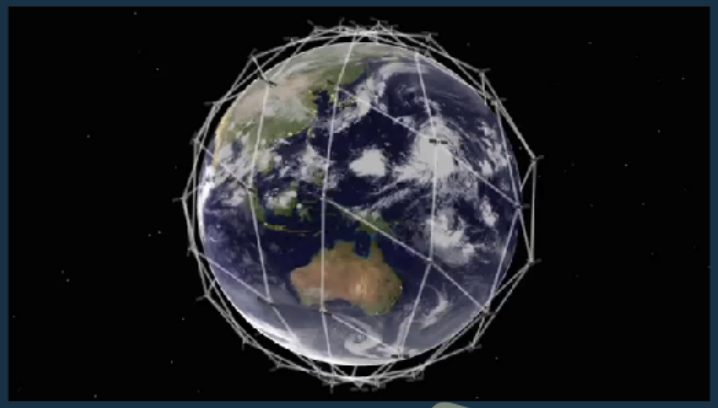
Model Checking Satellite Constellations

Yu Lu, Alice Miller, Gethin Norman, Chris Johnson
School of Computing Science, University of Glasgow

The Challenge

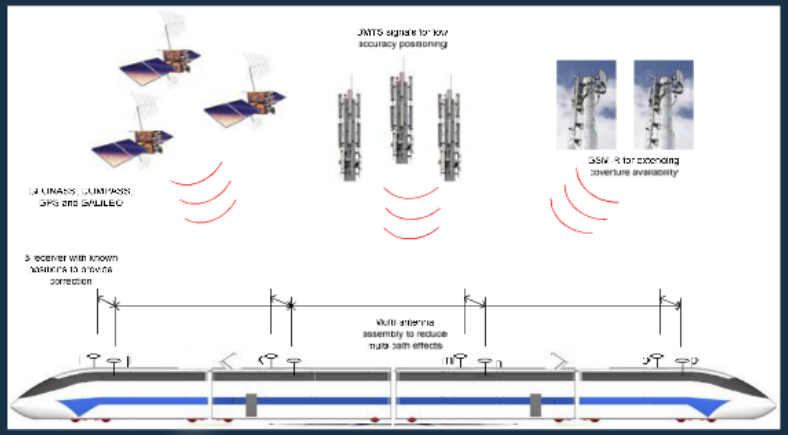
- Satellite systems: a core component for critical infrastructures
- Vulnerable to physical and cyber attacks & accidental faults
- System designers, engineers, and end users unaware of the failures



Why it is important

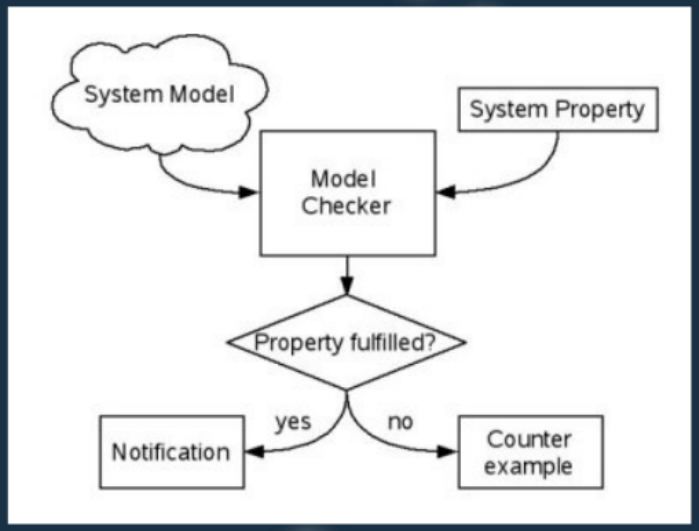
- Industrial critical applications depend on satellite constellations
- Consequences of failure in this are catastrophic

- European Train Control System (ETCS) Advanced Testing and Smart Train Positioning System (FP7-TRANSPORT-314219)



How it is solved

- Formally identify and quantitatively predict reliability, availability, maintainability, and safety (RAMS)
- Assess the likelihood and consequences of failure to operations
- Evaluate system performance & remove undesirable characteristics



