


Assessing the Security of a Navigation System: A Case Study using Enhanced Loran

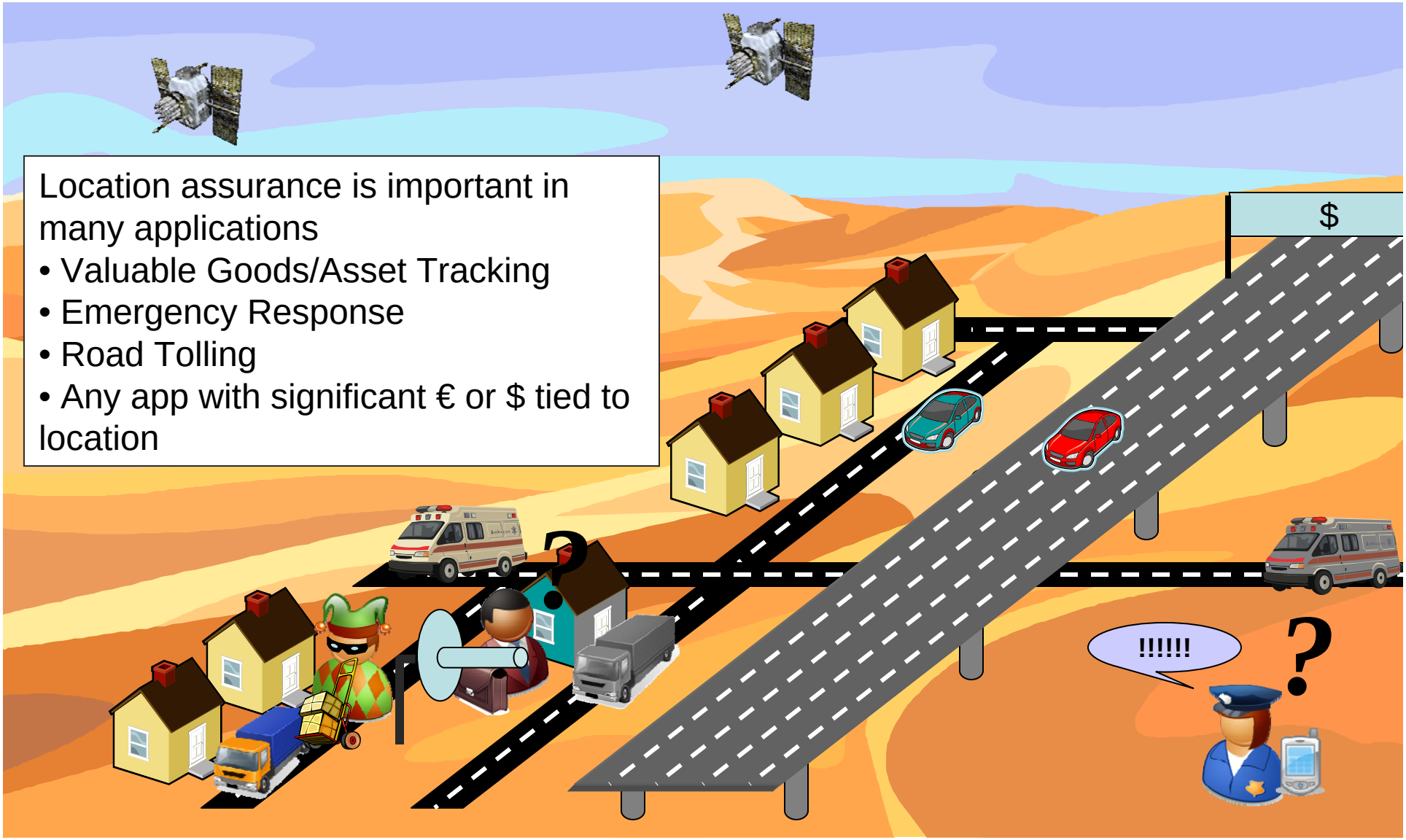
Sherman Lo, Benjamin Peterson, Per Enge

European Navigation Conference

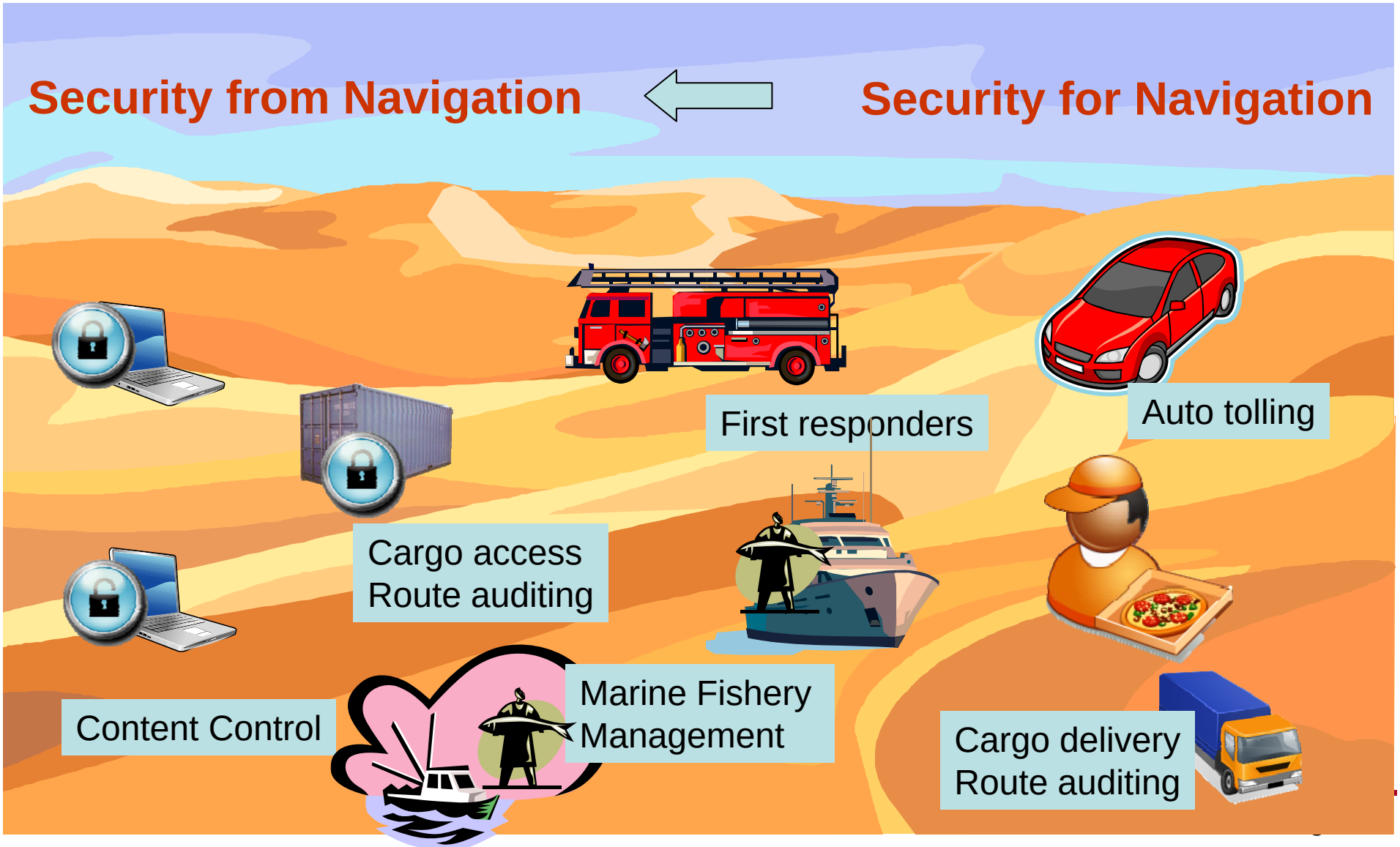
Naples, Italy

May 3-6, 2009

Need for Location Assurance



