Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Verification of Collision Avoidance Systems using Reachability Analysis ⋆

Jonas Nilsson [*,**] **Jonas Fredriksson** [**] **Anders C.E. Ödblom** [*]

[*] *Vehicle Dynamics and Active Safety Centre, Volvo Car Corporation, 40531 Göteborg, Sweden, (e-mail: jnilss94@volvocars.com, aodblom1@volvocars.com).*
[**] *Department of Signals and Systems, Chalmers University of Technology, 41296 Göteborg, Sweden,(e-mail: jonas.fredriksson@chalmers.se).*

Abstract: This paper presents a method for formal verification of automotive collision avoidance systems. Using viability theory and reachability analysis, we define when the system should intervene, i.e. the unsafe set, and when the system should not intervene, i.e. the safe set. Given these sets, we formulate the problem of verifying that a given system does not make incorrect decisions as an optimization problem. The method is demonstrated on a collision avoidance system example and, given the models used and absence of measurements errors, we show that the system does not make incorrect decisions. Furthermore, we describe and demonstrate how to evaluate the robustness to measurement errors, using the proposed framework.

1. INTRODUCTION

Current and future active safety systems cooperate with the driver to achieve the joint goal of safe driving. The resulting system is *semi-autonomous*, meaning that human-controlled operation may be disrupted by an autonomous system intervention. The decision to intervene is based on a Threat Assessment (TA) function, which at each time instant quantify the risk of the host vehicle being involved in an accident.

This paper addresses the problem of verifying that a given TA function makes correct decisions. Specifically, this means verifying that the system does not *miss* to intervene in unsafe situations and also that the system does not intervene *unnecessarily*, i.e. intervene in non-critical situations during normal driving. Since the input to the TA is based on sensors, the robustness to input errors, e.g. measurement errors, is also treated.

Verification is usually performed by evaluating test cases in the form of state trajectories, either using real vehicles, e.g. Lee and Peng [2005], Distner et al. [2009], or in simulation environments, e.g. Yang et al. [2003], Hillenbrand et al. [2006], Coelingh et al. [2006]. The number of possible input trajectories to the TA function is intractable, ruling out exhaustive evaluation strategies.

In contrast to evaluating state trajectories, as done in traditional simulation and real vehicle tests, we propose a novel set-based framework for analyzing under what conditions the absence of incorrect decisions may be guaranteed for a given TA function. Reachability analysis and viability theory are used to compute unsafe and safe sets, i.e. sets where an ideal system should or should not intervene respectively. Incorrect decisions in these sets, for a given TA function, are identified using optimization techniques. By separating the dynamics of the input space from the TA function, non-linear and ad-hoc TA functions are efficiently handled in the proposed framework.

We demonstrate how the proposed framework may be used for verification and sensitivity analysis on a TA function for rear-end collision avoidance. Results from this example show for what input errors, absence of unnecessary intervention may be guaranteed and also numerically describe the robustness to input errors over the safe set.

This paper is organized as follows. Section 2 presents related work and is followed by Section 3, where known results from reachability analysis and viability theory are presented. A problem formulation and a brief overview of the proposed framework is given in Section 4. Section 5 describes models of vehicle and object motion, as well as an example of a nonlinear TA function, while Section 6 demonstrates how to solve the verification and robustness problems formulated in Section 4 given the models and TA function in Section 5. Finally, Section 7 presents results and Section 8 gives concluding remarks.

2. RELATED WORK

Reachability analysis has been applied to both autonomous and semi-autonomous vehicle systems. The safety verification problem investigate if the autonomous system will enter a set of unsafe states. A similar analysis for semi-autonomous systems is commonly referred to as threat assessment. In this paper, we investigate if the TA function output enters a state which yields an incorrect decision.

⋆ This work was supported by the Swedish Automotive Research Program FFI - Vehicle and Traffic Safety, and the Vehicle and Traffic Safety Centre (SAFER)

In Althoff et al. [2009], stochastic forward reachable sets for the host vehicle and all other traffic participants are computed to determine the collision probability at each time step in a finite time horizon. This probability is used to verify that the planned trajectory for the host vehicle is safe. Safety verification of planned trajectories for coordinated maneuvers is done in Althoff et al. [2010]. The safety of Adaptive Cruise Control (ACC) is verified using reachability analysis in Kianfar et al. [2012] where a set is computed describing allowed deviation from desired position, relative speeds and accelerations which guarantee the absence of collisions.

