Enhanced Loran

Sherman Lo, Benjamin Peterson

With contributions from the FAA Loran Evaluation Team

Acknowledgments & Disclaimer

- The presenters gratefully acknowledge the Federal Aviation Administration (FAA) Loran evaluation team and Mitchell Narins

- The views expressed herein are those of the authors and are not to be construed as official or reflecting the views of the U.S. Coast Guard, Federal Aviation Administration, Department of Transportation or Department of Homeland Security or any other person or organization.

Executive Summary

- Enhanced Loran designed to provide back up/redundancy to GPS/GNSS in safety critical applications
  - Aviation, Maritime, Precise Time
- Loran for tactical purposes is possible with efficient transmitters
- Loran is difficult, but not impossible to spoof/jam

- Loran future still uncertain

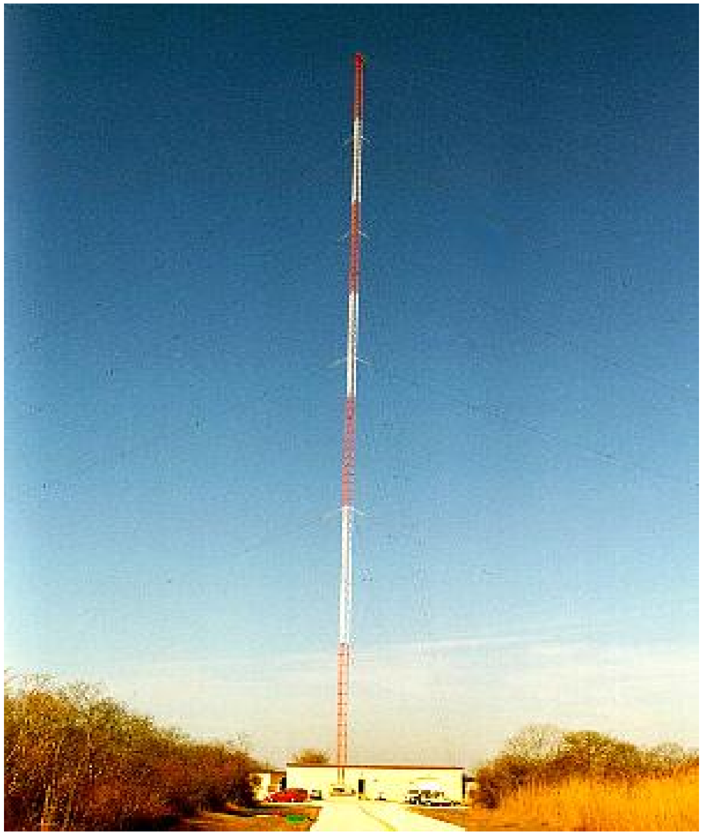
Outline

- General Overview of Loran
  - System & operations
  - Status
- Complement to GNSS in civil critical infrastructure
  - Aviation, Maritime, Timing
- Tactical Loran
- Loran & Jamming/Spoofing

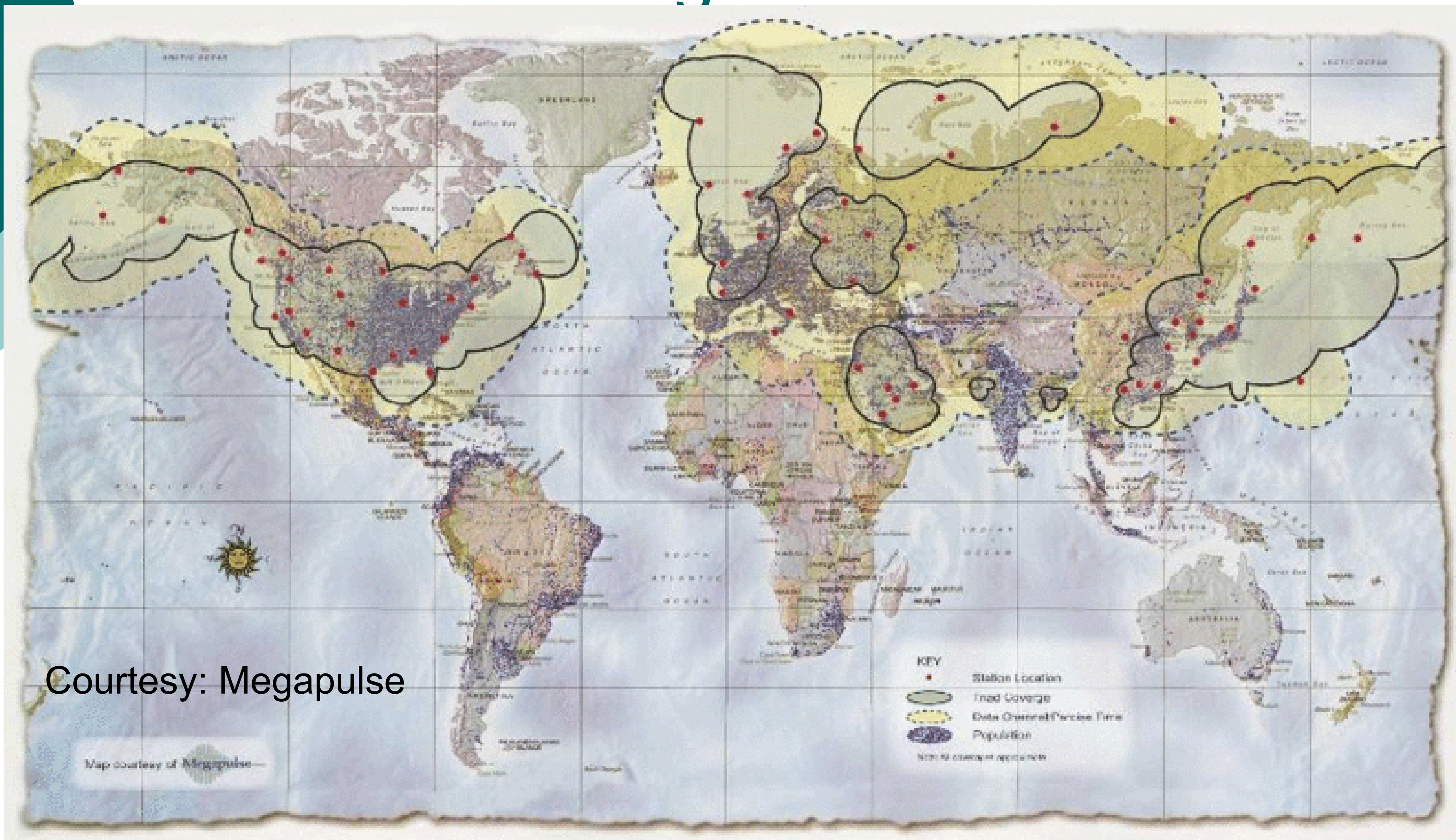
Loran Background

Loran History

- The first all weather continuous operating long range navigation system
  - Pulsed transmission, “TDMA”
- Operational 1958, operated by USCG
- Accuracy ~ 0.25 to 1 mile
  Repeatable ~ 18-90 m
- Horizontal navigation
- Enjoyed widespread use for maritime navigation
- 625’+ tall towers at 400+ kW

