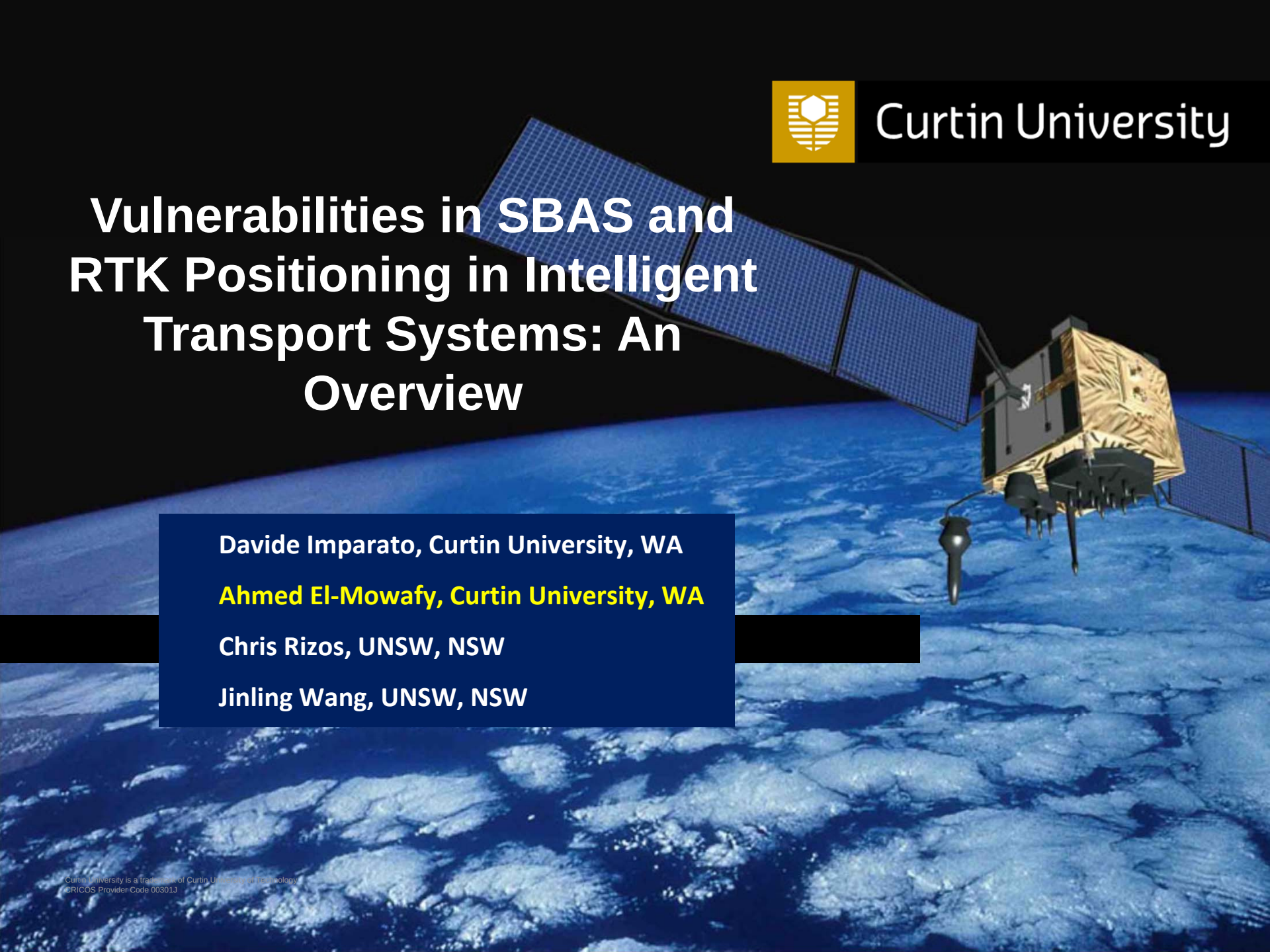


Vulnerabilities in SBAS and RTK Positioning in Intelligent Transport Systems: An Overview

