Secure, Resilient Time Distribution in Power Grids

Doug Arnold
Meinberg USA

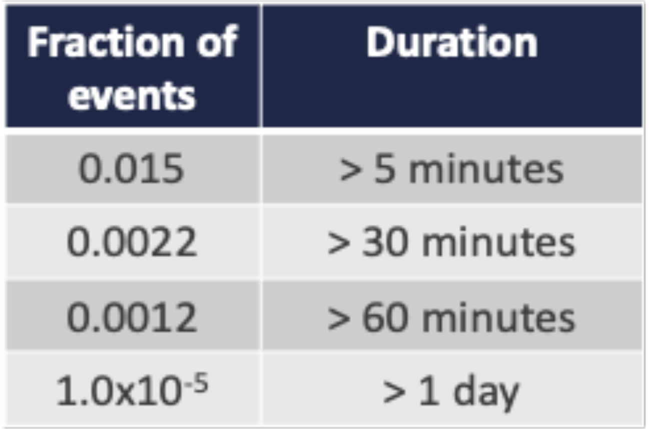
Thanks to Steffen Fries, Andrej Görbing, Andreas Güttinger, Siemens
Herb Falk, Outside the Box Consulting Services
for help with network security graphics

Summary

- Threats to reliable time distribution
  - GNSS jamming
  - GNSS spoofing
  - PTP message injection
- Mitigations
  - Holdover
  - Timing source diversity
  - Algorithms
  - Network security

GNSS Jamming and Spoofing

L1 + L2 Jammer
In stock at
Amazon
$24



Fraction of events	Duration
0.015	> 5 minutes
0.0022	> 30 minutes
0.0012	> 60 minutes
1.0x10^{-5}	> 1 day

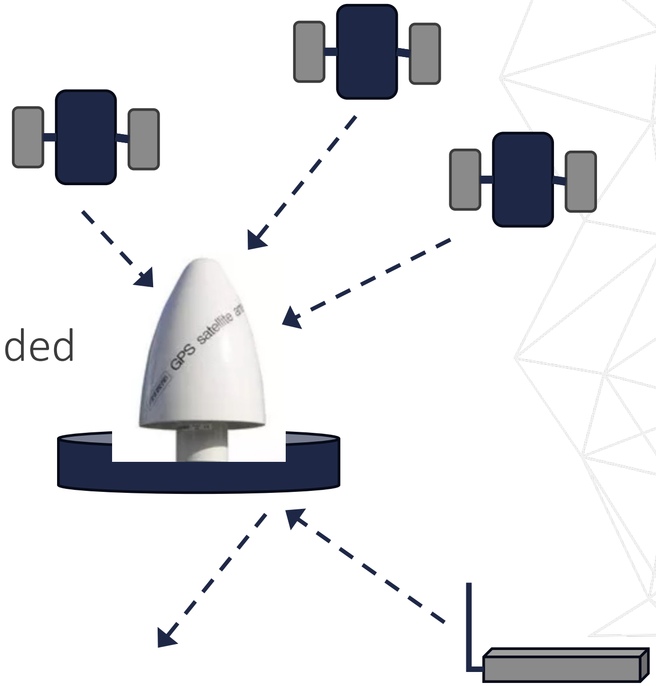
Data from STRIKE3 PROJECT
Most jamming short from vehicles
Long-term jamming rare in US

