Minimum-violating Planning with Conflicting Specifications

Jana Tůmová, Luis I. Reyes-Castro, Sertac Karaman, Emilio Frazzoli, Daniela Rus

Abstract—We consider the problem of automatic generation of control strategies for robotic vehicles given a set of high-level mission specifications, such as “Vehicle \( x \) must eventually visit a target region and then return to a base,” “Regions \( A \) and \( B \) must be periodically surveyed,” or “None of the vehicles can enter an unsafe region.” We focus on instances when all of the given specifications cannot be reached simultaneously due to their incompatibility and/or environmental constraints. We aim to find the least-violating control strategy while considering different priorities of satisfying different parts of the mission. Formally, we consider the missions given in the form of linear temporal logic formulas, each of which is assigned a reward that is earned when the formula is satisfied. Leveraging ideas from automata-based model checking, we propose an algorithm for finding an optimal control strategy that maximizes the sum of rewards earned if this control strategy is applied. We demonstrate the proposed algorithm on an illustrative case study.

I. INTRODUCTION

Control strategy synthesis for robotic systems with high-level, complex, formally-specified goals has recently gained considerable attention in the robotics literature. A diverse set of techniques, including sampling and cell decomposition of the environment based on triangulations and rectangular partitions have been used to obtain discrete models of robotic systems; and a variety of temporal logics, including the Computation Time Logic (CTL) [18], Linear Temporal Logic (LTL) [3], [16], [17], [21], [23], and \( \mu \)-calculus [13], [14] have been successfully utilized to express complex missions that arise in robotics applications. All these references focus on the control synthesis problem: find a control strategy that satisfies the given specification, if one exists; and report failure otherwise.

The usual execution of many robotic systems, however, involves cases when the mission specification can not be satisfied as a whole. Yet, in most such examples, it is desirable to synthesize a control strategy that fulfills the most important rules, although by (temporarily) violating some of the less important ones. Consider, for example, an autonomous car navigating in urban traffic. The car must reach its final destination while abiding by the rules of the road, in particular, staying in the right lane and avoiding collision with obstacles. However, for this robot (and a human driver), it is more important not to collide with any other car or pedestrian, than to stay in its own lane. In fact the latter rule is temporarily violated, for instance, when taking over a parked car. Another example is from the popular literature. Isaac Asimov’s “three laws of robotics” (see [1]) defines how robots shall interact with humans. According to these laws, a robot may violate any order given by a human operator, if another human life comes in danger. Hence, the latter rule is issued a higher priority than the former one.

Motivated by these examples, in this paper, we consider the problem of least-violating control synthesis, i.e., finding a control strategy that satisfies the most important pieces of the mission specification, even if the mission specification can not be fulfilled as a whole. The problem can be described as follows. Consider a deterministic transition system that models the robot and its environment. The states of the transition system may encode a select set of configurations of the robot (or \( n \) robots). Each state of the transition system is labeled with a set of atomic propositions. Examples for atomic propositions include “The robot is in a safe region,” or “The first robot is in region \( A \),” etc. A list of mission specifications, including tasks that need to be fulfilled and rules that must be obeyed, is given in the form of linear temporal logic. Each specification in the list is assigned a priority. Roughly speaking, the least-violating synthesis problem is to find a trace over the transition system that satisfies as many high-priority tasks as possible.

Our work is related to [19], [20], where the authors study the following problem: given an LTL specification and a model that does not satisfy this specification, decide whether or not the invalidity is limited to the provided model. Related literature includes also [4], where the authors aim to pinpoint the (un)realizable fragments of the specification to reveal causes of the specification violation.

Other related work includes the recent literature that aims to construct control strategies with minimal changes in the input. On one hand, in [7], [15], the authors aim to find a specification that (i) can be satisfied by the given model, and (ii) is close to the original specification according to a suitable metric. On the other hand, in [11] the author focuses on finding the least set of constraints (in the model) violating which results in the satisfaction of the specification.

Arguably, our work in this paper is closest to the one presented in [6], where the authors consider a transition system with the variables partitioned into control inputs for the car, controllable environment variables and disturbances. The mission specifications are captured as an ordered set of LTL formulas \( \Phi = (\phi_1, \ldots, \phi_n) \). The goal is to find the maximal index \( 1 \leq m \leq n \) and a strategy for the robot ensuring the satisfaction of the subset of formulas \( (\phi_1, \ldots, \phi_m) \) regardless of the environmental disturbances.

This work is supported in part by Michigan/AFRL Collaborative Center on Control Sciences, AFOSR grant FA 8650-07-2-3744, the US National Science Foundation, grant CNS-1016213, and the National Research Foundation of Singapore, through the Future Urban Mobility SMART IRG.

J. Tůmová is with Masaryk University, L. I. Reyes-Castro, S. Karaman, E. Frazzoli and D. Rus are with Massachusetts Institute of Technology (MIT). This work was initiated while the first author was visiting at MIT and Singapore-MIT Alliance for Research and Technology.
Variants of this problem have been addressed also from the perspective of control theory. For instance, in [5], the authors consider a system modeled as a Markov decision process and a set of specifications given in the form of Büchi automata, say $A_1,\ldots,A_n$, each of which is assigned a reward, say $rew_1,\ldots,rew_n$. They aim to find a strategy maximizing the total reward gained for the specifications weighted by the respective probabilities with which they are satisfied.

The solution builds on translating the problem into a linear programming problem. Unfortunately, the time complexity of their algorithm is exponential in the size of the automata.

In contrast, our approach takes as input a deterministic transition system, a set of LTL formulas $\phi_1,\ldots,\phi_n$ with rewards $rew_1,\ldots,rew_n$, and we aim to construct a strategy maximizing the total reward gained for the specification that are satisfied. We build the solution on automata-based approach to model checking, which allows us to avoid exponential complexity (in the size of the input automata).

The contribution of this paper can be summarized as follows. We propose an algorithm for finding a least-violating trajectory, when the given specification can not be satisfied as a whole. As opposed to a “brute-force solution” enumerating all the possible subsets of specifications and attempting to find a strategy for each subset, we build our solution on a single control strategy synthesis procedure, thus substantially reducing the overall computational cost. We demonstrate the proposed approach in an illustrative example.

