Spoofing GNSS Timing Receivers

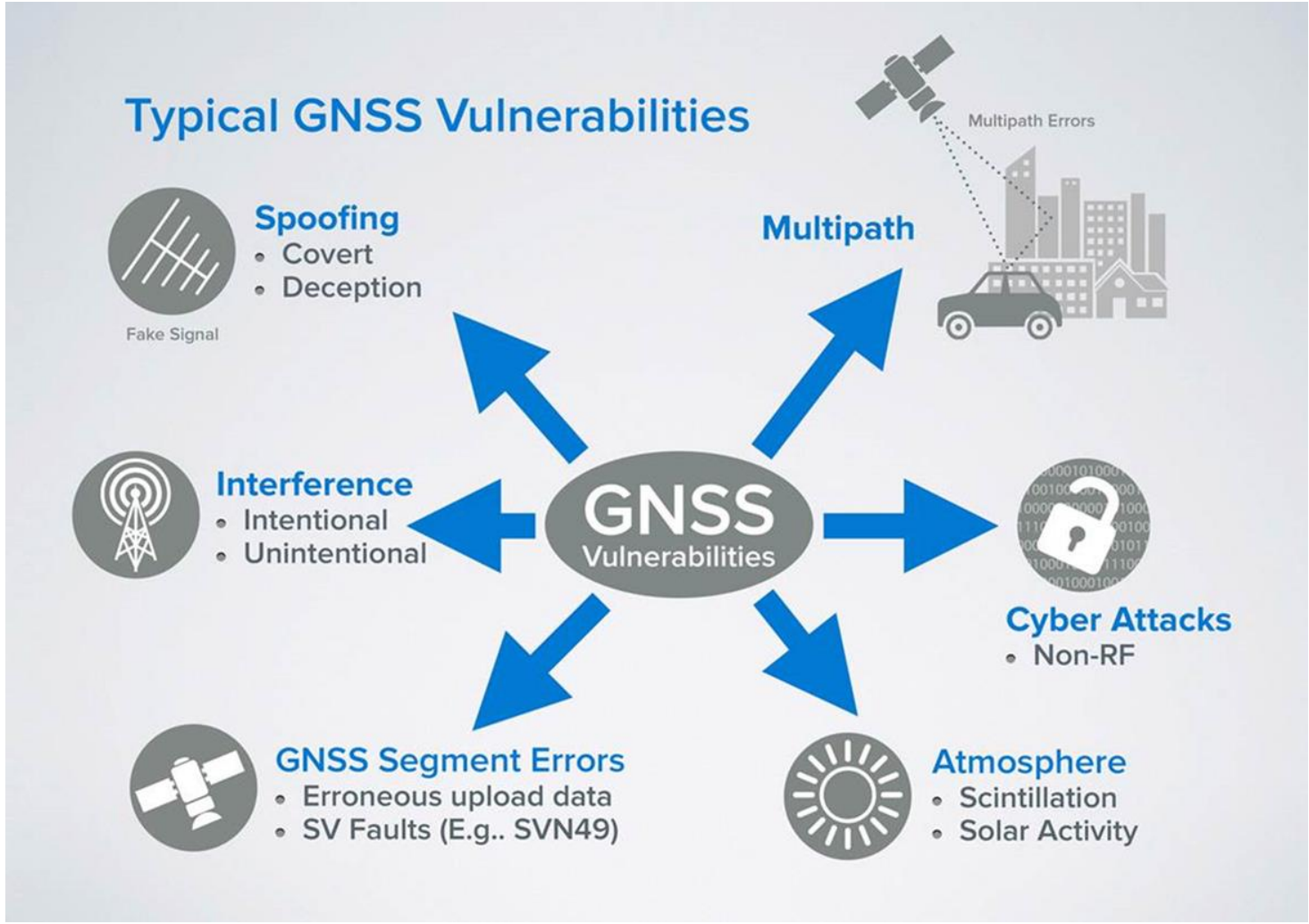
Tim Frost and **Guy Buesnel**

ITSF, November 2015

www.calnexsol.com
www.spirent.com

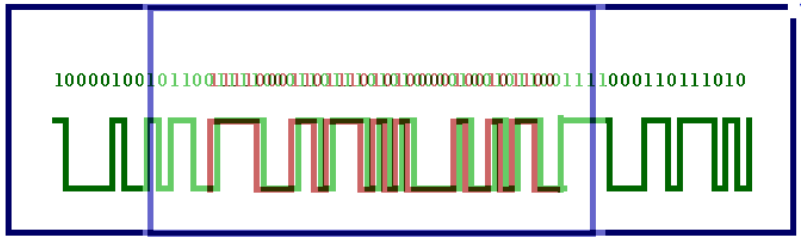
Introduction

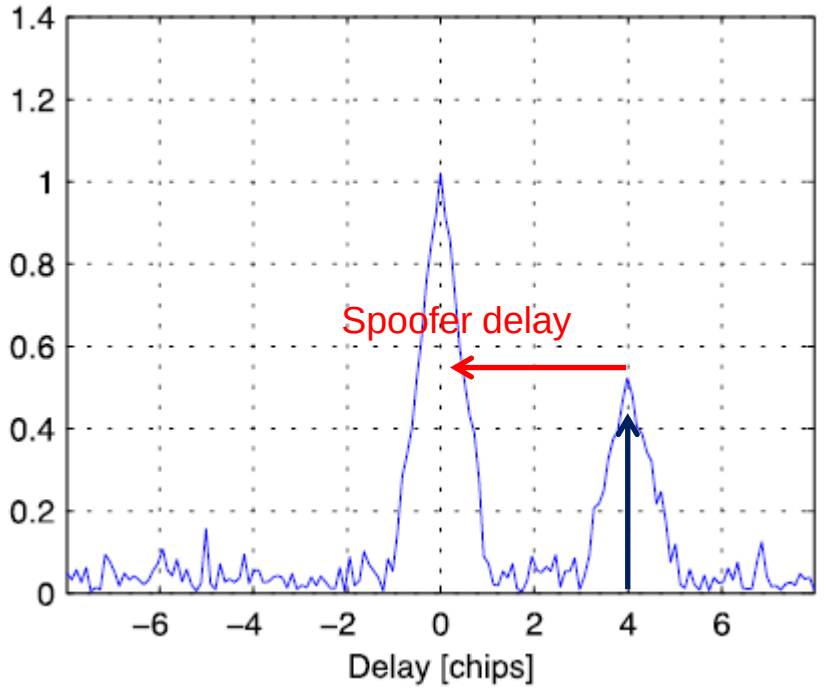
Overview of GNSS Vulnerabilities



GPS disruptions and Timing…

- The attacker might attempt to align code and power to the real signal to avoid jumps / lock loss
- The attacker might attempt to replay space navigation data in order to bypass data verification mechanisms (meaconing)
- The attacker might attempt to force the receiver to acquisition mode in order to cheat spoofing detection implemented in tracking loops
- The attacker might attempt to modify navigation data



