Estimation for decentralized safety control under communication delay and measurement uncertainty

Delphine Bresch-Pietri, Domitilla del Vecchio

Estimation for decentralized safety control under communication delay and measurement uncertainty

Delphine Bresch-Pietri [a] and Domitilla Del Vecchio [b]

[a] *CNRS, GIPSA-lab, Department of Automatic Control, 11 rue des Mathématiques, 38000 Grenoble, FRANCE*
e-mail: delphine.bresch-pietri@gipsa-lab.fr

[b] *Department of Mechanical Engineering, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge MA 02139, USA*
e-mail: ddv@mit.edu

Abstract

This paper addresses the design of a decentralized safety controller for two agents, subject to communication delay and imperfect measurements. The control objective is to ensure safety, meaning that the state of the two-agent system does not enter an undesired set in the state space. Assuming that we know a feedback map designed for the delay free-case, we propose a state estimation strategy which guarantees control agreement between the two agents. We present an estimation technique for bounded communication delays, assuming that the agents share the same internal clock, and extend it for infinitely-distributed communication delays by determining a lower bound for the probability of safety. We also explain how the proposed approach can be extended to a general system of N agents and discuss efficient computation of our estimation strategy. Performance of the controller and relevance of the proposed approach are discussed in light of simulations performed for a collision avoidance problem between two semi-autonomous vehicles at an intersection.

Key words: Multi-agent systems, Communication delay, Estimation/prediction approaches, Safety control.

1 Introduction

The concept of partially or fully automated agents has become central in various engineering areas, most notably in automated warehouses and logistics [14,43], and transportation systems (e.g., air traffic [19,22,33,39] or ground transportation [16,25,29,32,35]). In these applications, where (partially) automated agents cohabit with humans and with other similar agents, safety, that is, preventing collisions, has emerged as a major concern [7,10,21,24,27]. To achieve their goal, agents usually share information through dedicated networks [9,11,31] and determine relevant control actions in a decentralized manner based on the information at their disposal. Such information can be impacted by communication delays and, as a consequence, the agents may compute their control actions on the basis of possibly inconsistent information.

Numerous works have investigated the stability analysis of cooperative algorithms (consensus, rendezvous, flocking, synchronization, see [28] and [30] for recent reviews on the topic) in the face of communication or feedback delays. However, safety control, wherein a least conservative controller is designed to keep the state outside of an unsafe set, has scarcely been considered in this context. These controllers commonly aim at computing the maximal safe controlled invariant set or, equivalently, the complementary capture set [26,38,39,36]. Numerous solutions for special classes of systems or suitable conservative over-approximations have also been proposed as computationally appealing alternatives [3,23,37,42]. In particular, computationally efficient algorithms have been proposed for systems with two or more agents by leveraging the order preserving dynamics [1,5,8,13,16,18,40], which is important for transportation applications.

The objective of this paper is to determine a state estimation technique allowing one to use feedback maps designed for the delay-free case, preventing communication delay from compromising safety. The contribution of this work is to make the above approaches based on the computation of the maximal safe controlled invariant set, or its complement, applicable when communication delays occur.

The strategy that we advocate is grounded on the introduction of an additional component, a (synchronized) estimated state set obtained from delayed information. Counter-intuitively, to handle the decentralized nature of the control, we do not employ an estimation technique based on the most recent received data such as it is performed, for example, in [15]. On the contrary, we voluntarily over-approximate the estimated set. This guarantees that the agents employ the same information and thus *reach an agreement* on the control strategy to apply, that is, they choose their respective inputs in a way which is consistent with one another. In turn, this guarantees safety.

[1] The material in this paper was partially presented at the 2014 American Control Conference, Portland, OR, USA. This research was supported by NSF-CPS Award number 1239182.

For the sake of clarity, we only consider the case of two agents, and we sketch how the proposed estimation strategy can be extended to N agents. The delay model under consideration is a (potentially infinitely-distributed) white noise. The often observed information reordering (i.e., violation of first-in/first-out principle for communication channels) is represented by this system description. Other real-time effects such as dropout [12] or quantization [6] are not taken into account here. We prove that safety is guaranteed by the proposed synchronized estimation technique. Tuning of the parameters of the proposed estimator and its impact on safety control are also discussed. It appears that a tradeoff has to be reached between safety and closed-loop performance. For illustration, an application example is proposed in which two vehicles negotiate an intersection to avoid collision.

The paper is organized as follows. After defining some mathematical notations in Section 2, we start by presenting the problem under consideration in Section 3. Then, in Section 4, we design safety control for the case of a bounded communication delay before extending the proposed technique to the case of infinitely-distributed delays in Section 5. We provide an evaluation of the corresponding closed-loop performance in Section 6. Finally, we discuss extension to N agents and related computational aspects in Section 7 in view of implementation in Section 8.

2 Notation

In the following, m and p are positive integers. We denote with a superscript i the variables relative to agent i for $i \in \{1,2\}$, with a superscript L (resp. R) the variables relative to the local agent (resp. the remote one) and with a subscript the coordinate.

$|.|$ denotes the Euclidean norm whereas $\|\cdot\|_\infty$ is used for the infinity norm of a signal. The diameter of a set S is written as $D(S) = \sup_{(s_1,s_2)\in S\times S} |s_1 - s_2|$. The distance between a point x and a non-empty set S is written as $d(x,S) = \inf_{s\in S} |s - x|$ and the distance between two non-empty set S_1 and S_2 as $d(S_1,S_2) = \max\left\{\sup_{s_1\in S_1} \inf_{s_2\in S_2} |s_1 - s_2|, \sup_{s_2\in S_2} \inf_{s_1\in S_1} |s_1 - s_2|\right\}$. The boundary of a set S is written as ∂S and its closure as $\overline{S}$.

$\mathscr{C}^0_{pw}(S_1,S_2)$ represents the set of piecewise continuous functions defined on the set S_1 and taking values in S_2. For two vectors x and $\tilde{x}$ in $\mathbb{R}^p$, we will write $x \leq \tilde{x}$ if $x_i \leq \tilde{x}_i$ for all $1 \leq i \leq p$. For $S_1 \subset \mathbb{R}^p$, $S_2 \subset \mathbb{R}^p$ and $(\xi,\tilde{\xi}) \in \mathscr{C}^0_{pw}(S_1,S_2)^2$, we will write $\xi \leq \tilde{\xi}$ if $\xi(s) \leq \tilde{\xi}(s)$, for all $s \in S_1$. For two vectors x and $\tilde{x}$ in $\mathbb{R}^p$, such that $x \leq \tilde{x}$, we write $[x,\tilde{x}] = [x_1,\tilde{x}_1] \times [x_1,\tilde{x}_2] \times \ldots \times [x_p,\tilde{x}_p]$ and $\mathscr{I}(\mathbb{R}^p) = \left\{[x,\tilde{x}] \mid (x,\tilde{x}) \in (\mathbb{R}^p)^2\right\}$.

$\varphi(t,t_0,x_0,u) \in \mathbb{R}^p$ is the flow associated with a given dynamics at time $t \geq t_0$ corresponding to the initial condition $x_0 \in \mathbb{R}^p$ at time $t_0 \geq 0$ driven by the input signal $u \in \mathscr{C}^0_{pw}([t_0,\infty),\mathbb{R}^m)$. For a set $S \subset \mathbb{R}^p$, we write $\varphi(t,t_0,S,u) = \cup_{x_0\in S}\varphi(t,t_0,x_0,u)$. When possible, we will simply let $\varphi(t,S,u) = \varphi(t,0,S,u)$. For $x : \mathbb{R}_+ \to \mathbb{R}^p$ and $0 \leq t_1 \leq t_2$, we write $x|_{[t_1,t_2]} : s \in [t_1,t_2] \mapsto x(s)$. When necessary, we write $\varphi(t,S,u|_{[\bar{t},\bar{t}+t)})$ the flow at time $t \geq 0$ driven by a portion of the input signal $u \in \mathscr{C}_{pw}([0,\infty),\mathbb{R}^m)$, with $\bar{t} \geq 0$. A scalar continuous function $\alpha : \mathbb{R}_+ \to \mathbb{R}_+$ is said to be of class $\mathscr{K}$ if $\alpha(0) = 0$ and α is strictly increasing. A scalar continuous function $\gamma : \mathbb{R}_+ \to \mathbb{R}_+$ is said to be of class $\mathscr{K}_\infty$ if it is of class $\mathscr{K}$ and if $\alpha(t) \to \infty$ as $t \to \infty$.

In the sequel, a white noise refers to a stochastic signal with a constant power spectral density for any frequency included in its (potentially infinite) spectrum. We write $\mathbb{E}(X)$ for the expected value of a random variable X.

Finally, for $(x,y) \in \mathbb{R} \times (\mathbb{R}\setminus\{0\})$, we write $x \equiv 0 \mod y$ if there exists $n \in \mathbb{N}$ such that $x = ny$ and $\lfloor x \rfloor = m$ with $m \in \mathbb{N}$ such that $m \leq x < (m+1)$.

3 Problem statement

3.1 Agent dynamics

We consider that each agent is governed by the same dynamics subject to additive measurement errors[2], namely, for $i \in \{1,2\}$,

$$\dot{x}^i(t) = f^i(x^i(t),u^i(t)), \tag{1}$$
$$y^i(t) = x^i(t) + \sigma^i(t), \tag{2}$$

with $(x^i,y^i) \in \mathbb{R}^n \times \mathbb{R}^n$, $u^i \in [u_m,u_M] \subset \mathbb{R}^m$ and $\sigma^i \in [\sigma^i_m,\sigma^i_M] \subset \mathbb{R}^n$. Further, in the sequel, we consider the measurement map $h^i : y^i \in \mathbb{R}^n \mapsto [y^i - \sigma^i_M, y^i - \sigma^i_m]$ which is bounded set-valued and such that, for any output $y^i(t)$, $x^i(t) \in h^i(y^i(t))$. In other words, for any measurement y^i, each agent has access to a bounded set-valued function that returns the set of all states consistent with the current output. Finally, it is assumed that the vector field f^i satisfies the following property.

Assumption 1 For any initial condition $x_0 \in \mathbb{R}^n$ and any input $u \in \mathscr{C}_{pw}(\mathbb{R}_+,[u_m,u_M])$, the solution of (1) is global and unique.

Note that this assumption also applies to the extended dynamics

$$\dot{x}(t) = \left(f^1(x^1,u^1(t)), f^2(x^2,u^2(t))\right), \tag{3}$$
$$y = x + \sigma, \tag{4}$$

in which $x = (x^1,x^2)$ $y = (y^1,y^2)$ and $\sigma = (\sigma^1,\sigma^2)$. In the sequel, we write $u = (u^1,u^2)$, $h(y) = (h^1(y^1),h^2(y^2))$ and φ the flow associated with (3), which is well-defined according to Assumption 1.

[2] Note that other output maps could be considered, such as multiplicative bounded uncertainties for example. Provided that a corresponding bounded set-valued measurement map h^i exists, the proposed estimation strategy will hold.

3.2 Delay-free control design

Given an open set $\mathscr{B} \subset \mathbb{R}^{2n}$, define the capture set

$$\mathscr{C} = \big\{ S \subset \mathbb{R}^{2n} \mid \forall u \in \mathscr{C}_{pw}(\mathbb{R}_+, [u_m, u_M]^2)\ \exists\, t \geq 0 \quad \varphi(t,S,u) \cap \mathscr{B} \neq \emptyset \big\}\,.$$

Besides, define the operator

$$\Phi : \mathbb{R}_+ \times 2^{\mathbb{R}^{2n}} \times 2^{\mathscr{C}_{pw}(\mathbb{R}_+,[u_m,u_M]^2)} \to 2^{\mathbb{R}^{2n}} \qquad (t,S,U) \mapsto \cup_{u\in U}\, \varphi(t,S,u)\,. \quad (5)$$

Assumption 2 There exists a decreasing and Cartesian product-valued feedback law $\pi : 2^{\mathbb{R}^{2n}} \to 2^{[u_m,u_M]} \times 2^{[u_m,u_M]}$ such that, for all $S \subset \mathbb{R}^{2n}$ and $\tilde{u} \in 2^{\mathscr{C}_{pw}(\mathbb{R}_+,[u_m,u_M]^2)}$ such that $S \notin \mathscr{C}$ and $\tilde{u}(t) \subseteq \pi(\Phi(t,S,\tilde{u}|_{[0,t)}))$ for $t \geq 0$, then $\Phi(t,S,\tilde{u}|_{[0,t)}) \notin \mathscr{C}$, $t \geq 0$.

