ATIS-0900005

GPS Vulnerability

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

ATIS-0900005, *GPS Vulnerability*

Is an ATIS Standard developed by the **Synchronization (SYNC)** Committee.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-0900005

ATIS Technical Report on

GPS Vulnerability

Alliance for Telecommunications Industry Solutions

Approved September 7, 2017

Abstract

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

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Synchronization (SYNC) Committee engages industry expertise to develop and recommend standards and technical reports for synchronization technologies. SYNC is committed to proactive engagement with national, regional, and international standards development organizations and forums that share its scope of work. ATIS SYNC focuses on those functions and characteristics necessary to define and establish synchronization between networks and also on areas concerned with network phase/time characteristics that require theoretical, analytical, and empirical investigations to ensure that standards and reports meet the highest norms of technical integrity and completeness. ATIS SYNC also prepares recommendations on related subject matter under consideration in various North American and international standards organizations.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, SYNC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time it approved this document, SYNC, which is responsible for its development, had the following leadership:

L. Cosart, SYNC Chair and Technical Editor (Microsemi)
M. Calabro, SYNC Vice Chair and Technical Editor (Booz Allen Hamilton)
M. Weiss, Technical Editor (NIST)

Table of Contents

1 Scope 1
2 References 1
3 Definitions, Acronyms, & Abbreviations 2
3.1 Definitions 3
3.2 Acronyms & Abbreviations 3
4 Introduction 4
5 Known GPS Vulnerabilities 6
6 GPS Performance & Synchronization Requirements 10
7 GPS Vulnerability Mitigation & Alternatives to GPS Timing 14
8 Recommendations to Assure Time for Telecom 17

Table of Figures

Figure 4.1 – Known GPS vulnerabilities to telecom 6
Figure 5.1 – Critical infrastructure disruptions from 2009 U.S. Navy accidental jamming event 8
Figure 5.2 – Illustration of spoofing a boat's position 9
Figure 5.3 – Plot showing how the anomaly event impacted one GPS timing receiver 10
Figure 7.1 – Identified candidate mitigation strategies 14
Figure 7.2 – 10's of ns held in a 3-month measurement over commercial fiber (150 km link) . 15

Table of Tables

Table 5.1 – Summary of known vulnerabilities and their potential impacts to telecom 7
Table 6.1 – Time and phase end application synchronization requirements 11

ATIS Technical Report on –

GPS Vulnerability

1 Scope

The telecommunications industry requires reliable delivery of precision timing signals to enable operation of cellular networks. This report notes the telecommunications industry's dependence on the Global Positioning System (GPS) and highlights GPS vulnerabilities of concern to the communications sector.

2 References

At the time of publication of this technical report, the editions of the documents listed below were valid. Documents are subject to revision, and readers of this document are encouraged to refer to the most recent editions of the documents indicated below.

[1] ITU-T Recommendation G.8271, *Time and phase synchronization aspects of packet networks*.[1]

[2] ITU-T Recommendation G.8272, *Timing characteristics of primary reference time clocks*.[2]

[3] ITU-T Recommendation G.8272.1, *Timing characteristics of enhanced primary reference time clocks*.[3]

[4] ITU-T Recommendation J.211, *Timing interface for cable modem termination systems*.[4]

[5] IEEE Std 1588 – 2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*.[5]

[6] National Coordination Office for Space-Based Positioning, Navigation, and Timing, *Use of Foreign Satellite Navigation Signals*.[6]

[7] National Space-Based Positioning, Navigation & Timing Advisory Board Meeting Minutes, December 10-11, 2014.[7]

[8] Paige Atkins, Ron Repasi, National Telecommunications & Information Administration (NTIA)/Federal Communications Commission (FCC) *Radio Regulator Spectrum Management Perspectives & Priorities - Emerging Trends in Spectrum Efficient Technologies*, December 10, 2014.[8]

---

[1] This document is available from the International Telecommunications Union (ITU) at: < https://www.itu.int/rec/T-REC-G.8271/en >.

[2] This document is available from the ITU at: < https://www.itu.int/rec/T-REC-G.8272/en >.

[3] This document is available from the ITU at: < https://www.itu.int/rec/T-REC-G.8272.1/en >/

[4] This document is available from the ITU at: < https://www.itu.int/rec/T-REC-J.211-200611-I/en >.

[5] This document is available from the Institute of Electrical and Electronics Engineers (IEEE) at: < http://shop.ieeeusa.org >.

[6] This document is available from the National Coordination Office for Space-Based Positioning, Navigation, and Timing at: < http://www.gps.gov/spectrum/foreign/ >.

[7] This document is available from the National Space-Based Positioning, Navigation & Timing Advisory Board at: < http://www.gps.gov/governance/advisory/meetings/2014-12/minutes.pdf >

[8] This document is available from the National Telecommunications & Information Administration (NTIA)/Federal Communications Commission (FCC) at: < http://www.gps.gov/governance/advisory/meetings/2014-12/atkins-repasi.pdf >

[9] Jeff Coffed, Exelis, *The Threat of GPS Jamming – The Risk to an Information Utility*, January 2014.[9]

[10] Jeff Coffed, Harris Corporation, *The Threat of GPS Jamming – The Risk to an Information Utility*, January 2016.[10]

[11] Kang Wang, Shuhua Chen, Aimin Pan, Alibaba Group, *Time and Position Spoofing with Open Source Projects*.[11]

[12] Mark L. Psiaki, Todd E. Humphreys, *GPS Lies - Protecting GPS From Spoofers Is Critical to the Future of Navigation*, IEEE Spectrum August 2016.[12]

[13] Mark L. Psiaki, Todd E. Humphreys, *GNSS Spoofing and Detection*.[13]

[14] The Royal Academy of Engineering, *Global Navigation Space Systems: reliance and vulnerabilities*, March 2011.[14]

[15] M.A. Weiss, F.G. Ascarrunz, T. Parker, V. Zhang, X. Gao, *Effects Of Antenna Cables on GPS Timing Receivers,* 1999 Joint Meeting EFTF - IEEE IFCS.[15]

[16] Marc Weiss, Lee Cosart, James Hanssen, Jian Yao, *Precision Time Transfer using IEEE 1588 over OTN through a Commercial Optical Telecommunications Network*, ISPCS 2016 Proceedings.[16]

[17] Charles Schue, *Indoor Enhanced Loran: Demonstrating Secure Accurate Time at the NYSE*, April 19, 2016.[17]

[18] GPS World. *South Korea to build eLoran system after jamming incident*. May 3, 2016.[18]

[19] NIST, *Time Measurement and Analysis Service (TMAS).* July 13, 2017.[19]

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

Relevant definitions for topics in this technical report may be found in various ATIS, ITU-T, and ITU-R documents. These include the following:

[1] ATIS-0900101, *Synchronization Interface Standard*.[20]

---

[9] This document is available from Exelis at: < http://gpsworld.com/wp-content/uploads/2014/02/ThreatOfGPSJamming_FEB14.pdf >.

[10] This document is available from the Harris Corporation at: < https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf >.

[11] This document is available at: < https://www.blackhat.com/docs/eu-15/materials/eu-15-Kang-Is-Your-Timespace-Safe-Time-And-Position-Spoofing-Opensourcely-wp.pdf >.

[12] This article is available from the IEEE at: < http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation >.

[13] This document is available at: < https://radionavlab.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf >.

