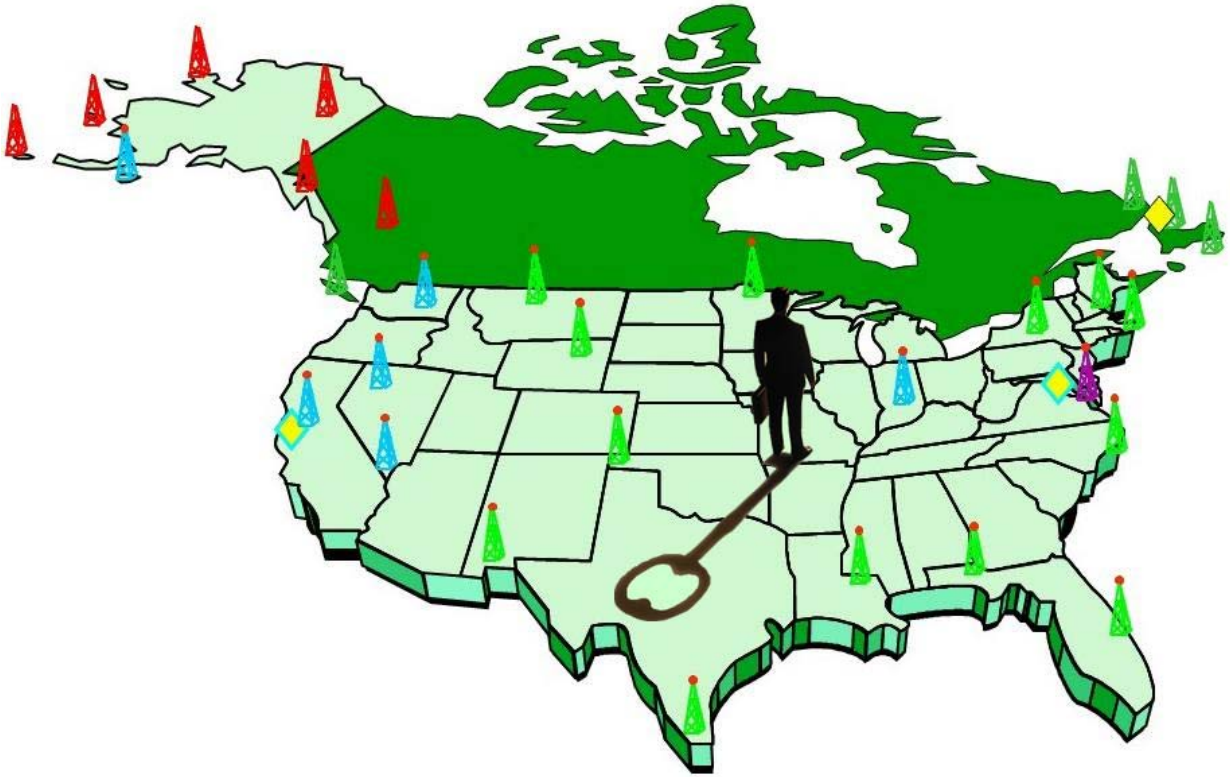
Geoencryption Using Loran



Di Qiu, Sherman Lo, Per Enge

Stanford University

Sponsored by FAA Loran Program

Why Geoencryption?

Unsecure world

- Data/Information security
- Piracy concern

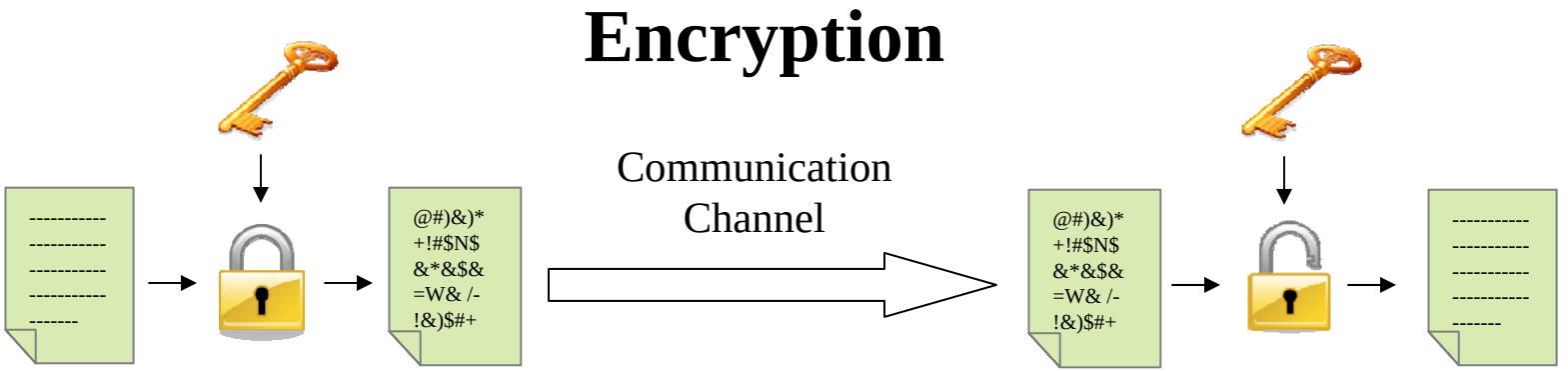
Traditional cryptosystems have inconveniences or weaknesses

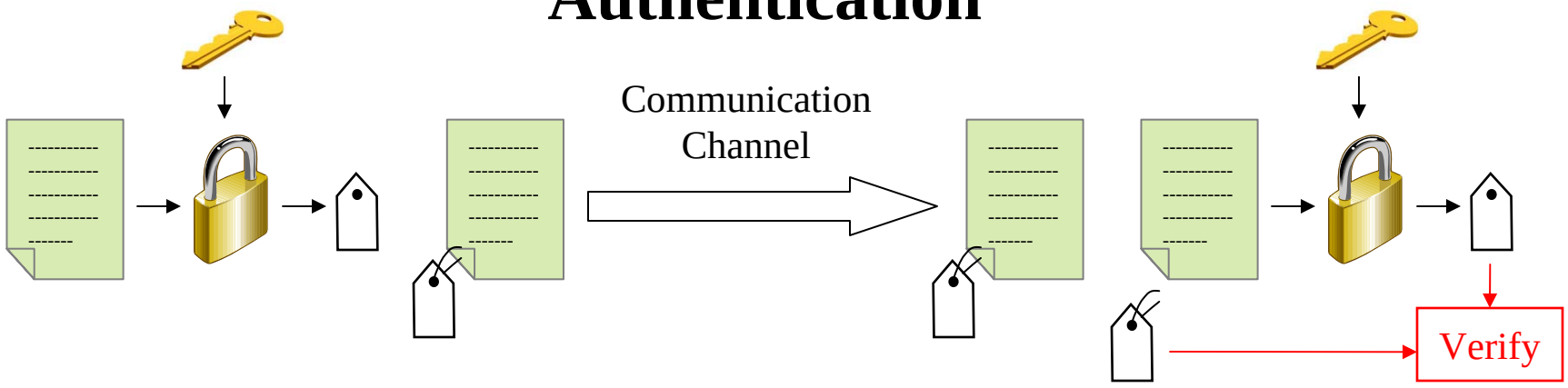
- Something you know: PIN, passwords
- Something you have: key, smart card
- Something you are: biometrics

Location for Security

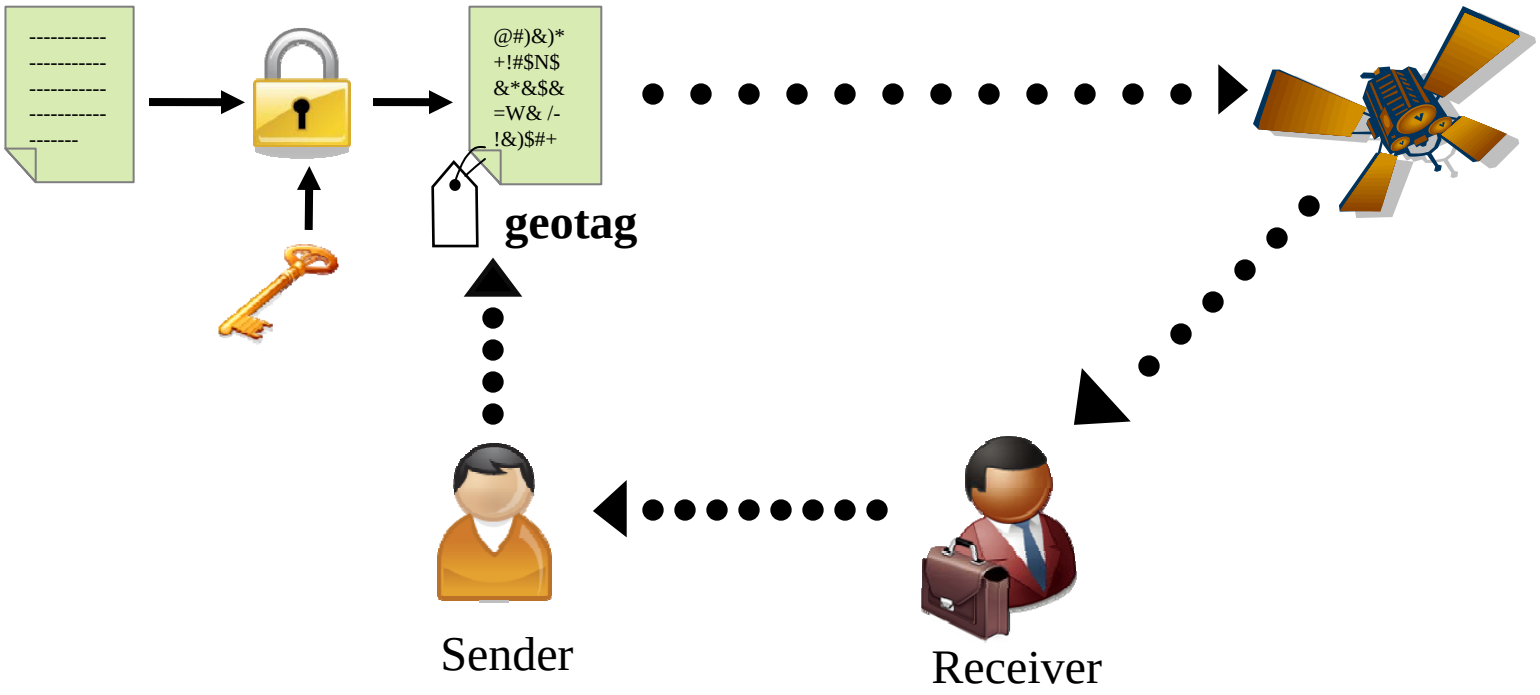
- Universality
  - Do all people have it?
- Collectability
  - How well can an identifier be captured or quantified?
- Circumvention
  - foolproof
- Uniqueness
  - Can people be distinguished based on an identifier?

