# Xin Wang

2117 NE Mason Rd Seattle WA 98195 ⊠ xinw22**0**uw.edu

Ph.D. Student in Transportation Engineering Homepage

₩ xinw22@uw.edu Homepage | Google Scholar

## Research Interests

#### Cyberseciruty in Intelligent transportation systems

- Adversarial attacks on traffic forecasting models...
- Machine unlearning for Intelligent Transportation Systems.

## Education

2022-Present Ph.D., Transportation Engineering, University of Washington, Seattle, WA

Advisor: Prof. Xuegang (Jeff) Ban

2020–2022 M.S., Statistics, Renmin University of China, Beijing, China

2016–2020 B.S., Applied Mathematics, Central South University, Changsha, China

## Research & Teaching

2022-Present Research Assistant, University of Washington, Seattle, WA

 Machine unlearning, adversarial robustness, and optimization for intelligent transportation systems.

Autumn 2024 Teaching Assistant, CET 513: Optimization in Transportation, UW CEE

O Lab sections, office hours, and grading.

# Industry Experience

Jan-May 2021 Machine Learning Engineer Intern, Baidu Inc., Beijing, China

- Multi-objective ranking optimization for online video search using Pareto-Efficient LTR (PE-LTR).
- Improved both NDCG and CTR; identified Pareto solutions with NSGA-II (fast non-dominated sorting, elitist MOEA).

### Journal Publications

Wang, Feilong, Xin Wang, Hong, Yuan, Rockafellar, R. Tyrrell, Ban, Xuegang Jeff. "Data poisoning attacks on traffic state estimation and prediction." *Transportation Research Part C* 168 (2024): 104577.

Wang, Feilong, Xin Wang, Ban, Xuegang Jeff. "Data poisoning attacks in intelligent transportation systems: A survey." *Transportation Research Part C* 165 (2024): 104750.

# Conference Proceedings

Xin Wang, Feilong Wang, Xuegang Jeff Ban. "Set-Valued Sensitivity Analysis of Deep Neural Networks." In *Proceedings of the AAAI Conference on Artificial Intelligence* 39(20) (2025): 21304–21311.

Feilong Wang, Xin Wang, Jeff Ban. "Infrastructure-enabled Defense Methods against Data Poisoning Attacks on Traffic State Estimation and Prediction." In Conference in Emerging Technologies in Transportation Systems (TRC-30), 2025.

## Manuscripts Under Review / Submitted

Xin Wang, Feilong Wang, Yuan Hong, Xuegang Ban. "Transferability in Data Poisoning Attacks on Spatiotemporal Traffic Forecasting Models." SSRN 4827065 (2024). Submitted to *Transportation Research Part C*.

Xin Wang, R. Tyrrell Rockafellar, et al. "Machine Unlearning of Traffic State Estimation and Prediction." arXiv:2507.17984 (2025). Submitted to ISTTT.

Xin Wang, Feilong Wang, Yuan Hong, R. Tyrrell Rockafellar, et al. "Model-Targeted Data Poisoning Attacks against ITS Applications with Provable Convergence." arXiv:2505.03966 (2025). Submitted to AAAI.

#### Invited Talks & Guest Lectures

- Jan 2025 **Data Poisoning Attacks on Traffic State Estimation and Prediction** *ISTTT 2025*
- June 2024 A Review of Data Poisoning Attacks in Intelligent Transportation Systems TRB 2025

#### Academic Service

Reviewer: Transportation Research Part C, TRB Annual Meeting, AAAI Conference on Artificial Intelligence