Symmetricom®

Mitigating GNSS Vulnerabilities in Commercial Network Timing Applications

Kris Sowolla

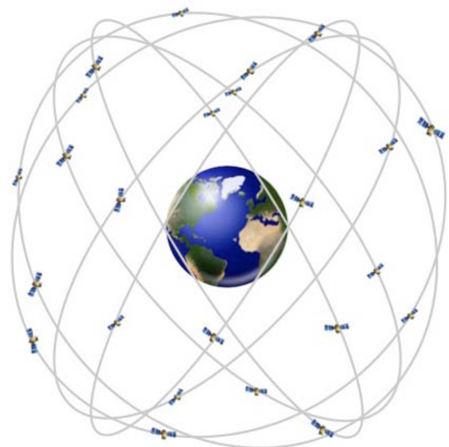
May 2013

Agenda

- Introduction and Overview of GNSS
- Vulnerabilities
- Mitigation

"Everyone" Depends on GNSS

Symmetricom



GOVERNMENT

COMMUNICATIONS

ENTERPRISE

POWER UTILITY

All market segments use GPS receiver technology to synchronize their network infrastructure

Precise Timing is More Important Than Ever

Symmetricom®

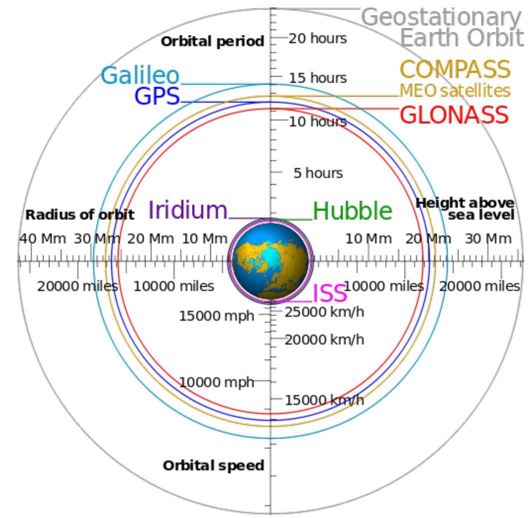
- Higher precision is needed
  - Seconds ⏩ Milliseconds ⏩ Microsecond ⏩ Nanoseconds
- More time-based correlation from widely dispersed sources and locations
  - Data centers and WANs, cloud networks, smart substations and WAMS, mobile small cell eICIC, transaction systems, operating centers, billing systems…
- Reactive, post event analysis ⏩ Proactive, automated operations

Once a routine network function,
timing and synchronization is now a sophisticated foundation technology that is essential to mission critical network operations and data applications.
And it must be protected.

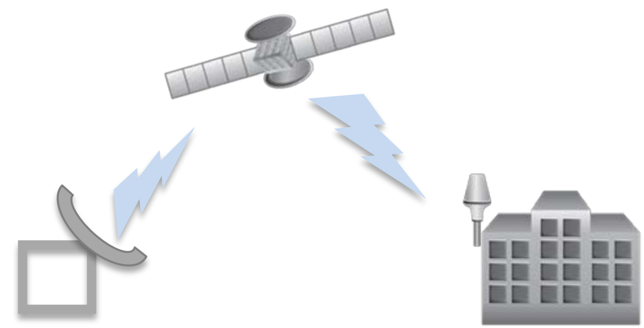
Global Navigation Satellite Systems (GNSS)

Symmetricom®

- GPS (United States)
  - Operational
- GLONASS (Russia)
  - Operational
- Beidou (aka Compass) (China)
  - Partially operational (regional system)
- Galileo (European Union)
  - In preparation stages
- Other regional systems are also in operation or being planned



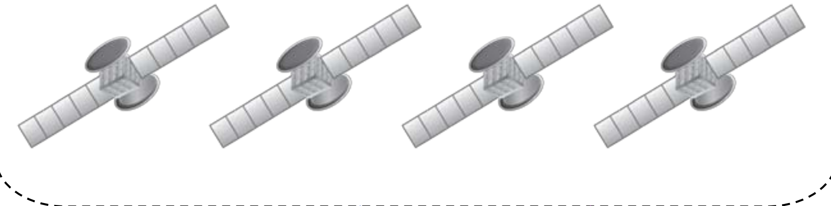
In general: an array of 24-30 satellites, in orbits over 19,000 km away, circling the earth every 12 hours



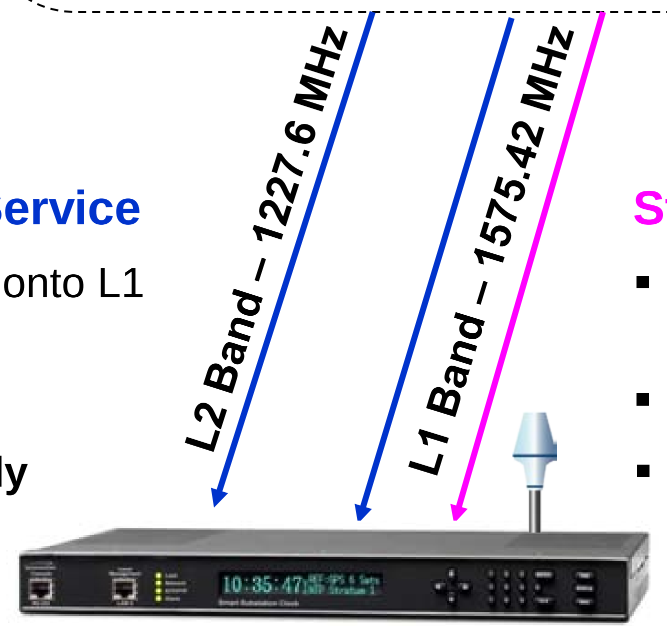
1. **Control Stations send position and time synchronization information to the satellites**
2. **Satellites send their position and time info to Earth**
3. **Receiver calculates its position and time**

GPS Transmit Power is Very Low

Multiple atomic clocks are on each satellite.