The map π is decreasing, i.e.,: for two sets S_1 and S_2 in $\mathbb{R}^{2n}$ such that $S_1 \subseteq S_2$, one has $\pi(S_1) \supseteq \pi(S_2)$. Qualitatively, this property indicates that any input keeping a set outside of the capture set should also keep any subset of it outside of the capture set.

Remark 1 This assumption is a direct extension to the generalized flow Φ of the following standard feedback definition: there exists a decreasing and Cartesian product-valued feedback law $\pi : S \subset \mathbb{R}^{2n} \mapsto 2^{[u_m,u_M]} \times 2^{[u_m,u_M]}$ such that, provided that $S \notin \mathscr{C}$ and that $u(t) \in \pi(\varphi(t,S,u|_{[0,t)}))$ for $t \geq 0$, then $\varphi(t,S,u|_{[0,t)}) \notin \mathscr{C}$, $t \geq 0$.

In general, it is possible to define π as a set-valued function, encompassing several feedback strategy alternatives. Yet, to facilitate agreement, we voluntarily consider it as Cartesian product-valued, i.e., with values in $2^{[u_m,u_M]} \times 2^{[u_m,u_M]}$. This point is crucial: it guarantees that the specific control action that one agent picks in its allowed set does not restrict the choice of the other agent. Hence, if both agents evaluate the feedback map with the same set at all times, they can individually pick their actions in their respective allowed set and still reach an agreement, without need to exchange additional information. Thanks to this property, in the sequel, we refer without ambiguity to the i^{th} ($i \in \{1,2\}$) component of the Cartesian product $\pi(S)$ as $\pi_i(S) \subseteq [u_m,u_M]$.

3.3 Agents communication and delays

From now on, we focus on one of the agents, referred to as "local agent". We introduce notations to outline the information that the local agent receives from the other (remote) agent and computations that it performs based on both this information and locally available data. To this end, we will use a superscript L (resp. R) for quantities computed by the local (resp. remote) agent with $(L,R) \in \{(1,2),(2,1)\}$. In the sequel, we use $\tilde{z}^L(t)$ to denote the information sent by the local agent and $Z^L(t)$ the set of information received by it at time t (Fig. 1). Similarly, we use $\tilde{z}^R(t)$ and $Z^R(t)$ for the quantities relative to the remote agent.

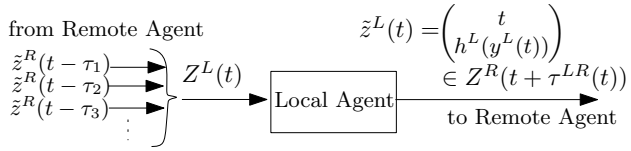


Fig. 1. Schematic view of the exchanged data defined in (6) from the point of view of the local agent L. The indicated delay values (τ_1, τ_2 and τ_3) are realizations of the white noise process τ^{RL}.

We assume that both agents share the same universal time t, obtained from GPS measurements for example [3], and use it to stamp exchanged data. Further, we consider that communication delays occur between the two agents, with independent but symmetric communication channels, i.e., the delays share the same model. Namely, we have

$$\tilde{z}^L(t) = \big(t, h^L(y^L(t))\big) \in Z^R(t + \tau^{LR}(t))\,, \quad (6)$$

in which $\tau^{LR} \geq 0$ is a continuous-time white noise process, which can be infinitely-distributed, and $\tau^{LR}(t)$ and $\tau^{RL}(t)$ have the same (time-invariant) probability density function but are independent. The travelling time from the remote agent R to the local agent L is $\tau^{RL}(t)$ (τ^{LR} represents the converse one). Referring to Fig. 1, the set $Z^L(t)$ may be empty (if no information is received at time t) or contain several elements. The definition (6) of the exchanged information implies that, for each information, the corresponding delay value is known, as the two agents can determine it by comparing the exchanged time stamp and the current time stamp.

3.4 Problem under consideration and proposed approach

The problem at stake here is: given a feedback map that guarantees safety in a context without communication delay as specified by Assumption 2, design a state estimation strategy allowing one to use that same feedback map to guarantee safety in the presence of communication delay and measurement uncertainties. We formulate this problem mathematically in the following statement.

Problem 1 *Given systems* (3)–(4) *subject to communication delay* (6)*, a bad set $\mathscr{B} \subset \mathbb{R}^{2n}$, and a feedback map satisfying Assumption 2, determine a state estimation procedure $t \in \mathbb{R}_+ \mapsto (\hat{x}^1(t), \hat{x}^2(t)) \subset \mathbb{R}^{2n} \times \mathbb{R}^{2n}$ and an initialization set $X_0 \subset \mathbb{R}^{2n}$ such that, with $U^1 : t \in \mathbb{R} \mapsto \pi(\hat{x}^1(t))$ and $U^2 : t \in \mathbb{R} \mapsto \pi(\hat{x}^2(t))$, if $x(0) \in X_0$, $u^1(t) \in U^1_1(t)$ and $u^2(t) \in U^2_2(t)$ for $t \geq 0$, then the solution of* (3) *satisfies $x(t) = \varphi(t, x(0), (u^1, u^2)) \notin \mathscr{B}$ for $t \geq 0$.*

Measurement uncertainty can be taken into account by a prediction/correction approach. To handle communication delay, as the current delay value is known, a natural idea that arises could be to estimate the current remote agent state by propagating the dynamics over a time interval of length equal to the current delay starting from a delayed measurement. However, as the remote agent inputs are unknown, the local agent can only obtain an interval of estimation of the remote

[3] We consider that the two agents are close enough so we can neglect the difference between the two received GPS signals [34].

agent state, while the remote agent knows its own state. Consequently, the two agents will evaluate the feedback map π defined in Assumption 2 on different sets[4] $\hat{x}^1(t)$ and $\hat{x}^2(t)$. Therefore, this strategy can cause the resulting applied control (u^1,u^2) to fail to guarantee safety.

In the sequel, we propose an estimation strategy guaranteeing that the two agents are using the same set to evaluate the feedback map, that is, $\hat{x}^1(t)=\hat{x}^2(t)$, which, in turn, guarantees safety.

4 Solution to Problem 1 for bounded delay: agreement procedure

In this section, in a first move, we assume that communication delays are bounded, i.e., $(\tau^{LR}(t),\tau^{RL}(t))\in[0,\tau_M]^2$ for all $t\geq 0$ with $\tau_M>0$ *known*.

4.1 Synchronization of delayed measurement

Introduce the delayed measurement set corresponding to a measurement $z\in Z^L(t)$ received by the local agent at time $t\geq 0$ as

$$\hat{h}^L_d(z)=\begin{cases}\begin{pmatrix}h^L(y^L(z_1))\\ z_2\end{pmatrix} & \text{if } L=1\\ \begin{pmatrix}z_2\\ h^L(y^L(z_1))\end{pmatrix} & \text{if } L=2\,,\end{cases} \tag{7}$$

in which $z=\tilde{z}^R(t-\tau_0)$ for a given $\tau_0\in[0,\tau_M]$, according to (6). Therefore, following (6), $z_1=t-\tau_0$ and $z_2=h^R(y^R(t-\tau_0))$. Specifically, the local agent has access to delayed possible states of the remote agent from the second coordinate of the measurement z_2. Employing the measurement time stamp $z_1=t-\tau_0$, it can use its own possible states $h^L(y^L(z_1))=h^L(y^L(t-\tau_0))$ to compute $\hat{h}^L_d(z)=h(y(t-\tau_0))$. Hence, the set $\hat{h}^L_d$, computed by agent L from locally available information, corresponds to the whole system state at time $t-\tau_0$.

Further, consider $\tau^*\geq 0$ and the corresponding delayed measurement set at time $t\geq 0$ as

$$\hat{h}^L_{d,syn}(t,\tau^*)=\left\{\hat{h}^L_d(z)\,|\,t-z_1=\tau^*\,,\ z\in Z^L(s)\text{ and }s\leq t\right\}, \tag{8}$$

which we call the synchronized delayed measurement set. It represents what the local agent thinks the whole system's state was at time $t-\tau^*$, based on measurements.

Lemma 1 *For $\tau^*=\tau_M$, the synchronized delayed measurement set* (8) *is such that $\hat{h}^L_{d,syn}(t,\tau_M)\neq\emptyset$ for $t\geq\tau_M$. Further, $\hat{h}^L_{d,syn}(t,\tau_M)=\hat{h}^R_{d,syn}(t,\tau_M)=h(y(t-\tau_M))$ for $t\geq\tau_M$.*

[4] Further, as the values of the two delays are different a priori, one agent cannot know what information the other agent has received and uses as a starting point for propagation in the estimation. This may cause the estimated set used by the remote agent to be unknown to the local agent.

Proof: First, following (8), one can observe that showing that $\hat{h}^L_{d,syn}(t,\tau_M)\neq\emptyset$ for $t\geq\tau_M$ is equivalent to show that, for $t\geq\tau_M$, there exists $s\in[t-\tau_M,t]$ such that $z\in Z^L(s)$ and $t-z_1=\tau_M$. Consider $\tilde{z}^R(t-\tau_M)$, the information sent by the remote agent at $t-\tau_M$. Following the delay definition (6), $\tilde{z}^R(t-\tau_M)\in Z^L(t_0)$ with $t_0=t-\tau_M+\tau^{RL}(t-\tau_M)\in[t-\tau_M,t]$. Therefore, there exists $z\in Z^L(t_0)$ such that $z=\tilde{z}^R(t-\tau_M)$ and, since $\tilde{z}^R_1(t-\tau_M)=t-\tau_M$ from (6), $z_1=t-\tau_M$ or equivalently $t-z_1=\tau_M$. Consequently, $\hat{h}^L_{d,syn}(t,\tau_M)\neq\emptyset$ for $t\geq\tau_M$.

Second, from (8), $\hat{h}^L_{d,syn}(t,\tau_M)=\hat{h}^L_d(z)$ with $z_1=t-\tau_M$. Thus, using (7) and as $z_2=h^R(y^R(z_1))$ from (6), one obtains

$$\hat{h}^L_{d,syn}(t,\tau_M)=\begin{pmatrix}h^1(y^1(t-\tau_M))\\ h^2(y^2(t-\tau_M))\end{pmatrix}=h(y(t-\tau_M))\,.$$

This concludes the proof. □

This lemma states that, when the delay is bounded by a known value τ_M, by picking $\tau^*=\tau_M$, the synchronized delayed measurement set is the same for both agents, and equal to the whole system's state at time $t-\tau_M$. Further, it also guarantees that it is well-defined: indeed, the information sent at time $t-\tau_M$ has been received at time t due to the fact that communication delay is upper-bounded by τ_M.

4.2 Solution to Problem 1

Our approach is grounded on the synchronization technique provided in Lemma 1, coupled with a prediction/correction approach and with the propagation of this corrected delayed estimation set with the same input sets for both agents. This is the subject of the following theorem, in which this procedure gives rise to the definition of the sets $\hat{x}^L_d(t)$, which we call the corrected delayed estimation set, and $\hat{x}^L(t)$, which we call the current estimation set. The corrected delayed estimation set contains $x(t-\tau_M)$, while the current estimation set $\hat{x}^L(t)$ contains the current system state $x(t)$.

