SAND2011-6545C

Low-Cost Mitigation of Privacy Loss due to Radiometric Identification

Jason Haas
Sandia National Laboratories
jjhaas@sandia.gov

Yih-Chun Hu
University of Illinois at Urbana-Champaign

Nicola Laurenti
University of Padova

Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Introduction

- Also called “radiometric identification”, “RF fingerprinting”, “wireless fingerprinting”

- Manufacturing tolerances in radio circuit components result in device-unique fingerprints

- Previous work
  - Useful for authentication
  - Serious privacy implications

Previous Work –

- Brik et al., Mobicom 2008
  - Large number of commercial 802.11b devices
  - Uncontrolled environment
  - Record using vector signal analyzer
  - Classifier has >99% accuracy
  - Used 5 features to establish identity – carrier frequency offset most telling

- Edman and Yener 2009 used a USRP2 to achieve similar results

Problems So Far

- Software defined radios (still) expensive

- Can wireless fingerprints be hidden?
  - *Cheaply?*
  - How well can a privacy attacker do?

- How do phase noise and interference affect attacker?

- Evaluate via simulation – MATLAB

Modified Cramer-Rao Bound

$$\underbrace{\frac{3}{2\pi^2 {T_0}^3 B} \frac{1}{\text{SNR}}}$$

Lower bound on variance in attacker's estimation

T_0	Observation time
B	Signal bandwidth
N	Number of identities
I	Mutual information
Δ	Frequency tolerance
$\hat{f}_c$	Frequency estimate

$$N = 2^{I(f_c, \hat{f}_c)} \approx 2\Delta \sqrt{\frac{\pi B {T_0}^3}{3e} \text{SNR}}$$

Number of identities

Mitigation

- Switch wireless identity at the PHY layer
  - Introduce small transmitter-controlled errors
  - Achieved through software and hardware
- Must coordinate switches across layers
- Carrier frequency
  - Apply small changes to oscillator
  - Ex., change voltage (e.g., with digital to analog converter) on voltage controlled oscillator (VCO)

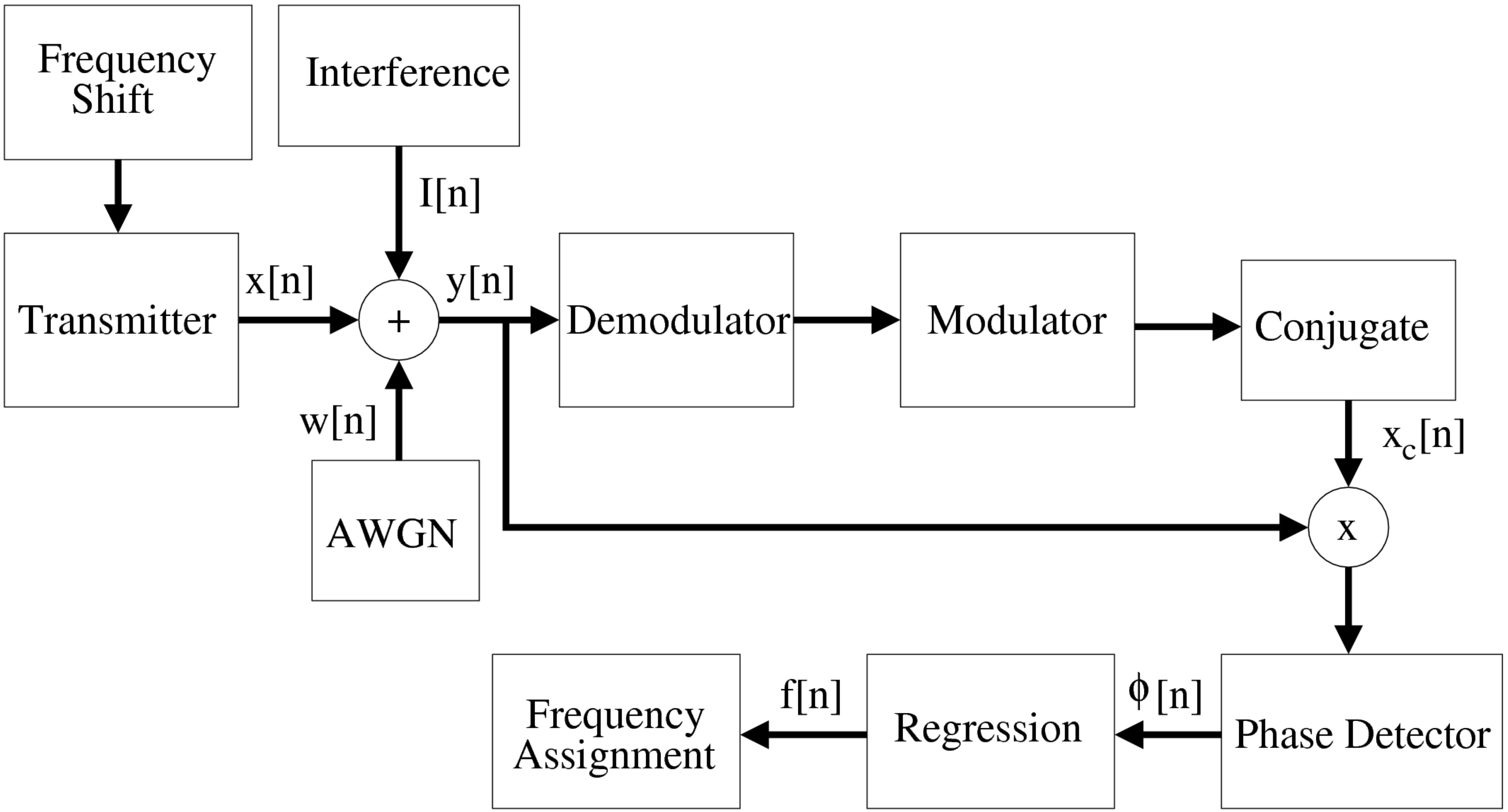
$$N = 2^{I(f_c,\hat{f}_c)} \approx 2\Delta\sqrt{\frac{\pi B {T_0}^3}{3e}\mathrm{SNR}}$$

} Number of identities

Privacy Simulations

- Implement maximum likelihood estimator for attacker
- Effects of interference on attacker
- How well would carrier frequency switching work?

