Verification of SATS Protocol:
Theorem Proving & Model Checking

Dileep Kini

SATS – Small Aircraft Transportation System

Small Aircrafts are growing in number

- Small Airports lack services and modern facilities
- Landing is very restrictive
- Throughput is small

SATS is a solution to increase accessibility and usage

- Requiring minimum infrastructure
- Maintain Safety

SATS Air Traffic Protocol

Allows multiple aircrafts in *Self Controlled Area* (SCA)

Specifies operational rules for aircrafts

- To avoid collision
- Maintain Progress

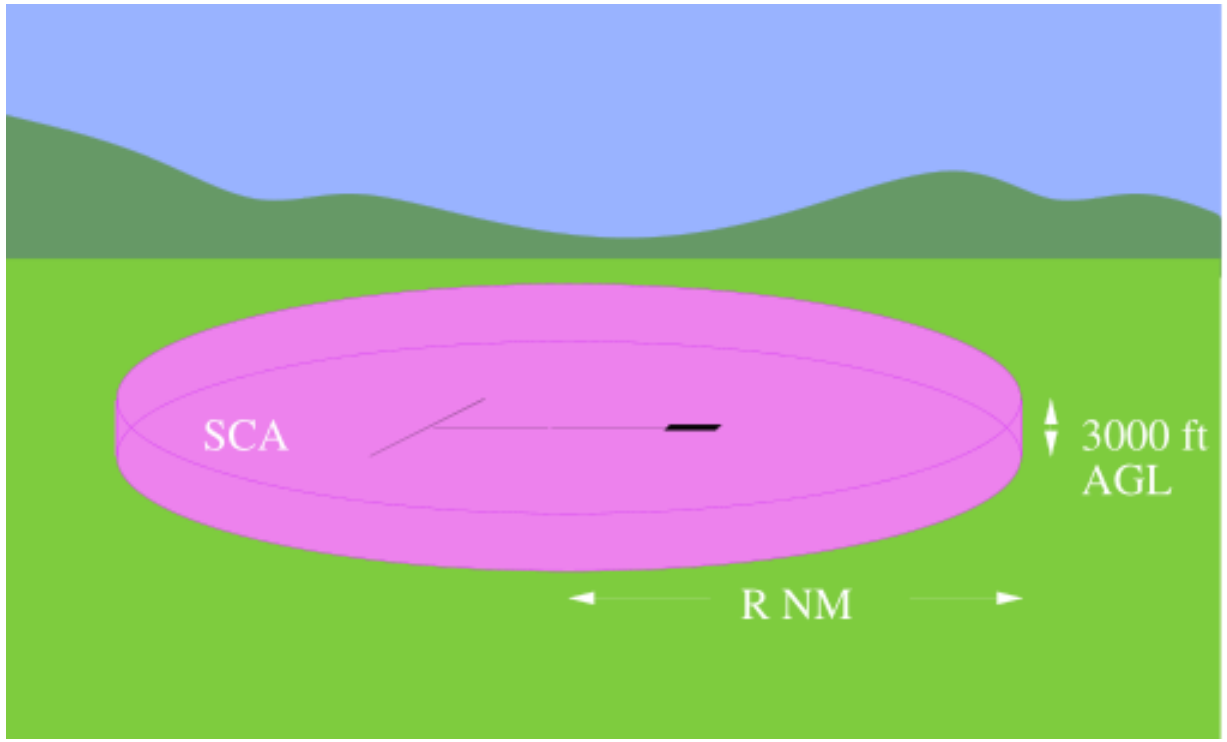
Requires

- Aircrafts have basic navigation tools
- Aircrafts able to communicate with Airport and each other

