

EDUCATION

- **Old Dominion University** Norfolk, VA, USA
Ph.D. in Computer Science Jan. 2023 – present
- **Harbin University of Science and Technology** Harbin, China
M.Eng in Electrical Engineering Sep. 2018 – Dec. 2021
- **Harbin University of Science and Technology** Harbin, China
BSc. in Electrical Engineering and Automation Sep. 2013 – Jul. 2017

RESEARCH EXPERIENCE

- **Old Dominion University** Norfolk, VA, USA
Graduate Research Assistant Jan. 2023 – Present
 - **AI Security:** Conducted research on adversarial attacks including bit-flip and backdoor attacks on neural networks. Results provide insights into reliability and trustworthiness of modern AI systems.
 - **Cybersecurity Education:** Contributed to T3-CIDERS project, developing instructional materials and leading training sessions in cybersecurity and data-enabled research.
- **Artificial Intelligence and Digital Economy Laboratory** Shenzhen, China
Software Developer Apr. 2022 – Nov. 2022
 - **Software Development:** Designed and implemented controller and data processing software for robotics platforms. Focused on reliable communication and modular system design.
- **Southern University of Science and Technology** Shenzhen, China
Research Assistant Jan. 2021 – Mar. 2022
 - **Data Analysis:** Collected and analyzed disaster event datasets using statistical and computational methods.
- **Xi'an Baimu Educational Technology Co., Ltd.** Xi'an, China
Physics Teacher Jan. 2018 – Sep. 2018

PUBLICATIONS

Yao Wang, **Chunyu Hu**, Jian Li, Rui Ning, Lusi Li, Daniel Takabi. Contrastive Multi-Hop Semantic Communication. *Proceedings of the IEEE Military Communications Conference (MILCOM)*, accepted (to appear), 2025.

Chunyu Hu, Rui Ning. Chunyu Hu, Rui Ning. Targeted Bit Flip Attack on Binary Neural Networks. *International Conference on Computing, Networking and Communications (ICNC)*, in preparation, 2026.

Yide Zhang, Changyu Hu, Chunyu Hu. Airplane Detection in Remote Sensing Images Using CNN. *Optoelectronic Technology*, vol. 37, pp. 66–71, 2017.

SELECTED PROJECTS

- **Bitflip Attack on Binary Neural Networks (BNN) 2025**
Analyzed vulnerabilities of BNNs under hardware-level bit perturbations. Work highlights importance of robustness against low-level faults.
Technologies: Python, PyTorch, Optimization
- **Backdoor Attack Robustness on Long-Tail Datasets 2025**
Explored limitations of backdoor triggers under real-world imbalanced datasets.
Technologies: Adversarial ML, Data Augmentation
- **Efficiency of BitNet on Heterogeneous Hardware 2024**
Benchmarked a compact LLM on different devices, studying efficiency-performance trade-offs.
Technologies: Model Compression, Neural Network Quantization
- **Linux-based Electric Energy Terminal 2022**
Developed software for energy data acquisition terminal, supporting multiple communication protocols (GPRS, Ethernet, RS485, RS232). Implemented process management, data storage, and integrity checks.
Technologies: C/C++, SQLite, Multi-threading, System Programming

- **Qt-based Electric Energy Client 2021–2023**

Designed client software for monitoring substations and power plants. Supported time-sharing collection and automated reporting.

Technologies: Qt, TCP/IP, SQLite

SKILLS

- **Programming:** Python, C, C++

- **Frameworks:** PyTorch, TensorFlow, Qt