Davide Imparato, Curtin University, WA

Ahmed El-Mowafy, Curtin University, WA

Chris Rizos, UNSW, NSW

Jinling Wang, UNSW, NSW

Contents

- Positioning methods for ITS
- Vulnerabilities: categorisation
- Vulnerabilities: characteristics and mitigation methods
- Conclusions

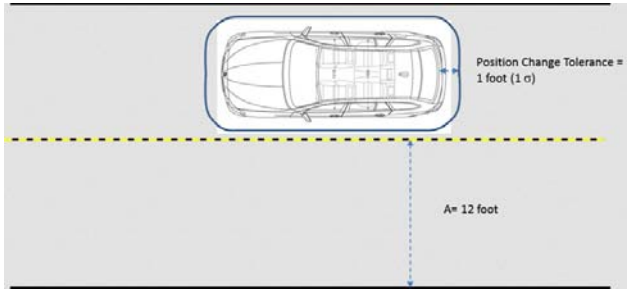
Why ITS

- Land transportation: areas for improvement:

- Make transportation safer, more efficient and reduce emissions: **Intelligent Transportation Systems (ITS)** → **C-ITS**, **Automated vehicles**, etc.
- Need of **GNSS** for absolute positioning

Satellite positioning accuracy requirements

- Road level (few m)
- Lane-level (< 1m)
- Where-in-lane level (sub-m)

