Proceedings of the 2002 American Control Conference
Anchorage, Alaska, May 8-10, 2002

Delay Predictive Models of the National Airspace System Using Hybrid Control Theory[1]

Alexandre M. Bayen[2] Pascal Grieder[3] Henny Sipma[4] George Meyer[5]
Claire J. Tomlin[6]

Abstract

We present a model for analyzing and simulating the propagation of delays through several sectors of the Oakland Air Route Traffic Control Center. Aircraft are represented as points moving along straight lines with constant velocity, and the air traffic controller is modelled as an action which can provide instantaneous heading and velocity changes to each aircraft. If the controller action is restricted to one velocity change per aircraft, we show that the problem of computing the time that the controller action must be applied in order to achieve an exact metering constraint on the spacing between aircraft, may be solved analytically. More generally, the problem of computing the time that controller action must be applied on each aircraft, in order to satisfy a metering constraint and minimize the overall arrival time, may be posed and solved as a linear program. We show that cases involving heading change may be solved analytically using the theorem prover STeP. Finally, we validate our results through our simulator of air traffic control action in the Oakland Center.

1 Introduction

We are interested in constructing models and methods to study delay propagation in the National Airspace System. In particular, we are interested in estimating the capacity of sectors of airspace, and in understanding how this capacity is locally influenced by the sector air traffic control. In this paper, we restrict our study to several sectors within the Oakland Air Route Traffic Control Center (ARTCC) in Fremont, CA. We model aircraft as points moving along straight lines with constant velocity, and we model the air traffic controller as an action which can provide instantaneous heading and velocity changes to each aircraft. Aircraft are constrained to remain separated from each other by a minimum safety distance; we use 5nm lateral separation here. The kind of constraint that we are interested in satisfying is a "metering constraint", which means that the time between aircraft arrivals at the exit point of a sector is constrained to be not less than ΔT seconds, where ΔT is dictated by capacities of sectors or landing capacities of the destination airport. We derive solutions to the following two flow problems:

1. *Given a metering constraint of ΔT, compute a controller policy which will force groups of aircraft to* exactly *satisfy the metering constraint at the sector exit point (each aircraft is separated by exactly ΔT) while maintaining separation;*
2. *Given a metering constraint of ΔT, compute a controller policy which provides at most one aircraft every ΔT while maintaining separation, and minimizes the overall arrival time of the aircraft within each group.*

We solve the first problem analytically for a single velocity change (we obtain a closed form solution), the second we solve using a linear program (LP), and thus obtain a numerical solution. Methods based on analytical models (which we will denote here as formal methods) are provably correct by design. This is in sharp contrast with simulation, which proves a result only for the parameters and initial conditions simulated. For example, the works of Feron and Bilimoria [1, 2] provide an analytic framework, upon which the authors build tools to assess throughput and safety of the flows they investigate. Other works investigate the impact of decentralized control on air traffic flow and airspace capacity [3, 4, 5]. We demonstrate how the analytical approach may be extended using the deductive theorem prover STeP (Stanford Temporal Prover, see [6]). We compare our results with those from simulation, using a sector controller which has a "myopic" view – each controller can only see and control aircraft within its own sector. The simulated controller attempts to minimize a cost function, which encodes a set of priorities for the controller: ensuring that loss of separation (LOS) never happens is highest priority, attempting to

[1]Research supported by a graduate fellowship of the Délégation Générale pour l'Armement (France), by NASA Ames under grant NASA/NCC 2-5422 and by the DARPA Software Enabled Control (SEC) Program administered by AFRL under contract F33615-99-C-3014.

[2]Corresponding author. Hybrid Systems Laboratory, Department of Aeronautics and Astronautics, Stanford University, CA 94305-4035. bayen@stanford.edu. Tel: (650)-736-1423.
[3]Department of Electrical Engineering, ETHZ, Switzerland.
[4]Department of Computer Science, Stanford, CA.
[5]NASA Ames Research Center, Moffett Field, CA.
[6]Hybrid Systems Laboratory, Department of Aeronautics and Astronautics, Stanford University, CA.

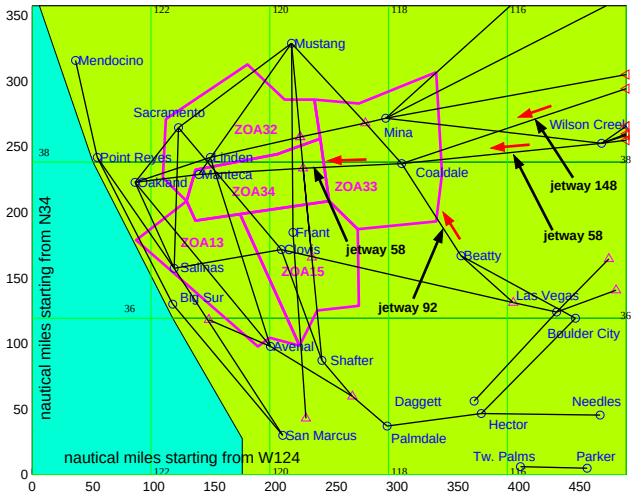

Figure 1: Airspace modeled by our simulator. The data modeled comes from FACET [7] as well as JEPPESEN high altitude enroute charts [9].

