Proceedings of the
47th IEEE Conference on Decision and Control
Cancun, Mexico, Dec. 9-11, 2008

Reachability Calculations for Automated Aerial Refueling

Jerry Ding, Jonathan Sprinkle, S. Shankar Sastry and Claire J. Tomlin

Abstract— **This paper describes Hamilton-Jacobi (HJ) reachability calculations for a hybrid systems formalism governing unmanned aerial vehicles (UAVs) interacting with another vehicle in a safety-critical situation. We use this problem to lay the foundations toward the goal of refining or designing protocols for multi-UAV and/or manned vehicle interaction. We describe here what mathematical foundations are necessary to formulate verification problems on reachability and safety of flight maneuvers. We finally show how this formalism can be used in the chosen application to inform UAV decisions on avoiding unsafe scenarios while achieving mission objectives.**

I. INTRODUCTION

In modern autonomous flight systems, the tasks of control and management of aircraft are often distributed between the onboard autonomous controller and external human operators. In safety-critical maneuvers, the decision authority almost exclusively resides with the human operators. However, this makes controlling large numbers of autonomous vehicles highly inefficient and prone to human errors. An important consideration is thus how the UAV would detect and respond to situations where the human input would place the UAV in imminent danger. In this paper, we develop a hybrid system formalism and some verification approaches for a particular safety-critical flight scenario, as a first step towards constructing automated decision protocols that can be formally verified to ensure the safe operation of mixed-initiative systems.

As a practical motivation, we consider the specific case of Automated Aerial Refueling (AAR). During a refueling operation, an unmanned aerial vehicle (UAV) first detaches from its formation and then approaches the rear of a tanker aircraft for refueling. The boom operator onboard the tanker would then lower a fuel boom (essentially a rigid fuel nozzle) to refuel the UAV. Once the refueling is complete, the operator would disconnect the boom and the UAV would rejoin its formation.

As we will discuss in this paper, the entire process can be formulated in terms of a hybrid system where a finite number of discrete states and state transitions are defined, as well as continuous control laws and system models defined within the individual states. With a hybrid system formulation, one could then apply reachable set theory [1] to verify the feasibility and safety of any given maneuver or operator command. There are many different ways to compute reachable sets, the method based on Hamilton-Jacobi PDEs, presented in [1], is used here.

For each state transition and escape maneuver, one could compute the capture reachable set, which is the set of aircraft states from which a maneuver can be completed within a finite time horizon. The UAV could then consult this data in real-time to determine a strategy for completing the refueling sequence under time constraints. Furthermore, given that the UAV would need to come into close proximity of the tanker aircraft, one would like to avoid collisions in the event of disturbances, for example air turbulence, variations in tanker aircraft speed, and mistakes in operator commands. Then one could compute unsafe reachable sets from which a collision would result if the UAV continued its current maneuver.

The capture sets and the unsafe sets could then be combined to determine the sequence of flight mode transitions to extricate the UAV from an unsafe zone and safely resume the refueling maneuver. This provides a powerful toolset for future work in constructing a formal decision protocol to ensure the safety of the tanker and the UAV during the refueling process even under faulty operator commands, and disturbances.

II. BACKGROUND

The use of Hamilton-Jacobi (HJ) reachable sets has seen successes in numerous aeronautical applications. In [1], one can find a comprehensive overview of the computation techniques underlying the HJ reachable set method, its connection with hybrid system theory, and several applications of the method to hybrid system verification.

Of particular interest to our discussion is the use of Hamilton-Jacobi methods in air traffic control. In [2] and [3], the authors present a method for detecting possible "loss of separation" between pairs of aircraft over a given airspace, based upon backward reachable sets computed using HJ PDEs, and using the framework of a dynamic game between aircraft and uncertainty.

The reachable set method has also been successfully used to verify safety of conflict resolution aircraft maneuvers [4],

This work was supported by the "Certification Technologies for Flight Critical Systems (CerTA FCS)" project, Air Force Research Labs, through a contract with Boeing Phantom Works; and in part by the Center for Hybrid and Embedded Software Systems (CHESS) at UC Berkeley, which receives support from the National Science Foundation (NSF awards #CCR-0225610 (ITR),#0720882 (CSR-EHS: PRET), #0647591 (CSR-SGER), and #0720841 (CSR-CPS)), the U. S. Army Research Office (ARO #W911NF-07-2-0019), the U. S. Air Force Office of Scientific Research (MURI #FA9550-06-0312 and AF-TRUST #FA9550-06-1-0244), the Air Force Research Lab (AFRL), the State of California Micro Program, and the following companies: Agilent, Bosch, DGIST, Lockheed Martin, National Instruments, and Toyota.

