Soft Walls: Algorithms to Enforce Aviation Security

Adam Cataldo
Prof. Edward Lee
Prof. Shankar Sastry

NASA JUP
January 22-23, 2004
NASA Ames, Mountain View, CA
Outline

- The Soft Walls system
- Objections
- Control system design
- Current Research
- Conclusions
A Deadly Weapon?

- Project started September 11, 2001
Introduction

- On-board database with “no-fly-zones”
- Enforce no-fly zones using on-board avionics
Early Prototype Using Stanford DragonFly UAVs

[Claire Tomlin, Jung Soon Jang, Rodney Teo]
Flight Test Result

Softwall algorithm takes control here

Nov 19th, 2003
Moffett Federal Air Field
Another Early Prototype, Demo’ed by Honeywell on National TV, Dec., 2003

• Based on advanced ground avoidance system
• Issues a warning when approaching terrain or a no-fly zone
• Takes over control from the pilot when approach is too close
• Returns control to the pilot after diverting
• Demonstrated on ABC World News Tonight Dec. 30, 2003

Both Prototypes use Autonomous Control

- Pilot or Path Planning Controller
- Soft Walls controller

Aircraft
Our End Objective is Not Autonomous Control but a Blending Controller

- Pilot
- Soft Walls
- Aircraft

bias pilot control as needed
Our End Objective

Maximize Pilot Authority,
but keep the aircraft out of forbidden airspace
Unsaturated Control

Pilot remains neutral

Pilot tries to fly into no-fly zone

Pilot turns away from no-fly zone

Control applied

No-fly zone
In the News

- **ABC World News Tonight with Peter Jennings**
  - Dec. 30, 2003

- **Radio Interviews**
  - NPR Marketplace
  - WTOP, Washington DC, July 14, 2003
  - As It Happens, CBC, July 9, 2003

- **Magazines**
  - New Scientist, July 2, 2003
  - Salon, December 13, 2001
  - Slashdot, July 3, 2003
  - Slashdot, Jan 3, 2004

- **Newspapers**
  - New York Times, April 11, 2002
  - Toronto Globe and Mail
  - The Washington Times
  - The Orlando Sentinel
  - The Straits Times (Singapore)
  - The Times of India
  - The Star (South Africa)
  - The Age (Australia)
  - Reuters, July 2, 2003

Objections

- Reducing pilot control is dangerous
  - reduces ability to respond to emergencies
There is No Emergency That Justifies Attempting to Land on Fifth Ave.

Although there are clearly regions of space where flying is absolutely unacceptable, regulatory restraint is required to avoid overconstraining the air space.

Today, some pilot responses to emergencies can result in a passenger aircraft being shot down.
Objections

- Reducing pilot control is dangerous
  - reduces ability to respond to emergencies

- There is no override
  - pilots want a switch in the cockpit
There are already regions of space for which no override switch enables transit.

Terrain imposes “hard wall” constraints on airspace. We are proposing that spaces be defined that are as surely constrained but more gently enforced.

Again, regulatory restraint is required to not overconstrain the airspace.
Objections

- Reducing pilot control is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - pilots want a switch in the cockpit
- Localization technology can fail
  - GPS can be jammed
Localization Backup

- Radio beacons
- Inertial navigation
  - drift limits accuracy
  - affects the geometry of no-fly zones
Objections

• Reducing pilot control is dangerous
  - reduces ability to respond to emergencies
• There is no override
  - pilots want a switch in the cockpit
• Localization technology can fail
  - GPS can be jammed

• Deployment could be costly
  - Software certification? Retrofit older aircraft?
Deployment

- Fly-by-wire aircraft
  - a software change
  - which is of course extremely costly

- Older aircraft
  - autopilot level?
  - Honeywell prototype?

- Phase in
  - prioritize airports
Objections

- Reducing pilot control is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - pilots want a switch in the cockpit
- Localization technology could fail
  - GPS can be jammed
- Deployment could be costly
  - how to retrofit older aircraft?

