Computation of Safety Control for Hybrid System with Applications to Intersection Collision Avoidance System

by

Geng Huang

Submitted to the Department of Mechanical Engineering
in partial fulfillment of the requirements for the degree of

Master of Science in Mechanical Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2015

Signature redacted

Author . . . .
Department of Mechanical Engineering
August 7, 2015

Signature redacted

Certified by . . . .
Domitilla Del Vecchio
Associate Professor
Thesis Supervisor

Signature redacted

Accepted by . . . .
David Hardt
Chairman, Department Committee on Graduate Theses

Computation of Safety Control for Hybrid System with Applications to Intersection Collision Avoidance System

by

Geng Huang

Submitted to the Department of Mechanical Engineering
on May 8, 2015, in partial fulfillment of the
requirements for the degree of
Master of Science in Mechanical Engineering

Abstract

In this thesis, I consider the problem of designing a collision avoidance system for the scenario in which two cars approach an intersection from perpendicular directions. One of the cars is a human driven vehicle, and the other one is a semi-autonomous vehicle, equipped with a driver-assist system. The driver-assist system should warn the driver of the semi-autonomous vehicle to brake or accelerate if potential dangers of collision are detected. Then, if the system detects that the driver disobeys the warning, the system can override the behavior of the driver to guarantee safety if necessary. A hybrid automaton model with hidden modes is used to solve the problem. A disturbance estimator is used to estimate the driver's reaction to the warning. Then, with the help of a mode estimator, the hybrid system with hidden modes is translated to a hybrid system with perfect state information. Finally, we generalize the solution for the application example to the solution of safety control problem for general hybrid system with hidden modes when the hybrid system satisfies some proposed constraints and assumptions.

Thesis Supervisor: Domitilla Del Vecchio
Title: Associate Professor

Acknowledgments

Through the support and help of many people, this thesis was made possible.

I would like to thank my parents and family for their love and support. They gave me the chance to get a good education, develop my ability, and realize my potential. All the support they have provided me over the years was the greatest gift anyone has ever given me.

I would like to thank my thesis advisor, Professor Domitilla Del Vecchio, for her guidance, understanding, and support.

I would like to thank Daniel Hoehener, who gave me so many valuable advices, and helped me substantially in the development of theory in this thesis.

I would like to thank all of my friends. It was these friends who made my success more enjoyable, and cheered me up when I failed.

I would thank NSF-CPS Award 1239182 for the support of my research. This funding allowed me to pursue and investigate research topics showed in this thesis.

Finally, I would like to express my gratitude to the MIT School of Engineering, and the Department of Mechanical Engineering, who gave the wonderful resources for studying, and working.

Contents

List of Figures

Chapter 1

Introduction

Improving driving safety is one of the main takes in developing road vehicles. Lots of attentions have been given to vehicle safety since the 1960's [25, 31]. The introductions of passive safety features such as seat belts, air bags and advanced lighting systems have substantially reduced the rate of crashes [17, 22]. However, despite the significant improvements, each year in United States, collisions of motor vehicles still result in 40,000 deaths, more than three million injuries, and over $130 billion in financial losses [4, 17]. Since the development of passive safety system could not provide further significant improvements in vehicle safety, the development of active safety protection system became the new trend of vehicle safety system development [29]. Different from passive safety system that reduces injuries of passengers in crash; active safety protection systems prevent potential crashes by warning the driver [26]. One of active safety protection systems is automotive collision avoidance system. Automotive collision avoidance system actively warns drivers of a potential collision event, allows the driver adequate time to take appropriate actions to avoid the collision event [11]. Numerical analysis of collision data strongly suggests that automotive collision avoidance system can tremendously reduce collisions [11]. Crash data collected by the U.S. National Highway Traffic Safety Administration (NHTSA) show that automotive collision avoidance system can theoretically prevent 37% to 74% of all police reported rear-end crashes [22, 35]. It can be seen that the introduction of collision warning systems resulted in significant reduction of crash fatalities, injuries, and property damage.

Intersection crashes account for 1.72 million crashes per year in the United States [25, 27, 14]. Studies by Daimler-Benz and NHTSA suggest that additional one second warning could reduce intersection accident rate by 50% to 90% [27, 30], and Eaton reported that the actual truck fleet accident frequency was reduced by 73% after the fleets being equipped with the VORAD Forward and Side Collision warning systems by Eaton [46, 19]. These results demonstrate the importance and benefits of the research on intersection collision avoidance system. However, due to the complicatedness of designing intersection collision avoidance systems and the limitations of the radar technology, intersection collision avoidance systems received less attention than the forward collision avoidance systems [47]. Thanks to vehicle-to-vehicle communication technologies, the development of intersection collision avoidance systems became practical [21, 26]. Previous research results show that it is possible to detect threats of collision by vehicles cooperatively sharing critical information, such as location, velocity and acceleration [30, 45, 28]. By sharing the information, each vehicle is able to predict the potential collision [30, 45]. However, the effectiveness of this technology depends on the percentage of vehicles on the road using it and the number of vehicles equipped with navigation and communication systems [31]. The Cooperative Intersection Collision Avoidance System for Violations (CICAS-V) project conducted by Mercedes-Benz Research and Development North America, Inc. developed a prototype system to prevent crashes by predicting stop-sign and signal controlled intersection violations and warning the violating driver [25].

In this thesis, we consider the design of intersection collision avoidance system involving a normal human driven vehicle and a vehicle equipped with the intersection collision avoidance system. When the potential of collision is detected, the system warns the driver (to accelerate or brake) based on the positions and velocities of the two cars. After receiving the warning, the driver has adequate time to react. Then, the system will estimate the driver's reaction to the warning, and the system can override the behavior of the driver if the driver disobeys the warning and a collision is about to happen. The scenario after the driver receives the issued waring can be divided into three sub-cases depending on the reaction of the driver regarding to the system warning of a potential collision. First, the driver obeys the warning and cross the intersection safely. Second, the driver disobeys the warning but could safely pass the intersection. Third, the driver ignores the warning in an unsafe condition and a crash is possible. Then the driver assist system will give the vehicle a control input to avoid collision by overriding the input from the driver. In some cases, the driver obeys the warning at the beginning, and later he/she disobeys the issued warning. This case is regarded as that the driver disobeys the warning from the assist system. In order to guarantee the effectiveness of the system, the design of the intersection collision avoidance system needs to be provable safe.

Also, in the collision warning system design, human factors play an important role [34]. The purpose of the warning is to alert the driver when there is a potential of collision and the driver is unaware of it [47]. A collision waning system should detect both the potential of collision and the driver's reactions regarding the collision warning and collision possibility [46]. If the driver has already taken an appropriate action, the intervention from the collision avoidance system should be discarded to reduce the annoying factor [22]. Also, a good warning system should minimize the additional attention load for the driver [46]. A system that gives excessive warning or overriding may desensitize and distract the driver and decrease the driving satisfaction [22]. Undesired warnings and overriding may also make the driver turn off the system completely [46]. Thus, it is important to design a collision system which is least conservative. A least conservative system requires that the control actions will only be taken when safety cannot be guaranteed otherwise.

Hybrid automaton is used to model the intersection collision avoidance system involving a human driven vehicle and a semi-autonomous vehicle with the collision avoidance system (driver assistance system) installed. Hybrid automaton can model continuous vehicle dynamics as well as discrete human decisions and overriding decisions from the driver assistance system [33, 36]. These features make it an ideal framework for the modeling, since driver usually switch between different driving actions [38]. Also, there are a lot of development of modeling and control techniques for hybrid systems that can be utilized.

Research has been done in the safety control problem for hybrid systems with perfect state information, with imperfect continuous state information, and with unknown modes when all transitions are driven by unknown disturbance events [39, 24].

There are numerous research results on safety control problem for hybrid systems in which modes and state information are well known [24, 20, 12, 2, 3, 37, 32, 14]. The hybrid control problem to guarantee safety is well formulated and solved using optimal control and leads to the Hamilton-Jacobi-Bellman (HJB) equation, which implicitly determines the maximal controlled invariant set and the least conservative feedback control map [6, 37]. However, exactly solving the HJB equation is computationally demanding. Thus, researchers have been working on approximate solutions to calculate the maximal controlled invariant set [18, 1]. Also, the termination of the computation of the maximal controlled invariant set has been investigated and works have been done to find special cases of the systems, for which termination can be proved [32].

The hybrid system control problem with imperfect state information has also been addressed [8, 9, 7, 15, 16, 13]. In those works, the mode of the system is assumed to be known but there are uncertainties in the continuous state. The controller is designed based on a state estimator for finite state systems [8, 9, 15, 14, 13]. Linear complexity state estimation and control algorithms are proposed for hybrid systems with order preserving dynamics [8, 9, 15, 13].

The intersection collision avoidance system design problem is formulated as a hybrid controller design problem for hybrid automaton in which modes are hidden since driver's decisions are unobservable and uncontrollable.

The hybrid system control problem for guaranteeing safety with unknown modes has been investigated in [40, 39, 41, 42, 43, 44]. There are literatures studying Hidden Mode Hybrid Systems (HMHSs), in which the mode is unknown and mode transitions are driven only by disturbance events [40, 39]. The lack of knowledge of mode and disturbance transition event gives a control problem with imperfect mode information. The control problem with imperfect mode information is translated to problem with perfect state information using derived non-deterministic or probabilistic information state [40, 39, 41]. The derived non-deterministic information state tracks all possible states compatible given the history of the system [40, 39, 41]. With the update law for the derived information state, the control problem can be reconstructed using the new derive states, and the problem becomes hybrid control design problem with perfect state information [40, 39, 41].

Control design problem for driver assistance system which gives driver warnings before overriding can be modeled as hybrid systems with hidden modes. Hybrid systems with hidden modes are special cases of hybrid automata. In hybrid systems with hidden modes, some modes are unknown and some mode transitions are driven by disturbance events. In this document, we consider mode transitions can be either driven by disturbance events or control events. Also, we consider the case such that the allowed ranges for continuous input signals are mode and time dependent. Warning and active safety systems for vehicle collision avoidance need to guarantee safety in the presence of human drivers, whose driving decisions and behaviors are unknown and are modeled as disturbance transition events and continuous disturbance signals. Also, in order to co-operate the design of warning the driver and overriding when needed, control events are modeled to trigger transitions between some modes. Continuous control signals are also involved in the system dynamics to fulfill the functionality of overriding. Thus, we study hybrid systems in which mode transitions can be driven by both unknown disturbance events and designed control events. Also, continuous disturbance and control signals are both involved in the system dynamics.

To solve the problem, first, we propose a hybrid control solution assuming all states and signals are well measured. Then, we consider the case in which disturbance transition events, mode of the system, and continuous disturbance signals are not known. We assume that the continuous state is well known. A disturbance estimator is used to estimate the continuous disturbance signals and further its results are used to estimate the mode of the system given the relationship between continuous disturbance signals, the disturbance transition events and the mode of the system. With the estimated mode, a new hybrid system with perfect knowledge about mode and transitions are constructed. Then, we modify the inputs to the hybrid control calculation algorithm based on the estimated values. Finally, a hybrid feedback control map is designed to prevent the flow of the system from entering the collision set for the current time and all future time.

Continuous state information, i.e., positions and velocities of the two vehicles, is assumed to be available. The continuous state information of the normal human driven vehicle could be provided by cameras and vision systems located at the intersection [21, 34, 28]. Using vehicle-to-infrastructure communication technologies, short range communications devices (dedicated short range communication 5.9 GHz in the United States) can distribute the state information to the driver assistance system installed on the semi-autonomous vehicle [47, 29, 28]. The continuous state information of the semi-autonomous vehicle can be provided by differential GPS and from the on-board computer of the semi-autonomous vehicle [45, 28]. Finally, the control algorithms would be executed with the on-board computers to help the driver cross the intersection safely.

Chapter 2

Motivation Example

We consider the scenario in which two cars approach an intersection from perpendicular directions. One of the cars is a human driven vehicle, and the other one is a semi-autonomous vehicle, equipped with a driver-assist system, referred to as controller in the following. The controller takes measurements of positions and speeds of the two cars as inputs. If, based on the inputs, the controller detects the potential of collision, it can issue braking or accelerating warnings to the driver of the semi-autonomous vehicle. After issuing the warnings, the controller uses its inputs (positions and speeds) to estimate whether the driver obeys the issued warning. If disobeying is detected, the controller can override the driver whenever this should become necessary.

In order to design the controller on the semi-autonomous vehicle, we model the whole system as a hybrid automaton, which will be introduced in the next section. The continuous dynamics of the system are the following.

The human driven vehicle is referred as Car 1 and the semi-autonomous vehicle is referred as Car 2. For $i = 1, 2$, we use p_i, v_i, and a_i to denote the position, speed, and acceleration of car i along its path. For $t \geq 0$, we have

$$\dot{p}_i(t) = v_i(t) \tag{2.1}$$

$$\dot{v}_i(t) = a_i(t). \tag{2.2}$$

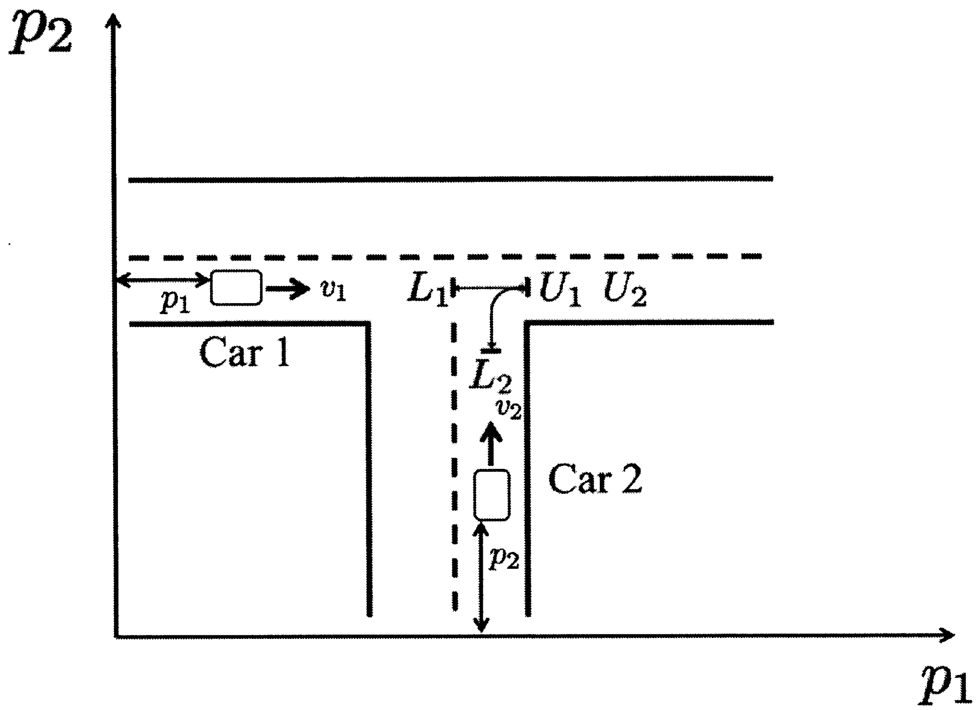

Figure 2-1: Problem scenario for intersection collision avoidance

We assume that the acceleration $a_1(t)$ at time $t \in \mathbb{R}^+$ of the human driven vehicle is determined by a disturbance signal $d_1(t)$. Similarly, the acceleration $a_2(t)$ of the semi-autonomous vehicle at time $t \in \mathbb{R}^+$ is determined by a disturbance signal $d_2(t)$ if the system is not in override mode and by a control signal $u(t)$ otherwise. Both disturbance and control signals are assumed to be bounded, i.e., $d_1(t), d_2(t) \in [-\bar{d}, \bar{d}]$ and $u(t) \in [-\bar{u}, \bar{u}]$ for all $t \in \mathbb{R}^+$. Defining the intersection as $Int = (L_1, U_1) \times (L_2, U_2)$, the objective of the controller is to guarantee that $(p_1(t), p_2(t)) \notin Int$ for all $t \geq 0$.

