Reachability Calculations for Automated Aerial Refueling

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

Abstract—This paper describes reachability calculations for a hybrid system formalism governing UAVs interacting with another vehicle in a safety-critical situation. We examine this problem to lay the foundations toward the goal of certifying certain protocols for flight critical systems. In order to pursue these goals, we describe here what mathematical foundations are necessary to inform protocol certification, as well as describe how such formalisms can be used to automatically synthesize simulations to test against certain danger areas in the protocol. This can provide a mathematical basis for the UAV to perhaps reject a command based on the known unsafe behavior of the vehicle. We describe how creating this formalism can help to refine or design protocols for multi-UAV and/or manned vehicle interaction to avoid such scenarios, or to define appropriate behaviors in those cases.

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. The mix of human input and autonomous operation introduces complexities in terms of how decision authority should be delegated to ensure safe operation of a given autonomous vehicle. This is further complicated by latencies in communication between the human operator and the UAV, which could render a command issued by a human operator obsolete or even dangerous once it has reached the UAV. 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 safety-critical flight maneuvers where the latency in communication is high and where large numbers of human operators could result in conflicting commands being issued by different operators, it becomes important to develop decision protocols that can be formally verified to ensure the safe operation of the mixed-initiative system.

This work was supported by the “Certification Technologies for Flight Critical Systems (CertIFCS)” 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-CP5)), 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

A. Motivation: Automated Aerial Refueling

Consider the specific case of Automated Aerial Refueling (AAR). During a refueling operation, the UAV first breaks away 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.

Throughout this process, the UAV comes into contact with three different human operators: the ground control station operator, the tanker aircraft pilot, and the boom operator. A graphical representation of the interaction between the human operators and the UAV is shown in Figure 1.

Fig. 1: UAV and Human Operator Interactions in AAR.

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 the optimal 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.
In such cases, one could compute unsafe reachable sets from which a collision would result if the UAV continues in 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 combined with the study of reachable sets under latency and uncertain system inputs, provides a powerful toolset with which one can construct a formal decision protocol to ensure the safety of the tanker and the UAV during the refueling process even under communication latencies, faulty operator commands, and external disturbances.

B. Organization

In the remainder of this paper we will provide some review of methods and approaches that are relevant to our goals. We continue with discussion the formalism in which we are describing the automated aerial refueling scenario. This is followed by the various reachable sets, and analysis of their impact when considered together. Finally, we will discuss how these foundations will allow future work in automating these calculations for various other protocols, and performing analysis as well as generating simulations to verify expected behaviors.

II. BACKGROUND

The use of Hamilton-Jacobi (HJ) reachable sets has seen successes in numerous aerodynamical 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. The collision avoidance problem is formulated as a dynamic game between adversarial aircraft, where a “pursuer” aircraft attempts to cause a collision, while an “evader” aircraft attempts to avoid a collision, both applying unknown inputs within specified bounds. Unsafe reachable sets were then calculated for worst case pursuer inputs and optimal evader inputs. This method was applied to large samples of Enhanced Traffic Management System (ETMS) data, and it successfully predicted all “loss of separation” situations, with a small number of false alarms. A similar formulation of the collision avoidance problem is employed in the current project, in the context of a single UAV and a tanker aircraft during AAR.

The reachable set method has also been successfully used to verify safety of conflict resolution aircraft maneuvers [4], 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. The conflict resolution sequence is specified within a hybrid system framework as a series of mode switches among a finite set of possible evasive maneuvers. The unsafe reachable sets were generated for each evasive maneuver and then used to determine the safety of any particular conflict resolution sequence. 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 in the verification of an automatic landing interface [6], as well as the safety of recapturing the glide-slope after an aborted landing maneuver [7]. In the first case, 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. The controllable flight envelopes were calculated using the reachable set method for both the Flare and TO/GA maneuvers, and the results indicated states where an aircraft may safely land, but can not safely initiate the TO/GA maneuver. This prompted efforts to construct an alternative landing interface that addresses this hidden safety concern. In the second case, 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.