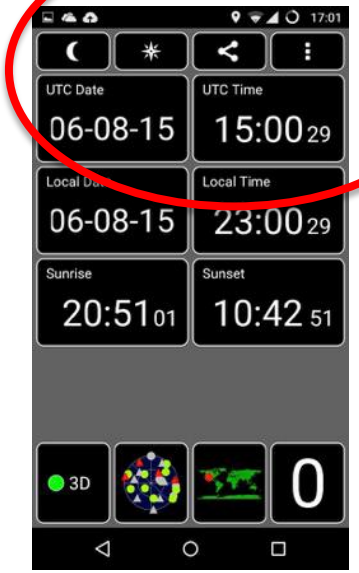


GPS Disruptions and Timing…

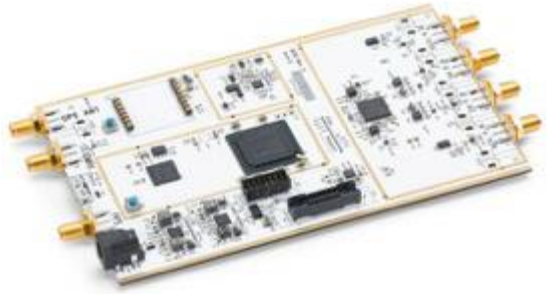
- Michael Robinson – DEFCON 23, August 2015:
  "Knocking my Neighbor's Kid's cruddy drone offline"
- Demonstrated effect of disrupted GPS Signal on a drone…
  - Non-GPS flying mode
  - Video feed started to jitter and video feeds were tagged as "unstable"

GPS Disruptions and Timing…

- Huang and Yuang – not GPS specialists - built and tested a low-cost GPS spoofer… demonstrated at DefCon
  - The cellphone clock was spoofed to display wrong date/time with auto-calibration enabled !!
  - One cellphone ended up displaying a time and date in the future – the other phone (well known brand) ended up “bricked”



Generating replica GNSS signals



- Low-cost Software Defined Radio boards easy to procure – not designed for hacking but low cost makes them attractive
- Used with Open Source Code – readily available online for:
  - GPS Transmitter
  - GPS Receiver

How to detect spoofing in a receiver

- Power Levels
  - Spoofing signal is likely to have a noticeably higher power level
  - Monitoring relative signal strengths: each signal should have a fixed relative power offset – if this changes suddenly, there's a problem
- Monitor Position
  - If a fixed timing receiver starts to move away from its surveyed position at 30mph there's a problem. The spoofer would need to modify all of the pseudo-ranges being received (obviously won't work in a single channel receiver)
- Bound and Compare Range Rates
  - Code and carrier range rate changes will be different for a spoof signal
- Doppler Shift Check
  - Spoofed signal is likely to be from a fixed position so Doppler is likely to be incorrect
- Verify Received Navigation Data
  - Compare almanac/ephemeris to known data
  - Check for 'missing/default' Navigation data
- Jump Detection
  - Observable should remain within a tolerable range, check for sudden changes