The warning and override mechanism is modeled as a finite state machine shown in Fig. 2-2. Initially, both cars are human-driven, and we denote that mode as h. If the potential danger of collision is detected, braking or accelerating warning will be issued to the driver of the semi-autonomous vehicle. In the following, we describe warning/overriding mechanism assuming an braking warning is issued, left branch of the tree in Fig. 2-2. The case of an accelerating waring is analogous, except that in the notation a superscript 1 is replaced with a superscript 2, right branch of the tree in Fig. 2-2. Issuing a braking warning results in a mode transition from h to mode w^1. We define the time instance at which a warning is issued as $t := 0$. After receiving the warning, the driver of the semi-autonomous vehicle needs time τ_{RT} to react, so the system will stay in mode w^1 for time $[0, \tau_{RT})$. When $t = \tau_{RT}$, the reaction time has passed and the driver should react to the issued warning. Obedience to the warning is represented by the discrete disturbance signal σ_d^{o1} and will trigger the mode transition from w^1 to ho^1. Similarly, if the driver disobeys the braking warning, the disturbance signal σ_d^{d1} will trigger the mode transition from w^1 to hd^1. hd^1 means that the driver has disobeyed the warning, and if necessary, the control system can override the driver of the semi-autonomous vehicle to guarantee safety. If disobeying braking warning has been detected, when necessary, σ_u^1 will be issued and the mode of the system will be switched ha^1.

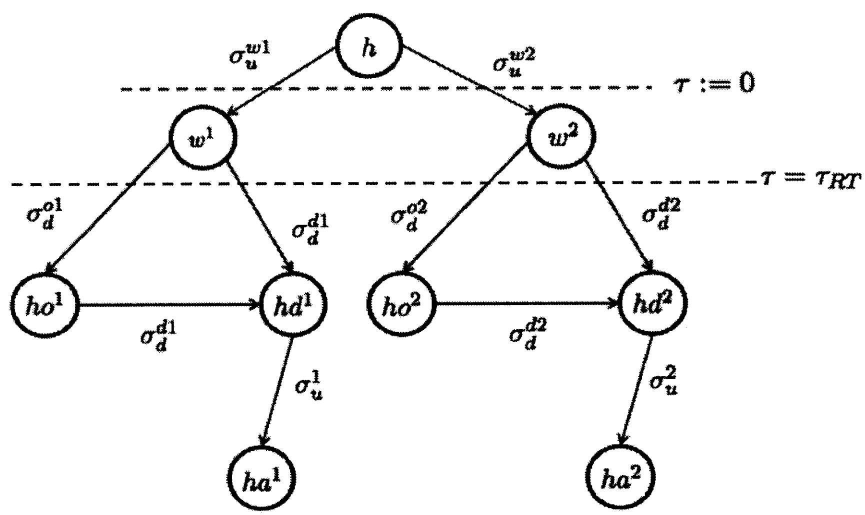

Figure 2-2: System H

Chapter 3

System Model

We start by introducing the notation of hybrid automaton.

Definition 1. A *hybrid automaton* is a tuple $H = (Q, X, U, D, \Sigma_u, \Sigma_d, R, f)$ in which Q is the finite set of system modes with $q \in Q$; X is the space of continuous states with $x \in X$; U is the set of continuous control inputs with $u \in U$; D is the set of continuous disturbance inputs with $d \in D$; Σ_u is the finite set of discrete control inputs with $\sigma_u \in \Sigma_u$; Σ_d is the finite set of discrete disturbance events with $\sigma_d \in \Sigma_d$; $R : Q \times \Sigma_u \times \Sigma_d \to Q$ is the mode update map; $f : X \times Q \times U \times D \to TX$ is the vector field with $\dot{x} = f(x, q, u, d)$ and TX is a tangent space of X.

In the example discussed in Section 2, we have $Q = \{h, w^1, w^2, ho^1, hd^1, ho^2, hd^2, ha^1, ha^2\}$. $X \subseteq \mathbb{R}^4$ and $x = \begin{bmatrix} p_1 \\ v_2 \\ p_2 \\ v_2 \end{bmatrix}$. $\Sigma_d = \{\sigma_d^{o1}, \sigma_d^{d1}, \sigma_d^{o2}, \sigma_d^{d2}\}$. $D \subset \mathbb{R}^2$ and $U \subset \mathbb{R}^1$. $\Sigma_u = \{\sigma_u^{w1}, \sigma_u^{w2}, \sigma_u^1, \sigma_u^2\}$. R is mode transition map in Fig. 2-2 and f is the longitudinal continuous dynamics of the two cars given in Eq. 2.1 and 2.2.

In this thesis, we define the $(Q, \Sigma = \Sigma_d \times \Sigma_u)$ as a directed acyclic graph (DAG). In the following, we will first introduce the structure of the hybrid automaton and then the execution of it.

3.1 The structure of hybrid automaton

The structure of the hybrid automaton can be described as a finite state machine. Each node in the DAG is a state, and the links between states are transitions driven by either discrete disturbance signals or discrete control signals. In DAG, there is a partial order property $\leq$. For vertices u and v, we have $u \leq v$ if there exists a directed path from u to v.

For a signal a and a time interval T, we define $a(T)$ to be the sequence of signal a in the time interval T. Starting from a state q_0, we define $\phi_q(t, q_0, \sigma_u([0,t)), \sigma_d([0,t))) := q(t)$ for $t \geq 0$ as the discrete flow of the system. Based on the partial order property of DAG, we have $q_0 \leq q(t)$.

Definition 2. For a set of mode Q with partial order property, we define $\min(Q) = q$ if $\forall q' \in Q, q' \geq q$. We define $\max(Q) = q$ if $\forall q' \in Q, q \geq q'$.

Here, we introduce some notations that are going to be used in the subsequent sections.

Definition 3. For a node $q \in Q$, we define

i $DisturbanceReach(q) = \{q' \mid \exists \sigma_d \text{ s.t. } R(q, \emptyset, \sigma_d) = q'\}$.

ii $ControlReach(q) = \{q' \mid \exists \sigma_u \text{ s.t. } R(q, \sigma_u, \emptyset) = q'\}$.

iii $DSR(q) = \{q' \mid \exists t \text{ and } \sigma_d([0,t)) \text{ s.t. } \phi_q(t, q, \emptyset, \sigma_d([0,t))) = q'\} \cup \{q\}$.

For example, we have $DisturbanceReach(w^2) = \{ho^2, hd^2\}$ and $DSR(w^2) = \{w^2, ho^2, hd^2\}$. $ControlReach(w^2) = \emptyset$ and $ControlReach(hd^2) = \{ha^2\}$.

Definition 4. We say that a node $q \in Q$ is a *head* if $\exists q'$ s.t. $q \in ControlReach(q')$.

In the example, w^1 and w^2 are both *head*.

For a node q which is a *head*, we call $DSR(q)$ as a $Connect(q)$.

Definition 5. For a node q which is a *head*, we define

i $Branch(q) = \{q' \in Connect(q) | ControlReach(q') \neq \emptyset\}$.

ii $NotTran(q) = Connect(q) \backslash Branch(Connect(q))$.

We denote a mode q as a q_{last} if $ControlReach(q) = \emptyset$ and $DisturbanceReach(q) = \emptyset$. In the example, ha^1 and ha^2 are both q_{last}.

Assumption 1. *For each node $q \in Q$, at least one of $DisturbanceReach(q)$ and $ControlReach(q)$ is empty.*

This implies that for all nodes $q \in Q$, the links directed from q can be either a discrete disturbance transition or a discrete control transition, but not both.

Assumption 2. *For all $q_1, q_2 \in Q$, $ControlReach(q_1) \cap DisturbanceReach(q_2) = \emptyset$.*

Assumption 2 implies that a node cannot be reached by both a discrete disturbance signal and a discrete control signal.

3.2 The execution of hybrid automaton

Here, we consider the execution of the hybrid automaton.

We define $R(q, \emptyset, \emptyset) = q$ for all $q \in Q$. The sequence $\{\tau_i\}_{i \in \mathbb{N}^+}$ with $0 \leq \tau_i \leq \tau_{i+1}$ represents the sequence of times at which node transitions occur with $(\sigma_u(\tau_i), \sigma_d(\tau_i)) \neq (\emptyset, \emptyset)$ and $(\sigma_u(t), \sigma_d(t)) = (\emptyset, \emptyset)$ for all $t \notin \{\tau_i\}_{i \in \mathbb{N}^+}$. We define the discrete trajectory $q(t)$ of system H as follows.

Given $q(0) = q_0$, we define $q(t) = q_0$ for $0 \leq t \leq \tau_1$. If $\tau_i \neq \tau_{i+1}$, then we define $q(t) = R(q(\tau_i), \sigma_u(\tau_i), \sigma_d(\tau_i))$ for $t \in (\tau_i, \tau_{i+1}]$. If for some $i \in \mathbb{N}^+$, $\tau_i = \tau_{i+1} = \cdots = \tau_{i+k} = \tau \geq 0$ with $k \in \mathbb{N}^+$ and finite, then $k+1$ mode transitions occur at time τ. For $j \in \{1, 2, 3, \cdots, k+1\}$, we define $(\sigma_u(\tau)_j, \sigma_d(\tau)_j)$ as the discrete signals triggering the j-th mode transition occurring at time τ. Also, we define $q(\tau)_j$ as the mode after the j-th mode transition happening at time τ. Then we have $q(\tau)_1 = R(q(\tau), \sigma_u(\tau)_1, \sigma_d(\tau)_1)$, and $q(\tau)_{m+1} = R(q(\tau)_m, \sigma_u(\tau)_m, \sigma_d(\tau)_m)$ for $m \in \{1, 2, 3, \cdots, k\}$. We define $q(t) = q(\tau)_{k+1}$ for $t \in (\tau, \tau_{i+k+1}]$.

For the continuous trajectory $x(t) \in X$ of system H, given $x(0) = x_0$, $\dot{x}(t) = f(x(t), q(t), u(t), d(t))$ with $u(t) \in U$ and $d(t) \in D$. Starting from x_0 and q_0, we define

$$\phi_x(t, x_0, q_0, u([0,t)), d([0,t)), \sigma_u([0,t)), \sigma_d([0,t))) := x(t)$$

as the continuous flow of the system.

For each mode $q \in Q$, we use $DTF(q) \in \{0, 1\}$ to indicate whether the mode q has dwell time or not. For $q \in Q$,

(1) if $DTF(q) = 1$, then mode q has dwell time, and we use $DT(q)$ to denote the dwell time of q. If at time instance t_1, the mode of system H is transited to q, $q(t_1) = q$, then for $\tau \in [t_1, t_1 + DT(q))$, we have $(\sigma_u(\tau), \sigma_d(\tau)) = (\emptyset, \emptyset)$, and $(\sigma_u(t_1 + DT(q)), \sigma_d(t_1 + DT(q))) \neq (\emptyset, \emptyset)$.

(2) if $DTF(q) = 0$, then mode q does not have dwell time.

In the example, $DTF(w^1) = 1$ and $DTF(w^2) = 1$ with $DT(w^1) = DT(w^2) = \tau_{RT}$. This means that after receiving the issued warning, the driver has time τ_{RT} to react. Within the reaction time, the driver's behavior is not used as driver's reaction to the warning. All of the other modes do not have dwell time.

Assumption 3. *For any mode $q \in Q$, if $DTF(q) = 1$, then there exists $q' \in Q$ such that $q \in ControlReach(q')$.*

Assumption 4. *For a mode $q \in Q$, if $DTF(q) = 1$ and $DisturbanceReach(q) \neq \emptyset$, then there exists a $q' \in DisturbanceReach(q)$ such that $DisturbanceReach(q) \subseteq DSR(q')$.*

Definition 6. For a mode q and $q' \in DisturbanceReach(q)$ with $DTF(q) = 0$, the *boundary between $Range_{d2}(q)$ and $Range_{d2}(q')$*, which is denoted as $BR_{d2}(q, q')$ is defined $BR_{d2}(q, q') = \partial Range_{d2}(q) \cap Range_{d2}(q')$.

For a mode $q \in Q$ and a mode $q' \in DisturbanceReach(q)$,

- if $DTF(q) = 0$, then the discrete disturbance signal σ_d which transits the mode from q to q' is applied if and only if the continuous disturbance signal d_2 cross the boundary of $Range_{d2}(q)$ and $Range_{d2}(q')$, $BR_{d2}(q, q')$, and go from $Range_{d2}(q)$ to $Range_{d2}(q')$;

- if $DTF(q) = 1$, then the discrete disturbance signal σ_d which transits the mode from q to q' is applied if and only if $DT(q)$ is reached and d_2 go from a value in $Range_{d2}(q)$ to a value in $Range_{d2}(q')$.

Assumption 5. *For a mode $q \in Q$ such that there exists a q' with $DTF(q') = 0$ and $q \in DisturbanceReach(q')$,*

- $Range_{d2}(q) \not\subseteq Range_{d2}(q')$;
- *at least one of* $\sup Range_{d2}(q) \geq \sup Range_{d2}(q')$ *and* $\inf Range_{d2}(q) \leq \inf Range_{d2}(q')$ *is true;*
- *furthermore, if* $\sup Range_{d2}(q) \geq \sup Range_{d2}(q')$, *then for* $q^n \in DisturbanceReach(q)$, *we have* $\sup Range_{d2}(q^n) \geq \sup Range_{d2}(q)$; *if* $\inf Range_{d2}(q) \leq \inf Range_{d2}(q')$, *then for* $q^n \in DisturbanceReach(q)$, *we have* $\inf Range_{d2}(q^n) \leq \inf Range_{d2}(q)$.

Assumption 6. *For all* $q_i, q_j \in DisturbanceReach(q)$ *with* $DTF(q) = 0$, $Range_{d2}(q_i) \cap Range_{d2}(q_j) \subseteq Range_{d2}(q)$.

Definition 7. For each mode $q \in Q$, we define $Range_d(q) \subseteq D$ as the *set of allowed continuous disturbance signals associated with mode* q, and we define $Range_u(q) \subseteq U$ as the *set of allowed continuous control signals associated with mode* q.

For example, $Range_d(ho^2) = [-\bar{d}, \bar{d}] \times [\bar{d} - \epsilon, \bar{d}]$ and $Range_u(ha^2) = [-\bar{u}, \bar{u}]$.

Assumption 7. *We consider the continuous dynamic of system H to be composed by two parallel systems S_1 and S_2. For $i = 1, 2$, we define system S_i as the following:*

$$\dot{x}_i(t) = A_i(q(t))x_i(t) + B_i(q(t))d_i(t) + E_i(q(t))u_i(t) \tag{3.1}$$

$$y_i(t) = C_i x_i(t) \tag{3.2}$$

where $d_i, u_i \in \mathbb{R}$. $x_1 \in \mathbb{R}^m$, $A_1(q)$ is a $m \times m$ matrix, $B_1(q)$ and $E_1(q)$ are $m \times 1$ matrices, $x_2 \in \mathbb{R}^n$, $A_2(q)$ is a $n \times n$ matrix, $B_2(q)$ and $E_2(q)$ are $n \times 1$ matrices. $d_i(t) \in Range_{di}(q(t), t) \subseteq \mathbb{R}$ where $Range_{di}(q(t), t)$ is the allowed range for $d_i(t)$ in mode $q(t)$ at time t. $u_i(t) \in Range_{ui}(q(t), t) \subseteq \mathbb{R}$, and $Range_{ui}(q(t), t)$ is the allowed range for $u_i(t)$ in mode $q(t)$ at time t. C_1 and C_2 are $1 \times m$ and $1 \times n$ matrices respectively.