Attacker Implementation



Attacker Estimator

- Tested 2000 transmissions without phase noise or interference – estimator achieves $1.44\sigma^2$

- Theory – 22.63 bits of precision required for perfect privacy

Attacker Model

- Receive 2 sets of 10 packets (1 second) from each vehicle
- Between 2 sets, vehicles switch carrier frequency identity
- Match estimated frequency offset between 2 sets
- ***Rank*** vehicles by closest frequency

Rank

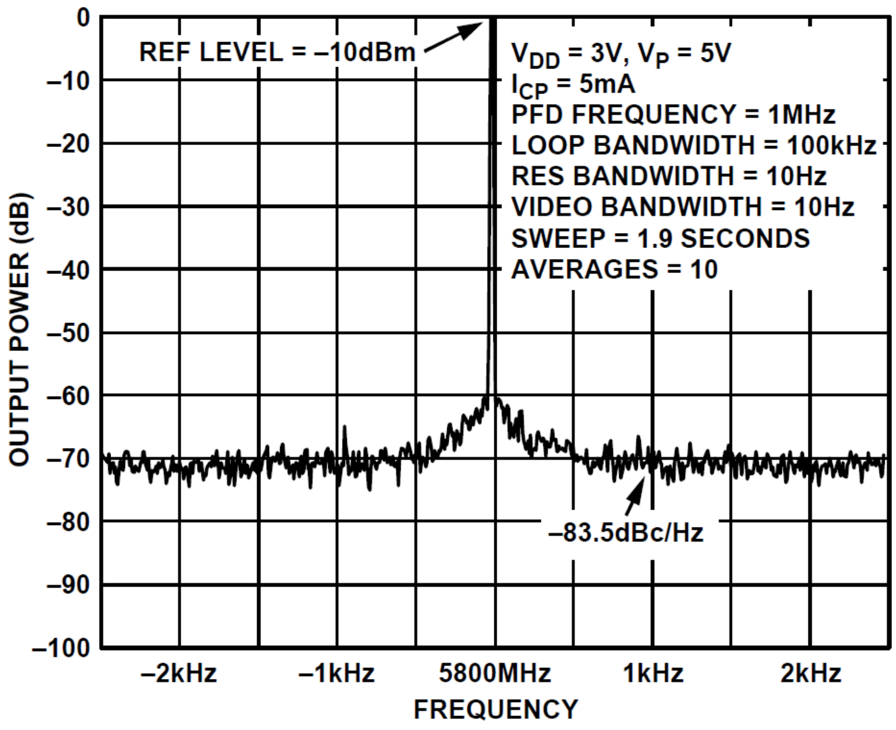
- Main idea – sort vehicles by likelihood, use other criteria later to refine

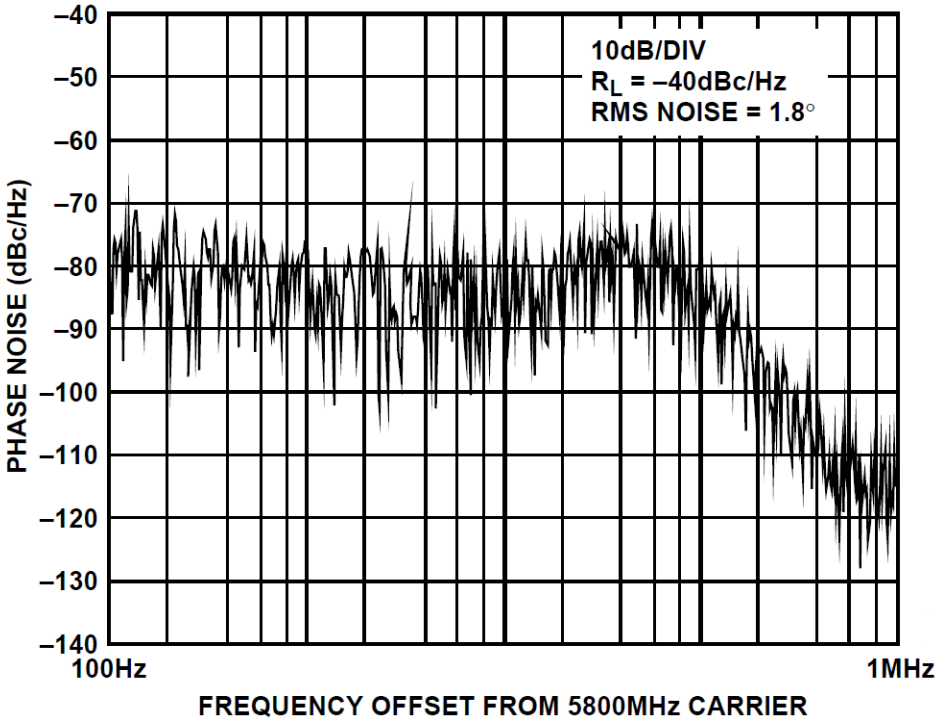
- Vehicle is x-most likely vehicle → Rank = x

- Metric
  - Probability(Rank ≤ x)
  - Calculated by omniscient viewer

Phase Noise Model

- Colored Gaussian noise
- Parameterized using AD 4106 (frequency synthesizer)

