Imperial College London

GNSS integrity monitoring for the detection and mitigation of interference

Dr. Shaojun Feng

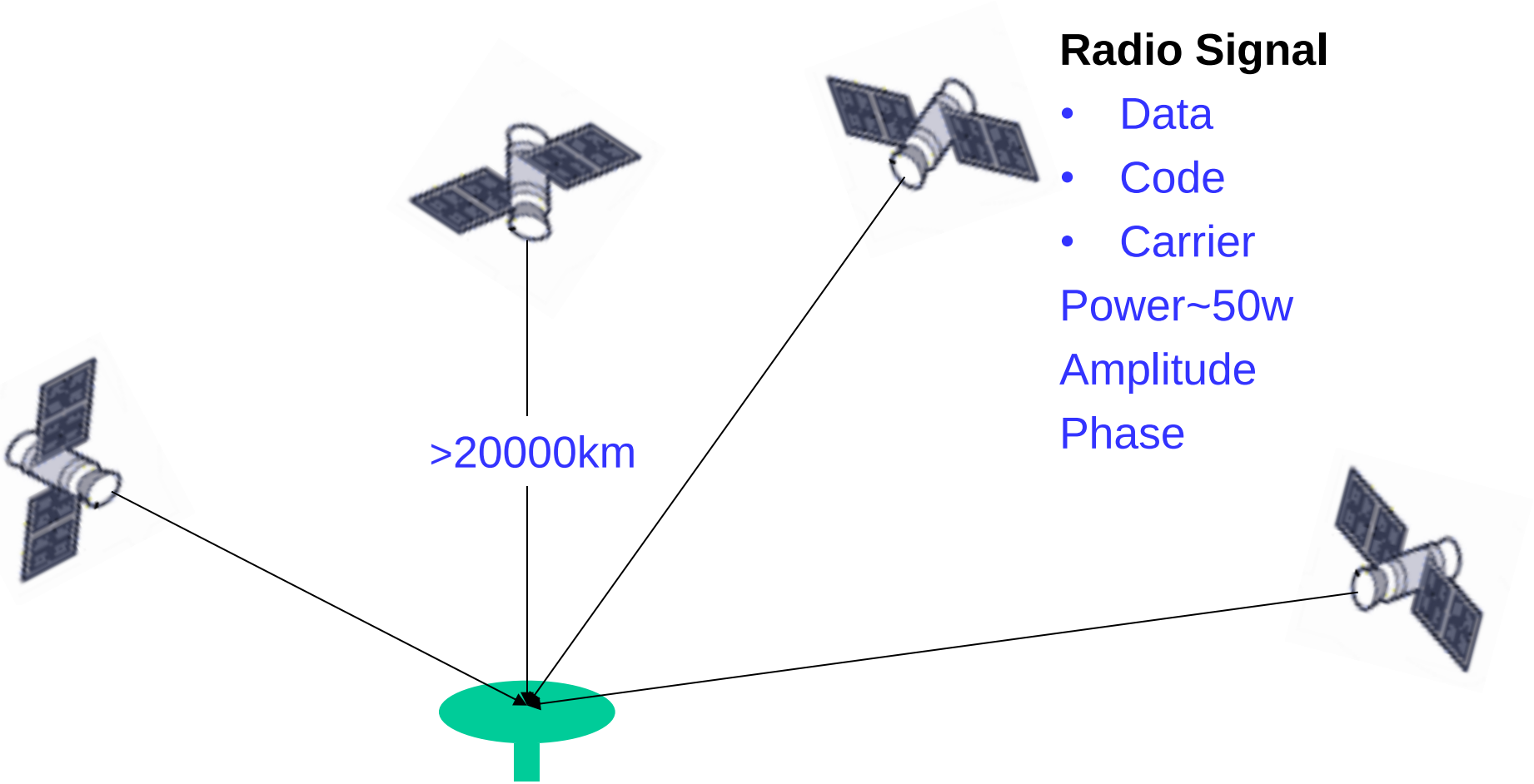
Centre for Transport Studies

Outline

- GNSS vulnerability
- GNSS integrity monitoring
- Cases study
  - GAARDIAN
  - ERAIM
- Conclusions

GNSS Vulnerability

Technical barriers in system design



Radio Signal

- Data
- Code
- Carrier

Power~50w

Amplitude

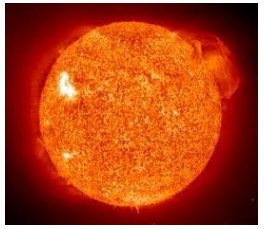
Phase

Power ~ -158dBW

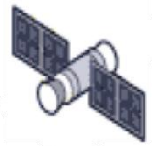
Lower than thermal noise

?