[14] This document is available from the Royal Academy of Engingeering at: < http://www.raeng.org.uk/publications/reports/global-navigation-space-systems >.

[15] This document is available at: < http://tf.boulder.nist.gov/general/pdf/1384.pdf >.

[16] This document is available from the IEEE Xplore Digital Library. < http://ieeexplore.ieee.org/Xplore/home.jsp >.

[17] This document is available at: < http://www.ursanav.com/wp-content/uploads/NYSE_Seminar_UrsaNav_19APR2016.pdf >.

[18] This document is available at: < https://www.gpsworld.com/south-korea-to-build-eloran-system-after-jamming-incident/ >.

[19] This document is available at: < https://www.nist.gov/programs-projects/time-measurement-and-analysis-service-tmas >.

[20] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at: < https://www.atis.org/docstore/product.aspx?id=25280 >.

[2] ITU-T Recommendation G.810, *Definitions and terminology for synchronization networks*.[21]

[3] ITU-T Recommendation G.8260, *Definitions and terminology for synchronization in packet networks*.[22]

[4] ITU-R Recommendation TF.686-3, *Glossary and definitions of time and frequency terms*.[23]

3.1 Definitions

3.1.1 Time accuracy: The level of agreement of the time of a clock compared to an ideal source of time such as coordinated universal time (UTC). This is specified as the magnitude of the time offset from the ideal source:

$$\text{Time accuracy} = |t - t_i|$$

where:

t = the time from the clock in question

t_i = the ideal time

3.1.2 WWVB: Time signal radio station operated by NIST

3.2 Acronyms & Abbreviations

AGPS	Assisted Global Positioning System
APNT	Alternative Positioning, Navigation, and Timing
ATIS	Alliance for Telecommunications Industry Solutions
BBU	Baseband Unit
CA	Carrier Aggregation
CDMA	Code Division Multiple Access
CFR	Code of Federal Regulations
CHAYKA	Russian terrestrial low frequency navigation system
C/N_0	Carrier to Noise Density Ratio
CoMP	Coordinated Multi-Point
DHS	Department of Homeland Security
DOT	Department of Transportation
DWDM	Dense Wavelength Division Multiplexing
E9-1-1	Enhanced 9-1-1
eLoran	Enhanced LORAN
ePRTC	Enhanced Primary Reference Time Clock
FCC	Federal Communications Commission
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

[21] This document is available from the ITU at: < https://www.itu.int/rec/T-REC-G.810/en >.

[22] This document is available from the ITU at: < https://www.itu.int/rec/T-REC-G.8260/en >.

[23] This document is available from the ITU at: < https://www.itu.int/rec/R-REC-TF.686/en >.

ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
LORAN	Long Range Navigation
LTE	Long-Term Evolution
LTE-A	LTE Advanced
MBMS	Multimedia Broadcast Multicast Service
MIMO	Multiple Input, Multiple Output
MBSFN	Multiple Broadcast Single Frequency Network
ms	millisecond
NASCTN	National Advanced Spectrum and Communications Test Network (NIST)
NIST	National Institute of Standards and Technology
NMA	Navigational Message Authentication
ns	nanosecond
OTDOA	Observed Time Difference Of Arrival
PNT	Positioning, Navigation, and Timing
PRTC	Primary Reference Time Clock
PTP	Precision Time Protocol
Rb	Rubidium
RF	Radio Frequency
RNSS	Radionavigation Satellite Service
RTT	Radio Transmission Technology
s	second
SCDMA	Synchronous Code Division Multiple Access
SDR	Software Defined Radio
STL	Satellite Time and Location
SYNC	ATIS Synchronization Committee
3GPP	3rd Generation Partnership Project
TAE	Time Alignment Errors
TBS	Terrestrial Beacon System
TDD	Time Division Duplex
TMAS	Time Measurement and Analysis Service from NIST
TX	Transmit
µs	microsecond
USNO	United States Naval Observatory
UTC	Coordinated Universal Time
WCDMA	Wideband Code Division Multiple Access
WDM	Wave Division Multiplexing
WiMAX	Worldwide Interoperability for Microwave Access

4 Introduction

Telecom timing has evolved in recent years from precision frequency delivery to precision time delivery. Requirements for precise time delivery have driven the industry toward the increased use of GPS and GPS-dependent technologies. This GPS dependency has left the telecommunications industry vulnerable to disruptions and manipulations of the GPS signal. Such disruptions may have economic, financial, and service impacts to carrier

network operators, suppliers, cellular services, and adjacent industries and government agencies that depend upon a functioning wireless communication infrastructure.

GPS receivers are essential to the telecom industry: The U.S. telecommunications industry has deployed a large number of GPS receivers and is constantly adding new receivers each year as the network grows, especially in wireless. These GPS receivers, which have a lifetime of more than 15 years, are used for precision timing from fixed locations. Based on industry estimates, fewer than 5% of these units are used to support optical networks and more than 95% are used to support the fixed infrastructure for wireless (i.e., wireless base stations – Code Division Multiple Access [CDMA], Long-Term Evolution [LTE], and Enhanced 9-1-1 [E9-1-1] augmentation systems). The telecommunications industry is dependent on these receivers for precision time accuracy. The time standard, UTC, can only be widely distributed from GPS with today's technology. There is no other option. In addition, the telecom GPS timing systems are the enabling systems for others systems such as E9-1-1 triangulation and Assisted GPS (AGPS), which are used to find the location of wireless handsets.

The impact of interference to GPS receivers deployed to the telecom industry would be significant: The GPS receivers deployed by the telecommunications industry each support many customers. While the total number of receivers may be lower than in other sectors, the impact of a problem with a telecom receiver has a larger impact because the receiver supports many customers. For instance, a problem with a precision timing GPS receiver located at a wireless base station could impact all wireless handset users that use that base station to connect the handsets to the fixed part of the wireless carrier's network. Considering the requirements related to network reliability and the provision of E9-1-1 positioning services, the correct operation of these GPS receivers is important both to the operation of carriers' networks and to users of voice, data, and location services.

Figure 4.1 summarizes at a high level the different challenges GPS receivers might face. Vulnerabilities to delivery of GPS time to a system include environmental phenomena, malicious interference and spoofing, incidental interference, adjacent band interference, poor antenna installations, and rare but present GPS segment errors. The diverse nature of these vulnerabilities, the impact of a problem on telecom customers, and the significant challenges that must be overcome to mitigate vulnerabilities provide strong motivation for an alternative timing dissemination system available at a national scale. There are several mature proposed solutions that would satisfy telecommunications sector timing requirements, and they are noted in this report.