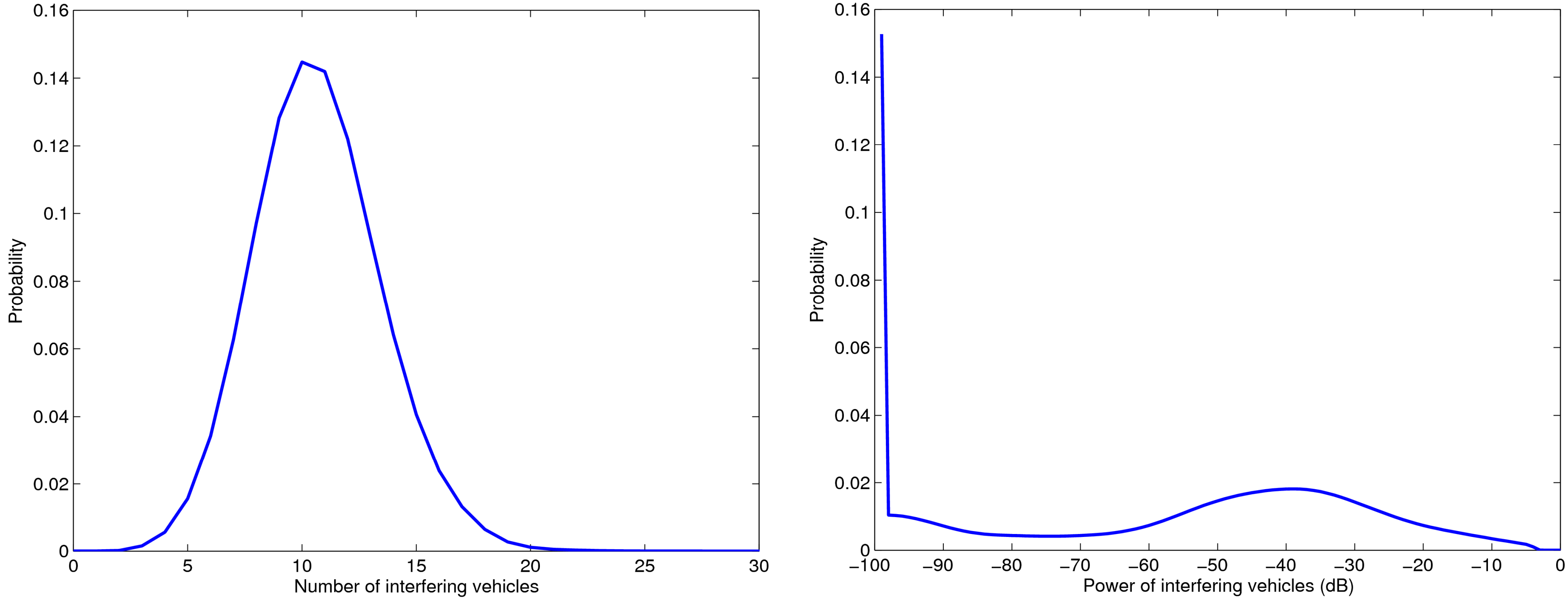




Interference Simulations

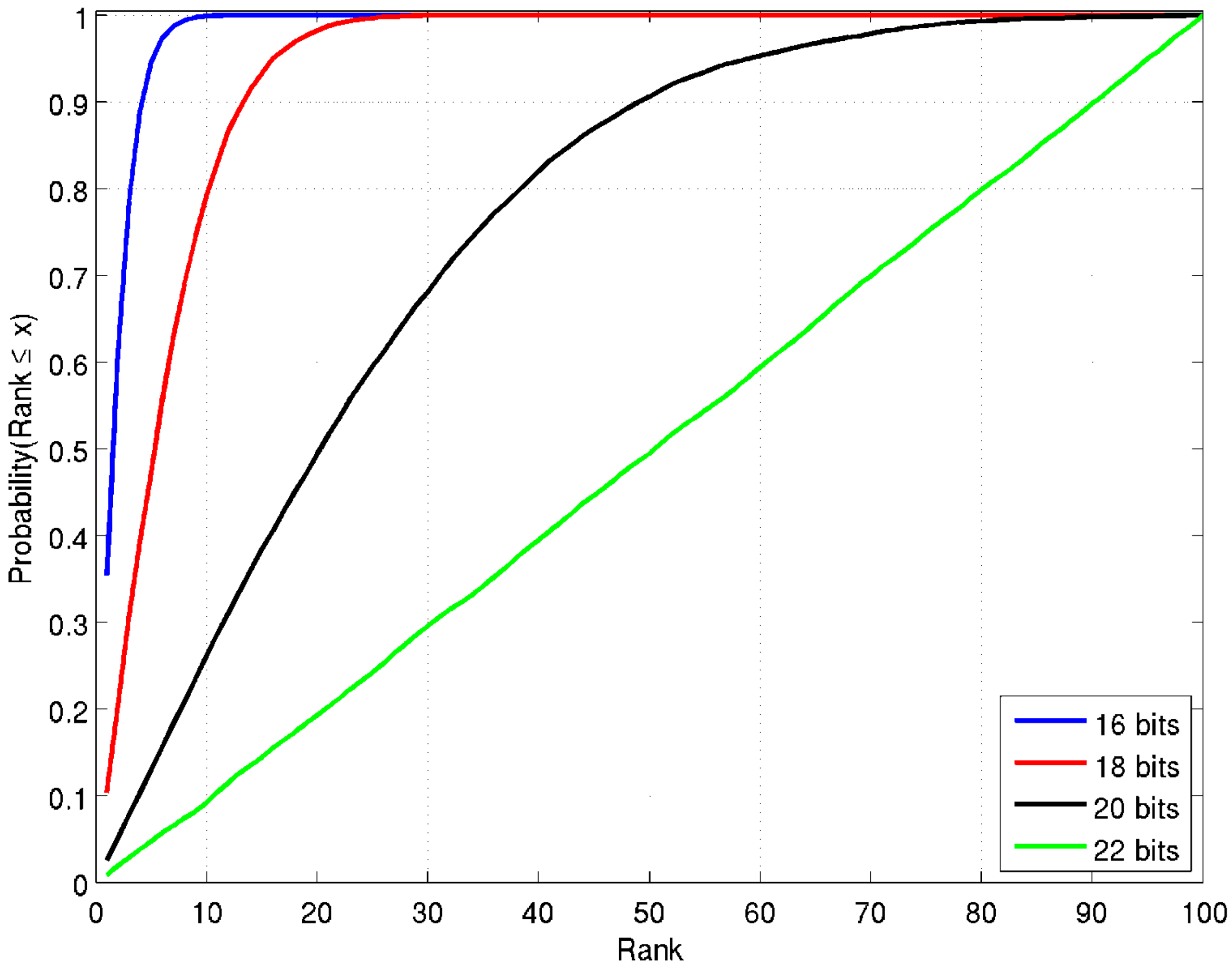
- Used VANET simulator to simulate part of Zürich, Switzerland
- 4.75 km x 4.0 km section – larger area reduces edge effects
- Downtown area
- ≈1280 vehicles active concurrently