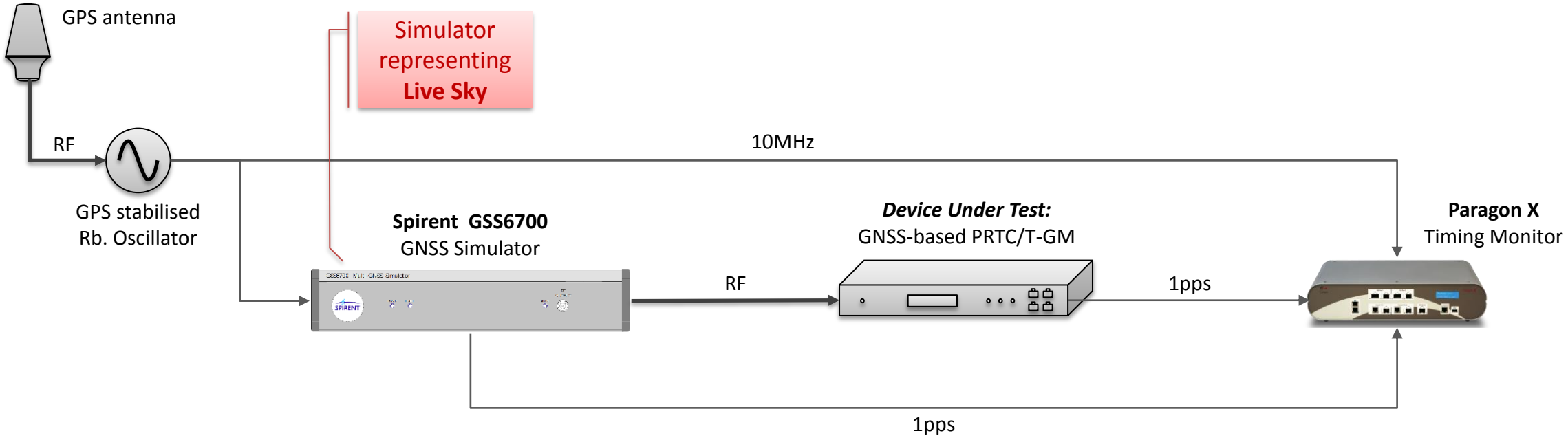
Experimental Results

Test 1: Pseudo-range Ramp

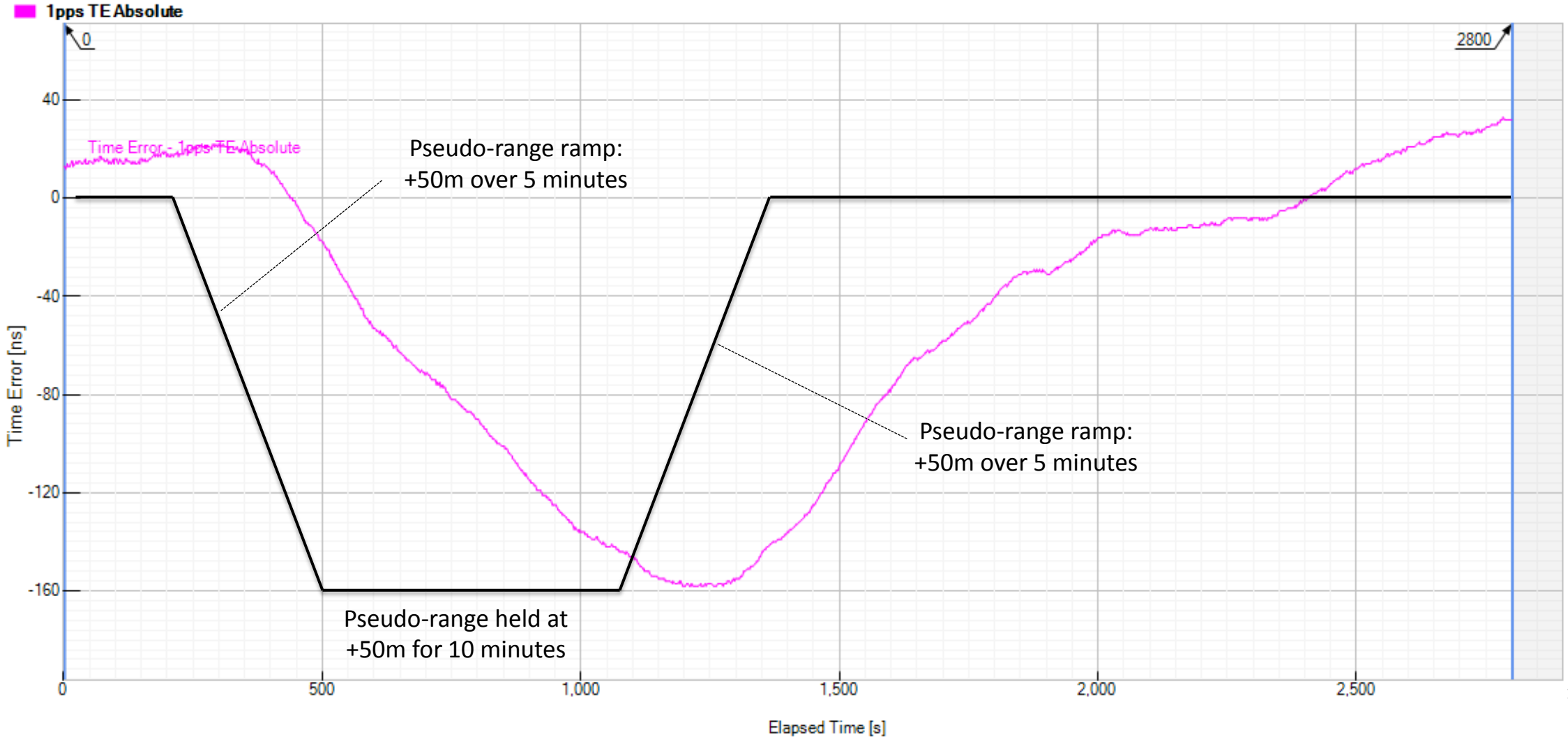
- Pseudo-range allows the receiver to calculate its distance from the satellites
- Changing the pseudo-range on one satellite will affect the receiver's position calculation
  - The satellite will appear to be either closer to or further away from the receiver than it actually is
- Changing the pseudo-range on all satellites keeps position stable, but affects the receiver's time calculation

- **Test applied:** gradually change the pseudo-range on all satellites and monitor effect on the receiver

