

WSTS-2016

Fault-tolerant time sync  
in enterprise: 5 years  
practical experience.



Fault and compromise detection  
and recovery in enterprise networks.

June 2016

# INTRODUCED FAULT-TOLERANCE INTO FULL PRODUCTION IN 2011

Key technologies were:

- Ability to monitor multiple time sources in both server (GM/stratum server) and client (slave)
- Protocol agnostic operation
- Tests for “compromise” of primary source and automated failover to next source.

---

a client may monitor two different Precision Time Protocol (PTP) “master clocks” and three different Network Time Protocol (NTP) servers.

In addition, if the time quality of [the] primary sources becomes questionable, [the client] can now switch from tracking one time source to another, according to a fail-over list provided at configuration time.

- **Sept 19, 2011, press release.**

---

# FOCUS OF OUR WORK IS IN ENTERPRISE COMPUTING NETWORKS: PARTICULARLY FINANCIAL SERVICES

- Commercial networks with
  - Enormous variation in network equipment
  - Standard computer servers at point of use
  - Required accuracy between hundreds of microseconds and sub-microsecond.
- Most often have shared network connections for timing and general data
- Cloud, Big data, Industrial automation, First Responder, Broadcast – have similar requirements

# BASIC APPROACH DISCUSSED IN 2011 WSTS TALK



## Partial solution: fail-over and traceability

```
SOURCE1() {  
  PTPCLIENTVERSION=2; PTPDOMAIN=80; IFACE=eth0;  
  UNICAST=1;  
}
```

```
SOURCE2 () { NTPSERVER=192.168.4.114; }
```

```
SOURCE3 () { NTPSERVER=nist1-ny.ustiming.org; }
```

For FINRA/OATS traceability

If PTP fails – use existing  
NTP distribution

Slide from talk WSTS 2011

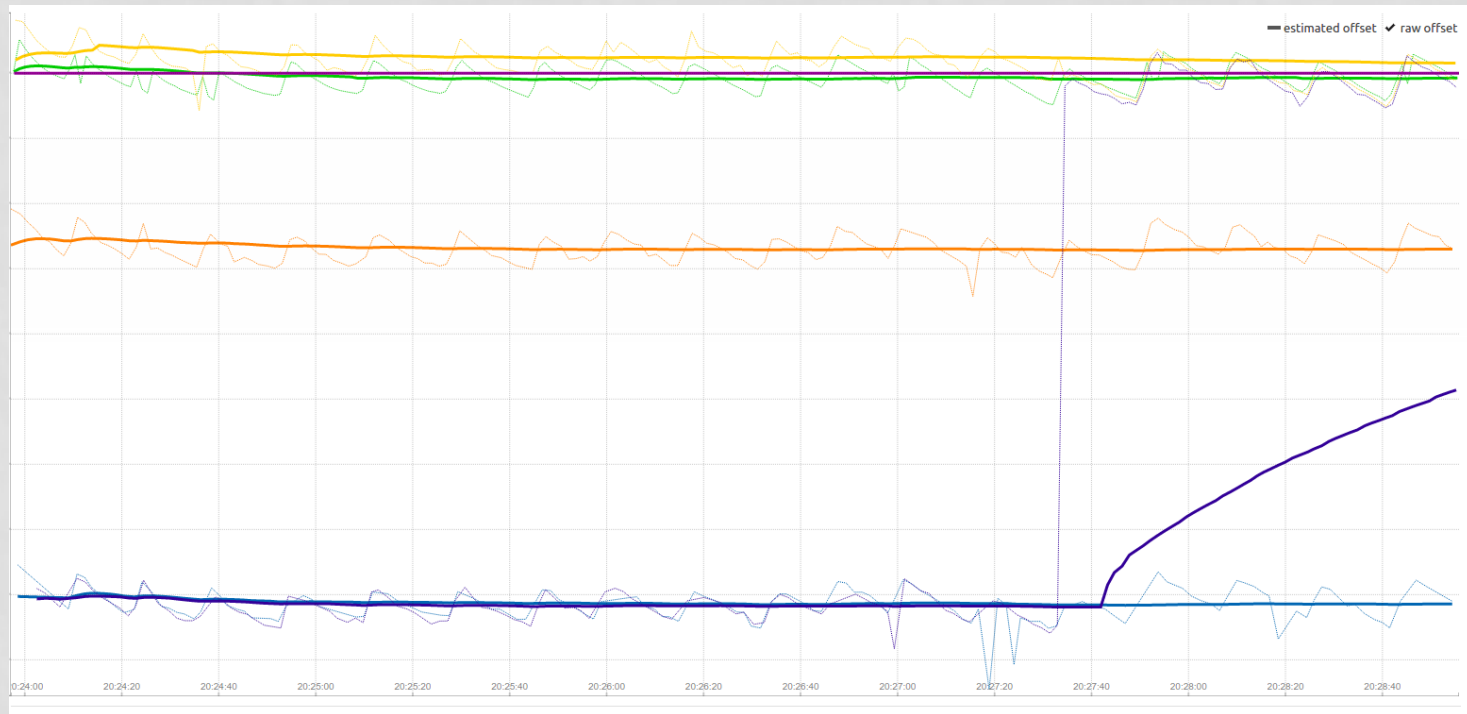
Copyright FSMLabs , 2011.



