ICAS 2010
27TH INTERNATIONAL CONGRESS OF THE AERONAUTICAL SCIENCES

FORMAL VERIFICATION OF SAFETY BUFFERS FOR SATE-BASED CONFLICT DETECTION AND RESOLUTION

Heber Herencia-Zapana*, Jean-Baptiste Jeannin, César Muñoz*****
National Institute of Aerospace, USA
****Cornell University, USA***
*****National Aeronautics and Space Administration, USA***

Keywords: *formal verification, safety buffers, tactical conflict detection and resolution*

Abstract

The information provided by global positioning systems is never totally exact, and there are always errors when measuring position and velocity of moving objects such as aircraft. This paper studies the effects of these errors in the actual separation of aircraft in the context of state-based conflict detection and resolution. Assuming that the state information is uncertain but that bounds on the errors are known, this paper provides an analytical definition of a safety buffer and sufficient conditions under which this buffer guarantees that actual conflicts are detected and solved. The results are presented as theorems, which were formally proven using a mechanical theorem prover.

1 Introduction

Advances in global positioning systems and communication technology have enabled new air traffic management concepts where the responsibility for separation is air/ground distributed. One of such concepts is state-based conflict detection and resolution (CD&R), a tactical approach for probing and solving air traffic conflicts that only relies on the state information, i.e., the current position and velocity vectors of the aircraft. Over the last years, several algorithms for state-based CD&R have been proposed [1, 3, 5, 8, 11]. Given the critical role that these systems play in the airspace system, some of these algorithms and concepts [7, 10, 11] have been formally analyzed for safety properties such as *independence*, i.e., minimum separation is guaranteed when one of the aircraft maneuvers, and *implicit coordination*, i.e., minimum separation is guaranteed when both aircraft maneuver with no explicit coordination between them [4]. In general, the verification that a given algorithm satisfies theses safety properties assume that the aircraft state information is accurately known.

The position provided by global navigation satellite systems like GPS is accurate up to a few meters (about 10m).[1] Errors in position and velocity data negatively affect the minimum separation guaranteed by CD&R systems. Therefore, when CD&R algorithms are used in practice, a safety buffer is added to the minimum separation to accommodate for the imprecision in the state information. The size of the safety buffers is usually determined by experimentation and simulation.

This paper presents a formal analysis of the effects of errors in position and velocity information of pairwise state-based CD&R algorithms. Under the assumption that the bounds of position and velocity errors in the state information of the ownship and traffic aircraft are known, this paper rigorously provides answers to questions such as (a) what is the actual minimum separation detected by a CD&R algorithm that assumes per-

[1] See `http://www.kowoma.de/en/gps/errors.htm`.

fect information? and (b) how large has to be the safety buffer to guarantee a given minimum separation when the conflict is resolved by a CD&R algorithm that assumes perfect information? The mathematical development presented in this paper, including formal proofs of all lemmas and theorems,[2] has been mechanically checked using the interactive theorem prover PVS (Prototype Verification System) [12], a higher-order logic based theorem prover developed by SRI International.[3] For readability, this paper uses standard mathematical notation instead of PVS syntax.

2 Basic Definitions

As typical of pairwise state-based CD&R approaches, a 2-dimensional airspace is considered with two distinguished aircraft: the *ownship* and the *intruder* aircraft, which represents a traffic aircraft. Moreover, aircraft dynamics are represented by a point moving at constant linear speed in a 2-dimensional Euclidean space.

2.1 Error Bounds

The ownship's and intruder's *actual* positions are denoted by the vectors $\mathbf{s_o} = (s_{ox}, s_{oy})$ and $\mathbf{s_i} = (s_{ix}, s_{iy})$, respectively. The ownship's and intruder's *actual* velocity vectors are denoted by $\mathbf{v_o} = (v_{ox}, v_{oy})$ and $\mathbf{v_i} = (v_{ix}, v_{iy})$, respectively. Since the actual vectors are unknown to CD&R algorithms, this paper also considers the *measured* position and velocity vectors of each aircraft, which are denoted $\mathbf{s_o^m} = (s^m_{ox}, s^m_{oy})$ and $\mathbf{v_o^m} = (v^m_{ox}, v^m_{oy})$, respectively, for the ownship; and $\mathbf{s_i^m} = (s^m_{ix}, s^m_{iy})$ and $\mathbf{v_i} = (v^m_{ix}, v^m_{iy})$, respectively, for the intruder aircraft. Bounds on the position and velocity errors are assumed to be known, i.e.,

