# NeuroAttack: Undermining Spiking Neural Networks Security through Externally Triggered Bit-Flips



| | |
|---|---|
| Title | NeuroAttack: Undermining Spiking Neural Networks Security through Externally Triggered Bit-Flips |
| Publication Type | Conference Paper |
| Year of Publication | 2020 |
| Authors | Venceslai, Valerio, Marchisio, Alberto, Alouani, Ihsen, Martina, Maurizio, Shafique, Muhammad |
| Conference Name | 2020 International Joint Conference on Neural Networks (IJCNN) |
| Keywords | adversarial attacks, Artificial neural networks, Biological neural networks, Biological system modeling, Cross Layer Security, cross-layer, cyber physical systems, deep neural networks, DNN, fault-injection attacks, Hardware, machine learning, Metrics, policy-based governance, pubcrawl, reliability, resilience, Resiliency, security, SNN, Spiking Neural Networks |
| Abstract | Due to their proven efficiency, machine-learning systems are deployed in a wide range of complex real-life problems. More specifically, Spiking Neural Networks (SNNs) emerged as a promising solution to the accuracy, resource-utilization, and energy-efficiency challenges in machine-learning systems. While these systems are going mainstream, they have inherent security and reliability issues. In this paper, we propose NeuroAttack, a cross-layer attack that threatens the SNNs integrity by exploiting low-level reliability issues through a high-level attack. Particularly, we trigger a fault-injection based sneaky hardware backdoor through a carefully crafted adversarial input noise. Our results on Deep Neural Networks (DNNs) and SNNs show a serious integrity threat to state-of-the art machine-learning techniques. |
| DOI | 10.1109/IJCNN48605.2020.9207351 |
| Citation Key | venceslai_neuroattack_2020 |

Cross Layer Security adversarial attacks Artificial Neural Networks Biological neural networks Biological system modeling cross-layer cyber physical systems deep neural networks DNN fault-injection attacks Hardware machine learning Metrics policy-based governance pubcrawl Reliability resilience Resiliency security SNN Spiking Neural Networks