For the current project, we draw from these previous projects in examining the use of multiple pre-computed reachable sets in guiding flight maneuver decisions, both for the case where control laws are fixed and where bounded uncertainties exist in the UAV and tanker inputs.

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 2.

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:
Fig. 2: Aerial Refueling Process.

1) Breakaway 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) Precapture: the UAV banks left towards a position directly behind the tanker aircraft.
3) Capture: 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) Postcapture: the UAV slows down and moves away from the tanker aircraft after the boom operator detaches the fuel boom.
5) Breakaway 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 Dynamics

First, we note that any formation of UAVs is refueled only one 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 dynamics of the two aircraft in relative coordinates. In our model, we assume that the two aircraft do not change altitude significantly in performing the aerial refueling maneuvers. Then placing both aircraft in a two dimensional plane with the tanker aircraft at the origin, the relative motion of the UAV with respect to the tanker can be modeled by the following kinematics equations

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

(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. The graphical representation of this coordinate system is shown in Figure 3.

C. Hybrid System Model

Given the consistent continuous dynamics, and different control law for each mode, a hybrid system model [8] 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 dynamics described in the previous section, with varying control inputs for each state.

From [8], a general hybrid system automaton \( H \) is defined as follows:

\[
H = (Q,X,\Sigma,V,Init,f,Inv,R)
\]

where \( Q \) is the set of discrete states of the automaton, \( X \) is the set of continuous state variables, \( \Sigma \) is the set of discrete input variables, \( V \) is the set of continuous input variables, \( Init \) is the set of initial states of the system, \( f \) is a vector field representing the evolution of the continuous state variables, \( Inv \) is the set of states and inputs for which continuous evolution is allowed, and \( R \) is a reset relation defining the discrete transitions in the hybrid automaton.

For the specific case of aerial refueling, 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 are the human commands to the UAV to transition between the waypoints. This includes \( \delta_{ij} \) 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. Now define a subset \(G\) of the continuous state space \(X\) as the set of unsafe states of the hybrid automaton (this will be made explicit later on), then the set of initial conditions is \(\text{Init} = Q \times G\). This ensures that the system starts in a safe state. The continuous dynamics \(f\) is given by equation (1). The reset relations \(R\) describing the transitions between the flight modes in the refueling sequence is shown in Figure 4.

We should note the Invariant \(\text{Inv}\) is defined so that the state based mode transitions are enforced. For example, defining \(T_{ij}\) as a neighborhood around the waypoint \(j\) that terminates the transition from waypoint \(i\) to \(j\), then the invariant for the discrete state “Breakaway 1,” which we will denote as \(q_{B1}\), is given by \(q_{B1}, \{x \in X | x \notin T_{12}\}, \Sigma, V\).

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 \(G_T \subset X\), where \(\tau \geq 0\), and a neighborhood around the waypoint \(T \subset X\). For a flight mode \(q_i\), the problem then becomes finding \(G_T\) such that if \(x(0) \in G_T\), then under the vector field \(f(q_i, x, u)\), \(x(\tau) \in T\), for some \(u \in U\). 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 \(G_T\) such that if \(x(0) \in G_T\), then under the vector field \(f(q_i, x, u)\), \(x(\tau) \in G\), for some \(u \in U\). 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

\[
\begin{align*}
    u_1 &= k_1(x_1 - x_{1f}) + v_0 \\
    u_2 &= k_2(x_2 - x_{2f})
\end{align*}
\]

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 modify the above control law by introducing upper and lower control limits. First, we introduce the following definition of saturation function \(sat: \mathbb{R} \times \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}\)

\[
\text{sat}(x, x_a, x_l) = \begin{cases}
    x_a, & x \geq x_a \\
    x, & x_l < x < x_a \\
    x_l, & x \leq x_l
\end{cases}
\]

With this definition, the modified control law is then

\[
\begin{align*}
    \tilde{u}_1 &= \text{sat}(u_1, u_{1max}, u_{1min}) \\
    \tilde{u}_2 &= \text{sat}(u_2, u_{2max}, u_{2min})
\end{align*}
\]

where \(u_1\) and \(u_2\) are given in equations (2) and (3), and \(u_{1max}, u_{1min}, u_{2max}, u_{2min}\) are respectively the upper and lower limits of the control inputs.