Probabilistic model checking

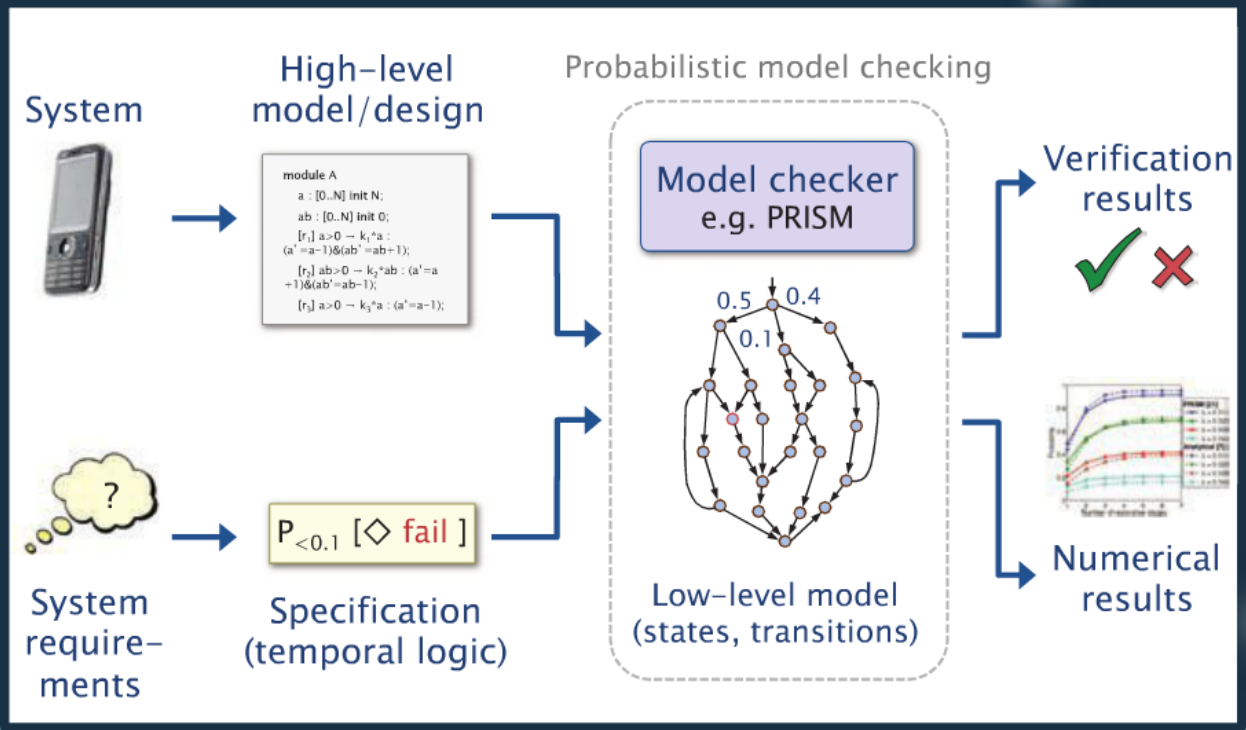