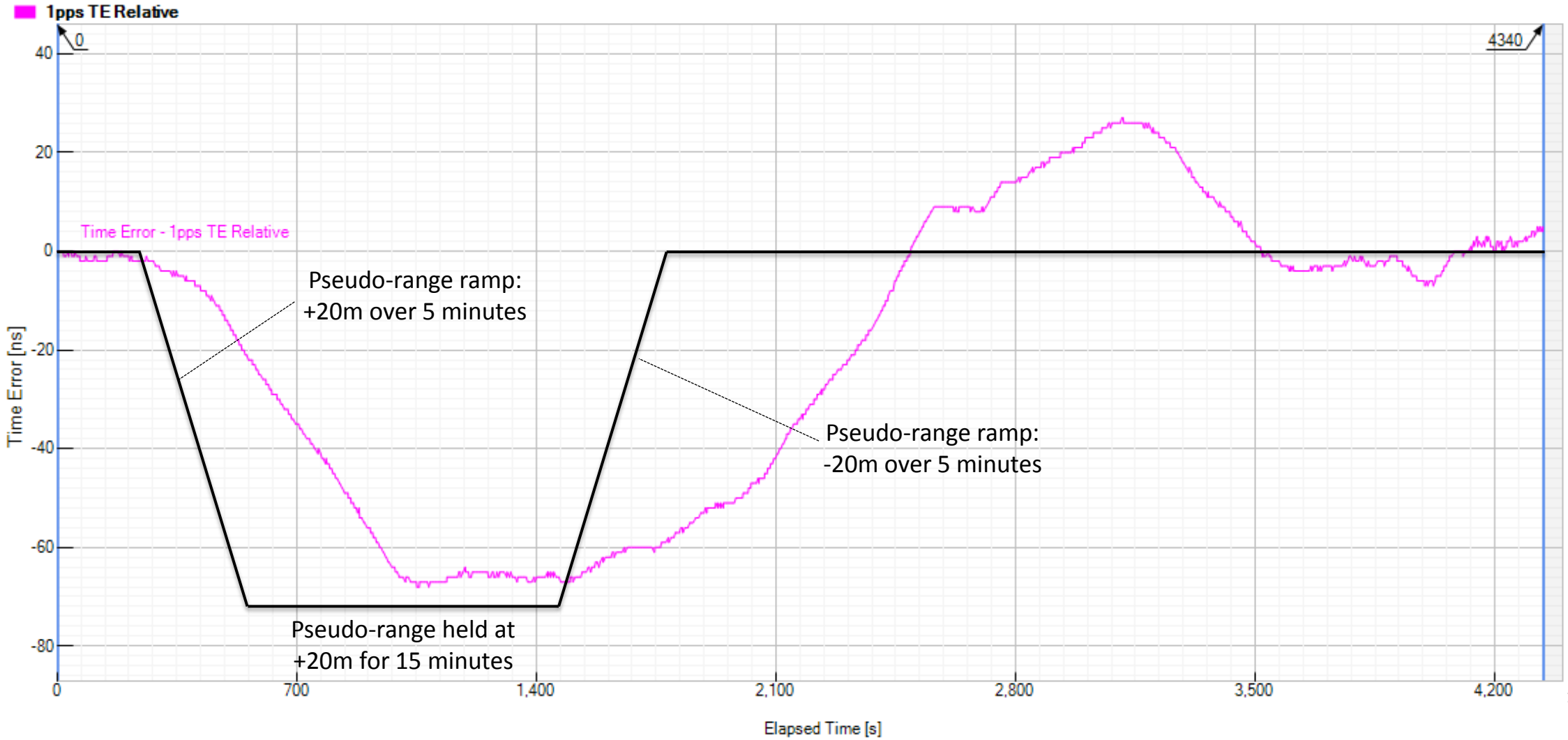
Experimental Setup 1: Pseudo-range Ramp



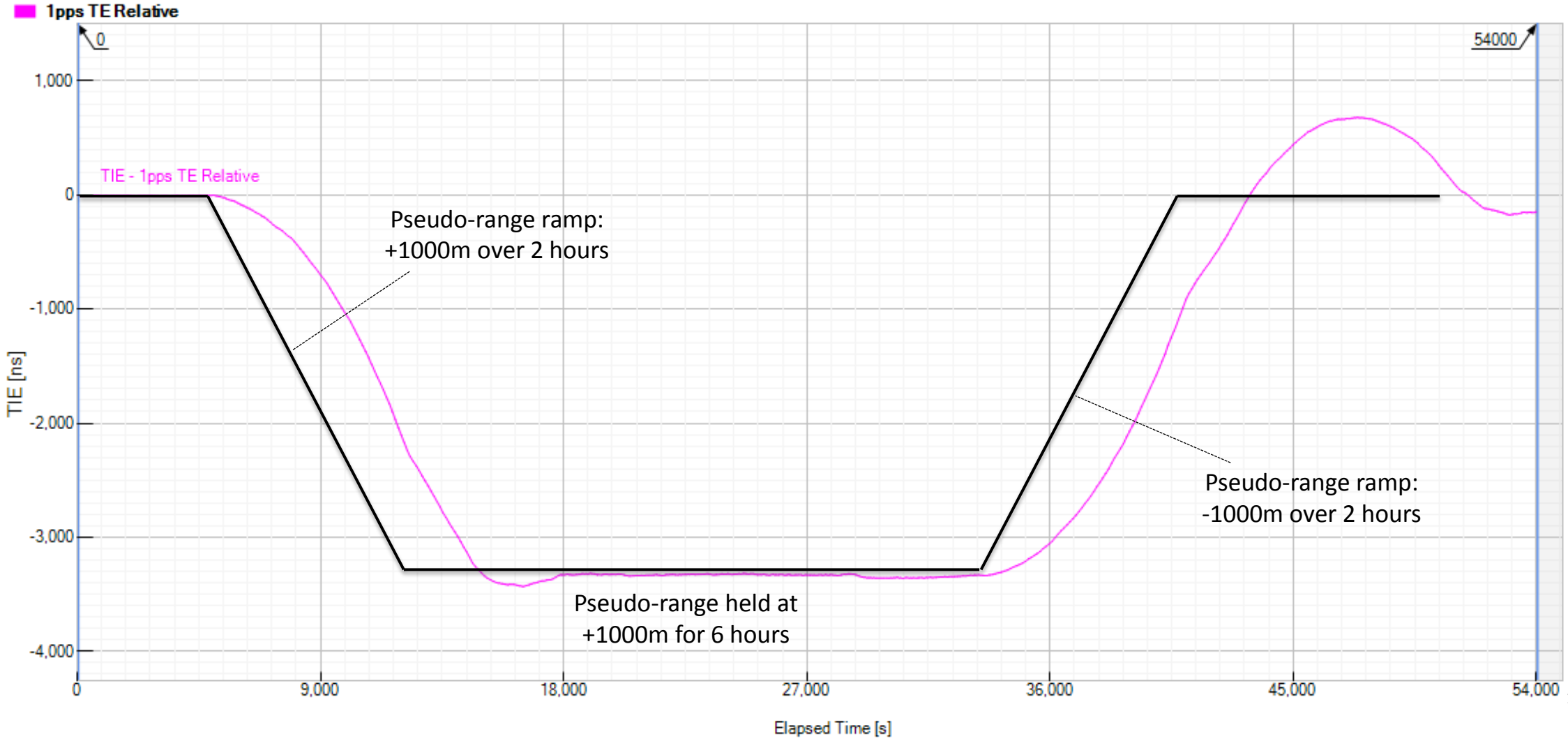
Device A: Response to Pseudo-Range Ramp



Device B: Response to Pseudo-Range Ramp



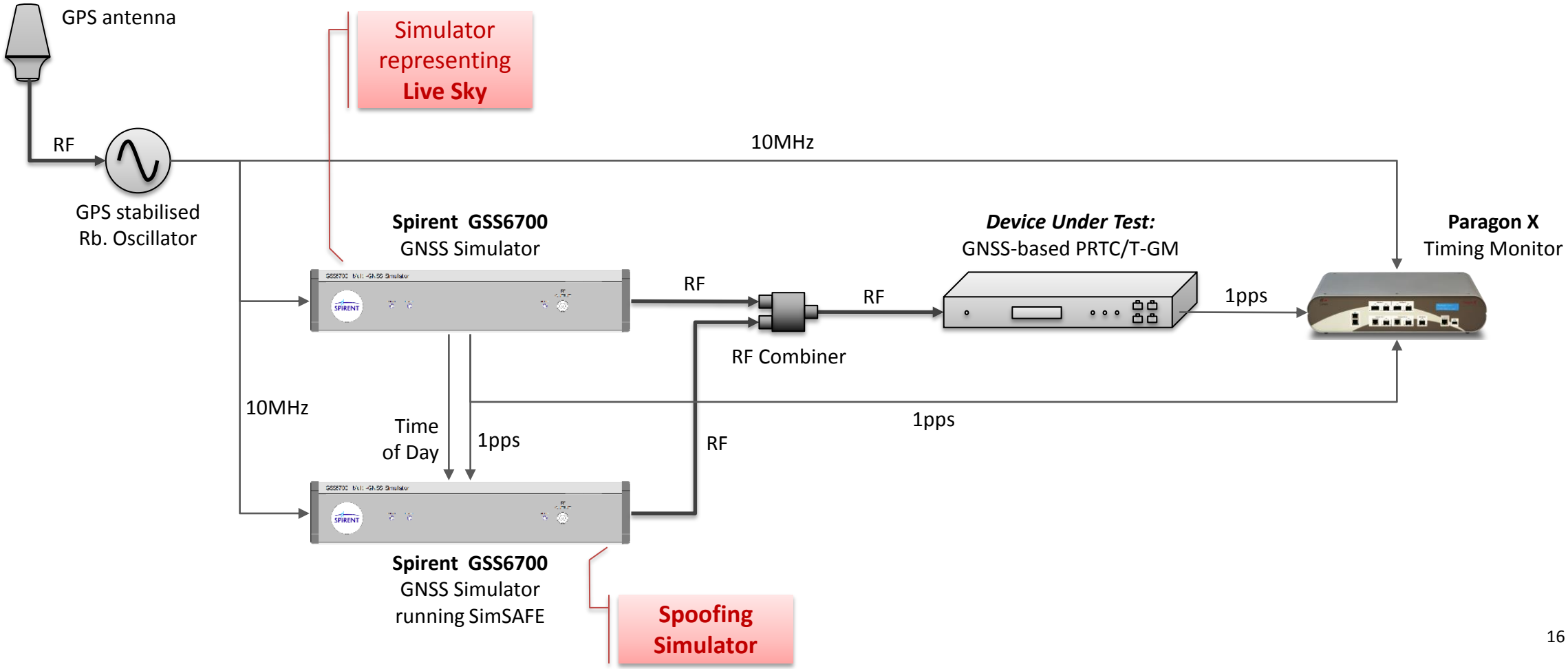
Device C: Response to Pseudo-Range Ramp



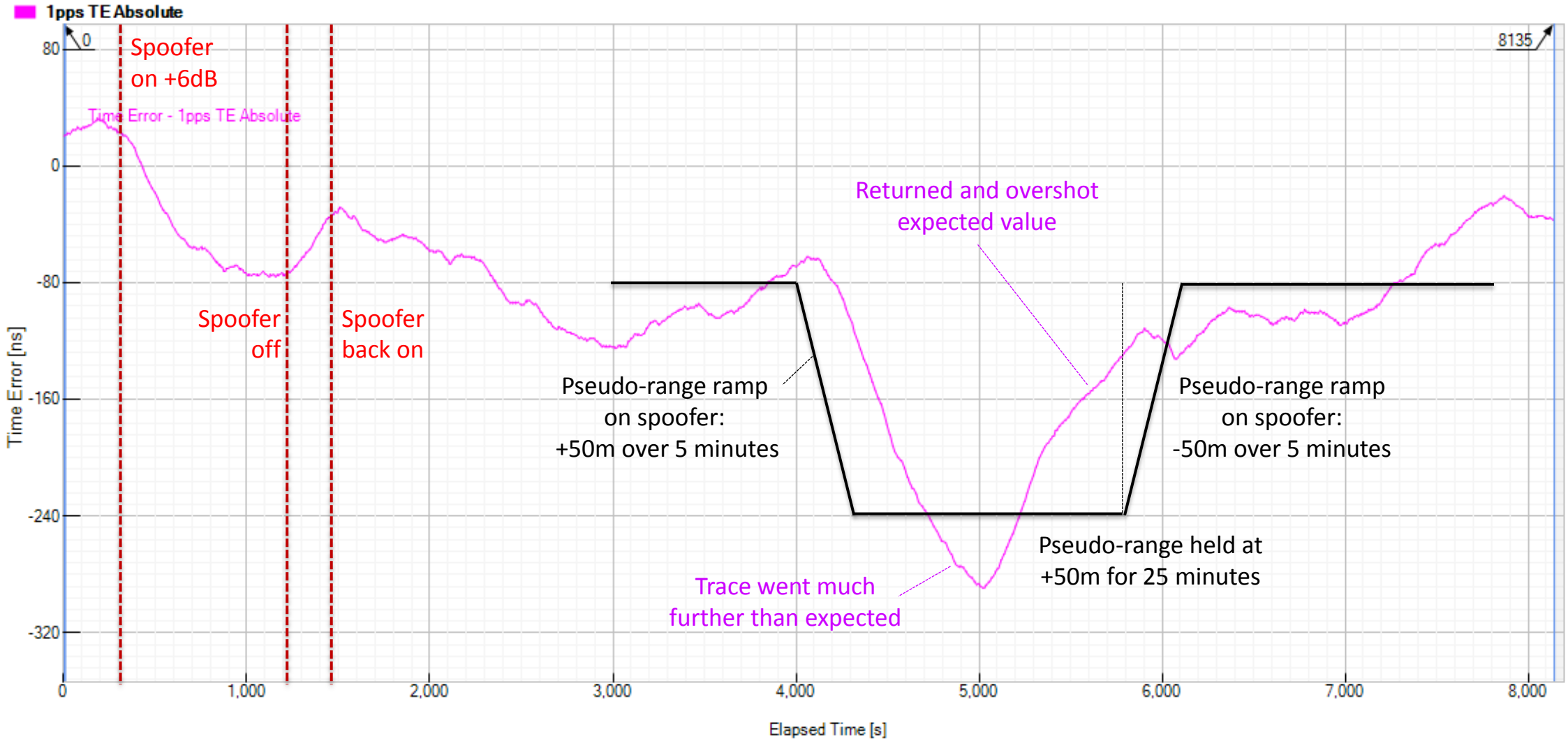
Test 2: Spoofing from Simulator

- Test 1 didn’t involve spoofing at all – it was just a test to see if the time could be manipulated