Secure Navigation

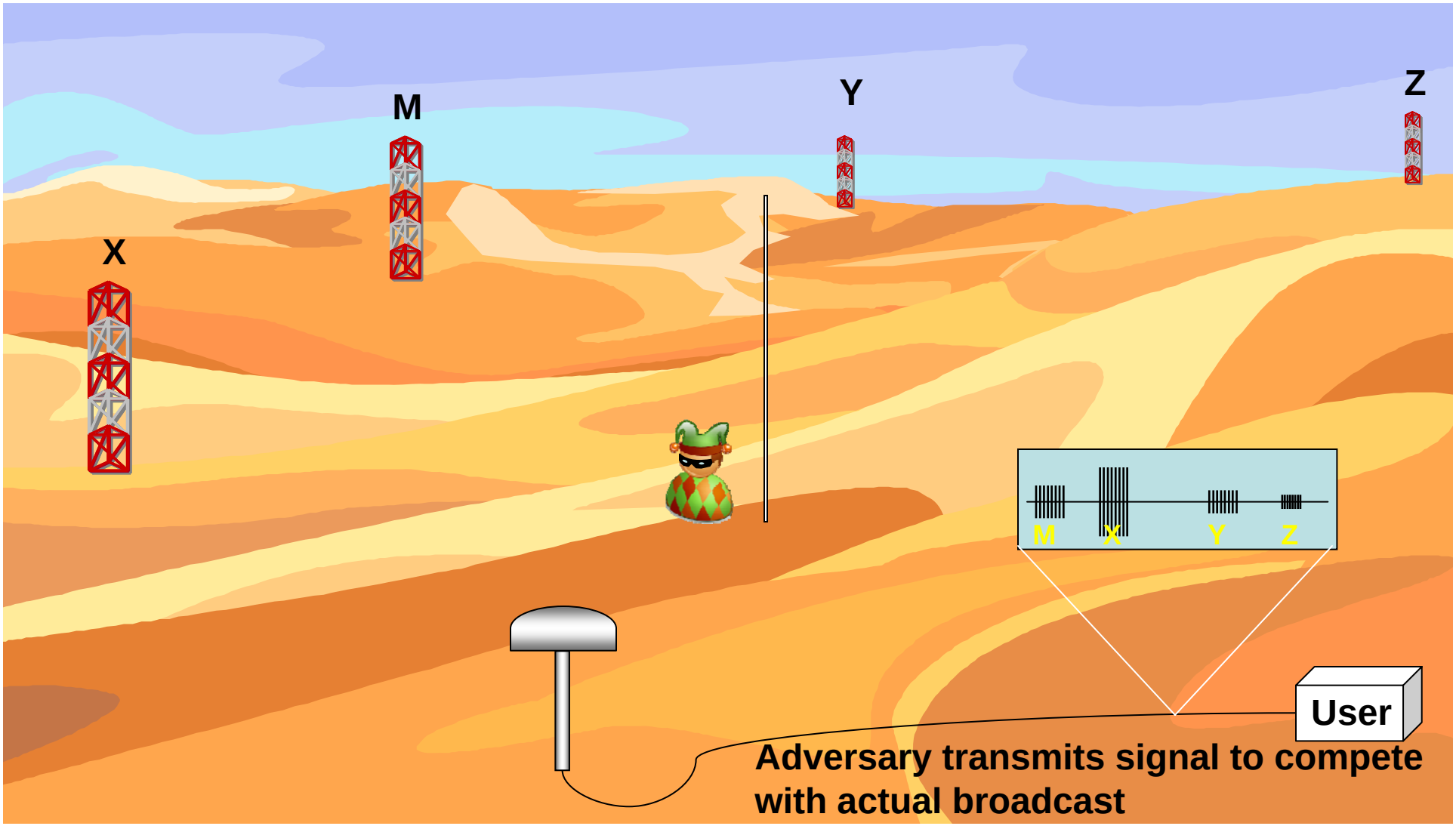


Loran and Secure Navigation

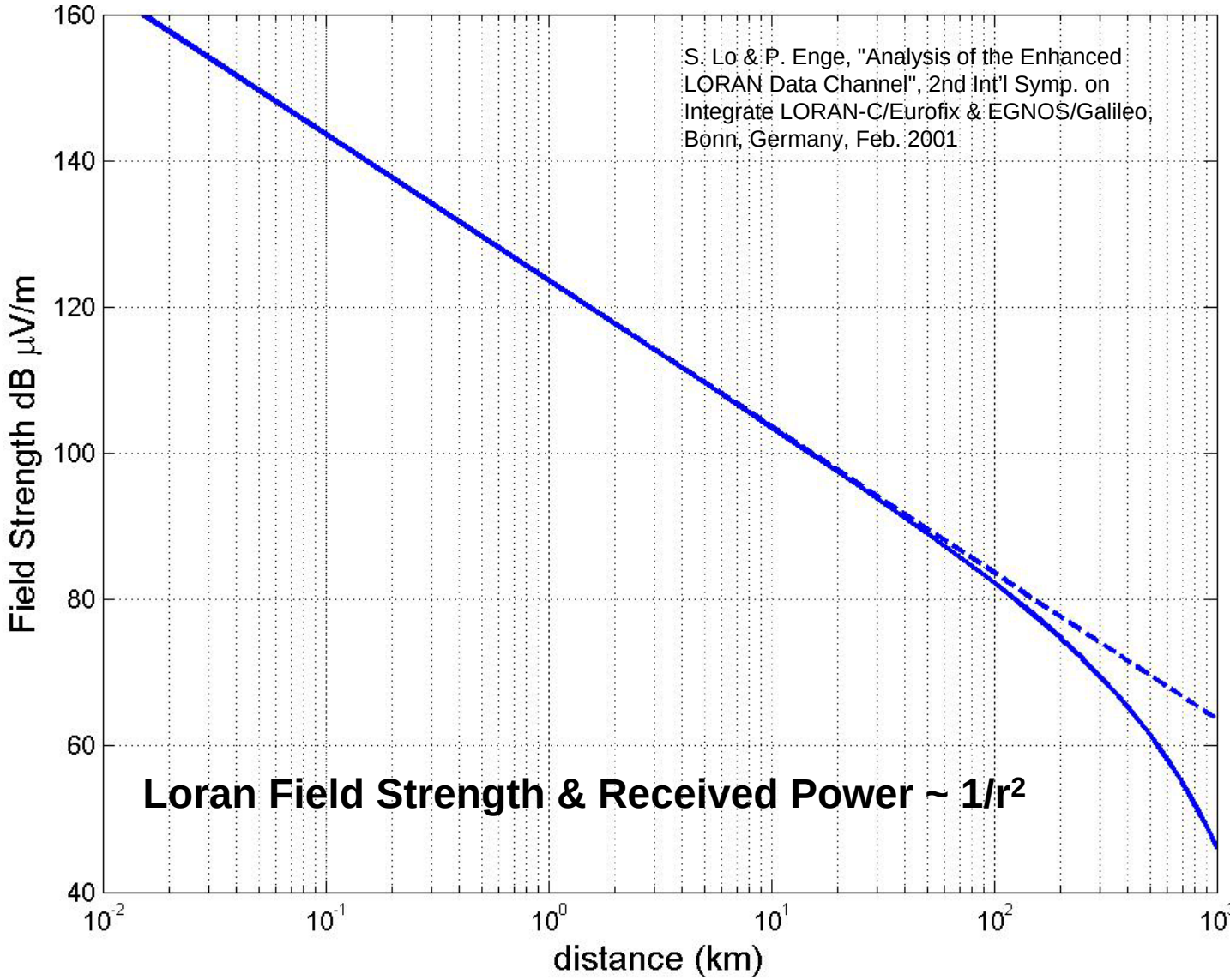
- Claim: Loran has properties that can aid navigation robustness against spoofing and jamming
- Assessment: Examine types attacks & determine robustness to attacks
