Chenyi Wang

Tucson, AZ 85704, USA
chenyiw@arizona.edu (612) 321-8888
Keywords: **AI/ML Security; Computer Vision; Robotics; Cyber-Physical System; Multi-Agent System**

Education

University of Arizona — Jan. 2023 – May. 2026 (Expected)
Doctor of Philosophy (PhD) in Electrical and Computer Engineering (ECE) — GPA: 4.00/4.00
Advisor: Dr. Ming Li, IEEE Fellow — *Herbold Fellow*

Columbia University — Sep. 2021 – Dec. 2022
Master of Arts (MA) in Statistics — GPA: 4.00/4.00

University of Minnesota, Twin Cities — Aug. 2018 – May 2021
Bachelor of Science (BS) in Statistics, Bachelor of Arts (BA) in Mathematics — GPA: 3.93/4.00
Minor in Computer Science (CS) — *High Distinction*, *Phi Beta Kappa*

Publications

C. Wang, Z. Li, M. Li, W. Wen
'Joint Semantic Feature Encoding and Transmission for Communication-Efficient Cooperative Perception'
Under review at ECCV 2026

Y. Liu, C. Wang, M. Li, Q. Zhang
'Adversarial Trust Poisoning in Vehicular Collaborative Perception'
Under review at VehicleSec 2026

C. Wang, R. Muller, R. Song, J.P. Monteuuis, Z.B. Celik, Y. Man, J. Petit, R. Gerdes, M. Li
'CP-FREEZER: Latency Attacks against Vehicular Cooperative Perception'
AAAI Conference on Artificial Intelligence (**AAAI**) 2026; Acceptance Rate: 17.6%

R. Muller, C. Wang, R. Song, J.P. Monteuuis, Y. Man, M. Li, R. Gerdes, J. Petit, Z.B. Celik
'Spatiotemporal Consistency: A Universal Defense Against Attacks on Autonomous Systems'
IEEE Security & Privacy 2025, Volume 23, Issue 6

C. Wang, R. Muller, R. Song, J.P. Monteuuis, J. Petit, Y. Man, R. Gerdes, Z.B. Celik, M. Li
'From Threat to Trust: Exploiting Attention Mechanisms for Attacks and Defenses in Cooperative Perception'
USENIX Security Symposium (**USENIX**) 2025; Acceptance Rate: 17.1%

R. Muller, R. Song, C. Wang, Y. Zhan, J.P. Monteuuis, Y. Man, M. Li, R. Gerdes, J. Petit, Z.B. Celik
'Investigating Physical Latency Attacks against Camera-based Perception'
IEEE Symposium on Security and Privacy (**SP**) 2025; Acceptance Rate: 14.8%

C. Wang, Y. Man, R. Muller, M. Li, Z.B. Celik, R. Gerdes, J. Petit
'Physical ID-Transfer Attacks against Multi-Object Tracking via Adversarial Trajectory'
IEEE Annual Computer Security Applications Conference (**ACSAC**) 2024; Acceptance Rate: 19.7%

Activities and Services

Program Committee

USENIX Security Artifact Evaluation Committee — 2026
VehicleSec Poster/Demo Committee — 2026
NDSS Symposium Poster Session Committee — 2026
EAI SmartSP Program Committee — 2026

Reviewer

AAAI Conference on Artificial Intelligence (AAAI) — 2026
IEEE Internet of Things Journal (IEEE IoT) — 2025
IEEE Transactions on Information Forensics & Security (IEEE TIFS) — 2024
IEEE Transactions on Cyber-Physical Systems (IEEE TCPS) — 2025
IEEE International Conference on Communications (IEEE ICC) — 2025
IEEE International Conference on Computer Communications and Networks (IEEE ICCCN) — 2023
USENIX Security Symposium — 2023, 2024, 2026
ACM Computer and Communications Security (ACM CCS) — 2023, 2024, 2025
USENIX Symposium on Vehicle Security and Privacy (VehicleSec) — 2023, 2025

Honors and Awards

- USENIX Security Symposium Student Travel Grant — 2025
- GPSC Student Travel Grant — 2024
- Herbold Fellowship, VehicleSec Student Travel Grant — 2023
- Columbia University Department of Statistics Fellowship, ASA JSM Award — 2022