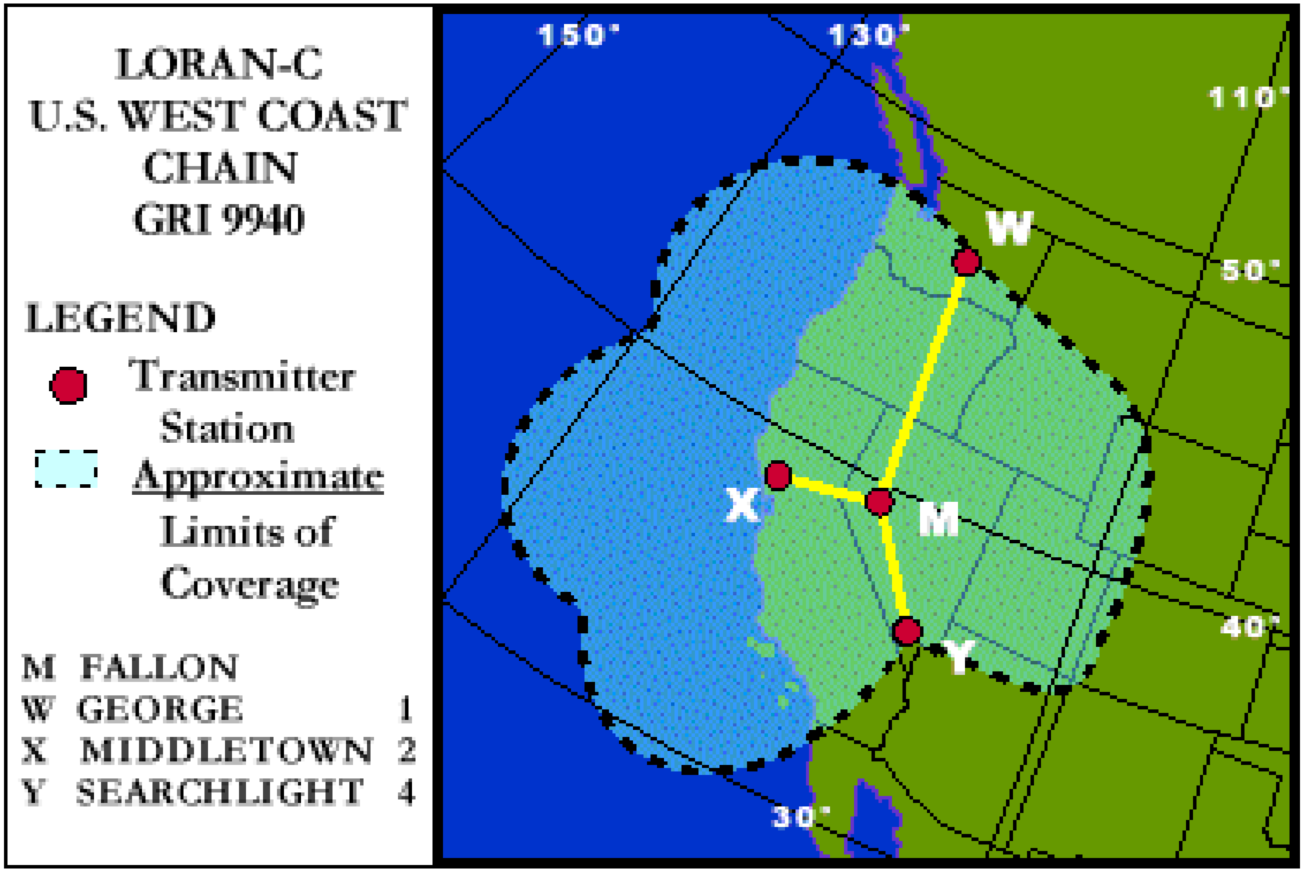


Loran Coverage Worldwide

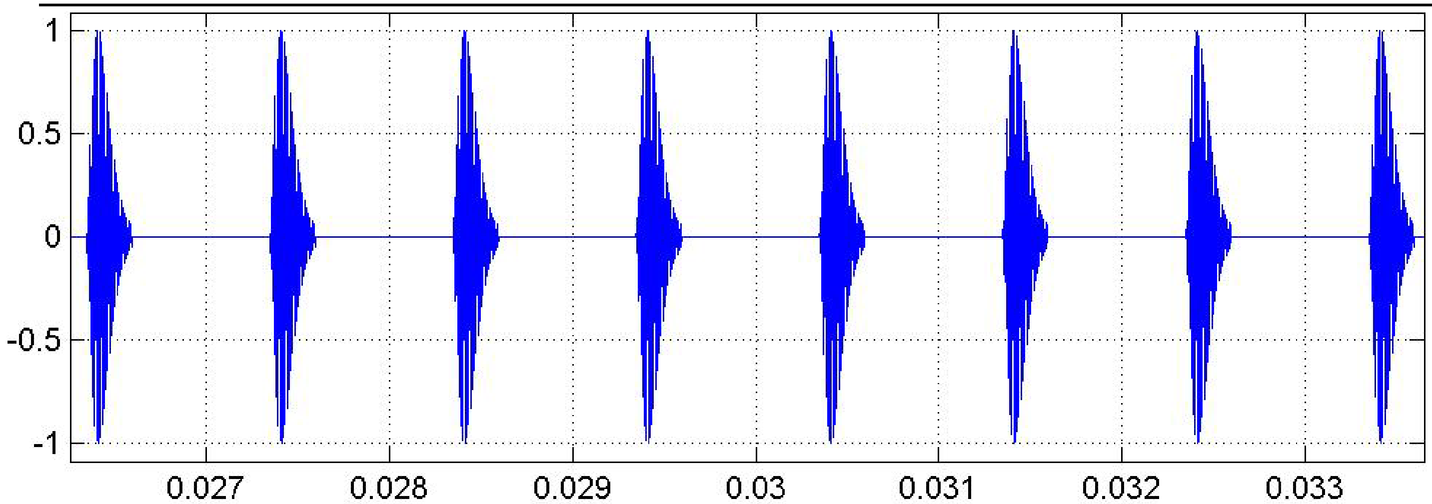


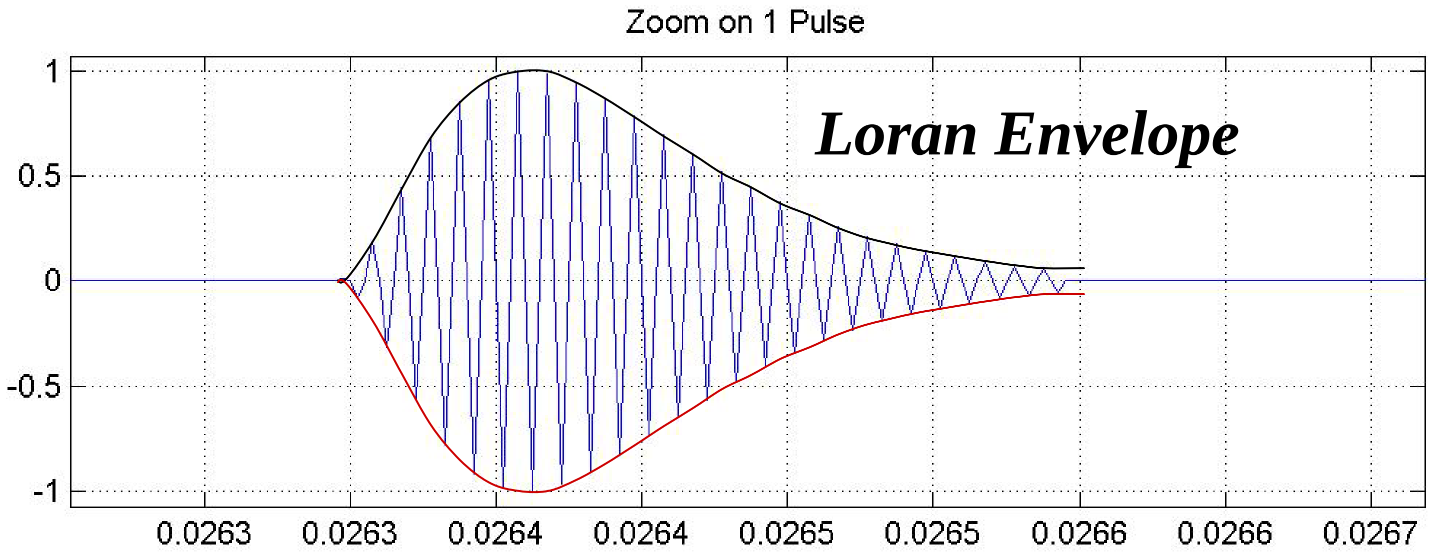
Courtesy: Megapulse

Loran Chain Concept

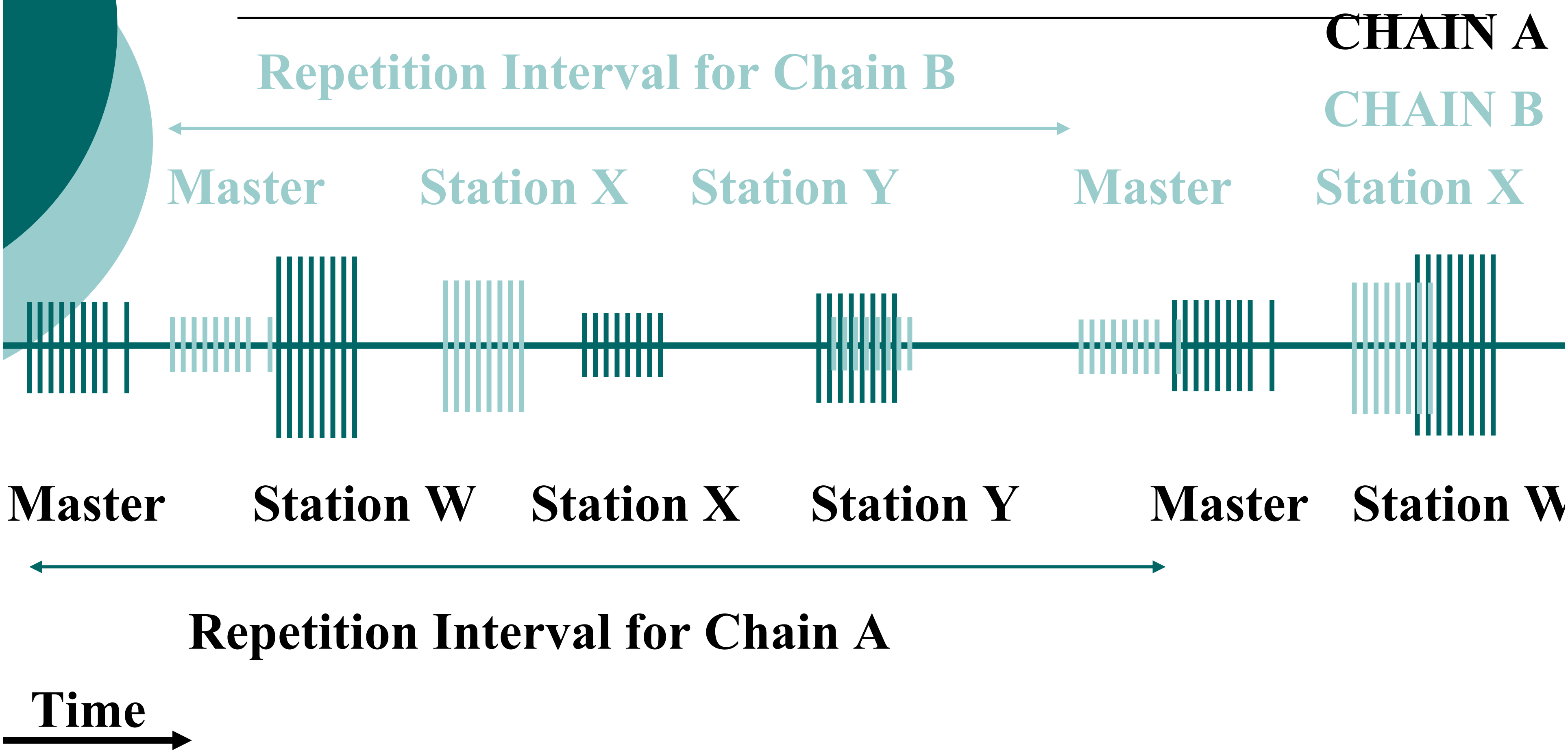


Zoom of Loran GRI



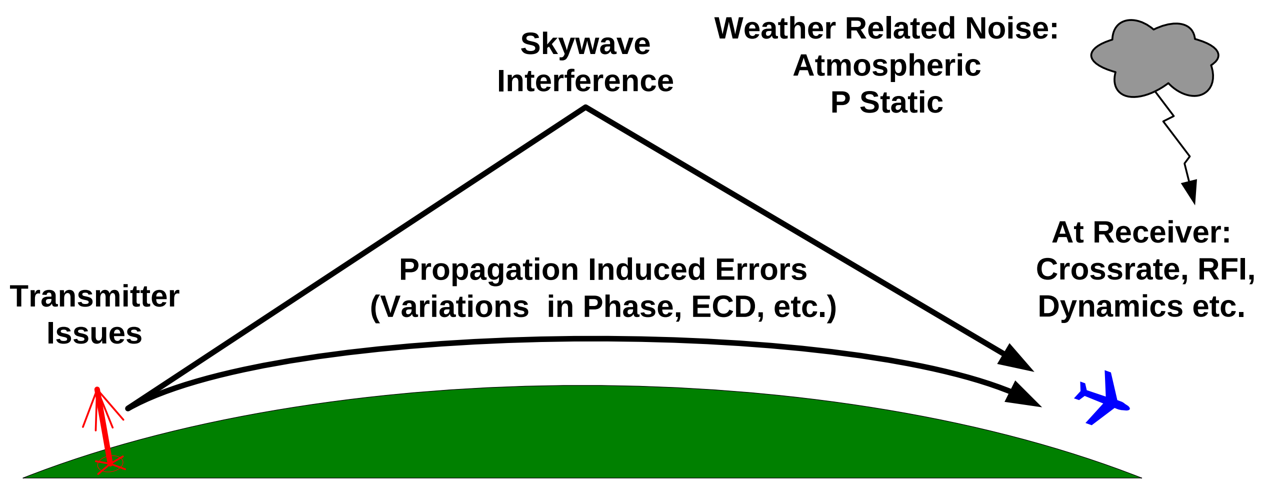


LORAN Chain Timeline



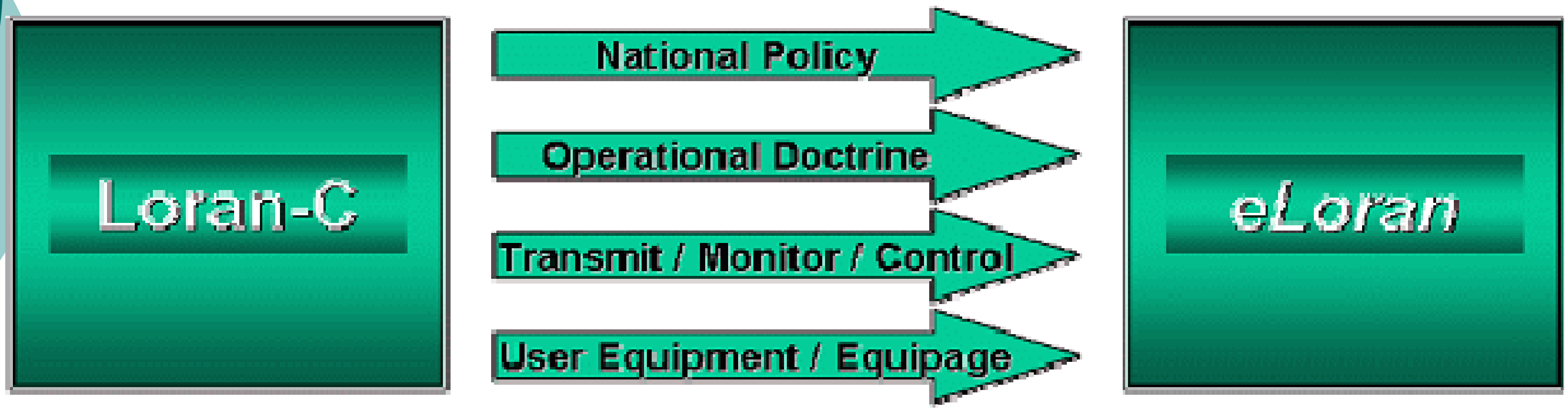
- Other Loran chains can cause interference on desired Loran signals

Major sources of uncertainty



- Noise
  - Thermal & atmospheric noise
  - Precipitation static
- Transmitter jitter (100-500 ns limit)
- Variation of propagation delay
  - Distance dependent (severe case: 500 m peak to peak)
  - Generally slowly varying in time
- Interference (often mitigated by processing)
  - Skywave
  - Crossrate
  - CW & RFI
- Reradiation
  - Large metallic elements (i.e. bridges)
  - Distortion about buildings

Enhanced Loran (*eLoran*)



- Next generation of Loran
- Provides changes to improve accuracy, reliability, integrity, availability
  - Governmental Policy changes (prop. delay (ASF) tables)
  - Operational changes (TOT control)
  - Transmitter equipment (control, Cs clock, etc,)
    - Data Channel (integrity, dLoran, timing)
  - User equipment (All in view receiver, H field antenna)
- These changes are or are being implemented

Loran Status

Loran Status

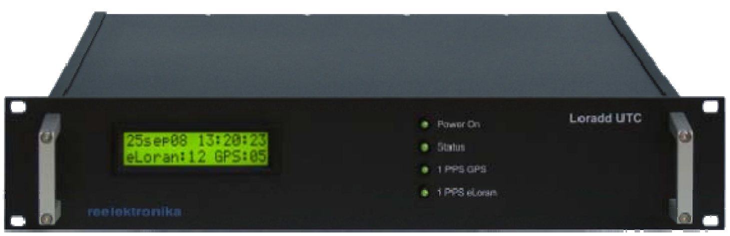
- The Presidental DHS budget (Feb 2009):
  - “supports the termination of outdated systems such as the terrestrial-based, long-range radionavigation (LORAN-C) operated by the U.S.Coast Guard resulting in an offset of $36 million in 2010 and $190 million over five years.”
  - No mention of eLoran is made (however eLoran needs Loran-C infrastructure)
- Federal Radionavigation Plan (Feb 2009) eLoran suggested as possible GPS back up
- Congressional stance TBD
  - Current language indicates support for keeping Loran ($37 M budgeted for operations & upgrade)

- **Bottomline: Loran future is uncertain**

eLoran Receiver Manufacturers

Timing Receivers

Symmetricom



reelektronika

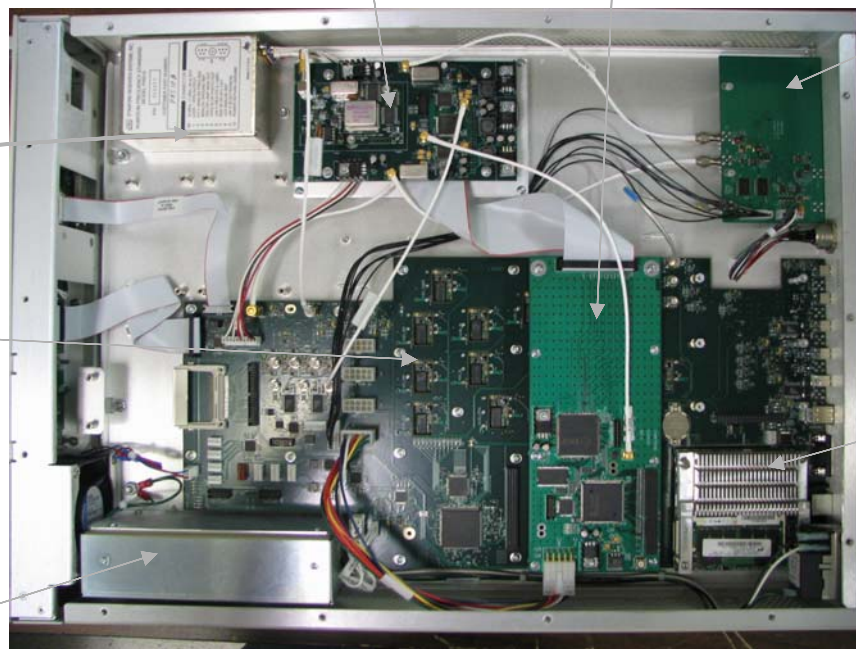
Navigation Receivers

CrossRate TECHNOLOGY

reelektronika

GPS/WAAS/eLoran Receivers for Maritime

Enhanced Loran Receiver



Front

Back

Courtesy: Kirk Montgomery, Symmetricom

Transmitter Manufacturers

- Megapulse
  - Built the current Loran solid state transmitters (SSX)
  - Based on tuned circuit - half cycle generators (HCG)
  - SSX use 16 to 32 HCG
- Nautel
  - Prototype efficient, low cost Loran transmitter in 2007-8
    - amplifier & combiner section
    - Efficient power recovery
  - Based on broadcast FM/AM, etc. amplifier technology

Loran Performance & Critical Infrastructure

Why have Loran and GNSS

- Relying more and more on GNSS for safety & economic infrastructure
  - Timing for cell tower, shipping, aviation, etc.
- Concerns about outage or unavailability of GNSS
  - reduce operational capability
- Loran has dissimilar characteristics
  - Signal power, frequency, characteristics
  - Failure modes independent from GNSS
- Loran has similar outputs
  - RNAV (lat,lon, time) - seamless to user
    - 2D vs 3D position for GPS
  - Could provide similar operational capabilities

Primary Areas of Interest

- Aviation
  - Enroute (RNP 1.0 type procedures)*
  - Terminal & Approach (NPA, LNAV, RNP 0.3)
  - Others? (Surveillance (ADS-B))
- Maritime
  - Ocean & Coastal Confluence Zone*
  - Harbor Entrance Approach (HEA)
- Timing & Frequency
  - < 50 ns timing accuracy (USNO)
  - Stratum 1 frequency source (10^{-11})*

* Available with Loran-C

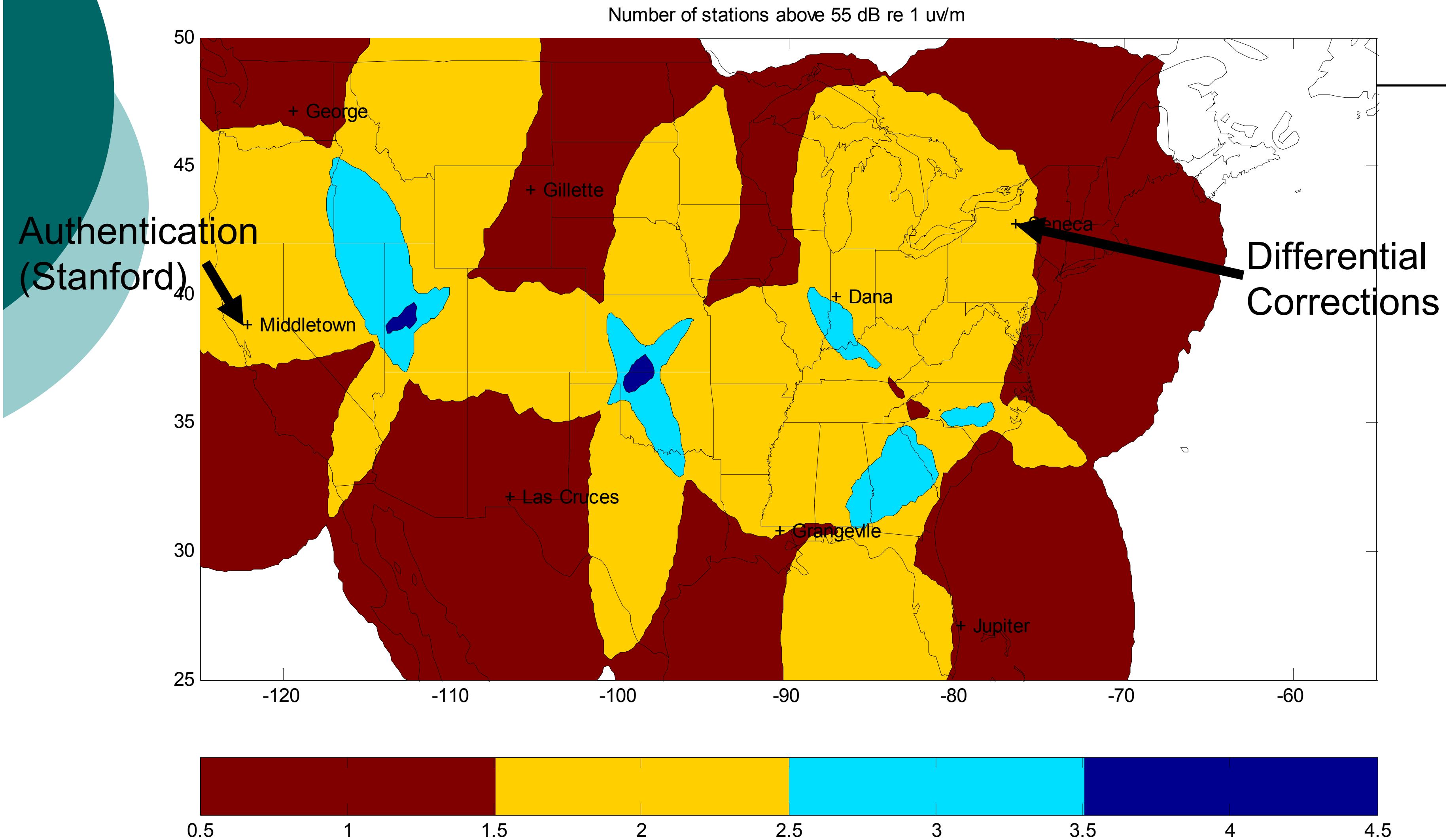
Loran vs. eLoran: Technical differences

- Data channel
- Differential corrections
  - Monitor sites & comms infrastructure
- Government provided propagation corrections
- Time of transmission control
  - All stations synchronized to UTC, hence easier ranging
  - Position domain errors generally lower
    - SAM control minimize error at 1 locale
- Transmitter clock
  - Improved clocks (already installed)
  - Improved algorithms/control loops
  - Tighter tolerances

