ABSTRACT

Self-adaptive systems increasingly need to reason about and adapt both structural and behavioral system aspects, such as in mobile service robots, which must reason about missions that they need to achieve and the architecture of the software executing them. Deciding how to best adapt these systems to run time changes is challenging because it entails considering mutual dependencies between the software architecture that the system is running and the outcome of plans for completing tasks, while also considering multiple trade-offs and uncertainties. Considering all these aspects in planning for adaptation often yields large solution spaces which cannot be adequately explored at run time. We address this challenge by proposing a planning approach able to consider the impact of mutual dependencies between software architecture and task planning on the satisfaction of mission goals. The approach is able to reason quantitatively about the outcome of adaptation decisions handling both the reconfiguration of the system’s architecture and adaptation of task plans under uncertainty and in a rich trade-off space. Our results show: (i) feasibility of run-time decision-making for self-adaptation in an otherwise intractable solution space by dividing-and-conquering adaptation into architecture reconfiguration and task planning sub-problems, and (ii) improved quality of adaptation decisions with respect to decision making that does not consider dependencies between architecture and task planning.

1 INTRODUCTION

Increasingly, self-adaptive systems need to consider adapting both structural and behavioral aspects of the system to achieve their goals. An important class of such systems is mobile service robots, which typically perform tasks such as fetching mail and escorting a visitor to an office [50]. To do this, a robot must carry out actions such as navigating between locations and interacting with humans. These systems operate in environments where obstacles might dynamically appear, light conditions may change, batteries might require recharging, and sensors may fail. Hence, these systems must adapt both their structure and behavior at run time to respond to changes in their operating environment, as well as to system changes that might include software and hardware faults. For example, a robot tasked with navigating to a specific location within a building might experience failure in the camera it is using to navigate. At that point, the system should (i) change the architecture (structure) to a new legal configuration that does not require the camera to navigate, and possibly (ii) replan the way in which the task (behavior) is going to be completed, since there might be more than one way of reaching the target location (e.g., through alternative paths), and the current one might be sub-optimal for the new architecture configuration in which the camera is not available.

However, obtaining the best combination of software architecture configuration and task plan specification is not straightforward due to the mutual dependencies between them. In general, the outcome of executing the same task specification (e.g., reaching the target location through a specific path) in different software configurations will differ depending on factors like energy efficiency of the configuration or safety aspects related to the accuracy of the sensors and navigation algorithms used. Conversely, adapting the task specification (e.g., the robot needs to find a new path because an obstacle is blocking the way) might require reconfiguration because the current architecture configuration may not be suitable for the new path, e.g., which might include dark corridors in which camera-based navigation is not an option anymore.

Accounting for such dependencies in decision making for adaptation poses a challenge because the size of the combined solution spaces for the architecture reconfiguration and task re-planning can easily become too large to be adequately explored at run time.

To deal with that problem, the MORPH reference architecture [6] suggests separating as much as possible structural reconfiguration and behavior synthesis problems. This is achieved by including a goal model manager component in its goal management layer that is in charge of decomposing requirements into achievable reconfiguration and behavior problems, which are assigned to different solvers. Then, the strategy management layer includes a negotiation process that is assumed to guarantee consistency among reconfiguration and behavior strategies when they are selected for
execution. However, our research has shown that such negotiation is not straightforward nor always feasible when there is a need to account not only for functionality, but also to optimize multiple extra-functional concerns (e.g., safety, timeliness, energy efficiency) and their trade-offs. This is because the quantitative guarantees associated with reconfiguration and behavior strategies depend heavily on different pieces of information from multiple heterogeneous models (e.g., energy consumption, software architecture, physical space, safety). These pieces of information are inter-related and change at run time, potentially invalidating any quantitative guarantees associated with pre-computed strategies. This calls for a solution able to co-adapt structure and behavior in a scalable way, as opposed to reconciling a posteriori pre-computed reconfiguration and behavioral strategies that might not provide quantitative guarantees.

In this paper we contribute an approach based on quantitative synthesis and verification that separates planning into architecture reconfiguration and task planning problems, dividing and conquering the solution space while still considering their mutual dependencies. This effectively co-adapts task plan specifications and architecture to optimize adaptation decisions. The approach is instantiated using Alloy [25] and the probabilistic model checker PRISM [29], which are used in tandem to reason quantitatively about the outcome of adaptation decisions. This allows run-time adaptation of the architecture and task plans, under uncertainty, and in a rich trade-off space. With respect to our previous work using quantitative verification for self-adaptation [10, 11, 36], that only dealt with structural adaptation, this approach dynamically constructs strategies that also control the functional behaviour of the system layer components, elaborating explicitly the distinction and coordination between configuration and behavior control.

Our results show that our approach: (i) enables automated run-time decision-making for self-adaptation in what was a priori an intractable solution space by dividing-and-conquering adaptation into sub-problems and (ii) improves the quality of adaptation decisions with respect to decision-making that reasons about structural adaptation only.

## 2 MOTIVATING SCENARIO

Mobile indoor service robots operate in environments where obstacles might dynamically appear, light conditions may change, and batteries may require recharging. They are also limited in what they can sense, creating uncertainty in their location, chances of collision against obstacles, and the resources that they may have left to complete a plan. In spite of this uncertainty, they must attempt to ensure safe operation, effective use of resources like battery, and timeliness of completing a task.

We illustrate our approach using a simple scenario (Figure 1), in which the mission of the robot is navigating to a target location (L5) from an initial location (L1) in the shortest possible time, with a limited battery, and without bumping into obstacles or walls. To achieve this goal, the robot can perform physical actions (e.g., move between locations) and change its configuration (e.g., change a sensor, its localization algorithm, or its speed setting).

While accomplishing the mission, the main concerns are: (i) **timeliness** — the robot should get to the target in the shortest possible time, (ii) **safety** — the robot should arrive at the target location without bumping into obstacles, and (iii) **efficiency** — the robot should minimize the energy used to get to the target location.

The problem that we want to solve is synthesizing specifications for the architecture and behavior of the robot to successfully complete the mission, attending to the criteria described above, despite situations that include component or sensor failure, obstacles blocking corridors, and unexpectedly low battery level.

