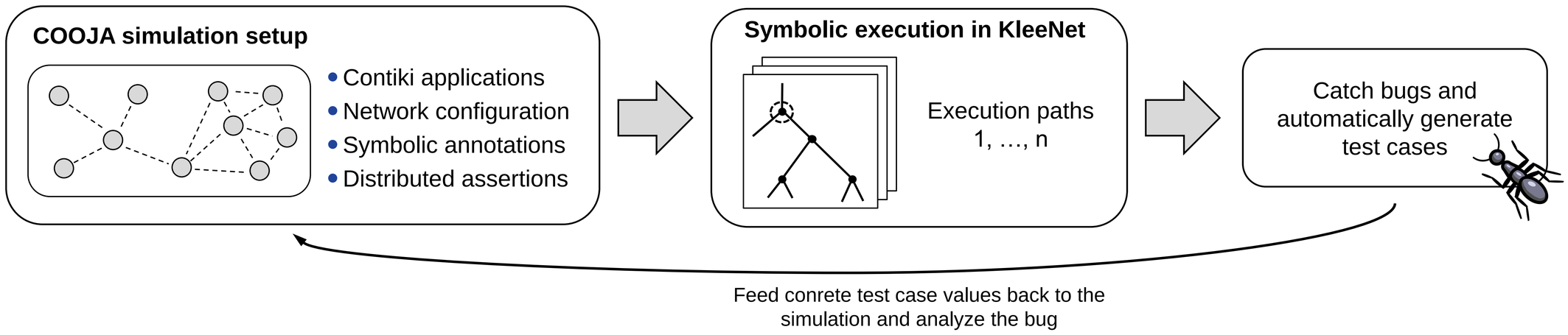
Integrating Symbolic Execution with Sensornet Simulation for Efficient Bug Finding

Seamless Transition Between Simulation and Testing



Integration Overview

COOJA (Österlind et al., SenseApp 2006)

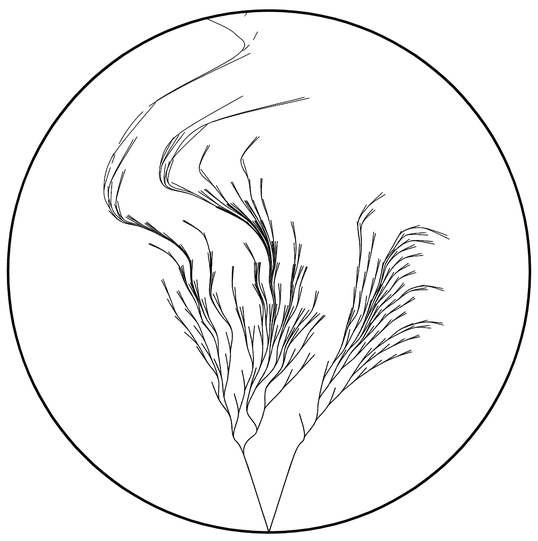
New plugin: COOJA/KleeNet

- **Configuration**
  - Checks current simulation setup
  - Configures node and network failures
  - Exports the setup to KleeNet readable configuration
- **Runtime monitoring**
  - Starts KleeNet
  - Visualizes emerging execution paths
  - Provides users with information about the number of active states
- **Replay**
  - Presents a summary with explored distributed scenarios and errors detected (if any)
  - Prepares concrete test case values for simulation
  - Users select a distributed scenario and start simulation, symbolic memory accesses are replaced with concrete test case values

KleeNet (Sasnauskas et al., IPSN 2010)

Core extensions

- **State scheduling**
  - Implemented COOJA's discrete event queue
  - → Mandatory for deterministic replay in COOJA
- **Distributed scenario prioritization**
  - Goal: Increase overall code and scenario coverage
  - Schedule "interesting" states first

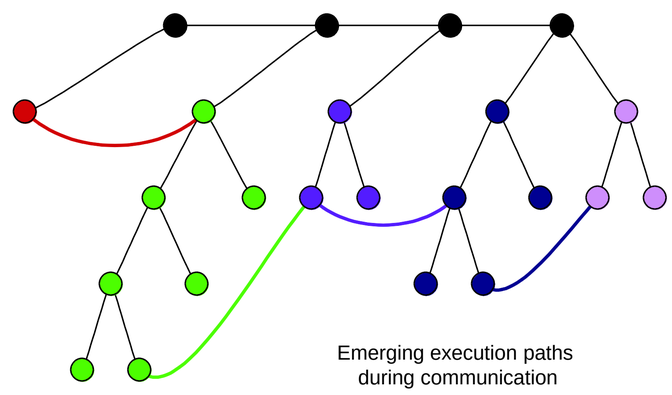


Execution path tree generated by TreeGraph script (http://klee.llvm.org)

Contiki (http://www.sics.se/contiki/)

New platform: coojakleenet

- **Platform internals**
  - Reuse of existing COOJA platform code
  - Replaces Contiki's multi-threading
- **Radio model**
  - Directed Graph Radio Medium (DGRM) with transmission delays
  - Further radio models can be easily added



Emerging execution paths during communication

New research opportunities

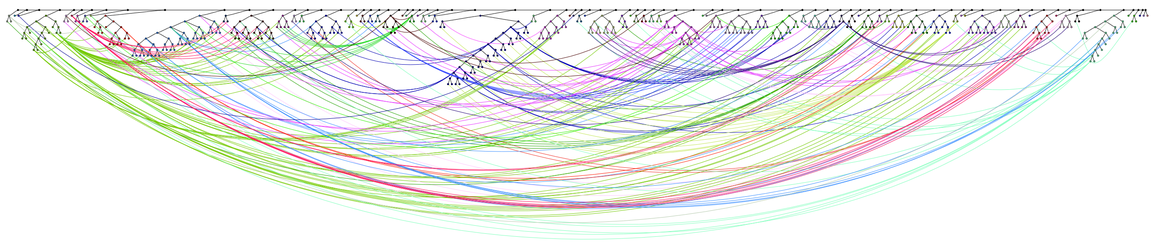
Rigorous sensornet testing

- **Seamless transition between simulation, testing, and testbed deployment**
  - Q: Can we reproduce particular sensornet behavior in different environments?
- **Early detection of suspicious execution patterns**
  - Create discriminative patterns from faulty sensornet executions
- **Deriving more general sensornet safety and correctness properties**
  - Q: Do all sensornets share common execution properties? If yes, how can we specify and check these?

Outlook

Soon

- **Contiki's nightly build tests using KleeNet**
- **Code release**
  - COOJA/KleeNet plugin: http://sourceforge.net/projects/contikiprojects/
  - KleeNet: http://www.comsys.rwth-aachen.de/research/projects/kleenet/



Swedish Institute of Computer Science | SICS

Fredrik Österlind, Adam Dunkels
http://www.sics.se

Raimondas Sasnauskas, Oscar S. Dustmann, Klaus Wehrle
http://www.comsys.rwth-aachen.de

RWTH AACHEN UNIVERSITY | COMSYS Communication & Distributed Systems