II. Preliminaries

Given a set $S$, let $|S|$, $2^S$, and $S^\omega$ denote the cardinality of $S$, the set of all subsets of $S$, and set of all infinite sequences of elements of $S$, respectively. A finite and infinite sequence of elements of $S$ is called a finite and infinite word over $S$, respectively. Given a finite word $w$ and a finite or infinite word $w'$ over $S$, we use $w \cdot w'$ and $w'' = w \cdot w' \cdot w''$ to denote the word obtained by concatenation of $w$ and $w'$, and by infinitely many repetitions of $w$, respectively.

A. Model and Specification

Definition 1 (Transition System) A labeled deterministic transition system is a tuple $T = (S, s_{init}, R, \Pi, L)$, where $S$ is a finite set of states; $s_{init} \in S$ is the initial state; $R \subseteq S \times S$ is a deterministic transition relation; $\Pi$ is a set of atomic propositions; $L : S \rightarrow 2^H$ is a labeling function.

A trace of $T$ is an infinite sequence of states $s = s_0s_1\ldots$ such that $s_0 = s_{init}$ and $(s_i,s_{i+1}) \in R$, for all $i \geq 0$. A trace $s = s_0s_1\ldots$ produces a word $w(s) = L(s_0)L(s_1)\ldots$.

Definition 2 (Formulas of the LTL) LTL formulas over the set $\Pi$ of atomic propositions are constructed inductively according to the following rules:

$$\psi ::= \top \mid \neg \psi \mid \phi \land \psi \mid X \phi \mid \phi U \psi,$$

where $\top$ is a predicate that is always true, $\pi \in \Pi$, $\neg$ (negation) and $\land$ (conjunction) are standard Boolean operators and $X$ (next) and $U$ (until) are temporal operators.

LTL formulas are interpreted over infinite words over $2^H$, such as those generated by the transition system from Def. 1. Informally speaking, the word $w = w(0)w(1)\ldots$ satisfies the atomic proposition $\pi$ (denoted by $w \models \pi$), if $\pi$ is satisfied in the first position of the word $w$, i.e., if $\pi \in w(0)$.

The formula $X \phi$ states that $\phi$ holds in the following state. The formula $\phi_1 U \phi_2$ states that $\phi_2$ is true eventually, and $\phi_1$ is true at least until $\phi_2$ is true. Furthermore, we define formulas $F \phi \equiv \top U \phi$ and $G \phi \equiv \neg (F \neg \phi)$ that state that $\phi$ holds eventually and always, respectively. LTL formulas can express various long term missions, including surveillance ($G^F \phi$, always eventually visit $\phi$), global absence ($G \neg \psi$, globally avoid $\phi$), reactivity ($G F \phi \Rightarrow G F \phi_2$, if $\phi_1$ holds in the future for all times, then so must $\phi_2$), among many others.

The language of all words that satisfy an LTL formula $\phi$ is denoted by $L(\phi)$. With a slight abuse of notation, we extend the satisfaction relation to traces of $T$, i.e., a trace $\tau$ satisfies $\phi$ (denoted by $\tau \models \phi$) if and only if the word $w$ produced by $\tau$ satisfies $\phi$. Similarly, a word $w$ and a trace $\tau$ satisfies a set of formulas $\Phi$: $(w \models \Phi$ and $\tau \models \Phi$) if and only if $w \models \phi$ and $\tau \models \phi$, for all $\phi \in \Phi$, respectively.

Given a formula $\phi$, we use $|\phi|$ to denote the size of the formula, i.e., the number of operators present in $\phi$, and we use $|\Phi|$ to denote $\sum_{\phi \in \Phi} |\phi|$.

Definition 3 ($\omega$-Automaton) An $\omega$-automaton is a tuple $A = (Q, q_{init}, \Sigma, \delta, Acc)$, where $Q$ is a finite set of states; $q_{init} \in Q$ is the initial state; $\Sigma$ is an input alphabet; $\delta \subseteq Q \times \Sigma \times Q$ is a non-deterministic transition relation; $Acc$ is the acceptance condition.

The semantics of $\omega$-automata are defined over infinite input words over $\Sigma$ (such as those generated by transition system from Def. 1 if $\Sigma = 2^H$). A run of the $\omega$-automaton $A$ over an input word $w = w(0)w(1)\ldots$ is a sequence of states $q = q_0q_1\ldots$, such that $q_0 = q_{init}$, and $(q_i, w(i), q_{i+1}) \in \delta$, for all $i \geq 0$. A finite run over a finite word $w_{fin} = w(0)\ldots w(l)$ is a finite sequence of states $q_{fin} = q_0\ldots q_{l+1}$, such that $(q_i, w(i), q_{i+1}) \in \delta$, for all $i \in \{0,\ldots,l\}$.

A run $\rho = q_0q_1\ldots$ is accepting if it satisfies the acceptance condition $Acc$. For Büchi automata (BA), $Acc$ is a set of states $F \subseteq Q$, and $\rho$ is accepting if it intersects $F$ infinitely many times. For generalized Büchi automata (GBA), the acceptance condition is a set of sets of states $F = \{F_1,\ldots,F_m\} \subseteq 2^Q$ and $\rho$ is accepting if it intersects $F_i$ infinitely many times for all $F_i \in F$. A word $w$ is accepted by $A$ if there exists an accepting run over $w$. The language of all words accepted by $A$ is denoted by $L(A)$.

An $\omega$-automaton is non-blocking if for all $q \in Q, \sigma \in \Sigma$ there exists $q' \in Q$, such that $(q,\sigma, q') \in \delta$. For each $\omega$-automaton $A = (Q, q_{init}, \Sigma, \delta, Acc)$ a language equivalent non-blocking $\omega$-automaton can be constructed simply by adding a new state $g_{new}$ to $Q$ and introducing a transition $(q,\sigma, g_{new})$ for all $q \in Q \cup \{g_{new}\}, \sigma \in \Sigma$, satisfying the property that $(q,\sigma, q') \notin \delta$ for all $q' \in Q$.