Encryption and Authentication

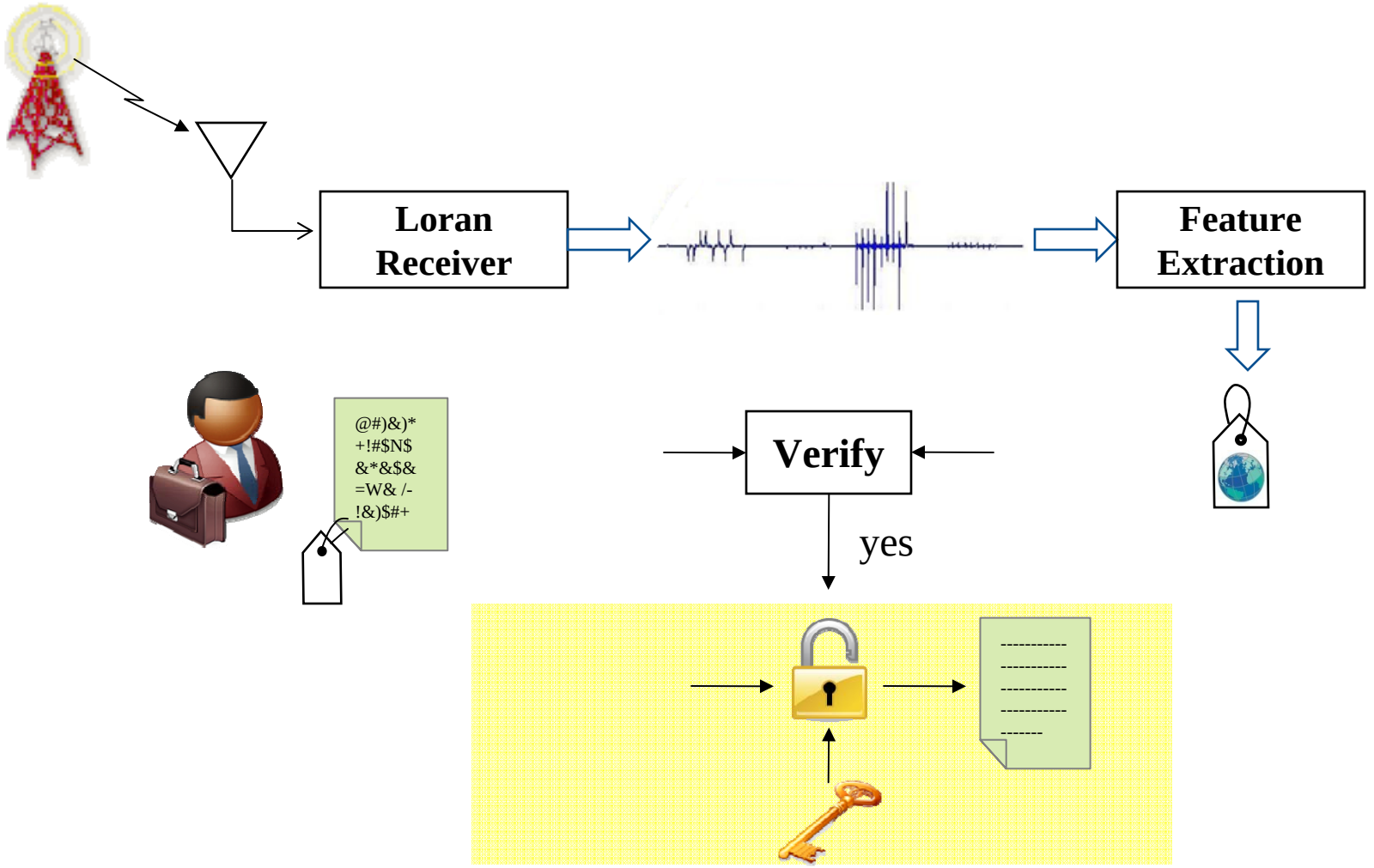




Geoencryption



Geodecryption



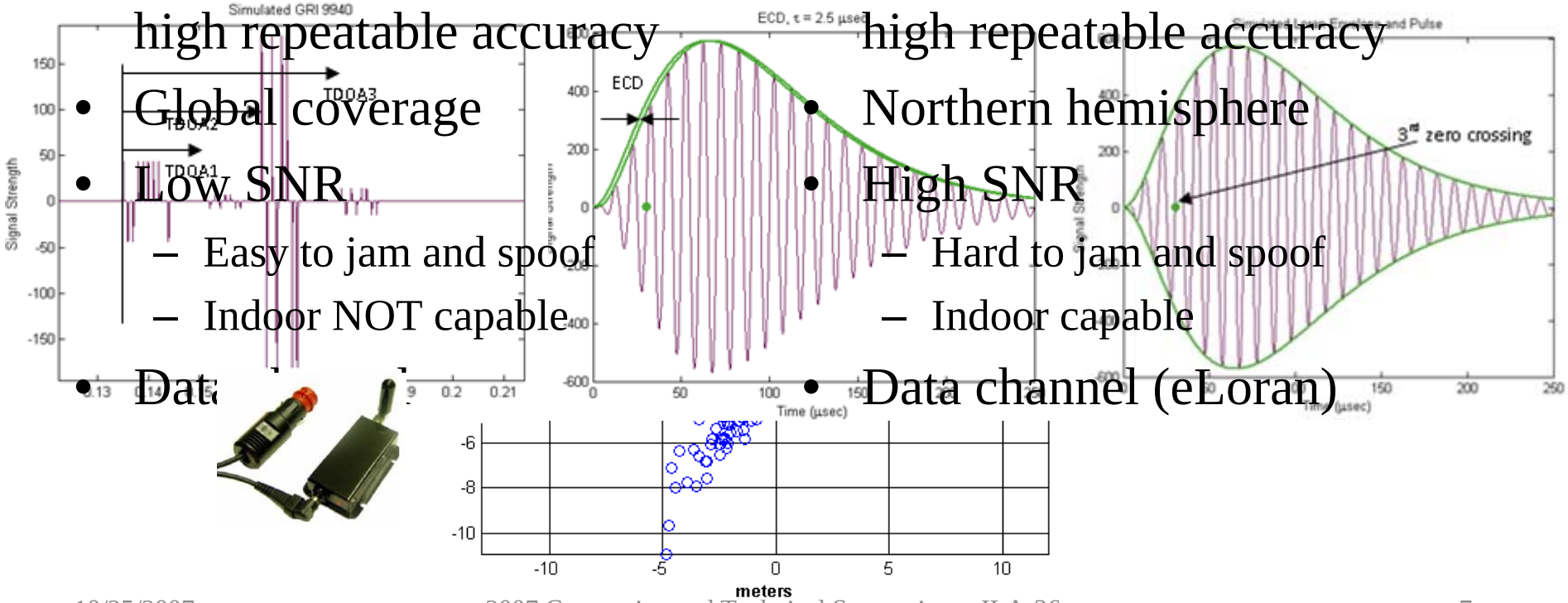
Why Loran?

GPS

- Non-stationary satellites
- High absolute accuracy, high repeatable accuracy
- Global coverage
- Low SNR
  - Easy to jam and spoof
  - Indoor NOT capable
- Data channel

Loran

- Stationary transmitters
- Low absolute accuracy, high repeatable accuracy
- Northern hemisphere
- High SNR
  - Hard to jam and spoof
  - Indoor capable
- Data channel (eLoran)



