

# Ning (Nicole) Wang

Email: [ningw@usf.edu](mailto:ningw@usf.edu)

[Homepage](#)

[Google Scholar](#)

## EDUCATION

**Virginia Tech**, Blacksburg, VA 09/2018-05/2023

- Ph.D. in Computer Engineering, advised by Dr. Wenjing Lou and Dr. Y. Thomas Hou
- Dissertation: Building trustworthy machine learning systems in adversarial environments

**Beijing University of Posts and Telecommunications**, Beijing 09/2015-03/2018

- M.S. in Electronics and Communication Engineering, advised by Dr. Qimei Cui
- Thesis: Modeling and performance analysis of vehicular network with stochastic geometry theory

**Beijing University of Posts and Telecommunications**, Beijing 09/2011-07/2015

- B.S. in Telecommunication Engineering

## RESEARCH INTEREST

- Security and privacy in machine learning: adversarial machine learning, federated learning, meta-learning, and differential privacy.
- Machine learning applied to cybersecurity: anomaly detection, network intrusion detection, contrastive learning, and intelligent IoT.

## WORK EXPERIENCE

**Assistant Professor** 08/2023 – Present  
Department of Computer Science and Engineering, University of South Florida, Tampa, FL

**Research Internship** in ByteDance Inc. 05/2022 – 08/2022

**Graduate Research Assistantship**, Virginia Tech 09/2018 – 05/2023

## PUBLICATIONS

### Conference proceedings

1. MINDFL: Mitigating the Impact of Imbalanced and Noisy-Labeled Data in Federated Learning With Quality and Fairness-Aware Client Selection  
C. Zhang, **N. Wang**, S. Shi, C. Du, W. Lou and Y.T. Hou  
*In the IEEE Military Communications Conference (MILCOM), 2023.*
2. Building Trustworthy Machine Learning Systems in Adversarial Environment  
**N. Wang**  
*Dissertation, 2023.*
3. Squeezing More Utility via Adaptive Clipping on Differentially Private Gradients in Federated Meta-Learning  
**N. Wang**, Y. Xiao, Y. Chen, N. Zhang, W. Lou and Y.T. Hou  
*In Annual Computer Security Applications Conference (ACSAC), 2022. (Acceptance rate: 24.0%)*

4. FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations  
**N. Wang**, Y. Xiao, Y. Chen, Y. Hu, W. Lou and Y.T. Hou  
*In the 2022 ACM on Asia Conference on Computer and Communications Security (AsiaCCS), 2022. (Acceptance rate: 18.4%)*
5. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning  
**N. Wang**, Y. Chen, Y. Hu, W. Lou and Y.T. Hou,  
*In the IEEE International Conference on Computer Communications (INFOCOM), 2022. (Acceptance rate: 19.9%)*
6. Transferability of Adversarial Examples in Machine Learning-based Malware Detection  
Y. Hu, **N. Wang**, Y. Chen, W. Lou and Y.T. Hou  
*In the IEEE Conference on Communications and Network Security (CNS), 2022. (Acceptance rate: 35.2%)*
7. MANDA: On Adversarial Example Detection for Network Intrusion Detection System  
**N. Wang**, Y. Chen, Y. Hu, W. Lou and Y.T. Hou  
*In the IEEE International Conference on Computer Communications (INFOCOM), 2021. (Acceptance rate: 19.9%)*
8. PriRoster: Privacy-preserving Radio Context Attestation in Cognitive Radio Networks  
R. Zhang, **N. Wang**, N. zhang, Z. Yan, W. Lou and Y.T. Hou  
*In the IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2019.*
9. Optimization Deployment of Roadside Units with Mobile Vehicle Data Analytics  
X. Cao, Q. Cui, S. Zhang, X. Jiang, and **N. Wang**  
*In IEEE Asia-Pacific Conference on Communications (APCC), 2018.*
10. Spatial Point Process Modeling of Vehicles in Large and Small Cities  
Q. Cui, **N. Wang** and M. Haenggi  
*In IEEE Global Communications Conference (GLOBECOM), 2017. (Acceptance rate: 39.0%)*
11. Energy efficiency maximization for CoMP joint transmission with non-ideal power amplifiers  
Y. Zhang, Q. Cui, and **N. Wang**  
*In IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017.*
12. Energy-efficient user access control and resource allocation in HCNs with non-ideal circuitry  
Y. Zhang, Q. Cui, and **N. Wang**  
*In IEEE International Conference on Wireless Communications and Signal Processing (WCSP), 2017.*
13. Optimal Pilot Symbols Ratio in terms of Spectrum and Energy Efficiency in Uplink CoMP Networks.  
Y. Zhang, Q. Cui, and **N. Wang**  
*In IEEE Vehicular Technology Conference (VTC Spring), 2017.*