Theorem 1 *Consider the plant* (1) *satisfying Assumption 1, a feedback law π satisfying Assumption 2, the synchronized delayed measurement set corresponding to τ_M defined in* (7)–(8) *and the operator Φ defined in* (5)*. Define, for $L\in\{1,2\}$,*

$$\begin{aligned}\hat{x}^L_d(t)=\Big\{&x\in\mathbb{R}^{2n}\mid\exists\,(x_0,w)\in\hat{h}^L_{d,syn}(\tau_M,\tau_M)\times U^L\\ &x=\varphi(t-\tau_M,x_0,w)\text{ and, for }s\in[\tau_M,t],\\ &\varphi(s-\tau_M,x_0,w|_{[0,s-\tau_M)})\in\hat{h}^L_{d,syn}(s,\tau_M)\Big\}\,,\ t\geq\tau_M\end{aligned} \tag{9}$$

$$\hat{x}^L(t)=\Phi(\tau_M,\hat{x}^L_d(t),U^L|_{[t-\tau_M,t)})\,,\ t\geq\tau_M \tag{10}$$

$$U^L(t)=\begin{cases}\pi(\hat{x}^L(t)) & \text{if } t\geq\tau_M\\ [u_m,u_M]^2 & \text{otherwise}\,.\end{cases} \tag{11}$$

Provided that $\Phi(\tau^M,h(x(0)+\sigma)),[u_m,u_M]^2)\notin\mathscr{C}$ and that

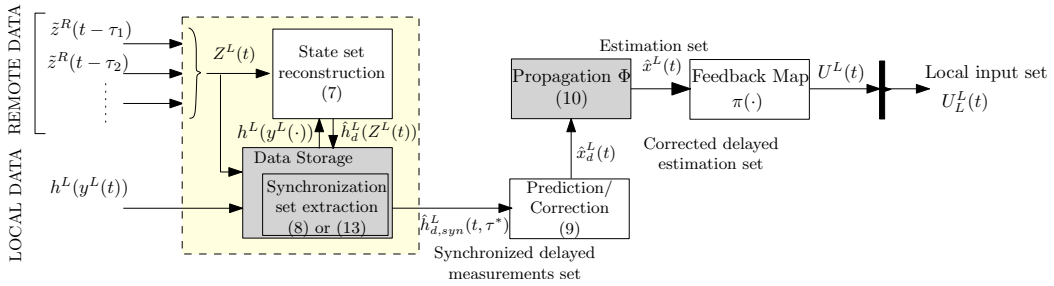


Fig. 2. Schematic view of the estimation strategy proposed in Theorem 1, performed locally by each agent (view of the local agent L here). The state set reconstruction block corresponding to (7) takes the measurement set $Z^L(t)$ and corresponding local measurement $h^L(y^L(\cdot))$ as inputs to compute $\hat{h}^L_d(Z^L(t))$. The data storage block takes as inputs that set of delayed measurement sets along with the current local measurement, to store past values of those data (over a finite horizon). It also extracts from those stored data the synchronized delayed measurement set corresponding to (8). To perform those operations, these two blocks exchange $\hat{h}^L_d(Z^L(t))$ and a (bounded) history of local measurements, which is simply denoted $\hat{h}^L(y^L(\cdot))$. In this diagram, we highlighted by the dashed box local computation on variables that may differ between the two agents. The indicated delay values (τ_1 and τ_2) are realizations of the white noise process τ^{RL}.

$u^L(t) \in U^L_L(t)$ *for* $t \geq 0$ *and* $L \in \{1,2\}$*, then, for* $L \in \{1,2\}$*,*

$$x(t) \in \hat{x}^L(t)\,,\ \hat{x}^L(t) \notin \mathscr{C} \text{ and } x(t) \notin \mathscr{B},\ t \geq 0\,.$$

The proposed controller architecture is represented schematically in Fig. 2. The local agent computes U^L, which is the set of control pairs agent L thinks should be applied by itself and the remote agent to guarantee safety. It then picks its own control input U^L_L in the L^{th} ($L \in \{1,2\}$) component.

The corrected estimation set (9) is the set of all possible states at time $t-\tau_M$ compatible with $\hat{h}^L_{d,syn}(t,\tau_M) = h(y(t-\tau_M))$ and with the flow. Hence, to estimate the current state, one simply has to propagate forward this corrected set with all allowed inputs (as the inputs applied by the remote agent on the interval $[t-\tau_M, t]$ are not known by the local one). This is the meaning of (10), which we use to compute the feedback map. As shown below, one can conclude that, because the synchronized delayed measurement set can be computed by both agents, as stated in Lemma 1, the same holds for the estimation set.

In order to further understand this design, note that one may want to sharpen the state estimation by employing the most recent received measurement in lieu of $\hat{h}^L_{d,syn}(t,\tau_M)$ in the definition (9) of $\hat{x}^L_d$. However, with such a technique, one cannot guarantee that the two agents employ the same information to compute the feedback map, as the most recent measurement has no reason to be the same for both. Alternatively, one might also not be interested in narrowing the state estimation and want to propagate directly the synchronized delayed measurement set without resorting to the corrected delayed estimation set (9). However, depending on the measurement errors model, it may not be possible to guarantee then that the estimation set remains outside of the capture set as sudden jumps can occur in the measurement errors. Conversely, the corrected state set (9) is a key element to guarantee this invariance property by relying on the dynamics and their continuity.

As a final remark, note that this results only holds under the condition $\hat{x}^L(\tau_M) \notin \mathscr{C}$ restricting the set of initial conditions. Indirectly, for a given initial condition, this puts constraints on the time the controller is turned on depending on measurement uncertainties and the value of τ_M as, from (7)–(11), $\hat{x}^L(\tau_M) = \Phi(\tau_M, y(0), [u_m, u_M]^2)$.

Proof of Theorem 1. Using Lemma 1, we start by highlighting the fact that, as $\hat{h}^L_{d,syn}(t,\tau_M) = \hat{h}^R_{d,syn}(t,\tau_M) = h(y(t-\tau_M)) \triangleq \hat{h}_{d,syn}(t,\tau_M)$ for $t \geq \tau_M$, then $\hat{x}^L_d(t) = \hat{x}^R_d(t) = \hat{x}_d(t)$, $\hat{x}^L(t) = \hat{x}^L(t) = \hat{x}(t)$ and $U^L(t) = U^R(t) = U(t)$ for $t \geq \tau_M$. Further, because $u^L(t) \in U^L_L(t)$ for $t \geq 0$, $u(t) = (u^1(t), u^2(t)) \in U_1(t) \times U_2(t) = U(t)$ for $t \geq 0$, as π is Cartesian product-valued, according to Assumption 2.

Then, we show that $x(t) \in \hat{x}(t)$ for $t \geq \tau_M$. From (9), using Lemma 1 and the fact that $x(t) \in h(y(t))$ for $t \geq 0$, one obtains that $x(t-\tau_M) = \varphi(t-\tau_M, x(0), u|_{[0,t-\tau_M)}) \in \hat{x}_d(t)$ for $t \geq \tau_M$, as $u(t) \in U(t)$ for $t \geq 0$. Therefore, as $u(t) \in U(t)$ for $t \geq 0$, $x(t) \in \hat{x}(t)$ for $t \geq \tau_M$.

Now, it remains to show that $\hat{x}(t)$ never enters the capture set. By contradiction, consider that this does not hold, namely that there exists $t_1 > 0$ such that $\hat{x}(t_1) \in \mathscr{C}$ and define $t_0 = \sup\{t \in [0,t_1] \mid \hat{x}(t) \notin \mathscr{C}\}$, which exists by definition of the capture set and the fact that, by assumption, $\hat{x}(\tau_M) \notin \mathscr{C}$. By definition of the capture set, t_0 is such that $\hat{x}(t) \notin \mathscr{C}$ for $0 \leq t < t_0$ and $\hat{x}(t) \in \mathscr{C}$ for $t \in (t_0, t_0+\delta)$ for a given $\delta > 0$. Consider $t_2 \in (t_0, t_0 + \min\{\tau_M, \delta\})$ (without loss of generality, in the following, we assume that $t_2 \geq 2\tau_M$) and $x \in \hat{x}_d(t_2)$. From (9), there exist $x_0 \in \hat{x}_d(\tau_M)$ and $w \in U|_{[0,t_2-\tau_M)}$ such that $x = \varphi(t_2-\tau_M, x_0, w)$ and $\varphi(s-\tau_M, x_0, w|_{[0,s-\tau_M)}) \in \hat{h}_{d,syn}(s,\tau_M)$ for $s \in [\tau_M, t_2]$. Consequently, $\varphi(s-\tau_M, x_0, w) \in \hat{h}_{d,syn}(s,\tau_M)$ for $s \in [\tau_M, t_2-\tau_M]$ and $\varphi(t_2-2\tau_M, x_0, w) \in \hat{x}_d(t_2-\tau_M)$ from (9). Then, there exists $\tilde{x}_0 \in \hat{x}_d(t_2-\tau_M)$ such that $x = \varphi(\tau_M, \tilde{x}_0, w|_{[t_2-2\tau_M, t_2-\tau_M)})$. As a result, from (5) and (10),

$$x \in \cup_{\tilde{x}_0 \in \hat{x}_d(t_2-\tau_M), w \in U|_{[t_2-2\tau_M, t_2-\tau_M)}} \varphi(\tau_M, \tilde{x}_0, w)$$
$$= \Phi(\tau_M, \hat{x}_d(t_2-\tau_M), U|_{[t_2-2\tau_M, t_2-\tau_M)}) = \hat{x}(t_2-\tau_M).$$

As x is any element of $\hat{x}_d(t_2)$, it follows that $\hat{x}_d(t_2) \subseteq \hat{x}(t_2-\tau_M)$ and, from (10), $\hat{x}(t_2) = \Phi(\tau_M, \hat{x}_d(t_2), U|_{[t_2-\tau_M, t_2)})$. From similar arguments, one can obtain that $\hat{x}_d(t_2) \subseteq \Phi(\xi, \hat{x}_d(t_2-\xi), U|_{[t_2-\xi-\tau_M, t_2-\tau_M)})$ for $\xi \in [0, \tau_M]$. Employing this last formula for $\xi = \tau_M - s$ with $s \in [0, \tau_M]$ and from (10), one obtains

$$\Phi(s, \hat{x}_d(t_2), U|_{[t_2-\tau_M, t_2-\tau_M+s)})$$

$$\begin{aligned}
&\subseteq \Phi(s, \Phi(\tau_M - s, \hat{x}_d(t_2-\tau_M+s), U|_{[t_2-2\tau_M+s, t_2-\tau_M)}), \\
&\qquad U|_{[t_2-\tau_M, t_2-\tau_M+s)}) \\
&\subseteq \Phi(\tau_M, \hat{x}_d(t_2-\tau_M+s), U|_{[t_2-2\tau_M+s, t_2-\tau_M+s)}) \\
&= \hat{x}(t_2-\tau_M+s). \qquad (12)
\end{aligned}$$

Besides, the feedback law is decreasing, according to Assumption 2. Therefore, from (12), for $0 \leq s \leq \tau_M$, $\pi(\hat{x}(t_2-\tau_M+s) \subseteq \pi(\Phi(s, \hat{x}_d(t_2), U|_{[t_2-\tau_M, t_2-\tau_M+s)}))$ and hence $U(t_2-\tau_M+s) \subseteq \pi(\Phi(s, \hat{x}_d(t_2), U|_{[t_2-\tau_M, t_2-\tau_M+s)}))$ for $0 \leq s \leq \tau_M$. As $\hat{x}_d(t_2) \in \hat{x}(t_2-\tau_M) \notin \mathscr{C}$ because $t_2 - \tau_M < t_0$, then $\Phi(s, \hat{x}_d(t_2), U|_{[t_2-\tau_M, t_2-\tau_M+s)}) \notin \mathscr{C}$ for $s \in [0, \tau_M]$, by Assumption 2. Therefore, in particular, for $s = \tau_M$, $\Phi(\tau_M, \hat{x}_d(t_2), U|_{[t_2-\tau_M, t_2)}) = \hat{x}(t_2) \notin \mathscr{C}$. As $t_2 \in (t_0, t_0+\delta)$, this is in contradiction with the fact that $\hat{x}(t) \in \mathscr{C}$ for $t \in (t_0, t_0+\delta)$. Therefore, $\hat{x}(t) \notin \mathscr{C}$, $t \geq 0$. Consequently, as $x(t) \in \hat{x}(t)$, $x(t) \notin \mathscr{B}$ for $t \geq 0$. □

5 Solution to Problem 1 in the case of an infinitely distributed delay

In this section, we use the elements previously presented to reason about safety in the case of an infinitely distributed delay. In this context, it is not possible to employ a delay upper-bound τ_M to compute a synchronized delayed measurement set, as such a bound does not exist. As a result, the synchronized delayed state defined in (8) for any $\tau^* \geq 0$ may not be well-defined, if the delayed measurement set of the remote agent $h^R(y^R(t-\tau^*))$ has not yet been received. Hence, we modify (8) as follows.

Define $\delta > 0$ and consider that $\Phi(t, \emptyset, U) = \emptyset$ for $t \geq 0$ and $U \in 2^{\mathscr{C}^0_{pw}(\mathbb{R}_+, [u_m, u_M]^2)}$. Introduce the synchronized delayed measurement set for $\tau^* \geq 0$ as $\hat{h}^L_{d,syn}(t, \tau^*) = \emptyset$ for $t \in [0, \tau^*)$ and, for $t \geq \tau^*$, as

$$\hat{h}^L_{d,syn}(t, \tau^*) =$$
$$\begin{cases}
\hat{h}^L_d(z) & \text{if } t-\tau^* \equiv 0 \mod \delta \text{ and if there exist } s \leq t \\
& \text{and } z \in Z^L(s) \text{ s.t. } t - z_1 = \tau^* \\
\Phi(\delta, \hat{h}^L_{d,syn}(t-\delta, \tau^*), U^L|_{[t-\delta-\tau^*, t-\tau^*)}) & \\
\qquad \text{if } t-\tau^* \equiv 0 \mod \delta \text{ and if } t - z_1 \neq \tau^* & \\
\qquad \text{for all } z \in Z^L(s) \text{ and } s \leq t & \\
\Phi\Big(t-\tau^* - \lfloor \frac{t-\tau^*}{\delta} \rfloor \delta, \hat{h}^L_{d,syn}(\lfloor \frac{t-\tau^*}{\delta} \rfloor \delta + \tau^*, \tau^*), & \qquad (13) \\
\qquad U^L|_{[\lfloor \frac{t-\tau^*}{\delta} \rfloor \delta, t-\tau^*)} \Big) \text{ otherwise}, &
\end{cases}$$

in which U^L is a feedback law left undefined for the moment.