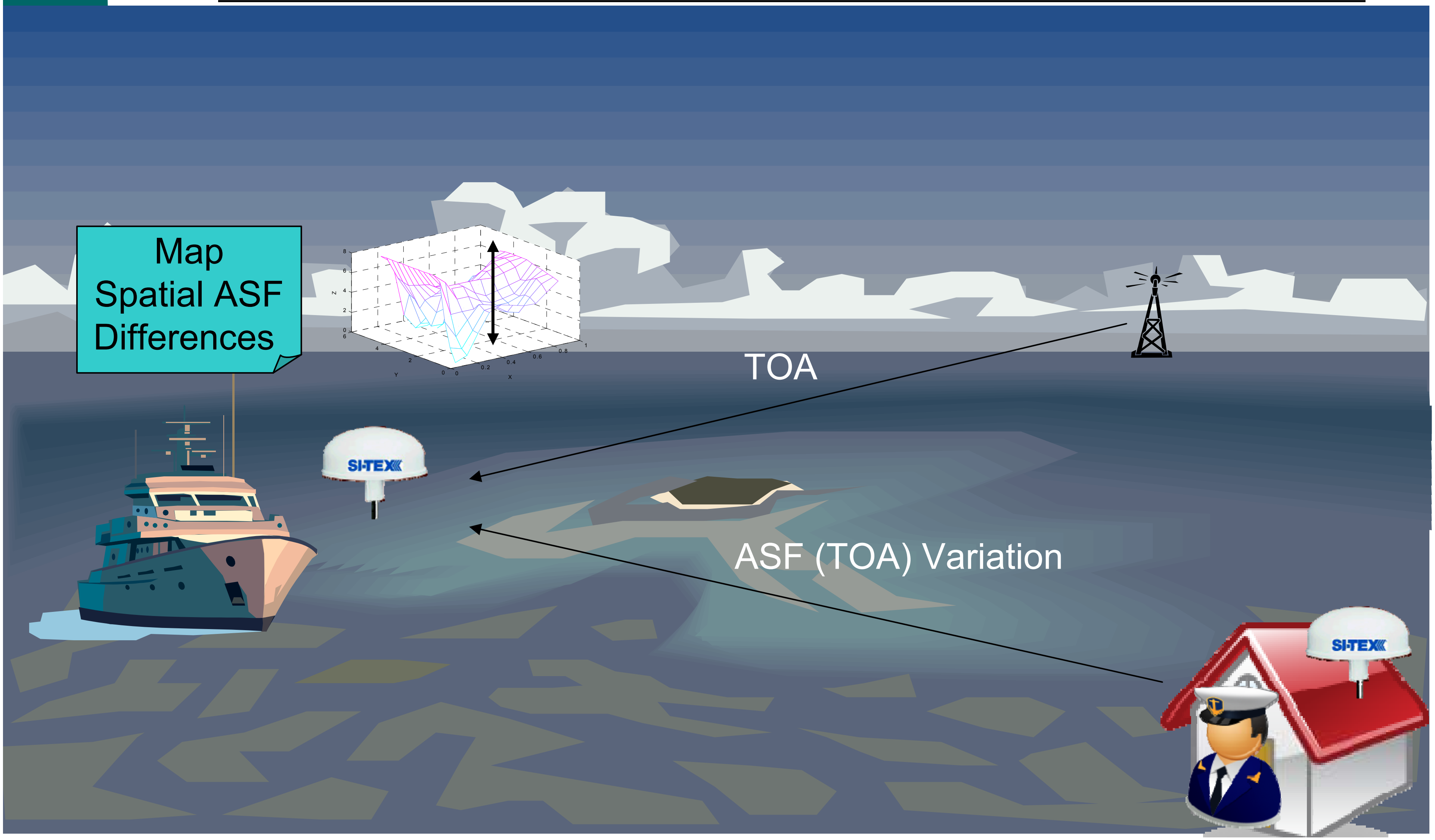
Enhanced Loran - Loran Data Channel

- Pulse position modulation on Loran signal
- 18.8 to 31.6 baud per channel, up to 4 channels on dual rated station
- Time of Day, Leap Seconds
- Differential Loran corrections for temporal variations in phase
  - Improves accuracy for harbor entrance to 10 m (95%)
    - Requires harbor survey for spatial variations
  - Comparable improvement in timing accuracy
- Stanford developing authentication methodology
  - Authentication messages transmitted from Middletown, CA

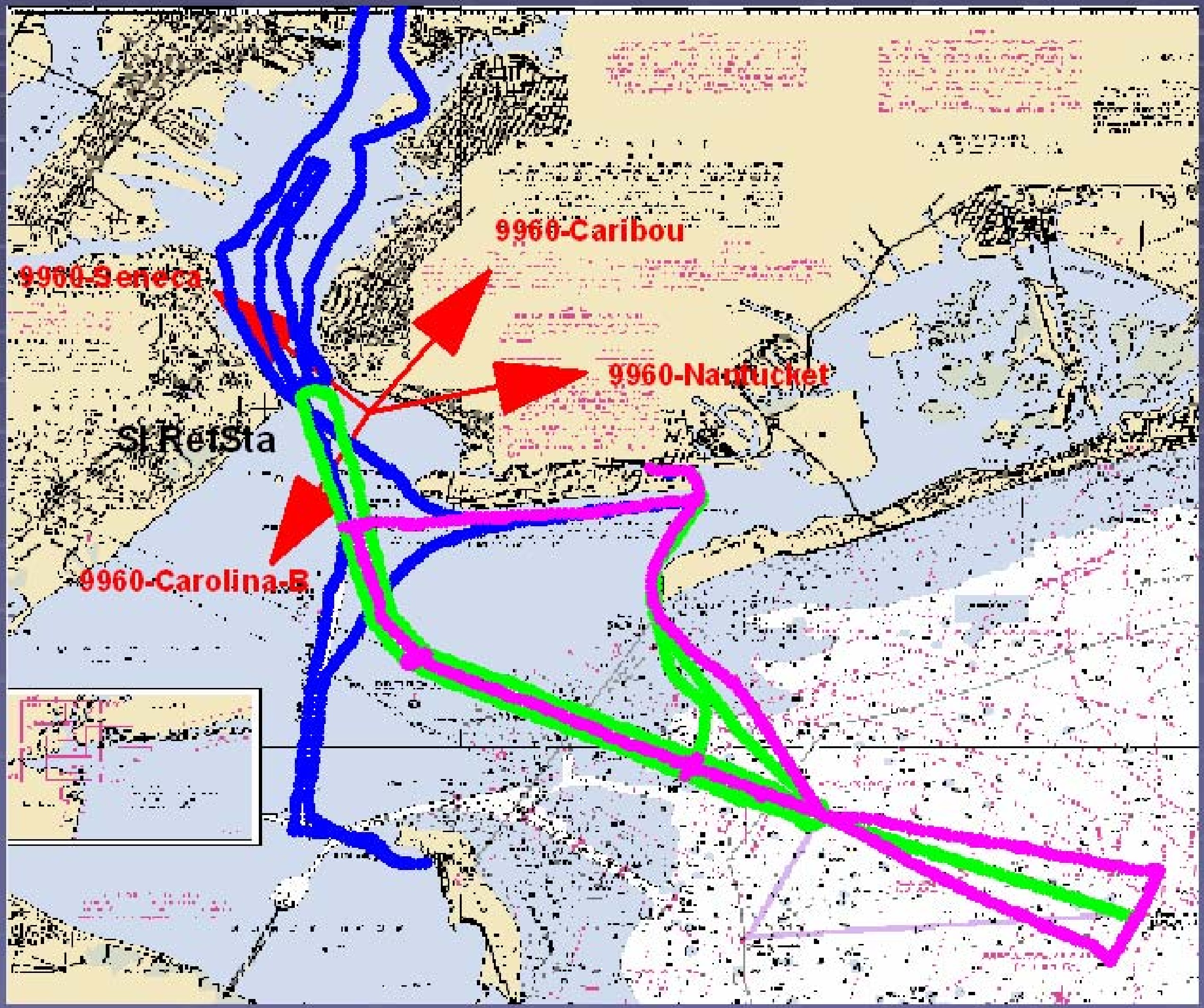
Current Loran Data Channel Coverage
(Time of Day only except Seneca & Middletown)



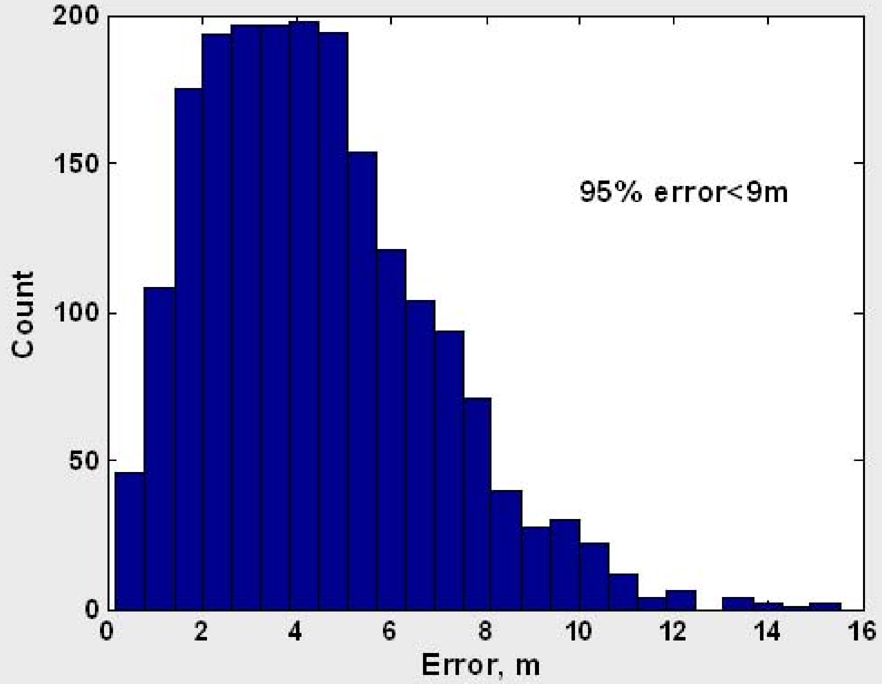
Differential Loran



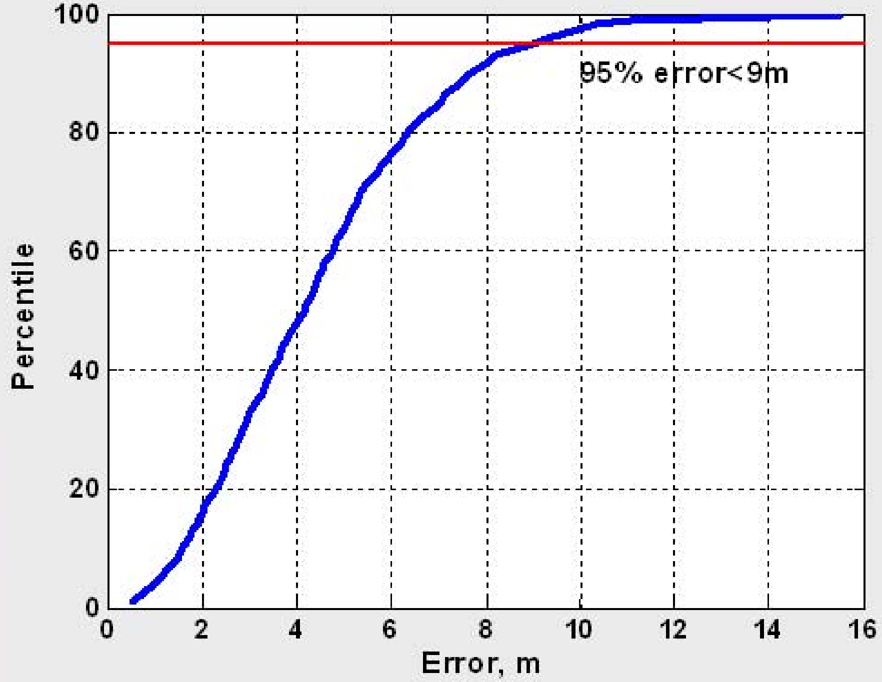
Phase 2 Tracks



Statistics



200
150
100
50
0
Count
95% error<9m
0
2
4
6
8
10
12
14
16
Error, m

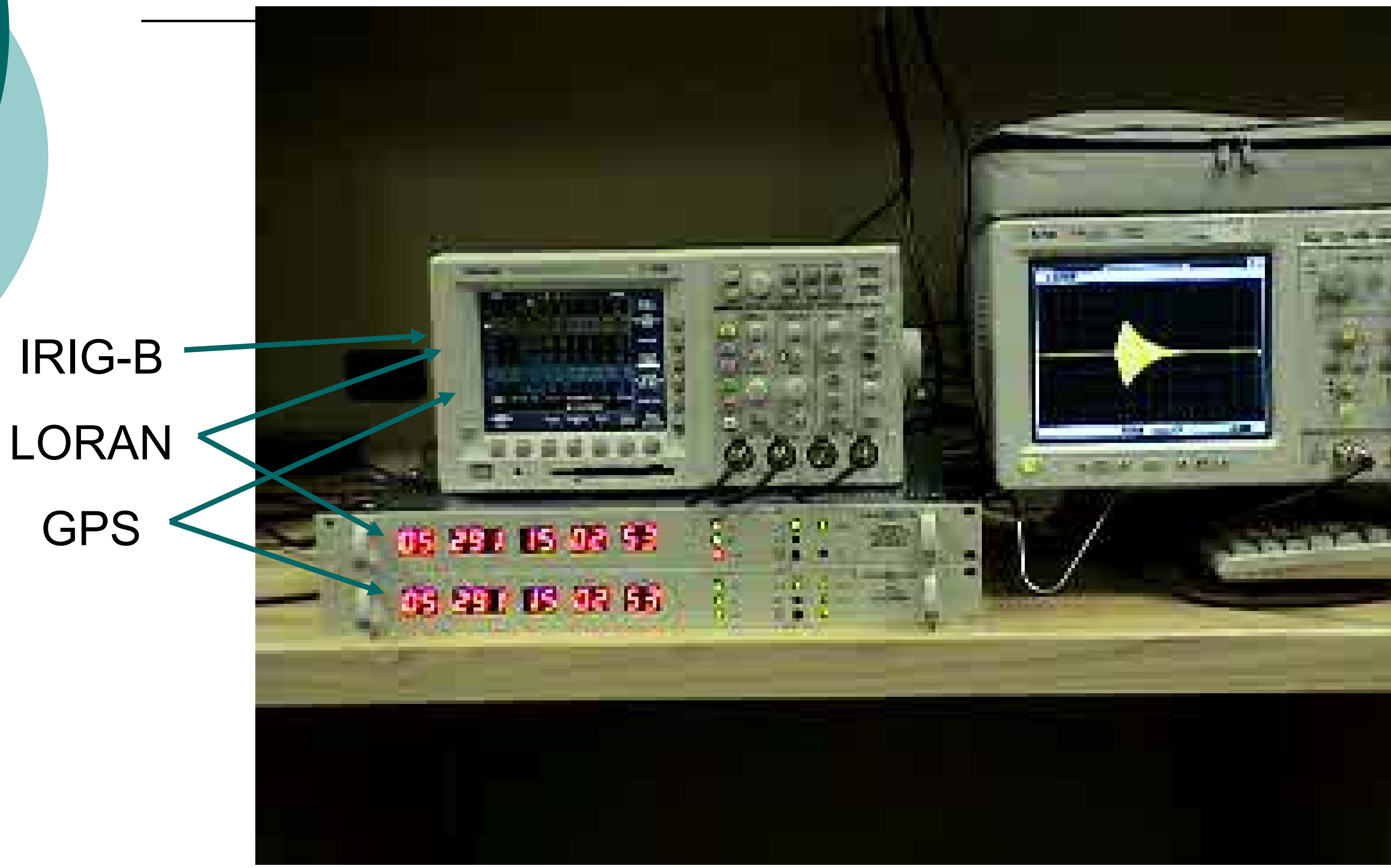


100
80
60
40
20
0
Percentile
95% error<9m
0
2
4
6
8
10
12
14
16
Error, m

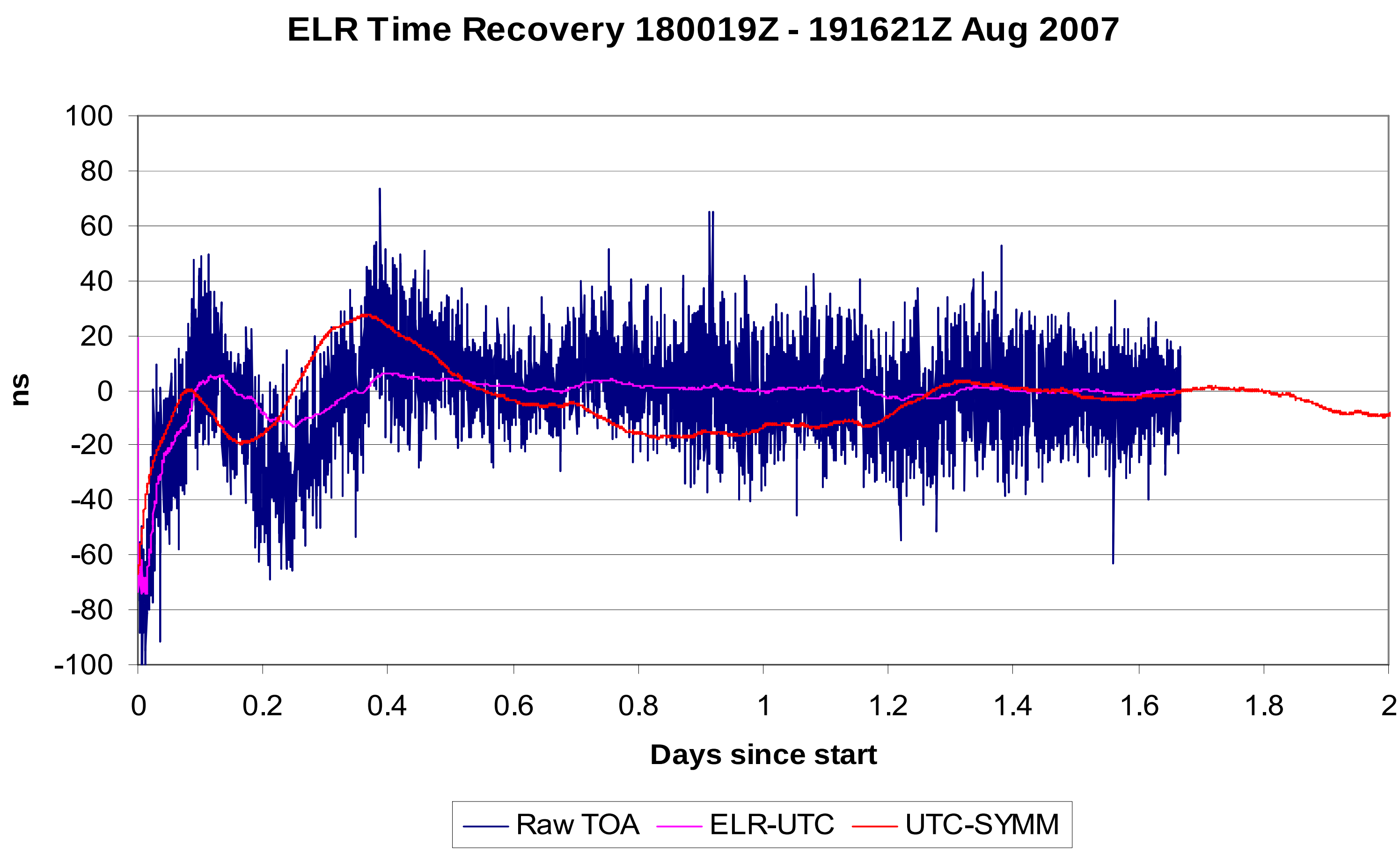
Enhanced Loran – GPS Independence

- Currently 5071 Cesiums steered using GPS
  - If GPS is lost, coasts for a few weeks on Cesiums, then UTC sync maintained using Loran signals (as is done in Europe & Russia)
- LSU investigating alternative to GPS for primary source of UTC
  - Including but not limited to TWSTT
  - Final solution is Kalman filter using TWSTT (or equivalent), GPS, & Loran
  - Sub-nanosecond level not needed for Loran but paper clock of 87 5071's; 3 each 29 remote sites compared at this level is national asset

