Ricky W. Butler et al.: NASA Langley's Formal Methods Research in Support of the Next Generation Air Transportation System, Proceedings of The Sixth NASA Langley Formal Methods Workshop, p.3–5

NASA Langley's Formal Methods Research in Support of the Next Generation Air Transportation System

Ricky W. Butler[1], *César A. Muñoz*[2]

[1] *NASA Langley Research Center, Hampton, Virginia 23681, USA*
[2] *National Institute of Aerospace, Hampton, Virginia 23666, USA*
R.W.Butler@nasa.gov, munoz@nianet.org
http://www.shemesh.larc.nasa.gov/fm

Extended Abstract

This talk will provide a brief introduction to the formal methods developed at NASA Langley and the National Institute for Aerospace (NIA) for air traffic management applications. NASA Langley's formal methods research supports the Interagency Joint Planning and Development Office (JPDO) effort to define and develop the 2025 Next Generation Air Transportation System (NGATS). The JPDO was created by the passage of the Vision 100 Century of Aviation Reauthorization Act in Dec 2003. The NGATS vision calls for a major transformation of the nation's air transportation system that will enable growth to 3 times the traffic of the current system. The transformation will require an unprecedented level of safety-critical automation used in complex procedural operations based on 4-dimensional (4D) trajectories that enable dynamic reconfiguration of airspace scalable to geographic and temporal demand.

The goal of our formal methods research is to provide verification methods that can be used to insure the safety of the NGATS system. Our work has focused on the safety assessment of concepts of operation and fundamental algorithms for conflict detection and resolution (CD&R) and self-spacing in the terminal area. Formal analysis of a concept of operations is a novel area of application of formal methods. Here one must establish that a system concept involving aircraft, pilots, and ground resources is safe. The formal analysis of algorithms is a more traditional endeavor. However, the formal analysis of ATM algorithms involves reasoning about the interaction of algorithmic logic and aircraft trajectories defined over an airspace. These trajectories are described using 2D and 3D vectors and are often constrained by trigonometric relations. Thus, in many cases it has been necessary to unload the full power of an advanced theorem prover. The verification challenge is to establish that the safety-critical algorithms produce valid solutions that are guaranteed to maintain separation under all possible scenarios. Current research has assumed perfect knowledge of the location of other aircraft in the vicinity so absolute guarantees are possible, but increasingly we are relaxing the assumptions to allow incomplete, inaccurate, and/or faulty information from communication sources.

The following is a list of the projects that the Langley/NIA formal methods team have been involved with:

- Airborne Information for LateralSpacing (AILS)
- CD3D and KB3D Conflict Detection and Resolution algorithms
- Runway Incursion Prevention System (RIPS)

- Small Aircraft Transportation System (SATS)
- Enhanced Oceanic Operations (EOO)
- Loss of Separation (LoS) Recovery Algorithms

In this talk we will look at three of these: SATS, KB3D, and LoS.

The goal of the SATS program was to significantly increase the capacity of regional airports. One of the most revolutionary aspects of the SATS approach is the use of a software system to sequence aircraft into the SATS airspace with no air traffic controller present. Obviously, there are serious safety issues associated with these software systems and their underlying key algorithms. A formal finite-state machine model of the SATS operational procedures using 24 transition rules was developed. This enabled an exhaustive analysis of the entire state space of the concept of operations and the proof of six safety properties. Nine issues were identified during the formal analysis. Two issues required changes to the rules of the ConOps, five issues were due to implicit or explicit omissions, and two were clarifications. All recommendations from formal methods team were adopted by SATS Conops Team.

The KB3D project developed and formally verified a new algorithm for conflict detection and resolution. The KB3D algorithm is a generalization of Karl Bilimoria's CD&R algorithm to 3 dimensions. The algorithm (KB3D) produces multiple solutions that only require a change in only one state parameter (i.e. heading, ground speed, or vertical speed). The algorithm has been formally verified to produce correct solutions when either one or both aircraft use the algorithm. KB3D is guaranteed to generate at least one valid solution for two aircraft with arbitrary trajectories. Usually the algorithm generates six different solutions. For two aircraft executing the CD&R algorithm, a proof has been completed that shows that the algorithm is implicitly coordinated. That is the algorithm produces solutions that send the two aircraft in opposite directions without any explicit communication between the aircraft. For the perfectly symmetric situation, KB3D uses a symmetry breaking mechanism. All of the proofs were accomplished using the Prototype Verification System (PVS) developed by SRI International.

Recent work at Langley has been developing a formal framework for the mathematical analysis of conflict resolution algorithms that recover from loss of separation. This work is motivated by some recent TMX simulation studies of the KB3D algorithm. The TMX studies explored the capabilities of KB3D to deal with multiple aircraft in complex traffic situations. The traffic density was approximately 3 times today's traffic and was generated by extrapolation from existing traffic patterns. There were almost no situations where a loss of separation occurred. But, it became clear to us that the KB3D algorithm should be generalized to recover from those situations. In this work we have developed a rigorous definition of correctness for vertical and horizontal maneuvers and simple criteria for loss of separation recovery algorithms that are sufficient to guarantee correctness. We have sought to make the criteria simple so that algorithms can be checked against the criteria in a straight-forward way. The criteria only uses information available to the local aircraft, but are powerful enough to prove distributed system properties. In particular, we propose rigorous definitions of horizontal and vertical maneuver correctness that yield horizontal and vertical separation, respectively, in a bounded amount of time. We also provide sufficient conditions for independent correctness, e.g., separation under the assumption that only one aircraft maneuvers, and for implicitly coordinated correctness, e.g., separation under the assumption that both aircraft maneuver. An important benefit of this approach is that different aircraft can execute different algorithms and implicit coordination will still be achieved, as long as they all meet the explicit

criteria of the framework. The mathematical framework has been formalized and mechanically verified using the Prototype Verification System (PVS) developed by SRI International.

References

[1] SATS project publications, http://research.nianet.org/fm-at-nia/SATS/

[2] KB3D project publications, http://research.nianet.org/fm-at-nia/KB3D/

[3] FM publications, http://shemesh.larc.nasa.gov/fm/fm-main-research.html