This synchronized delayed measurement set $\hat{h}^L_{d,syn}(t, \tau^*)$ is updated every δ units of time (Case 1–2 in (13)) and propagated forward meanwhile (Case 3 in (13)). At an update instant $t = n\delta + \tau^*$, if the delayed remote measurement set $h^R(y^R(n\delta))$ has been received, then Case 1 in (13) is active and $\hat{h}^L_{d,syn}(t, \tau^*) = h(y(n\delta))$, according to the definition of the delayed measurement set corresponding to a measurement (7). Otherwise, one keeps propagating forward the latter synchronized delayed measurement set $\hat{h}^L_{d,syn}((n-1)\delta, \tau^*)$ (Case 2 in (13)). Such a definition is inspired from the discrete-time case, in which the measurements are punctually received each time step and the corresponding information is updated. In order to further understand this definition, we point out that if there exists a delay upper-bound τ_M and if we choose $\tau^* = \tau_M$ and $\delta \to 0$, the synchronized delayed measurement set tends to the same as previously introduced in (8) as only Case 1 in (13) tends to be used. We now employ the new set in the control strategy.

Theorem 2 *Consider the plant* (1) *satisfying Assumption 1, the feedback law* π *defined in Assumption 2, the synchronized delayed measurement set defined through* (7)-(13) *for* $\tau^* \geq 0$ *and* $\delta \geq 0$ *and the operator* Φ *defined in* (5). *For* $L \in \{1, 2\}$, *let*

$$\begin{aligned}
\hat{x}^L_d(t) = \big\{ & x \in \mathbb{R}^{2n} \mid \exists\, (x_0, w) \in \hat{h}^L_{d,syn}(\tau^*, \tau^*) \times U^L \\
& x = \varphi(t-\tau^*, x_0, w) \text{ and, for } s \in [\tau^*, t], \\
& \varphi(s-\tau^*, x_0, w) \in \hat{h}^L_{d,syn}(s, \tau^*) \big\}, \; t \geq \tau^* \qquad (14)
\end{aligned}$$

$$\hat{x}^L(t) = \Phi(\tau^*, \hat{x}^L_d(t), U^L|_{[t-\tau^*, t)}), \; t \geq \tau^* \qquad (15)$$

$$U^L(t) = \begin{cases} \pi(\hat{x}^L(t)) & \text{if } t \geq \tau^* \text{ and } \hat{x}^L(t) \neq \emptyset \\ [u_m, u_M]^2 & \text{otherwise}. \end{cases} \qquad (16)$$

Provided that $\Phi(\tau^*, h(x(0)+\sigma)), [u_m, u_M]^2) \notin \mathscr{C}$, *and that* $u^L(t) \in U^L_L(t)$, *for* $L \in \{1, 2\}$ *and* $t \geq 0$, *then, for* $T \geq \tau^*$,

$$\begin{aligned}
&Pr(x(t) \notin \mathscr{B},\, t \in [0, T]) \geq \\
&\quad p^2(p^2 + (1-p^2)(1-p)^2)^{\lfloor (T-\tau^*)/\delta \rfloor} \triangleq \Pi(\delta, \tau^*), \qquad (17)
\end{aligned}$$

with $p = Pr(\tau^{RL}(t) \leq \tau^*) = Pr(\tau^{LR}(t) \leq \tau^*)$.

One can notice that the control strategy consists of the same elements as previously: prediction/correction approach (14), propagation (15) and evaluation of the feedback map with the estimation set in (16). Only the synchronized delay measurement set $\hat{h}^L_{d,syn}$ has been modified. Note that it is now possible for $\hat{h}^L_{d,syn}$ and $\hat{h}^R_{d,syn}$ to be different. This would in turn imply that the estimation set $\hat{x}^L$ and $\hat{x}^R$ are not equal. Hence, similarly to the case of bounded delay (Theorem 1), a sufficient condition to guarantee safety is that both agents employ the same synchronized delayed measurement set. This is the case if both agents have initially received the corresponding delayed remote measurement set, that is, $h^R(y^R(t-\tau^*))$ and then, at each update time t, either both agents have received the delayed remote measurement set or both have not. The probability of this event is $\Pi(\delta,\tau^*)$, as stated below.

One can note that the bound $\Pi(\delta,\tau^*)$ is increasing with respect to τ^* and with respect to δ. Indeed, the greater the synchronization delay τ^* is, the more probable it is that the first measurement has been received. Similarly, the greater the period of update the less probable it is that one agent employs more information than the other. Also, one can notice that this probability tends to zero while δ tends to zero. Hence, applying directly the estimation design (7)–(11) from the previous section, that is, picking $\delta = 0$, one cannot conclude on safety as $\Pi(\delta,\tau^*) = 0$ ($p < 1$ for any value of τ^* for an infinitely-distributed delay). This justifies our choice of mimicking the discrete-time framework and introducing a period of update $\delta \geq 0$ in (13).

Note that the probability $\Pi(\delta,\tau^*)$ also depends on the length of the considered time interval T and tends to zero as T tends to infinity, except in the case in which $\delta \underset{\infty}{\sim} T$. This is consistent with the fact that, as explained below, it is not possible to guarantee safety for all time while keeping updating the delayed measurement set.

Before providing the proof of the theorem, we give two intermediate lemmas.

Lemma 2 *Assume that* $\Phi(\tau^*, h(y(0)), [u_m, u_M]^2) \notin \mathscr{C}$*, and that, for* $L \in \{1,2\}$ *and* $t \geq 0$*,* $u^L(t) \in U^L_L(t)$*. For* $T \geq \tau^*$*, consider the following statements:*

A0: $x(t) \notin \mathscr{B}$ *for* $t \in [0,T]$*;*
B0: $\hat{x}^L(t) = \hat{x}^R(t) = \hat{x}(t)$ *and* $x(t) \in \hat{x}(t)$*, for* $t \in [\tau^*, T]$*;*
C0: $\hat{h}^L_{d,syn}(t,\tau^*) = \hat{h}^R_{d,syn}(t,\tau^*)$ *for* $t \in [\tau^*, T]$*,* $\hat{x}^L(\tau^*) = \hat{x}^R(\tau^*) = \hat{x}(\tau^*)$ *and* $x(\tau^*) \in \hat{x}(\tau^*)$*;*
D0: $\hat{h}^L_{d,syn}(t,\tau^*) = \hat{h}^R_{d,syn}(t,\tau^*) \neq \emptyset$ *for* $t \in [\tau^*, T]$.

Then, $Pr(A0) \geq Pr(B0) \geq Pr(C0) \geq Pr(D0)$.

Proof: We show that $B0$ implies $A0$, that $C0$ implies $B0$ and, finally, that $D0$ implies $C0$. Then, the conclusion of Lemma 2 follows.

($B0 \Rightarrow A0$) If $B0$ holds, then $U^L(t) = U^R(t) = U(t)$ for $t \geq 0$ and $u(t) = (u^1(t), u^2(t)) \in U_1(t) \times U_2(t) = U(t)$ for $t \geq 0$ as π is Cartesian product-valued. Then, using the same argument by contradiction as the one used in the proof of Theorem 1, one obtains that $\hat{x}(t) \notin \mathscr{C}$ for $t \in [\tau^*, T]$, that is, that $A0$ holds.

($C0 \Rightarrow B0$) Assume that $C0$ holds and consider $L \in \{1,2\}$. As $\hat{h}^L_{d,syn}(t,\tau^*) = \emptyset$ for $t \in [0,\tau^*)$, according to Cases 1–2 in (13), $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = \emptyset$ or $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = h(y(0))$. If $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = \emptyset$, then, following (9) and (15), $\hat{x}^L_d(t) = \emptyset$ and $\hat{x}^L(\tau^*) = \emptyset$ which contradicts $C0$. Therefore, $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = h(y(0))$. Further, from (9) and (15), as $\hat{h}^L_{d,syn}(t,\tau^*) = \hat{h}^R_{d,syn}(t,\tau^*) = \hat{h}_{d,syn}(t,\tau^*)$ for $t > \tau^*$, then $\hat{x}^L_d(t) = \hat{x}^R_d(t) = \hat{x}_d(t)$, $\hat{x}^L(t) = \hat{x}^R(t) = \hat{x}(t)$, $U^L(t) = U^R(t) = U(t)$ and $u(t) \in U(t)$ for $t \in [\tau^*, T]$. We now prove that $x(t) \in \hat{x}(t)$ for $t \in [\tau^*, \min\{\tau^* + n\delta, T\}]$ for $n \in \mathbb{N}$ by induction on n. Without loss of generality, in the following, we assume that $T > \delta$. Therefore, according to Case 3 in (13) and (15), for $t \in [\tau^*, \tau^* + \delta)$, we have

$$\begin{aligned}\hat{x}(t) =& \Phi(\tau^*, \hat{x}_d(t), U|_{[t-\tau^*,t)})\\ =& \Phi(\tau^*, \Phi(t-\tau^*, \hat{x}_d(\tau^*), U|_{[0,t-\tau^*)}), U|_{[t-\tau^*,t)})\\ =& \Phi(t, \hat{x}_d(\tau^*), U|_{[0,t)}) = \Phi(t, h(y(0)), U|_{[0,t)}).\end{aligned}$$

Thus, as $x(0) \in h(y(0))$ and as $u(t) \in U(t)$ for $t \geq 0$, $x(t) = \varphi(t, x(0), u) \in \hat{x}(t)$ for $t \in [\tau^*, \tau^* + \delta)$. Now, assume that $x(t) \in \hat{x}(t)$ for $t \in [\tau^*, \tau^* + n\delta)$ for a given positive integer n such that $n\delta + \tau^* \leq T$. We show that $x(t) \in \hat{x}(t)$ for $t \in [\tau^*, \tau^* + (n+1)\delta)$ if $\tau^* + (n+1)\delta \leq T$ and for $t \in [\tau^*, T]$ otherwise. If there exists $s \leq n\delta + \tau^*$ and $z \in Z^L(s)$ such that $n\delta = z_1$, then $\hat{h}_{d,syn}(n\delta + \tau^*, \tau^*) = h(y(n\delta))$ from (7) and (6). Then, for $t \in [n\delta + \tau^*, \min\{(n+1)\delta + \tau^*, T\})$, from Cases 3 in (13) and (14), we have

$$\hat{x}_d(t) = \Phi(t - \tau^* - n\delta, \hat{x}_d(n\delta + \tau^*), U|_{[n\delta, t-\tau^*)}),$$

and, using (15),

$$\hat{x}(t) = \Phi(t - n\delta, \hat{x}_d(n\delta + \tau^*), U|_{[n\delta,t)}).$$

Further, by definition of (14) and since $\hat{x}_d(\tau^*) = h(y(0))$, $x(t-\tau^*) \in \hat{x}_d(t)$ for $t \geq \tau^*$. Therefore, similarly, from (5) and as $u(t) \in U(t)$ for $t \in [0,T]$, one obtains that $x(t) \in \hat{x}(t)$ for $t \in [n\delta + \tau^*, \min\{(n+1)\delta + \tau^*, T\})$. The same argument and result also hold for $t = T$ if $T < (n+1)\delta + \tau^*$. Otherwise, if for all $s \leq n\delta + \tau^*$ and $z \in Z^L(s)$, $n\delta \neq z_1$, then, Case 2 holds in (13). Consequently, for $t \in [n\delta + \tau^*, \min\{(n+1)\delta + \tau^*, T\})$, using (15) and Case 3 in (13),

$$\begin{aligned}\hat{x}(t) =& \Phi(t - (n-1)\delta, \hat{x}_d((n-1)\delta + \tau^*), U|_{[(n-1)\delta,t)})\\ =& \Phi(t - (n-1)\delta - \tau^*, \Phi(\tau^*, \hat{x}_d((n-1)\delta + \tau^*),\\ & U|_{[(n-1)\delta,(n-1)\delta+\tau^*)}), U|_{[(n-1)\delta+\tau^*,t)})\\ =& \Phi(t - (n-1)\delta - \tau^*, \hat{x}((n-1)\delta + \tau^*), U|_{[(n-1)\delta+\tau^*,t)}).\end{aligned}$$

From the induction assumption, $x(t) \in \hat{x}(t), t \in [\tau^*, n\delta+\tau^*)$, and in particular $x((n-1)\delta+\tau^*) \in \hat{x}((n-1)\delta+\tau^*)$. As $u(t) \in U(t)$ for $t \in [\tau^*, T]$, it follows that $x(t) \in \hat{x}(t)$ for $t \in [n\delta+\tau^*, \min\{(n-1)\delta+\tau^*, T\})$. The same argument and result also hold for $t = T$ if $T < (n+1)\delta+\tau^*$. Therefore, by induction on n, $x(t) \in \hat{x}(t)$ for $t \in [\tau^*, T]$ and $B0$ holds.

