UNSW SYDNEY | Australia's Global University

Australian Centre for Space Engineering Research (ACSER)

Use of GNSS Data as Evidence

Presented by

Prof Andrew Dempster

ACSER
Australian Centre for Space Engineering Research

SNAP Lab

Sources

Andrew Dempster, “Use of GPS Data as Evidence in Court”, Proc IGNSS 2018, Sydney 7-9 Feb 2018

Andrew G Dempster “GNSS Data as Court Evidence: Lessons from Remote Sensing”, Proc ION-GNSS+, Miami, 26-28 Sep 2018

Andrew Dempster, Allison Keally, Gary Edmond, “Questions for Providers of Expert Opinion on Logged GNSS Evidence”, in preparation (abstract submitted to ION ITM, Reston, VA, Jan 2019)

Legal Concerns

Early days: liability

- "Space Law treaties cannot solve liability questions about the failure of a GNSS signal"
- ICAO has tried to create a treaty re GNSS liability: not yet
- Galileo used SA as a lever
- (ubiquity ➔ liable when GNSS not used..)

Legal Concerns

Specifically to do with GPS “errors”:

- Police forcing entry to the wrong home
- Repossession of wrong house
- Demolition of wrong house

Recent study (83 cases)

K J Berman, W B Glisson & L M Glisson, “Investigating the Impact of Global Positioning System Evidence”, 48th Hawaii International Conference on System Sciences, pp5234- 5243, 2015

- 19 criminal/ 11 civil classifications
- weight given to GNSS data “high” (8%) or “medium” (54%)
- Significant majority “admissible”

UNSW UG Solange Cunin Thesis – update for Aus

- What questions are asked in the cases?

Our Issue: Quality

"the prosecution service needs to examine the GPS evidence thoroughly and must present other supporting evidence for GPS evidence to be admissible evidence in court"

Ishwar Khadka, "The accuracy of location services and the potential impact on the admissibility of GPS based evidence in court cases", BSc(Hons) thesis, University of Derby, 2015

Aims

Provide guidance for expert witnesses giving opinions on GNSS data

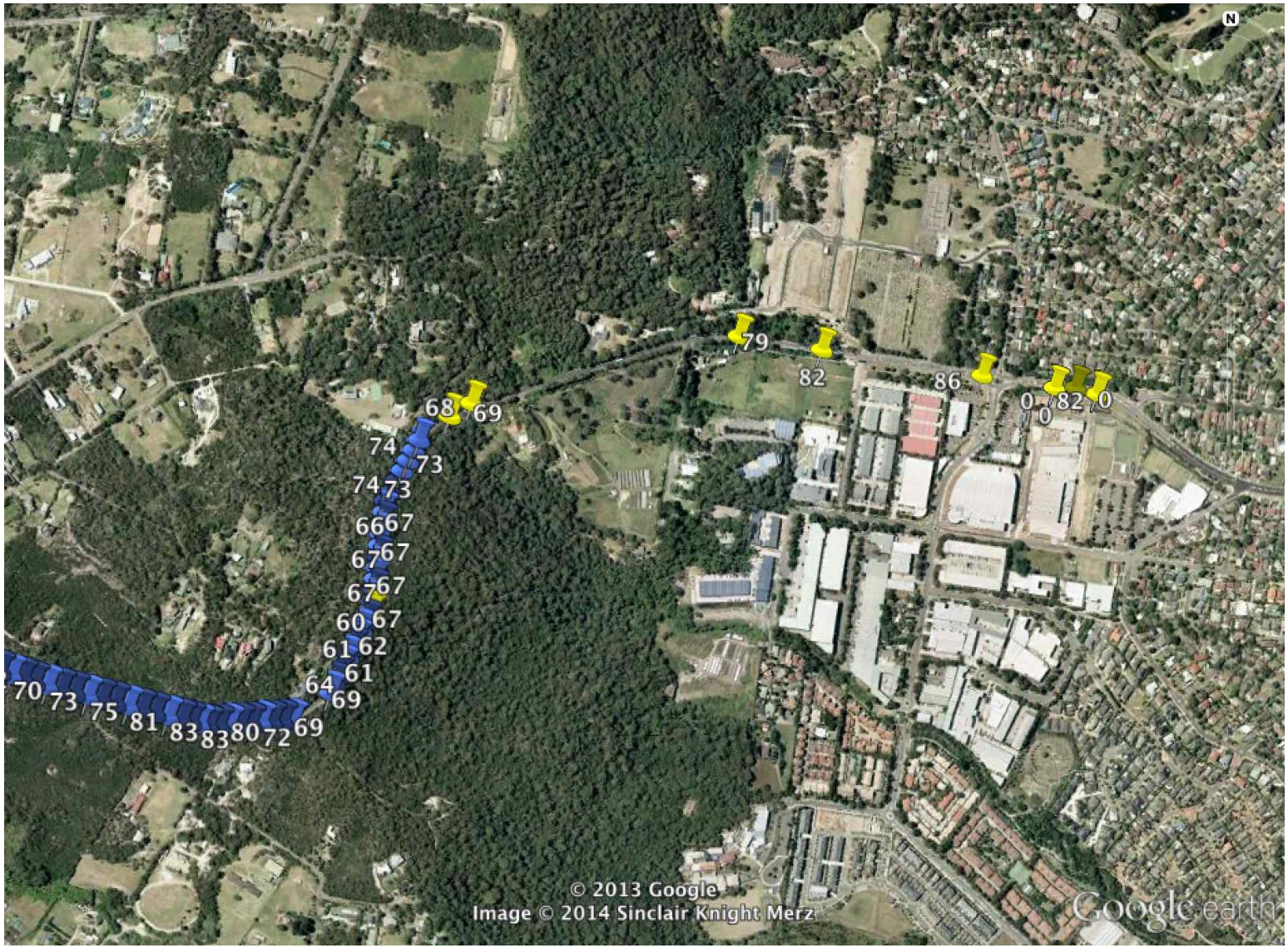
Recommend a standard for GNSS data logging

