Shanghao Shi

Ph.D. Candidate in Computer Science, Virginia Tech

Email: shanghaos@vt.edu
Phone: 540-251-9127
Address: 5-210 Virginia Tech Research Center, 900 N. Glebe Rd, Arlington, VA 22203
Homepage: `https://shishishi123.github.io/`

Education

Virginia Polytechnic Institute and State University (VT), Arlington, VA 09/2019 – 06/2025 (expected)

- Ph.D. in Computer Science @ CS Department
  Advisor: Prof. Wenjing Lou

Beijing University of Posts and Telecommunications (BUPT), Beijing, China 09/2015 – 06/2019

- B.S. in Telecommunication Engineering @ School of Information and Communication Engineering

Research Interests

□ **Adversarial Machine Learning and Trustworthy AI**
□ **Security and Privacy in 5G/Next G Mobile Networks**
□ **Cyber-physical and IoT Security**

Conference Publications

1. MedLeak – Harvesting Multimodal Medical Data in Secure Federated Learning with Crafted Models
   S. Shi, M. S. Haque, A. Parida, C. Zhang, M. G. Linguraru, Y. T. Hou, S. M. Anwar, and W. Lou
   *In the IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (**CHASE**), 2025.*
2. 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 the Network and Distributed System Security Symposium (**NDSS**), 2025.*
3. 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, W. Lou
   *In the ACM International Symposium on Mobile Ad Hoc Networking and Computing (**MobiHoc**), 2024.*
4. ProFLingo: A Fingerprinting-based Copyright Protection Scheme for Large Language Models
   H. jin, C. Zhang, **S. Shi**, W. Lou, and Y. T. Hou
   *In the IEEE Conference on Communications and Network Security (**CNS**), 2024. (**Best Paper Award**)*
5. Pri-Share: Enabling Inter-SAS Privacy Protection via Secure Multi-Party Spectrum Allocation
   H. Yu, **S. Shi**, Y. Shi, E. Burger, Y. T. Hou, and W. Lou
   *In the IEEE International Symposium on Dynamic Spectrum Access Networks (**DYSPAN**), 2024.*
6. TriSAS: Toward Dependable Inter-SAS Coordination with Auditability
   S. Shi, Y. Xiao, C. Du, Y. Shi, C. Wang, R. Gazda, Y. T. Hou, E. Burger, L. DaSilva, and W. Lou
   *In the ACM Asia Conference on Computer and Communications Security (**ASIACCS**), 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. Bijack: Breaking Bitcoin Network with TCP Vulnerabilities
   S. Li, **S. Shi**, Y. Xiao, C. Zhang, Y. T. Hou, and W. Lou
   *In the European Symposium on Research in Computer Security (**ESORICS**), 2023.*

9. MS-PTP: Protecting Network Timing from Byzantine Attacks
   S. Shi, Y. Xiao, C. Du, Md H. Shahriar, A.o Li, N. Zhang, Y. T. Hou, and W. Lou
   *In the ACM Conference on Security and Privacy in Wireless and Mobile Networks (**WiSec**), 2023.*
10. Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication
   Y. Xiao, **S. Shi**, N. Zhang, W. Lou, and Y. T. Hou
   *In the Annual Computer Security Applications Conference (**ACSAC**), 2020.*

Journal Publications

1. FeCo: Boosting Intrusion Detection Capability in IoT Networks via Contrastive Learning
   N. Wang, **S. Shi**, Y. Chen, W. Lou, and Y. T. Hou
   *In IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2025.*
2. BD-SAS: Enabling Dynamic Spectrum Sharing in Low-trust Environment
   Y. Xiao, **S. Shi**, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, and J. H. Reed
   *In IEEE Transactions on Cognitive Communications and Networking (**TCCN**), 2023.*
3. Decentralized Spectrum Access System: Vision, Challenges, and a Blockchain Solution
   Y. Xiao, **S. Shi**, W. Lou, C. Wang, X. Li, N. Zhang, Y. T. Hou, and J. H. Reed
   *In IEEE Wireless Communications (**WCM**), 2022.*
4. Challenges and New Directions in Securing Spectrum Access Systems
   S. Shi, Y. Xiao, W. Lou, C. Wang, X. Li, Y. T. Hou, and J. H. Reed
   *In IEEE Internet of Things Journal (**IOT-J**), 2021.*

ArXiv Preprints

1. BoBa: Boosting Backdoor Detection through Data Distribution Inference in Federated Learning
   N. Wang, **S. Shi**, Y. Xiao, Y. Chen, Y. T. Hou, and W. Lou
   *Under review by the European Symposium on Security and Privacy (**EuroS&P**), 2025.*

Teaching Experience

Graduate Teaching Assistant, Virginia Tech — Fall 2019

- CS 1604: Introduction to Python

Awards

BitShares Graduate Fellowship — 2021, 2023

- Awarded by Virginia Tech CS Department, funded by BitShares Inc.

National Scholarship — 2016

- Certified by Beijing University of Posts and Telecommunications.

Professional Experience

Conference Sub-Reviewer for,

- IEEE S&P 2022, 2023, 2024, 2025
- NDSS 2025
- ACM WiSec 2024
- IEEE CNS 2022
- ESORICS 2022
- ICCCN 2023

Journal Reviewer for,

- IEEE Internet of Things Journal
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Cognitive Communications and Networking
- IEEE/ACM Transactions on Networking