Spoofing GNSS Timing Receivers

Tim Frost and **Guy Buesnel**

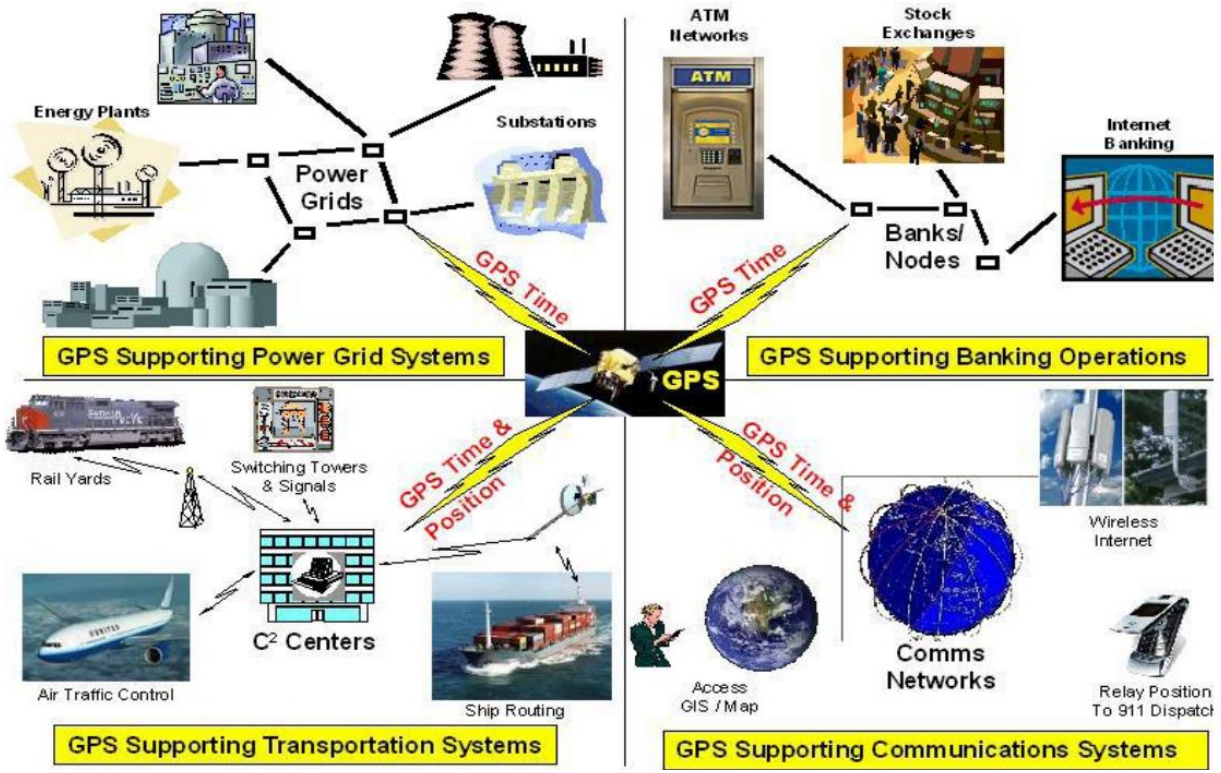
ITSF, November 2016

www.calnexsol.com
www.spirent.com

Introduction

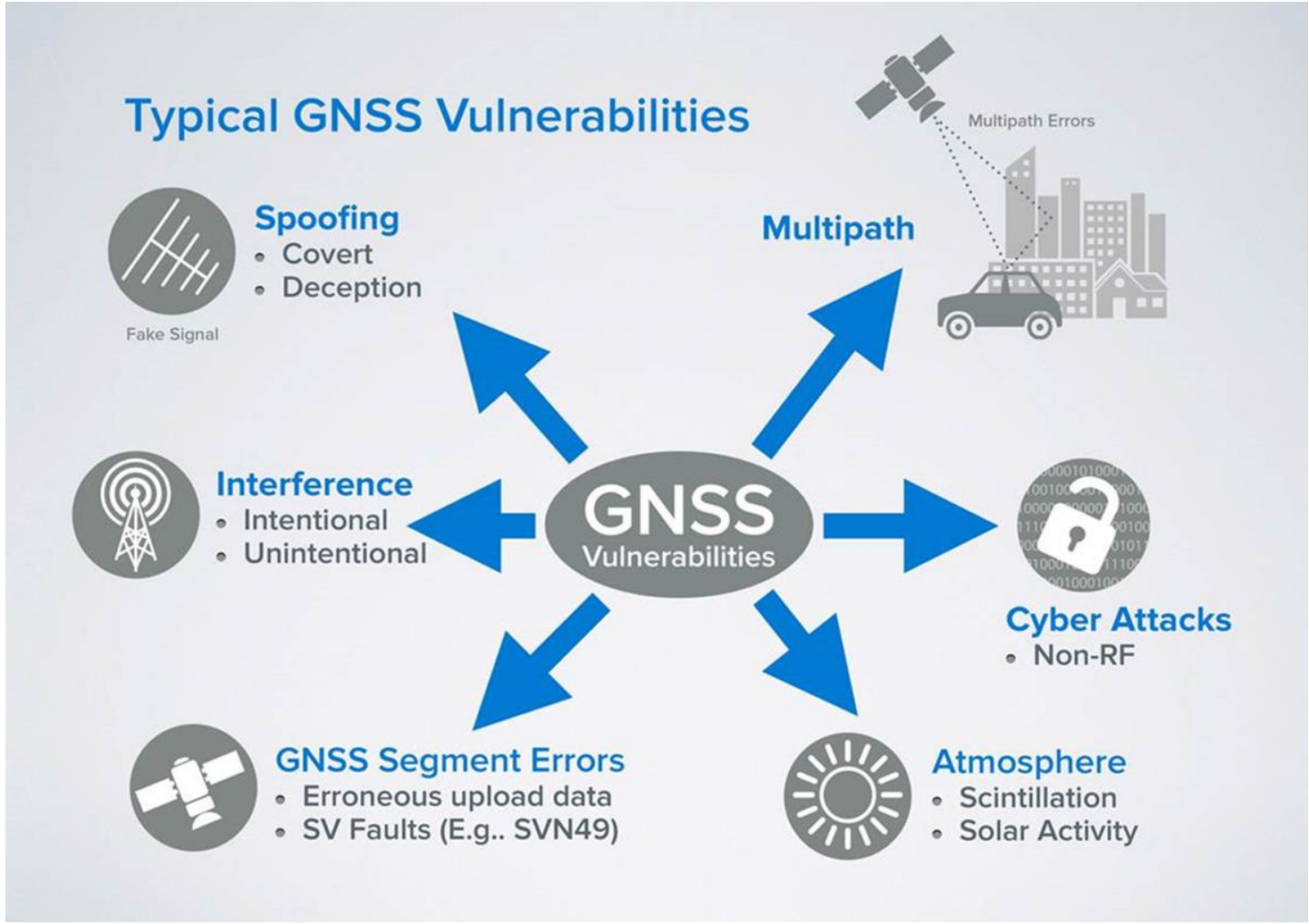
Dependence on GPS timing

- US Department of Homeland Security:
  "15 of the 19 Critical Infrastructure & Key Resources Sectors have some degree of GPS timing usage"



