Design and Performance Analysis of Location-Based Security System

by Di Qiu
Department of Aeronautics and Astronautics
Stanford University
qiudi@stanford.edu

Sponsored by FAA Loran Program CRDA 2000-G-028

Security Threats in Information Age

The New York Times

November 29 2007

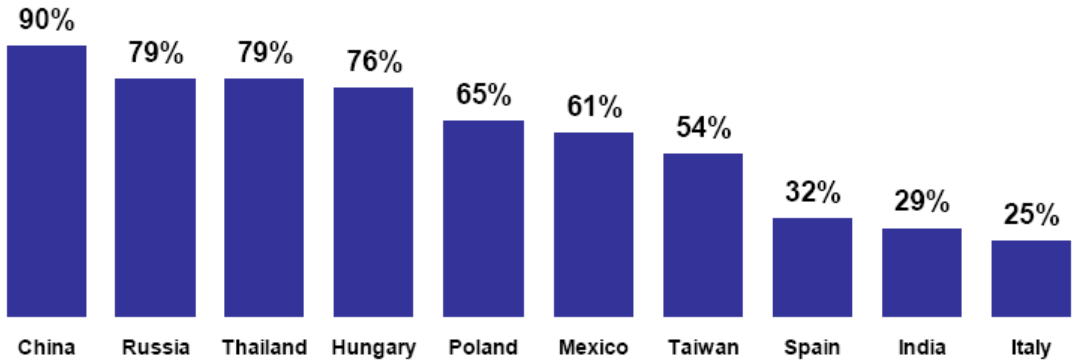
U.K. government's lost data 'worth billions to criminals'

U.K. Prime Minister Gordon Brown "profoundly regrets" the loss of 25 million child benefit records. In what is being called the "worst data disaster

- Data on 25 million / 60 million citizens
- $ 500 million loss
- Prime Minister Brown issued a public apology

More Threats

- Movie piracy
  - $ 6.1 billion in 2005
  - 62% from piracy of hard goods; 38% from Internet piracy



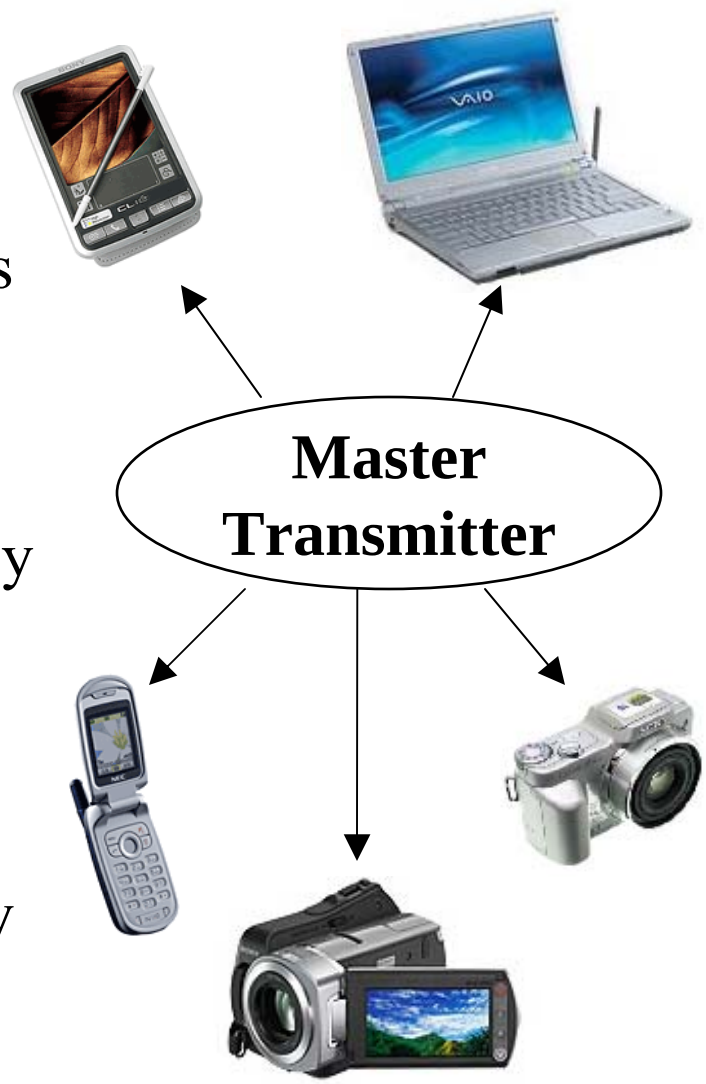
- Loss of electronic devices
  - Qualcomm CEO, Irwin Jacobs, had his laptop stolen off the podium of a hotel conference room in Sep. 2000.
  - Boeing has fired the employee whose laptop was stolen.

More Security from Location

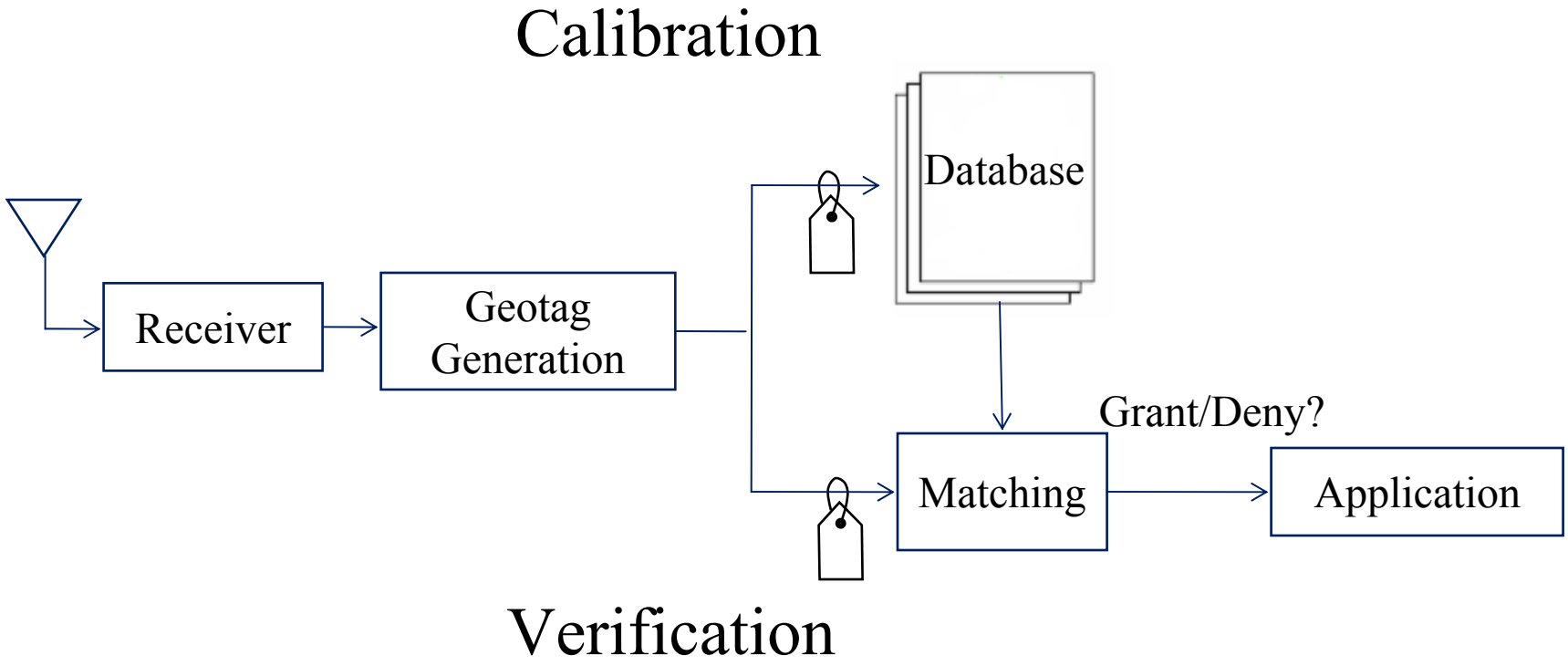
- Location for security?
- Encryption: 
  - hello world → □□□□□□□□□□"v□Z□&j
  - "Only the secrecy of the key provides security."
- Authentication
  - Source verification
  - Passwords, smart ID, biometrics

Applications

- Digital Manners Policy (DMP)
  - Microsoft pending patent
  - Remotely control electronic devices
- Data access control
  - Location validation
  - Digital film distribution proposed by Logan Scott and Dorothy Denning
- Geo-fencing
  - Ericsson and Intel
  - Anti-theft PC protection technology
  - Available by the second half of 2009

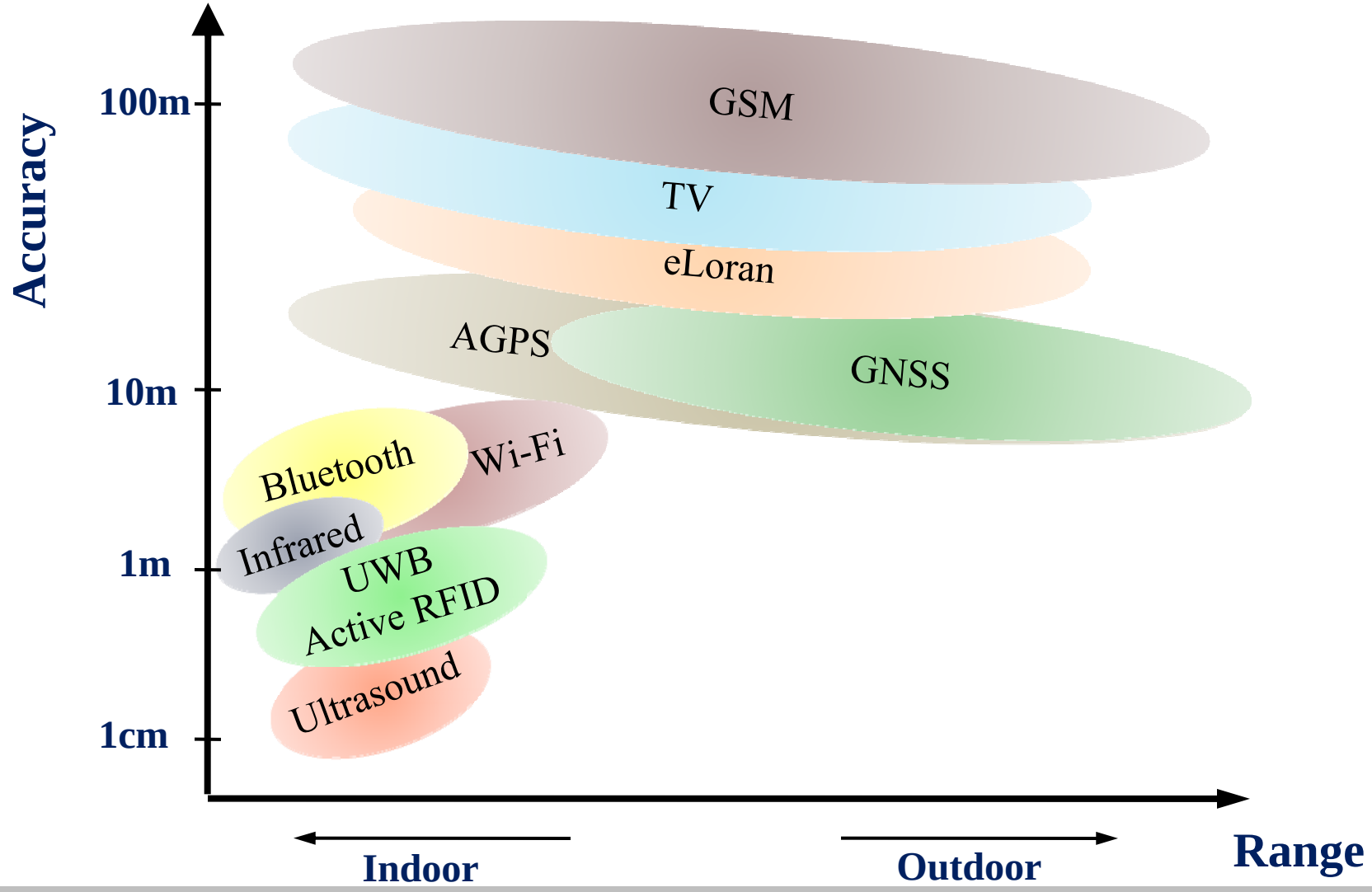


Data Access Control



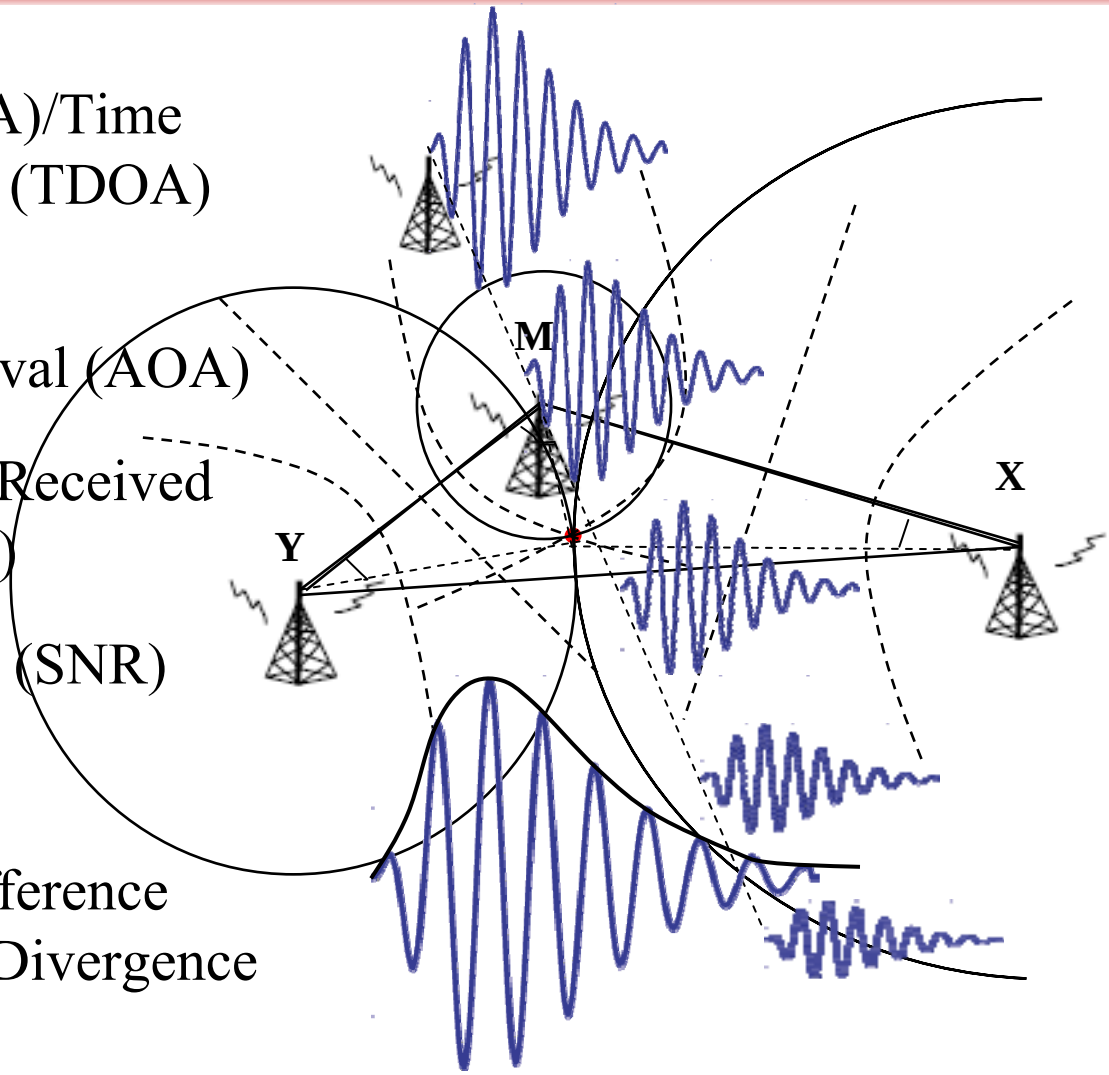
Reproducible geotag

Sensor Types

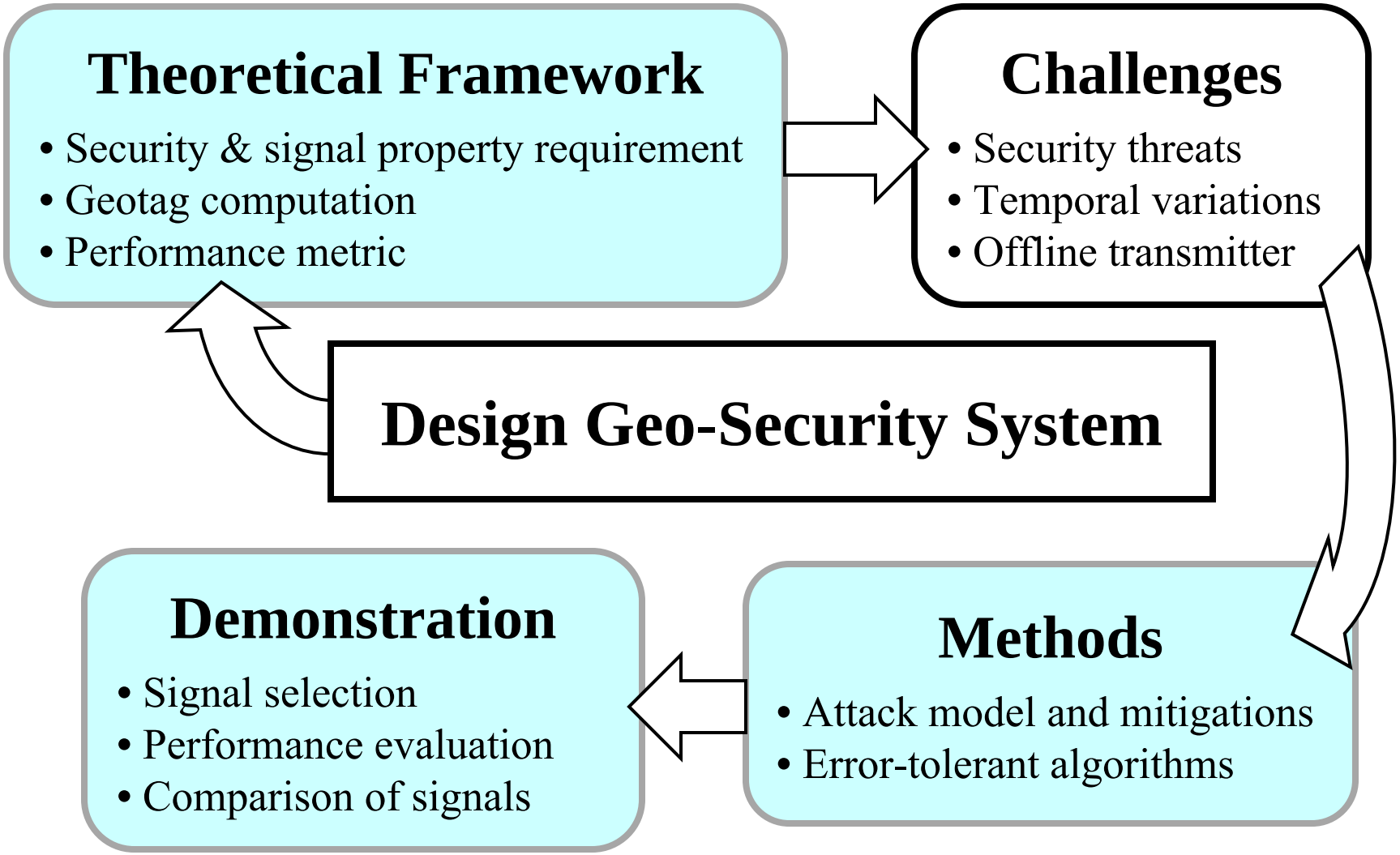


Location-Based Parameters

- Time of Arrival (TOA)/Time Difference of Arrival (TDOA)
- Direction of Arrival (DOA)/Angle of Arrival (AOA)
- Signal Strength (SS)/Received Signal Strength (RSS)
- Signal to Noise Ratio (SNR)
- Bit Error Rate (BER)
- Envelope to cycle difference (ECD)/Code Carrier Divergence (CCD)

