



Scott Freitas

Currently a Ph.D. student at Georgia Tech, studying machine learning in the department of Computational Science and Engineering advised by Polo Chau.

Research interests include **machine learning** and large scale **graph mining**, with application to cybersecurity, healthcare and finance.

Recent awards include NSF Graduate Research Fellowship (2018) and Outstanding Computer Science Masters student at ASU (2018).

 scottfreitas.com
 safreita@gatech.edu
 Curriculum Vitae (PDF)

 Github
 LinkedIn

Education

- Present — **Ph.D. in Machine Learning**
Aug. 2018 Georgia Institute of Technology, Atlanta, GA
Advisor: Duen Horng (Polo) Chau
- May 2018 **M.S. in Computer Science**
Summer 2017 Arizona State University, Tempe, AZ
Advisor: Hanghang Tong, Thesis: "Mining Marked Nodes in Large Graphs"
Overall GPA: 4.00/4.00
- May 2017 — **B.S. in Computer Science**
Aug. 2015 Arizona State University, Tempe, AZ
Overall GPA: 3.98/4.00
- May 2014 — **B.S.E. in Electrical Engineering**
Aug. 2010 Arizona State University, Tempe, AZ
Overall GPA: 3.64/4.00

Honors and Awards

- 2019 Raytheon Research Fellowship
Awarded for my PhD work in adversarial machine learning
- 2018 — 2023 NSF Graduate Research Fellowship
National Science Foundation recognizes and supports outstanding graduate students in STEM fields
- 2018 Outstanding Computer Science Masters Student (ASU)
Awarded to single master student demonstrating exemplary performance
- 2017 Best Demo Award, Runner Up at CIKM '17
For "Rapid Analysis of Network Connectivity"
- 2017 CIKM Travel Grant
Funding from NSF and SIGWEB to present at CIKM
- 2016 — 2017 FURI Grant
Undergraduate research grant awarded for work in network connectivity
- 2016 — 2017 Arizona Graduate Scholar Award
Merit scholarship awarded to select number of master students

2010 — 2014 **Provost's Scholarship**
Merit scholarship awarded to select number of incoming undergraduate students

Industry Research Experience

- Summer 2019 **Microsoft**, Seattle, WA
Research Intern, Windows Defender: Advanced Threat Protection
Mentor: Andrew Wicker, Joshua Neil
Developed graph based approach to quantifying and mitigating vulnerability to adversarial attacks on networks
- Summer 2013 **Naval Air Warfare Center**, Point Mugu, California
Research Intern, Naval Research Enterprise Internship Program (NREIP)
Mentor: Balaji Iyer
Explored methods of preventing electromagnetic interference from coupling into superconducting receivers

Academic Research Experience

- Present — **Georgia Institute of Technology**, Atlanta, GA
Aug. 2018 *Graduate Research Assistant, School of Computational Science and Engineering*
Advisor: Duen Horng (Polo) Chau
Member of the Polo Club of Data Science where we innovate scalable, interactive, and interpretable tools that amplify human's ability to understand and interact with billion-scale data and machine learning models
- May 2018 — **Arizona State University**, Tempe, AZ
Summer 2017 *Graduate Research Assistant, School of Computing, Informatics, and Decision Systems Engineering*
Advisor: Hanghang Tong
Conducted research in graph based connectivity analysis to improve local graph partitioning. Developed web-based prototype for explainable ranking in complex multi-layered networks.
- Summer 2017 **Arizona State University**, Tempe, AZ
Summer Research Assistant, School of Computing, Informatics, and Decision Systems Engineering
Mentor: Ross Maciejewski
Developed interactive augmented reality (AR) graph models in the Microsoft HoloLens.
- May 2017 — **Arizona State University**, Tempe, AZ
Jan. 2016 *Undergraduate Research Assistant, School of Computing, Informatics, and Decision Systems Engineering*
Mentor: Hanghang Tong
Developed fast graph mining algorithms for network connectivity analysis, and award winning web platform for visualization and analysis.