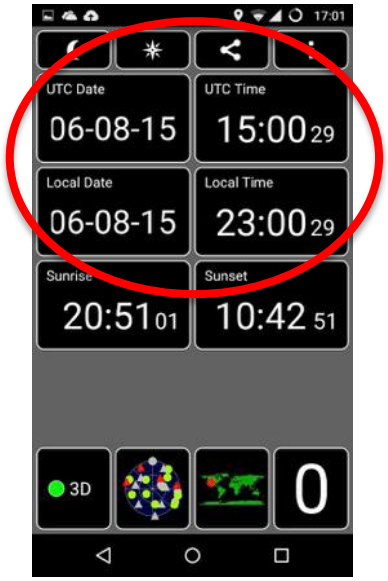
Source: http://www.gps.gov/multimedia/presentations/2012/10/USTTI

Overview of GNSS Vulnerabilities



GPS disruptions and Timing…

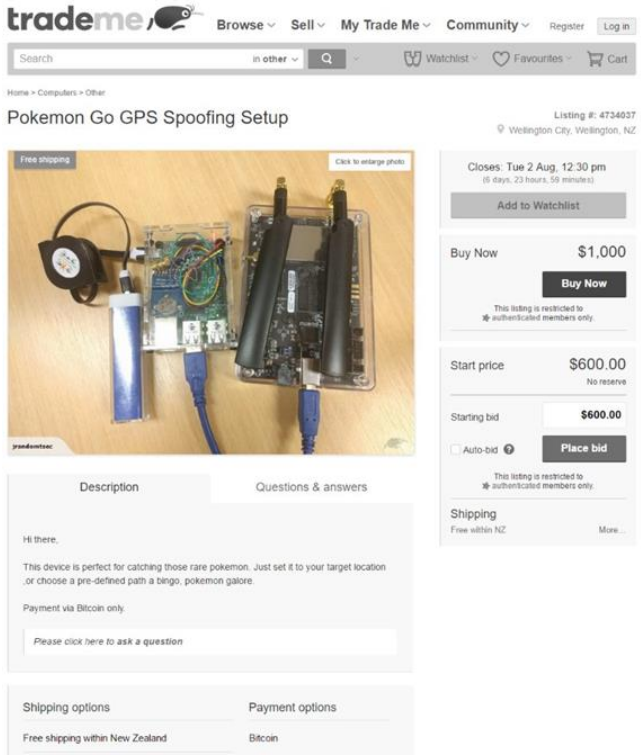
- DEFCON 23 - Huang and Yuang built a low cost SDR spoofer
- Tried it out on two brand leading smart phones…
- The Cellphone clock was spoofed to display wrong date/time with auto-calibration enabled !!
- One Cellphone ended up displaying a time and date in the future – and ended up “bricked”



First time (known) that non-GPS specialists have spoofed navigation signals successfully

GPS disruptions and Timing…

- And then in 2016 Pokemon GO suddenly spawned GPS spoofing as a mainstream attack….
  - In weeks evolved from application layer spoofing (jailbreaking operating system of mobile phone and installing a fake GPS application) – to full on meaconing and using SDR spoofing
  - Motivations: Financial Gain - sale of high value user accounts on the internet, Luring players to a location where they could be robbed



Main Types of spoofing attack

- Multi/Single channel (synchronized) with smooth deception signal
- Sinusoidal deception signal (targets more than one receiver)
  - “smart” jammer
- Jam than spoof
  - Forces receiver into acquisition mode
- Navigation data modification
- Data replay attack (Meaconing)
  - Can cheat any detection based on space data authenticity verification.

How to detect spoofing in a receiver

- Power levels
  - The spoofing signal is likely to have a noticeably higher power level
- Monitor position
  - If a fixed timing receiver starts “moving”, there’s a problem!!
- Bound and compare range rates
  - Code and carrier range rate changes will be different for a spoof signal
- Doppler shift check
  - Doppler shift is likely to be incorrect with a spoofer in a fixed location
- Verify received navigation data
  - Compare almanac/ephemeris to known data
  - Check for ‘missing/default’ navigation data
- Jump detection
  - Observable data should remain within a tolerable range, check for sudden changes

