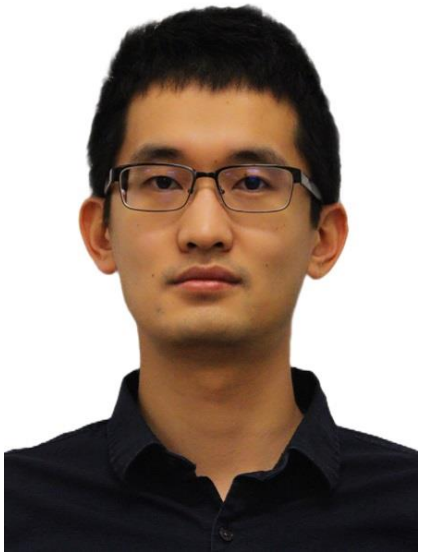
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE



Ze Zhang

Compiler Support for Robust and High Performance Autonomous Driving Environments

Thursday, September 8, 2022
9:30 – 11:30am
Virtual – Zoom
Passcode: 846378

ABSTRACT: With the emergence of autonomous vehicles, a transportation revolution is underway. Despite the potential benefits brought by self-driving cars, autonomous driving systems are still a maturing technology and face two unresolved problems. First, autonomous vehicles are vulnerable to malicious attacks and hardware faults that may compromise the safety and reliability of the system, so making these systems robust against adverse events is a high priority. Second, with the growing computation demands of machine learning models, execution latency has become a critical constraint on resource-limited vehicles. To address these challenges, this thesis proposes a set of compiler methods that can not only enhance the robustness of the self-driving system through efficient code generation techniques, but also improve its execution efficiency by optimizing machine learning models.

First, I present a lightweight and effective method to detect when illegal control flow occurs during runtime as a result of hardware faults. Different checking methods are explored to detect both short-distance and long-distance control flow errors. Further, a low-cost inter-procedural control flow protection scheme is investigated. The combination of proposed checking methods, PaSS, only incurs 19.1% performance overhead while providing 99.0% fault coverage. Second, I propose a centralized communication scheme which increases the safety of the execution environment by validating messages sent between different software modules. To enable the validation functionality of the central control module, we add program analysis algorithms to provide this module with system-level information and develop a domain specific language to describe the safety policies that it must enforce. This centralized framework, AVMaestro, can accurately detect sensor attacks and system anomalies while only incurring 5% end-to-end delay. In the last part of this thesis, I focus on optimizing inference performance of machine learning models. A novel graph substitution algorithm is developed to efficiently fuse parallel nodes in the computation graph of a machine learning model when doing so improves performance. Similarly, a set of node fission transformations is also developed to split one node into multiple nodes that can be executed in parallel. The proposed technique, GraphMorph, improves inference performance by up to 10.5% compared to state-of-the-art optimization approaches.

CHAIR: Prof. Scott Mahlke