J. Ding, S.S. Sastry and C.J. Tomlin are with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720, USA {jding,sastry,tomlin}@EECS.Berkeley.Edu

J. Sprinkle is with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721-0104, USA sprinkle@ECE.Arizona.Edu

978-1-4244-3124-3/08/$25.00 ©2008 IEEE

and closely spaced parallel approaches for airport runways [5]. In [4], the authors consider the case where two aircraft have intersecting planned trajectories, and so have to initiate a series of maneuvers to avoid collisions and then resume their desired trajectories. In [5], the authors extend the results from the collision avoidance scenario to the case where two aircraft attempt to land simultaneously on closely spaced runways. Several escape maneuvers are considered to prevent one aircraft from blundering into the unsafe zone of the other, and was successfully validated in extensive simulations. For the current application, we use a similar approach to constructing collision avoidance protocols based upon a finite set of escape maneuvers.

The reachable set method has also been successfully demonstrated as a valuable tool for informing human decisions. In [6], the authors consider the safety of the mode switch from a Flare landing maneuver to a Take-off/Go-Around (TO/GA) maneuver when ground conditions prevent a safe landing. In [7], the authors consider the re-initiation of the landing maneuver during TO/GA. The safe reachable sets for specific control laws were generated offline and then stored as look-up tables onboard an actual aircraft to determine in real-time whether a given glide-slope recapturing maneuver was safe. Computational reachability to aid in separation of aircraft is not limited to solving the HJ equation. In [8] the authors discuss the use of Markov chains to determine the reachability of some stochastic system in some lookahead time (potentially infinite). Air traffic management as a driving example for distributed control and stochastic analysis of safety-critical real-time systems is utilized in [9].

Switching between control strategies to achieve a final reachable set was discussed in [10]; the goal is to determine whether a final state can be reached. In our work, we focus instead on a known set of transitions, and aim to provide analysis on the timing of switches between these states.

Previous work by the authors [1] has utilized a *reach-avoid* operator to calculate the set of states from which system trajectories can reach an unsafe set without entering the set of states that can be rendered safe by mode switching. In this work we are interested in the set of states from which trajectories could reach a desired target set without entering the set of unsafe states.

In this paper we draw from this previous research in examining the use of multiple pre-computed reachable sets in guiding flight maneuver decisions, both for the case in which control laws are fixed and in which bounded uncertainties exist in the UAV and tanker inputs. The application solution, while utilizing many techniques demonstrated for air traffic control, is a significantly different problem. In particular, freedom to move in altitude aids in solving many air traffic control problems, but such maneuvers would violate our mission goals. We next discuss a formalization of the problem.

III. SCENARIO FORMALIZATION

A. Automatic Aerial Refueling (AAR)

In a typical aerial refueling process, a formation of unmanned aerial vehicles (UAVs) approaches a human piloted tanker aircraft. One by one, the UAVs perform a sequence of maneuvers to dock with a human operated fuel boom and then return to formation. A graphical top down view of the refueling process is shown in Figure 1.

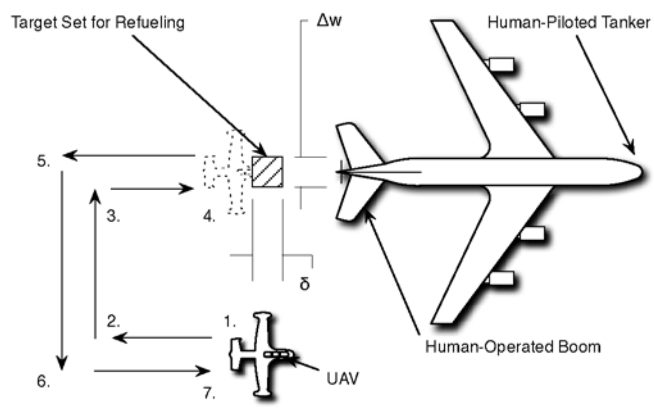


Fig. 1: Aerial Refueling Process. Each waypoint is described in the below enumeration.

The tanker aircraft is shown in the center, with the refueling UAV flying in formation to be refueled. In the actual refueling process, the UAV will always approach from a fixed position in the formation. For our modeling purposes, we will assume that the aircraft to be refueled approaches from a position behind and to the right of the tanker aircraft. From this position, the UAV will initiate a sequence of maneuvers through the numbered waypoints, under a combination of human operator commands and autonomous decisions. The possible maneuvers in the process include the following:

1) Detach 1: a single UAV detaches from a formation of UAVs in flight to a position slightly behind and to the right of a tanker aircraft.
2) Precontact: the UAV banks left towards a position directly behind the tanker aircraft.
3) Contact: the UAV approaches the tanker aircraft from behind to allow the boom operator on board the tanker to lower the fuel boom and catch the UAV.
4) Postcontact: the UAV slows down and moves away from the tanker aircraft after the boom operator detaches the fuel boom.
5) Detach 2: the UAV banks right towards a position directly behind the UAV formation.
6) Rejoin: the UAV speeds up and rejoins the formation to complete the refuel sequence.
7) Fall back: If at any point, a formation transition is deemed unsafe, for example in the case of wind turbulence, approach of enemy aircraft, or malfunction of the fuel boom, a fall back command may be issued to halt the state transition and to command the UAV to return to the previous state.