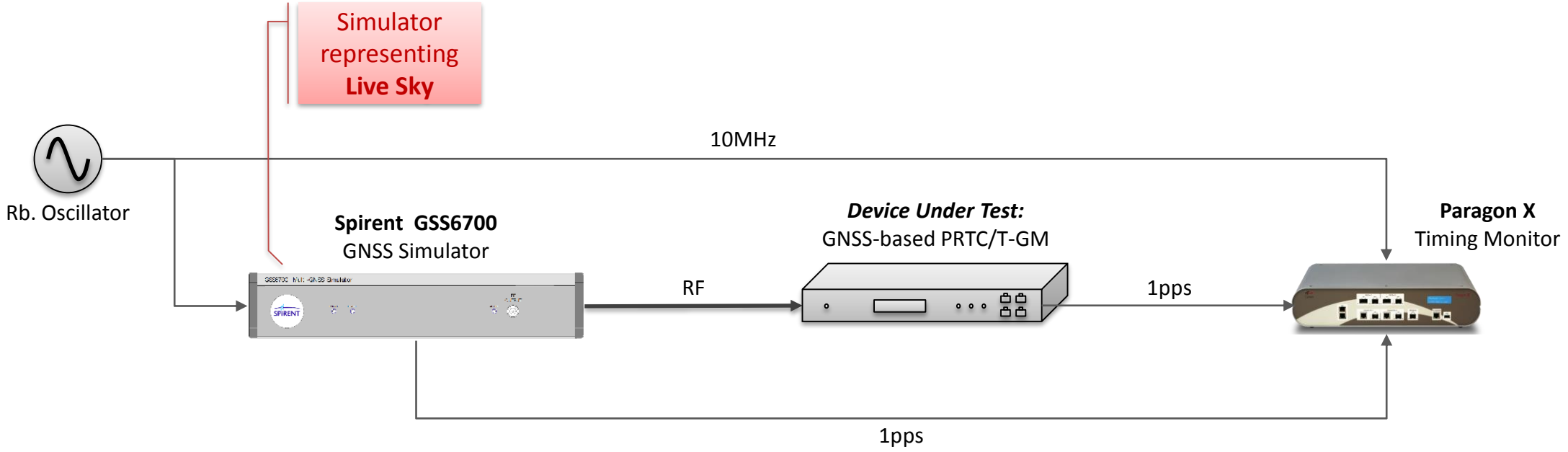
Experimental Results

Test 1: Pseudo-range Ramp

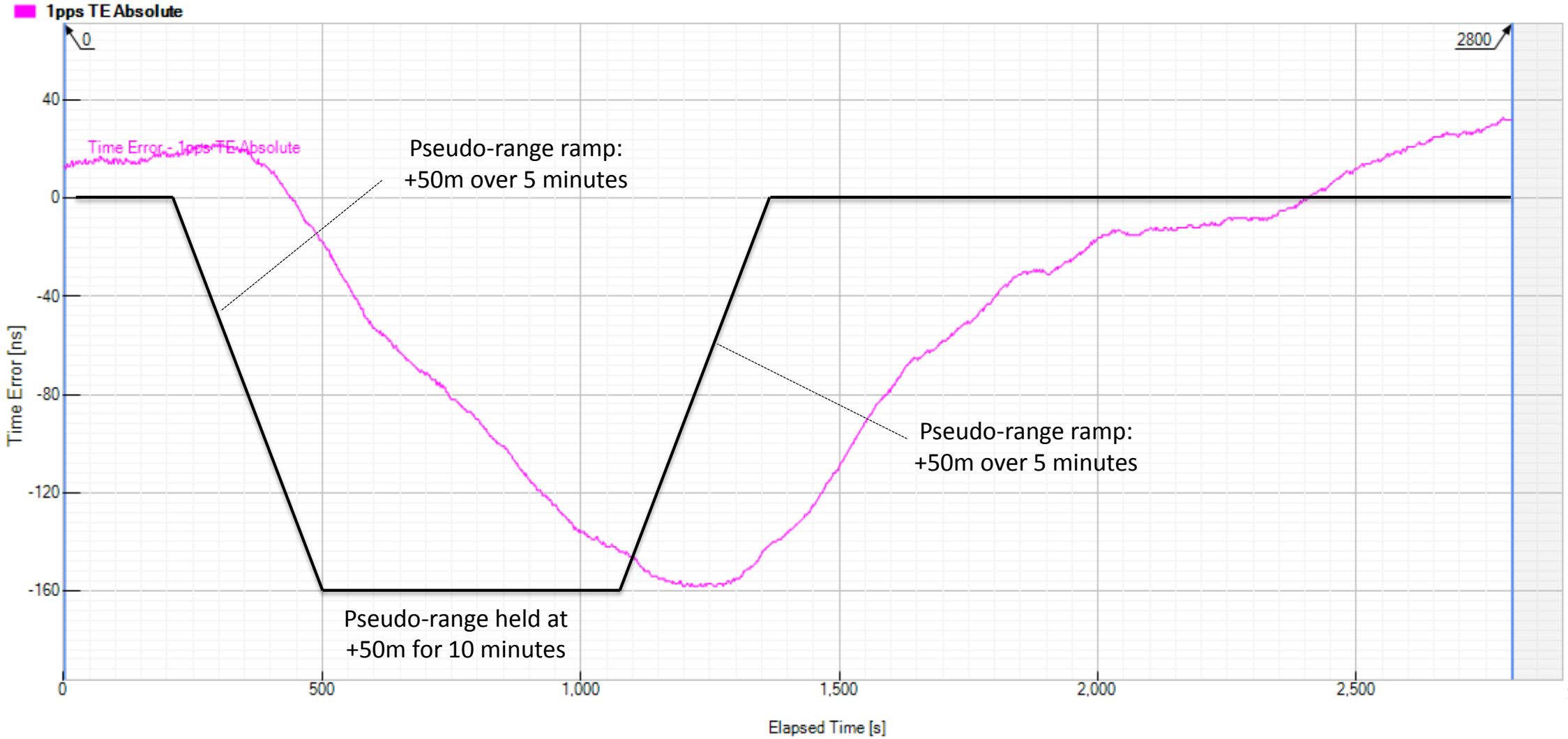
- Pseudo-range allows the receiver to calculate its distance from the satellites
- Changing the pseudo-range on one satellite will affect the receiver's position calculation
  - The satellite will appear to be either closer to or further away from the receiver than it actually is
- Changing the pseudo-range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



