LIANG TONG

ltong@nec-labs.com
https://liangtong.info/

RESEARCH INTERESTS

Much of my work lies at the intersection of machine learning (ML), artificial intelligence (AI), and security, with the goal of building trustworthy machine learning systems in various domains such as computer vision, anomaly detection, and malware classification. More specifically, I am interested in using machine learning in security applications and improving robustness of machine learning models themselves. I have also worked on mobile cloud computing, in which I designed edge architectures and transmission schemes for AI applications.

EDUCATION

Washington University in St. Louis *September 2018 - May 2021*
Ph.D. in Computer Science
Advisor: Yevgeniy Vorobeychik
Thesis: *Towards Deploying Robust Machine Learning Systems*

Vanderbilt University *June 2016 - August 2018*
M.S. in Computer Science
Advisor: Yevgeniy Vorobeychik

University of Electronic Science and Technology of China *September 2007 - June 2014*
M.Eng. & B.Eng. in Communication Engineering

National Taiwan University of Science and Technology *February 2010 - July 2010*
Exchange student in Electrical Engineering and Computer Science

RESEARCH & PROFESSIONAL EXPERIENCE

NEC Laboratories America, Inc. *February 2021 - Present*
Research Staff Member *Princeton, NJ*

- Conducted research on trustworthy machine learning systems.
- Developed a time-series analytical framework for robust quality parameter estimation in NEC's optical networks.

NEC Laboratories America, Inc. *May 2020 - August 2020*
Research Intern *Princeton, NJ*

- Worked with Dr. Zach Chen and Dr. Haifeng Chen on reliable face recognition.
- Developed FaceSec, a robustness assessment and enhancement framework for face recognition systems in adversarial settings.

Washington University in St. Louis *September 2018 - January 2021*
Research Assistant *St. Louis, MO*

- Member of WashU Computational Economic Research Lab directed by Prof. Yevgeniy Vorobeychik.
- Conducted research at the intersection of adversarial machine learning, security, and game theory.

Vanderbilt University *June 2016 - August 2018*
Research Assistant *Nashville, TN*

· Worked with Prof. Yevgeniy Vorobeychik on robust decentralized learning ecosystems.
· Developed a game-theoretic method for securing a collection of machine learning models simultaneously.

University of Tennessee *August 2014 - April 2016*
Research Assistant *Knoxville, TN*

· Worked with Prof. Wei Gao on designing edge cloud for mobile computing.
· Developed a hierarchical architecture for mobile cloud computing and a traffic scheduling method for mobile applications that offload computation to the edge cloud.

University of Electronic Science and Technology of China *September 2011 - June 2014*
Research Assistant *Chengdu, China*

· Worked with Prof. Lixiang Ma on cooperative wireless networking for autonomous cars.
· Developed a content downloading and sharing protocol for vehicular ad hoc networks.

PUBLICATIONS

1. **Liang Tong**, Zhengzhang Chen, Jingchao Ni, Wei Cheng, Dongjin Song, Haifeng Chen, Yevgeniy Vorobeychik. FACESEC: A Fine-grained Robustness Evaluation Framework for Face Recognition Systems. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021.
2. Tong Wu, **Liang Tong**, Yevgeniy Vorobeychik. Defending Against Physically Realizable Attacks on Image Classification. In *International Conference on Learning Representations (ICLR)*, 2020. **Spotlight Presentation**.
3. **Liang Tong**, Aron Laszka, Chao Yan, Ning Zhang, Yevgeniy Vorobeychik. Finding Needles in a Moving Haystack: Prioritizing Alerts with Adversarial Reinforcement Learning. In *AAAI Conference on Artificial Intelligence (AAAI)*, 2020.
4. **Liang Tong**, Bo Li, Chan Hajaj, Chaowei Xiao, Ning Zhang, Yevgeniy Vorobeychik. Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features. In *USENIX Security Symposium (Security)*, 2019.
5. **Liang Tong***, Sixie Yu*, Scott Alfeld, Yevgeniy Vorobeychik. Adversarial Regression with Multiple Learners. In *International Conference on Machine Learning (ICML)*, 2018.
6. **Liang Tong**, Wei Gao. Application-Aware Traffic Scheduling for Workload Offloading in Mobile Clouds. In *IEEE Conference on Computer Communications (INFOCOM)*, 2016. **Best Presentation in Session**.
7. **Liang Tong**, Yong Li, Wei Gao. A Hierarchical Edge Cloud Architecture for Mobile Computing. In *IEEE Conference on Computer Communications (INFOCOM)*, 2016.
8. Changyue Liu, Supeng Leng, Kun Yang, **Liang Tong**, Ke Zhang. A Cooperative Pricing Based Access Selection Mechanism for Vehicular Heterogeneous Networks. In *International Conference on Communications and Networking in China (ChinaCom)*, 2014.
9. **Liang Tong**, Lixiang Ma, Longjiang Li, Mao Li. A Coalitional Game Theoretical Model for Content Downloading in Multihop VANETs. In *IEEE Conference on Dependable, Autonomic and Secure Computing (DASC)*, 2013.
10. Mao Li, Tigang Jiang, **Liang Tong**. Spectrum Handoff Scheme for Prioritized Multimedia Services in Cognitive Radio Network with Finite Buffer. In *IEEE Conference on Dependable, Autonomic and Secure Computing (DASC)*, Dec. 2013.