Enhanced Loran Timing Receiver



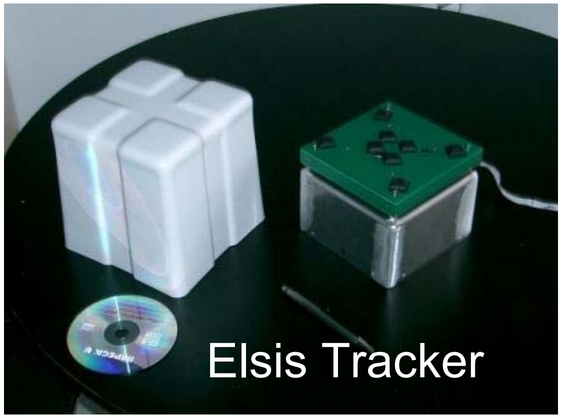
Time/Frequency Recovery



Courtesy: Kirk Montgomery, Symmetricom

Other Benefits

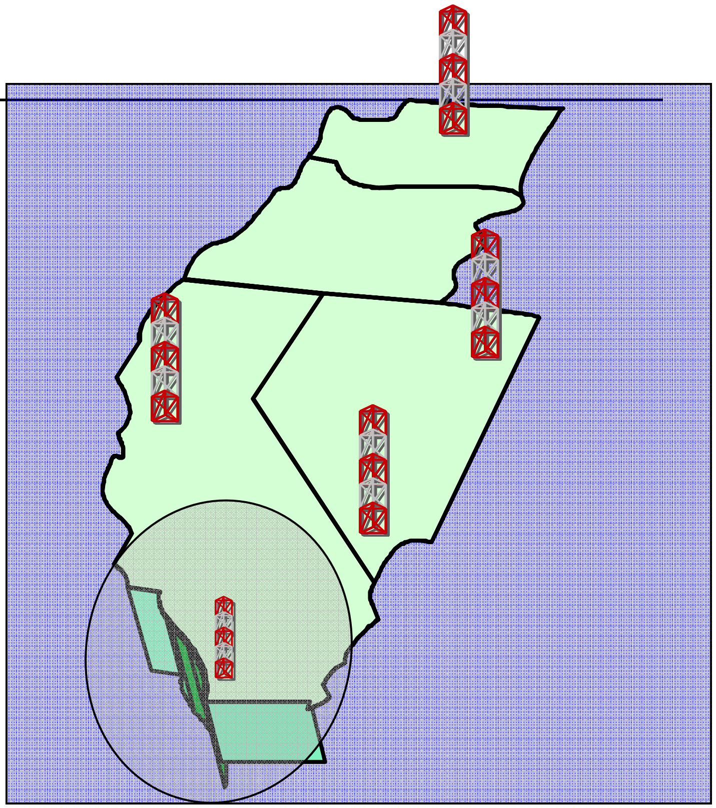
- Indoors & urban canyon
  - GNSS/Loran integration
  - Capability of reaching some places that are difficult for GNSS
- Static Heading
  - Can use dual loop antenna to get heading
- Authentication/Secure location
  - Authentication message tested
  - Many properties useful for location based security



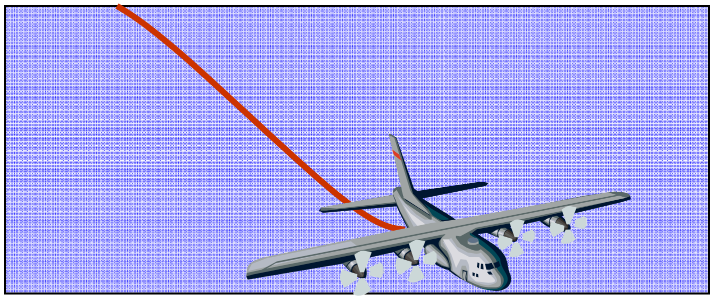
Tactical Loran

Efficient, Low Power Transmitters Enables Tactical Loran

- Fixed tactical Loran transmitters
  - Improve coverage for areas with Loran
    - Use existing assets w. shorter antennas
  - One Loran tx with other signals of opportunity
    - Loran provides diff. corrections for other signals
  - Loran mini chain for tactical purposes
    - Areas with no or inadequate Loran coverage



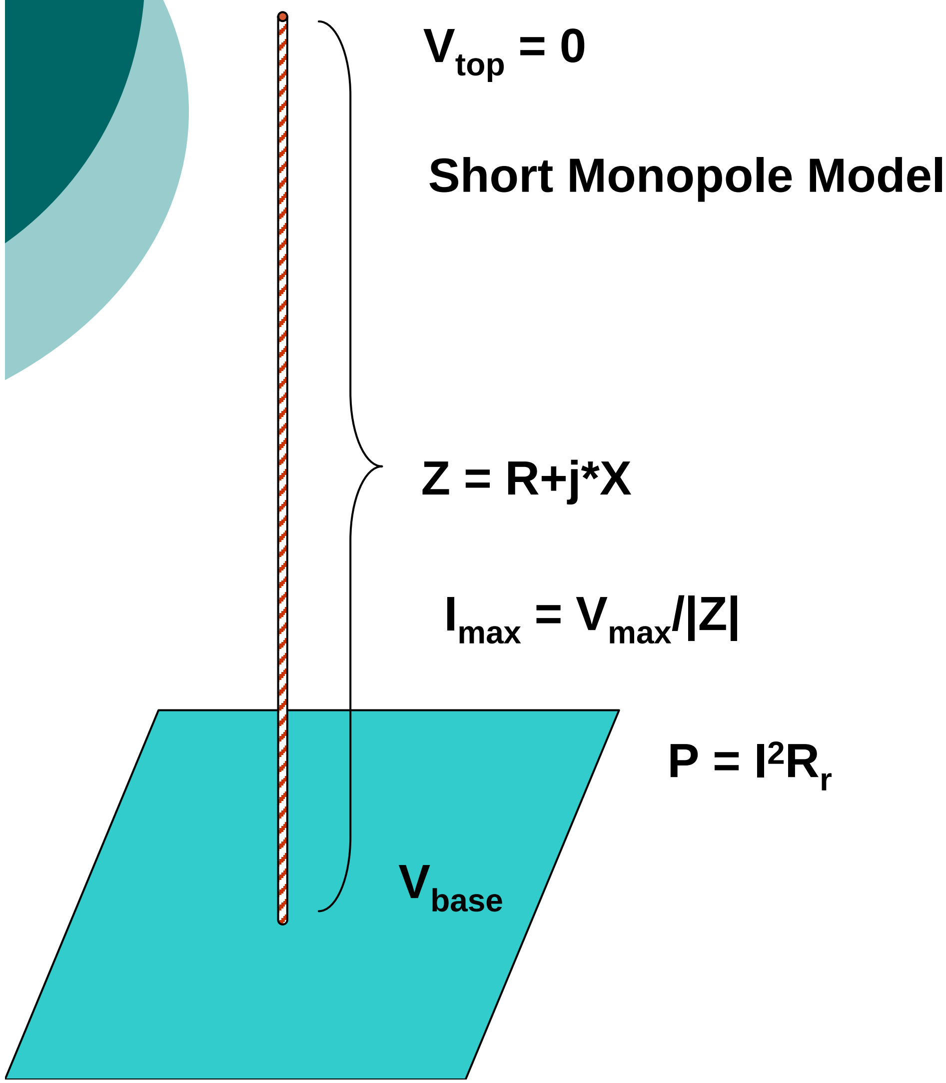
- Loran on Mobile Platform
  - Possibilities include: Aerostats, Airships, Fixed wing aircraft, Large navigational buoys, Offshore platforms



Basic Concept of Operations for DoD use of tactical Loran outside the US

- At least one Enhanced Loran transmitter
  - May be at fixed location or on moving platform
  - Loran Data Channel transmits
    - Location if moving
    - Differential corrections and integrity for Loran & other signals
- Base Station(s) measure(s) differential corrections and communicates to transmitter
  - Transmitter base station & can be co-located, but to get to sub 10 meter accuracy will require baselines of 10's of km & propagation surveys.
  - Base station need not have GPS availability

Radiation Power



- Short Monopole
  - Voltage zero at end and maximum at base
  - Limit is often this voltage differential (Max V)
  - Reactance mostly capacitative
- Resistance
  - Loss components (R_{loss})
  - Radiative component (R_r)
- Radiated Power
  - Current flow
  - Radiative Resistance (R_r)

Simple Model of Antenna Performance

- Radiation resistance for a short monopole & simple TLM over an ideal ground plane

$$R_r = 40\pi^2 \left(\frac{h}{\lambda}\right)^2 \Omega \qquad R_{r,TLM} = 80\pi^2 \left(\frac{h}{\lambda}\right)^2 \Omega$$

- Short antenna – reactance is essentially capacitative

$$X_A = \frac{-30\lambda}{\pi h}\left[\ln\left(\frac{h}{a}\right) - 1\right]\Omega$$

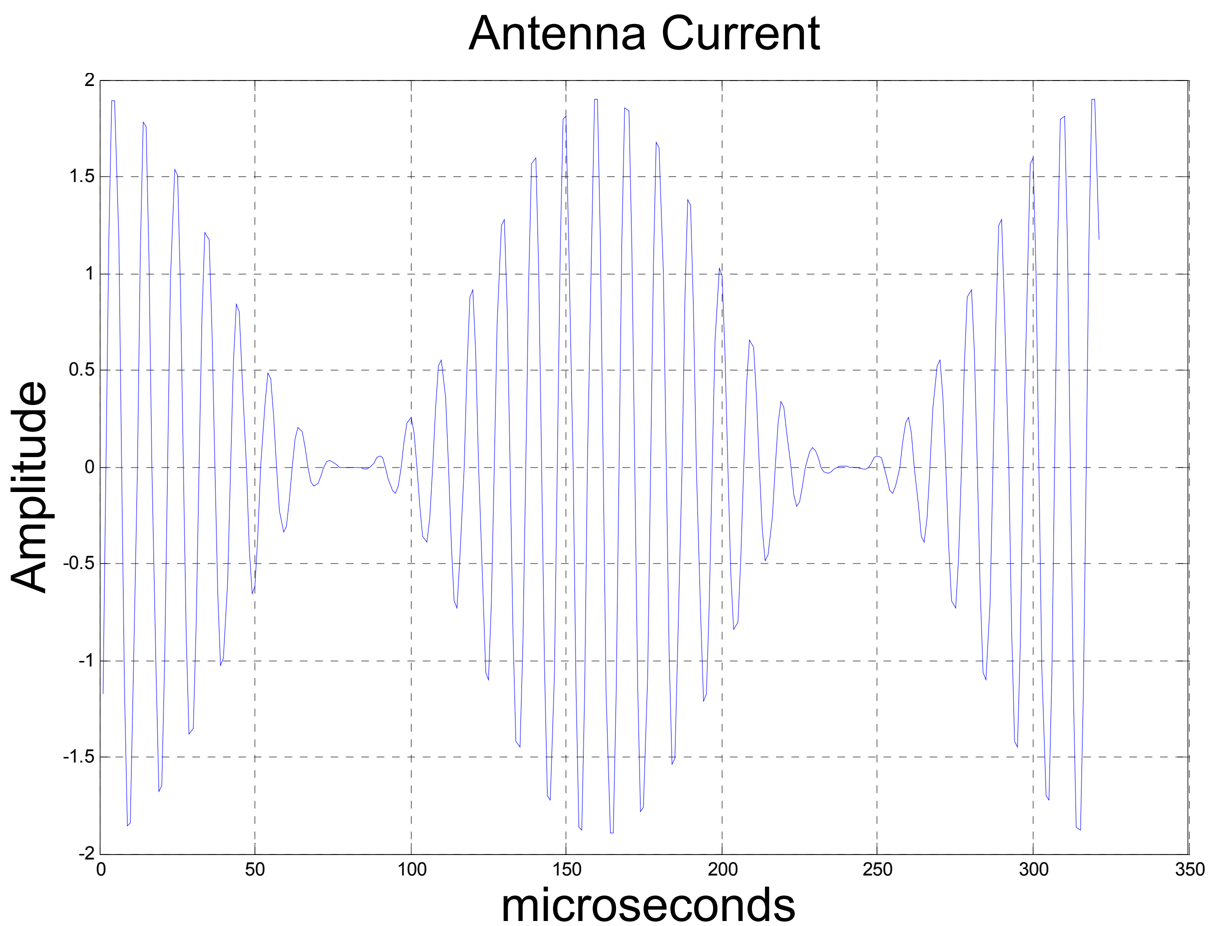
- Typical US Loran transmitter has 190 m TLM, slightly over 2 ohms, 700 amps peak current for 400 kW peak power
- Short antenna are high Q
  - Tune to 100 kHz requires adding inductive elements
  - Narrow band, significant energy is stored

Compatible Loran Signal

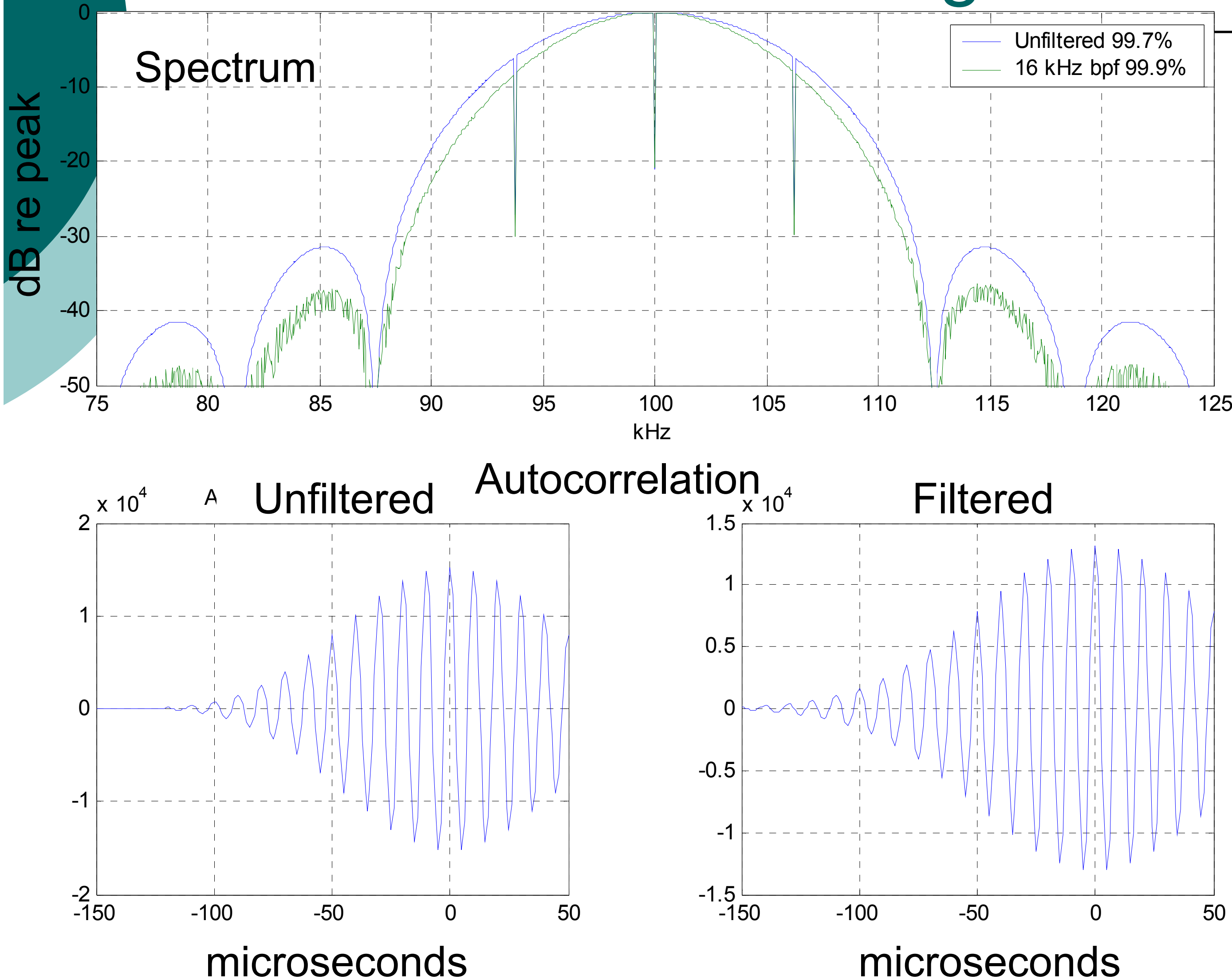
- Standard Loran signal may not be best
- Shorter range = less skywave
  - Skywave a prime driver of Loran signal design
  - Design signal with longer rise time and more dwell time at peak amplitude (narrower BW, more efficient)
  - Higher duty cycle also possible
    - More pulses for given time window
- Increased number of pulses per GRI (if it can be accommodated)
    - Longer time window
- Constraints
  - Spectrum
  - Transmitter limits on signal output, pulse/sec
  - Skywave

