Services for Fault-Tolerant Conflict Resolution in Air Traffic Management[*]

Paolo Masci
University of Pisa
Dpt of Information Engineering
via Diotisalvi, 2
Pisa, Italy
paolo.masci@iet.unipi.it

Henrique Moniz
University of Lisboa
Departamento de Informática
Edificio C6, Campo Grande
Lisboa, Portugal
hmoniz@di.fc.ul.pt

Alessandra Tedeschi
Deep Blue
Piazza Buenos Aires, 20
Rome, Italy
alessandra.tedeschi@dblue.it

[Project Paper]

ABSTRACT

Airborne Self-Separation is a new concept of dynamic management of air traffic flow, where pilots are allowed to select their flight paths in real-time. In this new operational concept, each aircraft is guided by an automated decision procedure and, based on the available information, enters into negotiations with surrounding aircraft in order to coordinate actions and avoid collisions. In this work, we explore the possibility of combining an approach based on Satisficing Game Theory together with fault-tolerant protocols to obtain a robust approach for conflict resolution and air traffic optimization in the context of Airborne Self-Separation.

1. INTRODUCTION AND MOTIVATION

Air Traffic Management (ATM) is the dynamic and integrated management of air traffic flow to minimize delays and congestion while guaranteeing safety and efficiency of operation in the airspace. ATM services are currently based on a rigid off-line flight planning, with little or no autonomy for pilots and companies. Indeed, in today's ATM the responsibility for maintaining a safe and efficient traffic flow is entirely delegated to ground-based air traffic controllers, that are in charge of issuing instructions to flight crews: the airspace is statically organized into sectors and airways, and controllers' skills are essential to maintain horizontal and vertical separation among aircraft. Unfortunately, such a controller-based approach to ATM does not scale up to cope with the increasing volume of future air traffic, which is expected to grow exponentially at a rate of 5 to 6 percent per year [6].

Several alternative solutions to overcome the limits of current ATM are actively under investigation. An interesting approach is *Airborne Self-Separation*, an operating environment in which pilots are allowed to select their route in real time and without any external control [19, 17, 9]. Therefore, pilots have more responsibility for the safe and efficient conduction of the flight. The advantages of Airborne Self-Separation, broadly conceived, will be twofold. First, it can lead to reduced costs, better fuel consumption and increased capacity. Indeed, optimization performed by the airlines can be more effective than the optimization performed by ground-based air traffic controllers, because different airlines can give higher priority to different parameters which depend on company strategy or other factors only known to the airline and crew. Second, the approach is decentralized which results into better scalability and resilience.

Aircraft are already equipped with communication systems allowing air-to-air and air-to-ground communication to assist flight crews in aircraft maneuvering. In particular, the Automatic Dependent Surveillance (ADS) is an air traffic surveillance technology currenlty installed on the aircraft. With the ADS system, each aircraft performs automatic and continuous transmission of information for use by other aircraft and ground facilities. Information may include the aircraft's identifier and the latitude/longitude, as well as user application data. The system is always active, and it requires no explicit intervention by the flight crew for proper functioning. The ADS system uses wireless communication, which is inherently unreliable, but the ADS technology does not provide services that guarantee reliable exchange of information. Hence, when needed, such services must be explicitly implemented on top of the ADS system. Furthermore, the increasing automation of ATM exposes the system to faults of malicious nature where some aircraft may sent purposely wrong or contradictory information in order to disrupt safe air traffic flow.

In this work, we explore the possibility of combining an approach based on game theory together with fault-tolerant agreement protocols to obtain a robust approach for conflict resolution and air traffic optimization in the context of Airborne Self-Separation. The remainder of the paper if organized as follows. Section 2 summarizes the main challenges for system design. The related work is discussed in Section 3. Section 4 presents Satisficing Game Theory (SGT), our game theory approach to Airborne Self-Separation. The

[*]This work was partially supported by the European Commission through the Network of Excellence ReSIST (IST-026764) and the Large-Scale Informatic Systems Laboratory (LASIGE).

SERENE 2008, November 17-19, 2008, Newcastle, UK.
Copyright 2008 ACM 978-1-60558-275-7/08/11...$5.00

fault-tolerant protocols and respective services are described in Section 5. Section 6 discusses some preliminary results. Finally, Section 7 concludes the paper.

2. CHALLENGES FOR SYSTEM DESIGN

Airborne Self-Separation can be presented as a coordination problem in a highly dynamic network topology that is formed by aircraft within communication range of each other. To this end, a number of interesting challenges need to be addressed from a distributed systems perspective:

Dynamism of the system. Given the mobile ad-hoc nature of the network, its topology is constantly changing and along with it, the set of neighboring aircraft.