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 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. The control laws for these maneuvers are the same as those in equations (4) and (5), with different constants and desired final locations. The control parameters are chosen to generate sharp turns to the left and right.

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 law for each of these maneuver assumes the form:

\[
\begin{align*}
    u_{1,34} &= \text{sat}(u_1, u_{1max}, u_{1min}) \\
    u_{2,34} &= \text{sat}(k_2x_2, u_{2max}, u_{2min})
\end{align*}
\]

Although the form of these control laws are again similar to those of equations (4) and (5). Different control parameters are chosen to result in a rapid change in speed and fast correction of the heading. The design choice of each of these control laws provides us with the ability to escape from any relative position of the UAV to the tanker.
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], [8] towards the calculation of the time varying reachable sets. We will first review the general Hamilton-Jacobi method allowing for input uncertainty, 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 \( \phi_0 : \mathbb{R}^3 \to \mathbb{R} \). If we are to call the target set \( \mathcal{T} = \mathcal{G}_0 \), then

\[
\mathcal{G}_0 = \{ x \in \mathbb{R}^3, \phi_0(x) \leq 0 \}
\]

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

\[
\mathcal{G}_\tau = \{ x \in \mathbb{R}^3, \phi(x, -\tau) \leq 0 \}
\]

As can be seen, the set of states where 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 \( \mathcal{U} \) and all disturbance inputs \( d(t) \) within the input space \( \mathcal{D} \) are bounded at any given time, and if the system dynamics \( f(x,u,d) \) satisfies certain continuity constraints, \( \phi(x,t) \) is the solution to the terminal value Hamilton-Jacobi PDE

\[
\frac{\partial \phi}{\partial t} + H(x, \frac{\partial \phi}{\partial x}) = 0, \quad \phi(x,0) = \phi_0(x)
\]

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

\[
H(x,p) = -\max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} p^T f(x,u,d)
\]

where \( p \) is a placeholder for \( \nabla \phi \). In the opposite case where the control input attempts to minimize the reachable set and the disturbance input attempts to maximize the reachable set, the Hamiltonian is defined as

\[
H(x,p) = -\max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} p^T f(x,u,d)
\]

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 dynamics \( \dot{x} = f(x,K(x)) \), which is input free. In this case, the Hamiltonian becomes

\[
H(x,p) = p^T f(x,u,d) = -(p_1 v_1 \cos x_3 + p_2 v_2 \sin x_3 + (p_1 x_2 - p_2 x_1 - p_3) u_2 - p_1 u_1)
\]

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. Given that the system becomes effectively input free when we specify the control inputs to the system, the computation of the capture set and unsafe set differs only in the formulation of the target set. 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:

\[
\mathcal{G}_0 = \{ x \in \mathcal{X}, d_0 \leq d(x) \} \setminus N
\]

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

For general system dynamics, the solution to the Hamilton-Jacobi 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 [9] for MATLAB, based upon the level set theory described extensively in [10] and [11]. 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 number of grid cells used. As such, there is a trade off between resolution and computational cost.

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>
<thead>
<tr>
<th>Maneuver</th>
<th>( k_1 )</th>
<th>( k_2 )</th>
<th>( x_{1f} )</th>
<th>( x_{2f} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breakaway 1</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Precapture</td>
<td>0.15</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Capture</td>
<td>5</td>
<td>5</td>
<td>0.25</td>
<td>0</td>
</tr>
<tr>
<td>Postcapture</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Breakaway 2</td>
<td>0.15</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Rejoin</td>
<td>5</td>
<td>5</td>
<td>0.25</td>
<td>1</td>
</tr>
</tbody>
</table>
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 Precapture maneuver (transition from waypoint 2 to 3) can be chosen to be

$$G_0 = \left\{ x_1 \in [0.75, 1.25], x_2 \in [-0.25, 0.25], x_3 \in [-\pi/9, \pi/9] \right\}$$

To compute the capture set of this maneuver, we used the Hamiltonian function defined in Section IV, substituting the Precapture 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 5.