BPSK-Raised Cosine Signal

- Example: 6.25 kHz BPSK x Raised Cosine
- Phase shift in nulls
  - Easier for tx
- 20.48 ms in length
  - 128 pulses
  - Vs. 8-10 ms (1 pulse/ms) Loran



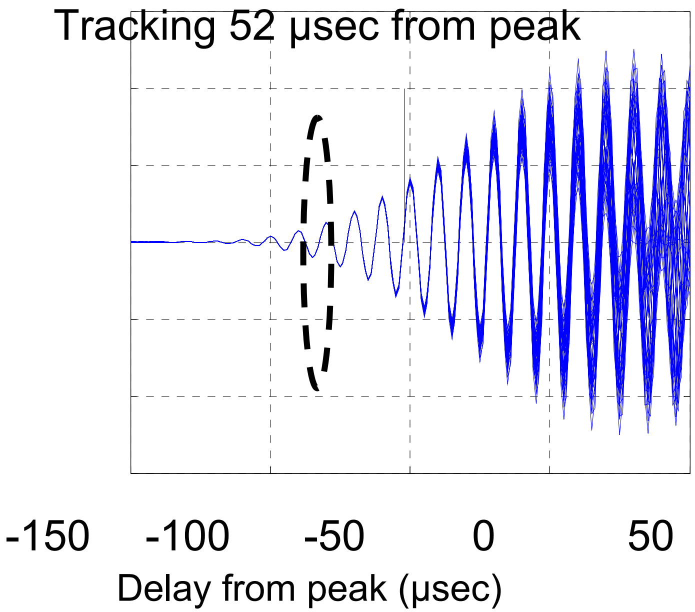
Spectrum & Autocorrelation of BPSK Raised Cosine Design



- Unfiltered & 16 kHz filtered BPSK designs
- Both designs within spectrum
  - 99.7%, 99.9%
- Reasonable autocorrelation for navigation
  - similar to Loran
  - Reasonable for transmission equip to output

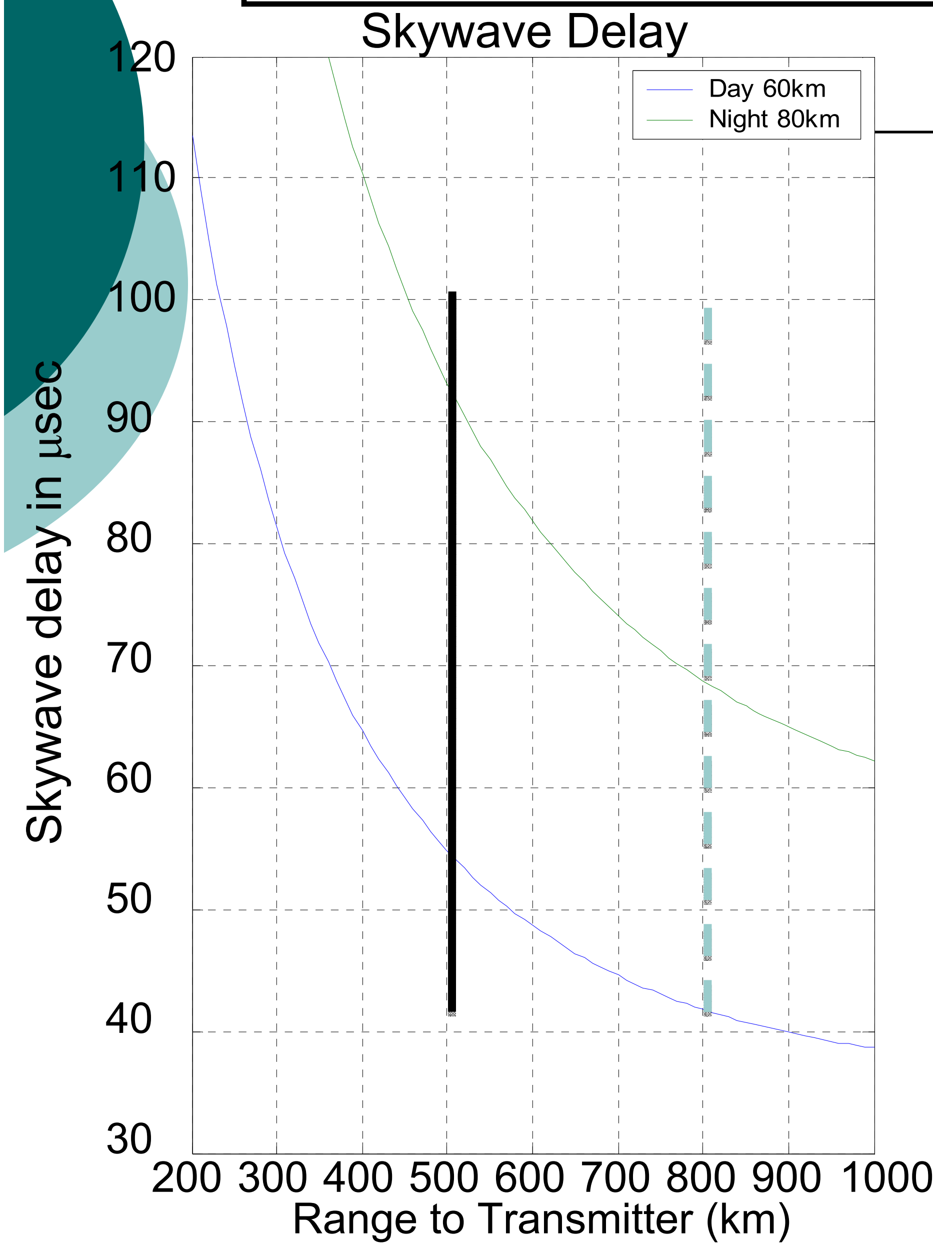
Nominal Performance of BPSK-RC vs. Loran

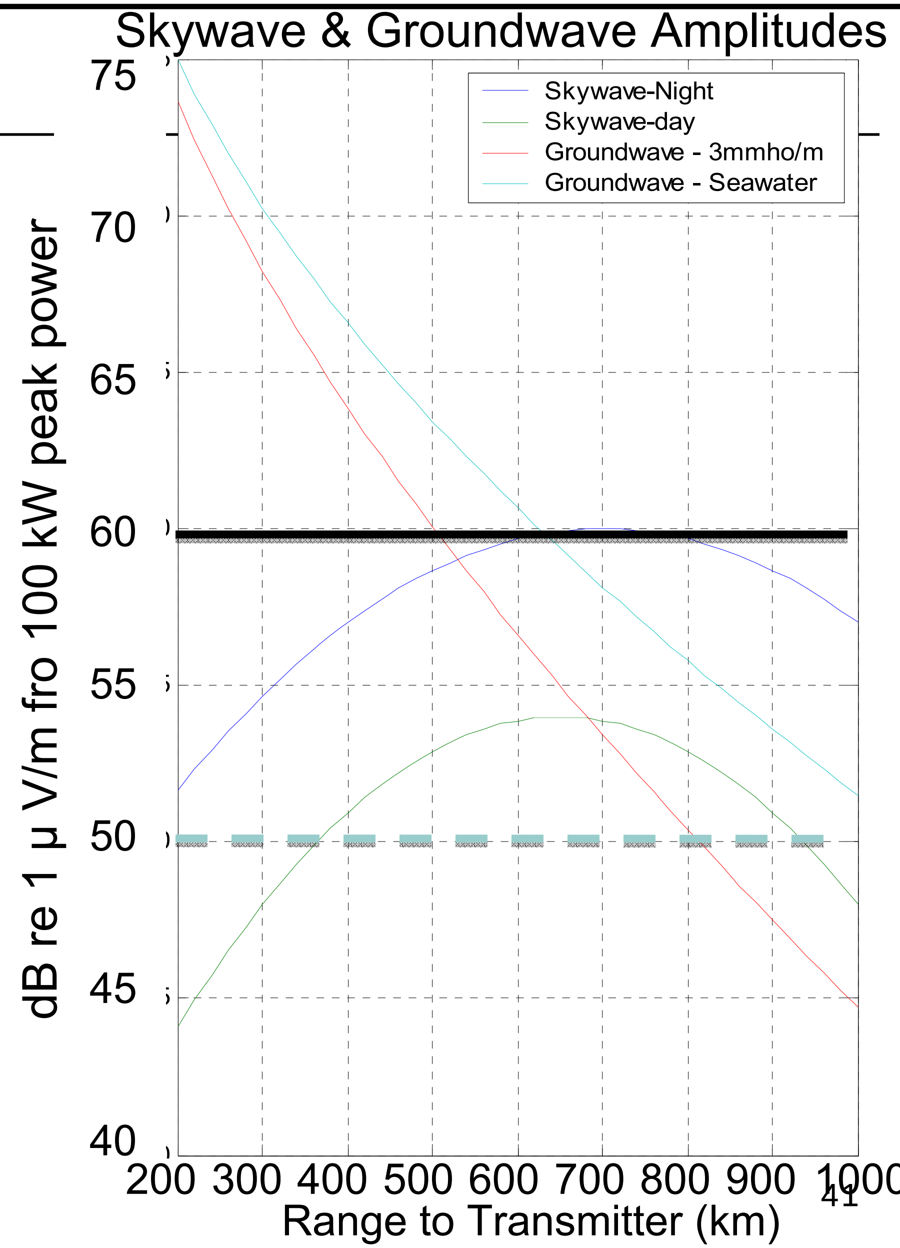
Tracking Pt. Re Peak	sigma TOA re Loran	sigma ECD re Loran	Equivalent Power Ratio	Normalized Power Ratio
-42 μs	0.166	0.329	36.4	14.2
-52 μs	0.213	0.423	22.0	8.6



Accounts for transmission length difference 20.48 ms (BPSK) vs 8 ms (Loran)

12.5 kW peak – 100 kW Equivalent Loran   1.25 kW peak – 10 kW Equivalent Loran





Skywave Assessment

	12.5 kW peak – 100 kW Equivalent Loran	1.25 kW peak – 10 kW Equivalent Loran
Range	800 km	500 km
Daytime		
Skywave delay	42 us	55 us
Skywave/Groundwave (SGR)	+3 dB	-10 dB
Nighttime		
Skywave delay	68 us	92 us
Skywave/Groundwave	+10 dB	-1 dB

(Assuming 3mmhos/m & sig strength of 50 dB re 1 uv/m)

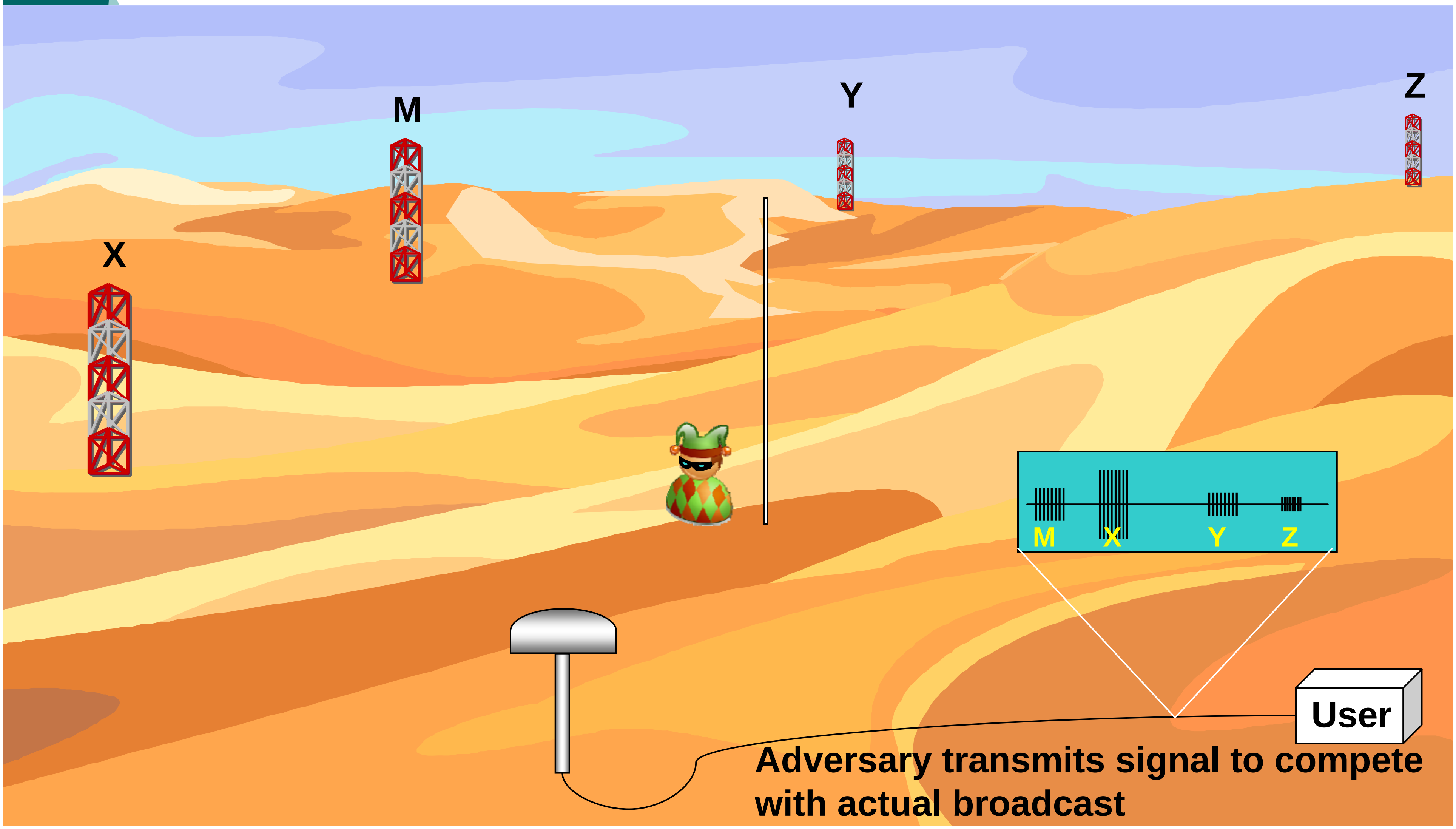
- For SGR < ~5 dB, 650 km

Loran & Navigation Security

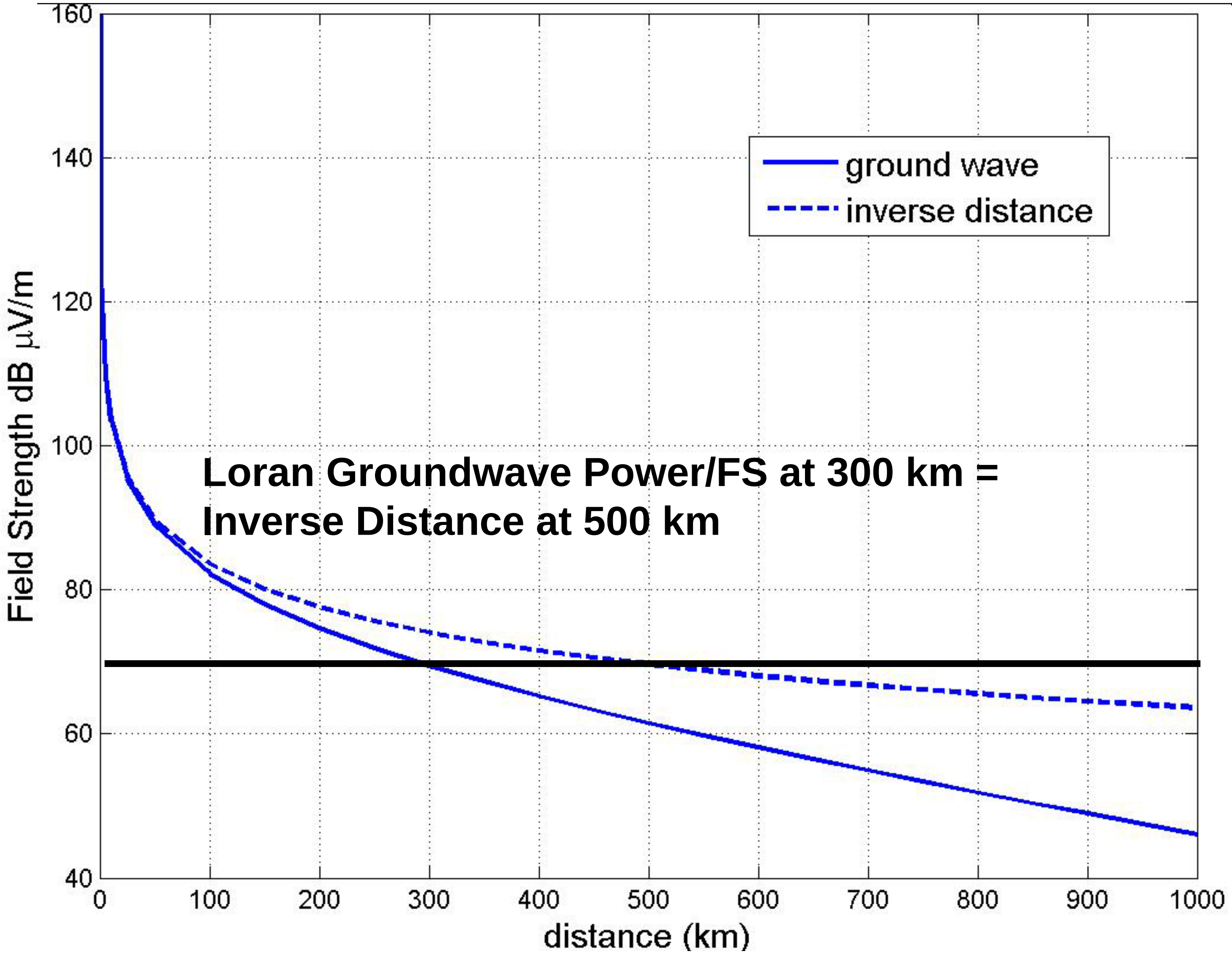
Loran and Secure Navigation

- Claim: Loran has properties that can be used navigation robustness against spoofing and jamming
- Obvious benefits in GNSS jamming
- Examine claim of robustness for various attacks
  - On air (Physical defense, Signal checks)
  - Off air
    - Direct injection (Authentication)
    - Rebroadcast injection (Cross check, Hidden information)