# MULTIPLE SOURCES – CROSS CORRELATED TO PRIMARY

One secondary permits minimal integrity check fail-over

Multiple high quality secondary sources permits “source check” to outvote primary



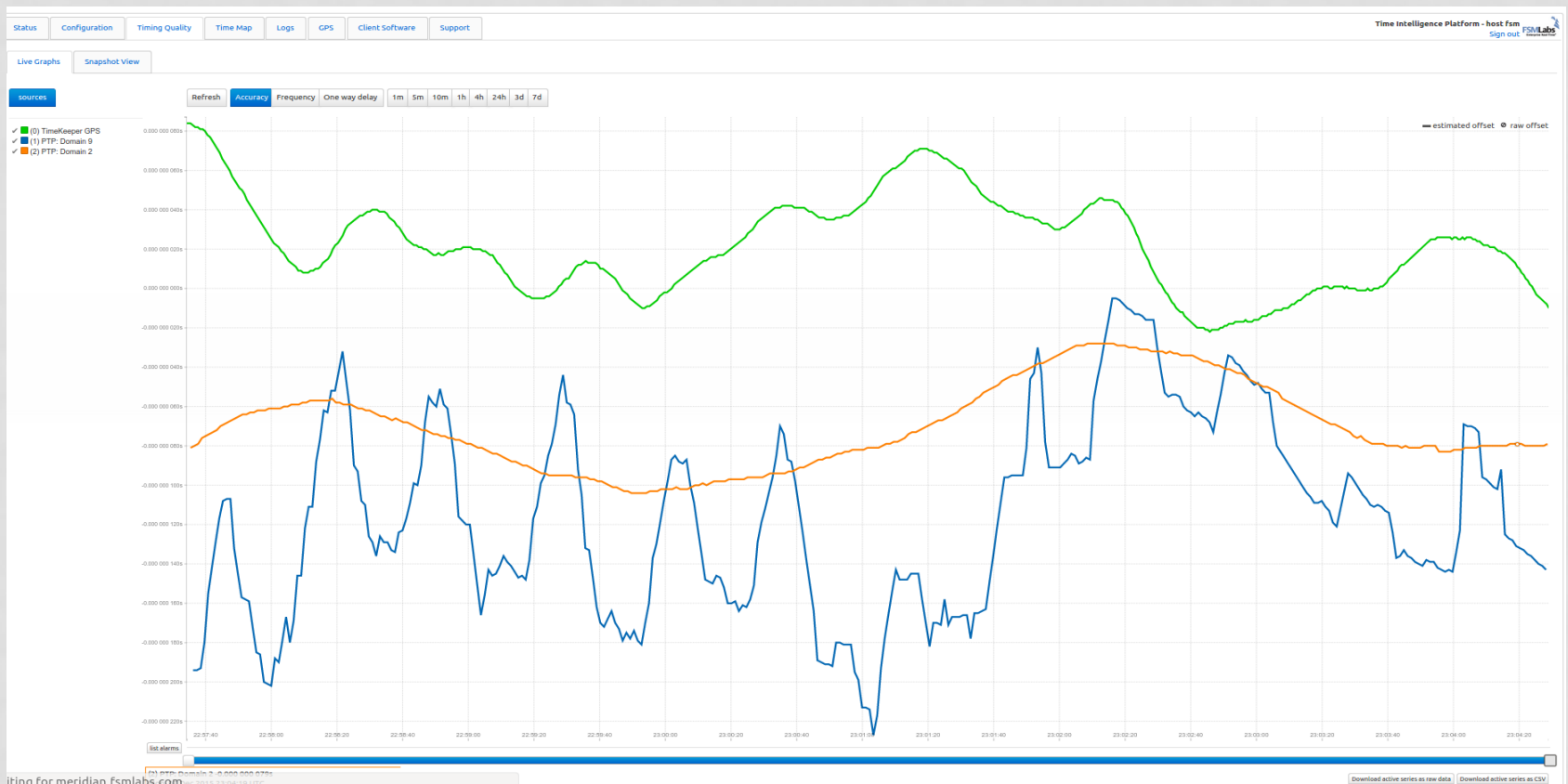
No attempt to aggregate sources to synthesize time.

