

Fnu Suya

85 Engineer's Way, Charlottesville, Virginia 22903, USA
fs5xz@virginia.edu • +1 (213) 590-6118 • <https://fsuya.org>

EDUCATION

- PhD Candidate, Department of Computer Science, University of Virginia** Aug 2017 – PRESENT
- Adviser: Prof. David Evans, Prof. Yuan Tian
 - Focus: Security and Privacy in Machine Learning
- PhD Student, Department of Computer Science, Arizona State University** Aug 2015 – May 2017
- Adviser: Prof. Guoliang Xue, Prof. Paolo Papotti
 - Focus: Game Theory and Incentive Mechanism Design, Privacy in Machine Learning
- BEng, Department of Electronic Engineering, China Agricultural University**
- Honors Program (most selective program) Aug 2010 – Jul 2014

RESEARCH EXPERIENCE

- Department of Computer Science, University of Virginia**
- Graduate Research Assistant* Aug 2017 – PRESENT
- Designed hybrid batch attack against DNN models in limited query setting and outperforms state-of-the-art black-box attacks significantly in terms of query efficiency.
 - Designed query efficient black-box attacks to ML classifiers based on Bayesian optimization.
- Department of Computer Science, Arizona State University**
- Graduate Research Assistant* Aug 2015 – May 2017
- Designed user profile obfuscation strategy based on Bayesian optimization to protect user privacy in black-box setting.
 - Designed optimal wireless transmission strategy in the presence of malicious adversaries from a Stackelberg game perspective.
 - Worked on designing truthful auction mechanism under sybil attack for radio spectrum allocation.
- Department of Electronic Engineering, Tsinghua University**
- Undergraduate Researcher* Aug 2014 – Feb 2015
- Designed an efficient transmission strategy for Cloud-RAN network with optimality guarantees under probabilistic quality-of-service constraints with imperfect channel state information.

PUBLICATIONS

- **Fnu Suya***, Saeed Mahloujifar*, David Evans, Yuan Tian “**Model-Targeted Poisoning Attacks: Provable Convergence and Certified Bounds**”, *Preprint*
- Jihong Wang, Minnan Luo, **Fnu Suya**, Jundong Li, Zijiang Yang, Qinghua Zheng “**Scalable Attack on Graph Data by Injecting Vicious Nodes**”, *The European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2020)*
- **Fnu Suya**, Jianfeng Chi, David Evans, Yuan Tian, “**Hybrid Batch Attacks: Finding Black-box Adversarial Examples with Limited Queries**”, *29th USENIX Security Symposium (Usenix Security 2020)*
- Yi Chen, Mingming Zha, Nan Zhang, Dandan Xu, Qianqian Zhao, Xuan Feng, Kan Yuan, **Fnu Suya**, Yuan Tian, Kai Chen, XiaoFeng Wang, Wei Zou, “**Demystifying Hidden Privacy Settings in Mobile Apps**”, *40th IEEE Symposium on Security and Privacy (Oakland 2019)*
- **Fnu Suya**, David Evans, Yuan Tian, “**Poster: Adversaries Don’t Care About Averages: Batch Attacks on Black-Box Classifiers**”, *39th IEEE Symposium on Security and Privacy (Oakland 2018)*
- **Fnu Suya**, Yuan Tian, David Evans, Paolo Papotti, “**Qury-limited Black Box Attacks to Classifiers**”, *NIPS Workshop on Machine Learning and Computer Security 2017*
- **Fnu Suya**, Yuanming Shi, Bo Bai, Wei Chen, Jun Zhang, Khaled B. Letaief, and Shidong Zhou, “**Optimal Stochastic Power Control with Compressive CSI Acquisition for Cloud-RAN**”, *IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2016*

| | | |
|----------------------------------|---|-------------|
| AWARDS & SCHOLARSHIPS | ▪ CS Graduate Research Award, University of Virginia | 2018 |
| | ▪ CS Department Fellowship, University of Virginia | 2017 |
| | ▪ NSF Travel Grant, GlobalSIP 2016 | 2016 |
| | ▪ CIDSE Doctoral Fellowship, Arizona State University | 2015 |
| | ▪ Excellent Student's Scholarship, China Agricultural University | 2011 – 2013 |
| TECHNICAL SKILLS | <ul style="list-style-type: none"> ▪ Proficient with TensorFlow, Python, Matlab, \LaTeX ▪ Familiar with PyTorch, C, C++, Shell script | |
| TEACHING EXPERIENCE | <ul style="list-style-type: none"> ▪ Teaching Assistant at University of Virginia <ul style="list-style-type: none"> • CS 6501: Learning Theory • CS 6501: Cryptography ▪ Teaching Assistant at Arizona State University <ul style="list-style-type: none"> • CSE 556: Game Theory • CSE 100: Introduction to C++ Programming • CSE 240: Introduction to Programming Languages | |
| ACADEMIC SERVICE | <ul style="list-style-type: none"> ▪ Journal Reviewer: China Communications ▪ External Reviewer: IEEE S&P, Usenix Security, NDSS, CCS, ASIACCS, NeurIPS, AAAI, SIGMOD, DASFAA, MobiHoc | |
| LANGUAGES | Mongolian (Native), Chinese (Proficient), English (Proficient) | |
| REFERENCES | Available Upon Request | |