$$\|\mathbf{s_o} - \mathbf{s_o^m}\| \leq \varepsilon_{so}, \tag{1}$$
$$\|\mathbf{s_i} - \mathbf{s_i^m}\| \leq \varepsilon_{si}, \tag{2}$$
$$|track(\mathbf{v_o}) - track(\mathbf{v_o^m})| \leq \varepsilon_{\alpha o}, \tag{3}$$
$$|\|\mathbf{v_o}\| - \|\mathbf{v_o^m}\|| \leq \varepsilon_{go}, \tag{4}$$
$$|track(\mathbf{v_i}) - track(\mathbf{v_i^m})| \leq \varepsilon_{\alpha i}, \tag{5}$$
$$|\|\mathbf{v_i}\| - \|\mathbf{v_i^m}\|| \leq \varepsilon_{gi}, \tag{6}$$

where ε_{so} and ε_{si} are strictly positive constants that denote the position error bounds for the ownship and intruder aircraft, respectively; $\varepsilon_{\alpha o}$ and $\varepsilon_{\alpha i}$ are strictly positive constants that denote the track error bounds for the ownship and intruder aircraft, respectively; and ε_{go} and ε_{gi} are strictly positive constants that denote the ground speed error bounds for the ownship and intruder aircraft, respectively. Furthermore, given a 2-dimensional vector $\mathbf{u}$, the expression $\|\mathbf{u}\|$ denotes the *norm* of $\mathbf{u}$, i.e.,

$$\|\mathbf{u}\| \equiv \sqrt{{u_x}^2 + {u_y}^2},$$

and $track(\mathbf{u})$ denotes the *track angle* of $\mathbf{u}$, i.e., the angle α measured clockwise from the North that satisfies

$$\mathbf{u} = (\|\mathbf{u}\| \sin\alpha, \|\mathbf{u}\| \cos\alpha).$$

Since $\varepsilon_{\alpha o}$, $\varepsilon_{\alpha i}$, ε_{go} and ε_{gi} are measure errors, they are small compared to the measured values. Therefore, the following inequalities are assumed.

$$\begin{aligned} \varepsilon_{\alpha o} &\leq \frac{\pi}{2}, \\ \varepsilon_{go} &\leq \|\mathbf{v_o^m}\|, \\ \|\mathbf{v_o^m}\|\,(1 - \cos\varepsilon_{\alpha o}) &\leq \varepsilon_{go}. \end{aligned} \tag{7}$$

$$\begin{aligned} \varepsilon_{\alpha i} &\leq \frac{\pi}{2}, \\ \varepsilon_{gi} &\leq \|\mathbf{v_i^m}\|, \\ \|\mathbf{v_i^m}\|\,(1 - \cos\varepsilon_{\alpha i}) &\leq \varepsilon_{gi}. \end{aligned} \tag{8}$$

2.2 Aircraft Separation

In a 2-dimensional airspace, the separation criterion for two aircraft is specified as a minimum

[2] For technical details on the proofs of the properties enounced in this paper, the reader is referred to the PVS development available at `http://shemesh.larc.nasa.gov/people/cam/ACCoRD`.

[3] PVS is electronically available at `http://pvs.csl.sri.com`.

horizontal separation D. A conflict between the ownship and the intruder occurs when there is a time within a lookahead time T such that the distance between the aircraft is less than D. Typically D is 5 nautical miles and T is 5 minutes. Formally, the ownship and the intruder aircraft are in conflict if there exists $0 \leq t \leq T$ such that at time t the following inequality holds

$$\|(\mathbf{s_o} + t\ \mathbf{v_o}) - (\mathbf{s_i} + t\ \mathbf{v_i})\| < D.$$

Since $(\mathbf{s_o} + t\ \mathbf{v_o}) - (\mathbf{s_i} + t\ \mathbf{v_i}) = (\mathbf{s_o} - \mathbf{s_i}) + t\ (\mathbf{v_o} - \mathbf{v_i})$, the predicate that characterizes conflict can be defined on $\mathbf{s} = \mathbf{s_o} - \mathbf{s_i}$ and $\mathbf{v} = \mathbf{v_o} - \mathbf{v_i}$, i.e., the relative position and velocity vector, respectively, of the ownship with respect to the intruder. That is, conflict can be viewed as a predicate on two vectors $\mathbf{s}$ and $\mathbf{v}$ rather than a predicate on four vectors $\mathbf{s_o}$, $\mathbf{v_o}$, $\mathbf{s_i}$, and $\mathbf{v_i}$. Thus, the predicate *conflict?* is defined as follows.

$$\begin{aligned} &\mathit{conflict?}(D, T, \mathbf{s}, \mathbf{v}) \equiv \\ &\qquad \exists\, 0 \leq t \leq T : \|\mathbf{s} + t\ \mathbf{v}\| < D. \end{aligned} \tag{9}$$

Since it greatly simplifies the notation, position and velocity will usually be given in the relative framework where the intruder is fix at the origin of the coordinate system and the ownship is moving relative to the intruder. In this relative view, $\mathbf{s}^m$ and $\mathbf{v}^m$ will denote the measured relative position and velocity vectors $\mathbf{s_o^m} - \mathbf{s_i^m}$ and $\mathbf{v_o^m} - \mathbf{v_i^m}$, respectively.