Definition 4 (GBA to BA) A generalized Büchi automaton $G = (Q_0, q_{init}, G, \Sigma, G_\delta, G_F = \{F_1,\ldots,F_m\})$, can be translated into a Büchi automaton $B = (Q, q_{init}, \Sigma, \delta, F)$, such that $L(B) = L(G)$ as follows: $Q = Q_0 \times \{1,\ldots,m\}; q_{init} =$
(q_{\text{init}}, q, 1); F = F_1 \times \{1\}; and \((q, j), \sigma, (q^*, j')\) ∈ δ if and only if \((q, \sigma, q')\) ∈ δ_G, and
   \begin{itemize}
   \item q ∉ F_j and j' = j, or
   \item q ∈ F_j and j' = (j \mod m) + 1.
   \end{itemize}

**Definition 5 (Automata Intersection)** Given n Büchi automata \(B_1, \ldots, B_n\) where \(B_i = (Q_i, q_{\text{init}}, i), \Sigma, \delta_i, F_i\) for all \(1 ≤ i ≤ n\), a Büchi automaton \(B = (Q, q_{\text{init}}, i), \Sigma, \delta, F\), such that \(L(B) = L(B_1) \cap \cdots \cap L(B_n)\) can be built as follows: \(Q = Q_1 \times \cdots \times Q_n \times \{1, \ldots, n\}\); \(q_{\text{init}} = (q_{\text{init}}(1), \ldots, q_{\text{init}}(n), 1)\); \(F = F_1 \times F_2 \times \cdots \times F_n \times \{1\}\); and \(((q_1, \ldots, q_n, j), \sigma, (q_1', \ldots, q_n', j')) \in \delta\) if and only if \((q_i, \sigma, q_i') \in \delta_i\) for all \(i \in \{1, \ldots, n\}\), and
   \begin{itemize}
   \item q_j ∉ F_j and j' = j, or
   \item q_j ∈ F_j and j' = (j \mod n) + 1.
   \end{itemize}

Intuitively, the set of states of \(B\) can be viewed as \(n\) copies (layers) of the Cartesian product of the sets of states \(Q_1 \times \cdots \times Q_n\). Given a state \(q = (q_1, \ldots, q_n, i) \in B\), we denote by layer(q) the last element of the tuple, i.e., layer\(((q_1, \ldots, q_n, i)) = i\).

Any LTL formula \(\phi\) over \(\Pi\) can be translated into a Büchi automaton \(B_\phi\) with alphabet \(2^\Pi\), such that \(L(\phi) = L(B_\phi)\). A number of standard translation algorithms (see, e.g., [8], [10]) rely on a three-step procedure: First, the formula is normalized, second, it is translated into a generalized Büchi automaton and third, the obtained GBA is finally translated into a language-equivalent Büchi automaton (see Def. 4).

A weighted \(\omega\)-automaton \(A = (Q, q_{\text{init}}, \Sigma, \delta, Acc, W)\) is an \(\omega\)-automaton, where \(Q, q_{\text{init}}, \Sigma, \delta, Acc\) are defined in the usual way, and \(W: \delta \rightarrow \mathbb{N}\) is a function assigning a weight to each transition.

Let \(p = q_0q_1 \ldots q_{l+1}\) be an accepting run over \(\sigma = \sigma_0\sigma_1 \ldots \sigma_t\) and a finite run over \(\sigma_{\text{fin}} = \sigma_0 \ldots \sigma_l\) of a weighted Büchi automaton \(B\), respectively. We use \(\text{pr}((p, \rho)) = \{q_i, \ldots, q_k | q_i, q_k ∈ F\} \) and \(\text{pr}(\rho_{\text{fin}}) = \{q_i, \ldots, q_k | q_i, q_k ∈ F_P, 0 ≤ i ≤ k ≤ l\}\) to denote the set of all finite fragments of \(p\) and \(\rho_{\text{fin}}\) that begin and end in an accepting state and do not contain any other accepting state. Note that each accepting run \(p\) and each finite run \(\rho_{\text{fin}}\) corresponds to a unique sequence of fragments. With a slight abuse of notation, we use \(W(q_1 \ldots q_k) = \sum_{j=i}^{k-1} W((q_j, \sigma_j, q_{j+1}))\) to denote the sum of the weights between the states of fragment \(q_j \ldots q_k\) of a run \(\rho\) over \(\sigma\) (or a finite run \(\rho_{\text{fin}}\) over \(\sigma_{\text{fin}}\)).

**B. Automata-Based Model Checking and Strategy Synthesis**

Given a transition system \(\mathcal{T}\) and a Büchi automaton \(B\), the model checking problem is to prove or disprove that all traces of \(\mathcal{T}\) satisfy \(B\), whereas the control strategy synthesis problem is to find a trace of \(\mathcal{T}\) that satisfies \(B\). Both of these problems can be addressed by constructing a product automaton \(P\) that captures all the behaviors of \(\mathcal{T}\) satisfying \(B\) and searching for an accepting run of \(P\).

**Definition 6 (Product Automaton)** A product automaton of a transition system \(\mathcal{T} = (S, s_{\text{init}}, R, \Pi, L)\) and a BA \(B = (Q, q_{\text{init}}, \Sigma, \delta, F)\) is a Büchi automaton \(P = T \otimes B\) where \(Q_P = S \times Q; q_{\text{init}} = (s_{\text{init}}, q_{\text{init}}); F_P = S \times F;\) and \(((s, q), (s', q'))\) ∈ \(\delta_P\) if
   \begin{itemize}
   \item \((s, s') ∈ R\) and \((q, L(s), q')\) ∈ \(\delta\).
   \end{itemize}

The product automaton has a trivial alphabet, which is therefore omitted. An accepting run \(\rho\) of the product automaton projects onto a trace \(\tau\) of \(\mathcal{T}\) (denoted by \(\tau = \alpha(\rho)\)) that satisfies the property captured by the Büchi automaton \(B\). Vice versa, any trace of \(\mathcal{T}\) satisfying the property corresponds to an accepting run of the product automaton. Furthermore, if there exists an accepting run \(\rho_P\) of \(P\), then there exists an accepting run \(\rho'_P\) of \(P\) in a prefix-suffix structure, i.e., \(\rho_P = \rho_{\text{pref}} \cdot \rho_{\text{sat}}\) for some finite sequences \(\rho_{\text{pref}}\) and \(\rho_{\text{sat}}\) of states of \(P\), such that the first state of \(\rho_{\text{sat}}\) is an accepting state from \(F_P\).