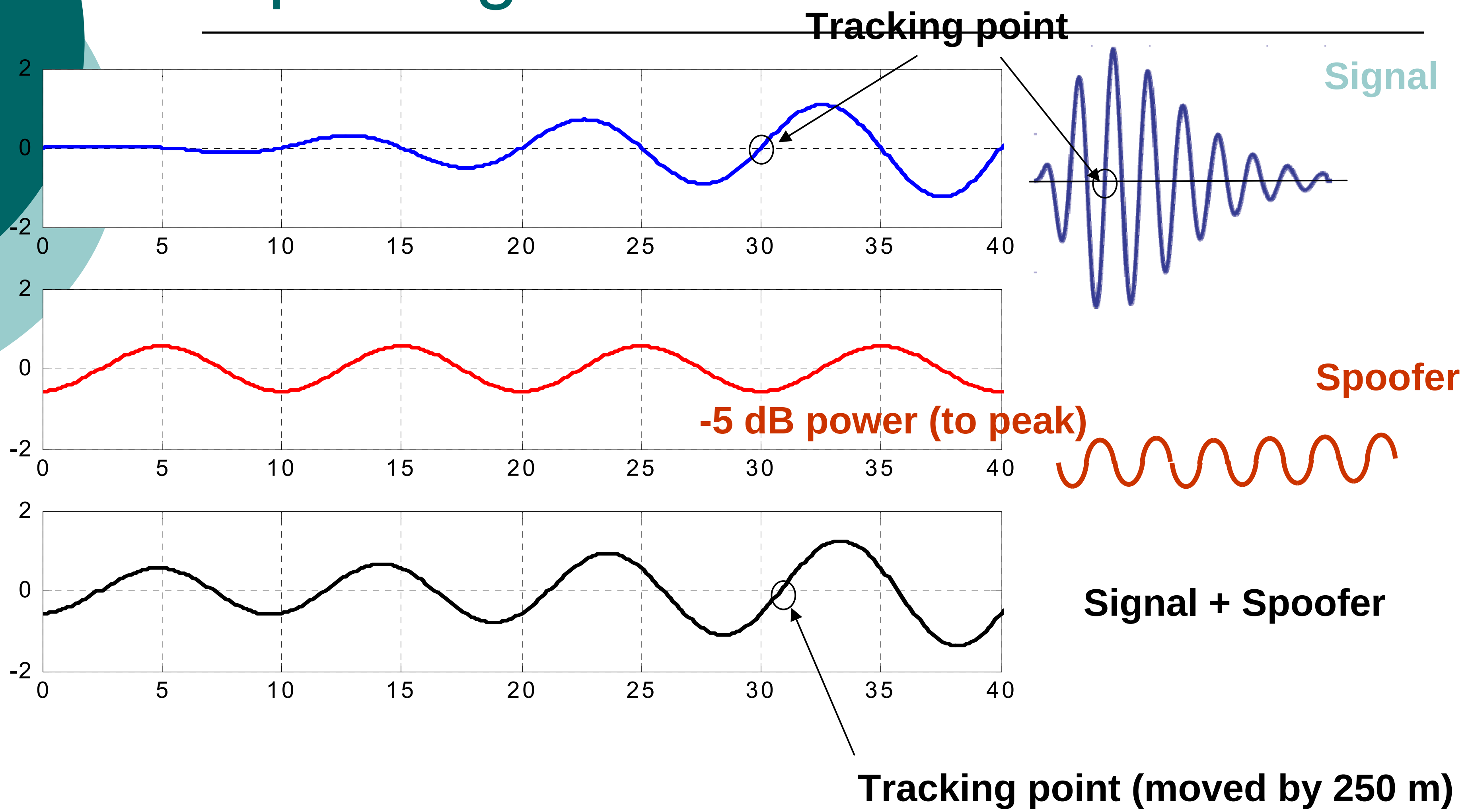
On Air Attack: Jamming & Spoofing



Typical Loran Field Strength (100 kW transmission)



Spoofing Loran with CW tone

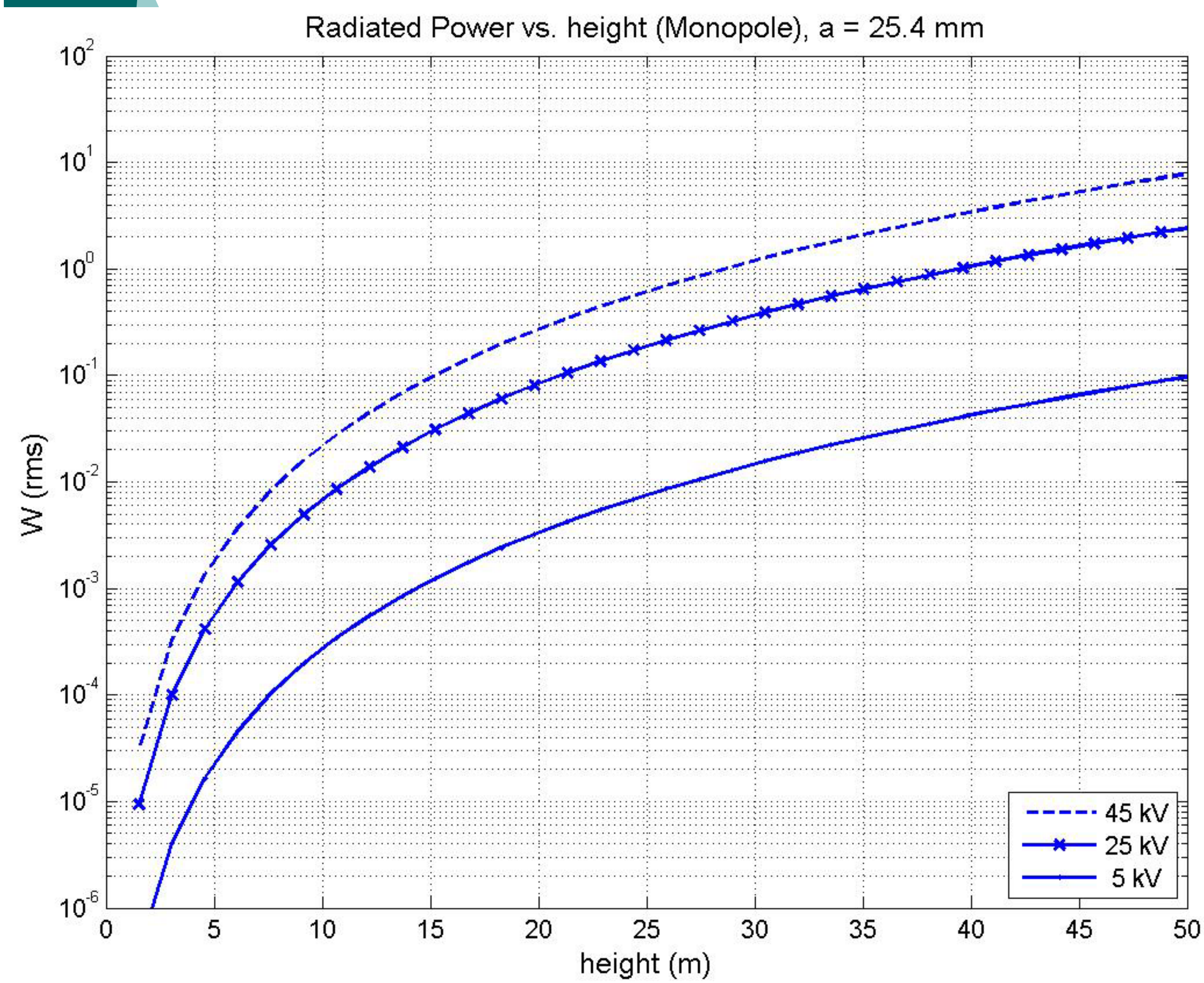


On Air Attacks: Competing with the Loran signal

- Scenario 1: Jamming equaling power of broadcast
  - 400 kW Loran tower at 300 km (~500 km if assume inverse distance^2)
    - you need ~40 W at 5 km or ~.4 W at .5 km
- Scenario 2: Spoofing by altering nominal signal
  - 30 m error at 5 (.5) km requires ~160 (1.6) mW (peak)
  - 150 m error at 5 (.5) km requires ~4 (.04) W (peak)

- Not a lot of power is required <u>but</u> it has to be radiated power
- Loran signal wavelengths makes efficient transmission difficult
  - Especially with short antenna
  - Limiting factor is voltage differential

Radiated Power vs. Minimum Antenna Height



- 45 kV max voltage diff.
- As h decreases
  - R_r decreases
  - X increases
  - I, give V_{max}, decreases
  - $P_r \sim 1/h^4$
- Very High Q
- Stored energy >> radiated energy
- Model less appropriate for larger antenna

Jamming/Spoofing Results

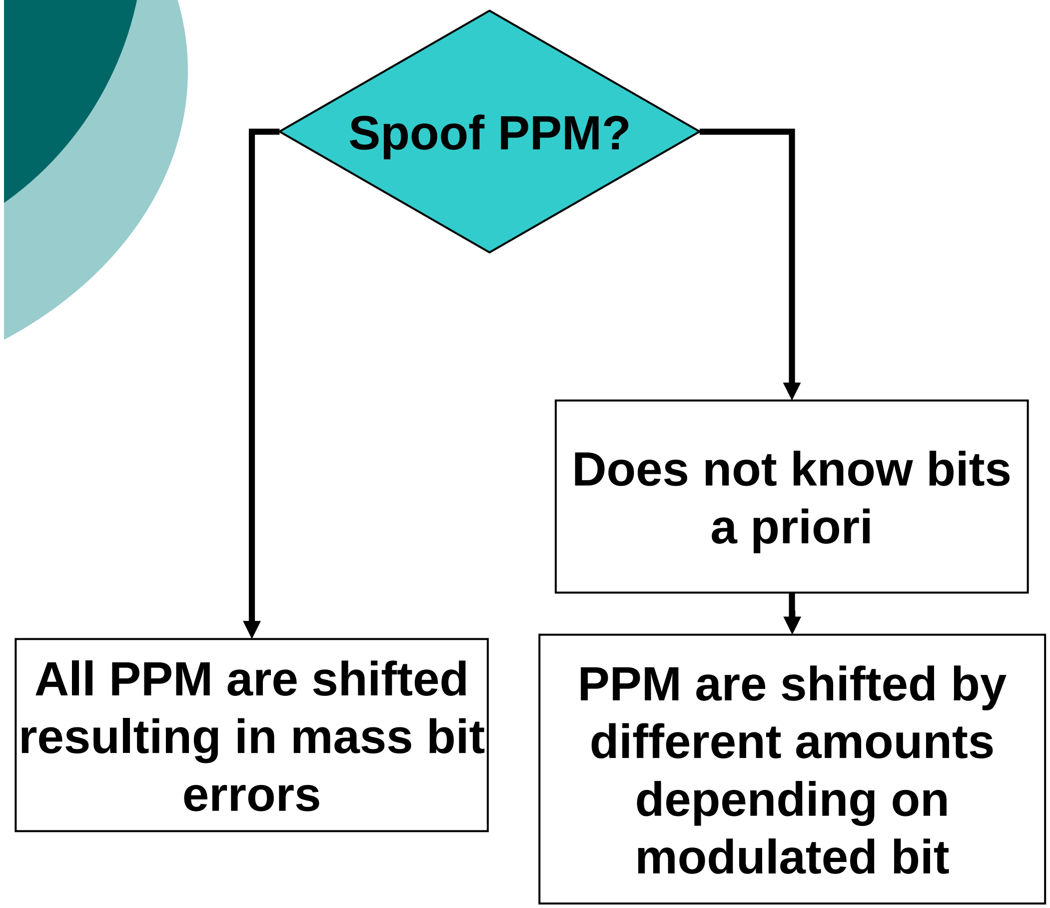
Scenarios (5 & 0.5 km)	**a = 2.3 mm**	**a = 25.4 mm**	**a = 50 mm**
Jamming (40 W, 0.4 W)	90 m, 27 m	78 m, 22 m	73 m, 21 m
Spoof 30 m error (160 mW, 1.6 mW)	21 m, 6 m	17 m, 5 m	16 m, 4 m
Spoof 150 m error (4 W, 40 mW)	49 m, 14 m	42 m, 12 m	39 m, 11 m

- Required monopole antenna for jamming are very large and likely difficult to set up
- Antennas for spoofing are smaller but still pose a set up problem

Detecting On-air Spoofing

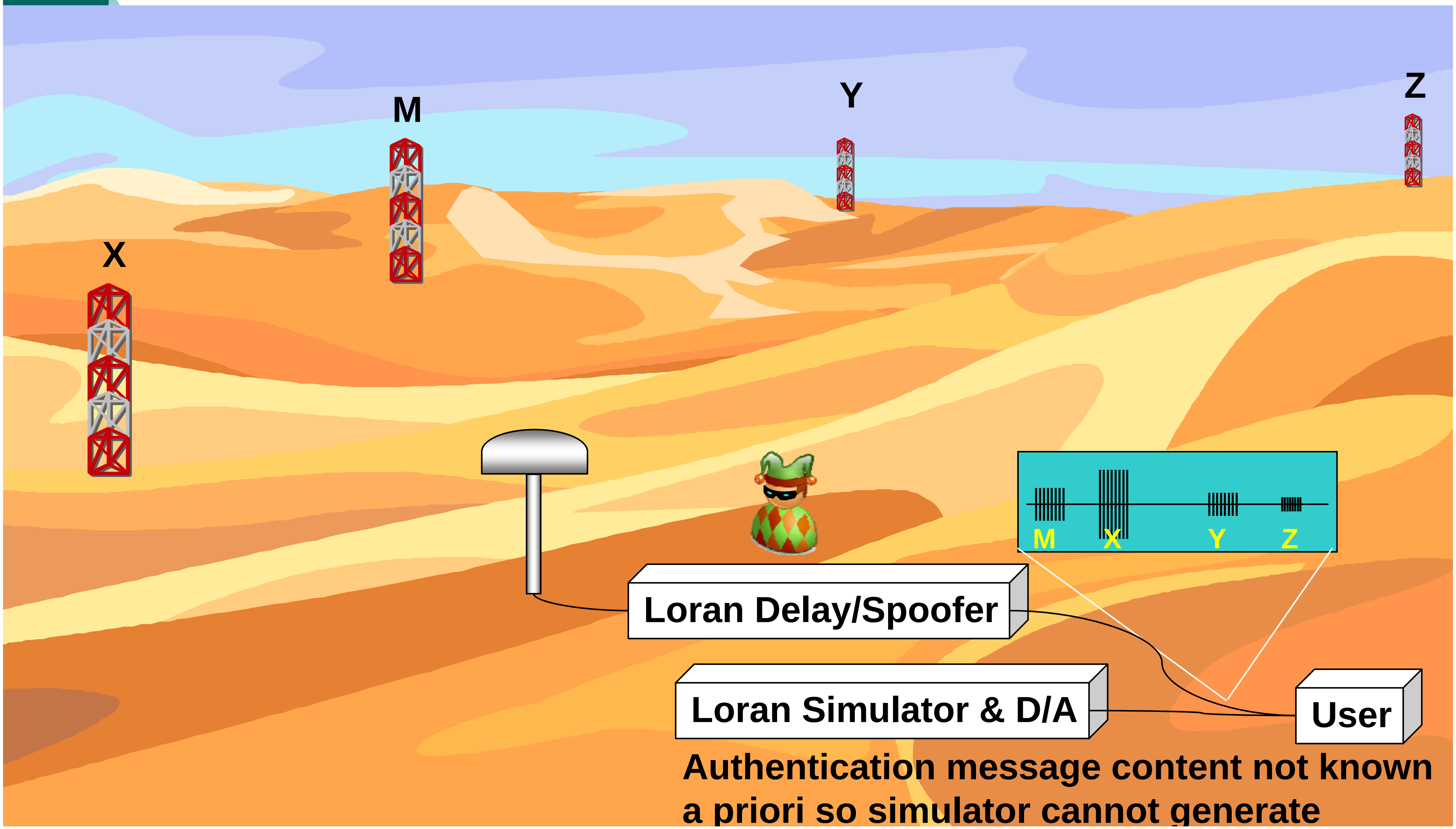
- Directional Antennas
  - H field antenna can determine signal direction
  - With one antenna, can spoof at most one signal without detection
- Affect on data modulation (PPM)
  - Randomness of data limits spoofed error
  - Some bits are affected more than others by described spoofing attacks
- Affect on different tracking points

Other Means of Detecting Spoofing



- Multiple tracking points
  - Loran shaped pulse
  - Different track point will have different errors
- Data Modulation
  - PPM pulse (9^{th} pulse) must be spoofed or it will be detected
  - Effect of data depends on bit modulated
  - Data bits not known a priori so effects will vary

