Secure Navigation and Timing Without Local Storage of Secret Keys

Kyle D. Wesson

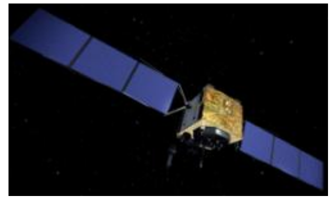
Committee

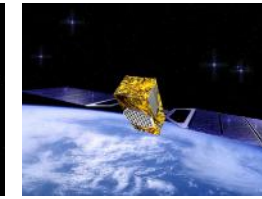
Dr. Todd E. Humphreys (supervisor)
Dr. Brian L. Evans (co-supervisor)
Dr. Ross Baldick
Dr. Lili Qiu
Dr. Ahmed H. Tewfik

Ph.D. Defense | The University of Texas at Austin | 9 April 2014

GNSS: The “Invisible Utility”

GNSS
GPS, GLONASS, Galileo, Compass/Beidou



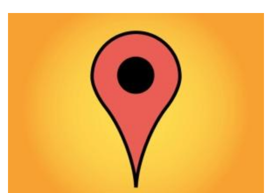
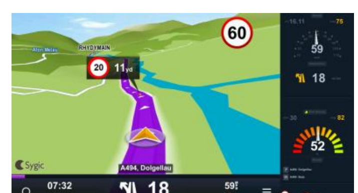
Sectors
Agriculture, Automation, Communication, Defense, Energy, Finance, Safety, Transportation



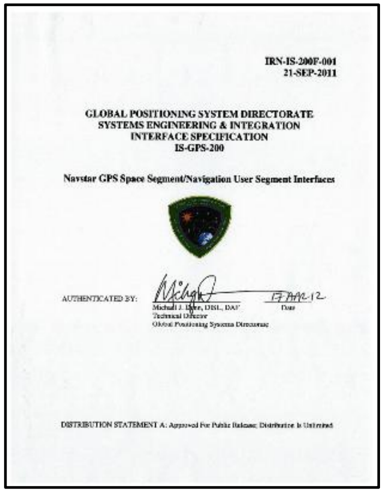




Applications
Position, Navigation, and Timing (PNT)

Civil GPS is Vulnerable to Spoofing



IRN-IS-200F-001
21-SEP-2011

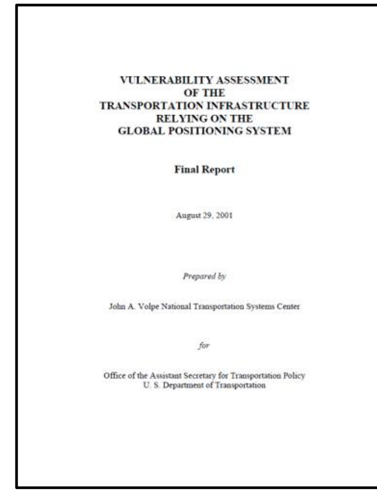
GLOBAL POSITIONING SYSTEM DIRECTORATE
SYSTEMS ENGINEERING & INTEGRATION
INTERFACE SPECIFICATION
IS-GPS-200

Navstar GPS Space Segment/Navigation User Segment Interfaces

AUTHENTICATED BY: [illegible] Date
Technical Director
Global Positioning Systems Directorate

DISTRIBUTION STATEMENT A: Approved For Public Release; Distribution Is Unlimited

An **open access** civil GPS standard makes GPS popular but also renders it vulnerable to **spoofing**