PREPRINTS

1. **Liang Tong**, Minzhe Guo, Atul Brakash, Yevgeniy Vorobeychik. Defending Against Non-Salient Adversarial Examples in Image Classification. In *arXiv Preprint*, 2021.

PATENTS

1. Yevgeniy Vorobeychik, Tong Wu, **Liang Tong**. Systems and Methods for Defending against Physical Attacks on Image Classification. US Patent App. 17/214,071, 2021.

INTERNS

- Nauman Ahad (Georgia Institute of Technology). Summer 2021.

REVIEWING

- *Journals*
  - IEEE Transactions on Dependable and Secure Computing
  - IEEE Transactions on Big Data
  - Artificial Intelligence Review
- *Conferences*
  - ACM Workshop on Artificial Intelligence and Security (AISec'17)
  - Workshop on the Security and Privacy of Machine Learning (SPML'19)
  - International Conference on Autonomous Agents and Multiagent Systems (AMMAS'20, '22)
  - International Conference on Computer Vision (ICCV'21)
  - ACM International Conference on Information and Knowledge Management (CIKM'21)
  - ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'21)
  - International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR'21)
  - AAAI Conference on Artificial Intelligence (AAAI'21,'22)
  - AAAI Workshop on Artificial Intelligence for Cyber Security (AICS'22)
  - AAAI WOrkshop on Trustworthy Autonomous Systems Engineering (TRASE'22)
  - ACM International Conference on Web Search and Data Mining (WSDM'22)
  - IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR'22)

INVITED TALKS

- Adversarial AI: from Models to Practice. NEC Laboratories America. October 2020.
- FACESEC: A Fine-grained Robustness Assessment and Enhancement Framework for Face Recognition Systems. NEC Laboratories America. August 2020.

TEACHING EXPERIENCE

- Teaching Assistant of CSE 411A AI and Society (Fall 2019), Washington University in St. Louis.
- Teaching Assistant of CSE 544T Special Topics in Computer Science Theory - Adversarial AI (Spring 2019), Washington University in St. Louis.

- Co-Instructor of CS 102 Introduction to Computer Science (Spring 2015), University of Tennessee
- Teaching Assistant of CS 160 Computer Organization (Fall 2014), University of Tennessee
- Teaching Assistant of Access Network Technology (Spring 2011), University of Electronic Science and Technology of China

HONORS & AWARDS

- AAAI Student Scholarship, 2020
- USENIX Security Student Grant, 2019
- INFOCOM Student Travel Award, 2016
- INFOCOM Best Presentation in Session, 2016
- EECS Department Excellence Fellowship, University of Tennessee, 2014
- The Third Prize in Southwestern China ACM Programming Contest for College Students, 2012
- UESTC First Class Scholarship for Overall Excellence, 2011
- The Second-Class People's Scholarship of UESTC, 2010, 2009, 2008

SKILLS

Python: Numpy, Tensorflow, PyTorch. C/C++. Java. Matlab