11-10

2011 SIAM Conference on Control and Its Applications

Part of MS33 Learning and Information Exploitation in Adversarial Networks

Learning and Resilience to Information Deception in Adversarial Networked Systems: The Necessity and Structure of a Trusted Core

Abstract. We investigate distributed inference and learning problems in networked systems with adversaries. We analyze the effects of adversarial attacks on the solutions and characterize the solution robustness and resiliency as functions of network topology and adversary distribution. We demonstrate that existence of a small subnetwork of "trusted nodes" (trusted core) provides substantial improvements to solution robustness and resilience. We characterize these improvements as functions of the degree of trust, connectivities and location of trusted nodes.

Authors

- *John Baras, University of Maryland, College Park, USA, baras@umd.edu*

CT11 Home | Program | Speaker Index | Hotel | Transportation | Registration

SIAM Conference Participation System
Problems using this system? Email wilden@siam.org.
Bug reports to duggan@siam.org.