To inform decision-making, we have four models that capture different aspects of the domain.

**Architecture.** Captures the modes in which the robot can operate, determined by the software components that can be employed at run-time (e.g., associated with sensor input processing, low-level navigation algorithms), their connections, and configuration parameters (e.g., speed, localization accuracy). This model includes:

- The current software configuration, including components, connections, and parameter settings. Configurations in this architecture contain three component categories (Figure 2): 1) **Sensing.** Manages physical sensors that capture information from the environment. (a) **Kinect:** Provides an image where each pixel also includes depth information that can be used to estimate distances to walls and obstacles. (b) **Lidar:** This sensor provides range information in a 2D plane covering 180°. (c) **Back Camera:** The robot has a rear facing camera that can be used by software to position the robot using visual information.

- **Localization.** This component enables understanding the robot’s location and orientation in space. It relies on different types of sensors such as **AMCL** (A-forest Monte Carlo Localization) and **Mrpt** (Multi-Resolution Path Planning) to estimate the robot’s position in the environment.

- **Auxiliary.** These components support specific functionalities such as **LaserscanNodelet** for providing depth information and **Marker Recognizer** for object detection.

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Energy cost</th>
<th>Accuracy</th>
<th>Requires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensing</td>
<td>lidar</td>
<td>Medium</td>
<td>Bad</td>
<td>laserscanNodelet</td>
</tr>
<tr>
<td></td>
<td>camera</td>
<td>Excellent</td>
<td>Good</td>
<td>markerRecognizer headlamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Localization</td>
<td>amcl</td>
<td>Excellent</td>
<td>Excellent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mrpt</td>
<td>Medium</td>
<td>Good</td>
<td></td>
</tr>
<tr>
<td></td>
<td>aruco</td>
<td></td>
<td>Good</td>
<td></td>
</tr>
<tr>
<td></td>
<td>laserscanNodelet</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>markerRecognizer</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>headlamp</td>
<td>Really bad</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 1: Simple mobile robotics scenario.](image1)

![Figure 2: Mobile robotics architecture configuration space.](image2)
2) **Localization.** Produces information about the position of the robot based on information captured by a sensor, or processed by another component. (a) **AMCL.** Implements a general-purpose localization scheme that fuses depth sensor information and odometry to estimate the pose of a robot on a known map [15]. (b) **MRPT:** Implements an alternative localization algorithm [4]. (c) **ArUco.** Takes an image from a camera and identifies the relative position of the camera to visual markers that are placed in the environment [41], using that knowledge to determine the position of the robot. This algorithm relies on a well lit environment to see the markers.

3) **Auxiliary.** Perform auxiliary functions and impact qualities like energy efficiency, localization accuracy and obstacle detection (which affects safety) in different ways. (a) **Headlamp.** The robot has an LED lamp to make visual information available in dark locations. (b) **Laserscan Nodelet.** Transforms data from Kinect to Lidar format, so that it can be consumed by standard localization components (i.e., AMCL and MRPT).

- The repertoire of behavior primitives that the robot can execute to change its configuration. We assume a pair of primitives to enable/disable every component in the architecture (e.g., enable_kinect, disable_lidar). For a configuration parameter (like speed setting), there is a primitive that sets the new value of the parameter (e.g., set_speed(value)).
- A formal model of the architectural style that prescribes which configurations are valid, encoding for instance, that some components require additional auxiliary components to interoperate with the rest of the system (c.f. table in Figure 2).

The architecture is represented in Acme [17], and was derived from an architecture discovery for ROS similar to [44].

**Physical Environment.** Describes the space that the robot is navigating. This model is captured as a graph, where nodes correspond to physical locations, and arcs correspond to trajectories between them. Arcs are tagged with attributes distance (5m and 3m for horizontal and vertical arcs in Figure 1, respectively) and risk (a probability value in [0,1] that captures the likelihood that the robot will bump into an obstacle when moving between the endpoints of the arc). In this simplified scenario, we assume that all arcs have a risk probability of 0, except for arc (l2, l3), which has a bump risk probability PBUMP which varies, depending on the robot’s configuration (e.g., a configuration with higher speed or less accurate obstacle detection will have a higher probability). This is modeled as an annotated graph.

**Power.** This model is queried to determine: (i) available resources (i.e., remaining battery energy), and (ii) cost of operations in a given configuration (e.g., how much energy it takes to move to a location with a given speed and set of sensors/components enabled). This is a linear regression model that was derived from experimentation on a Turtlebot [43], combined with documented power specifications of sensors, e.g. for the Lidar [2].

**Task.** Describes the task to accomplish, and its progress. In this scenario, we assume that the progress of the mission captures the location of the robot, its remaining battery level, the history of actions executed, and the remainder of actions to be executed. It also includes the repertoire of behavior primitives that the robot can execute to carry out an action in the physical environment. For simplicity, we assume that in this scenario the robot can carry out two types of action: (i) move between two locations in the map, and (ii) change its configuration, i.e., execute a sequence of reconfiguration primitives to enable/disable software components and/or set new values of its speed setting. This is modeled as a graph of robot actions represented using Instruction Graphs [35].

Analyzing system properties requires combining pieces of information from different models, which do not provide insight if considered individually. For example, the topology of the physical environment, operations, or the power model are not useful on their own, but they can be combined e.g., to estimate metrics like time to complete the robot’s mission, or the overall probability of bumping into an obstacle along the way. Moreover, even in this simplified scenario, the size of the combined reconfiguration and task plan solution spaces is in the order of magnitude of $10^6$ states and will grow exponentially with additional components and map waypoints. This makes moderate problem instances intractable for online monolithic planning approaches.

Hence, despite the apparent simplicity of this scenario, its characteristics make evident the need for approaches to: (i) integrate information from heterogeneous models and different levels of abstraction to generate and provide assurances about system behaviors, (ii) reason in a multi-dimensional space of concerns, (iii) capture and factor in uncertainties that affect the system, and (iv) scale when dealing with potentially intractable solution spaces.