Graphically, the separation criterion can be understood as an imaginary circular area of diameter D around each aircraft and a conflict between two aircraft as a predicted overlapping of these areas. In the alternative but equivalent relative view, only the intruder is surrounded by a circle, called the *protected zone*, of radius D. From this perspective, a conflict between these two aircraft is equivalent to the existence of a time $0 \leq t \leq T$ at which the ownship is in the interior of the intruder's protected zone. For example in the left side of Figure 1, the upper point represents the ownship with its velocity vector and its avoidance area (circle of diameter D around the aircraft). The lower point represents the traffic aircraft. The right side represents the same information in the translated coordinate system. The two aircraft are potentially in conflict because the half-line defined by the relative velocity vector $\mathbf{v}$ intersects the protected area around the traffic aircraft.

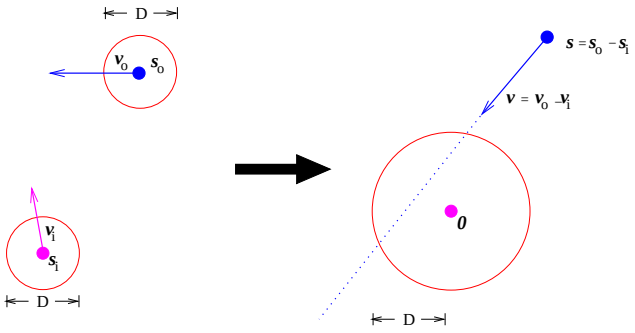

Fig. 1 Translated Coordinate System

2.3 Conflict Detection and Resolution Algorithms

A *conflict detection* algorithm `cd` is a function that takes as parameters D, T, and the measured position and velocity vectors of the aircraft, i.e., $\mathbf{s_o^m}$, $\mathbf{v_o^m}$, $\mathbf{s_i^m}$, $\mathbf{v_i^m}$. It returns a Boolean value such that $CD(D, T, \mathbf{s_o^m}, \mathbf{v_o^m}, \mathbf{s_i^m}, \mathbf{v_i^m}) = \texttt{true}$ if and only if

$$\mathit{conflict?}(D, T, \mathbf{s_o^m} - \mathbf{s_i^m}, \mathbf{v_o^m} - \mathbf{v_i^m}),$$

i.e., it returns `true` if there is a conflict assuming perfect state information.

A *conflict resolution* algorithm `cr` is a function that takes as parameters D, T, and the measured position and velocity vectors of the aircraft, i.e., $\mathbf{s_o^m}$, $\mathbf{v_o^m}$, $\mathbf{s_i^m}$, $\mathbf{v_i^m}$. It returns a set of velocity vectors $\mathbf{w_o^m}$ that, if implemented by the ownship in zero time, solves any impending conflict assuming perfect state information, i.e.,

$$\neg \mathit{conflict?}(D, T, \mathbf{s_o^m} - \mathbf{s_i^m}, \mathbf{w_o^m} - \mathbf{v_i^m}).$$

In this paper, these algorithms are abstract, i.e., no particular implementation of `cd` and `cr` are considered. In other words, the results that have been obtained hold for any state-based CD&R algorithm that correctly implement the specifications above such as those in KB3D [3] and NASA's ACCoRD [11].

This paper provides the mathematical definition of a safety buffer ψ that satisfies the following properties:

1. $\mathtt{cd}(D+\psi, T, \mathbf{s_o^m}, \mathbf{v_o^m}, \mathbf{s_i^m}, \mathbf{v_i^m}) = \mathtt{false}$ implies

$$\neg \mathit{conflict?}(D, T, \mathbf{s_o} - \mathbf{s_i}, \mathbf{v_o} - \mathbf{v_i}).$$

2. $\mathbf{w_o^m} \in \mathtt{cr}(D+\psi, T, \mathbf{s_o^m}, \mathbf{v_o^m}, \mathbf{s_i^m}, \mathbf{v_i^m})$ implies

$$\neg \mathit{conflict?}(D, T, \mathbf{s_o} - \mathbf{s_i}, \mathbf{w_o^m} - \mathbf{v_i}).$$

The first property states that a conflict detection algorithm that uses a protected zone extended by ψ has no missed-alerts. The second property states that a conflict resolution algorithm that uses a protected zone extended by ψ returns resolution maneuvers that guarantee an actual minimum separation D. The safety buffer ψ is an upper bound on the error in the minimum separation incurred by CD&R algorithms that assume precise aircraft state information.