VULNERABILITY ASSESSMENT
OF THE
TRANSPORTATION INFRASTRUCTURE
RELYING ON THE
GLOBAL POSITIONING SYSTEM

Final Report

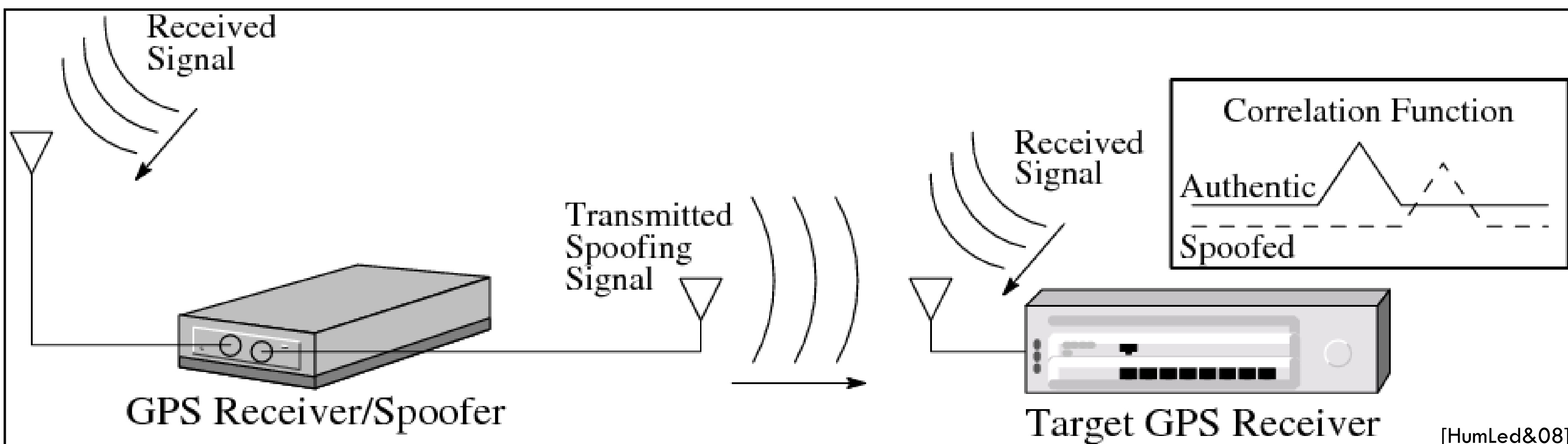
August 29, 2001

Prepared by

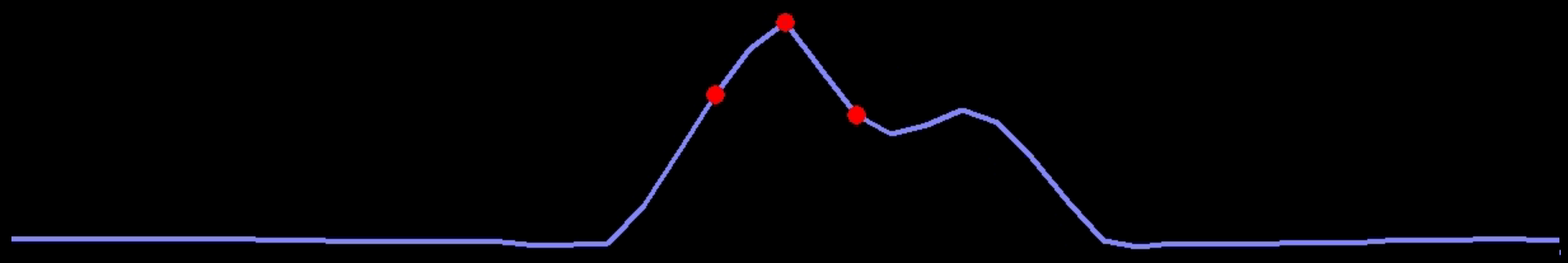
John A. Volpe National Transportation Systems Center

for

Office of the Assistant Secretary for Transportation Policy
U. S. Department of Transportation



Inside a Spoofing Attack



Spoofing Field Attacks

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

Civilian UAV, June 2012

- White Sands Missile Range, NM
- UAV commanded to hover at 12 m
- Spoofer at 620 m standoff distance
- 1 m/s spoofer-induced descent
- Saved from crash by manual override

[KerShe&14]

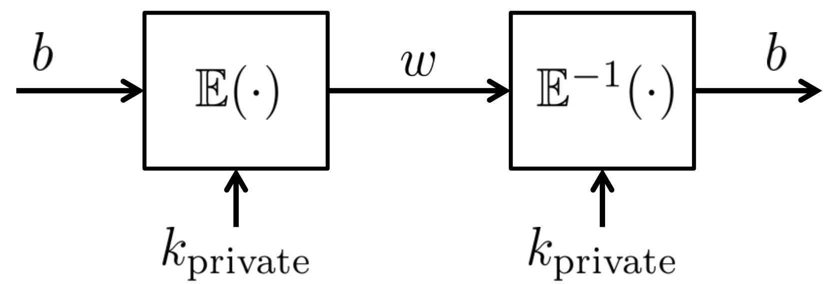
$80M Yacht, July 2013

- Mediterranean Sea
- Yacht sailed straight
- Spoofer at 3 m standoff distance
- Yacht veered off course 10 degrees
- Instantaneous capture without alarms

[BhaHum14]

Military GPS: Symmetric-Key Encryption

- Advantages
  - Near real-time authentication
  - Exclusive user group
  - Low computational cost to decrypt
- Disadvantages
  - Burdensome key management
  - Tamper resistant hardware
  - Trusted foundries increase cost
  - Expensive, inconvenient receivers



[USAF]

Thesis Statement

Both cryptographic and non-cryptographic **anti-spoofing techniques can secure civil GPS** and GNSS navigation and timing while **avoiding the serious drawbacks of local storage of secret cryptographic keys** that hinder military symmetric-key-based anti-spoofing.

Contributions: "Secure Navigation and Timing Without Local Storage of Secret Keys"

theory

technology

policy

Probabilistic Anti-Spoofing Framework

- Explain insufficiency of traditional data authentication
- Establish necessary security checks across network layers

GPS Spoofing Detection via Composite Hypothesis Testing

- Explain and exploit power–distortion tradeoff
- Illustrate composite hypothesis testing strategy against simulated and experimental data

Asymmetric Cryptographic GNSS Signal Authentication

- Develop backward compatible authentication scheme
- Propose practical and effective strategy to embed public key signature in GPS L2 or L5 CNAV message

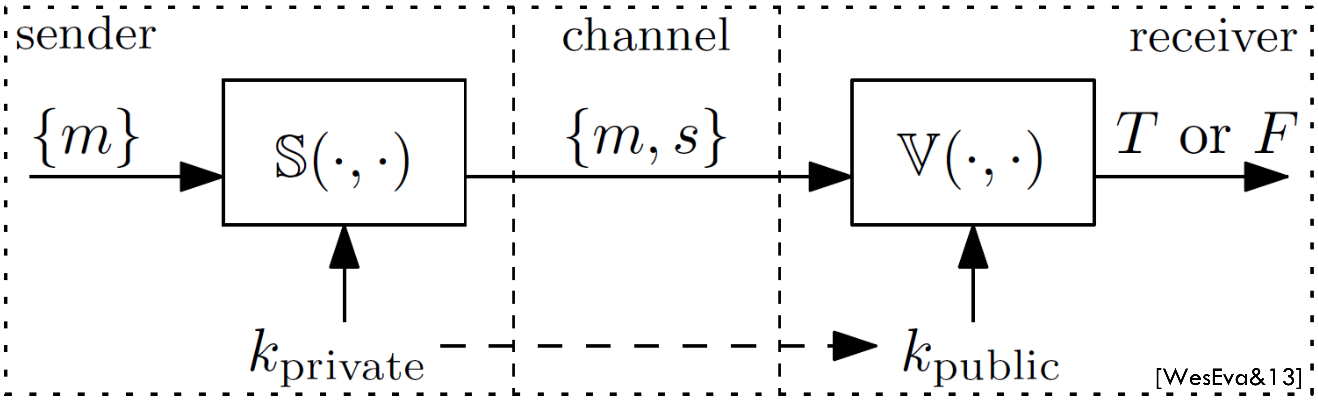
Case Study: Secure Navigation for Aviation