Publications

Extracting Knowledge For Adversarial Detection and Defense in Deep Learning

Scott Freitas, Shang-Tse Chen, Duen Horng (Polo) Chau
KDD Workshop: Learning and Mining for Cybersecurity (LEMINGS). Anchorage, Alaska, 2019.
[Project](#) [PDF](#) [BibTeX](#)

Local Partition in Rich Graphs

Scott Freitas, Nan Cao, Yinglong Xia, Duen Horng (Polo) Chau, Hanghang Tong
IEEE International Conference on Big Data (Big Data). Seattle, Washington, 2018.
[Project](#) [Demo](#) [PDF](#) [BibTeX](#)

X-Rank: Explainable Ranking in Complex Multi-Layered Networks

Jian Kang*, Scott Freitas*, Haichao Yu, Yinglong Xia, Hanghang Tong
ACM International Conference on Information and Knowledge Management (CIKM). Turin, Italy, 2018.
[Project](#) [Demo](#) [PDF](#) [BibTeX](#) * Authors contributed equally

Rapid Analysis of Network Connectivity

Scott Freitas, Hanghang Tong, Nan Cao, Yinglong Xia

ACM International Conference on Information and Knowledge Management (CIKM). Singapore, 2017.

[Project](#) [Demo](#) [PDF](#) [Video](#) [Code](#) [BibTeX](#) [🏆 Best Paper, Runner up](#)

Talks

D²M: Dynamic Defense and Modeling of Adversarial Movement in Networks

Aug. 2019 Microsoft Advanced Threat Protection Research Expo

Mining Marked Nodes in Large Graphs

Dec. 2018 Microsoft Advanced Threat Protection Group

May 2018 ASU Thesis

Local Partition in Rich Graphs

Dec. 2018 IEEE International Conference on Big Data

Rapid Analysis of Network Connectivity

Nov. 2017 ACM International Conference on Information and Knowledge Management (CIKM)

Network Connectivity Analysis and Visualization in Large Graphs

April 2017 Keynote Speaker: ASU Fulton Undergraduate Research Initiative (FURI)

Nov. 2016 ASU FURI Research Symposium

Press

Feb. 2019 "Raytheon Awards Two ML@GT Students Graduate Research Assistantships",

July 2018 "NSF Graduate Research Fellow wants to use computer science to solve society's toughest problems",

Teaching

Fall 2013 Undergraduate Teaching Assistant

Arizona State University, Tempe, AZ

Fulton Undergraduate Research Experience (FSE 294), Instructor: Joshua Lyon

Designed and taught introductory lesson plans to new engineering students

Grants and Funding

2019 — 2023 Guaranteeing AI Robustness against Deception (GARD)

DARPA Research Grant

Co-PIs: Duen Horng (Polo) Chau, Jason Martin, Cory Cornelius

Funded: Project selected

Contributed adversarial defense technique

2018 Amazon AWS Research Grant

Adversarial Re-Training and Model Vaccination for Robust Deep Learning

Co-PIs: Nilaksh Das, Haekyu Park, Duen Horng (Polo) Chau

Funded: \$5,000 AWS cloud credits

2019 Raytheon Research Fellowship

Extracting Knowledge For Adversarial Detection and Defense

Funded: \$25,000

2018 — 2023 NSF Graduate Research Fellowship Program (GRFP)

Multi-level Interdiction and Assistance Modeling for Natural Disasters

Funded: Full tuition + \$102,000

2016 — 2017 **FURI Grant**

Network Connectivity Analysis and Visualization in Large Graphs

Funded: \$3,000

Technology Skills

OS: Ubuntu, Unix Command Line, Windows

Programming: Python, Matlab, Java, C#, C++

Web and Writing: .NET Core, ASP.NET, HTML, CSS, JavaScript, D3, Bootstrap, LaTeX, Git

Machine Learning: Keras, TFLearn, Pytorch, Tensorflow, SciPy, Numpy, OpenCV, Pandas, Scikit-learn, NetworkX

Service

Reviewer

ACM SIGKDD Conference on Knowledge Discovery and Data Mining (**KDD**) 2019

International Conference on Machine Learning (**ICML**) 2019