

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
	<ul style="list-style-type: none">▪ 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
RESEARCH EXPERIENCE	<ul style="list-style-type: none">▪ 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	
	<i>Graduate Research Assistant</i>	Aug 2017 – PRESENT
	<ul style="list-style-type: none">• 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.	
RESEARCH EXPERIENCE	Department of Computer Science, Arizona State University	
	<i>Graduate Research Assistant</i>	Aug 2015 – May 2017
	<ul style="list-style-type: none">• 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.	
RESEARCH EXPERIENCE	Department of Electronic Engineering, Tsinghua University	
	<i>Undergraduate Researcher</i>	Aug 2014 – Feb 2015
	<ul style="list-style-type: none">• Designed an efficient transmission strategy for Cloud-RAN network with optimality guarantees under probabilistic quality-of-service constraints with imperfect channel state information.	
PUBLICATIONS	<ul style="list-style-type: none">▪ Jihong Wang, Minnan Luo, Fnu Suya, Jundong Li, Zijiang Yang, Qinghua Zheng “Attack on Graph Data by Injecting Vicious Nodes”, <i>Preprint</i>▪ Fnu Suya, Jianfeng Chi, David Evans, Yuan Tian, “Hybrid Batch Attacks: Finding Black-box Adversarial Examples with Limited Queries”, <i>29th USENIX Security Symposium (Usenix Security 2020)</i>▪ 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”, <i>40th IEEE Symposium on Security and Privacy (Oakland 2019)</i>▪ Fnu Suya, David Evans, Yuan Tian, “Poster: Adversaries Don’t Care About Averages: Batch Attacks on Black-Box Classifiers”, <i>39th IEEE Symposium on Security and Privacy (Oakland 2018)</i>▪ Fnu Suya, Yuan Tian, David Evans, Paolo Papotti, “Query-limited Black Box Attacks to Classifiers”, <i>NIPS Workshop on Machine Learning and Computer Security 2017</i>▪ 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”, <i>IEEE Global Conference on Signal and Information Processing (GlobalSIP) 2016</i>	
AWARDS & SCHOLARSHIPS	<ul style="list-style-type: none">▪ CS Graduate Research Award, University of Virginia	
	<ul style="list-style-type: none">▪ CS Department Fellowship, University of Virginia	

	<ul style="list-style-type: none"> ▪ NSF Travel Grant, GlobalSIP 2016 ▪ CIDSE Doctoral Fellowship, Arizona State University ▪ Excellent Student's Scholarship, China Agricultural University 	2016 2015 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, NIPS, AAAI, SIGMOD, DASFAA, MobiHoc 	
LANGUAGES	Mongolian (Native), Chinese (Proficient), English (Proficient)	
REFERENCES	Available Upon Request	