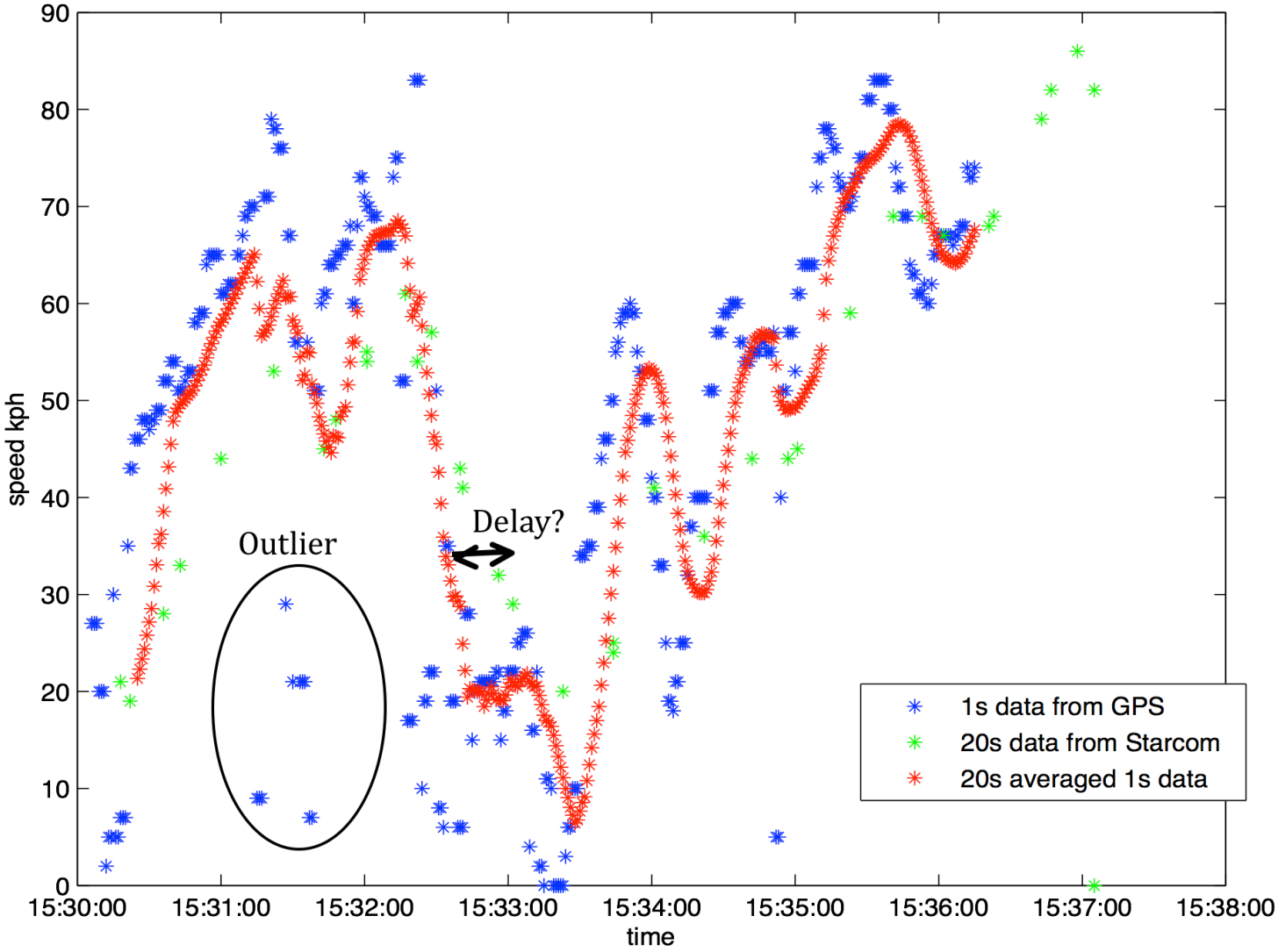
Motivating Example

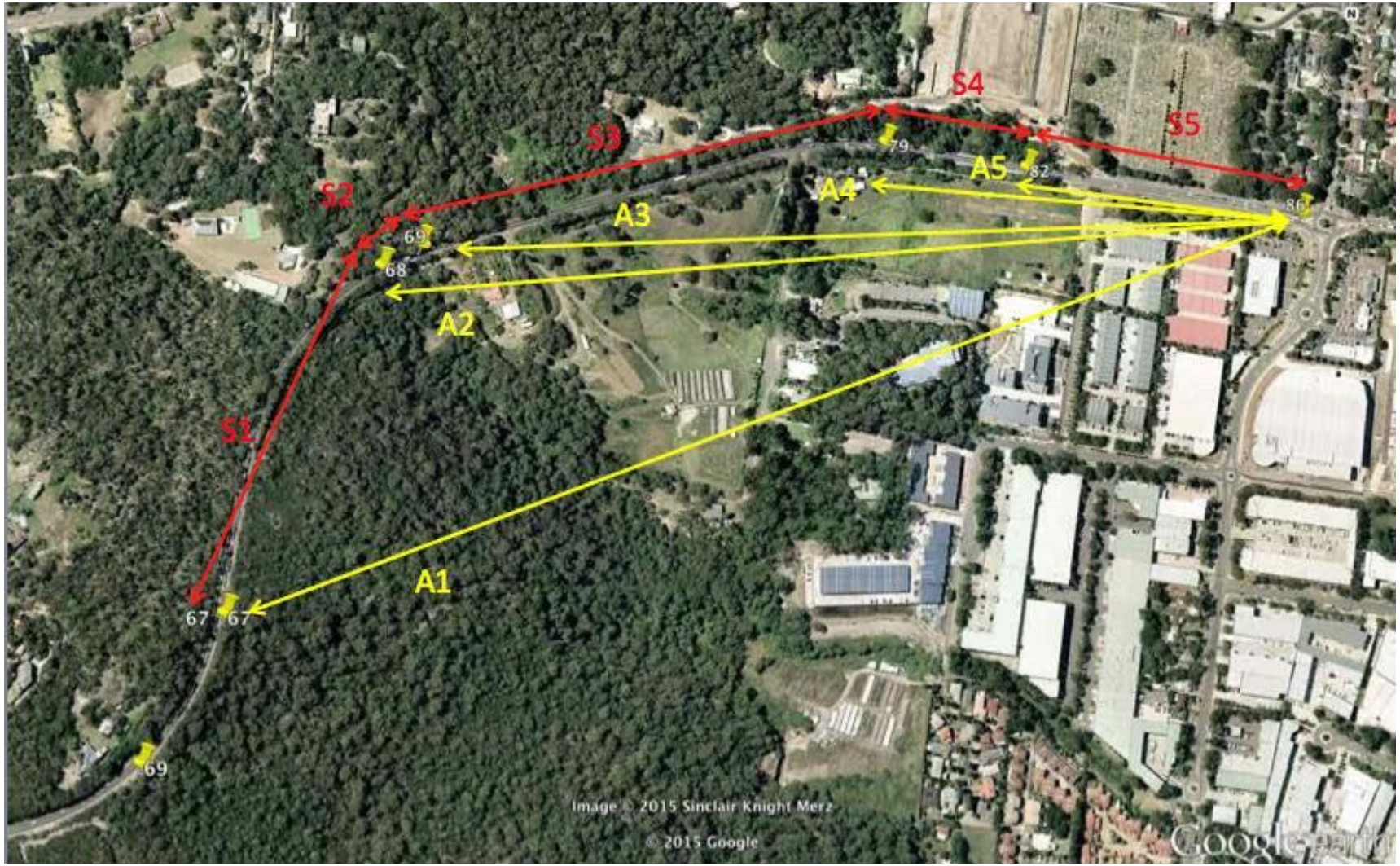
The Queen v Shane Anthony Day, 2014/00075246, NSW District Court

Mona Vale Road – dangerous driving causing death

Was the driver speeding?


N
79
82
86
0
82
0
0
68
69
74
73
74
73
66
67
67
67
67
67
60
67
61
62
61
64
69
70
73
75
81
83
83
80
72
69
© 2013 Google
Image © 2014 Sinclair Knight Merz
Google earth


90
80
70
60
50
40
30
20
10
0
speed kph
15:30:00
15:31:00
15:32:00
15:33:00
15:34:00
15:35:00
15:36:00
15:37:00
15:38:00
time
Outlier
Delay?
1s data from GPS
20s data from Starcom
20s averaged 1s data


S1
S2
S3
S4
S5
A1
A2
A3
A4
A5
67
67
68
69
69
79
82
86
Image © 2015 Sinclair Knight Merz
© 2015 Google

Sector	Length (m)	Speed (kph)
S1	358	72
S2	43	78
S3	482	87
S4	150	108
S5	292	96
A1	1148	74
A2	944	89
A3	905	90
A4	442	100
A5	292	96

What to Learn From This Case Study?