Interference Parameterization

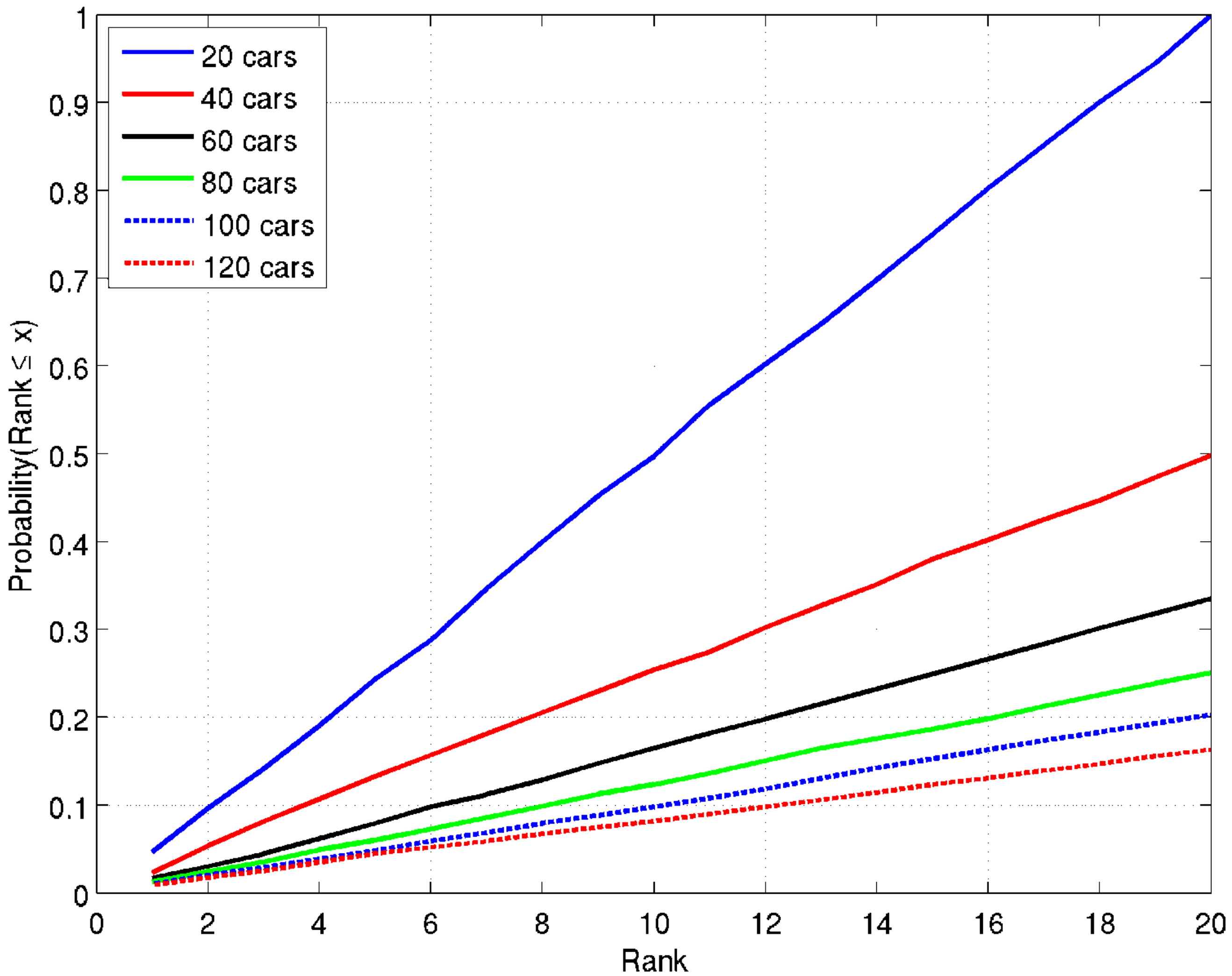


Zürich simulation results

Attacker Estimator – Without Phase Noise and Interference