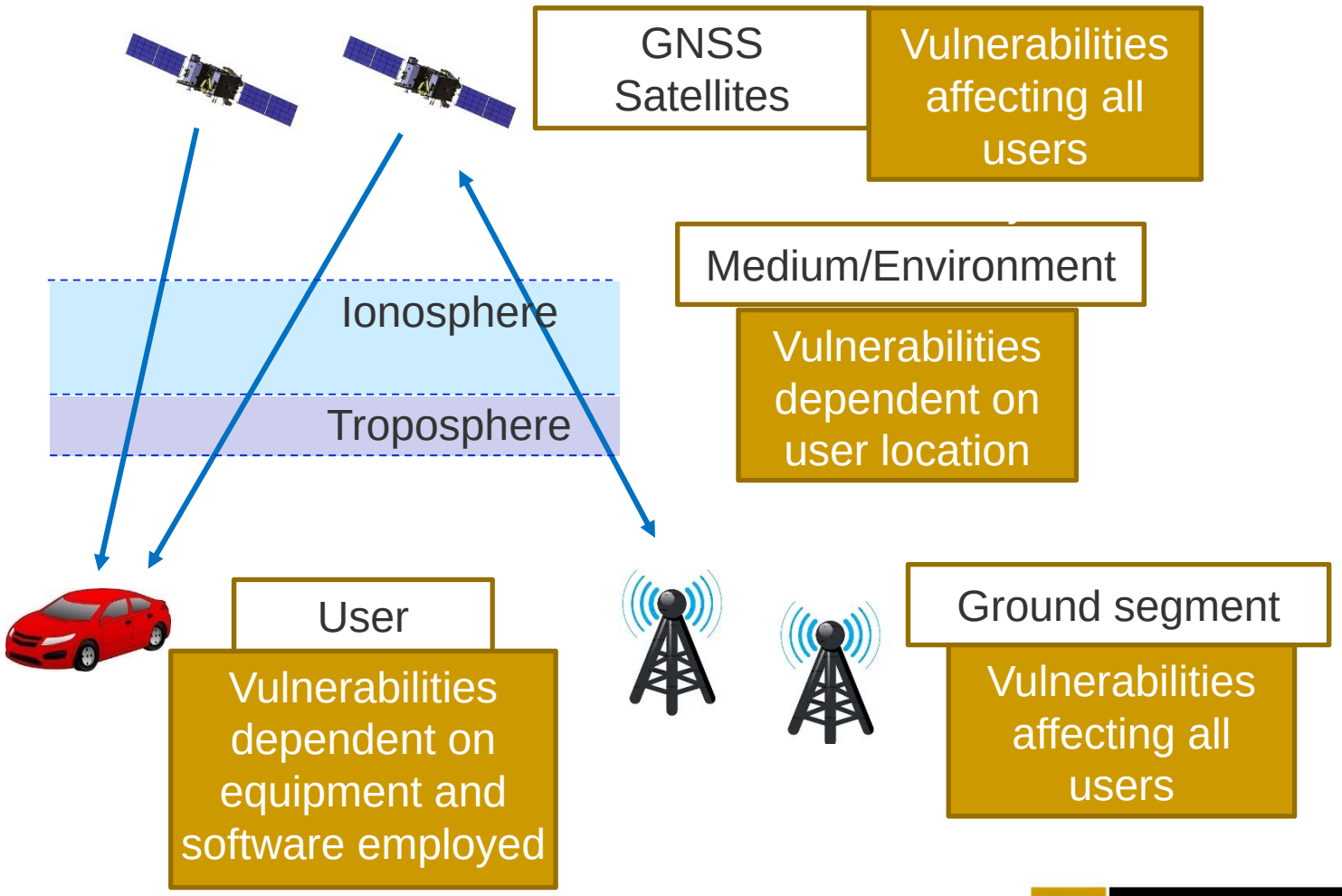


- Current systems mainly use SPS (Standard Positioning Service).
- SPS gives 1-5 m accuracy - not suitable for lane-level precision.
- Foreseen use of **differential** techniques as **SBAS, RTK** and PPP

