GPS Vulnerability Report

Prepared by

Alliance of Telecommunications Industry Solutions

Synchronization Working Group

Presented at WSTS 2017, April 6, 2017

Marc Weiss, NIST Consultant and ATIS representative,
marcweissconsulting@gmail.com

Lee Cosart, ATIS SYNC Chair, lee.cosart@microsemi.com

Table of Contents

Precision Timing Technologies are Critical to the Operation of US Telecommunications Infrastructure

- North American telecommunications networks are critically dependent on GPS-derived timing using stationary antennas with long lifecycles. **GPS facilitates the precise synchronization of networks** operated by different network providers and provides a means of meeting national and international telecom network synchronization standards.
- **Synchronization is necessary for network operation and scalability**, including many functions of wireless technologies and the realization of network performance objectives. **GPS-based network synchronization** is critically important for location-based services, and is necessary in many North American networks to meet FCC-mandated E911 emergency location services requirements.

This report provides a North American Telecom perspective on the impact of GPS vulnerabilities to telecom networks, and provides a series of comments and recommendations for consideration by the larger timing community.

Telecom Timing Requirements: Source Requirements

Application/ Technology	Accuracy	Specification
PRTC	100 ns	[ITU-T G.8272] (Primary Reference Time Clock)
ePRTC	30 ns	[ITU-T G.8272.1] (Enhanced Primary Reference Time Clock)

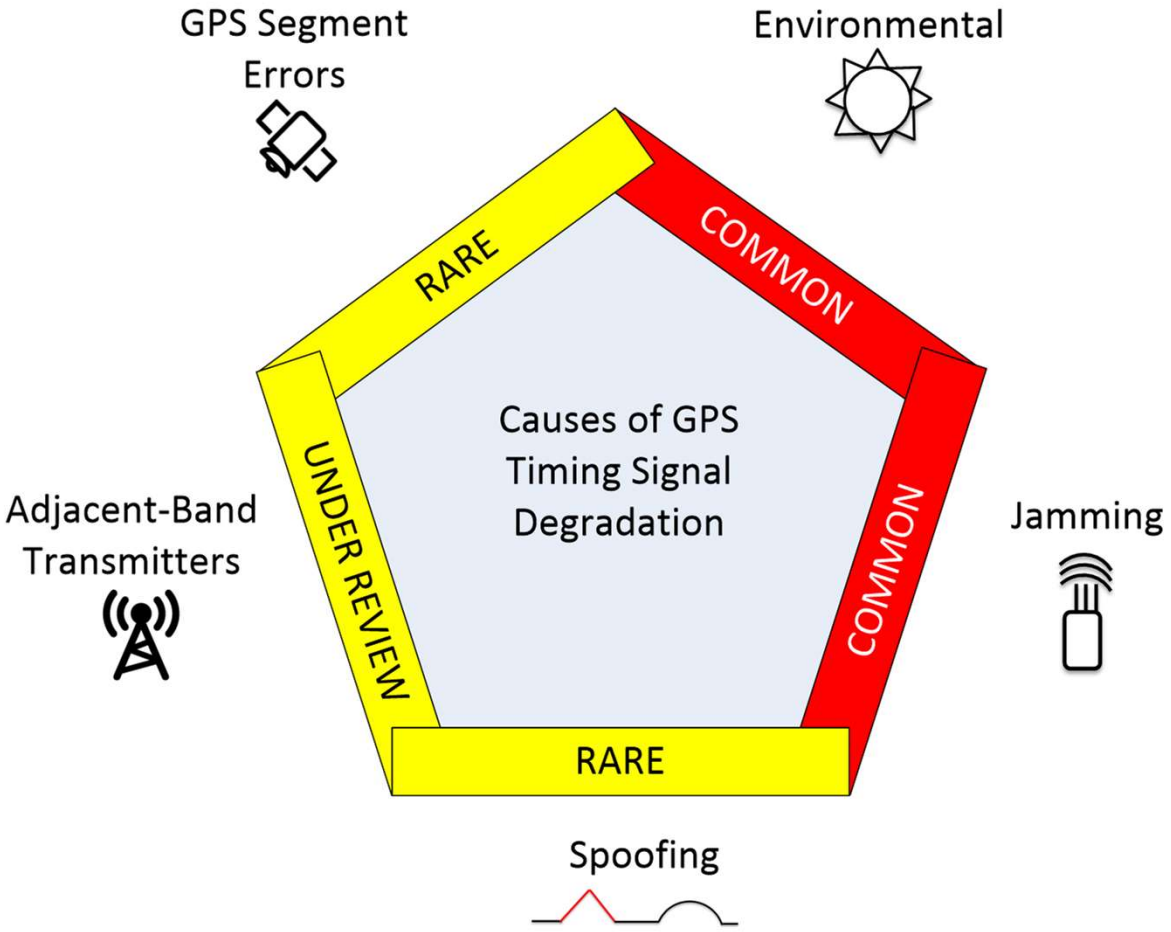
New Telecom Technologies Require Secure High-Performance Timing Sources.