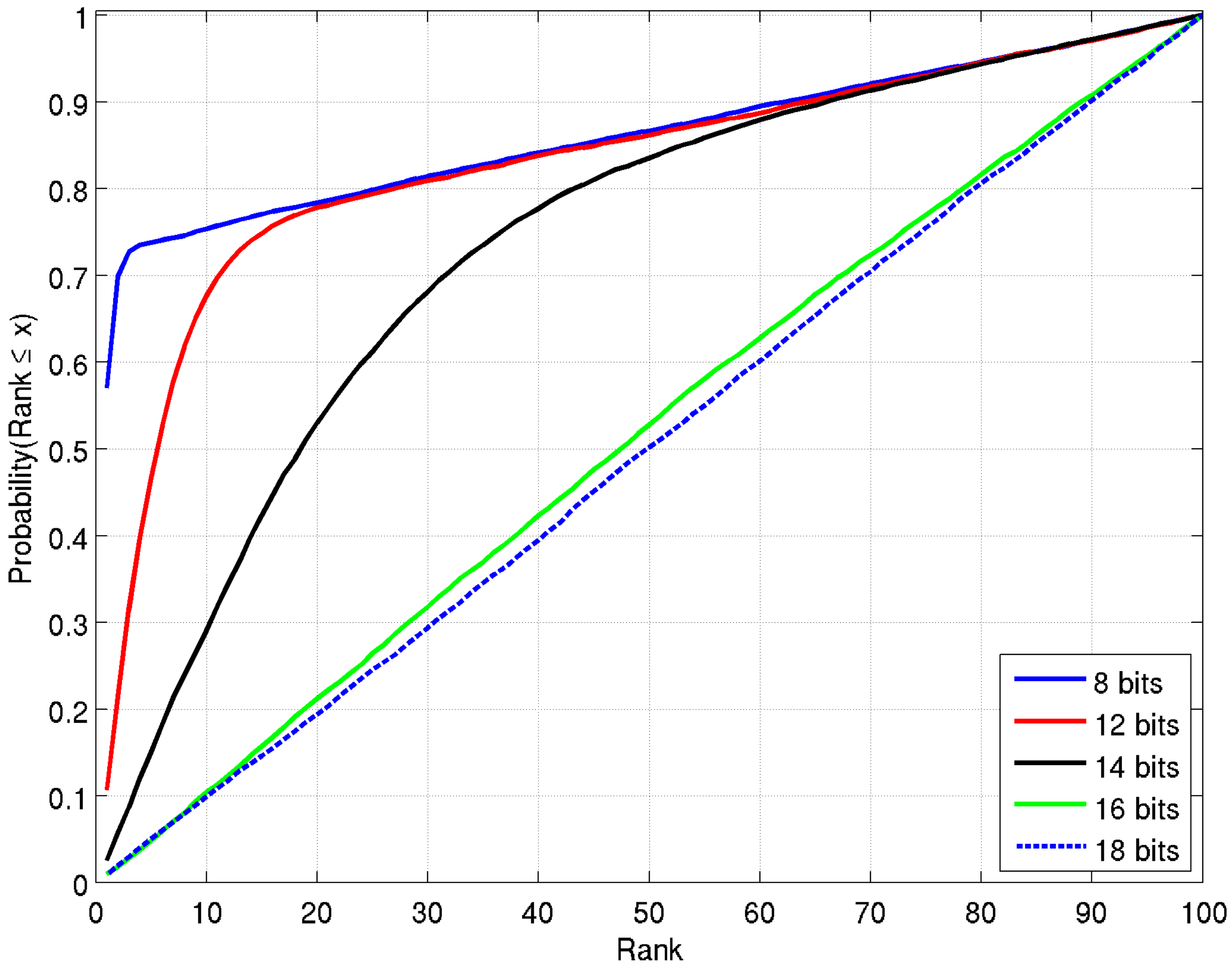
Varying Group Size



22 bits, with interference

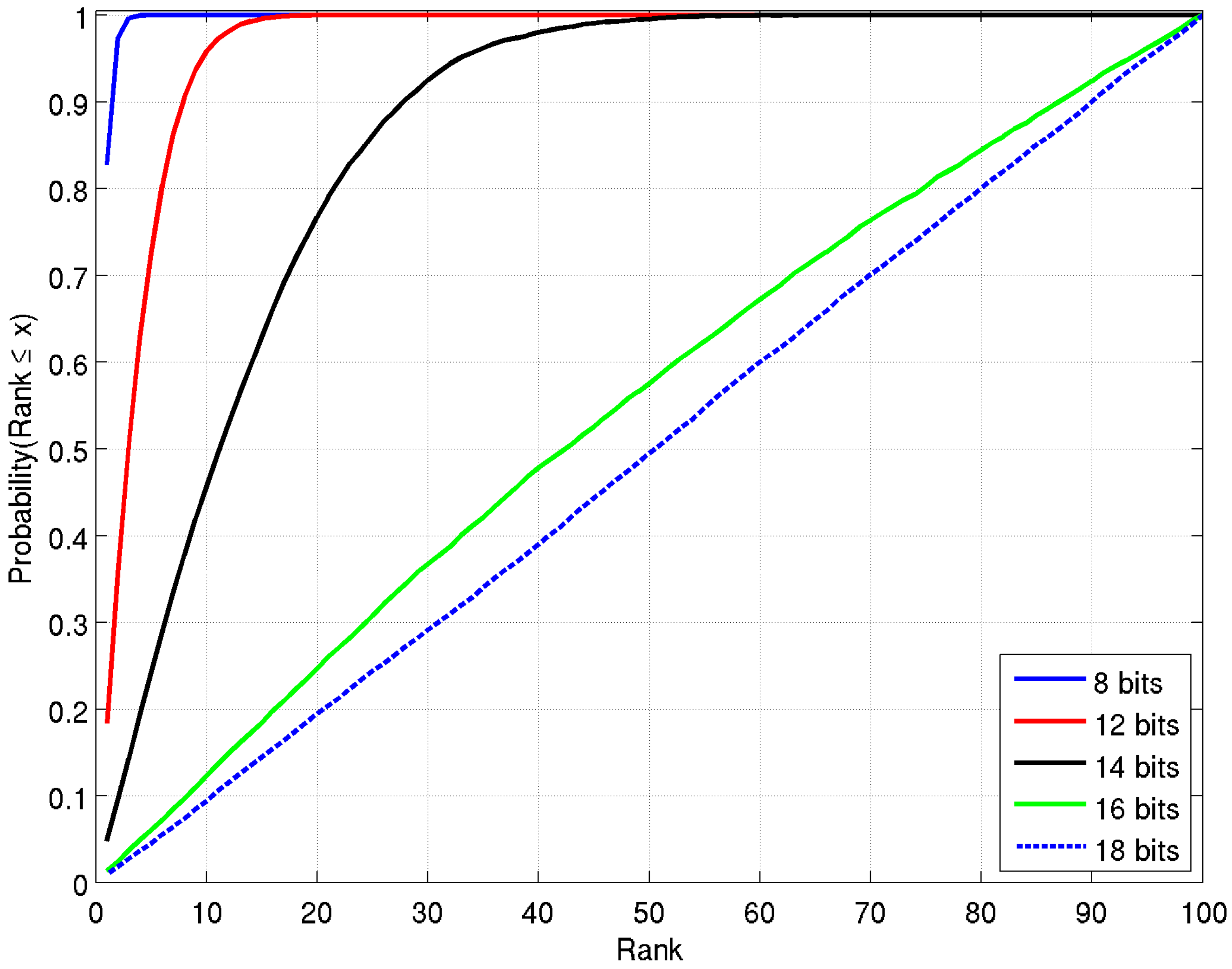
Sandia National Laboratories

Varying Precision – 100 Vehicles with Interference