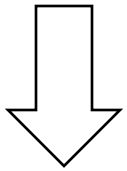


Approaches


Theoretical Framework
• Security & signal property requirement
• Geotag computation
• Performance metric
Challenges
• Security threats
• Temporal variations
• Offline transmitter
Design Geo-Security System
Demonstration
• Signal selection
• Performance evaluation
• Comparison of signals
Methods
• Attack model and mitigations
• Error-tolerant algorithms

Outline

- Theoretical framework
- Loran demonstration – performance
- Wi-Fi demonstration – multiplicity of signals
- Fuzzy extractors – continuity



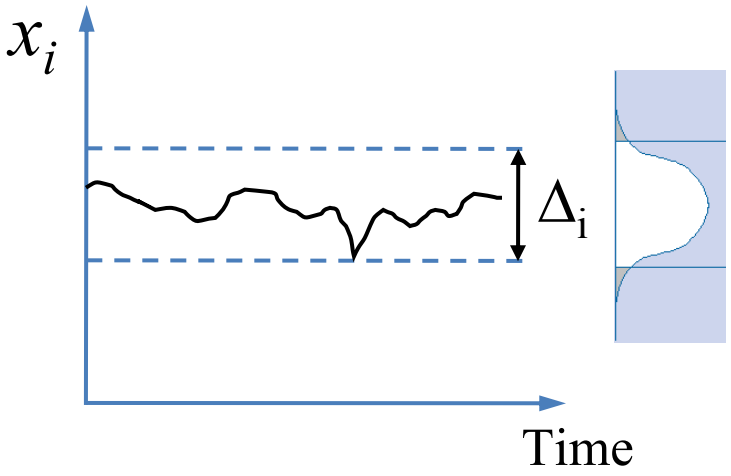
Robust geotag

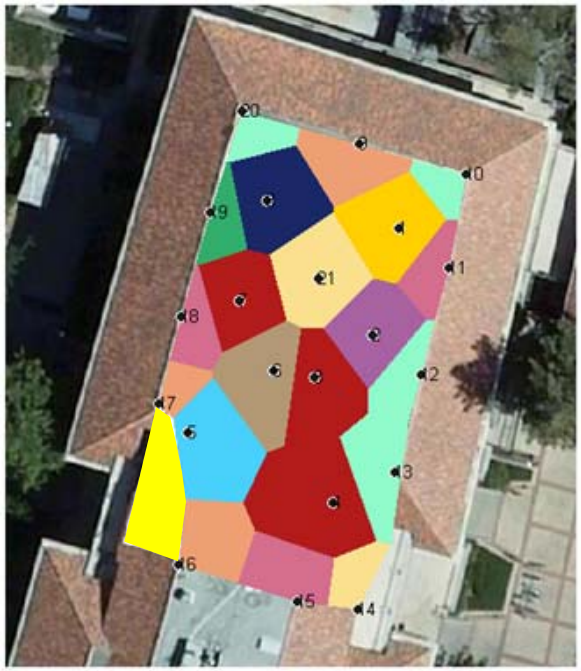
Theoretical Framework Design

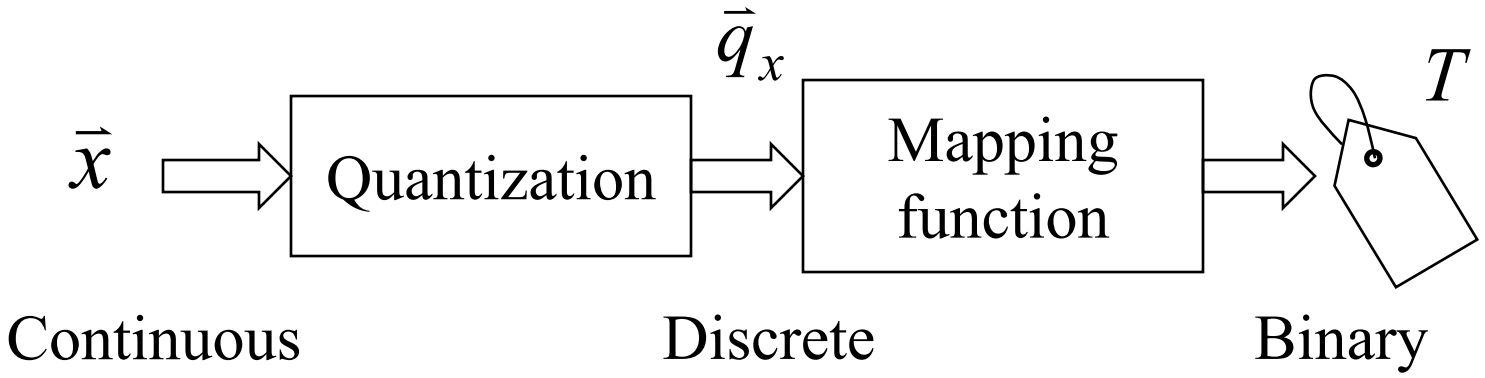
Theoretical Framework

- Basic architecture
  - Geotag generation
  - Attack model and attack mitigations
- Performance analysis
  - Consistency measure
  - Spatial decorrelation measure
  - Tradeoff

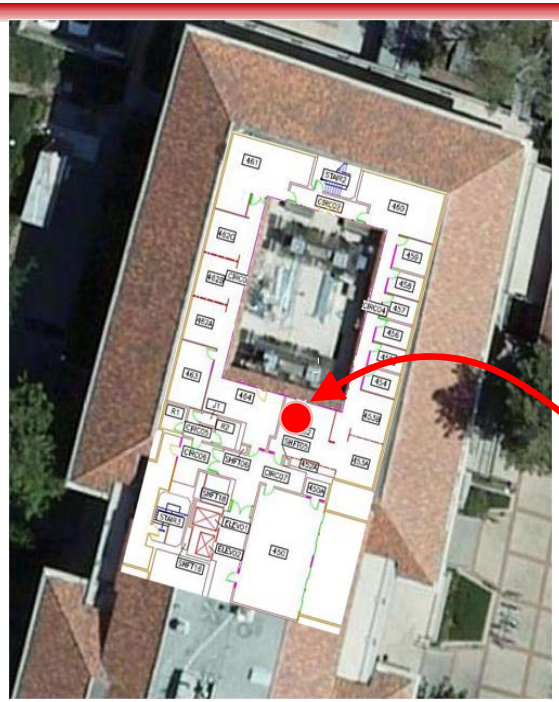
Geotag Generation







Attack Model

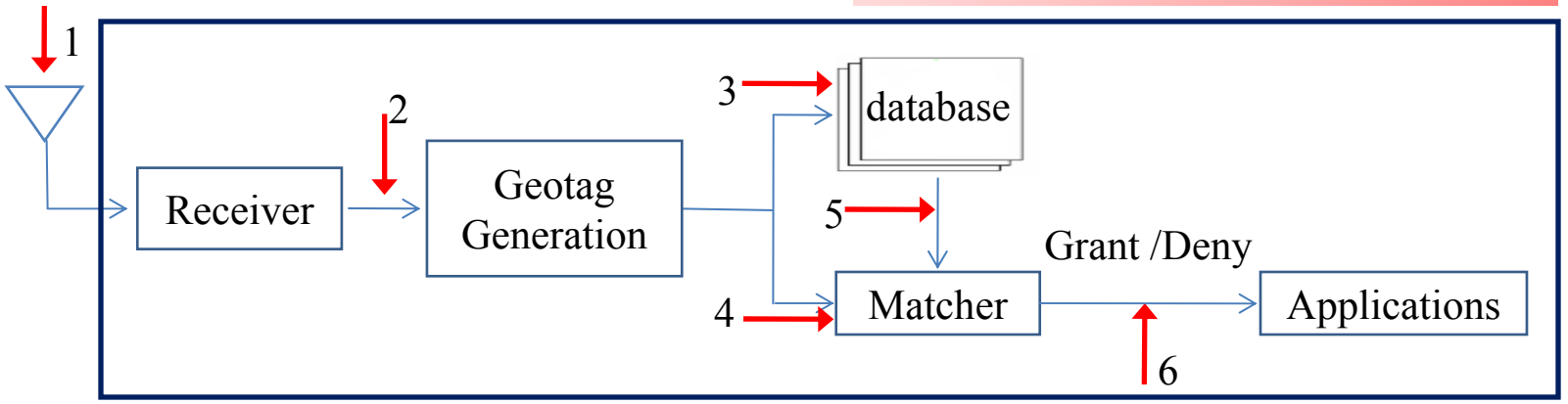


Assumptions

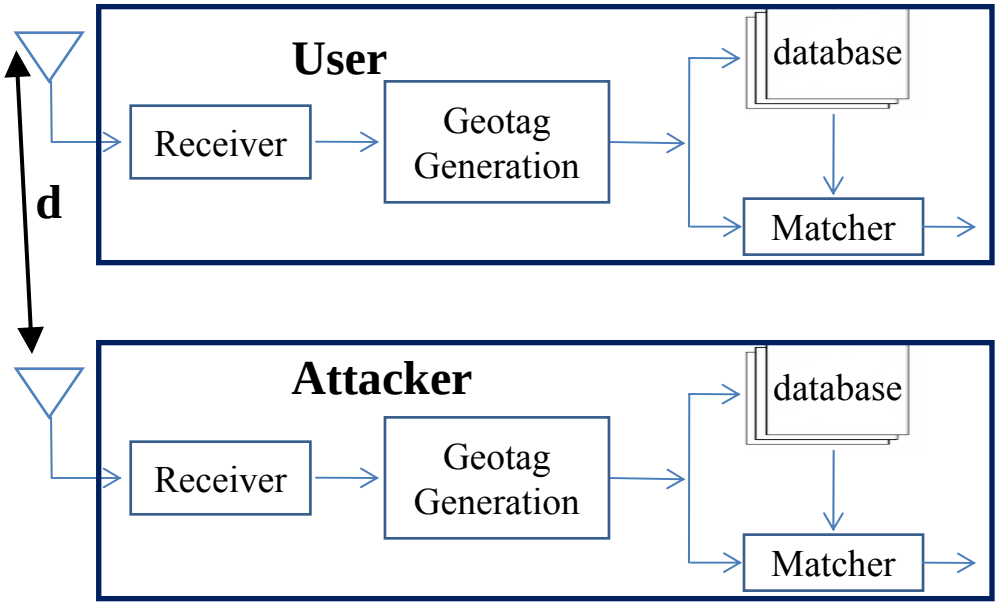
- Tamper resistant device
- Self-authenticated signal
  - Authenticate source
  - TESLA on Loran

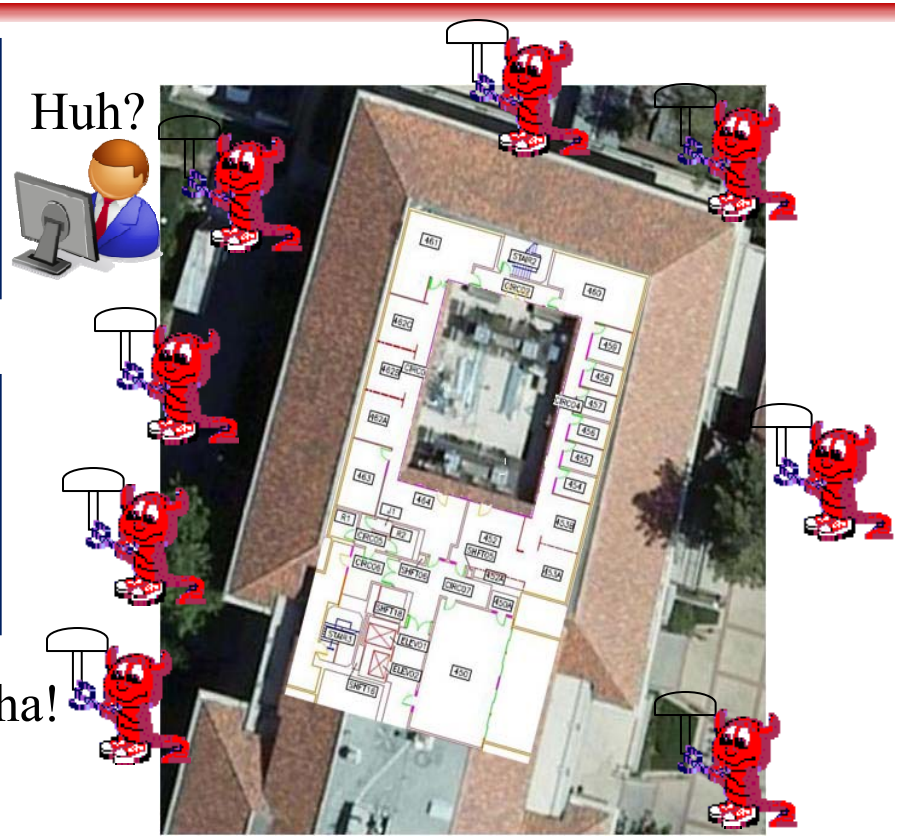
Types of Attacks

~~Spoofing~~ Trial and error



Trial and Error – "Parking Lot Attack"

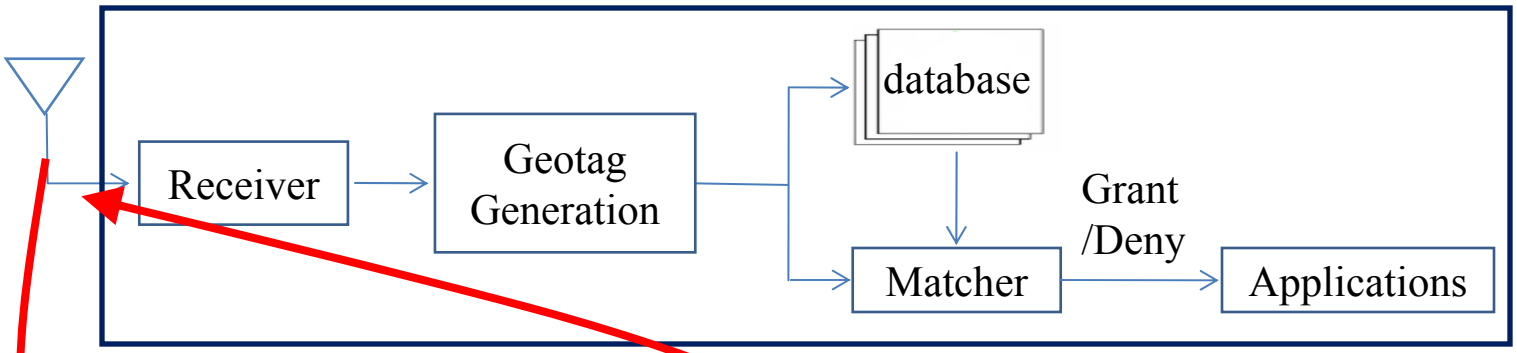


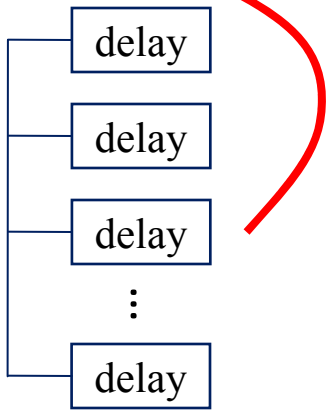


- False Reject Rate (FRR)
  - Fail to recognize user
  - Reproducibility
- False Accept Rate (FAR)
  - Recognize attacker instead
  - Spatial unpredictability

What is the security radius?
- Low FAR
- Spatial decorrelation

Smart Parking Lot Attack - Tampering

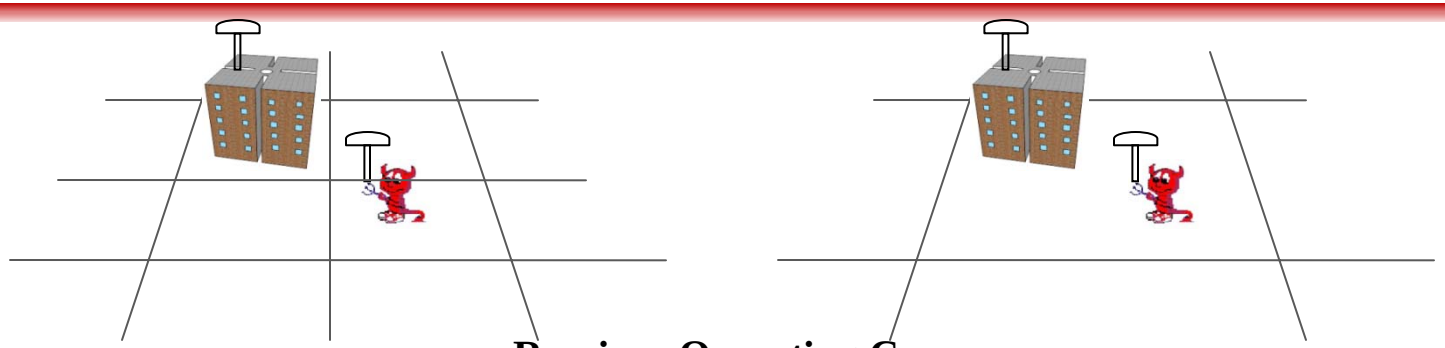


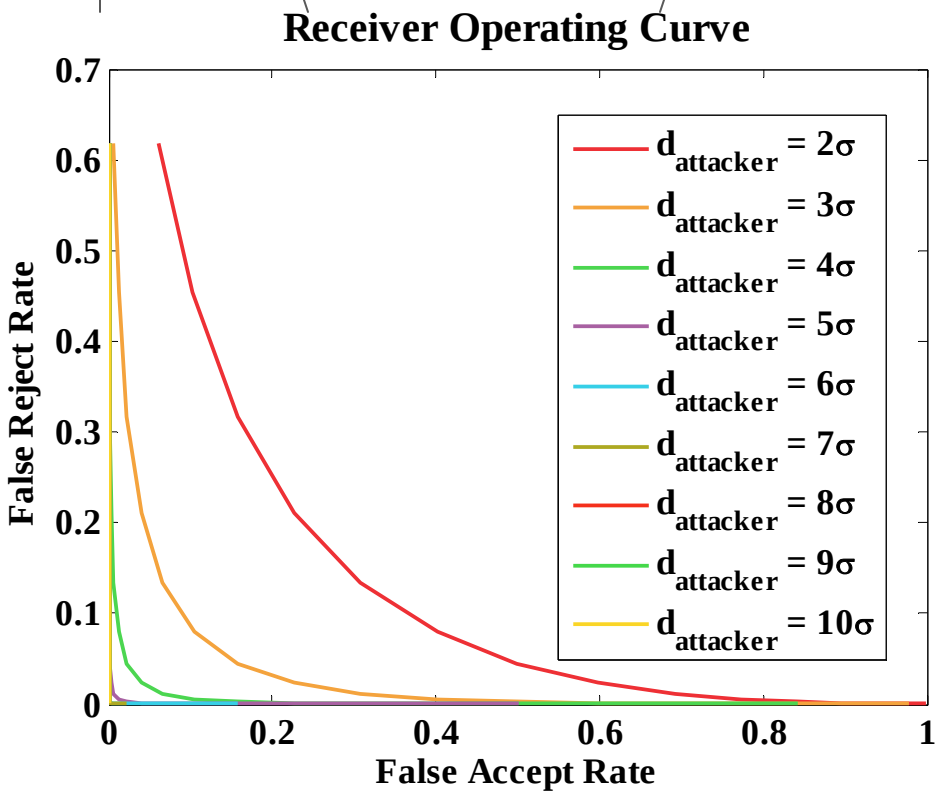


the analog delay device

Search space of parameters is reduced.