3 Relative Position and Velocity Errors

By simple algebraic manipulations and triangular inequality

$$\begin{aligned}\|\mathbf{s} - \mathbf{s}^m\| &= \|(\mathbf{s_o} - \mathbf{s_i}) - (\mathbf{s_o^m} - \mathbf{s_i^m})\| \\ &= \|(\mathbf{s_o} - \mathbf{s_o^m}) + (\mathbf{s_i} - \mathbf{s_i^m})\| \\ &\leq \|\mathbf{s_o} - \mathbf{s_o^m}\| + \|\mathbf{s_i} - \mathbf{s_i^m}\| \\ &\leq \varepsilon_{so} + \varepsilon_{si}.\end{aligned}$$

Therefore, the relative position error is bounded by $\varepsilon_{so} + \varepsilon_{si}$.

Theorem 1 (Relative Position Error) *Let* $\mathbf{s_o}$, $\mathbf{s_i}$, $\mathbf{s_o^m}$, $\mathbf{s_i^m}$, ε_{so}, *and* ε_{si} *be such that they satisfy formulas (1) and (2). The relative position error is bounded by a circle of radius*

$$\varepsilon_s \equiv \varepsilon_{so} + \varepsilon_{si}, \tag{10}$$

i.e., $\|\mathbf{s} - \mathbf{s}^m\| \leq \varepsilon_s$. *Moreover,* $\varepsilon_s > 0$.

Velocity errors are given in terms of track error bounds, $\varepsilon_{\alpha o}$ for the ownship and $\varepsilon_{\alpha i}$ for the intruder, and ground speed error bounds, ε_{go} for the ownship and ε_{gi} for the intruder. However, as illustrated by Figure 2, velocity errors are also bounded by a circle. In the case of the ownship, the velocity error bound ε_{vo} is defined from $\varepsilon_{\alpha o}$ and ε_{go} as follows.

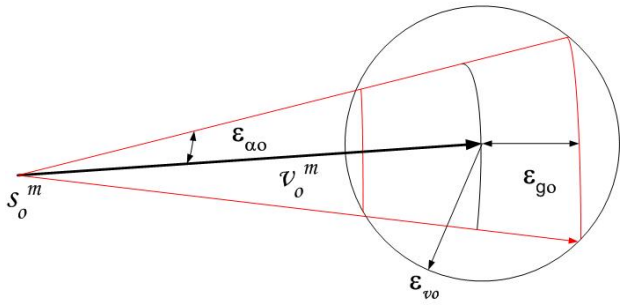

Fig. 2 Ownship Velocity Error Bounds

$$\varepsilon_{vo} \equiv \sqrt{2\|\mathbf{v_o^m}\|(\|\mathbf{v_o^m}\| + \varepsilon_{go})(1 - \cos\varepsilon_{\alpha o}) + \varepsilon_{go}{}^2}. \tag{11}$$

Similarly, the velocity error bound for the intruder ε_{vi} is defined from $\varepsilon_{\alpha i}$ and ε_{gi} as follows.

$$\varepsilon_{vi} \equiv \sqrt{2\|\mathbf{v_i^m}\|(\|\mathbf{v_i^m}\| + \varepsilon_{gi})(1 - \cos\varepsilon_{\alpha i}) + \varepsilon_{gi}{}^2}.$$

The following lemma states that ε_{vo} and ε_{vi} are indeed bounds on the velocity errors of the ownship and intruder aircraft, respectively.

Lemma 3.1 *Let* $\mathbf{v_o}$, $\mathbf{v_i}$, $\mathbf{v_o^m}$, $\mathbf{v_i^m}$, $\varepsilon_{\alpha o}$, ε_{go}, $\varepsilon_{\alpha i}$, *and* ε_{gi} *be such that they satisfy formulas (3)–(8). It holds that*

$$\begin{aligned}\|\mathbf{v_o} - \mathbf{v_o^m}\|^2 &\leq \varepsilon_{vo}^2, \\ \|\mathbf{v_i} - \mathbf{v_i^m}\|^2 &\leq \varepsilon_{vi}^2.\end{aligned}$$

Lemma 3.1 is used to estimate the relative velocity error as shown by the next theorem.