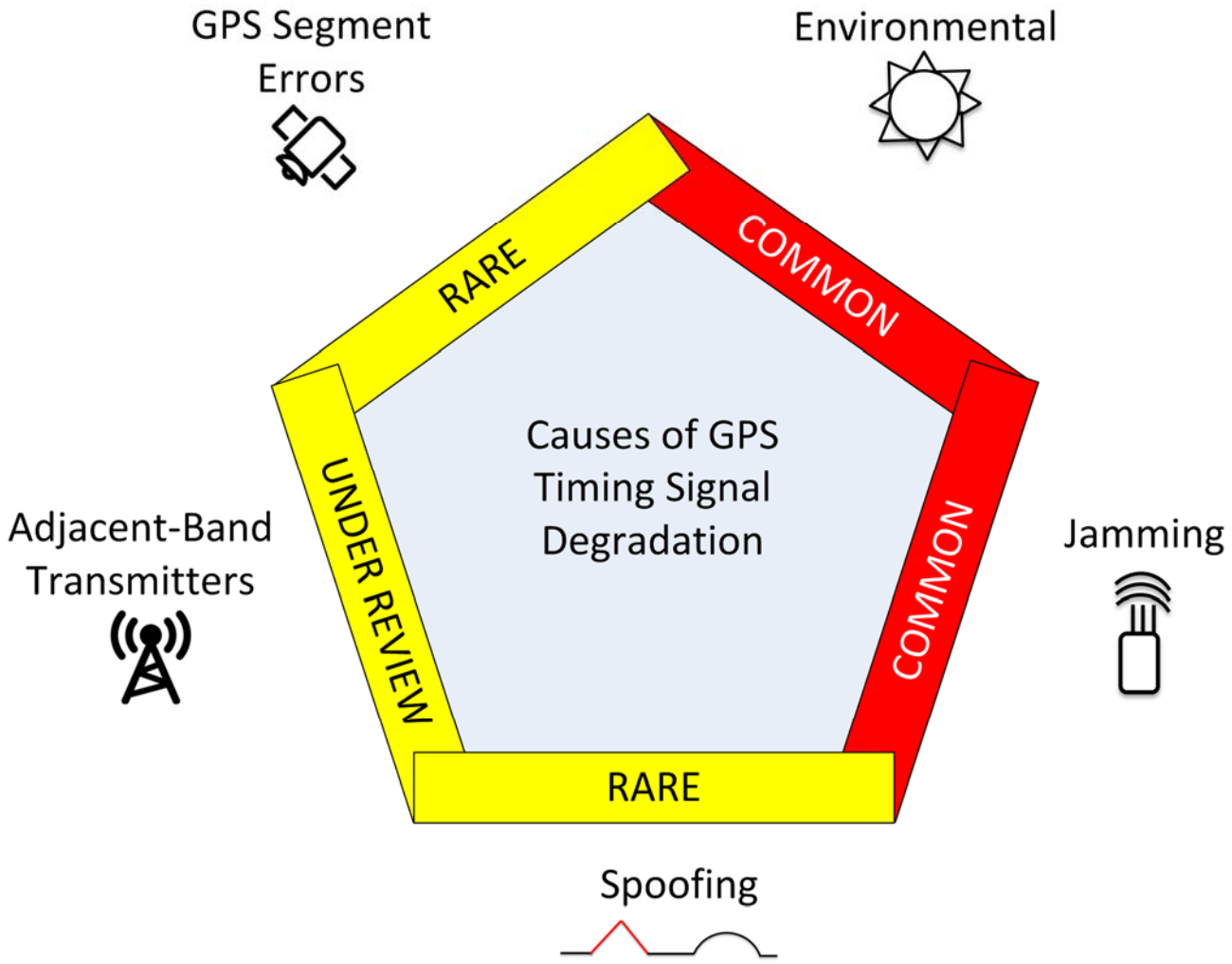

Figure 4.1 – Known GPS vulnerabilities to telecom

5 Known GPS Vulnerabilities

The communications industry is critically dependent upon GPS as a timing source. There is no other widely deployed timing infrastructure capable of satisfying telecom industry timing requirements. Alternative time dissemination architectures may still ultimately trace their time to a GPS receiver. For example, most Precision Time Protocol (PTP) Grand Masters derive their time from GPS or the Global Navigation Satellite System (GNSS).

FCC-licensed transmitters in the United States must obtain a special waiver if they intend to use a non-GPS Radionavigation Satellite Service (RNSS) receiver as a timing source.

> NOTE: The fundamental requirement is from CFR 47, see [6]. The specific and authoritative source of this information was Mr. Ron Repasi, Deputy Chief Engineering and Technology, FCC. See his comments about this in [7]. See also [8].

GPS receivers that supply time to telecommunications infrastructure nodes may be disseminating time over a wide area through a network-based protocol to many nodes, or may be locally installed at the edge of the network and be providing time to a single tower. The diversity of GPS antennas, receivers, receiver installation environments,

and receiver operating environments creates challenges for improving the resiliency of GPS holistically for the industry with any one solution or by mitigating any specific threat vector.

Table 5.1 – 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 anomalies	2016 UTC-offset error, January 2004 and July 2001 satellite clock failures.	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.
Environmental factors	GPS antenna installations, multipath interference, tropospheric impacts, ionospheric scintillation, solar weather.	Common	Improve training of the technicians who install antennas, alternative timing sources.

Today, Radio Frequency (RF) interference seen by GPS receivers is commonly caused by jamming devices in vehicles intended to block fleet tracking systems or bypass toll collection by disabling the GPS receiver. These jammers are generally not intended to degrade performance of other receivers, but do so incidentally due to their high transmit powers and disregard for other systems performance. From the effects of incidental jamming events caused by relatively low power (<5 Watts) transmitters, ATIS SYNC notes that intentional GPS jamming attacks on telecom GPS receivers would degrade network performance. If conducted in a technically savvy manner, an inexpensive jamming attack could cause a significant economic impact on the communications sector due to the difficulty of locating emitters and the eventual performance impacts on the larger telecom networks. An example of effects of jamming is the 2009 accidental jamming event due to a U.S. Navy test system in the San Diego harbor. Figure 5.1 (from [9] and [10]) shows some of the disruptions caused by this.