- Test 2 involves turning on a second simulator
  - Simulator 2 will be at slightly higher power (+6dB)
  - Simulators are synchronised together in position and time, so should be providing the same information
  - Objective is to see if the second simulator “takes over” the receiver
- Next step is to apply a pseudo-range ramp on the second simulator to see if it drags away the time of the receiver

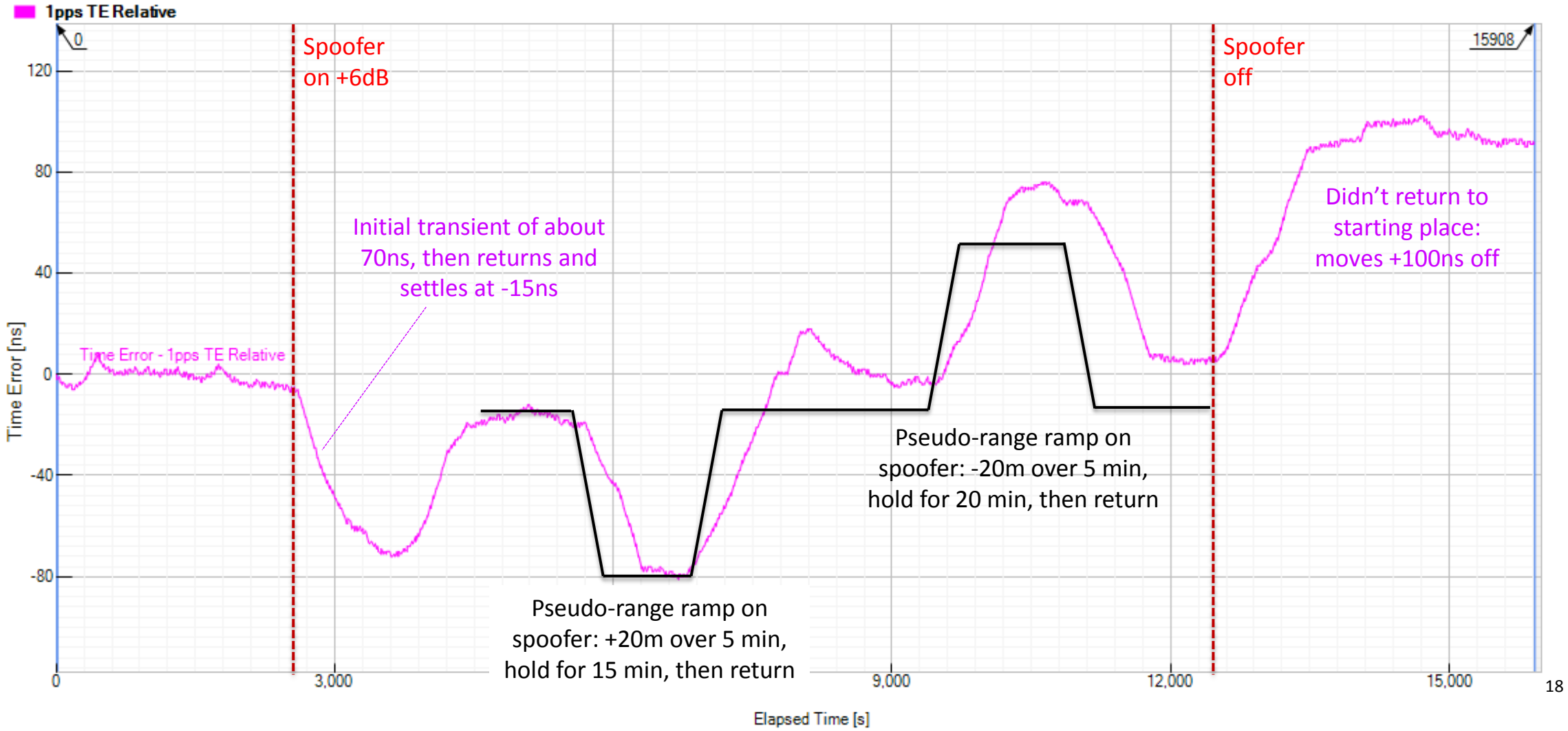
Experimental Setup 2: Spoofing from simulator