Tradeoff between FAR and FRR





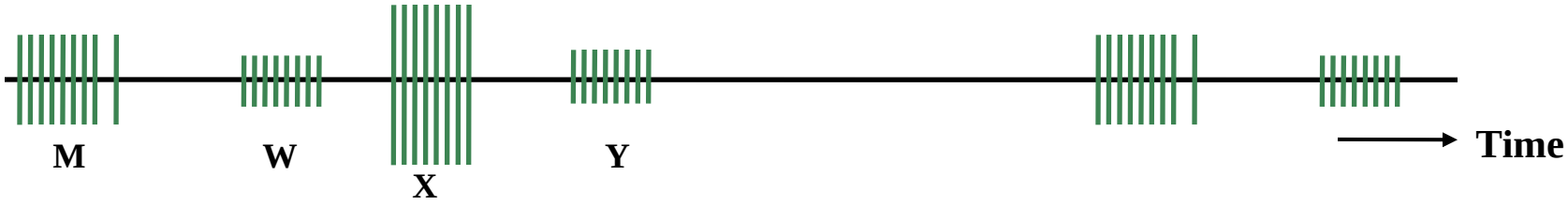
Loran as a Case Study

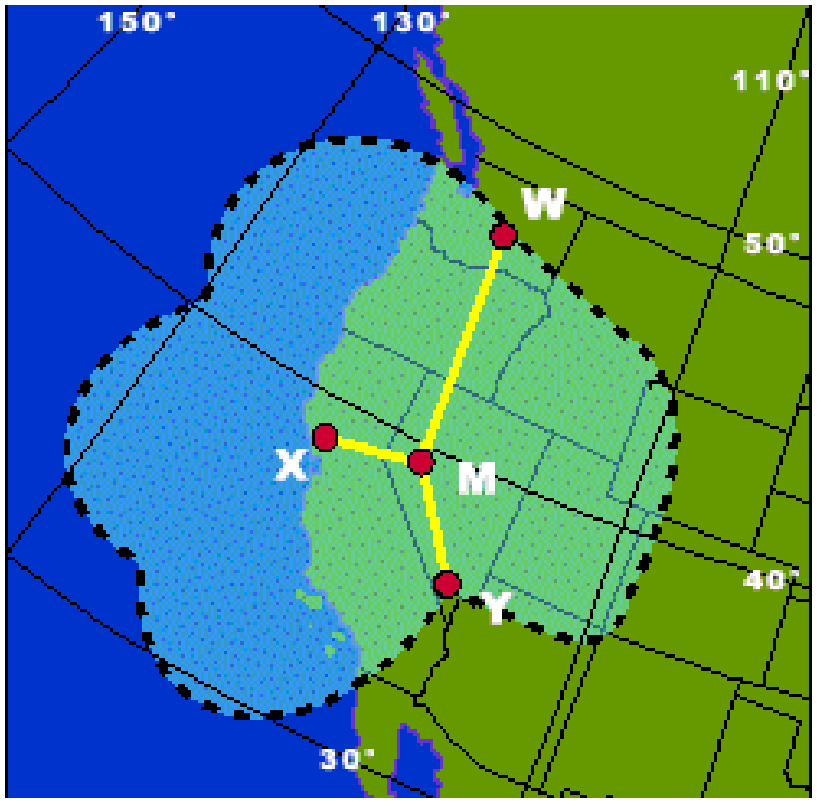
Loran for Geo-Security

Picture courtesy: Megapulse

- Low frequency
- High power: 400 k~1.6 MW
- Hard to jam
- Stationary transmitters
- Repeatable accuracy
- Indoor capable
- eLoran

Loran Basic Architecture





Picture Courtesy: Megapulse

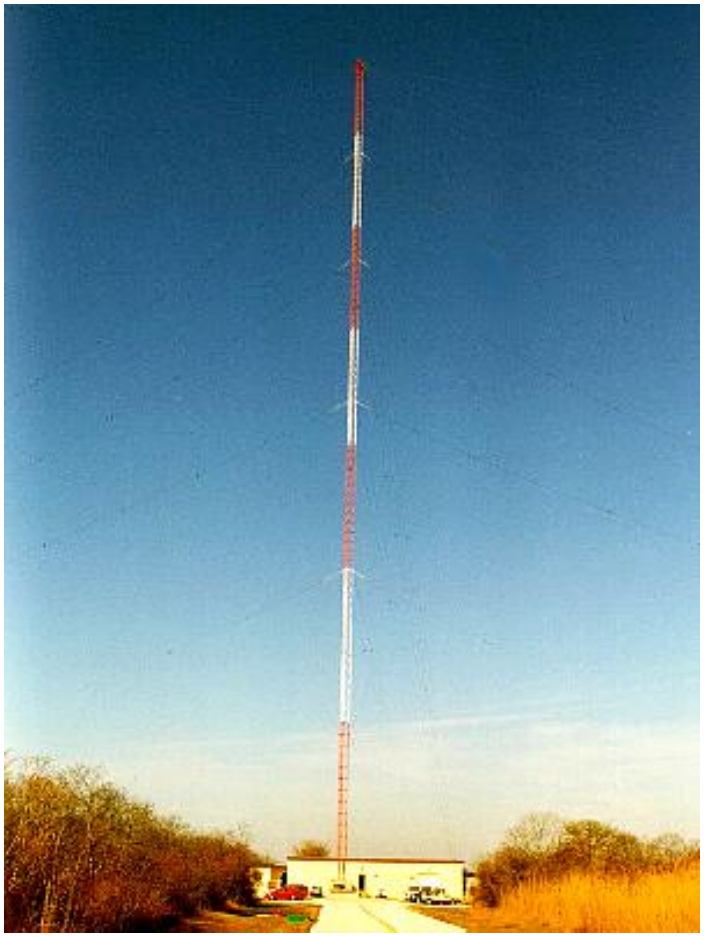
LORAN-C
U.S. WEST COAST CHAIN
GRI 9940

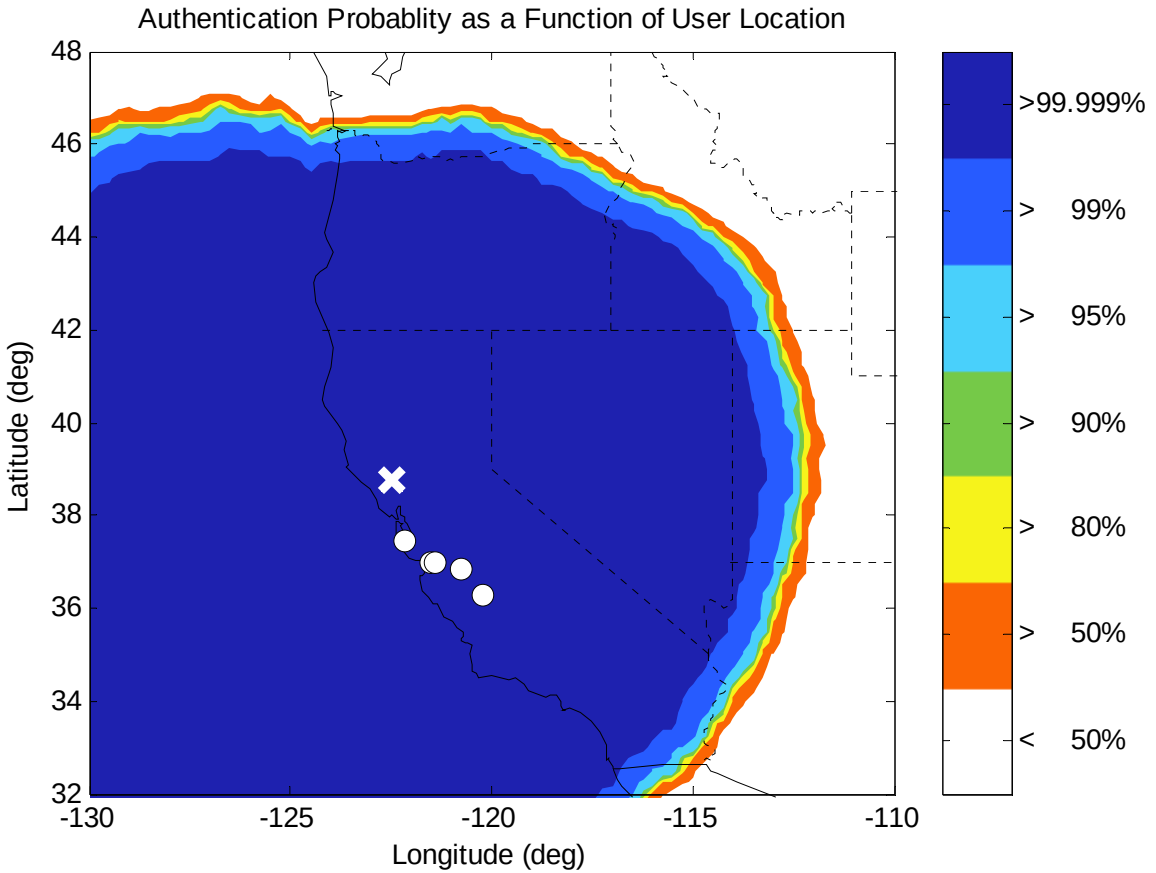
LEGEND

- **Transmitter Station**
- **Approximate Limits of Coverage**

M Fallon
W George
X Middletown
Y Searchlight

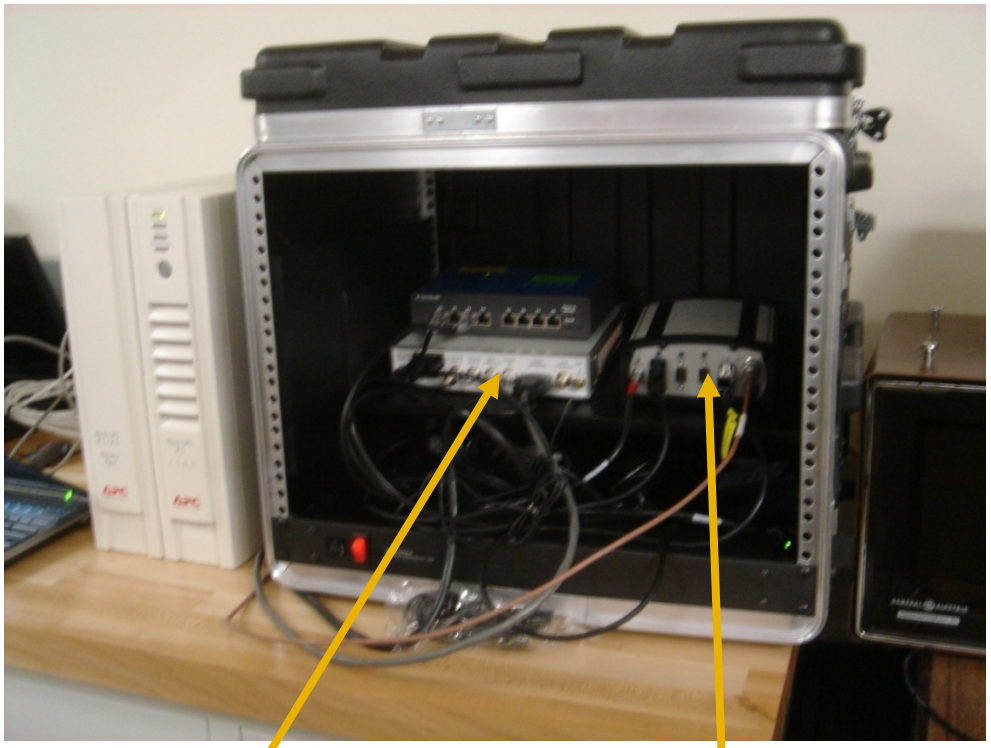
Middletown was Live with Stanford Designed Authentication Scheme