[for closed door session due to time constraints]

Probabilistic Anti-Spoofing Security Framework

Data Message Authentication

- Data message authentication predicated on
  - Performing brute-force search for secret key
  - Reversing one-way hash functions
- U.S. NIST measures cryptographic security in *years* [FIPS 186-3]
  - 128-bit symmetric-key-equivalent key strength secure beyond year 2030



Takeaway: $P_D \approx 1$ and $P_F \approx 0$

Security-Enhanced GPS Signal Model

$$
\begin{aligned}
Y_k &= \beta_{\mathrm{AGC}}[w_k \overbrace{c_k \cos(2\pi f_{\mathrm{IF}} t_k + \theta_k)}^{s_k} + N_k] \\
&= \beta_{\mathrm{AGC}} \left(w_k s_k + N_k \right)
\end{aligned}
$$

- Received spread spectrum signal Y_k
  - Automatic gain control β_{AGC}
  - Spreading code c_k
  - Carrier $\cos(2\pi f_{IF} t_k + \theta_k)$
- Security code w_k with period T_w
  - Generalization of binary modulating sequence
  - Either fully encrypted or contains periodic authentication codes
  - Unpredictable prior to broadcast
  - Cryptographically verifiable after broadcast

[WesRot&12], [Hum12]

Attacking Security-Enhanced GPS Signals

1. **Record and Playback or "Meaconing":**
   record and re-broadcast radio frequency spectrum

$$Y_k = \beta_{\mathrm{AGC}} \left(\alpha w_{k-d} s_{k-d} + N_{m,k} + w_k s_k + N_k \right)$$

re-broadcast with delay d and amplitude α — authentic signal

2. **Security Code Estimation and Replay (SCER) Attack:**
   estimate security code in real-time

$$Y_k = \beta_{\mathrm{AGC}} \left(\alpha \hat{w}_{k-d} s_{k-d} + w_k s_k + N_k \right)$$

security code estimate $\hat{w}$ — authentic signal

d can vary per satellite

[WesRot&12], [Hum12]

Can $\mathbb{V}$ Authenticate GNSS Signals?

- Consider a replay attack where spoofer has significant amplitude advantage $\alpha \gg 1$

$$
\begin{aligned}
Y_k &= \beta_{\mathrm{AGC}}(\alpha w_{k-d} s_{k-d} + N_{m,k} + w_k s_k + N_k) \\
&\approx w_{k-d} s_{k-d} + \tilde{N}_k
\end{aligned}
$$

- **But!**

$$\mathbb{V}(w_{k-d}, k_{\mathrm{public}}) = \mathrm{TRUE}$$

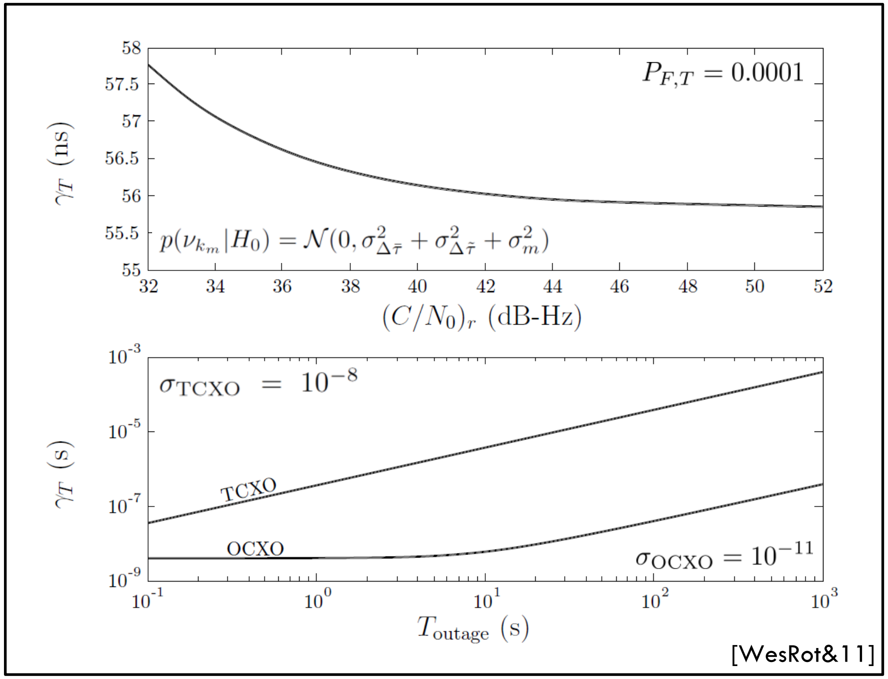
- Spoofer-induced delay undetectable
- Spoofer need not read or manipulate data to deceive receiver

$\mathbb{V}$ **cannot authenticate** GNSS signals because it cannot authenticate **signal arrival time**!