Simulator/Direct Injection attack



Defending against Direct Injection Attack

- Authentication
  - Verifies data/source but not precise timing
    - Susceptible to repeat back spoofing (time window)
  - Not enough to ensure nav authentication
- Hidden Information/Information cross checking
  - Requires some receiver knowledge
  - Time check (auth. time msg compare w. rx clock)
  - Location dependent information (confirm calculated position with known location properties)
  - Authenticated data may be needed
- Hidden code
  - GPS P(Y), Galileo PRS

Thoughts

- On Air Jamming is very difficult
  - Requires “large” antenna set up & voltage differences
  - Detectable due to size & time to set up
- On Air Spoofing is difficult
  - May use less power than jamming -> smaller but still significant antenna
  - Even if it can be broadcast, several factors can be used to detect & limit position error from spoofing
- Caveat: On air results apply to far field only
  - Not near-far field

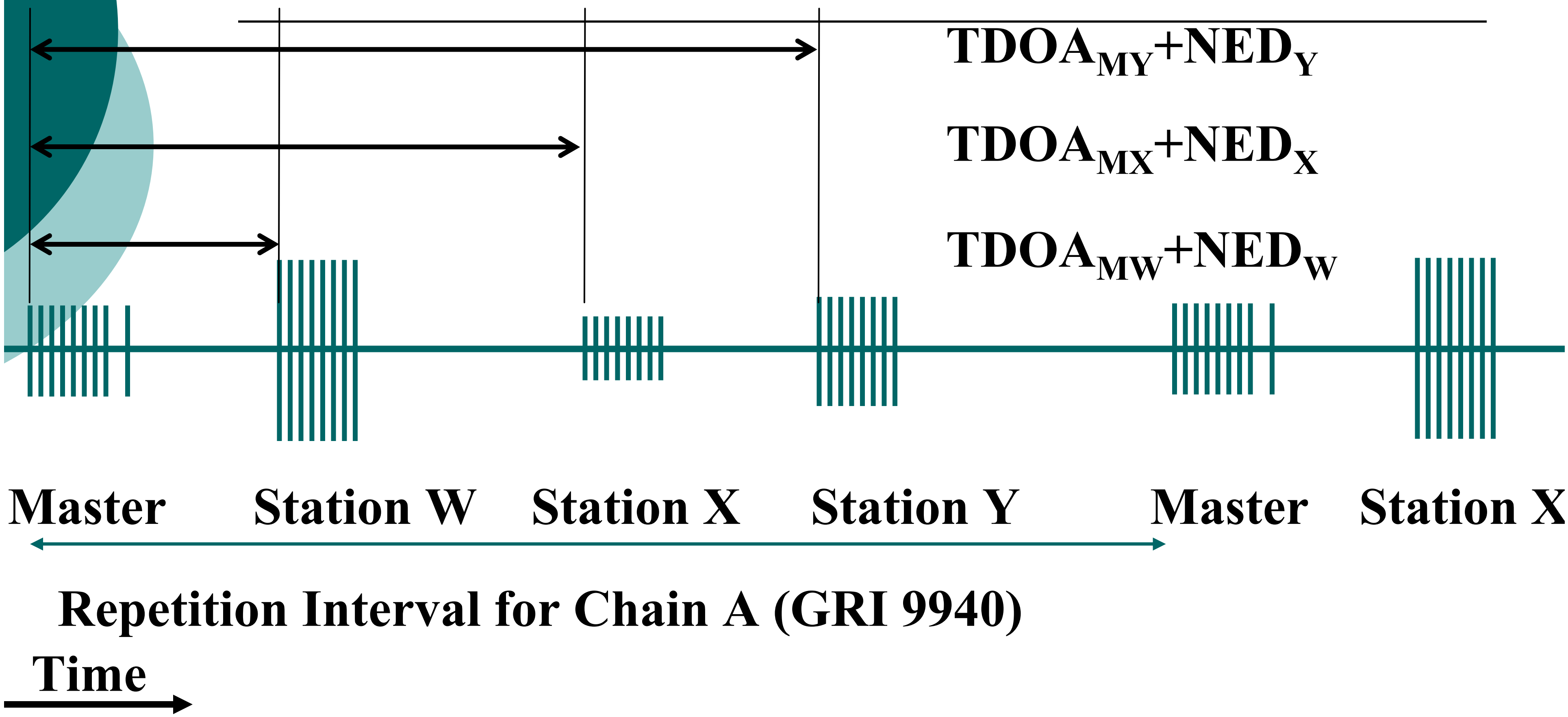
- Injection (Off Air) Attacks
  - eLoran has some potential defenses such as data authentication & location dependent makers
  - Attacks are difficult but not impossible
  - Researching ways of improving these defenses

Conclusions

- Loran is a good back up for GNSS
  - Capability, independence, interoperability, different mode of operations
  - Robustness to jamming/spoofing
  - Can serve multiple modes including timing
  - Other back ups exist
- Loran can serve tactical purposes
- Future of eLoran is uncertain

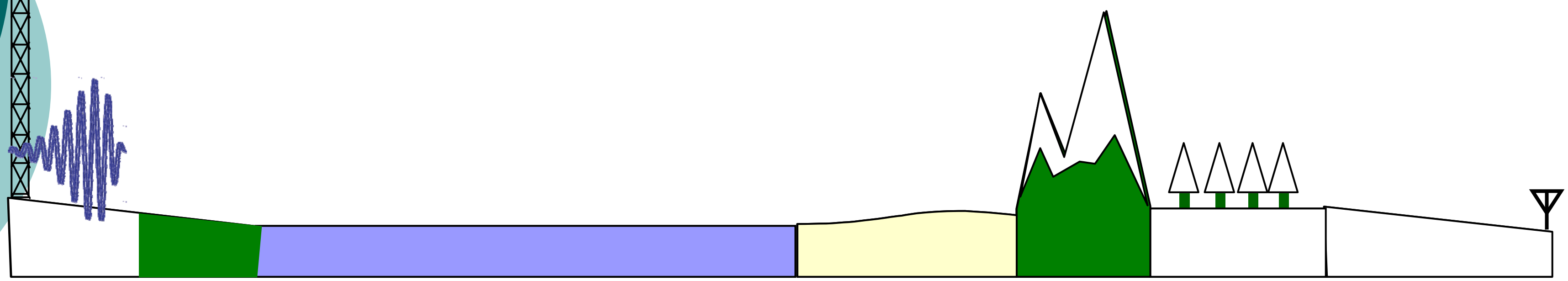
Backup

Getting Time Differences from Loran



- NED is the transmission delay from the master
- Absolute time, TOT control, allows for true pseudoranges

Temporal ASF Variations

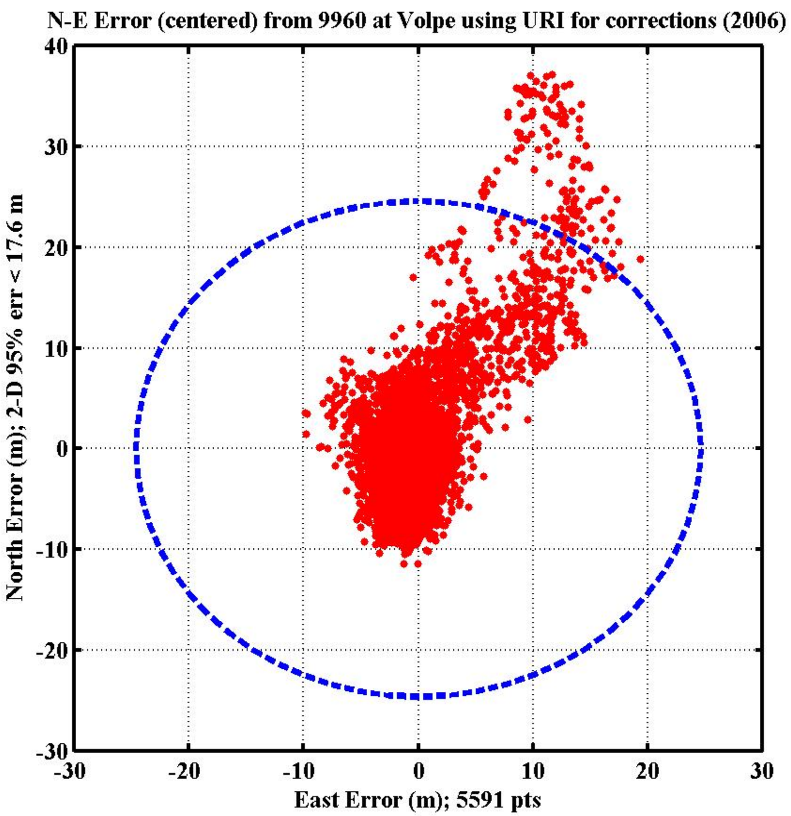


- As weather changes, properties such as terrain conductivity, permittivity, moisture level changes
- Results in different propagation speeds and variations in the delay on the pulse
- Phase delay (ASF) and ECD varies in time

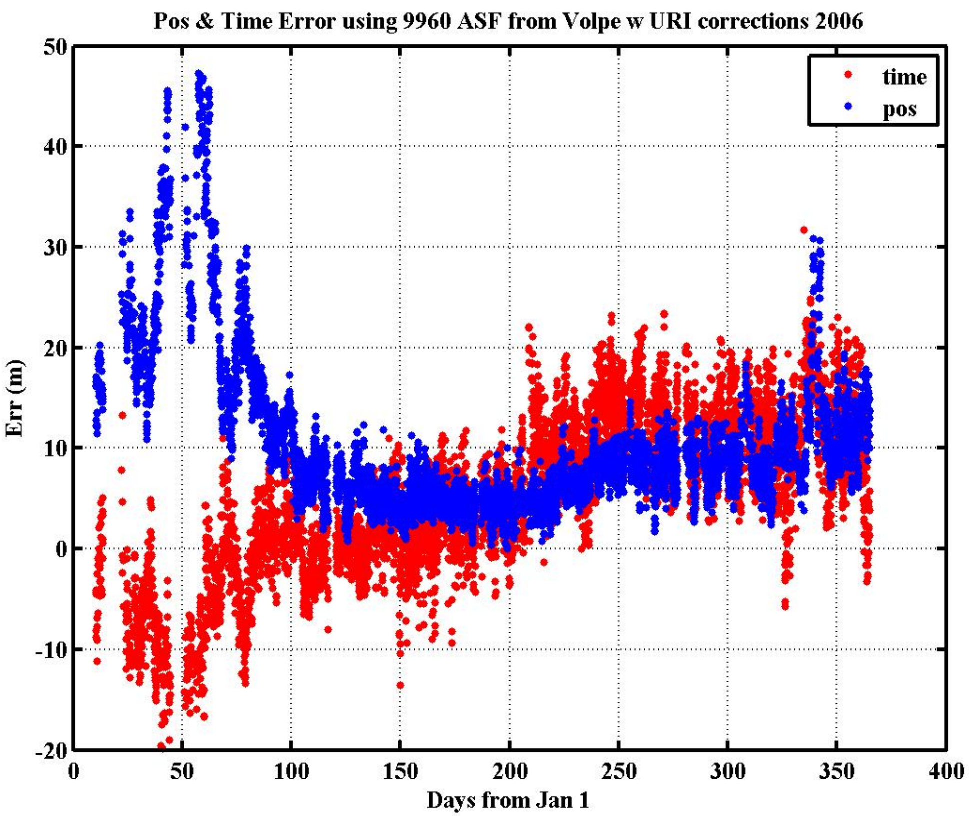
Major sources of uncertainty

- Noise
  - Thermal & atmospheric noise
  - Precipitation static
- Transmitter jitter (100-500 ns limit)
- Variation of propagation delay
  - Distance dependent (severe case: 500 m peak to peak)
  - Generally slowly varying in time
- Interference (often mitigated by processing)
  - Skywave
  - Crossrate
  - CW & RFI
- Reradiation
  - Large metallic elements (i.e. bridges)
  - Distortion about buildings

Differential Accuracy of Volpe Using URI



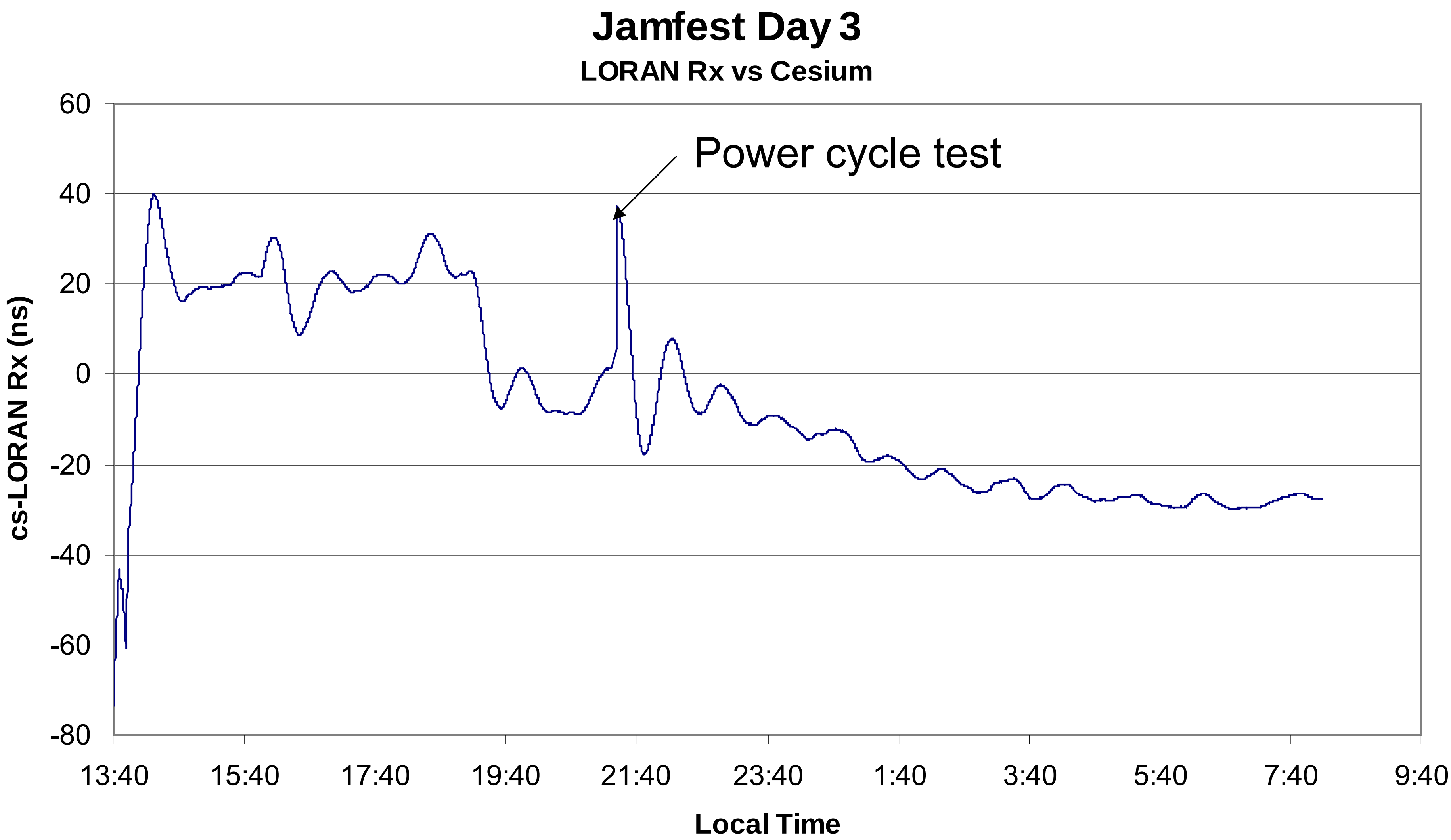
Differential Accuracy of Volpe Using URI