38.4 sec to authenticate the signal source with 50% BW

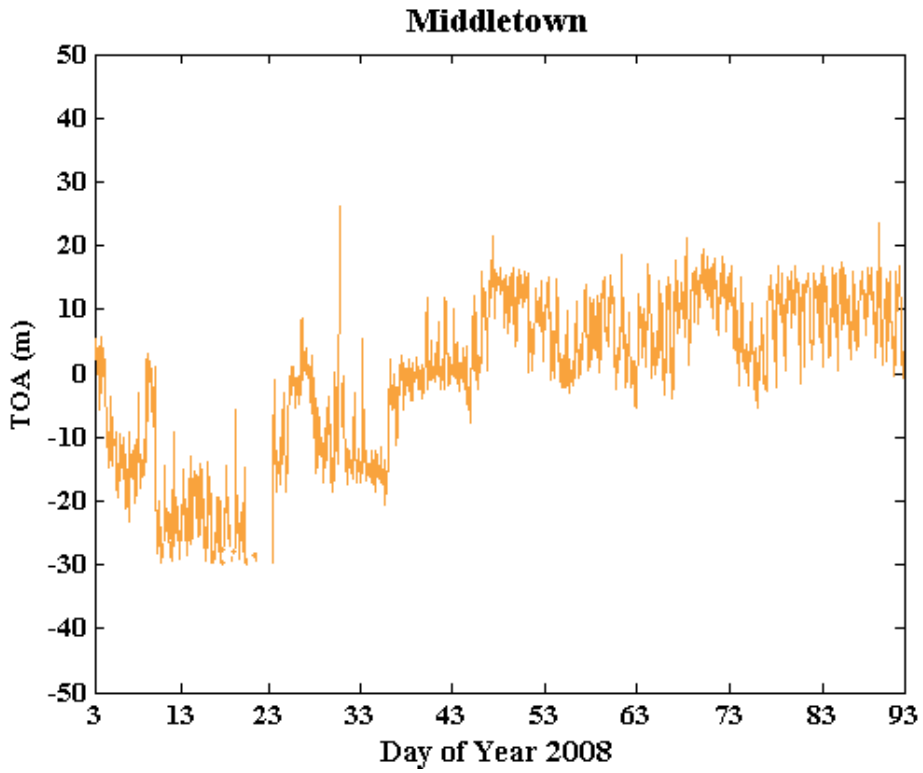
Stanford Seasonal Monitor Station

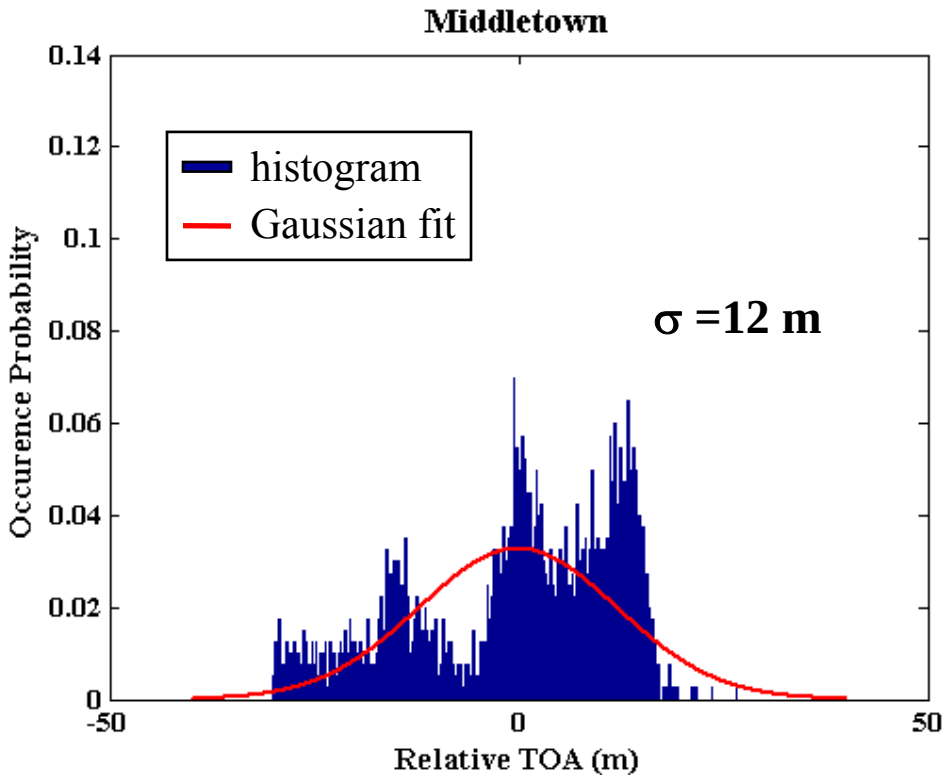


Loran Locus SatMate 1030

NovAtel GPS Receiver

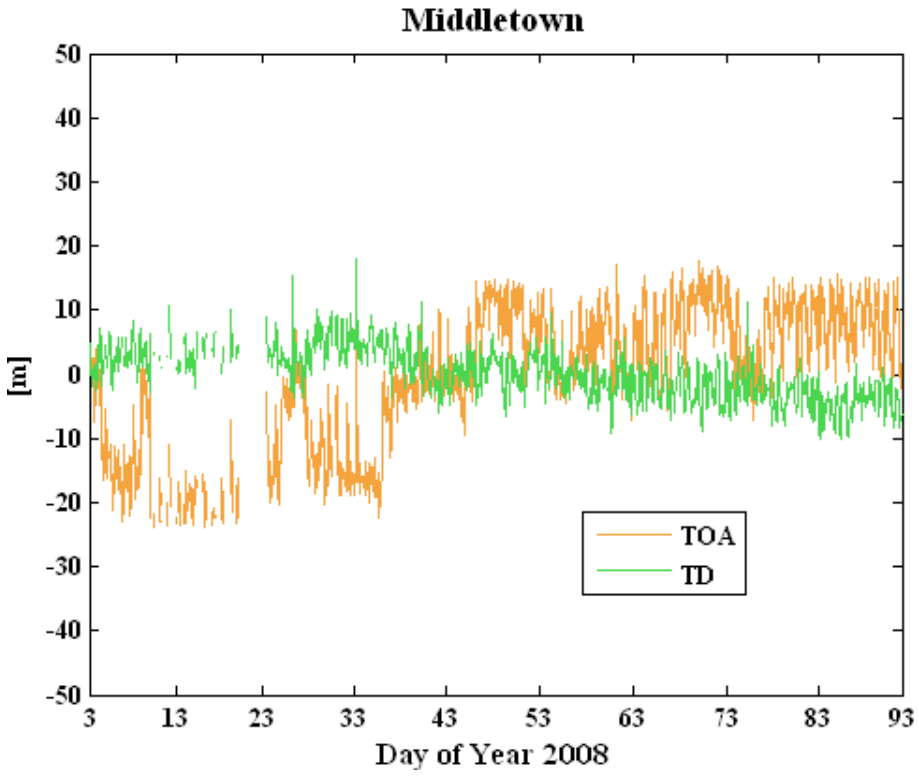
Loran Seasonal Monitor Data

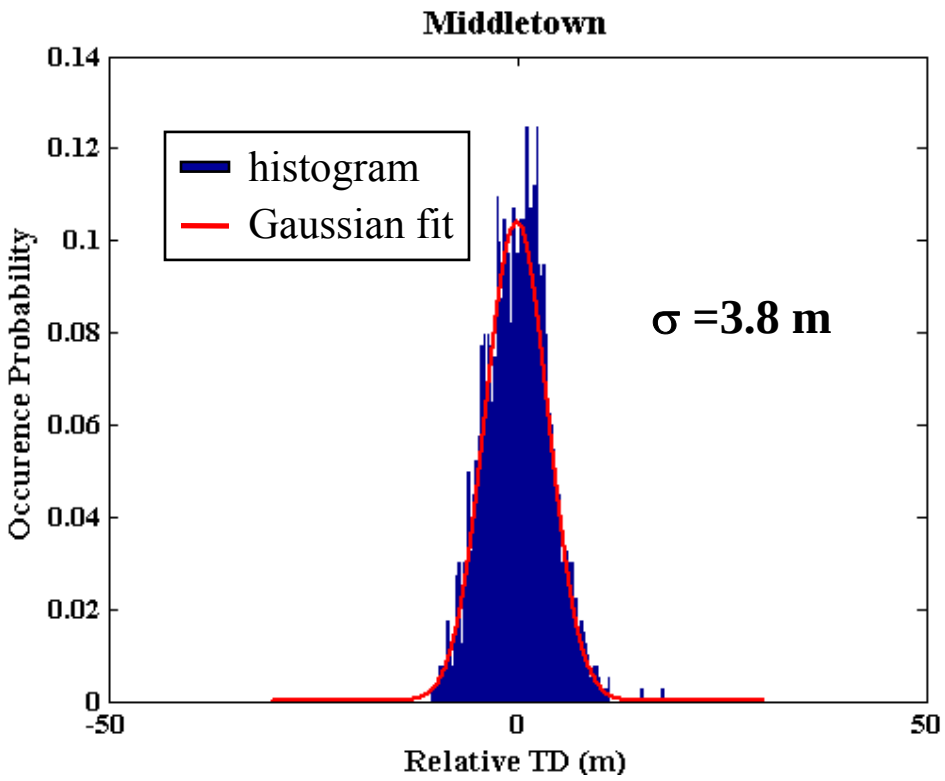




- TOA from Middletown over 90-day period
- Additional secondary factor (ASF)
- TOA is non-Gaussian

ASF Mitigation – Time Difference

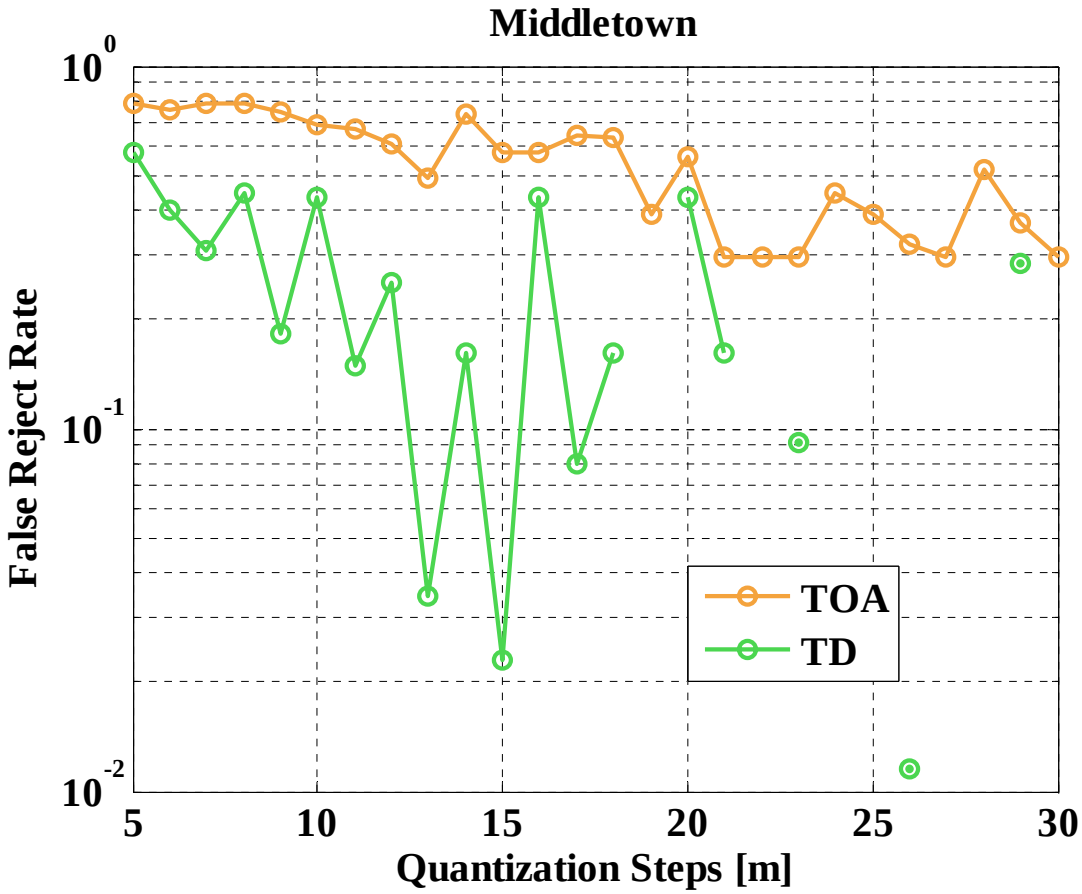




- TD is close to Gaussian after correction
- Spatial decorrelation
- Lose TOA from master station

Reproducibility based on 90-day Data

- Day 1: calibration
- Day 2 ~ 90 (89 days): verification
- Parameter: TOA/TD
- Station: Middletown

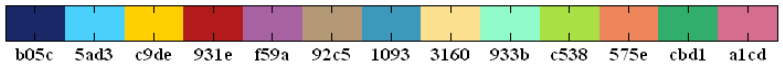


96% FRR improvement for Δ = 15m

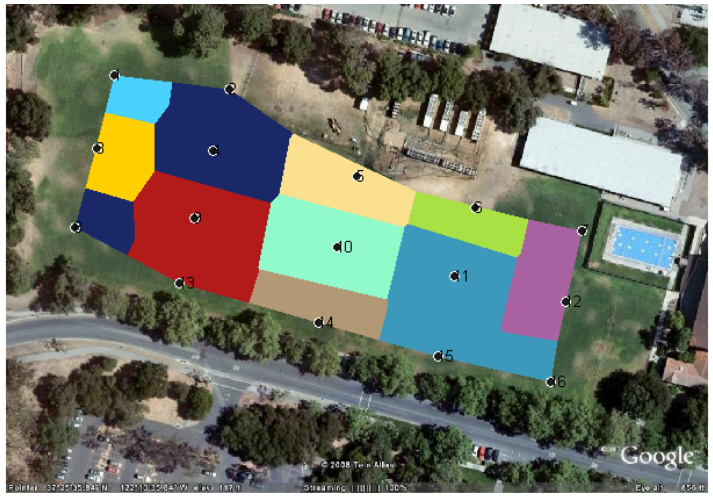
Data Collections for Spatial Decorrelation

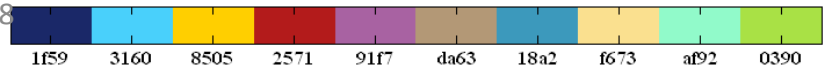
Parking Structure

Geotag Contour Plot

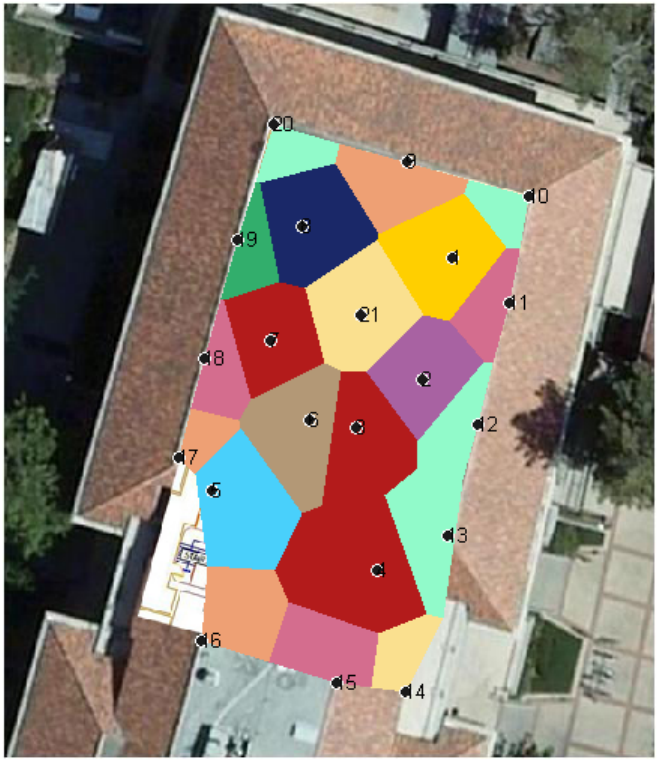


Soccer Field



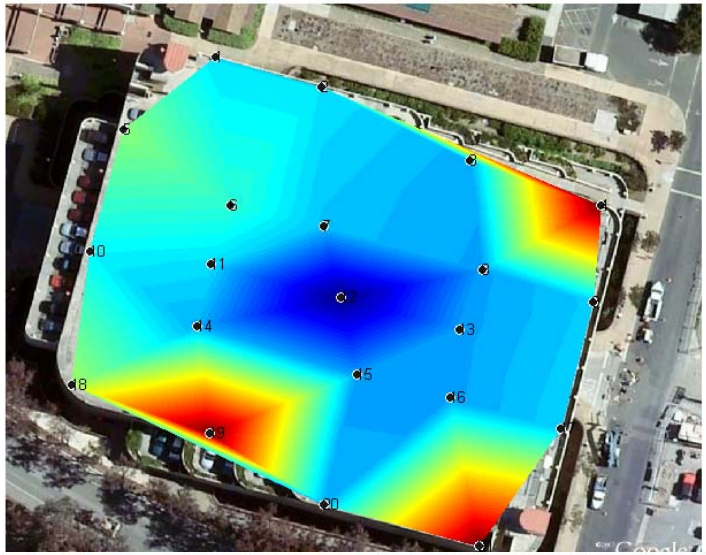


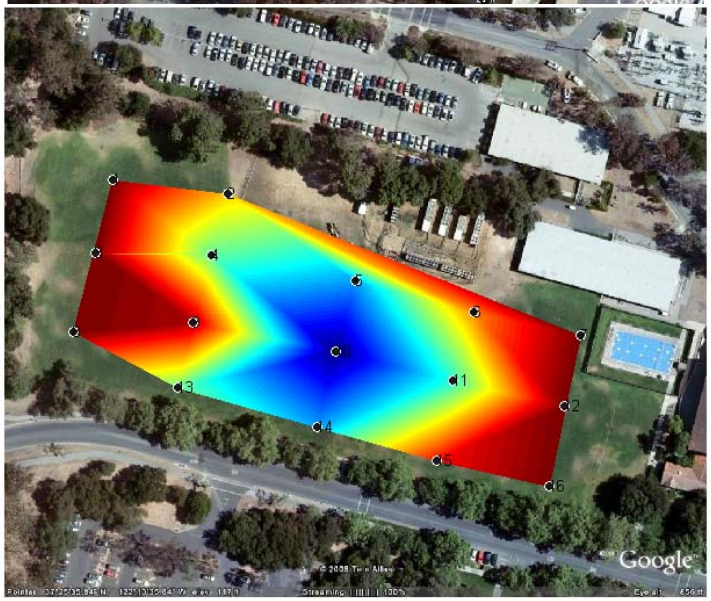
Geotag Contour Plot

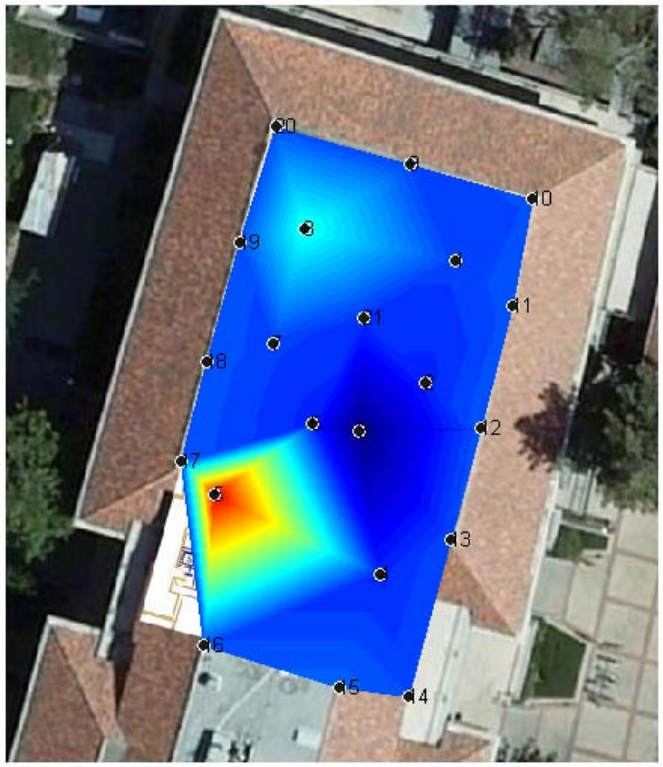


Office Building (Indoor & Outdoor)

Parking Lot Attack – Spatial Decorrelation



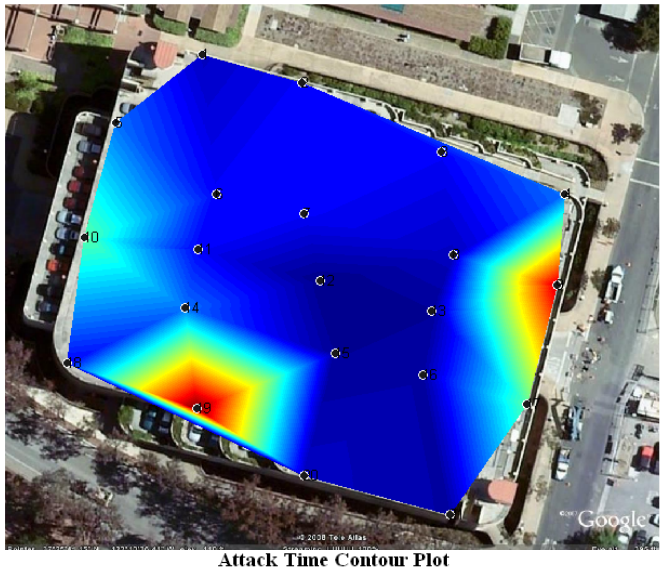




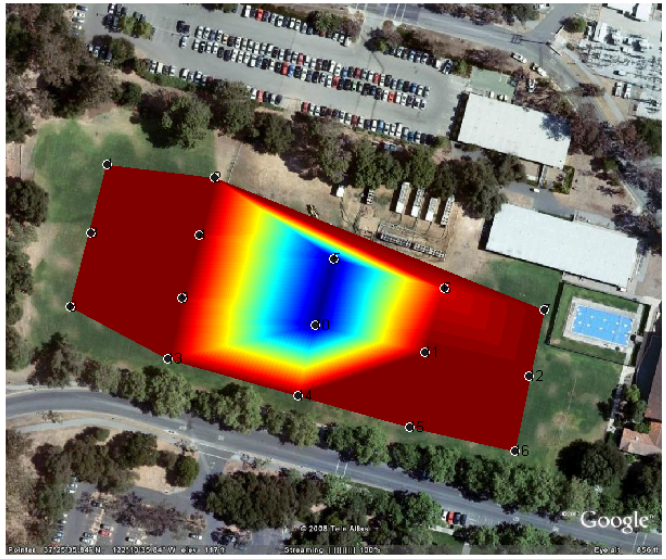
2^{12} => 43 hours
2^{24} => 248 months
2^{36} => 85792 years