Authentication Components (1/2)

Timing Consistency Check

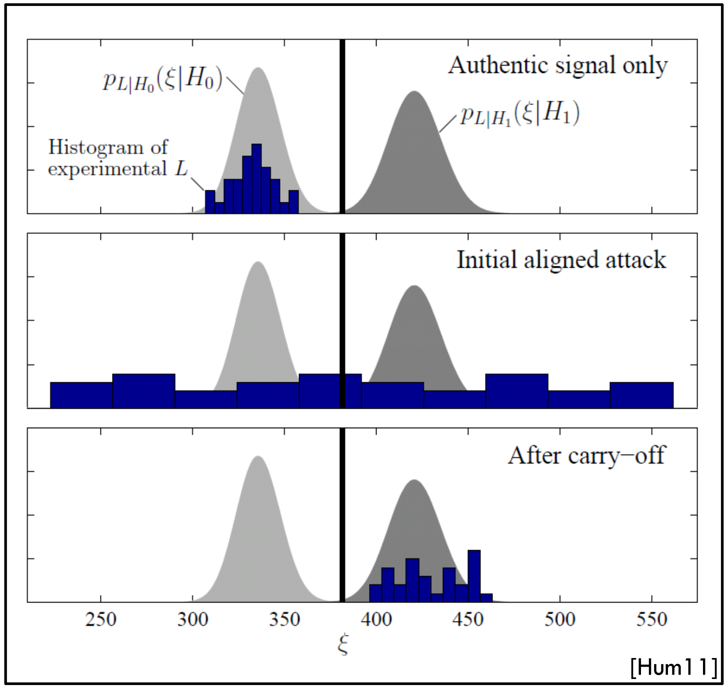
- **Hypothesis test** on difference between received and predicted code phase of spreading code



[WesRot&11]

Security Code Estimation and Replay (SCER) Detector

- **Hypothesis test** at physical layer to detect if security code arrived intact and promptly relative to local clock

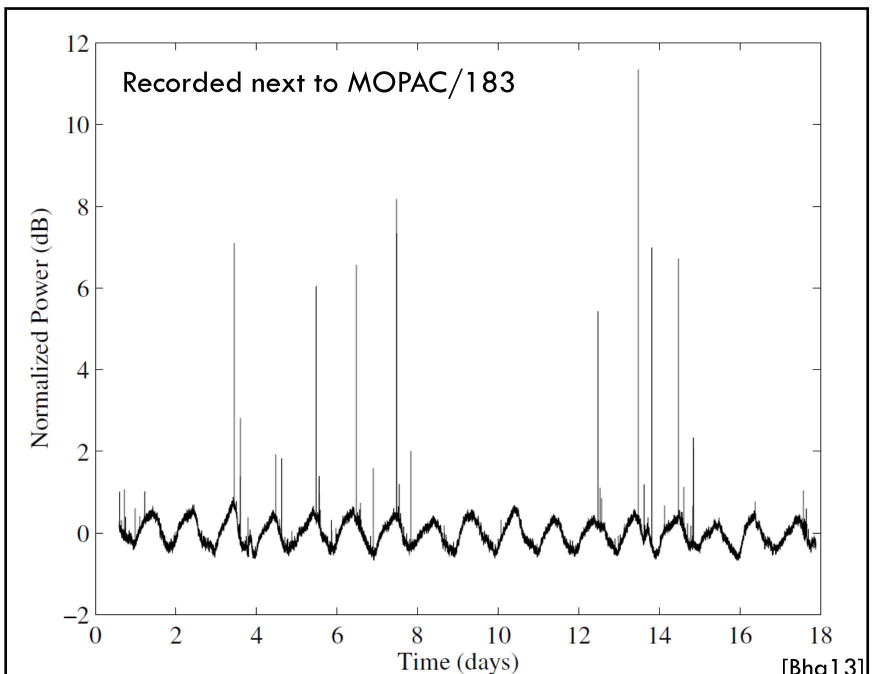


[Hum11]

Authentication Components (2/2)

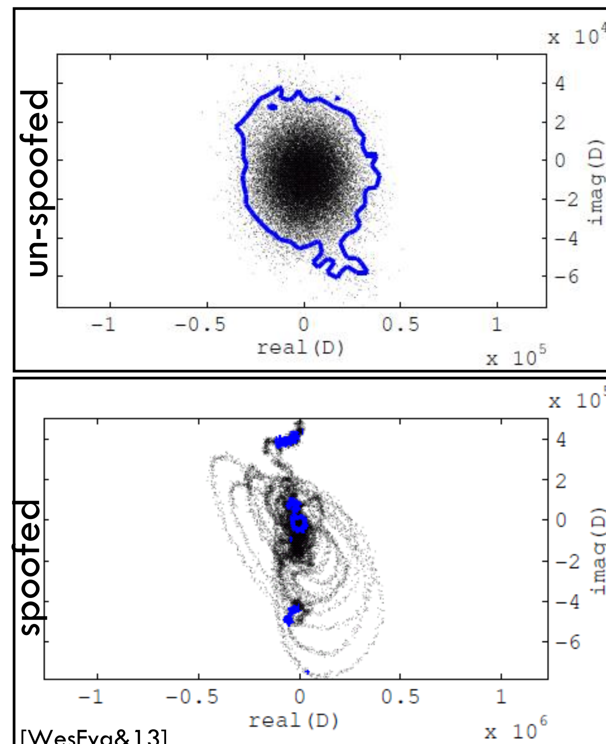
Total In-Band Power Monitor

- **Hypothesis test** on measured power
- Can ensure SCER detector operating assumption that $\eta \leq 4\,\mathrm{dB}$



Statistical Distortion Monitor

- **Statistical measure** of deviations caused by interaction of authentic and spoofing signals



