A Query-Based Approach for Test Selection in Diagnosis - Operating System Discovery as a Case Study

Contact Information

Francois Gagnon

Ph.D. Student

Carleton University

fgagnon@sce.carleton.ca

www.sce.carleton.ca/~fgagnon

NMAI Network Management & Artificial Intelligence Research Lab

www.nmai.ca

CARLETON university

www.carleton.ca

OS Discovery as Diagnosis

CONST: Each existing OS is a possible hypothesis
- Single-fault diagnosis

OBS: Network packets
- arp(X,Y,1,mac00_00_00_00_00_00)

SD: $h_1 \vee h_2 \vee \ldots \vee h_k \leftarrow o_1$
- Rule-based diagnosis
- Consistency-based reasoning
- winXP $\vee$ win2K $\leftarrow$ arp(X,Y,1,mac00_00_00_00_00_00)

TEST: OS discovery tests that can be used to fetch more observations
- Send a SYN packet on an open port to obtain a SYN/ACK packet
- Tests are "uniquely supporting"

Query-Based Test Selection

- **Currently:** What is the actual diagnosis?

- **Idea:** Provide a set of queries to the user.
  - Asking the right query prevents executing useless tests.
  - Adapt selection strategies to each query.

- **Queries:**
  - **Q1:** Is a given hypothesis the actual diagnosis?
    Does Windows XP SP1 run on the computer?
  - **Q2:** Does the actual diagnosis belong to a given set of hypotheses?
    Does the computer run an OS of the Windows family?
  - **Q3:** What is the actual diagnosis?
    Which OS runs on the computer?

Result

Answering Q1 can require up to n - 2 fewer tests than answering Q3.

- Consider the n tests t_1, t_2, ..., t_n and the n hypotheses h_1, h_2, ..., h_n.

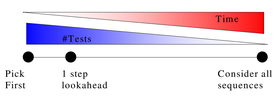
- Assume each test t_i has two possible outcomes:
  - refutes only h_i or
  - confirms only h_i, i.e., refutes every hypothesis except h_i

- Starting from $\{\{h_1\}, \{h_2\}, \ldots, \{h_n\}\}$, we can solve Q1 for any h_i with a single test, namely t_i.

- On the other hand, we need n – 1 tests to be guaranteed to solve the classical query.

- Thus, solving the classical query can require drastically more tests than solving the single-candidate query.

Test Selection Strategies



- **Currently:** Local 1-step lookahead entropy minimization

- **Idea:** Provide a spectrum of test selection strategies

- **Result:** 1-step lookahead is an **unbounded** approximation
  – See example 5.1 in paper

Future Work

- Can we get a bounded approximation in polynomial time?

- Study test selection strategies for other queries
  - Characterizing the optimal solution

- Study test selection strategies for different diagnosis problems (different properties)
  - Multiple-faults
  - Probabilities
  - More complexe tests

- Provide an experimental comparison of the test selection strategies
  - Using OS Discovery