The research addresses the following questions:

- Support property validation by developers and scientists
- Objectives of Research

The following:

- A formal experiment evaluated the effects that Prospec and
- Generates formalized specifications in the following languages:
- Specifies program properties using scopes and patterns as
- Formal specifications are difficult to understand and
- Software properties are typically domain specific.
- Formal Specification Challenges

Abstract

The Cyber-ShARE [1] Center of Excellence (Sharing Resources through Cyberinfrastructure to Advance Research and Education) was established in 2007 to advance and integrate education and research in uncertainty, trust, and optimization in support of cyber-infrastructures (CI). A concern in using CI is the inability to know whether services (discovered using CI) will behave as one would expect. Runtime verification techniques such as runtime monitors can provide the needed assurance. Runtime monitors require users to formally specify behavioral properties. Creation of formal specifications is difficult, and there is inadequate tool support for this task.

The Property Specification tool, Prospec [2], was developed to assist users in the automated creation and validation of formal specifications.

This work introduces a new version of Prospec, referred to as Prospec 2.0, that supports the formal specification of properties in particular those that can monitor software services discoverable through CI.

Formal Specification Challenges

- Software properties are typically domain specific.
- The expressiveness of the logic may not support the specification of a desired property.
- Formal specifications are difficult to understand and validate without a formal background.

Background: Property Specification (Prospec) Tool

- Allows users to formalize software properties based on high-level requirements.
- Specifies program properties using scopes and patterns as defined by the Specification Pattern System's (SPS) [3] and Composite Propositions (CP) [2].
- Generates formalized specifications in the following languages:
  - Future Internal Logic (FIL) [4].
  - Meta Event Definition Language (MEDL) [5].

Initial Results

- A formal experiment evaluated the effects that Prospec and SPS, have over the quality of the generated software property specifications with respect to completeness and correctness [7].
- The following research hypothesis was supported: users who specify software properties using Prospec correctly identify, on the average, more patterns and scopes than users who specify software properties using the SPS web site.
- The subjects provided comments for improving Prospec, which are being addressed through Prospec 2.0

Objectives of Research

- Refine Prospec to support generation of Linear Temporal Logic (LTL) [6] formulas.
- Support property validation by developers and scientists through:
  - Visual representation of formulas and
  - Structured English descriptions
- The research addresses the following questions:
  - What types of properties are of interest to scientists in the environmental and earth sciences?
  - Is the use of propositions in Prospec too restrictive for the types of properties that need to be specified? If so, what is needed to specify properties in these domains?
  - What is the best way to graphically present specifications for validation purposes?
  - Is the Mac PEIDL approach sufficient to map specification into appropriate language constructs?

Summary

- Prospec 2.0 will:
  - support OSI interoperability.
  - have a graphical user interface redesigned to better accommodate the needs of the developers and clients, i.e., scientists in the case of Cyber-ShARE.
  - generate traces of computation [8] of accepted and non-accepted behaviors of properties.
  - provide visual representation of properties. Figure 5 presents an example of a property visualization using Prospec 2.0.
  - The work is significant because generated formal specifications can be used in model checkers and runtime monitors in support of verification of software services.

References


Acknowledgements

- Dr. Oscar Mondragon, and Dr. Salamah Salamah for their mentorship.
- This research is partially supported by NSF Grants HRD-0734825 and CNS-0540952.

Prospec Snapshots

Fig 1. Scope Definition Screen. This screen allows users to specify the scope for the property. The user selects one of the five scopes from the menu on the left. The user can use the Guided Selection option if unsure about which scope to use. The user associates propositions to the scope using the menu on the top right. In the case a Composite Proposition is needed, the user can specify it by clicking in the Select CP button.

Fig 2. Scope Guided Selection Screen. This screen guides users into specifying the scope for the property. The left part of the screen prompt the user to answer a series of question to identify the desired scope. The decision tree in the right shows the current state of the decision process.

Fig 3. Pattern Definition Screen. This screen allows users to specify the pattern for the property. The user selects one of the five patterns from the menu on the left. The user can use the Guided Selection option if unsure about which pattern to use. The user associates propositions to the pattern by using the menu on the top right. In the case a Composite Proposition is needed, the user can specify it by clicking in the Select CP button.

Fig 4. Composite Proposition Selection Screen. This screen allows users to define composite propositions. The user decides if the CP is an event or a condition by reading the definition and by selecting the appropriate tab. The list of available propositions appear on the top right of the screen. The user selects a CP’s from the tab. The description of the CP appears in the description textbox in the lower right of the screen.

Fig 5. Property Visual Representation Screen. This screen presents a visual representation of the properties specified using Prospec 2.0 graphical interface. The representation uses finite state traces of computation along with a color scheme to identify different aspects of the property.