Security Analysis Outline

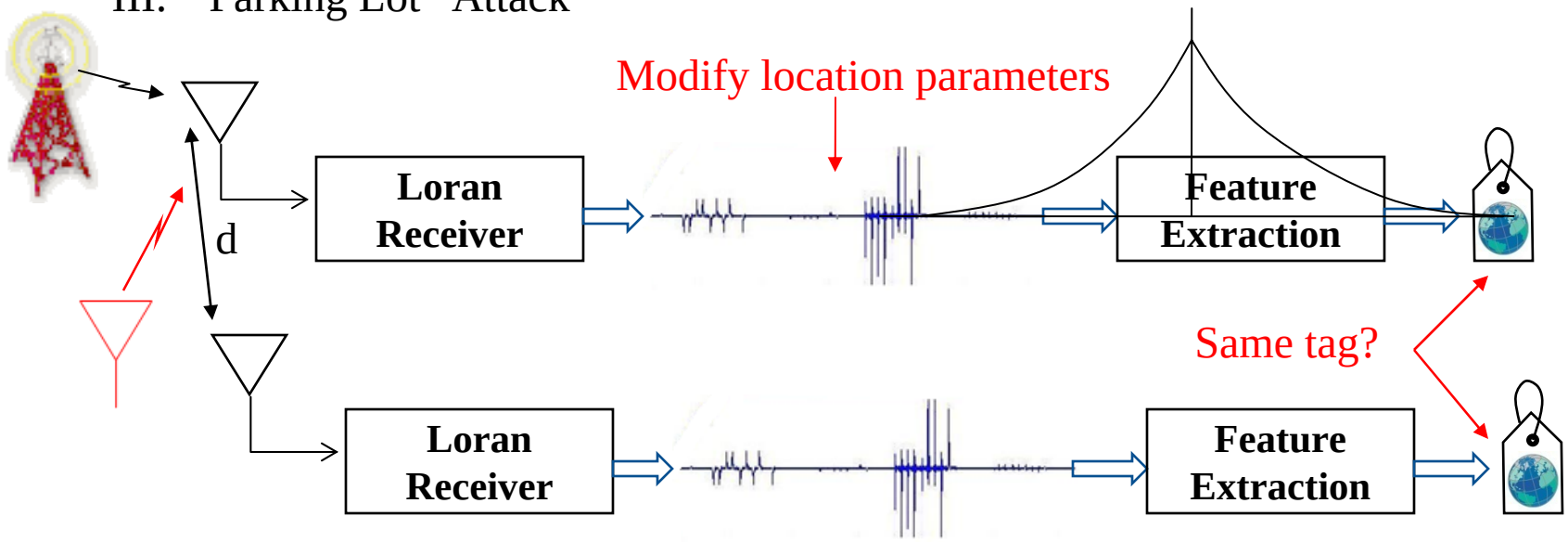
Security

Vulnerabilities of Protocol/Implementation

I. Spoof
II. Replay
III. "Parking Lot" Attack

Tag Size

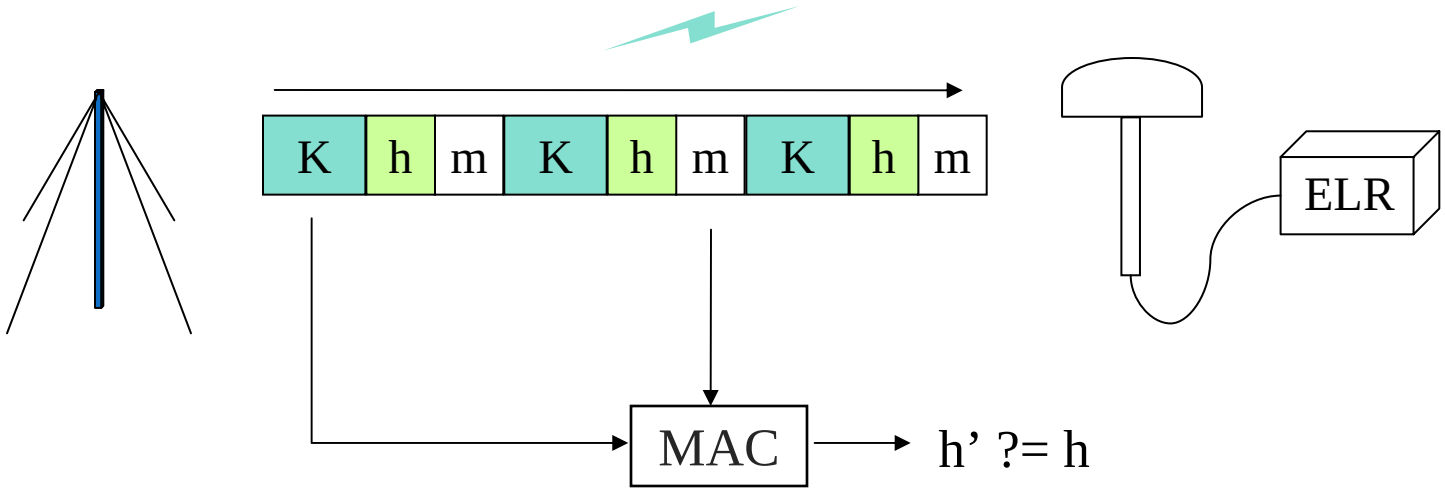
IV. Spatial decorrelation



Signal Authentication

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

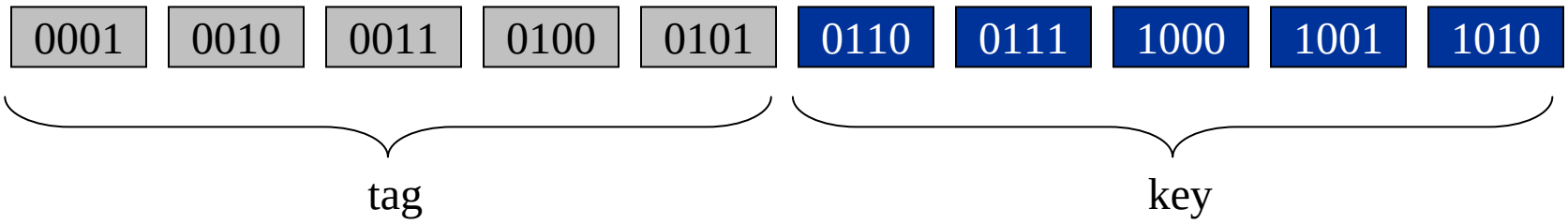
- TESLA – Timed Efficient Stream Loss-tolerant Authentication
- Authenticating message = key (K) + tag (h)
- Tag = MAC (Data, Key)



Authentication Test

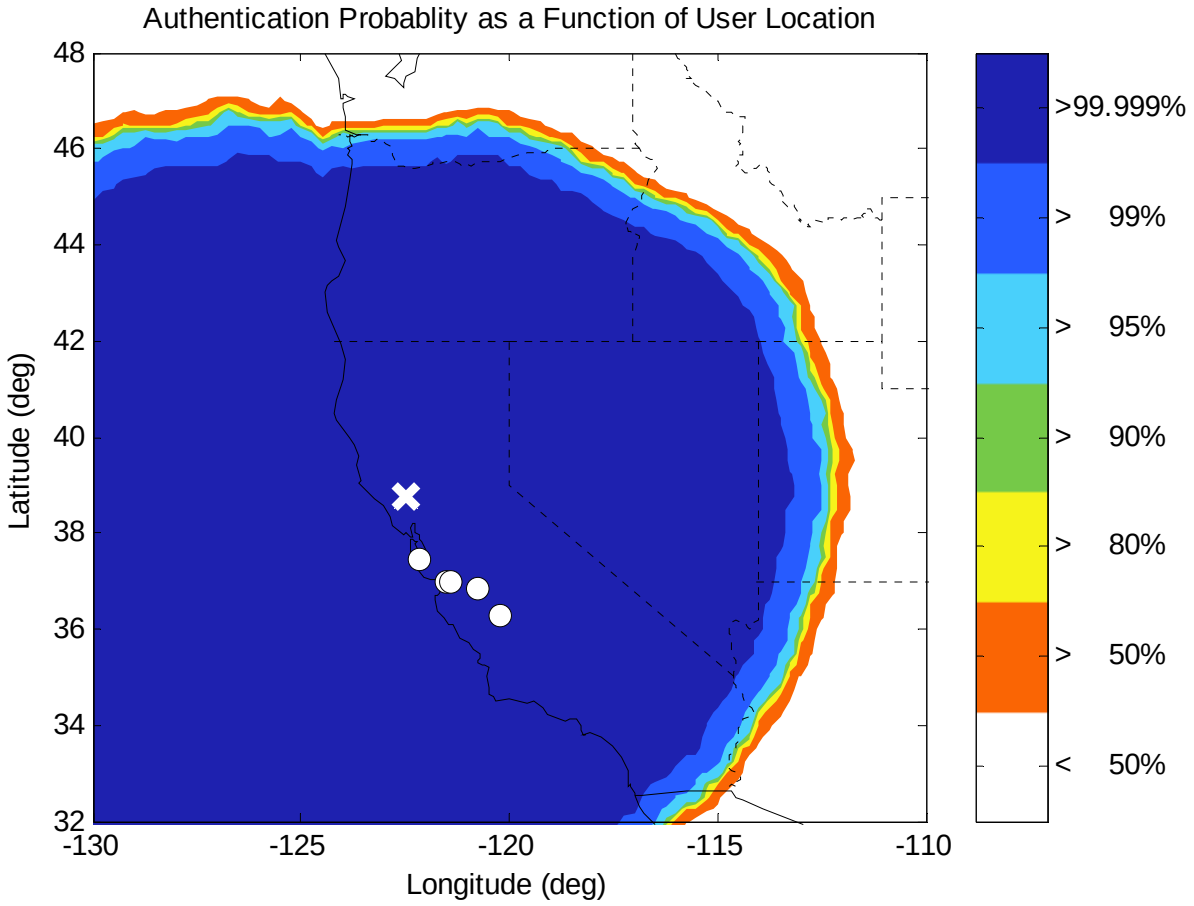
I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

- Middletown
- Circular TESLA chain
- 50% Bandwidth
- Message subtypes
  - Type 1-4 (0001-0100): first 148 bits of the tag
  - Type 5 (0101): last 12 bits of tag,
  - Type 6-9 (0110-1001): first 148 bits of key
  - Type 10 (1010): last 12 bits of key



