Diagnosis of Hybrid Systems with SMT: Opportunities and Challenges

Alban Grastien

Australian Government
Department of Broadband, Communications and the Digital Economy
Australian Research Council

NICTA Funding and Supporting Members and Partners
Australian National University
UNSW THE UNIVERSITY OF NEW SOUTH WALES
NSW Government Trade & Investment
Victoria The Place To Be
The University of Melbourne
The University of Sydney
Queensland Government
Griffith University
QUT
The University Of Queensland AUSTRALIA

(Informal) Problem Definition

NICTA

Diagnosis

Detect, identify, and isolate faults in a system given observations of the system's behaviour.

Model-Based Diagnosis

A description of the system, i.e., a model, can be used to reason about the system's behaviour.

Hybrid Systems

NICTA

Dynamic Systems the state variables of whom can

- vary discretely (finite number of changes)

$$\forall [t, t'] \in \mathbf{R}^2.\ \exists k \in \mathbf{N}.\ \exists t = t_1 < \cdots < t_k = t'.$$

$$\forall \tau, \tau' \in]t_i, t_{i+1}[.\ v@\tau = v@\tau';$$

- vary continuously

$$\forall [t, t'] \in \mathbf{R}^2.\ \forall \nu \in]v@t, v@t'[\ \Rightarrow\ \exists t_\nu \in [t, t'].\ v@t_\nu = \nu;$$

- exhibit both types of behaviour.

Existing Approaches

NICTA

1. Separate the continuous aspects from the discrete ones: **loses interconnection between the variables**
   - Indicators on the continuous variables estimate the current discrete state
   - Discrete event systems techniques verify that the evolution of the discrete state is consistent with the model

2. Hybrid state tracking (particle filters, etc.): requires **predictive (probabilistic) models**

As opposed to diagnosis of DES, different approaches imply different models and different capabilities

Our Approach

NICTA

Diagnosis *à la* de Kleer, Reiter, Williams

Diagnostic Test

Verify the consistency between the model, the observations, and some assumption (reduced to BMC / SMT)

Diagnostic Algorithm

Generate the diagnostic tests in order to produce the diagnosis ($\rightarrow$ DX-11)

Satisfiability Modulo Theory

NICTA

SAT with an underlying theory

Examples of theories:

- bit-vectors and arrays,
- linear and non-linear arithmetics,
- recursive datatypes,
- default logic, etc.

We are interested in linear arithmetics:

$$(A \vee B) \wedge (x - y \geq 0) \wedge (\neg A \rightarrow (y < 9)) \wedge \ldots$$

Bounded Model Checking for Hybrid Systems

NICTA

Model-Checking

Verify reachability properties over hybrid systems (example: mutexes)

Bounded MC

Search for (counter-)examples that involve n (discrete and continuous) transitions

Reduction from Diagnosis Test to BMC

A diagnostic test is satisfiable iff there exists a path on the model that generates the observations and satisfies the assumption

Translating a Diagnostic Test into SMT

NICTA

Defining the SMT Variables

- For all state variable v and all timestep t, is defined a variable $\boxed{v@t}$

- For all timestep t, is defined a variable $\boxed{\texttt{time@}t}$

$\Rightarrow$ a timestep is an instant!

- For all event e and all odd timestep t, is defined a variable $\boxed{e@t}$

Translating a Diagnostic Test into SMT

NICTA

Discrete Variables

- For every timestep t,

$$\boxed{e@t \rightarrow \text{prec}(e)@t}$$

$$CB\_trip@t \rightarrow (current@t > 80)$$

- For every timestep t,

$$\boxed{e@t \rightarrow \text{effect}(e)@(t+1)}$$

$$CB\_trip@t \rightarrow open@(t+1)$$

- For every discrete state variable v,

$$\boxed{v@t \neq v@(t+1) \rightarrow \bigvee_{e \in \text{affecting}(v)} e@t}$$

$$(\neg open@t \wedge open@(t+1)) \rightarrow (CB\_trip@t \vee CB\_operated@t)$$

Translating a Diagnostic Test into SMT

NICTA

Continuous Variables

- For every timestep t, for every continuous variable v,

$$\boxed{\texttt{time@}t = \texttt{time@}(t+1) \rightarrow v\texttt{@}t = v\texttt{@}(t+1)}$$

$$\texttt{time@}t = \texttt{time@}(t+1) \rightarrow \mathit{tpt}\texttt{@}t = \mathit{tpt}\texttt{@}(t+1)$$

- For every timestep t, for every continuous variable v,

$$\boxed{\mathrm{continuous\_constraint}(v, t, t+1)}$$

$$\mathit{tpt\_increasing}\texttt{@}t \rightarrow$$

$$((\mathit{tpt}\texttt{@}(t+1) - \mathit{tpt}\texttt{@}t) \geq 10 \times (\texttt{time@}(t+1) - \texttt{time@}t))$$

