

Education

China University of Geosciences (Wuhan)
Bachelor degree in Information Security
GPA: 87.67/100;
GRE: V158 Q168 AW:3.5

WUHAN, CHINA
Sept. 2014 – Jun. 2018

University of British Columbia
Master of Applied Science in Electrical and Computer Engineering Sept. 2018 - May 2020 (Expected)
Supervisor: Karthik Pattabiraman
Research interest: Fault tolerance, security and privacy of machine learning

VANCOUVER, CANADA

Research Experience

Reliability of Machine Learning Systems

Graduate Research

Understanding the error resilience of ML systems

Presented in SC'19

- *Research question:* How to precisely identify the critical bits in ML systems due to hardware transient faults (i.e., bit-flip), to guide the design of error-resilient ML systems.
- *Key insight:* We analyze the mathematical properties of common ML systems, and find many of them exhibit monotonicity, which constraints the fault propagation behaviors.
- We design a binary-search like fault injector to identify critical bits in the system.
- *Results:* Our approach can efficiently identify 99%+ of critical bits with 99%+ precision.
- Code: <https://github.com/DependableSystemsLab/TensorFI-BinaryFI>

Enabling error-resilient ML systems

Manuscript in preperation

- *Research question:* How to enhance the error resilience of ML systems leveraging the unique characteristics of critical faults in ML systems.
- *Key insight:* We selectively apply range restriction on certain ML computations in the models, to limit the fault amplification, thus preventing the faults leading to erroneous outputs.
- Our approach can be integrated into existing model without retraining.
- *Results:* Our approach enabled significant resilience boosting and would not degrade the accuracy of the model.

Wearable Computing Security

Undergraduate Research

- Lightweight and real-time key establishment scheme for wearable embedded devices.
- Sensing user real-time motion to secure communication between on-body devices.
- Leveraging the inherent randomness of the sensory data as a secret for secure key generation.

Publications

- Zitao Chen, Guanpeng Li, Karthik Pattabiraman “Using Range Restriction to Enable Error-Resilient Machine Learning Systems”, **Manuscript in preperation**.
- [SC'19] Zitao Chen, Guanpeng Li, Karthik Pattabiraman, Nathan DeBardeleben “BinFI: An Efficient Fault Injector for Safety-Critical Machine Learning Systems”, *In Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, AR: 20.9% (72/344) direct acceptance rate for regular papers.*
- [FGCS] Zitao Chen, Wei Ren, Yi Ren and Kim-Kwang Raymond Choo, “LiReK: A Lightweight and Real-time Key Establishment Scheme for Wearable Embedded Devices by Gestures or Motions”, *Future Generation Computer Systems* (2018): 84, 126-138, [2018 Impact Factor: 5.768]

Others

Open-source project: <https://github.com/DependableSystemsLab/TensorFI>

Sept. 2018 - present

Programming languages: Python, Java, C, C++

Teaching Experience: CPEN400A

2019

Award: Graduate Student Initiative: \$4000

2019