The (weighted) product automaton can be viewed as a (weighted) graph \((V, E)\) with the set of vertices \(V\) equal to the set of states \(Q_P\) and the set of edges \(E\) (and their weights) given by the transition function \(\delta_P\) (and the weight function \(W_P\)) in the expected way. A simple path in \(\mathcal{P}\) is a sequence of states \(p_1 \ldots p_t\) such that \((p_j, p_{j+1}) \in \delta_P\), for all \(1 ≤ j < l\), and \(p_j = p_{j'} \Rightarrow j = j',\) for all \(i ≤ j, j' ≤ l\). A cycle is a sequence of states \(p_1 \ldots p_{t+1}\), where \(p_i \ldots p_t\) is a simple path and \(p_{t+1} = p_1\). A state \(p'\) reachable from \(p\) if there is a simple path from \(p\) to \(p'\).

**Definition 7 (Maximal simple distance)** The maximal simple distance from \(p_f \in F_P\) to \(p\) in a weighted product automaton \(P\) is the maximal sum of edge weights on a simple path \(p_1 \ldots p_t\) from \(p_1 = p_f\) to \(p_t = p\), such that \(p_i \in F_P\), for all \(1 ≤ j < l\).

Efficient graph search algorithms can be used for finding a prefix \(\rho_{\text{pref}}\) (a simple path from the initial state to an accepting state in the product graph) followed by a periodically repeated suffix \(\rho_{\text{sat}}\) (a cycle in the product graph containing an accepting state) of an accepting run \(\rho = \rho_{\text{pref}} \cdot \rho_{\text{sat}}\) (a lasso-shaped path in the product graph). One of the standard algorithms to do so is nested depth-first search (DFS) [2], successfully implemented, for instance, in the pioneer model checker SPIN [12]. The (worst-case) running time complexity of this algorithm is linear in time and space with respect to the size (the number of states and transitions) of the product automaton \(\mathcal{P}\).

**III. Problem Formulation and Approach**

Let us consider a robot moving in a partitioned environment with its motion capabilities modeled as a labeled transition system \(\mathcal{T} = (S, s_{\text{init}}, R, \Pi, L)\) from Def. 1. Each region
of the environment is modeled as a state of the transition system and the robot’s ability to move between two regions is represented as transition between the corresponding states. In case several controlled robots are placed in the environment, the states of the transition systems encode positions of all the robots in the environmental regions i.e., for k robots, a state corresponds to an k-tuple of regions, where the i-th element of the tuple is the region in which the i-th robot is placed. The transitions between the states reflect the simultaneous motion capabilities of all the robots. The labeling function \( L \) maps each state of the transition system to a subset of atomic propositions from \( \Pi \) that hold true in this state, such as “Vehicle \( x \) is in a safe region.”.

There is a set of high-level missions to be accomplished by the robotic system expressed as a set of LTL formulas \( \Phi = \{ \phi_1, \ldots, \phi_n \} \) over \( \Pi \) with priorities of their satisfaction determined by a reward function \( rew : \Phi \rightarrow \mathbb{N} \). The value \( rew(\phi_i) \) represents the reward that is gained if specification \( \phi_i \) is accomplished. Without loss of generality, from now on, we assume that \( rew(\phi_i) \geq rew(\phi_j) \), for all \( 1 \leq i \leq j \leq n \).

A trace \( \tau \) of the transition system \( T \), we define trace reward as the sum of the rewards of all formulas from \( \Phi \) that are satisfied on this run.

**Definition 8 (Trace Reward)** Reward of a trace \( \tau \) of \( T \) is
\[
rew(\tau) = \sum_{\{ \phi_i | \tau \models \phi_i \}} rew(\phi_i).
\]

We are now ready to formally state our problem of finding “the best” trace of \( T \), i.e., “the least violating” motion of the robot (or the robots) in the environment with respect to the given set of mission specifications.

**Problem 1**
- a transition system \( T = (S, s_{init}, R, \Pi, L) \);
- a set of LTL formulas \( \Phi = \{ \phi_1, \ldots, \phi_n \} \) over \( \Pi \); and
- a reward function \( rew : \Phi \rightarrow \mathbb{N} \),

find a trace \( \tau \) of \( T \) that maximizes \( rew(\tau) \) from Eq. 1.

**Remark 1** Note, that if \( rew(\phi_i) = 2^{n-i} \), for each formula \( \phi_i \in \Phi \), then the set \( \Phi \) is in fact ordered according to the standard lexicographic ordering. In other words, it is always more important to satisfy \( \phi_i \) than \( \phi_{i+1} \land \ldots \land \phi_n \).

A straightforward solution to Prob. 1 is to consider all the possible subsets \( \Phi_I = \{ \phi_i | i \in I \} \), \( I \subseteq \{1, \ldots, n \} \) of formulas from \( \Phi \) and to find a trace \( \tau_I \) of \( T \) satisfying \( \Phi_I \) if such a trace exists. The search can be done using one of the known model-checking algorithms (e.g., the automata-based algorithm from Sec. II). A trace \( \tau_I \) maximizing \( rew(\tau_I) \) among the found ones maps to the desired robot path. However, this brute-force solution is not efficient as it requires up to \( 2^n \) model-checking procedure runs in the worst case.

In this paper, we suggest a method to alleviate the high computational demand of this straightforward solution. The main idea builds on automata-based approach to model-checking. We construct a single weighted Büchi automaton \( B_{all} \) for formula \( \bigwedge_{\phi_i \in \Phi} \phi_i \) and capture the rewards of the LTL formulas through its weights. Then, a weighted product automaton \( P = T \otimes B_{all} \) is built and an optimal accepting run of \( P \) is sought using a modification of the nested-DFS algorithm, with the computational complexity only slightly worse in comparison to the original nested-DFS. Roughly speaking, instead of up to \( 2^n \) model-checking procedure runs, we perform only a single execution of an altered model-checking algorithm.