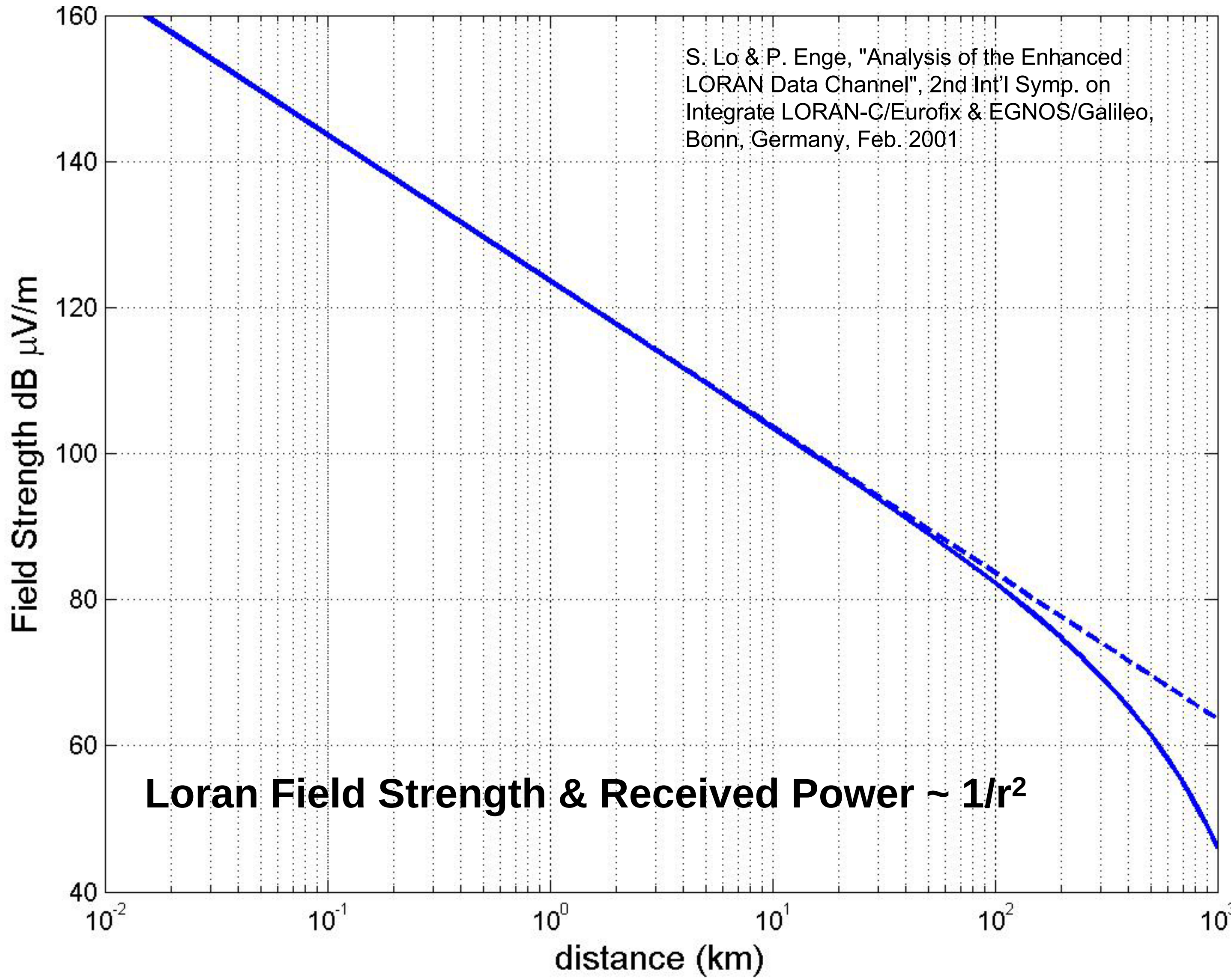
Time is the “common mode” error between all stations

Mobile Loran

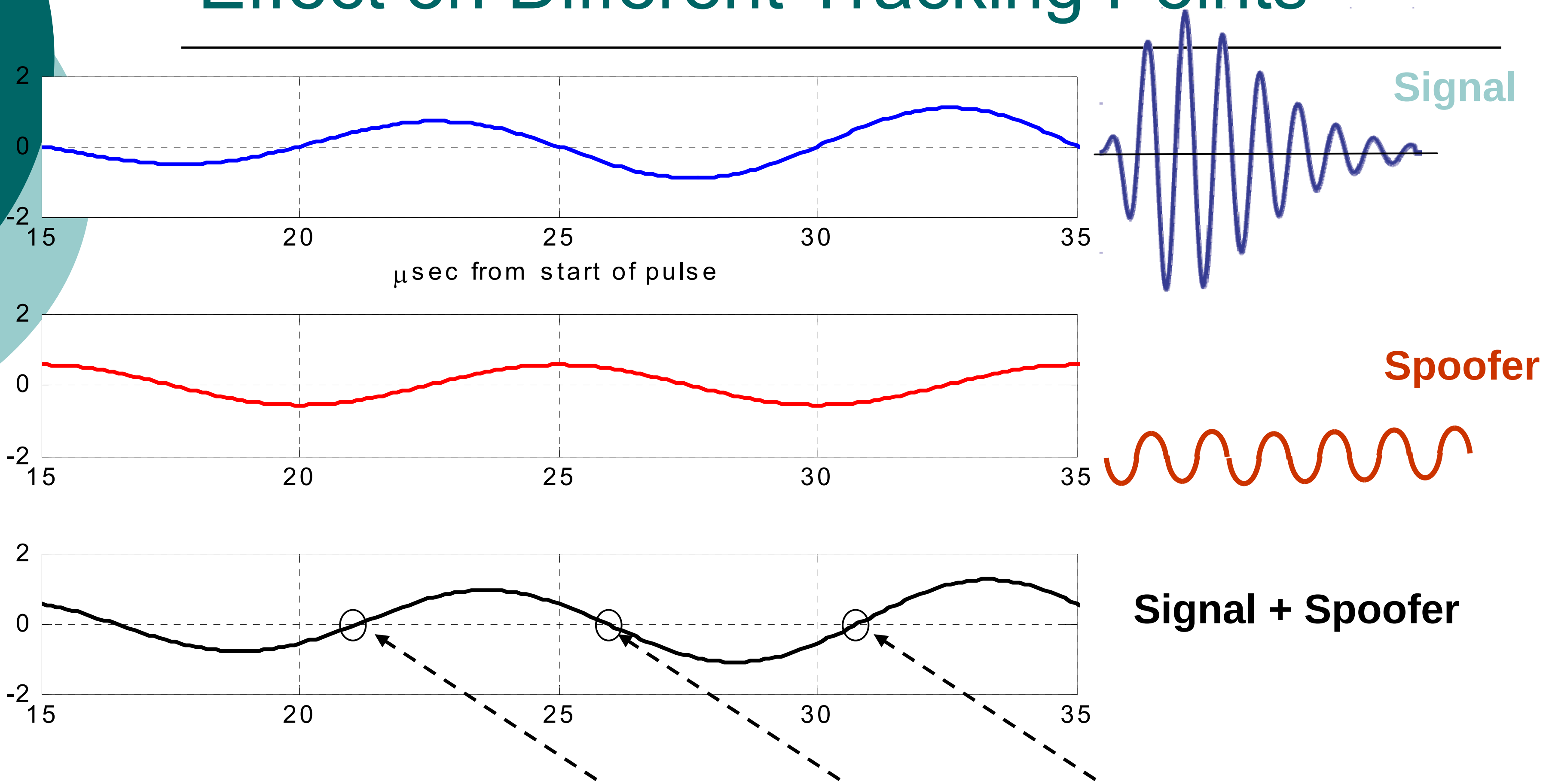
- Key issue: phase center errors for moving or tethered transmitters
- Removed by differential corrections
- Requires
  - Fixed base separate from transmitter
  - Moderate aircraft dynamics


Jamfest Day 3
LORAN Rx vs Cesium
Power cycle test
cs-LORAN Rx (ns)
60
40
20
0
-20
-40
-60
-80
13:40
15:40
17:40
19:40
21:40
23:40
1:40
3:40
5:40
7:40
9:40
Local Time

Typical Loran Field Strength (100 kW transmission)



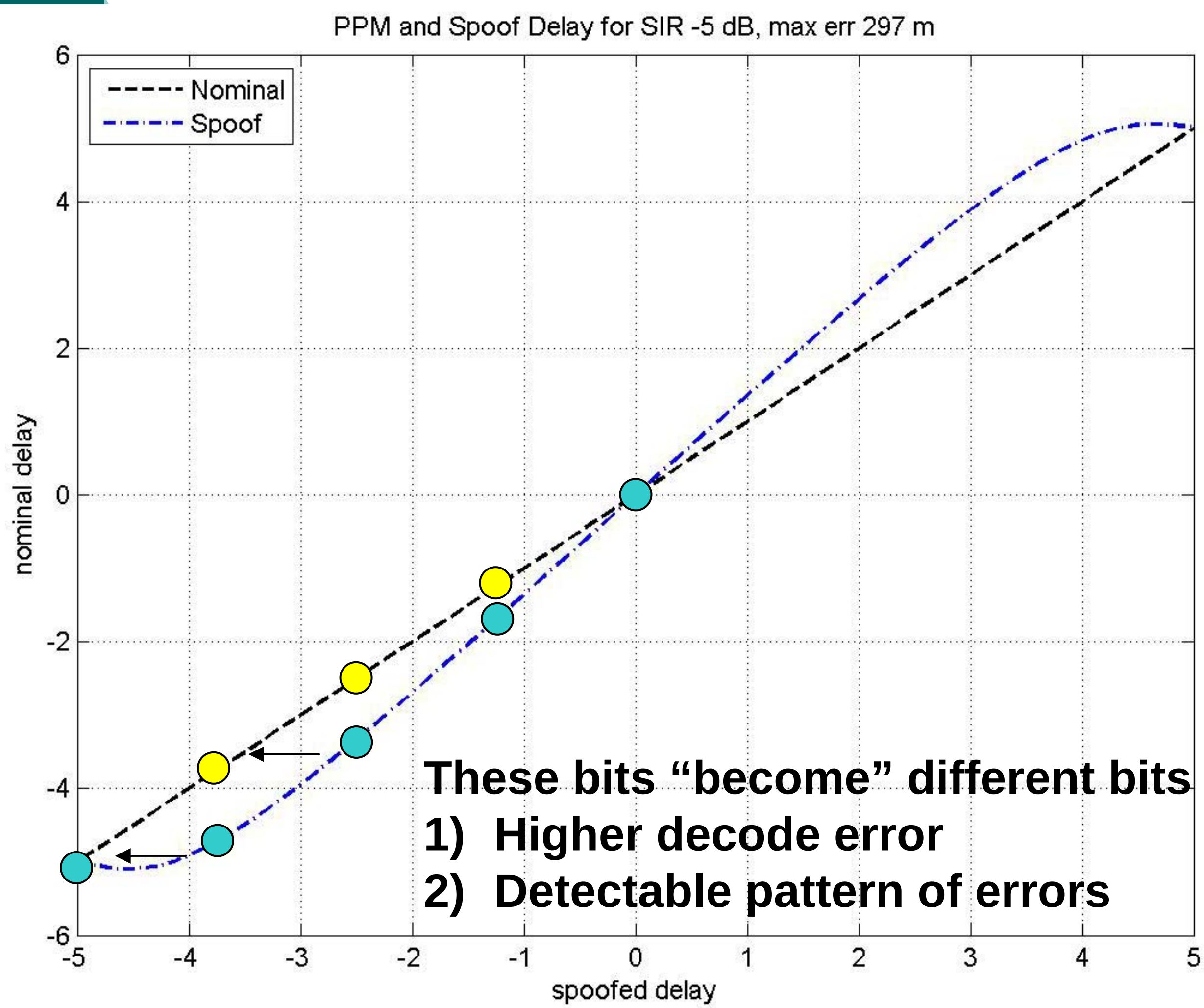
Effect on Different Tracking Points



Tracking point moved by: 1.4 μs (420 m) 1.0 μs (300 m) 0.8 μs (240 m)

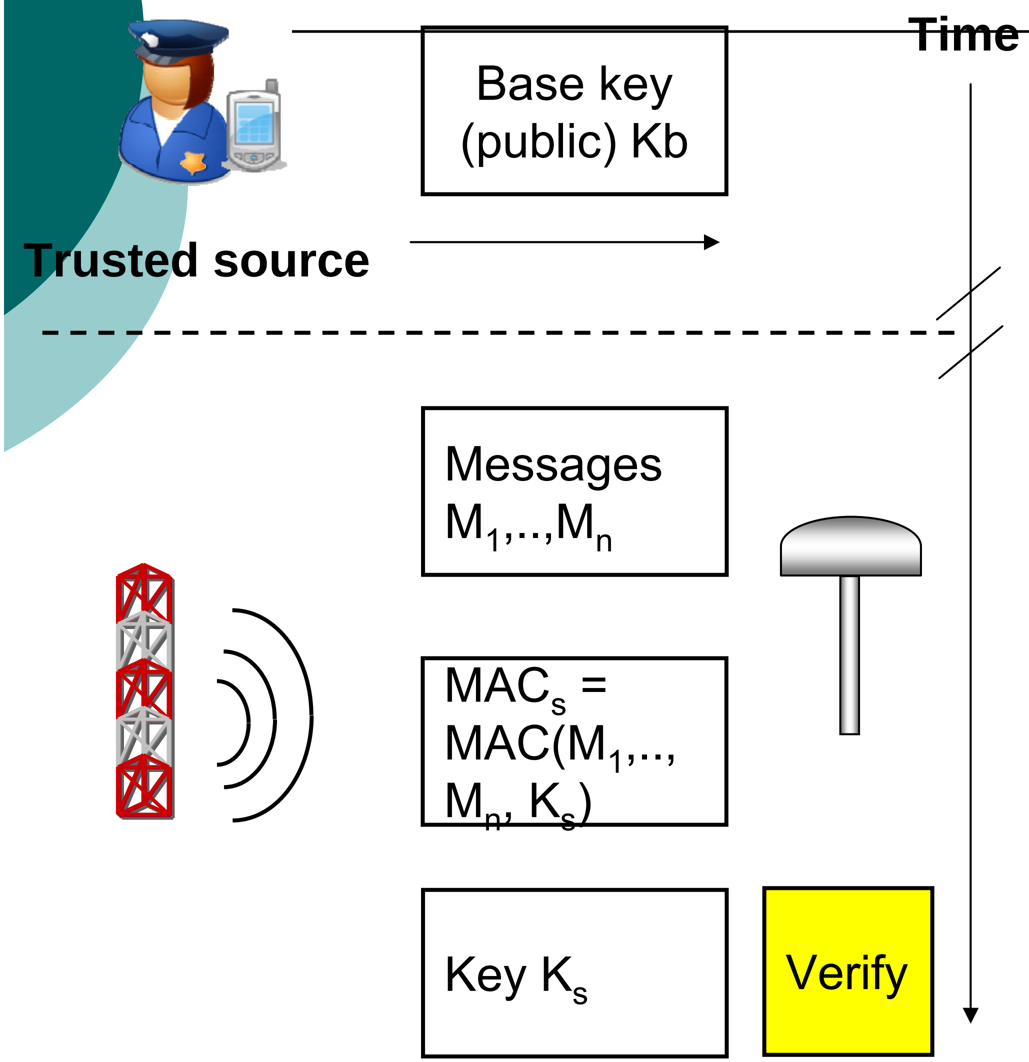
Differences are less than the effects on PPM but have more observations

Effect of spoofing on PPM data



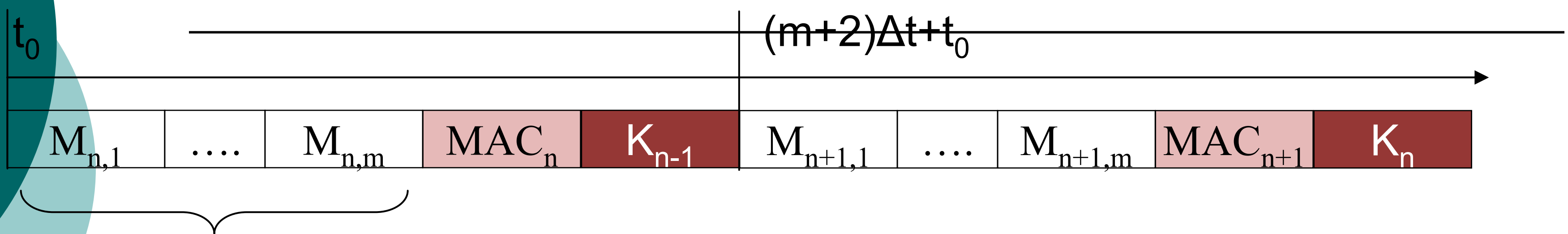
- Spoofing affects PPM bits different
  - Depends on delay
- Spoofer must spoof modulated pulses (otherwise detect)
- Too large a delay will make 2 bits look the same
  - ~ 250 m delay

Authentication in TESLA

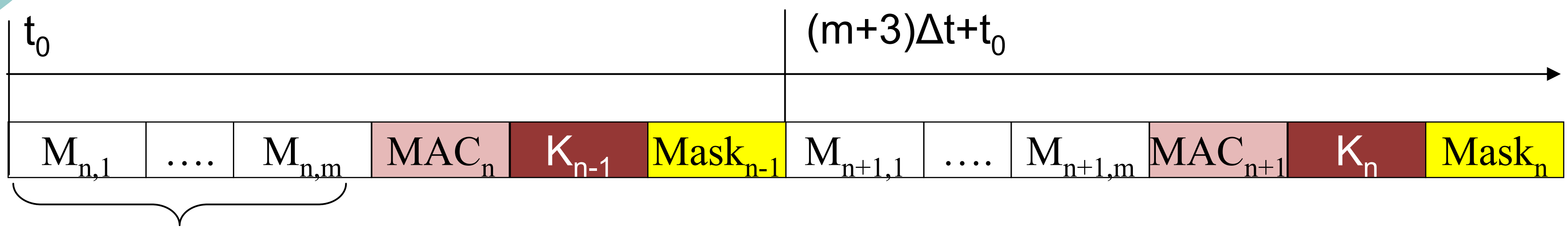


- 1. Get base key k_b
- 2. Receive messages (M_1,...M_n)
- 3. Receive MAC based on keyed hash of messages
  - MAC_s = MAC ([M_1...M_n], K_s)
  - Only transmitter has K_s
- 4. Receive key k_s
  - Verify MAC
  - Verify k_s with base key k_b
    - $k_b = H^s(k_s)$

TESLA and Modified



$$MAC_n = MAC(([M_{n,1} \ldots M_{n,m}]), H'(K_n))$$



$$MAC_n = MAC(([M_{n,1} \ldots M_{n,m}]), H'(K_n))$$

- Can modify TESLA to be
  - More BW efficient – multiple MACs per key
  - More message loss resistant
- Cost is reduced absolute security (though maybe not operational)

Source/Data Authentication

- Public key based
  - Only sender can generate, any one can verify
  - Digital signature on message hash
- Authentication using symmetric algorithms
  - More efficient (computational, data)
  - Message authentication code (MAC)
    - But key used for verification can also sign
  - Desire behavior such that only source can sign
    - Time Efficient Stream Loss-tolerant Authentication (TESLA)
    - Key distribution is delayed