Computer Science
Distinguished Lecture

Date: Friday, February 1, 2019
Time: 4:00pm
Location: 2200 Marston

Privacy and Security for Distributed Optimization and Learning

Consider a network of agents wherein each agent has a private cost function. In the context of distributed machine learning, the private cost function of an agent may represent the "loss function" corresponding to the agent's local data. The objective here is to identify parameters that minimize the total cost over all the agents. In machine learning for classification, the cost function is designed such that minimizing the cost function should result model parameters that achieve higher accuracy of classification. Similar problems arise in the context of other applications as well, including swarm robotics.

Our work addresses privacy and security of distributed optimization with applications to machine learning. In privacy-preserving machine learning, the goal is to optimize the model parameters correctly while preserving the privacy of each agent's local data. Privacy-preserving machine learning is becoming important due to the increasing reliance on user-generated data for machine learning. In security, the goal is to identify the model parameters correctly while tolerating adversarial agents that may be supplying incorrect information. When a large number of agents participate in distributed optimization, security compromise of some of the agents becomes increasingly likely. We constructively show that such privacy-preserving and secure algorithms for distributed optimization exist. The talk will provide intuition behind the design and correctness of the algorithms

Part of the Computer Science Seminar Series

IOWA STATE UNIVERSITY
Department of Computer Science
www.cs.iastate.edu

Nitin Vaidya is the Robert L. McDevitt, K.S.G., K.C.H.S. and Catherine H. McDevitt L.C.H.S. Chair of Computer Science at Georgetown University. He received Ph.D. from the University of Massachusetts at Amherst. He previously served as a Professor and Associate Head in Electrical and Computer Engineering at the University of Illiniois at Urbana-Champaign. He has co-authored papers that received awards at several conferences, including 2015 SSS, 2007 ACM MobiHoc and 1998 ACM MobiCom. He is a fellow of the IEEE. He has served as the Chair of the Steering Committee for the ACM PODC conference, as the Editor-in-Chief for the IEEE Transactions on Mobile Computing, and as the Editor-in-Chief for ACM SIGMOBILE publication MC2R.