Some Stringent Wireless Timing Requirements

Application/ Technology	Accuracy	Specification
CDMA2000	3 µs	[b-3GPP2 C.S0002] section 1.3; [b-3GPP2 C.S0010] section 4.2.1.1
TD-SCDMA	3 µs	[b-3GPP TS 25.123] section 7.2
LTE-TDD (home-area)	3 µs	[b-3GPP TS 36.133] section 7.4.2; [b-3GPP TR 36.922] section 6.4.1.2
WCDMA-TDD	2.5 µs	[b-3GPP TS 25.402] sections 6.1.2 and 6.1.2.1
WiMAX (downlink)	1.428 µs	[b-IEEE 802.16] table 6-160, section 8.4.13.4
WiMAX (base station)	1 µs	[b-WMF T23-001], section 4.2.2
LTE MBSFN	1 µs	Under study

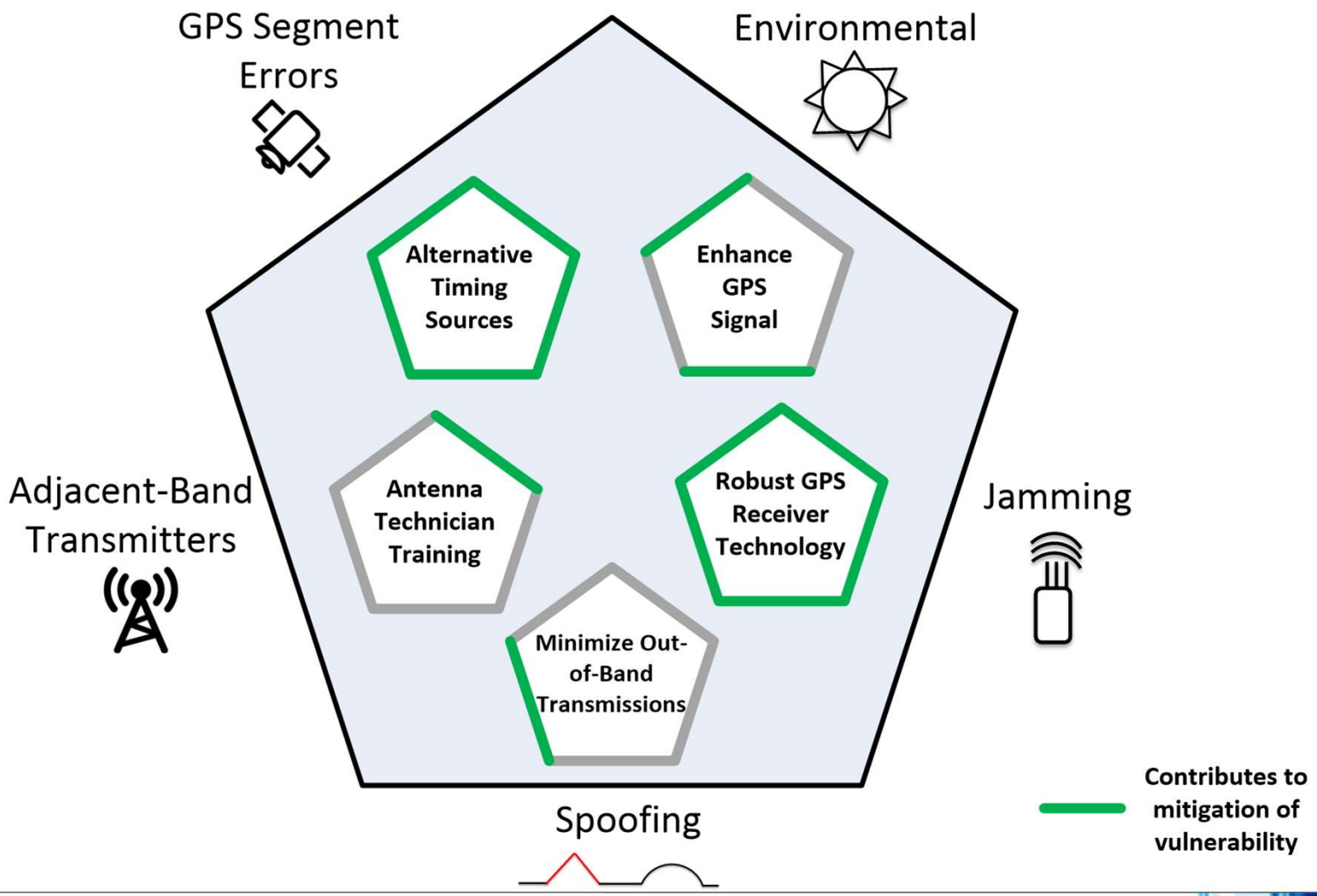
New Telecom Technologies Require Secure High-Performance Timing Sources.

