Ning (Nicole) Wang

Email: ning18@vt.edu Homepage Google Scholar

I will work as an assistant professor in the Department of Computer Science Engineering at the University of South Florida starting in the fall of 2023.

EDUCATION

Virginia Tech, Blacksburg, VA 09/2018-05/2023 (expected)

- 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.

RESEARCH EXPERIENCE

Graduate Research Assistantship, Virginia Tech 09/2018 – Present
(Affiliated with the Complex Networks and Security Research (CNSR) Lab)

- Working on the *multidisciplinary university research initiatives (MURI) program* funded by ONR.
  - Research focus is the security and privacy of federated learning, network anomaly detection in IoT networks.
  - Topics include federated learning, reinforcement learning, Byzantine-resilient distributed learning, privacy-preserving federated learning, and differentially private meta-learning; defense against adversarial example attacks, backdoor attacks, data/model inference attacks, data/model poisoning attacks, etc.
- Working on the *Secure and Trustworthy Cyberspace (SaTC) project* funded by NSF.
  - Research focus is the robustness of machine learning-based intrusion detection.
  - Topics include adversarial machine learning, adversarial example generation, adversarial example transferability, adversarial example detection, contrastive learning, curriculum learning, robust network intrusion detection, malware detection, etc.

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

- Worked on research and implementation of intelligent access control.

Research Assistantship, Beijing University of Posts and Telecommunications 09/2015 – 03/2018
(Affiliated with the Key Laboratory of Universal Wireless Communications)

- Worked on spatial point process modeling using real taxi data.

PUBLICATIONS

Conference proceedings

1. 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
   *accepted by Annual Computer Security Applications Conference (**ACSAC**), 2022. (Acceptance rate: 24.0%)*
2. 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%)*
3. 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%)*
4. 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%)*
5. 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%)*
6. 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.*
7. 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.*
8. 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%)*
9. 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.*

10. 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.*
11. 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

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. MINDFUL-FL: Mitigating the Impact of Imbalanced and Noisy Data in Federated Learning with Quality and Fairness-Aware Client Selection.
   C. Zhang, **N. Wang**, S. Shi, C. Du, W. Lou, Y.T. Hou
   submitted as a conference paper

TEACHING INTEREST

Network security, computer security, machine learning, information assurance, computer networks, wireless networks, cryptography, data structures and algorithms, computer programming, calculus, linear algebra, and other courses as required

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

PROFESSIONAL SERVICES

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 2022
- IEEE INFOCOM 2021