- Extension: How to use an assured signal to provide navigation security for integrated system (See paper)

Attack Space

On Air Attack: Jamming & Spoofing



Typical Loran Field Strength (100 kW transmission)



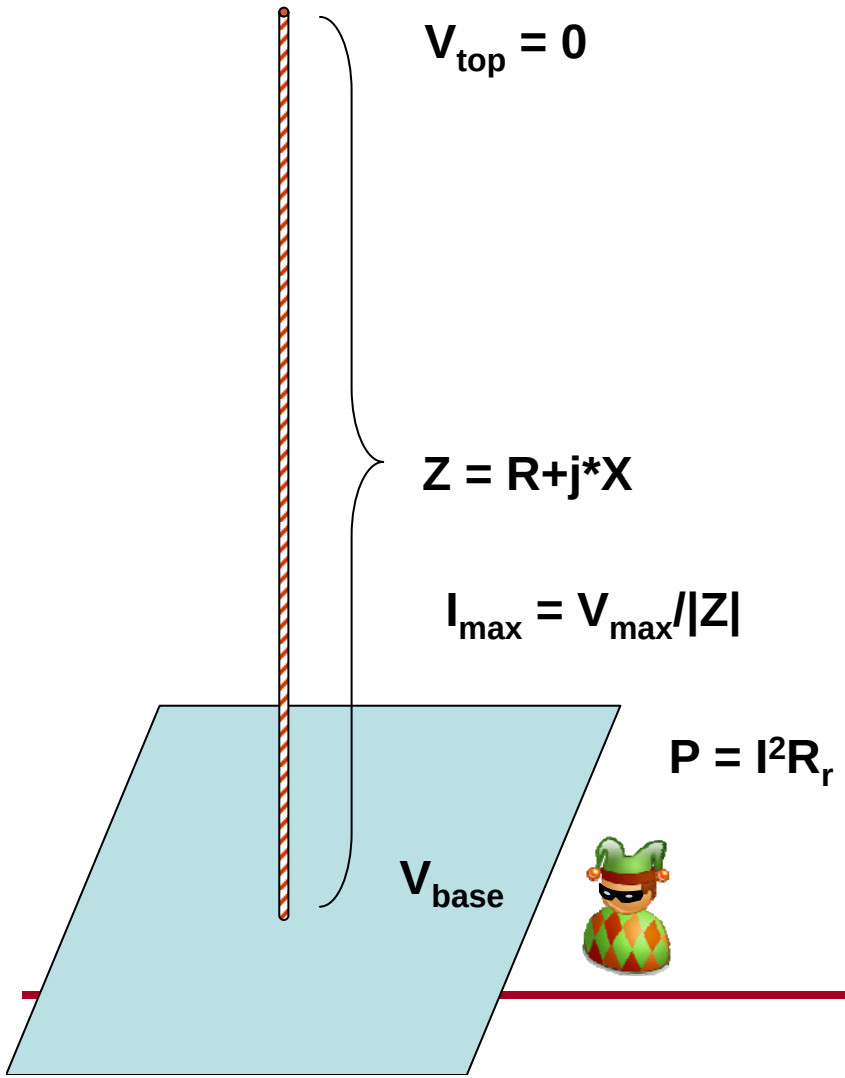
On Air Attacks: Competing with the Loran signal

