Software Engineering Seminar

Analysis of Neural Networks with Fuzzing

Description

Fuzzing is a testing technique, which is based on heuristic-driven random generation of test inputs. It was recently used in the detection of security vulnerabilities, in which it showed great success. Another current trend is the usage of neural networks in all kind of software systems, although the testing of neural networks is still poorly investigated. Recent work like *TensorFuzz* by Odena and Goodfellow [2] and *DeepHunter* by Xie et al. [3] apply fuzzing on the analysis of neural networks. There are also more focused approaches like *DLFuzz* by Guo et al. [1], which uses differential testing to expose incorrect behavior of the neural network.

The goal of this seminar topic is to collect the current research directions in fuzzing for neural networks. Therefore, it is is necessary to perform an initial literature analysis based on the provided publications. The student should examine and discuss the approaches given in the papers and compare them to each other and to similar existing techniques. Additionally, the student is asked to provide a critical discussion of the current research directions, which should also include an outlook for possible future work.

References

[1] Jianmin Guo, Yu Jiang, Yue Zhao, Quan Chen, and Jiaguang Sun. Dlfuzz: Differential fuzzing testing of deep learning systems. In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2018, pages 739–743, New York, NY, USA, 2018. ACM.

[2] Augustus Odena and Ian Goodfellow. Tensorfuzz: Debugging neural networks with coverage-guided fuzzing. *arXiv preprint arXiv:1807.10875*, 2018.

[3] Xiaofei Xie, Lei Ma, Felix Juefei-Xu, Hongxu Chen, Minhui Xue, Bo Li, Yang Liu, Jianjun Zhao, Jianxiong Yin, and Simon See. Deephunter: Hunting deep neural network defects via coverage-guided fuzzing. *arXiv preprint arXiv:1809.01266*, 2018.

Contacts

Yannic Noller (noller@informatik.hu-berlin.de)
Software Engineering Group
Institut für Informatik
Humboldt-Universität zu Berlin