Vulnerability – disturbances



- GNSS signal
  - Amplitude
  - Phase



Power~50w

Orbit Error

Ionopsheric Error

Tropospheric Error

Computed Range (r_C)

Observed Range (r_O)

Multipath Error

Receiver Error

SV Clock Error

RX Clock Error

SV Clock Error

Power~
-158dBW

interference

Vulnerability – Cause interference with GNSS PRN code

- Real signal (Reflected, retransmitted)
  - NLOS signal (lower signal strength)
  - Multipath signal (resulting higher or lower signal strength)
  - Shadowing (lower signal strength)

- Faked signal (e.g. spoofing, Simulator)
  - Signal strength higher or lower than nominal strength

Vulnerability – Cause interference without GNSS PRN code

- Interference frequency
  - Out-band
  - In-band
- Types
  - Narrow-band-limited Gaussian interference
  - Wide-band-limited Gaussian interference
  - Continuous-wave interference
  - Pulsed interference
  - Light-Squared-like interference
- Characteristics
  - Time stationary and time varying
  - Power level

Impact of interference to a GNSS receiver

- Denial of service e.g. jamming
- Degraded performance e.g. outband radio
- Deceived e.g. spoofing

- Clear evidence of threats acknowledged by (e.g.) the
  - Royal Academy of Engineering, UK
  - Volpe National Transportation System Centre, DOT USA
  - Department of Homeland Security, USA

Impact of interference to Critical GNSS applications

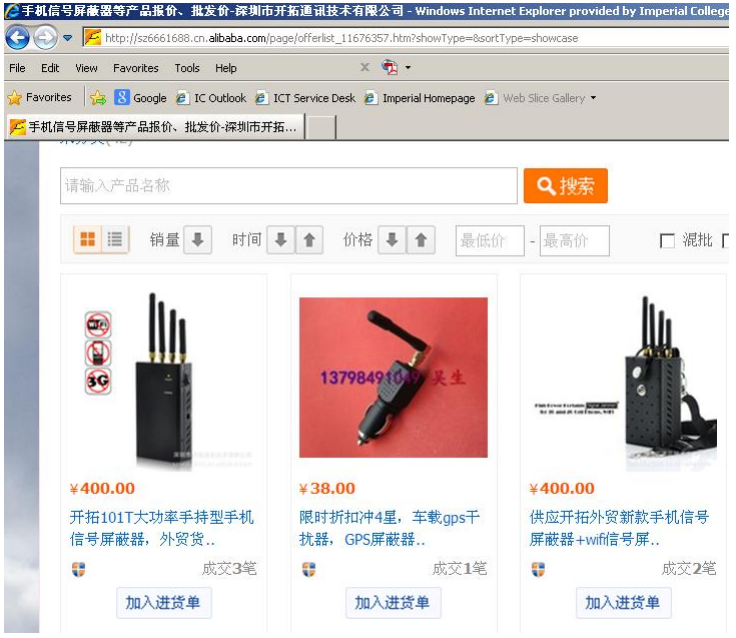
- Safety (e.g. aircraft navigation, emergence service)
- Liability (e.g. GNSS based road charging)
- Security
  - Mobile network synchronization
  - Theft (jamming GNSS based tracking assets)
  - Terrorist (spoofing attack on aircraft)