B. Aircraft Model

First we note that in a formation of UAVs, refueling occurs one vehicle at a time. As such, for the rest of this paper, we will be examining the interaction between a single UAV and the tanker aircraft. We take the approach of [1] and [4] by studying the continuous behavior of the two aircraft in relative coordinates. We assume that the two aircraft do not change altitude significantly in performing the aerial refueling maneuvers, and this is justified in the state of the practice for human-piloted maneuvers of this kind. In fact, using a change in altitude might jeopardize the success of the mission, as human operators would suspend the mission if loss of line of sight occurs; thus, there is motivation to preserve a 2D solution. Placing the two aircraft in a 2D plane can be modeled as:

$$\dot{x} = f(x,u) = \frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -u_1 + v_0 \cos x_3 + u_2 x_2 \\ v_0 \sin x_3 - u_2 x_1 \\ -u_2 \end{bmatrix} \quad (1)$$

The state variables in this equation are defined as follows:

- x_1 = longitudinal distance from the UAV to the tanker
- x_2 = latitudinal distance from the UAV to the tanker
- x_3 = heading of UAV relative to the tanker

The inputs to the system are defined as follows:

- u_1 = linear velocity of UAV
- u_2 = angular velocity of UAV

Finally, the parameter v_0 in this model is the constant, known velocity of the tanker. Here we model the tanker as moving in straight and level flight with a constant velocity.

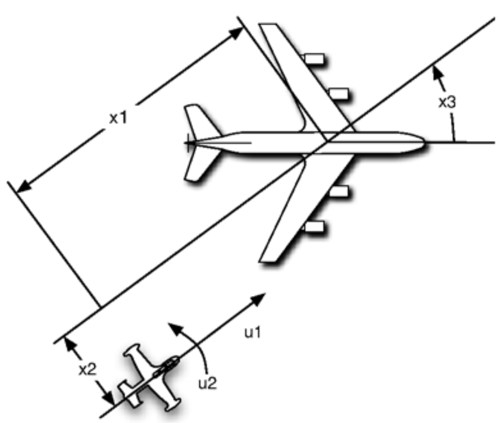


Fig. 2: 2D Kinematic Model.

C. Hybrid System Model

Given the consistent continuous behavior, and different control law for each mode, a hybrid system model [11] representing the aerial refueling process is ideal. We model the aerial refueling process as a sequence of transitions between a finite number of discrete states. In each discrete state, the aircraft move according to the continuous behavior described in the previous section, with varying control inputs for each state.

For details of the hybrid system formalism, we refer the interested reader to [11]. In the specific case of aerial refueling, we introduce the hybrid automaton given by Figure 3. In this model, we define the discrete states as the set of flight modes $Q = \{q_1, q_2, \ldots, q_n\}$, where each q_i is a discrete state in which the UAV is flying straight and level at a waypoint, or transitioning between the waypoints, or performing a fallback maneuver. The set of continuous state variables is $X = \{x_1, x_2, x_3\}$, where each x_i is as defined in the previous section. The set of discrete inputs is the human commands to the UAV to transition between the waypoints. This includes σ_{ij} for the commands to transition between waypoint i and j, as well as FB for the fallback command. The set of continuous inputs is $V = \{u_1, u_2\}$ where u_1 and u_2 are as defined in the previous section. The continuous behavior f is given by equation (1).

With this hybrid system formalism, we can now define some system verification problems we wish to solve. First, we would like to know for the transition flight modes, what is the set of positions and orientations that allows the UAV to reach a neighborhood around the desired waypoint within a specified time horizon. We define a time varying reachability set $\mathcal{G}_\tau \subset X$, where $\tau \geq 0$, and a neighborhood around the waypoint $T \subset X$. For a flight mode q_i, the problem then becomes finding $\mathcal{G}_\tau$ such that if $x(0) \in \mathcal{G}_\tau$, then under the vector field $f(q_i, x, u)$, $x(\tau) \in T$, for some $u \in V$. We call this the capture set for flight mode q_i. Second, we would like to find the set of states that could force the UAV into a collision with the tanker aircraft under a particular flight mode. We define a collision as the case where the states of the system enters the set of unsafe states G. Then we can again encode this as a reachability problem, where we want to find the set $\mathcal{G}_\tau$ such that if $x(0) \in \mathcal{G}_\tau$, then under the vector field $f(q_i, x, u)$, $x(\tau) \in G$, for some $u \in V$. We call this the unsafe set for flight mode q_i.