# 5 YEARS: OUR BASIC APPROACH HAS WORKED WELL

- Protocol agnostic multi-source is a big win (NTP can produce sub-microsecond sync despite what everyone knows).
- Failover triggered by client analytics (where the information is) is powerful.
- Single primary at any one time.
- Use protocols for interoperability, not algorithm design.

# WORKS FOR GPS CLOCK FAILOVER AS WELL AS CLIENT FAILOVER

This clock has 2 PTP sources and GPS(green) all within 200ns (40 Gbps network )





# SYSTEMS WITH SOURCE CHECK SURVIVED MANY FAILURES

- GPS Clock that silently lost GPS and switched to NTP backup, repeatedly.
- Overeager Network Security that cut off part of PTP protocol.
- Month premature Leap Second jumps
- Terrible Switch Boundary clocks that never worked.
- High speed WAN connect with 12 microseconds asymmetry not detected by network admins.



# OTHER SURVIVED FAILURES

- Lightning strikes on GPS antennas
- NTPd servers changing their own sources
- Broken or malfunctioning GPS clocks
- Bad oscillators (or overheated ones ) on boundary clocks
- GPS spoofing and jamming
- Misconfigured routers/switches
- Failed terrestrial PTP sources
- Lost PTP multicasts on switch restarts

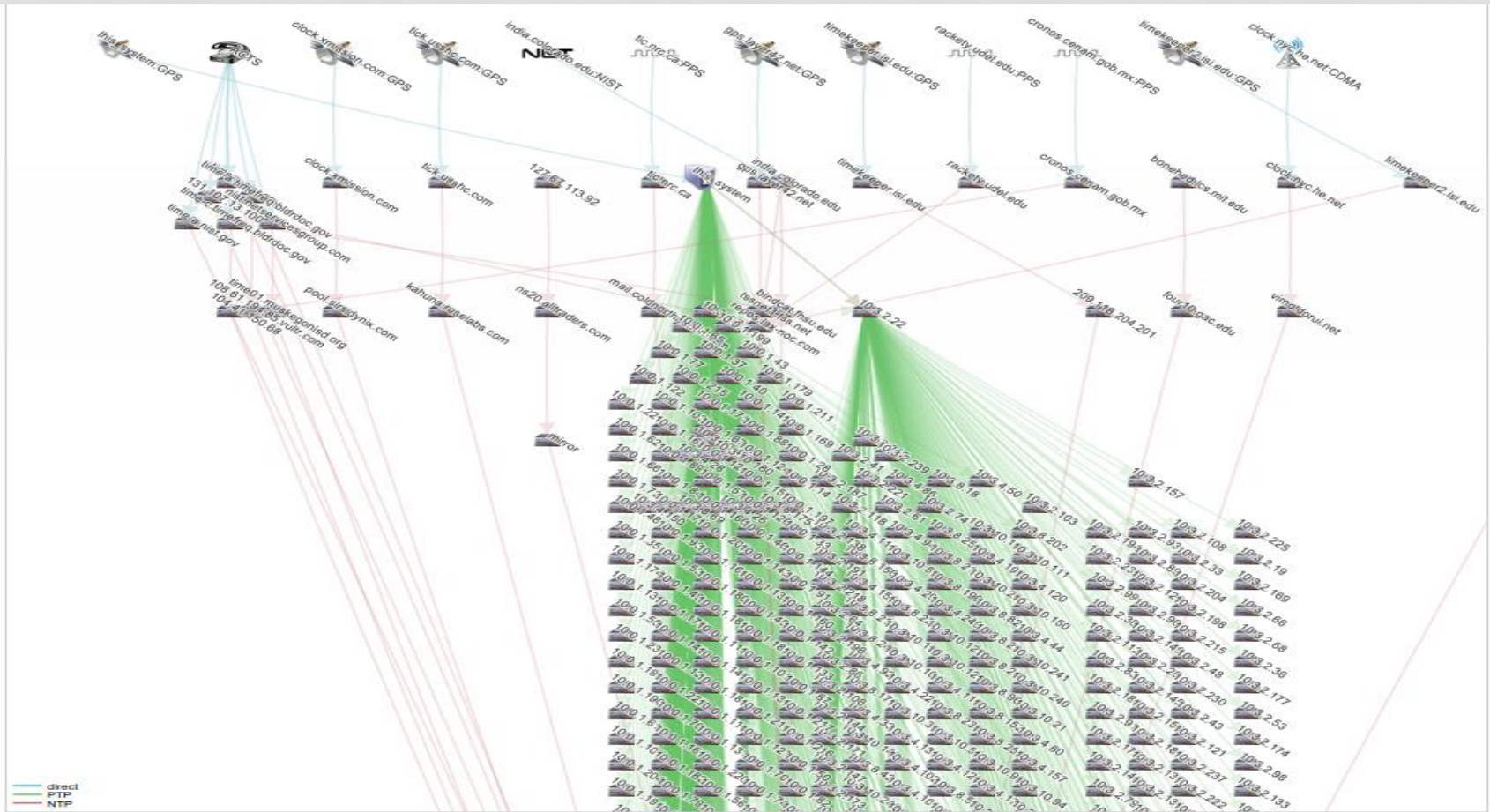
# SURPRISES

- Failures are more common than expected
  - Especially jamming and GPS reception
- Many systems had no reliable sources at all – so failover was not an issue.
- How quickly customers got used to it working and ignored failure signals since the system just recovered.