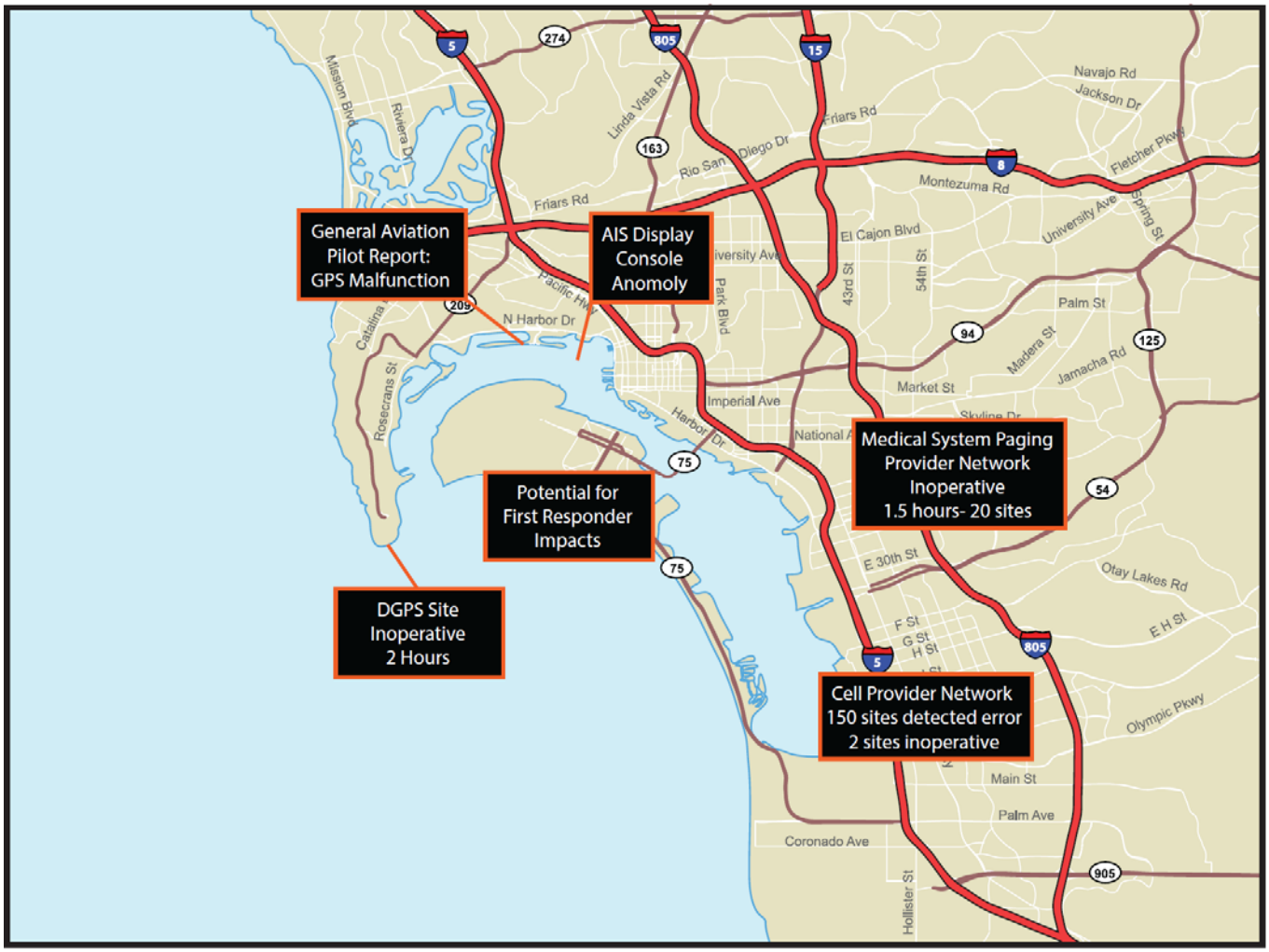

Figure 5.1 – Critical infrastructure disruptions from 2009 U.S. Navy accidental jamming event

GPS spoofing occurs when an illegitimate GPS constellation is broadcast by a rogue transmitter. ATIS SYNC acknowledges that there are reasonable and legal applications of GPS repeaters but notes that unless these repeaters are operated in a manner inconsistent with their licensing, they should not cause spoofing events. Basic GPS spoofing may consist of replacing the navigation data payload and transmitting a high-power asynchronous code phase. Though significant bodies of academic research exist that outline mitigation strategies to such spoofers, they would succeed in capturing most GPS receivers on the market today. Once captured, a spoofer may attempt to put the receiver into an error state by transmitting navigation data payloads that would result in generally undefined mathematical operations or in the case of a technically savvy spoofer, provide the receiver a false location, time, or both. ATIS SYNC notes that the effects of code-phase synchronous spoofers on a larger telecom network is an area that requires more study, but also emphasizes that current GPS receiver technology deployed in communications sector infrastructure is vulnerable to basic and advanced GPS spoofing. ATIS SYNC is concerned with the proliferation of open-source technologies and software that enable GPS spoofing by amateurs (see [11]). A discussion of spoofing and potential receiver defenses is in [12], an IEEE Spectrum article by Mark L. Psiaki and Todd E. Humphreys (see also [13]). Spoofing a boat's position is illustrated in Figure 5.2(originally from [12]). Spoofing time and maintaining position would work similarly.

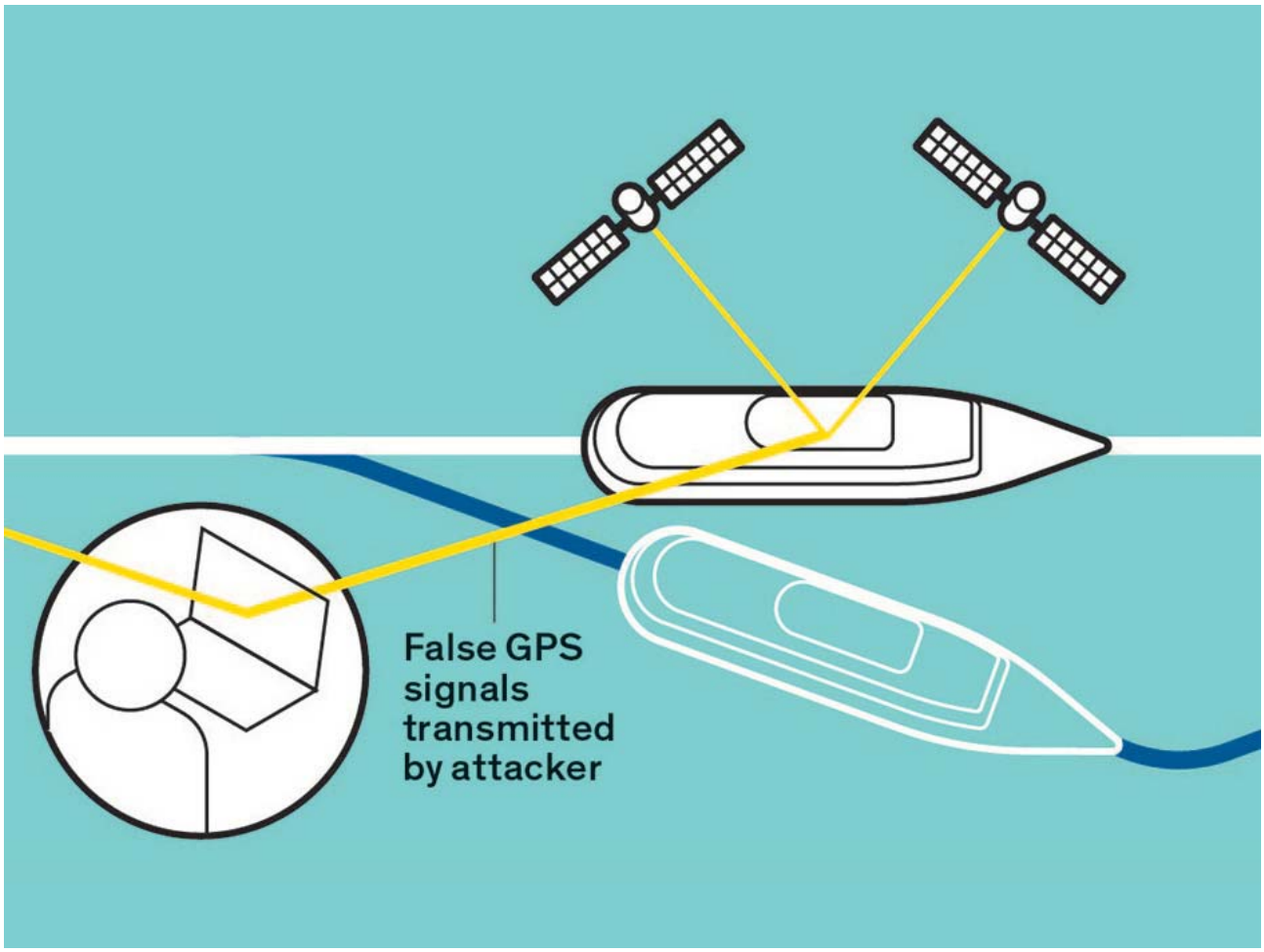

Figure 5.2 – Illustration of spoofing a boat's position

While GPS is extremely reliable, there have been a number of anomalous events in its history. It is reasonable to expect there will be others. Most recently, in January 2016, an error in the system caused a subset of satellites to transmit an incorrect UTC timing signal. This error caused certain models of timing receivers to alarm and indicate that GPS was failing or experiencing an outage. In some cases, these alarms required manual technician intervention to resolve. Figure 5.3 shows how the anomaly event impacted one GPS timing receiver during the day. Other failures have been documented in the history of GPS, including clock failures causing significant periods of bad data on January 1, 2004, and in July 2001 (see [14]). Though rare, these outages provide insight into the potential catastrophic impact of a large-scale GPS outage or spoofing event and motivate ATIS SYNC to advocate for Alternative Positioning, Navigation, and Timing (APNT) systems.