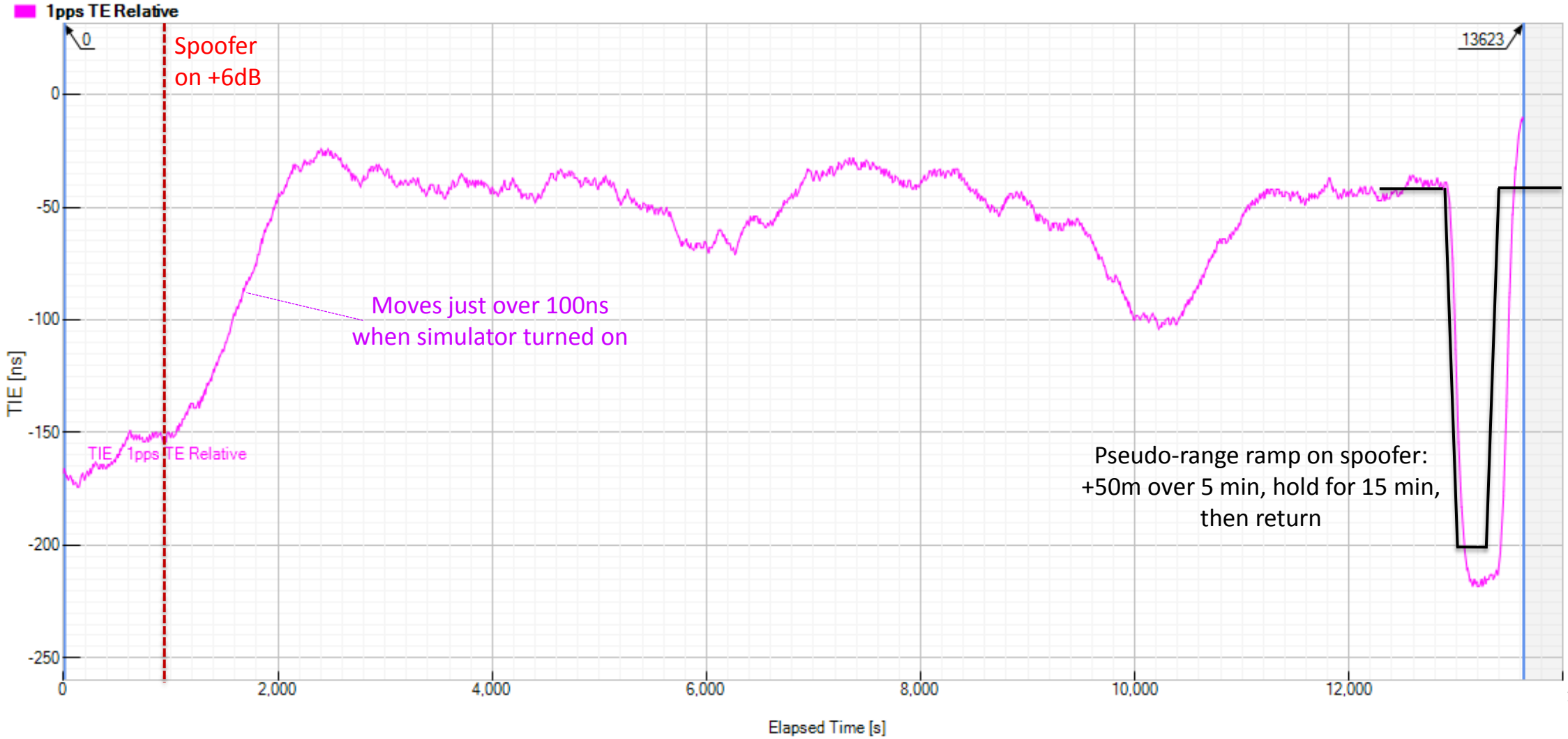
Device A: Spoofing from Simulator



Device B: Spoofing from Simulator



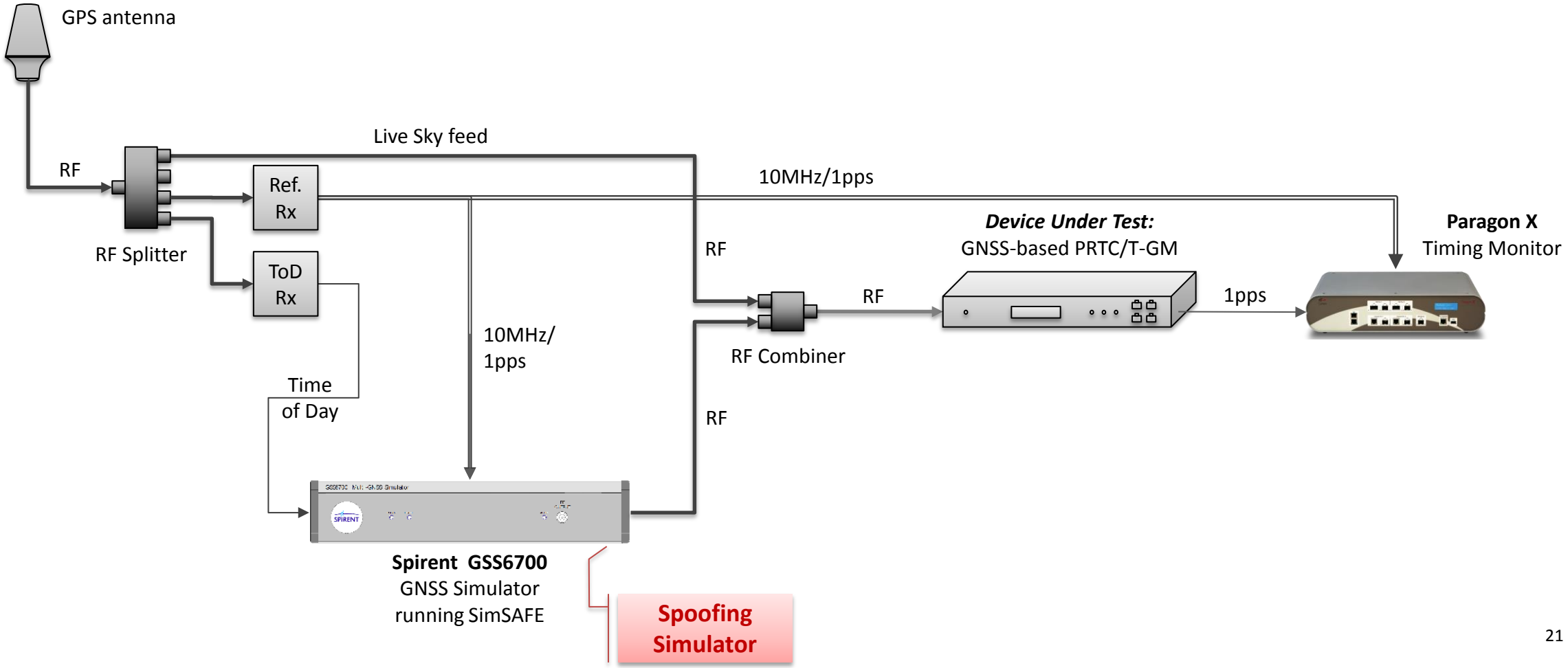
Device C: Spoofing from Simulator



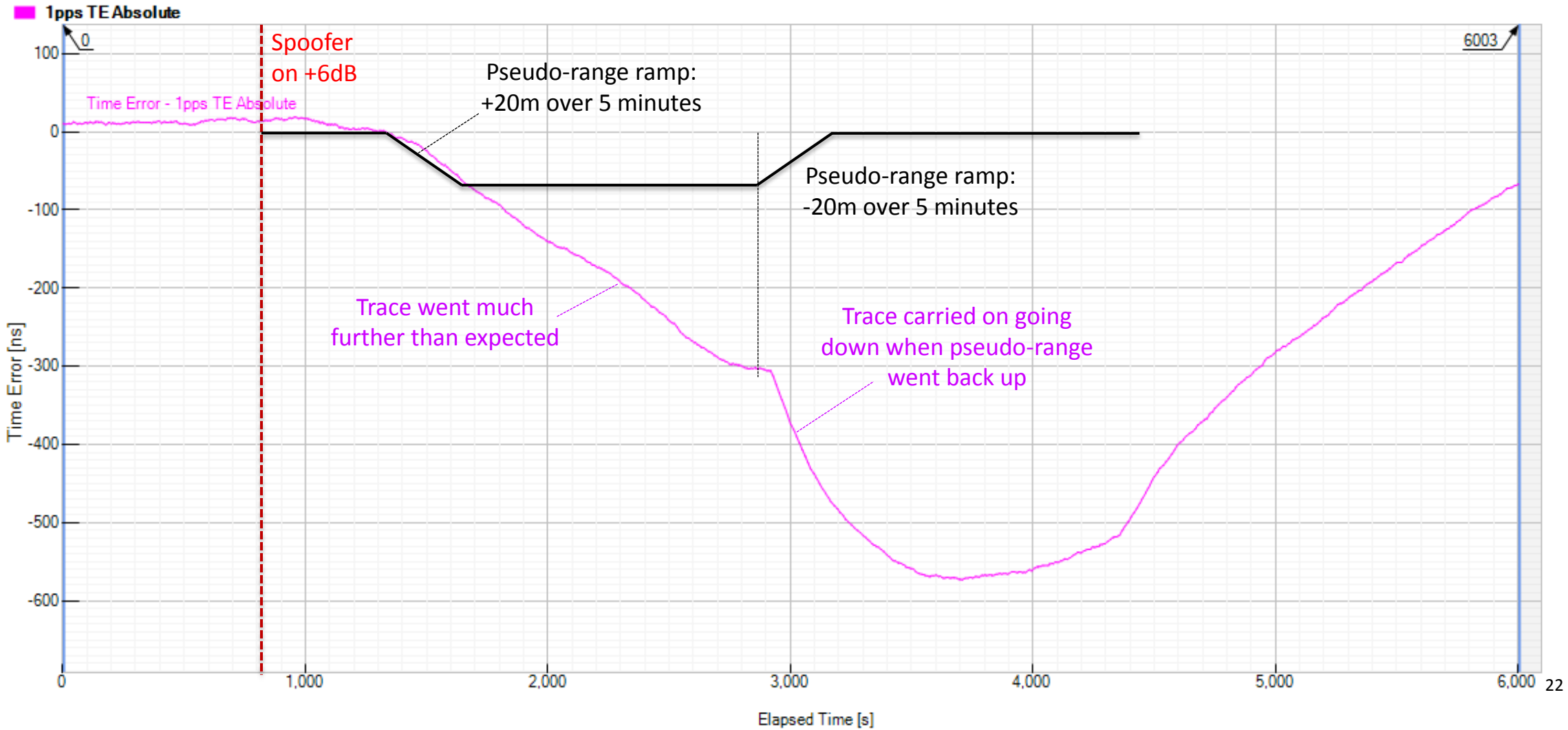
Test 3: Spoofing from Live Sky

- Test 2 was spoofing one simulator with another