D. Control Law Design

The feedback control laws to perform the different state transitions are applied through the inputs u_1 and u_2. For the sake of simplicity, we have chosen to use proportional control laws to control the UAV to the desired waypoints for the different maneuvers. For the transitions between the stationary states 1 through 7, the equations for the feedback laws are given by

$$u_1 = k_1(x_1 - x_{1f}) + v_0 \quad (2)$$

$$u_2 = k_2(x_2 - x_{2f}) \quad (3)$$

where k_1 and k_2 are the proportional control parameters, and x_{1f}, x_{2f} are the desired final location of the UAV relative to the tanker. To model the saturation in the control input, we restrict the above inputs to lie within some specified input ranges $[u_{1_{\min}}, u_{1_{\max}}]$ and $[u_{2_{\min}}, u_{2_{\max}}]$.

As mentioned in Section III-C, at any point during the refueling procedure evasive maneuvers may need to be performed in an attempt to avoid an imminent collision between UAV and the tanker aircraft. This could happen if the UAV

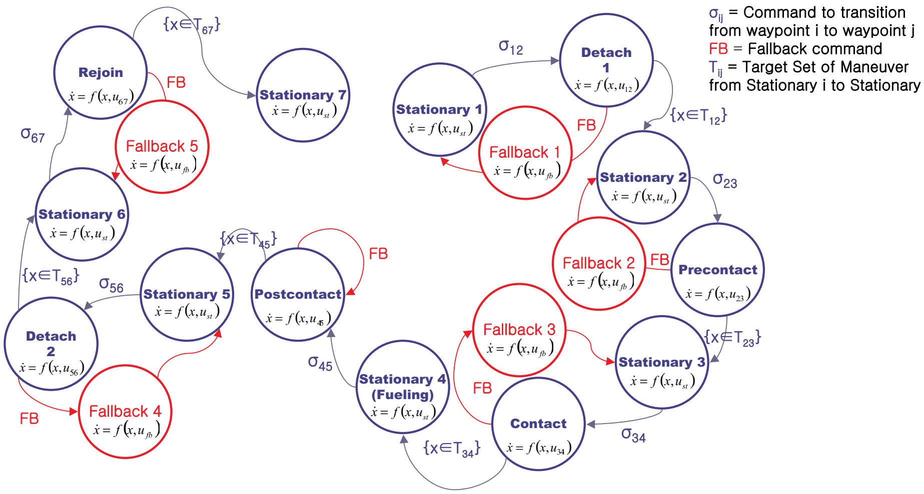


Fig. 3: Aerial Refueling Formation Transition Model. The initial state is Stationary 1.

deviates from its heading due to external disturbances when performing one of the formation transitions.

We define four different escape modes, based on relative cardinal locations around the tanker (before/behind on the left/right). For escape mode 1, the UAV attempts to move to a position to the left and behind the tanker, while for escape mode 2, the UAV attempts to move to a position to the right and behind the tanker. For escape mode 3, the UAV attempts to move to a position behind the tanker, while maintaining the same heading as the tanker aircraft. For escape mode 4, the UAV attempts to move to a position in front of the tanker, also while being aligned with the tanker heading. The control laws for these maneuvers take a similar form as the equations given above, with different proportional constants and desired final locations.

IV. REACHABLE SET CALCULATIONS

As mentioned in section III-C, two different types of reachable sets are used in the safety verification and construction of decision protocols for the aerial refueling procedure, namely the capture set and the unsafe set. We take the Hamilton-Jacobi approach [2], [11] towards the calculation of the time varying reachable sets. We will first review the general Hamilton-Jacobi method allowing for input uncertainty, and then adapt it for our hybrid automaton.

Mathematically speaking, one can define the target set implicitly as the sublevel set of a scalar function of the states [2] $\phi_0 : \mathbb{R}^3 \to \mathbb{R}$. If we are to call the target set $T = \mathscr{G}_0$, then

$$\mathscr{G}_0 = \left\{x \in \mathbb{R}^3, \phi_0(x) \le 0\right\} \tag{4}$$

Similarly, one can define the set of states controllable to $\mathscr{G}_0$ after time τ as the sublevel set of the level set function $\phi : \mathbb{R}^3 \times \mathbb{R} \to \mathbb{R}$. Let this set be $\mathscr{G}_\tau$, then

$$\mathscr{G}_\tau = \left\{x \in \mathbb{R}^3, \phi(x,-\tau) \le 0\right\} \tag{5}$$

As can be seen, the set of states at which the level set function is zero defines the boundary of the backward reachable set at time t. It has been shown in [2] that if all control inputs $u(t)$ within the input space $\mathbb{U}$ and all disturbance inputs $d(t)$ within the input space $\mathbb{D}$ are bounded at any given time, and if the system behavior $f(x,u,d)$ satisfies certain continuity constraints, $\phi(x,t)$ is the solution to the terminal value Hamilton-Jacobi PDE

$$\frac{\partial \phi}{\partial t} + H\left(x, \frac{\partial \phi}{\partial x}\right) = 0,\ \phi(x,0) = \phi_0(x) \tag{6}$$

In cases where the optimal control input attempts to maximize the reachable set, while the worst case disturbance input attempts to minimize the reachable set, the Hamiltonian is defined as

$$H(x,p) = -\max_{d\in\mathbb{D}} \min_{u\in\mathbb{U}} p^T f(x,u,d) \tag{7}$$

where p is a placeholder for $\nabla\phi$.