($D0 \Rightarrow C0$) Assume that $D0$ holds. As previously, for $L \in \{1,2\}$, $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = h(y(0))$ as, from $D0$, $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = \hat{h}^R_{d,syn}(\tau^*,\tau^*) = \hat{h}_{d,syn}(\tau^*,\tau^*) \neq \emptyset$. Consequently, $\hat{x}^L_d(\tau^*) = \hat{x}^R_d(\tau^*) = \hat{x}_d(\tau^*) = h(y(0))$ from (14), $\hat{x}^L(\tau^*) = \hat{x}^R(\tau^*) = \hat{x}(\tau^*)$ and, from (10), $\hat{x}(\tau^*) = \Phi(\tau^*, h(y(0)), U|_{[0,\tau^*)})$. Then, as $x(0) \in h(y(0))$, $x(\tau^*) \in \hat{x}(\tau^*)$ and $C0$ holds. □

Lemma 3 *Assume that* $\Phi(\tau^*, h(y(0)), [u_m, u_M]^2) \notin \mathscr{C}$, *and that for* $L \in \{1,2\}$ *and* $t \geq 0$, $u^L(t) \in U^L_L(t)$ *defined through* (14)–(16). *Consider the delays* τ^{LR} *and* τ^{RL} *introduced in* (6)*, the statement* $D0$ *defined in Lemma 2 and the following one, with* $T \geq \tau^*$*:*

E0: $\tau^{LR}(0) \leq \tau^*$, $\tau^{RL}(0) \leq \tau^*$ *and, for* $n \in \left\{1, \dots, \lfloor \frac{T-\tau^*}{\delta} \rfloor\right\}$, *either* $\tau^{LR}(n\delta) \leq \tau^*$ *and* $\tau^{RL}(n\delta) \leq \tau^*$ *or* $\tau^{LR}(n\delta) > \tau^*$ *and* $\tau^{RL}(n\delta) > \tau^*$.

Then, $Pr(D0) \geq Pr(E0)$.

Proof: First, from (13), the statement $D0$ is equivalent to $\tilde{D}0$

$$\tilde{D}0 : \hat{h}^L_{d,syn}(\tau^*,\tau^*) = \hat{h}^R_{d,syn}(\tau^*,\tau^*) \neq \emptyset \text{ and } \hat{h}^L_{d,syn}(t,\tau^*) = \hat{h}^R_{d,syn}(t,\tau^*) \text{ for } t \in (\tau^*, T].$$

We now show that a sufficient condition for $\tilde{D}0$ to hold is $E0$.

From Cases 1–2 in (13), $\hat{h}^L_{d,syn}(\tau^*,\tau^*) \neq \emptyset$ if there exist $s \leq 0$ and $z \in Z^L(s)$ such that $z_1 = 0$. Following (6), s is such that $\tau^{RL}(0) = s$. Therefore, if $\tau^{RL}(0) = \tau^{LR}(0) = s \leq \tau^*$, $\hat{h}^L_{d,syn}(\tau^*,\tau^*) = \hat{h}^R_{d,syn}(\tau^*,\tau^*) \neq \emptyset$. Besides, from Case 3 in (13), one can observe that $\hat{h}^L_{d,syn}(t,\tau^*) = \hat{h}^R_{d,syn}(t,\tau^*)$ for $t \in (\tau^*, T]$ if $\hat{h}^L_{d,syn}(n\delta+\tau^*,\tau^*) = \hat{h}^R_{d,syn}(n\delta+\tau^*,\tau^*)$ for $n \in \{0, \dots, \lfloor (T-\tau^*)/\delta \rfloor\}$. Therefore, $\tilde{D}0$ holds if $\tau^{LR}(0) \leq \tau^*$ and $\tau^{RL}(0) \leq \tau^*$ and $\hat{h}^L_{d,syn}(n\delta+\tau^*,\tau^*) = \hat{h}^R_{d,syn}(n\delta+\tau^*,\tau^*)$ for $n \in \{1, \dots, \lfloor (T-\tau^*)/\delta \rfloor\}$.

Consider $n \in \{1, \dots, \lfloor (T-\tau^*)/\delta \rfloor\}$ and assume that $\hat{h}^L_{d,syn}(t,\tau^*) = \hat{h}^R_{d,syn}(t,\tau^*)$ for $t \in [\tau^*, n\delta+\tau^*)$. From Cases 1–2 in (13), a sufficient condition for $\hat{h}^L_{d,syn}(n\delta+\tau^*,\tau^*) = \hat{h}^R_{d,syn}(n\delta+\tau^*,\tau^*)$ is that either there exists $s \leq n\delta+\tau^*$ and $z \in Z^L(s)$ such that $z_1 = n\delta$ for both $L = 1$ and $L = 2$ or that this does not hold for both $L = 1$ and $L = 2$. Consider $L \in \{1,2\}$. If $\tau^{RL}(n\delta) \leq \tau^*$, there exists $s \leq n\delta+\tau^*$ and $z \in Z^L(s)$ such that $z_1 = n\delta$. Therefore, a sufficient condition for $\hat{h}^L_{d,syn}(n\delta+\tau^*,\tau^*) = \hat{h}^R_{d,syn}(n\delta+\tau^*,\tau^*)$ is that either $\tau^{RL}(n\delta) \leq \tau^*$ and $\tau^{LR}(n\delta) \leq \tau^*$, or $\tau^{RL}(n\delta) > \tau^*$ and $\tau^{LR}(n\delta) > \tau^*$.

Consequently, a sufficient condition for $\tilde{D}0$ to hold is $E0$. It follows that $\Pr(D0) = \Pr(\tilde{D}0) \geq \Pr(E0)$. □

Proof of Theorem 2. Consider the statement $E0$ introduced in Lemma 3. From Lemmas 2–3, it follows that $\Pr(x(t) \notin \mathscr{B}, t \in [0,T]) \geq \Pr(E0)$. Further, as τ^{LR} and τ^{RL} are white noise processes, their realizations are independent from each other and one obtains

$$\Pr(E0) = \Pr(\tau^{RL}(0) \leq \tau^* \text{ and } \tau^{LR}(0) \leq \tau^*) \prod_{n=1}^{\lfloor (T-\tau^*)/\delta \rfloor} \Pr\big([\tau^{RL}(n\delta) \leq \tau^* \text{ and } \tau^{LR}(n\delta) \leq \tau^*] \text{ or } [\tau^{RL}(n\delta) > \tau^* \text{ and } \tau^{LR}(n\delta) > \tau^*]\big).$$

As the realizations of τ^{RL} and τ^{LR} are independent and have the same probability density function, it follows, letting τ denote $\tau^{RL}(t)$ or $\tau^{LR}(t)$, that

$$\Pr(E0) = \Pr(\tau \leq \tau^*)^2 \prod_{n=1}^{\lfloor \frac{T-\tau^*}{\delta} \rfloor} \Big[\Pr(\tau \leq \tau^*)^2 + \Pr(\tau > \tau^*)^2 - \Pr(\tau \leq \tau^*)^2 \Pr(\tau > \tau^*)^2\Big].$$

As, $\Pr(A0) = \Pr(x(t) \notin \mathscr{B},\ t \in [0,T]) \geq \Pr(E0)$, the result follows, noticing that $\Pr(\tau > \tau^*) = 1 - \Pr(\tau \leq \tau^*)$. □

6 Evaluation of closed-loop performance

In this section, we aim at providing an evaluation of the performance that can be obtained using the proposed technique, i.e., we determine how far from the bad set the trajectory generated by the control law can be with communication delay. With this aim, we define $\mathscr{U} = \left\{u \in \mathscr{C}_{pw}(\mathbb{R}_+, [u_m, u_M]^2) \mid u_L(t) \in U^L_L(t),\ t \geq \tau^*, L = 1,2\right\}$ and consider the following quantity

$$\inf_{t \in [0,T]} \sup_{u \in \mathscr{U}} d(\varphi(t, x_0, u), \mathscr{B}), \tag{18}$$

for $T \geq \tau^*$ and a given $x_0 \in \mathbb{R}^{2n}$ such that $\Phi(\tau^*, h(x_0+\sigma)), [u_m, u_M]^2) \notin \mathscr{C}$. This distance quantifies, for given initial conditions satisfying the assumptions of Theorems 1 and 2, how far from the bad set the trajectory generated by the proposed control law can be in the presence of communication delay. However, in the case of an infinitely-distributed delay, the probability of entering the bad set is not equal to zero and therefore the trajectory can actually intersect the bad set. This is why we will restrict the trajectories under consideration to safe ones.

First, we characterize further the dynamics under consideration.

Assumption 3 There exist a positive increasing scalar continuous function κ, class $\mathscr{K}$ functions α_1 and α_2 and a

class $\mathscr{K}_\infty$ function γ such that, for arbitrary pairs $(x_1,x_2) \in \mathbb{R}^n \times \mathbb{R}^n$ and $(u_1,u_2) \in \mathscr{C}^0_{pw}(\mathbb{R},\mathbb{R}^m) \times \mathscr{C}^0_{pw}(\mathbb{R},\mathbb{R}^m)$, the corresponding solutions of (1) satisfy, for $t \geq 0$,

$$\begin{aligned}|\varphi(t,x_1,u_1) - \varphi(t,x_2,u_2)| \\ \leq \kappa(t)\alpha_1(|x_1-x_2|) + \alpha_2(t)\gamma(\|u_2-u_1\|_\infty)\,. \end{aligned} \quad (19)$$

This assumption is motivated by Theorem 3.4 in [20]. Indeed, provided that the vector field is continuously differentiable with respect to the state x and to the input u, Assumption 3 holds.

To evaluate the closed-loop performance in the case of an infinitely-distributed delay, we have to guarantee that the considered trajectories do not enter the bad set and thus consider trajectories such that the statement $E0$ holds. As this event is not deterministically given, in the sequel, we consider a conditional expected value of the quantity (18).

Proposition 1 *Consider the plant* (1) *satisfying Assumptions 1 and 3 and the assumptions of Theorem 2. Define* $\mathscr{U} = \left\{ u \in \mathscr{C}_{pw}(\mathbb{R}_+,[u_m,u_M]^2) \mid u_L(t) \in U_L^L(t)\,,\, t \geq \tau^*, L = 1,2 \right\}$. *Then, for* $T \geq \tau^*$ *and for trajectories originating from* $x_0 = x(0)$ *such that the statement* $E0$ *defined in Lemma 3 holds, there exist a positive increasing scalar continuous function* κ, *class* $\mathscr{K}$ *functions* α_1 *and* α_2 *and a class* $\mathscr{K}_\infty$ *function* γ *such that*

$$\begin{aligned}\inf_{t\in[0,T]} \sup_{u\in\mathscr{U}} \mathbb{E}(d(\varphi(t,x_0,u),\mathscr{B})|E0) \leq \kappa(T)\alpha_1(|\sigma_M-\sigma_m|) \\ + \inf_{t\in[0,T]} \sup_{u\in\mathscr{U}} \mathbb{E}(d(\hat{x}^L(t),\mathscr{B})|E0) + G(\delta,\tau^*)\,, \end{aligned} \quad (20)$$

in which

$$\begin{aligned}G(\delta,\tau^*) = Pr(\tau \leq \tau^*)\times \\ \sum_{i=0}^{\lfloor (T-\tau^*)/\delta \rfloor -1} Pr(\tau > \tau^*)^i \alpha_2(\tau^* + (i+1)\delta)\gamma(|u_M-u_m|) \\ + Pr(\tau > \tau^*)^{\lfloor (T-\tau^*)/\delta \rfloor} \alpha_2(T)\gamma(|u_M-u_m|)\,. \end{aligned} \quad (21)$$

is increasing with respect to δ *and there exist* τ_0 *and* τ_1 *with* $0 < \tau_0 \leq \tau_1$ *such that* G *is decreasing for* $\tau \in [0,\tau_0)$ *and increasing for* $\tau \in (\tau_1,\infty)$.