A threat assessment approach for semi-autonomous vehicles is found in Falcone et al. [2011], demonstrated on a roadway departure application. A set of constraints describing "safe" driving is defined and used to compute a safe set at each time step over a finite prediction horizon via backwards reachable sets. If the current state is not a member of the corresponding safe set, the system will intervene. This approach is extended to handle bounded uncertainties in Ali [2012]. Two threat assessment strategies are proposed where theoretical guarantees may be issued that no unnecessary interventions or no missed interventions occur respectively, given bounded uncertainties are known. For large uncertainties issuing these guarantees will lead to either completely active or completely passive TA. In Gerdts and Xausa [2013], reachable sets are used to compute for what initial states a collision with a stationary obstacle may be avoided.

Our computation of a safe set is similar to the one proposed in Falcone et al. [2011], Ali [2012], but adapted to a rear-end collision avoidance system, as opposed to roadway departure avoidance. Also, instead of checking if the current state is a member of the safe set, we investigate whether or not an intervention may be initiated in the safe set. Work presented in Althoff et al. [2009], Gerdts and Xausa [2013], Falcone et al. [2011], Ali [2012] is primarily intended for online applications and therefore employ finite prediction horizons, whereas our work focus on asymptotic sets.

3. PRELIMINARIES

In this section we introduce definitions and results from reachabailty analysis and viability theory. For overviews on these topics, we refer to Kolmanovsky and Gilbert [1998], Mitchell [2007], Aubin et al. [2011]. First, we introduce some basic definitions. Let $\mathbb{N}^+$ be the set of all positive real numbers. Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{R}^n$ and define the *complement* of $\mathcal{A}$ in $\mathbb{R}^n$ as $\mathcal{A}^c \triangleq \mathbb{R}^n \setminus A$, where the *set difference* $\mathcal{B} \setminus A \triangleq \{z \in \mathcal{B} | z \notin \mathcal{A}\}$. The *Minkowski sum* is defined as $\mathcal{A} \oplus \mathcal{B} \triangleq \{z_A + z_B | z_A \in \mathcal{A}, z_B \in \mathcal{B}\}$.

Consider the state update function f of a discrete-time dynamical system

$$z(t+1) = f(z(t), u(t), w(t)), \tag{1}$$

where $z(t)$, $u(t)$ and $w(t)$ denote the state, input and disturbance vectors with appropriate dimensions respectively. The system in (1) is subject to constraints

$$z(t) \in \mathcal{Z} \subseteq \mathbb{R}^n, u(t) \in \mathcal{U} \subseteq \mathbb{R}^p, w(t) \in \mathcal{W} \subseteq \mathbb{R}^q, \tag{2}$$

where each of the sets $\mathcal{Z}$, $\mathcal{U}$ and $\mathcal{W}$ contains the origin in its interior. The system in (1) is referred to as the *nominal* system, if there are no disturbances, i.e. $\mathcal{W} = \{0\}$.

Now, we introduce some definitions for the nominal system:

Definition 1. For the nominal system $f(z, u, 0)$, subject to the constraints in (2), the one step *minimal backwards reachable set* is defined as

$$Pre(\mathcal{T}) \triangleq \{z \in \mathcal{Z} | f(z, u, 0) \in \mathcal{T}, \forall u \in \mathcal{U}\}. \tag{3}$$

This set include all states which, given that $u \in \mathcal{U}$, are guaranteed to evolve into $\mathcal{T}$ in one time step. To describe all backwards reachable states, over a finite horizon, we introduce the reachable tube:

Definition 2. For the nominal system $f(z, u, 0)$, subject to the constraints in (2), the *minimal backwards reachable tube* is defined recursively as

$$Pre^t(\mathcal{T}) \triangleq \bigcup_{\tilde{t} \in [0,t]} \Omega_{\tilde{t}}, \tag{4}$$

$$\Omega_t = Pre(\Omega_{t-1}), t \in \mathbb{N}^+, \Omega_0 = \mathcal{T}. \tag{5}$$

Next, we introduce the viability kernel, describing the initial states which remain in an admissible set $\mathcal{T}$, over the future horizon t, for some input $u(\cdot) \in \mathcal{U}$.

Definition 3. For the nominal system $f(z, u, 0)$, subject to the constraints in (2), the *viability kernel* is defined as

$$Viab^t(\mathcal{T}) \triangleq \\ \left\{z(0) \in \mathcal{T} | \exists u(\cdot) \in \mathcal{U} : \forall \tilde{t} \in [0, t], f(z(\tilde{t}), u(\tilde{t}), 0) \in \mathcal{T}\right\}, \tag{6}$$

where $Viab^\infty(\mathcal{T})$ are the initial states which respect the set constraints $\mathcal{T}$ for all future time. This set, $Viab^\infty(\mathcal{T})$, is also known as the maximal control invariant set.