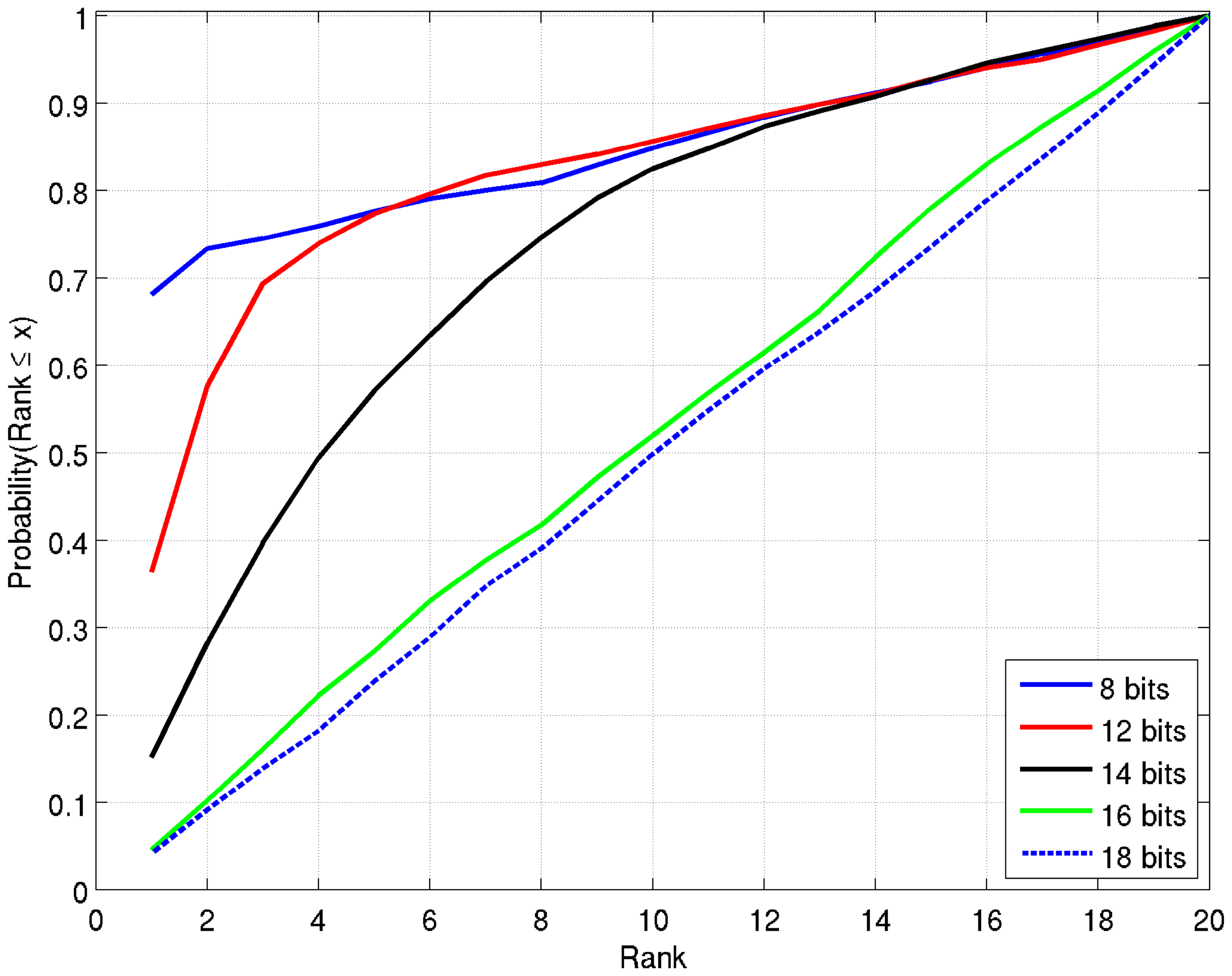


Sandia National Laboratories

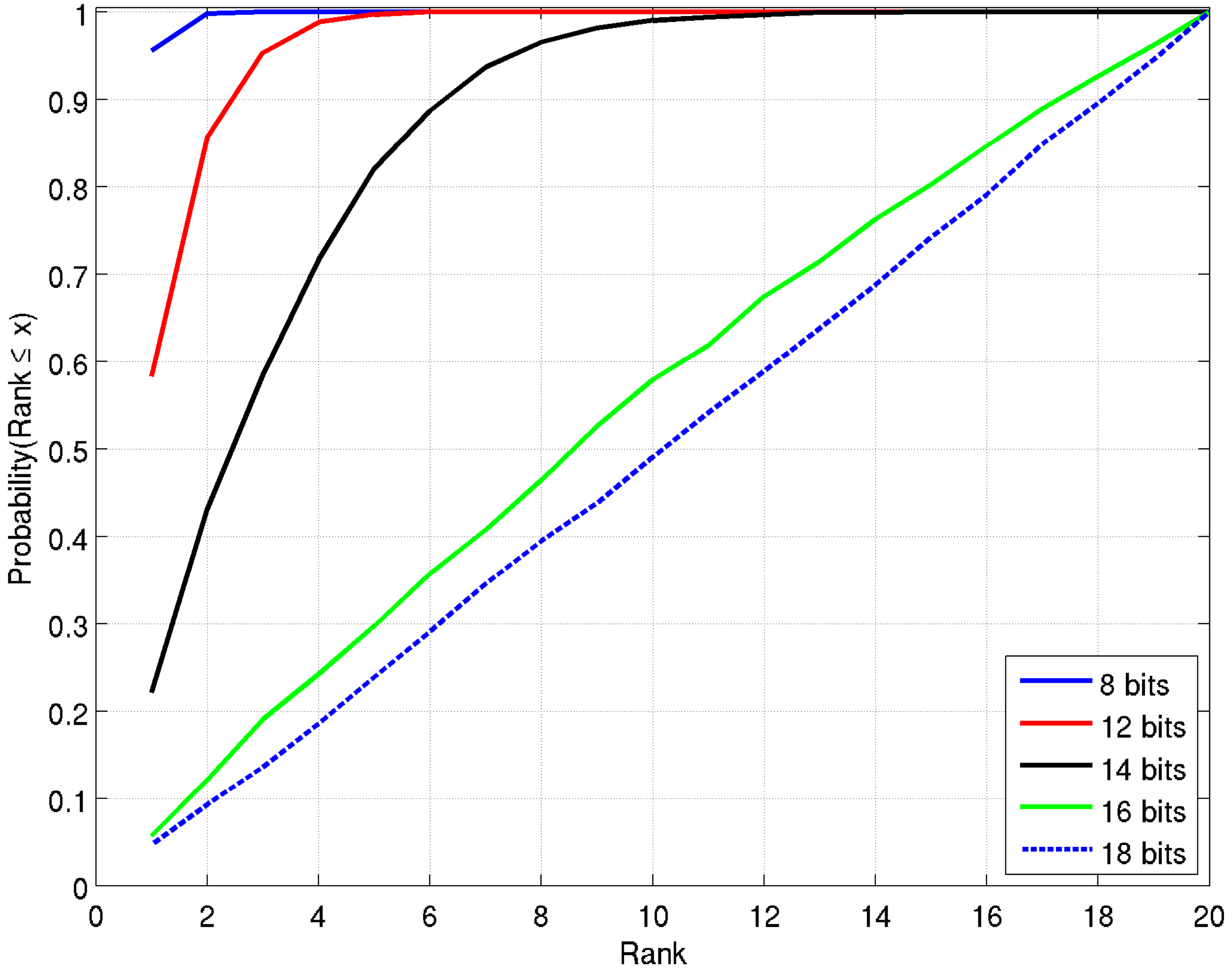
Varying Precision – 100 Vehicles without Interference