### 3 APPROACH

Our approach for reasoning about self-adaptation is intended mainly for run-time use in the planning activity of MAPE-K, which is concerned with determining how to best adapt the system at run time.

Considering the characteristics of the scenario and the challenges described in Section 2, a suitable approach to our problem should be: (i) reusable in a new context with low reengineering overhead, (ii) able to reason about multiple system aspects, trade-offs, and under uncertainty, (iii) able to scale, and (iv) able to provide formal guarantees about the solutions generated.

To satisfy those requirements, we propose an approach that hinges on a carefully orchestrated use of disparate formal methods like structural model synthesis and probabilistic model checking. Concretely, the rationale for our approach entails: (i) separating reconfiguration from mission planning, and (ii) carrying out reconfiguration planning before task planning to avoid exploring a larger state space in which candidate task plans are carried out in configurations that are later found to be infeasible. Figure 3 illustrates our approach, which divides the planning into two major stages: *Architecture reconfiguration planning*, which determines the legal software architectures of the robot given the current available and failed components (Step 1) and generates an adaptation strategy to adapt the robot to this new architecture (Step 2), and *Task planning* which replans the mission (Step 3) and determines the best architecture/mission combination through quantitative planning in PRISM. The result of this is a combined plan that adapts the software architecture of the robot and the robot mission to satisfy the quality trade-offs that are required (Step 4). The circled numbers and references to tables and listings in Figure 3 are elaborated on later.

**A Model-View Projection** (Section 3.1): (i) each problem domain model is projected into a view that abstracts its important features in an intermediate language (this projection is model type-specific
Table 1

<table>
<thead>
<tr>
<th>Available components</th>
<th>Legal configs</th>
<th>Reconfiguration actions</th>
<th>Task attribute quantifiers</th>
</tr>
</thead>
</table>

**(A)** generates a task plan via MDP policy synthesis that resolves the nondeterministic choices in which the robot and configuration actions are underspecified. In such a way, task planning is carried out in a context-sensitive manner with respect to the set of possible configurations in which the task can be executed, which might yield different outcomes in terms of timelines, energy efficiency, and safety.

### 3.1 Model-View Projection

System models are complex engineering artifacts written in a formal or semi-formal language, each capturing a different facet of the problem domain (e.g., energy or time). Directly integrating models into composite analyzable behaviors is a difficult task. To ease this process, we first provide abstractions of the models, which, following prior research, we term views [21]. A view contains a description of sets, relations, functions, and predicates that a model provides for behavioral reasoning. For instance, a configuration view for a mobile robot can provide a set of available system configuration options (such as speed and sensors to use), domains of their values, and constraints on which options can be used together (e.g., a robot can use visual navigation only if its visual sensors are on).

We construct views and manage the relations between them. For example, an architecture configuration view exposes a set of legal configurations, and a power view exposes a function $\text{pow}(\text{bp}, e)$ that returns the power needed to carry out behavioral primitive $\text{bp}$ (e.g., move between locations $\text{l1}$ and $\text{l2}$) in configuration $e \in \text{conf}$. Thus, the power view can be related to the configuration view.

We engineer views to expose model information relevant to behavioral reasoning and synthesis in the task domain.

### 3.2 Adaptation Planning

Our approach to adaptation planning is based on probabilistic model checking [28] which enables quantitative analysis and policy synthesis in systems that exhibit probabilistic behavior. These policies can be synthesized from MDP models that capture system behavior using standard temporal logics and model checkers like PCTL/PRISM and are guaranteed to achieve optimal expected probabilities and quantitative rewards [30].
In the remainder of this section, we first show how we combine MDP policy synthesis via model checking with formal description and reasoning about architectural styles for reconfiguration synthesis (Section 3.2.1). We then illustrate task planning (Section 3.2.2).

3.2.1 Architecture Reconfiguration Planning. Architecture reconfiguration planning is based on combining architectural synthesis techniques built on a formalization of architectural styles with plan synthesis that uses MDP policy synthesis via model checking. Architectural styles [46] characterize the design space of families of software systems as patterns of structural organization, defining a vocabulary of component/connector types and constraints that help designers constrain exploration to a set of legal system structures.

Definition 3.1 (Architectural Style). Formally, we characterize an architectural style as a tuple \((\Sigma, C_\Sigma)\), where:

- \(\Sigma = (\text{CompT}, \text{ConnT}, \Pi, \Lambda)\) is an architectural signature, such that:
  - \(\text{CompT}\) and \(\text{ConnT}\) are sets of component/connector types.
  - \(\Pi : (\text{CompT} \cup \text{ConnT}) \rightarrow 2^\mathbb{D}\) is a function that assigns sets of symbols typed by datatypes in a fixed set \(\mathbb{D}\) to architectural types \(\kappa \in \text{CompT} \cup \text{ConnT}\). \(\Pi(\kappa)\) represents the properties associated with type \(\kappa\). To refer to a property \(p \in \Pi(\kappa)\), we simply write \(\kappa.p\). To denote its datatype, we write \(\text{dtype}(\kappa.p)\).
  - \(\Lambda : \text{CompT} \cup \text{ConnT} \rightarrow 2^\mathbb{P} \cup 2^\mathbb{R}\) is a function that assigns a set of symbols typed by a fixed set \(\mathbb{P}\) to components and a set of symbols in a fixed set \(\mathbb{R}\) to connectors. \(\Lambda(\kappa)\) represents the ports of a component (conversely, the roles if \(x\) is a connector), which define logical points of interaction with \(\kappa\)’s environment.
- \(C_\Sigma\) is a set of structural constraints expressed in a constraint language based on first-order predicate logic similar to Acme [17] or OCL [51] constraints (cf. Table 1).

For the remainder of this section, we assume a fixed universe \(\mathcal{A}_\Sigma\) of architectural elements, i.e., a finite set of components and connectors for \(\Sigma\) typed by \(\text{ConnT} \cup \text{CompT}\). For a given architectural element \(c \in \mathcal{A}_\Sigma\), we denote its type as \(\text{type}(c)\). Moreover, we denote the set of components in \(\mathcal{A}_\Sigma\) as \(\mathcal{A}_{\text{Comp}}\) (\(\mathcal{A}_{\text{Conn}}\) for connectors).