It is straightforward to verify, see e.g. Cardaliaguet [1999], that $Viab^t(\mathcal{T}^c)$ and $Pre^t(\mathcal{T})$ are each others complement:

$$\left(Viab^t(\mathcal{T}^c)\right)^c = Pre^t(\mathcal{T}), \tag{7}$$

given that $\mathcal{T}$ is considered to be a target set, i.e. $z(0) \in \mathcal{T}$ implies that $z(t) \in \mathcal{T}, \forall t \in \mathbb{N}^+$.

This paper considers the case when the system in (1) is subject to disturbances, meaning that two alternative definitions are introduced for $Pre(\mathcal{T})$.

Definition 4. For the system in (1), subject to the constraints in (2), the one step *robust minimal backwards reachable set* is defined as

$$Pre_R(\mathcal{T}) \triangleq \{z \in \mathcal{Z} | f(z, u, w) \in \mathcal{T}, \forall u \in \mathcal{U}, \forall w \in \mathcal{W}\}. \tag{8}$$

Definition 5. For the system in (1), subject to the constraints in (2), the one step *uncertain minimal backwards reachable set* is defined as

$$Pre_U(\mathcal{T}) \triangleq \{z \in \mathcal{Z} | \exists w \in \mathcal{W} : f(z, u, w) \in \mathcal{T}, \forall u \in \mathcal{U}\}. \tag{9}$$

The robust minimal backwards reachable set definition guarantees that $\mathcal{T}$ is reached from $Pre_R(\mathcal{T})$ for all dis-

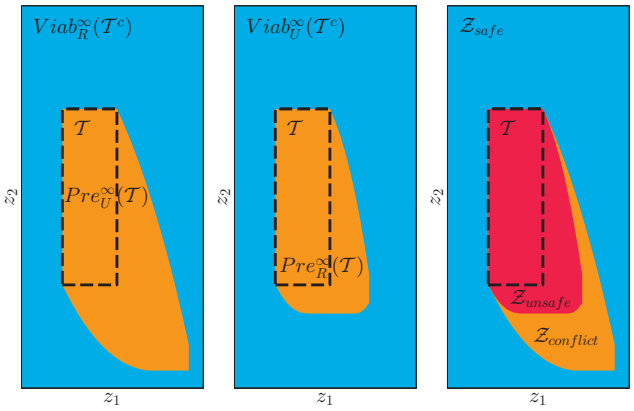

Fig. 1. The complementary properties of viability kernels and minimal backwards reachable tubes, see (10), are illustrated in (a) and (b). How these concepts are used to define safe, unsafe an conflict sets, see Definitions 6-8, is shown in (c).

turbances, while the uncertain minimal backwards reachable set definition only state that $\mathcal{T}$ may be reached from $Pre_U(\mathcal{T})$, for some disturbance. Robust and uncertain minimal backwards reachable tubes, $Pre_R^t(\mathcal{T})$ and $Pre_U^t(\mathcal{T})$ respectively, as well as robust and uncertain viability kernels, $Viab_R^t(\mathcal{T})$ and $Viab_U^t(\mathcal{T})$ respectively, are defined in analogy with Definitions 2 and 3.

The corresponding properties to (7) are

$$\left(Viab_R^t(\mathcal{T}^c)\right)^c = Pre_U^t(\mathcal{T}) \tag{10a}$$

$$\left(Viab_U^t(\mathcal{T}^c)\right)^c = Pre_R^t(\mathcal{T}), \tag{10b}$$

which is visualized in Figure 1.

4. PROBLEM FORMULATION AND PROPOSED APPROACH

Denote by $F(\theta(t))$ the threat assessment function where $F(\theta(t)) \geq 1$ represent a decision to intervene at time t and

$$\theta(t) \triangleq \begin{bmatrix} z(t) \\ u(t) \\ w(t) \end{bmatrix} \in \Theta = \mathcal{Z} \times \mathcal{U} \times \mathcal{W}. \tag{11}$$

Furthermore, let $\mathcal{Z}_{adm} \subseteq \mathcal{Z}$ denote the admissible set, which contains all non-collision states in $\mathcal{Z}$.

To verify that F makes correct decisions on when to intervene, the correct decision should ideally be defined, $\forall\theta$. The TA function F is designed to intervene when $\nexists u(\cdot)$ such that $z(\cdot)$ may be contained in the non-collision admissible set $\mathcal{Z}_{adm}$, for all future times. Thus, complete knowledge of the future disturbance w is needed to uniquely define a correct decision.