Probabilistic Anti-Spoofing Framework

- Measurement combines cryptographic & non-cryptographic checks

$$\boldsymbol{z} = [\overline{\mathbb{V}} \wedge E, \nu, L, P_T, D]^T \qquad P_F = \int_\gamma^\infty p_{\boldsymbol{z}|H_0}(\boldsymbol{\xi}|H_0)d\boldsymbol{\xi} \qquad P_D = \int_\gamma^\infty p_{\boldsymbol{z}|H_1}(\boldsymbol{\xi}|H_1)d\boldsymbol{\xi}$$

- Extensible to multiple hypotheses (multipath, spoofing, jamming, …)

- Challenges
  - deriving closed form $p_{\boldsymbol{z}|H_j}(\boldsymbol{\xi}|H_j)$
  - differentiating between hypotheses (multipath vs. spoofing)

Subsequent contributions illustrate framework for practical cryptographic and non-cryptographic techniques

GPS Spoofing Detection via Composite Hypothesis Testing

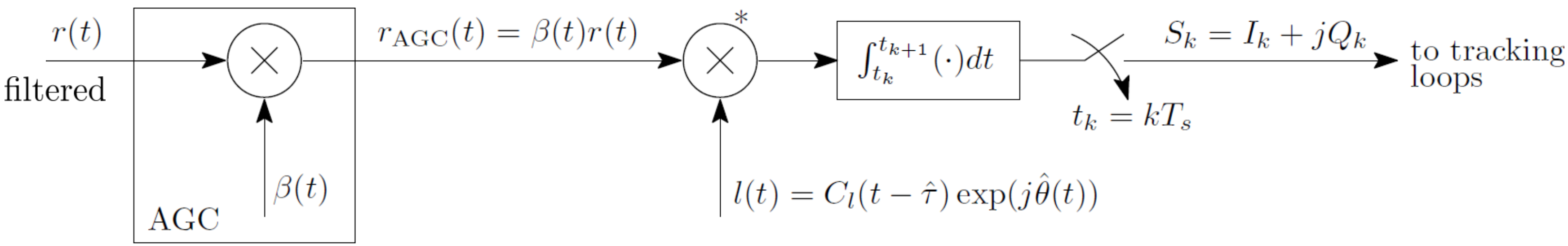
Non-Cryptographic Anti-Spoofing Overview

- Non-cryptographic techniques are enticing because they require no modification to GPS signal

	Non-Cryptographic Method	Extra Hardware	False Alarm Rate	Requires Motion	Increase Size	Addnl. Signals	Effective-ness
1	In-Band Power	No	High	No	No	No	Med
2	Sensor Diversity	Yes	Low	No	No	Yes	High
3	Single-Antenna Spatial Correlation	Yes	Low	Yes	No	No	High
4	Correlation Profile Anomaly Detection	No	High	No	No	No	Med
5	Multi-Element Antenna	Yes	Low	No	No	No	High
6	Distributed Antennas	Yes	Low	No	Yes	No	Med

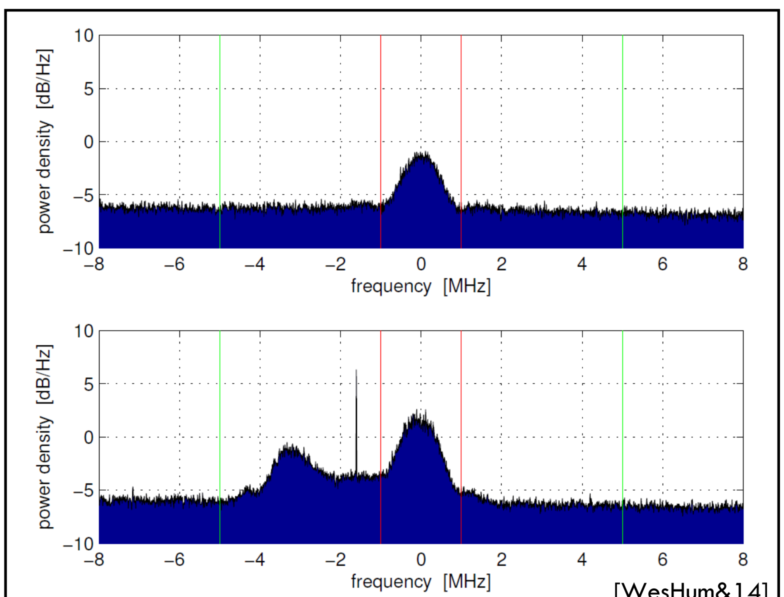
1- [Sco10], [DehNie&12], [Ako12]; **2**- [HumBha&10]; **3**- [BroJaf&12], [PsiPow&13]; **4**- [Phe01], [LedBen&10] , [MubDem10], [CavMot&10], [WesShe&11] , [WesShe&12], [GamMot&13]; **5**- [DeLGau&05], [Bor13]; **6**- [MonHum&09], [SwaHar13]