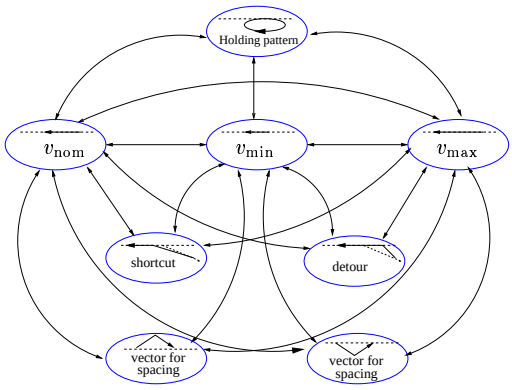

Figure 2: Hybrid automaton representing the actuation of one controller on a single aircraft. Each of the eight modes represents one possible state of the aircraft. The arrows joining these states are the mode switches, initiated by the controller.

meet the metering condition is of second highest priority, and efficiency criteria, such as delay minimization, are included at lower priority. We are currently in the process of validating this simulator against ETMS data [7, 8]. The simulation thus attempts to imitate the actions of a real controller; and the comparison between our analytical (and linear programming) results and the simulator results allows us to consider our analytic models as representative of reality. In Section 2, we present the model and simulation, in Section 3 we present our analytic results. The results in STeP for extending this analysis is presented in the Appendix. Finally, we describe our current work in using validated abstractions of this sector model as building blocks in a model of several networked sectors.

2 Simulations

We have created a simulator of air traffic flow in sectors 13, 15, 32, 33, 34 (see Figure 1; ZOA indicates Oakland Center). Full details of the model, as well as implementation details are given in [8]. This simulator attempts to imitate air traffic controller behavior by using a simple hybrid automaton model for each aircraft. Each aircraft is modeled as a system with eight possible modes, depicted in Figure 2: three different speeds, shortcuts or detours between jetways, two types of vector for spacing, and holding patterns. The maneuvers minimize a cost function designed to match controller priority in selecting the maneuvers:

$$J = \sum_{i=1}^{N} n^i_{\text{LOS}} \cdot w_{\text{LOS}} + \sum_{i=2}^{N} (T^i_{\text{breach}})^2 \cdot w_{\text{breach}}$$
$$+ \sum_{i=1}^{N} J^i_{\text{man}} + \sum_{i=1}^{N} (TOA^i_{\text{calc}} - TOA^i_{\text{real}}) \cdot w_{\text{delay}}$$
$$+ N_{\text{moved}} \cdot w_{\text{single move}}$$

Here, N denotes the number of aircraft in a given sector. Each term in the sum consists of a penalty: the respective subscripts "LOS", "breach", "man", "delay", "single move" respectively stand for loss of separation, breach of boundary condition, maneuver, delay, and single maneuver. These penalties are: the number n^i_{LOS} of losses of separation, the squared breach times of miles-in-trail constraints, the costs of each individual maneuver, the difference between predicted and actual time of arrival (TOA) at destination, the number of maneuvers. The logic of the air traffic controller is modeled as follows: the highest priority is to maintain separation, the next highest priority is to meet the metering constraint, the rest of the penalties reflect equal and lowest priority:

$$w_{\text{LOS}} \sim 10^{300} \gg w_{\text{breach}} \sim 10^5 \gg w_{\text{delay}} \sim 1$$

Each sector controller takes input flight plans within his own sector and attempts to generate a conflict-free environment according to the cost function and weights above. Each sector in the set of five that we are considering is actuated according to the minimum of J for the aircraft in that particular sector.

3 Analytical solutions to metered flows

In order to assess analytically how quickly a jetway can become saturated with aircraft, we create a simple model of merging flow. So far, we only deal with "quasi one-dimensional" flows, but the long term goal of this