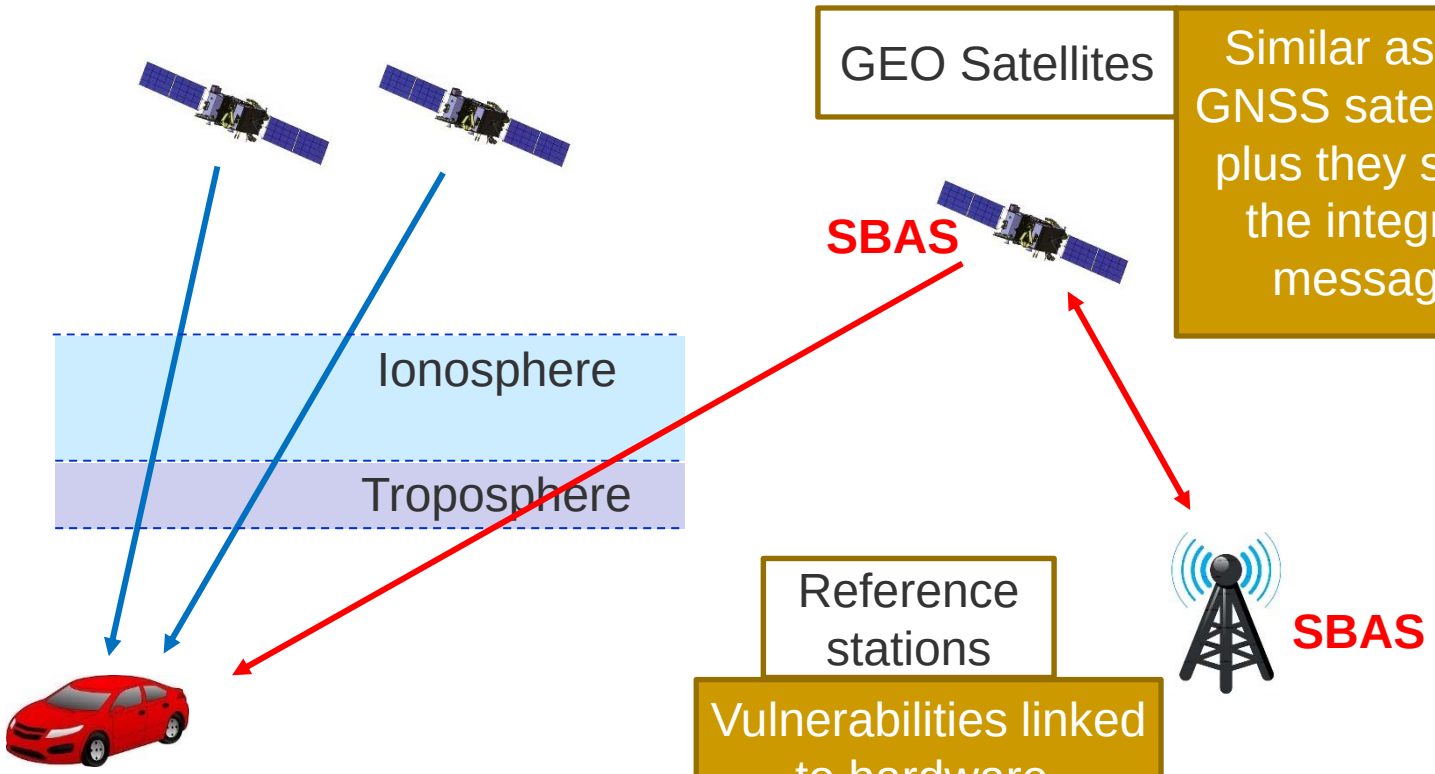
Integrity Monitoring for ITS

- Safety-critical applications → high **integrity** requirements
- Integrity:
  - Ability to **detect** and **identify faults** affecting the systems and provide a trustworthy position
  - warranty of safety
- Integrity monitoring methods:
  - External integrity monitoring: **SBAS, GBAS**
  - Internal integrity monitoring: **RAIM**
- Need to know the **vulnerabilities** of the system: faults, anomalies as well as nominal errors and biases possibly affecting the positioning