**IV. Problem Solution**

This section introduces our solution to Prob. 1 in detail. First, we present the construction of the weighted Büchi automaton \( B_{all} \) and the weighted product automaton \( P \). Second, the modified nested-DFS is given. Third, we discuss the solution correctness, completeness and complexity.

**A. Construction of the Weighted Automata**

Consider the set of mission specifications \( \Phi = \{ \phi_1, \ldots, \phi_n \} \) that are translated (e.g., using the algorithm from [8]) into generalized Büchi automata
\[
\mathcal{G}_{\phi_1} = (Q_1, q_{init,1}, \Sigma, \delta_1, F_1 = \{ F_{11}, \ldots, F_{1m_1} \}), \ldots,
\mathcal{G}_{\phi_n} = (Q_n, q_{init,n}, \Sigma, \delta_n, F_n = \{ F_{n1}, \ldots, F_{nm_n} \}),
\]
respectively. Without loss of generality, we assume that \( \mathcal{G}_{\phi_1}, \ldots, \mathcal{G}_{\phi_n} \) are all non-blocking. We build the weighted Büchi automaton \( B_{all} \) leveraging ideas from translation of generalized Büchi automata to Büchi automata (Def. 4) and from construction of a Büchi automaton for language intersection of several Büchi automata (Def. 5).

**Definition 9 (Weighted Büchi automaton)** A weighted Büchi automaton \( B_{all} = (Q, q_{init}, \Sigma, \delta, F, W) \) is defined as follows:
- \( Q = Q_1 \times \ldots \times Q_n \times \{(0,0),(1,1),\ldots,(1,m_1),(2,1),\ldots,(2,m_2),(n,1),\ldots,(n, m_n)\} \);
- \( q_{init} = (q_{init,1},\ldots,q_{init,n},(0,0)) \);
- \( t = ((q_1,\ldots,q_n, (j, l)), \sigma, (q'_{1},\ldots,q'_{n}, (j', l'))) \in \delta \) if \( (q_i, \sigma, q'_i) \in \delta_i \) for all \( i \in \{1,\ldots,n\} \), and
  1. \( (j, l) = (0,0) \) and 
    a. \( (j', l') = (0,0) \). Then \( W(t) = 0 \).
    b. \( j' > l' = 1 \). Then \( W(t) = rew(\phi_{j'} \wedge \phi_j) \).
  2. \( j \neq 0 \) and 
    a. \( (j', l') = (j, l) \) and \( q_j \notin F_j \). Then \( W(t) = 0 \).
    b. \( l \neq m_j, (j, l') = (j, l+1) \) and \( q_j \in F_j \). Then \( W(t) = 0 \).
    c. \( l = m_j, j < n, j \leq j', l' = 1 \) and \( q_j \in F_j \).
      Then \( W(t) = rew(\phi_{j'}) \).
    d. \( l = m_j, (j', l') = (0,0), \) and \( q_j \in F_j \).
      Then \( W(t) = 0 \).
- \( F = Q_1 \times Q_2 \times \ldots \times Q_n \times \{(0,0)\} \).

An example of the construction of \( B_{all} \) can be found in the extended version of this paper [22].

The automaton \( B_{all} \) accepts all words satisfying specifications \( \bigwedge_{\phi_i \in \Phi} \phi_i \), for all \( \Phi_I \subseteq \Phi \). The weights determine the “quality” of a particular run, i.e., they capture which
formulas are satisfied by this run. Formally, the purpose of weights is summarized in the following lemma.

**Definition 10 (Run Reward)** The reward of a run \( \rho \) of \( B_{all} \) is
\[
Rew(\rho) = \max \bigl\{ C \mid C = W(q_i \ldots q_l) \text{ for infinitely many } q_i \ldots q_l \in \text{Frag}(\rho) \bigr\}.
\]

Intuitively, a run \( \rho \) can be split into a sequence of fragments that is associated with a respective sequence of fragment weights. The run reward is equal to the maximal weight that appears in the sequence of fragment weights infinitely many times.

**Lemma 1** Consider a word \( w = w(0)w(1) \ldots \) where \( w \models \Phi_I \) and \( w \not\models \phi \), for all \( \phi \not\models \Phi_I \). There exists an accepting run \( \rho = q_0q_1 \ldots \) of \( B_{all} \) over \( w \), such that \( Rew(\rho) = \sum_{\phi_i \in \Phi_I} Rew(\phi_i) \). Furthermore, for each accepting run \( \rho' = q_0q_1' \ldots \) of \( B_{all} \) over \( w \) it holds, that \( Rew(\rho') \leq \sum_{\phi_i \in \Phi_I} Rew(\phi_i) \).

**Proof:** Follows from the construction of \( B_{all} \) and can be found in the extended version of this paper [22].

The second step in our algorithm is the construction of a product automaton \( P = \mathcal{T} \otimes B_{all} = (Q_P, p_{init}, \delta_P, F_P, W_P) \) (see Def. 6). Based on Lemma 1, the product automaton satisfies the following:

**Lemma 2** Let \( \tau \) be a trace of \( \mathcal{T} \). Then, there exists a run \( \rho_P \) of \( P \) such that the reward for the corresponding trace \( \tau = \alpha(\rho_P) \) on \( \mathcal{T} \) satisfies \( Rew(\tau) = Rew(\rho_P) \). Moreover, \( Rew(\tau) \geq Rew(\rho_P') \) for all \( \rho_P' \) with \( \alpha(\rho_P') = \tau \).

**Proof:** The proof follows directly from Lemma 1 and the fact that for each trace \( \tau \) that produces a word \( w = w(0)w(1) \ldots \) accepted by a run \( \rho = q_0q_1 \ldots \) of \( B_{all} \), there exists an accepting run \( \rho_P = p_0p_1 \ldots \) in \( P \), such that \( W((p_1, p_{i+1})) = W((q_i, w(i), q_{i+1})) \) and \( q_i \in F_P \iff p_i \in F_P \), for all \( i \geq 0 \).