The main questions:

- can you trust GNSS data?
- if not, what would make you trust it?

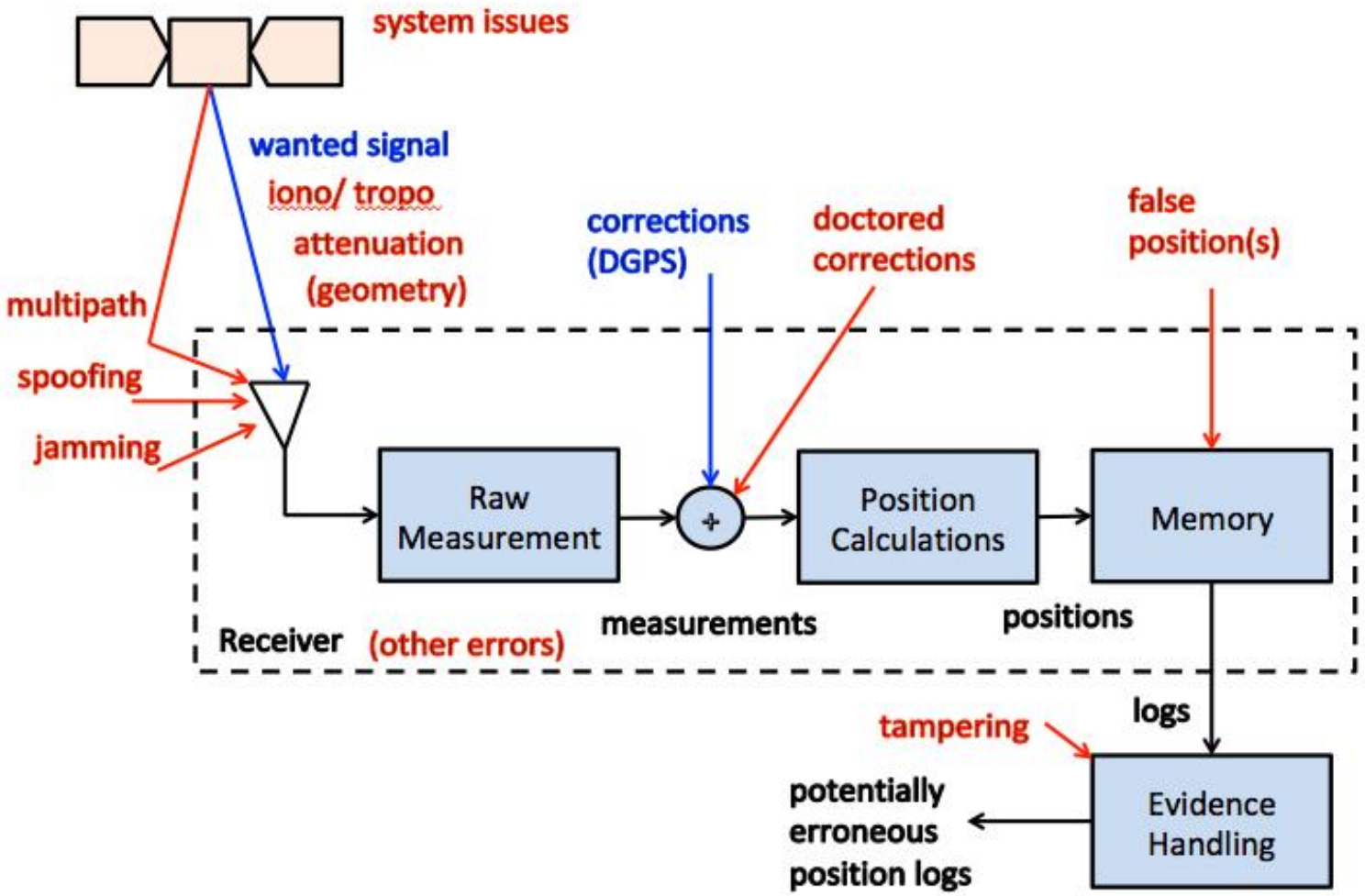
Questions

Different questions for the receiver and the expert witness

Examples	Questions for GPS Receiver	Questions for Expert Witness
Case Study 1 [2]	How fast was the vehicle going?	How fast was the vehicle going? Was it exceeding the speed limit? How valid is the GPS data?
Case Study 2 [2]	Where was the user?	How accurate was GPS at that time and place?
Both examples in [7]	How fast was the vehicle going?	Did the vehicle exceed the speed limit?

Table 1 Different questions asked of GNSS receivers and relevant expert witness in case studies in [2] [7]

Sources of Problems: GNSS



"how accurate was GPS at that time and place?" breaks down into :

1. Was the GPS system operating correctly at that time?
2. Was the ionosphere (and troposphere) behaving itself at that time? If not, was the receiver affected?
3. Was the receiver in a multipath environment? If so, was the receiver affected?
4. Were any of the satellite signals attenuated (e.g. by trees)? If so, was the position calculation affected?
5. Was the receiver jammed or spoofed?
6. Did the position calculation use satellites that had good geometry?
7. Was the position calculation done correctly?
8. Were the data recorded/ communicated/ logged correctly?
9. Was any extra data calculated and/or recorded that gives an indication of accuracy?
10. Were other inputs (other sensors, GPS corrections) used in the position calculation and was this process done correctly?
11. Was the data extracted and presented as evidence without being modified?

"Digital Forensics"

Daubert standard

[US] Used by trial judge to assess validity of expert witness's evidence

Factors

- Has technique in question been tested
- Has it been subjected to peer review/publication?
- Known potential error rate?
- Standards controlling of operation?
- Acceptance within relevant scientific community?

Legal Encyclopedia, Cornell Law School, law.cornell.edu/wex

Digital Forensics

"Criterion 1: Meaning. Has the meaning and, therefore, the interpretation of the electronic evidence been unaffected by the digital forensic process?

Criterion 2: Errors. Have all errors been reasonably identified and satisfactorily explained so as to remove any doubt over the reliability of the evidence?

Criterion 3: Transparency. Is the digital forensic process capable of being independently examined and verified in its entirety?

Criterion 4: Experience. Has the digital forensic analysis been undertaken by an individual with sufficient and relevant experience?"