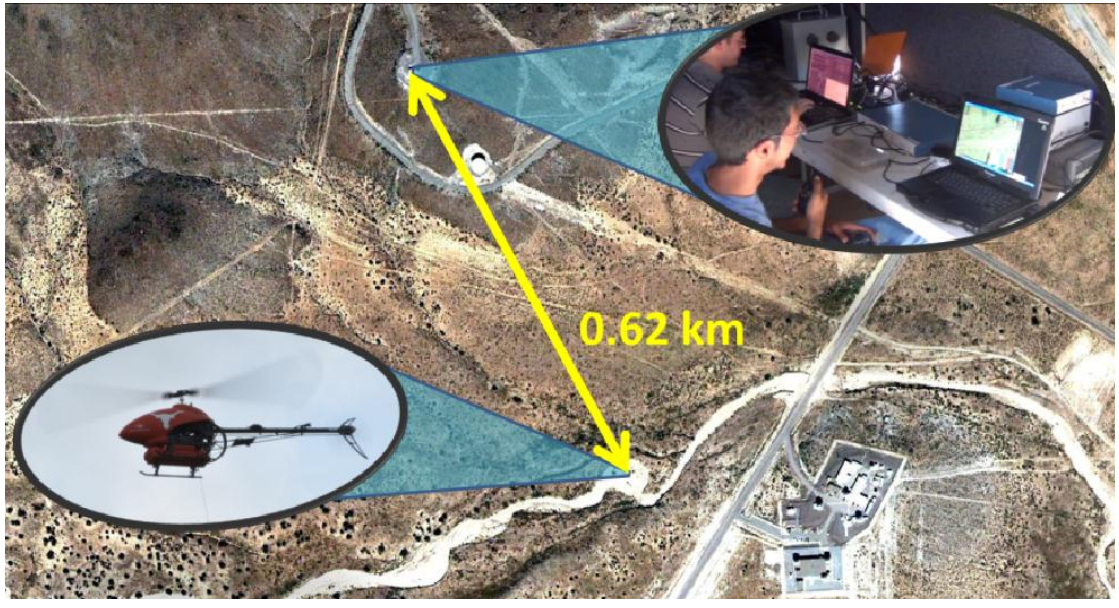
Motivation of jamming and spoofing

- Fun
- Criminal / terrorist
- Commercial
- Privacy protection
- Others

Examples of inteference

- San Diego
  - US Navy ship
- Newark airport
  - $33, 200mW GPS jammer
- University of Texas experiment
  - Performed spoofing attack successfully





Integrity of a navigation system

- Trust navigation system?

- System integrity
  - *trust* placed on the *correctness* of navigation solution- key safety parameter for aviation
  - navigation system required to deliver a warning (*an alarm*) of any malfunction (i.e. *alarm limit* exceeded) to users within a given period of time (*time-to-alarm*) and with a given probability (*1-integrity risk*).

Integrity Monitoring of GNSS

- System level
  - Global
  - Signal-in-Space (SIS)
- Network Level
  - Satellite Based Augmentation System (SBAS)
    - Wide area
    - SIS + Ionosphere
  - Ground Based Augmentation System (GBAS)
    - Local area
    - SIS + Ionosphere + troposphere
- User level
  - Receiver Autonomous Integrity Monitoring