**Lemma 3** For each run \( \rho_P \) there exists a run \( \rho_P' \) in prefix-suffix structure, such that \( Rew(\rho_P') = Rew(\rho_P) \).

**Proof:** Because \( \rho_P = p_0p_1 \ldots \) is infinite, there exist a state \( p \in F_P \) that appears on \( \rho_P \) infinitely many times and there exist a fragment \( \ldots p' \) starting in \( p \) such that \( W(p \ldots p') = Rew(\rho_P) \). Because \( p \) occurs on \( \rho_P \) infinitely many times, \( p \) is reachable from \( p' \). Therefore, run \( \rho_P \) is a sequence of states \( \rho_P = p_0p_1 \ldots p \ldots p' \ldots \). Let \( \rho_P = p_0p_1 \ldots (p \ldots p' \ldots p')^\omega \). Run \( \rho_P \) is in prefix-suffix structure, it is accepting and \( Rew(\rho_P') = Rew(\rho_P) \).

The two lemmas above provide us with guidance on computing the trace of \( \mathcal{T} \) with the maximal reward: it is enough to compute a run of \( \mathcal{P} \), in the prefix-suffix structure, that maximizes \( Rew(\rho_P) \) and project this run into a trace of \( \mathcal{T} \). This is stated in the following proposition.

**Proposition 1** Let \( \tau = s_0s_1 \ldots \) be a trace of \( \mathcal{T} \), such that \( \tau \models \Phi_I \) and \( \tau \not\models \phi \), for all \( \phi \not\models \Phi_I \). Then, there exists an accepting run \( \rho_P = (s_0, q_0)(s_1, q_1) \ldots \) in \( \mathcal{P} \) such that \( Rew(\rho_P) \) is in prefix-suffix structure and \( Rew(\rho_P) = \sum_{\phi_i \in \Phi_I} Rew(\phi_i) \).

The remaining task is to find a run \( \rho_P \) satisfying the condition (i) of Proposition 1 and maximizing \( Rew(\rho_P) \). The problem thus reduces to searching for a reachable cycle \( c \) (a repeated run suffix) in \( \mathcal{P} \) beginning (and thus also ending) in an accepting state that maximizes the value
\[
Rew(c) = \max_{p_i \ldots p_l \in \text{Frag}(c)} W(p_i \ldots p_l)
\]
among all such cycles. The following lemma helps narrow down the search even further, showing that it is enough to search for a particular type of cycle.

**Lemma 4** Given a cycle \( c \) in \( \mathcal{P} \) and a fragment \( p_i \ldots p_l \in \text{Frag}(c) \), there exists a simple path \( p_i \ldots p_l \), such that \( W(p_i \ldots p_l) = 0 \).

**Proof:** From the construction of the automaton \( B_{all} \), it follows that if there is a simple path from \((q_1, \ldots, q_n, (0,0)) \in Q \) to \((q'_1, \ldots, q'_n, (i,j)) \in Q \) in the automaton \( B_{all} \), then there exists a simple path from \((q_1, \ldots, q_n, (0,0)) \in Q \) to \((q'_1, \ldots, q'_n, (0,0)) \) that contains only states \( q \in Q \), such that \( layer(q) = (0,0) \). Thus, if there is a simple path from \((s, q_1, \ldots, q_n, (0,0)) \in Q \) to \((s', q'_1, \ldots, q'_n, (i,j)) \in Q \) in the product automaton \( \mathcal{P} \), then there exists also a simple path from \((s, q_1, \ldots, q_n, (0,0)) \) to \((s', q'_1, \ldots, q'_n, (0,0)) \) that contains only states \( p \in Q \), such that \( layer(p) = (0,0) \) The reward of such a simple path is 0.

Thanks to Lemma 4, it is enough to search for a cycle \( c \) maximizing Eq. 2, such that \( W(p_i \ldots p_l) = 1 \), for all fragments \( p_i \ldots p_l \in \text{Frag}(c) \), but one. Hence, without loss of generality, we can consider only cycles \( c = p_1 \ldots p_{i+1} \ldots p_l \) such that \( W(p_1 \ldots p_l) \neq 1 \) only for the first fragment \( p_1 \ldots p_{i+1} \) of the cycle. Such a cycle can be found by adapting standard nested depth-first search algorithm as we will show in the following section.

**Proposition 2** A maximal-reward trace of \( \mathcal{T} \) can be obtained as a projection \( \alpha(p_1 \ldots p_l) \cdot (\alpha(e))^\omega \) of a path \( p_0 \ldots p_l \) and a cycle \( c = p_{i+1} \ldots p_{i+1} \ldots p_l \), such that
- \( p_0 = q_{init} \), \( p_{i+1} \in \delta, p_{i+1} \in F_P \),
- \( W(p_j \ldots p_k) = 1 \), for all fragments \( p_j \ldots p_k \) in \( \text{Frag}(p_{i+1} \ldots p_{i+1}) \), and
- \( W(p_{i+1} \ldots p_l) \) for the first fragment \( p_{i+1} \ldots p_l \) in \( \text{Frag}(c) \) of the cycle is maximized.

**B. Weighted Nested Depth-First Search**

This section aims at searching for a path \( p_0 \ldots p_l \) followed by a cycle \( p_{i+1} \ldots p_{i+1} \) satisfying conditions of Prop. 2. The solution is summarized in Alg. 1 to Alg. 3.

