Formal Verification of Lateral and Temporal Safety Buffers for State-Based Conflict Detection

Anthony Narkawicz[*] César Muñoz[†] Heber Herencia-Zapana[‡]
George Hagen[§]

Abstract

This paper presents an analytical definition of lateral and temporal safety buffers to be used in state-based conflict detection algorithms. A lateral buffer is a distance to be added to the minimum lateral separation to accommodate for uncertainty in the surveillance information. A temporal buffer is a time to be added to the lookahead conflict detection time to accommodate for dropped surveillance messages due to signal attenuation. These safety buffers are defined using precise mathematical statements and the main theorems give numerical upper bounds on the probability of a missed alert. A particular case is considered where absolute bounds on the errors in position and velocity information are known. In this case, under well defined assumptions provided in the paper, safety buffers are given that guarantee mathematically that the probability of a missed alert is zero. The results are presented as theorems, which were formally proven using a mechanical theorem prover.

[*] anthony.narkawicz@nasa.gov, NASA Langley Research Center, Hampton, VA 23681, USA.

[†] cesar.munoz@nasa.gov, NASA Langley Research Center, Hampton, VA 23681, USA.

[‡] heber.herencia-zapana@nianet.org, National Institute of Aerospace, Hampton, VA 23666, USA. For this author, this work was supported by the National Aeronautics and Space Administration under NASA Cooperative Agreement NCC-1-02043.

[§] george.hagen@nasa.gov, NASA Langley Research Center, Hampton, VA 23681, USA.

Table of Acronyms and Symbols

ACCoRD	Airborne Coordinated Conflict Resolution and Detection
ADS-B	Automatic Dependent Surveillance-Broadcast
CD&R	Conflict Detection and Resolution
DO-242A	Minimum Operational Performance Standards for ADS-B
GPS	Global Positioning System
NACp	Navigation Accuracy Category for position
NACv	Navigation Accuracy Category for velocity
PVS	Prototype Verification System

α	Time interval between consecutive ADS-B broadcasts
$\mathcal{A}$	Random variable representing number of dropped ADS-B messages
D	Minimum horizontal distance
$\varepsilon_{\alpha o}$,$\varepsilon_{\alpha i}$	Upper bounds on track errors (ownship and intruder)
ε_{go},ε_{gi}	Upper bounds on ground speed errors (ownship and intruder)
ε_{so},ε_{si}	Upper bounds on position errors (ownship and intruder)
ε_{vo},ε_{vi}	Upper bounds on velocity errors (ownship and intruder)
η	Probability that a sent ADS-B message will be received
λ	Temporal safety buffer
$\mathbf{s}$,$\mathbf{v}$	Relative actual aircraft state (position and velocity vector)
$\mathbf{s}^m$,$\mathbf{v}^m$	Relative reported aircraft state (position and velocity vector)
$\mathbf{s}_o$,$\mathbf{v}_o$	Actual ownship state (position and velocity vector)
$\mathbf{s_o}^m$,$\mathbf{v_o}^m$	Reported ownship state (position and velocity vector)
$\mathbf{s}_i$,$\mathbf{v}_i$	Actual intruder state (position and velocity vector)
$\mathbf{s_i}^m$,$\mathbf{v_i}^m$	Reported intruder state (position and velocity vector)
t	Time variable
T	Lookahead time
ψ	Lateral safety buffer

1 Introduction

Conflict Detection and Resolution (CD&R) in Air Traffic Managament systems has been an area of active research since the last decade. In 2000, Kuchar and Yang [15] presented a taxonomy of conflict detection and resolution modeling methods that surveyed 68 different algorithms. One category in that taxonomy concerns the state propagation method. Probabilistic CD&R approaches use stochastic methods on predicted trajectory errors for estimating the probability of conflict or collision [2, 19–21]. These methods are generally used in ground systems as they are often computationally intensive.

Advances in global positioning systems and communication technology enable air traffic concepts to be considered where the aircraft separation requirement relies on airborne computer-based conflict detection and resolution (CD&R) systems. In some of these concepts, the conflict management functionality is structured in several layers [25]. In the upper layers, strategic CD&R systems provide advanced separation assurance functionality that takes into account long lookahead times, flight plans, special airspace restrictions, winds, and weather [14]. The lower layers typically deal with tactical decisions for short lookahead times. Since the lower layers provide the last line of defense in a multi-layered concept, tactical CD&R systems are considerably simpler and more efficient than strategic systems.

State-based CD&R algorithms [1, 6, 8, 12, 17] probe and solve conflicts by only using aircraft state information, i.e., the current position and velocity vectors of the aircraft, and a nominal point-mass model of aircraft trajectories. These assumptions allow for efficient implementations that rely on analytical methods. To accomodate for the difference between the actual aircraft trajectories and the predicted straight line trajectories used by these methods, it is generally assumed that state-based CD&R algorithms are frequently executed. Typically, state-based CD&R systems that are used in airborne concepts [12] are executed in each aircraft as frequently as position and surveillance information is updated, e.g., 1 Hz.

Given the safety-critical nature of tactical separation assurance systems, some state-based CD&R algorithms [6, 9, 16, 17] 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 [7]. These safety properties highly depend on the assumption that aircraft state information is accurately known.

The position provided by global navigation satellite systems like Global Positioning System (GPS) is accurate up to about ten meters[1] and surveillance information systems such as Automatic Dependent Surveillance-Broadcast (ADS-B) lose messages due to signal attenuation [24]. Errors in position and velocity negatively affect the safety performance of state-based CD&R systems. To mitigate these effects, state-based CD&R algorithms are used with safety buffers that ensure that the probability of a missed alert is low. This paper concerns lateral and temporal safety buffers for conflict detection algorithms. A lateral safety buffer increases the minimum lateral separation distance between aircraft to accomodate for uncertainty in surveillance information. A temporal safety buffer increases the lookahead time used in conflict detection logics. These safety buffers decrease the number of missed alerts but increase the number of false alerts.

Although related, safety buffers for conflict detection algorithms are not the same as safety buffers for conflict resolution algorithms. In particular, a precise formulation of safety buffers for conflict resolutions algorithms needs to take into account the effect of uncertainty on the resolution maneuvers. This paper only considers the problem of estimating guaranteed safety buffers for conflict detection algorithms. A preliminary work on safety buffers for conflict resolution algorithms is presented in [11].

Usually, appropriate values for safety buffers are determined by experimentation and simulation. Gazit and Powell propose in [10] a separation standard based on the probability distribution functions of GPS and radar errors. In [26], Zhao presents a semi-analytical approach to determine appropriate separation minima between aircraft that takes into con-

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

sideration wake-vortices and flight technical errors. That paper defines the uncertainty region as the difference between the measured 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. In [4], 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. In the context of strategic conflict detection, Karr [13] describes different types of prediction error and proposes an algorithm to detect conflicts between trajectories that uses a notion of dynamic safety buffers.

This paper presents a formal development of lateral and temporal safety buffers for conflict detection algorithms. The following assumptions are made throughout the paper.

- Aircraft are assumed not to change velocity during the lookahead time.
- Subsequent dropped ADS-B messages are independent events.

Specific formulas are given for these safety buffers, and a theorem is stated that represents a proved result that these formulas are correct and therefore satisfy a key probabilistic property. Section 2 contains formal definitions related to conflict detection algorithms. Section 3 models GPS and ADS-B errors with random variables on an arbitrary probability space. It is proved in that section that given random variables for positions and velocities, conflict between aircraft is also a random variable. Section 4 gives specific formulas for safety buffers for distance and time that can be used to provide upper bounds on the probability that a conflict detection algorithm will incorrectly miss a conflict. These formulas are then used to give safety buffers that guarantee that there are no missed conflicts, in the case where absolute bounds are known on position and velocity vectors for two aircraft and the probability of a given ADS-B message being dropped is zero. Finally, Section 5 presents a table that contains specific upper bounds on the probability that a correct conflict detection algorithm will miss a given conflict. This table depends on the document DO-242A [24], which specifies several system performance confidence-levels that are to be included in ADS-B messages detailing how precise and trusted the contained state information is.