Receiver Measurements



Total In-Band Power Measurement

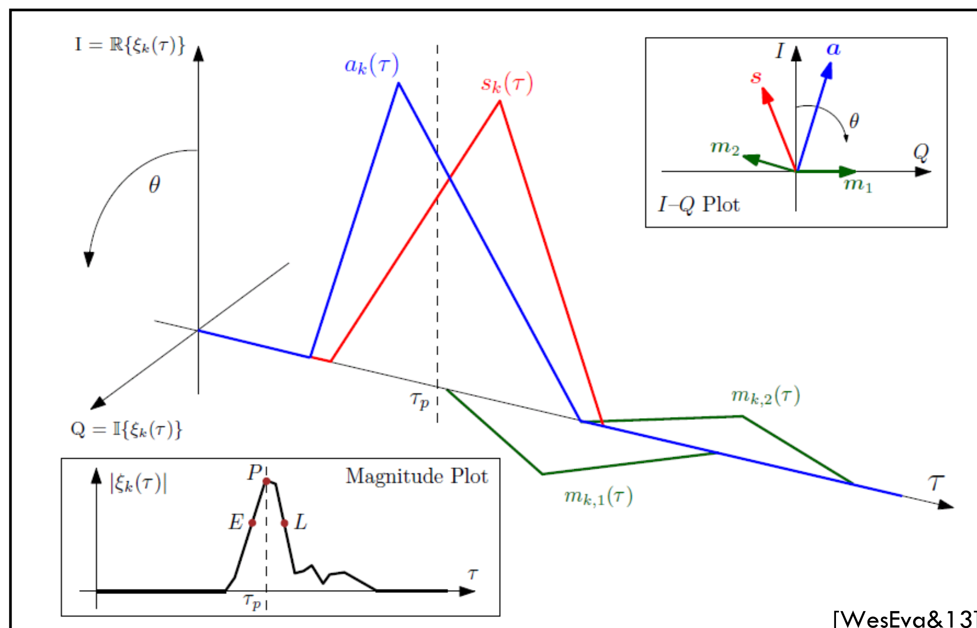
$$P_k = \lim_{T\to\infty} \frac{1}{T} \int_{-T/2}^{T/2} |r(t)|^2 dt$$



[WesHum&14]

Symmetric Difference Measurement

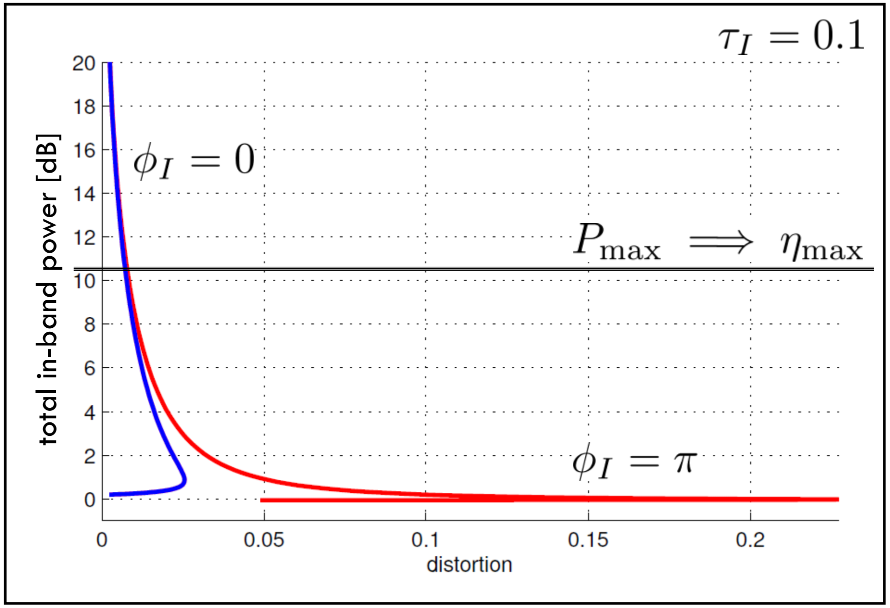
$$D_k^i(\tau_d) \triangleq |\xi_k^i(\tau_p - \tau_d) - \xi_k^i(\tau_p + \tau_d)|.$$



[WesEva&13]

Key Insight: Power—Distortion Tradeoff

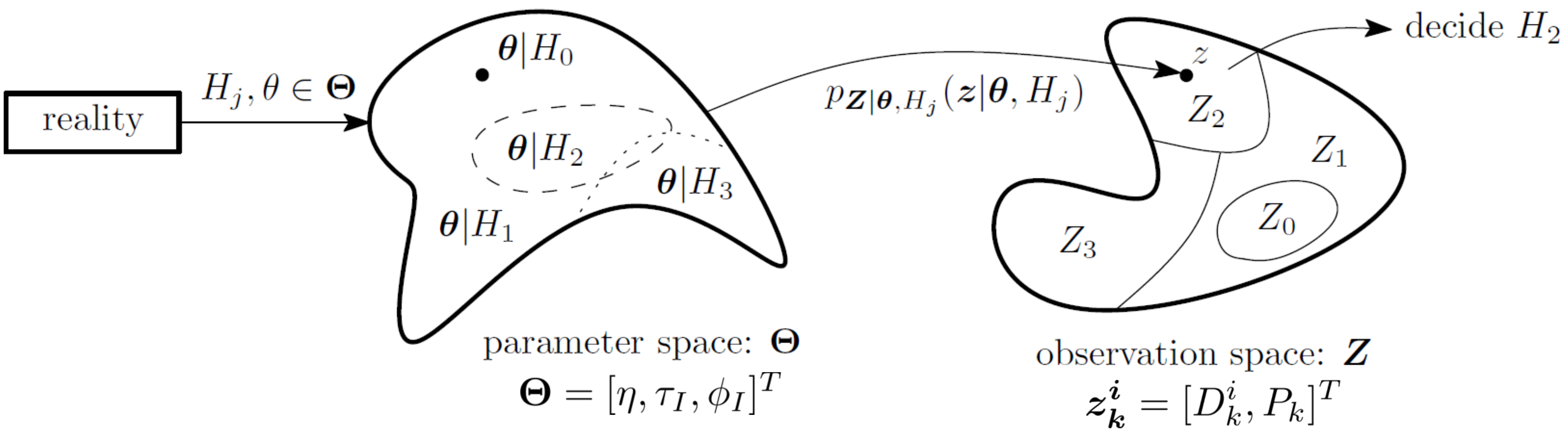
- Admixture of authentic and spoofed signals causes distortions in correlation function
- Assume spoofer cannot null or block authentic signals
- Consider spoofer's power advantage $\eta \triangleq 10\log_{10}(P_s/P_a)$
  - Successful capture requires $\eta > 0.4$ dB [She12]
  - What happens as $\eta \to \infty$? AGC maintains $E[\,\beta(t)\,|r(t)|^2\,] = 1$



