and research directions, as well as foster and strengthen cross-community collaborations on both theoretical studies and practical applications. Different from the previous workshops on adversarial machine learning, our proposed workshop seeks to explore the prospects besides reducing the unintended risks for sophisticated ML models.