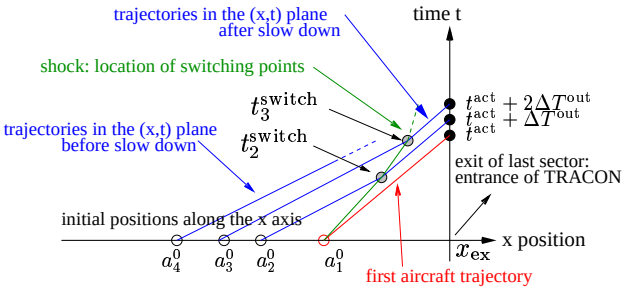

Figure 3: Shock construction (which represents the solution to the maximal throughput problem). The aircraft trajectories are represented in the (x,t) plane. They originate at $t=0$ from the horizontal axis (white circle on each trajectory). After some amount of time, the aircraft is switched to speed $\underline{v}$ at location $(x_i^{\text{switch}}, t_i^{\text{switch}})$ (shaded circle on each trajectory). Ultimately they reach x_{ex}, the entrance of TRACON (black circle).

approach is to be able to formulate multidimensional flows in the same way. The following scenario is investigated: N aircraft are converging at high velocity $\overline{v}$ to a jetway junction and "pile up" (meaning, fly at the minimal allowed separation, one behind the other) in the order of their original (predicted) arrival time at sector exit. The "piling up" process occurs by the controller slowing each aircraft to a lower velocity $\underline{v}$ (before or after the junction) in order to ensure that aircraft i (where $i \in [1,N]$) exits the sector at a prescribed time $t^{\text{act}}+(i-1)\Delta T^{\text{out}}$. Here ΔT^{out} represents the metering constraint (one aircraft every ΔT^{out} seconds) imposed at the exit of the sector, and t^{act} its time of activation, defined as the time when the first aircraft exits the sector. The position of aircraft i in time is thus described by two affine functions:

$$\begin{aligned} x_i(t) &= a_i^0 + \overline{v}t \quad t \in [0, t_i^{\text{switch}}] \\ x_i(t) &= b_i + \underline{v}t \quad t \in [t_i^{\text{switch}}, t^{\text{act}} + (i-1)\Delta T^{\text{out}}] \end{aligned}$$

Here, a_i^0 is the position of aircraft i at $t=0$, b_i is related to the switching time by $t_i^{\text{switch}} = (b_i - a_i^0)/(\overline{v}-\underline{v})$, and needs to be computed in order to satisfy required metering conditions. We are interested in solving the following problem: *Find the switching point and switching time* $(x_i^{\text{switch}}, t_i^{\text{switch}})$ *of each aircraft* i *so that each aircraft crosses the exit point* x_{ex} *of the sector at exactly* $t^{\text{act}} + (i-1)\Delta T^{\text{out}}$. For a given set of initial conditions $\{a_i^0\}_{i\in[1,N]}$, it can be shown quite easily that this problem is feasible if for all i:

$$\begin{aligned} & a_i^0 \geq x_{\text{ex}} - \overline{v}(t^{\text{act}} - (i-1)\Delta T^{\text{out}}) \\ \text{and} \quad & a_i^0 \leq x_{\text{ex}} - \underline{v}(t^{\text{act}} - (i-1)\Delta T^{\text{out}}) \end{aligned} \tag{1}$$

When this condition is met, the switching time and switching point of aircraft i are given by:

$$\boxed{\begin{aligned} t_i^{\text{switch}} &= \frac{x_{\text{ex}} - \underline{v}t^{\text{act}} - (i-1)\Delta L - a_i^0}{\overline{v}-\underline{v}} \\ x_i^{\text{switch}} &= a_i^0 + \frac{\overline{v}[x_{\text{ex}} - \underline{v}t^{\text{act}} - (i-1)\Delta L - a_i^0]}{\overline{v}-\underline{v}} \end{aligned}} \tag{2}$$

where $\Delta L := \underline{v}\Delta T^{\text{out}}$. ΔL is the equivalent "miles-in-trail" constraint corresponding to the ΔT^{out} throughput metering condition. It can be proved that if $\Delta L > 5$ nautical miles and $a_i^0 - a_{i-1}^0 > 5$ nautical miles, (2) preserves separation until x_{ex} (in fact indefinitely if the aircraft do not change speed after x_{ex}). The location of the $(x_i^{\text{switch}}, t_i^{\text{switch}})$ in space represents a wavefront. Upstream from the wavefront, aircraft are at maximal speed. Downstream from the wavefront, the aircraft are "piled up" at low speed in order to cross the x_{ex} boundary at $t^{\text{act}} + (i-1)\Delta T^{\text{out}}$ exactly. These results give conditions on the inflow (i.e. on the set of a_i^0) for the wavefront to move toward the exit of the sector (which means the traffic jam will thus disappear):

$$\begin{aligned} t_i^{\text{switch}} < t_{i+1}^{\text{switch}} \quad &\Leftrightarrow \quad \Delta L < a_i^0 - a_{i+1}^0 \\ x_{i+1}^{\text{switch}} < x_i^{\text{switch}} \quad &\Leftrightarrow \quad \left(\frac{1}{\Delta L}\right)\underline{v} < \left(\frac{1}{a_i^0 - a_{i+1}^0}\right)\overline{v} \end{aligned} \tag{3}$$