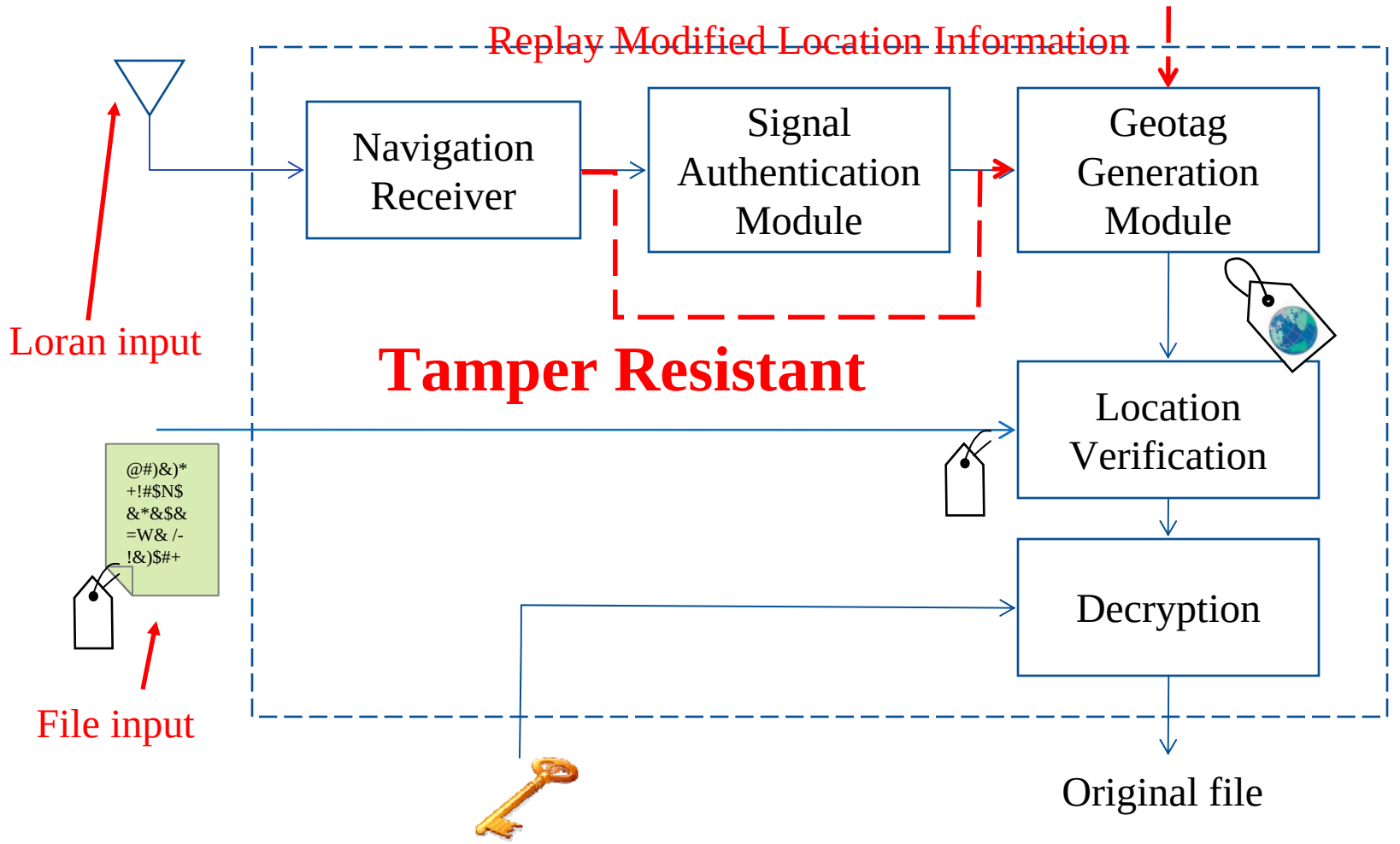
Authentication Test Result

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

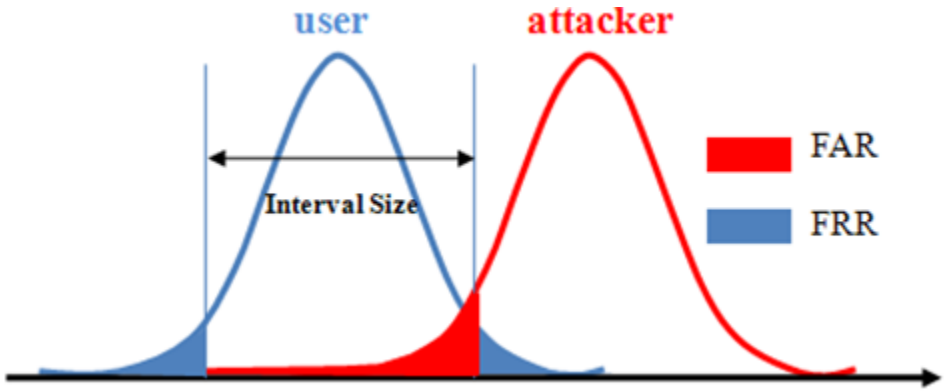


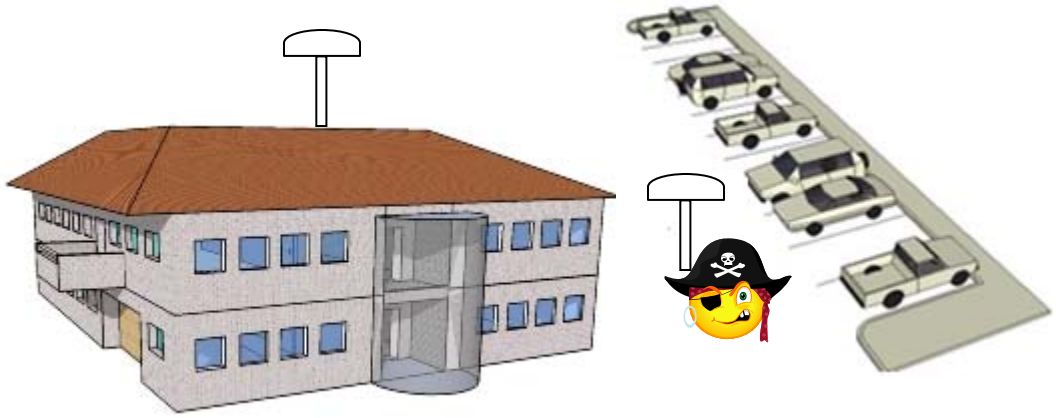
Loran Certified Receiver

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.



Parking Lot Attack

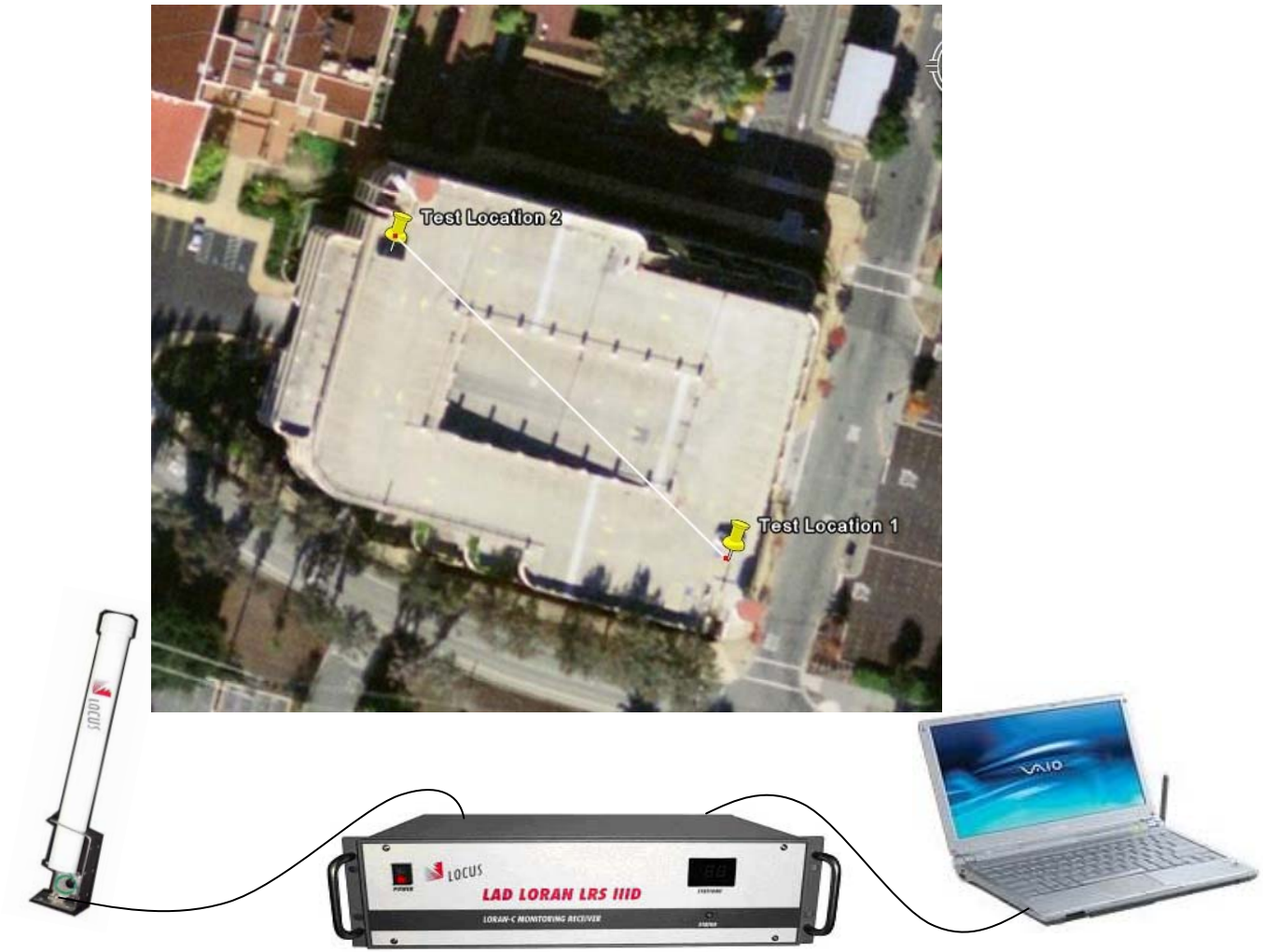




- False Accept Rate (FAR): % of unauthorized persons accepted in error
- False Reject Rate (FRR): % of authorized persons who are incorrectly denied acceptance
- Trade off between FAR and FRR

Data Collection

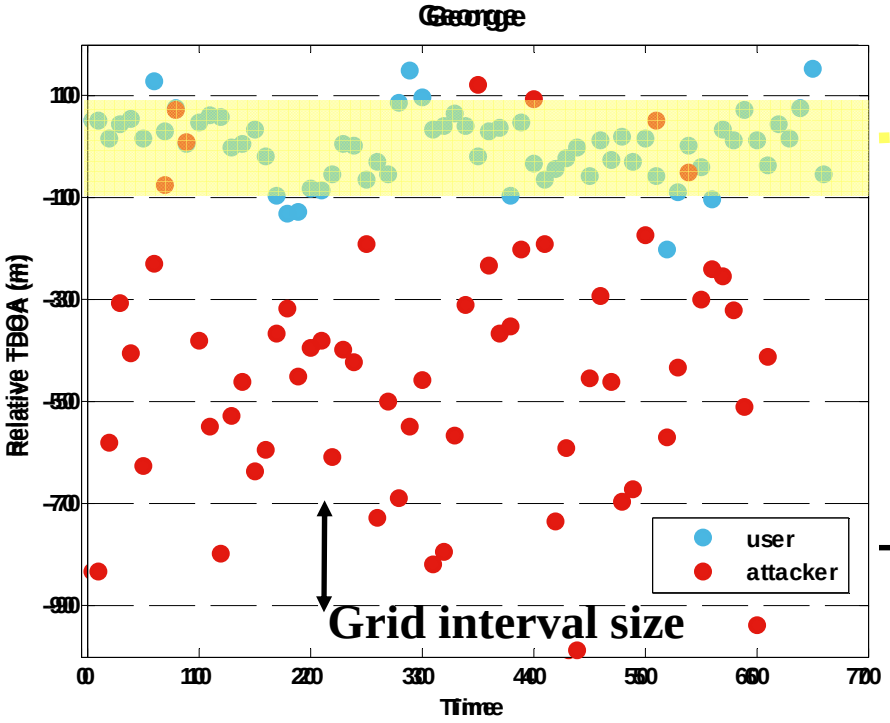
I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.



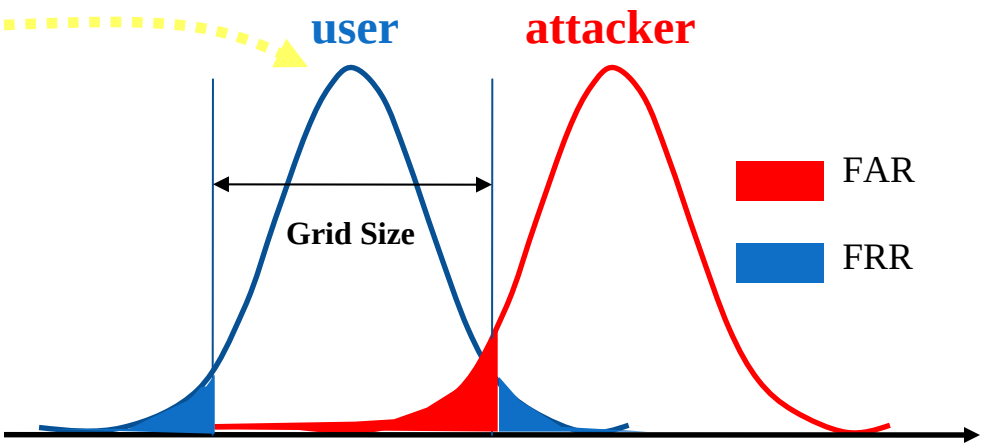
FAR & FRR Estimation

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

Experimental Analysis



Analytic Analysis

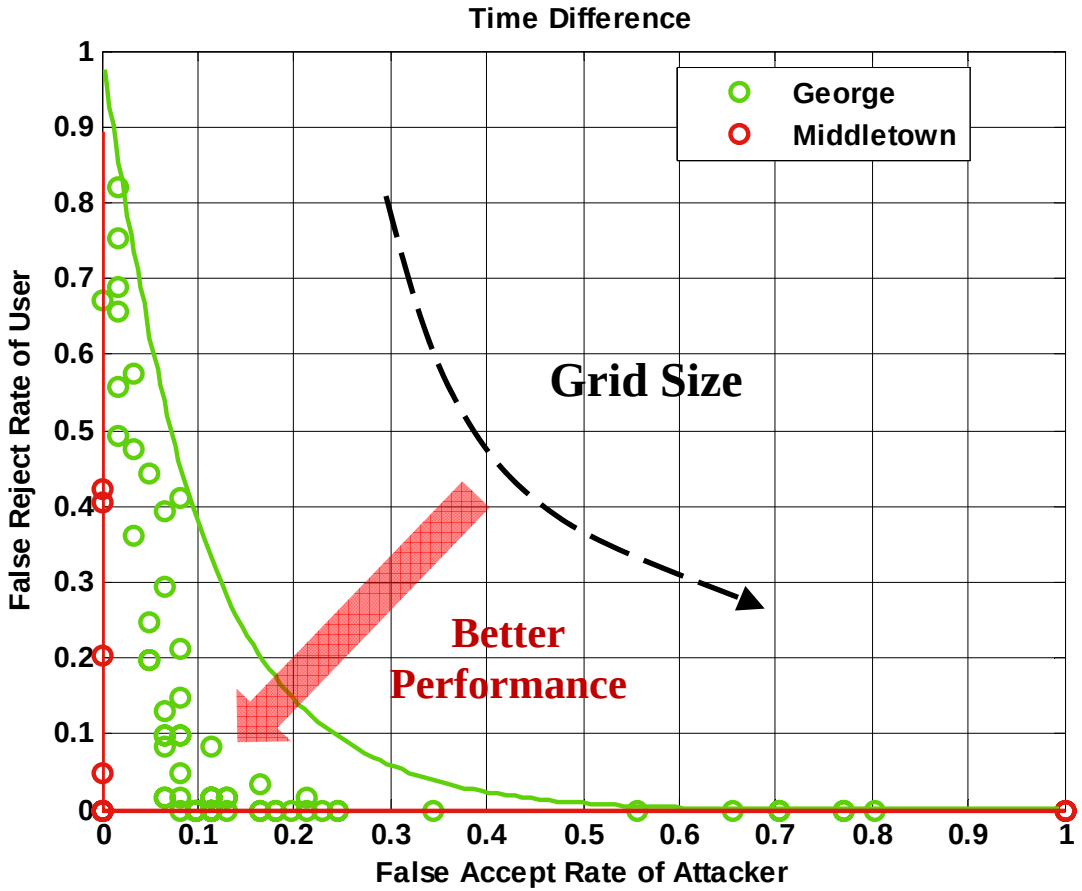


FAR = Q(interval size, σ, distance)

