Time Firewall: Securing the GNSS receivers against Spoofing/Jamming

Shemi Prazot

AccuBeat

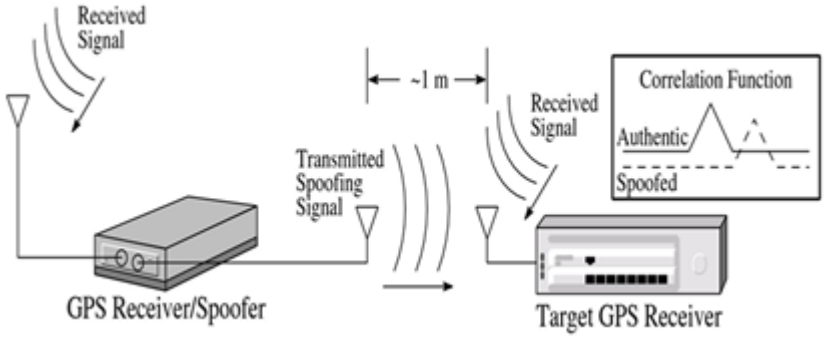
The need

- The GNSS systems are widely used for both *navigation* and *timing* in civilian infrastructures and military applications.
- Civil applications include synchronization of Communication networks, Energy companies, Financial institutions, computer networks and cellular base stations.



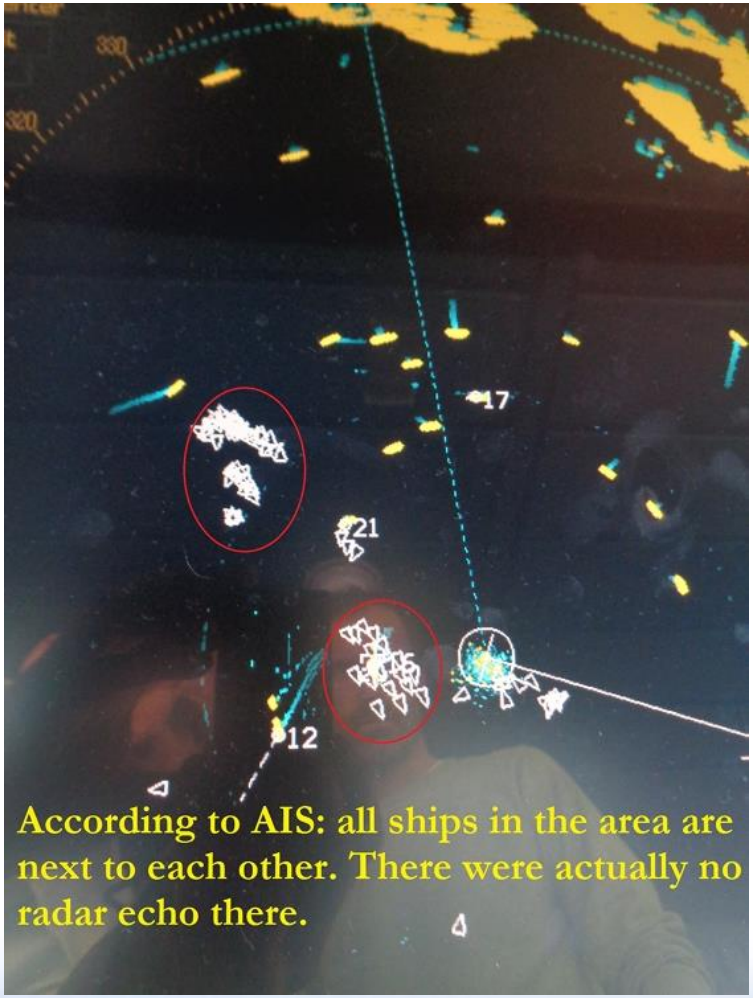
Motivation

- **The GNSS signals could be easily *jammed* or *spoofed*, intentionally or unintentionally, thereby posing a serious threat on the performance and functioning of critical systems.**



GPS spoofing using repeater which receive GPS signals and then retransmit them

GNSS spoofing: Black sea



Source: https://www.linkedin.com/pulse/mass-gps-spoofing-attack-black-sea-maritime-executive-goward/

Traditional solutions: Encrypted code

- P(Y) /M-code or similar codes
- Prevent straightforward spoofing

Disadvantages:

- Improve immunity to jamming, but fail at high enough jamming power.
- SAASM receivers are only available to authorized /military customers

Traditional solutions: multi constellations /frequencies

- Track multiple GNSS: GPS , Galileo , GLONASS, BeiDou, QZSS, IRNSS simultaneously
- Track multiple frequencies: for example: L1, L2 ,L5 of GPS

Disadvantages:

- Effective against simple spoofing.
- Force the advance spoofer to produce and transmit all possible GNSS signals simultaneously
- Require replacing existing GNSS receivers.