Known GPS Vulnerabilities to Telecom



Identified Candidate Mitigation Strategies

Each has significant challenges associated with implementation



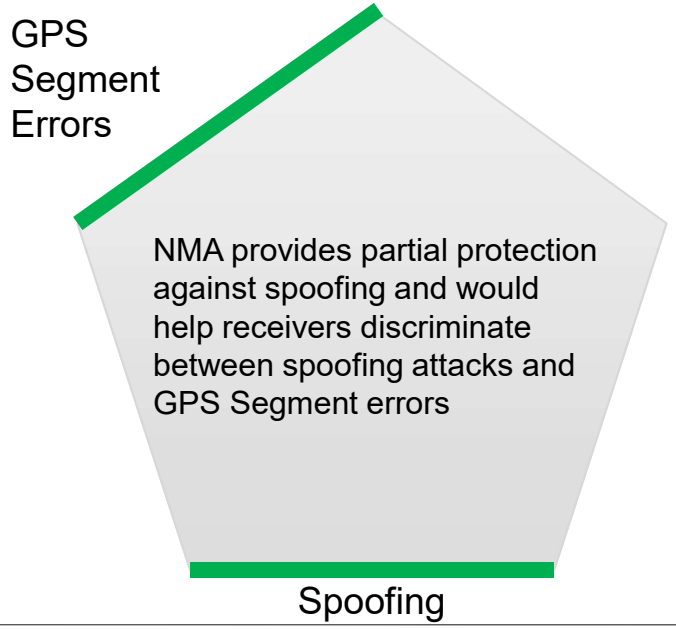
Summary of known vulnerabilities and their potential impacts to telecom

Degradation Source	Examples Observed Today	Frequency of Occurrence	Candidate Mitigation Strategies
RF interference	Nuisance jammers, unintentional emissions into the GPS band	Common	More robust GPS receiver technology, alternative timing sources
Jamming attack	High-powered jamming	Rare	Alternative timing sources, holdover
GPS Spoofing	"In the Wild" Spoofing observed at DEF CON 23/24; GPS-SDR-Sim	Rare	More robust GPS receiver technology, GPS enhancement, alternative timing sources
GPS system anomalies	2016 UTC offset error,	Rare	Alternative timing sources
Licensed adjacent band transmitters	No	N/A	More robust GPS receiver technology, alternative timing sources, minimize out-of-band emissions from the licensed adjacent band transmitters
Site setup and environmental factors	GPS antenna installations, multipath, tropospheric impacts, scintillation, solar weather	Common	Improve training of antenna installation technicians, alternative timing sources

ATIS SYNC asks for Further Study of GPS Navigation Message Authentication

SYNC Recommendations

- SYNC recommends that the US government agencies responsible for GPS consider adding signal-side security features, such as the Navigation Message Authentication (NMA) that the Galileo system has incorporated in their design, to the L2C, and L5 Modernized Civil Signals to enable a possible mitigation strategy against spoofing attacks on civil GPS signals. Signal-side protections such as NMA may be adopted in future GPS receivers used by GPS-dependent critical infrastructure. The Sector Coordinating Council representing the civil signal user community should poll users of civil signals for their level of interest in NMA on the modernized civil signals.



Licensed Adjacent Band Transmitters

SYNC Recommendations

- The telecommunications industry supports the efforts of the Federal Communications Commission to maximize the bandwidth available for wireless services, but it cannot support these efforts at the expense of degrading existing network operations.
- Given the critical nature of communications networks and the support that these networks provide for other critical infrastructure services, **ATIS SYNC believes that it is crucial to consider how signals in adjacent bands may impact this sector** and recommends that test plans for this complex testing be reviewed by neutral parties before any agency makes a decision to change the use of bands adjacent to GPS signals, to avoid any impact to voice and data services on existing and future networks.

