On the Formal Verification of Conflict Detection Algorithms

César Muñoz, Ricky W. Butler, Víctor A. Carreño, Gilles Dowek

21.4.2008

Contents of the article

- **motivation**: Air Traffic Control (ATC) $\longrightarrow$ *free-flight* (article from 14.5.2001)

- case study - simultaneous landing of 2 aircrafts *Airborne Information for Lateral Spacing ($AILS$)* - the alert algorithm verification

- physical equations give us axioms for PVS

- $AILS$ - correctness, uncertainty formally proved

Notation

x, y

bank angle ϕ

heading θ

ground speed v

evader

intruder

Assumptions

2 aircrafts

Maximal bank angle for commercial aircrafts

$$MaxBank = |\phi(t)| \leq 35\pi/180$$

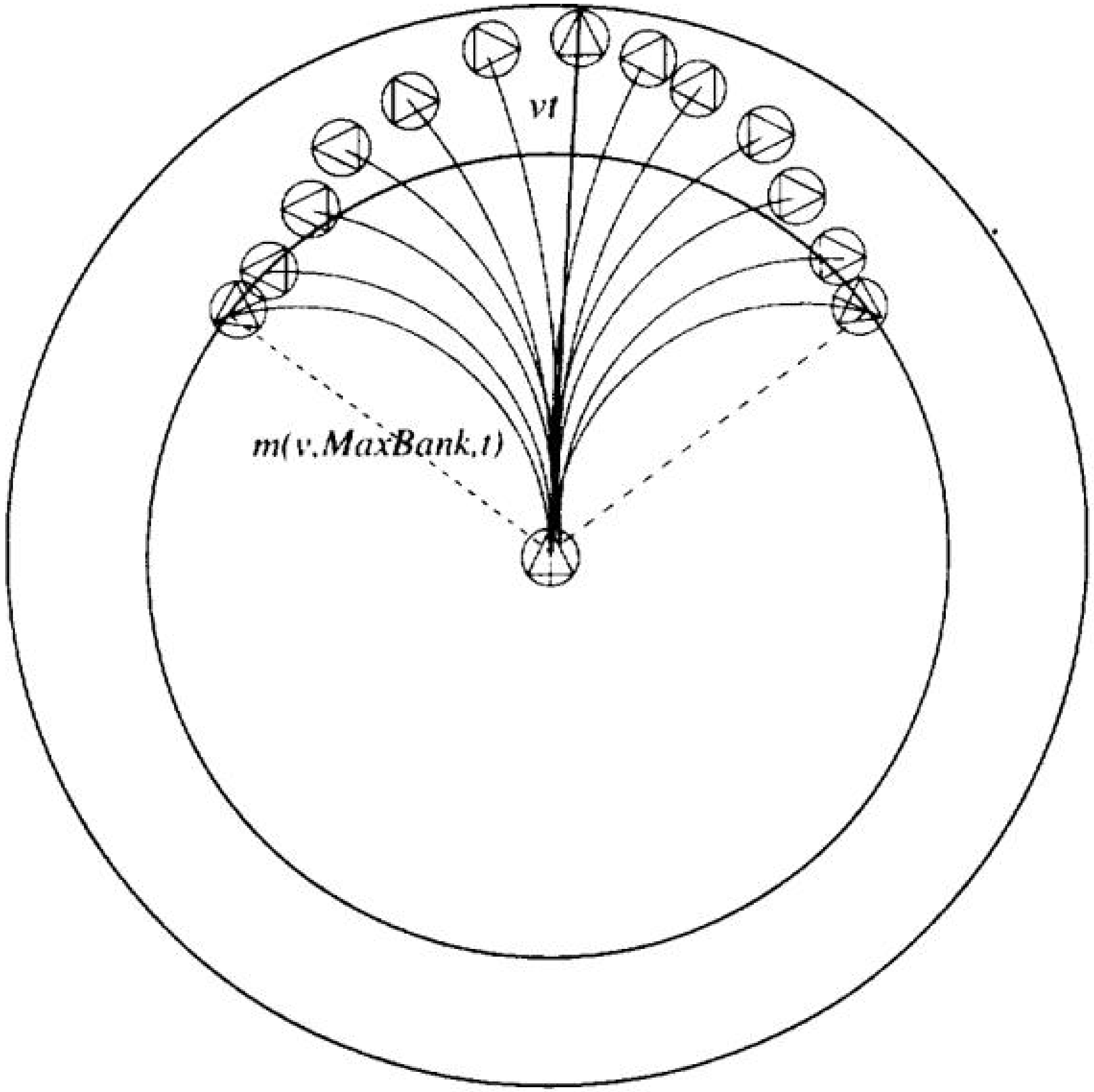
Minimal ground speed

$$v = 210 ft\, s^{-1} = 64.008\, m\, s^{-1}$$

2-dimensional trajectories

$$x'(t) = vcos(\theta(t)) \quad (1)$$
$$y'(t) = vsin(\theta(t)) \quad (2)$$
$$\theta'(t) = (g/v)tan(\phi(t)) \quad (3)$$

$$r(v, \phi) = v^2/(g\,tan(\phi)) \quad (4)$$
$$m(v, \phi, t) = 2r(v, \phi)sin(vt/2r(v, \phi)) \quad (5)$$
$$\rho(v) = (g/v)tan(MaxBank) \quad (6)$$


vt
m(v,MaxBank,t)

Theorems formally proven in PVS