# ADAPTIONS

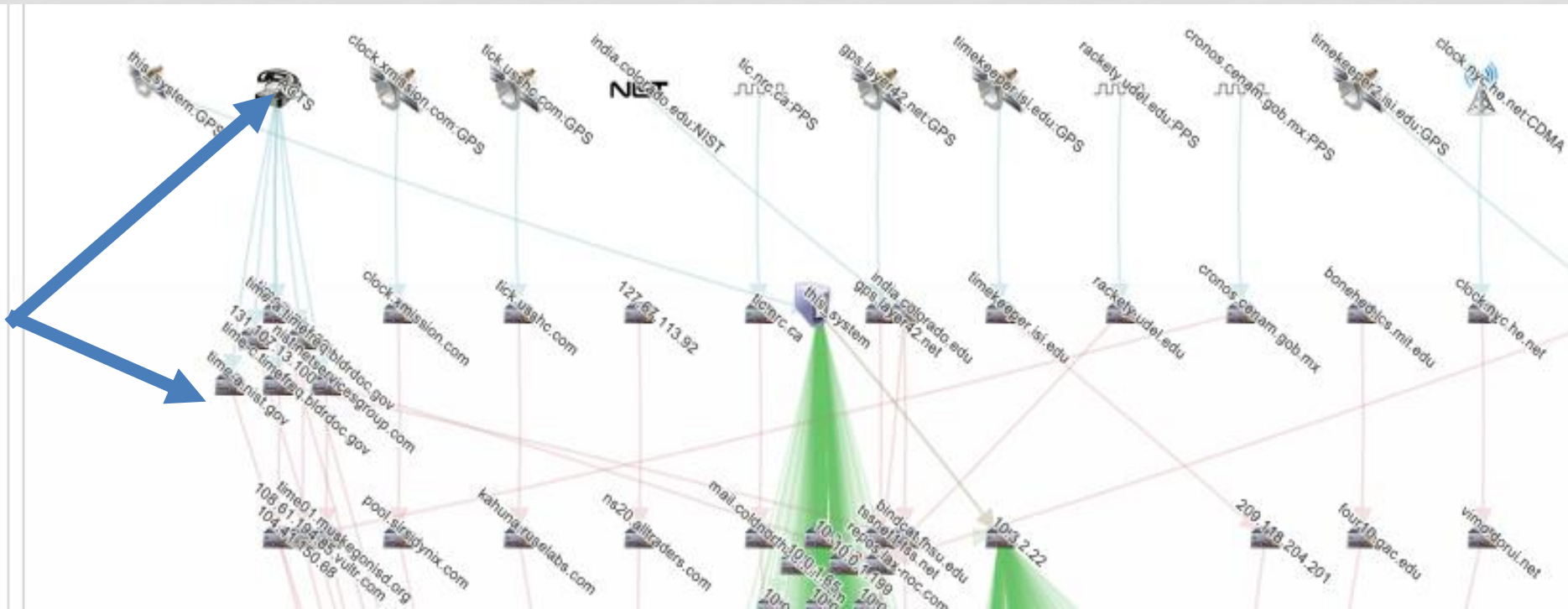
- Due to prevalence of systems with only one or zero reliable time sources, original failover could oscillate between weak sources. Fixed.
- Needed to radically improve diagnostics to help solve problems, find configurations (customers wanted fault tolerance and then repair)
  - Map of network time distribution
  - Deep diagnostic of GPS signal