- “Live sky” is more challenging, since the conditions are much less controlled
- Test 3 involves trying to spoof a live signal, and move the time of the receiver away from current time

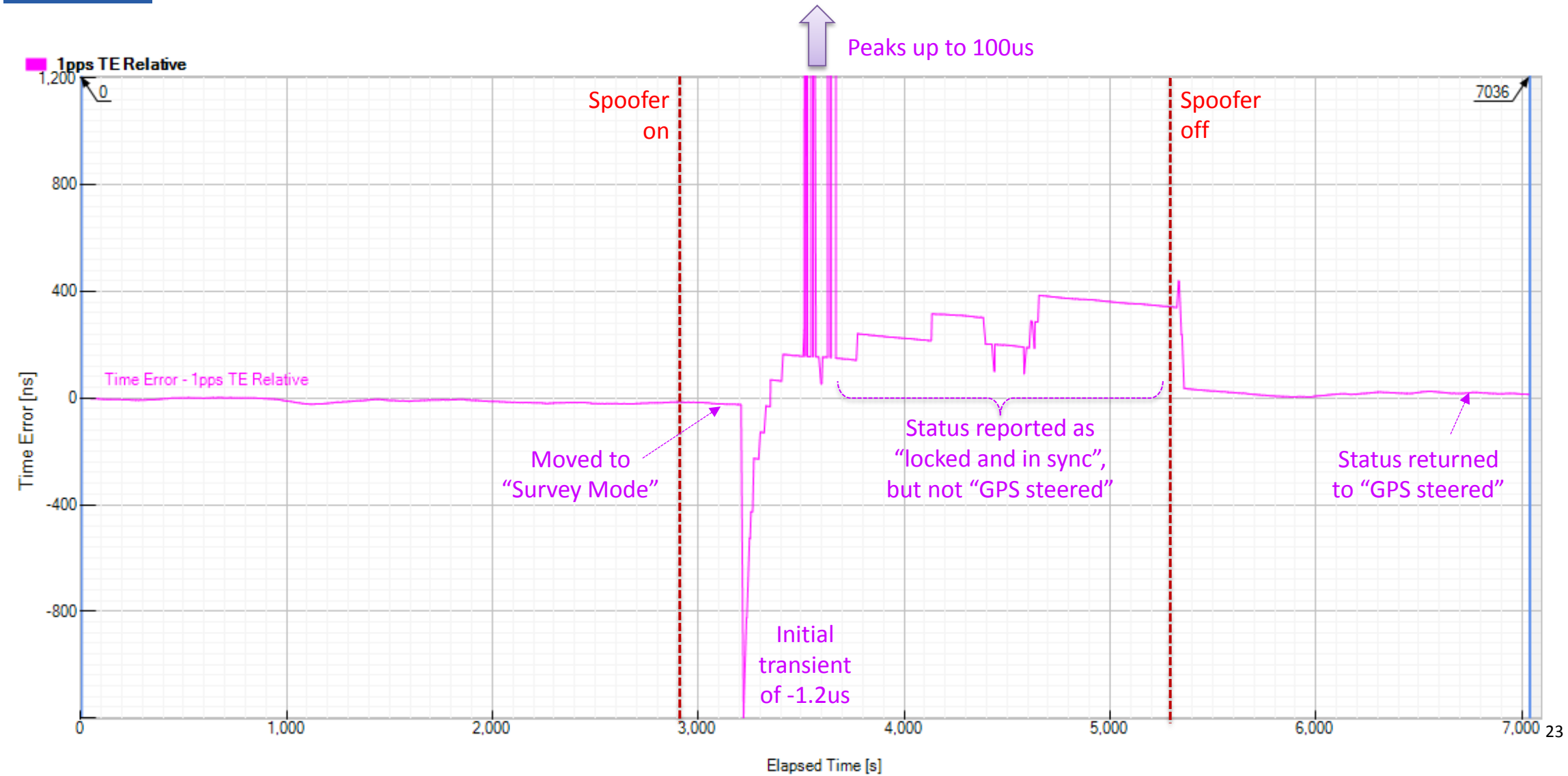
Experimental Setup 3: Spoofing from Live Sky



