Binhao Ma

binhaoma98@gmail.com github

EDUCATION

South-Central Minzu University **Sep. 2021 – Jul. 2024**
Master of Computer Science and Technology *GPA:3.87/4.00*

Zhejiang Yuexiu University **Sep. 2016 - Jul. 2020**
Bachelor of Electronic Commerce *GPA:3.3/4.00*

SPECIAL AREAS

- AI Security
- Deep Learning
- Data Security
- Backdoor Attack

HONORS & AWARDS

- National Scholarship, China 2023
- Outstanding Graduate Student, South-Central Minzu University 2023
- First-class scholarship, South-Central Minzu University 2023
- Third-class scholarship, South-Central Minzu University 2022
- Second-class scholarship, South-Central Minzu University 2021
- Government Scholarship, Zhejiang Province, China 2018, 2019

RESEARCH EXPERIENCE

Backdoor Attack Defense **May 2022 – Oct. 2023**
Advisor: Prof. Bo Meng

- Propose a multidomain active defense method composed of a mutual information (MI) generation module and ALL-to-ALL decoupling training to detect backdoor poisoned samples from multidomain datasets without using clean datasets.
- Demonstrate the advantages over other active and passive defense methods by extensively evaluating MNIST & MNIST-M, MNIST & USPS & MNIST-M, MNIST & USPS & SVHN, CIFAR10 & Tiny-ImageNet against various backdoor attacks.

Backdoor Attacks **Sep. 2022 – May 2023**
Advisor: Prof. Bo Meng

- Propose the DIT algorithm. The dynamic invisible trigger algorithm determines neural network decision boundaries, and generates natural images that neural networks tend to predict incorrectly.
- Propose DIHBA. Dynamic Invisible and High attack success rate with low poison ratio Boundaries Backdoor Attack, in which we use the decision boundary images generated by DIT as trigger images.
- Demonstrate the effectiveness of DIHBA in attacking networks with varying precision, as it can bypass the Strip and Neural Cleanse defense systems.
- To further enhance the effectiveness of dirty-label backdoor attacks, a more advanced proposal of clean-label attack is introduced that requires only knowledge of the target class for attack and does not rely on any training data information. Additionally, I propose two methods for injecting triggers.

JOURNAL PUBLICATIONS

- **Multidomain active defense: Detecting multidomain backdoor poisoned samples via ALL-to-ALL decoupling training without clean datasets**
  Binhao Ma, Jiahui Wang, Dejun Wang, Bo Meng*
  Neural Networks(JCR Q1, IF:7.8), 2023

- **DIHBA: Dynamic, invisible and high attack success rate boundary backdoor attack with low poison ratio**
  Binhao Ma, Can Zhao, Dejun Wang, Bo Meng*
  Computers & Security(JCR Q1, IF:5.6), 2023

- **A secure and decentralized SSI authentication protocol with privacy protection and fine-grained access control based on federated blockchain**
  Binhao Ma, Xurui Zheng,Can Zhao,Yibing Wang,Dejun Wang,Bo Meng*
  Plos one(JCR Q2, IF:3.7), 2022

- **A Non-injected Traffic Backdoor Attack on Deep Neural Network**
  Jiahui Wang, Jie Yang, **Binhao Ma**, Dejun Wang, Bo Meng*
  International Journal of Network Security(EI), 2023

- **Survey on Cross-Chain Protocols of Blockchain**
  Bo Meng*, Yibing Wang, Can Zhao, Dejun Wang, **Binhao Ma**
  Journal of Frontiers of Computer Science & Technology(CSCD), 2022

MANUSCRIPTS

- **Poison Dart Frog: A Clean-Label Attack with Low Poisoning Rate and High Attack Success Rate in the Absence of Training Data**
  Binhao Ma, Jiahui Wang, Dejun Wang, Bo Meng*
  Arxiv, 2023, [**code**] (USENIX Security'24 Fall 1st under review)

CHINESE PATENTS

- A Traffic Sign Recognition System and Method with Encoding and Decoding Anti-Interference Neural Network
  Bo Meng, **Binhao Ma**, Dejun Wang, Jun Wang

- One Multistyle Handwritten English Image Label Recognition System and Method
  Bo Meng, **Binhao Ma**, Dejun Wang, Jun Qing

- A Handwritten Digit Recognition System and Method Based on Anti-Interference Convolutional Neural Network
  Bo Meng, **Binhao Ma**, Dejun Wang, Jun Wang

FUNDING

- A Traffic Sign Recognition Algorithm Based on Anti-Interference Convolutional Neural Network **2023 – 2024**
  Binhao Ma, Jiahui Wang, Xiaolei Tian
  Graduate Innvation Fund, No. 3212023sycxjj162, South-Central Minzu University

TECHNICAL SKILLS

Languages: Python, Java, C, HTML/CSS, JavaScript, SQL
Technologies/Frameworks: Tensorflow, Pytorch, Numpy

SERVICE

Journal Reviewer:

- CMC-Computers, Materials & Continua
- Journal of Cyber Security

LANGUAGE

TOEFL: Preparing for the TOEFL, I will meet the requirements.