# TIME MAP - SHOWING ALL SOURCES AND CLIENTS



Green is PTP, red is NTP, blue is source

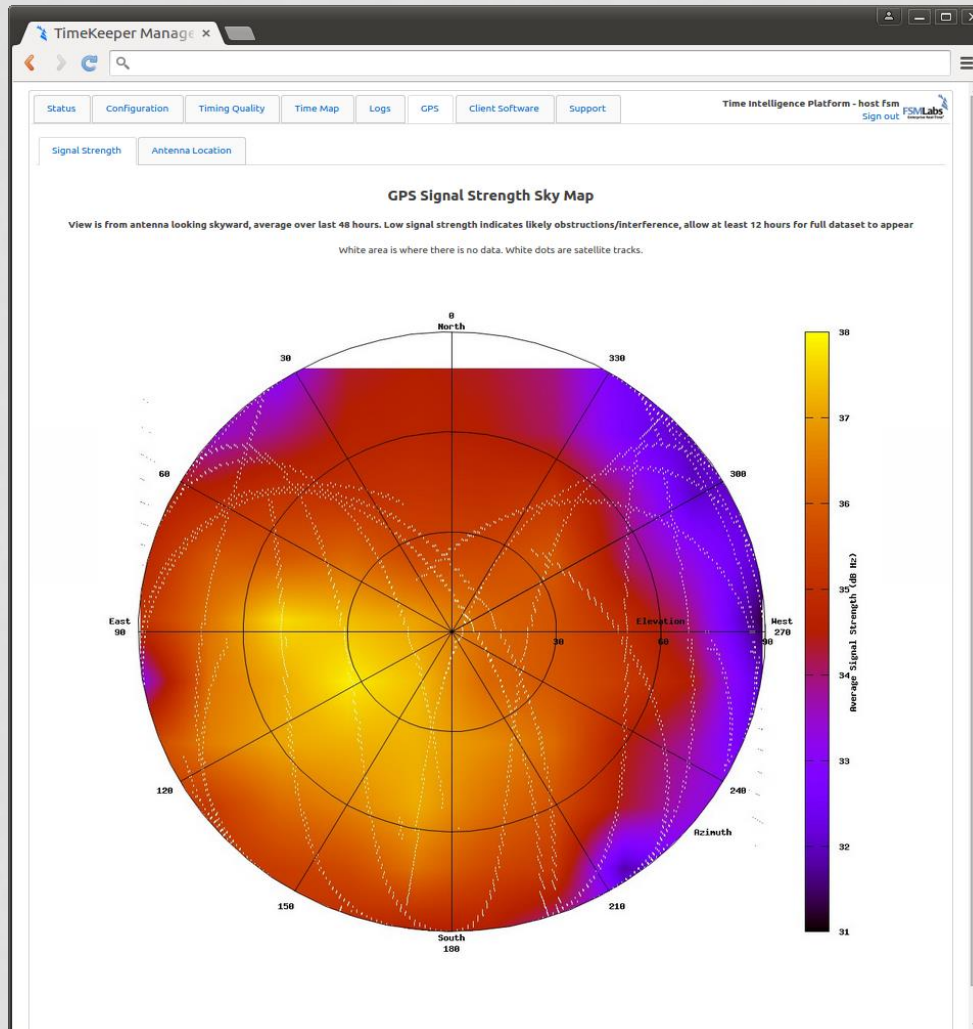
# TIME MAP - OFTEN SHOWED “INDEPENDENT” SOURCES WERE NOT.



Several “independent” sources taking data from same  
“ACTS” modem – bad sign.