Theorem 1 *YCGFTYS You Cannot Go Faster Than Your Speed.*

$$0 \leq t \;\Rightarrow\; \sqrt{(x(t) - x(0))^2 + (y(t) - y(0))^2} \leq vt$$

Theorem 2 *YCGSTYS You Cannot Go Slower Than Your Speed.*

$$0 \leq \rho(t) \leq 2 \;\Rightarrow\; \sqrt{(x(t) - x(0))^2 + (y(t) - y(0))^2} \leq vt$$

Assumptions

- evader - trajectory = straight line
- $\theta_e(t) = 0$, $\phi_e(t) = 0$, constant speed v_e parallel with the x-axis
- $\theta_i(t) = \theta$, $\phi_i(t) = 0$, constant speed v_i

Projected trajectories

$$x_e^*(t) = x_e(0) + v_e\, t \tag{7}$$

$$y_e^*(t) = y_e(0) \tag{8}$$

$$x_i^*(t) = x_i(0) + v_i\, t\, cos(\theta) \tag{9}$$

$$y_i^*(t) = y_i(0) + v_i\, t\, sin(\theta) \tag{10}$$

$$R(t) = \sqrt{\Delta_x(t)^2 + \Delta_y(t)^2}$$

Time of closest separation relative to t:

$$\tau(t) = -\frac{\Delta_x(t)\Delta'_x + \Delta_y(t)\Delta'_y}{{\Delta'_x}^2 + {\Delta'_y}^2}$$

Formally proven properties of τ

Lemma 3 *(derivative_eq_zero_min).*

$$R(t_1 + \tau(t_1)) \leq R(t_1 + t_2)$$

Lemma 4 *(asymptotic_decrease_tau).*

$$t_1 \leq t_2 \leq \tau(t) \;\Rightarrow\; R(t_1 + \tau(t_1)) \geq R(t_1 + t_2)$$