Formal characterization of architectural styles in Alloy [25] have proved to be a valuable tool for exploring rich solution spaces by synthesizing system configurations that satisfy the constraints imposed by an architectural style [3, 9, 13, 27, 32]. A configuration can be characterized as a graph that captures the topology of a feasible structure in the system.

Definition 3.2 (Configuration). A configuration in a style \(\mathcal{A} = (\Sigma, C_\Sigma)\) is a graph \(G = (N, E)\) satisfying the constraints imposed by \(C_\Sigma\), where: \(N\) is a set of nodes, s.t. \(N \subseteq \mathcal{A}_\Sigma\), and \(E\) is a set of pairs typed by \(\mathbb{P} \times \mathbb{R}\) representing attachments between ports and roles. We denote the set of legal configurations in \(\mathcal{A}\) by \(\mathcal{A}\).

Example 3.3. We can characterize the space of configurations in our scenario by the signature \(\text{CompT} = \{\text{laserScanTopicT}, \text{cameraT}, \ldots\}\), \(\text{ConnT} = \{\text{laserScanTopicT}, \ldots\}\), \(\Pi = \{\text{laserScanT}, \text{Status}, \text{Consumer}, \ldots\}\). Connectors correspond to topics to which the components publish and subscribe. Component properties in \(\Pi\) include \(\text{Status} \in \{\text{Enabled}, \text{Disabled}, \text{Offline}\}\), and Consumption, which captures a component’s contribution to energy consumption.

With these elements, we can specify a set of structural constraints that the style imposes on valid configurations (c.f. Table 1).

To generate models for architecture reconfiguration planning, we need to be able to encode architecture configurations as predicates in our model. To do so, we define an encoding function \(pred\) that takes a configuration and returns a predicate:

\[
pred(G) = \bigwedge_{n: \text{Status} = \text{Enabled}} \text{pred}_N(N) \land \bigwedge_{n: \text{Status} = \text{Disabled}} \neg \text{pred}_N(N)
\]

Function \(\text{pred}_N\) takes a node in a configuration graph, and returns a predicate that encodes the presence of that component/connector in the graph. We leave implicit bindings between components and connectors, which are not required because we assume no rewiring as possible reconfiguration actions (just enabling/disabling components). This encoding can be naturally extended to include in the conjunction additional terms encoding bindings.

We define a component status vector as the set of all possible component status values in the configuration space, i.e., \(\text{Comp}_S \equiv \{\text{Enabled}, \text{Disabled}, \text{Offline}\}\).

Definition 3.4 (Reconfiguration Planning Model). A parametric MDP model for reconfiguration is a tuple \((S, S_I, A, \Delta, r, G\mathcal{P})\), s.t.:

- \(S \subseteq \text{Comp}_S\) is the space of possible component status.
- \(S_I \subseteq \text{Comp}_S\) is a vector of initialization parameters for component status, which determines the starting reconfiguration point.
- \(A \equiv \{\text{Enable}, \text{Disable}\} \times \mathcal{A}_{\text{Comp}}\) is a set of actions to enable/disable components. We note the action (Enable, c) as Enable\_c. \(\Delta : S \times A \rightarrow S\) is a transition relation that differs from the standard MDP description, leaving out probabilistic extensions for unreliable reconfiguration primitives out of scope.
- \(r : A \rightarrow \mathbb{R}^+\) maps reconfiguration actions to rewards (costs).
- \(G\mathcal{P} \equiv \bigcup_{g \in \mathcal{G}} \text{pred}_G(g)\) encode legal configurations in \(\mathcal{G}\).

In practical terms, we build the MDP model as a set of modules in PRISM with the structure illustrated in Listing 1. In the listing, global variable turn (line 2) imposes a strict total order on which components can be reconfigured, eliminating unneeded interleavings and reducing remarkably the state space.

The model includes a set of \(\mathcal{A}_{\text{Comp}}\) modules (referred to in the listing as \(N\)). Every component’s behavior is encoded as a module with the corresponding enable and disable actions. There is no explicit action for the Offline status, since this indicates that the component is unavailable (e.g., due to failure), and reconfiguration actions over it are out of the system’s control. The parts highlighted in blue in the listing are those incorporated from the domain model views: \(\mathbb{D}\) sets the current status of a component, obtained from the monitoring infrastructure and exposed through the architecture view, and a set of formulas \(\mathcal{G}\) encode the alternative legal configurations (\(G\mathcal{P}\) obtained from function \(\text{pred}_G\) – Expression 1).

Finally, reconfiguration cost is encoded as a reward structure over reconfiguration actions (lines 16-20). For each action, we assign a cost \(\mathbb{D}\) that can encode different attributes like time employed in carrying out the reconfiguration action, or energy spent.

\footnote{For clarity, representation of port-role attachments is left implicit in our formalization.}

\footnote{Numbered elements in listings 1 and 2 correspond to those identified in Figure 3.}
Table 1: Architectural element definitions and constraints of the pub-sub robotics software architecture (excerpt).

<table>
<thead>
<tr>
<th>Type</th>
<th>Constraint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>abstract sig componentT [pub set topicT, sub set topicT]</td>
<td>Component definition.</td>
</tr>
<tr>
<td>definitions</td>
<td>abstract sig topicT [pub set componentT, sub set componentT]</td>
<td>Connector definition.</td>
</tr>
<tr>
<td>temporal</td>
<td><code>pred</code> onlyPublishesTo[c-componentT, t-topicT] [publishesTo[c, t] &amp; all t’ topicT-t</td>
<td>A component only publishes to a specific topic.</td>
</tr>
<tr>
<td>constraints</td>
<td>not publishesTo[c, t]'] ]</td>
<td></td>
</tr>
<tr>
<td>ROS</td>
<td>abstract sig sensingT, localizationT extends componentT [lone sig</td>
<td>Component type definitions.</td>
</tr>
<tr>
<td>definitions</td>
<td>lidarT, kinectT, cameraT extends sensingT []</td>
<td></td>
</tr>
<tr>
<td></td>
<td>lone sig laserScanTopicT, sensorMsgsImageTopicT, markerPoseTopicT extends topicT]</td>
<td>Sensing component type definitions.</td>
</tr>
<tr>
<td></td>
<td><code>pred</code> [all c-kineT [onlyPublishesTo[c, sensorMsgsImageTopicT, markerPoseTopicT</td>
<td>Kinect only publishes to image sensor message topic.</td>
</tr>
<tr>
<td>constraints</td>
<td>extends topicT]]</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>pred</code> [some kinectT =&lt;=&gt; some laserscanNodeletT]</td>
<td>Kinect requires laser scan translator component.</td>
</tr>
</tbody>
</table>