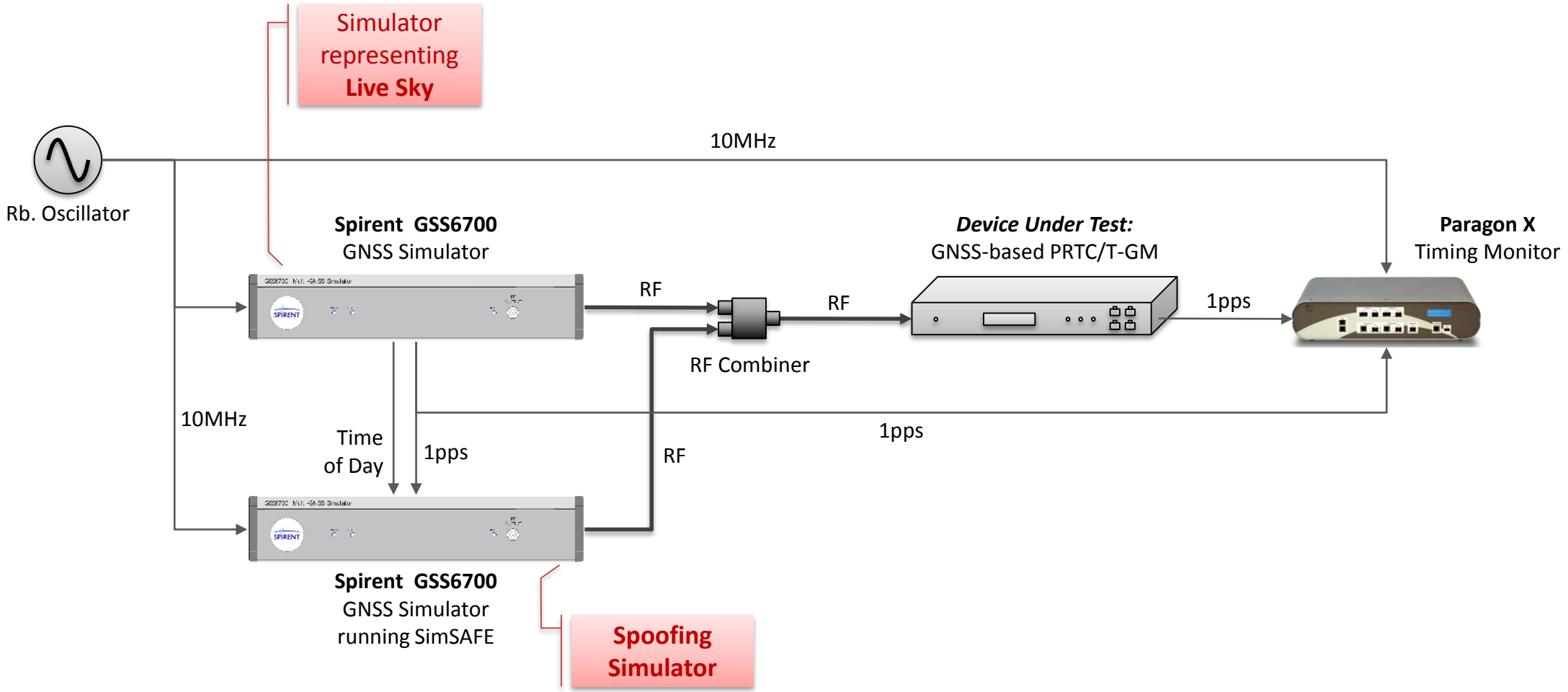
Device A: Response to Pseudo-Range Ramp



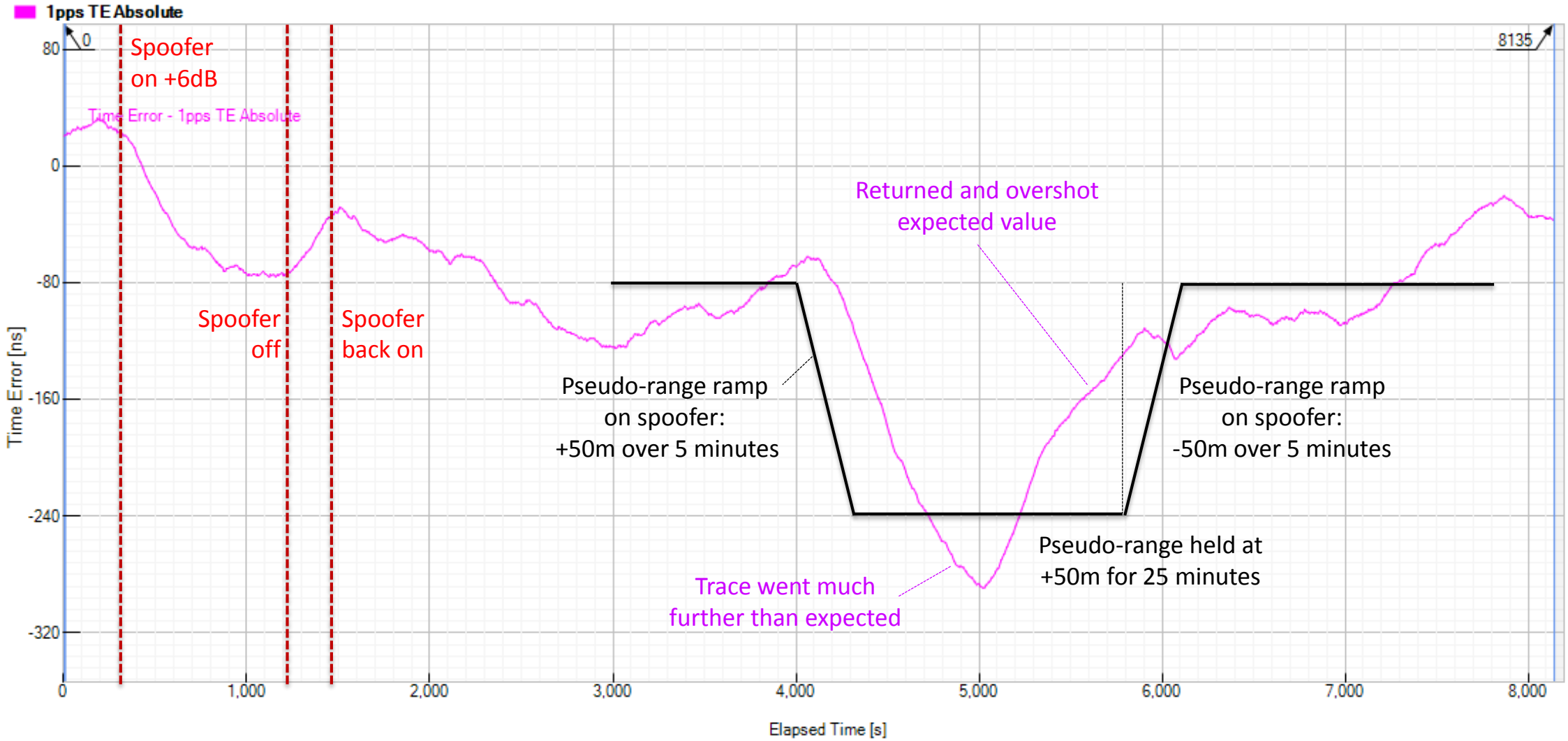
Test 2: Spoofing from Simulator

