Automated Extraction and Checking of Property Models from Source Code for Robot Swarms

E. Merlo, C. Pincirolli, J. Panerati, M. Famelis, G. Beltrame
May 9, 2022
**Overview**

**Buzz: a DSL for robot swarms**
- Simple, dynamically-typed language
- Open source compiler and runtime

**Main goal**
- Automatically extract static property models using Pattern Traversal Flow Analysis (PTFA)
- Models fed to a model checker to verify safety properties
Buzz Deployment

operator

robot network
Buzz Deployment

operator

Buzz script

ddebug info

bytecode

bytecode

bytecode

bytecode

robot network
Overall architecture
Method

- Possible manual specification of functions to be tracked
- The physical properties associated with domain specific functions tracked in the model
  - We track all functions in our experiments
- Property constraints are defined by developers (domain knowledge)
- Language-dependent front-end, language-independent from PTFA to model verification
- All automated!
## Results

### Performance

<table>
<thead>
<tr>
<th></th>
<th>ROSBuzz</th>
<th>Swarm Relays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size (LOCs)</td>
<td>4007</td>
<td>3490</td>
</tr>
<tr>
<td>Parsing + CFG (s)</td>
<td>26</td>
<td>34</td>
</tr>
<tr>
<td>Reachability analysis + model</td>
<td>53</td>
<td>71</td>
</tr>
</tbody>
</table>

### Extracted model

<table>
<thead>
<tr>
<th></th>
<th>ROSBuzz</th>
<th>Swarm Relays</th>
</tr>
</thead>
<tbody>
<tr>
<td>nodes</td>
<td>96</td>
<td>128</td>
</tr>
<tr>
<td>edges</td>
<td>202</td>
<td>266</td>
</tr>
</tbody>
</table>
Model Checking

- Allows verification of constraints
- Satisfaction of a forbidden predicate $\rightarrow$ violation
- Non-satisfaction of a property that must hold $\rightarrow$ violation
- E.g. taking-off without verifying the GPS location of the robot
- Tools
  - Alloy (slower)
  - Z3 (faster)
Z3 examples

ASSERT: (not (=> barrier_set_end barrier_ready_begin))
unsat :total-time 0.02)

ASSERT: (not (=> navigate_begin pathPlanner_begin))
unsat :total-time 0.01)
Conclusions

- Novel model extraction method of “as-implemented”
- Analysis of programs using Buzz
- Experiments on 2 medium-size systems for robotics research (ROSBuzz and SwarmRelays)
- Model checking of swarm robotics properties on test pairs from ROSBuzz and SwarmRelays developers
- Results manually validated, suggest that the approach is feasible and scalable