The construction of the $(x_i^{\text{switch}}, t_i^{\text{switch}})$ points is depicted in Figure 3. An example is depicted in Figure 4. The benefit of this formulation is that equation (2) gives an analytic solution to any set $\{a_i^0\}_{i\in[1,N]}$, thus providing a switching policy to apply, and a proof by design that this procedure is safe (if the aircraft are originally separated by more than 5 nm, they will always be). However, the condition that each aircraft reaches x_{ex} exactly at the time prescribed is restrictive (what is important is the flow rate but not the actual crossing times). Therefore it would be of greater use to pose the problem as follows: *Given* $\{a_i^0\}_{i\in[1,N]}$, *compute the switching policy which provides at most one aircraft every* ΔT^{out} *at* x_{ex} *while maintaining separation, and minimizes the arrival time of aircraft* N.

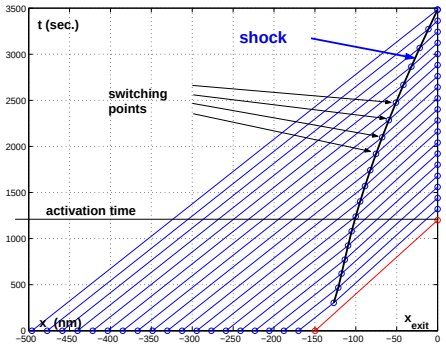

Figure 4: Shock obtained by (2) for a given set $\{a_i^0\}$ satisfying (1) for all $i \in [1,N]$. The shock therefore vanishes (here at time t=3500 sec.). In this case (3) is satisfied, and we thus see that: $x_i^{\text{switch}} < x_{i+1}^{\text{switch}}$, and $t_i^{\text{switch}} < t_{i+1}^{\text{switch}}$, i.e. the shock moves downstream. At $t=3500$, it vanishes. We see that $t_2^{\text{switch}} < t^{\text{act}}$, which means that in order to meet the metering conditions, action from the controller has to be taken prior to arrival of aircraft 1 at x_{ex}.

This cannot be solved analytically as easily because the arrival time of aircraft are now variables (i.e. are

not set as in the previous formulation, but need to be computed while satisfying constraints). However, this problem may be posed as a linear program: minimize the arrival time of aircraft N (**a.**), while separating the aircraft by more than ΔT^{out} at x_{ex} (**b.**), with at most one switch between the initial position $a_i^0 \leq x_{\text{ex}}$ and the exit x_{ex} (**c.**):

a. Minimize $[0, \cdots 0, -1]\vec{b}$

b. Subject to

$$\begin{bmatrix} -1 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & -1 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & -1 & 1 & 0 \\ 0 & \cdots & \cdots & 0 & -1 & 1 \end{bmatrix} \vec{b} \succeq \underline{v} \begin{bmatrix} \Delta T^{\text{out}} \\ \vdots \\ \vdots \\ \vdots \\ \Delta T^{\text{out}} \end{bmatrix}$$

c. $\vec{a} \preceq \vec{b} \preceq \frac{v}{\overline{v}}\vec{a} + \left(1 - \frac{v}{\overline{v}}\right) x_{\text{ex}}[1, \cdots, 1]^T$

where $\vec{a} = [a_1^0, \cdots, a_N^0]^T$ and $\vec{b} = [b_1, \cdots, b_N]^T$. Note that the RHS of **b.** in the previous formula can be changed to $[\Delta T_1, \cdots, \Delta T_N]^T$ in order to account for time-varying boundary conditions. The advantage of this formulation is the possibility to optimize an objective function (which is in the present case the arrival time of the last aircraft in the platoon, see Figure 5), at the price of a numerical solution. However this problem has been sufficiently well studied for us to consider the numerical results exact, modulo the accuracy provided by the code. An example of such construction is given

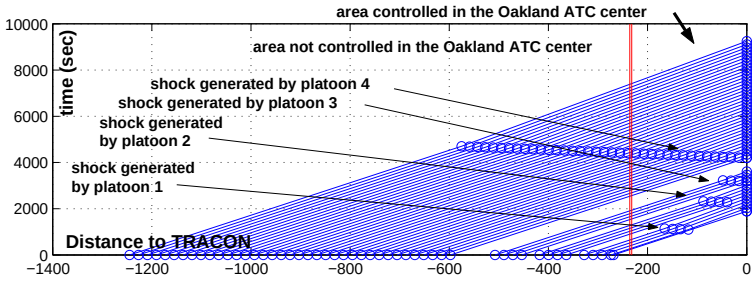

Figure 5: Shocks obtained for four successive platoons of aircraft using the linear programming formulation. Only the last one exits the Oakland ATC center and therefore generates a breach in metering conditions shown in Figure 6.

in Figure 5 with objective function $[-1, \cdots, -1]^T\vec{b}$, i.e. the sum of all aircraft arrival times is minimized. This figure displays four platoons of aircraft subjected to a 18 miles in trail at maximal speed $\overline{v}$. The first three platoons form three shocks which are included in the airspace controlled by the Oakland Center (Figure 5). The fourth clearly exits the controlled area, and the solution indicates that the corresponding aircraft need to be actuated prior to entry in the Oakland Center.