Self Controlled Area

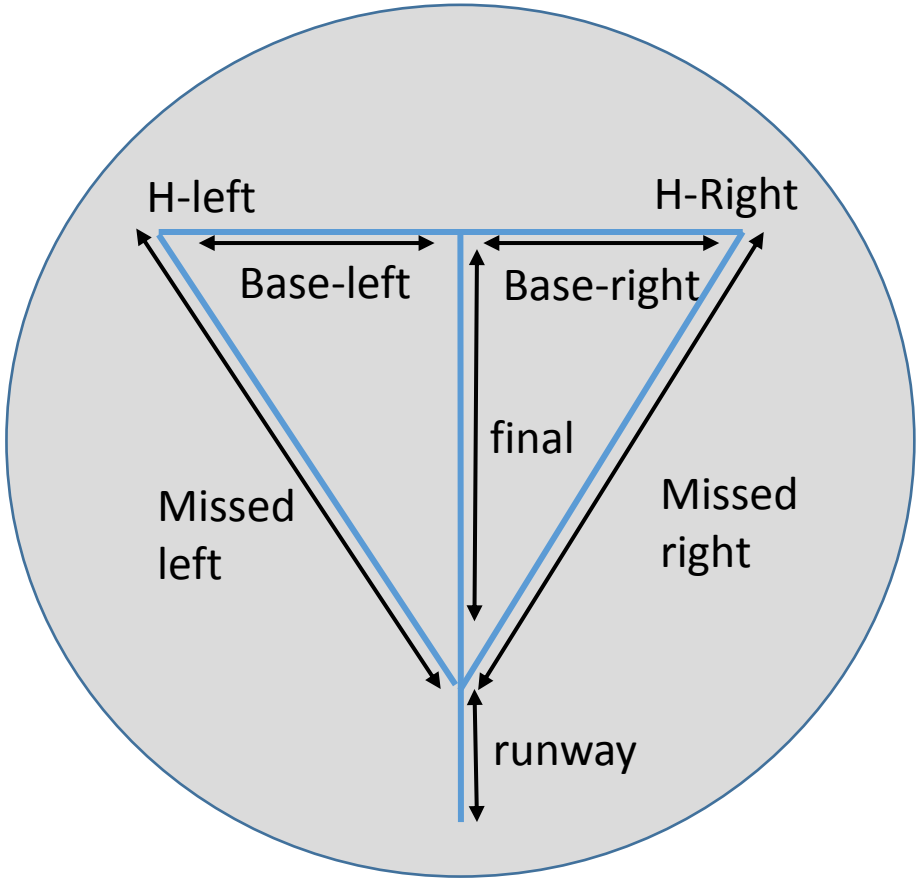
Encompasses volume around airport

Contains T-shaped approach to runway

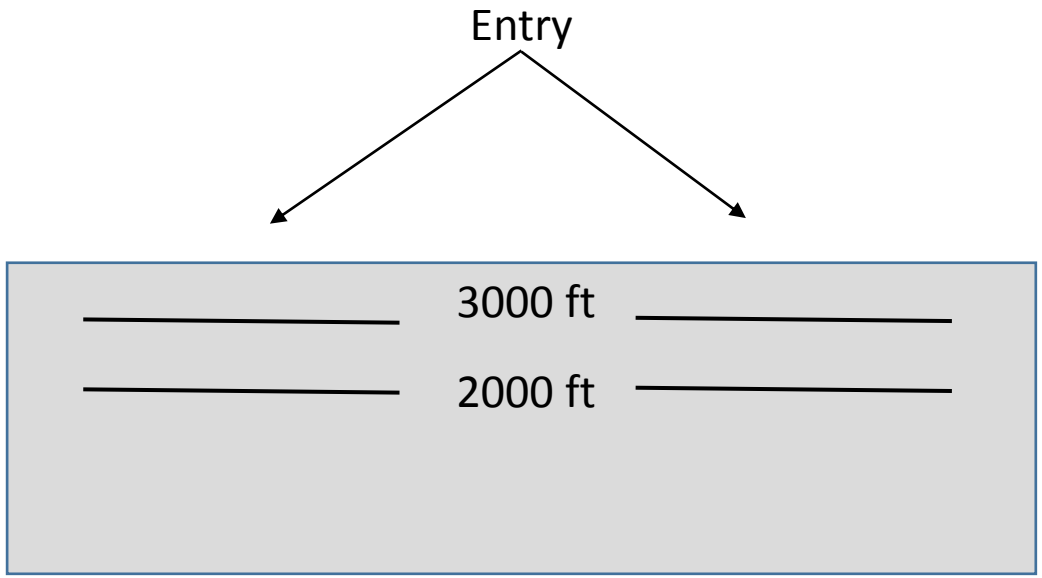


The Locations

Fixed regions/points in space



Top View



Holding levels
Ground View

The Framework

Each Aircraft i ($\in \mathbb{N}$) maintains the following

Variable	Type
x_i	$\mathbb{R}_{\geq 0}$
seq_i	$\mathbb{N}_{>0}$
m_i	$\{\ l\ , r\ \}$
loc_i	L

A global variable c maintained at the airport

Overview of Protocol

Allowed entry only when h3 is empty and < 2 aircrafts have the same missed approach assignment