$\eta_{\min} < \eta < \eta_{\max}$ ensures distortion

Composite Hypothesis Testing

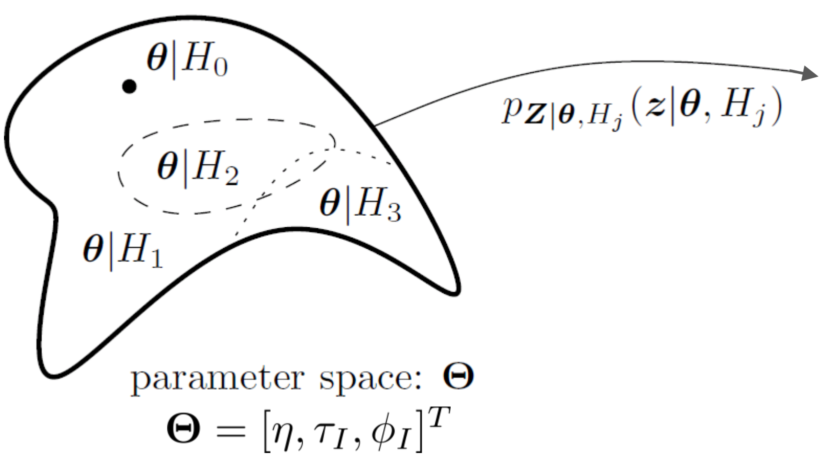
- How do we decide between hypotheses given $\boldsymbol{z}_{\boldsymbol{k}}^{\boldsymbol{i}} = [D_k^i, P_k]^T$?
- How do we represent uncertainty in interference model?



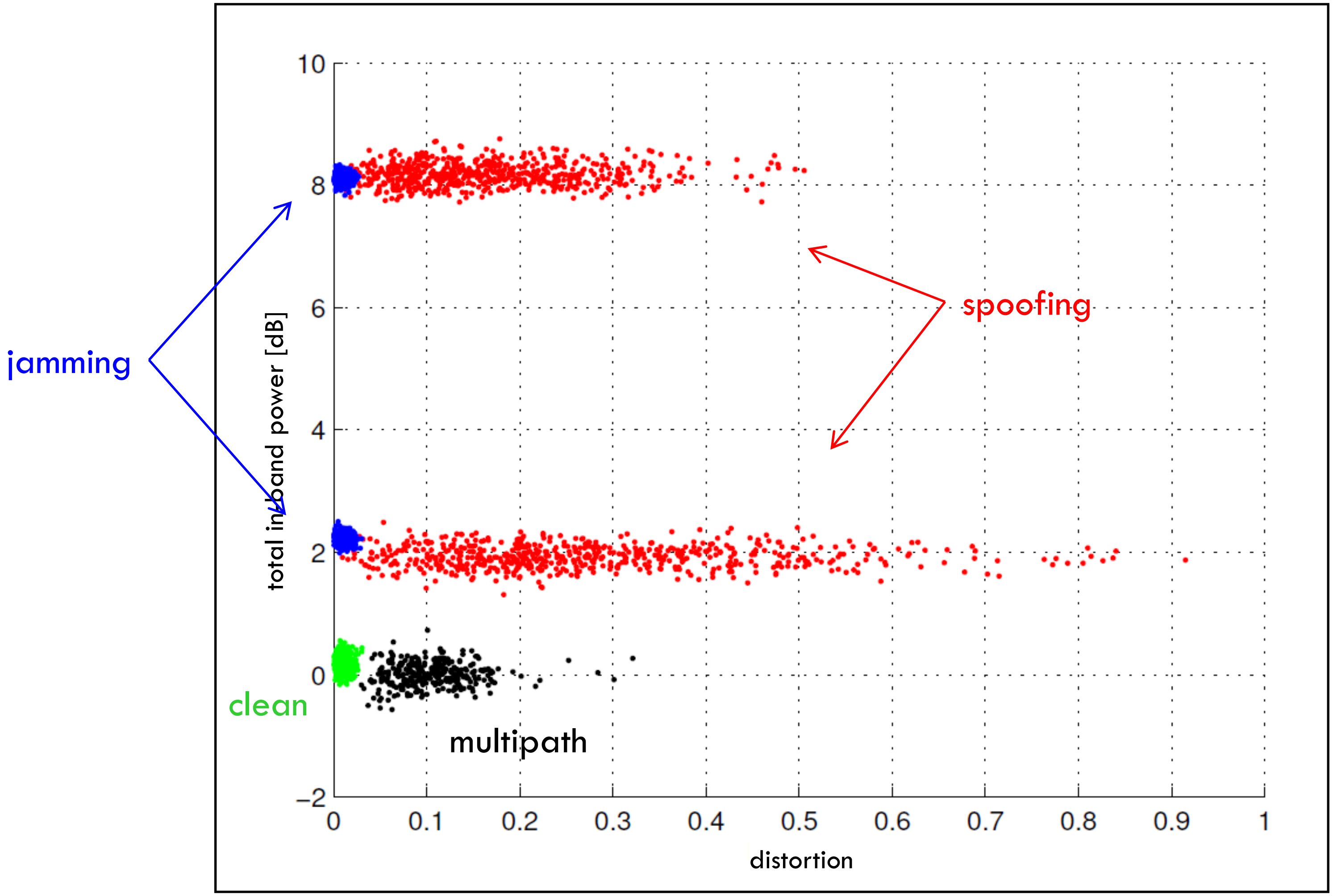
Parameter Space for Single-Interferer

$$r_I(t) = \eta\sqrt{P_a}D(t-\tau-\tau_I)C(t-\tau-\tau_I)e^{j(\phi-\phi_I)}$$

	hypothesis	η	τ_I	ϕ_I
H_1	multipath	$\sim$ Rayleigh	$\sim$ Exponential	$\sim$ Uniform$[0,2\pi]$
H_2	spoofing	$0.4\ \text{dB} \leq \eta$	$\tau \leq \tau_I$	$=0$ (worst case)
H_3	narrowband jamming	$0\ \text{dB} \ll \eta$	$D(\cdot)=C(\cdot)=1$ $\forall t,\tau,\tau_I$	$\sim$ Uniform$[0,2\pi]$