    - User location
    - SIS + Ionosphere + troposphere + multipath
- **All these methods are not designed for interference**

Interference detection and mitigation measures

- Independent monitoring
  - Purposes
    - Situational awareness
    - Law enforcement
  - Set up independent monitoring network
    - New monitoring network
    - Upgrade existing monitoring network
  - Define communication protocol/channels
  - Broadcast to users
- Receiver / User level
  - Signal processing based
  - Solutions based
  - Multiple sensors based

An independent monitoring approach- GAARDIAN

- **G**NSS **A**vailability, **A**ccuracy, **R**eliability an**D** **I**ntegrity **A**ssessment for timing and **N**avigation
  - capture and definition of user requirements for wide-range of applications
  - focus on intelligent integrity monitoring

chronos TECHNOLOGY

UNIVERSITY OF BATH

Imperial College London

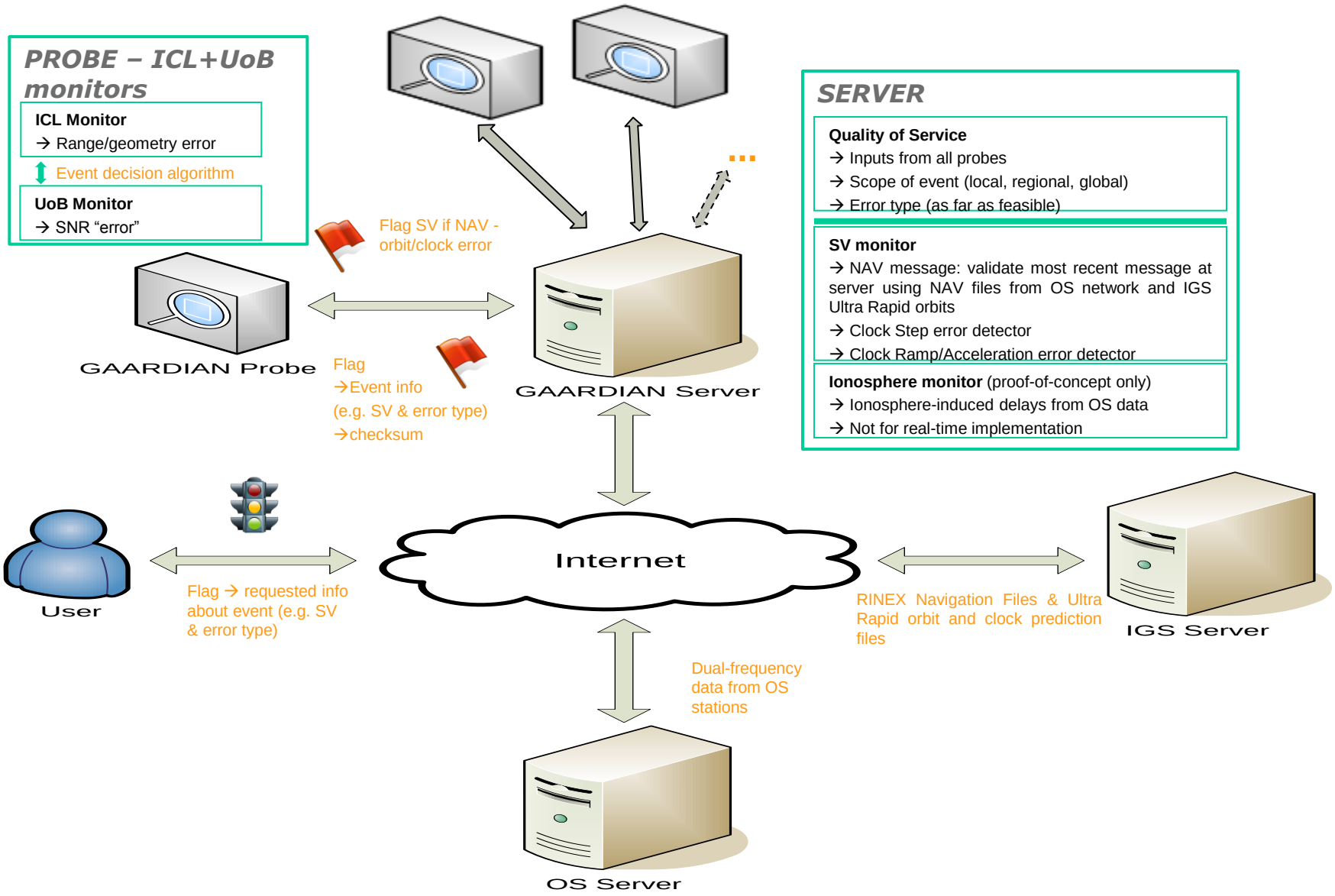
RESEARCH & RADIONAVIGATION
GENERAL LIGHTHOUSE AUTHORITIES
United Kingdom and Ireland