Now applying this case to our simulator with velocity changes only, we are able to actuate the three first

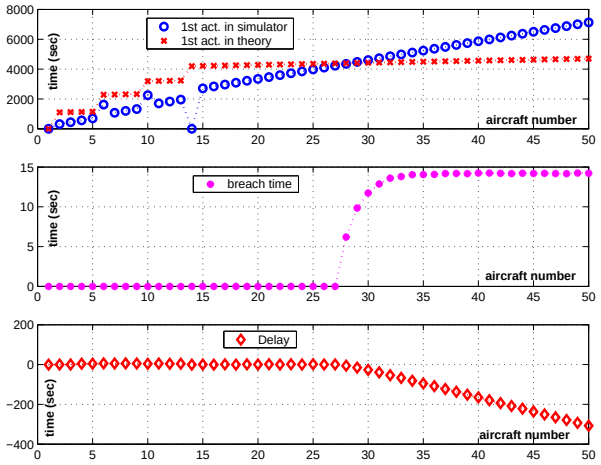

Figure 6: Delay times for four platoons of Figure 5.

platoons, and no breach in boundary conditions is observed (Figure 6 top and middle). The fourth platoon is so large that its required domain of actuation goes beyond the border of the Oakland ATC Center (Figure 5). We see, that as soon as the first switching time crosses the sector boundary, the predicted first time of actuation of the simulator becomes greater than the time of the analytical solution (Figure 6, aircraft 28). All following aircraft cannot be actuated in time and therefore breach the boundary condition by an amount shown in Figure 6 center, which reaches a steady state after aircraft 35. The breach time in the simulator can be predicted analytically and results from the impossibility of the shock wave to travel through the boundary of the sector. The best the simulator can do to meet the boundary conditions is to slow down the aircraft as soon as they enter the Oakland airspace. Doing so produces a flow separated by $\Delta L_{\text{inflow}}\frac{v}{\overline{v}}$ where $\Delta L_{\text{inflow}} = 18$ nm is the initial separation of the aircraft. Since the requested separation (for the metering conditions) at the exit of the sector is $\Delta L_{\text{outflow}} = 20$nm at maximal speed $\overline{v}$, the breach time will be:

$$t_{\text{breach}} = \frac{1}{\underline{v}}\left[\frac{\underline{v}}{\overline{v}}\Delta L_{\text{outflow}} - \frac{\underline{v}}{\overline{v}}\Delta L_{\text{inflow}}\right]$$

The predicted breach time in the case of Figure 5 is thus 14 sec. (which we verify on Figure 6). We now list the benefits of the analytical model we provide.

1. The use of formulae (1) and (2) provides a proof by design of the switching policy preserving separation while meeting metering conditions for merging traffic. This can be used on actual data for flight scheduling.
2. Formula (3) enables identification of upstream flows which will potentially generate airspace saturation. It enables classification of "jamming flows" vs. "non-jamming flows".
3. The linear programming formulation of the previous

problem enables the same predictions of more general flows (with platoons and holes), without analytical results but with guaranteed numerical accuracy.

4. Applications of these techniques include systematic computation of jamming times for jetway junctions used for future models. For example, the jamming time of a particular location $x_{\text{particular}}$ on a jetway can be computed by setting x_i^{switch} to $x_{\text{particular}}$ and solving for the smallest i satisfying the second equation in (2).

4 Conclusion

We thus have provided two models to assess how long it takes to saturate a given portion of airspace. We have correlated these results with numerical results obtained with our simulator, thus assessing their applicability to the real system. Our current interest is in producing similar models for more complex flows and extracting key parameters from the flow at sector level in order to build a higher scale model of the National Airspace System. We thus hope to be able to predict delay propagation in a wider area of the system.

References

[1] Z. Mao, E. Feron, and K. Bilimoria, "Stability of intersecting aircraft flows under decentralized conflict avoidance rules," in *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, (Denver, CO), August 2000.

[2] D. Dugail, Z.-H. Mao, and E. Feron, "Stability of intersecting aircraft flows under centralized and decentralized conflict avoidance rules," in *Proceedings of the AIAA Guidance, Navigation, and Control Conference*, (Montreal, Canada), August 2001.