- Scenario 1: Jamming equaling power of broadcast
  - 400 kW Loran tower at 300 km
    - ~500 km if assume inverse distance^2
    - Need ~40 W at 5 km or ~.4 W at .5 km
- Scenario 2: Spoofing by altering nominal signal
  - 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 wavelength makes efficient transmission difficult with short antenna

Radiation Power

Short Monopole Model



- Short Monopole
  - Voltage zero at end and maximum at base
  - Limit is often this voltage differential (dV_{max})
  - 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 over a ground plane

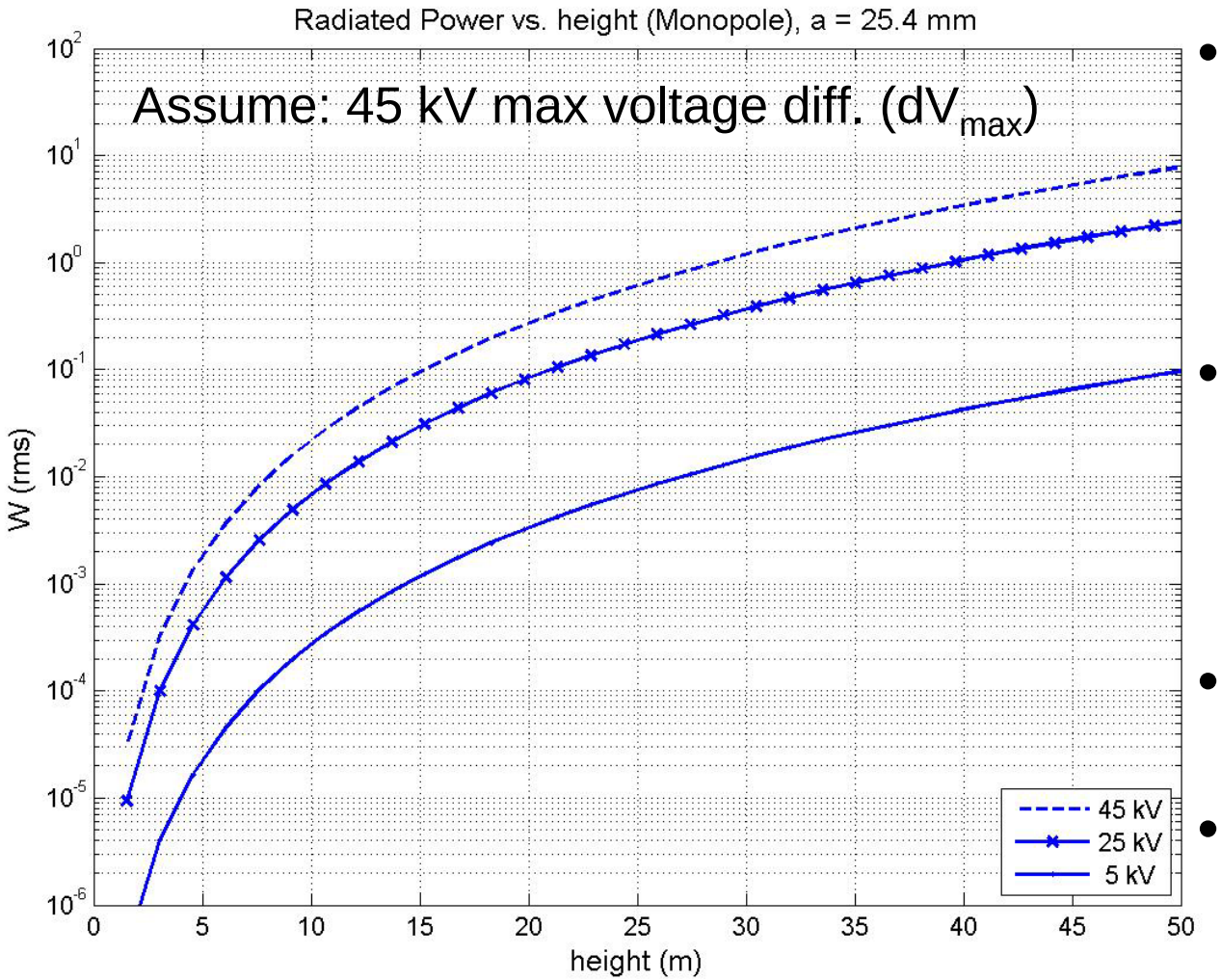
$$R_r = 40\pi^2 \left(\frac{\mathrm{h}}{\lambda}\right)^2 \Omega$$

- Short antenna – reactance is essentially capacitative

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

- Simple assumptions
  - Other impedances are not needed for the analysis (Ohmic losses, etc.)
  - Matching and transmitter system losses are not considered
  - Ideal ground plane but no guy wires, top loading

Radiated Power vs. Minimum Antenna Height



- Very High Q
  - Narrowband
  - Stored energy >> radiated energy
- As h decreases
  - R_r decreases
  - X increases
  - I, given dV_{max}, decreases
- $P_r \sim 1/h^4$
- Model less appropriate for larger antenna

