

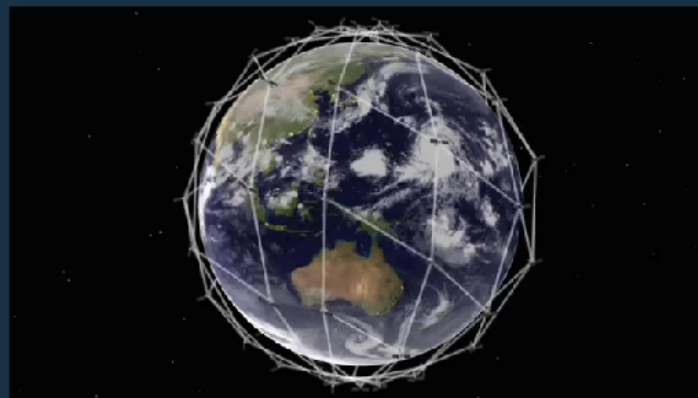


Model Checking Satellite Constellations

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

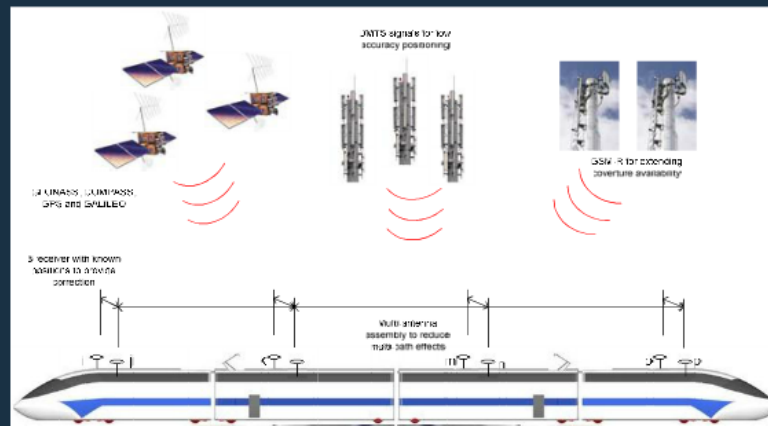
The Challenge

- 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



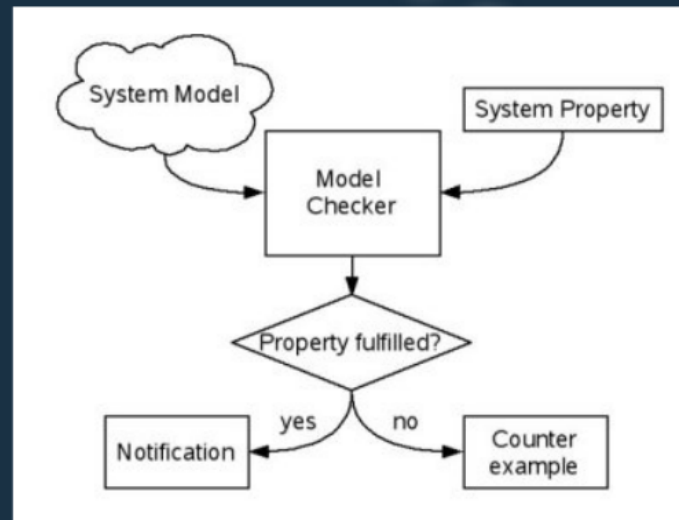
Why it is important

- 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

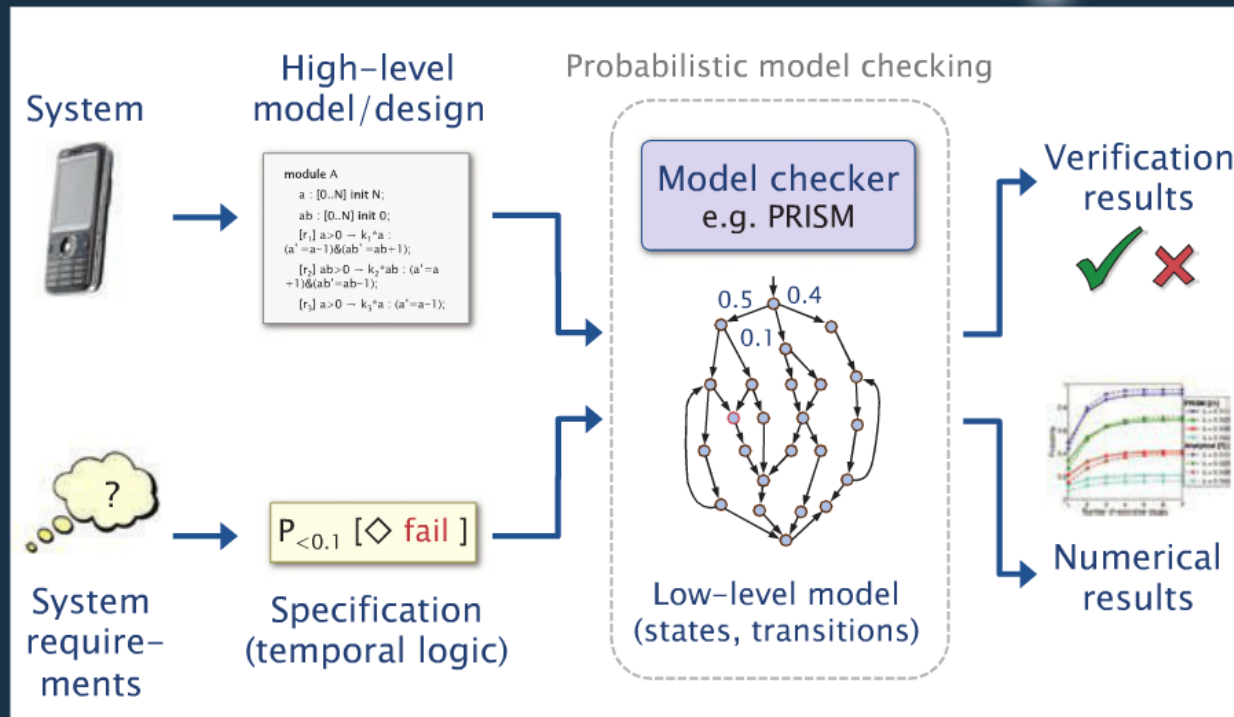
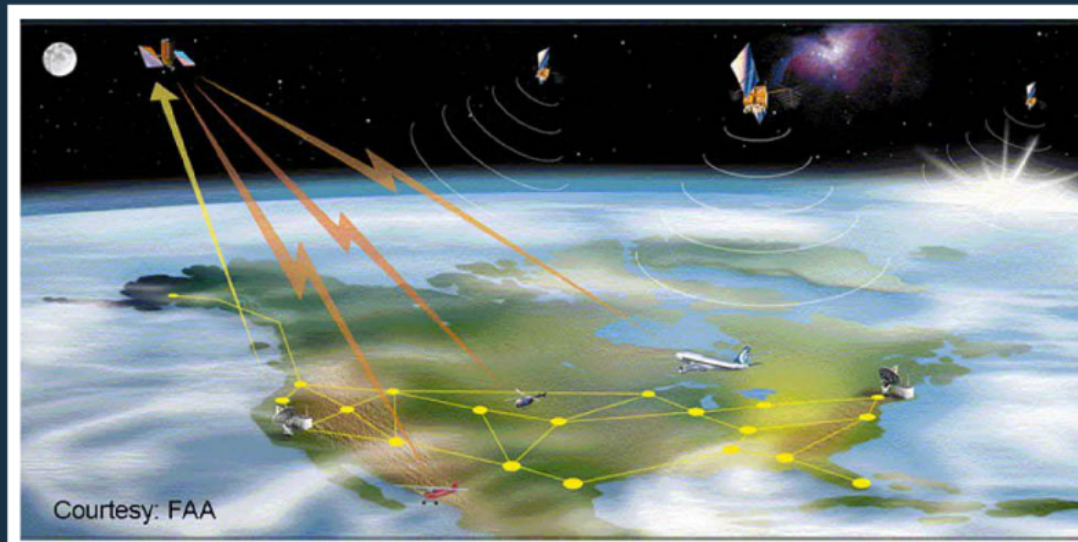


Figure . An overview of probabilistic model checking
(source: <http://www.prismmodelchecker.org/>)

Datasets with STK



> MODEL **> ANALYZE** **> VISUALIZE** **> EXTEND** **> SHARE**

- 1 Extensive database of models
- 2 Create platforms and payloads
- 3 Line-of-sight calculations
- 4 Geometry constraints
- 5 2D and 3D windows
- 6 Time/line view
- 7 Open API
- 8 File interoperability
- 9 Custom data products
- 10 HD videos

The screenshot shows the STK software interface with a 3D model of a satellite in orbit over Earth. A graph on the right displays data over time. The interface includes a toolbar, a file explorer on the left, and a console window at the bottom.