Translating a Diagnostic Test into SMT

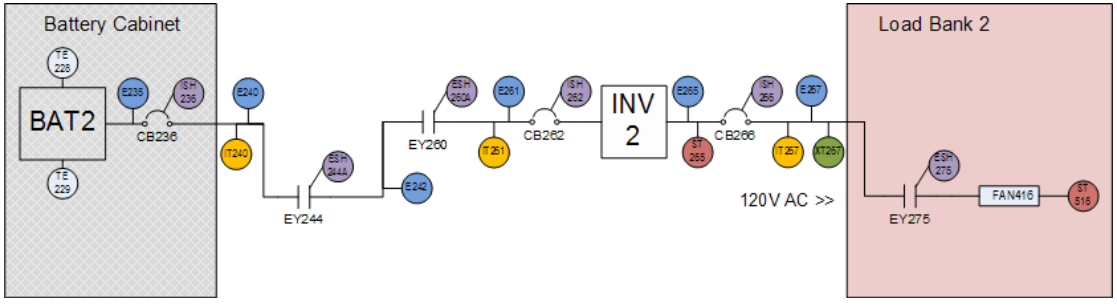
NICTA

- State-based observations:
  $\boxed{obs\_variable@obs\_time = obs\_value}$
  (but the noise must be implemented into the model)

- Assumption: similar to diagnosis by SAT
  $\boxed{\neg f1\_occed@n \ \wedge \ f2\_occed@n \ \wedge \ \neg f3\_occed@n}$

Experiments

Adapt-Lite System



- 10 components
- 16 sensors
- 129 real-valued state variables
- 154 Boolean state variables

- 5-second windows (10 obs.)
- Preferred-First Strategy [DX11]
- SMT solver `Z3` version 4.3.1 (similar results with `cvc3`)

Results

NICTA

Prob. instance	Time (s)	Card	# δ
1	3.428	0	1
2	5.314	1	2
3	5.298	1	1
4	3.476	1	1
5	6.477	2	4

Results

NICTA

Prob. instance	Time (s)	Card	# δ
1	3.428	0	1
2	5.314	1	2
3	5.298	1	1
4	3.476	1	1
5	6.477	2	4

- Most of the runtime is on solving satisfiable problems
- Existing methods run faster but assume that fault patterns can be derived from the model
- Enormous scope for improvement:
  - Already significant improvement from DX-13
  - Simply removing redundant variables simplifies the SMT problems

Benefits of the Approach

NICTA

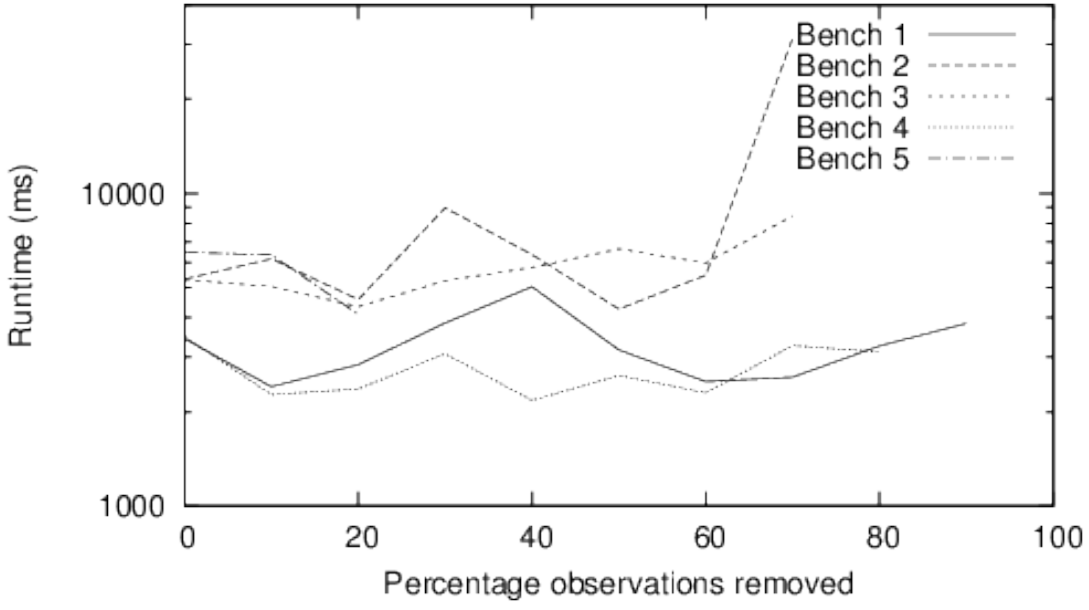
- Does not require a predictive model
- Is very flexible wrt. observations
- Justifies both diagnoses and non diagnoses

Second Round of Experiments

NICTA

Existing methods rely on strong assumptions about observability
What happens when observability is variable?

Remove observations at random



Issues to Solve

- Improve performance: similar to Bounded-Model Checking or SAT planning
- Incremental computation (cf. work with Frank Su)

Conclusion

NICTA

- SMT techniques can be used to solve diagnosis problem of hybrid systems
  - First solution that integrates all the dimensions of the problem
  - Very flexible wrt model and observations
- Many problems remain to be addressed, but they are well-identified