Synthesis of Insertion Functions for Opacity Enforcement

Yi-Chin Wu and Stéphane Lafortune, Department of EECS at University of Michigan

Motivations
- Opacity is a confidentiality property defined in Discrete Event Systems, which characterizes whether a secret of the system can be inferred by an outside observer.
- When the system is not opaque, it is desirable to automatically synthesize an opacity enforcer.

Contributions
- Propose a novel opacity enforcement mechanism using insertion functions.
- Characterize the i-enforceability property that insertion functions need to satisfy in order to enforce opacity.
- Develop an algorithm that enumerates all i-enforcing insertion functions.
- Develop an algorithm that synthesizes an i-enforcing insertion function.

Opacity Definition
- Opacity problem settings:
  (i) partially-observable system
  (ii) secret of the system
  (iii) an intruder that observes the system
- The secret is opaque if for every secret behavior, there is another non-secret behavior that looks the same.
- Example for Current-State Opacity: Secret is opaque if \( E_n=\{b\} \) but not opaque if opaque if \( E_n=\{a,b\} \).

Insertion Mechanism
- Insertion functions are run-time monitoring interfaces that insert extra observable events to the original system output behavior.
- To enforce opacity, insertion functions need to satisfy the i-enforceability property:
  - Safety: Every modified behavior looks like an existing non-secret behavior.
  - Admissibility: Every output behavior is allowed as a valid input to the insertion function.
- Opacity is i-enforceable if there is an i-enforcing insertion function.

Verification of I-enforceability & Synthesis of Optimal Insertion Functions

Identification of all safe insertions
- Insertion choices are not deterministic

Theorem
- Opacity is not i-enforceable if
  \[ P_{\text{uns}}(\{a\}) \neq P(L(\{a\})) \]

Group together the insertion choices responding to the same past output
- An insertion automaton is a finite encoding of an insertion function

Ongoing Work
- Synthesis of an optimal i-enforcing insertion function

References
- Y.C. Wu and S. Lafortune, Synthesis of Optimal Insertion Functions for Opacity Enforcement. Submitted to 52nd IEEE conference on Decision and Control.