The mathematical development presented in this paper has been specified and formally verified in the Prototype Verification System (PVS) [18].[2] PVS is a proof assistant that consists of a specification language, based on classical higher-order logic, and a mechanical theorem prover for this logic. The PVS specification language allows for the precise definition of mathematical objects such as *functions* and *relations*, and the precise statement of logical formulas such as *lemmas* and *theorems*. Proofs of logical formulas can be mechanically checked using the PVS theorem prover, which guarantees that every proof step is correct and that all possible cases of a proof are covered. All lemmas and theorems presented in this paper have been mechanically checked in PVS. For the sake of simplicity, only proof sketches of the main results are presented in the paper. The development presented here, including all definitions and formal proofs, is part of the Airborne Coordinated Conflict Detection and Resolution (ACCoRD) framework [17].

[2] Note to the reviewers: the formal mathematical development has been included as part of the submitted work and is available through the editor of the journal.

One of the advantages to mathematical derivations of properties is that it helps to identify those assumptions needed for a result to be true. It is often possible, when examining the derivation of a mathematical property, to note points where explicit assumptions are used and to record a list of those assumptions. In fact, a mechanical theorem prover such as PVS is much more powerful at recording the assumptions needed for a mathematical result. In fact, if a statement can be proved correct in a mechanical theorem prover, then each and every assumption needed can be explicitly read from the statement itself. Thus, if a result is proved correct in such a theorem prover, then it is absolutely correct in a mathematical sense and no further assumptions are needed.

The use of a formal language, e.g., in this case the specification language of PVS, enforces rigorous definitions of mathematical objects, where all dependencies are clearly specified. This level of rigor guarantees a very high confidence on the correctness of the results presented in this paper. However, this also makes the notation heavy and difficult to read for the non-expert reader. For this reason, the work presented here uses standard mathematical notation and does not assume that the reader is familiar with the syntax or semantics of the PVS language.

2 State-Based Conflict Detection

Pairwise state-based conflict detection systems use the state information of two aircraft, which here are referred to as the *ownship* and the *intruder*, to detect conflicts between them. The state information for an aircraft includes its current position and velocity, and these are represented by points and vectors in a Cartesian coordinate system. Since this paper focuses on lateral separation, it considers the two-dimensional space $\mathbb{R}^2$. It is noted, however, that the results presented in this paper hold in the three-dimensional airspace as well. That is, the lateral safety buffers presented in this paper can be safely used by 3D conflict detection algorithms.

Aircraft trajectories are represented by a point moving at constant linear speed. The vectors $\mathbf{s}_o, \mathbf{v}_o, \mathbf{s}_i$, and $\mathbf{v}_i$ will be used to represent the ownship's current position and velocity and the intruder's current position and velocity (at time $t = 0$), respectively. Thus, the predicted states of the ownship and the intruder at time t are given by $\mathbf{s}_o + t\,\mathbf{v}_o$ and $\mathbf{s}_i + t\,\mathbf{v}_i$, respectively. In later sections, $\mathbf{s}_o, \mathbf{v}_o, \mathbf{s}_i$, and $\mathbf{v}_i$ denote random variables with values in $\mathbb{R}^2$ to account for uncertainty in these vectors.

Under nominal operations, aircraft are required to maintain a certain separation. In the two-dimensional airspace, the separation requirement is specified by a minimum horizontal distance D. A predicted *conflict* between the ownship and the intruder aircraft occurs when there is a time $t \in [0, T]$ at which the predicted horizontal distance between the aircraft is projected to be less than D, i.e.,

$$\|(\mathbf{s}_o + t\,\mathbf{v}_o) - (\mathbf{s}_i + t\,\mathbf{v}_i)\| < D.$$

The time T is called the *lookahead* time. Typical values for D and T are 5 nautical miles and 5 minutes, respectively. In this paper these values are considered to be parameters.

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 conflicts can be defined in terms of the relative vectors $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$ and $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$, i.e., the relative position and velocity vectors, respectively, of the ownship with respect to the intruder. The predicted conflict predicate *predicted_conflict?*, which has as parameters the horizontal distance D, the lookahead time T, and the relative position and velocity of the aircraft, is formally defined as follows.

$$\textit{predicted\_conflict?}(D, T, \mathbf{s}, \mathbf{v}) \equiv \exists\, t \in [0, T] : \|\mathbf{s} + t\,\mathbf{v}\| < D.$$

Conflict detection algorithms check whether the predicate *predicted_conflict?* holds for the actual states of two aircraft. This paper considers a pairwise approach to conflict detection where each aircraft uses a conflict detection algorithm. The approach proposed in this paper takes the point of view of the ownship. However, the situation is symmetric from the point of view of the intruder aircraft.

Formally, a two-dimensional *conflict detection algorithm* is as a function `cd` with parameters D and T, written in subscript, that takes as arguments the state information of two aircraft. It returns a value in $\mathbb{B} = \{\texttt{True}, \texttt{False}\}$ that represents whether or not a conflict has been detected.

The state information used by a conflict detection algorithm is provided by positioning and surveillance systems such as GPS and ADS-B. In order to distinguish the actual states of the aircraft, represented by $\mathbf{s}_o, \mathbf{v}_o, \mathbf{s}_i, \mathbf{v}_i$, from the reported states provided by these systems, the measured position and velocity of the ownship and intruder aircraft will be represented by the vectors $\mathbf{s_o}^m, \mathbf{v_o}^m$ and $\mathbf{s_i}^m, \mathbf{v_i}^m$, respectively.

Since conflict detection algorithms are safety critical applications, it is imperative that they compute an answer that is trustworthy. A conflict detection algorithm is said to be *correct* if in the absence of measurement errors the algorithm does not issue false alerts and does not miss any alerts.

Definition 1 *A conflict detection algorithm* `cd` *is* correct *if and only if for all positions and velocity vectors* $\mathbf{s}_o, \mathbf{v}_o, \mathbf{s}_i, \mathbf{v}_i, \mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m$*, and* $\mathbf{v_i}^m$ *, with* $\mathbf{s_o}^m = \mathbf{s}_o, \mathbf{v_o}^m = \mathbf{v}_o, \mathbf{s_i}^m = \mathbf{s}_i$*, and* $\mathbf{v_i}^m = \mathbf{v}_i$*, the following formula holds*

$$\texttt{cd}_{D,T}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m) = \texttt{True} \Longleftrightarrow \textit{predicted\_conflict?}(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i).$$

In theory, conflict detection algorithms are designed to be correct, e.g., the conflict detection algorithm `CD2D`, which is part of NASA's Airborne Coordinated Conflict Resolution and Detection (ACCoRD) framework [17], satisfies this property. In practice, the existence of uncertainty in surveillance information implies that the equalities $\mathbf{s_o}^m = \mathbf{s}_o, \mathbf{v_o}^m = \mathbf{v}_o, \mathbf{s_i}^m = \mathbf{s}_i$, and $\mathbf{v_i}^m = \mathbf{v}_i$ may not hold. Thus, conflict detection algorithms, including correct algorithms such as `CD2D`, detect conflicts with inexact information, and they can therefore have false and missed alerts. Therefore, CD&R algorithms are generally used with slightly increased D and T values to accommodate for state information uncertainty. The added values are called *lateral and temporal safety buffers*, respectively, and their sizes are often determined by experimentation and simulation.

Increasing the size of these safety buffers will reduce number of missed alerts. However, as the size of the safety buffers increases, the number of false alerts increases as well. Missed alerts are an obvious cause of safety concerns. False alerts have also safety implications as they may diminish the confidence that crew members and air traffic controllers have on the separation assurance logic. Appropriate choices of safety buffers are crucial to the safety performance of a conflict detection system.

This paper provides analytical definitions of safety buffers and sufficient conditions under which correct conflict detection algorithms can be used without missing alerts. More precisely, definitions of non-negative numbers ψ (lateral safety buffer) and λ (temporal safety buffer) are provided such that under well-defined hypotheses on the information and communication uncertainty, it can be proved that

$$\textit{predicted\_conflict?}(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i) \Longrightarrow \mathtt{cd}_{D+\psi, T+\lambda}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m) = \mathtt{True}.$$

Furthermore, given probability distributions on errors in the differences $\mathbf{s}_o - \mathbf{s_o}^m$, $\mathbf{v}_o - \mathbf{v_o}^m$, $\mathbf{s}_i - \mathbf{s_i}^m$, and $\mathbf{v}_i - \mathbf{v_i}^m$, this paper provides a formula for an upper bound on the probability of missed alerts. A practical example is given where, under well-defined hypotheses, this probability is nonzero.