FRR = Q(interval size, σ)

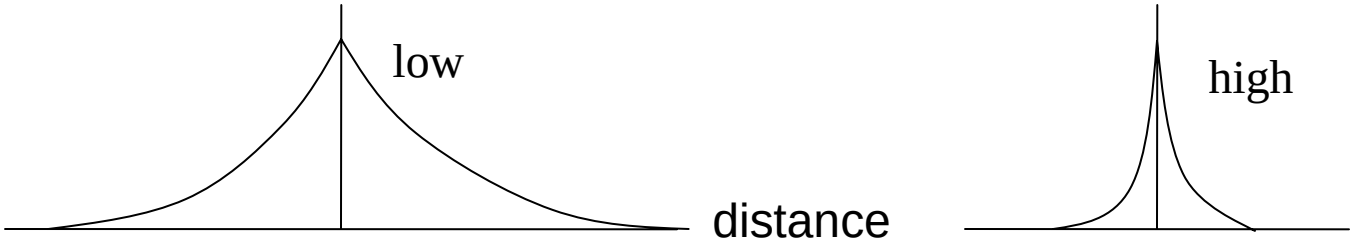
Receiver Operating Curve

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.



Spatial Decorrelation

- High spatial decorrelation is preferred.



- Evaluation functions
  - Distance measure
  - Error rates measure - FAR
  - Information measure - relative entropy D(p||q)
  - Dependence measure - correlation coefficient

Test Locations

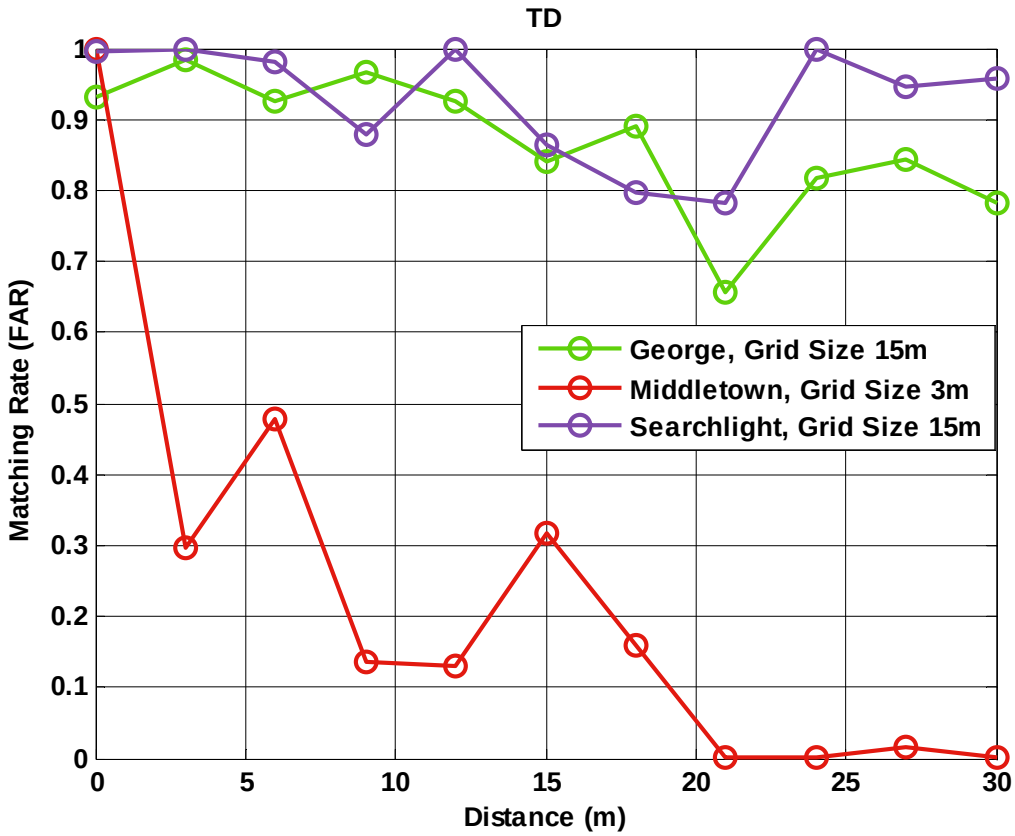
I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

False Accept Rate

- Different Stations

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

Station	SNR (dB)
Fallon	21
George	6
Middletown	32
Searchlight	8

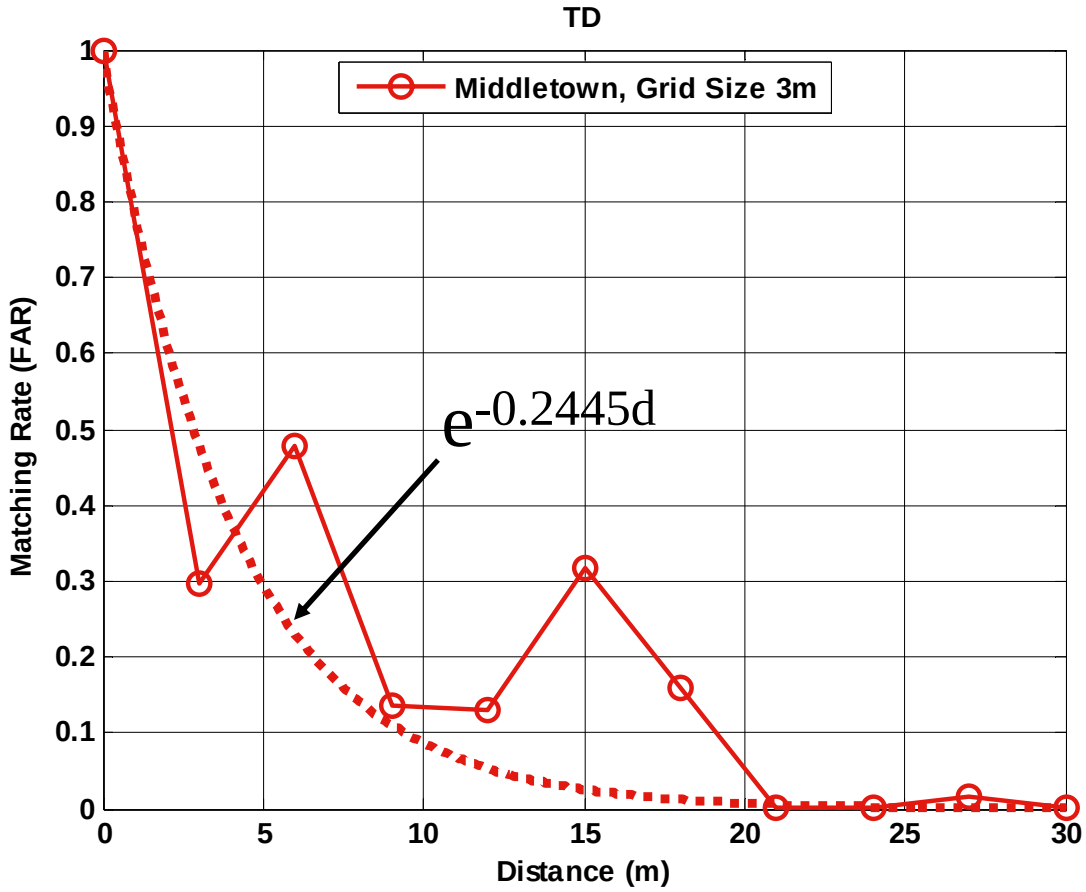


High SNR results in high spatial decorrelation.

Decorrelation Distance

FAR < 0.01

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

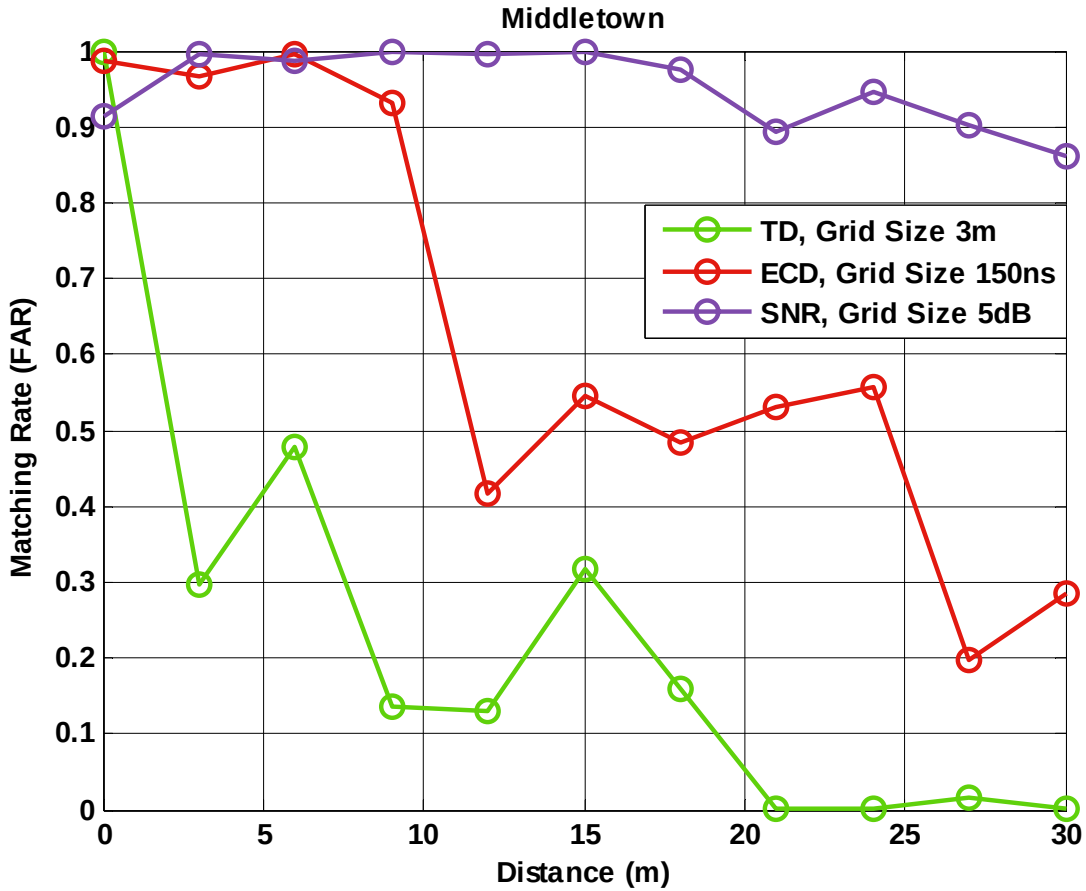


Decorrelation distance is **18** meters for Middletown.