Visibility of 4 satellites needed to solve for position and precise time applications



PPS

Precise Positioning Service

- P(Y) Code modulated onto L1 and L2 carrier
- Encrypted signals
- **Authorized users only**

SPS

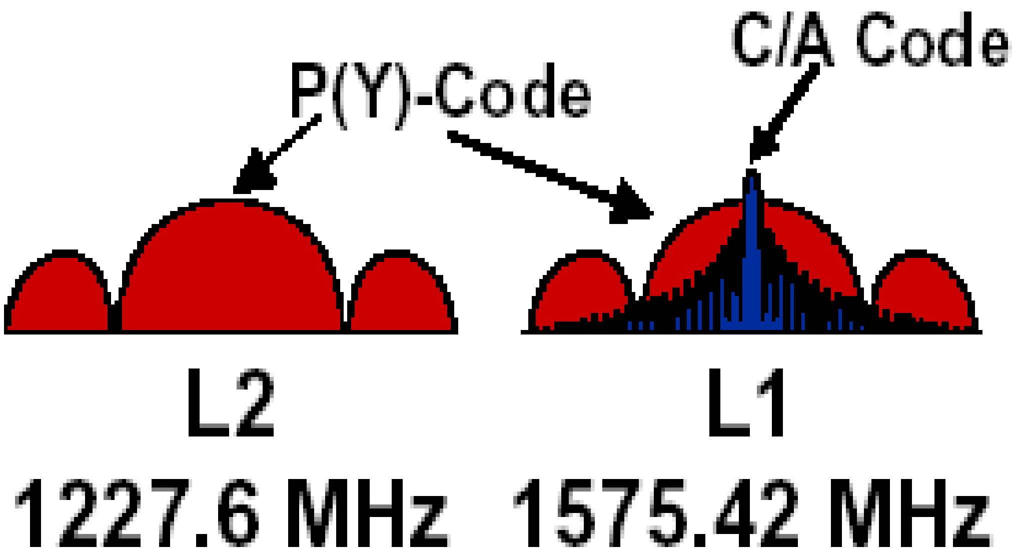
Standard Positioning Service

- C/A (Coarse Acquisition) Code modulated onto L1 carrier
- No encryption
- **Commercial, civil and gov't users (everybody)**

25 to 100 Watts, over 20,000 kilometers away!

GPS Signal Characteristics

Coarse Acquisition Code is the signal available for commercial purposes

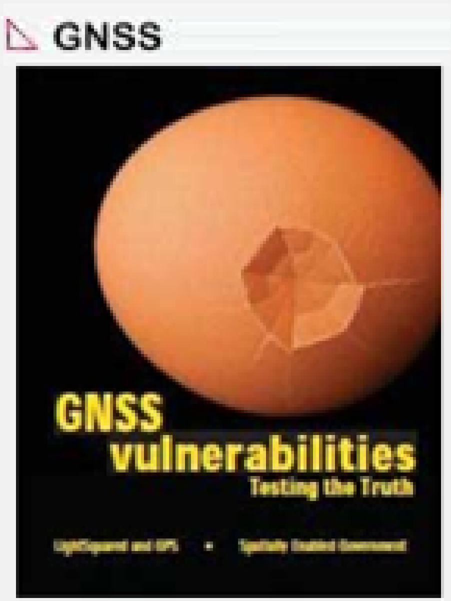


C/A Code is more vulnerable than the P(Y) code used by government/military

Vulnerabilities

GNSS Vulnerabilities are a Major Concern

Symmetricom



COORDINATES MAGAZINE
March 2012

Royal Institute of Navigation
Science Technology Practice

7th ANNUAL
GNSS VULNERABILITIES AND SOLUTIONS CONFERENCE
18 – 20 April, 2013

U.S. Department of Homeland Security

U.S. Department of Homeland Security

"Maintains a central database for reports of domestic and international interference to civil use of GPS …"

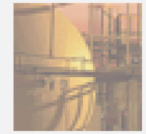
U.S. GPS Interference Detection and Mitigation (IDM) Program

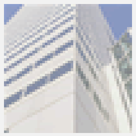
GNSS vulnerability is a growing concern in critical infrastructure applications