For the nominal system, not subject to disturbances, the system is guaranteed to evolve into a collision state $z \in \mathcal{Z}_{adm}^c$ if and only if $z \in Pre^\infty(\mathcal{Z}_{adm}^c)$, see Definition 2. Similarly, if $z \in Viab^\infty(\mathcal{Z}_{adm})$, it is always possible to find a control signal such that collision is avoided, i.e. $z \in \mathcal{Z}_{adm}$, for all future time. The complement property from (7) means that $Pre^\infty(\mathcal{Z}_{adm}^c)$ and $Viab^\infty(\mathcal{Z}_{adm})$ partition $\mathcal{Z}$ into two sets, one where interventions are needed and one where they are not.

In the presence of disturbances, the future safety of the system will depend on said future disturbances and it is not possible to partition $\mathcal{Z}$ into two sets which clearly discriminate between the correct system decisions. To describe correct decisions in the presence of disturbances, we introduce the following definitions:

Definition 6. For the system in (1), subject to the constraints in (2), the *safe set*, $\mathcal{Z}_{safe}$, is defined as

$$\mathcal{Z}_{safe} \triangleq Viab_R^\infty(\mathcal{Z}_{adm}). \tag{12}$$

Definition 7. For the system in (1), subject to the constraints in (2), the *unsafe set*, $\mathcal{Z}_{unsafe}$, is defined as

$$\mathcal{Z}_{unsafe} \triangleq Pre_R^\infty(\mathcal{Z}_{adm}^c). \tag{13}$$

This means that, given a proper choice of control input, the system will with certainty not collide if $z \in \mathcal{Z}_{safe}$, regardless of the future disturbance. Similarly, the system will with certainty collide if $z \in \mathcal{Z}_{unsafe}$, regardless of the future control and disturbance inputs. For the remaining states, whether or not the system collides will depend on the disturbance.

Definition 8. For the system in (1), subject to the constraints in (2), the *conflict set*, $\mathcal{Z}_{conflict}$, is defined as

$$\begin{aligned} \mathcal{Z}_{conflict} &\triangleq \mathcal{Z} \setminus \left(\mathcal{Z}_{safe} \bigcup \mathcal{Z}_{unsafe}\right) \\ &= Viab_U^\infty(\mathcal{Z}_{adm}) \setminus Viab_R^\infty(\mathcal{Z}_{adm}) \\ &= Pre_U^\infty(\mathcal{Z}_{adm}^c) \setminus Pre_R^\infty(\mathcal{Z}_{adm}^c). \end{aligned} \tag{14}$$

The three sets $\mathcal{Z}_{safe}$, $\mathcal{Z}_{unsafe}$ and $\mathcal{Z}_{conflict}$ now form a partition of $\mathcal{Z}$, see Figure 1, where the correct decision is unique in $\mathcal{Z}_{safe}$, $\mathcal{Z}_{unsafe}$ while in $\mathcal{Z}_{conflict}$ it cannot be uniquely determined.

Definition 9. For the threat function F, subject to the constraints in (11), a decision to intervene, i.e. $F(\theta) \geq 1$, is said to be *unnecessary* if $z \in \mathcal{Z}_{safe}$.

Definition 10. For the threat function F, subject to the constraints in (11), a decision not to intervene, i.e. $F(\theta) < 1$, is said to be *missed* if $z \in \mathcal{Z}_{unsafe}$.

The verification problem is now equivalent to checking if there are any missed or unnecessary interventions in $\mathcal{Z}$. For e.g. unnecessary interventions this means verifying that it is not possible to initiate an intervention from the safe set, i.e. that

$$\max_{\theta \in \mathcal{Z}_{safe} \times \mathcal{U} \times \mathcal{W}} F(\theta) < 1 \tag{15}$$

Note that to solve the verification problem, it is sufficient to acquire a bound on the constrained optimization problem on the left hand side.

Above, the verification problem has been formulated given that θ is known to the system. In practice, the system tries to measure and estimate $\hat{\theta}$ which may exhibit errors. The robustness to such errors will also be addressed in this paper.

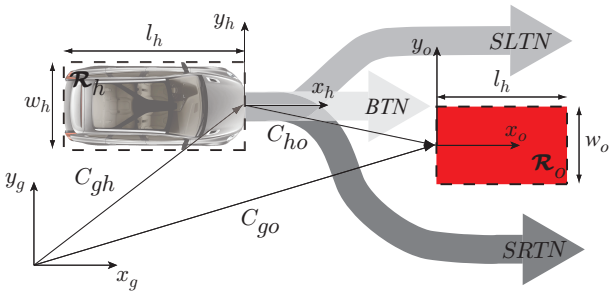

Fig. 2. Global and relative coordinate systems. The thick arrows indicate possible avoidance maneuvers considered by the threat assessment.

5. MODELING

This section describes models used to demonstrate the proposed method. We consider a host vehicle, equipped with a collision avoidance system, designed to avoid rear-end collisions. The relative motion between the host vehicle and the object is modeled as purely translational. This model is a satisfactory approximation, given that the relative rotation between the host vehicle and the object is limited. In practice, this means the model is valid when driving at high speeds, e.g. in motorways.

