2022 IEEE 30th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM) | 978-1-6654-8332-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/FCCM53951.2022.9786099

On the Single Event Upset Vulnerability and Mitigation of Binarized Neural Networks on FPGAs

Junning Fan
School of Computer Science and Engineering
UNSW
Sydney, Australia
junning.fan@student.unsw.edu.au

Oliver Diessel
School of Computer Science and Engineering
UNSW
Sydney, Australia
o.diessel@unsw.edu.au

Binarised neural networks (BNNs) have attracted research interest for embedded deep learning applications. BNNs are well suited to FPGA implementation since BNNs have small memory utilisations and make use of many binary logic operations in parallel. Moreover, the FPGA acceleration of BNNs has very high energy efficiency and performance [1], making FPGA-based BNNs attractive for implementing neural network capability in power-constrained satellite systems.

However, ionising radiation threatens the function of FPGA-based applications by inducing soft errors. The effect of ionising radiation altering the state of an SRAM memory cell is called a single event upset (SEU). SEUs are the primary class of soft error of concern for SRAM-based FPGAs as SEUs in the configuration memory can result in loss of circuit function [2]. An FPGA application's SEU susceptibility depends on the radiation flux, the FPGA fabric, resource utilisation, as well as the inherent fault tolerance of the algorithm. The application-dependency of SEU vulnerability is especially relevant for neural network accelerators on FPGAs, as the perceptron algorithm can maintain its output when there is a minor change in input or weight.

Applying FPGA-based neural network hardware in high radiation environments or safety-critical scenarios requires a solid understanding of the SEU vulnerability of such hardware. Therefore, it is important to understand the contribution to the SEU vulnerability from each component of the neural network accelerator and how the neural network model affects the vulnerability of the hardware. In addition, the techniques to harden a neural network against radiation need to be developed with an eye towards their efficiency.

This work studies the SEU vulnerability and hardening options for FPGA-based BNNs deployable on satellites. We tested fully-connected BNNs trained on image classification tasks since such networks are being considered for on-satellite image filtering to reduce downlink bandwidth requirements [3] [4]. We investigate the SEU vulnerability and characteristics of each layer in this representative BNN architecture. We study the distribution of vulnerable bits (critical bits) across layers, the severity of soft errors in layers, as well as the resource overhead of selective hardening methods. We conduct fault injection experiments targeting each layer's hardware to analyse how faults in each layer contribute to the accuracy loss of the BNN. We then develop resource-efficient soft error detection and mitigation techniques by selectively introducing redundancy to vulnerable components. We also construct validation datasets for verifying the integrity of the BNN accelerator with no extra hardware utilisation.

We showed that the impact of configuration memory upsets varies across layers. Layers with more neurons and layers with wider input activations cause smaller degradations in classification accuracy when affected by upsets than layers with fewer neurons and with narrower input activations. On the severity of soft errors, We found that while most faults in the BNN hardware have a minor impact on accuracy, some faults caused severe degradation in the networks' accuracies. We find that most of the severe faults occurred in the output layers of BNN hardware and consequently study efficient fault-tolerance and fault-detection techniques by selectively hardening the output layer. We conclude that the selective application of TMR on output layers offers tolerance to more than 60% of serious faults with resource overheads lower than 13%. The selective application of DWC on output layers detects more than 67% of serious faults with resource overheads lower than 7%. We also showed that more than 85% of upsets on critical bits can be detected by using less than 35% of images from the MNIST test sets.

References

[1] S. Liang, S. Yin, L. Liu, W. Luk, and S. Wei, "FP-BNN: Binarized neural network on FPGA," *Neurocomputing*, vol. 275, pp. 1072–1086, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925231217315655

[2] F. G. d. L. Kastensmidt, G. Neuberger, R. F. Hentschke, L. Carro, and R. Reis, "Designing Fault-Tolerant Techniques for SRAM-Based FPGAs," *IEEE Des. Test*, vol. 21, no. 6, p. 552–562, nov 2004. [Online]. Available: https://doi.org/10.1109/MDT.2004.85

[3] E. Lemaire, M. Moretti, L. Daniel, B. Miramond, P. Millet, F. Feresin, and S. Bilavarn, "An FPGA-Based Hybrid Neural Network Accelerator for Embedded Satellite Image Classification," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5.

[4] G. Bahl, L. Daniel, M. Moretti, and F. Lafarge, "Low-Power Neural Networks for Semantic Segmentation of Satellite Images," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV) Workshops*, Oct 2019.

978-1-6654-8332-2/22/$31.00 ©2022 IEEE