COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Haojun Ma

Automating the Verification of Distributed Systems

Monday, August 8, 2022
2:00 – 4:00pm
Virtual Event
Zoom

ABSTRACT: Designing and implementing distributed systems correctly is a very challenging task. Traditionally, people use tests to find and resolve bugs in their systems. But this approach doesn't scale to complex large systems, as there are too many possible interleaving of components. As a result, we still leave bugs in our systems.

To build systems with strong correctness guarantees, formal verification has been successfully used to prove the correctness of distributed systems. Although some approaches successfully applied formal verification to distributed systems and proved the implementation correct, writing a proof for a complex distributed system still requires an ultimate understanding of both the system and the formal method. And these approaches take years of manual effort to write a proof. Thus, formal verification is still not ready for real-world distributed applications.

In this dissertation, I aim to make formal verification more practical by reducing the manual effort required in writing a proof. I'll first show how I can combine the power of model checking to automatically verify a distributed protocol in I4. After that, Sift uses encapsulation to combine the automation from I4 with refinement to scale automation to verification of real distributed implementations. Finally, to make our verified system more practical, I move my focus to high-performance implementations and propose Cruiser to automatically generate such an implementation and its refinement proof to simplify the effort for developers.

CHAIR: Prof. Manos Kapritsos