

SUYA, FNU

85 Engineer's Way · Charlottesville · VA 22904 · (213) 590-6118 · fs5xz@virginia.edu

RESEARCH INTEREST

My main research interest is in machine learning security. Specifically, I am interested in evaluating robustness of machine learning models by designing better attack strategies. I am also interested in protecting data privacy in machine learning systems.

EDUCATION

	2017–PRESENT · UNIVERSITY OF VIRGINIA
<i>PhD</i>	Computer Science · Department of Computer Science GPA: 4.00/4.00
	2015–2017 · ARIZONA STATE UNIVERSITY
<i>PhD</i>	Computer Science · School of Computing, Informatics, and Decision Systems Engineering GPA: 4.00/4.00
	2010–2014 · Honors Program · CHINA AGRICULTURAL UNIVERSITY (CAU)
<i>BE</i>	Electronic and Information Engineering track · College of Information and Electrical Engineering GPA: 3.65/4.00

AWARDS

2018	Computer Science Graduate Research Award · University of Virginia
2017	Computer Science Department Fellowship · University of Virginia
2016	NSF Travel Grant · GlobalSIP 2016
2015	CIDSE Doctoral Fellowship · Arizona State University
2011–2013	Excellent Student's Scholarship · China Agricultural University

ACADEMIC EXPERIENCE

<i>Research Assistant</i>	01/2018–PRESENT · UNIVERSITY OF VIRGINIA · Advisor: DAVID EVANS, YUAN TIAN <ul style="list-style-type: none">- Designed hybrid black-box attack, which combines gradient and transfer black-box attacks, and improves upon state-of-the-art black-box attacks significantly in terms of attack success rate and query complexity.- Studied the problem of improving query efficiency of hybrid attack in limited query setting and proposed efficient and effective seed prioritization strategies.
<i>Research Assistant</i>	09/2017–11/2017 · UNIVERSITY OF VIRGINIA · Advisor: DAVID EVANS, YUAN TIAN <ul style="list-style-type: none">- Studied black-box attacks to machine learning classifiers with API access and applied Bayesian optimization to design black-box attack strategy with significantly improved query efficiency.
<i>Research Assistant</i>	09/2016–05/2017 · ARIZONA STATE UNIVERSITY · Advisor: PAOLO PAPOTTI <ul style="list-style-type: none">- Worked on protecting user privacy in online platforms with query interaction. Applied Bayesian optimization strategy to modify user profiles (i.e., injecting carefully chosen noises) such that user profiles cannot be exactly identified by platform providers.
<i>Research Assistant</i>	08/2015–05/2016 · ARIZONA STATE UNIVERSITY · Advisor: GUOLIANG XUE <ul style="list-style-type: none">- Worked on designing truthful auction mechanism under sybil attack for radio spectrum allocation problem.- Worked on designing robust wireless transmission strategy in the presence of malicious adversaries from a Stackelberg game perspective.

Research
Intern

08/2014–02/2015 · TSINGHUA UNIVERSITY · Advisor: WEI CHEN

- Studied power minimization problem for Cloud-RAN network with probabilistic Quality-of-Service constraints in the existence of imperfect channel state information (CSI). Proposed a power control algorithm to find solutions with optimality guarantees with reduced CSI signalling overhead.

Research
Assistant

03/2013 - 10/2013 · CHINA AGRICULTURAL UNIVERSITY · Advisor: MINZAN LI

- Developed Master-Slave mode of greenhouse group management system based on programmable logic controller (PLC) and ZigBee wireless sensor network.
- Developed remote control software for greenhouse monitoring system.

PUBLICATIONS

Jihong Wang, Minnan Luo, **Fnu Suya**, Jundong Li, Zijiang Yang, Qinghua Zheng “Attack on Graph Data by Injecting Vicious Nodes”, *Under Submission*

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 Dont 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*

TECHNICAL SKILLS

Programming

TensorFlow, PyTorch, Python, Matlab, C, C++

Language

Mongolian (Native), Chinese, English

COURSES

CS6501 Natural Language Processing

CS6501 Learning Theory

CS 6161 Algorithms (UVa)

CSE 575 Statistical Machine Learning (ASU)

CSE 572 Data Mining (ASU)

CSE 691 (Topic) Advanced Topics in Social Media Analysis (ASU)

CSE 691 (Topic) Optimization with Engineering Applications

CSE 556 Game Theory (ASU)

CSE 539 Applied Cryptography (ASU)

CSE 100 Introduction to C++ Programming (ASU, TA)

CSE 240 Introduction to Programming Languages (ASU, TA)

CSE 556 Game Theory (ASU, TA)

SERVICES

Journal Reviewer: China Communications

External Reviewer: MobiHoc, SIGMOD, DASFAA, NIPS, AAAI, ASIACCS, IEEE S&P, Usenix Security, NDSS, CCS