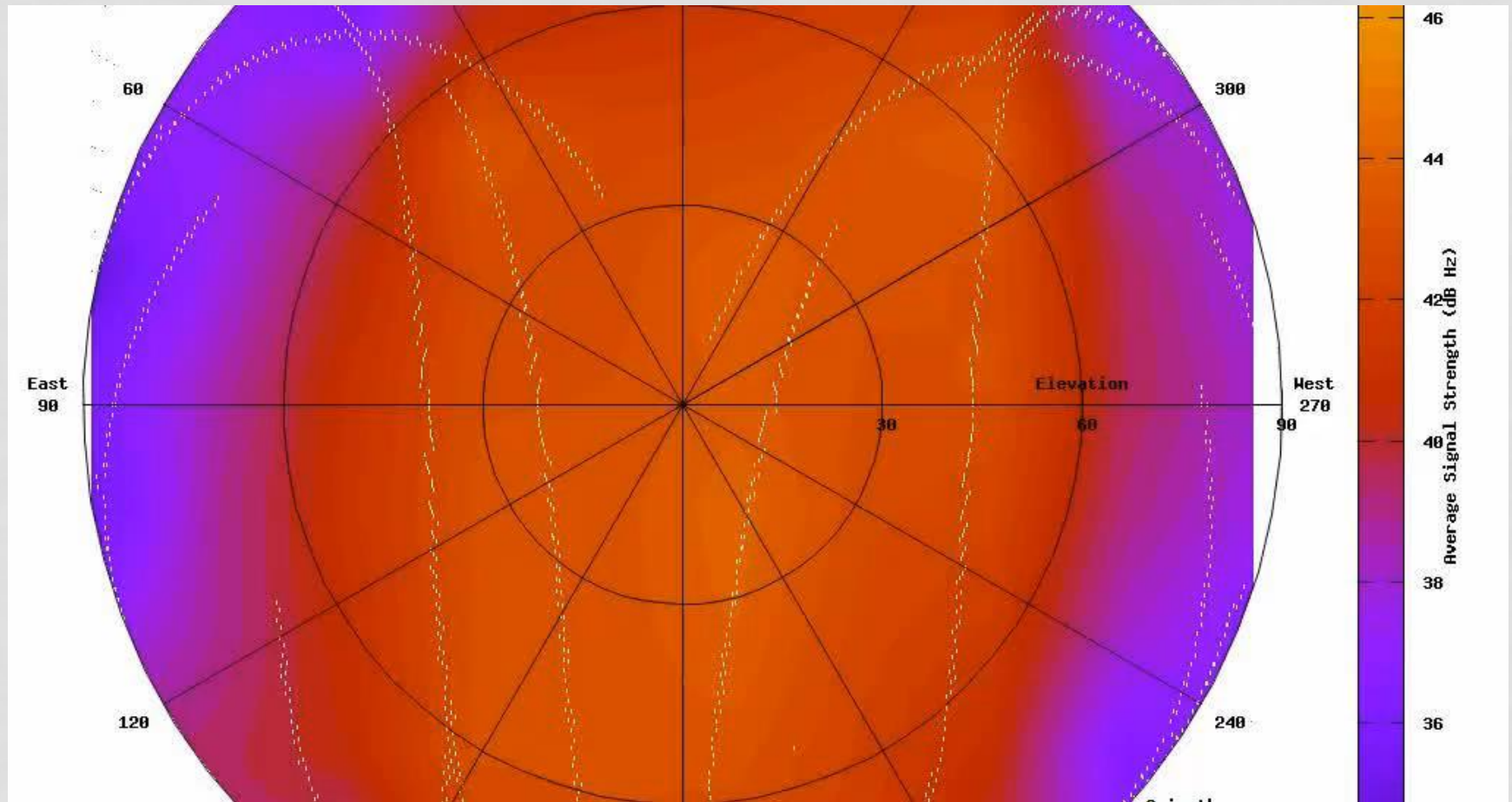


# SECOND KEY DIAGNOSTIC NEEDED TO HELP WITH GPS INTERFERENCE OR JAMMING ISSUES.



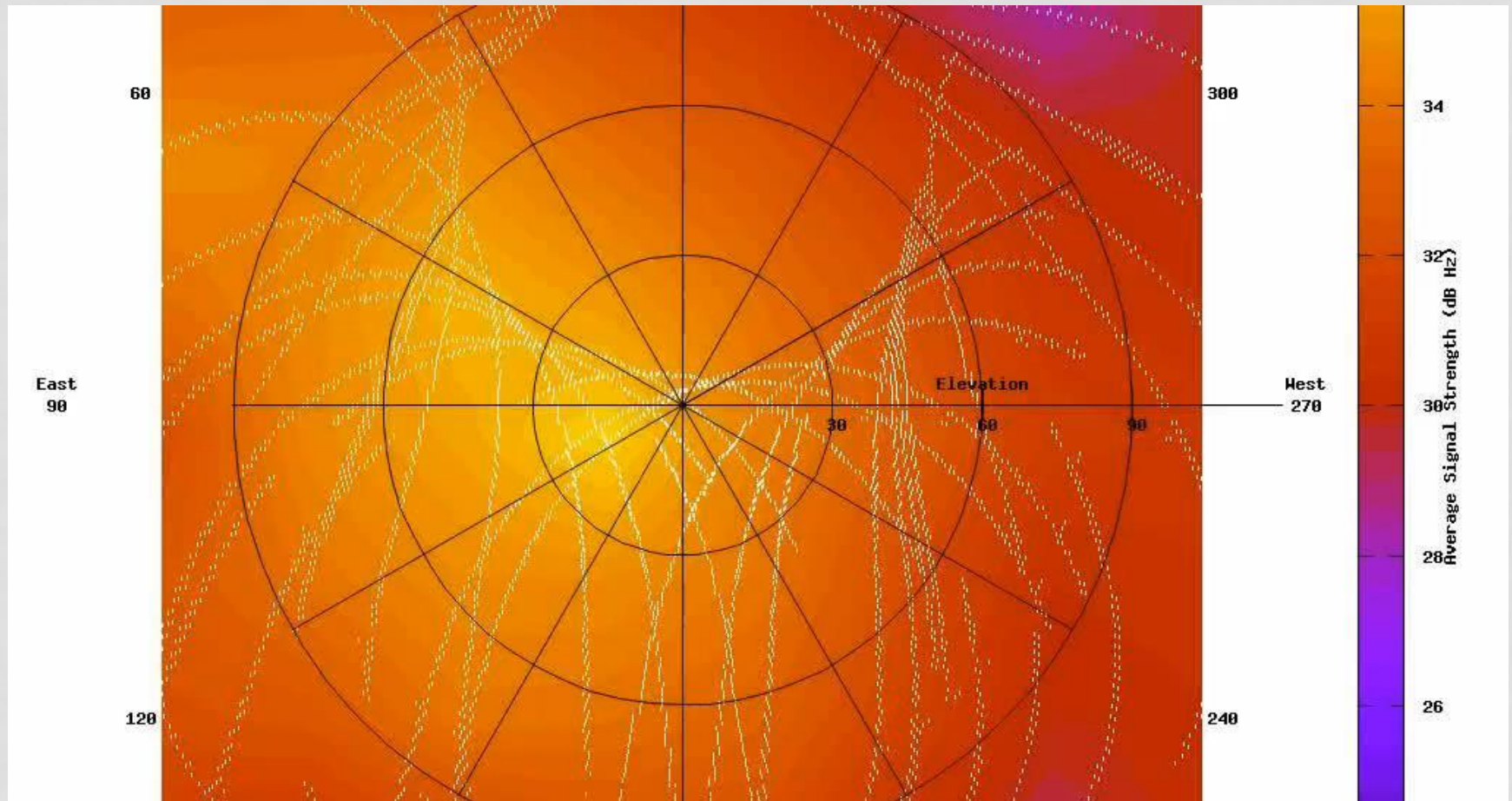
Build specialized heat map from GPS signal data so show composite picture of signal strength. Purple areas show blocked reception.

# NEW MEXICO DURING A JAMMING TEST AT WHITE SANDS.





# JAMMING AT LD4



# SUMMARY OF THE APPROACH

- Time protocol agnostic - PTP, PTP-Telecom, NTP, PPS, Bus Card, ... all are sources
- Multiple sources are essential for
  - Fault-tolerance
  - Security
  - Documentation (e.g. for regulators)
- Intelligence in client/slave: time consumer has information and analytics not available to time sources.

# 5 YEARS EXPERIENCE - SOME WITH GIANT NETWORKS

- Time distribution is really fragile with many points of failure.
- Existing systems are often terrible.
- Security and fault-tolerance are often indistinguishable
- Diagnostics is often as important as resilience.
- People are highly inventive about finding ways to break systems.

## CONTACT INFO

**Victor Yodaiken**  
**FSMLabs, Inc.**  
**11701 Bee Caves Road, Suite 200**  
**Austin, TX 78738**  
**USA**  
**yodaiken@fsmlabs.com**

**Telephone: 1-512-263-5530**

# BONUS SLIDE

Multiple Internet NTP sources pre-Leap Second 2015 as Google time servers “slew” off correct time