Varying Precision – 20 Vehicles, with Interference



Varying Precision – 20 Vehicles, without Interference

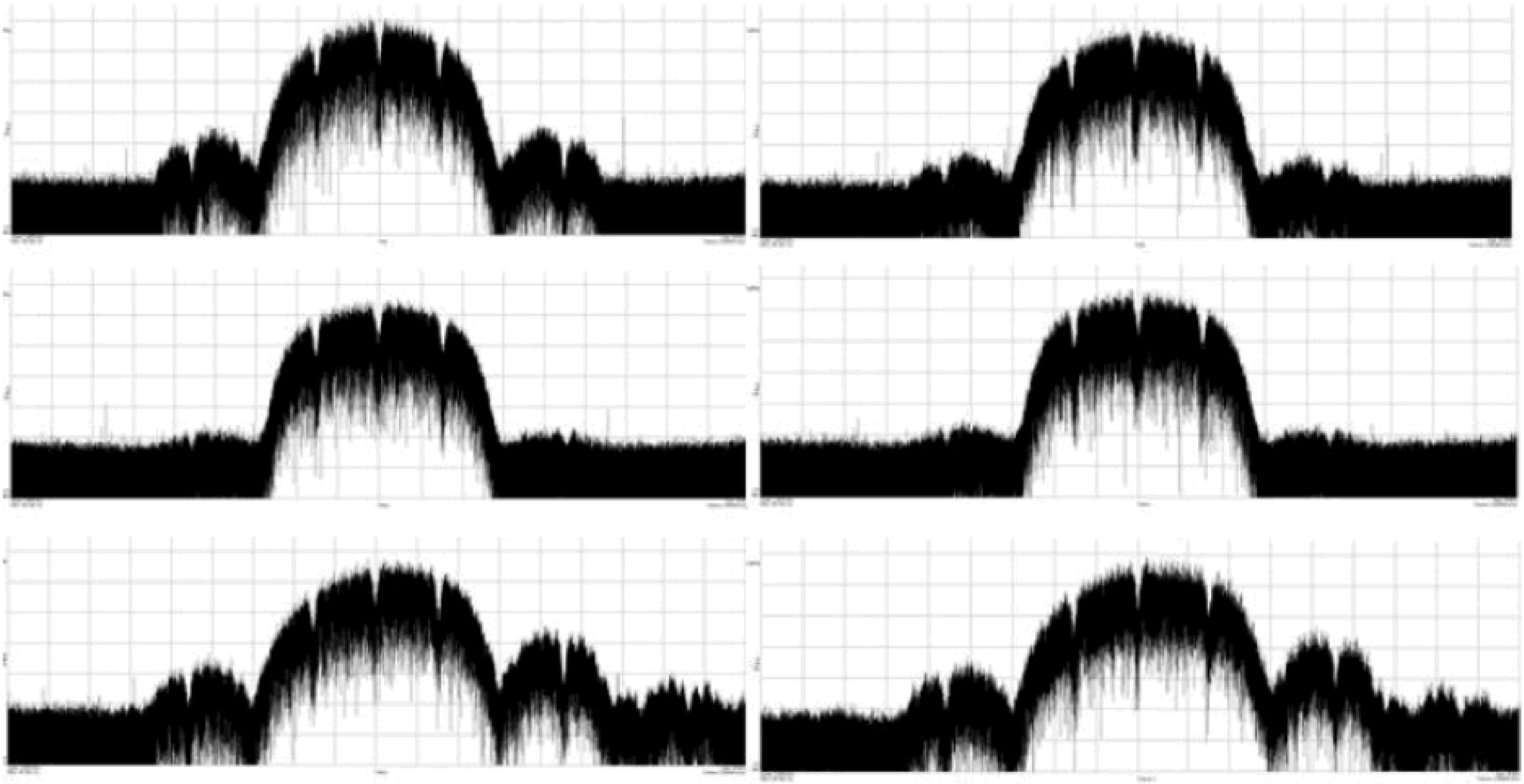


Wireless Fingerprinting – Summary

- Phase noise and interference help if do not require perfect privacy
- Quick drop-off in privacy with fewer bits of precision
- Interference provides asymptotic bound on attacker estimation
- May require 18 bits for identity switching

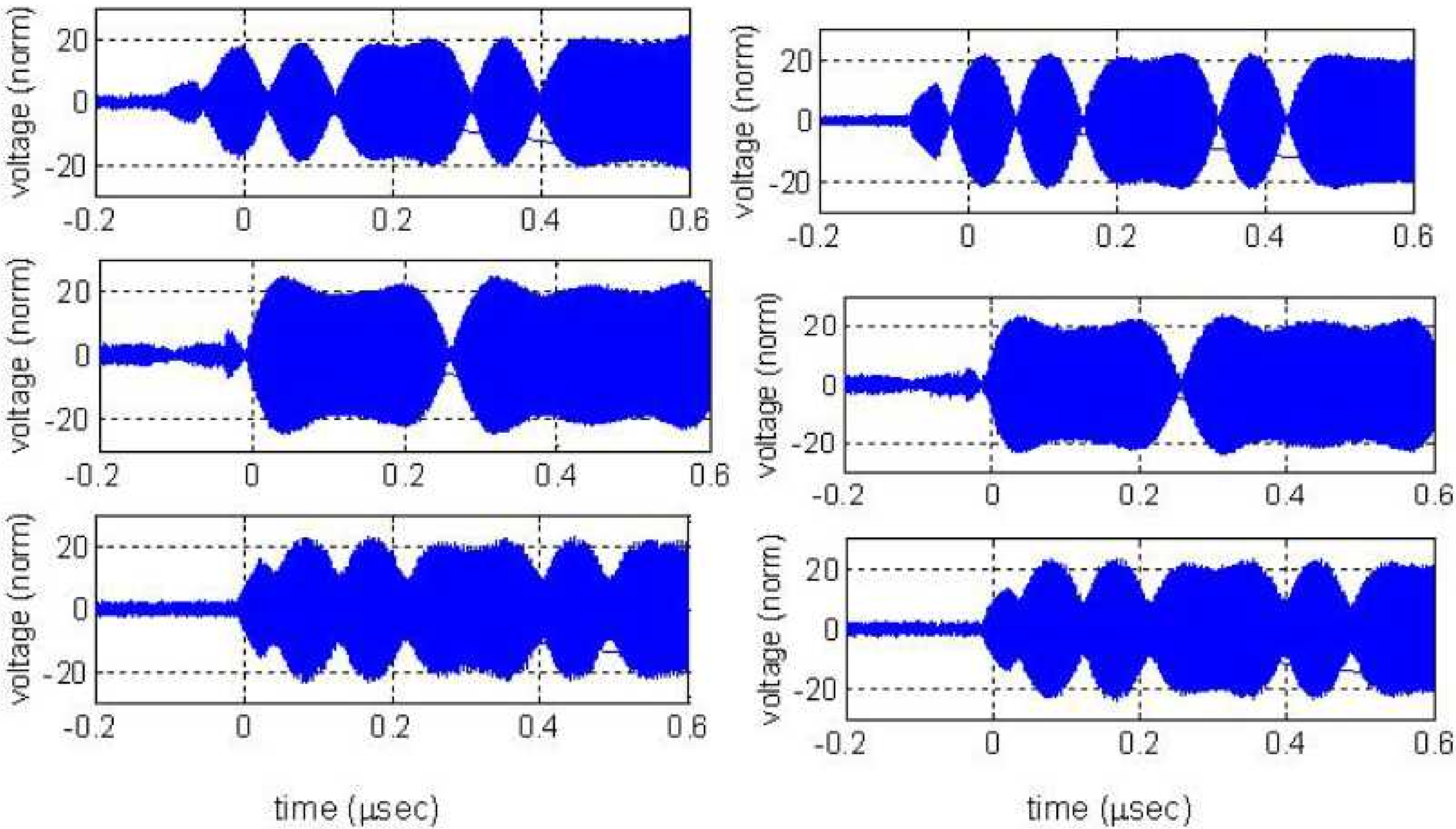
Thanks!