Amazon Prime
2-day delivery
< $350

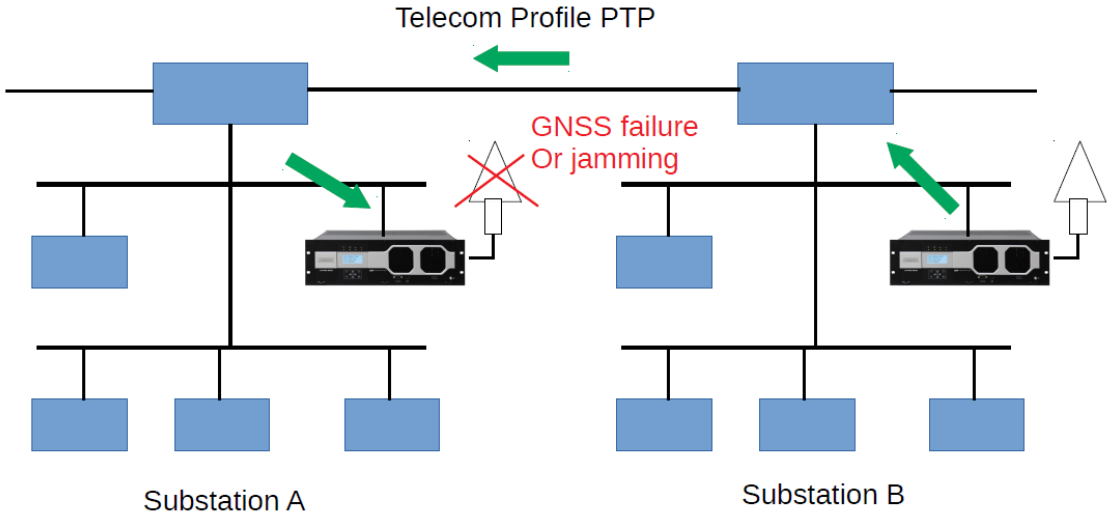
Software: free
gps-sdr-sim
at github

Jamming mitigations

- Holdover
  - PTP GMs typically have many oscillator choices
  - Substations are outside: **Temperature spec is the most important**
  - High end OCXOs often have better temperature specs than atomic clocks
- Source diversity
  - Time server with two GNSS receivers and separated antennas
  - PTP from next substation
  - Precise Time Network (ePTS in ITU-T)
  - Alt PNT (example: Iridium STL)
- Resistant GNSS antennas
  - Ground shielded
  - Phased array
    - Put Null in direction of jamming signal