- 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

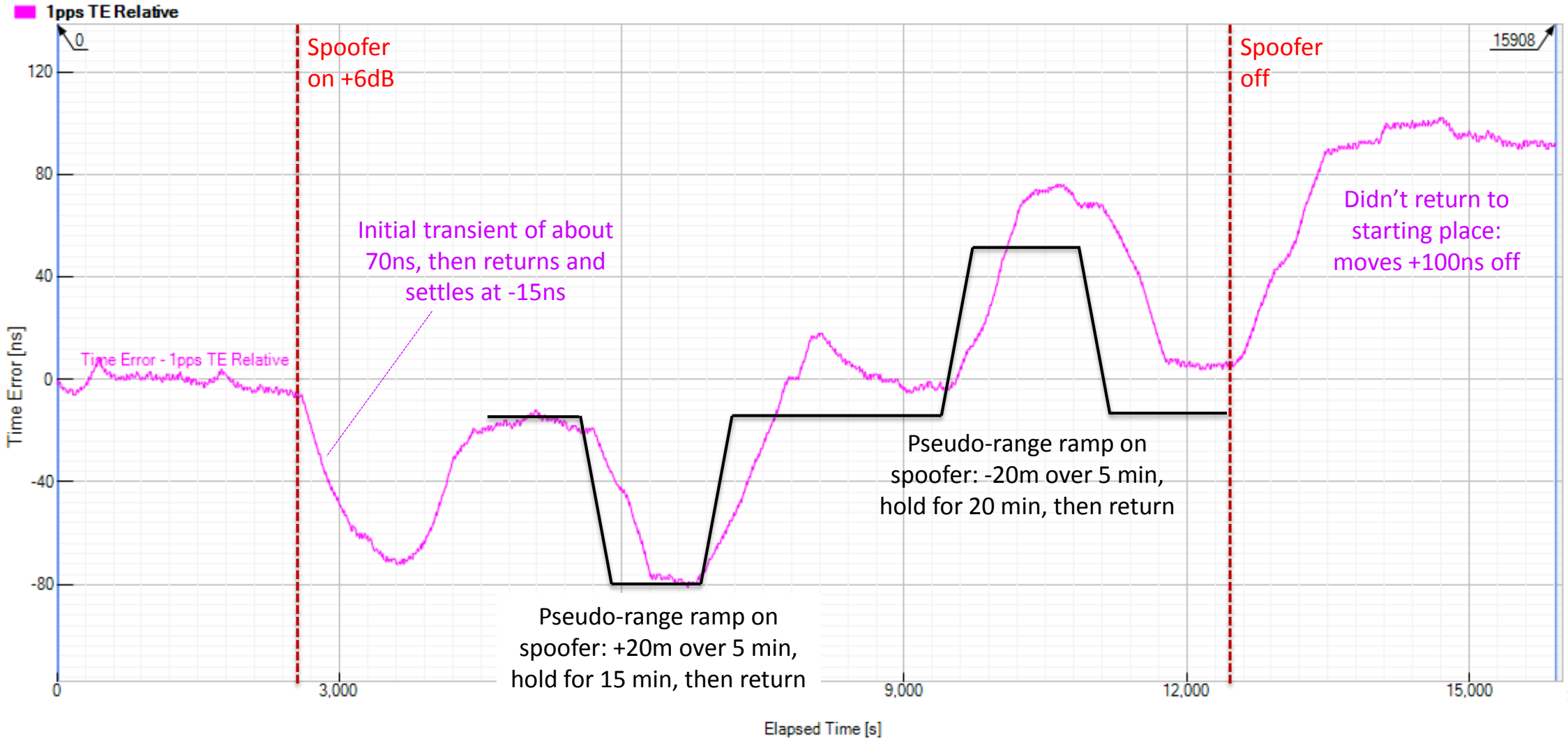
Experimental Setup 2: Spoofing from simulator