Synthesis of Reconfiguration Plans. Using a MDP model like the one described above, in which initialization of component status constants is done according to the monitored status of the components at run-time, we can carry out policy synthesis to determine the best legal reconfiguration plans. To illustrate the process, consider the PCTL property (2) that captures the reachability of a legal configuration (e.g., `conf_M` encoded in Listing 1, line 14).

\[
\begin{align*}
R\{\text{reconf\_cost}\}_{\text{min}} &\Rightarrow [F \text{ conf\_M}] \\
\end{align*}
\]

This property contains two parts: (i) a `reconf\_cost` quantifier, which indicates that the policy synthesis should resolve the nondeterminism in the model in such a way that it minimizes the accrued `reconf\_cost` (Listing 1, line 16), and (ii) a path formula, which indicates that the paths in the model over which the reward has to be optimized are those that lead to states where the reachability predicate (i.e., arriving at legal architecture configuration `conf\_M`) is satisfied. Model checking a property like the one described for every legal configuration with a probabilistic model checker can yield a set of policies. Translating from policies to sequential reconfiguration plans is straightforward, since the policies are deterministic. We define function `generate_R`, which yields the set of reconfiguration plans for a given parametric MDP reconfiguration model `MR` and an initial configuration state `i`:

\[
\bigcup_{g \in AG} \text{seq}_g(\sigma(MR, i, R\{\text{reconf\_cost}\}_{\text{min}} = [F \text{ pred}(g)]).p)
\]

Where `\sigma(MR, i, \phi)` designates the model checking function that synthesizes a policy for a model `MR` from an initial state `i`, and a PCTL property `\phi` (we denote by `\sigma(MR, i, \phi)`). Policy `g` is the quantitative result, i.e., the quantified cost for the policy generated in the Expression 2). Function `seq_g` is a simple function that turns a deterministic policy into a sequential plan. We also assume a simple function `label_plan` that assigns a symbolic label to a sequential plan. We note the set of symbolic labels for a set of reconfiguration plans `X` as `labels(X)`.

3.2.2 Task Planning. In addition to the architectural model of the system, we assume a set of additional views that expose relevant information for task planning. These pieces of information can be combined into building blocks for rich planning model construction.

We begin by introducing the view that describes the physical environment in which the task takes place.

**Definition 3.5 (Physical Environment View).** A physical environment view `\mathcal{V}_{PE} \subseteq LOC \times TRA` can be characterized as a simple directed graph, where `LOC` is a set of nodes representing locations, and `TRA` is a set of edges that represent valid trajectories between locations. We also equip the view with `\Pi_{LOC} : LOC \rightarrow 2^D` and `\Pi_{TRA} : TRA \rightarrow 2^D`, which are functions that assign sets of symbols typed by datatypes in a fixed set `D` to nodes and trajectories in the map, capturing relevant attributes, e.g., length of a trajectory, plane coordinates or id of a location.

In addition to the set of reconfiguration primitives `A`, there is a set of actions `O` that can be carried out in the physical world by the robot. Executing both types of action consumes resources which can be encoded in a resource view. We illustrate this section with a single resource view that corresponds to energy.

**Definition 3.6 (Resource View).** A resource view `\mathcal{V}_{R} : \mathbb{R}^{+} \times AG \times (O \cup A) \rightarrow \mathbb{R}^{+}` is characterized as a function that quantifies the amount of resources consumed by an action carried out during an arbitrary amount of time and in a given architectural configuration.

Execution of actions to accomplish a task also requires keeping track of the current progress of the task, as well as what has been done and remains to be done to satisfy system goals.

**Definition 3.7 (Task View).** In a task view `\mathcal{V}_{T} = (S, s_{I}, O, H, P, g)$: $S$ is the state space of the task, $s_{I} \in S$ is the current state of the task, $O$ is the set of robot operations, $H \in O^{*}$ is the history of executed actions, $P \in O^{*}$ are the pending actions, and $g$ is an abstract specification of the task’s goal. Although we give a general definition, in our scenario we assume that a state is a pair in $\mathcal{V}_{PE}.LOC \times \mathbb{R}^*$ of localization in the map and battery energy.

Now that we have defined the views, we introduce a definition of the task planning model.

**Definition 3.8 (Task Planning Model).** A model for task planning is an MDP $(S, s_{I}, A, \Lambda, r)$ where $S \subseteq AG \times V_{T}$. $S$ is the state space,
Listing 2: Task planning model structure.

\[ \text{s_f} \in S \] is a pair of architectural configuration \( c \) and the initial task state, \( A \equiv O \cup \text{labels}(\text{generate}(M_R, s_f, c)) \) is the set of actions that include operations of the robot in the physical world, as well as symbolic actions that correspond to architecture reconfiguration plans from the initial configuration \( s_f, c, A : S \times A \rightarrow D(S) \) is a (partial) probabilistic transition function, and \( r : S \times S \rightarrow \mathbb{R}^+ \) is a reward structure that maps transitions to rewards.