3 State Information Uncertainty

This paper considers two kinds of uncertainties: uncertainty due to measurement errors in global positioning systems such as GPS, and uncertainty due to infrequent traffic information updates from surveillance systems such as ADS-B. The effects on predicted conflicts, which assume constant velocities, are considered, so uncertainties due to possible velocity changes during the lookahead time period are not considered. Concretely, state information uncertainty is modeled through random variables that represent measurement errors due to (1) GPS position inaccuracy and (2) dropped ADS-B messages. Here, GPS and ADS-B are used for illustration purposes. The approach presented here could be adapted for uncertainty due to devices other than GPS and broadcast methods other than ADS-B.

Recall that a random variable is a function $f \colon \Omega \to X$, where $(\Omega, \sigma(\Omega))$ is a probability space, i.e., Ω is a set, $\sigma(\Omega)$ is a σ-algebra on the set Ω (a set of subsets of Ω), and there is a probability function P that maps elements of $\sigma(\Omega)$ to probabilities in the interval $[0, 1]$; cf. [22]. The set X is any measure space, and the function f must be *measurable*, in the sense of real analysis [23]. In what follows, the same probability space $(\Omega, \sigma(\Omega))$ will be used to model all of the random variables, e.g., GPS inaccuracy, dropped ADS-B message, conflict detection, etc. This is mathematically valid because even if two random variables are modeled with different probability spaces for their respective domains, equivalent random variables can be constructed whose domains are the *same* probability space. In fact, any random variable has an equivalent representation as a random variable with domain given by the uniform distribution on the interval $[0, 1]$; cf. [5].

Given a subset S of Ω such that $S \in \sigma(\Omega)$, the probability function P gives the *probability* $P(S)$ of S. Any random variable $f \colon \Omega \to X$ induces a probability *Prob* on measurable subset of X that is defined by $\mathit{Prob}(Y) = P(\{\chi \in \Omega \,|\, f(\chi) \in Y\})$, where Y is measurable. In addition, if X is a subset of the real numbers, then it is standard notation to define $\mathit{Prob}(f \geq r) = P(\{\chi \in \Omega \,|\, f(\chi) \geq r\})$ for $r \in \mathbb{R}$.

3.1 Modeling Uncertainty with Random Variables

Each aircraft uses GPS to determine its current state, i.e., its position, $\mathbf{s}_o$ or $\mathbf{s}_i$, and velocity vector, $\mathbf{v}_o$ or $\mathbf{v}_i$. ADS-B broadcasts this information to the airspace at regular intervals, and the interval between ADS-B broadcasts will be denoted α. Typically, the ADS-B system will be configured to broadcast this information once per second, i.e., $\alpha = 1$ second. Due to signal attenuation, it is possible that several consecutive position and velocity updates from the intruder have been dropped and were therefore not received by the ownship. This results in greater uncertainty in the values of the intruder's current state, i.e., $\mathbf{s}_i$ and $\mathbf{v}_i$. ADS-B message loss due to signal attenuation can be modeled as random variable:

$$\mathcal{A} \colon \Omega \to \mathbb{N},$$

where $(\Omega, \sigma(\Omega))$ is a probability space. The random variable $\mathcal{A}$ returns the number of consecutive ADS-B messages from the intruder that were not received by the ownship, since the last received message from the intruder. It is important to note that the length of time since the last ADS-B update from the intruder was received by the ownship is given by multiplying the return value of $\mathcal{A}$ by α. This length of time is modeled by the random variable $\alpha\mathcal{A}$ that maps $\chi \in \Omega$ into $\alpha\mathcal{A}(\chi)$, where the units of the domain are implicitly the units of α.

Standard inaccuracies in GPS position predictions, which are also used to predict velocities, imply that the measured positions $\mathbf{s_o}^m, \mathbf{s_i}^m$ and velocities $\mathbf{v_o}^m, \mathbf{v_i}^m$ may have errors. Thus, the actual positions $\mathbf{s}_o, \mathbf{s}_i$ and velocities $\mathbf{v}_o, \mathbf{v}_i$ are all modeled as random variables from Ω to $\mathbb{R}^2$:

$$\mathbf{s}_o, \mathbf{s}_i, \mathbf{v}_o, \mathbf{v}_i \colon \Omega \to \mathbb{R}^2.$$

The vectors $\mathbf{s_i}^m$ and $\mathbf{v_i}^m$ represent the intruder's reported position and velocity vectors, respectively, from the *last* ADS-B signal that was received by the ownship, and the vectors $\mathbf{s_o}^m$ and $\mathbf{v_o}^m$ represent the ownship's measured position and velocity at that time. If the current time is $t = 0$, then the time at which $\mathbf{s_o}^m, \mathbf{s_i}^m, \mathbf{v_o}^m, \mathbf{v_i}^m$ were measured is given by the random variable $\alpha\mathcal{A}$. Thus, if it is known that there are no errors in the measurements $\mathbf{s_o}^m, \mathbf{s_i}^m, \mathbf{v_o}^m, \mathbf{v_i}^m$, then the equalities $\mathbf{s}_o - \alpha\mathcal{A}\mathbf{v}_o = \mathbf{s_o}^m$, $\mathbf{s}_i - \alpha\mathcal{A}\mathbf{v}_i = \mathbf{s_i}^m$, $\mathbf{v}_o = \mathbf{v_o}^m$, and $\mathbf{v}_i = \mathbf{v_i}^m$ all hold *as random variables* $\Omega \to \mathbb{R}^2$. The random variables $\alpha\mathcal{A}$, $\mathbf{v}_o$, and $\mathbf{v}_i$ have units given by time, speed, and speed, respectively.

This paper focuses on the case where there are possible errors in the measurements $\mathbf{s_o}^m, \mathbf{s_i}^m, \mathbf{v_o}^m, \mathbf{v_i}^m$, modeled by the random variables $\mathbf{s}_o, \mathbf{s}_i, \mathbf{v}_o, \mathbf{v}_i$. In this case, the norms (i.e. errors) $\|(\mathbf{s}_o - \alpha\mathcal{A}\mathbf{v}_o) - \mathbf{s_o}^m\|$, $\|(\mathbf{s}_i - \alpha\mathcal{A}\mathbf{v}_i) - \mathbf{s_i}^m\|$, $\|\mathbf{v}_o - \mathbf{v_o}^m\|$, and $\|\mathbf{v}_i - \mathbf{v_i}^m\|$ are all random variables $\Omega \to \mathbb{R}_{\geq 0}$, and they therefore induce probabilites on subsets of $\mathbb{R}_{\geq 0}$, respectively. Thus, in the following sections, the probabilites

$$\begin{aligned} \mathit{Prob}(\|(\mathbf{s}_o - \alpha\mathcal{A}\mathbf{v}_o) - \mathbf{s_o}^m\|\| \geq a_o), \\ \mathit{Prob}(\|(\mathbf{s}_i - \alpha\mathcal{A}\mathbf{v}_i) - \mathbf{s_i}^m\| \geq a_i), \\ \mathit{Prob}(\|\mathbf{v}_o - \mathbf{v_o}^m\| \geq b_o), \text{ and} \\ \mathit{Prob}(\|\mathbf{v}_i - \mathbf{v_i}^m\| \geq b_i) \end{aligned}$$

will be used to bound the effects of GPS measurement errors on conflict detection. Here, the distances a_o and a_i and the speeds b_o and b_i are standardized navigation accuracy parameters.

Finally, given D and T, a conflict between the ownship and the intruder will be modeled as the random variable $\mathcal{C}_{D,T} : \Omega \to \mathbb{B}$ that maps $\chi \in \Omega$ into *predicted_conflict?*$(D, T, \mathbf{s}_o(\chi) - \mathbf{s}_i(\chi), \mathbf{v}_o(\chi) - \mathbf{v}_i(\chi))$.

The fact that the function $\mathcal{C}_{D,T}$ is a random variable is not immediately obvious. In fact, if κ is any Boolean function on four vectors, it is not necessarily true that $\kappa(\mathbf{s}_o, \mathbf{v}_o, \mathbf{s}_i, \mathbf{v}_i)$ is a random variable on Ω. While it is true that scalar multiples, sums, dot products, cross products, etc. of random variables $\Omega \to \mathbb{R}^2$ are also random variables, the definition of the random variable $\mathcal{C}_{D,T}$ involves an existential quantifier (i.e. $\exists$) in the definition of *predicted_conflict?*. However, the following lemma has been formally proved in PVS.