Device A: Spoofing from Simulator



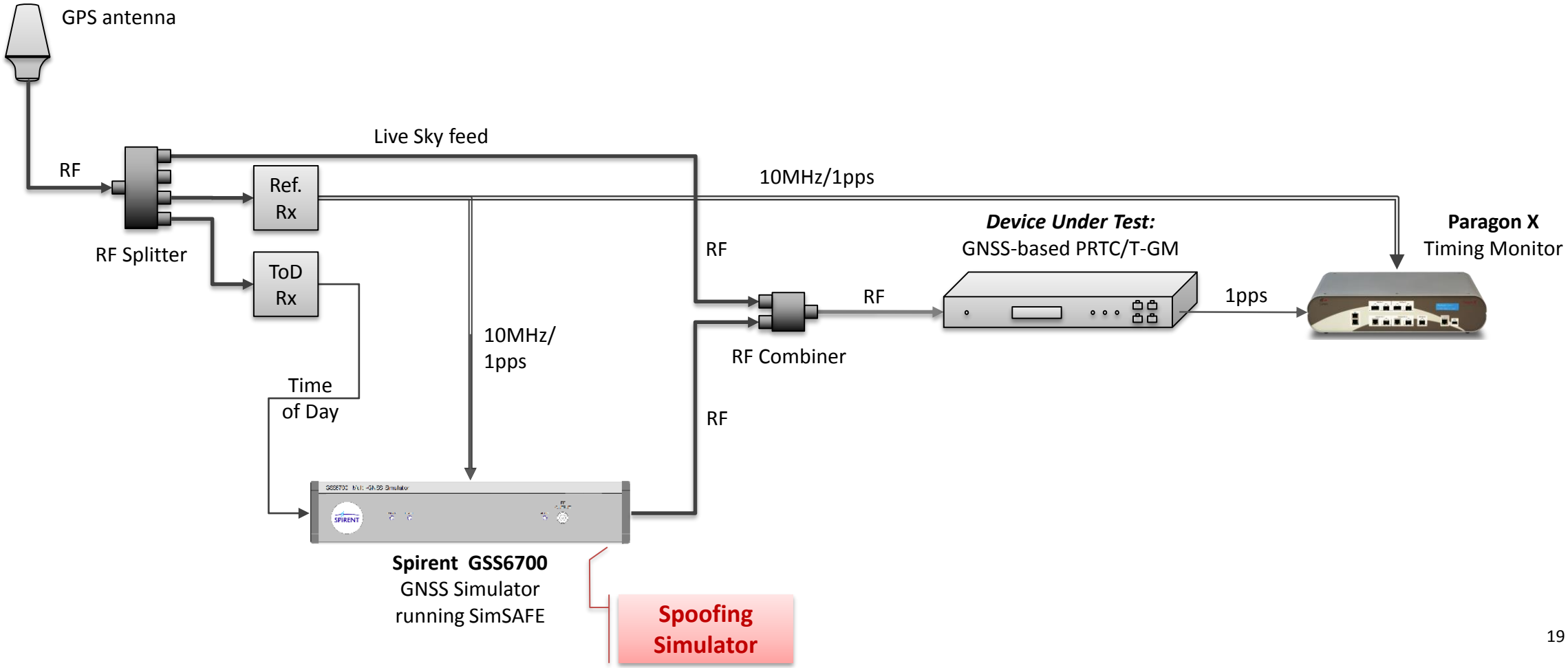
Device B: Spoofing from Simulator



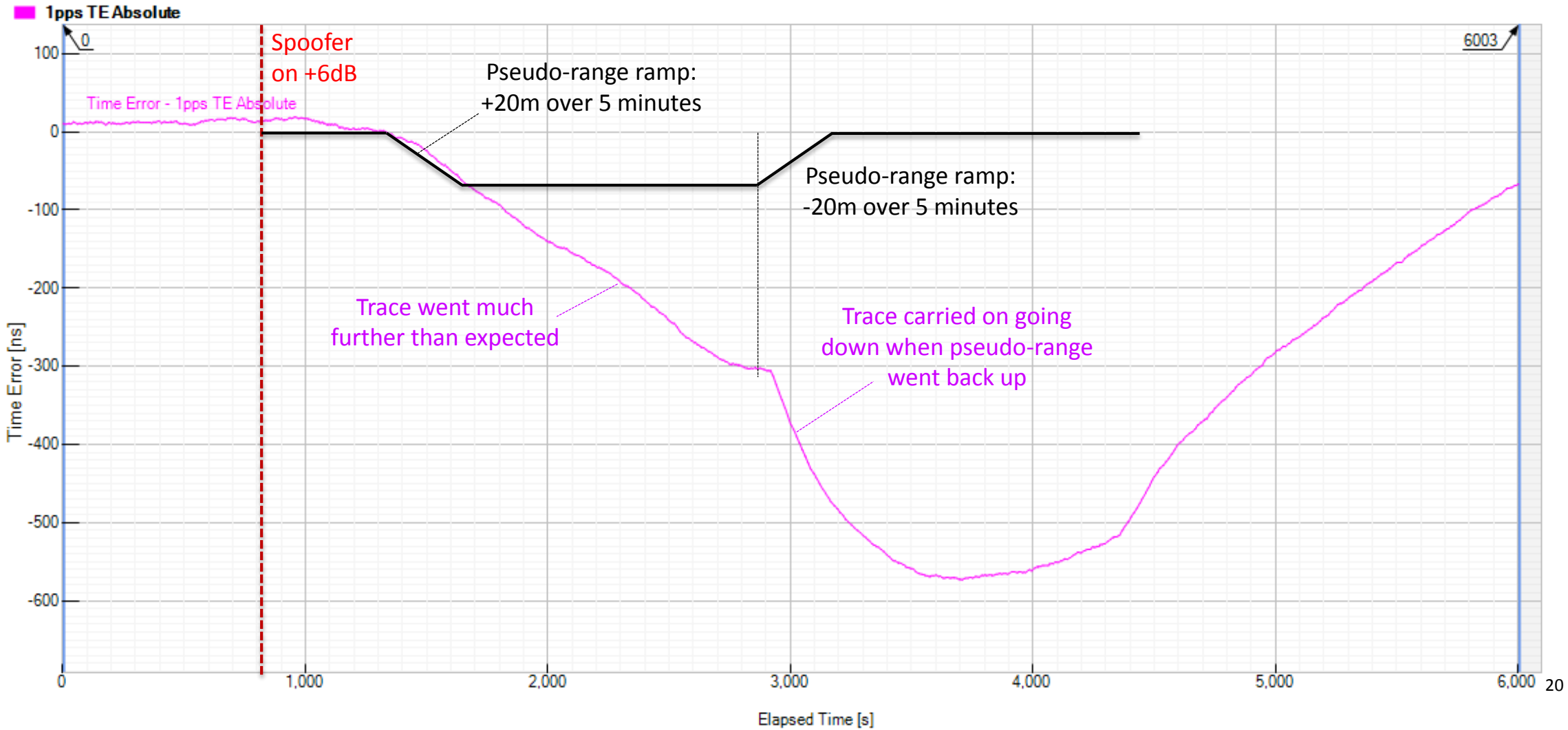