CIKR Sectors


Agriculture and Food


Banking and Finance

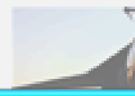

Chemical


Commercial Facilities

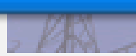

Communications

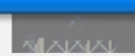

Critical Manufacturing

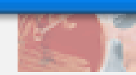

Dams

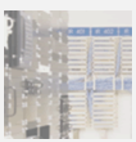

Defense Industrial Base

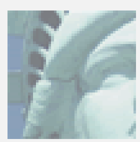

Emergency Services

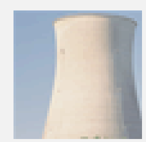

Energy

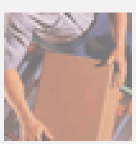

Government Facilities


Healthcare and Public Health

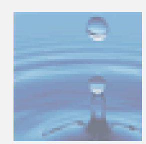

Information Technology


National Monuments and Icons


Nuclear Reactors, Materials and Waste


Postal and Shipping

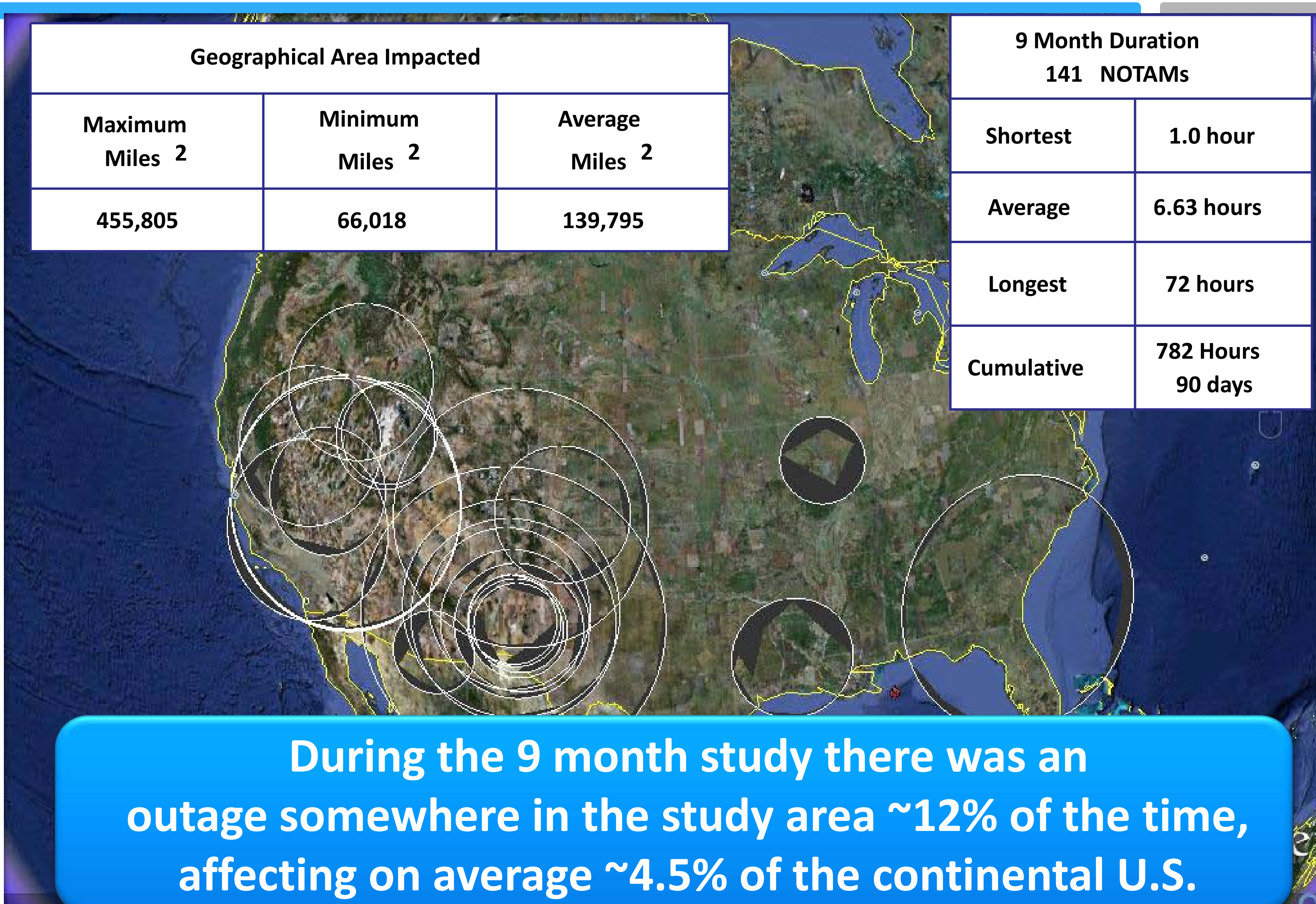

Transportation Systems


Water

GPS timing is used in 15 of the CIKRs and is essential in 11 of the 18.

GNSS Challenges: GPS tested by the U.S. DOD

Symmetricom



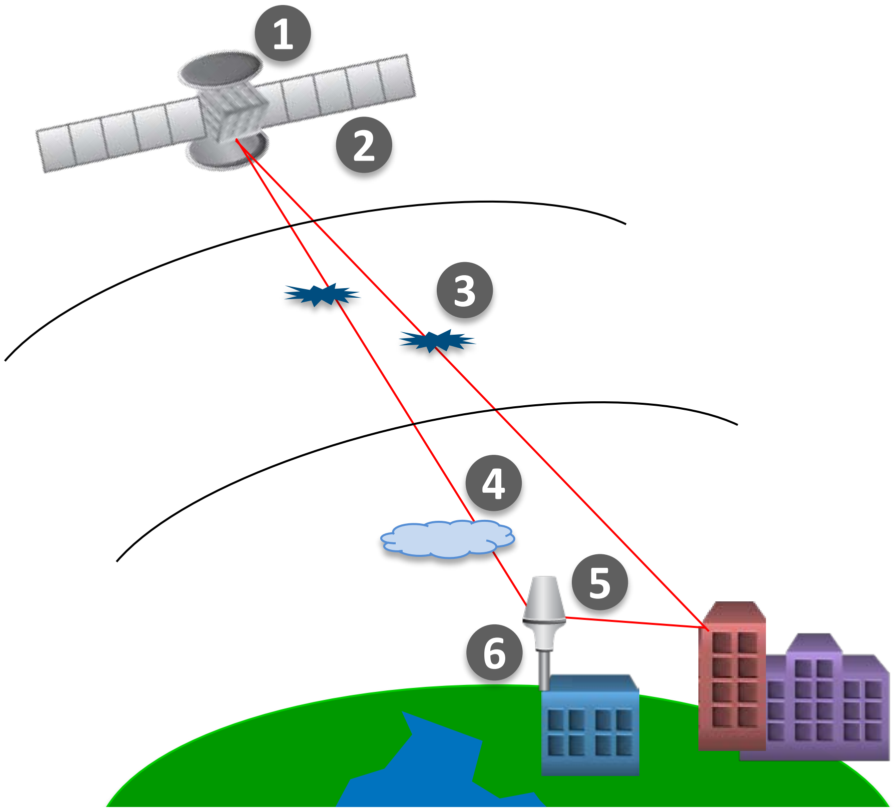
Geographical Area Impacted		
Maximum Miles ^{2}	Minimum Miles ^{2}	Average Miles ^{2}
455,805	66,018	139,795

9 Month Duration 141 NOTAMs	
Shortest	1.0 hour
Average	6.63 hours
Longest	72 hours
Cumulative	782 Hours 90 days

During the 9 month study there was an outage somewhere in the study area ~12% of the time, affecting on average ~4.5% of the continental U.S.

Source: FAA, 2010

Normal Operations Can Induce Errors

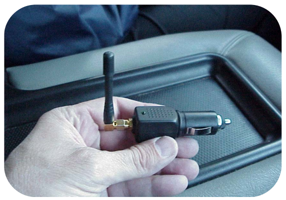


1. Orbit error
2. Satellite clock error
3. Ionospheric delay
4. Tropospheric delay
5. Multipath
6. Receiver noise

Everyday GPS Outages (Intentional)

Symmetricom

Jammers and Spoofing



Jammers

$55 Ebay

$83 GPS&GSM

Spoofing

Cheap jammers to sophisticated spoofing

Signal Characteristics of Civil GPS

Devices which claim to jam or "block" G
are widely available through a number of we
online entities. The cost of these devices ra
a few tens of dollars to several hundred. T
does not seem to correlate with the claim
the purveyors of these devices regarding th
and effectiveness of the product in question
ranges from a few meters to several tens
are advertised, but it will be shown that
effective ranges are significantly greater. Cl
true power consumptions range from a fra
Watt to several Watts.