In the example, we have $A_1(q) = A_2(q) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B_1(q) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $E_1(q(t)) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ for all $q \in Q$. If $q \neq ha^1$ and $q \neq ha^2$, then we have $B_2(q) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $E_2(q) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. If $q = ha^1$ and $q = ha^2$, then we have $B_2(q) = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $E_2(q) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

We define $C = \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}$. Any composed signal a of S_1 and S_2 are composed in a way such that $a = (a_1, a_2)$. For example, $x = (x_1, x_2)$ is the composed continuous state of the system and $y = (y_1, y_2)$ is the composed output signal. We have $y = Cx$. Also, $d(t) = (d_1(t), d_2(t)) \in Range_d(q(t), t) = Range_{d1}(q(t), t) \times Range_{d2}(q(t), t)$ and $u(t) = (u_1(t), u_2(t)) \in Range_u(q(t), t) = Range_{u1}(q(t), t) \times Range_{u2}(q(t), t)$.

Assumption 8. *For any mode $q \in Q$ with the following properties*

i $\exists q_1 \in Q$ *with* $q \in DisturbanceReach(q_1)$ *or* $\exists q_2 \in Q$ *with* $q_2 \in DisturbanceReach(q)$,

ii $DTF(q) = 0$,

we require $|\dot{d}_2| \leq \beta(q)$ *where* $\beta(q) \in \mathbb{R}^+$ *defines the allowed range for* $\dot{d}_2$ *in mode* q.

Assumption 9. *For any Connect, we have* $\forall q_1, q_2 \in Connect$,

i $\beta(q_1) = \beta(q_2)$.

ii $A_2(q_1) = A_2(q_2)$, $B_2(q_1) = B_2(q_2)$, *and* $E_2(q_1) = E_2(q_2)$.

Assumption 8 and 9 specify some requirements on S_2, and for S_1, there are no such requirements.

Assumption 10. *For* S_i, $\forall t \geq 0$, *if* $\forall \tau \in [0, t)$, $u_{ia}(\tau) \geq u_{ib}(\tau)$, $d_{ia}(\tau) \geq d_{ib}(\tau)$, *and* $x_{ia}(0) \geq x_{ib}(0)$, *then we have* $y_{ia}(t) \geq y_{ib}(t)$.

Chapter 4

Problem Formulation

In this section, we formulate the problem we want to solve.

We start by defining a set $Bad \subset \mathbb{R}^2$ such that $Bad = (L_1, U_1) \times (L_2, U_2)$ with $U_1 > L_1 > 0$ and $U_2 > L_2 > 0$.

Notice that the set Bad is an open rectangular set in $\mathbb{R}^2$.

Problem 1. *With $(C_1x_1(0), C_2x_2(0)) \notin Bad$, for any $t \geq 0$, given $q(t)$, $x(t)$ and $d(t)$ with $d(t) \in Range_d(q(t))$, for all $\tau \geq t$, design a least conservative control map $\pi : X \times Q \times D \to U \times \Sigma_u$, i.e., $(u([t,\tau)), \sigma_u([t,\tau))) = \pi(x(t), q(t), d(t))$, such that $(C_1x_1(\tau), C_2x_2(\tau)) \notin Bad$, $\forall d([t,\tau))$ and $\sigma_d([t,\tau))$.*

Here, the least conservative control map means that the control actions will only be taken if the continuous flow cannot be guaranteed to be kept outside Bad otherwise.

Chapter 5

Solution to Problem 1

We define

$$B^{\uparrow} = (L_1, \infty) \times (-\infty, U_2)$$
$$B^{\downarrow} = (-\infty, U_1) \times (L_2, \infty),$$

so we have $Bad = B^{\uparrow} \cap B^{\downarrow}$. We define the safe set for a set K given an initial disturbance signal d_0 and a mode q_0 as

$$W(K, d_0, q_0) = \{x_0 | \forall t \geq 0, \exists u([0,t)), \text{ and } \sigma_u([0,t)) \text{ s.t. } \forall \sigma_d([0,t)) \text{ and } d([0,t)) \text{ with } d(0) = d_0,\ C\phi_x(s, x_0, q_0, u([0,t)), d([0,t)), \sigma_u([0,t)), \sigma_d([0,t))) \notin K\ \forall s \in [0,t)\}.$$

Lemma 1. $W(Bad, d_0, q) = W(B^{\uparrow}, d_0, q) \cup W(B^{\downarrow}, d_0, q)$.

Proof. The statement $W(Bad, d_0, q) \supseteq W(B^{\uparrow}, d_0, q) \cup W(B^{\downarrow}, d_0, q)$ follows immediately from $Bad \subset B^{\uparrow}$ and $Bad \subset B^{\downarrow}$. Hence it suffices to show $W(Bad, d_0, q) \subseteq W(B^{\uparrow}, d_0, q) \cup W(B^{\downarrow}, d_0, q)$.

We pick any $x_0 = (x_{01}, x_{02}) \in W(Bad, d_0, q)$.

Then, for all $t \geq 0$, there exists $u([0,t))$ and $\sigma_u([0,t))$ s.t. for all $\sigma_d([0,t))$ and $d([0,t))$ with $d(0) = d_0$, $C\phi_x(s, x_0, q_0, u([0,t)), d([0,t)), \sigma_u([0,t)), \sigma_d([0,t))) \notin Bad = B^{\uparrow} \cap B^{\downarrow}$ for all $s \in [0,t)$.

Let's assume $C_1 x_{01} < U_1$ and $C_2 x_{02} < U_2$. Otherwise, the proof will be trivial because

$C_1x_1(t) = y_1(t)$ and $C_2x_2(t) = y_2(t)$ are increasing functions with respect to time.

For all $t \geq 0$, we consider that we apply the control signals $u([0,t))$ and $\sigma_u([0,t))$ s.t. for all $\sigma_d([0,t))$ and $d([0,t))$ with $d(0) = d_0$, $C\phi_x(s, x_0, q_0, u([0,s)), d([0,s)), \sigma_u([0,s)), \sigma_d([0,s))) \notin Bad = B^{\uparrow} \cap B^{\downarrow}$ for all $s \in [0,t)$.

We denote t_1 as the first time instance such that $C_1x_1(t_1) \geq L_1$. Then, because both $C_1x_1(t)$ and $C_2x_2(t)$ are continuous increasing functions with respect to time, we have either $C_2x_2(t_1) < L_2$ or $C_2x_2(t_1) \geq U_2$. Similarly, we denote t_2 as the time instance with $C_1x_1(t_2) = U_1$. Then, we have either $C_2x_2(t_2) \leq L_2$ or $C_2x_2(t_2) > U_2$.

Since both $C_1x_1(t)$ and $C_2x_2(t)$ are continuous increasing functions with respect to time, if $C_2x_2(t_1) < L_2$, then for all $t_1 < \tau < t_2$, we have $C_2x_2(\tau) < L_2$. If $C_2x_2(t_1) \geq U_2$, then for all $t_1 < \tau < t_2$, we have $C_2x_2(\tau) > U_2$.

In the case of $C_2x_2(t_1) < L_2$, for all $0 \leq t \leq t_1$ and $t \geq t_2$, $Cx(t) \notin B^{\downarrow}$. When $t_1 < t < t_2$, $Cx(t) \notin B^{\downarrow}$. Thus, in this case, $x_0 \in W(B^{\downarrow}, d_0, q)$. Similarly, in the case of $C_2x_2(t_1) \geq U_2$, $x_0 \in W(B^{\uparrow}, d_0, q)$.

As a result, $x_0 \in W(B^{\uparrow}, d_0, q) \cup W(B^{\downarrow}, d_0, q)$. $\square$

For a set K and a point x, we define $dist_K(x) = \inf_{k \in K} \|x - k\|_{\infty}$. For a set K, we define the oriented distance function from x to K as $b_K(x) = dist_K(x) - dist_{K^c}(x)$.

Given a finite state machine H, a point x_0, a mode q and $d_0 \in Range_{d2}(q)$, we define the value functions [10, 23]

$$V_H(x_0, q, d_0) = \max_{u([0,\infty)),\sigma_u([0,\infty))} \min_{d([0,\infty)),\sigma_d([0,\infty))} \min_{t \in [0,\infty)} b_{Bad}(C\phi_x(t, x_0, q_0, u([0,t)), d([0,t)), \sigma_u([0,t)), \sigma_d([0,t))))$$

$$V_H^{\uparrow}(x_0, q, d_0) = \max_{u([0,\infty)),\sigma_u([0,\infty))} \min_{d([0,\infty)),\sigma_d([0,\infty))} \min_{t \in [0,\infty)} b_{B^{\uparrow}}(C\phi_x(t, x_0, q_0, u([0,t)), d([0,t)), \sigma_u([0,t)), \sigma_d([0,t))))$$

$$V_H^{\downarrow}(x_0, q, d_0) = \max_{u([0,\infty)),\sigma_u([0,\infty))} \min_{d([0,\infty)),\sigma_d([0,\infty))} \min_{t\in[0,\infty)} b_{B^{\downarrow}}(C\phi_x(t, x_0, q_0, u([0,t)), d([0,t)),$$
$$\sigma_u([0,t)), \sigma_d([0,t))))$$

where σ_u and σ_d trigger the mode transitions in H, u and d are selected in the allowed ranges for specific modes in H, and $d_2(0) = d_0$.

Then, we have

$$W(Bad, d_0, q) = \{x_0 | V_H(x_0, q, d_0) \geq 0\}$$
$$W(B^{\uparrow}, d_0, q) = \{x_0 | V_H^{\uparrow}(x_0, q, d_0) \geq 0\}$$
$$W(B^{\downarrow}, d_0, q) = \{x_0 | V_H^{\downarrow}(x_0, q, d_0) \geq 0\}.$$

Corollary 1. *For a finite state machine H, a point x_0, a mode q and $d_0 \in Range_{d2}(q)$ compatible with q, $\{x_0 | V_H(x_0, q, d_0) \geq 0\} = \{x_0 | \max(V_H^{\uparrow}(x_0, q, d_0), V_H^{\downarrow}(x_0, q, d_0)) \geq 0\}$.*

Proof.

$$\begin{aligned} W(Bad, d_0, q) &= \{x_0 | V_H(x_0, q, d_0) \geq 0\} \\ &= W(B^{\uparrow}, d_0, q) \cup W(B^{\downarrow}, d_0, q) \\ &= \{x_0 | V_H^{\uparrow}(x_0, q, d_0) \geq 0\} \cup \{x_0 | V_H^{\downarrow}(x_0, q, d_0) \geq 0\} \\ &= \{x_0 | \max(V_H^{\uparrow}(x_0, q, d_0), V_H^{\downarrow}(x_0, q, d_0)) \geq 0\}. \end{aligned}$$

□

In the following, we will only show the case for $B^{\uparrow}$, and the case for $B^{\downarrow}$ can be done similarly.

For each *Connect* in the finite state machine, we consider a mode (denoted as q_h) such that for all $q \in Connect$ with $DTF(q) = 0$, $q_h \notin DisturbanceReach(q)$, and $DTF(q_h) = 0$. If $|DisturbanceReach(q_h)| > 1$, then for $q^* \in DisturbanceReach(q_h)$ with $\inf Range_{d2}(q^*) \geq$ inf

$Range_{d2}(q_h)$, we remove all q' with $q' \geq q^*$ from the finite state machine. We denote the remained finite state machine as $H_{cut}^{\uparrow}$.

Given a mode q, we use *CurrentConnect* to denote the *Connect* q is in. We consider the current continuous disturbance signal d_2 to be d_0. We consider the current state of the system to be x_0. We use *ChildConnect* to denote the *Connect* the system can transit to from the current mode. We use q_{end} to denote the mode from which *CurrentConnect* can transit to *ChildConnect* and we use q_p to denote the mode such that $q_{end} \in DisturbanceReach(q_p)$ and $DTF(q_p) = 0$. We define q_n to be the *head* of the *ChildConnect*, and we define $d^* = \inf Range_{d2}(q_n)$.

Now, we consider two cases: $DTF(q) = 0$ and $DTF(q) = 1$.

(1) $DTF(q) = 0$.

We define $t_{tran} = \frac{d_0 - \inf Range_{d2}(q_p)}{\beta}$ if $d_0 \geq \inf Range_{d2}(q_p)$, and we define $t_{stay} = \frac{d_0 - \inf Range_{d2}(q_{end})}{\beta}$.

Then, we define $u^{\uparrow}_{tran}([0, t_{tran})) = (u^{\uparrow}_{tran1}([0, t_{tran})), u^{\uparrow}_{tran2}([0, t_{tran})))$ and $d^{\uparrow}_{tran}([0, t_{tran})) = (d^{\uparrow}_{tran1}([0, t_{tran})), d^{\uparrow}_{tran2}([0, t_{tran})))$ such that for $\tau \in [0, t_{tran})$

(a) $u^{\uparrow}_{tran1}(\tau) = \inf Range_{u1}(q)$

(b) $u^{\uparrow}_{tran2}(\tau) = \sup Range_{u2}(q)$

(c) $d^{\uparrow}_{tran1}(\tau) = \sup Range_{d1}(q)$

(d) $d^{\uparrow}_{tran2}(\tau) = d_0 - \beta\tau$.

We define

$$x_{0n} = \phi_x(t_{tran}, x_0, q, u^{\uparrow}_{tran}([0, t_{tran})), d^{\uparrow}_{tran}([0, t_{tran})), \emptyset, \sigma^{\uparrow}_{dtran}([0, t_{tran})))$$

with $\sigma^{\uparrow}_{dtran}([0, t_{tran}))$ being compatible with $d^{\uparrow}_{tran}([0, t_{tran}))$.

For $t \geq 0$, we define $u^{\uparrow}_{stay}([0, t)) = (u^{\uparrow}_{stay1}([0, t)), u^{\uparrow}_{stay2}([0, t)))$ and $d^{\uparrow}_{stay}([0, t)) = (d^{\uparrow}_{stay1}([0, t)), d^{\uparrow}_{stay2}([0, t)))$ such that for $\tau \in [0, t)$

(a) $u^{\uparrow}_{stay1}(\tau) = \inf Range_{u1}(q)$

(b) $u^{\uparrow}_{stay2}(\tau) = \sup Range_{u2}(q)$

(c) $d^{\uparrow}_{stay1}(\tau) = \sup Range_{d1}(q)$

(d) $d^{\uparrow}_{stay2}(\tau) = \max(d_0 - \beta\tau, \inf Range_{d2}(q_{end}))$.

For $t \geq 0$, we define

$$d_{B^{\uparrow}stay}(t) = d_{B^{\uparrow}}(C\phi_x(t, x_0, q, u^{\uparrow}_{stay}([0,t)), d^{\uparrow}_{stay}([0,t)), \emptyset, \sigma^{\uparrow}_{dstay}([0,t))))$$

with $\sigma^{\uparrow}_{dstay}([0,t))$ being compatible with $d^{\uparrow}_{stay}([0,t))$.

Also, for $t \geq 0$, we define $u^{\uparrow}_c([0,t)) = (u^{\uparrow}_{c1}([0,t)), u^{\uparrow}_{c2}([0,t)))$ and $d^{\uparrow}_c([0,t)) = (d^{\uparrow}_{c1}([0,t)), d^{\uparrow}_{c2}([0,t)))$ such that for $\tau \in [0,t)$

(a) $u^{\uparrow}_{c1}(\tau) = \inf Range_{u1}(q)$

(b) $u^{\uparrow}_{c2}(\tau) = \sup Range_{u2}(q)$

(c) $d^{\uparrow}_{c1}(\tau) = \sup Range_{d1}(q)$

(d) $d^{\uparrow}_{c2}(\tau) = \max(d_0 - \beta\tau, \inf Range_{d2}(q_p))$.

For $t \geq 0$, we define

$$d_{B^{\uparrow}c}(t) = d_{B^{\uparrow}}(C\phi_x(t, x_0, q, u^{\uparrow}_c([0,t)), d^{\uparrow}_c([0,t)), \emptyset, \sigma^{\uparrow}_{dc}([0,t))).$$

with $\sigma^{\uparrow}_{dc}([0,t))$ being compatible with $d^{\uparrow}_c([0,t))$.

It should be noted that if the current mode q is q_{end} and $ControlReach(q) \neq \emptyset$, then being trapped in the current $Connect$ is not possible . In this case, q_p does not exist, and we define $\min_t d_{B^{\uparrow}c}(t) = \infty$.