Openness of the communication medium. Due to its nature, wireless communications are inherently unreliable being affected by factors such as electromagnetic interference, collisions among transmissions. Moreover, loss of connectivity due to aircraft falling out of the communication range of each other must be taken into account, as well as contention to access the shared communication medium, which may cause transmissions to be delayed for arbitrarily long periods of time.

Strict safety requirements. Since failures can have catastrophic consequences (e.g., a collision between two aircraft), the system must be resilient to failures and ensure a safe operation despite them. To this end, failure mode assumptions, i.e., assertions on the types of errors that may introduced in the system, must be clearly stated.

3. RELATED WORK

A variety of techniques have been proposed so far for conflict resolution in the context of Airborne Self-Separation. Readers interested are redirected to [14, 4] for more extensive surveys on approaches to Airborne-Self Separation.

In [13], aircraft resolve conflicts as soon as they are detected. Multiple conflicts are addressed in sequence, trying to select a maneuvering decision to let the aircraft pass in front of or behind the conflicting aircraft. The strategies select maneuvering choices depending on smallest heading change and estimated collision time. In [15], a conflict scheme is proposed and evaluated in a scenario consisting of two perpendicular flows of air traffic that intersect at a fixed point. In [20], a resource allocation approach to collision avoidance is proposed. The approach divides the airspace into cells; then, to ensure separation, each cell is constrained to be occupied by only one aircraft at a time. In [18], a geometric approach to collision detection and resolution is proposed. A set of linear constraints on maneuvering options are used to specify routes of aircraft. The number of constraint formulations grows as $O(2^n)$ in the number of visible aircraft. The worst-case maneuvering requirements during state transitions are used to assess safety. In [2], a conflict resolution algorithm for en-route traffic conditions is evaluated through Monte Carlo simulation. Quantitative risk estimates are reported and results analysed in terms of safety. In [10], geometrical solutions are reported for basic scenarios and then an extension is proposed for more general situations.

Fault-tolerant agreement protocols for wireless networks represent relatively recent research within the scientific community. Chockler et al. propose consensus algorithms for systems where nodes fail only by crashing and messages are lost due to collisions [3]. They resort to a specialized failure detector which determines when message collisions occur and allows nodes to take some recovery actions. Koo et al. focus on a weaker problem, reliable broadcast, in multi-hop radio networks where each node adheres to pre-determined transmission schedule [12]. Their algorithm tolerates faults of malicious nature, but, as in [3] they rely on collision-detection information to solve the problem and assume messages are only lost due to collisions. Finally, Drabkin et al. present a (reliable) broadcast protocol for wireless ad-hoc networks in asynchronous systems [5]. This is done by extending the model with three types of failure detectors: mute, verbose, and trust that detect messages sent too often, messages not sent, and incorrect nodes, respectively. The broadcast protocol is then built by combining together these failure detectors along with the use of digital signatures and gossiping.

4. GAME THEORY FOR CONFLICT AVOIDANCE

Recent research in ATM have focused on solutions for conflict avoidance that are based on fixed sets of rules that dictate actions based on situational geometry. These approaches have offen very good performances in 'specific' situation, but acceptable performance in arbitrary situations cannot be always guaranteed. Moreover, they are generally not directly applicable in real-world scenarios, because of the high computational cost involved in dealing with dynamic environments. To address these problems, techniques based on the framework of game theory for multi-agent systems are currently under investigation, because they are designed to address situations where there is no centralized control and where there is a clear global objective function that needs to be optimized.

The main difficulty in applying game theory to multi-agent systems is that it is difficult to define the global objective function in terms of what is best for each agent [21]. A recent technique that tries to overcome such limit is based on Satisficing Game Theory (SGT) [11], which seeks for an "adequate" solution to the multi-agent system, rather than the optimal solution. Basically, SGT defines the objective function by means of two utility functions, selectability and rejectability, which represent benefits (selectability) and costs (rejectability) for each agent of making a choice. There may exist dependence between utility functions of different agents. In order to specify and analyse such system, utility functions can be conveniently viewed as marginals of a multivariate global probability function, in which dependences are expressed as conditional probabilities between variables. This way, a directed graph can be used to specify the system, and a solution can be obtained through standard Bayesian analysis.