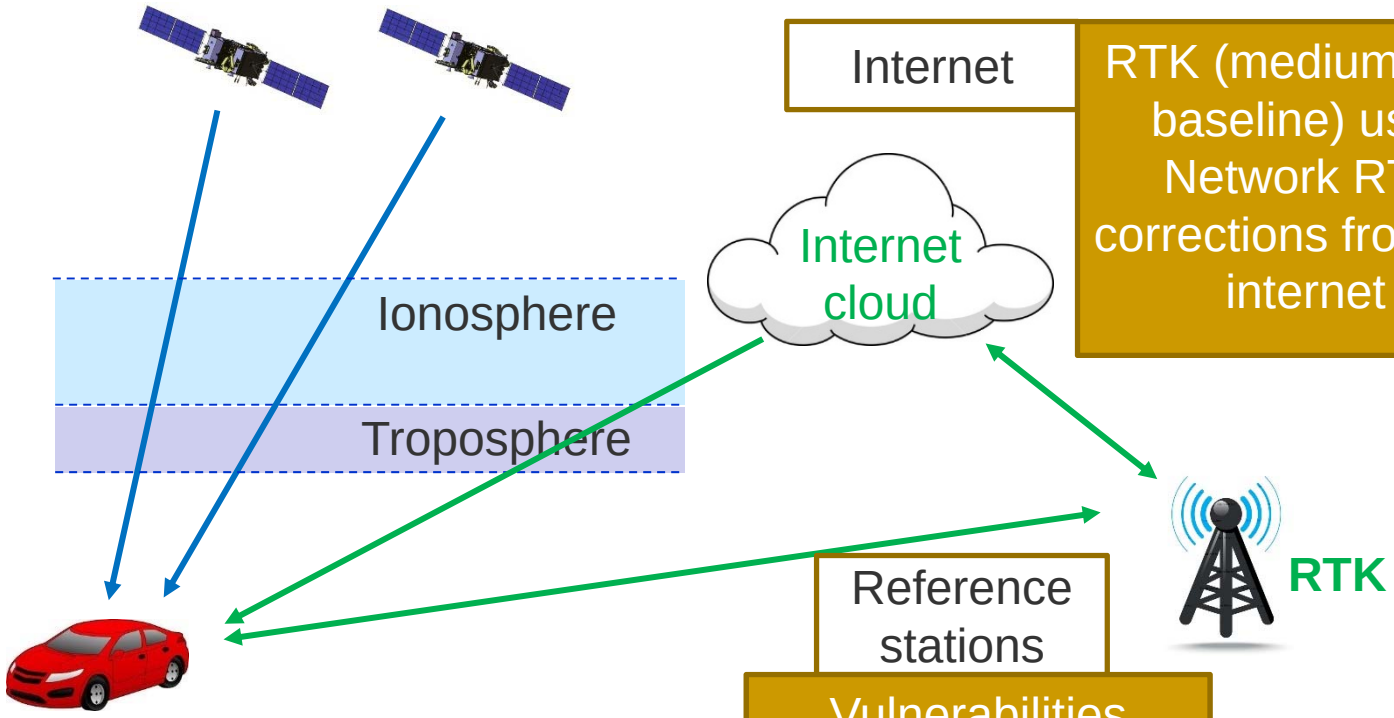
GNSS Vulnerabilities



SBAS



RTK

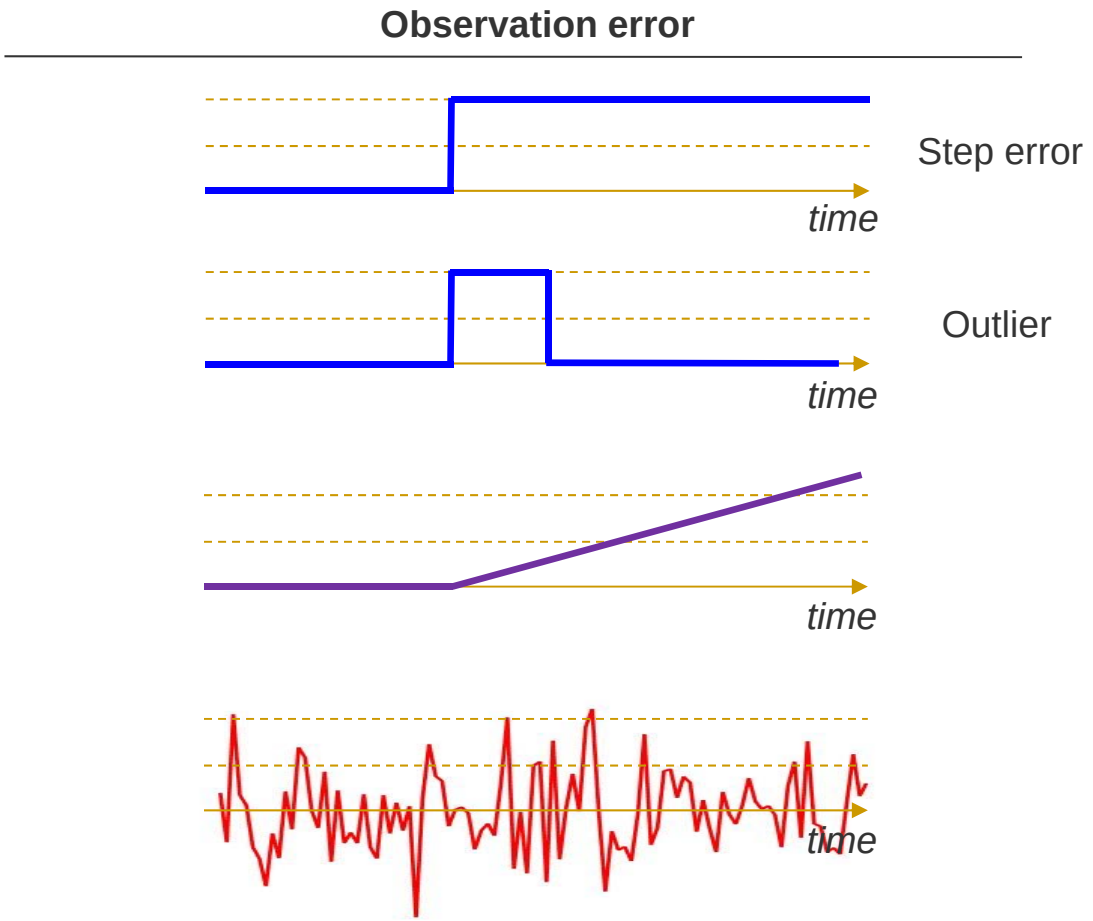


Vulnerabilities classification

GNSS system	Medium/ Environment	User	Overlay service/ Positioning method
Space segment • Satellite clock jump/drift • Signal deformation • Power fluctuations **Ground segment** • Bad ephemeris upload • Attack **Communications**	**Atmosphere** • Ionospheric gradients/storms • Scintillation in ionosphere • Tropospheric storms **Heavy multipath** **NLOS** **Interference** • Unintentional • Intentional: jamming and spoofing	**Receiver** • Leap seconds and roll-overs • System upgrades • Bugs **Antenna**	**SBAS** • GEO satellites • Reference stations • Master stations • Communications **RTK** • Reference stations • Communications • Carrier-phase related: cycle-slips, carrier-phase multipath

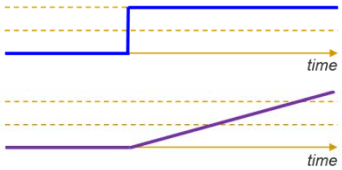
Fault/anomalies models

- Step error/outlier
- Ramp
- Random noise



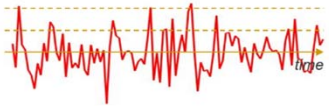
