Zitao Chen • zitaoc@ece.ubc.ca • +1-778-316-8835

Education

University of British Columbia — Vancouver, Canada
Master of Applied Science in Electrical and Computer Engineering *Sept. 2018 - May 2020* (Expected)
GPA: 82.8/100
Supervisor: Karthik Pattabiraman
Research interest: Fault tolerance, security and privacy of machine learning

China University of Geosciences (Wuhan) — Wuhan, China
Bachelor degree in Information Security *Sept. 2014 – Jun. 2018*
GPA: 87.67/100

Research Experience

Reliability of Machine Learning Systems — Graduate Research

Understanding the error resilience of ML systems *Presented in SC'19*

- *Research question:* How to efficiently identify the critical bits in ML systems due to hardware transient faults (i.e., bit-flip). These are the bits that could corrupt the ML's outputs, e.g., misclassification.
- *Key insight:* Analyze the mathematical properties of common ML computations, and find many of them exhibit monotone property, which constrains the fault propagation behavior.
- Design a binary-search like fault injector to identify critical bits in the system.
- *Results:* The approach can efficiently identify 99%+ of critical bits with 99%+ precision.
- Code: https://github.com/DependableSystemsLab/TensorFI-BinaryFI

Boosting the error resilience of ML systems *Manuscript under review*

- *Research question:* How to efficiently enhance the error resilience of ML systems.
- *Key insight:* Propose to selectively restrict the ranges of values in DNNs, which can dampen the large deviations (due to critical faults) into smaller ones. The reduced deviations can be tolerated by the inherent resilience of DNNs, i.e., the systems can still generate correct outputs.
- The proposed technique can be integrated into existing models without retraining.
- *Results:* The approach: 1) enables significant resilience boosting; 2) does not degrade the accuracy of the model; and 3) with low runtime overhead.

Wearable Computing Security — Undergraduate Research

- *Research question:* How to leverage the sensory signals from wearable devices for efficient authentication.
- *Insight:* Selectively exploit the sensory data (due to device vibration or hardware imprecision) for random key generation, without extra feature processing.
- *Result:* The approach enables lightweight and real-time random key generation for wearable devices.

Publications

- **[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*, 2019 **Acceptance rate: 20.9% (72/344) direct acceptance 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) [Impact Factor: 5.768]

Unpublished Manuscript

- Zitao Chen, Guanpeng Li, Karthik Pattabiraman"Boosting Error-Resilience of Deep Neural Networks through Range Restriction" **Manuscript under review and available upon request.**

Others

Open-source project: https://github.com/DependableSystemsLab/TensorFI Sept. 2018 - present
Teaching Experience: CPEN400A 2019
Programming languages: Python, Java, C, C++
Award: Graduate Student Initiative: $4000 2019