We note that for the hybrid system automaton defined in Section III-C, the set of disturbance inputs is empty. To generate the reachable sets for a particular feedback control law $u = K(x)$ as defined in Section III-D, one would use the system behavior $\dot{x} = f(x, K(x))$, which is input free.

With this formulation of the Hamiltonian, we are now able to generate the reachable sets for each of the formation transitions and evasive maneuvers with fixed control inputs. For capture sets, the target set is chosen to be a closed set of states around a desired waypoint. The general form of such a target set is given below:

$$\mathscr{G}_0 = \left\{ \begin{array}{l} x_1 \in \left[x_{1_{\min}}, x_{1_{\max}}\right] \\ x_2 \in \left[x_{2_{\min}}, x_{2_{\max}}\right] \\ x_3 \in \left[x_{3_{\min}}, x_{3_{\max}}\right] \end{array} \right. \tag{8}$$

For unsafe sets, the set of unsafe final states is chosen to be a disk around the tanker aircraft with a slight dent behind the tanker to allow the UAV to approach the fuel boom. Precisely, this set is given by

$$\mathscr{G}_0 = \left\{x \in X \mid x_1^2 + x_2^2 \le d_0\right\} \setminus N \tag{9}$$

where d_0 is the unsafe radius, and N is a neighborhood of states around the boom location ($x_1 = D$, $x_2 = 0$).

We will note however, that the results could be easily extended to cases where we allow for uncertainty in tanker inputs that lie within certain deterministic bounds, thus adding robustness into the capture and unsafe sets that are generated. Specifically, we will introduce a case where the tanker velocity v_0 in Eq. (1) is not constant, but rather allowed to vary within a range $[v_{\min}, v_{\max}]$. In the framework of the HJ equations, the disturbance input space is given by $\mathbb{D} = \{v_0 : v_0 \in [v_{\min}, v_{\max}]\}$.

For general system dynamics, the solution to the H-J PDE is difficult to compute analytically. Several high resolution numerical approximation schemes exist to compute the level set function. For this project, computations of the reachable sets were performed using the Toolbox for Level Set Methods developed by Prof. Ian Mitchell of University of British Columbia [12] for MATLAB, based upon the level set theory described extensively in [13] and [14]. In the numerical approximation scheme, the continuous state space is divided into a finite number of grid cells, and each grid cell is assigned a numerical value of the level set function during the reachable set computation. The computation cost of the level set method is strongly tied to the dimension of the problem and the number of grid cells used.

V. ANALYSIS OF RESULTS

To validate the capture and unsafe reachable sets, we constructed MATLAB simulations of various refueling sequence scenarios. For the simulation results shown in this section, we set the velocity of the tanker aircraft to be $v_0 = 0.2$. Furthermore, we assume that the velocity input has the saturation limits $[0.05, 0.5]$, and the angular velocity input has the saturation limits $[-\pi/6, \pi/6]$. The control law parameter values used for the simulation are summarized in Table I.

TABLE I: Control Law Parameters

Maneuver	k_1	k_2	x_{1f}	x_{2f}
Detach 1	5	5	1	1
Precontact	0.15	5	1	0
Contact	5	5	0.25	0
Postcontact	5	5	1	0
Detach 2	0.15	5	1	1
Rejoin	5	5	0.25	1

A. Capture Sets Computation and Simulation

As mentioned in the previous section, the target set for capture reachable sets is chosen to be a neighborhood around the set of desired final states. In terms of the control laws, the desired spatial location is given by the x_{1f} and x_{2f} parameters. Since we would like the UAV to end its maneuver with a heading roughly the same as that of the tanker aircraft, the desired final relative heading is zero. For example, the target set for the Precontact maneuver (transition from waypoint 2 to 3) can be chosen to be

$$\mathscr{G}_0 = \begin{cases} x_1 \in [0.75, 1.25] \\ x_2 \in [-0.25, 0.25] \\ x_3 \in [-\pi/9, \pi/9] \end{cases} \tag{10}$$