We build the MDP in a PRISM encoding of the robot behavior using the pattern illustrated in Listing 2, in which the robot module includes variables: \( b \) for capturing the battery energy level (initialized with the value exposed from the task view \( \hat{\phi} \)), \( I \) for robot location (with an initial value \( \delta \) from the task view), \( c \) for the robot’s architecture configuration (initialized with information \( \Theta \) from the architecture view), \( \rho \) to keep track of whether reconfiguration has been carried out, and \( \text{collided} \) which captures if the robot has collided against some obstacle (lines 2-5). Based on these variables, we also define formulas that capture: (a) goal satisfaction (line 15) encoding that the robot location is the target location, and (b) stop condition (line 16), which holds when the robot satisfies the goal or does not have energy to operate. The module’s behavior is defined by two groups of guarded commands:

- **Reconfiguration actions** (line 7). There is one reconfiguration action command for every legal reconfiguration. Action labels in the reconfiguration commands (e.g., \( [\text{t_set_conf}_M] \)) are obtained via \( \text{labels}(\text{generate}(M_R, s_f, c)) \) (cf. Definition 3.8). Each reconfiguration command is guarded to make sure that: (a) the target configuration is not already active, (b) there is sufficient energy in the battery to reconfigure \( \text{deplete_battery_reconf}_{X} \) (11), lines 7-8, are the energy costs of reconfiguration plans, computed using Expression 2), (c) reconfiguration has not been carried out, and (d) the stop condition does not hold.

- **Task actions** (line 9). These commands encode the actions of the robot in the physical world. In this case, these actions correspond to movements between locations in the physical environment. For every trajectory between locations \( lx \) and \( ly \) in the physical environment \( \text{V}_{PE}, \text{TRA} \) (c.f. Definition 3.5), there is a set of commands (one per configuration) that encodes the movement of the robot between those locations. Every command:

  - Checks in its guard that: (a) the current location is \( lx \), (b) the stop condition has not been reached, and (c) the current configuration is the one to which the command corresponds.

  - Includes two updates with probabilities \( p_{\text{col_conf_A}}(lx \rightarrow ly) \) and its complementary outcome, which encode the likelihood of colliding while going through the trajectory in configuration \( A \). This probability is one of the attributes with which we tag our physical environment view (c.f. \( \Pi_{TRA} \), Definition 3.5). Each of these updates: (a) the location variable, (b) the depletion of the battery, and (c) the collision status. For battery updating, the model defines a set of formulas (11), line 11) where different battery depletions are encoded per-configuration. These values \( e_{lx \rightarrow ly} \) are obtained by querying the resource (i.e. energy) view \( V_E \) with the specific action and configuration that the command corresponds to (c.f. Definition 3.6).

Our task planning model also incorporates a reward structure that enables quantifying metrics associated with planning concerns like timeliness and energy efficiency. Lines 17-24 illustrate reward structures used to capture timeliness and energy efficiency. For timeliness, line 18 shows how the structure encodes time reward for an action that moves the robot from location \( lx \) to \( ly \), accruing different amounts of time \( t_{lx \rightarrow ly} \) depending on the configuration that the robot is in. These times are computed by combining the distance attribute of the trajectories in the physical environment view \( V_{PE}, \text{TRA} \) with the speed setting of the robot’s configuration. Line 20 shows how time is accrued for reconfigurations. \( \text{t_set_conf}_A \) (11) is the time it takes to reconfigure, obtained from the evaluation of the reconfiguration cost analogous to the one encoded in Expression 2, in which cost is expressed in terms of time. For energy efficiency, Line 23 encodes a simple reward that corresponds to the level of battery \( b \) when the robot reaches the stop condition.

**Generating Task Plans.** Generating a task plan entails:

- **(A) Synthesis of candidate solution plans.** For generating task candidate plans, we instantiate a set of alternative probabilistic models \( M_{f_p} \) (cf. Definition 3.8), in which the set of robot operations is fixed to a specific path between its current and the target location. These paths are computed using Dijkstra’s algorithm and ranked by ascending distance. We set a threshold \( n_{f_p} \) that fixes the number of paths to extract from the top of the ranking. We perform this step for efficiency reasons, because synthesizing paths as part of MDP policy synthesis is rather costly. Hence, the only decision left underspecified for model checking is selecting the best reconfiguration for a specific candidate solution model. This results in \( n_{f_p} \) runs of the model checker instead of one, but the computational cost is reduced orders of magnitude, compared to considering the full solution space in a single model checking run.

- **(B) Quantifying the value of metrics for the different concerns of every candidate solution entails model checking the candidate solution models in \( M_{f_p} \) against the PCTL properties in Table 2:**
Table 2: PCTL properties for mission planning.

<table>
<thead>
<tr>
<th>Name</th>
<th>PCTL Formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\phi_1$</td>
<td>$R{\text{time}}_{\min}=F,\text{goal}$</td>
<td>Time to target location.</td>
</tr>
<tr>
<td>$\phi_2$</td>
<td>$R{\text{energy}}_{\max}=F,\text{goal}$</td>
<td>Remaining energy at target location.</td>
</tr>
<tr>
<td>$\phi_3$</td>
<td>$P_{\max}^{\text{goal}}=F,\text{goal} \land \neg\text{collided}$</td>
<td>Non-collision probability.</td>
</tr>
</tbody>
</table>

- **(a)** The process starts by generating the optimal policy for the priority concern for every candidate solution $\sigma_i^f \triangleq \sigma(m_i^f, cs, \Phi, p)$, where $\Phi \in \{\phi_2, \phi_3, \phi_1\}$ is the PCTL formula for the prioritized concern, $m_i^f \in M_{f,o}$, $i \in \{1 \ldots n_{f,o}\}$, and $cs \in AG \times V_T$ (c.f., Definition 3.8). The current state combining configuration and task state from which the solution is being computed.

- **(b)** Once the optimal policy for the priority $\sigma_i^f$ has been generated for each candidate, we quantify how good this candidate solution is by computing an attribute value vector:

  $$(\sigma_i^f(m_i^f, cs, \phi_1).q, \sigma_i^f(m_i^f, cs, \phi_2).q, \sigma_i^f(m_i^f, cs, \phi_3).q)$$

  Where $\sigma_i^f(\ldots)$ denotes that model checking is constrained to a version of the model in which the policy is fixed to $\sigma_i^f$. We designate the set of attribute vectors for $M_{f,o}$ as $V_{f,o}$.