Steven P. Powell is a Senior Engineer with the GPS and Ionospheric Studies Research Group in the Department of Electrical and Computer Engineering at Cornell University. He has M.S. and B.S. degrees in Electrical Engineering from Cornell University. He has been involved with the design, fabrication, testing, and launch activities of many scientific experiments that

ABSTRACT

This paper surveys the signal properties of 18 commercially available GPS jammers based on experimen-

Software attacks

GPS Software Attacks

Tyler Nighswander
Carnegie Mellon University
Pittsburgh, PA, USA
tylerni7@cmu.edu

Brent Ledvina
Coherent Navigation
San Mateo, CA, USA
ledvina@coherentnavigation.com

Jonathan Diamond
Coherent Navigation
San Mateo, CA, USA
diamond@coherentnavigation.com

Robert Brumley
Coherent Navigation
San Mateo, CA, USA
brumley@coherentnavigation.com

David Brumley
Carnegie Mellon University
Pittsburgh, PA, USA
dbrumley@cmu.edu

ABSTRACT

Since its creation, the Global Positioning System (GPS) has grown from a limited purpose positioning system to a ubiquitous trusted

grown from a limited purpose positioning system to a ubiquitous trusted source for positioning, navigation, and timing (PNT) data. While GPS is commonly known for personal navigation, it is also

In this work, we systematically map out a larger attack surface by viewing GPS as a computer system. Our surface includes higher level GPS protocol messages than previous work, as well as the GPS OS and downstream dependent systems. We develop a new hardware platform for GPS attacks, and develop novel attacks against GPS infrastructure. Our experiments on consumer and professional-grade receivers show that GPS and GPS-dependent systems are significantly more vulnerable than previously thought. For example, we show that remote attacks via malicious GPS broadcasts are capable of bringing down up to 30% and 20% of the global CORS navigation and NTRIP networks, respectively, using hardware that costs about the same as a laptop. In order to improve security, we propose systems-level defenses and principles that can be deployed to secure critical GPS and dependent systems.

Everyday GNSS Outages (Unintentional)

Mechanical, Human Error

Antennas are easily damaged and can interfere with each other

Human error in GNSS system operations

GPS cable conduit dangling in the wind

Harmonics or radiation from nearby electronics, failures or misaligned transmission equipment

Natural, Environmental

Lightning hits and high winds take out antennas, antenna icing

Solar flares, atmospheric phenomena

Foliage causes signal masking

Not so Everyday Outages…

“Blue Team Jamming”

Governments may intentionally jam GPS to stop terrorist activities for example:

- Five GPS phones that were used by the terrorists during the Nov 26, 2008 attacks in Mumbai
- Terrorists using GPS to navigate and organize anti-government activities
- War

Outages Happen

Event	Duration	Cause & Impact
Moss Landing, CA	15 April – 22 May, June	TV antenna pre-amp radiating in GPS/L1 band, GPS
San Diego, CA	22 Jan, 2007	wide-scale denial of GP
Leesburg, VA	July 2011 - January 2012	Control Center, ZDC
Las Vegas	March 2012	Las Vegas airport ground stop for approximately 1 hour

March 2011: a U.S. military reconnaissance aircraft was forced to land … due to GPS jamming…jamming supposedly originating with the North Koreans.

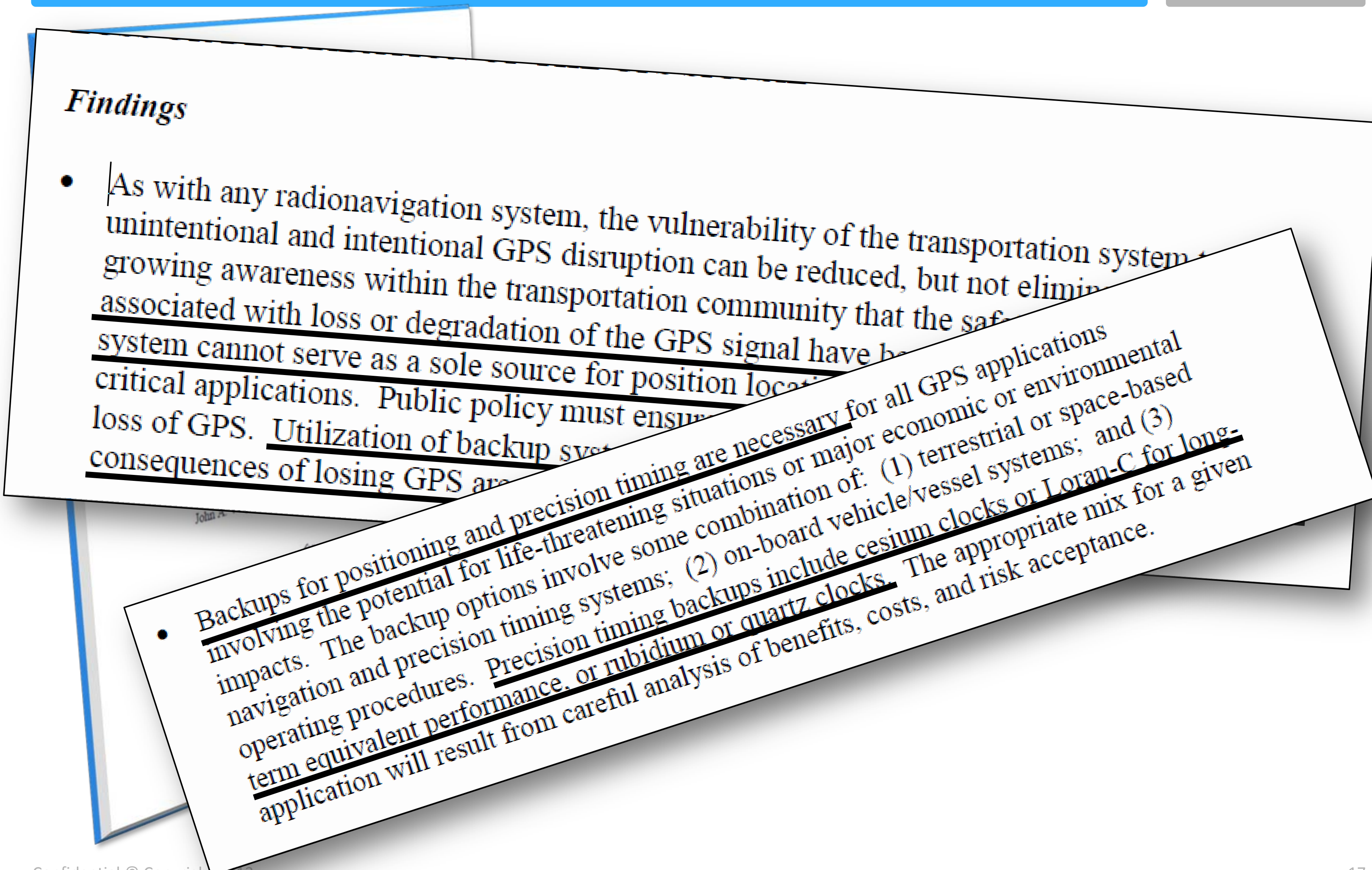
March 2011: North Korean military units jammed GPS signals in some parts of South Korea. …. It was believed that 146 cell sites were knocked out.

Dec 2011 Iranian state media claimed GPS meaconing (among others technique) was used to capture a U.S drone aircraft.