Lemma 5 *(asymptotic_increase_tau).*

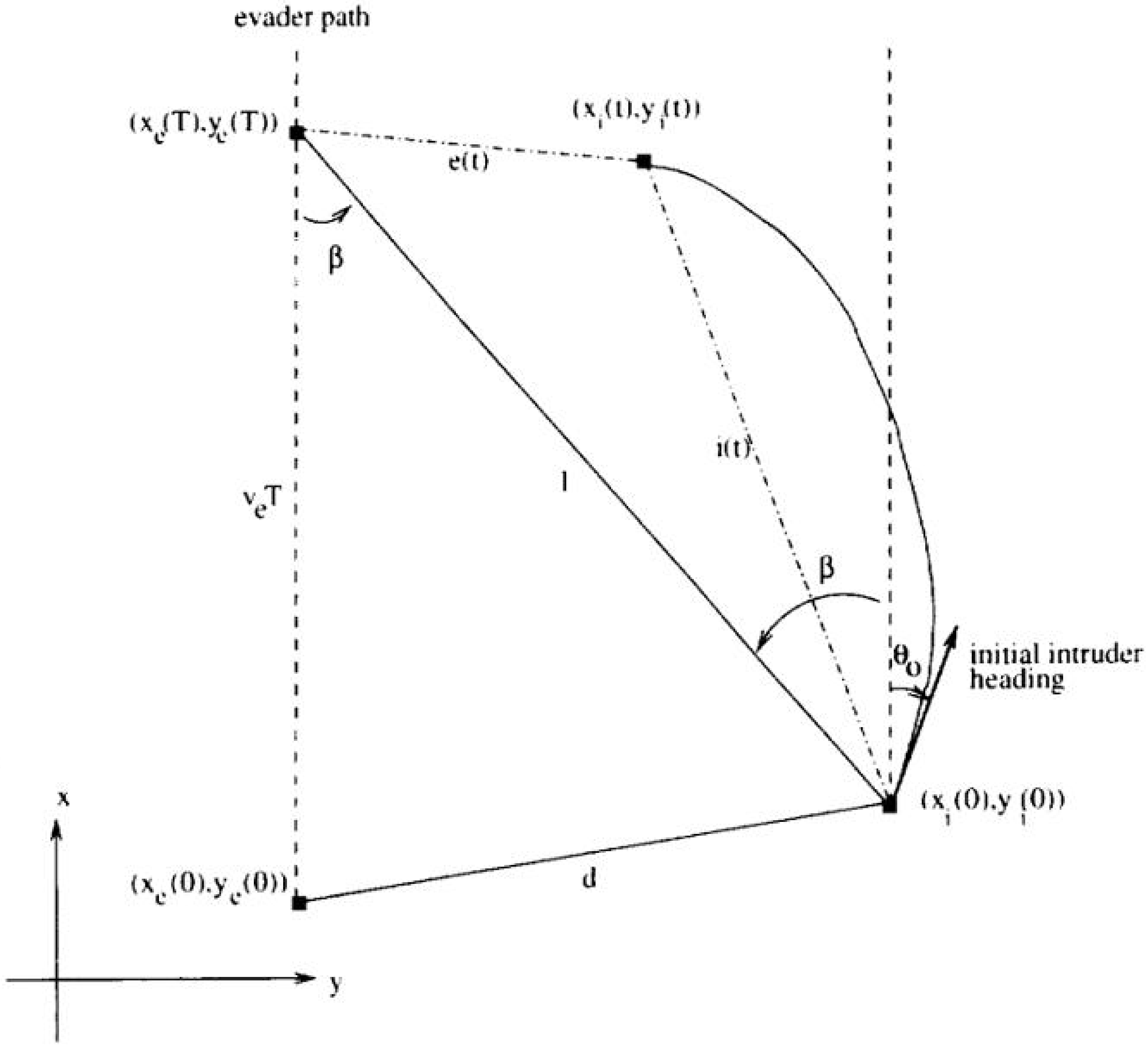
$$\tau(t) \leq t_1 \leq t_2 \;\Rightarrow\; R(t_1 + \tau(t_1)) \leq R(t_1 + t_2)$$

General Conditions for Conflict Avoidance

$$D_{ie}(t_i, t_e)$$

$$conflict_{ie}(t) \equiv D_{ie}(t,t) \leq ConflictRange$$

$(\neg conflict_{ie}(T)$ does not exclude earlier conflicts.)