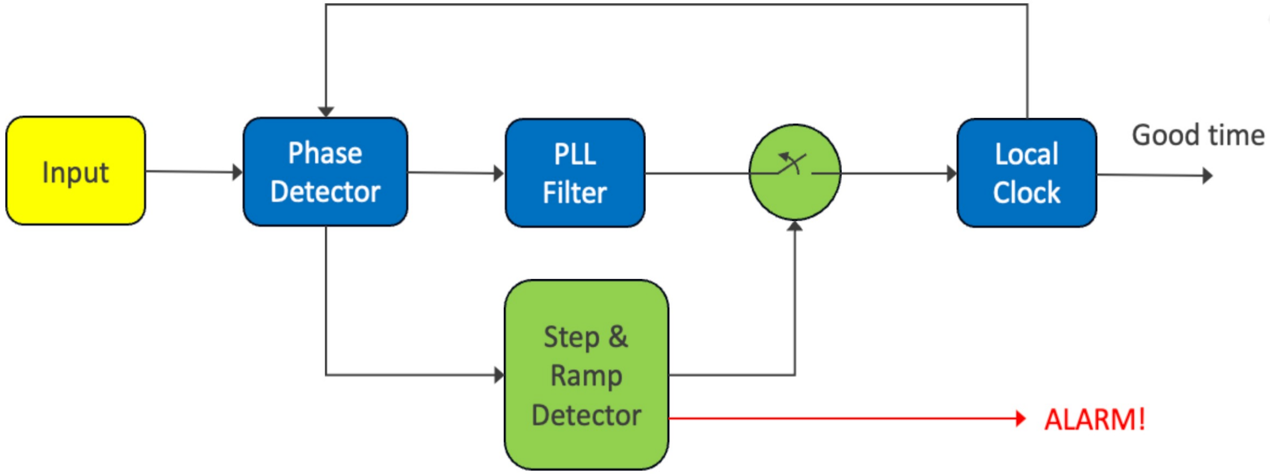


Ground shielded antenna



Spoofing mitigations

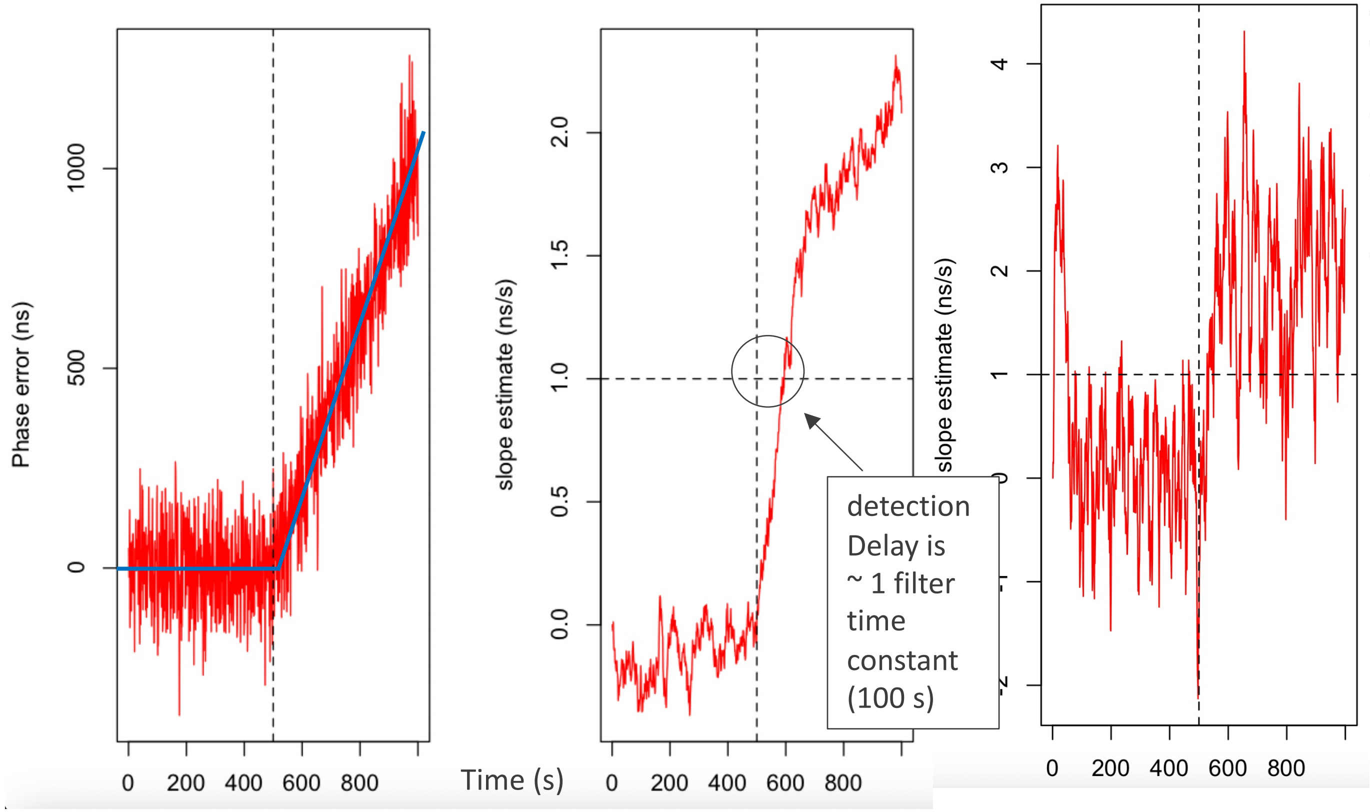
- Resistant GNSS antennas
  - Ground shielded
  - Phased array
    - Put Null in direction of jamming signal if spoofing detected
- Resistant GNSS receivers
  - Detect high signal level
  - Stationary receiver is moving
  - Multiple constellations and bands harder to spoof
- Satellites with encrypted messages
  - Iridium STL (LEO)
  - Atomicron
- Resistant Time servers
  - GNSS is jumping or steering my oscillator too fast



Using your local clock as a BS detector
The more stable the oscillator the more sensitive the detector