5.1 Coordinate Systems

Denote by $P_g = [x_g \; y_g]^T$ a point in a fixed global reference frame and by $P_{\tilde{h}}$ and $P_{\tilde{o}}$ the corresponding point in the moving reference frames of the host vehicle and object respectively. Furthermore, denote by h and o the reference frames corresponding to reference frames $\tilde{h}$ and $\tilde{o}$ respectively, but considered fixed at each time instant.

The origins of the reference frames for the host vehicle and object are defined according to Figure 2. Furthermore, the extension of the host vehicle and object in the 2D position space are defined by the polytopes, $\mathcal{R}_h \subset \mathbb{R}^2$ and $\mathcal{R}_o \subset \mathbb{R}^2$ respectively, both depicted in Figure 2.

5.2 Relative Motion

For the relative motion of an object in the host vehicle reference frame, we define the state, input and disturbance as

$$z \triangleq \begin{bmatrix} C_{\tilde{h}\tilde{o}} \\ \dot{C}_{\tilde{h}\tilde{o}} \end{bmatrix}, u \triangleq \ddot{C}_{h\tilde{h}}, w \triangleq \ddot{C}_{o\tilde{o}}. \tag{16}$$

Thus, the host acceleration input, $\ddot{C}_{h\tilde{h}}$, is treated as an input u, and the object acceleration input, $\ddot{C}_{o\tilde{o}}$, is treated as a disturbance w.

Assuming that the motion is pure translation yields

$$\dot{z} = Az - Bu + Bw, \tag{17}$$

where

$$A = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 \\ I \end{bmatrix}. \tag{18}$$

The state space of interest, $\mathcal{Z}$, for the system in (17), is chosen as a hypercube. Figure 3 displays the boundaries in the position domain. The input constraints, $\mathcal{U}$ and $\mathcal{W}$, are chosen to reflect acceleration levels from normal driving.

5.3 Threat Assessment

This section presents an example of a threat assessment function, F, which in this paper is used as a test subject in the presented framework. The TA below is designed for avoiding rear-end collisions. The position of the object relative the host vehicle $C_{\tilde{h}\tilde{o}} = [x_{\tilde{h}\tilde{o}} \; y_{\tilde{h}\tilde{o}}]^T$, is denoted $[x \; y]^T$ for reasons of readability. For more detailed derivations on the threat function below, see Jansson [2005] and Nilsson and Ödblom [2010].

Now, consider the constant acceleration maneuvers which successfully avoid a collision at the last possible time instant using steering-only or braking-only inputs, according to Figure 2. The amount of needed acceleration required by the host vehicle to avoid a collision is for these maneuvers described by the *Steer Left/Right Threat Number* (SLTN/SRTN) and the *Brake Threat Number* (BTN), where a threat number > 1 indicate that the corresponding maneuver cannot avoid a collision. F is chosen such that $F > 1$ if none of the considered maneuvers successfully avoid a collision:

$$F(\theta) \triangleq \begin{cases} \min\{BTN, SRTN, SLTN\} & \text{if } \theta \in \Theta_F \\ -\infty & \text{otherwise} \end{cases},$$
$$\Theta_F = \{\theta \in \mathbb{R}^8 | x \geq 0, \dot{x} \leq 0\}. \tag{19}$$

Note that the state and inputs from the system in (17) are the arguments to F.

Definition 11. The STN is defined as

$$STN = \frac{\ddot{y}_{h\tilde{h},req}}{\ddot{y}_{h\tilde{h},max}} = \frac{\ddot{y}_{h\tilde{h}} + \ddot{y} + \frac{2}{t_{tc}^2(} \left(y \pm \frac{w_h + w_o}{2} + \dot{y} t_{tc}\right)}{\pm a_{y,max}} \tag{20}$$

where $\ddot{y}_{h\tilde{h},req}$ is the lateral acceleration required for the host to avoid the collision, $a_{y,max} > 0$ is the maximum available lateral acceleration and t_{tc} is the time-to-collision, obtained from solving

$$x + \dot{x} t_{tc} + \ddot{x} \frac{t_{tc}^2}{2} = 0 \tag{21}$$

The avoidance maneuvers by steering to the left and right are evaluated by two separate threat numbers, $SLTN$ and $SRTN$. The expression for these two are both given by (20) by choosing plus for $SLTN$ or minus for $SRTN$, in the two $\pm$.

