Chunyu Hu
PhD Student in Cybersecurity & AI Security | Old Dominion University
Email: chu034@odu.edu
Phone: 757-235-7070

Education

- **Old Dominion University** — Norfolk, VA, USA
  Ph.D. in Computer Science (focus: AI Security) — *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
  B.Sc. in Electrical Engineering and Automation — *Sep. 2013 – Jul. 2017*

Research Experience

- **Old Dominion University** — Norfolk, VA, USA
  Graduate Research Assistant — *Jan. 2023 – Present*
  - **Adversarial Machine Learning**: Conduct research on model robustness and attack surfaces, including bitflip and backdoor attacks.
  - **AI Security**: Explored vulnerabilities of Binary Neural Networks (BNN) to bit-level perturbations and robustness of backdoor attacks under imbalanced datasets.
  - **Model Efficiency**: Benchmarked large language model compression (BitNet) across heterogeneous devices, analyzing trade-offs between efficiency and accuracy.
  - **Curriculum Development**: Developed instructional materials for AI and cybersecurity courses under NSF-funded T3-CIDERS program.
- **Southern University of Science and Technology** — Shenzhen, China
  Research Assistant — *Jan. 2021 – Mar. 2022*
  - **Data Analysis**: Collected and analyzed disaster event data using network science for resilience modeling.
- **Artificial Intelligence and Digital Economy Laboratory** — Shenzhen, China
  Software Developer — *Apr. 2022 – Nov. 2022*
  - **Robotics Software**: Designed and implemented controller software for robotics platforms.

Selected Projects

- **Targeted Bitflip Attack on Binary Neural Networks (BNN)** (2025)
  Investigated BNN vulnerabilities to optimization-based bit-level perturbations; identified critical parameters affecting accuracy. *Technologies: Optimization Theory, Robustness Analysis*
- **Backdoor Attack Robustness on Imbalanced Long-Tail Datasets** (2025)
  Studied success rates of backdoor poisoning under data imbalance and augmentation. Results showed significant reduction in attack success under realistic settings. *Technologies: Adversarial ML, Data Augmentation*
- **Efficiency and Effectiveness Exploration of BitNet** (2024)
  Benchmarked compressed LLMs across diverse hardware, identifying trade-offs in efficiency and accuracy. *Technologies: Model Compression, Edge AI Benchmarking*
- **Curriculum Development for T3-CIDERS Project** (2023–2025)
  Contributed to NSF-funded program on integrating cyberinfrastructure with cybersecurity education. Created training materials and served as instructor.

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.