Step and Ramp Detection

- False alarms must be rare
- Monitored clock corrections will be noisy and must be filtered
  - Filtering takes time, so detection will be delayed
  - After detecting an error back out clock corrections from the filter delay interval
- Some spoofers jam first to get the receiver to reinitialize before acquiring the spoofed signal
  - The local clock PLL should perform a sanity check before reinitializing after holdover
- Complex algorithms vs simple algorithms
  - Complex algorithms can often out-perform simple ones, in most test cases
  - Complex algorithms are more likely to fail in unpredictable ways than simple ones



detection Delay is ~ 1 filter time constant (100 s)

white phase noise
dev = 100 ns

Slope estimator
Turns ramp into slope
But amplifies noise and requires filtering

filter time constant 30 s results faster detection,
but with false positives

PTP security

PTP Security Threats

- Compromised device in network
  - Compromised switch alters messages
  - Compromised switch delays messages
  - Compromised device injects messages
- False Grandmaster
  - With false Clock Quality values and/or low Priority1 value.
  - Wins BMCA
- Other PTP message injection
  - Replay attack
  - Messages with with forged GM clock Identity

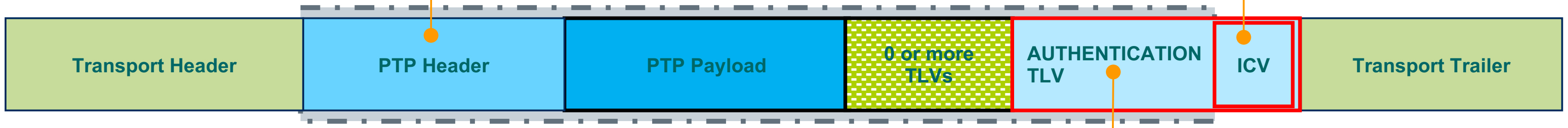
Easiest attack vector (switches have better security)

Aspects of PTP security

- Authenticate message integrity
- Authenticate and authorize security system users
- Automated key management
  - Needed for real (non-lab) networks

Utilized common header information:
- sourcePortIdentity
- sequenceNo

Integrity Check Value (ICV) providing integrity protection for marked PTP packet area



PTP Authentication TLV

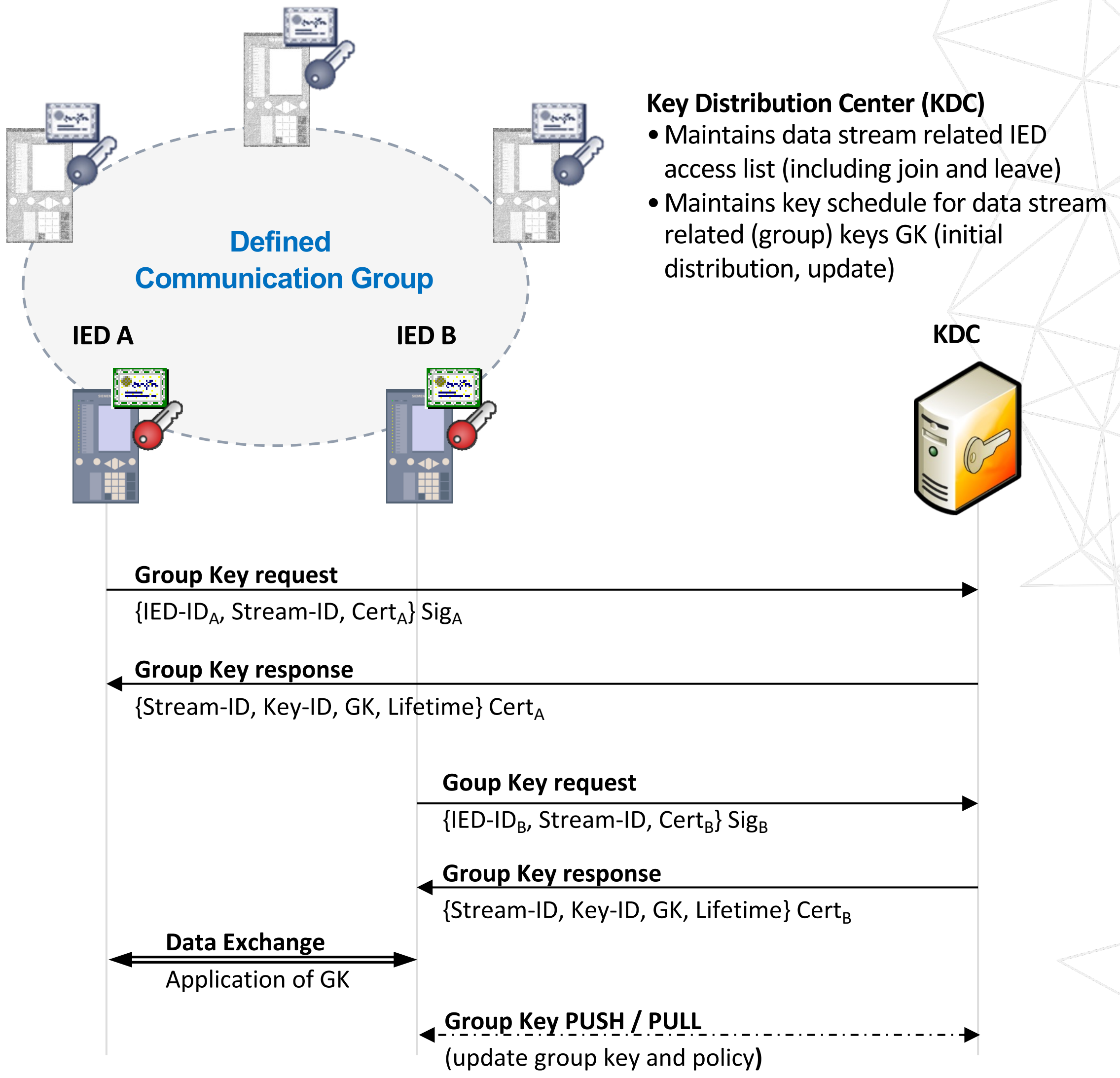
AUTHENTICATIONTLV, structured to support different key management options