Test 3: Spoofing from Live Sky

- 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

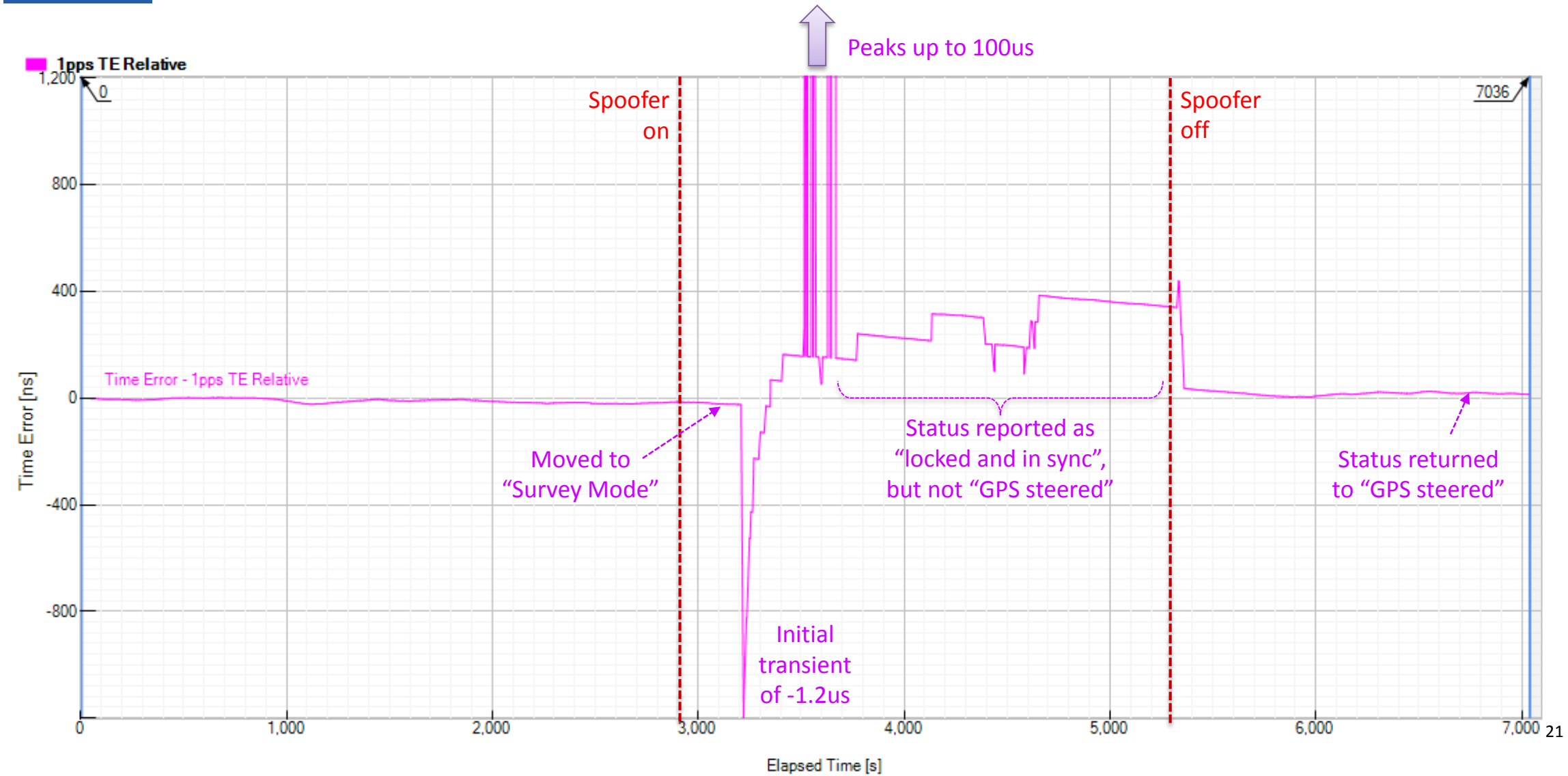
Experimental Setup 3: Spoofing from Live Sky