For all states within this reachable set, the UAV is guaranteed to be driven into the desired target set within 10 seconds under the Precapture 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 (Breakaway 2). By this, we can guarantee that if the UAV reaches the target set for Breakaway 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 Breakaway 2 transition includes the target set for the Postcapture transition. In this manner, we obtain a sequence of time horizons that can be used as the transition timings.

In Figure 6, 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. Unsafe Sets Computation and 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, unexpected environment 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 remove itself from the unsafe zone into a part of the state space where it could resume the refueling process.

Here we will describe one such scenario and show how the unsafe set can be used to generate the sequence of maneuvers to avoid the unsafe zone. In Figure 7, we see that at time \( t = 0 \), the UAV starts at a position just in front of the tanker, perhaps after having just missed the fuel boom. If the UAV does not have the help of reachable set, then it might choose to steer right and then backup into the reachable set of the “Capture” maneuver. However, with the unsafe reachable set for the steering right maneuver (shown as dashed line) superimposed on top of the UAV, it can be clearly seen that the UAV is inside the unsafe reachable set for that maneuver. After running the simulation for 5 seconds, the UAV indeed enters the unsafe zone of the tanker aircraft due to its inability to steer fast enough to avoid the tanker.

However, suppose that we approach the same situation with the reachable set data for all of the escape modes available. In this case, the UAV could easily perform a lookup operation to check whether it is inside the unsafe set of any of the escape modes. It would then select an escape maneuver whose unsafe set does not include the current state of the UAV. In this example, the UAV could select the speed up maneuver (escape mode 4), whose unsafe set is almost exclusively behind the tanker aircraft. After this maneuver has been performed long enough so that the UAV is outside the unsafe set of the steering right maneuver (escape mode 2), the UAV could perform a mode switch and steer right. This agrees with the intuition that the UAV needs to give itself some cushion before performing the steering maneuver. The result from this simulation is shown in Figure 8. As expected, the UAV does not enter the unsafe zone of the tanker aircraft throughout the escape sequence. This sequence of maneuvers was constructed by inspection of the reachable sets superimposed on the trajectories of the UAV. An algorithm for autonomous decisions can be built based on intuition obtained from this simulation.

Fig. 7: Unsafe Escape Maneuver. Since the UAV begins within the unsafe set, transitioning immediately into the prescribed escape maneuver violates rules of separation. Note that since the maneuver is to turn right, that the unsafe set veers to the left of the tanker.

(a) Escape Mode 2 (Steer Right) (b) UAV enters tanker’s unsafe zone, initiated at \( t = 0 \) seconds. shown here at \( t = 4 \) seconds.

Fig. 8: Safe Escape Maneuver. Since the UAV begins in an unsafe region to initiate Escape Mode 2, it uses Escape Mode 4 to travel out of the unsafe region, prior to calling that maneuver.

C. Fallback/Waveoff Scenario Simulation

As shown in the hybrid system model for the refueling maneuver presented earlier, during any of the refueling maneuvers, the UAV may encounter unexpected situations such as turbulence, malfunctioning fuel boom, etc., that prevent the safe completion of a given maneuver. In such cases, the UAV may receive operator commands to abandon its current maneuver and perform a fallback. If no human operator commands are received, the UAV may also initiate fallback autonomously based upon unsafe reachable set data. When the UAV is close to the tanker, there is also the possibility that in performing certain fallback maneuvers, the trajectory of the UAV may enter the unsafe zone of the tanker aircraft. Thus, the task becomes avoiding unsafe mode switches, as well as minimizing the time it takes to reach the fallback location.

In our fallback 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 Capture 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. The UAV would then use the time horizon over which the reachable sets are generated to come up with an estimate of the time to reach. If reachable sets are generated for multiple time horizons, the UAV could then choose the sequence with the minimum time to reach.

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 would be to simply back up the UAV directly and then perform the capture 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 Capture maneuver. It is important to note that part of the reachable set for the Capture 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 9. 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.

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 reaches 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 realizability. 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