Lemma 1 *The Boolean function $\mathcal{C}_{D,T}$ is a random variable on Ω.*

Proof: The conflict detection algorithm `CD2D` is equivalent to the predicate *predicted_conflict?* (the proof of this fact is provided in the PVS formal development available from [17]). Thus, the predicate *predicted_conflict?* can be replaced by `CD2D` in the definition of $\mathcal{C}_{D,T}$ without changing the function. It therefore suffices to show that the function that maps an element χ of Ω to $\texttt{CD2D}_{D,T}(\mathbf{s}_o(\chi), \mathbf{v}_o(\chi), \mathbf{s}_i(\chi), \mathbf{v}_i(\chi))$ is a random varible. This expression is of the form

$$\texttt{CD2D}_{D,T}(\mathbf{s}_o(\chi), \mathbf{v}_o(\chi), \mathbf{s}_i(\chi), \mathbf{v}_i(\chi)) = \begin{cases} f(\chi) & \text{if } g(\chi) = 0, \\ h(\chi) & \text{if } g(\chi) / = 0, \end{cases}$$

where $f, h \colon \Omega \to \mathbb{B}$ and $g \colon \Omega \to \mathbb{R}$ are all random variables. This function is equal to $f \cdot \texttt{Char}_E + h \cdot \texttt{Char}_{\neg E}$, where $E = \{\chi \in \Omega \,|\, g(\chi) = 0\}$, $\neg E$ is the complement of E, and `Char` denotes the characteristic function of a given set. Since the function g is a random variable, E and $\neg E$ are by definition elements of $\sigma(\Omega)$, and so their characteristic functions are random variables. Hence, the function $f \cdot \texttt{Char}_E + h \cdot \texttt{Char}_{\neg E}$ is a sum of products of random variables, and it is therefore a random variable as well. □

Since $\mathcal{C}_{D,T}$ is a random variable, the probability that the two aircraft are actually in conflict is formally defined as

$$\mathit{Prob}(\mathit{predicted\_conflict?}(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)) = P(\{\chi \in \Omega \,|\, \mathcal{C}_{D,T}(\chi) = \texttt{True}\}).$$

3.2 Distribution of the ADS-B Random Variable

Under the assumption that there is no ADS-B signal interference due to multiple intruder aircraft, the distribution of ADS-B message loss $\mathcal{A}$ follows a Poisson distribution as discussed in [3], where it is used to model signal attenuation. Other failures of ADS-B systems, such as faulty equipment, are not addressed in this paper. The probability that a given ADS-B message from the intruder aircraft will not be received by the ownship, which is equal to $p(\{0\})$, is (approximately) given by $1 - \left(\frac{r}{r_0}\right)^k$ with $r \leq r_0$, where $k = 6.4314$ and $r_0 = 96.6$ nmi (178.9 km) [3]. The number r is the current distance between the two aircraft. Thus, if it is known that the ownship and the intruder are no greater than 60 nmi (111 km) apart, a reasonable distance for most commercial aircraft given short lookahead times such as 3 minutes, then the probability that a given message will be received is bounded below by 0.953, where in the formal language of random variables, this is expressed as $P(\{\chi \in \Omega \,|\, \mathcal{A}(\chi) = 0\}) \geq 0.953$. The specific probability 0.953 is not critical to the constructions in this paper. Thus, the probability that a given ADS-B message sent by the intruder will be received by ownship will be denoted by the variable η:

$$\eta = P(\{\chi \in \Omega \,|\, \mathcal{A}(\chi) = 0\}).$$

The key assumption that can be used to deduce that $\mathcal{A}$ follows a Poisson distribution is that whether any particular ADS-B message from the intruder aircraft is received by the ownship is independent from whether any other, different, ADS-B message from the intruder is received, for $i \geq 0$. This implies that for each $i \geq 0$, the probability that the last ADS-B message sent by the intruder that was received by the ownship was the $i+1$-st message ago (sent $\alpha \cdot i$ in the past) is given by

$$P(A_i) = \eta(1-\eta)^i, \tag{3.1}$$

where

$$A_i = \{\chi \in \Omega \,|\, \mathcal{A}(\chi) = i\}.$$

This is because the last i messages (sent $0, \alpha 1, \ldots$ and $\alpha i - 1$ seconds ago) have been dropped, which has a probability of $(1-\eta)^i$ of occurring, and the message sent exactly i-seconds ago was not dropped, which has a probability of η of occurring.

4 Safety Buffers

As noted in previous sections, the correctness of a conflict detection algorithm $\texttt{cd}_{D,T}$ can be affected by errors in GPS measurements or delays in ADS-B message updates. To counteract the effects of these errors on the conflict detection probe `cd`, a distance ψ and a non-negative time λ can be artificially added to the distance D and the time T when they are used as parameters in `cd`. That is, to make the algorithm more likely to return `True`, the parameters $D + \psi$ and $T + \lambda$ can be used in place of D and T in the algorithm `cd`. The distance ψ and the time λ are called *lateral and temporal safety buffers*, respectively, because the algorithm $\texttt{cd}_{D+\psi,T+\lambda}$ is more likely to return `True` than $\texttt{cd}_{D,T}$, and hence they are more conservative from a safety standpoint.

4.1 Probability of Conflict

Given the use of safety buffers ψ and λ in the conflict detection algorithm `cd`, as described above, a missed alert occurs when $\mathtt{cd}_{D+\psi,T+\lambda}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m)$ returns `False` but the aircraft are actually in conflict. So an upper bound for the probability of a missed alert is actually an upper bound on the probability *Prob*(*predicted_conflict?*$(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)$) that the aircraft are actually in conflict (cf. Section 3.1). Define $\mathcal{G}$ to be the set of $\chi \in \Omega$ where at least one of the following inequalities holds:

$$\begin{aligned} \|(\mathbf{s}_o(\chi) - \alpha\mathcal{A}(\chi)\mathbf{v}_o(\chi)) - \mathbf{s_o}^m\|| &\geq a_o, \\ \|(\mathbf{s}_i(\chi) - \alpha\mathcal{A}(\chi)\mathbf{v}_i(\chi)) - \mathbf{s_i}^m\| &\geq a_i, \\ \|\mathbf{v}_o(\chi) - \mathbf{v_o}^m\| &\geq b_o, \text{ or} \\ \|\mathbf{v}_i(\chi) - \mathbf{v_i}^m\| &\geq b_i. \end{aligned}$$

Define $\mathcal{T} = \{\chi \in \Omega \,|\, \mathcal{C}_{D,T}(\chi) = \mathtt{True}\}$. Note that the set Ω decomposes as an infinite union of pairwise disjoint sets $\Omega = \bigcup_{i=0}^{\infty} A_i$, where A_i is defined in Section 3.2. Recall that for a given set Z, Z^c denotes the complement of Z. Then standard probabilistic manipulations can be used to show that the probability *Prob*(*predicted_conflict?*$(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)$) decomposes as an infinite sum as follows.

$$\begin{aligned} \mathit{Prob}(\mathit{predicted\_conflict?}(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)) &= P(\mathcal{T}) \\ &= P(\mathcal{T} \cap \mathcal{G}) + P(\mathcal{T} \cap \mathcal{G}^c) \\ &= P(\mathcal{T} \cap \mathcal{G}) + P\left(\bigcup_{i=0}^{\infty}(\mathcal{T} \cap A_i \cap \mathcal{G}^c)\right) \qquad (4.2) \\ &= P(\mathcal{T} \cap \mathcal{G}) + \sum_{i=0}^{\infty} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c). \end{aligned}$$

Since $A_i \subset \mathcal{T} \cap A_i \cap \mathcal{G}^c$, it holds that *Prob*(*predicted_conflict?*$(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)$) $\leq P(\mathcal{G}) + \sum_{i=0}^{\infty} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c)$. This formula implies that for any non-negative number d, which represent a specific number of messages, the following series of inequalities hold.

$$
\begin{aligned}
\mathit{Prob}(\mathit{predicted\_conflict?}(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)) &\leq P(\mathcal{G}) \, + \sum_{i=0}^{\infty} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c) \\
&= P(\mathcal{G}) \, + \sum_{i=d+1}^{\infty} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c) + \sum_{i=0}^{d} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c) \\
&\leq P(\mathcal{G}) \, + \sum_{i=d+1}^{\infty} P(A_i) \, + \sum_{i=0}^{d} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c) \qquad (4.3) \\
&= P(\mathcal{G}) \, + \sum_{i=d+1}^{\infty} \eta(1-\eta)^i \, + \sum_{i=0}^{d} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c) \\
&= P(\mathcal{G}) \, + \, (1-\eta)^{d+1} \, + \sum_{i=0}^{d} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c).
\end{aligned}
$$

The second to last equality follows trivially from the equation for $P(A_i)$ in Section 3.2. Finally, the last equality follows directly from the standard formula for the sum of a geometric series.