In the ATM context, SGT can be applied as follows. Selectability and rejectability of each aircraft represent the benefits and costs of the aircraft's maneuvering choices. Benefits are essentially proportional to the optimality of the possible route. Costs, on the other hand, are proportional to the risk of collision with another aircraft. Correctly defining dependence between utility functions is the most important design factor, because dependences that are not necessary, besides increasing the cost to analyse the system, may also lead to unsatisfactory solutions (e.g., longer routes, complex maneuvering). In [11], a technique is proposed to correctly define dependencies: aircraft are ranked according to a certain policy, and then selectability of an aircraft is conditioned upon the selectability of all higher-ranked aircraft that are within a certain proximity range. Rejectability of agents are unconditioned: each aircraft responds to threats with exclusive self-interest. SGT scales well to high number of aircraft, since two important simplification can be safely applied: indirect influences between selectability functions can be discarded, and each aircraft can represent all viewable aircraft as a single entity that summarises their maneuvering choices [11].

4.1 Assumptions and Limits

SGT poses several shortcomings when applied to real-world scenarios. Namely, it makes two implicit assumptions about the information used to compute aircraft maneuvering: (1) information is homogeneous, and (2) information is fresh. Homogeneous means that aircraft have no contradictory information about any other aircraft. Fresh means that it always reflects the current state of other aircraft. For the SGT algorithm to function under these assumptions with a mere information exchange (i.e., every aircraft broadcasting its individual information), the system must be synchronous, i.e., information exchange can happen only at fixed time steps, and communication links must be reliable, i.e., no message must be lost at each time step.

Unfortunately, in a real environment things are never that tidy. Moreover, the wireless communication medium is inherently unreliable: if messages are sent out by aircraft within overlapping time intervals, then a collision occurs, leading to message loss. This may lead to failure scenarios that can disrupt SGT operation. For instance, if two aircraft in a collision course have incomplete or outdated information about each other, it is possible for each of them to derive maneuvering decisions that may further put them into a conflict. Additionally, may the communications subsystem of one of them fail, even if only temporarily, before their information about each other is harmonized, it is possible that a collision happens since both of them could be convinced that it is responsibility of the other aircraft to maneuver around.

5. FAULT-TOLERANT AGREEMENT SERVICES

We aim to employ fault-tolerant agreement protocols to design to a set of services that enhance the robustness of SGT even in the presence of faults of malicious nature. Based on classical distributed systems algorithms (i.e., consensus [8]), tailor-made for the ATM operating environment, the services can be made tolerant to a number of communication faults, and hence guarantee correct operation to SGT even if some messages exchanged between aircraft get lost or corrupted.

The provided services comprise *geographical group membership*, *rank consistency*, and *view augmentation*. These are described below.

Geographical group membership. This service, based on the aircraft geographic distribution at each instant, organizes them into sectors (or groups). Aircraft belong to the same group if they are within a proximity range R. It ensures that for every group, at least a majority of the aircraft is correctly aware of its membership.

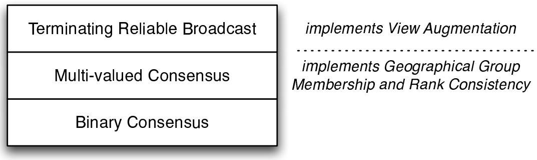
Terminating Reliable Broadcast
Multi-valued Consensus
Binary Consensus
implements View Augmentation
implements Geographical Group Membership and Rank Consistency

Figure 1: Protocol stack.

Rank consistency. Built on top of the geographical group membership, it ensures that aircraft have a consistent global view of each other within each group. It is defined in two variants: strong consistency and weak consistency. The strong consistency variant guarantees that every aircraft in group sees every other aircraft in the same way. This leads to a global deterministic ranking of aircraft within a sector by SGT. The weak consistency variant ensures that at least a majority of aircraft within a group will see every other aircraft in the same way. This guarantees that at least a majority of aircraft within a group will construct the same ranking in SGT.

View augmentation. Built on top of the two other services, expands an aircraft's awareness beyond its groups. Instead of being limited to the aircraft belonging to its groups, aircraft become aware of the members belonging to every adjacent group. Two groups are adjacent if both have at least one aircraft in common. This expanded view of the environment can be useful for further reliability and optimization of traffic flow.

The implementation of these services is supported by a stack of protocols that provides agreement algorithms to be used as primitives. The stack is depicted in Figure 1 and is composed, bottom-up, by a binary consensus protocol, a multi-valued consensus protocol, and a terminating reliable broadcast protocol.

5.1 System Model and Protocols

The system is modeled as set of n processes (i.e., the aircraft) that exchange information in synchronous steps. In order to capture the transient nature of faults in wireless environments it is determined that the transmissions of up to f processes per round may be faulty where $n = 3f + 1$. This includes both omission faults (where a message is lost) and corruption faults (where the contents of a message are changed). The latter captures the potential malicious behavior of processes.

