Online Safety Control of a Class of Hybrid Systems

Sherif Abdelwahed
sherif.abdelwahed@vaderbilt.edu

Gabor Karsai
gabor@vuse.vanderbilt.edu

Gautam Biswas
biswas@vuse.vanderbilt.edu

Institute for Software Integrated Systems
Vanderbilt University, Nashville, TN,

Abstract

In this paper we outline a supervisor synthesis procedure for safety control of a class of hybrid systems. The procedure is conducted online based on a limited exploration of the state space. We establish feasibility conditions for online controllability with respect to the safety specifications, and provide an upper limit for the accuracy error of the online controller.[1]

1 Introduction

Hybrid systems are dynamic systems with both discrete-event and continuous-time based components. Examples of hybrid systems include traffic networks, automotive systems, robots, and manufacturing systems. Considerable research work has been dedicated recently to the study of hybrid systems. See for example [1, 6] and the references therein.

In this paper, we present an online approach to the safety control of hybrid systems. The safety control problem requires the system to move to a predetermined safe region from a given set of initial states in the state space of the system. The proposed approach does not require the existence of a finite quotient equivalent for the system. Moreover, the approach can be adapted to accommodate possible changes in the system parameters that may occur as a result of a fault or parameter changes in time-varying systems.

The proposed procedure is conceptually similar to the model predictive control approach [5, 7] in which a limited time forecast of the process behavior at each state is optimized according to given criteria. Also related to our work is the limited lookahead supervision of discrete event systems (DES) [3]. In this approach a tree of all possible states is generated up to a given depth, then a control action is chosen to satisfy the specification. Online DES supervision was extended to a class of extended state machines in [2].

2 Switching Hybrid Systems

In this paper we consider a special class of hybrid systems, referred to as *switching systems*, with dynamics described by the discrete-time equation

$$\boldsymbol{x}(k+1) = \boldsymbol{\phi}(\boldsymbol{x}(k), \boldsymbol{r}(k))$$

where $k \in 0, 1, \ldots$ is the time index, $\boldsymbol{x}(k) \subset \mathbb{R}^n$ is the discrete state vector, and $\boldsymbol{r}(k) \subset \mathbb{R}^m$ is the discrete valued input vector at time k. We will use X and R to denote the state space and the input set for the system, respectively. We assume that the set of inputs R is finite. Boldface letters are used to denote vectors and vector-valued signals. For a vector $\boldsymbol{x}$ we will write x_i to denote its ith component.

The above representation is general enough to describe a wide class of hybrid systems, including nonlinear systems and piecewise linear systems. The requirement that the input set R is finite is typical in many practical computer-controlled systems, where the input is usually discrete and restricted within certain limits.

3 Online Safety Control

The problem of safety control is stated as follows. Given a switching system H and a set of safe states X_s and a set initial states $X_o \subseteq X$ where $X_s \subset X_o$, design a supervisor S that can drive the system from any state in X_o to X_s in a finite time using a finite sequence of inputs. In addition, the supervisor is required to keep the system stable within the set X_s.

We propose an online supervision algorithm that explores only a limited part of the system state space and selects the next input based on the available information about the current state. For the safety control problem, the selection of the next step is based on a distance map $D_s : \mathbb{R}^n \to \mathbb{R}$ that defines how close the current state is to the safe region. The distance map can be generally defined as follows: $D_s(\boldsymbol{x}) = 0$ for all points $\boldsymbol{x} \in X_s$ and for all other points ($\boldsymbol{x} \notin X_s$),

$$D_s(\boldsymbol{x}) = \min\{a \in \mathbb{R} \mid (\exists \boldsymbol{x}' \in X_s) \ \|\boldsymbol{x} - \boldsymbol{x}'\| = a\}$$

where $\|.\|$ is a proper norm for $\mathbb{R}^n$. In other words,

[1] Funded, in part, by the DARPA IXOs Software-Enabled Control Program under AFRL contract F33615-99-C-3611.