Formula (4.3) has been formally proved in PVS and can be found in the ACCoRD development at [17]. The number d can be chosen so that the finite sum is a good approximation to the infinite sum (since $(1-\eta)^{d+1}$ is quite small). Therefore, Formula (4.3) states that

$$
\mathit{Prob}(\mathit{predicted\_conflict?}(D, T, \mathbf{s}_o - \mathbf{s}_i, \mathbf{v}_o - \mathbf{v}_i)) \approx P(\mathcal{G}) \, + \, (1-\eta)^{d+1} \, + \sum_{i=0}^{d} P(\mathcal{T} \cap A_i \cap \mathcal{G}^c),
$$

when d is sufficiently large.

4.2 Probability of a Missed Alert

Suppose now that confidence intervals are known for the accuracy of the random variables $\mathbf{s}_o, \mathbf{s}_i, \mathbf{v}_o$, and $\mathbf{v}_i$. That is, suppose that probabilities p_{so}, p_{vo}, p_{si}, and p_{vi} are known such that

$$
\begin{gathered}
\mathit{Prob}(\|(\mathbf{s}_o - \Upsilon \mathbf{v}_o) - \mathbf{s_o}^m\|| \geq a_o) \leq p_{so}, \\
\mathit{Prob}(\|(\mathbf{s}_i - \Upsilon \mathbf{v}_i) - \mathbf{s_i}^m\| \geq a_i) \leq p_{si}, \\
\mathit{Prob}(\|\mathbf{v}_o - \mathbf{v_o}^m\| \geq b_o) \leq p_{vo}, \text{ and} \\
\mathit{Prob}(\|\mathbf{v}_i - \mathbf{v_i}^m\| \geq b_i) \leq p_{vi}.
\end{gathered}
\qquad (4.4)
$$

It follows immediately that

$$
P(\mathcal{G}) \leq p_{so} + p_{si} + p_{vo} + p_{vi}. \qquad (4.5)
$$

Examples of such bounds p_{so}, p_{vo}, p_{si}, and p_{vi} on these probabilities can be found in DO-242A [24], which specifies several system performance confidence-levels that are to be included in ADS-B messages, and details how precise and trusted the contained state information is.

Formulas (4.3) and (4.5) imply that if $P(\mathcal{T} \cap A_i \cap \mathcal{G}^c) = 0$ for $i \leq d$, then the probability that $\mathtt{cd}_{D,T}(\mathbf{s}_o, \mathbf{s}_i, \mathbf{v}_o, \mathbf{v}_i) = \mathtt{True}$ is bounded above by $p_{so} + p_{si} + p_{vo} + p_{vi} + (1-\eta)^{d+1}$. The following lemma presents particular choices of the safety buffers ψ and λ that can be used to ensure that this bound is satisfied. The lemma refers to the distances a_o and a_i and the speeds b_o and b_i that define the probabilities $p_{so}, p_{vo}, p_{si}, p_{vi}$. It also uses the time α, which is the regular interval at which ADS-B messages are sent by the intruder aircraft. The value τ is an upper bound to the predicted time of closest approach.

It is important to note that the next lemma is a mathematical statement and holds for all input vectors and real numbers. In the context of this paper, it is interpreted as a statement about aircraft positions and velocities, but it holds as a general mathematical statement. In this paper, it is used for conflict detection between aircraft that are flying with constant velocities in a situation where subsequent dropped messages are independent events, but none of these assumptions is needed for the lemma to be true. It has been formally proved as a mathematical statement in PVS.

Lemma 2 *Let* $\mathbf{s}^m = \mathbf{s_o}^m - \mathbf{s_i}^m$, $\mathbf{v}^m = \mathbf{v_o}^m - \mathbf{v_i}^m$ *with* $\|\mathbf{v}^m\| > b_o + b_i$, d *be an integer, and*

- $\lambda = \alpha d$,
- $\tau = (\|\mathbf{s}^m\| + a_o + a_i + \lambda \cdot (\|\mathbf{v}^m\| + b_o + b_i))/(\|\mathbf{v}^m\| - b_o - b_i)$,
- $\psi = a_o + a_i + (\min(T, \tau) + \lambda)(b_o + b_i)$.

If $\mathtt{cd}_{D+\psi, T+\lambda}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m) = \mathtt{False}$*, then, for* $j \in \{0, \ldots, d\}$, $P(\mathcal{T} \cap A_j \cap \mathcal{G}^c) = 0$.

Proof: It suffices to prove that, given the hypotheses of this lemma, $\mathcal{T} \cap A_j \cap \mathcal{G}^c$ is empty. Suppose by way of contradiction that $\chi \in \mathcal{T} \cap A_j \cap \mathcal{G}^c$. Since $\chi \in \mathcal{T}$, it follows that $\mathtt{cd}_{D,T}(\mathbf{s}_o(\chi), \mathbf{s}_i(\chi), \mathbf{v}_o(\chi), \mathbf{v}_i(\chi)) = \mathtt{True}$. Since $\chi \in A_j$, $\mathcal{A}(\chi) = j$. Finally, since $\chi \in \mathcal{G}^c$, the equations $\|(\mathbf{s}_o(\chi) - \alpha j \mathbf{v}_o(\chi)) - \mathbf{s_o}^m\| < a_o$, $\|(\mathbf{s}_i(\chi) - \alpha j \mathbf{v}_i(\chi)) - \mathbf{s_i}^m\| < a_i$, $\|\mathbf{v}_o(\chi) - \mathbf{v_o}^m\| < b_o$, and $\|\mathbf{v}_i(\chi) - \mathbf{v_i}^m\| < b_i$ are all satisfied.

As in Section 2, let $\mathbf{s}$ and $\mathbf{v}$ denote the relative position and velocities $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$ and $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$. It is easy to see that $\|\mathbf{s}(\chi) + t\mathbf{v}(\chi)\|^2$ is a quadratic in t that attains its minimum at $t = -\mathbf{s}(\chi) \cdot \mathbf{v}(\chi)/\|\mathbf{v}(\chi)\|^2$. Thus, the fact that $\mathtt{cd}_{D,T}(\mathbf{s}_o(\chi), \mathbf{s}_i(\chi), \mathbf{v}_o(\chi), \mathbf{v}_i(\chi)) = \mathtt{True}$ (since $\chi \in \mathcal{T}$) implies that there exists $t^* \in [0, \min(T, -\mathbf{s}(\chi) \cdot \mathbf{v}(\chi)/\|\mathbf{v}(\chi)\|^2)]$ such that $\|\mathbf{s}(\chi) + t^*\mathbf{v}(\chi)\| < D$. Then $t^* + \alpha j \in [0, \min(T, -\mathbf{s}(\chi) \cdot \mathbf{v}(\chi)/\|\mathbf{v}(\chi)\|^2) + \lambda]$ and since $\mathbf{s} = \mathbf{s}_o - \mathbf{s}_i$ and $\mathbf{v} = \mathbf{v}_o - \mathbf{v}_i$, it suffices to show that $\|\mathbf{s}^m + (t^* + \alpha j)\mathbf{v}^m\| < \psi + D$, which is a contradiction, since $\mathtt{cd}_{D+\psi, T+\lambda}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m) = \mathtt{False}$. If it can be proved that