False Accept Rate

- Different Location Parameters

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.



TDOA/TOA > ECD > SNR

Geotag Size

- Information measure
  - Entropy
- Key/Geotag size
  - Station coverage
  - Information density
  - Spatial decorrelation

Parameter	Entropy (bits)
TDOA	15.5
ECD	6.0
SNR	4.3

25.8 bits

Conclusion

- Defeated vulnerabilities of geoencryption protocol and implementation
  - Signal authentication & certified receiver
- Spatial decorrelation of Loran location parameters
  - Geotag size from Middletown is 26 bits
  - At least 2^{26} trials of different locations to break it
- How to increase geotag size?
  - Look into more parameters
  - Fuzzy extractor

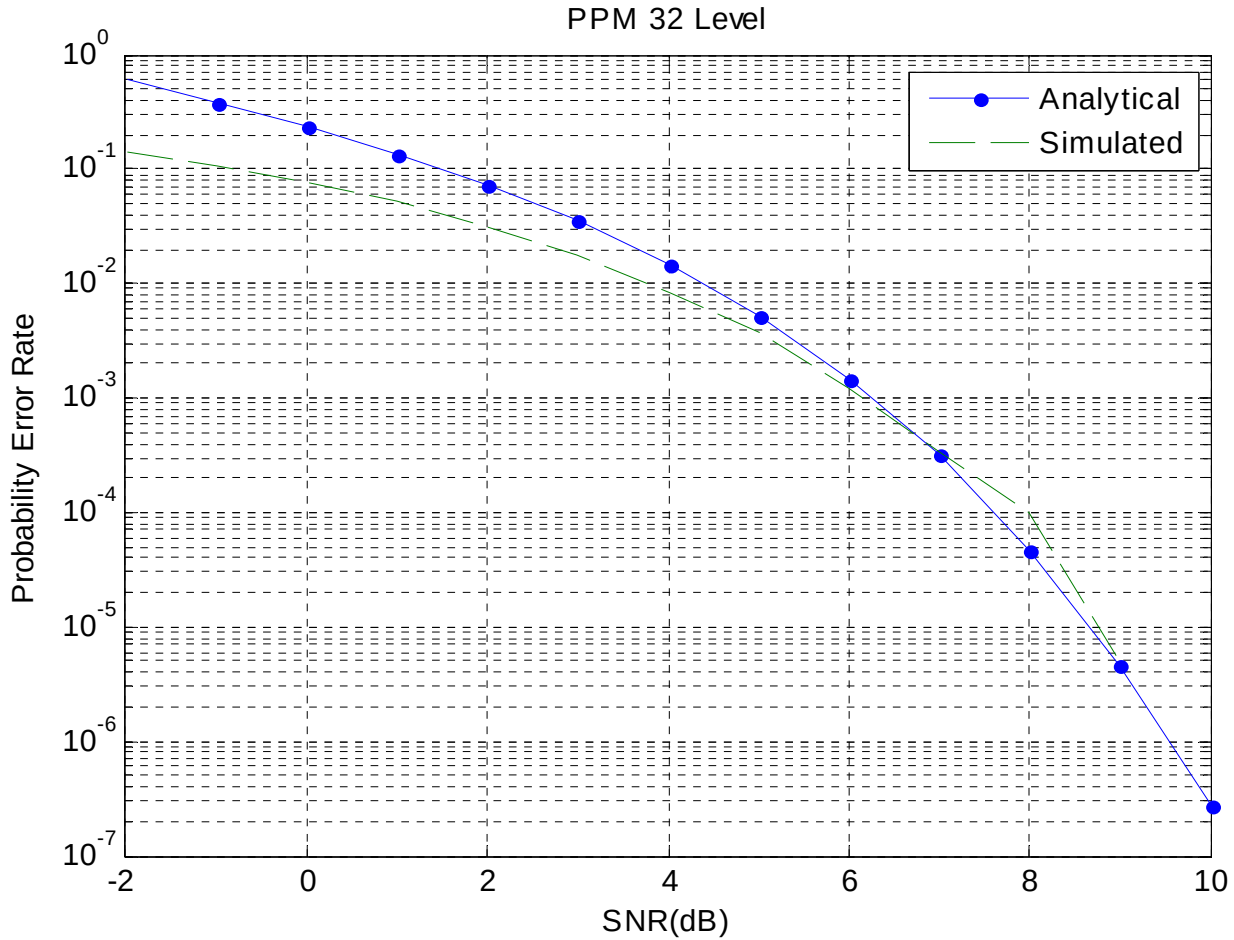
Acknowledgement

The authors would like to thank Ben Peterson, Kirk Montgomery, Jim Shima and USCG for their help during the research.

Backup Slides

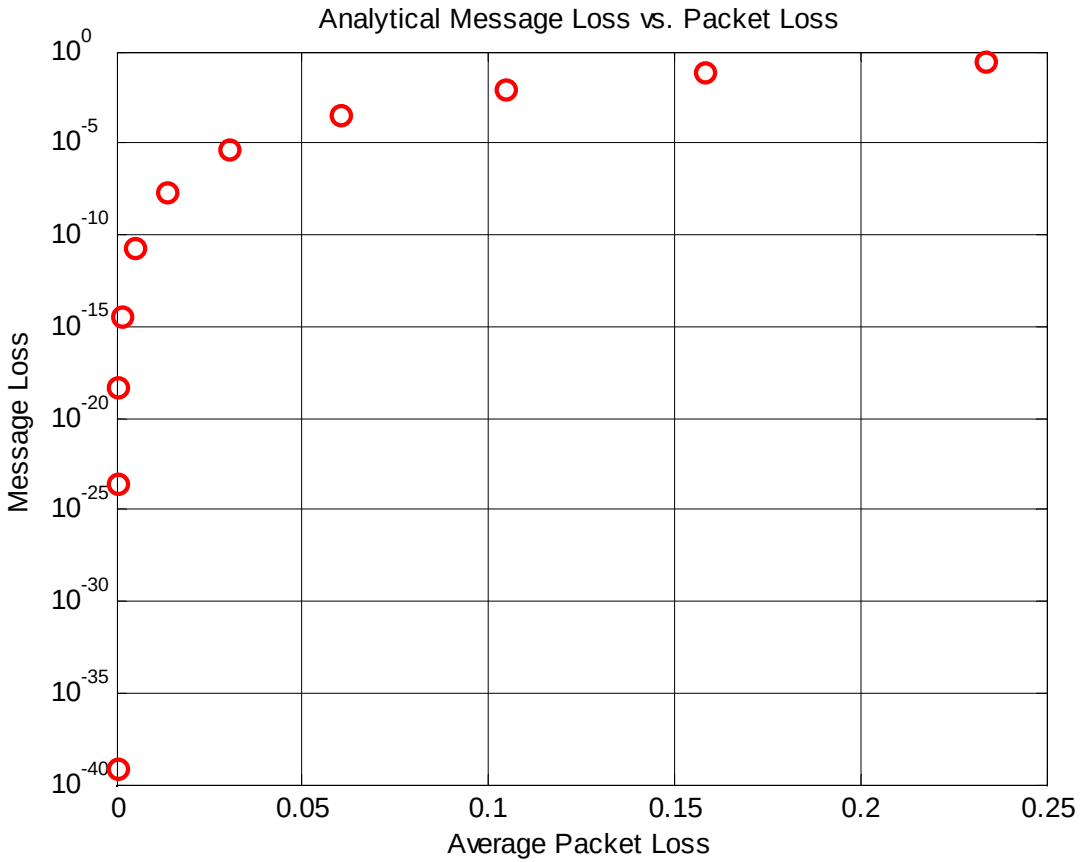
Demodulation Performance

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.



Message Loss

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

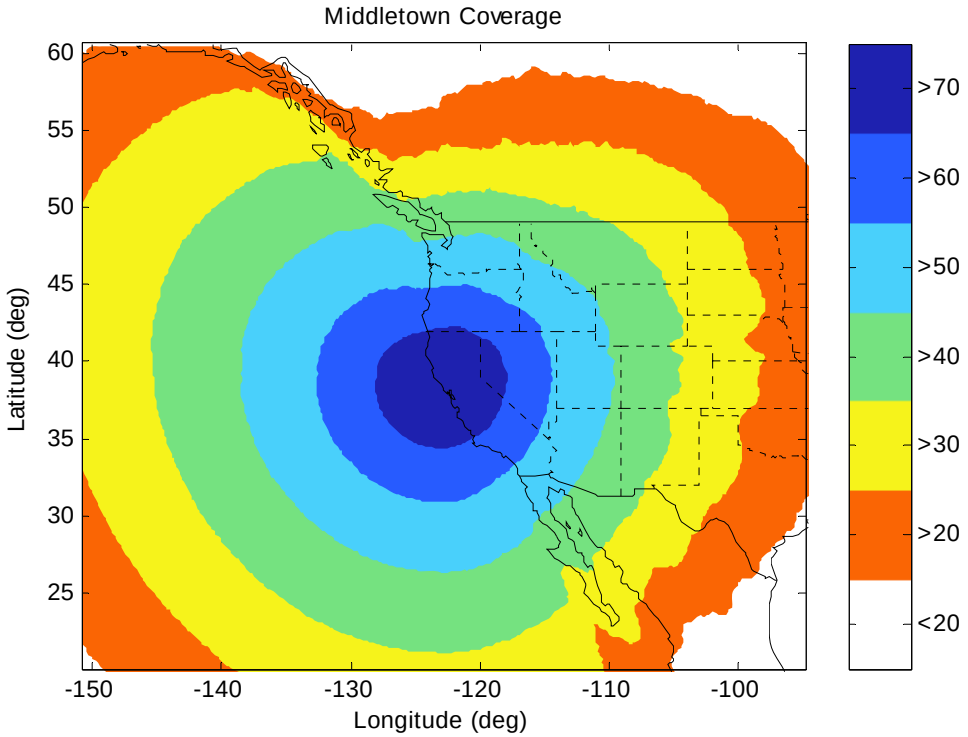


$$\Pr(error / decorder\_failure) = \sum_{j=t+1}^{n} \binom{n}{j} p^{j} (1-p)^{n-j}$$