$D_s(\boldsymbol{x})$ is the minimal distance between $\boldsymbol{x}$ to the safe region X_s.

The online supervision algorithm starts by constructing the tree of all possible future states from the current state $\boldsymbol{x}_c$ up to a specified depth. To avoid the Zeno effect, in which the controller may try to preempt time indefinitely through continuous switching, we require that any input switching event is followed by at least one sampling period. The exploration procedure identifies the set of states with the minimal distance from X_s based on the distance map D_s. A state $\boldsymbol{x}_m$ is then chosen from this set based on certain optimality criterion (for example, minimal input switching), or simply picked at random. The chosen state is then traced back to the current state $\boldsymbol{x}_c$ and the event leading to $\boldsymbol{x}_m$ is used for the next step.

A hybrid system H is said to be *online controllable* in the region $X_o \subseteq X$ if there exists $\check{\delta}_{X_o} > 0$ such that for any partition $\{n^+, n^-\}$ of the set $[1 \dots n]$ there exists an input $\boldsymbol{r} \in R$ such that $(\forall \boldsymbol{x} \in X_o)(\forall i \in [1 \dots n])$,

$$\begin{aligned} i \in n^+ &\Rightarrow \phi_i(\boldsymbol{x}, \boldsymbol{r}) - x_i > \check{\delta}_{X_o}, \\ i \in n^- &\Rightarrow x_i - \phi_i(\boldsymbol{x}, \boldsymbol{r}) > \check{\delta}_{X_o} \end{aligned}$$

That is, H is online controllable in the region X_o if at any state $\boldsymbol{x} \in X_o$ it is always possible to find an input that can control the next step direction by incrementing some components of $\boldsymbol{x}$ and decrementing the other components.

Consider a hybrid system H which is online controllable within a region X_o. For a state $\boldsymbol{x}_o \in X_o$ write $\boldsymbol{\phi}_c(\boldsymbol{x}_o, k)$ for the state $\boldsymbol{x}(k)$ obtained from the online control algorithm after k time steps starting from $\boldsymbol{x}_o$. The *accuracy error* of the online controller within the region X_o and for a distance map D_s after k time steps is defined as follows,

$$E_k(X_o, D_s) = \min\{D_s(\boldsymbol{\phi}_c(\boldsymbol{x}_o, k)) \mid \boldsymbol{x}_o \in X_o\}$$

That is, $E_k(X_o, D_s)$ is the minimal distance to the safe region that can be obtained starting at any state in X_o after k time steps. The accuracy error of the online controller can be estimated based on the upper limit of the distance covered by the system in a single step. Write $\hat{\delta}_{X_o}$ for the maximal single step absolute change to any component in a state $\boldsymbol{x} \in X_o$ under any input from R, namely $\hat{\delta}_{X_o}$ is equal to

$$\max\{|\phi_i(\boldsymbol{x}, \boldsymbol{r}) - x_i| \mid \boldsymbol{x} \in X_o, \boldsymbol{r} \in R,\ i \in [1 \dots n]\}$$

Write $\hat{\boldsymbol{\delta}}_{X_o}$ for the vector $(\hat{\delta}_{X_o}, \dots, \hat{\delta}_{X_o})$.

Proposition 1 There exists $N > 0$ such that

$$(\forall k > N) \quad E_k(X_o, D_s) \leq 0.5\|\hat{\boldsymbol{\delta}}_{X_o}\|$$

□

Therefore, an online controllable system H can be driven by the online controller in finite time to a safe region $X_s \subseteq X_o$ with a maximum accuracy error of $0.5\|\hat{\boldsymbol{\delta}}_{X_o}\|$. In the implementation of the online control, the sets X_o and X_s are adjusted to take into account this accuracy error as well as the existence of measurement noise.