[3] D. Bertsimas and S. S. Patterson, "The air traffic flow management problem with enroute capacities," *Operations Research*, vol. 46, pp. 406–422, 1998.

[4] A. Bicchi, A. Marigo, G. Pappas, M. Pardini, G. Parlangeli, C. Tomlin, and S. Sastry, "Decentralized air traffic management systems: Performance and fault tolerance," in *Proceedings of the IFAC Workshop on Motion Control*, (Grenoble, France), 1998.

[5] J. Alliot, N. Durand, and G. Granger, "FACES: A free flight autonomous and coordinated embarked solver," in *Proceedings of the 2nd USA/Europe Air Traffic Management R& D Seminar*, December 1998.

[6] Y. Kesten, Z. Manna, and A. Pnueli, "Verification of clocked and hybrid systems," *Acta Informatica*, vol. 36, no. 11, pp. 837–912, 2000.

[7] K. Bilimoria, B. Sridhar, G. Chatterji, K. Seth, and S. Graabe, "FACET: Future ATM concepts evaluation tool," in *3rd USA/Europe Air Traffic Management R&D Seminar*, (Naples, Italy), June 2001.

[8] A. Bayen, P. Grieder, and C. Tomlin, "A control theoretic predictive model for sector based air traffic flow." January 2002.

[9] Jeppesen, "High altitude enroute charts," tech. rep., http://www.jeppesen.com, February 2000.

5 Appendix: formal proofs in STeP

The formulations of Section 3 are limited by their inherent simplistic geometry (quasi one-dimensional traffic). In order to deal with general flow configurations, it is possible to automate part of the analysis using a theorem prover (STeP) [6] to formally prove no loss of separation given certain maneuvers. Below we present a simple example used to assess the feasibility of this approach and to illustrate the technique.

We model the junction of jetways 92 and 148 into 58 (taken to be a straight line extension of jetway 148 for convenience) at Coaldale (see Figure 1). We consider two aircraft: aircraft 1 approaches Coaldale from the east on jetway 148 and aircraft 2 approaches Coaldale from the south on jetway 92. If the relative positions of aircraft 1 and aircraft 2 are such that a loss of separation might happen near Coaldale, aircraft 2 is rerouted onto a shortcut bypassing Coaldale. The situation is depicted in Figure 7. We cast the system in a hybrid automaton format consisting of both discrete actions (aircraft switching jetways) and continuous components (the positions of the aircraft). A hybrid transition system (HTS) $\mathcal{H} : \langle V, \Theta, \mathcal{T}, \mathcal{C}, \mathcal{A} \rangle$ consists of the following components (see [6]):

1. V: a set of system variables, including both discrete, that is modified according to discrete transitions, and continuous variables, whose behavior is governed by differential equations. A *state* of the system is a valuation of all variables.

2. Θ: an assertion over V characterizing initial states.

3. $\mathcal{T}$: a set of discrete transitions. Each transition τ is written as the combination of an enabling condition, an assertion that characterizes the states in which the transition can be taken, and a list of assignments to V, indicating the values in the next state if the transition is taken.

4. $\mathcal{C}$: a set of constraints. Each constraint is an assertion over V. Time can progress only if all constraints are true. Constraints are used to force transitions to be taken.

5. $\mathcal{A}$: a set of activities, where an activity consists of an enabling condition defined on discrete variables only, determining in which states the activity applies, and a set of differential equations describing the behavior of the continuous variables.

A behavior of an HTS is an infinite sequence of states $\sigma : s_0, s_1, \ldots$, such that:

1. The state s_0 satisfies the initial condition Θ.

2. For all $i \geq 0$, some transition $\tau \in \mathcal{T}$, takes the system from s_i to s_{i+1}.

In this setting we model our system as follows:

1. V: the continuous variables are the positions of the two aircraft: (x_1, y_1), and (x_2, y_2) ranging over the reals. The discrete variables are the jetways the two aircraft are currently on: j_1 and j_2 taking value in $\{jw_{148}, jw_{92}, jw_{\text{off}}\}$, and a clock c that measures the time elapsed since the initial position, or the last transition taken.