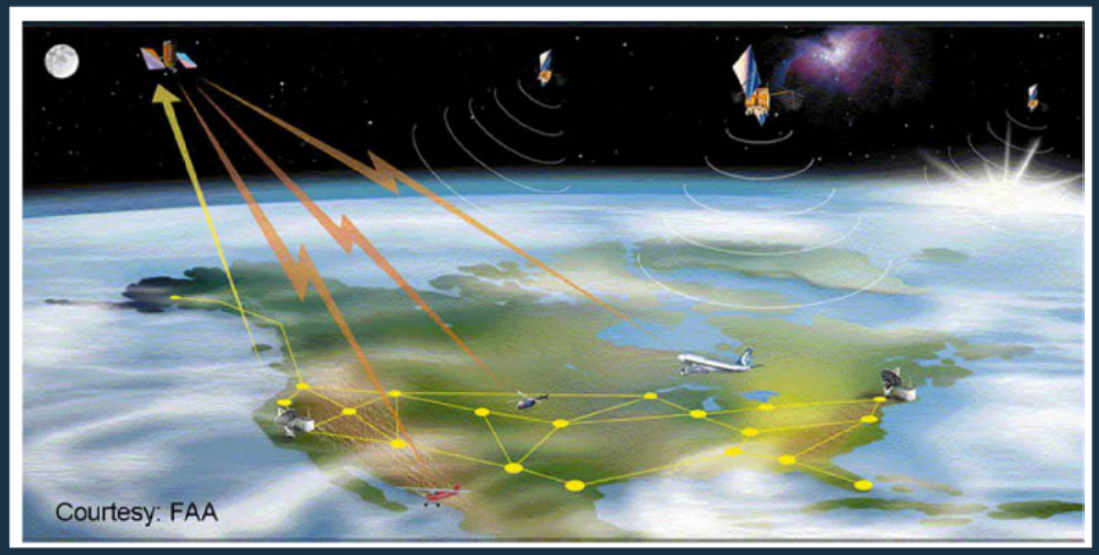
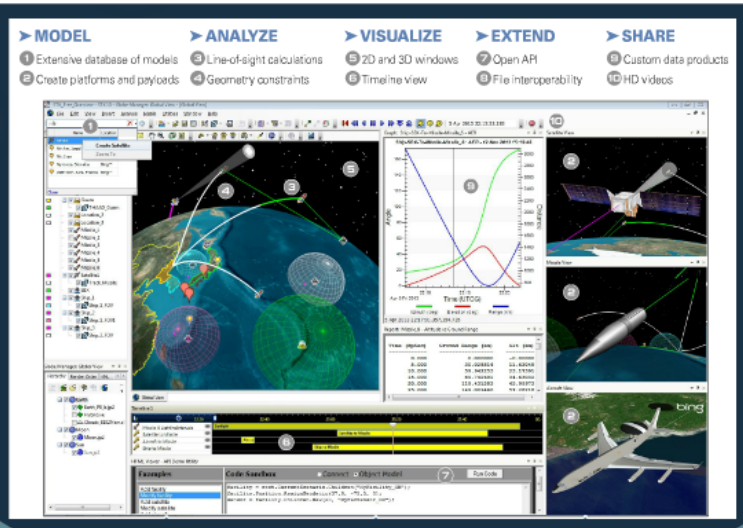