Smart Attack – Attack Time Reduction

Attack Time Contour Plot

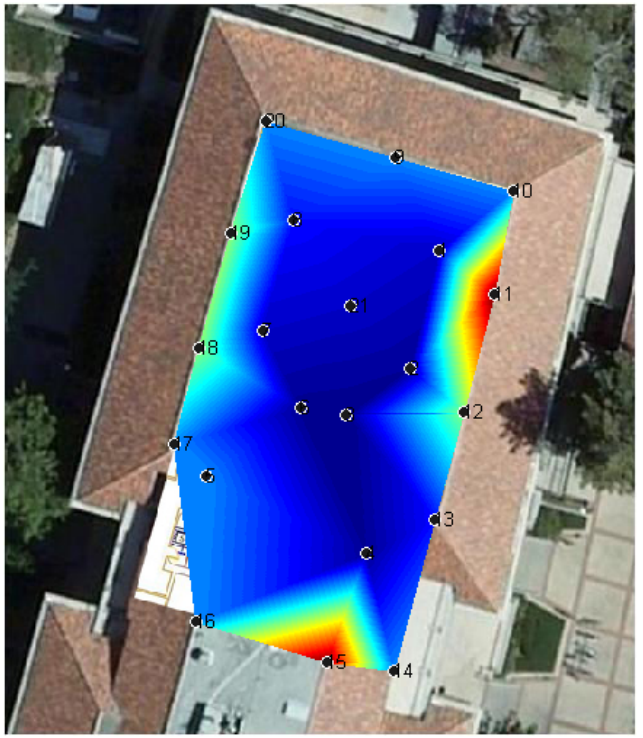


Attack Time Contour Plot



0-min 36-min 72-min 108-min 144-min 180-min

Attack Time Contour Plot



0-min 16-min 32-min 48-min 64-min 80-min

Wi-Fi as a Case Study

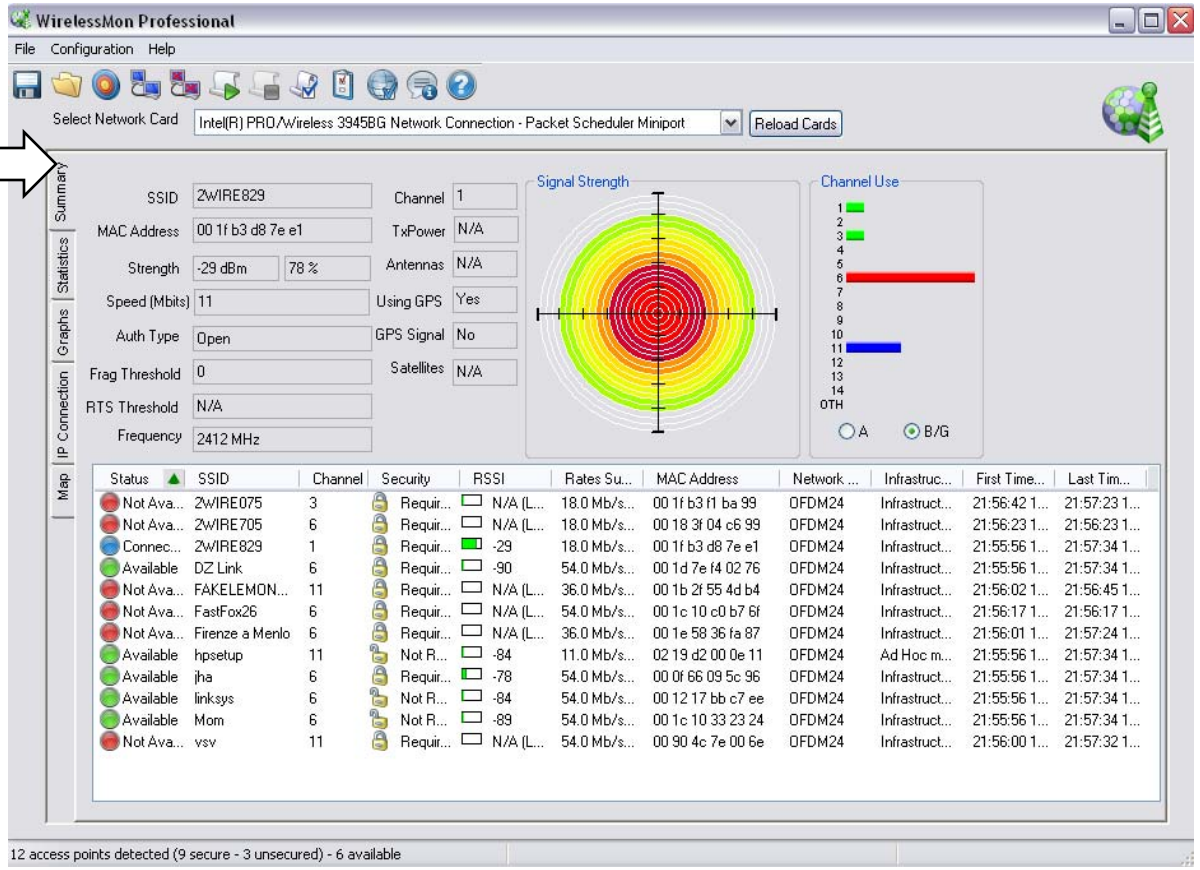
Wi-Fi Data Collection Setup

Intel(R) PRO/Wireless 3945BG

NMEA0813

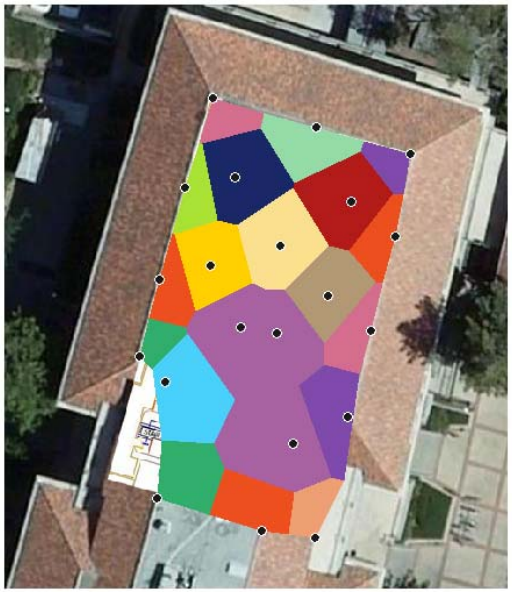
Garmin GPS 35PC

WirelessMon

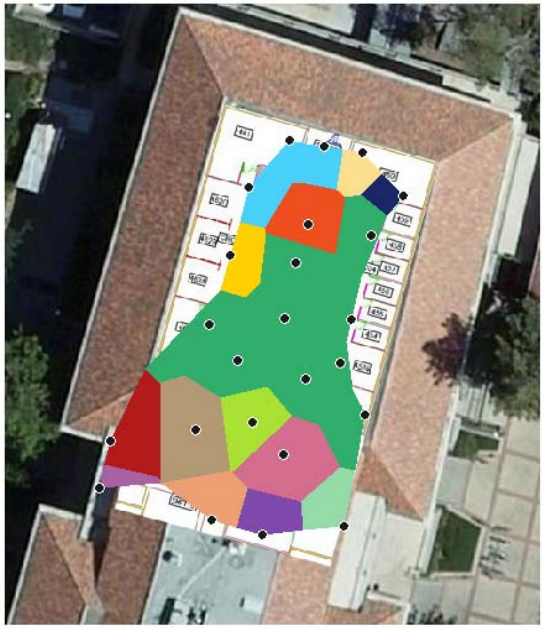


Spatial Decorrelation

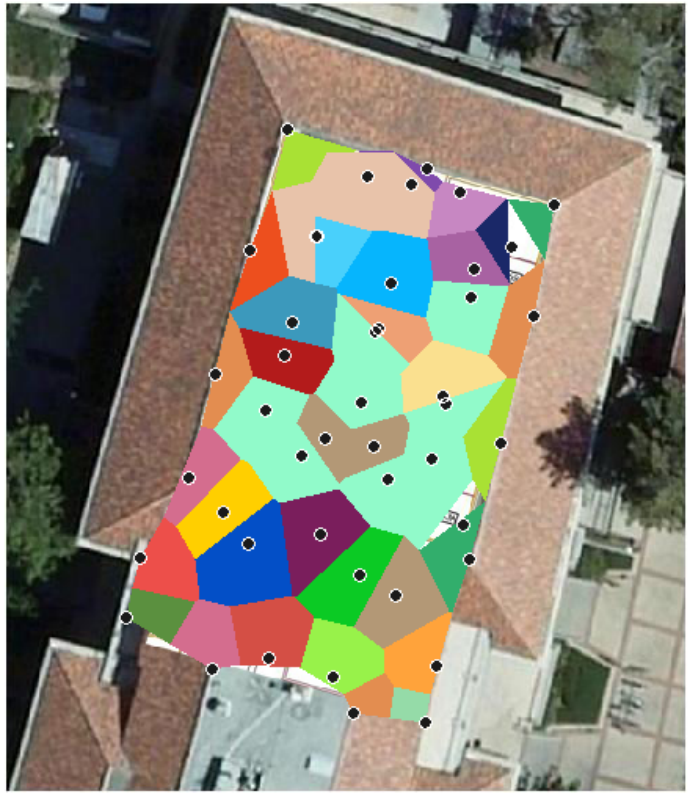
Loran

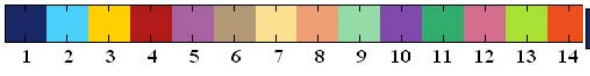


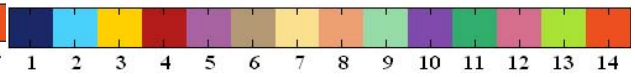
WiFi



Loran + WiFi



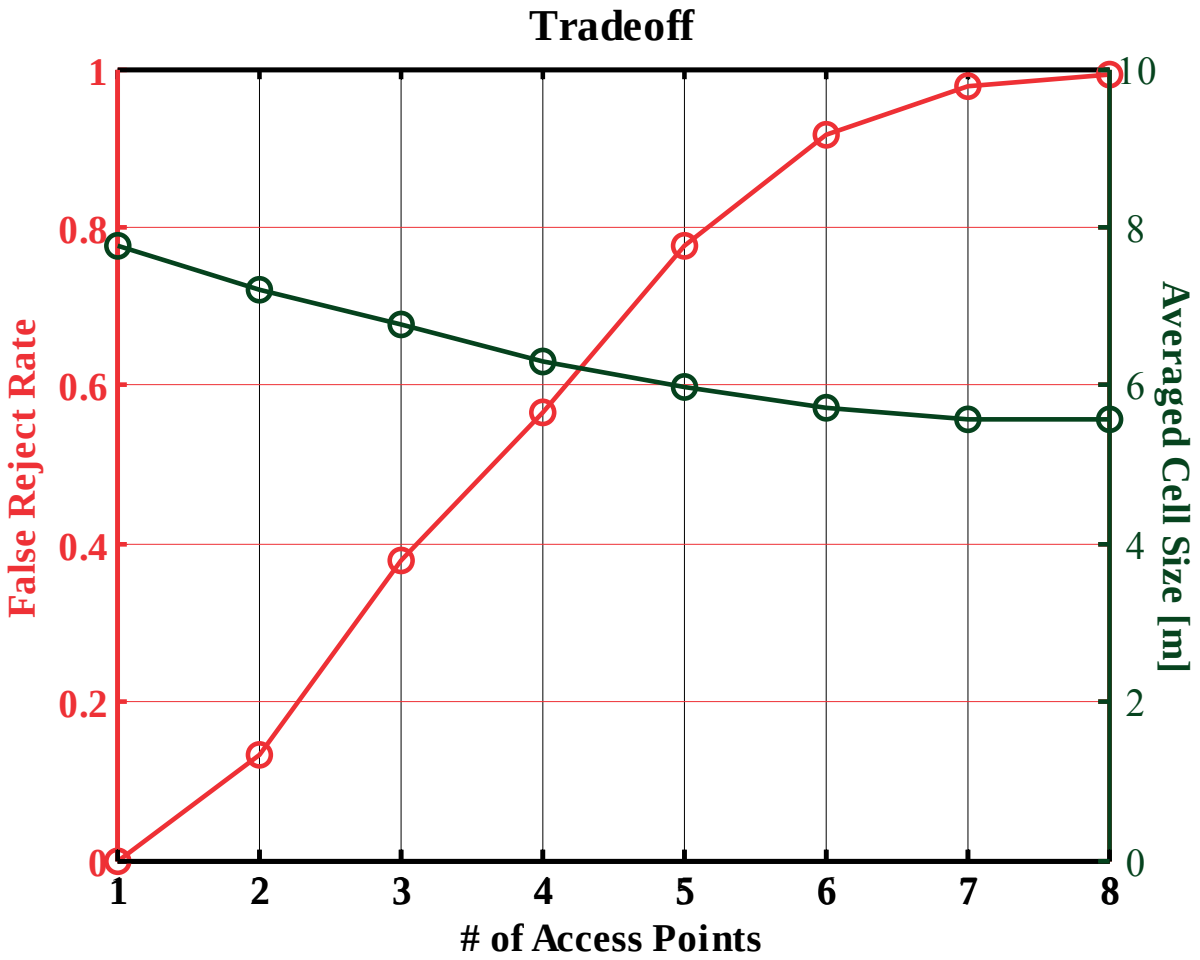




Cell Size	Loran	Wi-Fi (4 APs)	Integrated
Average	10.3 m	12.3 m	8.1 m
Minimum	6.2 m	3.9 m	2.7 m

21% cell size reduction

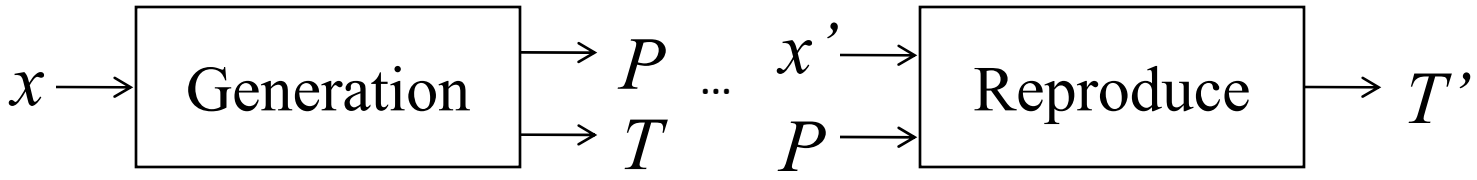
Tradeoff – Office Building



- MAC + RSS
- 28% cell size reduction
- 100% FRR increase
- Loss > Gain

Fuzzy Extractors

Fuzzy Extractor



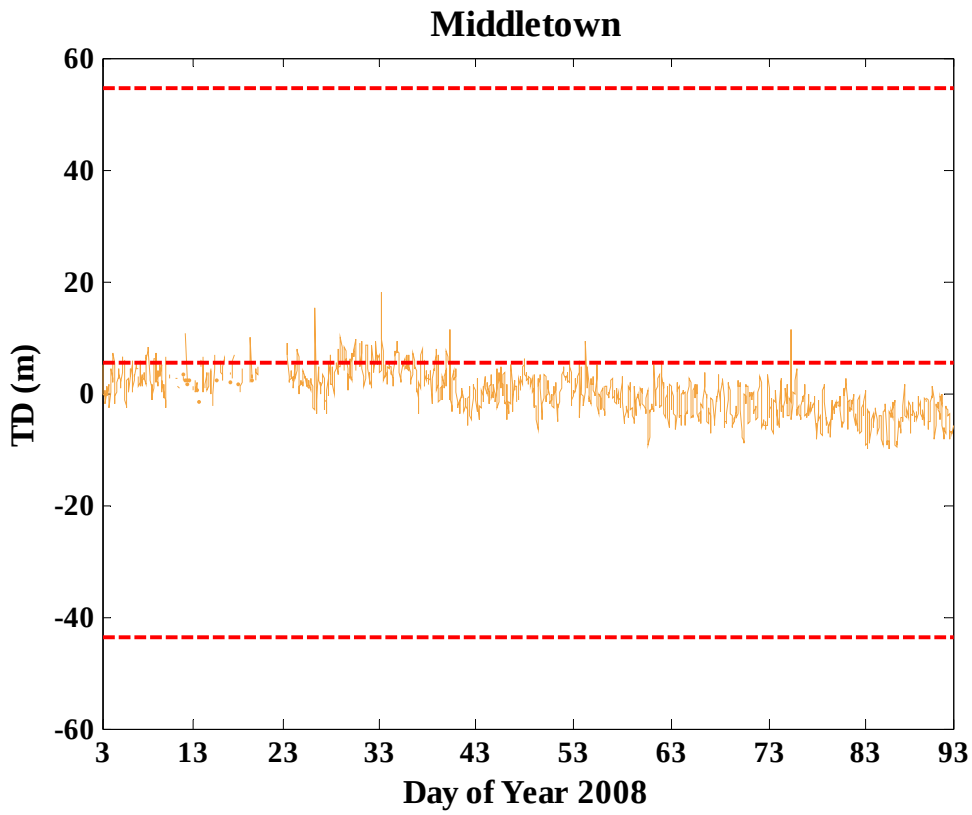
Definition. A fuzzy extractor is a tuple (M, t_0, Gen, Rep), where M is the metric space with a distance function *dis*, Gen is a generate procedure and Rep is a reproduce procedure, which has the following properties:

1. If $dis(x, x') \leq t_0$, $T' = T$.
2. If $dis(x, x') \geq t_0$, $T' \neq T$.

Y. Dodis el al., "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," 2004.

Error Patterns

- Random noise
- Seasonal bias: ASF
- Quantization error
- Missing parameters
  - Implementation issues or station shutdown
  - Loss track of transmitters

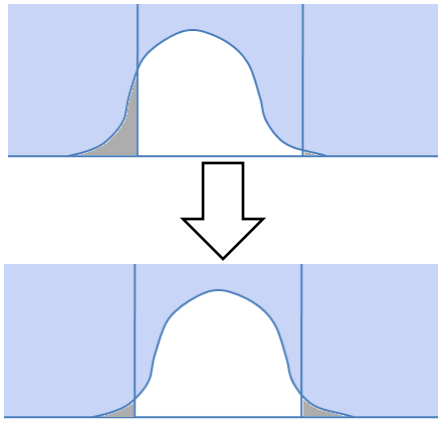


Tag at calibration ≠ Tag at verification

Fuzzy Extractor for Distance Metrics

Fuzzy extractors for location data

- Euclidean metric
  - Random noise and bias
  - Quantization error
  - Offset adjustment



