Formal Verification of an Optimal Air Traffic Control Resolution and Recovery Algorithm

A. Galsion, C. Muñoz, M. Ayala-Rincón

7.4.2008

Introduction

- CD&R: conflict detection and resolution
- CD&R systems are designed to increase traffic awareness and provide corrective maneuvers for impeding conflicts

K3BD – three dimensional distributed CD&R algorithm

- designed and formally verified by the Formal Method Group at NIA and NASA
- uses position and velocity vectors to detect and solve conflict
  - vertical speed
  - ground speed
  - heading
- pairwise tactical algorithm

Introduction II.

- every member of the traffic has a cylindric *protected zone* of diameter D and height H
- *conflict* is a predicted loss of separation within lookahead time T
- when a conflict is detected, K3BD outputs a choice of a resolution maneuvers for the ownship

K3BD extensions

1. *time arrival constraints* – K3BD computes recovery maneuvers which brings the ownship back to its target at a scheduled time
2. *implicitly coordinated strategy*
   - *strategy* is a procedure that selects a subset of the resolution maneuvers proposed by K3BD
   - *coordinated strategy* guarantee that aircrafts using the same aircraft system will not fly into each other directions
   - coordination is *implicit* if the only communication required to achieve the coordination is the broadcasted information of the aircraft
   - it has been formally verified that K3BD supports implicitly coordinated resolution strategy

K3BD properties & K2BD

- in K3BD resolution maneuvers protected zones touch, but do not overlap
- modifies only one component of the original velocity vector
- its resolutions are not necessarily optimal from the geometrical point of view (optimal resolution – all three parts changed)

K2BD is an 2D version of K3BD that compute optimal resolution maneuvers for combined variations of speed and heading

Geometrical Framework

- airspace is 2D cartesian coordinate system
- flat earth assumption
- aircraft can change speed and course in zero time (typical for CD&R algorithm with short lookahead time – 5min)
- uses relative coordinate system – traffic is at the origin, ownship's position is given relatively to the traffic

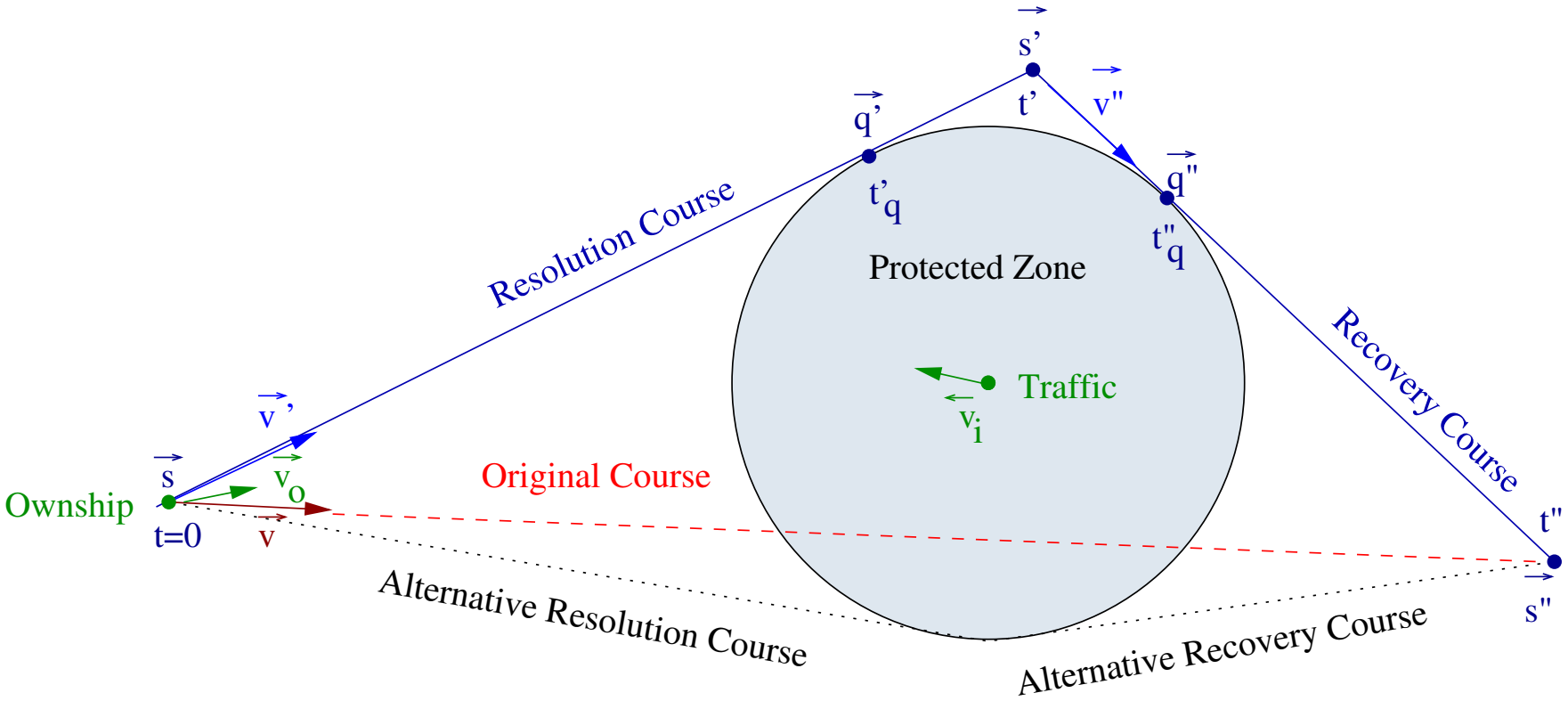
protected zone is a cylinder of diameter 2D located in the centre of the coordinate system