The parameters $\check{\delta}_{X_o}$, $\hat{\delta}_{X_o}$ can be used to reduce the search tree in the online control algorithm. The algorithm can safely stop exploring if there is no prospect of further reduction in the current minimal distance along any path starting from the current node up to the limit of the search tree. This can easily be determined using the values $\check{\delta}_{X_o}$, $\hat{\delta}_{X_o}$, and the predefined depth of the search tree.

4 Example: two-tank system

Consider the two tank system reported in [4] and shown in Figure 1. In this system, a liquid is pumped at a constant rate into Tank 1 through valve v_1 which can be switched on ($v_1 = 1$) or off ($v_1 = 0$). A unidirectional valve v_{12} is used to control the flow of liquid from Tank 1 to Tank 2. In tank 2, the liquid is drained out at a constant rate.

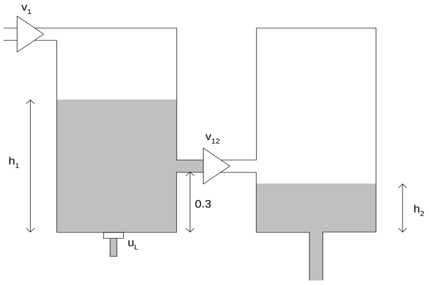

Figure 1: The two-tank system

The system can be represented as hybrid system H with two continuous variables h_1, h_2 representing the height of the fluid in the each tank respectively and two binary inputs v_1, v_{12}. The dynamics of the two tank system can be described by the following nonlinear difference equations.

$$\begin{aligned} h_1(t+1) &= a_1 v_1 - b\, v_{12}\, sq(h_1(t) - 0.3)\ + h_1(t) \\ h_2(t+1) &= b\, v_{12}\, sq(h_1(t) - 0.3)\ - a_2 + h_2(t) \end{aligned}$$

where $sq(x) = \sqrt{x}$ if $x \geq 0$ and 0 otherwise, a_1 and a_2 are constants depending on the flow rates into Tank1 and from Tank2 respectively, and b depends on the flow rate from Tank1 to Tank2. The following table shows the effect of different input combinations on the directions (signs) of the differences $\Delta h_1 = h_1(t+1) - h_1(t)$ and $\Delta h_2 = h_2(t+1) - h_2(t)$.

Input (v_1, v_{12})	Δh_1			Δh_2		
	$+$	0	$-$	$+$	0	$-$
$(0,0)$	F	T	F	F	F	T
$(0,1)$	F	$h_1 \leq .3$	$h_1 > .3$	$h_1 > c_1$	$h_1 = c_1$	$h_1 < c_1$
$(1,0)$	T	F	F	F	F	T
$(1,1)$	$h_1 < c_2$	$h_1 = c_2$	$h_1 > c_2$	$h_1 > c_1$	$h_1 = c_1$	$h_1 < c_1$

In the above table T and F indicate the true (always) and false (never) conditions respectively, $c_1 = (a_1/b)^2 + 0.3$, and $c_2 = (a_2/b)^2 + 0.3$. Based on the above table it is easy to verify that the system is online controllable within the region defined by

$$(\frac{a_2}{b})^2 + 0.3 + \epsilon < h_1 < (\frac{a_1}{b})^2 + 0.3 - \epsilon$$

where ϵ is any chosen small positive number. Within this region $\hat{\boldsymbol{\delta}}_{X_o}$ and $\check{\boldsymbol{\delta}}_{X_o}$ are approximately $\sqrt{2}a_1$ and $\sqrt{2}\epsilon$ respectively.

The safety specification of the two tank system is to keep the level of the fluids in the two tanks within a specified limits, namely

$$X_s = \{(h_1, h_2) \mid h_1 \in [\hat{h}_1, \check{h}_1] \text{ and } h_2 = [\hat{h}_2, \check{h}_2]\}$$

given that the system is initiated within a region $X_o \supset X_s$. To satisfy such specification, the parameters a_1, a_2, and b must be tuned so that the system is online controllable within the specified initial region X_o.