- Hamming metric
  - Missing parameters
  - *dis*(*x, x'*) is the number of positions in which the strings x and x' differ
  - Reed-Solomon error correcting code

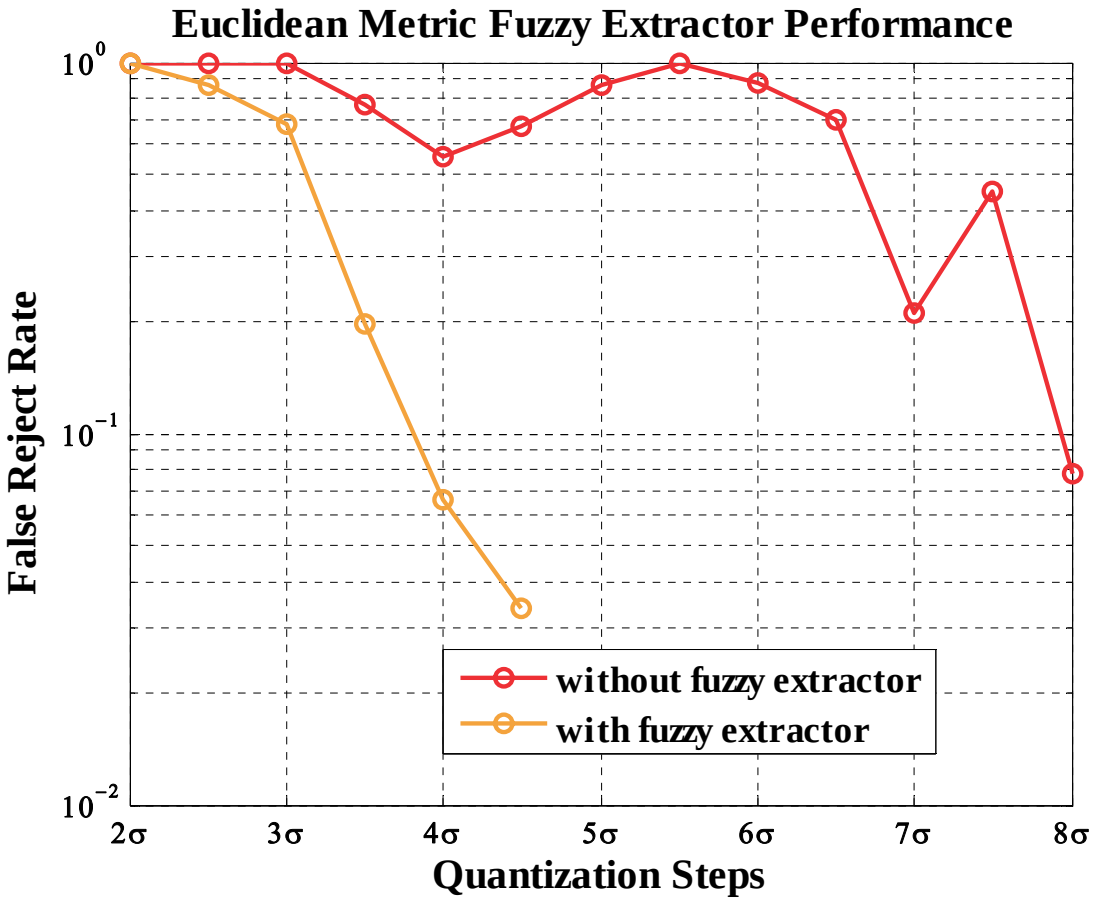
Performance of Euclidean Fuzzy Extractor

- 90 days Seasonal Data

GRI 9940

15 parameters

$$\left\{\begin{array}{c} TD \\ SS \\ ECD \\ SNR \end{array}\right\}$$



84% FRR improvement for $\Delta = 4\sigma$

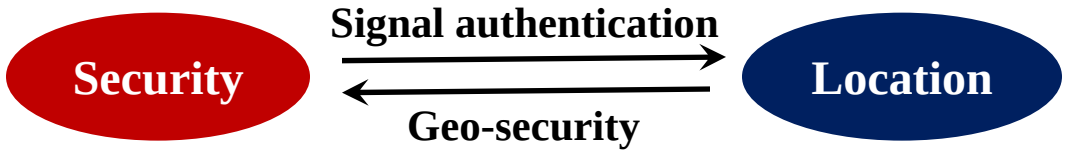
Conclusion

- Location information is good for security applications.
- Tamper-resistance device and self-authenticated signal are required for geo-security system.
- Loran tags are reproducible and unpredictable.
  - Security radius is 10 ~ 20 meters.
- Multiplicity of signals provides robust geotag.
  - Fuzzy extractors
- Stanford filed many patents on geo-security.

Thank You!

Backup Slides

Signal Authentication Survey

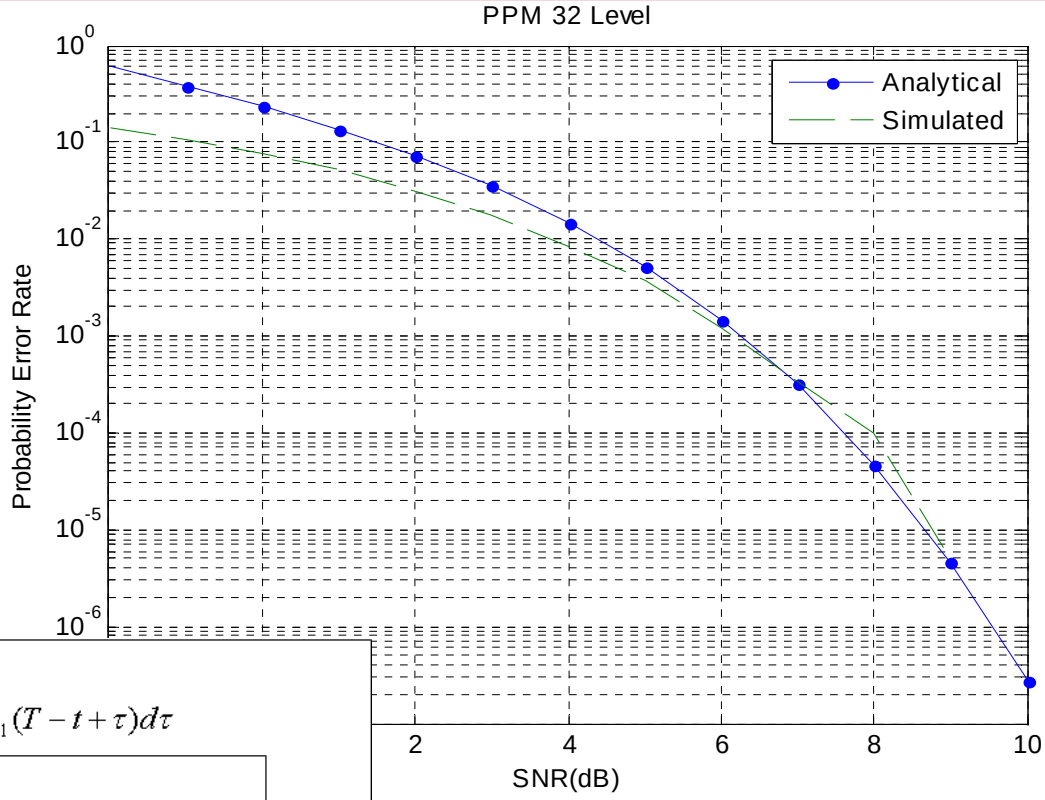


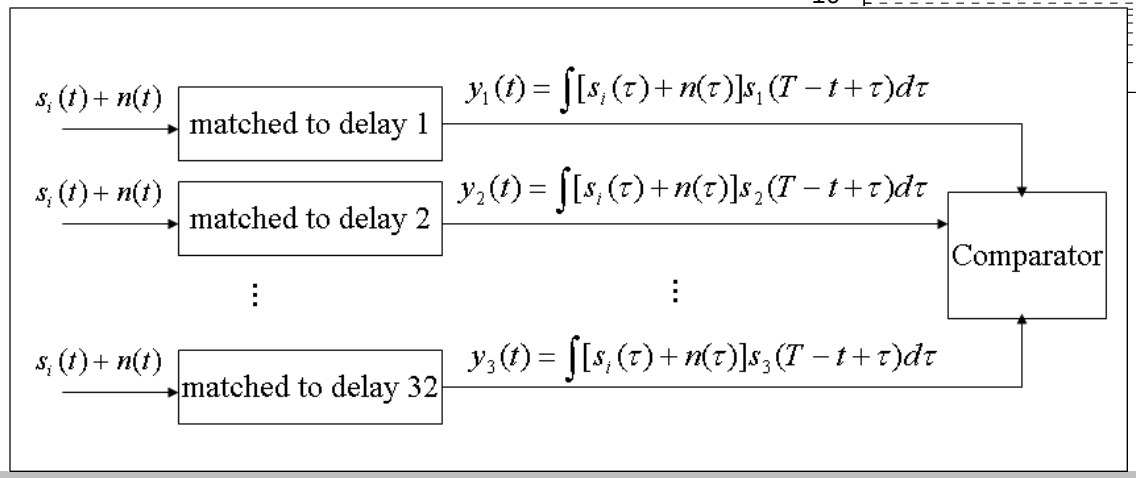
- GPS P(Y) code – encrypted PRN code for military use
- Logan Scott proposed authenticated GPS signal for civil navigation
  - Digital signature to authenticate navigation data
  - Spread spectrum security codes (SSSC) and digital signature
  - Tamper resistant Civil Anti-spoof Security Module to process SSSC
- Proposed authenticated Galileo signal
  - Safety of Life (SoL) service - authenticated navigation data
  - Commercial Service (CS) - encrypt the navigation data
  - Public Regulated Service (PRS) - both encrypted ranging codes and navigation messages
- Proposed TESLA on Loran

Probability of Error in the Presence of Gaussian Noise

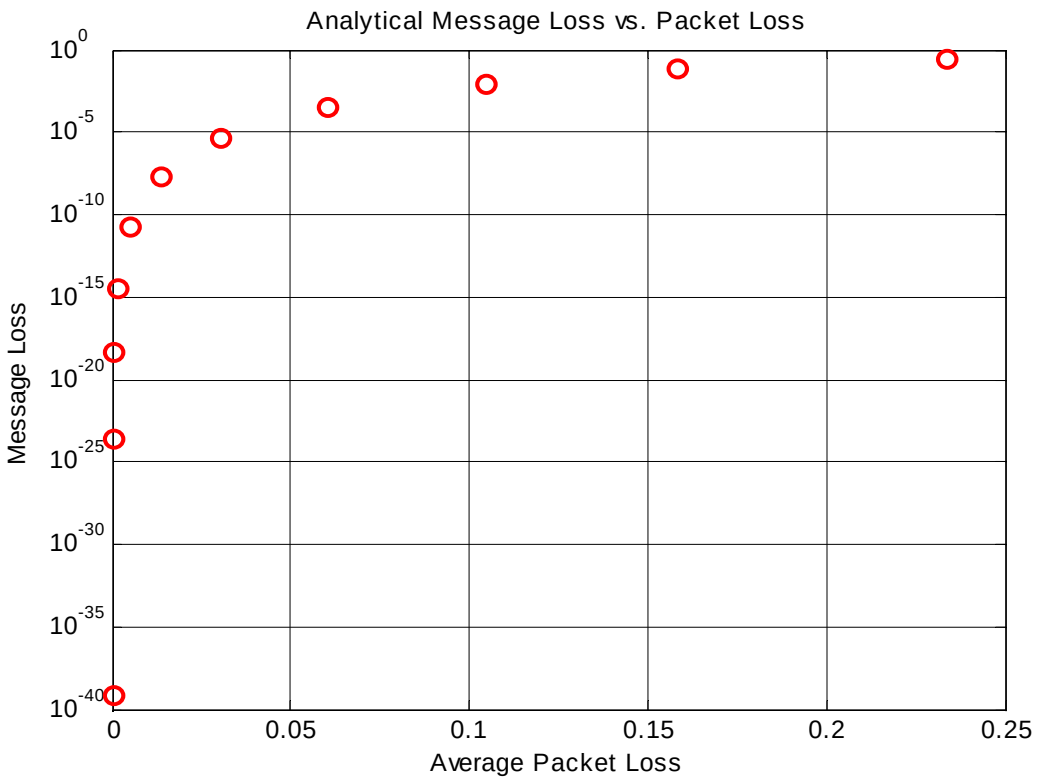
- A matched filter: convolutions of the time-reversed version of reference signals with the input signal
- 30 kHz NEBW

$$P_e = \frac{1}{M}\sum_{i=1}^{M}\sum_{\substack{j=1 \\ i\neq i}}^{M} F_{norm}\left(\frac{\int [s_j(t)-s_i(t)]s_i(t)dt}{\sqrt{\frac{N_0}{2}d_{ij}^{\,2}\int_{-\infty}^{\infty}|h(t)|^2\,dt}}\right)$$





Probability of Message Loss



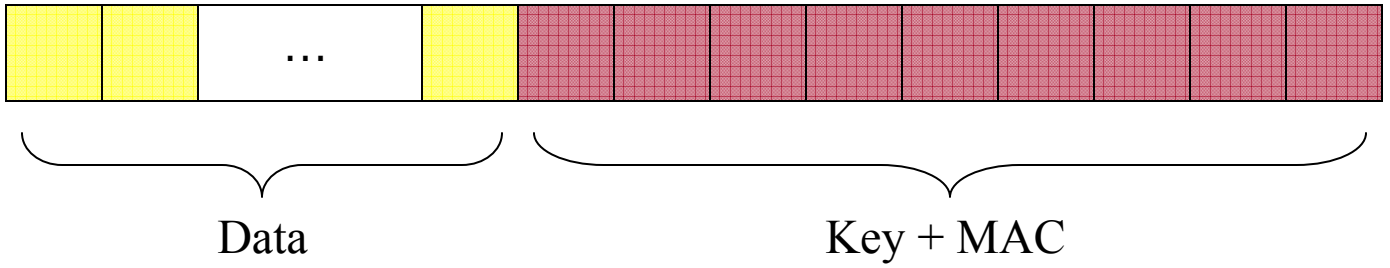
- 1 packet = 5 symbols
- BER → packet loss
- 1 message = 24 packets packet loss → message loss
- RS code
- Error correction performance