#### Journal articles

1. MANDA: On Adversarial Example Detection for Network Intrusion Detection System  
**N. Wang**, Y. Chen, Y. Xiao, Y. Hu, W. Lou and Y.T. Hou  
*In IEEE Transactions on Dependable and Secure Computing (TDSC), 2022 (early access)*
2. Vehicle distributions in large and small cities: Spatial models and applications  
Q. Cui, **N. Wang**, and M. Haenggi  
*In IEEE Transactions on Vehicular Technology (TVT), vol. 67, no. 11, pp. 10176-10189, August 2018.*

3. Energy-efficient resource allocation for hybrid bursty services in multi-relay OFDM networks.  
Y. Zhang, Q. Cui, **N. Wang**, Y. Hou, and W. Xie  
*In Science China Information Sciences*, vol. 60, no. 10 pp. 1-18, October 2017.

### Under review & Preprint

1. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning  
**N. Wang**, S. Shi, Y. Chen, W. Lou, Y.T. Hou  
*submitted to IEEE Transactions on Dependable and Secure Computing (TDSC)*
2. FLARE: Defending Federated Learning against Model Poisoning Attacks via Latent Space Representations  
**N. Wang**, Chaoyu Zhang, Y. Xiao, Y. Chen, W. Lou and Y.T. Hou  
*submitted to IEEE Transactions on Dependable and Secure Computing (TDSC)*
3. Scale-MIA: A Scalable Model Inversion Attack against Secure Federated Learning via Latent Space Reconstruction  
S. Shi, **N. Wang**, Y. Xiao, C. Zhang, Y. Shi, Y. T. Hou, W. Lou  
*arXiv preprint arXiv:2311.05808*, 2023

### TEACHING Experience

CIS 6930 Security & Privacy in Machine Learning	Fall, 2023
CIS 4219 Human Aspects in Cybersecurity	Spring, 2024

### AWARDS AND RECOGNITIONS

ACSAC Conferenceship	2022
IEEE INFOCOM Student Travel Grant	2022
IEEE ICNP Student Travel Grant	2022
IEEE CNS Student Travel Grant	2022
BUPT Excellent Graduate Student Award	2016 & 2017

### TUTORIALS

Ning Wang 'Trustworthy Machine Learning Systems under Adversarial Environments', the 26th International Symposium On Wireless Personal Multimedia Communications (WPMC'23)

### PROFESSIONAL SERVICES

#### Committee for:

- Program committee for ACM Workshop on Moving Target Defense (MTD23) colocated with ACM conference on computer and communications (CCS23).
- Program committee for the sixth ACM Workshop on Wireless Security and Machine Learning (WiseML 2024), in conjunction with ACM WiSec 2024.
- Will serve as Technical Program Committee for AsiaCCS 2025 and INFOCOM 2025.

#### Conference reviewer for:

- IEEE Symposium on Security and Privacy (S&P) 2023
- European Symposium on Research in Computer Security (ESORICS) 2022
- IEEE Conference on Communications and Network Security (CNS) 2019
- IEEE International Conference on Sensing, Communication, and Networking (SECON) 2019

- IEEE International Conference on Fog Computing (ICFC) 2019

**Journal reviewer for:**

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE/ACM Transactions on Networking (ToN)
- IEEE Transactions on Cloud Computing (TCC)
- IEEE Transactions on Artificial Intelligence (TAI)

**Talks for:**

- ACSAC 2022
- LASER@ACSAC 2022 workshop
- AsiaCCS 2022
- IEEE CNS 2022
- IEEE INFOCOM 2021, 2022