- Complexity
  - software certification
Not As Complex as Air Traffic Control

- Self-contained avionics system (not multi-vehicle)

- Human factors is an issue:
  - pilot training?
  - air traffic controller training?
Objections

- Reducing pilot control is dangerous
  - reduces ability to respond to emergencies
- There is no override
  - pilots want a switch in the cockpit
- Localization technology could fail
  - GPS can be jammed
- Deployment could be costly
  - how to retrofit older aircraft?
- Deployment could take too long
  - software certification

- Fully automatic flight control is possible
  - throw a switch on the ground, take over plane
Potential Problems with Ground Control

- **Human-in-the-loop delay on the ground**
  - authorization for takeover
  - delay recognizing the threat

- **Security problem on the ground**
  - hijacking from the ground?
  - takeover of entire fleet at once?

- **Requires radio communication**
  - hackable
  - jammable
Relationship to Flight Envelope Protection

- With flight envelope protection, the limits on pilot-induced maneuvers are known
- Knowing these limits enables tighter tolerances, and hence tighter geometries for no-fly zones.

see http://softwalls.eecs.berkeley.edu for FAQ
Here’s How It Works
Previous Algorithm: What We Want to Compute

No-fly zone

Backwards reachable set
States that can reach the no-fly zone even with Soft Walls controller

Can prevent aircraft from entering no-fly zone
The Backwards Reachable Set for the Stanford no–fly Ellipse

Theorem [Computing $G(t)$]:

$$G(t) = \{ x : J(x, t) < 0 \}$$

where $J(x, t)$ is the unique viscosity solution to:

$$- \frac{\partial J(x, t)}{\partial t} = \min\{0, \max_u \min_d H(x, \frac{\partial J(x, t)}{\partial x}, u, d)\}$$

$$H(x, \frac{\partial J}{\partial x}, u, d) \equiv \frac{\partial J}{\partial x} f(x, u, d)$$
What We Create

- The terminal payoff function $l: X \rightarrow \text{Reals}$

- The further from the no-fly zone, the higher the terminal payoff
Our Control Input

Backwards Reachable Set

optimal control at boundary

dampen optimal control away from boundary

optimal payoff function

State Space

Backwards Reachable Set
How we computing the optimal payoff (analytically)

- We solve this equation for $J^*$: $\text{Reals}^n \times [0, \mathcal{D}) \rightarrow \text{Reals}$

$$\frac{\partial}{\partial T} J^*(y, T) - \min_{e \in D} \min_{v \in U} \left\{ 0, \min \max \left( \nabla_y J^*(y, T) \right) \right\} f(y, v, e) = 0$$

- $J^*$ is the viscosity solution of this equation
- $J^*$ converges pointwise to the optimal payoff as $T \rightarrow \mathcal{D}$
- (Tomlin, Lygeros, Pappas, Sastry)
How we computing the optimal payoff (numerically)

- (Mitchell)

- Computationally intensive: n states \( \Rightarrow O(2^n) \)
Current Research: Model Predictive Control

- **Discretize Time**
  \[ x_{k+1} = f(x_k, u_k, d_k) \]

- **Control Algorithm—At Each Step**
  1. Compute safe control inputs for next N steps
  2. Calculate optimal control input for next N steps
  3. Use only the first optimal input
Computing Safe Control Inputs (Pappas)

• Given:
  - control inputs
  - pilot inputs
  - no-fly zone

• Compute:
  - safe control inputs

  If the next $N$ control inputs are in the safe set, then the state will remain outside the no-fly zone.

• We assume:
  $$x_{k+1} = f(x_k) + Bu_k + Cd_k$$
Calculating Optimal Input

- We want the control input to equal zero whenever possible
- We want the control input to change slowly from each input to the next
- We minimize, over the safe control inputs,
Stanford DragonFly UAVs

[Dragonfly 2]

[Ground Station]

[Dragonfly 3]

[Claire Tomlin, Jung Soon Jang, Rodney Teo]
Another Experimental Platform

- In collaboration with the Penn UAV team
Conclusions

• Embedded control system challenge
• Control theory identified
• Future design challenges identified
• http://softwalls.eecs.berkeley.edu
Acknowledgements

- Ian Mitchell
- George Pappas
- Xiaojun Liu
- Shankar Sastry
- Steve Neuendorffer
- Claire Tomlin