Figure . An overview of probabilistic model checking (source: http://www.prismmodelchecker.org/)

Datasets with STK





Modelling

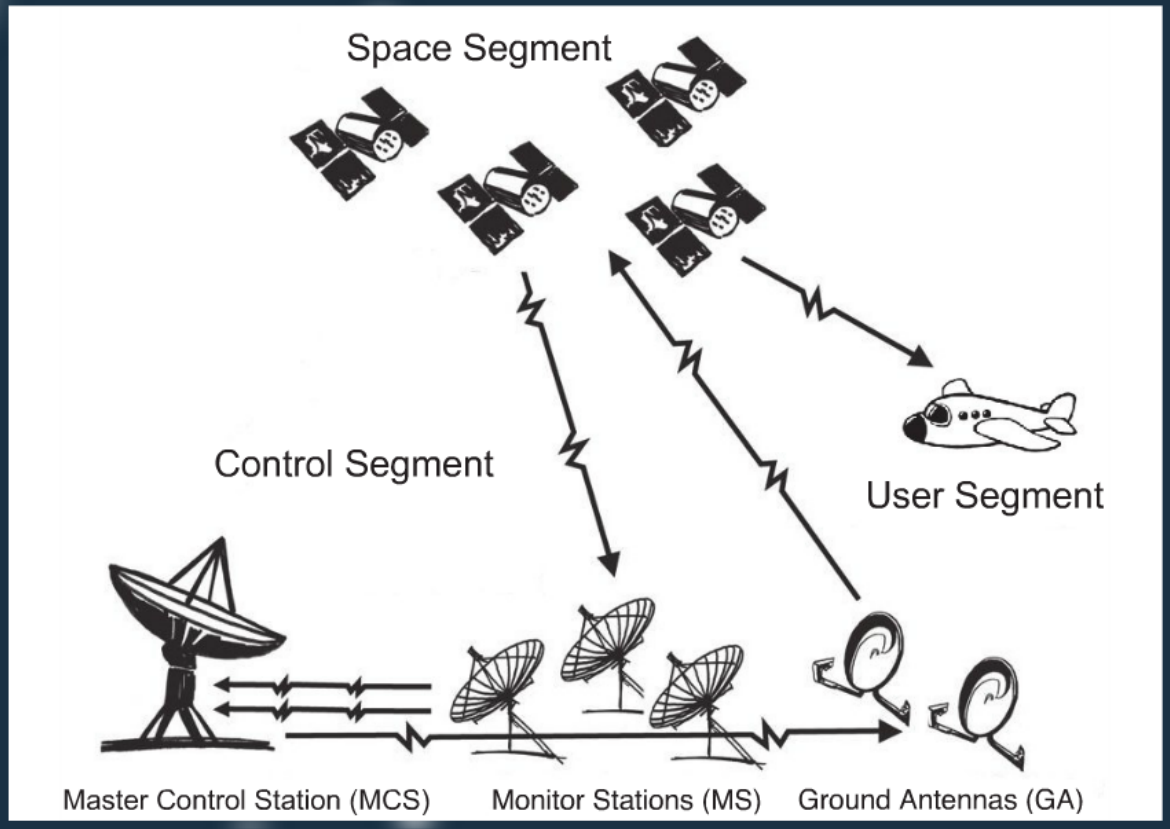
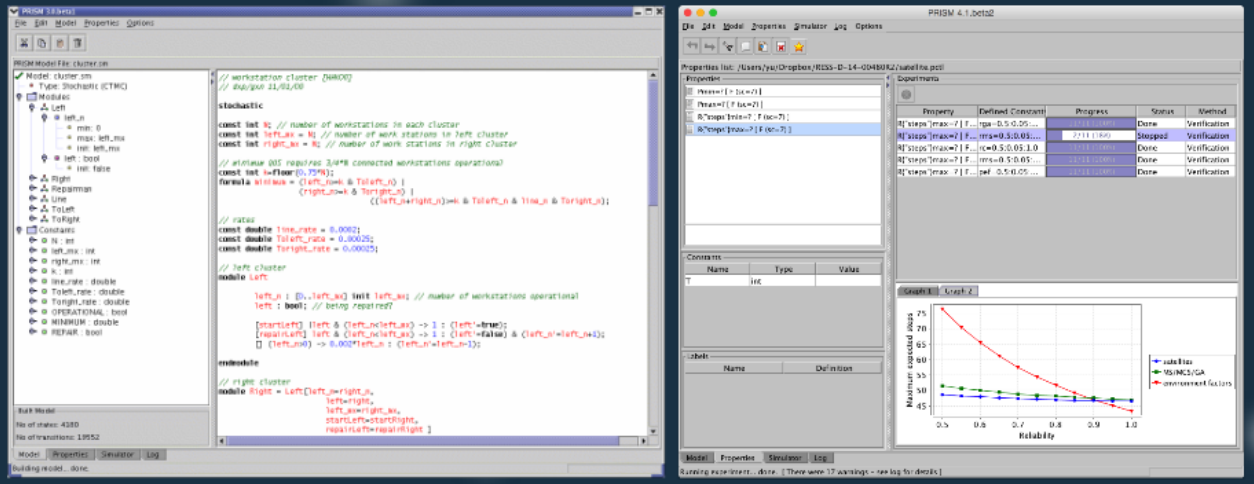


Figure. Reference models of agents

Model Checking with PRISM



Time	Nondeterminism	Probabilistic Models
discrete	no	discrete-time Markov chains (DTMCs)
	yes	Markov decision processes (MDPs) probabilistic automata (PAs)
continuous	no	continuous-time Markov chains (CTMCs)
	yes	**probabilistic timed automata (PTAs)** **priced probabilistic timed automata (PPTAs)**