May 2012: "North Korea pumps up the GPS jamming in week-long attack"

Source: Examples compiled from published reports and open literature

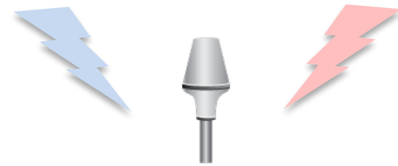
Timing Backups are Necessary



Mitigation

Mitigation Alternatives

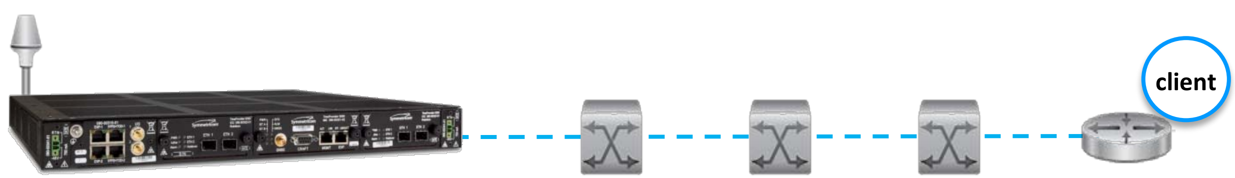
- Dual GNSS Reception



- Oscillator Holdover

- Cesium Primary Reference

- Network Distributed Timing



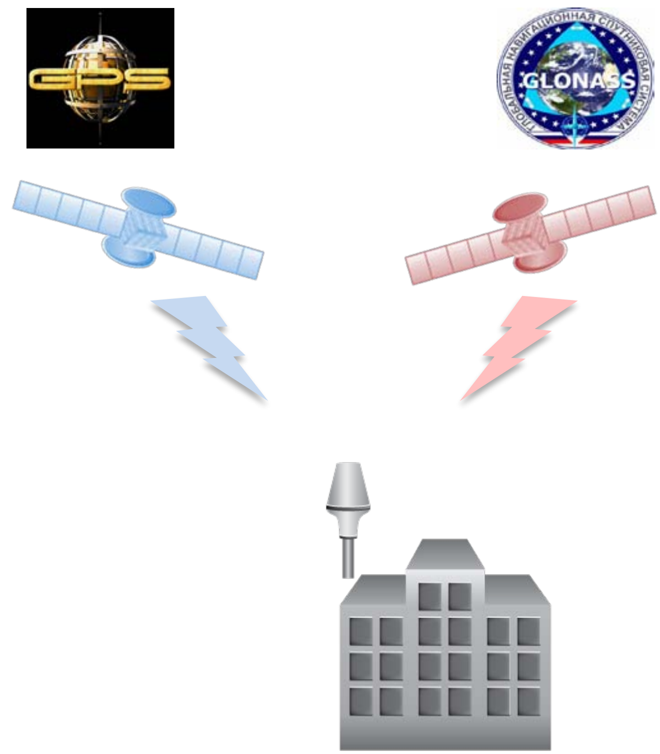
Each has pros and cons, benefit and cost differences.

Not mutually exclusive—can be used in combination for complete protection.

Dual GNSS Reception

Symmetricom

- Many modern receivers are able to use both GPS and GLONASS signals
  - Galileo and Beidou in the future
- See 24+ satellites at a time instead of just ~12
- If one system is impaired (anything from war to human error) the other keeps you in service
- Another benefit: increases the probability of viewing satellites in urban canyons, obstructed environments.



Holdover

Symmetricom

Holdover: continuing operation when the primary timing and synchronization source is lost.

When GPS is lost, timing is held by the oscillator in the equipment.

- The period of effective holdover depends on three criteria
  - Timing requirements of the application
  - Performance of the holdover oscillator—higher quality oscillators provide longer holdover
  - Temperature changes, both degrees of change and speed of change, affect holdover performance

There are a wide variety of oscillator types in use today.
Each provides a different performance/cost profile.

OCXO and Rubidium are most common when holdover is important.

Examples of Holdover Requirements and Performance

Symmetricom®

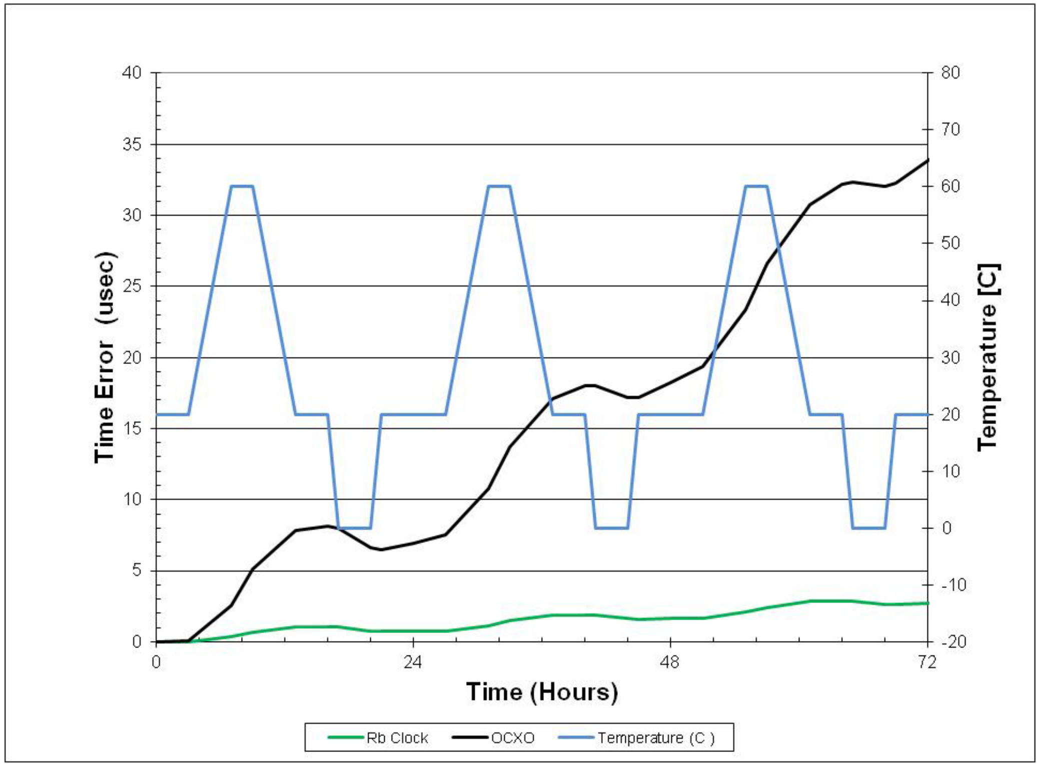
- Power Substation LANs
  - Smart Grid Substations require ±1 µsec timing accuracy (IEC 61850)
  - OCXO: about 10 minutes
  - Rubidium: about 8 hours
- Wireless Networks: GSM and LTE-FDD
  - Base stations require 16 ppm accuracy (frequency) at the network interface (3GPP)
  - OCXO: about 1 month
  - Rubidium: years (CDMA, with phase timing requirement: 3 to 7 days)
- Wireless networks: LTE-TDD and LTE-A
  - ±1.5 µsec to ±5 µsec: phase timing standards are still works-in-progress (3GPP)
  - OCXO: about 30 minutes (±1.5µsec)
  - Rubidium: about 24 hours (±1.5µsec)
- Enterprise: Data Center LANs
  - No standard, but lets say ± 1 millisecond is the objective (using NTP)
  - OCXO: about 1 day
  - Rubidium: over 60 days
- Enterprise: High Frequency Trading Network LANs
  - No standard, but lets say ± 1 microsecond is the objective (using PTP)
  - OCXO: about 10 minutes
  - Rubidium: about 8 hours

Actual performance will vary widely depending on the quality (cost) of the oscillator and environmental conditions.

