UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

PhD Defence

Thursday October 19, 2023 at 9AM, online via Zoom (Remote)

Wenjing Zhang

Machine Learning Approaches to Spatial-Temporal Density Release with Information-Theoretic Privacy

Chair: Dr. Andrew Hamilton-Wright
Advisor: Dr. Xiaodong Lin
Advisory: Dr. Lei Lei [SoE]
Non-Advisory: Dr. Ahmed Refaey Hussein [SoE]
External Examiner: Dr. Jelena Misic [Toronto Metropolitan University]

Abstract:

In the era of data-driven decision-making and advanced analytics, the increasing volume of spatial-temporal data has revolutionized various domains, offering valuable insights into human mobility, transportation patterns, and societal behavior. However, the release of such data poses significant challenges to individuals' privacy due to the potential revelation of sensitive information. This thesis focuses on addressing the privacy concerns associated with the release of spatial-temporal data by leveraging information theory and machine learning techniques. The primary goal of this thesis is to promote spatial-temporal data privacy protection with information theory and establish rigorous, scalable, and efficient machine learning frameworks for privacy enhancing technologies.

The thesis contributes through formulating and applying information-theoretic privacy metrics to spatial-temporal density data for rigorous guarantees and creating scalable, efficient privacy-preserving mechanisms using state-of-the-art machine learning. The results demonstrate information theory and machine learning's potential to safeguard spatial-temporal density data, allowing responsible use for research and decision-making while preserving privacy. This work emphasizes the necessity for continued technical exploration into privacy foundations and enhancing connections between privacy-related research across disciplines: machine learning, information theory, statistics, game theory, and data science.