Jamming/Spoofing Results

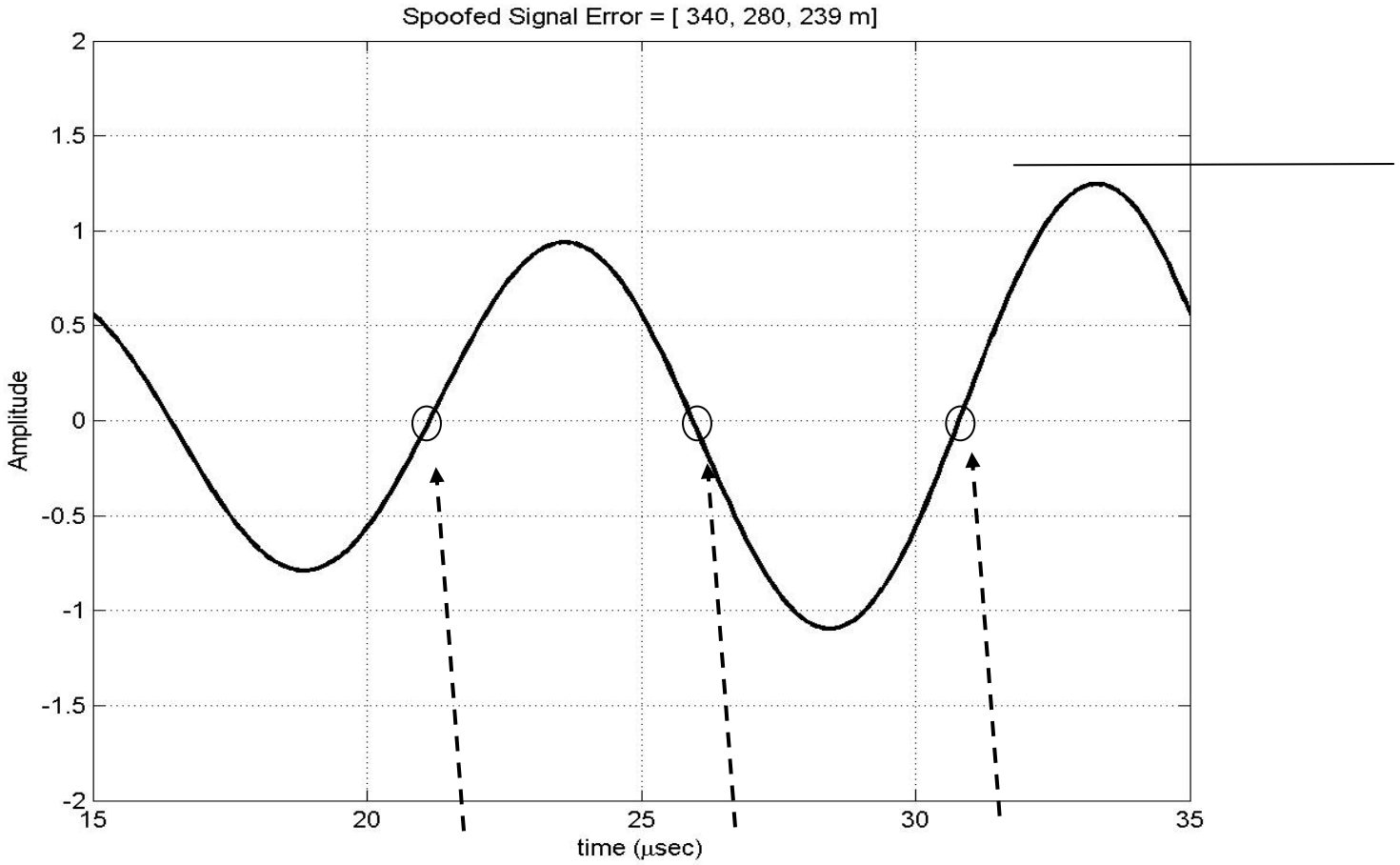
Scenarios (5 & 0.5 km)	**a = 2.3 mm**	**a = 25.4 mm (wire radius)**	**a = 50 mm**
Jamming (40 W, 0.4 W)	90 m, 27 m	78 m, 22 m	73 m, 21 m
Spoof 150 m error (4 W, 40 mW)	49 m, 14 m	42 m, 12 m	39 m, 11 m

- 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 spoofing 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
  - See paper
- Affect on different tracking points