Indrajit Ray and Sujeet Shenoi (eds), "Advances in Digital Forensics IV", International Federation for Information Processing, Springer, New York, 2008, p30

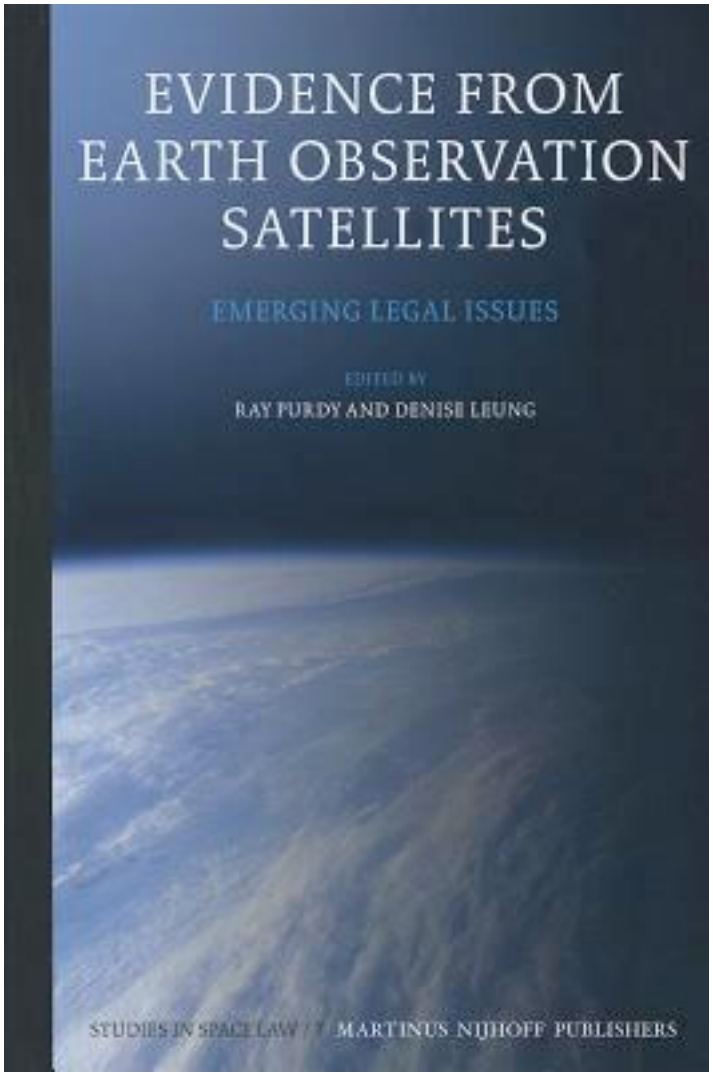
Example: Securing Evidence

"Systems which are powered on (running) need to be handled with care, as there is the potential to make unwanted changes to the evidence if these are not dealt with correctly. Such systems should only be accessed by appropriately trained officers…

1. Secure and take control of the area containing the equipment. Do not allow others to interact with the equipment;
2. Photograph the device in situ, or note where it was found, and record the status of the device and any on-screen information;
3. If the device is switched on, power it off. It is important to isolate the device from receiving signals from a network to avoid changes being made to the data it contains. For example, it is possible to wipe certain devices remotely and powering the device off will prevent this.
4. Seize cables, chargers, packaging, manuals, phone bills etc. as these may assist the enquiry and minimise the delays in any examination;
5. Packaging materials and associated paperwork may be a good source of PIN/PUK details;
6. Be aware that some mobile phone handsets may have automatic housekeeping functions, which clear data after a number of days. For example, some Symbian phones start clearing call/event logs after 30 days, or any other user defined period. Submit items for examination as soon as possible."

Association of Chief Police Officers (UK), "ACPO Good Practice Guide for Digital Evidence", version 5, *March 2012* p33

Lessons from Remote Sensing



Lessons from Remote Sensing

Scientific, technology and policy context

EO: UN principles guide behaviour and uses of EO data ➔ GNSS has ICG mission and vision statements ?

“states have the right to launch and operate EO satellites designed to capture environmental data and those states that are sensed have the right to access the data thereby collected”

EO nation state v nation state; GNSS sensed (i.e. positioned) party an individual, right to sensed data a more local (national, regional) jurisdiction.

Use of GNSS data

EO data must be authenticated:

"Evidence is authenticated when testimony establishes that it is real and that it is, or depicts, that which it is purported to be. Federal Rule of Evidence 901 deals with authentication generally, and it requires that a "condition precedent to admissibility" is evidence "that the matter in question is what its proponent claims."[31] Evidence that must be authenticated before it may be admitted includes writings, tangible objects such as guns, and photographs.[32]

…

[31] Federal Rule of Evidence 902 provides that certain classes of documents are "self-authenticating" and require no further evidence of their authenticity for admission, although there may be other limitations such as relevance. Certain public documents under seal, certified public records, and newspapers fall within the class of self-authenticating documents.

[32] The same approach is taken for sound recordings. If a witness testifies that a relevant recording is an accurate reproduction of what he or she heard, it generally will be admitted."

"A similar approach to authenticate images taken by automated or remotely operated photographic processes has become more accepted. It commonly is called the "silent witness" theory, because there is no live witness to the events captured. Verification of such photographic evidence depends not on a person able to testify that they saw what was captured on film, but on the reliability of the process involved in creating the film. … courts often will be more comfortable with satellite information that has been verified in some manner. Observations by witnesses, photographs, or other evidence, known as 'ground-truthing,' may be an additional method to not only authenticate the remote satellite imagery, but also provide the court with more familiar forms of evidence that may tend to corroborate the satellite information and make admission more likely"

Use of GNSS Data

GNSS “self-authentication” – integrity

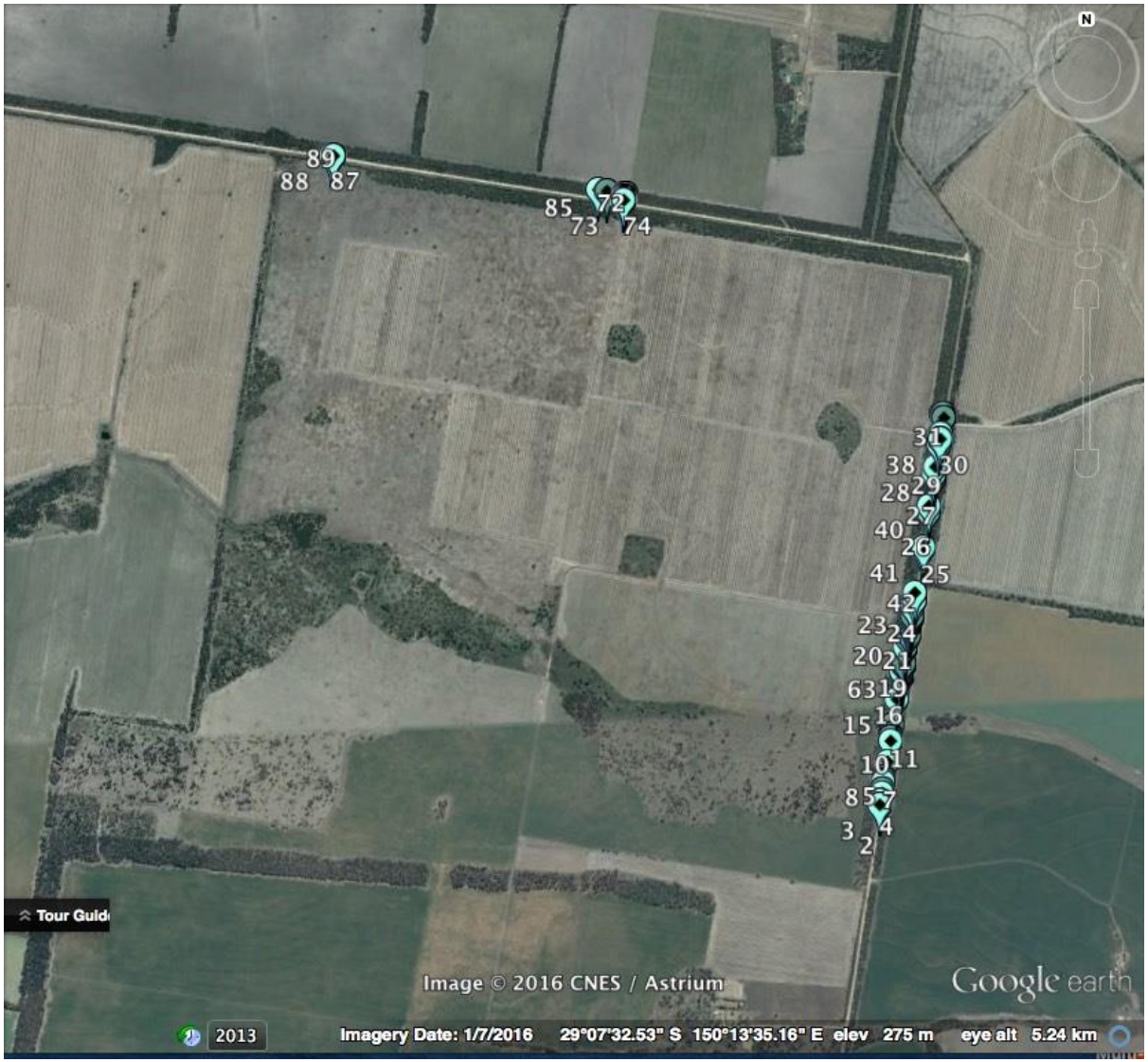
GNSS expert witnesses must educate court :“it is the judge’s responsibility to see to it that the expert’s testimony rests on a reliable foundation and is relevant”