First, let us focus on a solution of the following subproblem: Given an accepting state \( p_f \in F_P \), find a cycle that maximizes value in Eq. 2 among all cycles that begin and end in \( p_f \). A modification of breath-first graph search algorithm can be used to do so as described in Alg. 3. Intuitively, the
Algorithm 1 weighted_nested_DFS(P)

**Input:** product automaton P

**Output:** solution to Prob. 1
1. weight_max = 0; prefix_max = ε; cycle_max = ε
2. stack_outer = empty; visited_outer = ∅
3. visited_inner = ∅; visited_ps = ∅
4. for all p ∈ Qp do
5. p.dist = 0; p.pred = ⊥
6. end for
7. run := DFS(P, pinit)
8. if run ≠ ε then
9. return trace := α(run)
10. else
11. return find_arbitrary_trace(T)
12. end if

The algorithm systematically searches the graph P and maintains in p.dist the approximation of the maximal simple distance (Def. 7) from p₁ to p, for each state p. The correctness of the algorithm relies on the fact that when p is processed on line 2 of the procedure propagate (Alg. 4), the value of p.dist is set to the actual maximal simple distance from p₁ to p. When all states that are reachable from state p₁ are visited in Alg. 4, the second phase (lines 14-25) of Alg. 3 is executed to check whether p₁ is also reachable from p, considering p one by one in descending order of their dist.

Second, the cycle satisfying conditions of Prop. 2 can be found by running Alg. 3 from each p₁ ∈ F reachable from the initial state, potentially traversing the whole graph |F|-times. However, leveraging ideas from nested DFS algorithm, the complexity can be reduced. The idea is to run Alg. 3 from states in F₁ in particular order that ensures the states visited during previous executions of Alg. 3 do not need to be visited again. The correctness of this idea is based on the correctness of the standard nested DFS and the following lemma.

**Lemma 5** Let p₁ ∈ F be reachable from p₁ ∈ F₁ and p ∈ Q₁ be reachable from both p₁ and p₁. If there exists a cycle c from state p₁ ∈ F₁ containing state p, then there exists a cycle c’ from p₁ ∈ F with reward Rew(c’) ≥ Rew(c).

**Proof:** Because p₁ is reachable from p, p is reachable from p₁, and p₁ is reachable from p₁, then p₁ is reachable from p₁. Therefore, there exists a cycle c’ = p₁...p₁...p...p₁...p₁, where p₁...p...p₁ = c. Clearly Rew(c’) ≥ Rew(c).

The overall solution can be summarized as follows:
1) Each of the formulas φ ∈ Φ is translated into a generalized Büchi automaton Gφ.
2) A weighted Büchi automaton B_all is built (see Def. 9).
3) A weighted product automaton P = T ⊗ B_all is constructed (see Def. 6).
4) Alg. 1 is run on P.

**Correctness and Correctness:** Based on Lemmas 1–5 and Propositions 1–2, the soundness and completeness properties of the algorithm are summarized in the following theorem.

**Theorem 1 (Soundness and completeness)** Given a transition system T, a set of LTL formulas Φ and the reward function rew, the suggested algorithm returns solution to Prob. 1.

C. Complexity Analysis

**Theorem 2** Let |T| and |Φ| denote the size of the input transition system and the size of the missions specification, respectively. The computational complexity of Alg. 1 is in O(|P| · log |P|), where |P| is the size of the product automaton, which is in O(|T| · 2O(|Φ|)).

1) Discussion: The translation from an LTL formula φ into a generalized Büchi automaton can be done in in
$2^{|\phi|}$ time and space. In particular, one of the well-known translation algorithms \cite{DBLP:journals/tcs/Rutten00} transforms $\phi$ into a generalized Büchi automaton with at most $2^{|\phi|}$ states and $|\phi|$ sets in its acceptance condition. If the obtained GBAs for specifications $\phi_1, \ldots, \phi_n \in \Phi$ are all non-blocking, the worst-case size of $B_{\text{all}}$ is $2^{|\Phi|} \cdot (1 + |\Phi|)$. On the other hand, in case $k$ of the obtained GBAs are blocking, the worst-case size of $B_{\text{all}}$ is $2^{|\Phi|+k} \cdot (|\Phi| + k + 1)$. Although the size of the resulting GBA is exponential with respect to the size of the input specification, the sizes of the individual formulas are usually small and in many cases, the GBAs are significantly smaller than the worst-case bound. Many optimization techniques have been also developed among the formal methods literature to reduce the sizes of the GBAs.

The size of the product automaton $P$ is $|T| \cdot |B_{\text{all}}|$ in the worst case, with at most $|T| \cdot 2^{|\Phi|+k}$ in one layer, where $k$ is the number of blocking GBAs obtained in translation of the formulas from $\Phi$. The cumulative number of steps made in sorting the set $\text{search}_\text{from}$ on line 14 of Alg. 3 is bounded by O$(|L_P| \cdot \log |L_P|)$, where $|L_P| = \{p \in Q_P \mid \text{layer}(p) = (0,0)\}$ is the size of the initial layer of $P$. Altogether, the complexity of Alg. 1 is in $O(|P| + |L_P| \cdot \log |L_P|)$.

In contrast, the “brute-force” approach that tries to find a trace satisfying $\Phi_I$, for each $\Phi_I \subseteq \Phi$ has the worst time complexity characterized as follows. A Büchi automaton $B_{\Phi_I}$ for $\Phi_I$ can be constructed with $2^{|\Phi_I|} \cdot |\Phi_I|$ number of states in the worst case. A nested DFS algorithm is then run on $P = T \cdot B_{\Phi_I}$, reaching complexity $O(|P|)$. Hence, the solution is linear with respect to the size of $|T| \cdot \sum_{\Phi_I \subseteq \Phi} 2^{|\Phi_I|} \cdot |\Phi_I|$.

The benefit of our algorithm (Alg. 1) in comparison to the brute-force solution increases with the increasing number of non-blocking GBAs obtained from the translation from LTL formulas. Note, that for some LTL formulas, the smallest existing corresponding GBA is non-blocking. In particular many useful specifications, such as $F\phi$ (reachability), $G F \phi$ (surveillance), $G F \phi_1 \Rightarrow GF \phi_2$ (reactivity), $G(\phi_1 \Rightarrow F\phi_2)$ (response), or $F(\phi_1 \land F\phi_2)$ (sequencing), where $\phi, \phi_1, \phi_2$ are arbitrary Boolean combinations of atomic propositions, belong to this class.