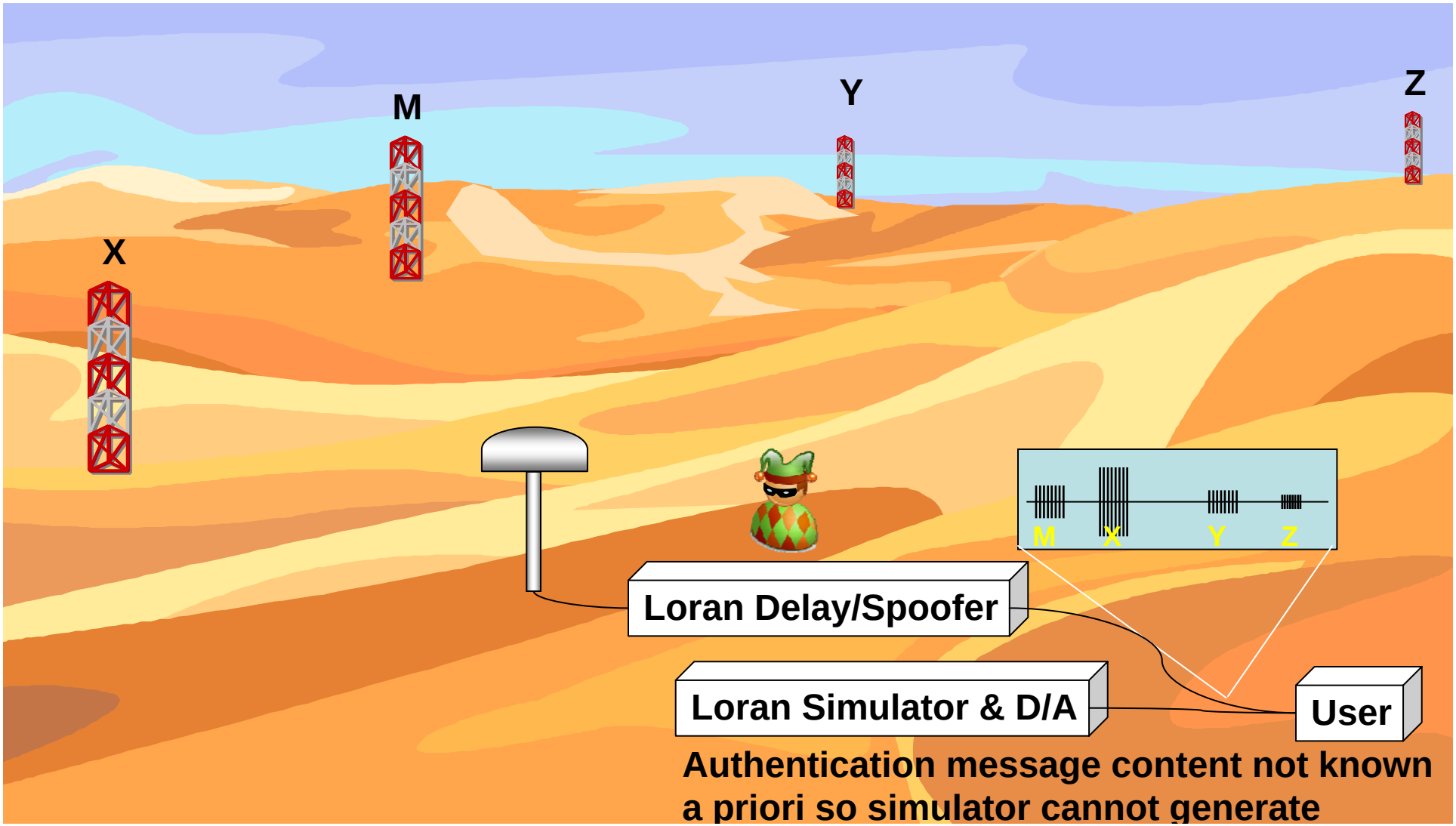
Effect on Different Tracking Points



Tracking point moved by: **1.13 μs (340 m)** **0.93 μs (280 m)** **0.8 μs (240 m)**

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

Simulator/Direct Injection attack



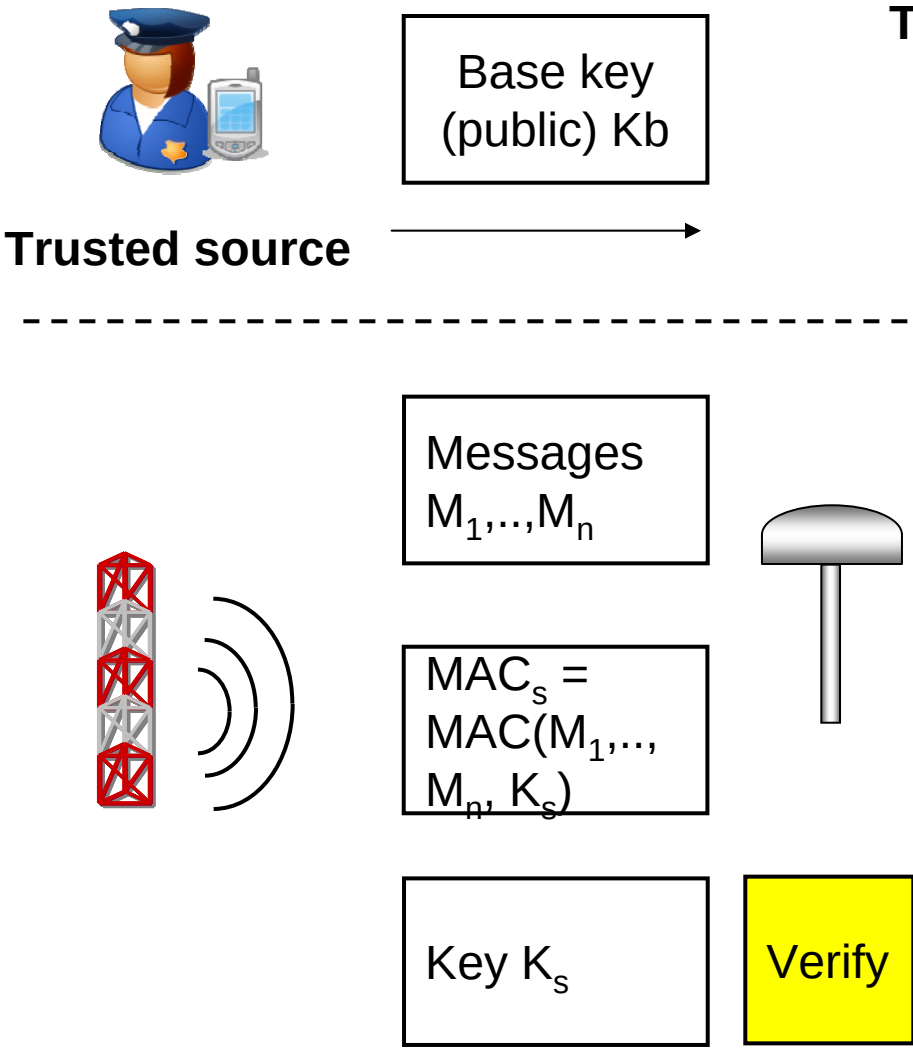
Defending against Direct Injection Attack