Vulnerabilities - GNSS Space Segment

- Satellites (Space segment)
  - Satellite clock



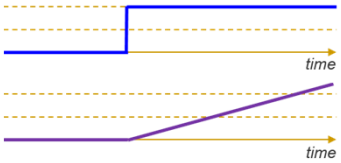
  - Code-carrier signal deformations

  - Power fluctuations



- GPS – Likelihood: ~10^{-5} events/hour (by design, at most 1.43 x 10^{-5})
- Available history of outages for GPS only.
- Range errors up to kms (clock errors)

- Ground
  - Wrong ephemeris upload



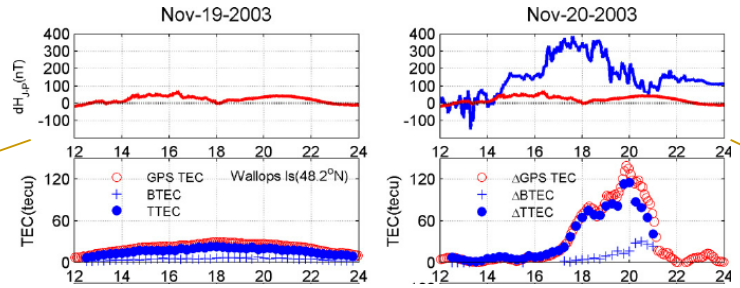
- GPS – Likelihood: <10^{-5} events/hour
- Satellite fault or
- Constellation fault (EOP)

  - Incorrect modelling of Earth Orientation Parameters
  - Manned operations, hardware failure

Likelihood: Very unlikely

Vulnerabilities - Atmosphere

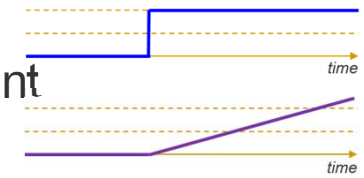
➢ Ionosphere



Quiet day

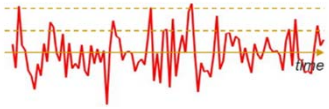
Stormy day

- Spatial/temporal gradient



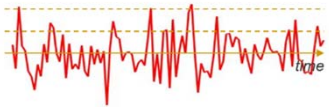
- Dependent on latitudes
- Likelihood of storm (data history): ~10^{-4} events/hour
- First order eliminated with dual-Freq.