Authentication Performance

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

SNR



Bandwidth

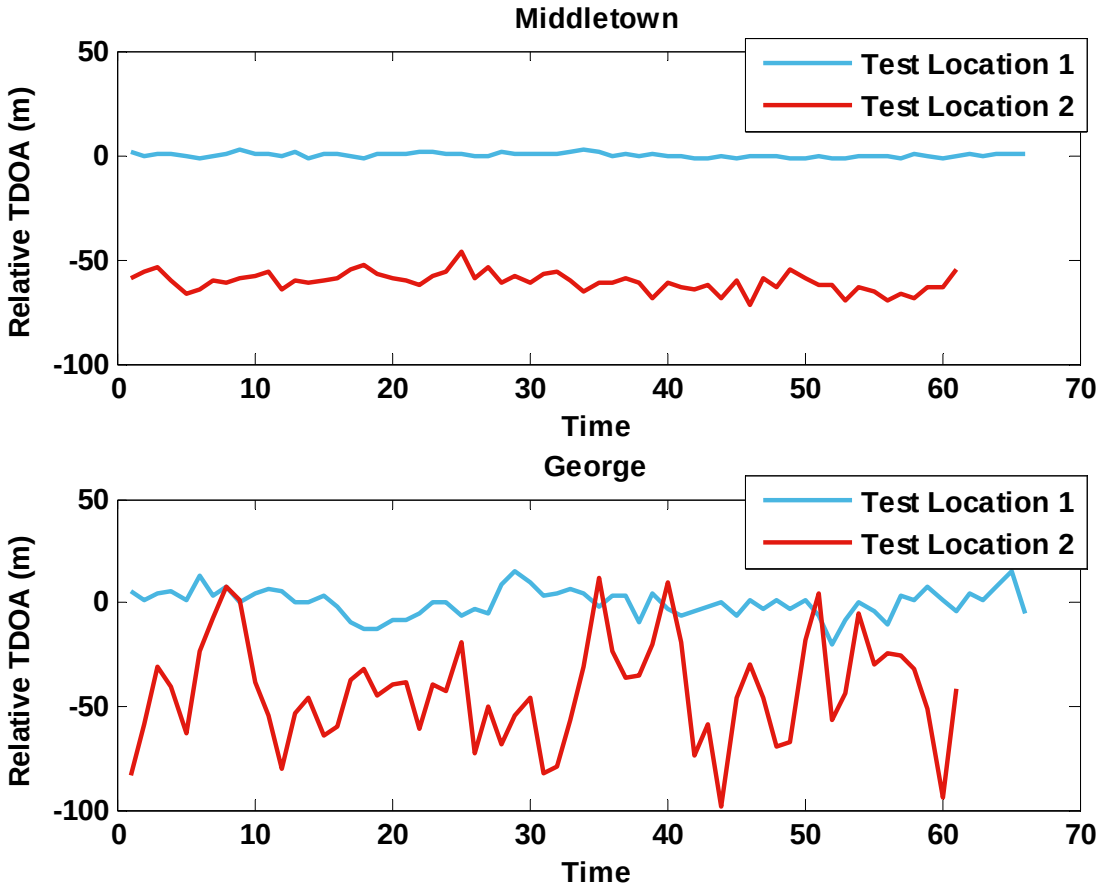
TESLA Segment
- Data
- Authentication (320 bits)

320/37 → 9 Loran messages
50% BW → 18 Loran messages

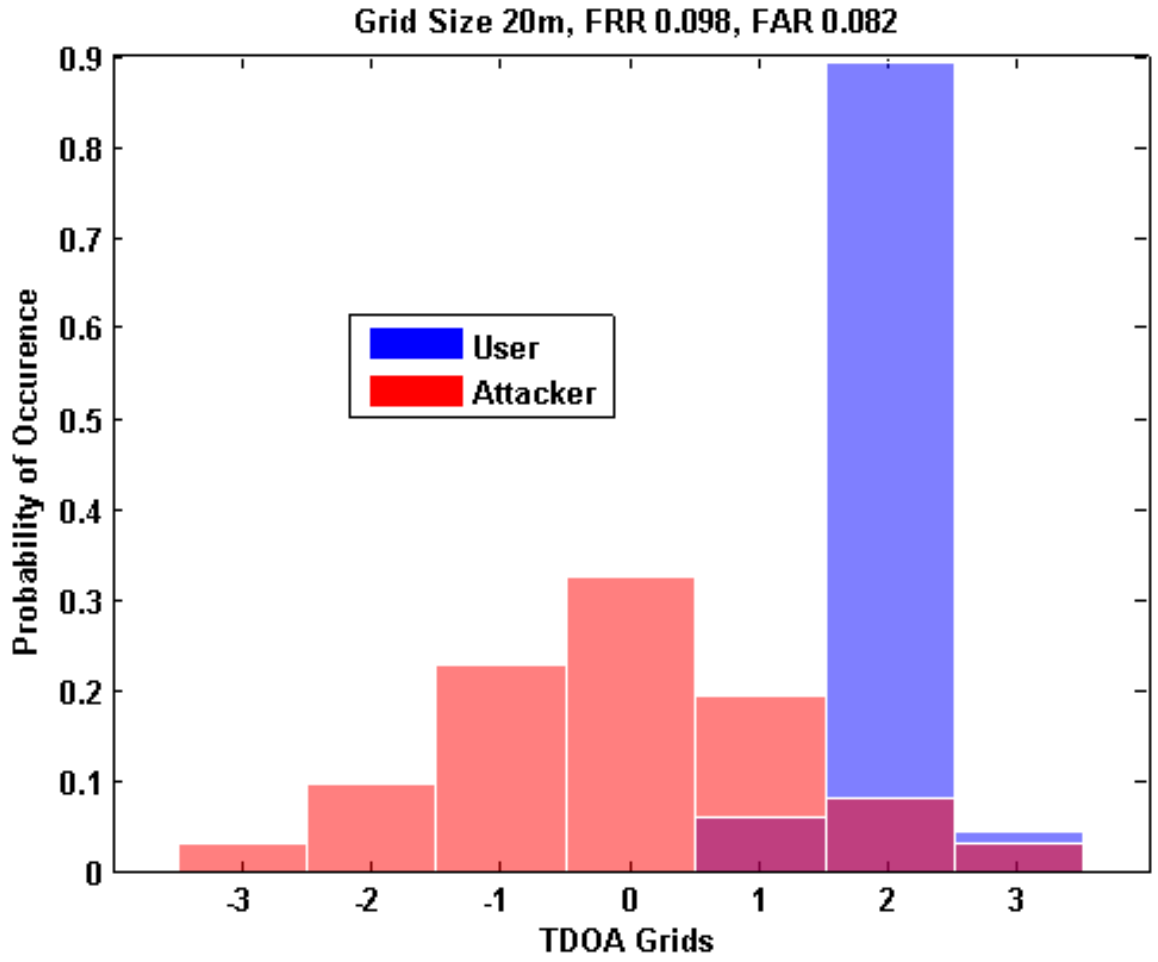
Authentication probability is proportional to SNR & BW.

TDOA Data

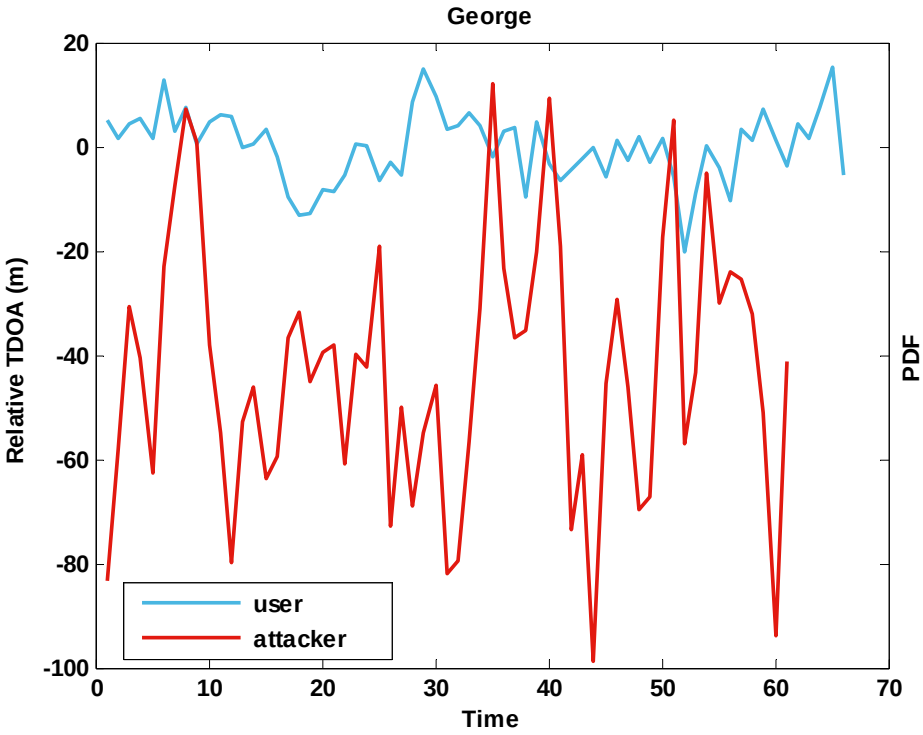
I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.