- 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

Source/Data Authentication

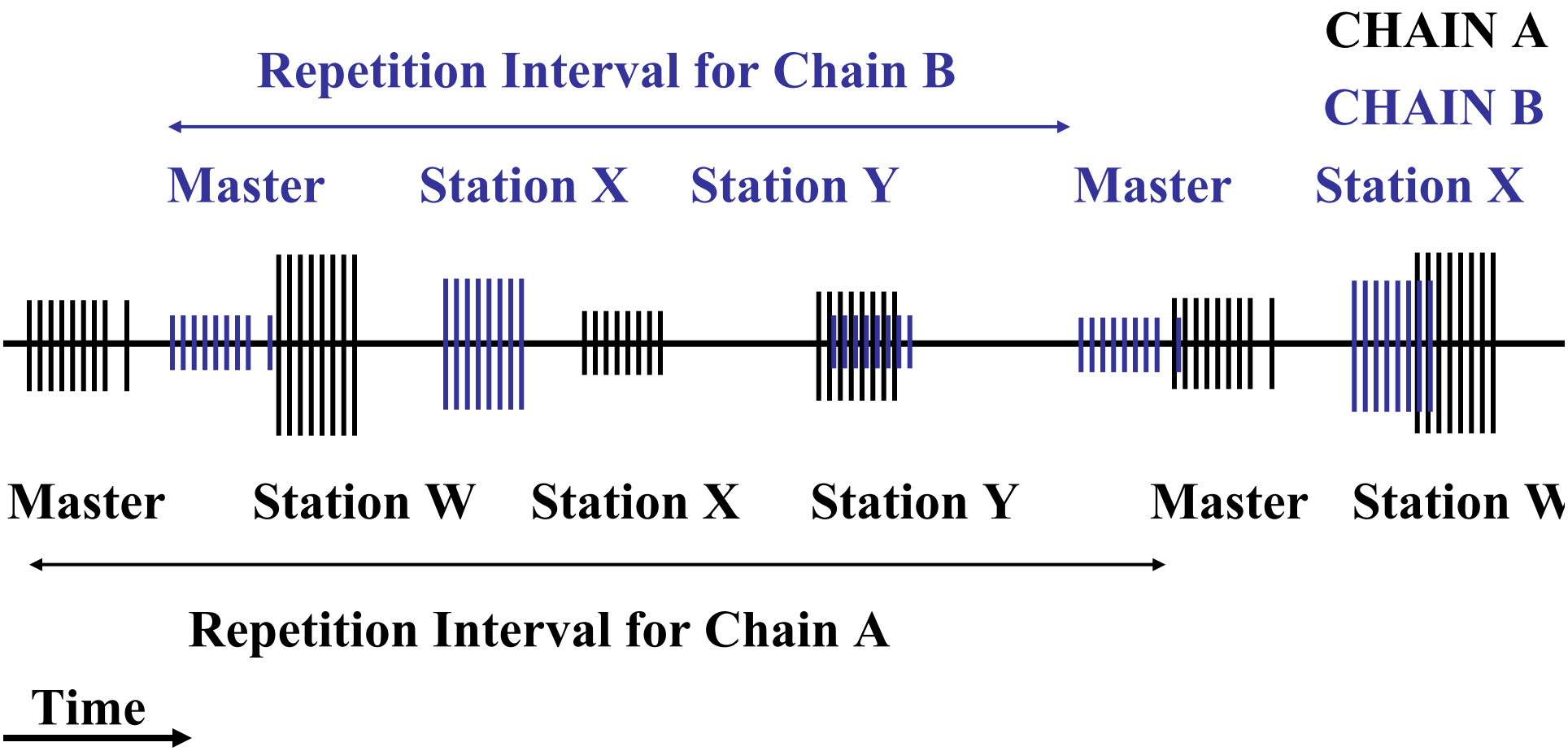
- Public key based
  - Only sender can generate, any one can verify
  - Digital signature on message hash
- Authentication using symmetric algorithms
  - More efficient (computational, data)
  - Message authentication code (MAC)
    - But key used for verification can also sign
  - Desire behavior such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

Example Data Authentication: TESLA



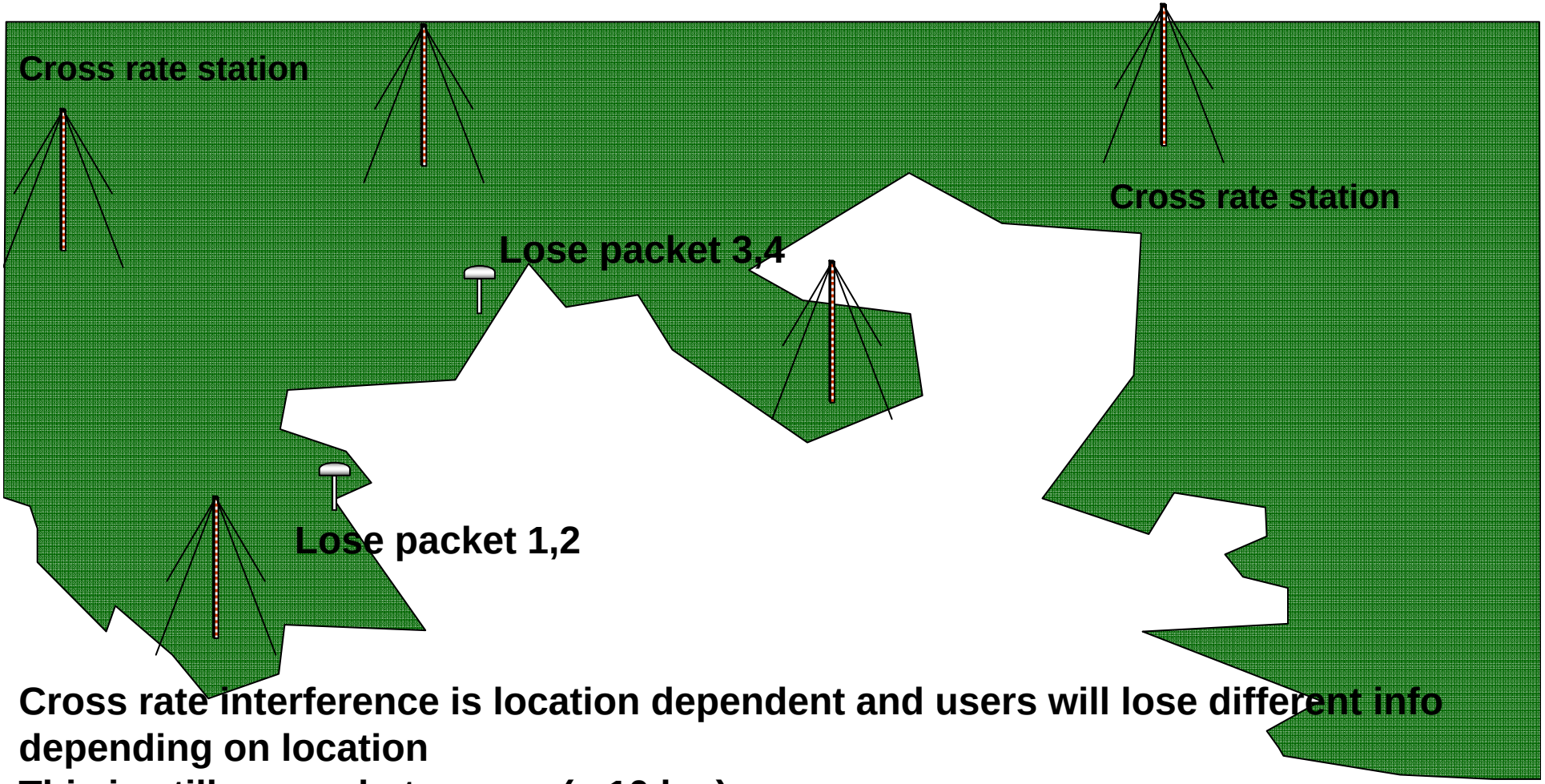
- Examining modifying to better suit navigation
- Modify TESLA to be
  - More BW efficient – multiple MACs per key
  - More message loss resistant
- Cost is reduced absolute security (though maybe not operational)

