SAND2018-7741D

The Center for Cyber Defenders

Expanding computer security knowledge

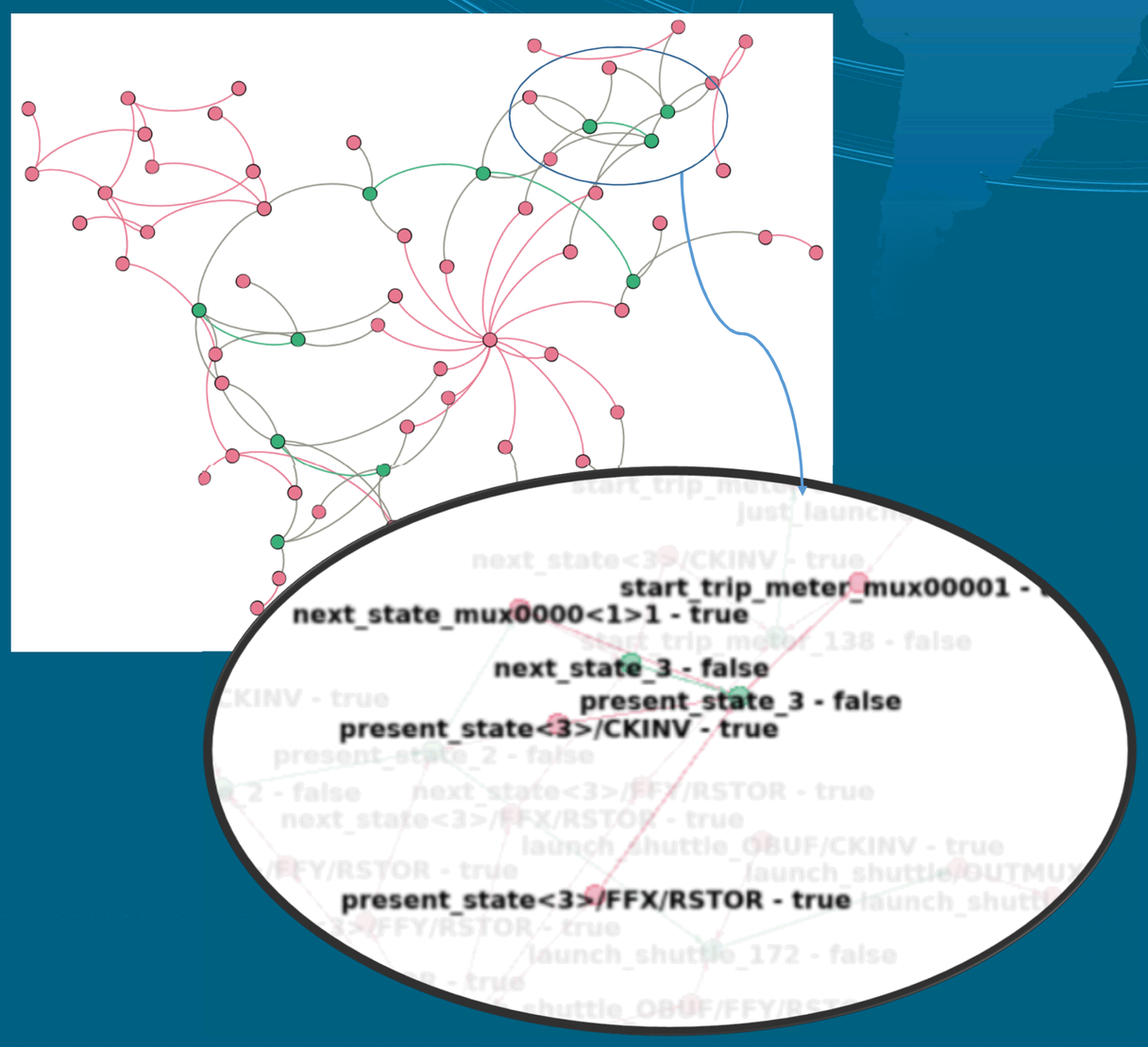
Leveraging SystemVerilog Coverage on Boolean Nodes to Detect Suspicious Logic in a Boolean Network

Lucia Zhang, University of Southern California

Project Mentor: Vivian Kammler

Problem Statement

There is often potential for malicious designs to be implemented into electronic devices. It is difficult to control the design process and especially hard to detect these threats. One of the main threats is insertion of hardware Trojans, which we attempt to identify by examining SystemVerilog coverage for input signals.



Boolean Network with attributes

Objectives and Approach

- Correlate low coverage of input signals to nodes suspected of containing Trojans
- Create a more efficient way of generating cover groups

Implementation:

- Start with an FPGA design, generate a Boolean network to identify inputs of each Boolean node, do so automatically by parsing inputs in a Python script
- Define a SystemVerilog cover group for each Boolean node and its inputs and output
- Run simulation of design including cover groups

Results

- Preliminary results:
  - Correlation of coverage data and critical nodes, but large number of false positives
  - Work on improving sensitivity especially for nodes with large number of inputs

Impact and Benefits

- Help detect suspicious logic in devices that can be used for applications ranging from financial to military security
- Can determine whether or not coverage analysis can be used as an effective verification tool to identify Trojans

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.