- **(C) Candidate solution generation**, for which we maximize a utility function over attribute vectors (in the expression below, function $\sigma_i^f$ returns the optimal policy $\sigma_i^f$ from which an attribute value vector was generated):

  $$p_f^* = \sigma_i^f(\arg\max_{v \in V_{f,o}} u(v))$$

4 EVALUATION

In this section, we evaluate our approach along two dimensions: (i) Run-time tractability – can our planning approach work at run time to adapt a robot using off-the-shelf robotic software and adapt to errors and changes in the environment to complete missions? and (ii) Quality improvement – does the approach generate plans with higher utility than the standard self-adaptive practice of considering only the structural aspects of the system?

We use a scenario similar to the one in Section 2, but with a more realistic robot environment with 58 intersections (used as waypoints for planning). Some corridors contain small obstacles that are out of the range of one of the robot sensors (Lidar), meaning that in some configurations the robot has a high chance of colliding with them. The obstacles are static, but unknown to the planner. Similarly, some corridors are known to be dark, which means that they will be non-navigable if the robot is using light-sensitive sensors. To enable visual localization, ArUco markers are spaced every 2m on the walls. Figure 4 shows the map used, with the known dark corridors and preplaced obstacles, as well as an example of ArUco markers in the lower right.

The robot has three speed settings: (i) safe (0.24m/s) meaning that collisions with walls or obstacles do not cause damage to them or the robot, but the probability of mission success is diminished because they may block the robot, (ii) normal (0.35m/s) the starting speed of the robot for all experiments, and (iii) high (0.68m/s). This setup allowed us to explore an interesting range of adaptations where multiple adaptations of architecture and missions could be found to complete the mission. To instigate adaptation, perturbations of the robot or environment include turning off lights in the environment, causing sensor failure, or killing the localization node (simulated software crash) while the robot is conducting a mission.

Figure 4: Map used for evaluation and ArUco markers.

The goal of the planner is to find plans that will optimally complete a mission by finding a combination of software architecture, path through the environment, and speed, to reach a goal. The path is a series of waypoints – the underlying robot navigation software controls how to get from one waypoint to another. In our scenario, the planner can be used to optimize three different utility functions: (a) favor timeliness will favor plans that reach the goal quickly; (b) favor efficiency will choose plans that minimize battery consumption; and (c) favor safety will search for plans that minimize the chance of damaging collisions with obstacles. This enables us to test the multi-dimensional quality aspect of our approach.

For efficiency, we defined the power consumption for each element in the architecture in milliwatt hours (mwh), based on physical experiments with the robot and documented power specifications of sensors. For timeliness and safety, we experimentally ran the robot at least eleven times over each segment in the map for every configuration and speed and calculated the average time and probability of collision from the collected data.

4.1 Experiment Setup and Results

4.1.1 Run-time tractability. To show that our approach is tractable and works on real robot software we integrated it as a planner in Rainbow [16] and ran Rainbow in a loop on top of (mostly) existing third-party robotic software written for the Turtlebot described earlier. These missions took as input the waypoints to visit and instructed the robot accordingly. We used the standard ROS node MoveBase[42] for navigation between waypoints.

We simulated the robot using the Gazebo simulator [18] v7.9, with a world generated from our map, including walls with spaced ArUco markers and physics (e.g., lighting, gravity, friction, mass). We added plugins to simulate power consumption, in addition to using standard simulations for the sensors and actuators. We customized Rainbow, developing probes, gauges, and models to interact with the robot. We also developed analyses for mission and robot state, architecture, and power. Finally, we wrote an adaptation manager implementing the approach described in this paper and integrated it with Alloy and PRISM. The adaptation manager synthesizes plans encoded as instruction graphs given to the robot which manages configuration and mission changes.

The starting condition of each test was a tuple (start_waypoint, target_waypoint, start_configuration, utility_preference). To enable the comparison, we ran each test under three conditions: (A) no perturbations, and no adaptation; (B) same as A, but with perturbations, and (C) same as B but with adaptation enabled. When the test
Figure 5: Differences in reconfigurations and predicted utility during comprehensive testing.

driver determined that the test was finished (mission completed, no solution found, or timed out), it used ground truth readings of the current state of the robot and location in the world to evaluate the mission. A test case was graded Pass if the C condition got closer to the target than B and did so with better utility (i.e., how much time it took, how much battery was left over, whether the robot hit anything in the environment). It was graded inconclusive if both the B and C conditions performed the mission similarly, and Fail if the C condition completed the missions worse than B.

In total, we ran 838 test triples (a total of 2514 runs), in which 272 of the cases failed A condition. These triples included a random distribution of perturbations including killing both node and sensor. Our results were that adaptation restored mission success and utility score. Of the 838 test cases, 646 passed, 21 failed, and 171 were inconclusive. Interestingly, of the 272 cases where A failed, adaptation allowed mission success in 170 (62.5%) of those cases.

4.1.2 Co-adaptation quality improvement. One of the important aspects of our approach is that allowing a planner to co-adapt task and architecture models will result in better plans. To evaluate this, we ran experiments comparing Adapting only architecture vs. adapting architecture and mission, exploring more exhaustively the adaptation state space. Exhaustive exploration is challenging because of the number of tests that need to be considered. For the example above, we want to test all missions under each starting configuration favoring each of the utilities, allowing each perturbation and lighting condition which yields 297,420 starting conditions.

In total, we ran 838 test triples (a total of 2514 runs), in which 272 of the cases failed A condition. These triples included a random distribution of perturbations including killing both node and sensor. Our results were that adaptation restored mission success and utility score. Of the 838 test cases, 646 passed, 21 failed, and 171 were inconclusive. Interestingly, of the 272 cases where A failed, adaptation allowed mission success in 170 (62.5%) of those cases.

