Computer Science Seminar

Privacy in the field: Protecting Sensitive Data for AI Applications

Ferdinando Fioretto

School of Industrial and Systems Engineering, Georgia Institute of Technology

February 11, 2019
10:00 - 10:50 am
209 Computer Science Building
Refreshments will be served at 9:45 am outside CS209

Advances in artificial intelligence and data science have allowed the development of products that leverage individuals data to provide valuable services. However, the use of this massive quantity of personal information raises fundamental privacy concerns. Differential Privacy (DP) has emerged as the de-facto standard to addresses the sensitivity of such information and can be used to release privacy-preserving datasets.
Despite its large theoretical value, when these private datasets are used as inputs to complex machine learning or optimization tasks, they may produce results that are fundamentally different from those obtained on the original datasets.

In this talk, I will focus on the problem of releasing privacy-preserving datasets for complex data analysis tasks. I will introduce the notion of Constrained-Based Differential Privacy (CBDP) which allow us to cast the data release problem to an optimization problem whose goal is to preserve the salient features of the original dataset. Finally, I will discuss two applications of CBDP for large socio-technical systems related to the optimization of operations in transportation systems and energy networks.

Bio: Ferdinando (Nando) Fioretto is a postdoctoral researcher at the Georgia Institute of Technology. His research focuses on artificial intelligence, data privacy, and multiagent coordination. Nando has published in several top-ranked artificial intelligence journals and conferences. He has organized workshops, special tracks, and gave tutorials in top-ranked AI conferences, and has served the program committee of various artificial intelligence conferences, including AAAI, IJCAI, AAMAS, and CP. He is the recipient of a best student paper award (CMSB, 2013), a most visionary paper award (AAMAS workshop series, 2017), and a best AI dissertation award (AI*IA, 2017).

MISSOURI S&T