2. $\mathcal{T}$: the system has four transitions, representing that (i) aircraft 2 turns from jetway 92 to jetway 148:

$$\tau_1 : \; j_2 = jw_{92} \; \wedge \; y_2 = y_c \; \wedge \; j_2' = jw_{148}$$

(ii) aircraft 2 turns from jetway 92 to the shortcut when loss of separation could occur at point A in Figure 7:

$$\tau_2 : \left(\begin{array}{c} j_2 = jw_{92} \; \wedge \; j_2' = jw_{\text{off}} \wedge \\ x_{1i} \geq x_{2i} - 5 + r \cdot (y_{1i} - y_{2i} - 5) \wedge \\ x_{1i} \leq x_{2i} + 5 + r \cdot (y_{1i} - y_{2i} - 5) \wedge \\ c = t_\ell - t_d \end{array} \right)$$

where $r = (v_{92x} - v_{148x})/v_{92y}$, (x_{1i}, y_{1i}) is the initial position of aircraft 1 (same for aircraft 2), the subscripts x and y on the velocities v_{92}, v_{148} and v_{58} represent the x and y components of those velocities, t_ℓ is the time from the initial position until potential loss of separation under the given conditions: $t_\ell = (y_{1i} - y_{2i} - 5)/v_{92y}$, (x_c, y_c) the coordinates of Coaldale, and t_d is the prescribed lead time to switch before loss of separation occurs; (iii) aircraft 2 turns from jetway 92 to the shortcut when loss of separation occurs between point A and Coaldale:

$$\tau_3 : \left(\begin{array}{c} j_2 = jw_{92} \; \wedge \; j_2' = jw_{off} \wedge \\ x_{1i} \leq x_{2i} + 5 + r \cdot (y_{1i} - y_{2i} - 5) \wedge \\ x_{1i} \leq x_{2i} + 5 + r \cdot (y_{1i} - y_{2i}) \wedge \\ c = (x_{1i} - x_{2i} - 5)/(v_{92x} - v_{148x}) - t_d \end{array} \right)$$

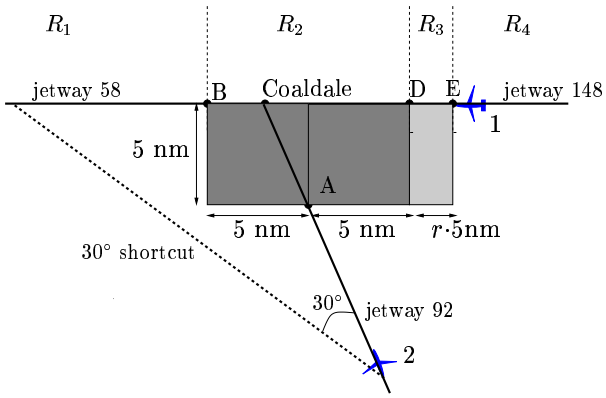

Figure 7: R_1 to R_4 represent the four regions investigated by STeP for the proof (see Figure 8); $r = \frac{v_{92x} - v_{148x}}{v_{92y}}$; the boxes represent a square of 5nm used for conflict detection. Jetways 58 and 148 are identical.

(iv) aircraft 2 merges from the shorcut to jetway 148 (jetway 58):

$$\tau_4 : \; j_2 = jw_{\text{off}} \; \wedge \; y_2 = y_c \; \wedge \; j_2' = jw_{148}$$

3. The constraints are as follows: (i) Aircraft 2 must never get to the north of Coaldale:

$$C_1 : \; y_2 \leq y_c$$

(ii) when there could be a loss of separation at Coaldale, aircraft 2 must not stay on jetway 92 beyond a prescribed switching time (which will be computed by this method and certified):

$$C_2 : \quad \begin{array}{l}(j_2 = jw_{92} \; \wedge \; x_{1i} \geq x_{2i} - 5 + r \cdot (y_{1i} - y_{2i} - 5) \; \wedge \\ x_{1i} \leq x_{2i} + 5 + r \cdot (y_{1i} - y_{2i} - 5)) \; \rightarrow \; c \leq t_\ell - t_d\end{array}$$

and similarly for transition τ_3 and τ_4.

4. The system has four activities, one per aircraft and jetway:

$$\begin{array}{l} A_1 : j_1 = jw_{148} \; \rightarrow \; \dot{x}_1 = v_{148x} \; \wedge \; \dot{y}_1 = 0 \\ A_2 : j_2 = jw_{92x} \; \rightarrow \; \dot{x}_2 = v_{92x} \; \wedge \; \dot{y}_2 = v_{92y} \\ A_3 : j_2 = jw_{\text{off}} \; \rightarrow \; \dot{x}_2 = v_{\text{off}x} \; \wedge \; \dot{y}_2 = v_{\text{off}y} \\ A_4 : j_2 = jw_{148} \; \rightarrow \; \dot{x}_2 = v_{148x} \; \wedge \; \dot{y}_2 = 0 \end{array}$$

The objective is to derive the control policy such that the two aircraft, independent of their initial positions, maintain sufficient separation, expressed by the invariant:

$$x_1 - x_2 \geq 5 \; \vee \; x_1 - x_2 \leq -5 \; \vee \; y_1 - y_2 \geq 5$$

We prove this using an *invariance diagram*, a concise representation of a proof that a system satisfies an invariance property. An invariance diagram is a directed graph consisting of a set of nodes N and a set of edges E, in which the nodes are labeled with assertions. Associated with an invariance diagrams are a set of verification conditions:

Initiation: each initial state must be represented in the diagram: $\Theta \; \rightarrow \; \mu(N)$ where $\mu(N)$ refers to the disjunction of the assertions of all nodes in N.
Consecution: for each state in the diagram, its successor state must also be in the diagram, that is, for each node $n \in N$, for each transition $\tau \in \mathcal{T}$ and for each timestep allowed by the constraints, $\mu(n) \; \wedge \; \tau(V, V') \; \rightarrow \; \mu'(n) \; \vee \; \mu'(succ(n))$ where $\mu(n)$ refers to the assertion labeling node n, and $\mu(succ(n))$ refers to the disjunction of the assertions labeling the successor nodes of n. Primed values refer to the values of the variables in the next state.

If all verification conditions associated with the diagram are valid, then the system satisfies the property $\mu(N)$, and automatically any property implied by $\mu(N)$. The diagram for the system under consideration is shown in Figure 8. For lack of space most of the assertions from the diagram are omitted. For this we have taken the following values for the parameters:

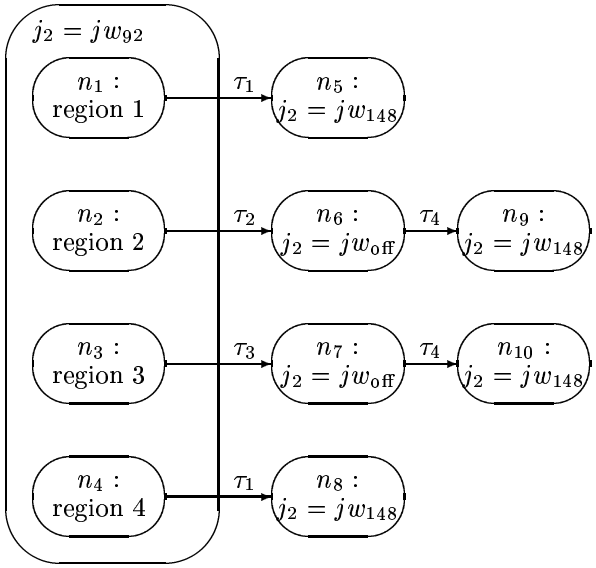

Figure 8: Invariance diagram for proving safety of the aircraft encounter. The four regions are constructed manually. The rest of the proof is realized by STeP.

$$\begin{array}{l} v_{148x} = -0.13, \; v_{148y} = 0, \; v_{92x} = -0.08, \; v_{92y} = 0.1 \\ v_{\text{off}x} = -0.12, \; v_{\text{off}y} = 0.05 \\ y_{1i} = 60, \; x_{2i} = 91, \; y_{2i} = 15 \\ x_c = 57, \; y_c = 60 \end{array}$$

which correspond to a speed of $M = 0.85$ at 33,000ft and a shortcut of 30°. All distances are given in nm and velocities in nm/s. Note that the initial position x_{1i} is unspecified. The proof covers all values of $x_{1i} \in \mathbb{R}$. In fact this corresponds to aircraft 2 being 10 minutes from Coaldale, and aircraft 1 in a range of 10 to 12 minutes from Coaldale. The diagram proves [1] that for all initial positions of aircraft 1 on jetway 148, that is for all values of x_{1i} in the given range, for the given initial position of aircraft 2, for the given velocities, and for the prescribed maneuver of switching to the shortcut, there exists a safe switch of aircraft 2 as long as it happens at least $t_d = 400$ sec before Coaldale.

This example illustrates the initial feasibility of the use of STeP as an automated analysis tool for this problem. Even more interesting is the fact that the complexity of the computation is quadratic in the number of aircraft, and thus we feel that the potential of STeP is good for automating the analysis of several aircraft, which cannot be done by hand.

[1] Full proof available from the authors. Here is a quick sketch.
Nodes n_1 through n_4 characterize the four different regions aircraft 1 would be in when aircraft 2 reaches point A. If aircraft 1 would be in region 2 or 3, aircraft 2 is switched onto the shortcut by transitions τ_2 and τ_3 respectively. If the aircraft would be in regions 1 or 4, no loss of separation will occur, because aircraft 1 is either well ahead (region 1) or well behind (region 4) when aircraft 2 reaches point A. Therefore no switch is necessary, and transition τ_1 is taken to transfer to jetway 148.
Nodes n_6 and n_7 represent the states where aircraft 2 is on the shortcut, and the remaining nodes represent the states where both aircraft are on jetway 148.
For all nodes, the assertions labeling the nodes imply the property

$$x_1 - x_2 \geq 5 \; \vee \; x_1 - x_2 \leq -5 \; \vee \; y_1 - y_2 \geq 5$$