A Static Analysis Framework For Embedded Systems

Nathan Cooprider

John Regehr's Embedded Systems Group
TinyOS

- OS for wireless sensor network devices
- nesC – language designed for building applications for the TinyOS platform
  - It is really just an extension to C
  - The produced code is then compiled by gcc
- C – the lingua franca of embedded systems software development
CIL

- **C** Intermediate Language – developed at UCB
- Cleans up **C** to a few core constructs
  - removes syntactic sugar (like “->” notation)
  - arrays become pointers
  - all loops become while loops
- Works on real programs
  - handles ANSI-**C** Microsoft **C**, and GNU **C**
  - SPEC 95, linux kernel, , bzip
The Framework

- Classical dataflow analysis
  - Maintain variable information
  - Analyze until a fixed point is reached
  - Perform transformation based on analysis
- It's an infrastructure for future research
- Future work: Concurrency, backwards operations, degrees of context and/or path sensitivity
Flexibility

- The transformation, analysis, and variable information may all be switched out
  - Transformations: constant propagation, program verification through asserts, code elimination
  - Analysis: symbolic execution
  - Variable information: constant domain, value set domain, parity domain, interval domain, bitwise domain