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

Authentication Bandwidth

TESLA Segment (packet) { Data messages; Key 160-bit; MAC 160-bit }

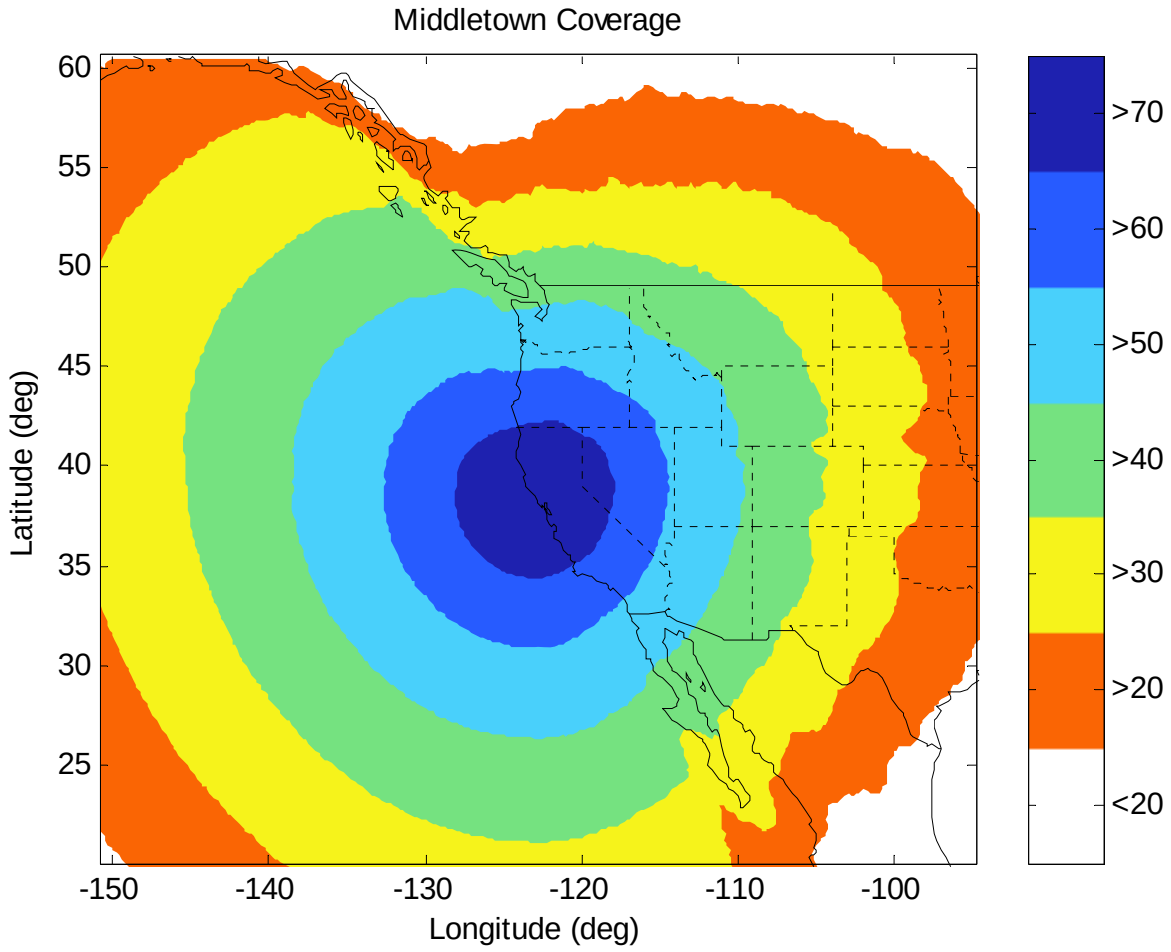
320/37 ⟶ 9 Loran messages



50% BW → 18 Loran messages

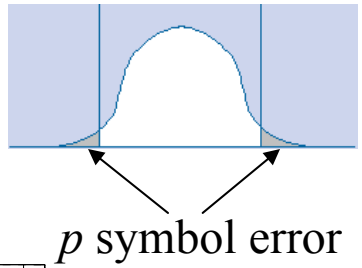
90% BW → 10 Loran messages

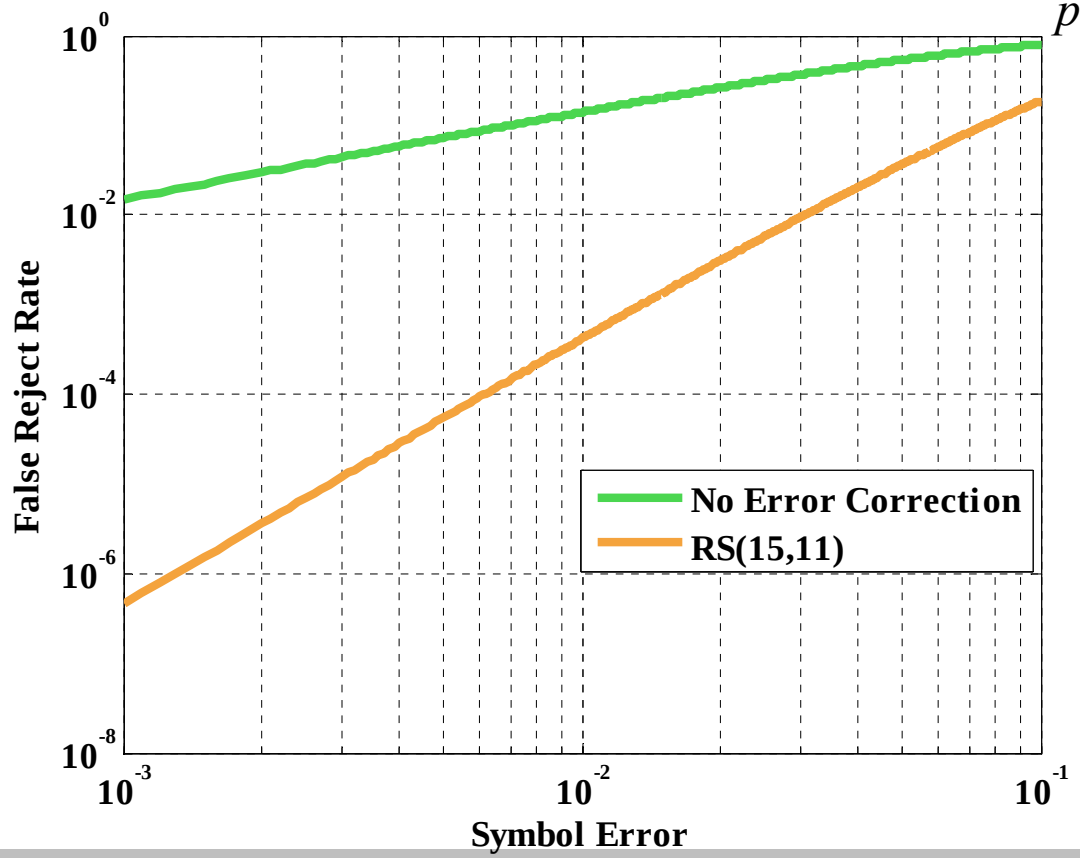
Middletown Field Strength Distribution



Performance Analysis
– Multiple Location Parameters

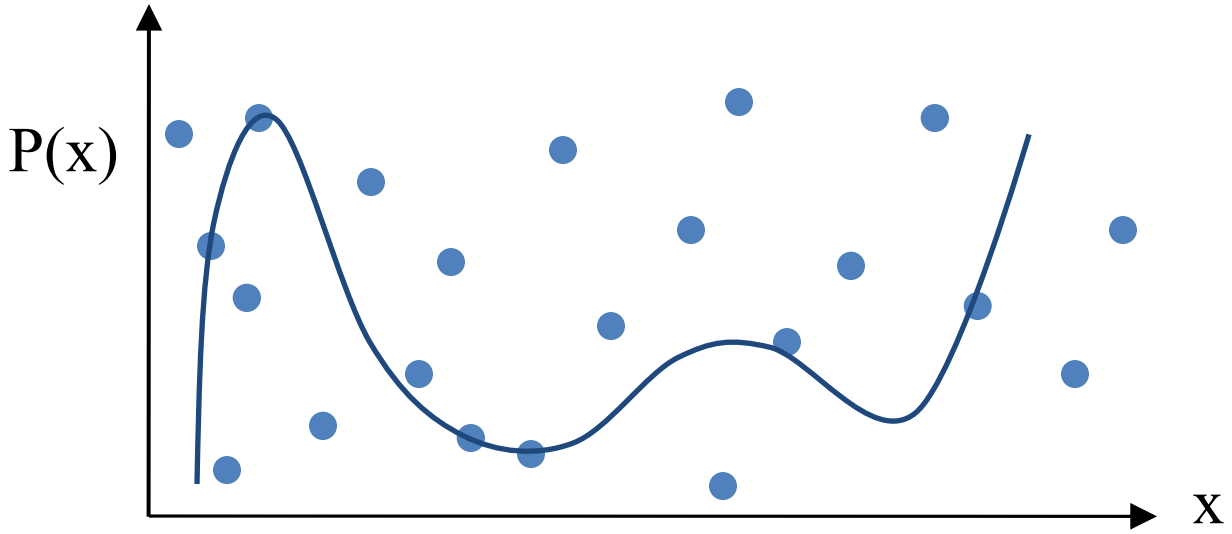
$$\Pr\{\text{error or decode failure}\} = \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j}$$





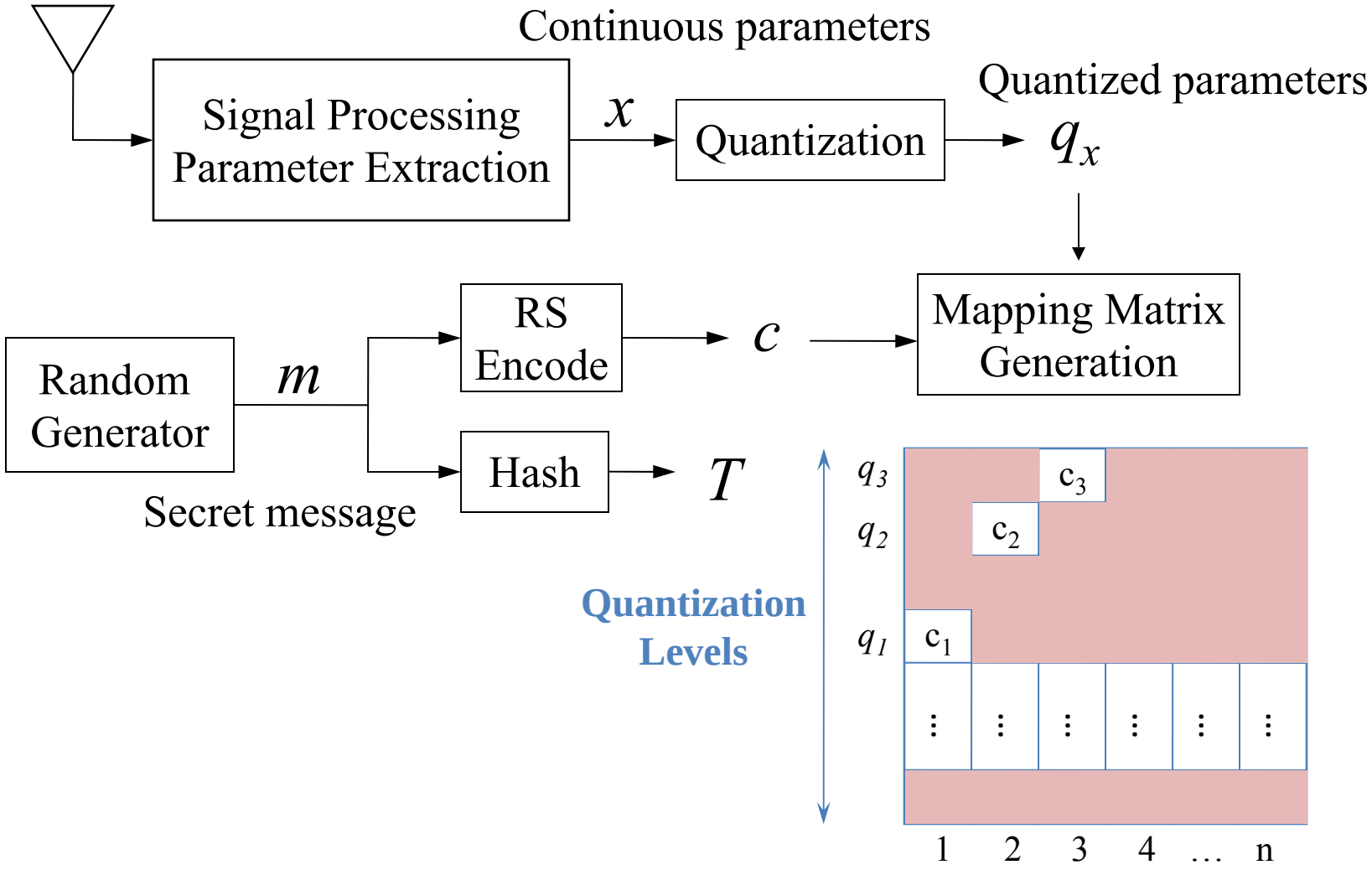
Key Idea of Fuzzy Encryption

- Construct a polynomial by encoding the secrets
- Project parameters on the polynomial
- Randomly create chaff points
- Recover the secrets using the received parameters



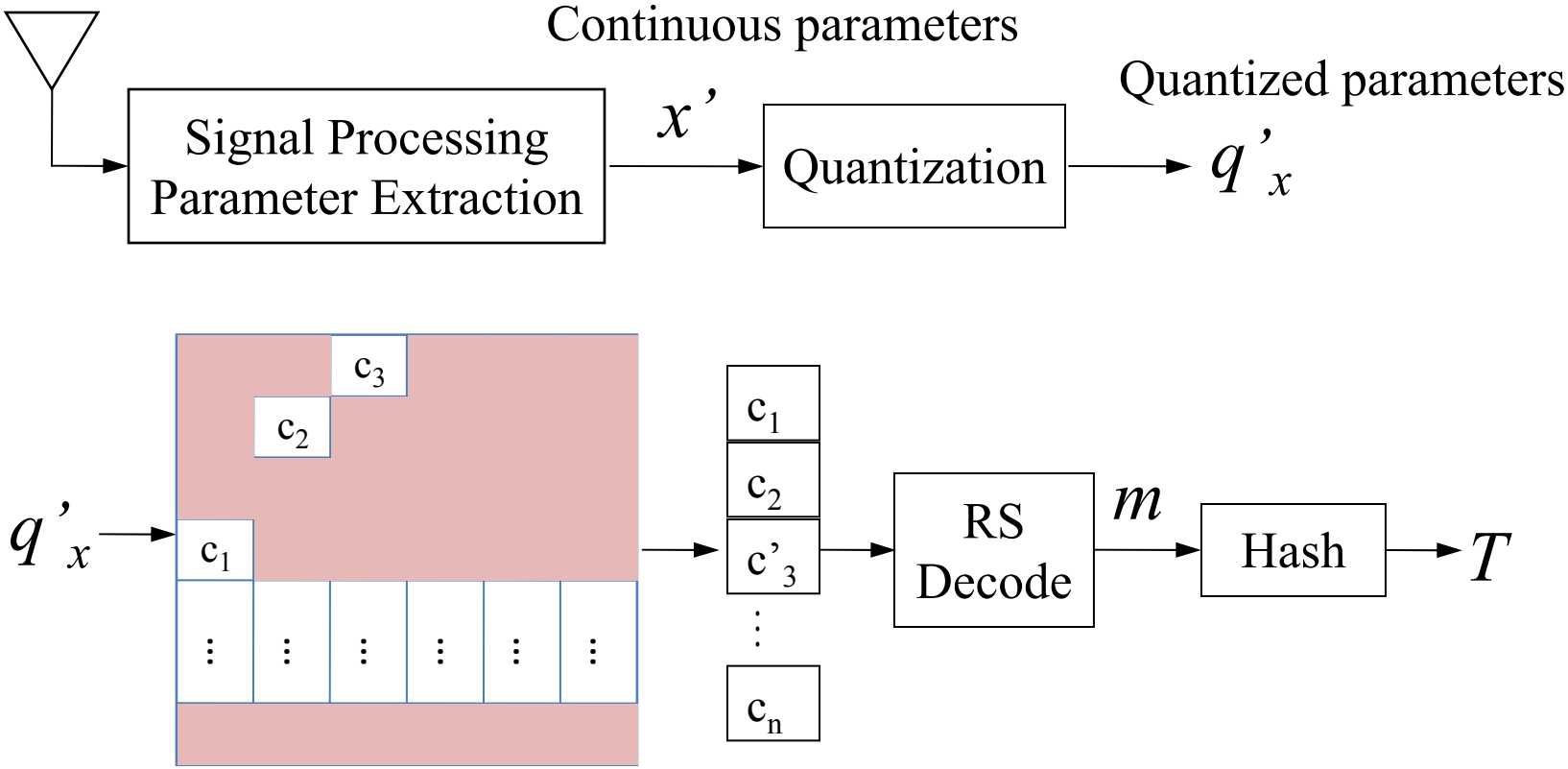
Fuzzy Extractor for Hamming Distance

"Lock"

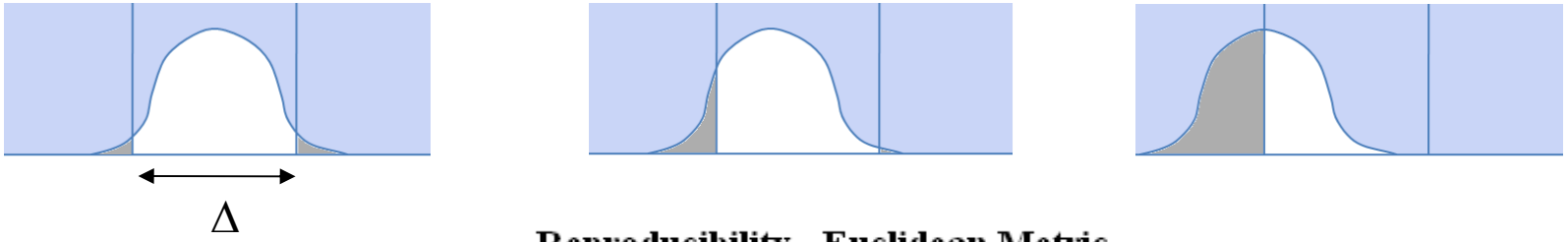


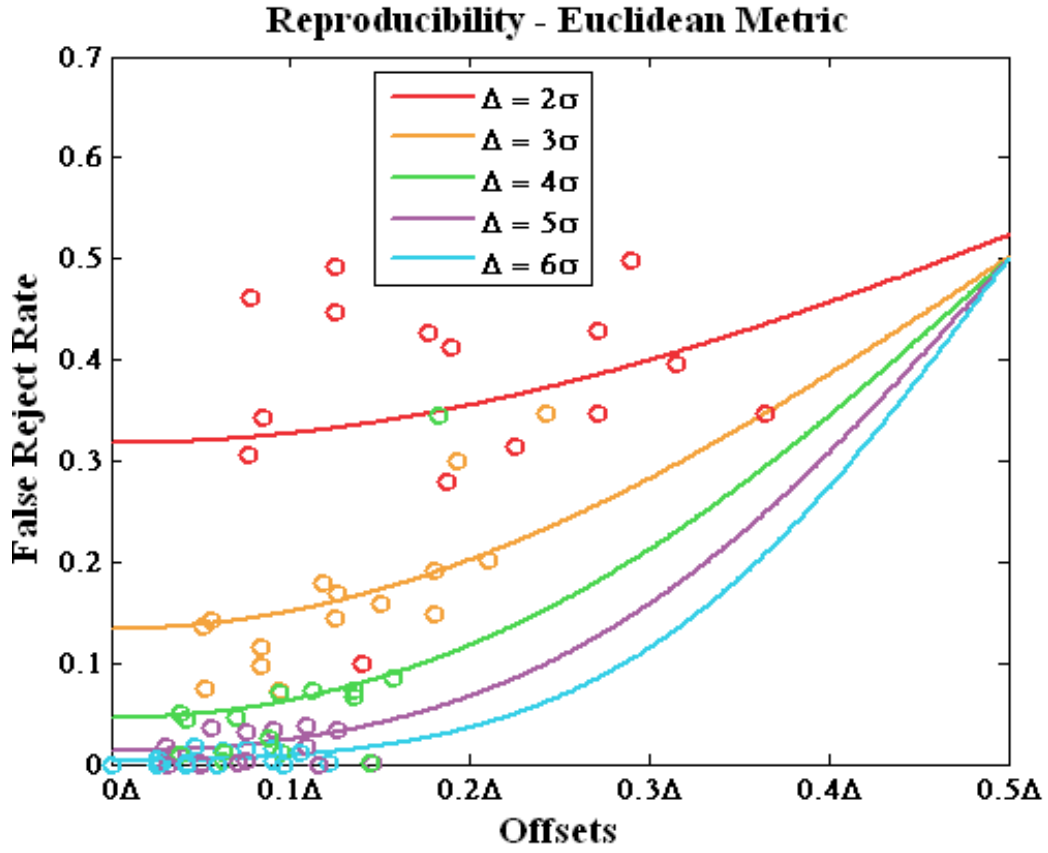
Fuzzy Extractor for Hamming Distance

"Unlock"