Theorem 2 (Relative Velocity Error) *Let* $\mathbf{v_o}$, $\mathbf{v_i}$, $\mathbf{v_o^m}$, $\mathbf{v_i^m}$, $\varepsilon_{\alpha o}$, ε_{go}, $\varepsilon_{\alpha i}$, *and* ε_{gi} *be such that they satisfy formulas (3)–(8). The relative velocity error is bounded by a circle of radius*

$$\varepsilon_v \equiv \varepsilon_{vo} + \varepsilon_{vi}, \tag{12}$$

i.e., $\|\mathbf{v} - \mathbf{v}^m\| \leq \varepsilon_v$. *Moreover* $\varepsilon_v > 0$.

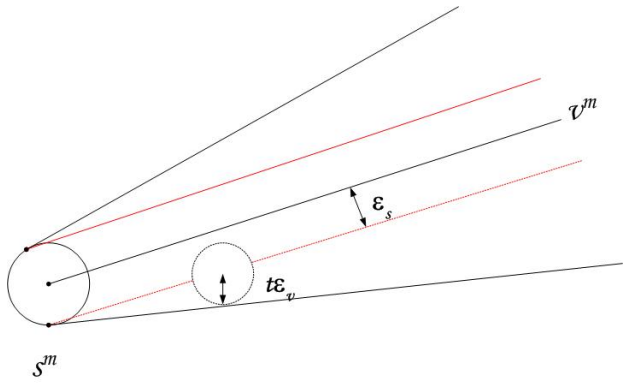

Fig. 3 Cone of Possible Trajectories

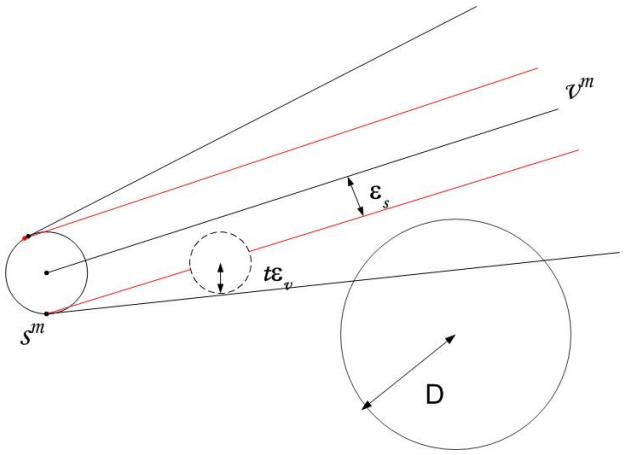

Fig. 4 Missed-alerts

In the relative coordinate system, the position and velocity error bounds ε_s and ε_v define a cone in the airspace that contains all possible linear trajectories around the measured position and velocity vectors $\mathbf{s}^m$ and $\mathbf{v}^m$. This cone is illustrated by Figure 3.

4 Conflict Detection and Resolution Under Uncertainty

To accommodate for the difference between the actual aircraft states and the measured ones, state-based CD&R algorithms are typically used with a protected zone extended by a safety buffer. This section provides analytical formulas to compute a safety buffer for state-based conflict detection and resolution algorithms that guarantees no missed-alerts and an actual minimum separation D.

4.1 Conflict Detection

Because of position and velocity uncertainties, $\mathit{conflict?}(D,T,\mathbf{s},\mathbf{v})$ does not necessary imply $\mathit{conflict?}(D,T,\mathbf{s}^m,\mathbf{v}^m)$. For instance, Figure 4 illustrates situations where the actual position and velocity vectors $\mathbf{s}$ and $\mathbf{v}$ may lead to a conflict, but that conflict is not detected with the measured state information $\mathbf{s}^m$ and $\mathbf{v}^m$.

The following theorem provides the definition of a safety buffer ψ that guarantees that a state-based conflict detection algorithm has no missed-alerts.