Definition 12. The BTN is defined as

$$BTN = \frac{\ddot{x}_{h\tilde{h},req}}{\ddot{x}_{h\tilde{h},max}} = \frac{\ddot{x}_{h\tilde{h}} + \ddot{x} - \frac{\dot{x}^2}{2x}}{-a_{x,max}} \tag{22}$$

where $\ddot{x}_{h\tilde{h},req}$ is the longitudinal acceleration required for the host to avoid the collision and $-a_{x,max} < 0$ represents the maximum available longitudinal deceleration.

6. VERIFICATION

This section demonstrates how to solve the verification and robustness problems formulated in Section 4 using the motion, threat assessment and error models from Section 5. First, the admissible set, i.e. the non-collision set, is defined followed by methods for computing safe and unsafe sets. Next, an approach for verifying the absence of incorrect decisions, in these sets, is presented. Finally, methods for estimating robustness to errors are described.

6.1 Admissible Set

The host vehicle and object are modelled as 2D-polytopes, more specifically rectangles, as defined by Figure 2. Collision between the two is equivalent to the two sets having a non-zero intersection. Under normal operating conditions, it is assumed that the driver of the host vehicle maintains a margin of at least $[x_m \;\; y_m]^T$. In terms of relative coordinates, this is expressed as

$$-(l_h + l_o + x_m) \leq x_{\tilde{h}\tilde{o}} \leq x_m \tag{23a}$$

$$-\left(\frac{w_h + w_o}{2} + y_m\right) \leq y_{\tilde{h}\tilde{o}} \leq \frac{w_h + w_o}{2} + y_m. \tag{23b}$$

These position constraints, describing a collision, define the polytope $\mathcal{R}_{col} \subset \mathbb{R}^2$.

The set of non-admissible states is given by

$$\mathcal{Z}^c_{adm} = \mathcal{R}_{col} \times \mathbb{R}^2. \tag{24}$$

Consequently, the admissible set $\mathcal{Z}_{adm}$ now describe all non-collision states $z \in \mathbb{R}^4$.

6.2 Computing the Safe and Unsafe Sets

The safe, $\mathcal{Z}_{safe}$, and unsafe, $\mathcal{Z}_{unsafe}$, sets from Definitions 6 and 7 may be computed in different ways, by utilizing the complement properties in (10). Both $\mathcal{Z}_{safe}$ and $\mathcal{Z}_{unsafe}$ may be computed either through the minimal reach tube of the non-admissible set, $Pre^{\infty}(\mathcal{Z}^c_{adm})$, or the viability kernel of the admissible set $Viab^{\infty}(\mathcal{Z}_{adm})$.

We choose to compute the minimal reach tubes since the non-admissible set $\mathcal{Z}^c_{adm}$ in (24) is convex, meaning that there exist efficient methods to compute $Pre^{\infty}(\mathcal{Z}^c_{adm})$. Details on such methods are presented in e.g. Kolmanovsky and Gilbert [1998].

6.3 Verification

Consider the optimization problem in (15), given that the inputs are not subjected to measurement errors. A safe set expressed as a union of polytopes, $\mathcal{Z}_{safe} = \bigcup_{i=1}^{n} \mathcal{Z}_{safe,i}$, means that (15) may be decomposed into n optimization problems subject to polytopic, and thus convex, constraints. Depending on the properties of F, a suitable method can be chosen to solve each subproblem.

We briefly outline how to solve (15) for choice of F defined by (19). For details, we refer to Boyd and Vandenberghe [2004]. In (19), F is a minimum of three threat numbers which individually are monotonic when $F \geq 0$, and thus quasilinear. This means that F is quasiconcave and (15) may be formulated as quasiconvex optimization problem. This is solved using bisection, where a convex feasibility problem is solved in each iteration.

6.4 Error Robustness

This section shows how the verification problem in (15) may be solved when the input to the threat function F is subject to errors. As an example, we consider a bounded polytopic error on the state, $\mathcal{Z}_e \subset \mathbb{R}^n$. If $\mathcal{Z}_{safe}$ describes possible safe states, then

$$\tilde{\mathcal{Z}}_{safe} = \mathcal{Z}_{safe} \oplus \mathcal{Z}_e, \tag{25}$$

describes all the corresponding states which may be propagated through F when $z \in \mathcal{Z}_{safe}$.