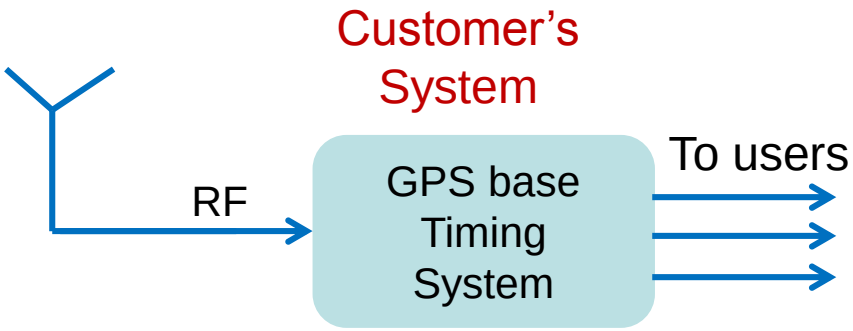
Traditional solutions: Adaptive antennas

- Multiple antenna elements are used to adaptively change the apparent receiving strength of the antenna array, creating nulls in specific direction of the jammer/spoofer
- Spoofing /jamming detection is based on power / direction algorithm

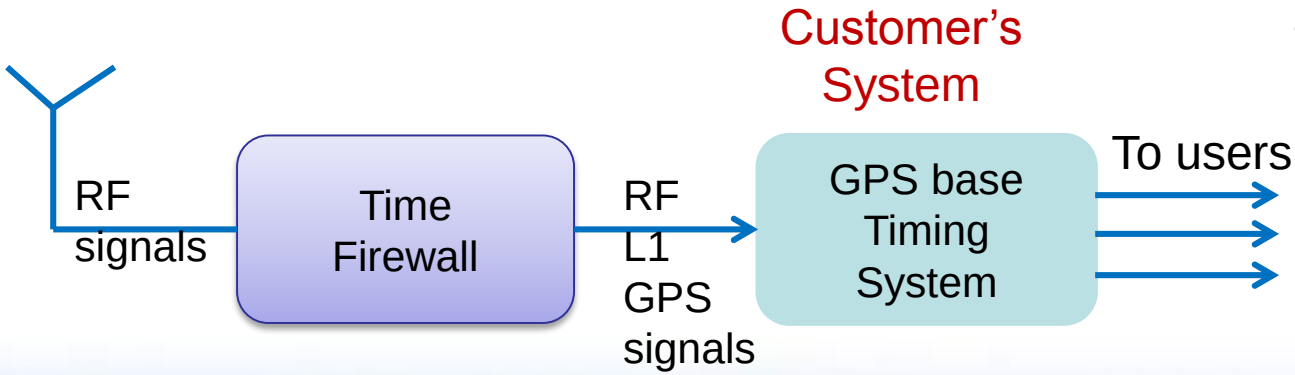
Disadvantages:

- Effective against jamming, partly effective against spoofing
- Limited by the number of treats by the number of elements
- Limited against low power spoofing from different directions (especially for stationary receivers)