Specification

- Quantitative Aspects of Correctness
  - Time, Probabilities, Resources
- Specifications
  - Probabilistic temporal logics (PCTL, CSL, Probabilistic LTL)

- – (unary minus)
- *, / (multiplication, division)
- +, – (addition, subtraction)
- <, <=, >=, > (relational operators)
- =, != (equality operators)
- ! (negation)
- & (conjunction)
- | (disjunction)
- <=> (if-and-only-if)
- => (implication)
- ? (condition evaluation: `condition ? a : b` means "if `condition` is true then a else b")
- **P** (probabilistic operator)
- **S** (steady-state operator)
- **R** (reward operator)
- **A** (for-all operator)
- **E** (there-exists operator)

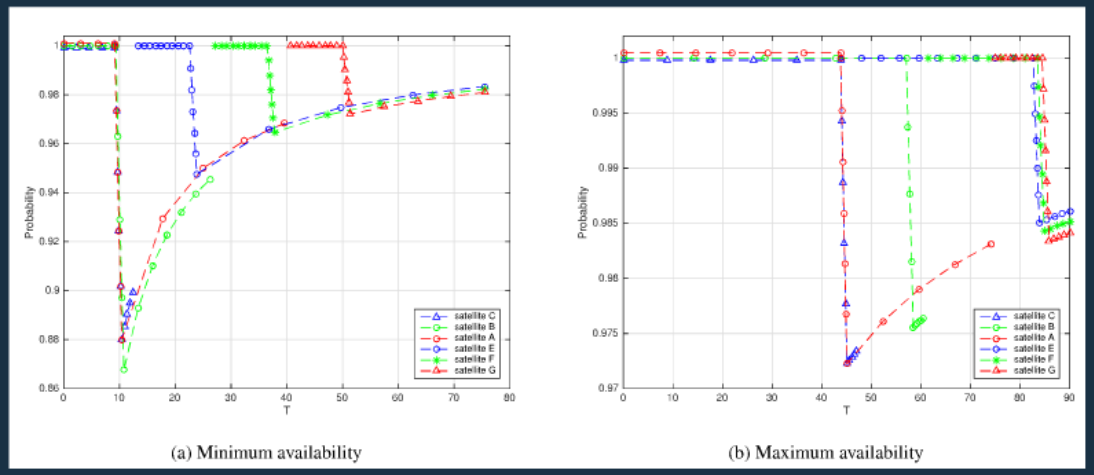
Figure . Operators (source: http://www.prismmodelchecker.org/)

- PCTL Properties
- $P\max =? \left[F\left(\text{spec1} \wedge \text{spec2}\right)\right]$
- $R\left\{\text{“energy”}\right\}\min =? \left[F\left(\text{spec3}\right)\right]$
- $P\max =? \left[\text{spec4} \wedge \left(\neg \text{spec5} \mathcal{U} \text{spec6}\right)\right]$

Verification

Name	PRISM notation	Meaning
"*avail. satellite*"	$\mathbf{P}_{min\geq 1}[F(sc=7)]$	Whether satellite C is available during the navigation?
"min. *avail. satellite*"	$\mathbf{R}_{min=?}[F(sc=6)]$	The minimum available time of satellite C
"max. *avail. satellite*"	$\mathbf{R}_{max=?}[F(s4=4)]$	The maximum expected time of navigation mission
"*min. unavail. channel*"	$\mathbf{R}_{min=?}[F(s5=3)]-\mathbf{R}_{min=?}[F(s5=2)]$	The minimum unavailable time of channel e3
"*max. unavail. channel*"	$\mathbf{R}_{max=?}[F(s5=6)]-\mathbf{R}_{max=?}[F(s5=5)]$	The maximum unavailable time of channel e1
"*min. avail. time bound satellite*"	$\mathbf{P}_{min=?}[F\leq T(sc=6)]$	The minimum probability that C done transmission with U within T
"*max. avail. time bound satellite*"	$\mathbf{P}_{max=?}[F\leq T(se=7)]$	The maximum probability that E done transmission with U within T

Summary of PRISM properties used



(a) Minimum availability

(b) Maximum availability

Availabilities of satellites