(2) $DTF(q) = 1$.

Definition 8. $NoTranDT(q) = \{q' | q' \in DisturbanceReach(q)$ and $ControlReach(q') = \emptyset\}$.

Now, we use q_t to denote $\max(NoTranDT(q))$.

We denote the time the mode has stayed in q as RT_s, and we denote $RT_l = DT(q) - RT_s$ as the remaining time the mode will stay in q. We define $t_{tran} = max(0, \frac{\inf Range_{d2}(q_t) - \inf Range_{d2}(q_p)}{\beta})$, and we define $t_{stay} = \frac{\inf Range_{d2}(q_t) - \inf Range_{d2}(q_{end})}{\beta}$.

Then, we define $u^{\uparrow}_{tran}([0, RT_l + t_{tran})) = (u^{\uparrow}_{tran1}([0, RT_l + t_{tran})), u^{\uparrow}_{tran2}([0, RT_l + t_{tran})))$ and $d^{\uparrow}_{tran}([0, RT_l + t_{tran})) = (d^{\uparrow}_{tran1}([0, RT_l + t_{tran})), d^{\uparrow}_{tran2}([0, RT_l + t_{tran})))$ such that for $\tau \in [0, RT_l + t_{tran})$

(a) $u^{\uparrow}_{tran1}(\tau) = \inf Range_{u1}(q)$

(b) $u^{\uparrow}_{tran2}(\tau) = \sup Range_{u2}(q)$

(c) $d^{\uparrow}_{tran1}(\tau) = \sup Range_{d1}(q)$

(d) $d^{\uparrow}_{tran2}(\tau) = \inf Range_{d2}(q)$ if $\tau \in [0, RT_l]$ and $d^{\uparrow}_{tran2}(\tau) = \inf Range_{d2}(q_t) - \beta(\tau - RT_l)$ if $\tau \in (RT_l, RT_l + t_{tran})$.

We define

$$x_{0n} = \phi_x(RT_l + t_{tran}, x_0, q, u^{\uparrow}_{tran}([0, RT_l + t_{tran})), d^{\uparrow}_{tran}([0, RT_l + t_{tran})), \emptyset, \sigma^{\uparrow}_{dtran}([0, RT_l + t_{tran})))$$

with $\sigma^{\uparrow}_{dtran}([0, RT_l + t_{tran}))$ being compatible with $d^{\uparrow}_{tran}([0, RT_l + t_{tran}))$.

For $t \geq 0$, we define $u^{\uparrow}_{stay}([0, t)) = (u^{\uparrow}_{stay1}([0, t)), u^{\uparrow}_{stay2}([0, t)))$ and $d^{\uparrow}_{stay}([0, t)) = (d^{\uparrow}_{stay1}([0, t)), d^{\uparrow}_{stay2}([0, t)))$ such that for $\tau \in [0, t)$ with $t \geq RT_l$

(a) $u^{\uparrow}_{stay1}(\tau) = \inf Range_{u1}(q)$

(b) $u^{\uparrow}_{stay2}(\tau) = \sup Range_{u2}(q)$

(c) $d^{\uparrow}_{stay1}(\tau) = \sup Range_{d1}(q)$

(d) $d^{\uparrow}_{stay2}(\tau) = \inf Range_{d2}(q)$ if $\tau \in [0, RT_l]$. If $\tau > RT_l$, then

   i if $q_{end} \notin DisturbanceReach(q)$, then $d^{\uparrow}_{stay2}(\tau) = \max(\inf Range_{d2}(q_t) - \beta(\tau - RT_l), \inf Range_{d2}(q_{end}))$;

   ii if $q_{end} \in DisturbanceReach(q)$, then $d^{\uparrow}_{stay2}(\tau) = \inf Range_{d2}(q_{end})$.

For $t \geq 0$, we define

$$d_{B^{\uparrow}stay}(t) = d_{B^{\uparrow}}(C\phi_x(t, x_0, q, u^{\uparrow}_{stay}([0, t)), d^{\uparrow}_{stay}([0, t)), \emptyset, \sigma^{\uparrow}_{dstay}([0, t))))$$

with $\sigma^{\uparrow}_{dstay}([0,t))$ being compatible with $d^{\uparrow}_{stay}([0,t))$.

Also, for $t \geq 0$, we define $u^{\uparrow}_{c}([0,t)) = (u^{\uparrow}_{c1}([0,t)), u^{\uparrow}_{c2}([0,t)))$ and $d^{\uparrow}_{c}([0,t)) = (d^{\uparrow}_{c1}([0,t)), d^{\uparrow}_{c2}([0,t)))$ such that for $\tau \in [0,t)$ with $t \geq RT_l$

(a) $u^{\uparrow}_{c1}(\tau) = \inf Range_{u1}(q)$

(b) $u^{\uparrow}_{c2}(\tau) = \sup Range_{u2}(q)$

(c) $d^{\uparrow}_{c1}(\tau) = \sup Range_{d1}(q)$

(d) $d^{\uparrow}_{c2}(\tau) = \inf Range_{d2}(q)$ if $\tau \in [0, RT_l]$ and $d^{\uparrow}_{c2}(\tau) = \max(\inf Range_{d2}(q_t) - \beta(\tau - RT_l), \inf Range_{d2}(q_p))$ if $\tau > RT_l$.

For $t \geq 0$, we define

$$d_{B^{\uparrow}c}(t) = d_{B^{\uparrow}}(C\phi_x(t, x_0, q, u^{\uparrow}_{c}([0,t)), d^{\uparrow}_{c}([0,t)), \emptyset, \sigma^{\uparrow}_{dc}([0,t))).$$

with $\sigma^{\uparrow}_{dc}([0,t))$ being compatible with $d^{\uparrow}_{c}([0,t))$.

It should be noted that if q_t or q_p does not exist, then being trapped in the current *Connect* is not possible. In this case, we define $\min_t d_{B^{\uparrow}c}(t) = \infty$.

For any x_0, d_0 and H, we define $V^{\uparrow}_{H}(x_0, \emptyset, d_0) = -\infty$.

Proposition 1. $V^{\uparrow}_{H}(x_0, q, d_0) = \min(\max(\min_t d^{\uparrow}_{Bstay}(t), \max_{q_n \in ControlReach(q_{end})} V^{\uparrow}_{H^{\uparrow}_{cut}}(x_{0n}, q_n, d^*)), \min_t d^{\uparrow}_{Bc}(t))$, *where* $q_{end} \in DSR(q)$ *and* $DisturbanceReach(q_{end}) = \emptyset$.

Given the current mode of the system, we can determine the *Connect* the mode is in. Then, there are three options we have.

(1) The mode of the system transits within $NotTran(q)$ and the mode of the system is trapped in the current *Connect* without the ability to transit to other *Connects*. If staying within $NotTran(q)$ gives a negative value function, which means that $\min_t d^{\uparrow}_{Bc}(t) < 0$, then the whole value function will have a negative value and no control map can guarantee safety.

(2) The mode of the system transits to $Branch(q)$. Now, the controller can decide whether to stay in the mode of $Branch(q)$, or transit the next *Connect*, based on which way provides a larger value function.

(a) If staying in $Branch(q)$ provides a non-negative value, then a non-negative value of the whole value function is found and a control map exists to guarantee safety.

(b) If staying in $Branch(q)$ provides a negative value, then it means that staying in $Branch(q)$ cannot guarantee safety and transiting to the next *Connect* is needed. At the end, if the system reaches the *Connect* from which no more *Connect* transitions are possible, and staying in that *Connect* is not safe, then the value function has a negative value, and no control map can guarantee safety.

In order to prove Proposition 1, we will first introduce the following propositions. Based on the following propositions, Proposition 1 is a direct result.

Proposition 2. *For all $t > 0$, if for all $0 \leq s < t$, we have $u^1(s) = (u_1^1(s), u_2^1(s))$ and $u^2(s) = (u_1^2(s), u_2^2(s))$ such that $u_1^1(s) \geq u_1^2(s)$ and $u_2^1(s) \leq u_2^2(s)$, and $d^1(s) = (d_1^1(s), d_2^1(s))$ and $d^2(s) = (d_1^2(s), d_2^2(s))$ such that $d_1^1(s) \leq d_1^2(s)$ and $d_2^1(s) \geq d_2^2(s)$, then starting from $x_0 = (x_{01}, x_{02})$, using the same continuous dynamics, we have $d_{B^\uparrow}((y_1^1(t), y_2^1(t)))$ $\leq d_{B^\uparrow}((y_1^2(t), y_2^2(t)))$, where $(y_1^1(t), y_2^1(t))$ is the point reached using u^1 and d^1, and $(y_1^2(t), y_2^2(t))$ is the point reached using u^2 and d^2.*

Proof. By the order preserving property, it is know that $y_1^1(t) \geq y_1^2(t)$ and $y_2^1(t) \leq y_2^2(t)$. By the definition of the oriented distance function, $d_{B^\uparrow}((y_1(t), y_2(t)))$ either equals to $L_1 - y_1(t)$ or $y_2(t) - U_2$. Since $L_1 - y_1^1(t) \leq L_1 - y_1^2(t)$ and $y_2^1(t) - U_2 \leq y_2^2(t) - U_2$, we have $d_{B^\uparrow}((y_1^1(t), y_2^1(t))) \leq d_{B^\uparrow}((y_1^2(t), y_2^2(t)))$. □

What we have shown implies that staying in the same *Connect* (which means that the same continuous dynamics are used), decreasing u_1, increasing u_2 will increase the value function and increasing d_1, decreasing d_2 will decrease the value function.

For any $t \geq 0$, if we are given $\sigma_d([0,t))$ and $\sigma_u([0,t))$, then Proposition 3 follows directly from Proposition 2.

For $t \geq 0$, if we are given $\sigma_d([0,t))$ and $\sigma_u([0,t))$, then for each time instance $t \geq 0$, we have $u_1(t) \in [u_1^l(t), u_1^u(t)]$, $u_2(t) \in [u_2^l(t), u_2^u(t)]$, $d_1(t) \in [d_1^l(t), d_1^u(t)]$ and $d_2(t) \in [d_2^l(t), d_2^u(t)]$. If we are given the upper and lower bounds for u_1, u_2, d_1 and d_2, for $t \geq 0$, we define $u^\uparrow([0,t)) = (u_1^\uparrow([0,t)), u_2^\uparrow([0,t)))$ such that for all $\tau \in [0,t)$, we have $u_1^\uparrow(\tau) = u_1^l(\tau)$ and

$u_2^\uparrow(\tau) = u_2^u(\tau)$. Also, we define $d^\uparrow([0,t)) = (d_1^\uparrow([0,t)), d_2^\uparrow([0,t)))$ such that for all $\tau \in [0,t)$, we have $d_1^\uparrow(\tau) = d_1^u(\tau)$ and $d_2^\uparrow(\tau) = d_2^l(\tau)$.

Proposition 3.

$$\max_{u([0,\infty))} \min_{d([0,\infty))} \min_{t\in[0,\infty)} b_{B^\uparrow}(C\phi_x(t, x_0, q_0, u^\uparrow([0,t)), d^\uparrow([0,t)), \sigma_u([0,t)), \sigma_d([0,t))))$$
$$= \min_{t\in[0,\infty)} b_{B^\uparrow}(C\phi_x(t, x_0, q_0, u^\uparrow([0,t)), d^\uparrow([0,t)), \sigma_u([0,t)), \sigma_d([0,t)))).$$

Notice that if we are given $\sigma_d([0,t))$ and $\sigma_u([0,t))$, then for each time instance, we need to pick the optimal continuous control and disturbance signals to optimize the oriented distance. If $\sigma_d([0,t))$ and $\sigma_u([0,t))$ are not given and we need to pick optimal $\sigma_d([0,t))$ and $\sigma_u([0,t))$ to optimize the value function, then we optimize the value function by changing the bounds for the continuous signals $u([0,t))$ and $d([0,t))$ using $\sigma_d([0,t))$ and $\sigma_u([0,t))$.

From Proposition 2, another result we have is the following proposition.

Proposition 4. $V_H^\uparrow(x_0, q, d_0) = V_{H_{cut}^\uparrow}^\uparrow(x_0, q, d_0)$.

Proof. From Proposition 2, it is known that the disturbance signals minimize the value function by picking the minimal continuous disturbance signal at each time instance. Thus, the node removed from H will never be reached and considered in the calculation of the value function because going through those removed nodes will increase the minimal continuous disturbance signal we can pick. As a result, the value function calculated considering H will be the same as the value function calculated considering $H_{cut}^\uparrow$. □

Given the current mode of the system, the mode of the system will either get stuck in the current *Connect* or reach a mode, from which either the mode of the system can go to another *Connect*, or no more transitions are possible. The discrete disturbance signal will select among getting stuck and go to "the last" mode of the current *Connect* in order to minimize the value function. If the mode of the system reaches the last mode of the current *Connect*, then the discrete control signal will select whether to stay or go to the following *Connect* in order to maximize the value function. Thus, we have Proposition 1.

Proposition 5. *For all x_0, q and d_0, if $V_H(x_0, q, d_0) > 0$, then there exists an s s.t.,*

$$V_H(\phi_x(s, x_0, u^\dagger([0,s)), d([0,s)), \emptyset, \sigma_d([0,s))), \phi_q(q, \emptyset, \sigma_d([0,s))), d_0(s)) > 0$$

for all $d([0,s))$ and $\sigma_d([0,s)))$.

Proof. If $V_H(x_0, q, d_0) > 0$, then we know that there exist control signals, such that no matter what disturbance signals are applied, on trajectories of (y_1, y_2), the point which is most closed to the set Bad has a positive distance from the set Bad. Among the trajectories, let us pick the trajectory whose most closed point to Bad has the smallest distance. This trajectory corresponds to the best case control and worst case disturbance. We denote that point as $Cx_d = (C_1x_{d1}, C_2x_{d2})$. There exists a $\delta > 0$ and a neighborhood $Ne(Cx_d)_\delta$ around Cx_d such that for any point $y^* \in Ne(Cx_d)_\delta$, $\|Cx_d - y^*\| \leq \delta$ and $b_{Bad}(y^*) > 0$. Let's denote $\inf_{y^* \in Ne(Cx_d)_\delta} b_{Bad}(y^*) = Cri_d$. For a trajectory of (y_1, y_2) (denoted as TJ), we define the distance from the trajectory TJ to the set Bad as $\inf_{p \in TJ} b_{Bad}(p)$. Because both y_1 and y_2 are continuous with respect to time and increasing, then there exists a neighborhood around Cx_0, such that trajectories of (y_1, y_2) starting from any point in the neighborhood have a minimum distance greater or equal than Cri_d. Since both y_1 and y_2 are continuous with respect to time, then there exists an s s.t.,

$$V_H(\phi_x(s, x_0, u^\dagger([0,s)), d([0,s)), \emptyset, \sigma_d([0,s))), \phi_q(q, \emptyset, \sigma_d([0,s))), d_0(s)) > 0$$

for all $d([0,s))$ and $\sigma_d([0,s)))$.

It should be noted that if the controller is able to apply discrete control signals to switch $Connect$, then the mode of the system has arrived to a q_{end} which is a $Branch$ mode as defined in Definition 5. When the mode of the system has arrived q_{end}, and no discrete control signals are applied, then in the future, applying the discrete control signals is still possible. □

Proposition 6. *For all $s > 0$, there exists $\sigma_d^\dagger([0,s)))$ and corresponding $d^\dagger([0,s))$ such that*

$$V_H(x_0, q, d_0) \geq V_H(\phi_x(s, x_0, u^\dagger([0,s)), d^\dagger([0,s)), \emptyset, \sigma_d^\dagger([0,s))), \phi_q(q, \emptyset, \sigma_d^\dagger([0,s))), d_0(s)).$$

Proof. This is trivial from the definition of the value function since by applying σ_u, we try to maximize the value function. $\square$

In the calculation of the value function, it is assumed that q and d_2 are measured. In that case, given a finite state machine H, we can calculate the value function to find the control map. However, if d_2 and q are not directly measured, then we need to modify the hybrid system so that we can still use the solution to Problem 1 to find the control map.