$t^* + \alpha j \leq \min(T, \tau) + \lambda$, then the result will follow, since

$$\begin{aligned}
&\|\mathbf{s}^m + (t^* + \alpha j)\mathbf{v}^m\| \\
&= \|(\mathbf{s_o}^m - \mathbf{s_i}^m) + (t^* + \alpha j)(\mathbf{v_o}^m - \mathbf{v_i}^m)\| \\
&= \|(\mathbf{s_o}^m - \mathbf{s_i}^m) + (t^* + \alpha j)(\mathbf{v_o}^m - \mathbf{v_i}^m) - (\mathbf{s}(\chi) + t^*\mathbf{v}(\chi)) + (\mathbf{s}(\chi) + t^*\mathbf{v}(\chi))\| \\
&= \|(\mathbf{s_o}^m - (\mathbf{s}_o(\chi) - \alpha j\mathbf{v}_o(\chi))) - (\mathbf{s_i}^m - (\mathbf{s}_i(\chi) - \alpha j\mathbf{v}_i(\chi))) + (t^* + \alpha j)(\mathbf{v_o}^m - \mathbf{v}_o(\chi)) \\
&\qquad - (t^* + \alpha j)(\mathbf{v_i}^m - \mathbf{v}_i(\chi)) + (\mathbf{s} + t^*\mathbf{v}(\chi))\| \\
&\leq \|\mathbf{s_o}^m - (\mathbf{s}_o(\chi) - \alpha j\mathbf{v}_o(\chi))\| + \|\mathbf{s_i}^m - (\mathbf{s}_i(\chi) - \alpha j\mathbf{v}_i(\chi))\| \\
&\qquad + (t^* + \alpha j)\|\mathbf{v_o}^m - \mathbf{v}_o(\chi)\| + (t^* + \alpha j)\|\mathbf{v_i}^m - \mathbf{v}_i(\chi)\| + \|\mathbf{s} + t^*\mathbf{v}(\chi))\| \\
&= \|\mathbf{s_o}^m - (\mathbf{s}_o(\chi) - \alpha\mathcal{A}(\chi)\mathbf{v}_o(\chi))\| + \|\mathbf{s_i}^m - (\mathbf{s}_i(\chi) - \alpha\mathcal{A}(\chi)\mathbf{v}_i(\chi))\| \\
&\qquad + (t^* + \alpha j)\|\mathbf{v_o}^m - \mathbf{v}_o(\chi)\| + (t^* + \alpha j)\|\mathbf{v_i}^m - \mathbf{v}_i(\chi)\| + \|\mathbf{s} + t^*\mathbf{v}(\chi))\| \\
&< a_o + a_i + (t^* + \alpha j)b_o + (t^* + \alpha j)b_i + D \\
&\leq a_o + a_i + (t^* + \lambda)(b_o + b_i) + D \\
&\leq \psi + D.
\end{aligned}$$

Since $t^* + \alpha j \in [0, \min(T, -\mathbf{s}(\chi) \cdot \mathbf{v}(\chi)/\|\mathbf{v}(\chi)\|^2) + \lambda]$ and $\alpha j \leq \lambda$, it therefore suffices to prove that $-\mathbf{s}(\chi) \cdot \mathbf{v}(\chi)/\|\mathbf{v}(\chi)\|^2 \leq \tau$. The Cauchy-Schwartz inequality implies that $-\mathbf{s}(\chi) \cdot \mathbf{v}(\chi) \leq \|\mathbf{s}(\chi)\| \cdot \|\mathbf{v}(\chi)\|$, so it suffices to prove that $\|\mathbf{s}(\chi)\|/\|\mathbf{v}(\chi)\| \leq \tau$. This inequality can be verified by proving the following two inequalities.

$$\begin{aligned}
\|\mathbf{s}(\chi)\| &\leq \|\mathbf{s}^m\| + a_o + a_i + \lambda \cdot (\|\mathbf{v}^m\| + b_o + b_i), \\
\|\mathbf{v}(\chi)\| &\geq \|\mathbf{v}^m\| - b_o - b_i.
\end{aligned}$$

These two formulas follow from basic applications of the triangle inequality and the facts that $\|(\mathbf{s}_o(\chi) - \alpha j\mathbf{v}_o(\chi)) - \mathbf{s_o}^m\| < a_o$, $\|(\mathbf{s}_i(\chi) - \alpha j\mathbf{v}_i(\chi)) - \mathbf{s_i}^m\| < a_i$, $\|\mathbf{v}_o(\chi) - \mathbf{v_o}^m\| < b_o$, $\|\mathbf{v}_i(\chi) - \mathbf{v_i}^m\| < b_i$, and $\alpha j \leq \lambda$. □

The following theorem uses Lemma 2 to give an upper bound on the probability of a missed alert, if the safety buffers ψ and λ given in that lemma are used. This theorem follows trivially from that lemma and Formula (4.3) and has also been proved in in the PVS theorem prover. Just as for Lemma 2, it is important to note that the next theorem is a mathematical statement and therefore holds for all input vectors and real numbers. In the context of this paper, it is interpreted as a statement about aircraft that are flying with constant velocities in a situation where subsquent dropped messages are independent events, but it holds as a general mathematical statement without even these assumptions.

Theorem 1 *Let* $\mathbf{s}^m = \mathbf{s_o}^m - \mathbf{s_i}^m$, $\mathbf{v}^m = \mathbf{v_o}^m - \mathbf{v_i}^m$ *with* $\|\mathbf{v}^m\| > b_o + b_i$, d *be an integer, and*

- $\lambda = \alpha d$,
- $\tau = (\|\mathbf{s}^m\| + a_o + a_i + \lambda \cdot (\|\mathbf{v}^m\| + b_o + b_i))/(\|\mathbf{v}^m\| - b_o - b_i)$,
- $\psi = a_o + a_i + (\min(T, \tau) + \lambda)(b_o + b_i)$.

If $\mathtt{cd}_{D+\psi,T+\lambda}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m) = \mathtt{False}$*, the probability of a missed alert, i.e. the probability that* $\mathtt{cd}_{D,T}(\mathbf{s}_o, \mathbf{s}_i, \mathbf{v}_o, \mathbf{v}_i) = \mathtt{True}$*, is no greater than* $p_{so} + p_{vo} + p_{si} + p_{vi} + (1-\eta)^{d+1}$*, where* η *is the the probability that a given ADS-B message sent by the intruder will be received by ownship.*

A *missed alert* is a conflict that is not detected. Artificially increasing the distance D and the lookahead time T in the conflict probe `cd` will make missed alerts less likely. The theorem above gives specific formulas for safety buffers that can be used to ensure that the probability of a missed alert is sufficiently small. The speeds b_o and b_i, and the probabilities p_{so}, p_{vo}, p_{si} and p_{vi} are variables in this theorem and can be changed based on the application. Formulas (4.4) and (4.5) express the relationships between $a_o, a_i, b_o, b_i, p_{so}, p_{vo}, p_{si}$ and p_{vi}. Given these inputs, the associated upper bound for the probability of a missed alert is

$$p_{missed-alert} = p_{so} + p_{vo} + p_{si} + p_{vi} + (1-\eta)^{d+1}. \tag{4.6}$$

In the equation above, the amount ψ that D should be artificially increased to ensure that the probability of a missed alert is less than $p_{missed-alert}$ is given by

$$\psi = a_o + a_i + (\min(T,\tau) + \lambda)(b_o + b_i), \tag{4.7}$$

where as above, α denotes the time period between consecutive ADS-B broadcasts by the intruder aircraft. It should be noted that Formulas (4.7) and (4.6) imply that if the velocity b dominates the calculation of ψ, then as ψ increases, d increases as well, and so the probability of a missed alert decreases.