Rubidium Atomic Clock Holdover

- Service continuity
- Fewer truck rolls
- Fewer off-hour repair calls

Rubidium versus OCXO time error over temperature changes



Rubidium performance is 5 to 8 times better than OCXO.

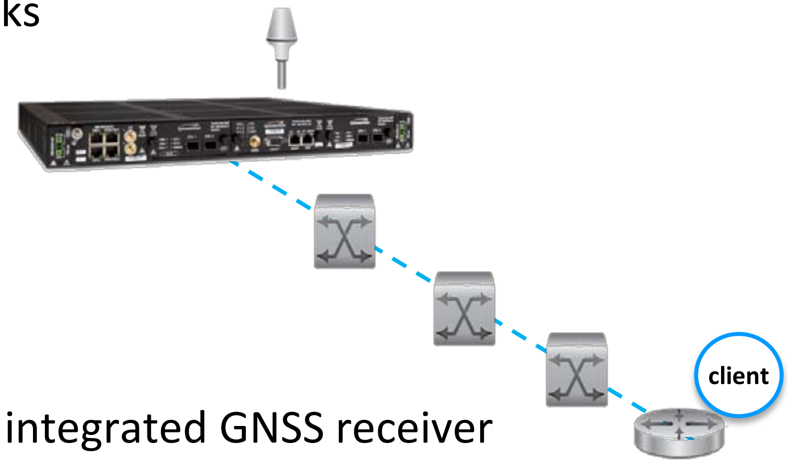
Ultimate Holdover: Cesium Technology

- Cesium technology is considered the most comprehensive holdover option against GNSS vulnerabilities
  - No meaningful frequency drift
  - Maintains 5×10^{-15} accuracy over the life of the instrument
- Critical for long-term autonomous operation
- No on-going calibration required
- More expensive than Rubidium and OCXO
  - Consumes more power and space
- Typical commercial applications
  - Telecommunications infrastructure
  - Power Utility infrastructure
  - Research facilities

Cesium atomic frequency is used as the international definition of the second

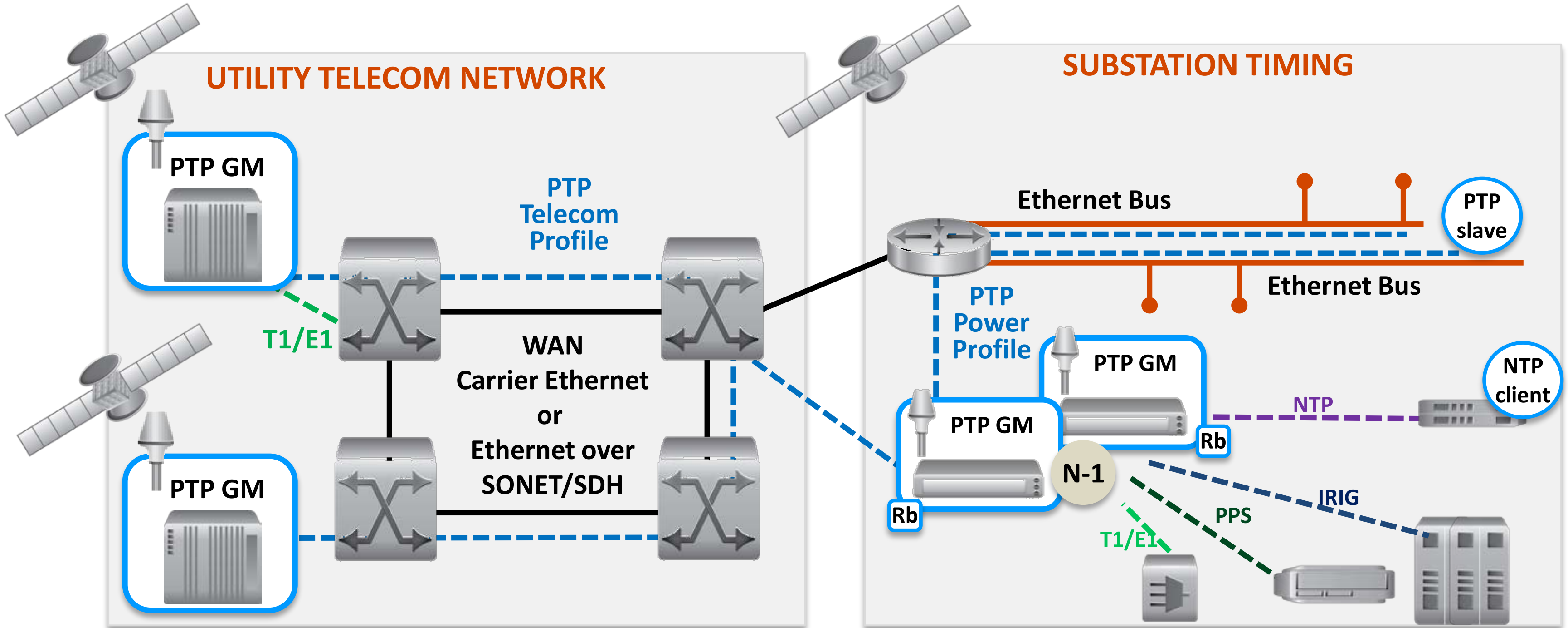
Network Distributed Timing

- Local and Wide Area Networks:
  - Communications Service Providers: Wireless and Wireline
  - Power Utilities: Data and Control Centers, Telecom Network, Substation Networks
  - Information & Communications Technology Operations: High Frequency Trading, Data Centers & WANs, Cloud Computing Networks
- Timing Technologies
  - GNSS remains the primary reference source
  - IEEE 1588 Precision Time Protocol (PTP)
  - Network Time Protocol (NTP)
- Primary Timing Equipment
  - PTP Grandmaster Clock or NTP Time Server with integrated GNSS receiver and/or Cesium reference
  - PTP or NTP client embedded in networked equipment
  - Oscillators (OCXO, rubidium) in network equipment for extended holdover



