

# *Preserving Auto-Driving: a GAN-based Approach to Protect Vehicular Camera Data*

Dr. Wei Li

Assistant Professor, Department of Computer Science  
Georgia State University

Friday, October 11, 2:00pm – 2:50pm, Location: MH: 3.01.18

**Abstract:** The autonomous driving (auto-driving) technology has been promoted significantly by the rapid advances in computer vision and deep neural networks. Auto-driving vehicles, nowadays, are fully equipped with numerous sensors such as cameras, geo-sensors, and radar sensors, to capture real-time data inside the vehicles and outside surroundings. Meanwhile, the captured data contains lots of private information about vehicles, drivers and passengers and thus faces a high risk of privacy breaches. Especially, side-channel information can be mined from camera data to identify vehicles' locations and even trajectories, raising serious privacy issues. Unfortunately, the issue, how to resist location-inference attack for camera data in auto-driving, has never been addressed in literature. In this talk, a GAN-based image-to-image translation method, named Auto-Driving GAN (ADGAN), will be introduced. Through performance comparisons between ADGAN and the state-of-the-art, the superiority of our proposed ADGAN can be validated – offering an effective tradeoff between recognition utility and privacy protection for camera data.

## Biography



Dr. Wei Li currently is an Assistant Professor in the Department of Computer Science at Georgia State University. Dr. Li received her Ph.D. degree in Computer Science from The George Washington University in 2016. Her current research mainly spans the areas of security and privacy for the Internet of Things and Cyber-Physical Systems, secure and privacy-aware computing, Big Data, Blockchain, Game Theory, and algorithm design and analysis. Dr. Li has published more than 40 papers in international journals and conferences. Dr. Li has served as the Publication Chair for WASA 2018 and IEEE PAC 2018 and 2017, and the technical program committee member for several international conferences, including INFOCOM 2020, ICDCS 2019, and Globecom 2019, etc. She is a member of IEEE and ACM.