LORAN Chain Timeline



- Loran cross rate interference depends on time and location

Location Dependent Information

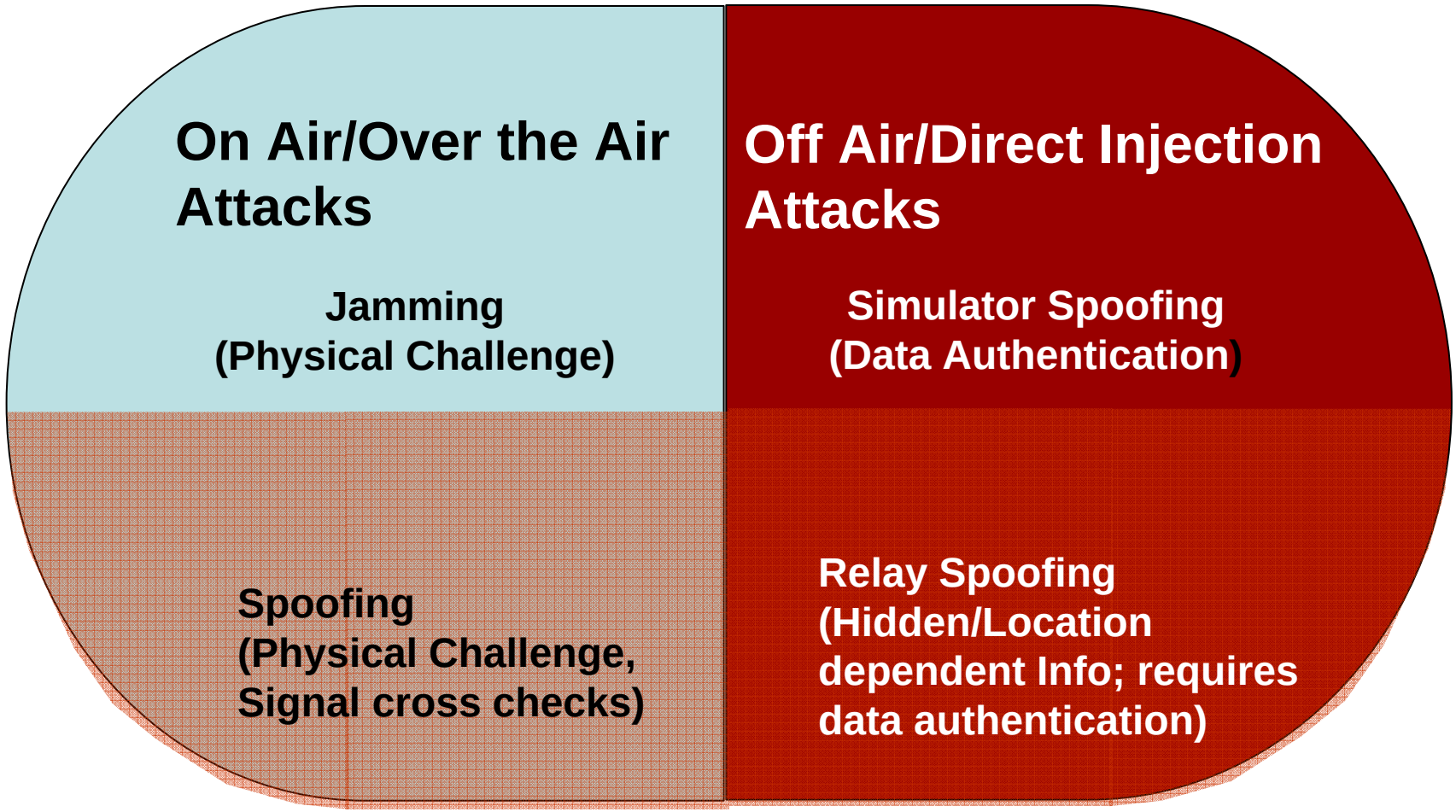


Cross rate interference is location dependent and users will lose different info depending on location

This is still somewhat coarse (~ 10 km)

Note: Lossed info can also be confirmed using FEC

Attack/Defense Space



Conclusions

- Need to apply thorough security/attack evaluation to study navigation security
- 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
- 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

Acknowledgments & Disclaimer

- The authors gratefully acknowledge the support of the Federal Aviation Administration and Mitchell Narins under Cooperative Agreement 2000-G-028.

- 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.