POSTER SESSION 1 (10:00 – 11:00)

Gatherly Link for Poster Session: https://workshopsdayone.event.gatherly.io/

1. Trojan Signatures in DNN Weights
2. Defending Object Detection Networks Against Adversarial Patch Attacks
3. Impact of Colour on Robustness of Deep Neural Networks
4. Evasion Attack STeganography: Turning Vulnerability Of Machine Learning To Adversarial Attacks Into A Real-world Application
5. Can Targeted Adversarial Examples Transfer When the Source and Target Models Have No Label Space Overlap?
6. A Hierarchical Assessment of Adversarial Severity
7. Detecting and Segmenting Adversarial Graphics Patterns from Images
8. Enhancing Adversarial Robustness via Test-time Transformation Ensembling
9. Countering Adversarial Examples: Combining Input Transformation and Noisy Training
10. On Adversarial Robustness: A Neural Architecture Search perspective
11. Leveraging Test-Time Consensus Prediction for Robustness against Unseen Noise
12. Are socially-aware trajectory prediction models really socially-aware?

POSTER SESSION 2 (16:00 – 17:00)

Gatherly Link for Poster Session: https://workshopsdayone.event.gatherly.io/

13 On the Effect of Pruning on Adversarial Robustness

14 Mental Models of Adversarial Machine Learning

15 An Adversarial Attack on DNN-based Adaptive Cruise Control Systems

16 Encouraging Intra-Class Diversity Through a Reverse Contrastive Loss for Single-Source Domain Generalization

17 Towards Achieving Adversarial Robustness Beyond Perceptual Limits

18 Optical Adversarial Attack

19 Patch Attack Invariance: How Sensitive are Patch Attacks to 3D Pose?

20 Can Optical Trojans Assist Adversarial Perturbations?

21 Towards Category and Domain Alignment: Category-Invariant Feature Enhancement for Adversarial Domain Adaptation

22 Backdoor Learning Curves: Explaining Backdoor Poisoning Beyond Influence Functions

23 AdvFoolGen: Creating Persistent Troubles for Deep Classifiers

24 Efficient Training Methods for Achieving Adversarial Robustness Against Sparse Attacks