Theorem 3 (Conflict Detection) *Let* $\mathbf{s_o}$, $\mathbf{v_o}$, $\mathbf{s_i}$, $\mathbf{v_i}$, $\mathbf{s_o^m}$, $\mathbf{v_o^m}$, $\mathbf{s_i^m}$, $\mathbf{v_i^m}$, ε_{so}, ε_{si}, $\varepsilon_{\alpha o}$, ε_{go}, $\varepsilon_{\alpha i}$, *and* ε_{gi} *be such that they satisfy formulas (1)–(8). If*

$$cd(D+\psi,T,\mathbf{s_o^m},\mathbf{v_o^m},\mathbf{s_i^m},\mathbf{v_i^m}) = \mathit{false},$$

then

$$\neg \mathit{conflict?}(D,T,\mathbf{s_o}-\mathbf{s_i},\mathbf{v_o}-\mathbf{v_i}),$$

where

$$\tau \equiv \min(T, \frac{(\|\mathbf{s}^m\|+\varepsilon_s)(\|\mathbf{v}^m\|+\varepsilon_v)}{(\|\mathbf{v}^m\|-\varepsilon_v)^2})$$
$$\psi \equiv \varepsilon_s + \tau\,\varepsilon_v,$$

and $\varepsilon_s, \varepsilon_v$ *are defined as in theorems 1 and 2, respectively.*

4.2 Conflict Resolution

In a similar way to conflict detection algorithms, state-based conflict resolution algorithms that assume precise aircraft state information may return resolution maneuvers that do not keep the aircraft separated.

The conflict detection safety buffer ψ can also be used with conflict resolution algorithms to compute resolution maneuvers that keep aircraft separated (assuming that the resolution maneuvers are implemented in zero-time by the ownship). Indeed, let $\mathbf{w_o^m}$ be a resolution maneuver for the ownship computed by `cr`, i.e.,

$$\mathbf{w_o^m} \in \mathtt{cr}(D+\psi,T,\mathbf{s_o^m},\mathbf{v_o^m},\mathbf{s_i^m},\mathbf{v_i^m}).$$

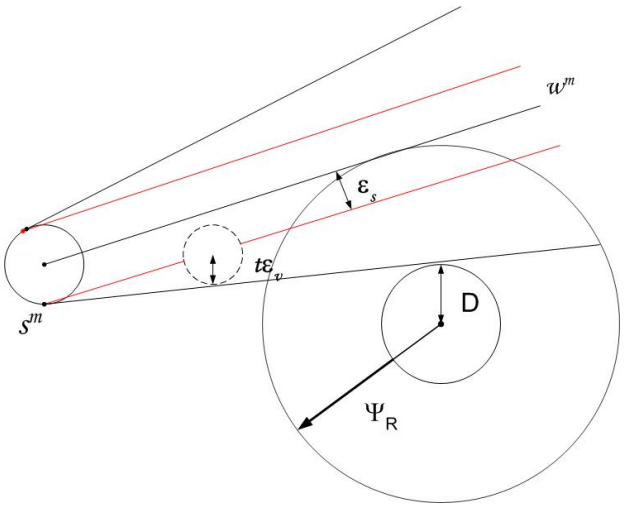

Fig. 5 Conflict Resolution Under Uncertainty

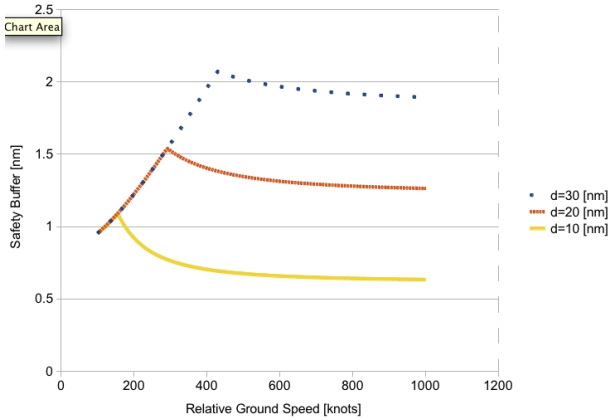

Fig. 6 Relative Ground Speed vs. Safety Buffer

By definition of `cr`,

$$\neg \mathit{conflict?}(D+\psi, T, \mathbf{s_o^m} - \mathbf{s_i^m}, \mathbf{w_o^m} - \mathbf{v_i^m}).$$

Thus, by definition of `cd`,

$$\texttt{cd}(D+\psi, T, \mathbf{s_o^m}, \mathbf{w_o^m}, \mathbf{s_i^m}, \mathbf{v_i^m}) = \texttt{false}.$$

By Theorem 3,

$$\neg \mathit{conflict?}(D, T, \mathbf{s_o} - \mathbf{s_i}, \mathbf{w_o^m} - \mathbf{v_i}).$$