Due to space limitation, the proof of this proposition is not provided here but can be found in [4].

According to Proposition 1, the distance of the trajectory from the bad set, i.e., the conservatism of the proposed control strategy, can be quantified by three terms corresponding to three different phenomena: (i) the magnitude of measurement uncertainties; (ii) the performance of the nominal feedback law introduced in Assumption 2; and (iii) the synchronization technique introduced in (13)–(16). Note that, without measurement uncertainties and communication delay, the left-hand side of (20) is equal to the right hand-side, since $|\sigma_M - \sigma_m| = 0$ and one can chose $\delta = \tau^* = 0$ and therefore $G(\delta,\tau^*) = 0$. This bodes well for the tightness of the bound.

From Theorem 2, one concludes that the probability of safety Π increases when increasing the synchronization delay τ^* and the period of update δ. However, from Proposition 1, one obtains inverse requirements for closed-loop performance. Indeed, in the case of no-collision, the bound proposed in Proposition 1 increases while increasing δ and τ^*. Therefore, a tradeoff has to be reached between probability of safety and closed-loop performance. This point is illustrated in Section 8 through an example.

7 Computation approaches and extension to N agents

In this section, we focus on computational aspects of our estimation strategy and also discuss its generalization to N agents.

7.1 Computation approaches related to the estimation strategy

In view of real-time application, we discuss methods allowing efficient implementation of the proposed strategy. Computational burden has two main sources: (i) the computation of the operator Φ given in (5); and (ii) the computation of the capture set introduced through Assumption 2. We detail them in the following.

Efficient computation of the operator Φ. This operation requires to explore the entire control set. It is possible to simplify this computation when the dynamics under consideration satisfy the following monotonicity assumption [2]: *the flow is monotone with respect to the input and the initial condition, i.e.,*

$$\begin{aligned}\forall t \in \mathbb{R}_+ \; \forall (x,\tilde{x}) \in \mathbb{R}^n \times \mathbb{R}^n \; \forall (u,\tilde{u}) \in \mathscr{C}^0_{pw}(\mathbb{R}_+,[u_m,u_M])^2 \\ x \leq \tilde{x},\; u \leq \tilde{u} \;\Rightarrow\; \varphi^i(t,x,u) \leq \varphi^i(t,\tilde{x},\tilde{u})\,, \end{aligned}$$

(see [13,18] where other technical assumptions are provided). Under this assumption, for a closed interval S and a closed set-valued function U, the operator (5) can be calculated as

$$\begin{aligned}\Phi :& \mathbb{R}_+ \times \mathbb{R}^{2n} \times \mathscr{C}_{pw}(\mathbb{R}_+,\mathscr{I}([u_m,u_M]^2)) \to 2^{\mathbb{R}^{2n}} \\ & (t,S,U) \mapsto [\varphi(t,\min(S),s\geq 0 \mapsto \min U(s)), \\ & \qquad \varphi(t,\max(S),s\geq 0 \mapsto \max U(s))]\,. \end{aligned}$$

The complexity of the required operations is linear with the input dimension and with the state dimension [13,18].

Complexity arising from the computation of the capture set. Previously developed techniques for the efficient computation of the capture set can be employed in our context [1,3,5,8,13,16,18,23,37,40,42]. As long as those satisfy

Assumption 2, the proposed estimation technique can be directly applied. Related performance degradation corresponding to (a potential) over-approximation of the capture set are taken into account in our approach through the second term of the bound (20) obtained in Section 6.

Yet, computation of the capture set for an arbitrary number of agents is still a major practical difficulty: it has been shown in [8] that this problem is NP-hard with respect to the number of involved agents. However, it is still possible to rely on alternative approximate solutions to compute the nominal feedback map with algorithms of polynomial complexity, such as the robust scheduling techniques proposed in [5], which still satisfy Assumption 2. We now discuss this point.

7.2 Extension to N agents

Assuming that the exchanged data is also stamped with a sender identification marker and that all communication channels can be modeled similarly, the estimation strategy proposed in this paper can be easily extended to N agents. We discuss here the scalability of this estimation strategy and the satisfaction of Assumption 2.

Scalability of the proposed estimation strategy. Consider the estimation strategy (7)–(10). Assume that the dynamics are monotone. Then, following the remarks made in the previous subsection, one can observe that its computational complexity is linear with respect to the number of agents and hence scalable. To see this, note that the number of operations involved in the computation of the corrected delayed estimation set (9) and the estimation set (10) grows linearly with the space dimension and the input dimension. Those grow themselves linearly with the number of agents N. Computation of the synchronized delayed measurement set through (7)–(8) only requires the local agent to fill, with local data and data received from the $N-1$ agents, a given look-up table of size $N \times \tau^*/(\Delta T)$ (writing ΔT the discrete time step). Hence, one can conclude that the proposed estimation technique is scalable with the number of agents.

Efficient computation of the feedback map for N agents. The problem of computing the capture set as given in Assumption 2 in the case of N agents trying to avoid pair-wise collisions has been addressed in [8]. It required the assumption of perfect state information, which has been relaxed in [5]. In particular, the resulting algorithms produce either the entire control set or a single N-tuple as the allowed control inputs at any time. This guarantees that the control map is in the form of a Cartesian product at any time, as required by Assumption 2. Hence, for N agents, Theorem 1 and Proposition 1 would still hold under their current form and the resulting controllers could be efficiently computed online by using the algorithms proposed in [5,8].

In the case of an infinitely-distributed delay, one cannot guarantee that the agents evaluate the feedback map with the same estimation set $\hat{x}^L$. Hence, Theorem 2 would slightly change as follows.

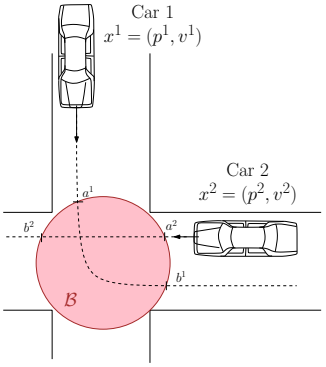


Fig. 3. Intersection scenario. A collision occurs if two vehicles are in the bad set $\mathscr{B}$ at the same time.

Remark 2 (Theorem 2 for N agents.) *Consider the plant* (1) *satisfying Assumption 1, the feedback law* π *satisfying Assumption 2, the delayed measurement set* $\hat{h}_d^L$ *defined in* (7) *and the operator* Φ *defined in* (5)*. Define* $\tau^*, \delta \geq 0$ *and, for* $L \in \{1,\dots,N\}$ *and* $t \geq \tau^*$*, the synchronized delayed measurement set* (13)*, the corrected delayed state set* (14)*, the estimated set* (15) *and the control set* (16)*. Provided that* $\Phi(\tau^*, h(y(0)), [u_m, u_M]^2) \notin \mathscr{C}$*, and that, for* $L \in \{1,\dots,N\}$ *and* $t \geq 0$*,* $u^L(t) \in U_L^L(t)$ *then, writing* $p = Pr(\tau^{RL}(t) \leq \tau^*) = Pr(\tau^{LR}(t) \leq \tau^*)$*,*

$$\forall T \geq \tau^* \quad Pr(x(t) \notin \mathscr{B},\, t \in [0,T]) \geq p^N (p^N + (1-p^N)(1-p)^N)^{\lfloor (T-\tau^*)/\delta \rfloor}.$$

This result can be obtained from arguments similar to those employed in Section 5. One can notice that a sufficient condition for safety is that: (i) the N agents have initially received the τ^*-delayed measurements (the probability of this event is p^N, as all white noise are independent); and (ii) at each update time $\tau^* + n\delta$, either all have received the τ^*-delayed measurements or all have not (the probability of this event is $(p^N + (1-p^N)(1-p)^N)^{\lfloor (T-\tau^*)/\delta \rfloor}$, for the same reasons as previously). The product of those two probabilities hence gives the above result.

8 Simulation results

In this section, we illustrate the merits of our approach by applying the proposed control strategy to a two-vehicle collision avoidance problem. We consider two human-driven vehicles approaching the traffic intersection depicted in Fig. 3. The vehicles are equipped with GPS and exchange their respective position and speed via Vehicle-to-Vehicle (V2V) communication. The control objective is to guarantee that the two vehicles do not enter the intersection simultaneously, by overriding the driver when necessary, despite communication delay and measurement uncertainties.

8.1 Vehicle dynamics and delay-free feedback map

For each vehicle $i \in \{1,2\}$, we denote (see Fig. 3) the longitudinal displacement along its path by $x_1^i = p^i$ and the

longitudinal speed by $x_2^i = v^i$. The considered longitudinal dynamics for vehicle $i \in \{1,2\}$ are

$$\dot{x}_1^i = x_2^i, \quad \dot{x}_2^i = \mathrm{Sat}_{[v_m,v_M]}\left\{au + b - c(x_2^i)^2, x_2^i\right\}, \qquad (22)$$

in which the input $u = R\tau_w - f_b \in [0, u_M]$ ($u_M > 0$) is expressed in terms of the wheel torque τ_w, the wheel radius R and the brake force f_b, $a > 0$, $b < 0$ and $c > 0$ are given constants and $Sat_{[v_m,v_M]}$ is the saturation operator on the interval $[v_m, v_M]$ (with $0 < v_m \leq v_M$). This model is obtained from Newton's law, assuming that the road is flat. In particular, the term $c(x_2^i)^2$ accounts for the aerodynamic drag [41]. Finally, the operator Sat is employed to guarantee that the vehicle does not stop ($v_m > 0$) nor exceeds a maximum speed $v_M > 0$ (to respect road speed limitations). One can check that these dynamics satisfy Assumption 1. Further, they also satisfy Assumption 3 with $\alpha_2(t) = \frac{a}{\max\{1,2cv_M\}} e^{\max\{1,2cv_M\}t}$ and $\gamma = Id$, applying Theorem 3.4 in [20] with $L = \max\{1, 2cv_M\}$ and $\mu = a|u_M - u_m|$. Finally, to account for GPS inaccuracy, we consider that the measurements are subject to an additive bounded noise: $y^i(t) = x^i(t) + \sigma^i(t)$ in which σ^i takes values into the interval $[\sigma_m^i, \sigma_M^i]$ ($\sigma_m^i \leq \sigma_M^i$). The bad set consists of two path portions in which the vehicles cannot be located at the same time, i.e., $\mathscr{B} = (a^1, b^1) \times \mathbb{R} \times (a^2, b^2) \times \mathbb{R}$.