The following is a formulation of Theorem 1 in PVS. The purpose of including the statement here is not technical, but rather so that the reader can conceptualize what is meant by a statement that is proved in PVS, which checks proofs that are entered into it by a human for logical correctness. The specifics of the PVS notation are unimportant, so most of the technical details are omitted.

```
Theorem1 : THEOREM
    sm = som-sim AND vm = vom-vim AND norm(vm)>bo+bi AND
    P(GsetPosition(so,som,vo,alpha,A,ao)) <= prso AND
    P(GsetVelocity(vo,vom,bo)) <= prvo AND
    P(GsetPosition(si,sim,vi,alpha,A,ai)) <= prsi AND
    P(GsetVelocity(vi,vim,bi)) <= prvi AND
    lambda = alpha*d AND
    tau = (norm(sm)+ao+ai+(lambda)*
      (norm(vm)+bo+bi))/(norm(vm)-bo-bi) AND
    psi = ao+ai+(min(T,tau)+lambda)*(bo+bi) AND
    cd(D+psi,T+lambda,som,vom,sim,vim)=FALSE AND
    adsb_distr?(eta)(A)
    IMPLIES
      P({chi:Omega | conflict_rv(D,T,so,vo,si,vi)(chi) = True})
        <= prso+prvo+prsi+prvi+expt(1-eta,d+1)
```

4.3 Special Case: Absolute Bounds

The special case when absolute bounds on the positions and speeds of the ownship and the intruder are known and when there are no messages lost is considered next. That is, rather than letting $\mathbf{s}_o, \mathbf{s}_i, \mathbf{v}_o, \mathbf{v}_i$ denote random variables, it is assumed in this section that these are positions and velocities, respectively, i.e., elements of $\mathbb{R}^2$. It is further assumed that there are no dropped ADS-B messages. Thus, each of the equations $\|\mathbf{s}_o - \mathbf{s_o}^m\| < a_o$, $\|\mathbf{s}_i - \mathbf{s_i}^m\| < a_i$, $\|\mathbf{v}_o - \mathbf{v_o}^m\| < b_o$, and $\|\mathbf{v}_i - \mathbf{v_i}^m\| < b_i$ is satisfied. In this case, Theorem 1 gives a safety buffer ψ for the separation distance D that ensure no missed alerts, assuming that there are no information delays such as dropped ADS-B messages. Thus, in the following corollary, each of the probabilities p_{so}, p_{vo}, p_{si}, and p_{vi} and the integer d, all occurring in the statement of Theorem 1, are zero. The corollary is a mathematical statement and therefore holds for all input vectors and real numbers. In the context of this paper, it is interpreted as a statement about aircraft that are flying with constant velocities, in a situation where the errors on the positions and velocities have known bounds and the probability of a message being dropped is zero. However, it holds as a general mathematical statement without these assumptions.

Corollary 1 *Let* $\mathbf{s}^m = \mathbf{s_o}^m - \mathbf{s_i}^m$, $\mathbf{v}^m = \mathbf{v_o}^m - \mathbf{v_i}^m$ *with* $\|\mathbf{v}^m\| > b_o + b_i$, *and*

- $\tau = (\|\mathbf{s}^m\| + a_o + a_i)/(\|\mathbf{v}^m\| - b_o - b_i)$,
- $\psi = a_o + a_i + \min(T, \tau)(b_o + b_i)$.

If predicted_conflict?$(D, T, \mathbf{s}, \mathbf{v})$ *holds, then,* $\mathtt{cd}_{D+\psi,T}(\mathbf{s_o}^m, \mathbf{v_o}^m, \mathbf{s_i}^m, \mathbf{v_i}^m) = \mathtt{True}$.

Corollary 1 is proved in PVS by using Theorem 1 with α and d both equal to 0. The statement of that theorem depends on a probability space Ω, but it is true for any choice of Ω. To prove Corollary 1, the trivial probability space $(\Omega, \sigma(\Omega))$, where $\Omega = \{1\}$, $\sigma(\Omega) = \{\phi, \{1\}\}$, $P(\phi) = 0$, and $P(\{1\}) = 1$, is used.

It may be the case that instead of bounds on the measurement errors of the velocity vectors $\mathbf{v}_o$ and $\mathbf{v}_i$, bounds are known on the errors in the measurements of the ground speeds $\|\mathbf{v}_o\|$ and $\|\mathbf{v}_i\|$ and track angles *track*$(\mathbf{v}_o)$ and *track*$(\mathbf{v}_i)$ of the two aircraft. This may be the case when velocity information is broadcast not as a vector but as a track angle and ground speed pair. In this case, error bounds on track angles and ground speeds can be used to deduce error bounds on the velocity vectors themselves, thereby reducing this problem to that solved by Corollary 1.

Recall that the track angle *track*$(\mathbf{u})$ of a vector $\mathbf{u}$ is the angle $\alpha \in [0, 2\pi)$ that satisfies

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

Here, ε_{so}, ε_{si}, $\varepsilon_{\alpha o}$, ε_{go}, $\varepsilon_{\alpha i}$, and ε_{gi} will denote the errors on the positions, track-angles, and ground speeds of the ownship and the intruder, respectively, i.e.,

$$
\begin{aligned}
\|\mathbf{s}_o - \mathbf{s_o}^m\| &\leq \varepsilon_{so}, \\
\|\mathbf{s}_i - \mathbf{s_i}^m\| &\leq \varepsilon_{si}, \\
|\mathit{track}(\mathbf{v}_o) - \mathit{track}(\mathbf{v_o}^m)| &\leq \varepsilon_{\alpha o}, \\
|\|\mathbf{v}_o\| - \|\mathbf{v_o}^m\|| &\leq \varepsilon_{go}, \\
\mathit{track}(\mathbf{v}_i) - \mathit{track}(\mathbf{v_i}^m)| &\leq \varepsilon_{\alpha i}, \\
|\|\mathbf{v}_i\| - \|\mathbf{v_i}^m\|| &\leq \varepsilon_{gi},
\end{aligned}
\tag{4.8}
$$

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.

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

$$
\begin{aligned}
\varepsilon_{\alpha o} &\leq \frac{\pi}{2}, \\
\varepsilon_{go} &\leq \left\|\mathbf{v_o}^m\right\|, \\
\left\|\mathbf{v_o}^m\right\|(1 - \cos\varepsilon_{\alpha o}) &\leq \varepsilon_{go}, \\
\varepsilon_{\alpha i} &\leq \frac{\pi}{2}, \\
\varepsilon_{gi} &\leq \left\|\mathbf{v_i}^m\right\|, \\
\left\|\mathbf{v_i}^m\right\|(1 - \cos\varepsilon_{\alpha i}) &\leq \varepsilon_{gi}.
\end{aligned}
\tag{4.9}
$$

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 1, velocity errors are also bounded by a circle.

The following lemma can be used to apply Corollary 1 in the case where error bounds on track angles and ground speeds are known instead of error bounds on the velocity vectors themselves. As for Corollary 1, it is interpreted as a statement about aircraft that are flying with constant velocities, in a situation where the errors on the positions and velocities have known bounds and the probability of a message being dropped is zero. However, it holds as a general mathematical statement about vectors and real numbers, without any extra assumptions, including these assumptions about aircraft and dropped messages.

Lemma 3 *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* (4.8) *and* (4.9)*. It holds that*

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

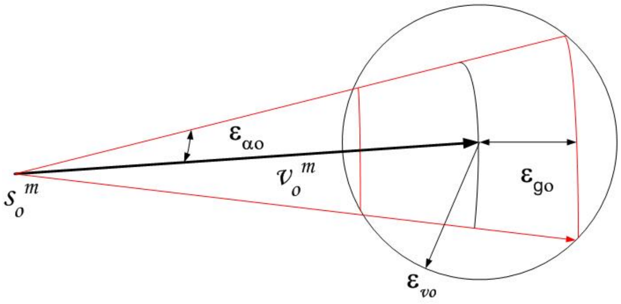

Figure 1: Ownship Velocity Error Bounds

where

$$\varepsilon_{vo} = \sqrt{2\left\|\mathbf{v_o}^m\right\|(\left\|\mathbf{v_o}^m\right\| + \varepsilon_{go})(1-\cos\varepsilon_{\alpha o}) + {\varepsilon_{go}}^2},$$

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

5 Numerical Examples

DO-242A [24] specifies several system performance confidence-levels that are to be included in ADS-B messages detailing how precise and trusted the contained state information is. The relevant ones to this paper are the navigation accuracy categories for position and velocity (NAC_P and NAC_V). The 12 NAC_P categories define a maximum distance for errors in position (NAC_P 11 is < 3 m, NAC_P 0 is ≥ 10 nmi); similarly the 5 NAC_V categories define maximum velocity error (NAC_V 4 is < 0.3 m/s, NAC_V 0 is ≥ 10 m/s). That is, these numbers specify the parameters a_0, a_i and b_o, b_i, respectively. Both NAC_P and NAC_V specify that the stated values will fall within a 95% confidence interval, which is equivalent to saying that p_{so}, p_{vo}, p_{si} and p_{vi} are all equal to 0.05.

The ADS-B model described in Section 3.2 predicts that when aircraft are 60 nmi (111 km) apart, $\eta \geq 0.95325$ (to 5 decimal places), while if they are 20 nmi (37 km) apart, $\eta \geq 0.99996$.