Alternative solution

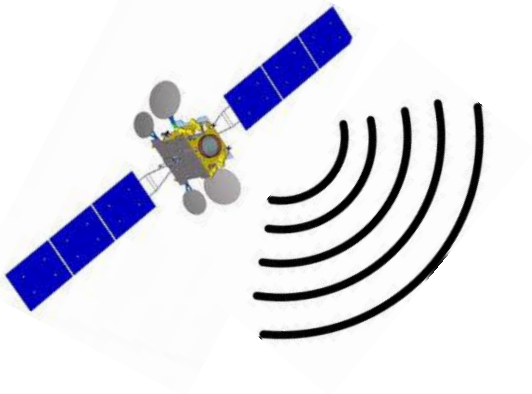


Existing system



TFW solution

TFW concept



Spoofer

Spoofing Alert

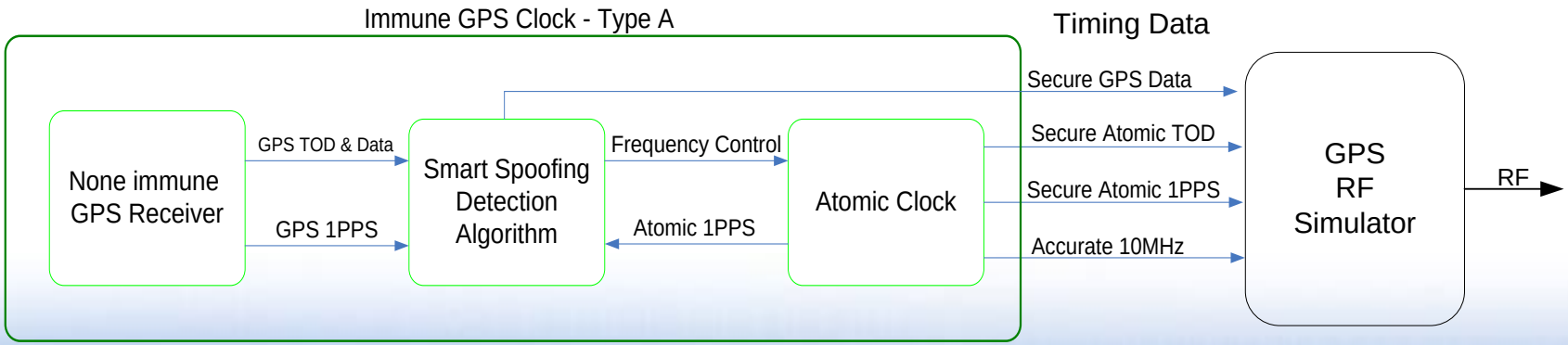
Time Fire Wall

RF signal

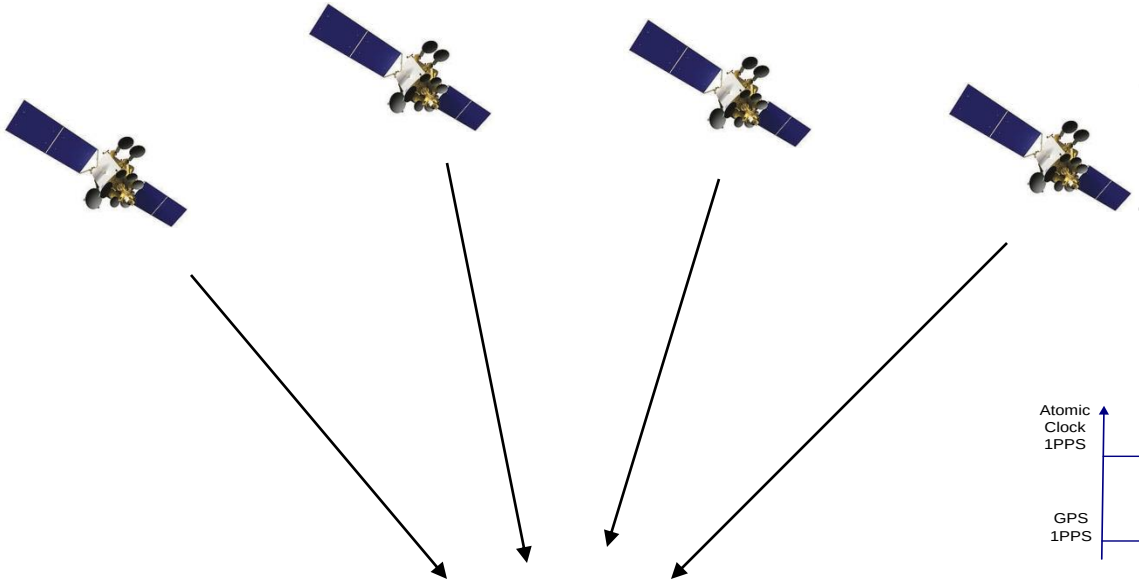
GNSS receiver
& Timing server

TFW: How it works

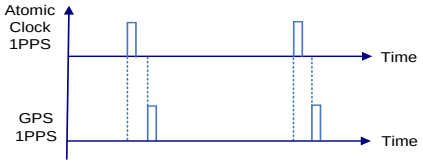
- A novel algorithm detect spoofing by comparing the received time versus the correct time from the atomic clock
- The algorithm used the validated time received from the GPS for updates of the atomic clock
- The timing and location data is delivered to the GPS simulator which translate them to RF signals



Spoofing Detection : using reference



The high stability of the atomic clock is used as reference for the spoofing detector