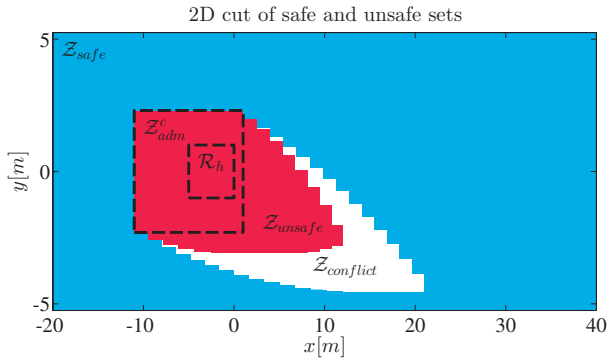

Fig. 3. Computed safe, $\mathcal{Z}_{safe}$, and unsafe, $\mathcal{Z}_{unsafe}$, sets, cut through $\dot{x}_{\tilde{h}\tilde{o}} = -15\,m/s$ and $\dot{y}_{\tilde{h}\tilde{o}} = 3\,m/s$.

Solving (15) for $\tilde{\mathcal{Z}}_{safe}$ now answers the question if F is robust to the error $\mathcal{Z}_e$ in the set $\mathcal{Z}_{safe}$. Note that given a partition of $\mathcal{Z}_{safe}$, this method can be applied individually on each subset.

7. RESULTS

Computational results have been generated using the Model Parametric Toolbox (MPT), Herceg et al. [2013]. The system in (17) is discretized with a sampling time $T_s = 0.1\,s$ and the TA example from Section 5.3 is analyzed using the methods in Section 6. All computations are performed in the full dimensional space for a scenario when the host vehicle is approaching an object. For clarity, all sets are orthogonally cut and visualized only in the position domain.

Figure 3 exemplifies the computed safe and unsafe sets. Note how this implicitly shows the conflict set, which is the set where the future behaviour of the disturbance, i.e. the object, will decide if there will be a collision or not.

The verification problem in (15) is solved for different magnitudes on the error bound, $|e_x|$. This may be interpreted as a varying sensor measurement error, added on the longitudinal position $x_{\tilde{h}\tilde{o}}$, and bounded in magnitude by $|e_x|$. Figure 4 shows the maximum $|e_x|$ for which it can be guaranteed that no unnecessary interventions are initiated in the safe set, i.e. the robustness to these errors.

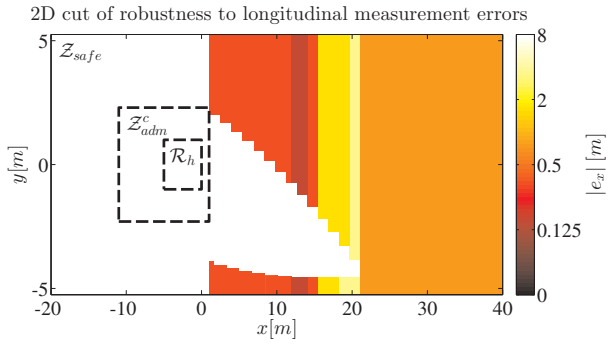

Fig. 4. The robustness to additive errors on longitudinal position, $x_{\tilde{h}\tilde{o}}$, is shown for a cut of $\mathcal{Z}_{safe}$ through $\dot{x}_{\tilde{h}\tilde{o}} = -15\,m/s$ and $\dot{y}_{\tilde{h}\tilde{o}} = 3\,m/s$. The color of each subset indicates the maximum error which does not lead to an incorrect decision to intervene.

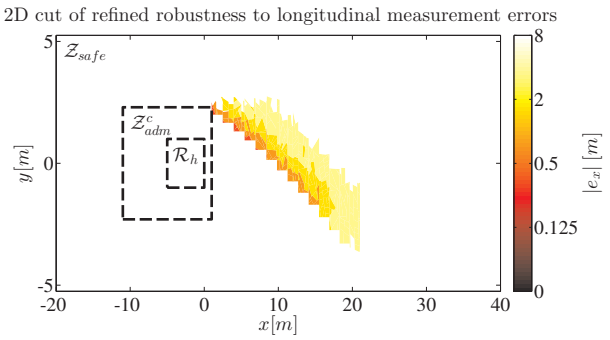

Fig. 5. A refined partition of the robustness to additive errors on longitudinal position, $x_{\tilde{h}\tilde{o}}$, shown for a cut of $\mathcal{Z}_{safe}$ through $\dot{x}_{\tilde{h}\tilde{o}} = -15\,m/s$ and $\dot{y}_{\tilde{h}\tilde{o}} = 3\,m/s$. The color of each subset indicates the maximum error which does not lead to an incorrect decision to intervene.

The minimum robustness for the cut of $\mathcal{Z}_{safe}$ shown in Figure 4, as well as the complete set $\mathcal{Z}_{safe}$, is $0.25\,m$.

The partition of $\mathcal{Z}_{safe}$ in Figure 4 is quite coarse, which is beneficial from a computational point of view but does not clearly pinpoint parts of state space with low robustness. To address this, Figure 5 demonstrates a refined partition, obtained by sequentially splitting the subsets of $\mathcal{Z}_{safe}$ using a heuristic algorithm.