In the next section, we will introduce a disturbance estimator to estimate d_2. Then, based on the estimation of d_2, we will construct a hybrid system based on H with modified $Range_{d_2}$ and transition evoking events.

Chapter 6

A Disturbance Estimator

In this section, we will introduce a disturbance estimator presented in [5].

6.1 Problem Statement and Assumptions

We consider systems described by

$$\dot{x} = Ax + Bd + Wu \tag{6.1}$$

$$y = Cx \tag{6.2}$$

where $x(t) \in \mathbb{R}^n$ is the system state and $y(t) \in \mathbb{R}^p$ is the measured output at time $t \in \mathbb{R}$. The continuous control signal $u(t) \in \mathbb{R}^w$ models the control inputs to the system, and the continuous disturbance signal $d(t) \in \mathbb{R}^m$ models all uncertain in the system and it is regarded as an unknown state-independent time-varying input. A, B, C and W are known constant real matrices.

In order to estimate $x(t)$ and $d(t)$, we need the following two assumptions.

Assumption 11. *$rank(CB) = rank(B)$.*

Assumption 12. *For every complex number λ with nonnegative real part, $rank(\begin{bmatrix} A - \lambda I & B \\ C & 0 \end{bmatrix}) = n + rank(B)$.*

We design of matrices P, L, and G as the followings:

(1) Find S and T such that $\hat{A} = T^{-1}AT = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, $\hat{B} = T^{-1}B = \begin{bmatrix} B_1 \\ 0 \end{bmatrix}$, and $\hat{C} = S^{-1}CT = \begin{bmatrix} C_{11} & 0 \\ 0 & C_{22} \end{bmatrix}$.

(2) Find $\hat{P}$, $\hat{L}$, and $\hat{G}$ such that

$$\hat{P} > 0 \tag{6.3a}$$

$$\hat{P}(\hat{A} + \hat{L}\hat{C}) + (\hat{A} + \hat{L}\hat{C})^T \hat{P} < 0 \tag{6.3b}$$

$$\hat{B}^T \hat{P} = \hat{G}\hat{C}. \tag{6.3c}$$

To do that, we need to follow the following steps.

(a) Choose L_{22} such that $A_{22} + L_{22}C_{22}$ is Hurwitz.

(b) Choose $P_{22} > 0$, then $\hat{P} = \begin{bmatrix} I_{m*} & 0 \\ 0 & P_{22} \end{bmatrix}$

(c) Define

$$Q_{22} = -[P_{22}(A_{22} + L_{22}C_{22}) + (A_{22} + L_{22}C_{22})^T P_{22}] > 0$$
$$\tilde{Q}_{11} = A_{11} + A_{11}^T + (A_{12} + A_{21}^T P_{22}) Q_{22}^{-1} (A_{12}^T + P_{22} A_{21})$$

Choose $\kappa > \frac{\lambda_{max}(\tilde{Q}_{11})}{2}$. Then we have $\hat{L} = \begin{bmatrix} -\kappa C_{11}^{-1} & 0 \\ 0 & L_{22} \end{bmatrix}$.

(d) Make $\hat{G} = \begin{bmatrix} B_1^T C_{11}^{-1} & 0 \end{bmatrix}$.

(3) The transformations

$$P = (T^T)^{-1} \hat{P} T^{-1} \tag{6.4a}$$

$$L = T \hat{L} S^{-1} \tag{6.4b}$$

$$G = \hat{G} S^{-1}. \tag{6.4c}$$

transform $\hat{P}$, $\hat{L}$, and $\hat{G}$ to P, L, and G.

6.2 A State and Disturbance Estimator

We construct the state and disturbance estimator as follows.

$$\dot{\hat{x}} = A\hat{x} + B\hat{d} + Wu + L(C\hat{x} - y) \tag{6.5a}$$

$$\dot{\hat{d}} = -\gamma G(C\hat{x} - y) \tag{6.5b}$$

where γ is a positive scalar, the initial estimate $\hat{x}(t_0) = \hat{x}_0$ is arbitrary, and $\hat{x}(t)$ and $\hat{d}(t)$ are the estimates of $x(t)$ and $d(t)$ respectively. We need $\|d(t)\| \leq \beta_1$ and $\|\dot{d}(t)\| \leq \beta_2$.

We define $\alpha = \frac{\lambda_{min}(P^{-1}Q)}{2} > 0$ and $a = (\frac{\lambda_{max}(P)}{\lambda_{min}(P)})^{\frac{1}{2}}$. Based on the analysis in [5], by making $\gamma \geq \max\{\frac{\beta_1^2}{2\mu_1}, \frac{\beta_2^2}{2\mu_2}\}$ where μ_1 and μ_2 are two non-negative real numbers which can be chosen arbitrarily. We define

$$Bound(\gamma, t) = a\{\|B^L(A+LC)\|[(\frac{\mu_1}{2\alpha})^{\frac{1}{2}} + \|e(t_0)\|e^{-\alpha(t-t_0)}] + \|B^L\|[(\frac{\mu_2}{2\alpha})^{\frac{1}{2}} + \|\dot{e}(t_0)\|e^{-\alpha(t-t_0)}]\}. \tag{6.6}$$

Then, we have $d(t) \in dRange(\gamma, t) = [\hat{d}(t) - Bound(\gamma, t), \hat{d}(t) + Bound(\gamma, t)]$.

Chapter 7

Mode Estimation

In this section, we consider the construction of a mode estimator based on the result from the disturbance estimator.

It should be noted that mode estimation is needed

- when the mode of the system is in a *Connect*, whose *head* q_h does not have dwell time, contains more than one mode;
- or when the mode of the system is in a *Connect*, whose *head* q_h has dwell time, contains more than two modes.

Let's consider the mode of the system is in a *Connect* which satisfies the two conditions for requiring mode estimation, and we define the time instance at which the mode of the system enters the *Connect* as $\tau = 0$. We record the time instance for entering the *Connect* as t^*. The disturbance estimator is started when $\tau = 0$. It should be noted that the time instance in the *Connect*, τ, corresponds to a time instance t for running the whole hybrid system with the relationship $t = t^* + \tau$.

Given the *Connect* $q(t)$ is currently in, we use the following algorithm to calculate $\hat{q}(t)$.

Given a *Connect*, we use $NoDTMode(Connect) = \{q \in Connect | DTF(q) = 0\}$.

When the dwell time of the *head* has passed, we will begin to do the mode estimation. If *head* does not have dwell time, then we start mode estimation as soon as the mode of the system enters the *Connect*.

From Algorithm 1, Corollary 2 is a direct result.

Algorithm 1 Calculation of $\hat{q}(t)$

procedure PROCEDURE FOR CALCULATING $\hat{q}(t)(Connect)$
    $ModeR = NoDTMode(Connect)$ and $\hat{q}(t) = NoDTMode(Connect)$
    while $q(t) \in NoDTMode(Connect)$ **do**
        $\hat{q}(t) = DSR(\min(\{q | q \in ModeR \text{ and } Range_{d2}(q) \cap dRange(\tau) \neq \emptyset\}))$
        $ModeR = \hat{q}(t)$
    end while
end procedure

Corollary 2. *For $t \geq 0$, we have $q(t) \in \hat{q}(t)$.*

Corollary 2 shows that the mode estimator is a correct estimator since the true of the system is always contained in the estimated modes.

Chapter 8

Transformations from H to $\hat{H}$

In this section, we consider how to construct the hybrid system $\hat{H}$ based on the structure of H.

From system H to $\hat{H}$, the structure of the finite state machine remains the same. The ranges for u_1, u_2 and d_1 in corresponding modes are the same. We need to modify the evoking conditions for discrete disturbance transitions and $Range_{d_2}$ for each mode.

For each mode $q \in H$, we label the mode of $\hat{H}$ at the corresponding position as $\hat{q}$.

For the evoking conditions for discrete disturbance transitions, since the disturbance transitions events and the continuous disturbance signals cannot be directly measured, we use the mode estimation method introduced in the previous section to determine whether there will be a mode transition in system $\hat{H}$.

For each *Connect*, we define the time instance at which the mode of the system enters the *Connect* as $\tau = 0$, and the disturbance estimation is started at $\tau = 0$. For two modes q_1 and q_2 in the *Connect* with $q_2 \in DisturbanceReach(q_1)$ and $DTF(q_1) = 0$ and $DTF(q_2) = 0$,

- if $\sup Range_{d2}(q_2) > \sup Range_{d2}(q_1)$, then the event $\inf dRange(\tau) > \sup Range_{d2}(q_1)$ triggers the mode transition from $\hat{q}_1$ to $\hat{q}_2$;

- if $\sup Range_{d2}(q_2) \leq \sup Range_{d2}(q_1)$, then the event $\sup dRange(\tau) < \inf Range_{d2}(q_1)$ triggers the mode transition from $\hat{q}_1$ to $\hat{q}_2$.

For a mode $q \in Q$ with dwell time, the corresponding mode $\hat{q} \in \hat{Q}$ has the same dwell time. Disturbance transitions leaving $\hat{q}$ is triggered by the dwell time and $Range_{d2}$ of the modes in the $DisturbanceReach(\hat{q})$.

For modifying $Range_{d_2}(q)$ of $q \in Q$, we consider the modification method introduced below.

For $q \in Q$ such that

(i) $ControlReach(q) \neq \emptyset$

(ii) $\exists q' \in Q$ s.t. $ControlReach(q') = \{q\}$

(iii) $DTF(q) = 1$

we have $Range_{d_2}(\hat{q}) = Range_{d_2}(q)$.

For other cases, we consider the modifications below.

Again, for each $Connect$, we define the time instance at which the mode of the system enters the $Connect$ as $\tau = 0$. It should be noted that $\tau = 0$ is the time when we start the disturbance estimation. Then, for each $\tau \geq 0$, $Range_{d_2}$ for each mode is calculated as the following.

For $q \in Q$ and $DTF(q) = 0$, we consider $q' \in DisturbanceReach(q)$.

- If $BR_{d2}(q, q') = \sup Range_{d2}(q)$, then the corresponding bound $BR_{d2}(\hat{q}, \hat{q'}) = BR_{d2}(q, q') + 2Bound(\tau)$.
- If $BR_{d2}(q, q') = \inf Range_{d2}(q)$, then the corresponding bound $BR_{d2}(\hat{q}, \hat{q'}) = BR_{d2}(q, q') - 2Bound(\tau)$.

After the modification, the hybrid system H can be transformed to $\hat{H}$. H and $\hat{H}$ share the same finite state machine structure. $Range_{d_2}(q)$ is modified for each mode. In order to calculate the value function for $\hat{H}$, we consider the following modifications to the input signals.

The inputs to the algorithm of finding the control map at time instance t are $q(t)$, $x(t)$, $d_2(t)$, and a hybrid system H. In system $\hat{H}$, at each time instance t, $q(t)$ is known by mode estimation. $x(t)$ is measured. For the $Connect$ which $q(t)$ belongs to, we define the time instance at which the mode of the system enters the $Connect$ as $\tau = 0$. Then, d_2 at time instance t with corresponding τ are determined as the following.

- For calculating value functions with $B^{\uparrow}$, we use $d_2(t) = \inf dRange(\tau)$.
- For calculating value functions with $B^{\downarrow}$, we use $d_2(t) = \sup dRange(\tau)$.

The block diagram in Fig 8-1 shows how to calculate the value function using the results from disturbance estimator and mode estimator at each time instance $t \geq 0$.

- Using $dRange(t)$, we modify $Range_{d2}(q)$ to get $Range_{d2}(\hat{q})$.
- The same finite state machine structure is kept from H to $\hat{H}$.
- Using mode estimator and $dRange(t)$, we estimate the mode of the system, $\hat{q}(t)$. $\hat{q}(t)$ is used as the input to the algorithm for calculating value function.
- We use $\inf dRange$ and $\sup dRange$ to calculate $V^{\uparrow}$ and $V^{\downarrow}$ respectively.
- The continuous state $x(t)$ is used as input to the algorithm.

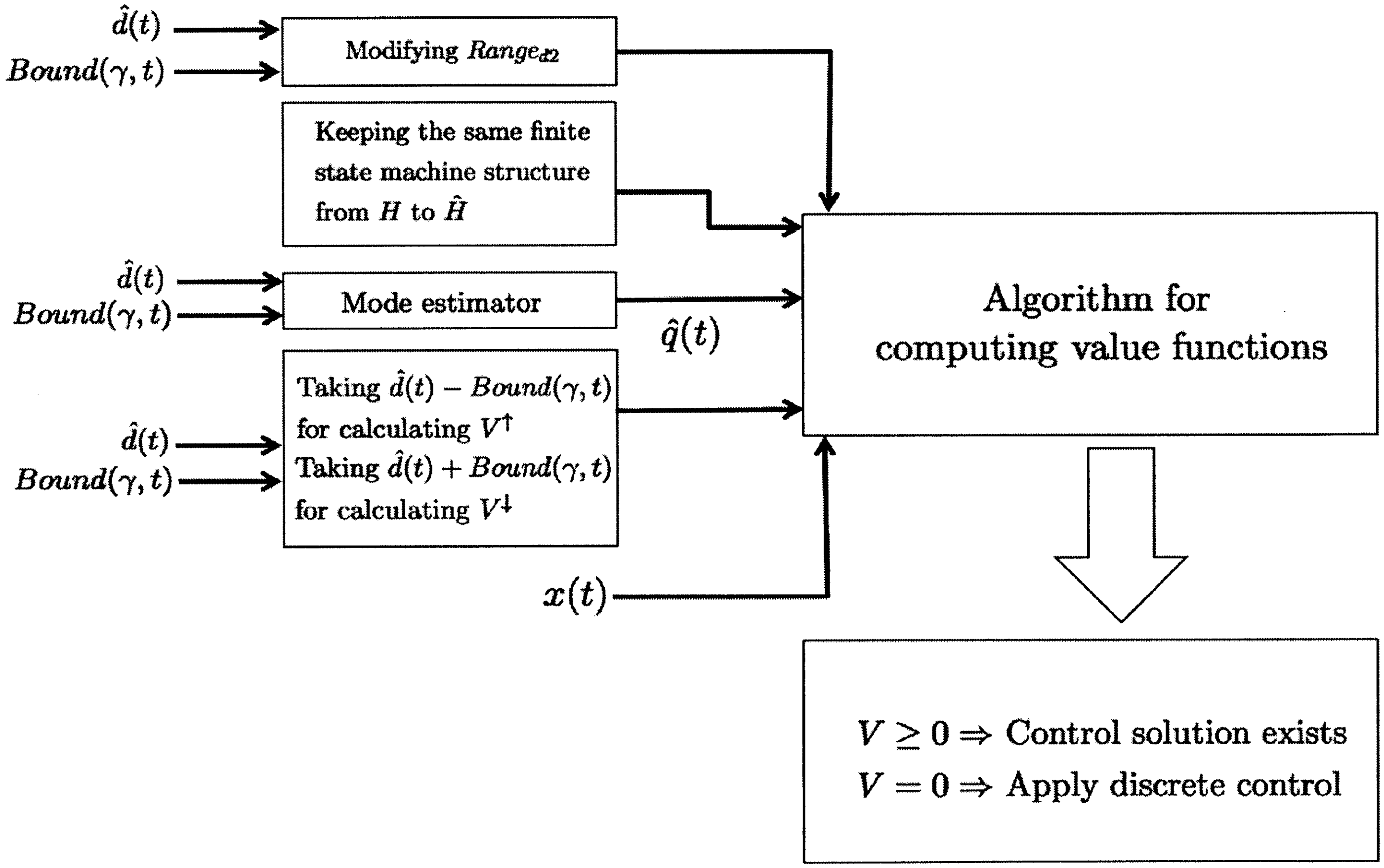

Figure 8-1: Calculate the value function using results from disturbance and mode estimator

In the simulation example, the system H is transformed in to $\hat{H}$ which is shown in Fig 8-2.