V. RESCUE MISSION EXAMPLE

Let us consider an example of a complex military rescue mission. Assume that friendly units $F_1, F_2, F_3$ have been captured in an enemy territory. They are guarded by enemy units (called targets) $T_1, \ldots, T_7$, which need to be engaged before an autonomous vehicle can proceed to pick up the captured friendly units and bring them to the friendly base. A particular configuration is depicted in Fig. 1.a). While friendly units $F_1$ and $F_2$ can be rescued by engaging targets $T_1, T_4, T_7$, and $T_2, T_6, T_7$, respectively, unit $F_3$ can be rescued by engaging targets $T_3$ and $T_2$. Suppose that we have two unmanned aerial vehicles (UAVs) $V_1$ and $V_2$ and an autonomous ground vehicle $V_3$ under our command, with their capabilities and weaknesses as described below.

- $V_1$ can engage $T_1, T_3$, is vulnerable to $T_2, T_5$, and can engage $T_4, T_6, T_7$ at the cost of self-destruction (i.e., it can be sacrificed to engage a target $T_4, T_6, or T_7$).
- $V_2$ can engage $T_2, T_5$, is vulnerable to $T_1, T_3$, and can engage $T_4, T_6, T_7$ at the cost of self-destruction.
- $V_3$ can pickup and transport $F_1, F_2, F_3$, but is vulnerable to all active targets.

The mission is to rescue and pickup the friendly units $F_1, F_2$ and $F_3$ and bring them to the base (Base). At the same time, the goal is not to loose any of the vehicles...

Alg. 4 propagate($P, \text{queue}_\text{curr}, \text{queues}_\text{all}, \text{search}_\text{from}$)

1: repeat
  2: \hspace{1em} $p := \text{queue}_\text{curr}.\text{front and pop}()$
  3: if $p \notin \text{visited}_\text{inner}$ then
    4: \hspace{2em} \text{visited}_\text{inner} := \text{visited}_\text{inner} \cup \{p\}$
  5: \hspace{1em} for all $p' \in \text{succs}(p)$ do
    6: \hspace{2em} if $p'.\text{dist} < p.\text{dist} + W_P(p, p')$ then
      7: \hspace{3em} $p'.\text{dist} := p.\text{dist} + W_P(p, p')$; $p'.\text{pred} := p$
    8: \hspace{2em} if $\text{layer}(p') = 0 \land p' \notin \text{search}_\text{from}$ then
      9: \hspace{3em} $\text{search}_\text{from} = \text{search}_\text{from} \cup \{p'\}$
    10: end if
    11: \hspace{2em} if $\text{layer}(p') = \text{layer}(p)$ then
      12: \hspace{3em} $\text{queue}_\text{curr}.\text{push}(p')$
    13: \hspace{2em} else if $\text{layer}(p') = i$ for some $i \geq 1$ then
      14: \hspace{3em} $\text{queues}_\text{all}[i].\text{push}(p')$
    15: end if
  16: end if
  17: end for
  18: end if
  19: until $\text{queue}_\text{curr} = \text{empty}$
TABLE I: Mission specification.

<table>
<thead>
<tr>
<th>Mission Specification</th>
<th>LTL Formula: $\phi$</th>
<th>rew($\phi$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pickup $F_1$, and bring it to $Base$, for all $i \in {1, 2, 3}$</td>
<td>$F(p_{V_i}^F \land F(p_{Base}^V))$, for $i \in {1, 2, 3}$</td>
<td>10</td>
</tr>
<tr>
<td>Do not pick up $F_3$ before picking up $F_1$, for all $i \in {1, 2}$</td>
<td>$G(p_{V_i}^F \Rightarrow G(\neg p_{V_i}^F))$, for $i \in {1, 2}$</td>
<td>10</td>
</tr>
<tr>
<td>Do not lose vehicle $V_k$ and bring $V_k$ to $Base$, for all $k \in {1, 2, 3}$</td>
<td>$G(\neg a_{V_3}) \land F(p_{Base}^V)$, for $i \in {1, 2, 3}$</td>
<td>1</td>
</tr>
</tbody>
</table>

$V_1, V_2, V_3$. Let $p_{V_i}^F$, $p_{Base}^V$, and $a_{V_i}$ denote the atomic propositions “Vehicle $V_k$ is at the location of the friendly unit $F_j$”, “Vehicle $V_i$ is at $Base$”, and “Vehicle $V_i$ is active”, respectively. Individual goals are expressed as LTL formulas (see Table I) and assigned priorities through the reward function. The reward function, among others, specifies that saving the friendly units is more important than not loosing the vehicles $V_1, V_2, V_3$. Note, that because enemy target $T_7$ cannot be destroyed by any of the vehicles at no cost to their integrity, at least one vehicle must be sacrificed to save the friendly units. Although not so obvious, one can also observe that friendly units $F_1$ and $F_2$ cannot both be rescued.

In order to validate our algorithm, we developed a C++ implementation which takes as an input a deterministic transition system and a list of generalized Büchi automata obtained from the LTL formulas with the use of an off-the-shelf tool such as LTL2BA [9]. The reward gained if the optimal control strategy of the vehicles is applied is 22 units, as expected. Figures 1.(b)–1.(d) illustrate different stages of the system run. First, vehicles $V_1$ and $V_2$ engage enemy targets $T_1$ and $T_2$, respectively (Fig. 1.(b)). Then, $V_1$ destroys enemy target $T_2$ before launching a self-destructive attack on $T_4$ (Fig. 1.(c)). Later, vehicle $V_2$ engages enemy target $T_2$, and vehicle $V_3$ proceeds to pickup $F_1$ and $F_3$, in that order (see Fig. 1.(d)). Finally, the remaining vehicles return to $Base$.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have studied the least-violating controller synthesis problem, *i.e.*, roughly speaking, to find a trajectory that satisfies the most important pieces of the specification, when the specification can not be satisfied as a whole. We have proposed an algorithm that provides substantial computational savings when compared to a straightforward solution. We have analyzed the proposed algorithm in terms of correctness, completeness and computational complexity. We have also demonstrated the performance of the proposed algorithm on an illustrative example.

There are many directions for future work. In particular, synthesis of optimal strategies that are least violating, and also synthesis of such strategies to be implemented in dynamic environments are possible directions for future work.

REFERENCES