8. CONCLUDING REMARKS

We have presented a framework for formally verifying that a given TA function for collision avoidance makes correct decisions. The method uses reachability analysis and viability theory to define safe and unsafe sets. In these sets, the correctness of decisions and the robustness to errors, for a given TA function, is assessed using optimization techniques.

The method may provide guarantees that no incorrect decisions are made, at any point in the state space of interest. By separating the evaluated TA function from the dynamics of the input state space, it is possible to evaluate non-linear and ad-hoc TA functions. The computed robustness may be used to direct other types of testing towards relevant scenarios.

We remark that the simple dynamical model used in this paper is not valid in all operating conditions. Extending the proposed framework to more complex vehicle dynamics models is part of future work. Also, incorporating a wider variety of error models is an interesting topic.

REFERENCES

Mohammad Ali. *Decision Making and Control for Automotive Safety*. Phd thesis, no 3413, issn 0346-718x, Chalmers University of Technology, Göteborg, Sweden, 2012.

M. Althoff, O. Stursberg, and M. Buss. Model-Based Probabilistic Collision Detection in Autonomous Driving. *IEEE Transactions on Intelligent Transportation Systems*, 10(2):299–310, June 2009.

Matthias Althoff, Daniel Althoff, Dirk Wollherr, and Martin Buss. Safety verification of autonomous vehicles for coordinated evasive maneuvers. *2010 IEEE Intelligent Vehicles Symposium*, pages 1078–1083, June 2010.

Jean-Pierre Aubin, Alexandre M. Bayen, and Patrick Saint-Pierre. *Viability Theory*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2 edition, 2011.

Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, Cambridge, 2004. ISBN 9780511804441.

Pierre Cardaliaguet. Set-valued numerical analysis for optimal control and differential games. In *Stochastic and Differential Games*, pages 177–247. Birkhäuser Boston, 1999.

Erik Coelingh, Henrik Lind, W Birk, and D Wetterberg. Collision Warning with Auto Brake. In *FISITA World Congress*, Yokohama, Japan, 2006.

Martin Distner, Mattias Bengtsson, Tomas Broberg, and Lotta Jakobsson. City Safety - A system addessing rear-end collisions at low speeds. In *Proceedings of the 21st International Technical Conference on the Enhanced Safety of Vehicles (ESV)*, Stuttgart, Germany, 2009.

Paolo Falcone, Mohammad Ali, and J Sjoberg. Predictive threat assessment via reachability analysis and set invariance theory. *IEEE Transactions on Intelligent Transportation Systems*, 12(4):1352–1361, 2011.

Matthias Gerdts and Ilaria Xausa. Avoidance Trajectories Using Reachable Sets and Parametric Sensitivity Analysis. *System Modeling and Optimization*, pages 491–500, 2013.

Martin Herceg, Michal Kvasnica, Colin N Jones, and Manfred Morari. Multi-Parametric Toolbox 3.0. In *the European Control Conference*, pages 502–510, Zurich, Switzerland, 2013.

Jorg Hillenbrand, Andreas M. Spieker, and Kristian Kroschel. A Multilevel Collision Mitigation Approach - Its Situation Assessment, Decision Making, and Performance Tradeoffs. *IEEE Transactions on Intelligent Transportation Systems*, 7(4):528–540, December 2006.

Jonas Jansson. *Collision Avoidance Theory with Application to Automotive Collision Mitigation*. Dissertation no 950, Linköping University, 2005.

Roozbeh Kianfar, Paolo Falcone, and Jonas Fredriksson. Reachability analysis of cooperative adaptive cruise controller. In *IEEE Conference on Intelligent Transportation Systems*, pages 1537–1542, September 2012.

I Kolmanovsky and EG Gilbert. Theory and computation of disturbance invariant sets for discrete-time linear systems. *Mathematical Problems in Engineering*, 1998.

K. Lee and H. Peng. Evaluation of automotive forward collision warning and collision avoidance algorithms. *Vehicle System Dynamics*, 43(10):735–751, October 2005.

IM Mitchell. Comparing forward and backward reachability as tools for safety analysis. In *10th International Workshop, Hybrid systems: computation and control*, pages 428–443, Pisa, Italy, 2007. Springer Berlin Heidelberg.

Jonas Nilsson and Anders C.E. Ödblom. On Worst Case Performance of Collision Avoidance Systems. In *IEEE Intelligent Vehicles Symposium*, pages 1084–1091, San Diego, USA, 2010.

L Yang, JH Yang, E Feron, and V Kulkarni. Development of a performance-based approach for a rear-end collision warning and avoidance system for automobiles. In *IEEE Intelligent Vehicles Symposium*, pages 316–321, 2003.