Theorem 4 (Conflict Resolution) *Let* $\mathbf{s_o}$, $\mathbf{v_o}$, $\mathbf{s_i}$, $\mathbf{v_i}$, $\mathbf{s_o^m}$, $\mathbf{v_o^m}$, $\mathbf{s_i^m}$, $\mathbf{v_i^m}$, ε_{so}, ε_{si}, $\varepsilon_{\alpha o}$, ε_{go}, $\varepsilon_{\alpha i}$, *and* ε_{gi} *be such that they satisfy formulas (1)–(8). If*

$$\mathbf{w_o^m} \in \mathit{cr}(D+\psi, T, \mathbf{s_o^m}, \mathbf{v_o^m}, \mathbf{s_i^m}, \mathbf{v_i^m}),$$

then

$$\neg \mathit{conflict?}(D, T, \mathbf{s_o} - \mathbf{s_i}, \mathbf{w_o^m} - \mathbf{v_i}).$$

Figure 5 illustrates Theorem 4, where the relative vector $\mathbf{w}^m$, which denotes $\mathbf{w_o^m} - \mathbf{v_i^m}$, is assumed to be tangent to the extended protected zone.

5 Numerical Examples

Assume the following error bound values:

- $\varepsilon_{so} = \varepsilon_{si} = 10$ feet.
- $\varepsilon_{\alpha o} = \varepsilon_{\alpha i} = 3$ degrees.
- $\varepsilon_{go} = \varepsilon_{gi} = 5$ knots.

These values are used as indicators and do not represent actual error values of a global positioning system such as GPS.

Figure 6 plots relative ground speed, i.e., $\|\mathbf{v}^m\|$ in knots, against the corresponding safety buffer, i.e., ψ in nautical miles, for 3 different distances $d = \|\mathbf{s}^m\|$ between the aircraft: 10 nautical miles, 20 nautical miles, and 30 nautical miles. The value of ψ depends on the minimum between the lookahead time T and the time of minimum approach between the aircraft. When the aircraft are far away, the value of T dominates the expression and the size of the buffer increases as the relative ground speed increases. Eventually, the time of minimum approach dominates the expression and from that point on the size of the buffer decreases as the relative ground speed increases.

Figure 7 and 8 use a fixed relative ground speed of 400 knots. Figure 7 shows that the safety buffer increases as the track error varies from 1^o to 5^o, assuming that the ground speed error bound is 5 knots. Similarly, Figure 8 shows that the safety buffer increases as the ground speed error varies from 1 knot to 5 knots, assuming that the track error bound is 3 degrees. Not surprisingly, the track error has a greater impact on the value of

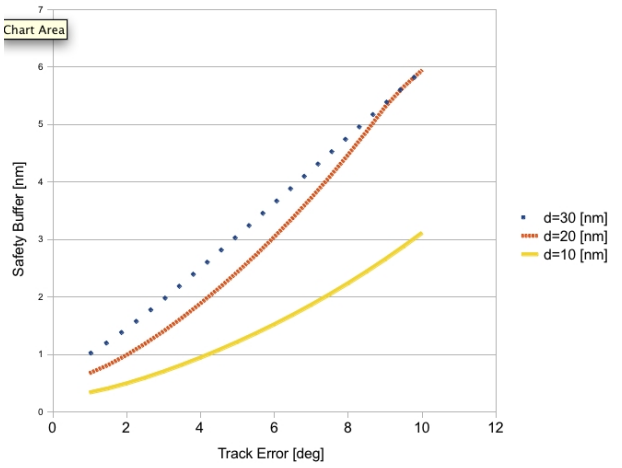

Fig. 7 Track Error vs. Safety Buffer

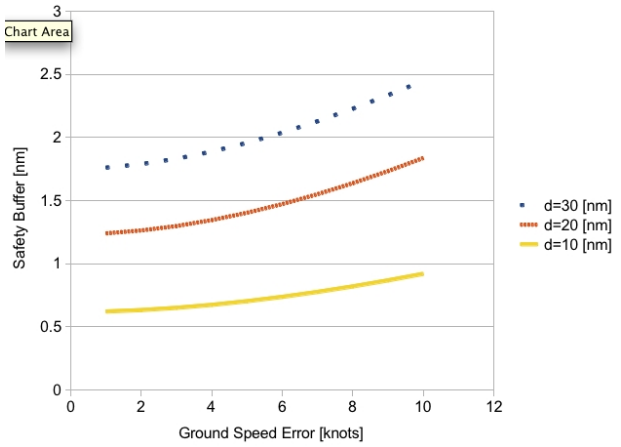

Fig. 8 Ground Speed Error vs. Safety Buffer

ψ than the ground speed error. Indeed, the track error bound determines the span of the cone of possible trajectories depicted in Figure 3.