As shown in [18], the dynamics (22) are monotone. Along with the structure of the bad set, this property can be exploited to reformulate the capture set in terms of restricted sets, which are simple to compute. With this aim, we consider a constant input $u \in [u_m, u_M]^2$, the corresponding restricted capture set $\mathscr{C}_u = \left\{x \in \mathbb{R}^{2n} \,|\, \exists t \geq 0 \; \varphi(t, x, u) \in \mathscr{B}\right\}$ and define the constant input signals $u_A = (u_M, u_m)$ and $u_B = (u_m, u_M)$. Then, we have, following [17],

$$\mathscr{C} = \left\{S \subset \mathbb{R}^{2n} \mid S \cap \mathscr{C}_{u_A} \neq \emptyset \text{ and } S \cap \mathscr{C}_{u_B} \neq \emptyset\right\}.$$

A feedback control map satisfying Assumption 2 [5] is

$$\pi(S) = \begin{cases} u_B & \text{if } S \cap \mathscr{C}_{u_A} \neq \emptyset \text{ and } S \cap \partial\mathscr{C}_{u_B} \neq \emptyset \\ u_A & \text{if } S \cap \partial\mathscr{C}_{u_A} \neq \emptyset \text{ and } S \cap \overline{\mathscr{C}_{u_B}} \neq \emptyset \\ \left[u_m, u_M\right]^2 & \text{otherwise}. \end{cases} \qquad (23)$$

[5] This can be shown by contradiction as follows, taking advantage of the fact that (23) satisfies the property stated in Remark 1. Without loss of generality, we consider that, when $S \in \mathscr{C}$, $\pi(S)$ is a singleton. Assume that Assumption 2 does not hold. Then, there exist $S \notin \mathscr{C}$ and $\tilde{\pi} \in 2^{\mathscr{C}^0_{pw}(\mathbb{R}_+, [u_m,u_M]^2)}$ with $\tilde{\pi}(t) \in \pi(\Phi(t, s, \tilde{\pi}|_{[0,t)}))$ and $\tilde{t} \geq 0$ such that $\Phi(t, s, \tilde{\pi}|_{[0,\tilde{t})}) \in \mathscr{C}$. By definition of the capture set, there exists $t^* \in [0, \tilde{t})$ such that $S_0 = \Phi(t^*, S, \tilde{\pi}|_{[0,t^*)}) \notin \mathscr{C}$ and $\Phi(t, S, \tilde{\pi}|_{[0,t)}) \in \mathscr{C}$ for $t \in (t^*, t^* + \delta)$ for a given $\delta > 0$. Then, following (23), $\pi(S_0) = u_0$ ($u_0 = u_L$ or $u_0 = u_H$ depending on the set S_0). Consequently, $\pi(\Phi(s, S_0, \tilde{\pi}|_{[t^*,t^*+s)}))$ is a singleton for $0 \leq s \leq \delta$ and so is $\tilde{\pi}(t) \subseteq \pi(\Phi(s, S_0, \tilde{\pi}|_{[t^*,t^*+s)}))$. Therefore, $\Phi(\delta, S_0, \tilde{\pi}|_{[t^*,t^*+\delta)}) = \varphi(\delta, S_0, \tilde{\pi}|_{[t^*,t^*+\delta)}) \in \mathscr{C}$ with $S_0 \notin \mathscr{C}$ and $\tilde{\pi}(s) \in \pi(\varphi(s, S, \tilde{\pi}|_{[t^*,t^*+s)})$ for $s \in [0, \delta]$. This is in contradiction with Remark 1. Therefore, Assumption 2 holds.

Therefore, Theorems 1, 2 and Proposition 1 hold. As explained in Section 7.1, it is possible to implement the proposed control algorithm in an efficient manner. In particular, all sets can be determined from their upper and lower bounds, which are easily propagated with extreme control values.

In the sequel, when $\pi(S) \subset [u_m, u_M]^2$, we say that automatic control of the vehicles is taken, meaning that at least one driver is overridden and cannot control the vehicle.

8.2 Simulation set-up

For simulation, we consider $a = 3$, $b = -1$, $c = 0.01$ with $v_m = .5$ km/h (approx. 1.39 m/s) and $v_M = 50$ km/h (approx. 13.9 m/s). The bad set is $\mathscr{B} = (40, 50) \times \mathbb{R} \times (40, 50) \times \mathbb{R}$. We consider a discrete-time implementation with a time step $\Delta T = .1$ s. In discrete time, we consider the (continuous) set to be on one of the boundaries $\partial\mathscr{C}_{u_A}$ or $\partial\mathscr{C}_{u_B}$ when it is outside it while its prediction one step forward in time is inside it. The initial positions are randomly generated on the interval $[0.8, 1.4] \times [0.8, 1.4]$ and the initial speeds are both 27.5 km/h (approx. 7.65 m/s). The driver input follows a uniform distribution on the interval $[u_m, u_M]$. The additive measurement disturbances follow a uniform distribution on $[\sigma_m, \sigma_M] = [-1, 1] \times [-0.1, 0.1]$.

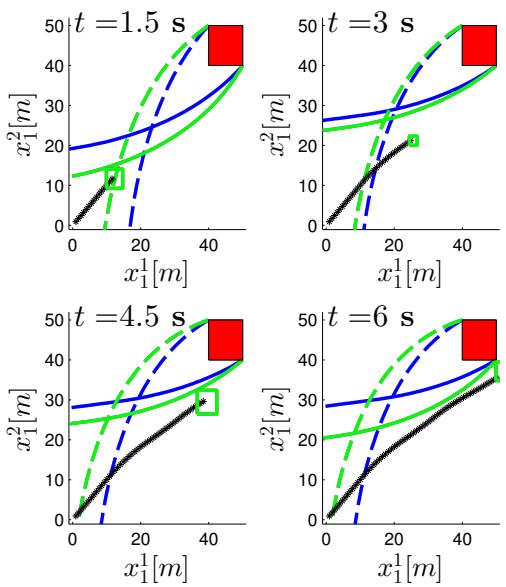
In the sequel, we consider an infinitely-distributed delay. Simulations were performed with a discrete Poisson delay distribution with (normalized) coefficient $\lambda = .6$. For these parameter values and for each vehicle, computation of the control law with Matlab took an average of 7.3 ms (with an upper bound of 11.9 ms) [6]. Note that this computation time grows linearly with the synchronization delay parameter N_τ (s.t. $\tau^* = N_\tau \Delta T$).

8.3 Simulation results for an infinitely-distributed delay

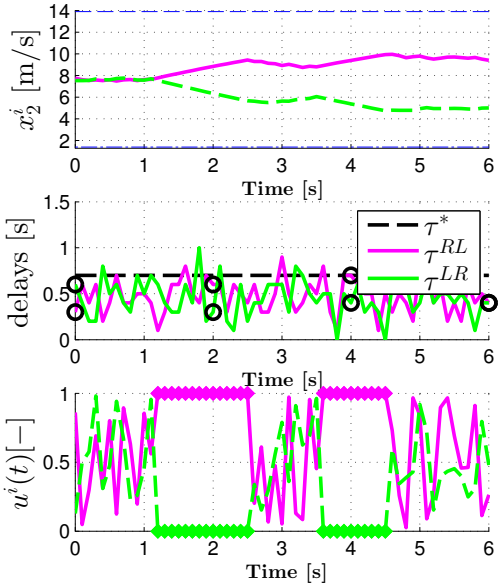
Fig. 4 and 5 depict two different simulation results obtained with $\delta = 2$ s and $\tau^* = 0.7$ s. One can directly observe that in the first case (Fig. 4) the control strategy leads to collision avoidance, while, in the second case (Fig. 5), it fails to guarantee safety as the trajectory intersects the bad set. This difference in behaviors can be understood in light of the delays evolution pictured in Fig. 4(b) and Fig. 5(b).

First, in Fig. 4(b), one can observe that, for any $n = 0, \ldots, 3$, $\tau^{LR}(n\delta) \leq \tau^*$ for $(L, R) \in \{(1,2), (2,1)\}$. In other words, at the update times $\tau^* + n\delta$, both vehicles update their synchronized delayed measurement set. This implies that the estimation set $\hat{x}^i(t)$, $i = 1, 2$, computed by the two vehicles are equal: both the projections on the (x_1^1, x_1^2) plane of the sets and the slices of the restricted capture set corresponding to the current speed estimate coincide (see Fig. 4(a)). Besides, the current state lies inside the estimation set as expected. The essence of the control strategy is visible in Fig. 4(a): the

[6] The CPU running Matlab is an Intel Core-Duo 2.9 GHz processor, with 8 GB of memory and a 350 GB hard drive.



(a) Dynamic evolution of the closed-loop system on the (x_1^1, x_1^2) plane. The black asterisks represent the trajectory of the system projected onto the (x_1^1, x_1^2) plane and the red box the projection of $\mathscr{B}$. Slices of $\mathscr{C}_{u_A}$ (solid line) and $\mathscr{C}_{u_B}$ (dashed line) corresponding to the current (resp. estimated) speeds are pictured in blue (resp. green). Green rectangles represent the projection of $\hat{x}^L(t)$ in the (x_1^1, x_1^2) plane.



(b) Plots of the speeds, communication delays and control inputs (in magenta for Vehicle $L = 1$ and in green for Vehicle $R = 2$). The circles in the delay plots correspond to the information used for update: if the delay values are smaller than or equal to τ^*, the information will be received and used τ^* units of time later while discarded if the delay values are greater than τ^*. The inputs corresponding to automatic control of the vehicles ($U^L(t) = \{u_A\}$ or $U^L(t) = \{u_B\}$ for $L \in \{1,2\}$) are represented with dots in the bottom plot.

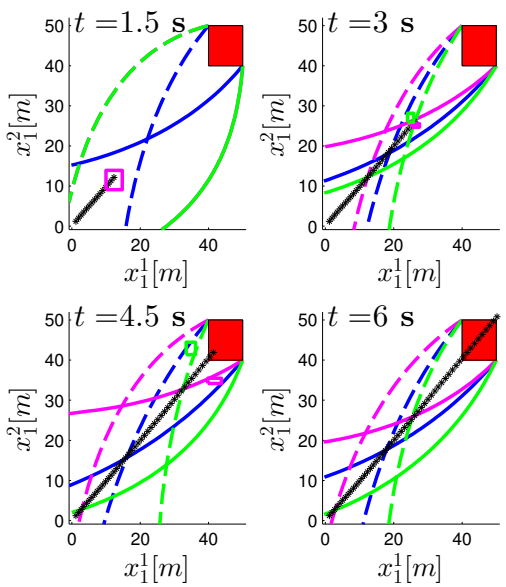
Fig. 4. Simulation results for an infinitely-distributed communication delay (uniform Poisson distribution). The control strategy guarantees collision avoidance.

proposed controller guarantees that the estimation set does not belong to the capture set. As a result, when the estimation set reaches the slice of $\mathscr{C}_{u_B}$ around $t = 1.2$ s, automatic control is activated, meaning that the control set is reduced to $\{u_B\} = \{(u_m, u_M)\}$. As a result, the estimation set then slides along the slice of $\mathscr{C}_{u_B}$ until having gone over the bad set.

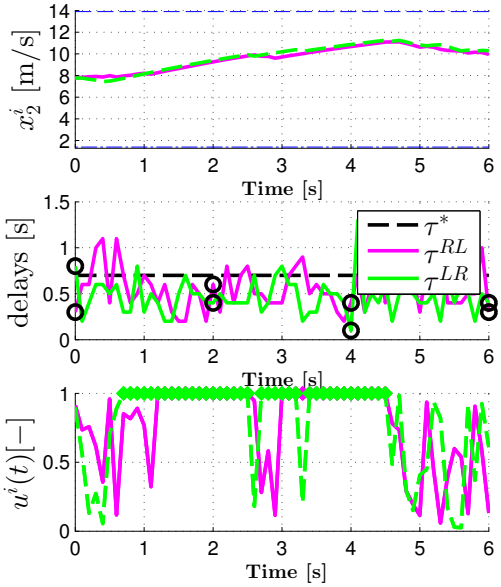
Second, one can observe in Fig. 5(b) that $\tau^{12}(0) > \tau^*$ while $\tau^{21}(0) < \tau^*$, meaning that only one vehicle updates its synchronized delayed measurement set at $t = \tau^*$. Correspondingly, the two vehicles employ distinct estimation sets, which is visible in Fig. 5(a) as the projections of both the system set and the slices of the capture set do not coincide. This leads to the following critical situation which can be observed in the top-right corner of Fig. 5(a): for Vehicle 1, the estimation set reaches the boundary ∂C_{u_A} after reaching ∂C_{u_B} while, for Vehicle 2, the inverse situation holds. Therefore, the two vehicles fail to agree on the control strategy to apply and both accelerate (Vehicle 1 applies the first component of u_A and Vehicle 2 the second of u_B). Further, even if updates of the synchronized delayed measurement set are performed at $t = \tau^* + \delta$, $t = \tau^* + 2\delta$, etc., for both vehicles, the estimation sets $\hat{x}^1$ and $\hat{x}^2$ are different for all times, as it can be observed in Fig. 5(a). Indeed, from (15), the estimation set $\hat{x}^L$ is obtained by propagating this common delayed state but with different input sets U^L.

It is worth noticing that such a situation of asymmetry between the information used by the agents does not necessarily imply collision. Indeed, it is possible that, even with different estimation sets, the two agents apply the same control and that, consequently, no collision occurs. This depends on various factors, randomly chosen in simulation, such as the driver input. One can observe this fact in the table of Fig. 6, in which the percentage of trajectories without collision is compared to the percentage of trajectories with occurrence of the situation $E0$ (see Lemma 3), for various values of the tuning parameters. One concludes that trajectories without collision are more frequent than trajectories with occurrence of the situation $E0$. Non-occurrence of the situation $E0$ does not necessarily imply collision, as explained above. For the considered example, the bound Π is therefore somewhat conservative but provides qualitative information on how the tuning parameters τ^* and δ affect the probability of safety. Indeed, as illustrated in Fig. 6, one can observe that the effects of τ^* and δ on the obtained bound of the closed-loop performance, analyzed in Section 6, also directly impact the performance [7].