The binary consensus protocol, at the bottom of the stack, represents the most basic form of agreement (i.e., on a single bit of information) and it is used as a building block for the remaining protocols. Basically, each process p_i proposes a value v_i and all processes decide on the same value $d \in \{0, 1\}$. Additionally, the protocol guarantees that if all correct processes propose the same initial value v, then the decision value is v.

On top of the binary consensus is built the multi-valued consensus protocol. This protocol allows processes to agree on a value v from an arbitrary domain $\mathcal{V}$. Each process proposes a value $x_i \in \mathcal{V}$ and they all decide on a value v proposed by some process or on a default value $\perp \notin \mathcal{V}$. The protocol also ensures that if all processes propose the same value v, then the decision value is v, and that if a decision is made on a value $v \neq \perp$, then v was proposed by at least one process whose transmissions were not faulty. Multi-valued consensus represents a much more useful abstraction (i.e., agreement on any kind of information) and is used to implement two of the proposed services: group membership and rank consistency. The relationship between consensus and group membership is well-known [7], while the rank of aircraft is just a piece of arbitrary information that can be trivially agreed using multi-valued consensus.

Finally, on top of the stack there is the terminating reliable broadcast protocol that is used to implement the view augmentation service. It is an information dissemination protocol that provides strong properties. It allows a process to transmit a message with value m that is guaranteed to be delivered uniformly at all processes: either every process delivers m or every process delivers a default value $\perp$. In either case, processes always deliver a message even if the sending process is affected by transmission failures. In this case, processes must be able to deliver a message $\perp$ not actually broadcast by the sending process.

6. PRELIMINARY EVALUATION AND RESULTS

The distributed decision procedure of SGT has been tested in [1] by running the algorithm inside an ad-hoc simulation environment developed in Java. Simulations were performed for two-dimensional scenarios, for both fixed geometries and completely random traffic patterns and arbitrary traffic densities. Different test scenarios, well-known in literature, like Choke Point scenario, Perpendicular Flows scenario and the Random Flights scenario. In the Choke Point scenario all aircraft begin from evenly spaced points on a circle. The destination of each aircraft is the point on the circle opposite its starting point. Thus, all aircraft are set to pass through the centre of the circle at the same time, creating a considerable challenge for any conflict resolution algorithm. Applying SGT we obtain good results both in terms of absence of missed separation and efficiency. No loss of separation occurred for a maximum of 14 aircraft in a circle of 50 nmi radius, i.e. a regime of very high densities. The Perpendicular Flow scenario is made up of two traffic flows: one from left to right and the other from top to bottom. In this scenario, aircraft must perform conflict avoiding maneuvers approaching the intersection point. There are no missed separations for an arbitrarily large number of aircraft (keeping a fixed distance between aircraft bigger than the separation radius), but increasing the number of aircraft, there is a consequent loss of the overall efficiency of the system. In the Random Flights scenario, which reflects open airspace with no obstacles other than other aircraft, aircraft appear at random points on an outer circle. They are assigned a random destination point on the inner circle. We performed several simulation runs, up-to 14 aircraft in a square with a virtual 100 nautical miles side, which represents a density that is approximatively twice the current European average density. In all simulation runs we obtained no missed separation. Results from these preliminary simulation experiments are encouraging, but further study is needed in order to assess safety constraints when dealing with unreliable communication between aircraft.

The fault-tolerant agreement protocols we intend to use as basis to support SGT operation have been evaluated in wireless environments in [16]. The practicability of such protocols have been demonstrated in wireless environments with their execution times being around the hundreds of milliseconds. These results, however, were provided by protocols that are not specially fit for wireless environments. For instance, they rely on reliable point-to-point channels for their correct operation which hinders their performance on shared and broadcast mediums such as wireless networks. Considerable performance enhancements are to be expected by redesigning such protocols specifically to wireless environments such that the features provided by these environments can be properly exploited.

7. CONCLUSIONS AND FURTHER WORK

With the steady increase of air traffic volume, the demand for automated decision-support systems for ATM will grow. Decisions that are fundamentally based on human interaction will have to be progressively replaced by more efficient forms of control without adversely affecting safety. We propose to combine an approach taken from the framework of Game Theory with fault-tolerant agreement protocols in order to obtain a dependable solution to ATM. Preliminary evaluation of the two components of the proposed system are encouraging to the feasibility of the solution. Further study is still needed. Currently, we are integrating the two components of the system in order to evaluate the proposed solution inside the Omnet++ [22] network simulator, which supports wireless environments and node mobility through the INET framework extension. Future work includes also exploring the possibility of using formal frameworks to specify and verify basic properties of the proposed system.