Device A: Spoofing from Live Sky

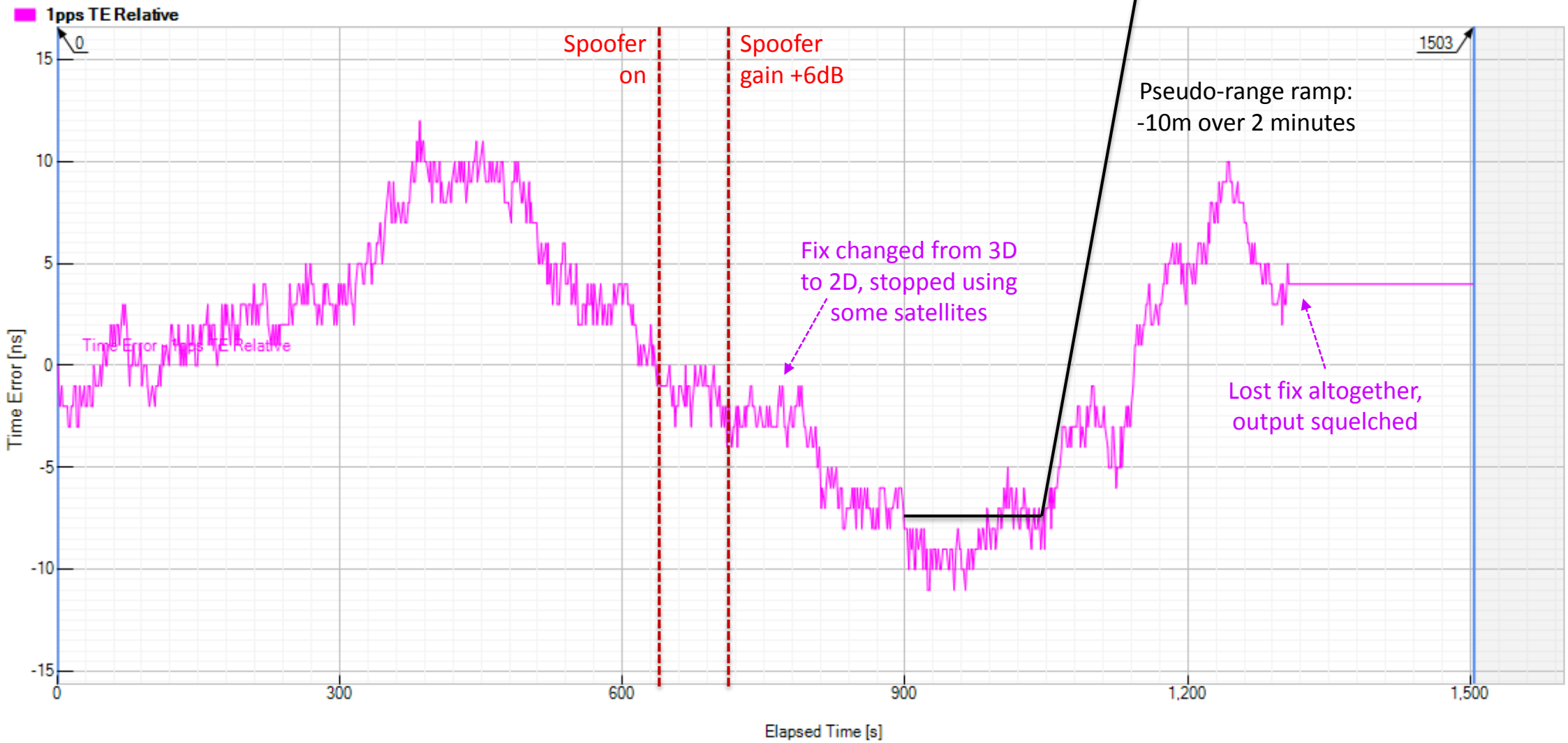


Device B: Spoofing from Live Sky

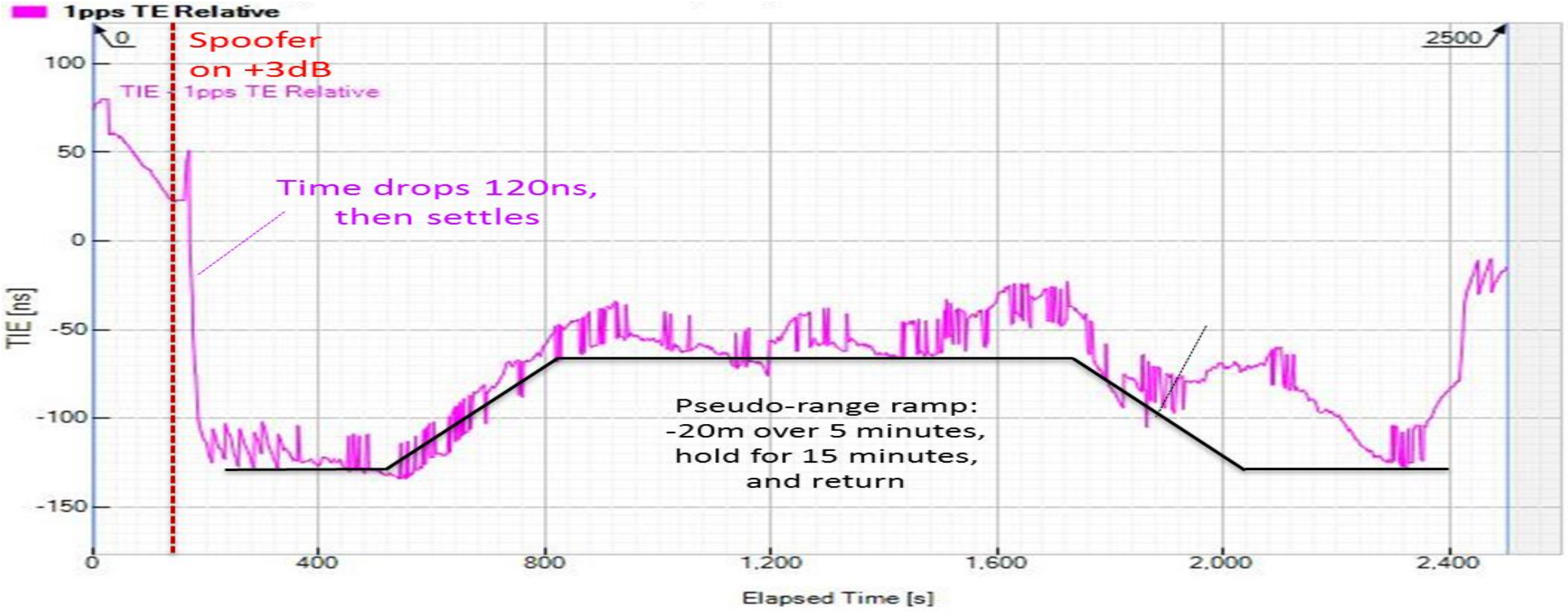


Device C: Spoofing from Live Sky

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

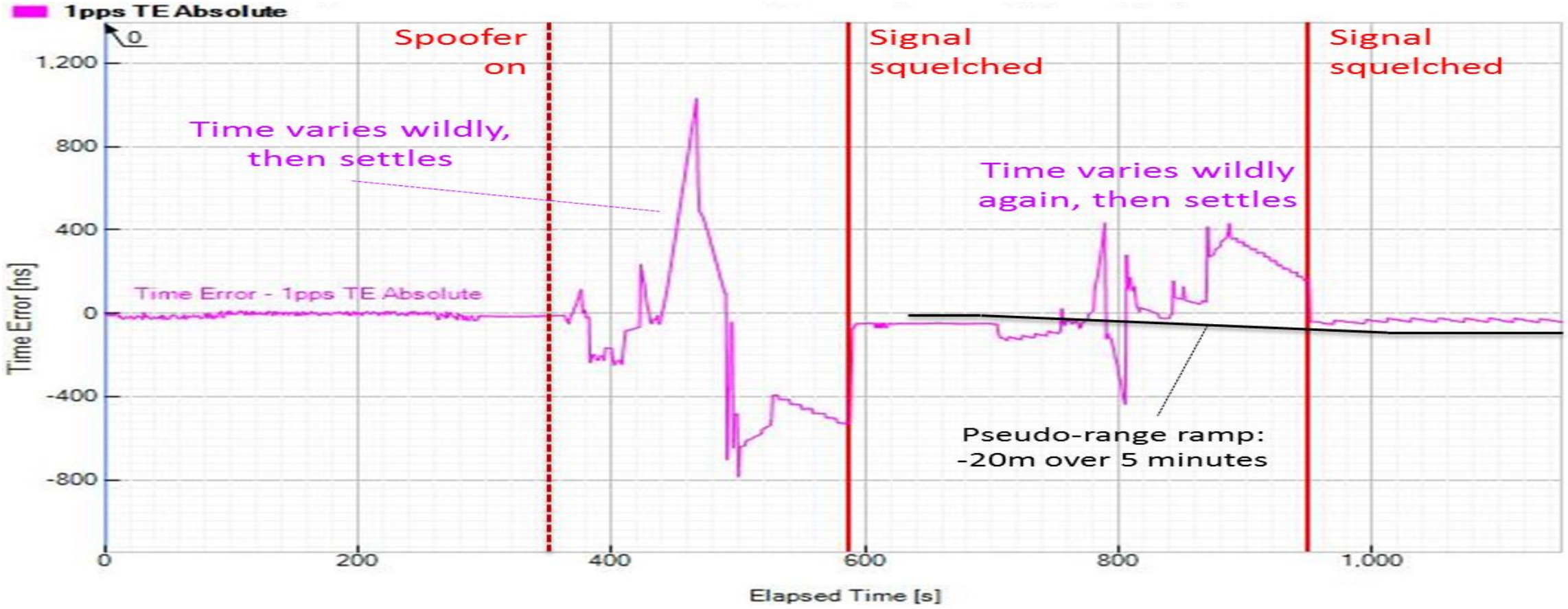


Device D: Spoofing from Live Sky



- RAIM and multipath detection turned OFF

Device D: Spoofing from Live Sky



- RAIM and multipath detection turned ON

Conclusions

- Spoofing from live-sky proved more difficult than the simulation initially
  - Once power levels (live sky and simulated) were aligned it was straightforward to tweak the simulated power level in order to take over the target receiver
- There are warning signs in the receiver that a spoofing attack is in progress
  - Good RAIM (Receiver Autonomous Integrity Monitoring) is important
  - Testing response of existing systems important – a crude attack can cause unexpected behaviour
- Know your system:
  - Risk Assessment: understand exposure to threats, likely impacts and system behaviour
  - Testing: test against realistic threat vectors to highlight unexpected system behaviour
  - Develop Defence Strategies: Use the information from test/audit to design defence strategies
- 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)

Thank you for listening!

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

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

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