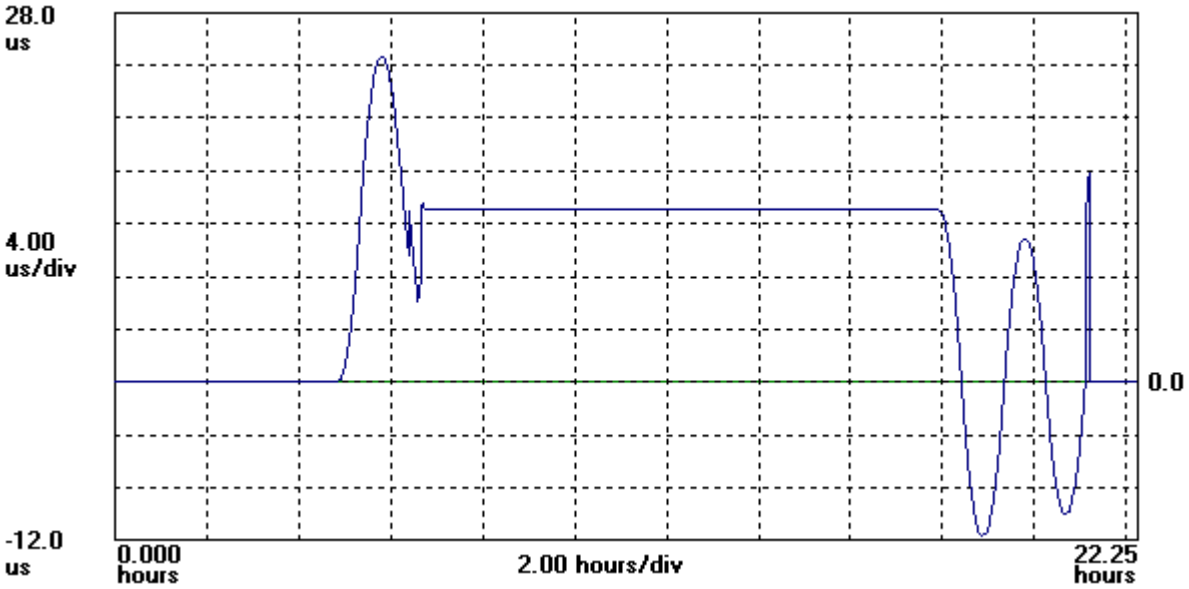

Figure 5.3 – Plot showing how the anomaly event impacted one GPS timing receiver

Because of the extreme value of bandwidth for communications systems, there is great interest in using spectrum near GPS signals for signals that are significantly stronger. Such signals can interfere with certain GPS receivers that do not have the filters necessary to reject these adjacent-band transmissions. In part, this can be due to the design of traditional GPS antennas that may have a pass-band that includes parts of the spectrum not allocated to GPS. In addition, any transmitter that has out-of-band emissions that are not properly limited could directly disrupt a GPS receiver by producing energy in a GPS band. ATIS SYNC notes that well-designed antennas and spectral separation of transmissions from GPS bands can limit adverse effects of adjacent band transmissions on GPS receivers. ATIS SYNC also notes that the lifecycle of a typical GPS antenna installation supporting communications sector infrastructure is long, and that while antennas robust against this type of interference may exist today, a number of antennas deployed to existing infrastructure may be vulnerable to this type of interference.

Although GPS spoofing and system errors as described in Table 5.1 are rare occurrences, they can have serious impacts to communications sector performance. GPS spoofing has become a commodity enabled by open-source software releases and commercially available and inexpensive software-defined radio platforms. There is now an active open-source developer community working on sophisticated GPS signal transmitters deployable to these Software Defined Radio (SDR) platforms (see [11]). Today, these systems can execute data replacement attacks and simple code phase attacks, and it is reasonable to expect that more sophisticated types of attacks will be released in the future. GPS spoofing attacks can mimic the effects of a GPS system error. For example, the GPS UTC Offset error in January 2016 that put many GNSS timing receivers into a holdover mode and required manual resets of equipment could have been just as easily caused by a spoofing event.

6 GPS Performance & Synchronization Requirements

There are many different synchronization requirements in telecom. Because GPS signals are vulnerable to interference, telecom systems must have timing references that meet relevant requirements both during operation without external interference, as well as in the presence of intentional or unintentional interference, in order to maintain services with reliability requirements. Different specifications support different services that telecom provides. As different specifications are exceeded, some services would fail and others would not. Examples of some timing requirements for LTE in telecom are in Table 6.1, which also includes other examples. Table 6.1 is based on ITU-T G.8271 [1] Appendix II with some additions. The table is comprised of three sections: (1) standards for timing sources; (2) other existing timing requirements, wireless in particular; and (3) new timing requirements under study. However, it is not clear what fails if the specifications are exceeded. Because manufacturers use

proprietary algorithms, there will generally be different results to timing failures, and these cannot be publicly known because the information is generally proprietary.

Table 6.1 – Time and phase end application synchronization requirements

Application/ Technology	Accuracy	Specification
PRTC (Primary Reference Time Clock) **(Source)**	±100 ns with respect to UTC	[ITU-T G.8272]
ePRTC (Enhanced Primary Reference Time Clock) **(Source)**	±30 ns with respect to UTC	[ITU-T G.8272.1]
CDMA2000	± 3 µs with respect to CDMA System Time, which uses the GPS timescale (which is traceable and synchronous to UTC except for leap second corrections). ± 10 µs with respect to CDMA System Time for a period not less than 8 hours (when the external source of CDMA system time is disconnected).	[b-3GPP2 C.S0002] section 1.3 [b-3GPP2 C.S0010] section 4.2.1.1
TD-SCDMA (NodeB TDD mode)	3 µs maximum deviation in frame start times between any pair of cells on the same frequency that have overlapping coverage areas.	[b-3GPP TS 25.123] section 7.2
WCDMA-TDD (NodeB TDD mode)	In TDD mode, to support Intercell Synchronization and Handoff, a common timing reference among NodeB is required, and the relative phase difference of the synchronization signals at the input port of any NodeB in the synchronized area shall not exceed 2.5 µs.	[b-3GPP TS 25.402] sections 6.1.2 and 6.1.2.1
W-CDMA MBSFN	12.8 µs for MBMS over a single frequency network, where the transmission of NodeB is closely time synchronized to a common reference time.	[b-3GPP TS 25.346] sections 7.1A and 7.1B.2.1
LTE MBSFN	Values < ± 1 µs with respect to a common time reference (continuous timescale) have been mentioned.	Under study
W-CDMA (Home NodeB TDD mode)	Microsecond level accuracy (no hard requirement listed).	[b-3GPP TR 25.866] section 8
WiMAX	1) The downlink frames transmitted by the serving base station and the Neighbour base station shall be synchronized to a level of at least 1/8 cyclic prefix length (which is equal to 1.428 µs). At the base station, the transmitted radio frame shall be time-aligned with the 1PPS timing pulse. 2) The base station transmit reference timing shall be time-aligned with the 1PPS pulse with an accuracy of ± 1 µs.	[b-IEEE 802.16] table 6-160, section 8.4.13.4 [b-WMF T23-001] section 4.2.2
LTE-TDD (Wide-Area Base station)	3 µs for small cell (< 3 km radius). 10 µs for large cell (> 3 km radius). Maximum absolute deviation in frame start timing between any pair of cells on the same frequency that have overlapping coverage areas.	[b-3GPP TS 36.133]) section 7.4.2