Admissibility of GNSS evidence: future work (different jurisdictions treat it differently, e.g. a “document” or not [16].)

Simple “Authentication” Example

The Queen v Ian Robert Turnbull, 2014/00223920, NSW Supreme Court.

Question: is the GPS accurate?


N
89
88
87
85
72
73
74
31
38
30
28
29
27
40
26
41
25
42
23
24
20
21
63
19
15
16
10
11
8
5
7
3
4
2
Tour Guid
Image © 2016 CNES / Astrium
Google earth
2013
Imagery Date: 1/7/2016 29°07'32.53" S 150°13'35.16" E elev 275 m eye alt 5.24 km


N
24
42
23
43
22
44
21
Tour Guide
Image © 2016 CNES / Astrium
Google earth
2013
Imagery Date: 1/7/2016 29°07'48.43" S 150°14'31.35" E elev 285 m eye alt 467 m

Privacy and copyright impacts

Privacy and copyright concerns quite different for EO and GNSS.

Privacy more of an issue for GNSS: personal, ubiquitous (recorded, often without user knowledge), and often made available to purchasers (without the knowledge, and with only dubious consent, of the user).

Copyright less of an issue: EO data product expensive, protected by copyright/ GNSS often not considered a “document”.

GNSS data in the courtroom

(Authentication again)

Trust in and transparency of GNSS data

EO evidence can be obscured (e.g. by clouds), have trouble being recorded by the camera (e.g. by single event upsets due to radiation in space) or timing of the image.

Demonstrating evidential weight: creation, transmission and storage. Creation quite different for GNSS

EO imagery governed by, not true for GNSS

Trust in the EO data: digital signatures and time stamps (GNSS logged data?)

Lessons (for EO community)

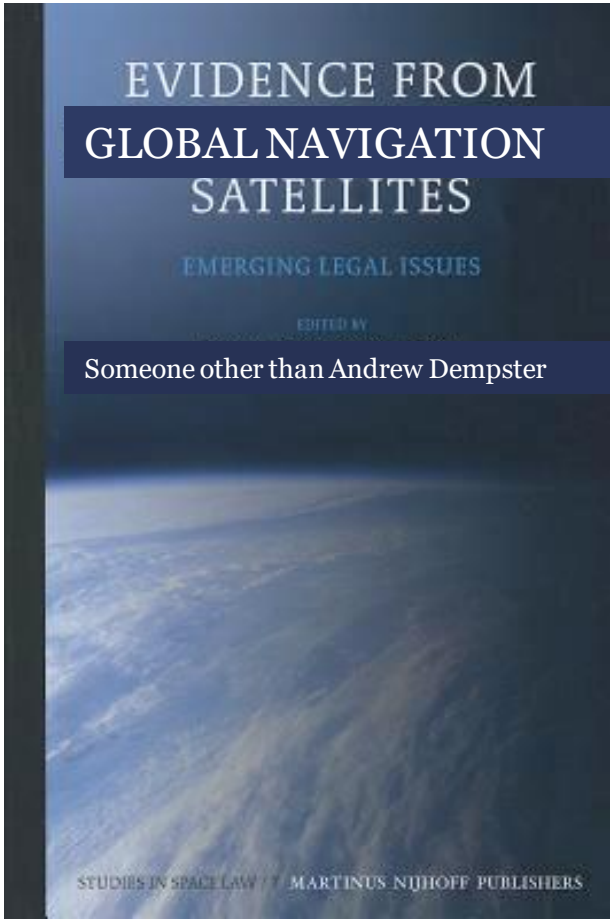
1. Corroborate if possible
2. Build in controls to give greater confidence
3. Ask data suppliers to authenticate the first stage
4. Legislate that the defence must prove incorrect functioning of the system (!)
5. Use systems such as digital signatures to authenticate
6. Follow standards in recording data
7. Write a standard specifically for EO evidence

Lessons

GNSS community to write a similar textbook?

Contact me:

a.dempster@unsw.edu.au



What else can be done?

Receiver can detect and report on a number of the identified problems:

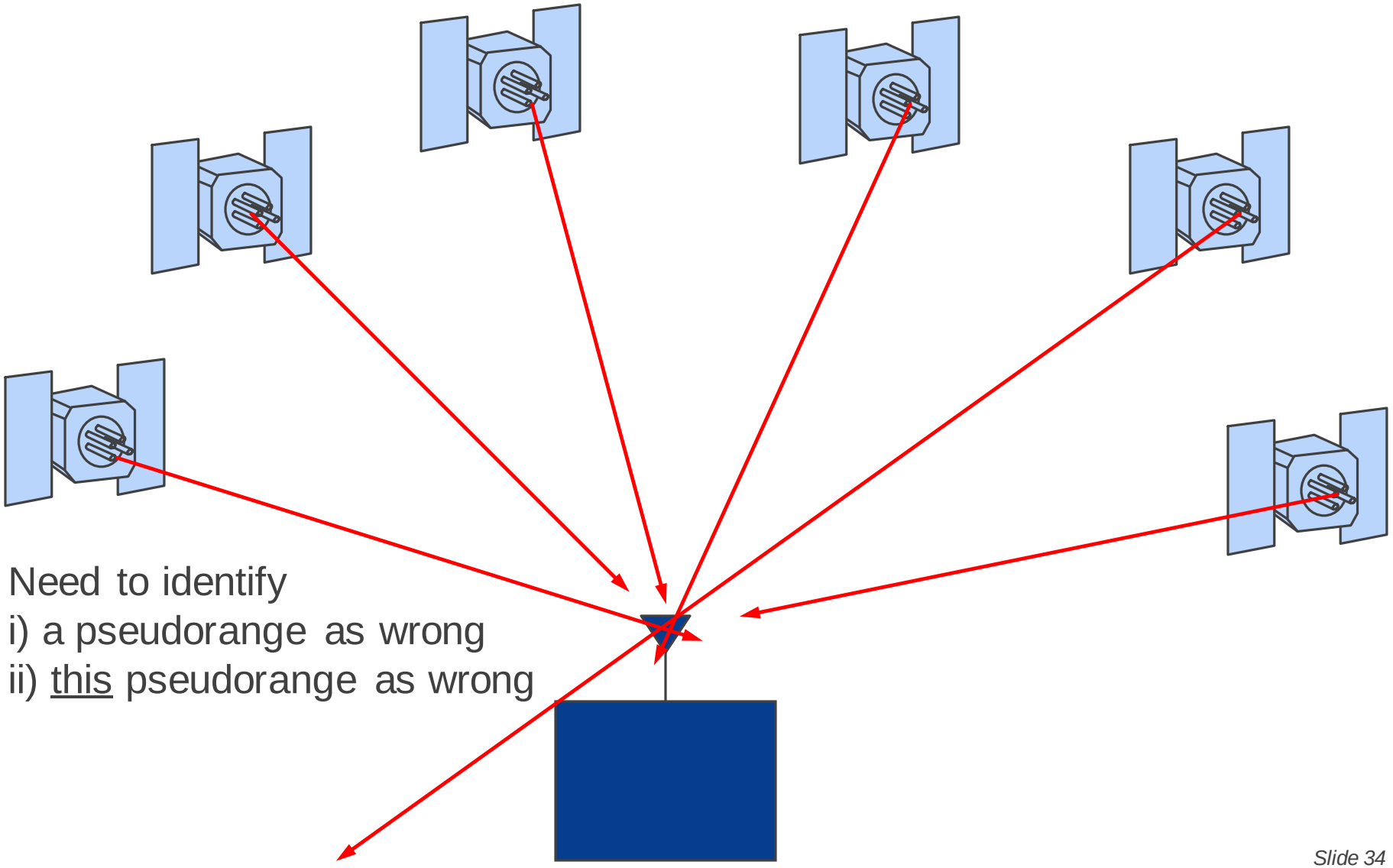
- Attenuated signals
- Poor geometry (satellite set enough)
- Jamming/ spoofing
- Integrity: Iono/ Multipath/ Attenuated signal

Integrity

e.g. Receiver Autonomous Integrity Monitoring (RAIM) seeks to isolate a poor pseudorange

Originally for a “bad” satellite (led to SBAS), but now any isolated bad measurement

The RAIM Problem



Need to identify
i) a pseudorange as wrong
ii) this pseudorange as wrong

How many Satellites?

We need redundancy (i.e. > 4 sats), but how many?

If we used 5, one of which was malfunctioning, we could create 5 sets of 4 sats, 4 of which would contain the malfunctioning sat and produce results inconsistent from each other and the correct set - we couldn't tell which set was right! ie we *could* tell we had a malfunctioning sat but not which one

Use 6 sats, so there are C(6,4) = 15 sets of 4, of which C(5,4) = 5 would be consistent

RAIM: System Requirements

RAIM is basically a self-consistency check on measurements

Implies redundancy (and good geometry when individual satellites are removed from the set for checking)

Need:

- as many satellites in view as possible
- satellites in good geometry

RAIM Approaches

Snapshot:

- only current redundant measurements are used in self-consistency check

Averaging/filtering schemes

- uses past and present measurements, as well as inferred vehicle motion

Snapshot uses less information but has the advantage of relying only on current information - it hasnt used potentially poor information to estimate the current state

Integrity Terms

Alert Limit: The alert limit for a given parameter measurement is the error tolerance not to be exceeded without issuing an alert.

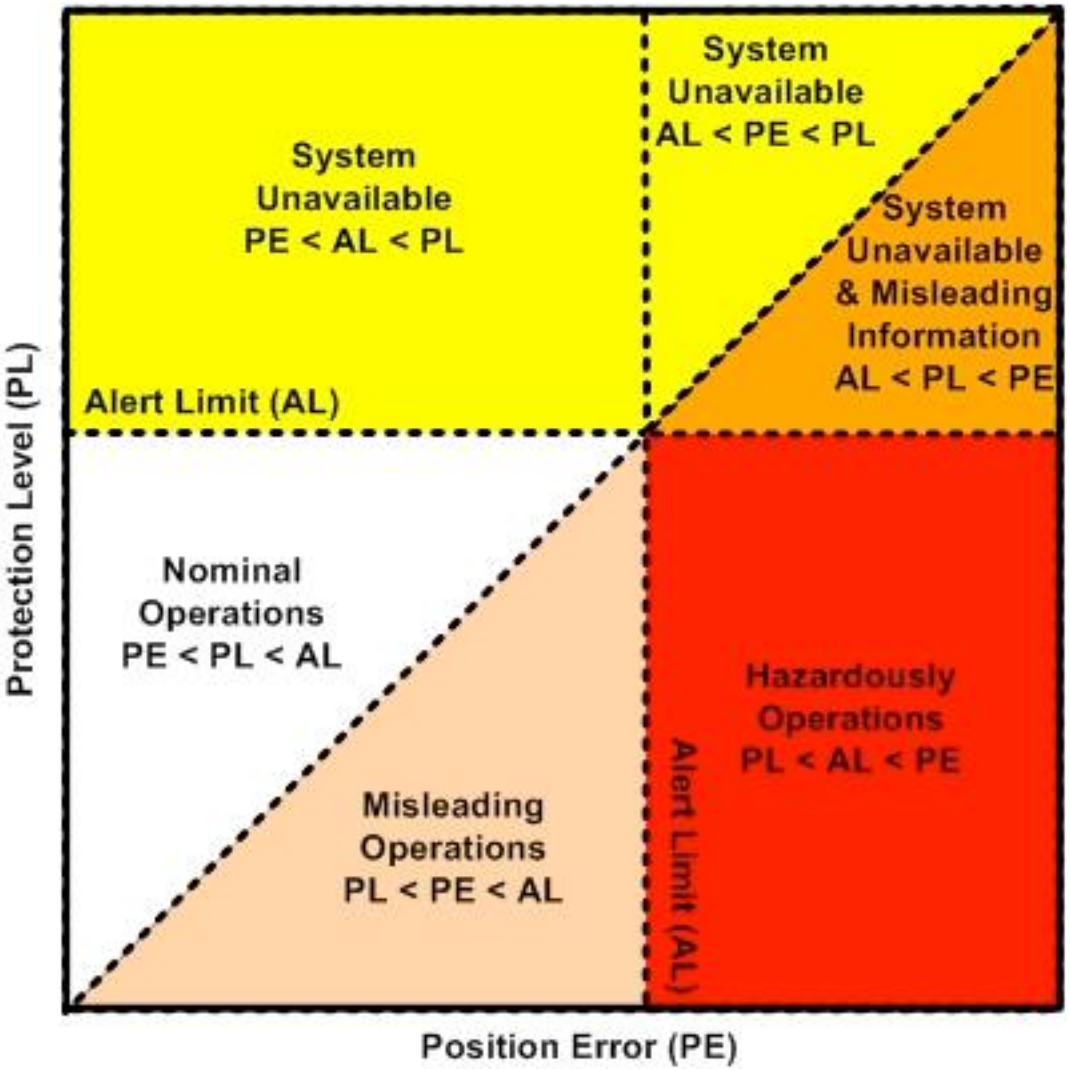
Time to Alert: The maximum allowable time elapsed from the onset of the navigation system being out of tolerance until the equipment enunciates the alert.