6 Related Work and Conclusion

In [13], Zhao presents a semi-analytical approach to determine appropriate separation minima between aircraft that takes into consideration wake-vortices and flight technical errors. The paper defines the uncertainty region as the difference between the measure and actual trajectories in an interval of time. The uncertainty region is an ellipsoid and the interval time is the maximum between the surveillance interval and the time needed for conflict avoidance. The paper does not study the effect of uncertainty regions on the conflict detection and resolution logic. In [2], Consiglio et al. measured the impact of wind prediction to determine the additional safety buffer needed to preserve separation. The study is based on high-fidelity simulation. Erzberger et al. [6] propose a conflict detection algorithm that uses stochastic analysis on predicted trajectory errors for estimating the probability of conflict as a function of the state information. In the context of strategic conflict detection, Karr [9] describes different types of prediction error and proposes an algorithm to detect conflicts between trajectories that uses a notion of dynamic safety buffers.

The focus of this paper is the analytical definition of a safety buffer for state-based conflict detection and resolution algorithms assuming that the position and velocity errors are unknown but bounded. The approach presented here can be seen as a worst-case analysis and may be used as a base-line for more precise calculations that take into account aircraft performance, different type of trajectory errors, and intent information.

Last, but not least, it is emphasized that the mathematical development presented in this paper has been mechanically checked in a theorem prover. Given the critical nature that CD&R systems play in the next generation of air traffic systems, this verification step provides additional correctness evidence to the safety case of these systems.

References

[1] K. Bilimoria. A geometric optimization approach to aircraft conflict resolution. In *Guidance, Navigation, and Control Conference*, volume AIAA 2000-4265, Denver, CO, August 2000.

[2] Maria Consiglio, Sherwood Hoadley, and B. Danette Allen. Estimation of separation buffers for wind-prediction error in an airborne

separation assistance system. In *Proceedings of the 8th USA/Europe Air Traffic Management R&DSeminar, ATM 2009*, Napa, California, June–July 2009.

[3] G. Dowek, A. Geser, and C. Muñoz. Tactical conflict detection and resolution in a 3-D airspace. In *Proceedings of the 4th USA/Europe Air Traffic Management R&DSeminar, ATM 2001*, Santa Fe, New Mexico, 2001. A long version appears as report NASA/CR-2001-210853 ICASE Report No. 2001-7.

[4] G. Dowek and C. Muñoz. Conflict detection and resolution for 1,2,...N aircraft. In *6th AIAA Aviation Technology, Integration and Operations Conference (ATIO)*, Belfast, Northern Ireland, September 2007.

[5] M. Eby. A self-organizational approach for resolving air traffic conflicts. *Lincoln Laboratory Journal*, 7(2):239–254, 1994.

[6] Heinz Erzberger, Russell A. Paielli, Douglas R. Isaacson, and Michelle M. Eshowl. Conflict detection and resolution in the presence of prediction error. In *Proceedings of the 1st USA/Europe Air Traffic Management R&DSeminar, ATM 1997*, Saclay, France, June 1997.

[7] A. Galdino, C. Muñoz, and M. Ayala. Formal verification of an optimal air traffic conflict resolution and recovery algorithm. In *Proceedings of the 14th Workshop on Logic, Language, Information and Computation*, Rio de Janeiro, Brazil, July 2007.

[8] J. Hoekstra, R. Ruigrok, R. van Gent, J. Visser, B. Gijsbers, M. Valenti, W. Heesbeen, B. Hilburn, J. Groeneweg, and F. Bussink. Overview of NLR free flight project 1997-1999. Technical Report NLR-CR-2000-227, National Aerospace Laboratory (NLR), May 2000.

[9] David Karr. Conflict detection with dynamic buffers. Technical report, Titan corporation, May 2005.

[10] J. Maddalon, R. Butler, A. Geser, and C. Muñoz. Formal verification of a conflict resolution and recovery algorithm. Technical Report NASA/TP-2004-213015, NASA Langley Research Center, NASA LaRC,Hampton VA 23681-2199, USA, April 2004.

[11] C. Muñoz, A. Narkawicz, R. Butler, and G. Dowek. Mathematical framework for the design and verification of state-based separation assurance algorithms. Manuscript.

[12] S. Owre, J. Rushby, and N. Shankar. PVS: A prototype verification system. In Deepak Kapur, editor, *11th International Conference on Automated Deduction (CADE)*, volume 607 of *Lecture Notes in Artificial Intelligence*, pages 748–752, Saratoga, NY, June 1992. Springer-Verlag.

[13] Yiyuan J. Zhao. A systematic procedure for determining separation minima. In *Proceedings of 26th International Congress of the Aeronautical Sciences, ICAS 2006*, Hamburg, Germany, September 2006.