Importance of ATHENTICATION TLV proven experimentally

- Research by Marist College and IBM
  - Experimentally demonstrated attacks with injected and manipulated messages in PTP networks
  - Tested both ptp4l (open source) and commercial PTP implementations
  - Both injected and manipulated messages were rejected when they did not have an AUTHENTIFICATION message with a correct ICV
  - See for example:
- L. McPadden, E. Herrera, C. Decusatis, P. Wojciak, C. Kaiser, S. Guendert, "Covert Channels and Data Injection Vulnerabilities for IEEE 1588 Precision Time Protocol using PTP4L," Proceedings of the 55th Annual Precise Time and Time Interval Systems and Applications Meeting, pp 77-86, Long Beach CA, January 2024.

PTP attack mitigations

- Delay Attacks
    - Can't be mitigated by cryptography
    - Compare time from multiple paths
        - PRP, HSR
    - Compare time from IRIG-B
- Injected message attacks
    - Boundary Clocks with Master-only ports
        - BC does not input time from downstream devices
    - MACsec
        - MACsec ASICS can have little jitter because they have to work at line rate
    - PTP Authentication TLV + GDOI key management
        - GDOI already can be used with GOOSE and SV
        - IEEE 1588d-2023 defines use with PTP



Key Distribution Center (KDC)

- Maintains data stream related IED access list (including join and leave)
- Maintains key schedule for data stream related (group) keys GK (initial distribution, update)

Group Key request
{IED-ID$_A$, Stream-ID, Cert$_A$} Sig$_A$

Group Key response
{Stream-ID, Key-ID, GK, Lifetime} Cert$_A$

Goup Key request
{IED-ID$_B$, Stream-ID, Cert$_B$} Sig$_B$

Group Key response
{Stream-ID, Key-ID, GK, Lifetime} Cert$_B$

Data Exchange
Application of GK

Group Key PUSH / PULL
(update group key and policy**)**

Summary

- Threats to reliable time distribution
  - GNSS jamming (mostly short term in North America)
  - GNSS spoofing (First you must detect it)
  - PTP message injection (BMCA makes PTP especially vulnerable)
- Mitigations
  - Holdover (OCXO might be best)
  - Timing source diversity (GNSS, Alt PNT, PTP, PTN)
  - Algorithms (Smart antennas, receivers, and time servers)
  - Network security (MACsec, GDOI)

Thank You!

I am happy to answer questions we didn't get to.

send me an email:
doug.arnold@meinberg-usa.com

MEINBERG

The Synchronization Experts.