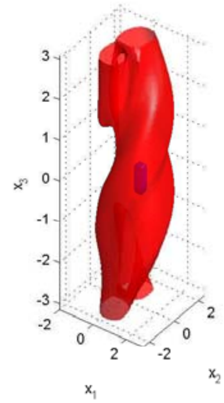
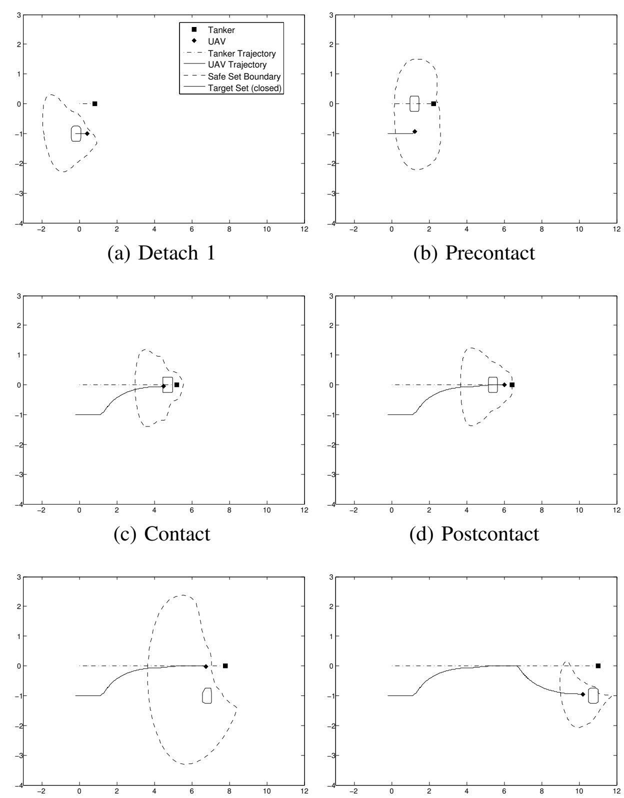


Fig. 4: Capture Set for Transition 2 to 3 (Precontact), x_1 and x_2 represent longitudinal and lateral offset (respectively), and x_3 represents the offset in heading between the UAV and tanker.

To compute the capture set of this maneuver, we used the Hamiltonian function defined in Section IV, substituting the Precontact control law for u_1 and u_2. For a choice of 10 seconds for the time horizon, the capture set generated for this maneuver is shown in Figure 4.



(a) Detach 1 (b) Precontact

(c) Contact (d) Postcontact

(e) Detach 2 (f) Rejoin

Fig. 5: Refueling sequence simulation with capture sets.

For all states within this reachable set, the UAV is guaranteed to be driven into the desired target set within 10 seconds under the Precontact flight mode. The reachable sets for other flight modes can be generated similarly using different specifications of the target set and control constants.

Using our MATLAB simulation environment, we constructed a complete simulation of the refueling sequence with the reachable sets superimposed on the trajectories of the UAV. It was found that if we generate capture sets for each flight mode over multiple time horizons, they can be used to design the transition timing of the refueling process. First, we find the capture sets for the last transition (Rejoin). We then find the smallest time horizon at which the capture set includes the target set of the next to last transition (Detach 2). By this, we can guarantee that if the UAV reaches the target set for Detach 2, it will reach the target set for Rejoin within this time horizon. We then propagate this backward by finding the smallest time horizon at which the capture sets for the Detach 2 transition includes the target set for the Detach transition. In this manner, we obtain a sequence of time horizons that can be used as the transition timings.

In Figure 5, the complete set of reachable sets is plotted as the UAV transitions from one maneuver to another in a refueling sequence. For each maneuver, it is shown that if the UAV reaches the target set of the current maneuver, then it is guaranteed to be within the backward reachable set of the next maneuver.

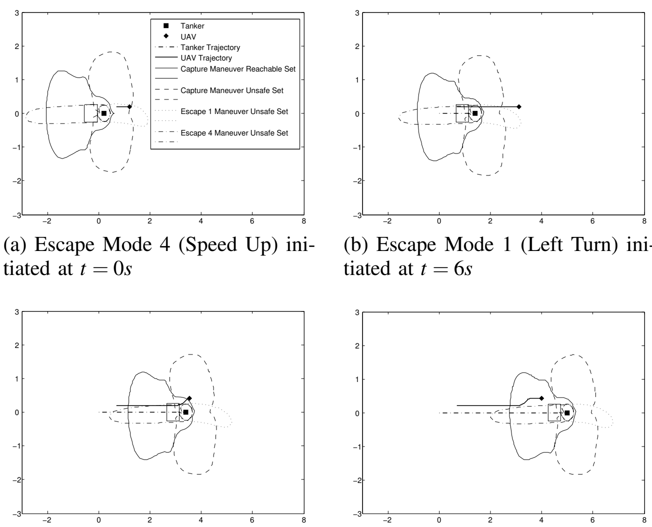
B. Fallback/Waveoff Scenario Simulation

As defined in Section III-C, the unsafe set for a given maneuver is the set of states from which the UAV could enter an unsafe zone around the tanker aircraft using the corresponding control laws for the maneuver. In a deterministic situation, the control laws are designed so that the UAV would never enter the unsafe set while performing any maneuver. However, in practical situations, environmental factors such as wind turbulence and variations in tanker velocity could cause the UAV to miss the fuel boom and stray into the unsafe zone of the tanker aircraft. In these cases, the UAV would have to execute a sequence of escape maneuvers to avoid a collision with the tanker while completing the maneuvers necessary for the refueling process.