Previous Work – Frequency Domain



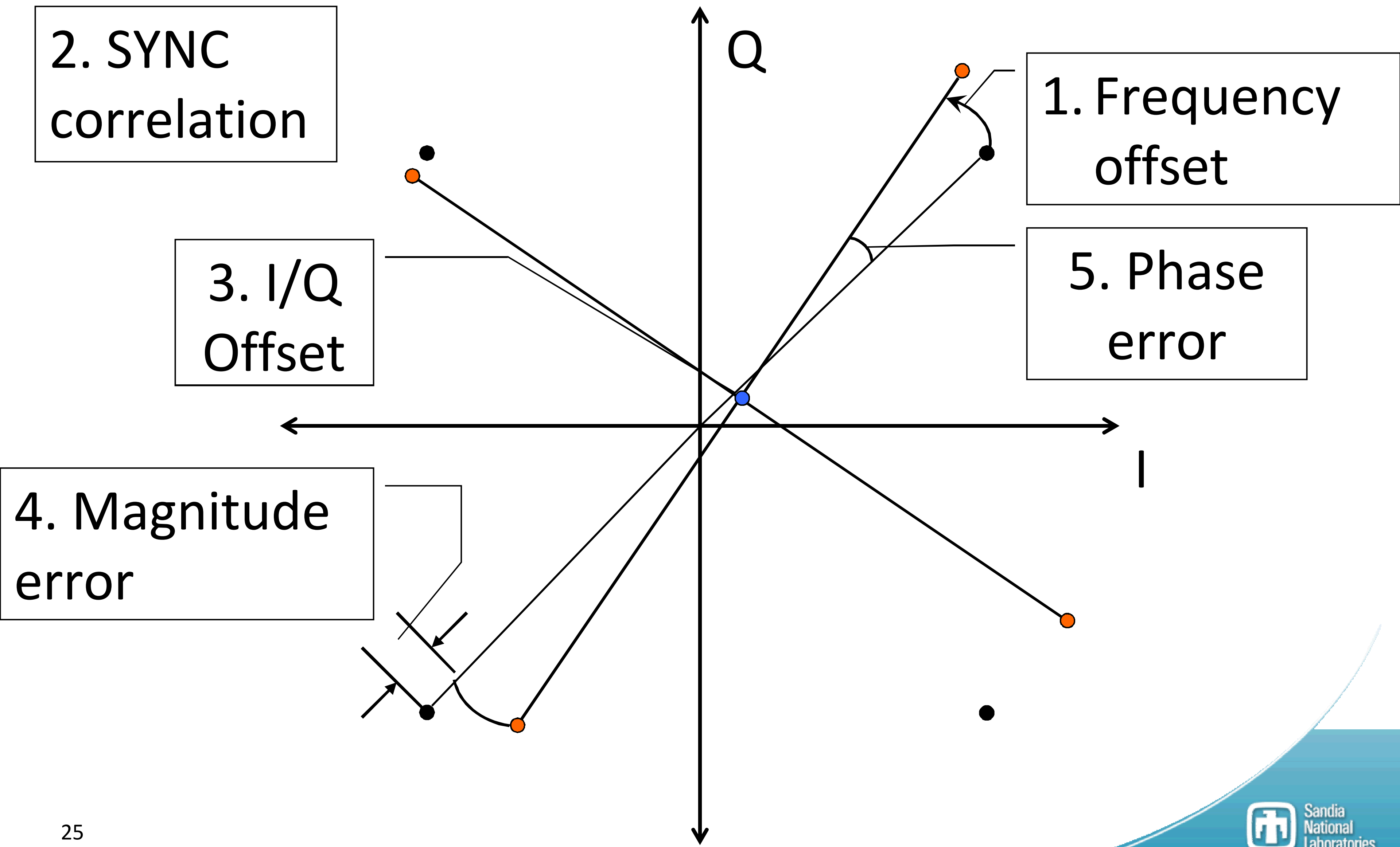
Obtained from Remley et al., “Electromagnetic Signatures of WLAN Cards and Network Security”, 2005 IEEE ISSPIT

Previous Work – Time Domain



Obtained from Remley et al., “Electromagnetic Signatures of WLAN Cards and Network Security”, 2005 IEEE ISSPIT

Previous Work – 5 Features



Previous Work – Edman & Yener, RPI Tech. Report, 2009

- “Real-world” deployment (much cheaper hardware)
- Record using USRP2 software defined radio
- Uncontrolled environment, 3 IBM laptops
- Classifier (same as Brik et al.): 87.5% accurate
- Imitate radios with USRP2: 55% successful

Theory – Attacker Limitations

- Modified Cramer-Rao Bound – bound on attacker's variance (D'Andrea, 1994)

$$\sigma^2 \geq \frac{3}{2\pi^2 {T_0}^3 B} \frac{1}{\mathrm{SNR}}$$