Application/ Technology	Accuracy	Specification
LTE-TDD (home-area base station)	1) 3 µs for small cell (< 500m radius). For large cell (> 500 m radius), 1.33 + $T_{propagation}$ µs time difference between Base Stations, where $T_{propagation}$ is the propagation delay between the Home base station and the cell selected as the network listening synchronization source. In terms of the network listening synchronization source selection, the best accurate synchronization source to GNSS should be selected. If the Home base station obtains synchronization without using network listening, the small cell requirement applies. 2) The requirement is 3.475 µs but in many scenarios a 3 µs sync requirement can be adopted.	[b-3GPP TS 36.133] section 7.4.2 [b-3GPP TR 36.922] section 6.4.1.2
LTE-TDD to CDMA 1xRTT and HRPD handovers	eNodeB shall be synchronized to GPS time. With external source of CDMA system time disconnected, the eNodeB shall maintain the timing accuracy within ± 10 µs with respect to CDMA system time for a period of not less than 8 hours.	[b-TS 3GPP TS 36.133] section 7.5.2.1
LTE Advanced (LTE-A)	Phase/Time requirements for the applications listed below are currently under study: • Carrier Aggregation (CA) • Coordinated Multipoint Transmission (also known as Network- Multiple Input, Multiple Output [MIMO]) • Relaying function	[b-TR 3GPP TS 36.814]
IP network delay monitoring	The requirement depends on the level of quality that shall be monitored. As an example, ± 100 µs with respect to a common time reference (e.g., UTC) may be required. ± 1 ms has also been mentioned.	Note 3
Intra-band non-contiguous carrier aggregation with or without MIMO or TX diversity, and inter-band carrier aggregation with or without MIMO or TX diversity (Notes 4,7,8)	260 ns	[b-3GPP TS 36.104] section 6.5.3.1
Intra-band contiguous carrier aggregation, with or without MIMO or TX diversity (Notes 4,7,8)	130 ns	[b-3GPP TS 36.104] section 6.5.3.1
Location Based Services using Observed Time Difference Of Arrival (OTDOA) (Notes 4,6,7)	100 ns	
MIMO or TX diversity transmissions, at each carrier frequency (Notes 4,7,8)	65 ns	[b-3GPP TS 36.104] section 6.5.3.1
More emerging LTE-A features that require multiple antenna co-operation within a cluster. (Notes 4,5,7)	x ns	
NOTE 1: In the case of mobile applications, the requirements are generally expressed in terms of phase error between base stations. In the case of a centralized master, the requirement could be expressed as ± half of the accuracy requirement applicable to the specific technology.		

Application/ Technology	Accuracy	Specification
NOTE 2: The requirements are generally valid during normal conditions. The applicable requirements during failure conditions are for further study. NOTE 3: For IP network delay monitoring, there is no standard requirement yet. Requirements are operator dependent (depending on the application). NOTE 4: The requirement is expressed in terms of relative error with respect to another base station, both of which have the same reference. NOTE 5: The performance requirements of the LTE-A features are under study. The value for x is for further study. NOTE 6: 100 ns supports approximately 30-40m of location accuracy when using OTDOA with a minimum of three base stations. There is currently no published specification. NOTE 7: The requirements are expressed in terms of relative error between antennas (i.e., base station sectors), both of which have the same timing reference. Although phase/time accuracy requirements for CA and Coordinated Multi-Point (CoMP) are generic and are not defined for any particular network topology, this level of phase error budget implies that the antennas for which the requirements apply are typically co-located with or connected to the same Baseband Unit (BBU) via direct links. NOTE 8: Note that the three items in the table referring to MIMO may not translate to a synchronization requirement as they refer to timing within a particular base station rather than between base stations. These are Time Alignment Errors (TAE) expressed as minimum requirements.		

Time accuracy requirements have become tighter in recent years. ITU-T Study Group 15, Question 13 establishes time and frequency standards for international telecom systems. ITU-T G.8272 [2] sets the requirement for a Precision Reference Time Clock (PRTC) at 100 ns against UTC. A new standard, G.8272.1 [3] has developed an enhanced Precision Reference Time Clock (ePRTC), which requires 30 ns accuracy against UTC. 5G systems will have new timing requirements that may be more difficult to maintain. These requirements make stringent limits on the performance of GPS. Testing to show conformance has significant implications. Timing receivers have a direct dependency on the delay through the antenna, cable, and receiver system, in direct contrast to positioning and navigation receivers, which only need differential satellite delays to be stable. In addition to the delay of the GPS time code through individual elements of the receiver system, reflections in the elements add internal multi-path delays that can cause timing changes in the 10's of ns (see [15]). Hence timing receivers have special needs for testing.

The spectrum for wireless systems is valuable, and there is a desire to use bands adjacent to GPS signals for wireless services. In addition, if other GNSS are approved for U.S. telecom timing references, there will be other bands of the spectrum that will be vulnerable to interference. The telecommunications industry supports efforts to maximize the bandwidth available for wireless services, but it cannot support these efforts at the expense of degrading existing network operations, in particular the dependence on GPS or GNSS timing for system operations. As industries propose the use of bands for wireless data adjacent to approved GNSS, results of testing must be considered to show that proposed transmissions do not interfere with required timing performance.

ATIS SYNC has a number of recommendations with regard to testing that are discussed in the recommendations section. These recommendations discuss: 1) open testing, 2) the consideration of testing results in deciding adjacent band signal transmissions, and 3) various specifics of testing that are relevant to timing receivers and telecom networks.