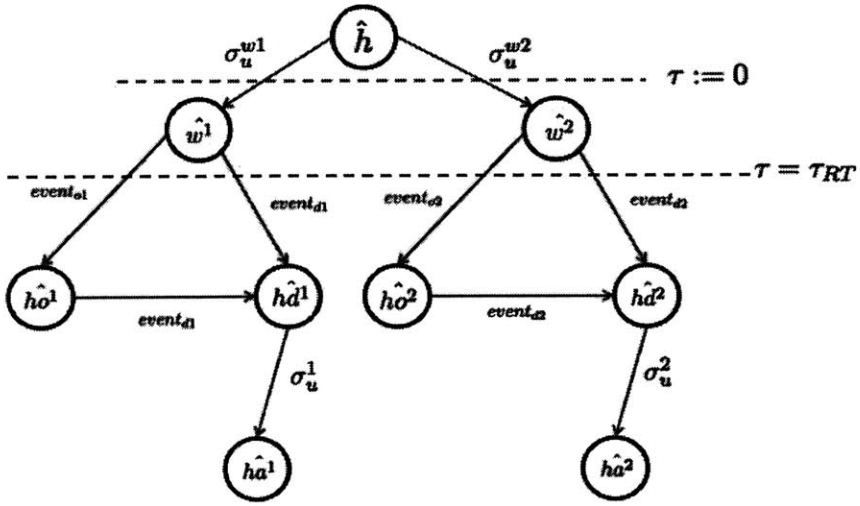

Figure 8-2: System $\hat{H}$

From H to $\hat{H}$, we modify the $Range_{d_2}$ for ho^1, hd^1, ho^2, and hd^2. We have $Range_{d_2}(\hat{ho^1}) = [-\bar{d}, -\bar{d} + \epsilon + 2Bound(t)]$, $Range_{d_2}(\hat{hd^1}) = [-\bar{d}, \bar{d}]$, $Range_{d_2}(\hat{ho^2}) = [\bar{d} - \epsilon - 2Bound(t), \bar{d}]$, and $Range_{d_2}(\hat{hd^2}) = [-\bar{d}, \bar{d}]$.

For the mode transition events, we have:

- $event_{o1}$: $\inf dRange(t) < -\bar{d} + \epsilon$
- $event_{d1}$: $\inf dRange(t) \geq -\bar{d} + \epsilon$
- $event_{o2}$: $\sup dRange(t) > \bar{d} - \epsilon$
- $event_{d2}$: $\sup dRange(t) \leq \bar{d} - \epsilon$.

All of other parameter ranges and finite state machine structure remain the same from H to $\hat{H}$.

Chapter 9

Simulation Example

In this section, we consider the solution to the motivation example. We define the intersection as $Int = (L_1, U_1) \times (L_2, U_2)$ and we need to design the control system such that $(p_1(t), p_2(t)) \notin Int$ for any $t \geq 0$. Thus, the set $Bad = (L_1, U_1) \times (L_2, U_2)$ in this example.

9.1 Model of Finite State Machine H

We model the whole system as a finite state machine H as shown in Fig. 9-2. For all $t \geq 0$, we have $a_1(t) = d_1(t)$. $a_2(t) = u_2(t)$ if the system is in the overriding mode (ha^1 and ha^2). Otherwise, we have $a_2(t) = d_2(t)$. Now, we introduce the allowed range for each mode.

For all modes q in the finite state machine, we have $Range_{d1}(q) = [-\bar{d}, \bar{d}]$, and $Range_{u2}(q) = [-\bar{u}, \bar{u}]$. We do not consider $Range_{u1}(q)$ since u_1 does not appear in the system dynamics for all modes. For $Range_{d2}(q)$, we have $Range_{d2}(q) = [-\bar{d}, \bar{d}]$ if $q \neq ho^1$ and $q \neq ho^2$. We have $Range_{d2}(ho^1) = [-\bar{d} + \epsilon, \bar{d}]$ and $Range_{d2}(ho^2) = [-\bar{d}, \bar{d} - \epsilon]$.

We need to construct a control map $(\sigma_u^{w1}([0,t)), \sigma_u^{w2}([0,t)), \sigma_u^1([0,t)), \sigma_u^2([0,t)), u_2([0,t)))$ such that for all possible $(\sigma_d^{d1}([0,t)), \sigma_d^{o1}([0,t)), \sigma_d^{d2}([0,t)), \sigma_d^{o2}([0,t)), d_1([0,t)), d_2([0,t)))$, $(p_1(t), p_2(t)) \notin Bad$ for all $t \geq 0$.

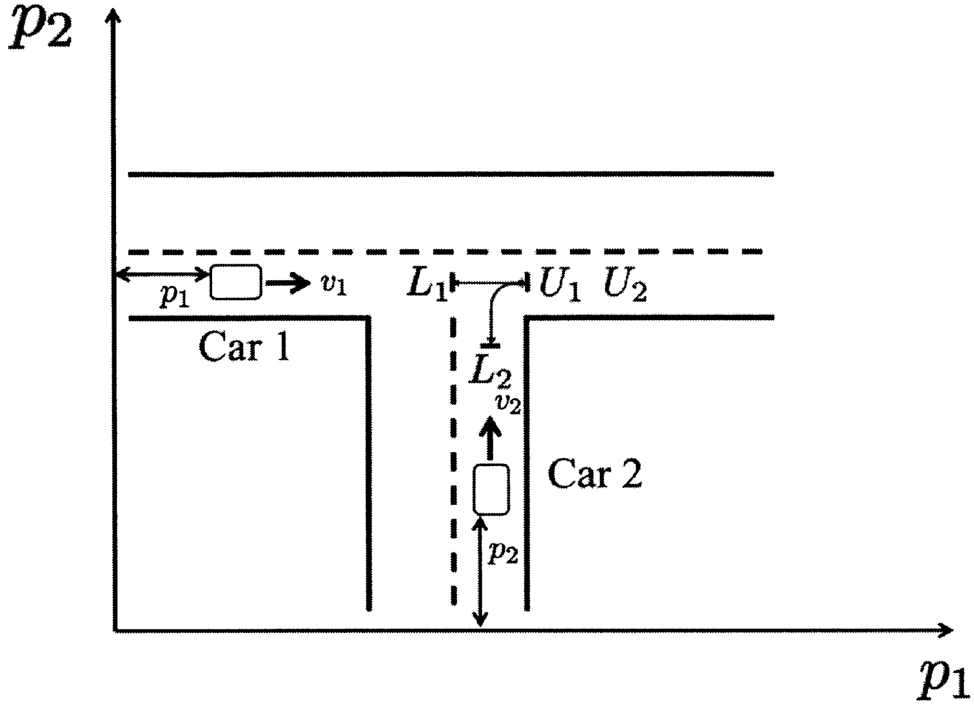

Figure 9-1: Problem scenario

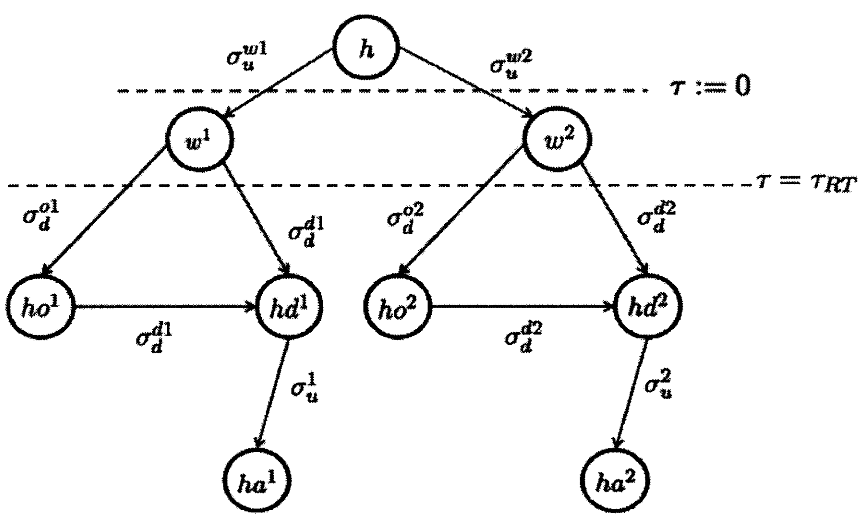

Figure 9-2: System H

9.2 Construction of Estimation Finite State Machine $\hat{H}$

Since we cannot measure the reaction of the driver of the semi-autonomous vehicle to the issued warning, which means that σ_d^{o1}, σ_d^{d1}, σ_d^{o2}, and σ_d^{d2} are not known, the system H is a hybrid system with hidden modes. Thus, we consider to construct an estimation hybrid system $\hat{H}$. In order to construct $\hat{H}$, we need to estimate the acceleration input from the driver of the semi-autonomous vehicle, i.e., we need to estimate d_2 in order to estimate whether the driver has disobeyed the issued warning or not.

We consider to use the disturbance estimator defined in Eq. (6.5a) and Eq. (6.5b). For this simulation example, we have $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $W = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ and $C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Running the disturbance estimator, we get $d_2(t) \in dRange(t) = [\hat{d}_2(t) - Bound(t), \hat{d}_2(t) + Bound(t)]$.

For $t \geq \tau_{RT}$, we define

- $event_{o1}$: $\inf dRange(t) < -\bar{d} + \epsilon$
- $event_{d1}$: $\inf dRange(t) \geq -\bar{d} + \epsilon$
- $event_{o2}$: $\sup dRange(t) > \bar{d} - \epsilon$
- $event_{d2}$: $\sup dRange(t) \leq \bar{d} - \epsilon$.

Let's assume that the braking warning is the issued warning. If $event_{d1}$ happens at $t \geq \tau_{RT}$, we know $d_2(t) \notin [-\bar{d}, -\bar{d} + \epsilon]$, which means that the driver must have disobeyed the braking warning at time t. If $event_{o1}$ happens at $t \geq \tau_{RT}$, we cannot detect disobeying braking warning since it is possible that $d_2(t) \in [-\bar{d}, -\bar{d}+\epsilon]$. It should be noted that $event_{o1}$ taking place cannot guarantee that the driver of Car 2 obeys the issued warning.

Based on the disturbance estimation, we construct the finite state machine $\hat{H}$ as in Fig. 9-3. In $\hat{H}$, the boundary between $\hat{ho}^1$ and $\hat{hd}^1$ and the boundary between $\hat{ho}^2$ and $\hat{hd}^2$ need to be modified. $BR_{d2}(\hat{ho}^1, \hat{hd}^1) = -\bar{d} + \epsilon + 2Bound(\tau)$ with τ being the disturbance estimator running time after braking warning is issued. Similarly, we have $BR_{d2}(\hat{ho}^2, \hat{hd}^2) = \bar{d} - \epsilon - 2Bound(\tau)$ with τ being the disturbance estimator running time after accelerating warning is issued.

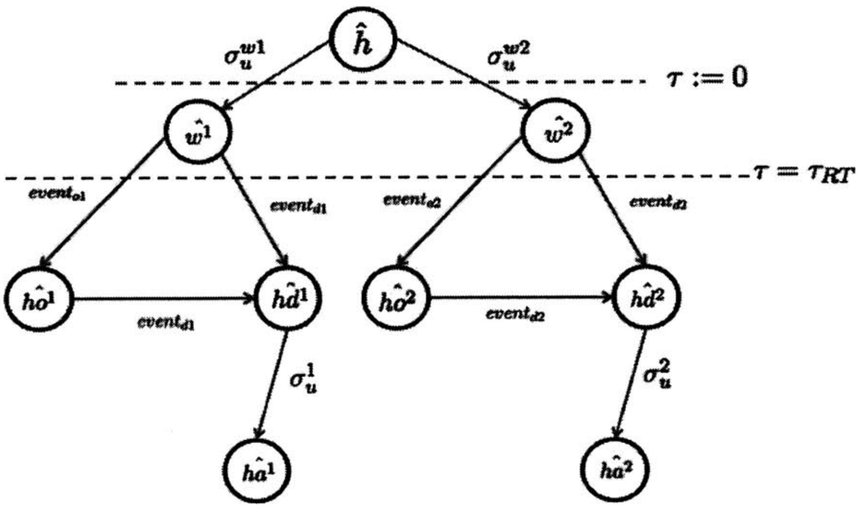

Figure 9-3: System $\hat{H}$

Fig. 9-4 and Fig. 9-5 show $Range_{d2}(\hat{ho}^1)$ and $Range_{d2}(\hat{ho}^2)$ for each time instance t after starting the disturbance estimator. For example, in Fig. 9-5, the region between $\bar{d}$ and the red trajectory is $Range_{d2}(\hat{ho}^2)$ for each time instance.

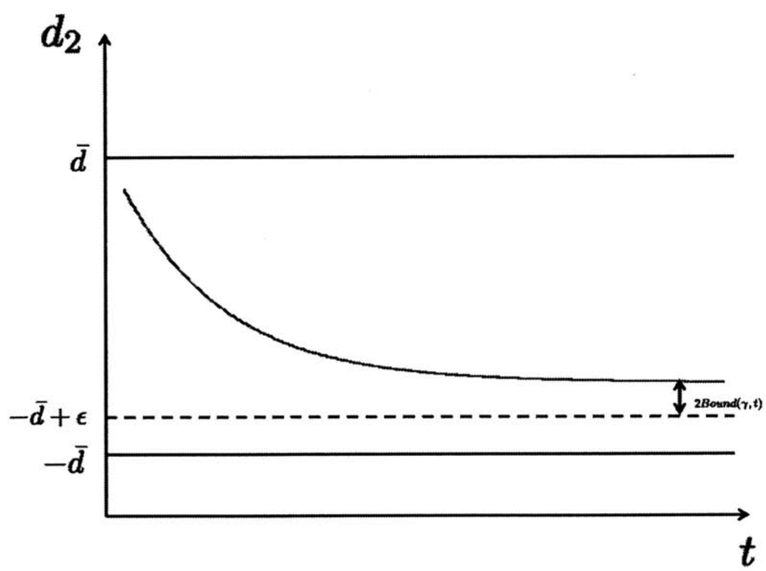

Figure 9-4: $Range_{d2}(\hat{ho}^1)$

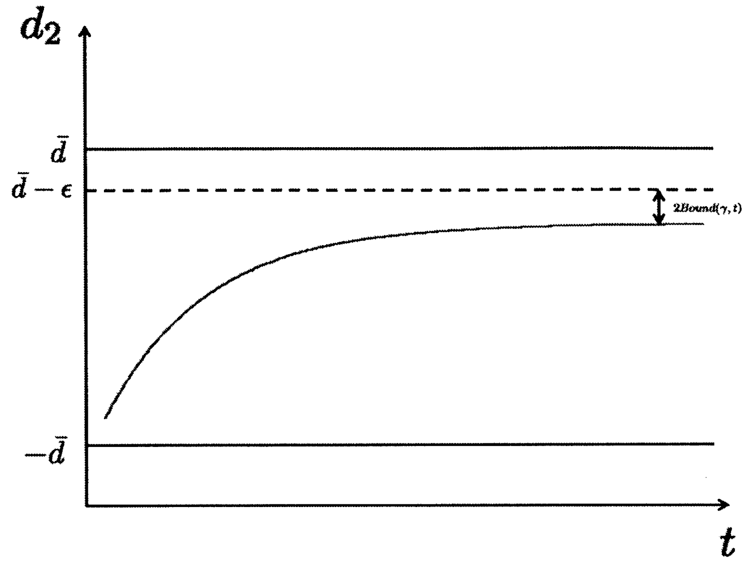

Figure 9-5: $Range_{d2}(\hat{ho}^2)$

In order to calculate the value function V, we need to consider two cases:

- issuing braking warning, which corresponds to calculating $V^{\downarrow}$;
- issuing accelerating warning, which corresponds to calculating $V^{\uparrow}$.