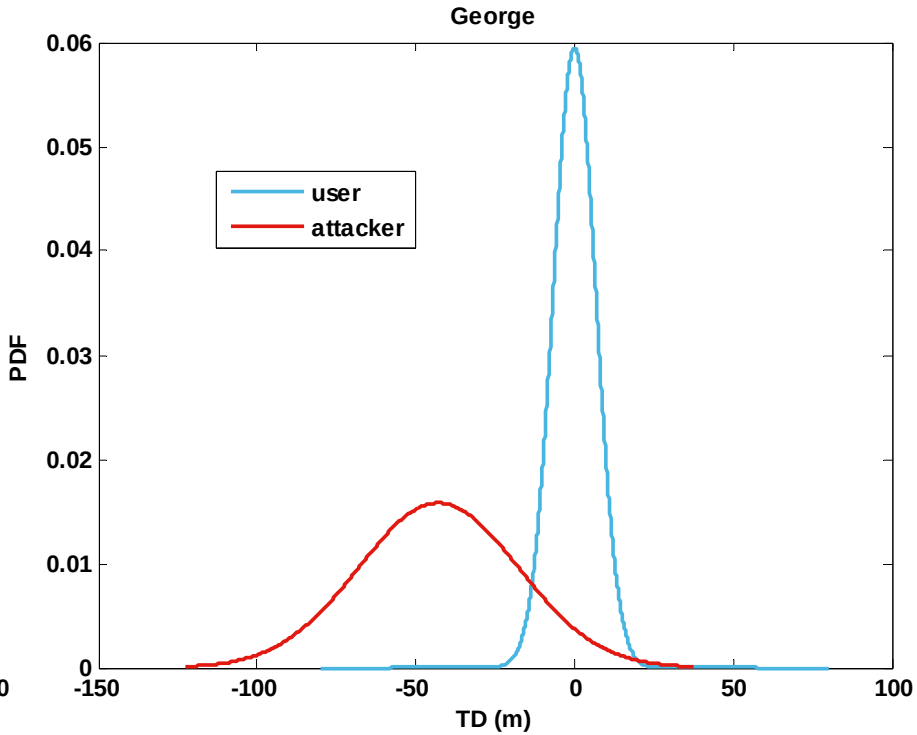


Distribution of Quantized TDOA
- Grid Size 20m, Station George

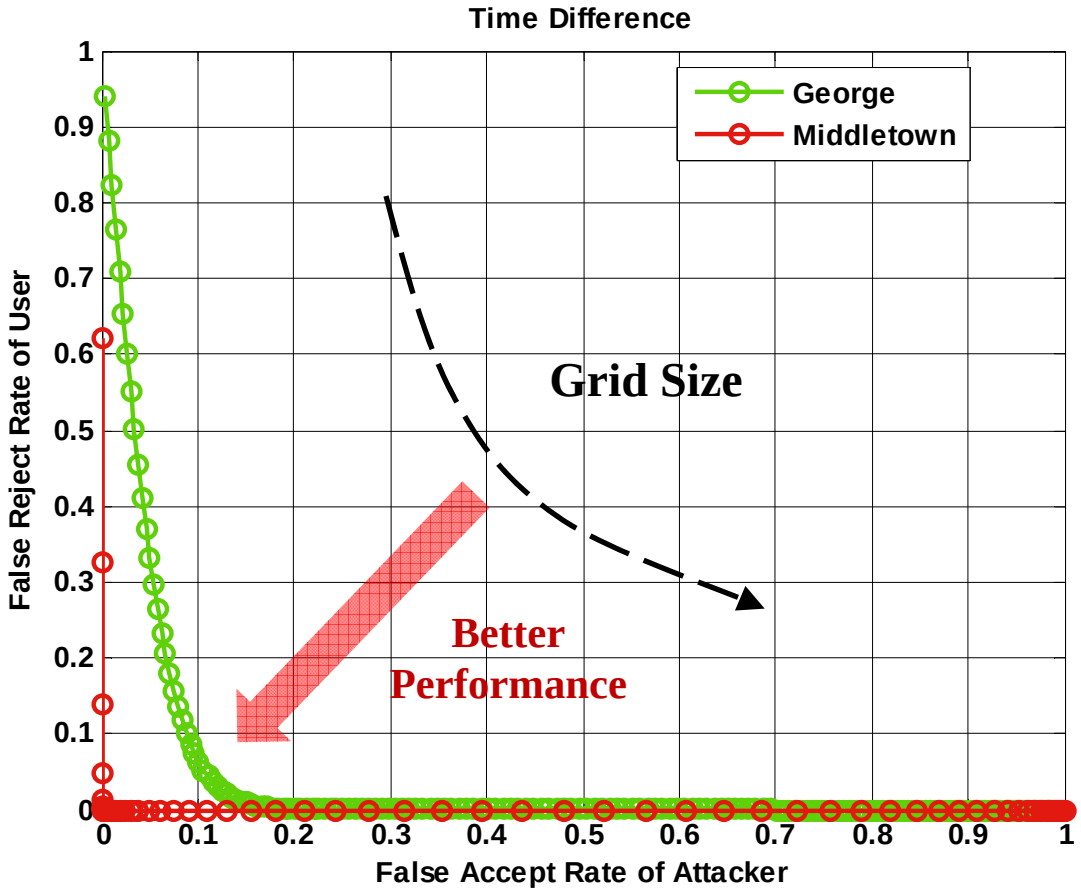


PDF


George
Relative TDOA (m)
Time
user
attacker
20
0
-20
-40
-60
-80
-100
0
10
20
30
40
50
60
70

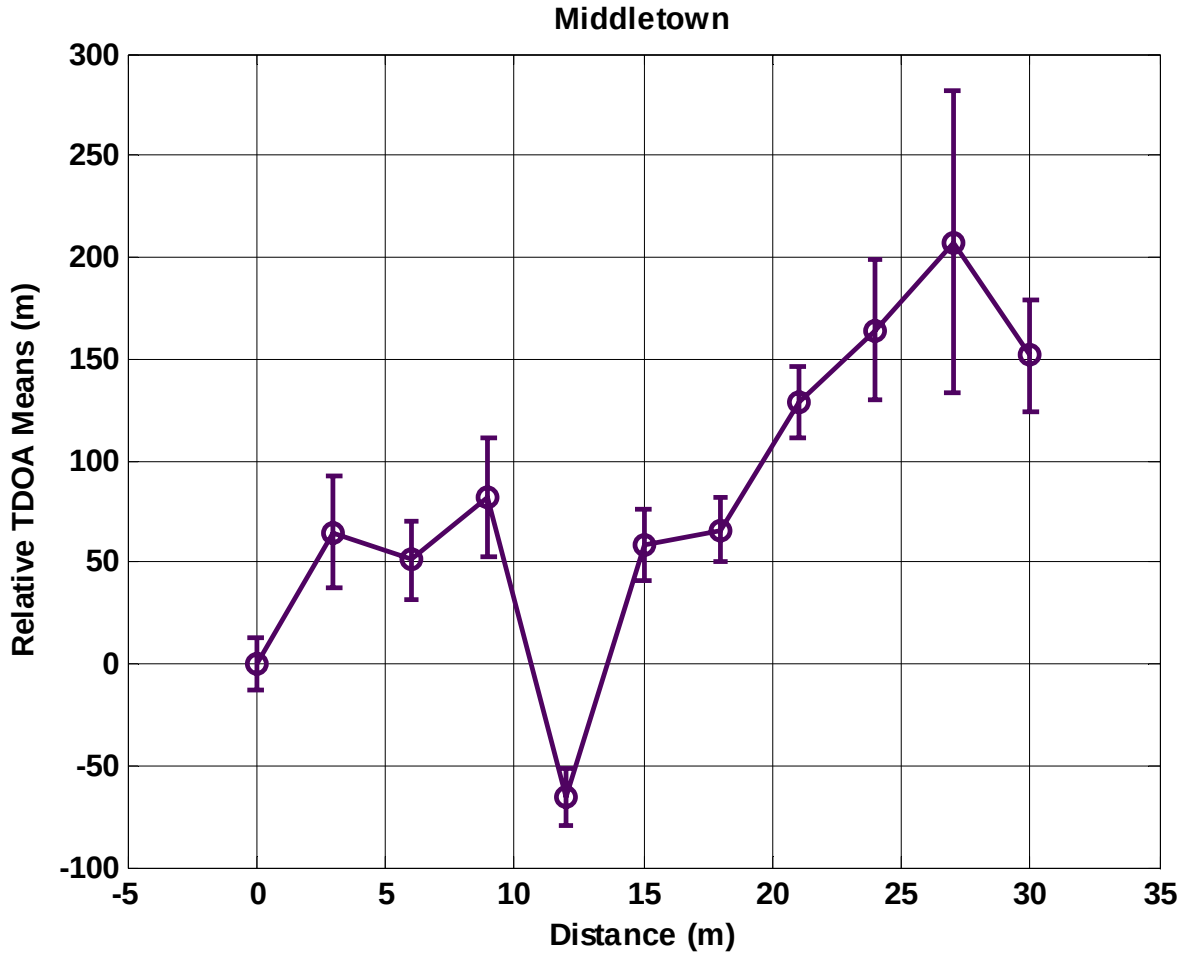

George
PDF
TD (m)
user
attacker
0.06
0.05
0.04
0.03
0.02
0.01
0
-150
-100
-50
0
50
100

Receiver Operating Curve



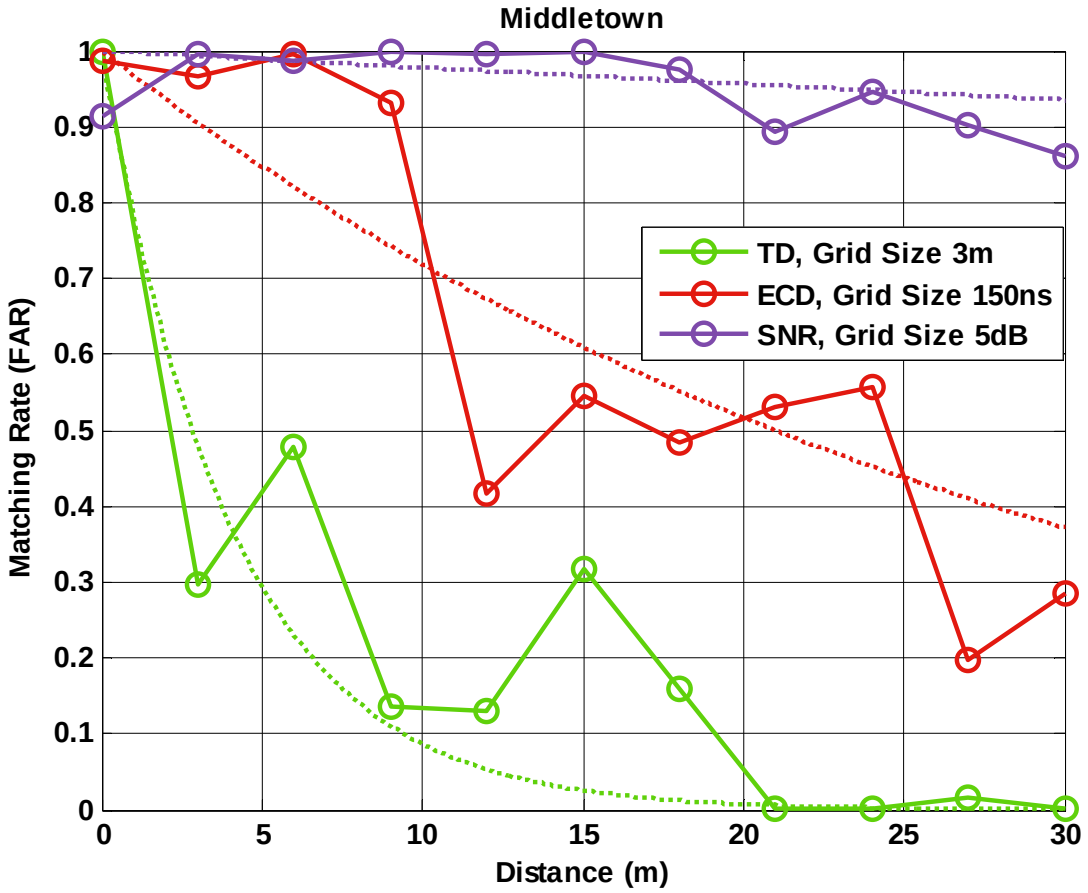
TDOA Measurements

I. Spoof
II. Replay
III. Parking lot
IV. Spatial decorr.



Decorrelation Distances

- Different Parameters



Relative Entropies