NPL National Physical Laboratory

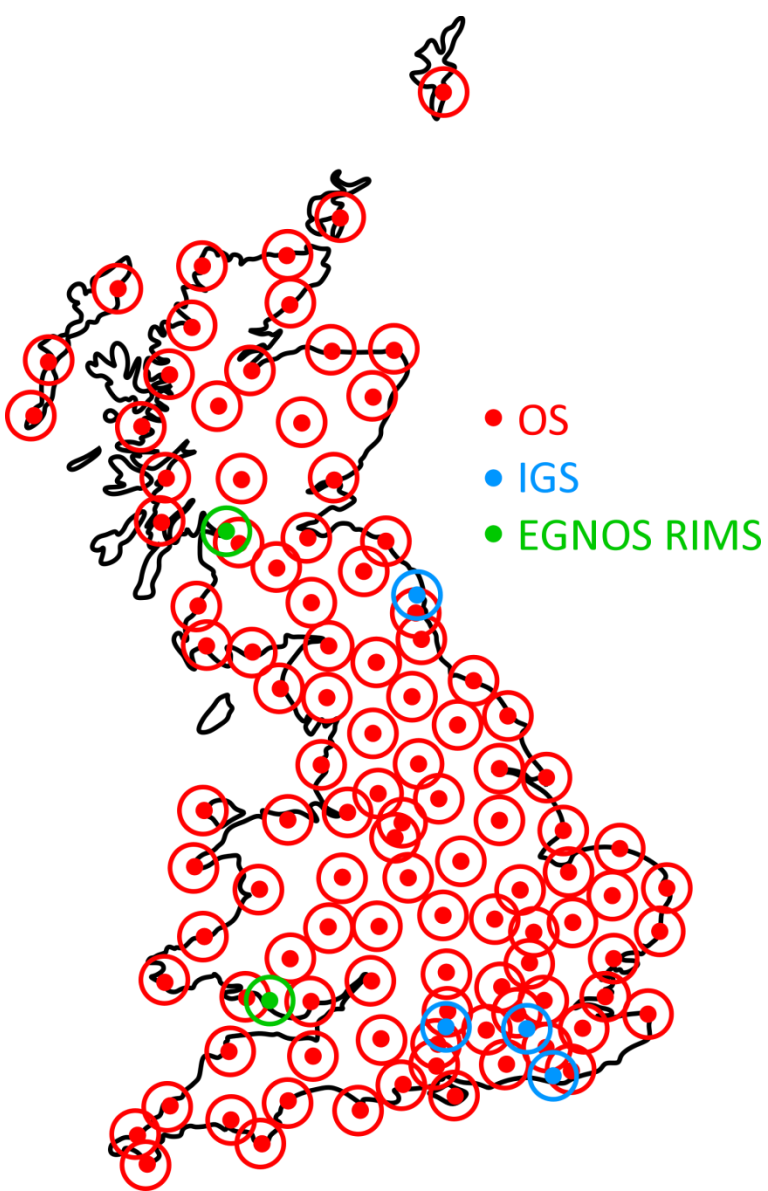
OS Ordnance Survey®

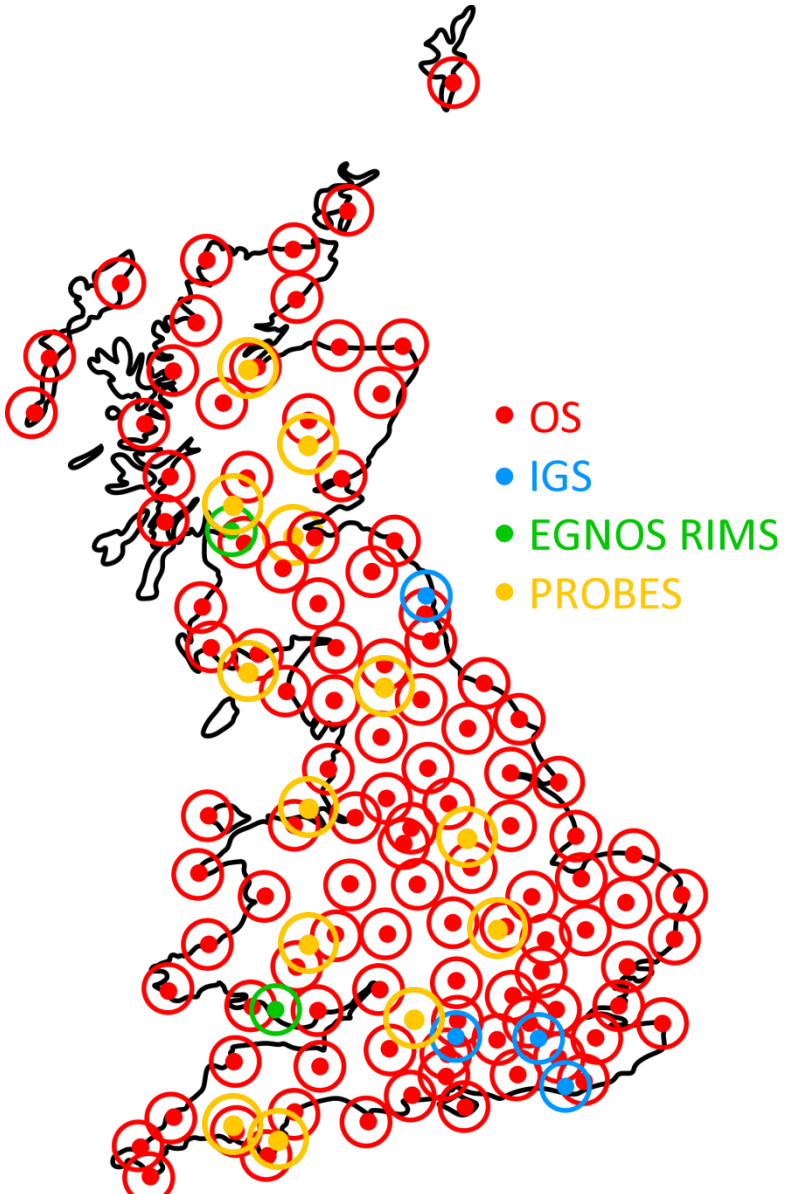
BT

Overall GAARDIAN Architecture



Monitoring network





GAARDIAN Probe

- **Using atomic clock**
- **Placed in a known position**
- **Comparison of computed and surveyed positions**

- **Integrity of ranging signals**
  - flag satellites
  - aid failure identification

- **Output**
  - set of metrics
  - user-configurable thresholds
  - intelligent data reduction
  - enable users to decide whether LBS can be provided for their application

GAARDIAN Server

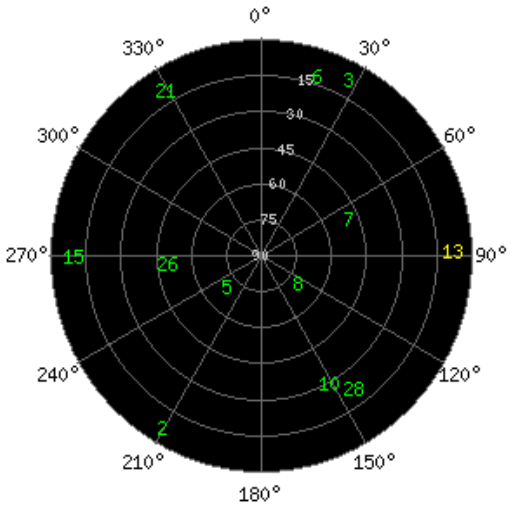
- **Two components:**
  - space-segment health monitor (SSHM)
  - network-domain monitoring (NDM)
- **SSHM inputs from** real-time data from OS stations
  - monitors → early detection of space segment failures (user range errors)
  - metric to detect ramp errors using time differential carrier phase
  - outputs: status of visible satellites
    - » estimated performance
    - » monitoring level
- **NDM inputs from network of probe integrity monitors**
  - qualifies type of failure for each satellite
  - enables users to determine (according to threshold) whether LBS is supported
  - QoS