If the braking warning is issued, then the mode of the system may get trapped in the mode $\hat{ho}^1$ without the ability to switch to the overriding mode $\hat{ha}^1$, or it may transit to $\hat{hd}^1$ and the controller can choose whether to stay in $\hat{hd}^1$ or switch to $\hat{ha}^1$ based on which of the two will provide a larger value for the value function. In the second case, when necessary, the controller will issue the signal σ_u^1 to switch to $\hat{ha}^1$ since in ha^1, a_2 can take the value $-\bar{u}$ for each time instance, and that will give a larger value for the value function. In the first case, the worst case disturbance profile compatible with getting trapped in $\hat{ho}^1$ is shown in Fig. 9-6. Since the value of a_2 at each time instance equals to d_2, which is always larger than $-\bar{u}$, the value of the value function for getting trapped in $\hat{ho}^1$ will be smaller than the value of the value function for the second case. The selection between the two cases are done by discrete disturbance signal, which always selects the smaller one. Thus, the disturbance profile for d_2 shown in Fig. 9-6 will be used to decide when to issue the braking warning. For the accelerating warning, the same analysis follows and the disturbance profile for d_2 shown in Fig. 9-7 will be used to decide when to issue the accelerating warning.

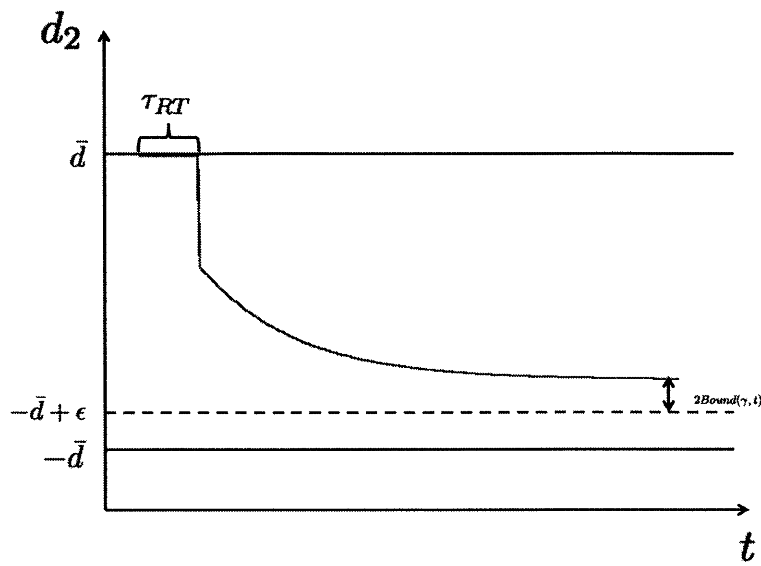

Figure 9-6: Worst case disturbance profile of d_2 for getting trapped in $\hat{ho}^1$

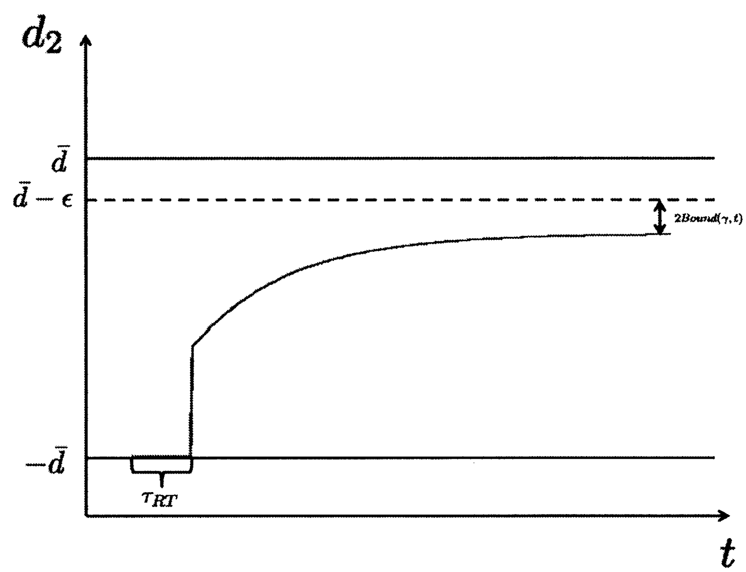

Figure 9-7: Worst case disturbance profile of d_2 for getting trapped in $\hat{ho}^2$

9.3 Simulation Results

We consider the simulation example shown in the following figures.

We have $\bar{u} = 4m/s^2$, $\bar{d} = 1m/s^2$, $L_1 = 22m$, $U_1 = 26m$, $L_2 = 22m$, and $U_2 = 26m$. $v_{min} = 1m/s$ and $v_{max} = 32m/s$ are saturations for the speeds of the two cars. We have

$\tau_{RT} = 0.5s$ and $\epsilon = 0.2m/s^2$. Initially, we have $p_1(0) = 0m$, $p_2(0) = 4m$, $v_1(0) = 3m$ and $v_2(0) = 6m$. $dt = 0.02s$ is the simulation time step.

Next, we will show the simulation results in Fig. 9-8 to 9-15. In the simulation, the accelerating warning case is shown, and after receiving the warning, the driver will disobey the warning. At the end, overriding is needed to guarantee safety. From Fig. 9-8 to 9-15 except Fig. 9-11, there are two plots in each figure.

- The left plot shows $\mathbb{R}^2$ space. The horizontal axis represents p_1. The vertical axis represents p_2. The red rectangle is the *Bad* set. The black circle represents the point $(p_1(t), p_2(t))$ for each $t \geq 0$. From the black circle, either a red trajectory or a blue dashed trajectory is plotted. The red and blue trajectories represent the predicted trajectory if the optimal control and disturbance signals are used. Thus, the distance between the trajectories and the set *Bad* (in this simulation, it is the distance between the trajectories and the point (L_1, U_2)) will represent the value of the value function. If the red or blue trajectory in the plot is above the point (L_1, U_2), no discrete control signal is needed to apply. If the trajectory goes through the point (L_1, U_2), the corresponding discrete control signal should be applied.

- The right plot shows the two perpendicular lanes and the intersection. The blue asterisk represents Car 1 and the black asterisk represents Car 2. For each time instance, we cannot have both of the two asterisks inside the red rectangle, which represents the intersection.

The simulation results are shown below.

(a) Initially, both of the two car will be human driven and the mode of the system will start from mode $\hat{h}$. We calculate the value function $V^{\uparrow}$ using the disturbance profile for d_2 as shown in Fig. 9-7. The corresponding predicted trajectory is shown as the red trajectory in Fig. 9-8. The red trajectory is above the point (L_1, U_2), which means that $V^{\uparrow}$ has a positive value. This guarantees that the overall value function V has a positive value. Thus, no control signal needs to be applied.

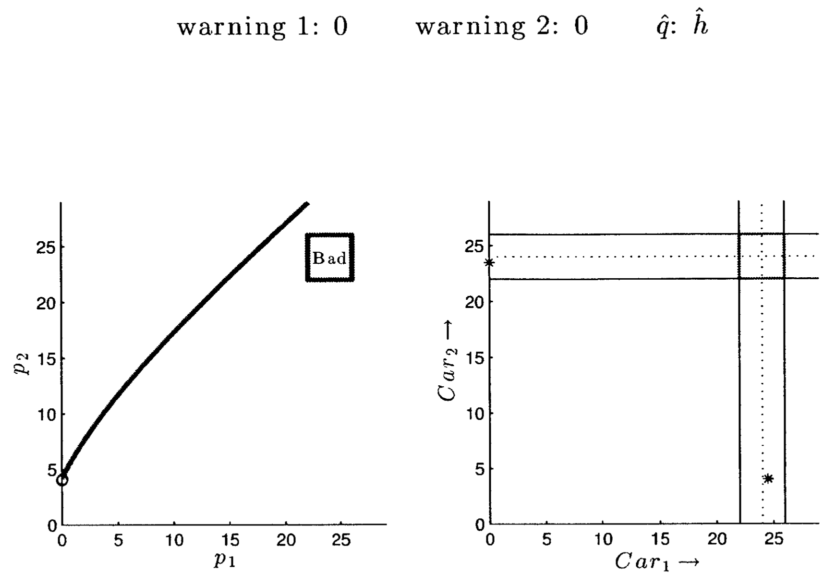

Figure 9-8: Initially, both of the two cars are human driven and the mode of the system is $\hat{h}$.

(b) In Fig. 9-9, the red trajectory goes through the point (L_1, U_2), which means that $V^{\uparrow} = 0$ at this point. At the same time, $V^{\downarrow}$ gives a negative value, which means that braking cannot guarantee safety. Thus, the overall value function has a zero value and the corresponding discrete control signal σ_u^{w2} needs to be applied. The controller gives the driver of the semi-autonomous vehicle accelerating warning. Then the mode of the system will be switched to $\hat{w^2}$.

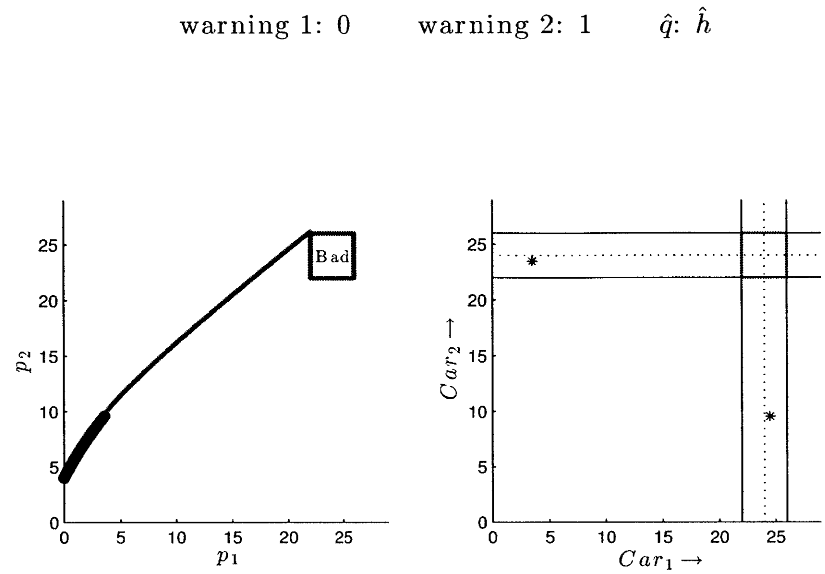

Figure 9-9: When the red trajectory goes through the point (L_1, U_2), the value of the value function is 0, and the control signal σ_u^{w2} should be applied.

(c) Now, the mode of the system has been switched to $\hat{w}^2$, and the system will stay in mode $\hat{w}^2$ for time τ_{RT} so that the driver can react to the warning. The blue trajectory in Fig. 9-10 represents the predicted trajectory associated with the case in which the driver disobeys the issued warning and overriding with the maximum control input is performed by the controller.

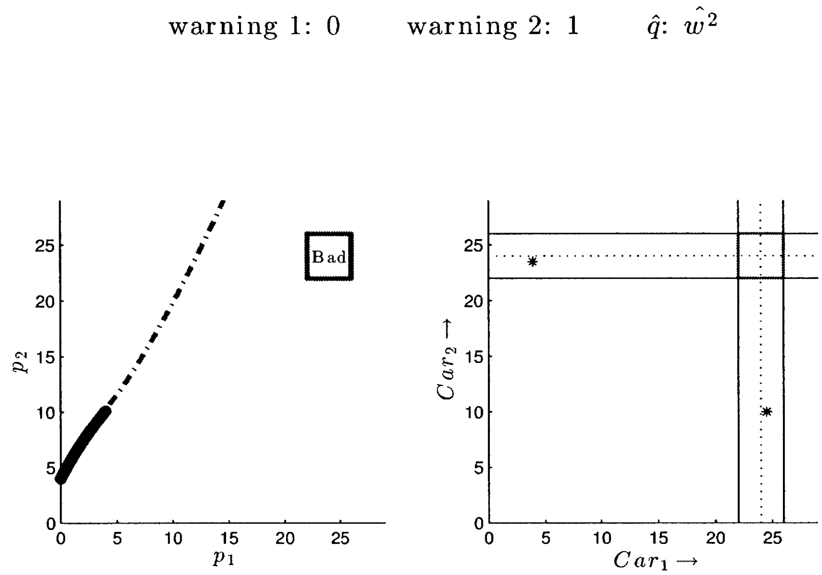

Figure 9-10: The mode of the system has been switched to $\hat{w}^2$. The system will stay in $\hat{w}^2$ for time τ_{RT}.

(d) After the reaction time τ_{RT} has passed, the controller needs to use the result from the disturbance estimator to estimate whether the driver has disobeyed the issued warning or not. In Fig. 9-11, the true disturbance signal d_2 is plotted as the red line. The blue trajectory represents $\hat{d}_2$ and the upper and lower bounds of *dRange* are plotted as the black dashed lines. When the upper bound of *dRange* crosses the line $\bar{d} - \epsilon$, disobeying is detected and the mode of the system will be switched to $\hat{hd}^2$.

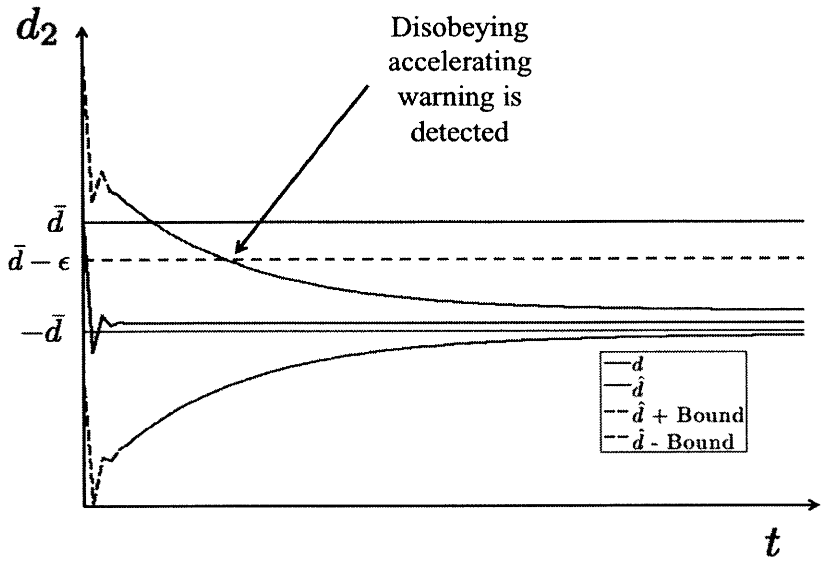

Figure 9-11: Disobeying the accelerating warning is detected.

When the mode of system has been switched to $\hat{hd}^2$, which means that disobeying accelerating warning has been detected, the controller can decide to stay in $\hat{hd}^2$ or transit to $\hat{ha}^2$. At this moment, the optimal trajectory corresponds to switching to mode $\hat{ha}^2$ and applying $\bar{u}$, and it is plotted as the blue trajectory in Fig. 9-12. The blue trajectory is above the point (L_1, U_2), so a positive value function value is guaranteed and no discrete control signal needs to be applied at this moment.

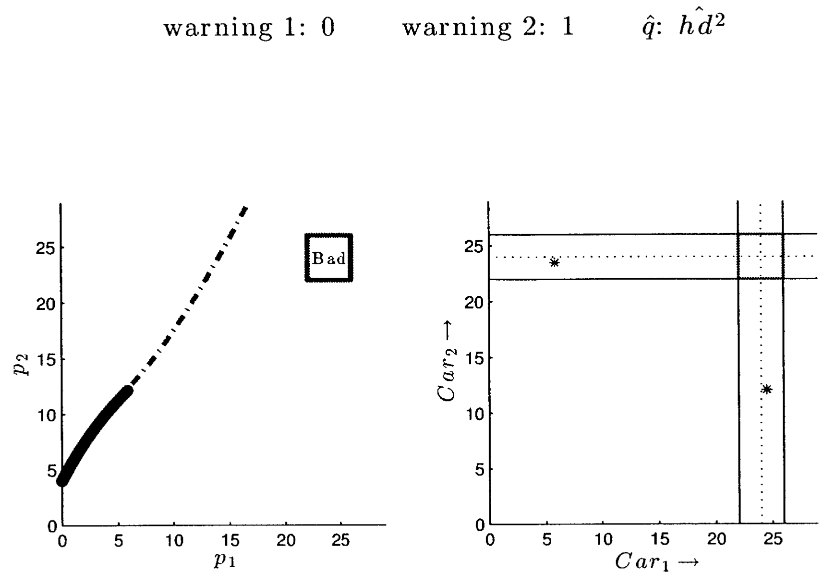

Figure 9-12: After disobeying accelerating warning is detected, the mode of the system will be switched to $h\hat{d}^2$. The blue dashed trajectory is generated using the maximum control for a_2.