[7] Besides, one can observe that the difference between the two percentages provided in the table of Fig. 6 becomes smaller as τ^* and δ increase. This trend can be explained by the fact that the initial positions and speeds have been chosen as identical for all tuning parameters values and, specifically, to satisfy the condition $\Phi(\tau^*, h(y(0)), [u_m, u_M]^2) \notin \mathscr{C}$ required by the theorem. Therefore, for low values of τ^* and δ, it is possible that, even if one agent has not received the measurement $h^R(y^R(0))$ at time τ^*, the latter



(a) Dynamic evolution of the closed-loop system on the (x_1^1, x_1^2) plane. The black asterisks represent the trajectory of the system projected onto the (x_1^1, x_1^2) plane and the red box the projection of $\mathscr{B}$. Slices of $\mathscr{C}_{u_A}$ (solid line) and $\mathscr{C}_{u_B}$ (dashed line) corresponding to the current (resp. estimated) speeds are pictured in blue (resp. magenta for Vehicle 1 and green for Vehicle 2). Magenta (for Vehicle 1) and green (for Vehicle 2) rectangles or crosses (in the case of a singleton) represent the projection of $\hat{x}^L(t)$ in the (x_1^1, x_1^2) plane.



(b) Plots of the speeds, communication delays and control inputs (in magenta for Vehicle $L = 1$ and in green for Vehicle $R = 2$). The circles in the delay plots correspond to the information used for update: if the delay values are smaller than or equal to τ^*, the information will be received and used τ^* units of time later while discarded if the delay values are greater than τ^*. As $\tau^{12}(0) > \tau^*$, Vehicle 2 does not receive any information at $t = \tau^*$ while Vehicle 1 does. This leads to the use of two different estimation sets, as can be observed in Fig. 5(a).

Fig. 5. Simulation results for an infinitely-distributed communication delay (uniform Poisson distribution). The control strategy fails to prevent collision at the intersection.

Finally, one can observe in Fig. 4(a) that, at time 1.5 s, the estimation set reaches the boundary of the capture set while the system state does not. Therefore, automatic control is applied before actually reaching the capture set: the delay is responsible for performance degradation. The tradeoff between performance and safety, analyzed in Section 6, is illustrated in the left plot of Fig. 6.

9 Conclusion

In this paper, we have addressed distributed safety control for two agents, subject to communication delay, by designing a state estimation procedure which guarantees control agreement between the two agents. The proposed state estimation allows to use feedback maps designed for the delay-free case, provided they are used jointly with an additional ingredient which consists of a synchronization of the delayed measurements used for the estimation.

The requirement of simultaneous computation of the estimation set can seem quite fragile from an implementation point of view. Robustness of this estimation strategy to missynchronization between the two agents is a direction of future work. Extension of the proposed technique to dropouts should also be investigated.

$h^R(y^R(\delta))$ at time $\delta + \tau^*$ is still outside of the capture set and therefore safety can still be guaranteed. This leads to a more conservative bound for low values of τ^* and δ, which is likely to be specific to the simulation set-up.

References

[1] H Ahn, Colombo A., and D. Del Vecchio. Supervisory control for intersection collision avoidance in the presence of uncontrolled vehicles. In *Proc. of the American Control Conference*, 2014.

[2] D. Angeli and E. D Sontag. Monotone control systems. *IEEE Transactions on Automatic Control*, 48(10):1684–1698, 2003.

[3] C. Belta, V. Isler, and G. J. Pappas. Discrete abstractions for robot motion planning and control in polygonal environments. *IEEE Transactions on Robotics*, 21(5):864–874, 2005.

[4] D. Bresch-Pietri and D. Del Vecchio. Evaluation of closed-loop performance of an estimation strategy for decentralized safety controller under communication delay and measurement uncertainties. https://hal.archives-ouvertes.fr/hal-01122553

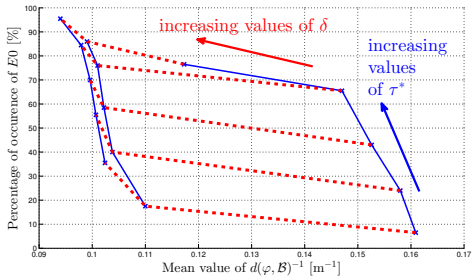
[5] L. Bruni, A. Colombo, and D. Del Vecchio. Robust multi-agent collision avoidance through scheduling. In *Proc. of the IEEE Conference on Decision and Control*, 2013.

[6] R. Carli and F. Bullo. Quantized coordination algorithms for rendezvous and deployment. *SIAM Journal on Control and Optimization*, 48(3):1251–1274, 2009.

[7] J. Choi, S. Oh, and R. Horowitz. Distributed learning and cooperative control for multi-agent systems. *Automatica*, 45(12):2802–2814, 2009.

[8] A. Colombo and D. Del Vecchio. Efficient algorithms for collision avoidance at intersections. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, pages 145–154. ACM, 2012.

[9] CAMP Vechile Safety Communications Consortium. Vehicle safety communications project task 3 final report : Identify intelligent



$\delta \setminus \tau^*$	0.5	0.6	0.7	0.8	0.9
2	78 | 6.5	82 | 24	92.5 | 43	93.5 | 65	98.5 | 76.5
4	82 | 17.5	84.5 | 40	93 | 58.5	94 | 76	99 | 86
6	82 | 35.5	86.5 | 55	87 | 70	95 | 84.5	98.5| 95.5
8	86 | 54.5	94 | 72	90.5 | 77	95 | 86.5	98.5 | 96
10	85 | 62.5	89.5 | 75	92 | 77.5	96 | 87.5	99 | 96

Fig. 6. Simulation results for 200 trajectories generated for an infinitely-distributed communication delay (Poisson distribution) and for various tuning parameters ($\delta = 2,\ldots,10$ s and $\tau^* = 0.5,\ldots,0.9$ s). The initial positions are generated randomly on the interval $[0.6,1.2]\times[0.6,1.2]$ and the initial speeds are both 0.5 m/s. The driver input follows a uniform distribution on the interval $[u_m,u_M]$. Left: percentage of occurrences of the situation $E0$ with respect to the inverse of the mean of the obtained distance to the bad set for safe trajectories. The dotted red curves indicated variations for a given fixed value of τ^* ($\tau^* = 0.5,\ldots 0.9$ s) and the blue lines for a given value of δ ($\delta = 2,4,6$ s) . Right: table of percentages of trajectories without collision (left number) and with occurrence of the situation $E0$ (right number, see Lemma 3) for 200 trajectories generated for an infinitely-distributed communication delay (Poisson distribution). The two entries of the table are the period of update δ and the synchronization delay τ^*, respectively.

vehicle safety applications enabled by DSRC. Technical report, Tech. Rep. DOT HS 809859, 2005.

[10] D. Dimarogonas, S. Loizou, K. Kyriakopoulos, and M. Zavlanos. A feedback stabilization and collision avoidance scheme for multiple independent non-point agents. *Automatica*, 42(2):229–243, 2006.

[11] U.S. DOT. Vehicle safety communications – Applications VSC-A second annual report. Technical report, National Highway Traffic Administation (NHTSA), 2008.

[12] F. Fagnani and S. Zampieri. Average consensus with packet drop communication. *SIAM Journal on Control and Optimization*, 48(1):102–133, 2009.

[13] R. Ghaemi and D. Del Vecchio. Control for safety specifications of systems with imperfect information on a partial order. *IEEE Transactions on Automatic Control*, 59:982–995, 2014.

[14] E. Guizzo. Three engineers, hundreds of robots, one warehouse. *Spectrum, IEEE*, 45(7):26–34, 2008.

[15] V. Gupta. On the effect of stochastic delay on estimation. *IEEE Transactions on Automatic Control*, 56(9):2145–2150, 2011.

[16] M. R. Hafner, D. Cunningham, L. Caminiti, and D. Del Vecchio. Cooperative collision avoidance at intersections: Algorithms and experiments. *IEEE Trans. Intelligent Transportation Systems*, 14:1162–1175, 2013.

[17] M. R. Hafner and D. Del Vecchio. Computation of safety control for uncertain piecewise continuous systems on a partial order. In *Proc. of the Conference on Decision and Control*, pages 1671–1677, 2009.

[18] M. R. Hafner and D. 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.

[19] J. Hu, J. Lygeros, M. Prandini, and S. Sastry. Aircraft conflict prediction and resolution using brownian motion. In *Proc. of the 38th IEEE Conference on Decision and Control*, volume 3, pages 2438–2443. IEEE, 1999.

[20] H. Khalil. *Nonlinear Systems*. 3rd Edition, Prentice Hall, 2002.

[21] H. Kowshik, D. Caveney, and P. R. Kumar. Provable systemwide safety in intelligent intersections. *IEEE Transactions on Vehicular Technology*, 60(3):804–818, 2011.

[22] J. Krozel and M. Peters. Strategic conflict detection and resolution for free flight. In *Proc. of the 36th IEEE Conference on Decision and Control*, volume 2, pages 1822–1828, 1997.

[23] C. Le Guernic. *Reachability analysis of hybrid systems with linear continuous dynamics*. PhD thesis, Université Joseph Fourier, 2009.

[24] J. Lee and B. Park. Development and evaluation of a cooperative vehicle intersection control algorithm under the connected vehicles environment. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):81–90, 2012.

[25] X.-Y. Lu, P. Varaiya, R. Horowitz, D. Su, and S. E. Shladover. Novel freeway traffic control with variable speed limit and coordinated ramp metering. *Transportation Research Record: Journal of the Transportation Research Board*, 2229(1):55–65, 2011.

[26] J. Lygeros, C. Tomlin, and S. Sastry. Controllers for reachability specifications for hybrid systems. *Automatica*, 35(3):349–370, 1999.

[27] V. Milanés, J. Pérez, E. Onieva, and C. González. Controller for urban intersections based on wireless communications and fuzzy logic. *IEEE Transactions on Intelligent Transportation Systems*, 11(1):243–248, 2010.

[28] R. Olfati-Saber, J. A. Fax, and R. M. Murray. Consensus and cooperation in networked multi-agent systems. *Proceedings of the IEEE*, 95(1):215–233, 2007.

[29] F. Özgüner, Ü. Özgüner, O. Takeshita, K. Redmill, Y. Liu, G. Korkmaz, A. Dogan, K. Tokuda, S. Nakabayashi, and T. Shimizu. A simulation study of an intersection collision warning system. In *Proc. of the international workshop on ITS telecommunications*, 2004.

[30] W. Ren and R. Beard. *Distributed consensus in multi-vehicle cooperative control: Theory and applications*. Springer, 2008.

[31] C. L. Robinson, D. Caveney, L. Caminiti, G. Baliga, K. Laberteaux, and P. R. Kumar. Efficient message composition and coding for cooperative vehicular safety applications. *IEEE Transactions on Vehicular Technology*, 56(6):3244, 2007.

[32] Y. Shen, Ü. Özgüner, K. Redmill, and J. Liu. A robust video based traffic light detection algorithm for intelligent vehicles. In *Proc. of the IEEE Intelligent Vehicles Symposium*, pages 521–526. IEEE, 2009.

[33] R. Slattery and S. Green. Conflict-free trajectory planning for air traffic control automation. Technical Report 108790, NASA Technical Memorandum, 1994.

[34] B. Sterzbach. GPS-based clock synchronization in a mobile, distributed real-time system. *Real-Time Systems*, 12(1):63–75, 1997.

[35] D. Teodorović and P. Lučić. Intelligent parking systems. *European Journal of Operational Research*, 175(3):1666–1681, 2006.

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

[37] C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.

[38] C. Tomlin, I. Mitchell, and R. Ghosh. Safety verification of conflict resolution manoeuvres. *IEEE Transactions on Intelligent Transportation Systems*, 2(2):110–120, 2001.

[39] C. Tomlin, G. J. Pappas, and S. Sastry. Conflict resolution for air traffic management: A study in multiagent hybrid systems. *IEEE Transactions on Automatic Control*, 43(4):509–521, 1998.

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

[41] R. Verma, D. Del Vecchio, and H. K. Fathy. Development of a scaled vehicle with longitudinal dynamics of an HMMWV for an ITS testbed. *IEEE/ASME Transactions on Mechatronics*, 13(1):46–57, 2008.

[42] R. Vidal, S. Schaffert, J. Lygeros, and S. Sastry. Controlled invariance of discrete time systems. In *Hybrid Systems: Computation and Control*, pages 437–451. Springer, 2000.

[43] P. R. Wurman, R. D'Andrea, and M. Mountz. Coordinating hundreds of cooperative, autonomous vehicles in warehouses. *AI Magazine*, 29(1):9, 2008.