7 GPS Vulnerability Mitigation & Alternatives to GPS Timing

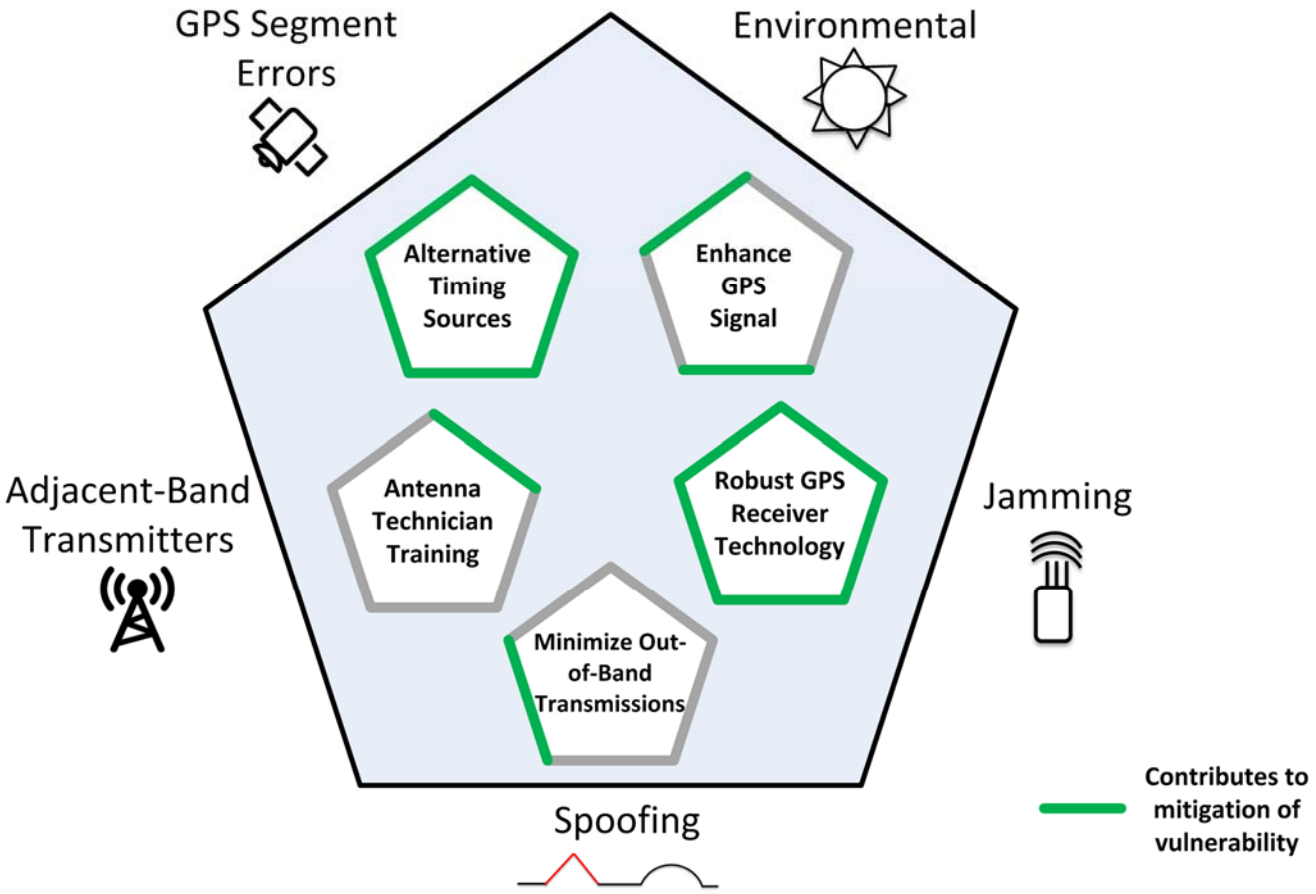

Figure 7.1 – Identified candidate mitigation strategies

ATIS SYNC has discussed several proposals to mitigate GPS vulnerabilities on critical infrastructure receivers:

1. Navigational Message Authentication on modernized GPS civil signals.
2. Atomic clock time holdover.
3. Sync over fiber.
4. eLoran.
5. WWVB.
6. Terrestrial beacons.
7. Communication satellite timing.
8. Differential time transfer.

Atomic clock time holdover, sync over fiber, eLoran, WWVB, terrestrial beacons, communication satellite timing signals, and differential time transfer (proposals 2, 3, 4, 5, 6, 7, and 8, respectively) are methods for transporting time and phase synchronization that are technologically diverse from GPS; these solutions could continue to operate to deliver time and phase sync even if there were a total failure of the GPS system, as long as the master clock for any of these systems was independent of GPS.

All proposals with the exception of #1 provide an independent or semi-independent timing mechanism to a receiver. These methods all have the additional benefit of being immune from inherent localized sources of GPS degradation

such as multipath and GPS antenna installations. Proposals such as #1 that harden the GPS signal itself, or make the GPS receiver more robust to false or degraded signals, are still sensitive to GPS-wide failure modes.

ATIS SYNC notes that there are a number of mitigation strategies for GPS receivers to resist interference. A number of bodies including ATIS SYNC are considering establishing standards addressing these.

1. Navigational Message Authentication (NMA) on L2C and L5

There are currently no signal-side security features available on Civil GPS civil signals that could be used to mitigate intentional or unintentional spoofing events. The addition of Navigational Message Authentication (NMA) to some, or all, of the modernized GPS signals would provide a tool GPS civil signal receivers could use to mitigate spoofing events. ATIS SYNC has spent a considerable amount of time discussing the merits of NMA, and notes that the telecom sector is presently using only L1 C/A GPS receivers for timing and synchronization. Telecom sector use of NMA on L2C or L5 would require the deployment of additional receivers, or replacement or enhancement of existing L1 receivers with a dual frequency version supporting L1 and L2, or L5, operation. ATIS SYNC further notes that NMA does not help mitigate jamming, GPS interference, or the other vulnerabilities identified in Table 5.1. While NMA on L2C would not be immediately usable by current telecom receivers, the long-term application of NMA on GPS civilian signals may become an important defense against a spoofing attack.

2. Atomic Clock Time Holdover

The use of a high-stability atomic clock provides a means of maintaining precise time in the event of loss of GPS. One example of this is the ePRTC defined in ITU-T G.8272.1 [3], which couples GNSS with an autonomous primary reference atomic clock. In the event of a GNSS outage, the ePRTC provides two weeks of time holdover better than ±100 ns to UTC.

The use of a highly stable clock, in addition to providing for time holdover, also provides a mechanism for detecting spoofing, as it functions as an independent source of stable time.

3. Sync over Fiber

Private sector companies and National Institute of Standards and Technology (NIST) are conducting a proof of concept trial of transporting very high precision time and phase synchronization over fiber using IEEE-1588v2 PTP (see [5]). PTP packetizes time and phase information for delivery over a packet-based network such as Ethernet, which is in turn transported over fiber. PTP is susceptible to impairments due to packet delay variation and asymmetry in the forward versus reverse transmission paths. SYNC finds the results to date of this trial encouraging; 18 ns deviation was held in a measurement lasting 3 months of PTP over Dense Wavelength Division Multiplexing (DWDM) using commercial optical fiber connecting UTC (NIST) and UTC (United States Naval Observatory [USNO]) over a span of 150 km. There is a need, however, to determine if PTP can be used to transport very high precision time and phase sync over the vast distances required to cover the continental U.S.; this is to be investigated in a follow-on experiment. For further information on this experiment, see [16].

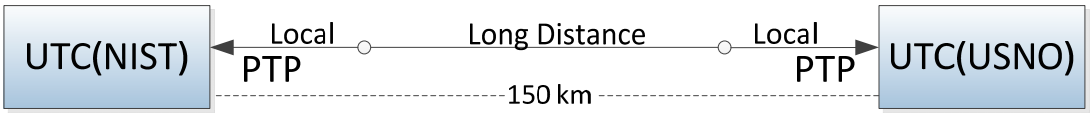

Figure 7.2 – 10's of ns held in a 3-month measurement over commercial fiber (150 km link)

ATIS SYNC notes that there is a second proposal for sync over fiber that may develop in the future. ITU-T standard J.211 [4] describes a two way protocol transported over the physical layer that includes a mechanism to correct for transport delay and asymmetry. It is not packet based and thus is not impaired by delay variation. ATIS SYNC has

been advised that this technology could be adapted to fiber transport using telecom industry standard Wave Division Multiplexing (WDM) technology.

