Xilong Wang

e-mail Google Scholar
website LinkedIn

Education

University of Science and Technology of China (USTC) Hefei, Anhui, China
Undergraduate of Information Security 2019 - Present

- Overall GPA: 3.86/4.3 Ranking: **2**/66
- Highlight Courses: Probability Theory & Mathematical Statistics (98), Stochastic Process (95), Mathematical Analysis (96), Linear Algebra (93), Introduction to Algorithms (91), Compiler Theory (91), Computer Networks (96), Discrete Mathematics (95), Function of Complex Variable (96), C Programming (90), Signals and Systems (98)

Purdue University West Lafayette, IN, USA
Undergraduate Research Program Fall 2023

- Advisor: **Xiangyu Zhang**, Samuel Conte Professor of Computer Science
- Research Topic: Security for Large Language Models (LLM)

Research Interests

Security and Privacy, including Data Hiding, Watermarking, Steganography, security for Large Language Models (LLM), secure Federated Learning, secure Reinforcement Learning, and Differentially Private Transfer Learning.

Publication

† indicates an Equal Contribution.

1. ICStega: Image Captioning-based Semantically Controllable Linguistic Steganography.
   X. Wang, Y. Wang, K. Chen, J. Ding, W. Zhang, and N. Yu.
   IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2023.

2. Provably Robust Federated Reinforcement Learning.
   M. Fang[†], **X. Wang**[†], and **Neil Gong**.
   Submitted to *USENIX Security '24*.

3. DFLGuard: Robust and Communication-efficient Decentralized Federated Learning.
   M. Fang, **X. Wang**, and **Neil Gong**
   Submitted to *IEEE Transactions on Dependable and Secure Computing (TDSC)*.

4. Exploring the Benefits of Differentially Private Pre-training and Parameter-Efficient Fine-tuning for Table Transformers.
   X. Wang, C.M. Yu, and **Pin-Yu Chen**
   Submitted to *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2024.

Research Experience

1. Provably Rubust Federated Reinforcement Learning Mar 2023 - Present
Advisor: **Neil Gong**, Assistant Professor, Duke University

- Proposed the Normalized attack, the first model poisoning attacks tailored to Byzantine-robust FRL.
- Introduced an efficient ensemble FRL method that is provably secure against poisoning attacks.
- Experiments highlight that our Normalized attack can notably compromise robust foundational aggregation rules. Additionally, our ensemble method shows significant capability in defending both existing and our proposed attacks.

Submitted to USENIX Security '24.

2. Exploring the Benefits of Differentially Private Pre-training and Parameter-Efficient Fine-tuning for Table Transformer
Mar 2023 - July 2023, Advisor: **Pin-Yu Chen**, Principal Research Scientist, IBM Research AI; MIT-IBM Watson AI Lab

- Implemented various kinds of parameter-efficient techniques in the fine-tuning stage instead of full tuning.
- We study the use of DP-SGD for both pre-training and fine-tuning, thus ensuring end-to-end privacy.
- Experiments show that parameter efficiency improves by over **97.86%**, with accuracy surpassing baselines in most cases.

Submitted to IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2024

3. DFLGuard: Robust and Communication-efficient Decentralized Federated Learning Sept 2022 - Feb 2023

Advisor: **Neil Gong**, Assistant Professor, Duke University

- Proposed DFLGuard, the first DFL method that is both robust and communication efficient.
- Proposed RAR-based communication architectures to efficiently implement robust aggregation rules.
- Showed the robustness and communication efficiency of DFLGuard both theoretically and empirically.

Submitted to IEEE Transactions on Dependable and Secure Computing (TDSC)

4. ICStega: Image Captioning-based Semantically Controllable Linguistic Steganography May 2022 - Aug 2022

Advisor: **Weiming Zhang**, Professor, USTC

- Created a new scenario for linguistic steganography, where the secret messages are embedded into the image-text pairs.
- Unlike previous approaches, the stego text generated by us is semantically controllable.
- Proposed an optimized sampling strategy, which balances the trade-off between accuracy and diversity.

Published a paper on IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2023

5. Social Bot-based Linguistic Steganography May 2021 - May 2022

Undergraduate Innovation and Entrepreneurship Training Program, USTC

Advisor: Prof. **Weiming Zhang**, Professor, USTC

Leader of the research group

- Created a social bot that automates tweeting, retweeting, liking, and commenting, closely mimicking real users.
- Introduced an automatic steganography system using social bots, saving significant time compared to manual methods.
- Disguised our social bot as a news summarizer, thus enhancing behavioral security.

Was awarded as National Chiefly Supported Program (highest award)

Honors

1. Outstanding Student Scholarship, Golden award **(top 5%)** Oct 2020
2. Outstanding Student Scholarship, Golden award **(top 5%)** Oct 2021
3. National College Student Imformation Security Contest, second prize Aug 2022
4. Chinese Mathematics Competitions, second prize in Anhui Province Oct 2020

Presentation

ICStega: Image Captioning-based Semantically Controllable Linguistic Steganography June 2023

ICASSP 2023, Video Presentation, Rhodes Island, Greece

Teaching

Teaching Assistant 2023 Spring

221006 - Design and Practice of Information Security II

Skills

Programming languages: C++, C, Python, Java, MATLAB **Web Technologies:** HTML, CSS, Django, JavaScript

ML/AI: Pytorch, Tensorflow, MXNet, Transformers **Miscellaneous:** MySQL, Linux, Git, Latex, Markdown

English: TOEFL: 102 (R: 28; L: 27; S: 23; W: 24)

Extracurricular Activities & Interests

1. USTC EEIS department Football Team Sept 2019 - Present
   - Won the 2nd place in the USTC Champions League.
2. Purdue Chinese Football Club Sep 2023 - Present