(e) When the blue trajectory touches the point (L_1, U_2) as shown in Fig. 9-13, a zero value for the value function is given, and at this moment, σ_u^2 needs to be applied. The mode of the system will be switched to $h\hat{a}^2$ and overriding mode is entered.

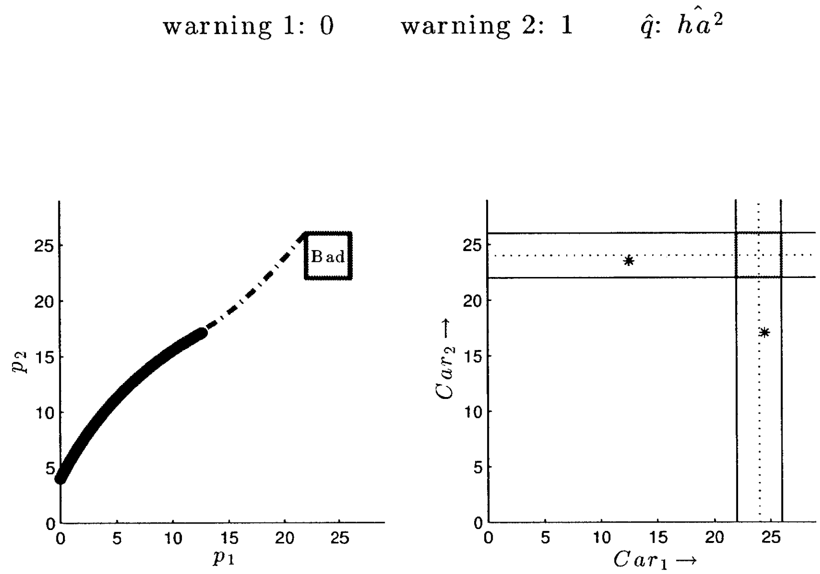

Figure 9-13: When the blue dashed trajectory passes through (L_1, U_2), the control signal σ_u^2 will be applied and the system will transit to the overriding mode.

(f) In the mode $\hat{ha}^2$, the maximum control input $\bar{u}$ will be used. Since the disturbance input d_1 is picked to be $\bar{d}$, which is the worst case disturbance for d_1 in this example, the predicted trajectory will always pass through the point (L_1, U_2) as shown in Fig. 9-14. This will always provide a zero value for the value function.

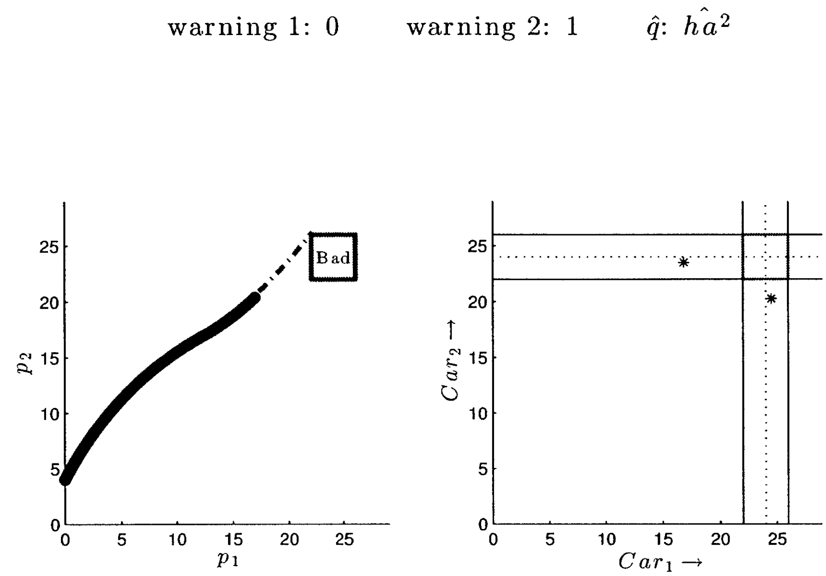

Figure 9-14: In the overriding mode, $\bar{u}$ will be applied to a_2.

(g) Finally, the intersection is passed and no collision occurs.

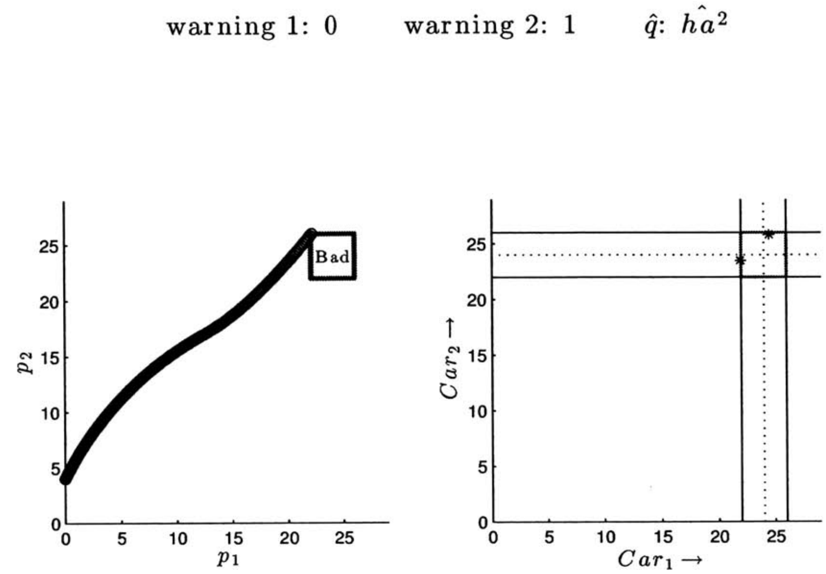

Figure 9-15: Finally, the two cars pass the intersection safely.

Chapter 10

Conclusion and Future Work

In this document, a least conservative safety controller is proposed for the design of hybrid control map for hybrid system with hidden modes and bounded disturbances. The control map is provably safe and least conservative by solving the optimization problem of the value function. Also, the design of the controller takes dwell time into consideration.

The limitation of the algorithm is that the functionality of the algorithm will be highly affected by the complexity of the hybrid system.

- For hybrid system with complex structures, (for example, loops between modes, transitions leaving a mode being driven by both discrete control and disturbance signals, and much more complex structure within a *Connect*), the algorithm may not work.
- The functionality of the algorithm depends on the shape of the set *Bad*. If the set *Bad* is not a rectangle or convex set, the algorithm may not work.
- The estimation of an one-dimensional continuous disturbance signal is used for mode estimation. For extension of the current work, a system affected by more high-dimensional continuous disturbance signals may be needed to consider.

Bibliography

[1] Parosh Aziz Abdulla and K Rustan M Leino. Tools and algorithms for the construction and analysis of systems. *Lecture Notes in Computer Science*, 6605, 2011.

[2] Eugene Asarin, Oded Maler, and Amir Pnueli. Symbolic controller synthesis for discrete and timed systems. In *Hybrid systems II*, pages 1–20. Springer, 1995.

[3] J-P Aubin, John Lygeros, Marc Quincampoix, Shankar Sastry, and Nicolas Seube. Impulse differential inclusions: a viability approach to hybrid systems. *Automatic Control, IEEE Transactions on*, 47(1):2–20, 2002.

[4] BN Campbell, JD Smith, and WG Najm. Analysis of fatal crashes due to signal and stop sign violations. Technical report, 2004.

[5] Martin Corless and Jay Tu. State and input estimation for a class of uncertain systems. *Automatica*, 34(6):757–764, 1998.

[6] Elena De Santis, Maria Domenica Di Benedetto, and Luca Berardi. Computation of maximal safe sets for switching systems. *Automatic Control, IEEE Transactions on*, 49(2):184–195, 2004.

[7] Martin De Wulf, Laurent Doyen, and Jean-François Raskin. A lattice theory for solving games of imperfect information. In *Hybrid Systems: Computation and Control*, pages 153–168. Springer, 2006.

[8] Domitilla Del Vecchio. A partial order approach to discrete dynamic feedback in a class of hybrid systems. In *Hybrid Systems: Computation and Control*, pages 159–173. Springer, 2007.

[9] Domitilla Del Vecchio. Observer-based control of block-triangular discrete time hybrid automata on a partial order. *International Journal of Robust and Nonlinear Control*, 19(14):1581–1602, 2009.

[10] Michel C Delfour and J-P Zolésio. *Shapes and geometries: metrics, analysis, differential calculus, and optimization*, volume 22. Siam, 2011.

[11] R Ervin, J Sayer, D LeBlanc, S Bogard, M Mefford, M Hagan, Z Bareket, and C Winkler. Automotive collision avoidance system field operational test report: methodology and results. Technical report, 2005.

[12] Yan Gao, John Lygeros, and Marc Quincapoix. The reachability problem for uncertain hybrid systems revisited: a viability theory perspective. In *Hybrid systems: computation and control*, pages 242–256. Springer, 2006.

[13] Reza Ghaemi and Domitilla Del Vecchio. Control for safety specifications of systems with imperfect information on a partial order. *IEEE Trans. Automat. Contr.*, 59(4):982–995, 2014.

[14] Michael R Hafner, Drew Cunningham, Lorenzo Caminiti, and Domitilla Del Vecchio. Cooperative collision avoidance at intersections: Algorithms and experiments. *Intelligent Transportation Systems, IEEE Transactions on*, 14(3):1162–1175, 2013.

[15] Michael R Hafner and Domitilla Del Vecchio. Computation of safety control for uncertain piecewise continuous systems on a partial order. In *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*, pages 1671–1677. IEEE, 2009.

[16] Michael R Hafner and Domitilla Del Vecchio. Computational tools for the safety control of a class of piecewise continuous systems with imperfect information on a partial order. *SIAM Journal on Control and Optimization*, 49(6):2463–2493, 2011.

[17] Brett O Hall. Collision avoidance system, April 24 2001. US Patent 6,223,125.

[18] Thomas A Henzinger, Benjamin Horowitz, Rupak Majumdar, and Howard Wong-Toi. Beyond hytech: Hybrid systems analysis using interval numerical methods. In *Hybrid systems: Computation and control*, pages 130–144. Springer, 2000.

[19] Qingfeng Huang, Ronald Miller, Perry McNeille, David Dimeo, and Gruia-Catalin Roman. Development of a peer-to-peer collision warning system. *Ford Techincal Journal*, 5(2), 2002.

[20] AB Kurzhanski and P Varaiya. Ellipsoidal techniques for hybrid dynamics: the reachability problem. In *New Directions and Applications in Control Theory*, pages 193–205. Springer, 2005.

[21] Long Le, Andreas Festag, Roberto Baldessari, and Wenhui Zhang. Vehicular wireless short-range communication for improving intersection safety. *Communications Magazine, IEEE*, 47(11):104–110, 2009.

[22] Neil Lerner, James Jenness, Emanuel Robinson, Timothy Brown, Carryl Baldwin, and Robert Llaneras. Crash warning interface metrics final report. Technical report, 2011.

[23] John Lygeros, Karl Henrik Johansson, Slobodan N Simic, Jun Zhang, and Shankar S Sastry. Dynamical properties of hybrid automata. *Automatic Control, IEEE Transactions on*, 48(1):2–17, 2003.

[24] John Lygeros, Claire Tomlin, and Shankar Sastry. Controllers for reachability specifications for hybrid systems. *Automatica*, 35(3):349–370, 1999.

[25] Michael Maile and Luca Delgrossi. Cooperative intersection collision avoidance system for violations (cicas-v) for avoidance of violation-based intersection crashes. *Enhanced Safety of Vehicles*, 2009.

[26] Ronald Miller and Qingfeng Huang. An adaptive peer-to-peer collision warning system. In *Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th*, volume 1, pages 317–321. IEEE, 2002.

[27] Wassim G Najm, John D Smith, and Mikio Yanagisawa. Pre-crash scenario typology for crash avoidance research. In *DOT HS*. Citeseer, 2007.

[28] Panos Papadimitratos, A La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *Communications Magazine, IEEE*, 47(11):84–95, 2009.

[29] I Phase. Automotive collision avoidance system field operational test.

[30] J Pierowicz, B Pirson, A Bittner, ML Lloyd, and E Jacoy. *Intersection collision avoidance using ITS countermeasures.* 2000.

[31] NOTE TO READER. Development and validation of functional definitions and evaluation procedures for collision warning/avoidance systems. 1999.

[32] Omid Shakernia, George J Pappas, and Shankar Sastry. Semi-de1cidable synthesis for triangular hybrid systems. In *Hybrid Systems: Computation and Control*, pages 487–500. Springer, 2001.

[33] Tatsuya Suzuki. Advanced motion as a hybrid system. *Electronics and Communications in Japan*, 93(12):35–43, 2010.

[34] Louis Tijerina. Issues in the evaluation of driver distraction associated with in-vehicle information and telecommunications systems. *Transportation Research Inc*, 2000.

[35] Louis Tijerina, S Johnston, E Parmer, HA Pham, and MD Winterbottom. Preliminary studies in haptic displays for rear-end collision avoidance system and adaptive cruise control system applications. Technical report, 2000.

[36] Claire J Tomlin, John Lygeros, and S Shankar Sastry. A game theoretic approach to controller design for hybrid systems. *Proceedings of the IEEE*, 88(7):949–970, 2000.

[37] Claire J Tomlin, Ian Mitchell, Alexandre M Bayen, and Meeko Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.

[38] Claire J Tomlin, Ian M Mitchell, Alexandre M Bayen, and Meeko KM Oishi. Computational techniques for the verification and control of hybrid systems. In *Multidisciplinary Methods for Analysis Optimization and Control of Complex Systems*, pages 151–175. Springer, 2005.

[39] Rajeev Verma and Domitilla Del Vecchio. Continuous control of hybrid automata with imperfect mode information assuming separation between state estimation and control. In *Decision and Control, 2009 held jointly with the 2009 28th Chinese Control Conference. CDC/CCC 2009. Proceedings of the 48th IEEE Conference on*, pages 3175–3181. IEEE, 2009.

[40] Rajeev Verma and Domitilla Del Vecchio. Control of hybrid automata with hidden modes: Translation to a perfect state information problem. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5768–5774. IEEE, 2010.

[41] Rajeev Verma and Domitilla Del Vecchio. Control of hidden mode hybrid systems: Algorithm termination. In *Intelligent Transportation Systems (ITSC), 2011 14th International IEEE Conference on*, pages 1174–1180. IEEE, 2011.

[42] Rajeev Verma and Domitilla Del Vecchio. Development and experimental validation of a semi-autonomous cooperative active safety system. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pages 4849–4854. IEEE, 2011.

[43] Rajeev Verma and Domitilla Del Vecchio. Semiautonomous multivehicle safety. *Robotics & Automation Magazine, IEEE*, 18(3):44–54, 2011.

[44] Rajeev Verma and Domitilla Del Vecchio. Safety control of hidden mode hybrid systems. *Automatic Control, IEEE Transactions on*, 57(1):62–77, 2012.

[45] Mark Vollrath and Ingo Totzke. In-vehicle communication and driving: An attempt to overcome their interference. In *Driver Distraction Internet Forum sponsored by the United States Department of Transportation*, 2000.

[46] EATON VORAD. The benefit of collision warning systems for commercial vehicles. In *Presentation at ITS America 2001 Annual Meeting*, 2001.

[47] Zhengrong Yang, Takashi Kobayashi, and Tsuyoshi Katayama. Development of an intersection collision warning system using dgps. Technical report, SAE Technical Paper, 2000.