Integrity Risk: Probability that, at any moment, the position error exceeds the Alert Limit.

Protection Level: Statistical bound error computed so as to guarantee that the probability of the absolute position error exceeding said number is smaller than or equal to the target integrity risk.

(Wikipedia)

Stanford-ESA Integrity Diagram



Common Logging Formats

Can they log useful information?

Do they?

NMEA Messages: Common

GGA: time, lat, long, fix quality (GPS, DGPS, PPS, RTK, RTK float, dead-reckoned, manual, or simulated), no. satellites, HDOP, altitude, height of Geoid

GSA: 3D fix, satellites, PDOP, HDOP, VDOP.

GSV: satellites, elevation, azimuth, signal to noise (SNR)

NMEA Messages: More Useful

GRS (Range residuals): time, residuals for each satellite.

GST (Pseudorange noise statistics): time, RMS value of residuals, error ellipse semi-major axis, semi-minor axis, orientation, lat 1 sigma, long 1 sigma, height 1 sigma

Any Other Formats Provide Quality Info?

GPX: none

Android phones: provide raw range measurements

Aircraft “black box” has no requirement for quality – even position!

ADS-B has accuracy and integrity (protection limits)

AIS has position and whether RAIM guarantees 10m accuracy

Those 11 Questions

Question	Source of Answer	Authenticated by Other "Witness"?	Receiver-Based Detection?	Integrity helps?
GNSS System OK?	GNSS NANU	Y	Y (slow)	Y
Iono/ Tropo OK?	Networks	Y	Y?	Y
Multipath?	Rx	Y	Y	Y
Attenuation?	Rx	Y	Y	Y
Jam/ spoof?	Rx +	Y	Y	?
Geometry OK?	Rx, post-processing	Y	Y	Y
Calcs OK?	Hard	Y	Y?	N
Recorded OK?	Hard	Y	Y?	N
Accuracy indicated?	Rx	?	Y	Y
Other inputs used?	Hard	Y	Y?	Y?
Extracted OK?	Digital forensics	Y	N	N

Future Work

Expert witness check list

Recommendations for data logging standard, including a specific integrity indication

Rank evidence types by quality (even if just verbal: poor, moderate, good)

From Solange's work:

- Guidance to the court/ criteria for selection of an expert

- Different types of GNSS data source (covert tracker, data logger, phone, police GNSS)

- Admissibility

The End

Extra Slides

Snapshot Algorithms

Examine one instant in time

Methods:

- Range comparison method
- Least-squares residuals method
- Parity Method

Linearise the algebraic problem about a particular position

Linearised System

We can define the system as before except we isolate out the pseudorange error:

$$\Delta\rho = \mathbf{H}\Delta\mathbf{x} + \varepsilon$$

where ε (n x 1) is measurement error vector with usual errors plus malfunctions

However, if solved as before:

$$\Delta\mathbf{x} = \mathbf{H}^{-1}\Delta\rho$$

position would incorporate malfunction error

Range Comparison Method

Take 4 satellites and perform a linearised solution

Evaluate errors for the extra 2 sats and if either is out of range, signal malfunction

The “out-of-range” threshold is set so that the 1/15000 false alarm rate is achieved

Least-Squares Residuals method

$$\Delta \mathbf{x} = (\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T \Delta \rho$$

From the least-squares solution, predict the observables:

$$\Delta \rho_{\text{predicted}} = \mathbf{H}\ \Delta \mathbf{x}$$

and difference to get the residuals:

$$w = \Delta \rho - \Delta \rho_{\text{predicted}} = \left[\mathbf{I} - \mathbf{H}(\mathbf{H}^T \mathbf{H})^{-1} \mathbf{H}^T\right] \Delta \rho$$

from which we get our SSE observable:

$$SSE = w^T w$$

Least-Squares Residuals method

For SSE:

- positive threshold only is needed
- for pseudoranges with the same error statistics, the threshold for a constant alarm-rate algorithm depends only on no. pseudoranges

using a test statistic of $\sqrt{SSE/(n-4)}$ gives linear relationship between statistic and pseudorange bias error (useful as 2D position error is proportional to pseudorange bias error)

Parity Method

Set up an equation that uses a matrix **P** which has mutually orthogonal rows of unity magnitude, orthogonal to the columns of **H** :

$$\begin{bmatrix} \Delta\mathbf{x} \\ \mathbf{p} \end{bmatrix} = \begin{bmatrix} (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T \\ \mathbf{P} \end{bmatrix} \Delta\rho$$

This produces parity vector **p** (two elements if 6 sats in set)