In our example scenario, we consider the case where the UAV starts at an unsafe location close to the tanker and chooses to initiate, without operator commands, a sequence of maneuvers to a safe location where it is feasible to perform the Contact maneuver. If the unsafe sets were not a concern, the UAV could construct a sequence of maneuvers by ensuring that the target set of one maneuver lies within the reachable set of the next maneuver, much like how the refueling sequence was constructed in Section V-A.

However, in this case, we have the further constraint that at the start of any maneuver in the sequence, the UAV cannot be inside the unsafe set of that maneuver. In this case, although the maneuver which minimizes the time to reach the fuel boom would be to simply back up the UAV directly and then perform the Contact maneuver, this would clearly cause the UAV to enter the unsafe zone of the tanker aircraft. By taking into account the unsafe sets, the UAV would instead need to speed up and then steer left so as to be able to safely backup into the reachable set for the Contact maneuver. It is important to note that part of the reachable set for the Contact maneuver actually intersects with the unsafe set for the same maneuver. The states where the sets intersect would result in the UAV arriving at the fuel boom in desired time, but also having entered the unsafe zone of the tanker in that process. To avoid this situation, the UAV would need to back up far enough so that it is within the part of the reachable set that does not intersect with the unsafe set.

The complete sequence of maneuvers is shown in Figure 6. The fallback sequence described here is obtained from repeated simulations using multiple reachable sets. The sets are computed offline, and the datasets used at runtime. Computation:simulation time ratios, using high accuracy, range from 70:1 to approximately 1400:1.



(a) Escape Mode 4 (Speed Up) initiated at $t = 0s$

(b) Escape Mode 1 (Left Turn) initiated at $t = 6s$

(c) Escape Mode 3 (Move Back) initiated at $t = 16s$

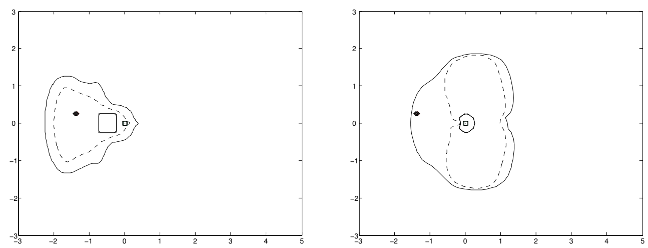
(d) Fallback maneuver complete, shown here at $t = 24s$

Fig. 6: Maneuvers for Fallback Scenario.

C. Comparison of Capture Sets and Unsafe Sets under Worst Case Tanker Speed Input

In the preceding simulations, all reachable sets and unsafe sets were generated using completely known control laws and system behavior. Although it may be reasonable to expect relatively accurate measurements of the instantaneous location and relative heading of the UAV using modern navigational instruments, there is a degree of uncertainty associated with the velocity of the tanker. This uncertainty may not be significant for maneuvers far enough from the tanker aircraft. However, for the Contact maneuver where the UAV would need to come into close proximity with the tanker aircraft, even slight variations in the tanker aircraft speeds may endanger the safety of the maneuver.

The Hamilton-Jacobi formulation of reachable sets gives a convenient method to account for this uncertainty in the tanker aircraft velocity. As seen in the reachable set section, we can allow this velocity to fluctuate within a specified range $[v_{\min}, v_{\max}]$ as an input to the system. For the reachable set calculations, one needs to only maximize or minimize the Hamiltonian as necessary over the range of this input. Using this method, the worst case capture set and unsafe set were obtained under uncertain but bounded tanker velocity and are shown in Figure 7 (a) and (b), along with the same sets calculated under deterministic tanker velocity.



(a) “Contact” reachable set without uncertainty (outer line), with uncertainty (inner line).

(b) “Contact” unsafe set with uncertainty (outer line), without uncertainty (inner line).

Fig. 7: Reach/Unsafe Set under Worst Case Tanker Speed.

As expected, the worst case capture set with added uncertainty is smaller than that without uncertainty. This is due to the fact that under worst case tanker aircraft speed input, the tanker is effectively trying to prevent the UAV from entering the refueling zone. Similarly, the worst case unsafe set under uncertainty is shown to be larger than that without uncertainty. This results from the worst case tanker speed input which effectively tries to force a collision with the UAV. In the context of the maneuver designed for the second fallback scenario described in the previous section, the reachable set from which it is safe to reach the fuel boom without encroaching on the unsafe zone of the tanker is significantly reduced under uncertain tanker velocity. This may force the UAV to return to waypoint 3 before re-initiating the capture maneuver.