Spoofer

Atomic Clock

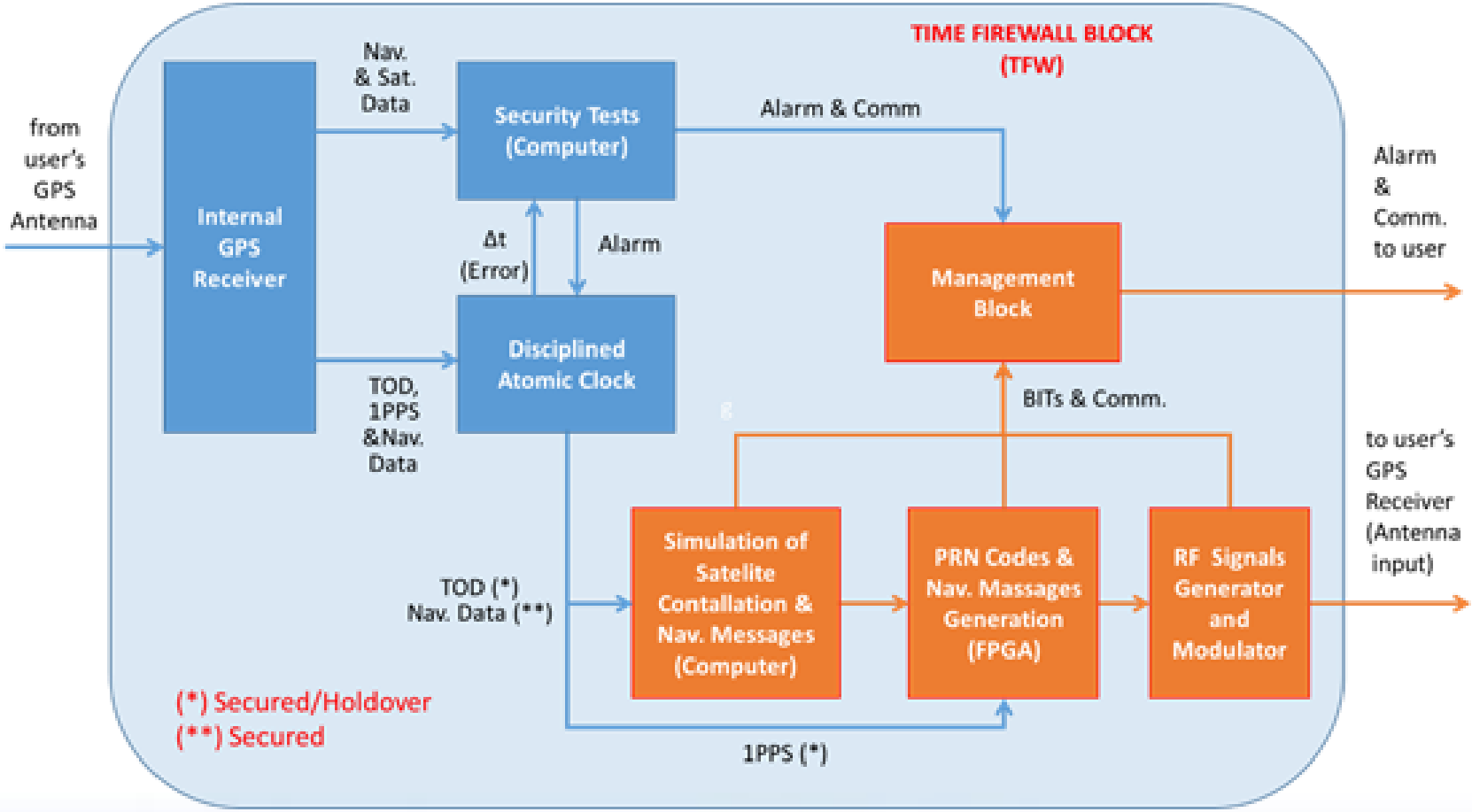
Atomic Clock 1PPS

GPS 1PPS

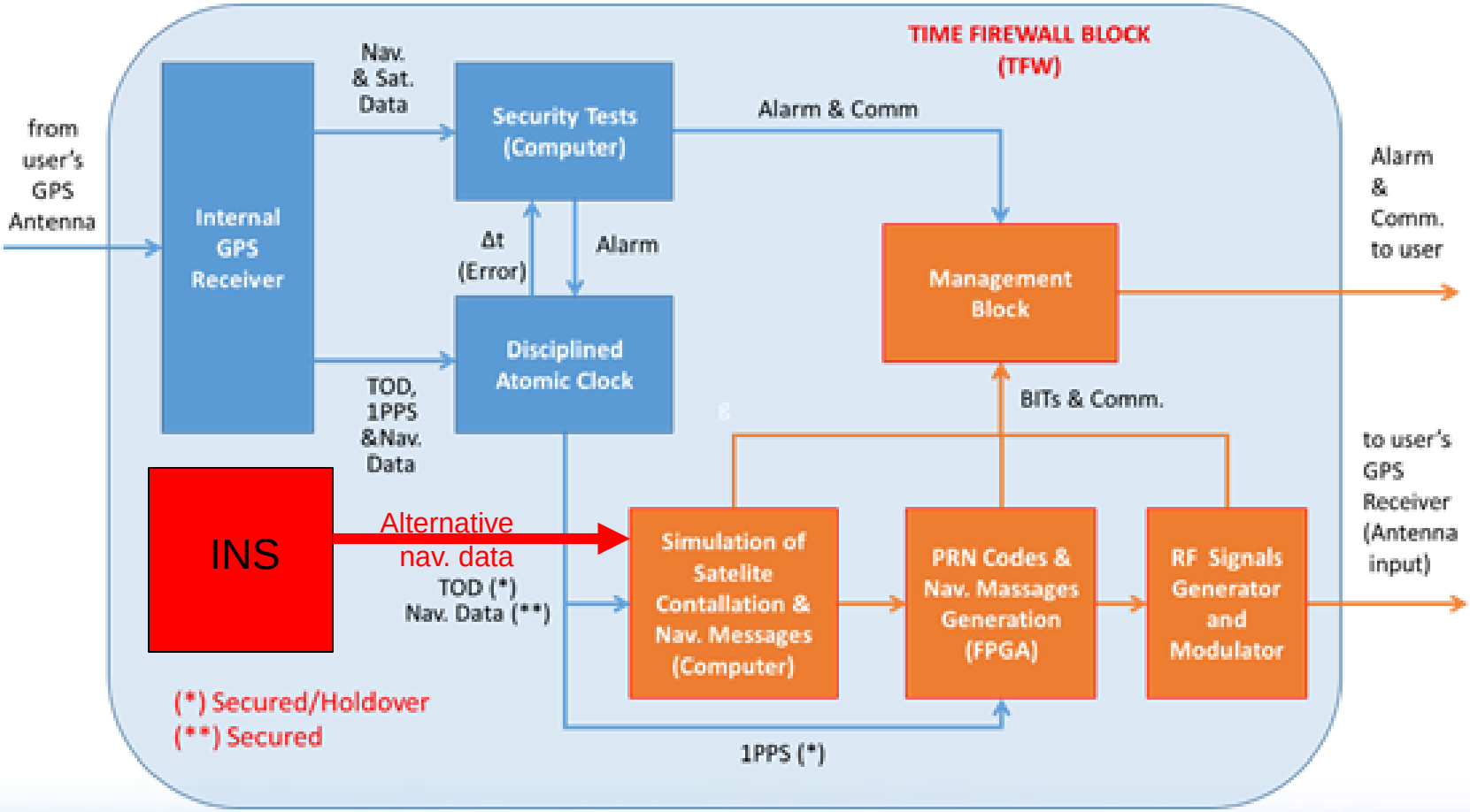
Smart Algorithm

Spoofing Alert

Time Firewall



TFW for moving systems



Rack mount Time Fire Wall

Power supply input

RF input from GPS antenna

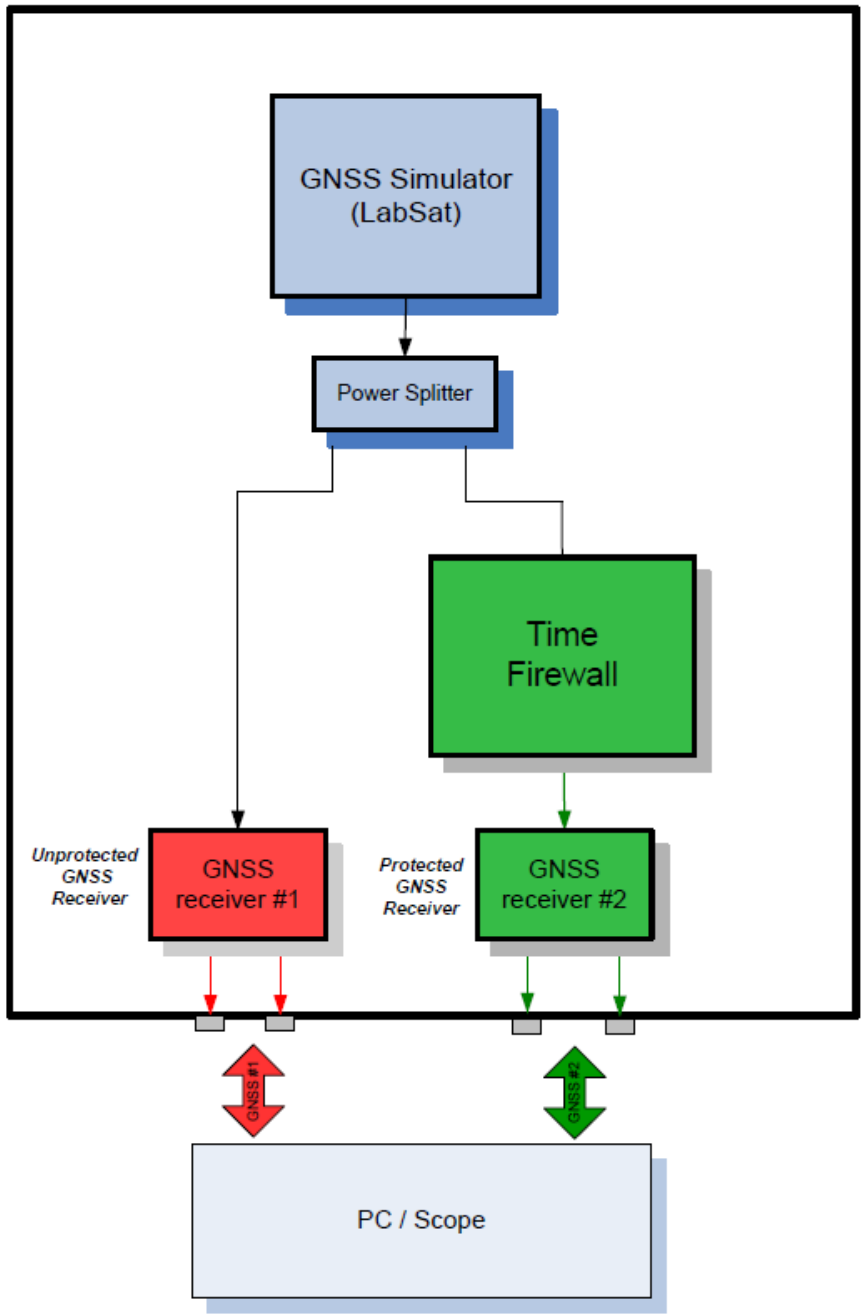
RF L1 GPS output to GPS receiver

Key Attributes of the TimeFireWall™

- ✓ *Ensures Accurate Time during a GNSS Jamming or Spoofing attack*
- ✓ *Easy to install without disruption to existing legacy equipment*
- ✓ *Remote updates with new algorithms using the LAN*
- ✓ *Patented Solution*