8. REFERENCES

[1] F. Bellomi, R. Bonato, V. Nanni, and A. Tedeschi. Satisficing game theory for distributed conflict resolution and traffic optimisation. Technical report, Deep Blue s.r.l., Rome, Italy, 2008.

[2] H. Blom, B. Obbink, and G.J.Bakker. Safety risk simulation of an airborne self separation concept of operation. In *7th AIAAATIO Conference*, 2007.

[3] G. Chockler, C. Newport, M. Demirbas, T. Nolte, and S. Gilbert. Consensus and collision detectors in wireless ad hoc networks. In *In PODC Õ05: Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing*, pages 197–206. ACM Press, 2005.

[4] D. Dimarogonas and K. Kyriakopoulos. Inventory of decentralized conflict detection and resolution system in air traffic. Deliverable D6.1–Hybridge Project, June 2003.

[5] V. Drabkin, R. Friedman, and M. Segal. Efficient byzantine broadcast in wireless ad hoc networks. In *In Proceedings of the IEEE International Conference on Dependable Systems and Networks*, pages 160–169, 2005.

[6] Eurocontrol. Annual report eurocontrol 1998-1999.

[7] R. Guerraoui. The generic consensus service. *IEEE Transactions on Software Engineering*, 27:29–41, 2001.

[8] R. Guerraoui and A. Schiper. Consensus: the big misunderstanding. In *Proceedings of the IEEE*

International Workshop on Future Trends in Distributed Computing Systems, Oct. 1997.

[9] J. Hoekstra, R. Ruigrok, and R. van Gent. Free flight in a crowded airspace? *Astronautics and Aeronautics*, 193(32):533–545, 2001.

[10] I. Hwang, J. Kim, and C. Tomlin. Protocol-based conflict resolution for air traffic control. *ATCA Quarterly*, 15(1), 2007.

[11] F. Johnson, J. Hill, J. Archibald, R. Frost, and W. Stirling. A satisficing approach to free flight. *Networking, Sensing and Control, 2005. Proceedings. 2005 IEEE*, pages 123–128, March 2005.

[12] C.-Y. Koo, V. Bhandari, J. Katz, and N. H. Vaidya. Reliable broadcast in radio networks: the bounded collision case. In *PODC '06: Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, pages 258–264, New York, NY, USA, 2006. ACM.

[13] J. Krozel, M. Peters, K. D. Bilimoria, C. Lee, and J. Mitchell. System performance characteristics of centralized and decentralized air traffic separation strategies. Fourth USA/Europe Air Traffic Management Research and Development Seminar, 2001.

[14] J. Kuchar and L. Yang. A review of conflict detection and resolution modeling methods. *IEEE Transactions on Intelligent Transportation Systems*, 1(4):179–189, 2000.

[15] Z. Mao, D. Dugail, E. Feron, and K. Bilimoria. Stability of intersecting aircraft flows using heading-change maneuvers for conflict avoidance. *Intelligent Transportation Systems, IEEE Transactions on*, 6(4):357–369, December 2005.

[16] H. Moniz, N. F. Neves, M. Correia, A. Casimiro, and P. Verissimo. Intrusion tolerance in wireless environments: An experimental evaluation. In *PRDC '07: Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing (PRDC 2007)*, pages 357–364, Washington, DC, USA, 2007. IEEE Computer Society.

[17] B. D. Nordwall. Free flight: Atc model for the next 50 years. *Aviation Week and Space Technology*, 143(5):38–39, July 1995.

[18] L. Pallottino, E. Feron, and A. Bicchi. Conflict resolution problems for air traffic management systems solved with mixed integer programming. *Intelligent Transportation Systems, IEEE Transactions on*, 3(1):3–11, March 2002.

[19] T. S. Perry. In search of the future of air traffic control. *IEEE Spectr.*, 34(8):18–35, 1997.

[20] S. Resmerita and M. Heymann. Conflict resolution in multi-agent systems. In *IEEE Conference on Decision and Control*, pages 37–42, 2003.

[21] W. Stirling. Social utility functions-part i: theory. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 35(4):522–532, Nov. 2005.

[22] A. Varga. The omnet++ discrete event simulation system. In *Proceedings of the European Simulation Multiconference*, pages 319–324, Prague, Czech Republic, June 2001. SCS – European Publishing House.