$$P = \{(x, y, 0) \mid x^2 + y^2 < D^2\}$$

loss of separation at time t:

$$s + t\mathbf{v} \in P$$

aircraft are said **to be in conflict** if there exists a time $0 < t < T$ when they are to loose separation


s'
t'
v"
q'
q"
t'q
t"q
Resolution Course
Protected Zone
Recovery Course
Traffic
vi
v'
s
vo
Ownship
Original Course
t=0
v
t"
s"
Alternative Resolution Course
Alternative Recovery Course

Resolution is a new velocity vector $\mathbf{v_0'}$ for the ownship. The resolution is correct if for all $t > 0$:

$$s + t(\mathbf{v_0}' - \mathbf{v_i}) \notin P \tag{1}$$

Resolutions $\mathbf{v_0}'$ and $\mathbf{v_i'}$ are *coordinated* for the ownship and the traffic aircraft iff $\forall t > 0$:

$$s + t(\mathbf{v_0'} - \mathbf{v_i'}) \notin P \tag{2}$$

Arrival time $t'' > 0$ determines a way point s'', called target point:

$$s' = s + t''\mathbf{v} \tag{3}$$

Resolution/recovery maneuver for arrival time t'' is a triple $(t', \mathbf{v_0'}, \mathbf{v_0''})$ where $t' > 0$ is a time of switch, $\mathbf{v_0'}$ is a velocity resolution for the ownship and $\mathbf{v_0''}$ is a recovery for the ownship.

Resolution is *correct* iff

- $\mathbf{v_0'}$ is a correct resolution for the ownship

$$s + t'\mathbf{v'} + t\mathbf{v''} \notin P \tag{4}$$

- $\mathbf{v_0''}$ is a correct recovery for the ownship

$$s + t'\mathbf{v'} + (t'' - t')\mathbf{v''} = s'' \tag{5}$$

Resolution $\mathbf{v_0'}$ is smaller than a resolution $\mathbf{v_a'}$, denoted $\mathbf{v_0'} \preceq \mathbf{v_a'}$ iff

$$||\mathbf{v_0'} - \mathbf{v_0}|| \leq ||\mathbf{v_a'} - \mathbf{v_0}|| \tag{6}$$

Functions of K2BD

k2bd

inputs:

- initial relative ownship position $s = (s_x, s_y)$
- absolute velocities $\mathbf{v_0} = (\mathbf{v_{0x}}, \mathbf{v_{0y}})$, $\mathbf{v_i} = (\mathbf{v_{ix}}, \mathbf{v_{iy}})$
- parametr $e = \pm 1$ – determines the particular tangent

outputs:

- $(\mathbf{v'_{0x}}, \mathbf{v'_{0y}})$

Functions of K2BD

recovery

inputs:

- the same as k2bd
- arrival time t''

outputs:

- $(t', \mathbf{v''_{0x}}, \mathbf{v''_{0y}})$
- t' – time of switch
- $(\mathbf{v''_{0x}}, \mathbf{v''_{0y}})$ – recovery velocity vector

Verification

- the resolution and recovery maneuvers are correct (satify formula 3,4,5)
- it was shown that resolution $\mathbf{v}'_{\mathbf{0}}$ computed by k2bd is optimal with respect to the order $\preceq$
- assumptions:
  - absolute ground speeds are different from zero
  - initial relative position and target point are external to P
  - the aircraft are in conflict before t''
- the correctness of the system has been formaly verified using Prototype Verification System (PVS) with the use of general results on real analysis available in NASA PVS Libraries and strategies for the manipulation of real expressions from PVS package Field and Manip