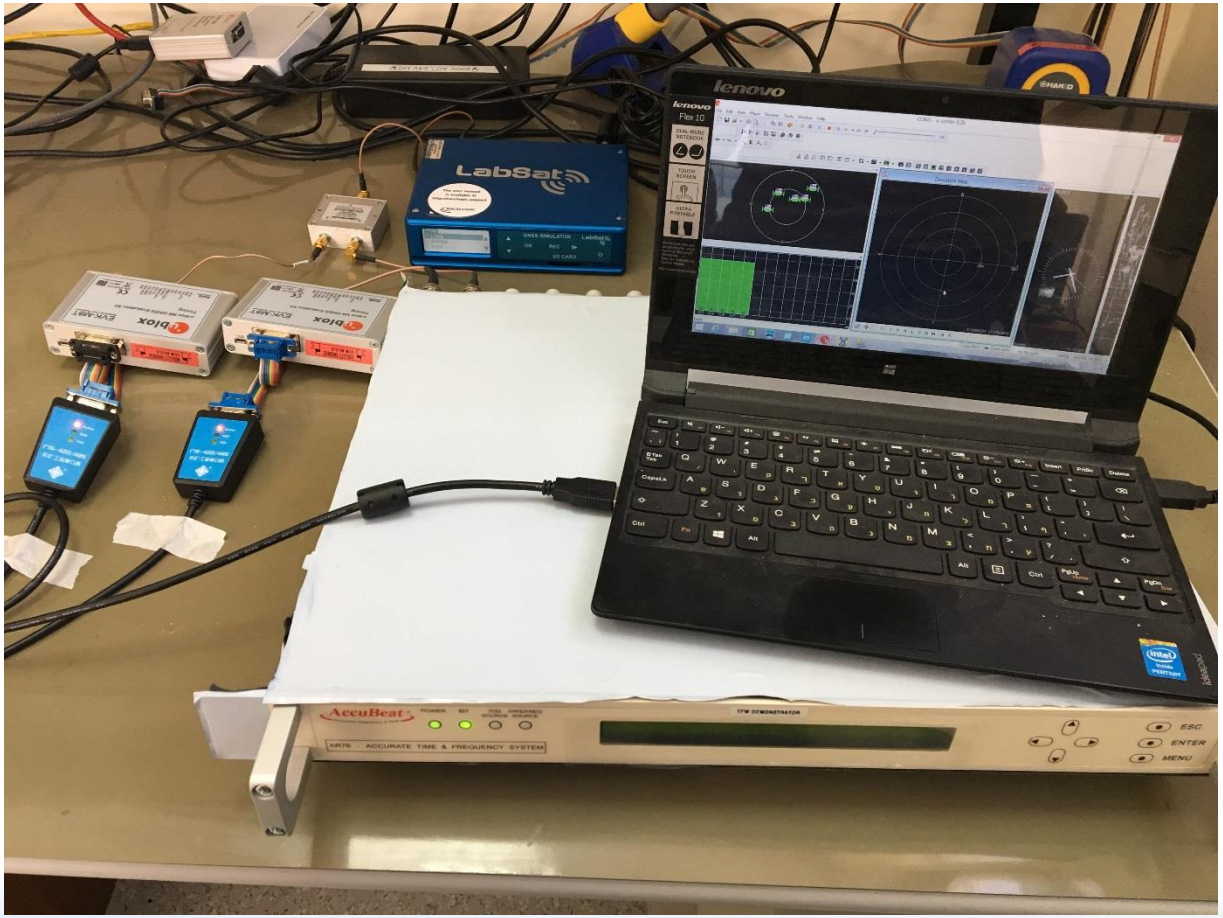
AccuBeat Ltd.
Accurate Frequency & Time

Testing setup



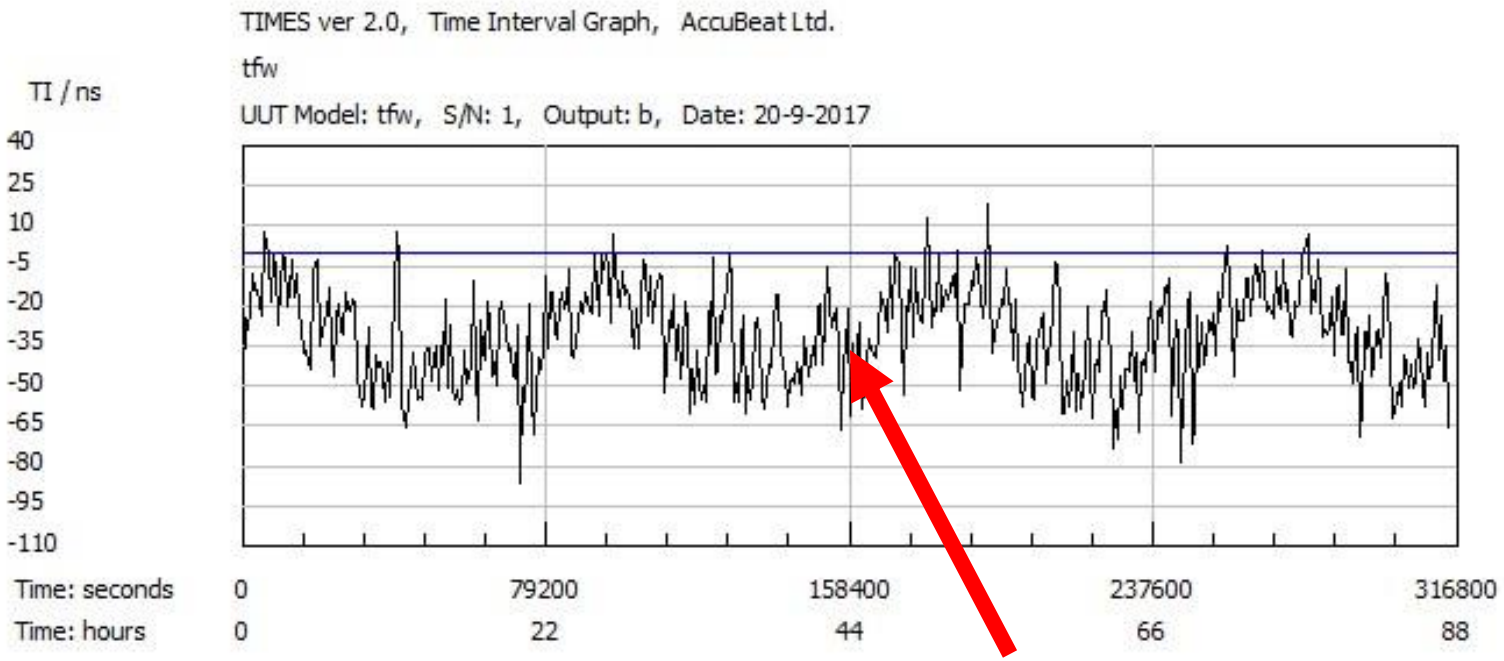
AccuBeat Ltd.
Accurate Frequency & Time

Testing setup



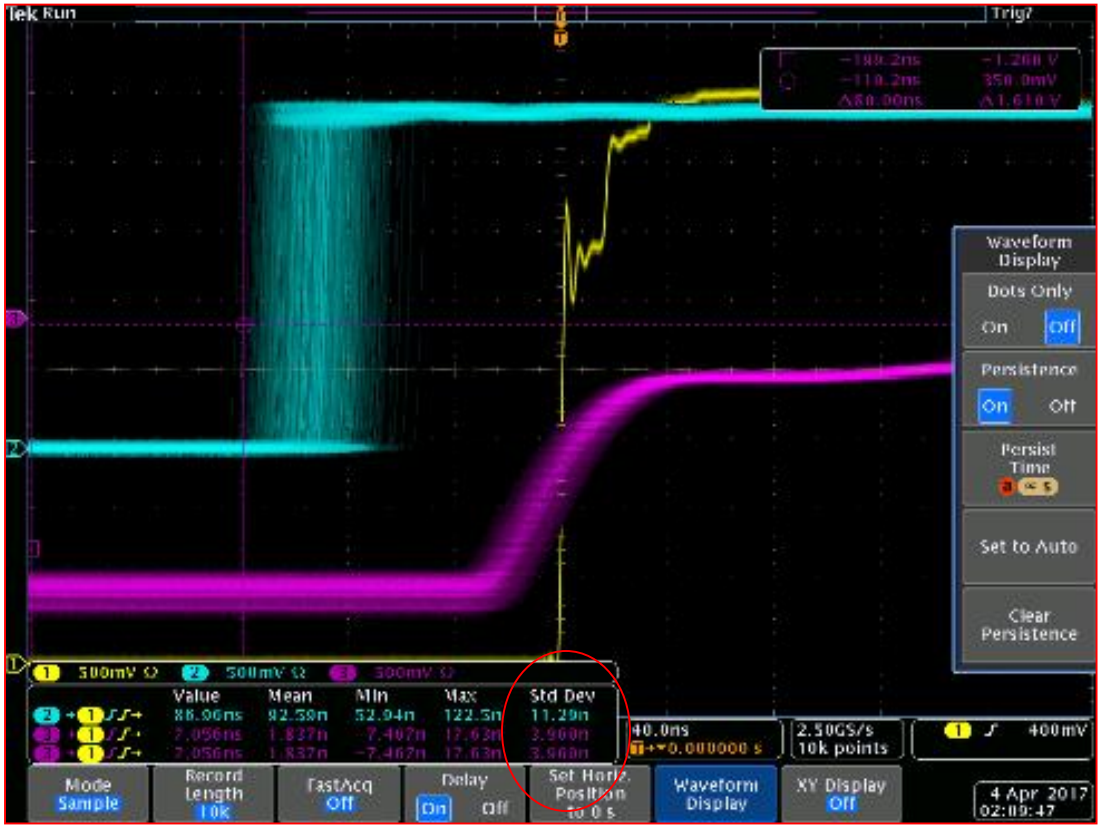
TFW: results

- 1PPS long-term stability (Peak to peak): 110ns
- 1PPS short-term stability (RMS):15ns (limited by receiver)



