Liang Tong

Washington University in St. Louis

(+865)309-9371
liangtong@wustl.edu
www.liang-tong.me

Research Interests

Machine learning (ML), Security, Artificial Intelligence (AI). Specifically, I have strong interests in design, analysis and implementation of robust machine learning systems, as well as their applications in security and computer vision.

Education

2018–2021 (expected) **Washington University in St. Louis**.
Ph.D. student in Computer Science
Advisor: Prof. Yevgeniy Vorobeychik

2016–2018 **Vanderbilt University**.
Ph.D. student in Computer Science (transferred to Washington University in St. Louis)
M.S. in Computer Science
Advisor: Prof. Yevgeniy Vorobeychik

2011–2014 **University of Electronic Science and Technology of China**.
M.Eng. in Electronic and Communication Engineering

2007–2011 **University of Electronic Science and Technology of China**.
B.S. in Communication Engineering

2010 **National Taiwan University of Science and Technology**.
Exchange student in Computer Science

Research Experience

2018– **Adversarial Machine Learning in Detection Systems**.
Washington University in St. Louis
Advisor: Prof. Yevgeniy Vorobeychik
Publication: ICLR'20 [1], AAAI'20 [2], USENIX Security'19 [3]

2016–2018 **Robust Multi-agent Learning**.
Vanderbilt University
Advisor: Prof. Yevgeniy Vorobeychik
Publication: ICML'18 [4]

2014–2016 **Designing Edge Cloud for Mobile Computing**.
University of Tennessee, Knoxville
Advisor: Prof. Wei Gao
Publication: INFOCOM'16 [5], INFOCOM'16 [6]

2011–2014 **Designing Cooperative Wireless Networks**.
UESTC, China
Advisor: Prof. Lixiang Ma
Publication: ChinaCom'14 [7], DASC'13 [8], DASC'13 [9]

Publications

[1] Tong Wu, **Liang Tong**, and Yevgeniy Vorobeychik. *Defending Against Physically Realizable Attacks on Image Classification*, In Proceedings of the 8th International Conference on Learning Representations (ICLR), May 2020, to appear. (**Spotlight**)

[2] **Liang Tong**, Aron Laszka, Chao Yan, Ning Zhang, and Yevgeniy Vorobeychik, *Finding Needles in a Moving Haystack: Prioritizing Alerts with Adversarial Reinforcement Learning*, in Proceedings of the 34th AAAI Conference on Artificial Intelligence (AAAI), Feb. 2020, to appear.

[3] **Liang Tong**, Bo Li, Chan Hajaj, Chaowei Xiao, Ning Zhang, and Yevgeniy Vorobeychik, *Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features*, in Proceedings of the 28th USENIX Security Symposium (Security), Aug. 2019.

[4] **Liang Tong***, Sixie Yu*, Scott Alfeld, and Yevgeniy Vorobeychik, *Adversarial Regression with Multiple Learners*, in Proceedings of the 35th International Conference on Machine Learning (ICML), July 2018. (* indicates equal contributions)

[5] **Liang Tong**, Yong Li, and Wei Gao, *A Hierarchical Edge Cloud Architecture for Mobile Computing*, in Proceedings of the 35th IEEE Conference on Computer Communications (INFOCOM), April 2016.

[6] **Liang Tong** and Wei Gao, *Application-Aware Traffic Scheduling for Workload Offloading in Mobile Clouds*, in Proceedings of the 35th IEEE Conference on Computer Communications (INFOCOM), April 2016. (**Best Presentation in Session**)

[7] Changyue Liu, Supeng Leng, Kun Yang, **Liang Tong**, and Ke Zhang, *A Cooperative Pricing Based Access Selection Mechanism for Vehicular Heterogeneous Networks*, in Proceedings of the 9th International Conference on Communications and Networking in China (ChinaCom), Aug. 2014.

[8] **Liang Tong**, Lixiang Ma, Longjiang Li, and Mao Li, *A Coalitional Game Theoretical Model for Content Downloading in Multihop VANETs*, in Proceedings of the 11th IEEE Conference on Dependable, Autonomic and Secure Computing (DASC), Dec. 2013.

[9] Mao Li, Tigang Jiang, and **Liang Tong**, *Spectrum Handoff Scheme for Prioritized Multimedia Services in Cognitive Radio Network with Finite Buffer*, in Proceedings of the 11th IEEE Conference on Dependable, Autonomic and Secure Computing (DASC), Dec. 2013.

Honors & Awards

2020 AAAI Student Scholarship

2019 USENIX Security Student Grant

2016 INFOCOM Student Travel Award, Best Presentation in Session

2011 UESTC First Class Scholarship for Overall Excellence

Professional Activities

Talks *Improving Robustness of ML Classifiers against Realizable Evasion Attacks Using Conserved Features*, 28th USENIX Security Symposium (Security), Aug. 2019, Santa Clara, CA, USA.

A Hierarchical Edge Cloud Architecture for Mobile Computing, 35th IEEE Conference on Computer Communications (INFOCOM), April 2016, San Francisco, CA, USA.

Application-Aware Traffic Scheduling for Workload Offloading in Mobile Clouds, 35th IEEE Conference on Computer Communications (INFOCOM), April 2016, San Francisco, CA, USA.

A Coalitional Game Theoretical Model for Content Downloading in Multihop VANETs, 11th IEEE Conference on Dependable, Autonomic and Secure Computing (DASC), Dec. 2013, Chengdu, China.

Reviews IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Wireless Communication, IEEE Transactions on Vehicular Technology, Artificial Intelligence Review, AAMAS, ICML workshop on the Security and Privacy of Machine Learning, ACM AISec, IEEE CSF, IEEE ICC, IEEE INFOCOM.

Teaching

Fall 2019 *Curriculum Developer* for CSE 411A AI and Society at Washington University in St. Louis.

Spring 2018 *Teaching Assistant* and *Curriculum Developer* for CSE 544T Special Topics in Computer Science Theory (Adversarial AI) at Washington University in St. Louis.

Spring 2015 *Course Instructor* for CS 102 Introduction to Computer Science at University of Tennessee, Knoxville.

Skills

Python, PyTorch, Tensorflow, C++/C, Linux.

References

Yevgeniy Vorobeychik
Associate Professor
Computer Science and Engineering Dept.
Washington University in St. Louis
✉ yvorobeychik@wustl.edu

Bo Li
Assistant Professor
Computer Science Dept.
University of Illinois at Urbana-Champaign
✉ lbo@illinois.edu

Ning Zhang
Assistant Professor
Computer Science and Engineering Dept.
Washington University in St. Louis
✉ zhang.ning@wustl.edu