VI. CONCLUSION AND FUTURE WORK

Using a state transition diagram for discrete dynamics and a state space model for continuous behavior, we have formulated the refueling process as a hybrid system model. Simple proportional control laws were chosen to control the UAV to desired locations during the refueling process.

With a hybrid system model, system verification is formulated as a hybrid system verification problem. Through the Hamilton-Jacobi formulation of reachable sets, we were able to use numerical techniques to compute the capture sets and unsafe sets for all maneuvers in the refueling process. Results from the reachable set simulations demonstrated that the use of capture set and unsafe set data allows us to design the transition timing of the refueling sequence, detect unsafe maneuvers, and design fallback maneuvers that reach the desired target set in minimum time while avoiding collisions with the tanker aircraft.

The challenge going forward will be to combine the results of the reachable set simulations and construct a formal algorithm with which the UAV could generate autonomous decisions for formation transitions based on operator commands, its onboard state, and reachable set data. To ensure the reliability of the reachable sets used for synthesizing flight critical decisions, one also needs to investigate techniques for increasing the accuracy of the reachable sets without significant increases in computation cost.

VII. ACKNOWLEDGMENTS

The authors gratefully acknowledge the contribution of Dr. James L. Paunicka, and Jim Barhorst of Boeing Phantom Works, who aided in the development of the AAR scenario. In addition, Dr. Doug Stuart of Boeing Phantom Works provided valuable feedback with regards to questions of discrete reachability. Also, many of the research ideas that produced this work were conceived in David Homan’s yearly meetings on Verification and Validation at Wright-Patterson AFB in Dayton, OH. In those meetings, our work was influenced in the conversation and presentations of many of those participants, and we are grateful for their contribution.

REFERENCES

[1] C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi, “Computational techniques for the verification of hybrid systems,” *Proceedings of the IEEE*, vol. 91, no. 7, pp. 986–1001, July 2003.

[2] I. Mitchell, A. Bayen, and C. Tomlin, “A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games,” *IEEE Transactions on Automatic Control*, vol. 50, no. 7, pp. 947–957, July 2005.

[3] A. M. Bayen, “Computational control of networks of dynamical systems: Application to the national airspace system,” Ph.D. dissertation, Stanford University, Stanford, CA, 2003.

[4] C. Tomlin, I. Mitchell, and R. Ghosh, “Safety verification of conflict resolution manoeuvres,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 2, no. 2, pp. 110–120, June 2001.

[5] R. Teo and C. J. Tomlin, “Computing danger zones for provably safe closely spaced parallel approaches,” *Journal of Guidance, Control, and Dynamics*, vol. 26, no. 3, pp. 434–443, May-June 2003.

[6] M. Oishi, I. Mitchell, A. Bayen, C. Tomlin, and A. Degani, “Hybrid verification of an interface for an automatic landing,” *Proceedings of the 41st IEEE Conference on Decision and Control*, vol. 2, pp. 1607–1613, 10-13 Dec. 2002.

[7] J. Sprinkle, A. D. Ames, J. M. Eklund, I. Mitchell, and S. S. Sastry, “Online safety calculations for glideslope recapture,” *Innovations in Systems and Software Engineering*, vol. 1, no. 2, pp. 157–175, September 2005. [Online]. Available: http://www.springerlink.com/openurl.asp?genre=article&id=doi:10.1007/s11334-005-0017-x

[8] M. Prandini and J. Hu, “A stochastic approximation method for reachability computations,” in *Stochastic Hybrid Systems*. Springer Berlin/Heidelberg, 2006, vol. 337/2006.

[9] H. Bloom and J. Lygeros, Eds., *HYBRIDGE Final Project Report*, 2005.

[10] R. R. Burridge, A. A. Rizzi, and D. E. Koditschek, “Sequential composition of dynamically dexterous robot behaviors,” *The International Journal of Robotics Research*, vol. 18, 1999.

[11] C. Tomlin, J. Lygeros, and S. Shankar Sastry, “A game theoretic approach to controller design for hybrid systems,” *Proceedings of the IEEE*, vol. 88, no. 7, pp. 949–970, Jul 2000.

[12] I. M. Mitchell and J. A. Templeton, “A toolbox of Hamilton-Jacobi solvers for analysis of nondeterministic continuous and hybrid systems,” *Hybrid Systems Computation and Control*, vol. 3414/2005, pp. 480–494, Feb. 2005.

[13] S. Osher and R. Fedkiw, *Level Set Methods and Dynamic Implicit Surfaces*. Springer-Verlag, 2002.

[14] J. A. Sethian, *Level Set Methods and Fast Marching Methods*. Cambridge University Press, 1999.