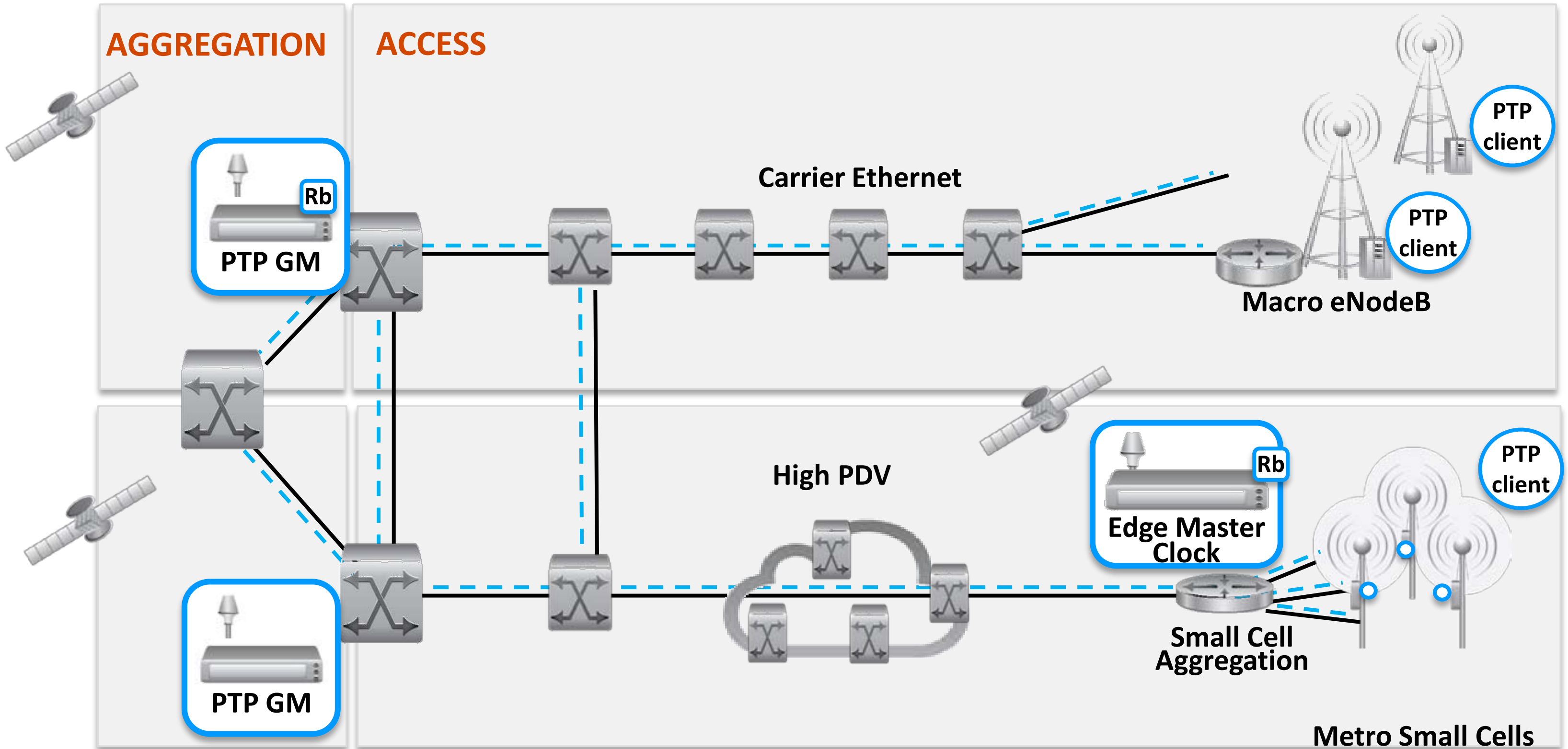
Back-up the primary reference with another source a long distance away, mitigating local impairments and outages

Network Distributed Timing
Power Utility: Substation Networks



- PTP Grandmaster in the substation, microsecond accuracy for Smart Grid measurement equipment
- Redundant deployment for N-1 protection
- Eliminate "GPS antenna farms"
- Rubidium for extended holdover
- Backup and support with PTP over the telecom network

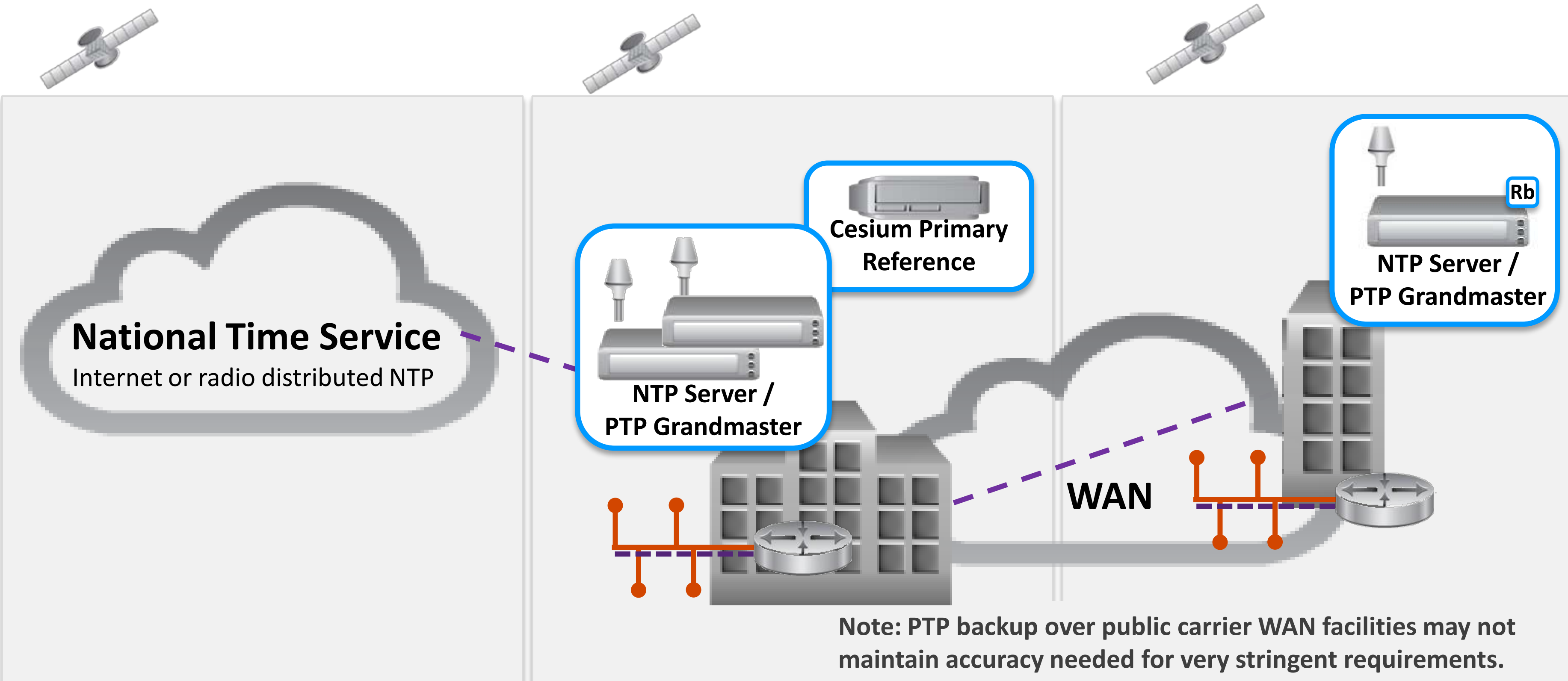
Network Distributed Timing
CSP: 3G and 4G Mobile Networks