Special properties of **p** ensure

$$\mathbf{p}^T\mathbf{p} = w^T w = SSE$$

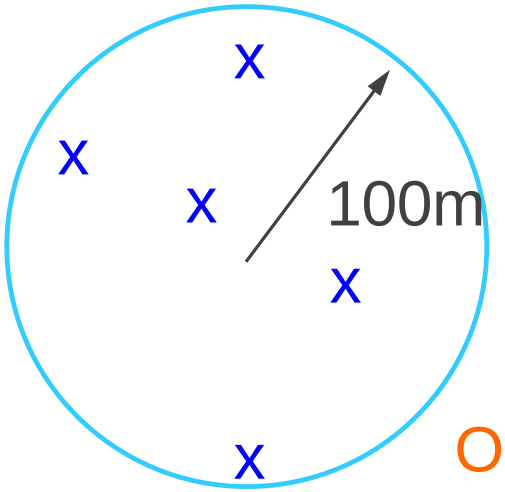
Maximum Separation of Solutions method

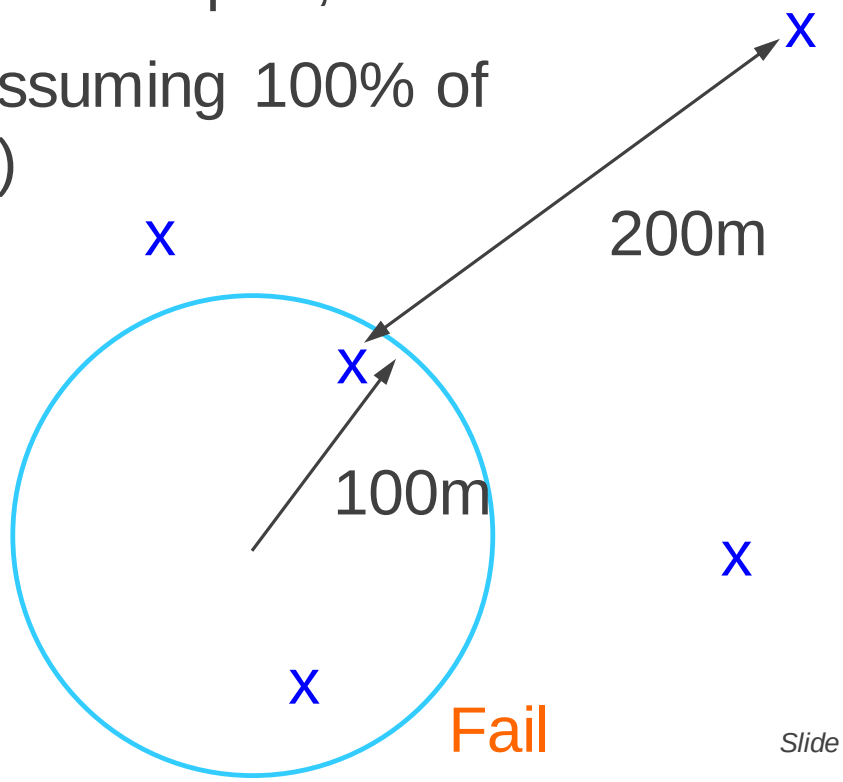
Assume no more than one satellite failure

Evaluate all solutions, leaving one sat out

If pair of solutions is more than 200m apart, failure

Protects against 300m errors, assuming 100% of errors < 100m (actually 95%)





Eliminating Poor Sets

Sets with poor geometry must be marked inadmissible

May still give a good position but there is insufficient redundancy to ensure integrity

Must be careful eliminating poor geometry, as any periods of inadmissibility reduce system availability

Inadmissibility: $HDOP_{max}$

DOP is a reasonable measure of geometry (as it is for positioning) because if DOP is too high, we know that it is difficult to identify an error in pseudorange

Check each set with one satellite missing and if $HDOP_{max}$ is above a threshold, mark the complete set as inadmissible (i.e. can't be relied upon for integrity)

Only a coarse measure of geometry quality

Inadmissibility : δH_{max}

Evaluate $HDOP_i$ for the n subsets

Evaluate HDOP for the complete set

$\delta H_{max} = max_i[HDOP_i^2 - HDOP^2]^{1/2}$

Threshold δH_{max}

Gives more reliable result than $HDOP_{max}$

Failure Isolation

So far, all techniques have been for malfunction *detection*

OK where a backup nav system exists, but no good for sole-means

Failure Detection and Isolation (FDI)

FDI: Parity method

Remember the parity vector **p** which indicated malfunction:

$$\begin{bmatrix} \Delta\mathbf{x} \\ \mathbf{p} \end{bmatrix} = \begin{bmatrix} (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}^T \\ \mathbf{P} \end{bmatrix} \Delta\rho$$

The orthogonality property of **P** ensures:

$$\mathbf{p} = \mathbf{P}\Delta\rho = \mathbf{P}(\mathbf{H}\Delta x + \varepsilon) = \mathbf{P}\varepsilon$$

i.e. **P** projects the error onto **p**. If there is a bias *b* in pseudorange *i*,

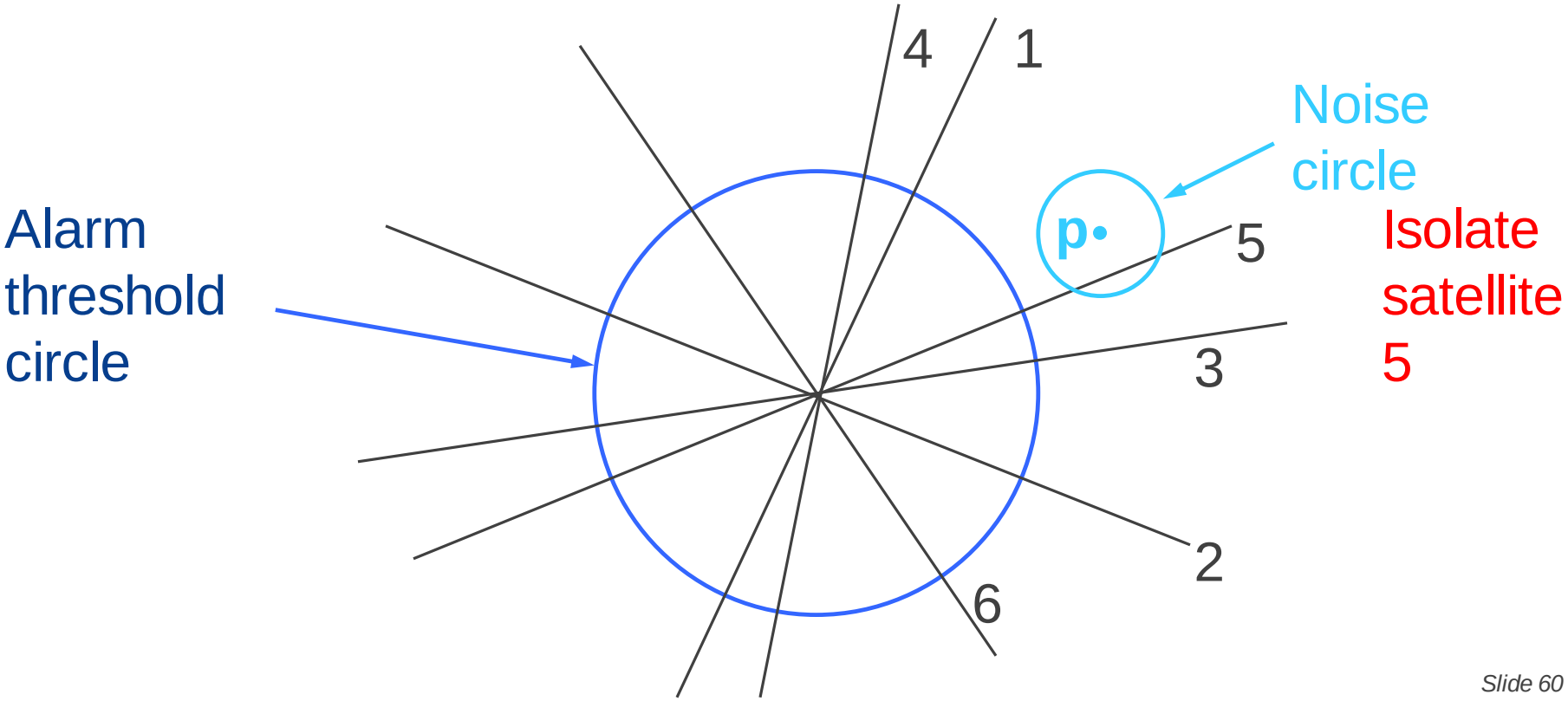
$$\mathbf{p} = \begin{bmatrix} p_{1i} \\ p_{2i} \end{bmatrix} b$$

i.e. a point on a line with slope p_{2i}/p_{1i}

FDI: Parity method

Each satellite has a unique line associated with it

Rule: select line closest to **p**



References

B W Parkinson and J J Spilker Jr., “Global Positioning System: Theory and Applications”, vols I & II, American Inst Aeronautics & Astronautics, 1996