Example Result

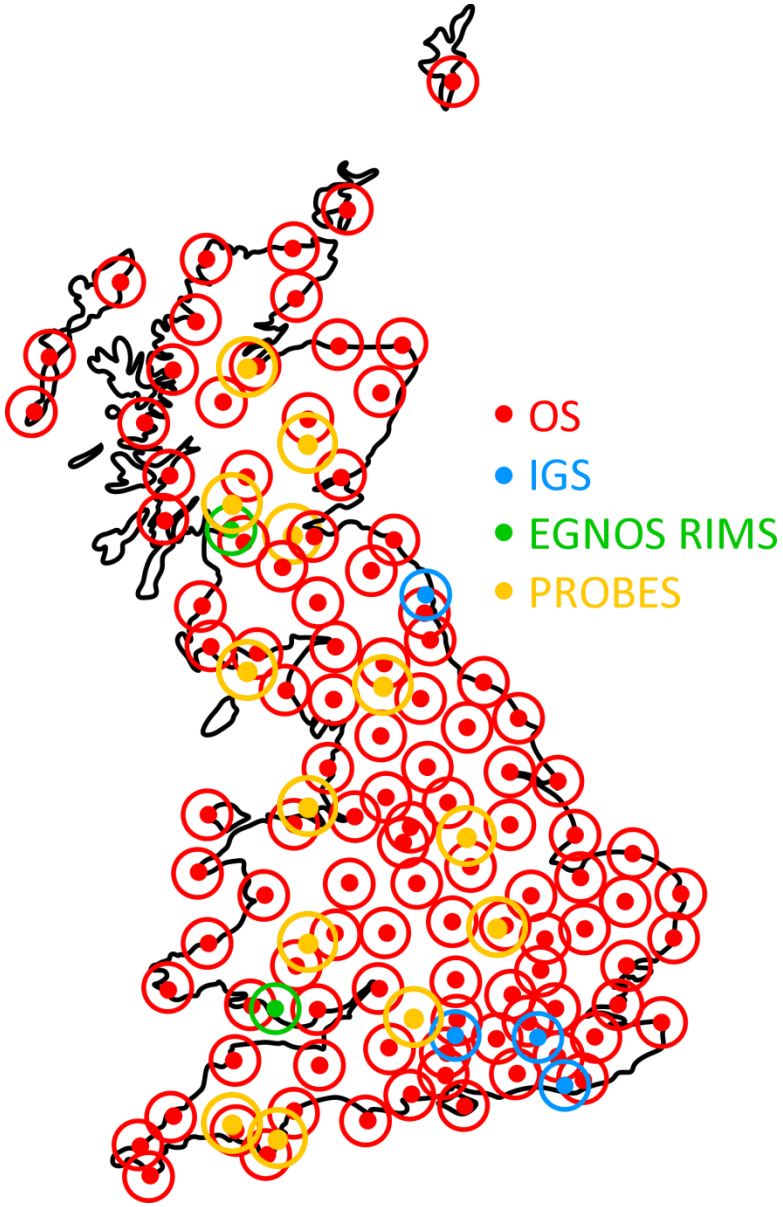
Network detail

ICL | Devices

SV Network Skyplot



PRN	Stations	Worst	URA	Error	Monitor
2	14	SCAO	2.0		
3	5	STOR	2.0		
5	15	BUXT	2.0		
6	6	LERI	2.0		
7	15	FRAE	2.0		
8	15	KINT	2.9		
10	15	KINL	4.0		
13	9	STRA	2.0		
15	15	LERI	2.0		
21	15	DUNG	2.8		
26	15	CAML	2.0		
28	15	GORS	2.0		



A user level monitoring approach- ERAIM

- Receiver Autonomous Integrity Monitoring (RAIM)
  - Based on pseudorange measurement
  - Based on consistency check
  - One failure assumption

- Conventional RAIM
  - Achieved a certain level of success e.g. NPA
  - Incapable in the presence of interference
    - multiple failures
    - consistent multiple failures (e.g. spoofing)