evader path
$(x_e(T), y_e(T))$
$(x_i(t), y_i(t))$
e(t)
β
i(t)
l
v_eT
β
θ_o
initial intruder heading
$(x_i(0), y_i(0))$
$(x_e(0), y_e(0))$
d
x
y

$T \geq 0$, situations implying $\neg conflict_{ie}(T)$:

1. no_conflict_gt_max:
   $l > MaxDistance$, where $MaxDistance = v_i T + ConflictRange$, or

2. no_conflict_lt_min:
   $(l < MinDistance) \wedge (0 \leq \rho T \leq 2\pi)$,
   where $MinDistance = m(v_i, MaxBank, T) - ConflictRange$, or

3. no_conflict_omega:
   $(l > ConflictRange + v_i) \wedge (\rho T \leq \pi - \rho) \wedge (Omega(\beta + \theta(0)))$,
   where $Omega(\sigma) \equiv \sigma \in [\pi/2, 3\pi/2]$

4. If $v_i = v_e = 250 ft/s$, $AlertRange = 1400 ft$ (the AILS concept) ails_no_conflict_tau_le0:

$$(MinDistance \leq l \leq MaxDistance) \wedge (9.5 \leq T \leq 10) \wedge$$

$$(\neg Omega(\beta + \theta(0))) \wedge (d > AlertRange) \wedge (\tau(0) \leq 0)$$

Formal Verification of Inequalities

- square root: $\sqrt{a}^2 = a$ for $a \leq 0$

- monotonic_anti_deriv:
  $(c \in [a, b] \Rightarrow f'(c) \leq g'(c)) \Rightarrow (f(b) - f(a) \leq g(b) - g(a))$

- PI: $314/100 \leq \pi \leq 315/100$

- SIN: $(0 \leq a \leq \pi) \Rightarrow (sin_{lb}(a) \leq sin(a) \leq sin_{ub}(a))$

- COS: $(-\pi/2 \leq a \leq \pi/2) \Rightarrow (cos_{lb}(a) \leq cos(a) \leq cos_{ub}(a))$

Relative Coordinates

$$\begin{pmatrix} \widehat{x}(t) \\ \widehat{y}(t) \end{pmatrix} = \begin{pmatrix} cos(\theta(0)) & sin(\theta(0)) \\ -sin(\theta(0)) & cos(\theta(0)) \end{pmatrix} \begin{pmatrix} x(t) - x_e(T) \\ y(t) - y_e(t) \end{pmatrix}$$

isometric, (isometric_evader, isometric_intruder, majoration)

no_conflict_gt_max, no_conflict_lt_min, no_conflict_Omega, ails_no_conflict_tau_le0

AILS alert algorithm

input: projection of the trajectory - position, heading, speed (constant ground speed $250 ft/s$), bank angle

evader: on localizer

intruder: constant bank angle, can stay on the circle or leave it by a tangential trajectory with <3 deg

time-steps 0.5 s

output: the distance and time of minimal separation (alert if exceeds tresholds)

The original $AILS$ algorithm written in $FORTRAN$ at Langley Research Center, latest (2001) - for experimental Boeing 757 - by Honeywell.

Only traffic warnings assumed in the article.

PVS code . . . .

Verification of the AILS alert algorithm

Theorem 6 *(ails_correctness)*

$$\forall i, e.\ 9.5 \leq T \leq 10 \ \wedge conflict_{ie}(T)$$

$$\Rightarrow ails\_alert(measure2state(i, 0), measure2state(e, 0))$$

Theorem 7 *(ails_uncertainty)*

$$\exists s_i, s_e : State.\ \forall i, e :$$

$$(s_i = measure2state(i, 0) \wedge s_e = measure2state(e, 0) \wedge) :$$

$$(ails\_alert(s_i, s_e) \ \wedge \ \neq conflict_{ie}(T))$$

Conclusions of the article

- verification is better than simulation (certainty)
- continuous functions (discretization - errors)
- PVS and nonlinearities

Future work

1. > 2 aircrafts.

2. Vertical coordinate.

3. Data measurement errors.