4. eLoran

In October 2014, SYNC reviewed presentations on a joint government and private sector proposal that addresses the development of a new eLoran type system in the U.S. for delivering very high precision time and phase sync. This type of signal is very long wavelength, very high powered, would be very difficult to jam and spoof, and penetrates buildings well. In 2016 an eLoran receiver coupled with a Rb oscillator demonstrated the ability to independently track UTC within 30 ns of a reference in the New York Stock Exchange [17]. The receiver used an eLoran broadcast from Wildwood, NJ. Though still under development and consideration in the United States, ATIS SYNC notes that eLoran is already available and used as a GNSS alternative in Europe, and that areas that experience regular GPS-denial in Southeast Asia are implementing eLoran as an APNT system [18]. ATIS SYNC also notes that there is a Russian terrestrial low frequency navigation system, CHAYKA, which is similar to Loran-C.

5. WWVB

ATIS SYNC notes that it is technologically feasible to develop a very high precision timing reference similar to WWVB that would operate in RF spectrum. Such a solution has been discussed in ATIS SYNC. Sub-1 GHz RF spectrum signals penetrate buildings very well, and a timing source in that spectrum could be a viable backup to GPS for timing references. This proposal would require development to determine how best to provide the accuracies required for telecom needs.

6. Terrestrial Beacons

ATIS SYNC also notes that it is technologically feasible to develop a very high precision timing reference based on terrestrial beacons. Such a solution has been discussed in ATIS SYNC. At least one Terrestrial Beacon System is being deployed in the U.S. to provide high precision timing and frequency in GPS-challenged areas, such as Indoors and Urban Canyons and as a backup to GPS in other areas. Terrestrial Beacons can deliver very precise time and frequency synchronization. The received Terrestrial Beacon System (TBS) signals from multiple terrestrial transmitters are significantly more powerful than space-based GPS signals and provides for geographic redundancy of the signal. The signaling for TBS positioning has been standardized in 3GPP and the technology also enables 3D indoor location for “Mission Critical” location.

7. Communication Satellite Timing

Communication satellite constellations may have timing signals that can provide GPS independence. A mature example of such a system is the Satellite Time and Location (STL) signal broadcast over the Iridium constellation. The STL clock reference is based on an atomic clock located at a ground station that is trained to a GPS reference. Satellites that are not designed for navigation and timing missions generally use clocks that have much higher error than GPS clocks and require continuous calibration from ground stations. Using Iridium as an example, the STL clock deviation from GPS is of the order sub-100 ns to 500 ns (depending on the Iridium satellite). Non-GPS satellites may also have meaningful signal strength advantages relative to GPS that make their use more robust and less dependent upon environmental variables.

8. Differential Time Transfer

This is a useful method of transferring time from a system that already has correct time to the targeted user. If GPS is lost in a local area, such as due to interference or jamming, UTC from GPS can be provided using a differential

time transfer method that is available from the area that still has GPS to the area without GPS. Many of the mitigation systems discussed above that provide time to a user can be used in a differential mode. PTP is a differential time transfer system, only providing UTC if the Grand Master from which PTP transfers time has UTC. GPS common-view time transfer, a differential method, supports the Time Measurement and Analysis Service (TMAS) from NIST to deliver UTC (NIST) to remote users [19].

Of particular interest is combining GPS with a time transfer system such as WWVB or eLoran. These systems might not have sufficient accuracy for a particular application as stand-alone systems, but might have a stable enough differential time transfer over a few 10's of km. To explain this, consider two stations, *A* and *B*, that have GPS co-located with a WWVB receiver, and that have a communication channel between them. Let GPS minus WWVB at *A* be Δt_A, and at *B* be Δt_B, and assume that GPS is providing UTC with enough accuracy for the relevant application. Then the difference $\Delta t_A - \Delta t_B$ cancels UTC from GPS, and gives Δ_{WWVB}, the difference of time from WWVB at *B* minus WWVB time at *A*, which can be communicated between *A* and *B.* Because the wavelength of the WWVB signal is 5 km, this value will remain fairly constant over several 10's of km. Then, if station *B* loses GPS, but both still have WWVB time, UTC from GPS at station *B* would be time from WWVB at station *B* plus Δ_{WWVB}. Hence, time can be provided to station *B* from station *A* using WWVB in a differential mode.

8 Recommendations to Assure Time for Telecom

Given the current observed threat profile, ATIS SYNC believes there is an urgent need for GPS timing backup/fallback in critical infrastructure and multiple solutions be considered and evaluated. Different systems may have different requirements which will benefit from a diversity of solutions.

ATIS SYNC recognizes that the FCC is considering adjacent band signals. 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.

ATIS SYNC makes the following general recommendations with the intent to reduce telecom industry and communications sector susceptibility to GPS vulnerabilities:

ATIS SYNC Recommendations

1. ATIS SYNC recommends that telecom carriers explore including time-sync networks engineered to provide time as a service both internally and externally.
2. ATIS SYNC recommends that the U.S. government agencies responsible for GPS consider adding signal-side security features, such as Navigation Message Authentication (NMA), to the L2C, and L5 Modernized Civil Signals as a possible mitigation strategy against spoofing attacks on civil GPS signals. ATIS SYNC asks that the Sector Coordinating Council representing the civil signal user community poll civil signal users for their interest in NMA on the modernized civil signals.
3. An eLoran system (or equivalent) 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. The physical and cyber security of eLoran transmission stations should be a consideration in their operation.
4. ATIS SYNC acknowledges ongoing efforts in the U.S. Department of Homeland Security (DHS) and Department of Transportation (DOT) to understand critical infrastructure GPS vulnerabilities and encourages these efforts to continue to consider alternative timing solutions to augment critical infrastructure.
5. The U.S. government agencies responsible for NIST and USNO should continue to empower scientists and engineers to work cooperatively with SYNC and industry on GPS vulnerability and backup issues. SYNC would welcome the participation of NIST and/or USNO scientists and engineers to share their technical views and jointly develop solutions that industry can use.
6. Work in ATIS SYNC is contribution driven. ATIS SYNC requests the Communications Sector Coordinating Council to encourage carrier and equipment supplier participation in ATIS SYNC, to share their ideas via contributions and to progress the evaluation of the proposals listed.

7. ATIS 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.
8. ATIS SYNC makes the following recommendations with regard to future GPS receiver testing:
    a. ATIS SYNC encourages open testing where the precision timing GPS receiver type is represented and impact can be measured for timing accuracy versus both industry specifications and other requirements (see Table 6.1). Test plans should be available for review by the general interested public, including ATIS SYNC. All test data (including unprocessed/raw data collected) and results should be made available for review. The testing recently performed by the National Advanced Spectrum and Communications Test Network (NASCTN) reflects the type of transparent testing we recommend.
    b. Test designs should consider variables that uniquely affect stationary GPS precision timing receivers used by telecom and other U.S. critical infrastructure sectors (and may not impact navigation and positioning receivers). Examples of variables to account for in GPS precision time receiver testing include:
        i. Considering the specific needs of timing devices, key performance indicators other than C/N_0 should be measured. In particular, the GPS and UTC time produced by a receiver should be measured and variations should be characterized for any test case.
        ii. Delay variations through receiver electronics are critically important for timing receivers. 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) that RF electronics typically experience. If not compensated for, these variations would negatively impact the GPS and UTC time produced by a receiver.

    c. ATIS SYNC believes the results of existing GPS adjacent band studies and any related technical work should be considered 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.