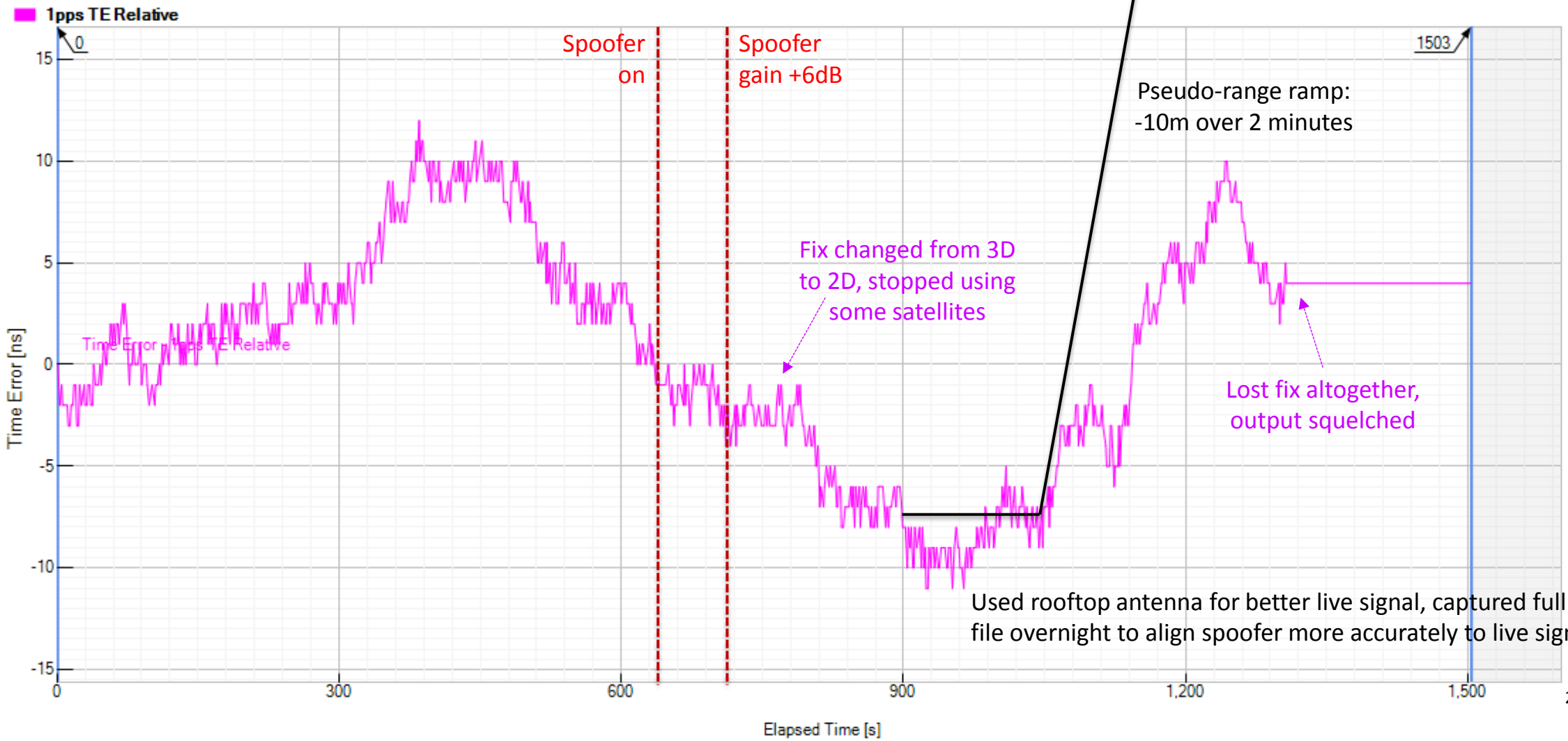
Device A: Spoofing from Live Sky



Device B: Spoofing from Live Sky



Device C: Spoofing from Live Sky



Used rooftop antenna for better live signal, captured full orbital file overnight to align spoofer more accurately to live signal

Conclusions

- Spoofing from live-sky proved more difficult than the simulation
  - Not sure why this was the case
    - Most likely due to alignment of the faked signal in the receiver correlators
    - Atmospheric disturbance (heavy rain) affected the first two tests
  - Not always sure that the receiver had been spoofed, although unusual behaviour was observed and the timing receivers were rendered unusable
  - Evidence that real-life spoofing with a crude attack is relatively easy if the receiver has no detection mechanism
  - Need to do more work here to understand the issues experienced
- There are warning signs in the receiver that a spoofing attack is in progress
  - Receiver detection is possible in all but the most sophisticated attacks
  - Testing response of existing systems important – especially as a crude attack can cause unexpected behaviour
- Use of complementary or back-up systems is important
  - Use of holdover when uncertain over authenticity of signal
  - Redundancy (e.g., e-LORAN as a complementary system, PTP as a non-wireless based approach)

Acknowledgements

The following people all helped to make this experiment possible:

- Fabio Simon-Gabaldon – Spirent
- Richard Boyles – Spirent
- Charles Curry – Chronos
- Richard Elsmore – Chronos
- Duncan Davidson – Calnex

THANK YOU FOR LISTENING!

Tim Frost, Calnex Solutions,
tim.frost@calnexsol.com

Guy Buesnel, Spirent,
guy.buesnel@spirent.com