- PTP Grandmasters are deployed near the core or near the edge depending on timing requirements ability of backhaul to maintain accuracy
- Multiple deployment locations allow Grandmasters to backup each other

Network Distributed Timing Computing Centers

- Data Centers, Billing Centers, Operating Centers, Cloud Networks



- Multiple time sources
- NTP peering, PTP redundant master clock deployments
- Dial-up and radio broadcasts
- National time services: NIST, USNO, JJY, ITU-R TF583.4

Summary

COMMUNICATIONS

ENTERPRISE

POWER UTILITY

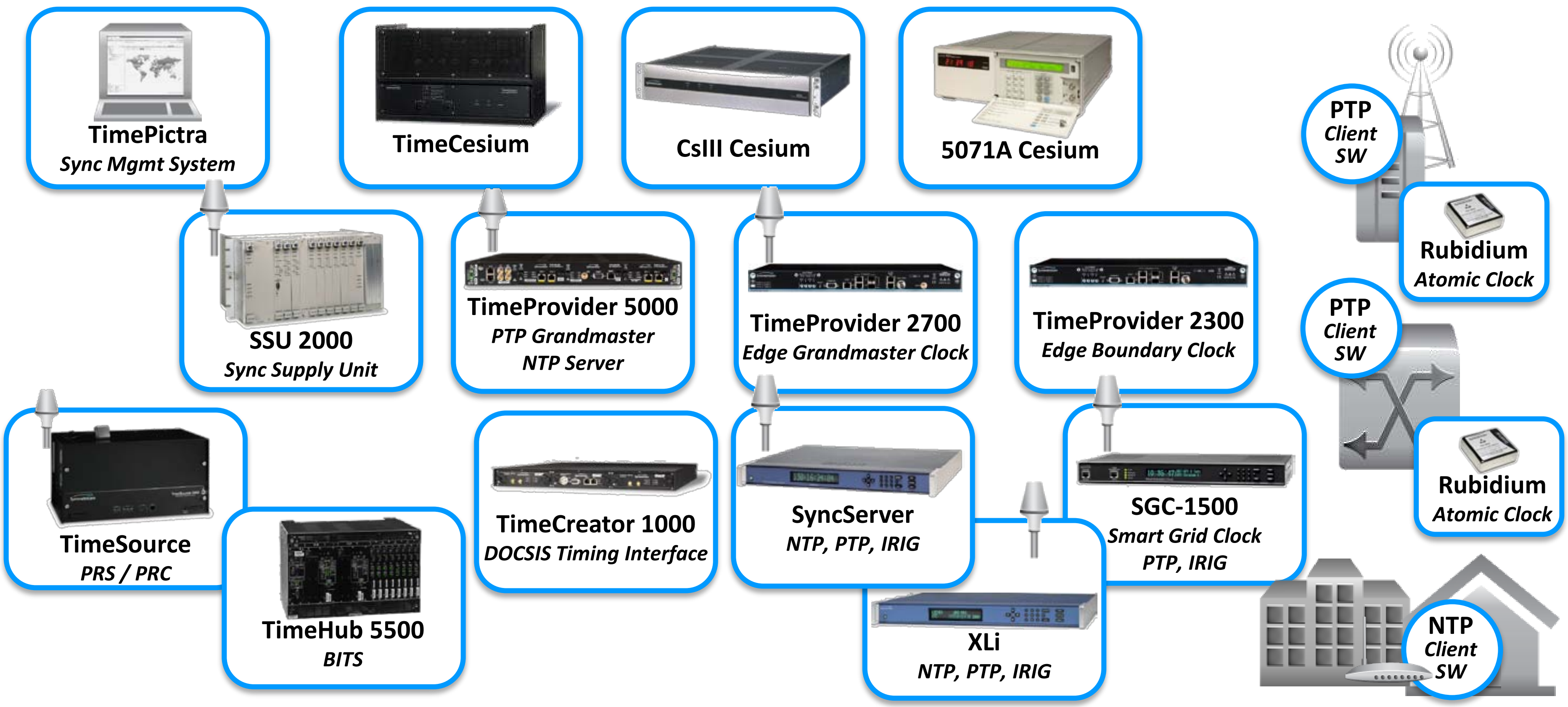
GOVERNMENT

Protect your time

- Dual GNSS reception: GPS and GLONASS
- Extended holdover: rubidium or cesium
- Multiple primary time sources: redundant clocks and alternatives sources, distributed geographically

- Each has pros and cons, but they are not mutually exclusive. Best practices will use them in combinations.

Symmetricom Solutions



Symmetricom is well positioned to ensure our customers are able to protect against GPS vulnerabilities across all applications

Visit our website or contact us for additional information.

www.symmetricom.com

Thank You.

Mitigating GNSS Vulnerabilities In Commercial Networks

Kris Sowolla
ksowolla@symmetricom.com

Related, recorded webinars from Symmetricom:

“Mitigating GPS Vulnerabilities in Mission Critical Applications”
“NTP or PTP: Which is the Best Network Timing Protocol for your Enterprise Application Needs”

A link will be in your “Thank You” email message.

Symmetricom, Inc.
2300 Orchard Parkway
San Jose, CA 95131-1017
Tel: +1 408-428-7907
Fax: +1 408-428-6960

www.symmetricom.com