Alternative PNT Systems should be developed and implemented in the United States

SYNC Recommendations

- An eLoran system (or equivalent such as WWVB) should be developed and implemented in the U.S. to provide a near-term alternative to GPS for the telecom system and other critical infrastructure.
  - Capable of providing UTC-traceable time to < 100 ns
  - Extremely robust against intentional and unintentional RF interference
  - Extremely robust against signal spoofing due to required power levels
  - Robust against environmental factors that GPS receivers are susceptible to
  - Mature and proven technology
  - Indoor reception
- Terrestrial Beacons – SYNC notes that it is technologically feasible to develop a very high precision timing reference based on terrestrial beacons
- A mature example of a timing singal from communications satellites is the Satellite Time and Location (STL) signal broadcast over the Iridium constellation

Multi-GNSS may be critical to enable resilient telecom infrastructure

SYNC Recommendations

- SYNC supports and encourages the FCC Communications, Security, and Interoperability Council to recommend simplification of use of foreign GNSS as alternative timing sources for FCC licensed transmitters.

Dialogue in the Timing Community

SYNC Recommendations

- The US government agencies responsible for NIST and USNO should continue to empower scientists and engineers, particularly with timing expertise, to work cooperatively with SYNC on GPS vulnerability and back up issues. This would provide opportunities for the agency scientists and engineers to share their technical views and jointly develop solutions that industry can use.
- All work in ATIS standards committees, including SYNC, is contribution driven. SYNC encourages carrier and equipment supplier participation in ATIS SYNC.
- If agency representatives are available, SYNC would participate in a periodic dialog to share information with the US government agencies on issues related to GPS vulnerability mitigation and GPS augmentation.

Unique Issues Associated with Testing Precision Timing Receivers for Adjacent Band Interference

SYNC Recommendations

- The major difference for testing between a timing receiver and a navigation receiver is that the stability of the delay through the antenna and receiver is critical for a precision timing receiver.
- Timing requirements for telecom are becoming increasingly stringent.
- Examples of variables to account for include:
  - KPI's other than C/N0 should be measured. In particular, the GPS and UTC time produced by a receiver should be measured
  - Some mitigation methods for jamming, spoofing, and adjacent band transmitters may introduce variable delay paths as a function of environmental conditions (e.g. temperature variation)

Conclusions

- The ATIS SYNC committee represents the timing issues of the North American telecom networks.
- North American telecommunications networks are critically dependent on GPS-derived timing using stationary antennas. Future networks will likely require even tighter timing constraints.
- Alternatives to GPS timing for telecom all have significant limitations.
- While the telecommunications industry supports efforts to maximize the bandwidth available for wireless services, it cannot support these efforts at the expense of degrading existing network operations. Hence any proposed adjacent band signal must be tested to ensure it does not degrade network functions.

ATIS SYNC Encourages Open Testing of Precision Timing GPS receivers

SYNC Recommendations

- ATIS SYNC encourages open GPS Vulnerability testing where the precision timing GPS receiver type is represented.
- Any impact of an adjacent band transmission on this specific type of GPS receiver should be measured for timing accuracy versus both industry specifications (e.g. for LTE wireless networks) and other requirements (e.g. E911 positioning requirements).
- Measurement of C/N_0 alone does not sufficiently characterize timing degradation that may be introduced by adjacent band transmissions and their mitigation techniques on timing receivers.
- Raw test results and post-processed data should be made available.
- Test plans should be available for review and comment by the general interested public.
- The statistical and deterministic uncertainty of measurements should be established.

Unique Issues Associated with Testing Precision Timing Receivers for Adjacent Band Interference

SYNC Recommendations

- The major difference for testing between a timing receiver and a navigation receiver is that the stability of the delay through the antenna and receiver is critical for a precision timing receiver.
- Timing requirements for telecom are becoming increasingly stringent. Granting a license to transmit in a band adjacent to GPS should consider the impact on emerging timing requirements.
  - For example, testing of the change in the delay with temperature should be done for any antenna/receiver system, over an appropriate temperature range.
  - Though using a sharp cutoff in a pass band may allow a navigation receiver to function in the presence of an adjacent band signal, such a filter may, if not properly designed, add unacceptable delay instability over time or temperature for a precision timing receiver, particularly for new and newly developing requirements.