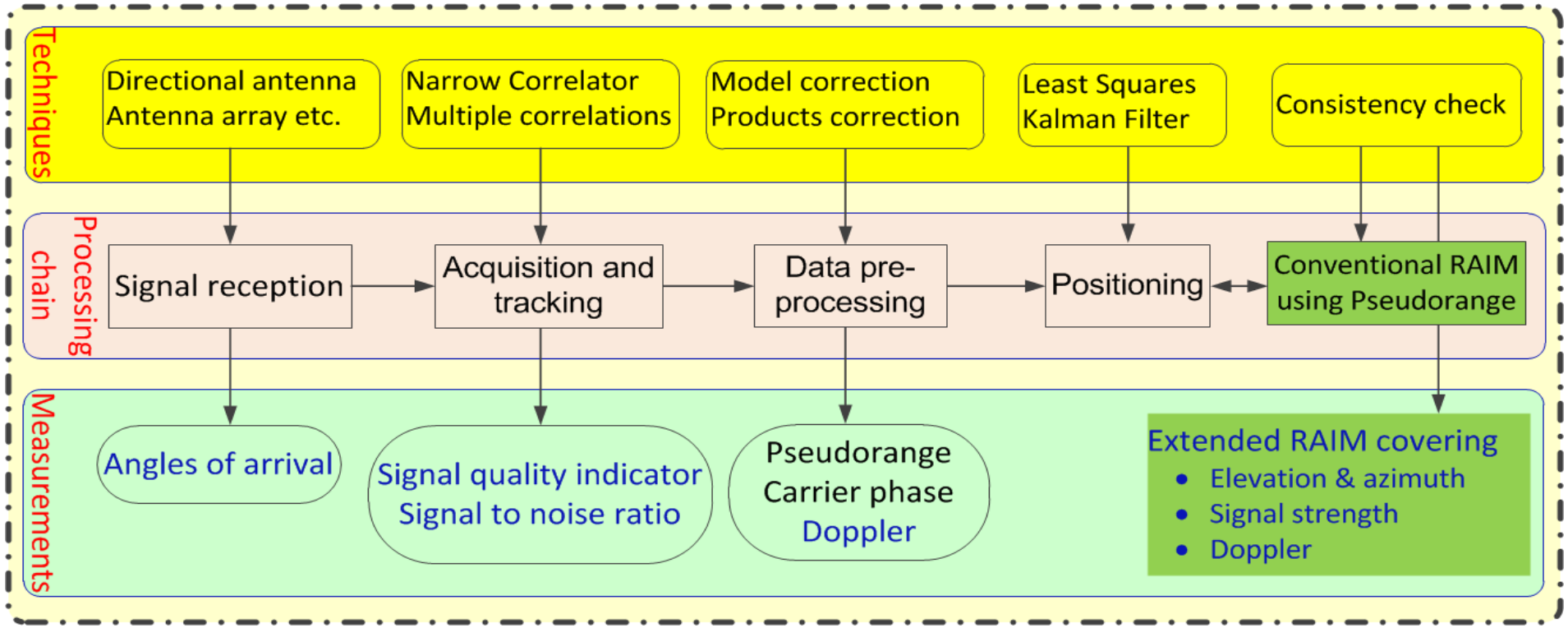
Matrix of spoofer characteristics

A. Signal retransmission
B. Signal record and playback
C. General signal generator
D. GNSS signal simulator
E. Modified pesudolite
F. Dedicated spoofer

I. Height of transmitter antenna
II. Sparse distribution of transmitter
III. Distance between transmitter and receiver
IV. Synchronization with real signal
V. Knowledge of targeted receiver
VI. Multiple PRNs
VII. Attack scheme