TFW: results

- 1PPS from 2 different customer GPS receivers which receive the SAME TFW signal
- The yellow is the 1pps reference from atomic clock
- Noise and offset are limited by the receiver, not the TFW!



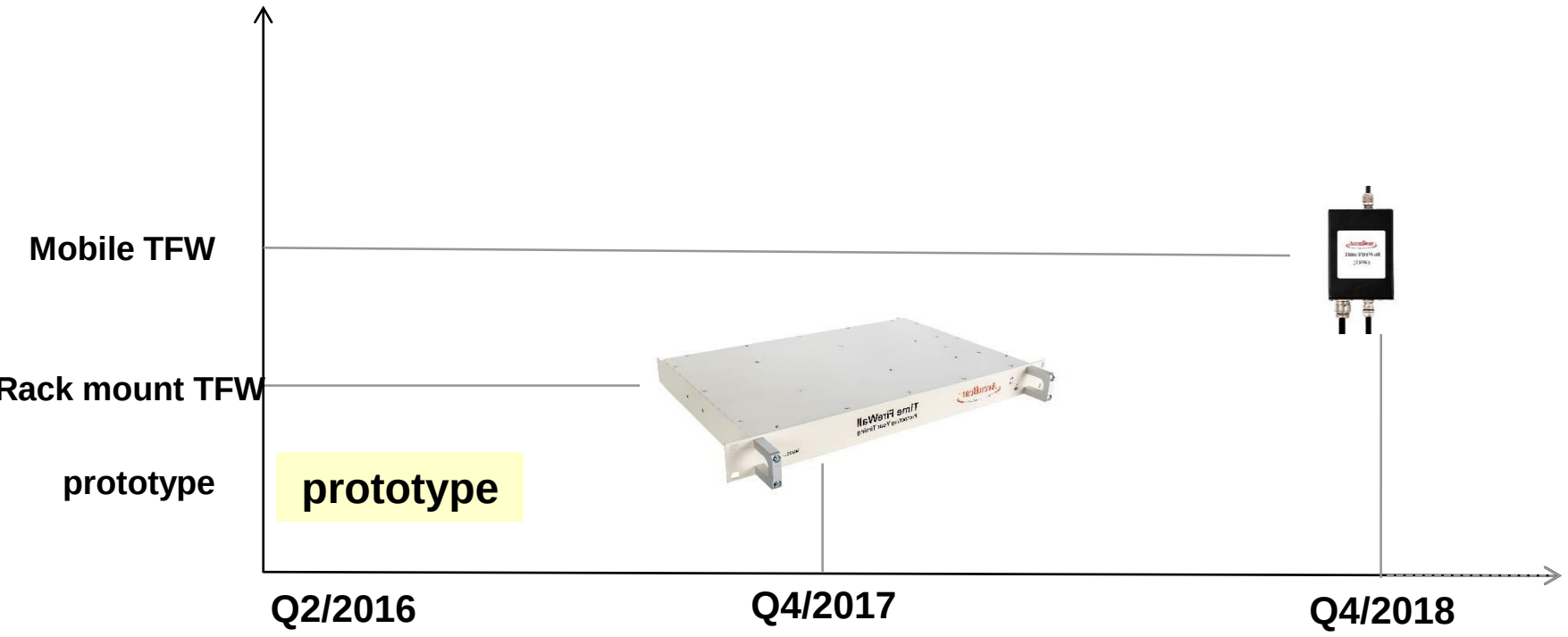
Summary

- GNSS systems can be easily jammed or spoofed
- Existing solution for civilian markets are limited
- Time FireWall can easily be inserted into a legacy timing solutions between GNSS antenna and time server
- Time FireWall output is L1 GPS RF signal with holdover of ~1us per day based on Rb clock.

AccuBeat Ltd.
Accurate Frequency & Time

Back Up

TFW Roadmap


Mobile TFW
Rack mount TFW
prototype
prototype
Q2/2016
Q4/2017
Q4/2018