The online controller can accommodate parameter changes of the model as long as the system is tuned to remain online controllable. For example, consider the possibility of leak in the first tank as shown in Figure 1. In this case, the difference equation for h_1 can be written as follows

$$\begin{aligned} h_1(t+1) = & a_1(v_1 - \alpha\, u_L\, sq(h_1(t)) - \\ & b\, v_{12}\, sq(h_1(t) - 0.3) + h_1(t) \end{aligned}$$

where u_L is an uncontrolled binary input indicating the presence of leak in the first tank, and $0 < \alpha < 1$ is the estimated fraction of the inflow from v_1 that is drained due to the leak. For small α and for $h(t) > 0.3$, the term $a_1(v_1 - \alpha\, u_L\, sq(h_1(t)))$ can be approximated to $a_1(v_1 - \alpha\, u_L)$. In this case, it can be checked that the system is online controllable in the region

$$(\frac{a_2}{b})^2 + 0.3 + \epsilon < h_1 < \left(\frac{a_1(1-\alpha)}{b}\right)^2 + 0.3 - \epsilon$$

Therefore, the online controllability of the system can be maintained under the possibility of small leak in Tank1 by either reducing the initial region of operation, X_o, or adjusting the inflow parameter a_1 to compensate the effect of the leak.

Figure 2 shows the fluid level and the input values for the two tank system under online control with tree depth of 7 in the presence of 5% measurement noise. It is assumed that a leak with $\alpha = 0.4$ occurred at time $t = 350$. The safe region is defined by $h_1 \in [0.55, 0.65]$ and $h_2 \in [0.11, 0.09]$. For a tree depth of 7 there are 5461 nodes to explore at each time step, however, using the information about $\hat{\boldsymbol{\delta}}_{X_o}$ and $\check{\boldsymbol{\delta}}_{X_o}$ an average of 748 nodes are explored at each time step.

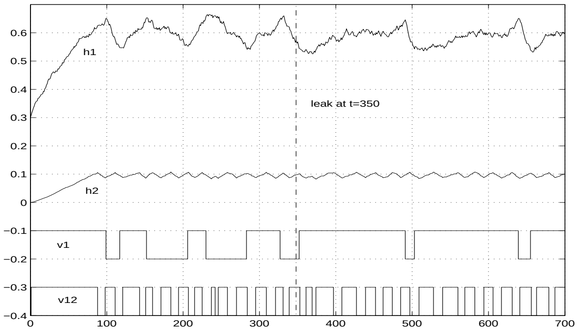

Figure 2: Fluid levels in the controlled two-tank system

5 Conclusion

In this paper we presented a limited lookahead approach for safety control of a general class of hybrid systems. In future work, we will investigate more efficient tree exploration techniques, and redefine online controllability to take into account the position of the initial state relative to the safe regions.

References

[1] P. Antsaklis, editor. *Special Issue on Hybrid Systems.* Proceedings of the IEEE. 2000.

[2] Y.-L. Chen and F. Lin. Safety control of discrete event systems using finite state machines with parameters. In *Proc. of American Cont. Conf.*, VA, 2001.

[3] S. L. Chung, S. Lafortune, and F. Lin. Limited lookahead policies in supervisory control of discrete event systems. *IEEE Trans. Autom. Control*, 37(12):1921–1935, December 1992.

[4] J. Lunze. Laboratory three tanks system: Benchmark for the reconfiguration problem. Technical report, Tech. Univ. of Hamburg-Harburg, Germany, 1998.

[5] M. Morari and J. Lee. Model predictive control: Past, present and future. *Computers and Chemical Engineering*, 23:667–682, 1999.

[6] J. Zaytoon P. Antsaklis, X. Koutsoukos. On hybrid control of complex systems: a survey. *European Journal of Automation*, 32:1023–1045, 1998.

[7] S. Qin and T. Badgewell. An overview of industrial model predictive control technology. *Chemical Process Control*, 93(316):232–256, 1997.