<table>
<thead>
<tr>
<th>Table 3: Timing (in s) for different planning characteristics. Δ indicates the change when considering architecture only.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base (mean)</td>
</tr>
<tr>
<td>Reconfig. planning</td>
</tr>
<tr>
<td>Path finding</td>
</tr>
<tr>
<td>Task planning</td>
</tr>
<tr>
<td>Total time</td>
</tr>
</tbody>
</table>

Table 5 shows the time data for the planner under different conditions. The time to construct the Alloy and PRISM files from templates was negligible and so was not considered. First, in the base planner case, the planner takes on average 15.1s, spending 5.57s generating configurations (which involves finding valid new configurations using Alloy and then PRISM to construct reconfiguration plans), 3.59s using Dijkstra’s algorithm to generate paths, and 5.94s model checking reconfigurations against the selected paths to generate the most optimal plan. When only considering reconfigurations, there is a significant difference in the amount of time that the planner takes (saving >7%, mostly because it does not need to generate alternative paths, only model checking on the existing path to determine the best reconfiguration). With an average task execution time of 224s, this represents a 3.1% increase in time using our approach. Furthermore, if we analyze the uncategorized results, we determine that for this additional time, adaptation finds 4636 (12.46%) more solutions with good utility (i.e., adaptation with > 0.5 utility). Also, the overall increase in utility is 0.09 (9%) across solutions found. This indicates that the extra time spent to find these better adaptations is worth it in this domain.

5 RELATED WORK

Our work draws from several research areas, such as self-adaptive systems [12, 24], formal specification/synthesis of software architectures [3, 27, 32], and probabilistic model checking [21, 28, 45].
Self-adaptive systems. Including our own prior work, discussed in Section 1, support for generation of optimal structure that also considers the richer context of task execution as a primary concern in self-adaptive systems is still limited. Tajalli et al. [49] introduce an approach that uses planning via model checking and architecture-based mechanisms for adaptation, and Sykes et al. [47, 48] introduce assembly of configurations, using extra-functional information to guide the process. These approaches do not account for any uncertainties or dependencies among domain facets that might impact task completion or qualities.

Self-adaptation in cyber physical systems (CPS) is a cross-layer concern, where using multiple feedback loops and models poses challenges that remain mostly unaddressed, mapping concerns to layers and adaptation mechanisms, coordination of adaptation mechanisms within and across layers, achieving system-wide consistency of adaptation [37]. Recent work started addressing some of these challenges: MORPH [6] is a reference architecture to improve consistency among configuration and behavior management that advocates separating reconfiguration and behavior strategy synthesis, and reconciling them posteriori when they are selected for execution. Compared to MORPH, our approach attempts to preserve combined quantitative guarantees of the reconfiguration and behavior strategies by synthesizing them semi-independently (separate solvers, but exchanging information among them). Borda et al. [5] tackle compositional verification by proposing a language to model self-adaptive CPS, although without incorporating any solution synthesis mechanisms. Gerostathopoulos et al. [19] introduce an approach that uses homeostasis as a principle to maintain operational state by adjusting a fixed set of adaptation strategies.

Formal specification and synthesis of software architectures. Some architecture synthesis approaches [3, 32] focus on structural properties. In addition to that, more recent approaches [7, 8] also consider behavioral, quantitative, and probabilistic aspects of system descriptions to optimize quantitative guarantees of generated architectures under uncertainty. However, these have limited support to reason about the wider context of a system in terms of the tasks that have to be performed and the mechanisms available to achieve self-adaptation. Within the large body of work on software architecture for robotics [1], only a small subset of approaches consider the wider context of tasks or self-adaptive capabilities: Park et al. [38] introduce a task-based approach that generates optimal software architecture to make robots provide service reliably with limited resources. Edwards et al. [14] introduce an approach that relies on architectural middleware to ensure consistency between a system’s architecture and its implementation. These approaches are not equipped to reason under uncertainty or produce specifications of task plans that go beyond reconfiguration of the architecture.

Quantitative verification/planning under uncertainty. Planning in partially unknown environments for robotics has already been explored in various works [20, 31, 34]. Out of these approaches, the closest to ours [31] generates mobile robot controllers with probabilistic time-bounded guarantees on successful task completion, which also try to satisfy other soft goals. Task specifications are analysed using multi-objective MDP model checking, providing an efficient mechanism for exploring the task solution space, but has limited support to capture the richer execution context in the planning, including the software running on the robot.

6 DISCUSSION AND FUTURE WORK
In this paper we have presented a framework for self-adaptation in mobile robotics that considers interdependencies among multiple domain facets (and in particular, between architecture and task plans), multiple tradeoffs, and uncertainty. To the best of our knowledge, other existing approaches sometimes cover changes only to the task plan or to the architecture, while in other cases, they are not able to consider uncertainties and dependencies that impact adaptation outcomes and quantitative guarantees (cf., Section 5). While we have focused on mobile service robots, we believe that our approach would also apply in other domains where dependencies exist between structure and behavior, e.g., patrolling drones, assisted living [33], and disaster recovery [39].

We have shown that combining formal methods with complementary strengths allows reasoning about both structural and behavioral adaptation a rich trade-off space and under uncertainty: including simple behavioural models to models with richer structure and semantics (e.g., architecture and environment).

Our results show that divide-and-conquer reconfiguration and task planning while still considering their dependencies leads to remarkable improvements over considering only one of them, or treating them as independent problems, and that the resulting implementation is tractable within reasonable time constraints for the class of application we describe.

Despite the advantages shown by our approach, our study includes the following limitations: (L1) Specific type of mobile robotics scenario and mission, (L2) Simplified architectural model, in which we assume a restricted set of valid configurations that the planner can consider, consisting of the software components, their connections, and a limited set of configuration parameters, (L3) Generating formal specifications from information exposed through views is view-specific and hand-coded, (L4) Evaluation run in simulation only. This potential limitation is mitigated somewhat in the independent evaluation (Section 4.1.1), which was run on a real mission using the robot’s full software stack, under a high-fidelity simulated environment.

In future work, we will address (L1) by exploring our approach in other domains mentioned above to provide a broader assessment of its generalizability. We will address (L2) by exploring the extension of our approach using machine learning to help improve the scalability in larger configuration spaces, extending our preliminary work in this direction [26]. We will address (L3) by investigating how to streamline model integration using tools and languages designed for model transformations like ATL and QVT [22].

ACKNOWLEDGMENTS
This material is based on research sponsored by AFRL and DARPA under agreement number FA8750-16-2-0042. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the AFRL, DARPA or the U.S. Government.

REFERENCES