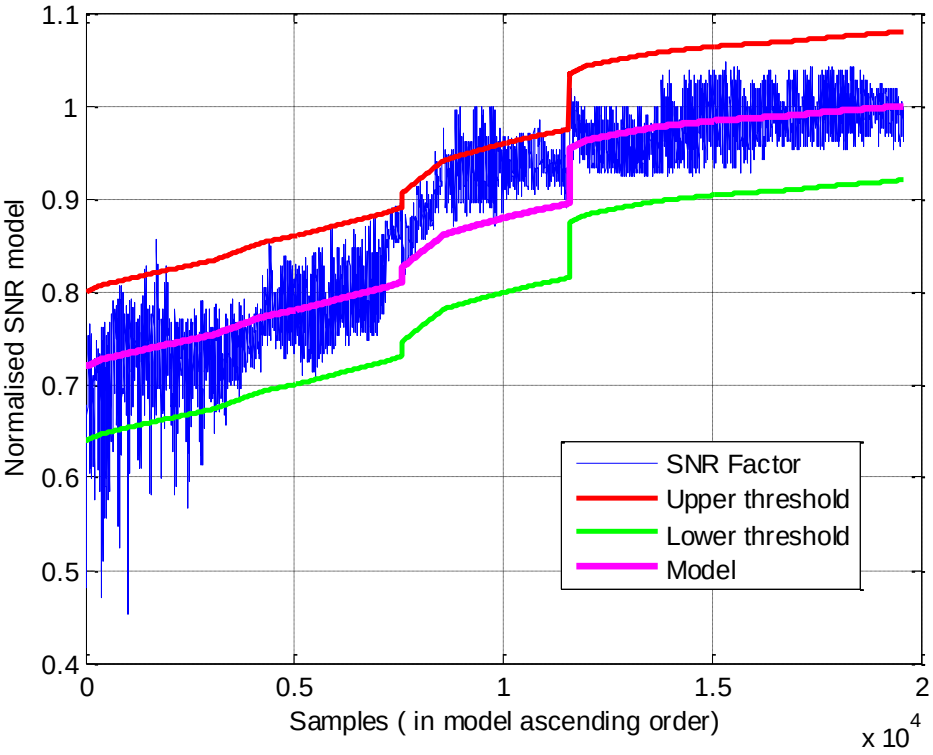
	A	B	C	D	E	F	Real
I	Low	Low	Low	Low	Low	Low	High
II	No	No	No	No	Possible	Possible	Yes
III	Short	Short	Short	Short	Short	Short	Long
IV	Almost	No	No	No	Yes	Yes	NA
V	No	No	No	location	No	location	No
VI	Yes	Yes	Yes	Yes	Possible	Yes	Yes
VII	Stronger signal	Stronger signal	Stronger signal	Jamming before spoofing	Stronger signal	Hide, fool and attack	NA

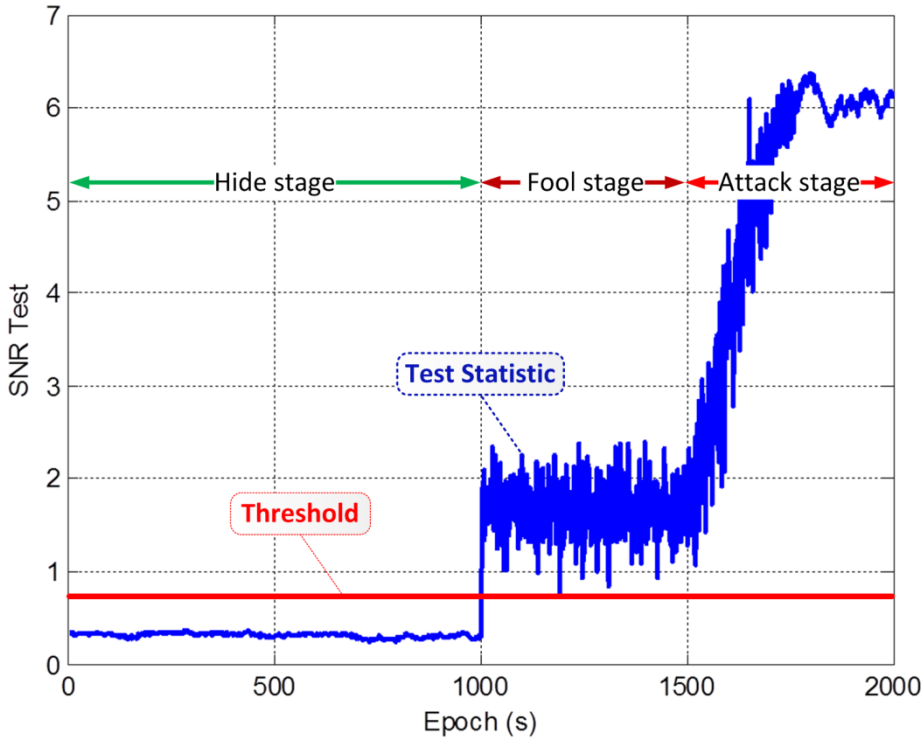
Extended RAIM (ERAIM)



Example Results

The hide-fool-attack scheme is taken as an example for testing. The signal strengths of theoretical and measured are used to generate a SNR model and factor respectively (Fig. left). It is therefore used to detect potential spoofing (Fig. right).





Conclusions

- GNSS is vulnerable
- There are challenges in the detection and mitigation of interference
- Integrity monitoring targeting interference at both network and user level are necessary
- GAARDIAN
  - Architecture implemented shown to be successful
  - Offline testing successfully show GAARDIAN performs as required

- ERAIM
  - The spoofing can not be perfect
  - RAIM needs to be extended to include angle of arrival, signal strength and Doppler measurements.
  - ERAIM can effectively detect most malicious interference spoofing.

Thank you for your attention

More information

http://www3.imperial.ac.uk/geomatics