Ning (Nicole) Wang

Email: ningw@usf.edu Homepage Google Scholar

RESEARCH INTEREST

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

WORK EXPERIENCE

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

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

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

PUBLICATIONS

Conference proceedings

1. BoBa: Boosting Backdoor Detection through Data Distribution Inference in Federated Learning
   Zhengyuan Jiang, Xingyu Lyu, Shanghao Shi, Yang Xiao, Yimin Chen, Thomas Hou, Wenjing Lou and **Ning Wang**
   Accepted by European Conference on Artificial Intelligence (ECAI), 2025
2. Let the Noise Speak: Harnessing Noise for a Unified Defense Against Adversarial and Backdoor Attacks
   Md Hasan Shahriar, **Ning Wang**, Naren Ramakrishnan, Y. Thomas Hou, and Wenjing Lou
   Acccepted by European Symposium on Research in Computer Security (ESORICS), 2025
3. Beyond Uniformity: Robust Backdoor Attacks on Deep Neural Networks with Trigger Selection

S Li, X Lyu, **N Wang**, T Li, D Chen, Y Chen
in Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), 2025

4. 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, and W. Lou
   *In network and distributed system security (**NDSS**), 2025*

5. Adversarial Attacks on Federated Learning Revisited: a Client-Selection Perspective
   X. Lyu, S. Li, **N. Wang**, T. Li, D. Chen, Y. Chen
   *In the IEEE Conference on Communications and Network Security (**CNS**), 2024.*

6. Hermes: Boosting the Performance of Machine-Learning-based Intrusion Detection System through Geometric Feature Learning
   C. Zhang, S. Shi, **N. Wang**, X. Xu, S. Li, L. Zheng, R. Marchany, M. Gardner, Y.T. Hou, and W. Lou
   *In the 25th International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (**MOBIHOC**), 2024*

7. 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.*

8. Building Trustworthy Machine Learning Systems in Adversarial Environment
   N. Wang
   Dissertation, 2023.

9. 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%)*

10. 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%)*

11. 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%)*

12. 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%)*

13. 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%)*

14. 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.*
15. 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.*
16. 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%)*
17. 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.*
18. 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.*
19. 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. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning
   N. Wang, S. Shi, Y. Chen, W. Lou, Y.T. Hou
   *IEEE Transactions on Dependable and Secure Computing (**TDSC**), Vol. 22, Issue 4, pp. 4215-4230, July-Aug 2025.*
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
   *IEEE Transactions on Dependable and Secure Computing (**TDSC**), Vol. 22, Issue 3, pp 2607-2623 May-June 2025.*
3. 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**), Vol. 20, Issue 2, pp. 1139-1153, March-April 2023.*
4. 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.*
5. 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.

TEACHING EXPERIENCE

CIS 6930 Security & Privacy in Machine Learning	Fall, 2023
CIS 4219/CIS 6218 Human Aspects in Cybersecurity	Spring, 2024, 2025

AWARDS AND RECOGNITIONS

ACSAC Student 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

Workshop & Tutorial

- 2024 CRA Career Mentoring Workshop.
- 2024 NSF Aspiring CPS PIs Workshop.
- 2024 CISE CAREER workshop.
- Tutorial on 'Trustworthy Machine Learning Systems under Adversarial Environments', at the 26th International Symposium On Wireless Personal Multimedia Communications (WPMC'23).

PROFESSIONAL SERVICES

Technical Program Committee for:

• IEEE Military Communications Conference (MILCOM)	2024, 2025.
• ACM ASIA Conference on Computer and Communications Security (ASIACCS)	2025.
• Network and Distributed System Security Symposium NDSS	2025, 2026.
• IEEE International Conference on Computer Communications (INFOCOM)	2025, 2026.
• ACM Workshop on Adaptive and Autonomous Cyber Defense (AACD)	2024.
• ACM Workshop on Moving Target Defense (MTD) colocated with CCS	2023.
• The sixth ACM Workshop on Wireless Security and Machine Learning WiseML,	2024.

Chair:

- Web Chair for IEEE International Conference on Computer Communications (INFOCOM 2025, 2026)

Journal reviewer for:

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE/ACM Transactions on Networking (ToN)
- IEEE Transactions on Cloud Computing (TCC)
- IEEE Transactions on Artificial Intelligence (TAI)
- IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI)
- IEEE Journal on Selected Areas in Communications (JSAC)
- IEEE Communications Surveys and Tutorials (COMST)
- IEEE Internet of Things Journal (IoT)
- IEEE Transactions on Computers (TC)
- IEEE Network Magazine
- ACM Transactions on Internet of Things
- Journal of Intelligent & Fuzzy Systems (IFS)