- Scintillations



- Occur with ionospheric storms
- Contained range errors
- Risk of loss of locks and cycle-slips

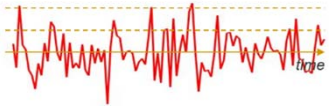
➢ Troposphere



- Usually neglected.
- Gaussian model assures errors overbounding

Vulnerabilities – work environment

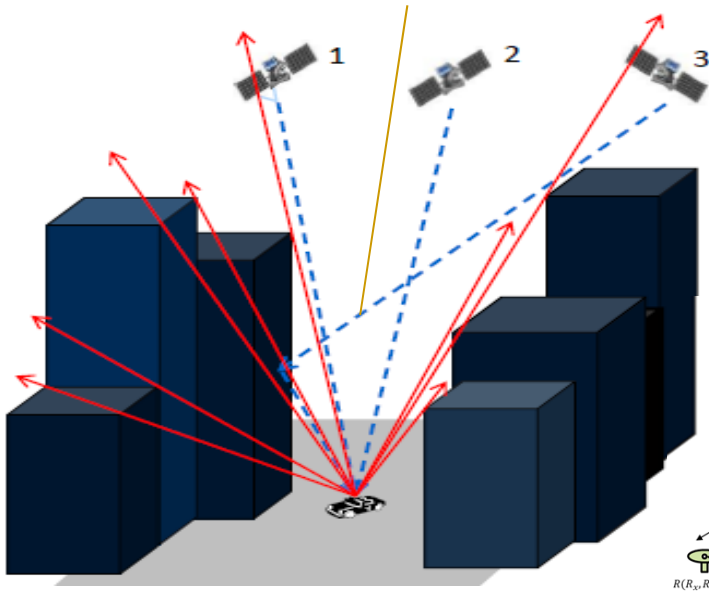
- Multipath and NLOS



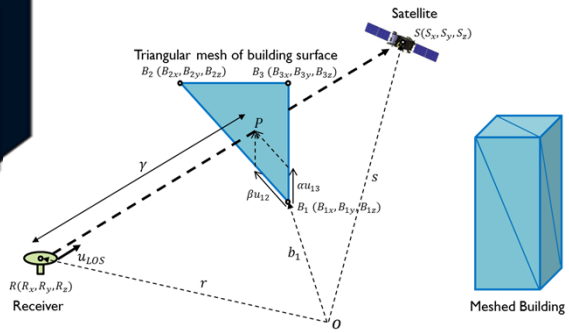
- Main threat in ITS
- high risk in urban areas
- Range errors up to hundreds of meters (NLOS)
- Effect intensified with iono-free combination

Mitigations:

- Multipath mitigation at the antenna
- 3D city-models – ray-tracing algorithms
- SNR monitoring
- Non-Gaussian error models



Example of NLOS



Curtin University

Vulnerabilities - the user

- Receiver

  - Receiver dependent
  - Component replacements/failures
  - Overheating
  - Software bugs
  - Inadequate manned

- Antenna

  - Antenna dependent.
  - Component replacements/failures
  - Overheating
  - Site displacement

Nominal errors

- Antenna biases
- Inter-frequency biases (IFB)

Trimble geodetic receiver

u-blox receiver and antenna

Trimble geodetic antenna

SBAS specific vulnerabilities

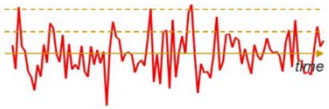
- GEO satellites
  - Same as GNSS satellites +
  - Risk of wrong information uplink (but Integrity message usually very robust)
- Reference stations
  - Same as user: receiver and antenna faults +
  - Nominal errors:
  - Reference station position errors (surveyed position)
- Master stations
  - Errors in data processing
  - Estimation errors for the corrections to be
- Communications
  - Risk of wrong broadcast of range corrections and integrity information.
  - Risk mitigated by using robust data-link messages and redundancy of GEO satellites.