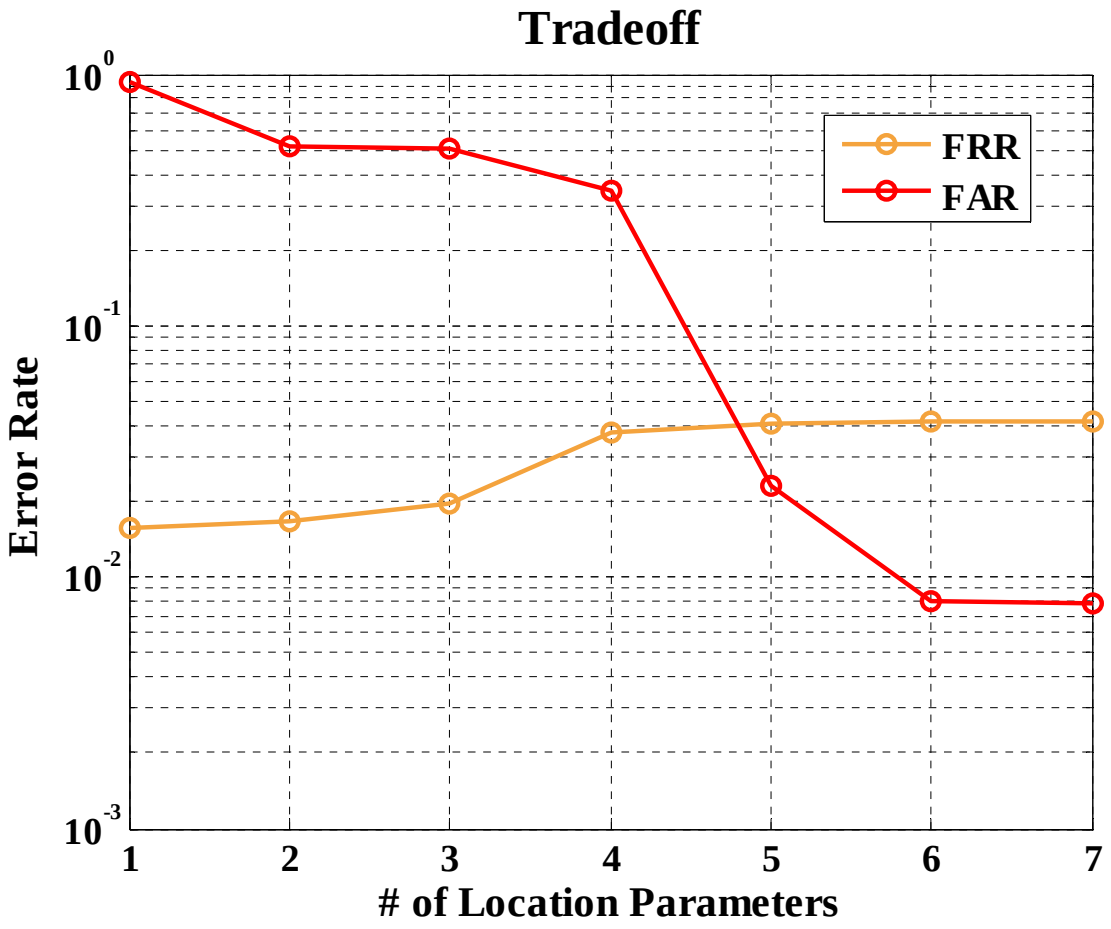


One Location Parameter



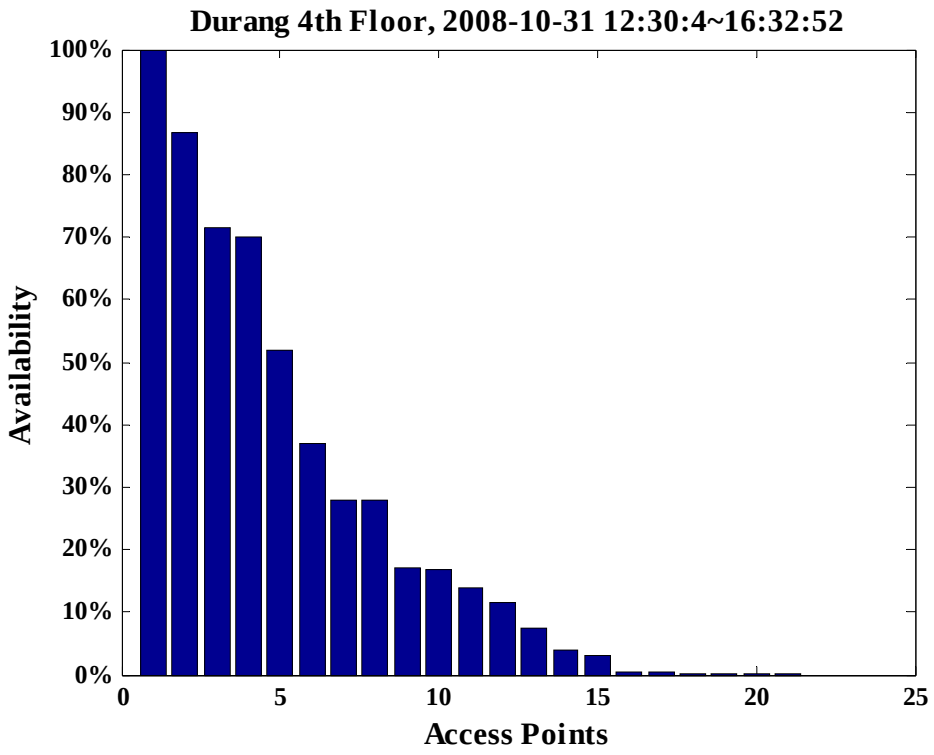


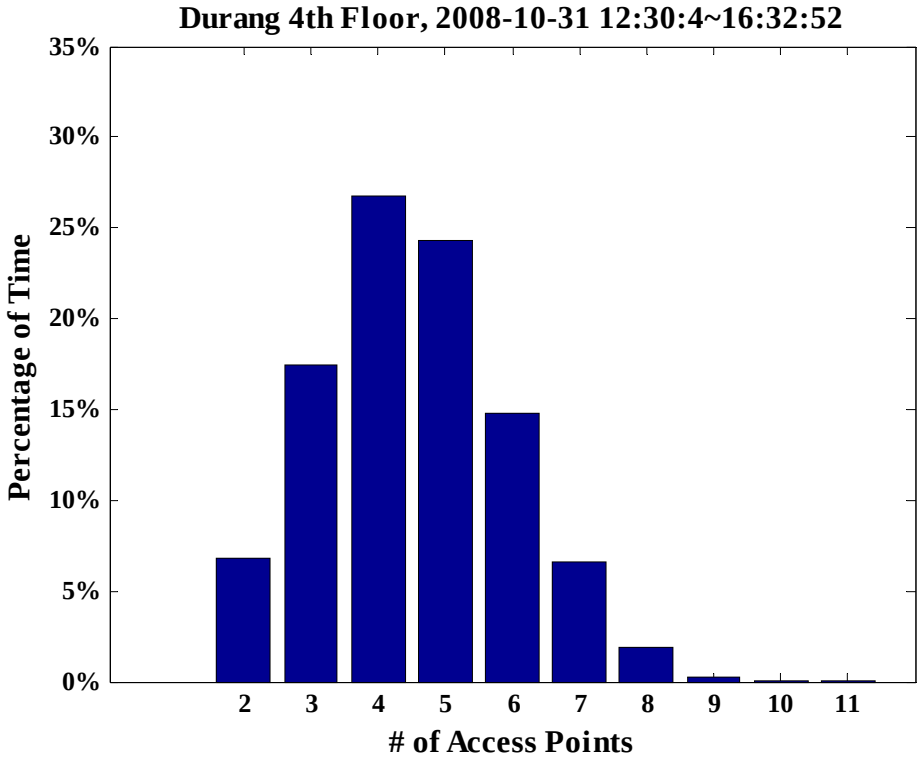
Tradeoff between FAR and FRR



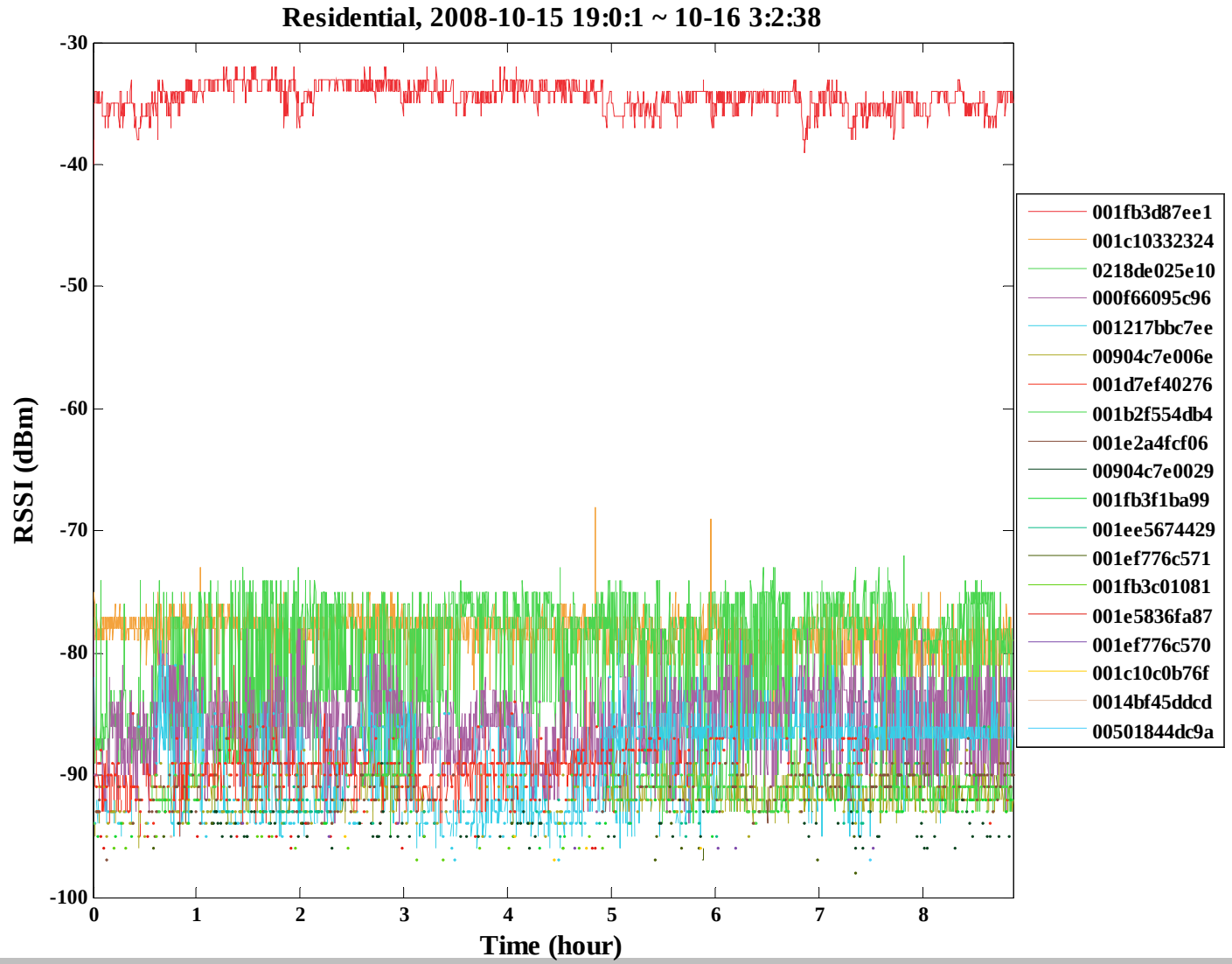
- $\Delta = 6\sigma$
- FRR 0.01→0.04
- FAR 0.9→0.008
- Optimal N = 5

Availability – Office Building

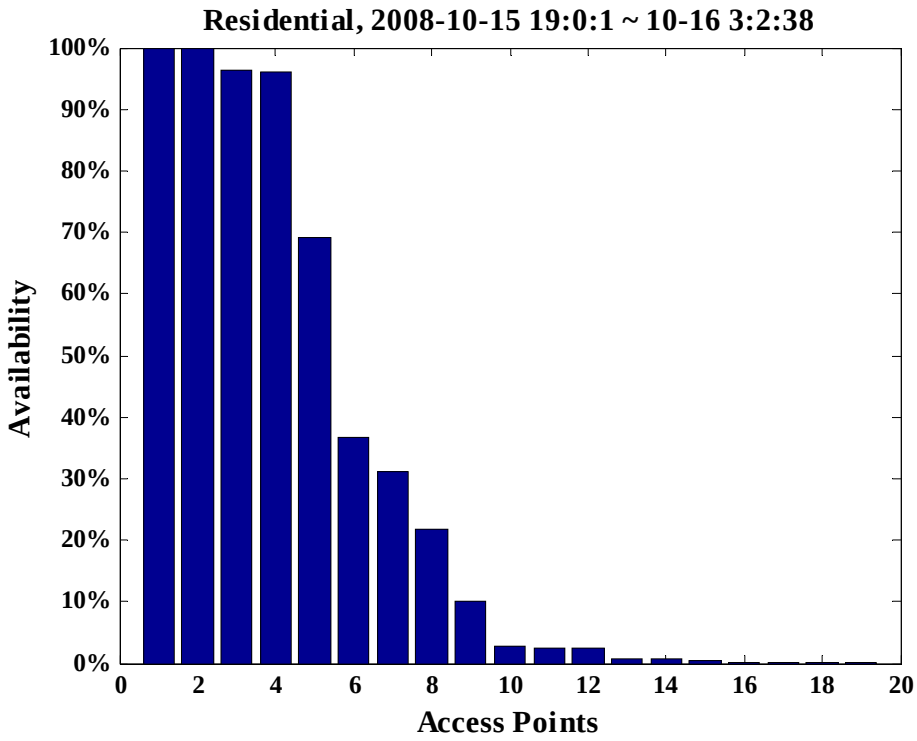


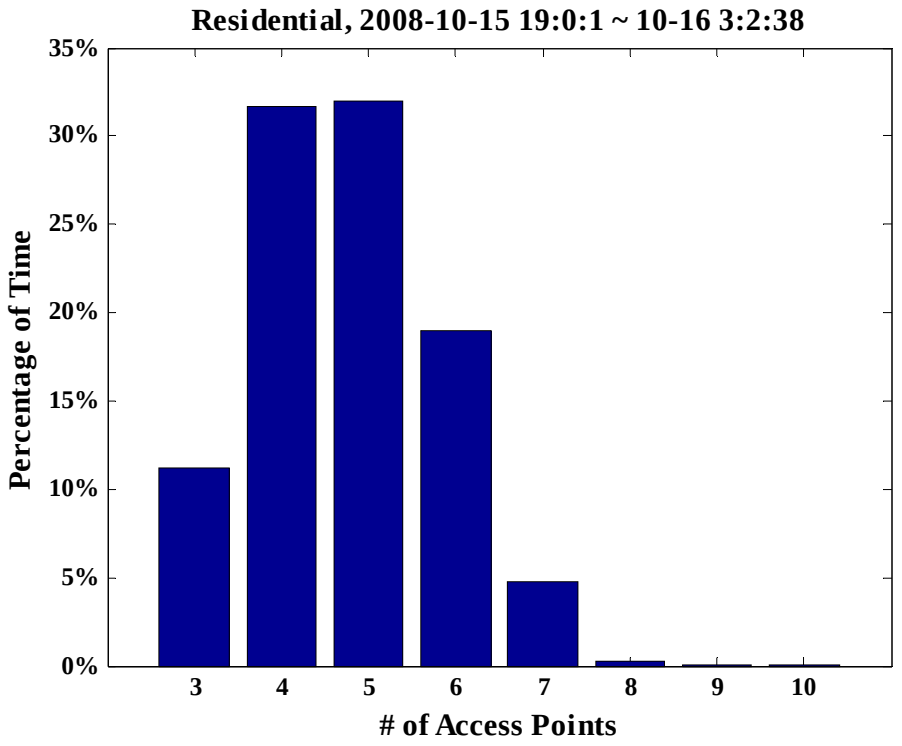


RSSI Monitor

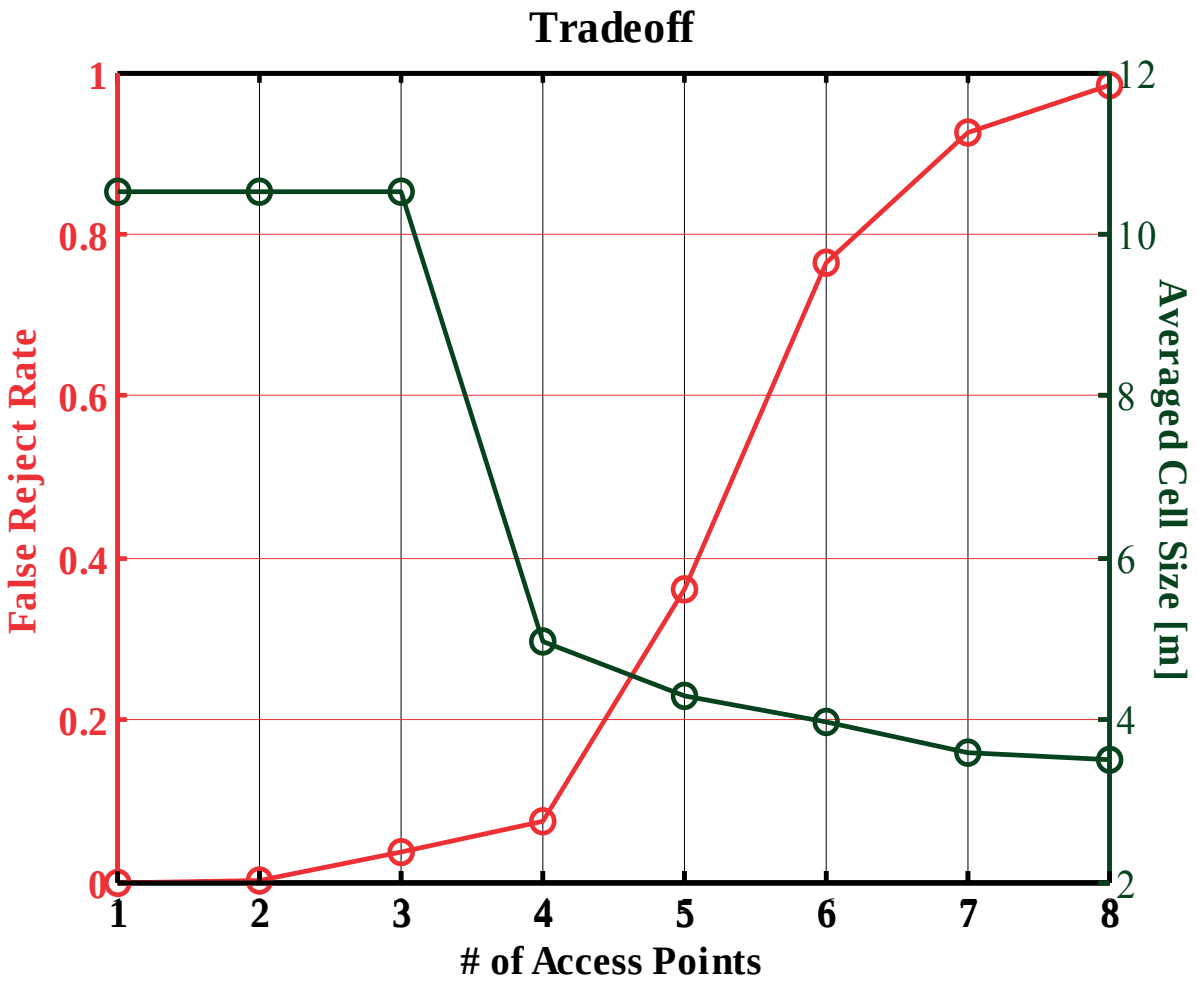


Availability – Residential





Tradeoff - Residential



- Wi-Fi
- MAC + RSS
- 28% cell size reduction
- 98% FRR increase
- Loss > Gain