Table 1 assumes both aircraft can produce data within the NAC_P 9 category (position error < 30 m) and the NAC_V 4 category (velocity error < 0.3 m/s). These numbers along with Equations (4.6) and (4.7) are used to compute the amount the distance that D needs to be increased, i.e., ψ, as well the associated upper bounds on the probabilities of missed alerts for varying choices of d. More accurate position data can reduce ψ by approximately 0.03 nmi (556 m), while less accurate data, especially velocity, can significantly increase the buffer ψ. Recall that, as above, d denotes the number of consecutive ADS-B messages from the intruder that were not received by the ownship, since the last received message from the intruder. The following table assumes that ADS-B updates from the aircraft are broadcast once per second ($\alpha = 1$ second and $\lambda = d$ seconds). The relative ground speed $\|\mathbf{v}^m\| = 514$ m/s corresponds to two aircraft heading directly at each other, each traveling at approximately 500 knots. Furthermore, $\|\mathbf{v}^m\| = 206$ m/s corresponds to aircraft approaching each other at speeds of 200 knots.

T	$\|\mathbf{s}^m\|$	$\|\mathbf{v}^m\|$	ψ (D buffer)	$p_{missed-alert}$			
(s)	(nmi)	(m/s)	($\lambda = 0$ to 3 s)	$\lambda = 0$ s	$\lambda = 1$ s	$\lambda = 2$ s	$\lambda = 3$ s
300	60	514	0.10 nmi (190-193 m)	0.24675	0.20219	0.20010	0.20000
300	60	206	0.13 nmi (240-242 m)				
180	60	514	0.09 nmi (168-170 m)				
180	60	206	0.09 nmi (168-170 m)				
300	20	514	0.06 nmi (103-107 m)	0.20004	0.20000	0.20000	0.20000
300	20	206	0.09 nmi (168-172 m)				
180	20	514	0.06 nmi (103-107 m)				
180	20	206	0.09 nmi (168-170 m)				

Table 1: Lookahead, distance, relative speed, buffer sizes, and probability of missed alert

Note that Equation (4.7) compensates for situations where the projected time of closest approach, i.e., the term τ in Theorem 1, is known to be less than the lookahead time T. If both aircraft are 20 nmi from each other and are traveling at 500 knots, they could collide in as few as 72 seconds.

It should also be noted that the upper bounds on the probabilities of missed alerts in this table are high. However, this is not due to imprecision in the presented methods but to the fact that the confidence intervals specified in DO-242A are for 95% confidence and provide little knowledge of what is happening the other 5% of the time. These formulas are quite practical, and in fact could be used to calculate the probability of missed alerts that are significantly smaller if more precise confidence intervals were available for the positions and velocities of the aircraft. For instance, if 99.999% confidence intervals were available for position and velocity errors in DO-242A, these formulas would provide safety buffers that guarantee that the probability of a missed alert for a state-based conflict is less than 0.004%. In general, the confidence intervals specified in DO-242A are too liberal to ensure greater than 95% reliability for state-based conflict detection systems, since they allow aircraft to broadcast incorrect state information up to 5% of the time. Thus, to ensure near 100% reliability of state-based conflict detection systems, confidence intervals greater than those found in DO-242A for position and velocity errors would be required.

6 Conclusion

This paper concerns lateral and temporal safety buffers in state-based conflict detection methods. These methods use the current state of the aircraft and a mass-point trajectory model (*nominal trajectories*, according to Kuchar and Yang's taxonomy) to alert a predicted violation of separation minima. In airborne concepts, state-based systems are used as backup of more advance separation assurance systems. For these kinds of systems, an approach for modeling aircraft state information uncertainty is proposed. The approach is illustrated with models of errors in GPS and ADS-B devices. However, other type of devices can be modeled in similar ways. These probabilistic models used to estimate the probability of a missed alert. From that estimation, analytical definitions of safety buffers are provided that ensure that the probability of a missed alert is sufficiently small. Numerical examples of safety buffers for GPS and ADS-B parameters are given.

The analysis presented in this paper considers uncertainty in the current state information and dropped messages due to signal attenuation. Therefore, trajectory uncertainties, such as navigation errors, and communication errors due to dependent events are not part of the proposed uncertainty modeling approach. It can be argued that this simplification yields analytical definitions of safety buffers that are appropriate for airborne state-based conflict detection systems, since these systems are executed in each aircraft as frequently as position and surveillance information is updated. Future work will consider a trajectory prediction model that uses previous state information of the aircraft.

This paper only addresses the analytical definition of separation buffers for lateral separation. While it is true that lateral safety buffers are most useful for detecting horizontal conflicts, it is easy to see how they could be used for 3D conflict detection as well. If a lateral conflict detection algorithm returns false, then it is guaranteed that the aircraft are not in 3D conflict for this lookahead time as well.

The results presented in this paper have been mechanically checked using an interactive theorem prover (PVS), which provides strong guarantees that the mathematical development is correct. The use of a mechanical theorem prover requires a detailed description of the problem and a meticulous proof process. This level of rigor is justified by the critical role that aircraft separation plays in the overall safety of the next generation of air traffic management systems. It should be noted that the current development in PVS models only piecewise linear aircraft trajectories, which are, arguably, good approximations of actual trajectories over short lookahead times (e.g. less than 3 minutes).

References

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

[2] L.M.B.C. Campos and J.M.G. Marques. On the trhee-dimensional collision probabilities relevant to ATM. In *Proceedings of 27th International Congress of the Aeronautical Sciences, ICAS 2010*, Nice, France, September 2010.

[3] W. W. Chung and R. Staab. A 1090 extended squitter Automatic Dependent Surveillance Broadcast (ADS-B) reception model for air-traffic-management simulations. In *AIAA Modeling and Simulation Technologies Conference and Exhibit*, 2006.

[4] 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.

[5] M. H. A. Davis. *Markov Models and Optimization.* Chapman and Hall, first edition, 1993.

[6] Gilles Dowek, Alfons Geser, and César 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.

[7] Gilles Dowek and César 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.

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

[9] 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.

[10] Ran Y. Gazit and J. David Powell. The effect of GPS-based surveillance on aircraft separation standards. In *Proceedings of the IEEE Position Location and Navigation Symposium 1996*, pages 360–367, 1996.

[11] Heber Herencia-Zapana, Jean-Baptiste Jeannin, and César Muñoz. Formal verification of safety buffers for state-based conflict detection and resolution. In *Proceedings of 27th International Congress of the Aeronautical Sciences, ICAS 2010*, Nice, France, 2010.

[12] 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.

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

[14] David A. Karr, David A. Roscoe, and Robert A. Vivona. An integrated flight-deck decision-support tool in an autonomous flight simulation. In *Proceedings of the AIAA Modeling and Simulation Technologies Conference and Exhibit*, number AIAA 2004-5261, Providence, Rhode Island, August 2004.

[15] James Kuchar and Lee Yang. A review of conflict detection and resolution modeling methods. *IEEE Transactions on Intelligent Transportation Systems*, 1(4):179–189, December 2000.

[16] Jeffrey Maddalon, Ricky Butler, Alfons Geser, and César 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.

[17] NASA Langley Formal Methods Team. Airborne Coordinated Conflict Resolution and Detection (ACCoRD) framework, 2010. http://shemesh.larc.nasa.gov/people/cam/ACCoRD/.

[18] 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.

[19] Russell Paielli and Heinz Erzberger. Conflict probability estimation for free flight. Technical Memorandum 110411, NASA, October 1996.

[20] Maria Prandini, Jianghai Hu, John Lygeros, and Shankar Sastry. A probabilistic approach to aircraft conflict detection. *IEEE Transactions on Intelligent Transportation Systems*, 1(4):199–220, December 2000.

[21] Maria Prandini and Oliver Watkins. Probabilistic aircraft conflict detection. Technical report, HYBRIDGE Project IST-2001-32460, May 2005.

[22] J. S. Rosenthal. *A First Look at Rigorous Probability Theory.* World Scientific Publishing Co. Pte. Ltd., second edition, 2009.

[23] H. L. Royden. *Real Analysis.* Prentice Hall, third edition, 1988.

[24] Minimum aviation system performance standards for Automatic Dependent Surveillance Broadcast (ADS-B). DO-242A, RTCA, June 2002. Section 2.1.2.12–2.1.2.15.

[25] David J. Wing, Robert A. Vivona, and David A. Roscoe. Airborne tactical intent-based conflict resolution capability. In *9th AIAA Aviation Technology, Integration, and Operations Conference (ATIO)*, Hilton Head, South Carolina, USA, September 2009.

[26] 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.