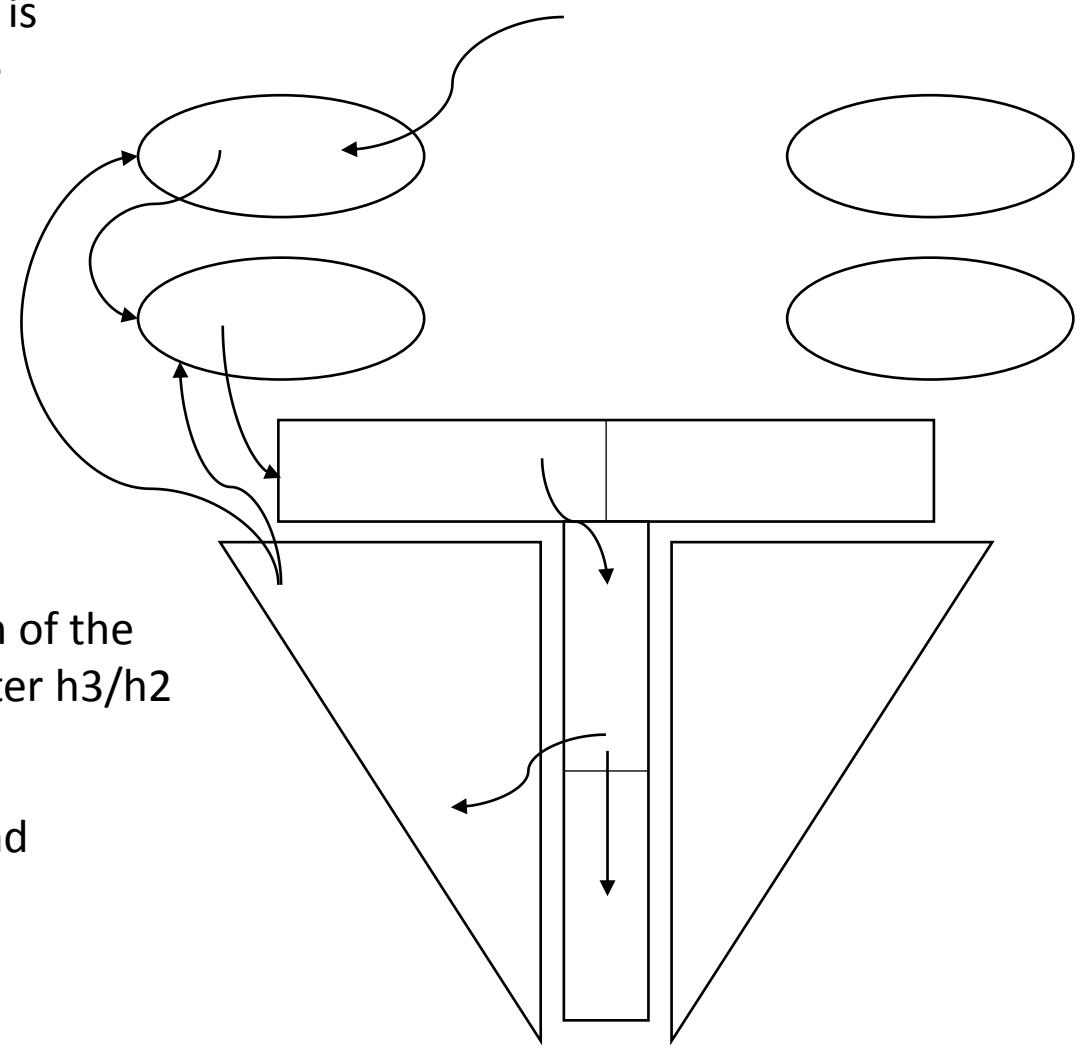
Can move to h2 if empty

Move to base segment if the aircraft before is safe distance ahead

Enter final approach when length of base covered

After covering length of the missed approach enter h3/h2

After covering the length of the final approach either land on the runway or enter the assigned missed approach



$$seq_i = c + 1;$$
$$c = c + 1;$$
$$m_i = l$$

Put the aircraft in the end of the sequence

Once the aircraft exits the runway decrease everyone's sequence

Verification

Our aim is to prove

- Separation Assurance
- Maintain Sequence

The Difficulty: we have to prove these for any arbitrary large number of aircrafts in the system

Theorem Proving

First we prove a key property:

- No more than 4 aircrafts in the system at any time

Holds independent of continuous dynamics

We prove this mechanically in PVS

Simulation relation from continuous to discrete version

Model Checking

Assume timed dynamics for aircraft speed

Model is going to be parallel composition of 4 aircrafts

Use UPPAAL to model check properties against model

- Properties can be specified in restricted TCTL

Model Checking

Separation Assurance:

$$\forall\Box((A_0.app \wedge A_1.app) \rightarrow (4 < |x_0 - x_1|))$$

Maintaining Sequence:

$$\forall\Box(\bigwedge(seq_0 = 1, seq_1 = 2, A_0.app, A_1.app) \rightarrow (x_0 > x_1))$$

Limitations

Rectangular Dynamics difficult to convert Timed Dynamics

Properties not expressible in UPPAAL’s TCTL

- Progress : Aircraft either lands or has infinitely many opportunities to do so