RTK specific vulnerabilities

- Reference stations
- Communications

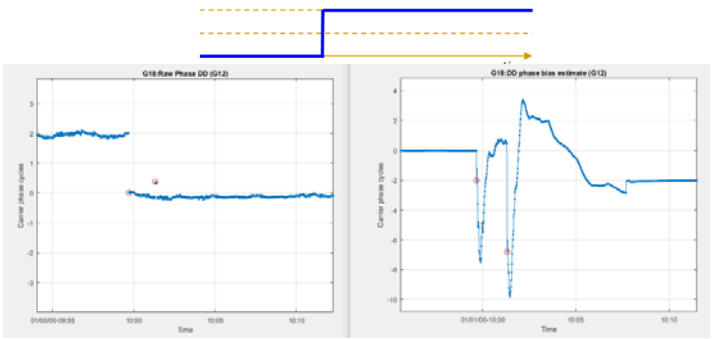
- Same as for SBAS, however
- Precision required is higher: smaller errors/biases have significant impact.
- Standard RTK infrastructure and messages are generally less robust than SBAS.

- Carrier-phase multipath



- Critical in determining the Time to Ambiguity Resolution (TAR).
- Quality of receiver dependent

- Wrong ambiguity /Cycle-slips



- Main RTK-specific threat
- Can cause wrong ambiguity fixing and result in large errors

Mitigation:

- Ad-hoc detection tests
- Use of multi-frequency for powerful tests

Summary Table

Cause	Characteristics	Impact	Model	Likelihood
GNSS system				
Satellite clock jump	Clock misbehaviour that results in an abrupt change in the transmitted signal.	Range error of up to kilometres.	Step error	$\sim 10^{-5}$/hr per satellite
Satellite clock drift	Clock misbehaviour that introduces a slow ramp type error in the transmitted signal.	Range errors can grow gradually to few kilometres.	Ramp error	$\sim 10^{-5}$/hr per satellite
Ephemeris information error	Increases with the time lapse between two consecutive uploads.	Range errors of up to 40 metres (Ochieng et al. 2003).	Step/Ramp error	$\sim 10^{-5}$/hr per satellite
Incorrect modelling of Earth Orientation Parameters (EOP)	Increases with the time lapse between two consecutive uploads.	Constellation-wide fault, positioning error up to hundreds of metres (Perea Diaz et al. 2014).	Step/Ramp error	$< 10^{-5}$/hr per system
Signal deformations	Deformation of signal correlation function.	Range errors of few metres.	Step error / Random noise	$\sim 10^{-5}$/hr per satellite
Low signal power / Power fluctuations	May be due to satellite attitude instability or hardware wear.	Increased random noise (errors of few metres). Could result in loss of lock.	Random noise	$\sim 10^{-5}$/hr per satellite
Code-carrier incoherence	Failure to maintain coherence between broadcast code and carrier (Simili and Pervan 2006). Observed only on GEO satellites and GPS L5 signals.	Range errors up to few metres.	Ramp error	$\sim 10^{-5}$/hr per satellite

Summary

- Vulnerabilities have been categorised on the basis of their source
- Specific vulnerabilities of 2 positioning methods used in ITS – SBAS and RTK – have been identified
- Likelihood of occurrence of most impactful anomalies is under investigation
- Mathematical models for the main vulnerabilities is under investigation (some were suggested)

Thank you

Questions