Modelling

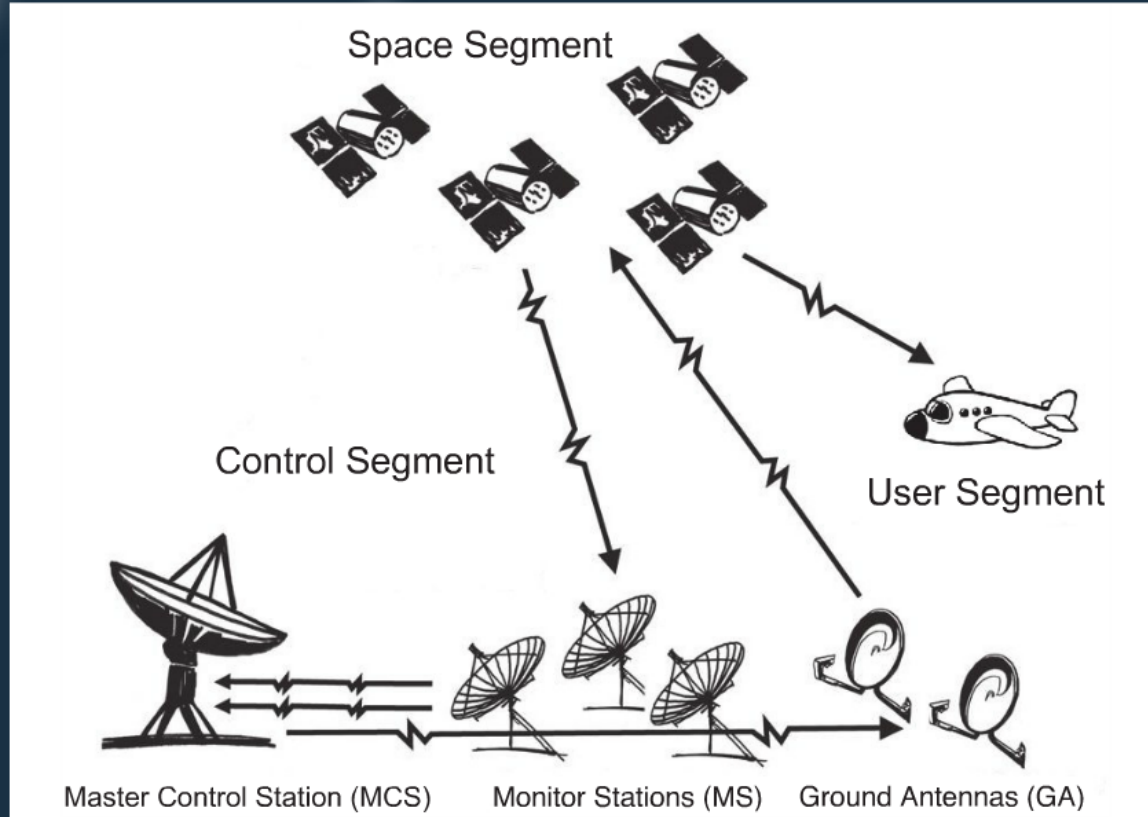


Figure. Reference models of agents

Model Checking with PRISM

The left screenshot shows the PRISM GUI with a model tree on the left and a code editor in the center. The code defines a workstation cluster with two clusters, left and right, each with a certain number of workstations. It specifies transition rates for various operations and defines a formula for the number of operational workstations.

The right screenshot shows the PRISM GUI with a properties list on the left, a table of verification results in the center, and a line graph on the right. The table lists properties such as $P_{\text{max}}[\text{max} \# \{ F \}]$ and $P_{\text{min}}[\text{min} \# \{ F \}]$ for different reliability values. The graph plots the number of states against reliability, showing a decreasing trend as reliability increases.

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)

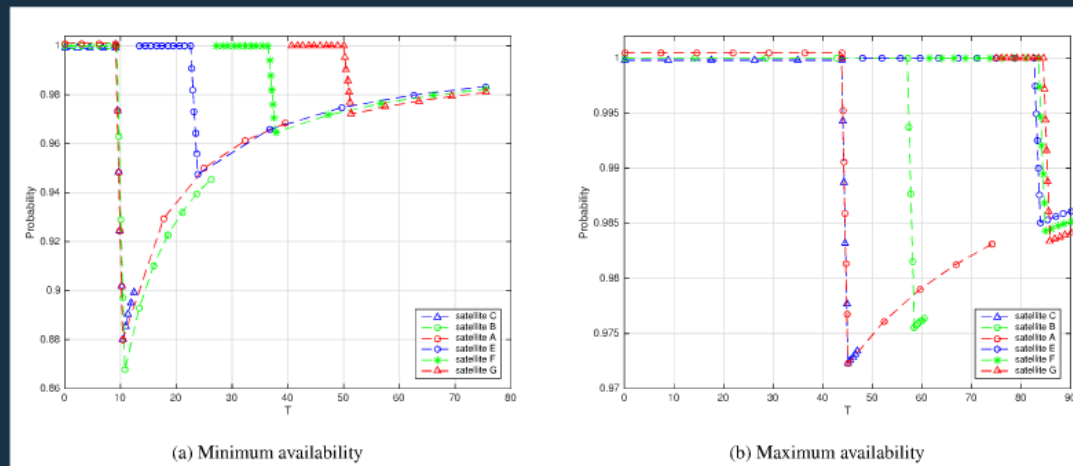
Figure . Operators (source: <http://www.prismmodelchecker.org/>)

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

Verification

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

Summary of PRISM properties used



Availabilities of satellites