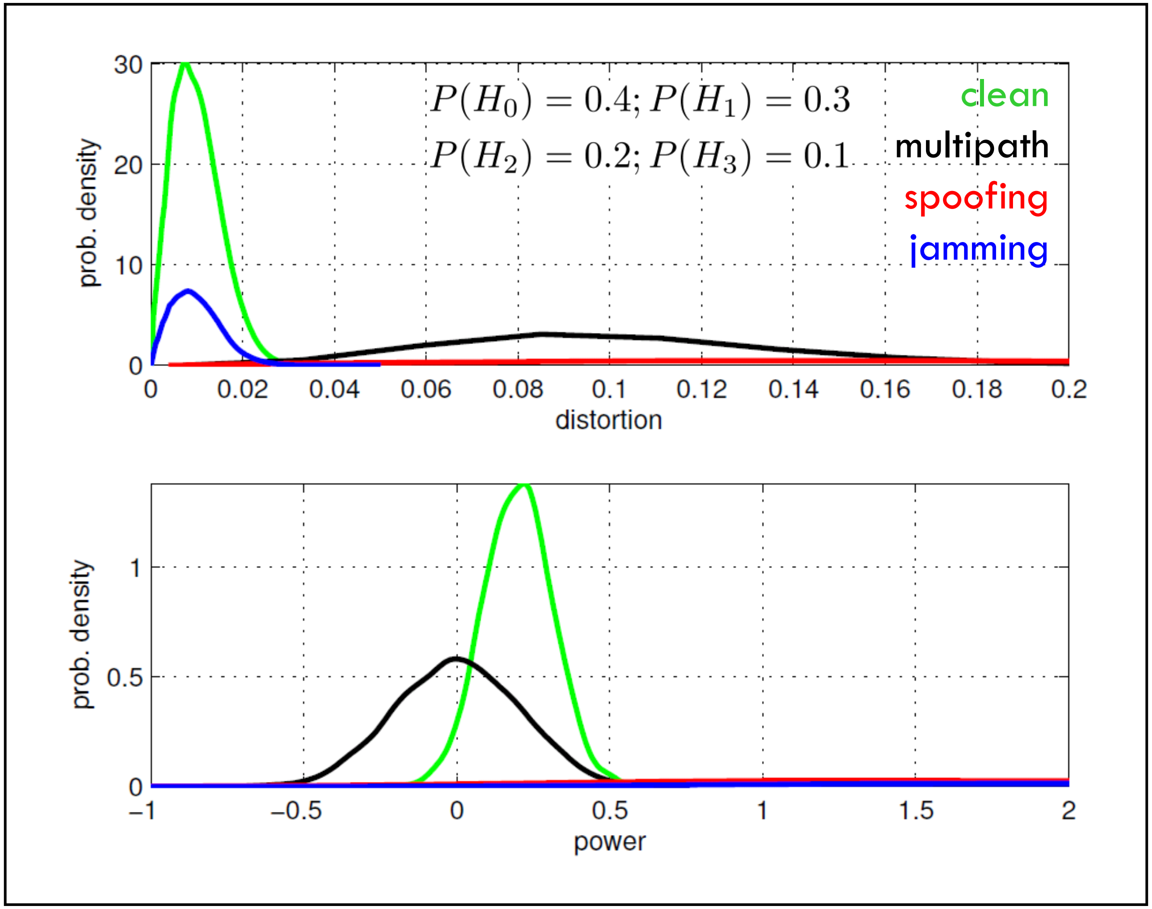


Simulated Observation Space



Simulated Observation Space

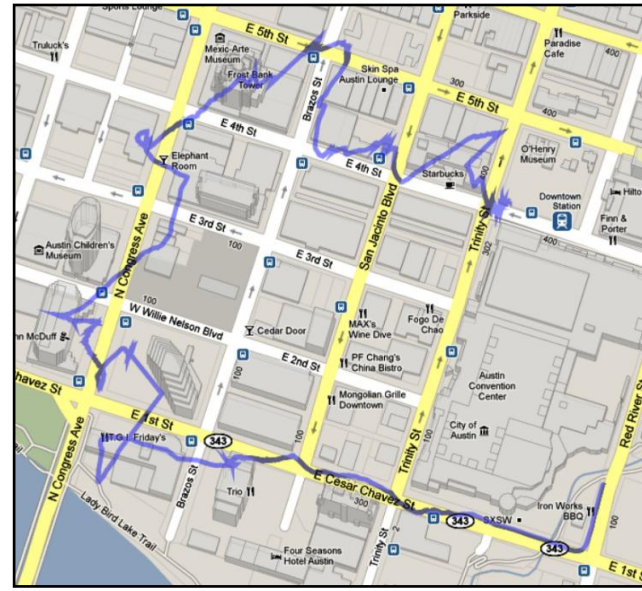
- Weighted marginals of simulated probability space reveal difficulty of detection based on distortion or power alone

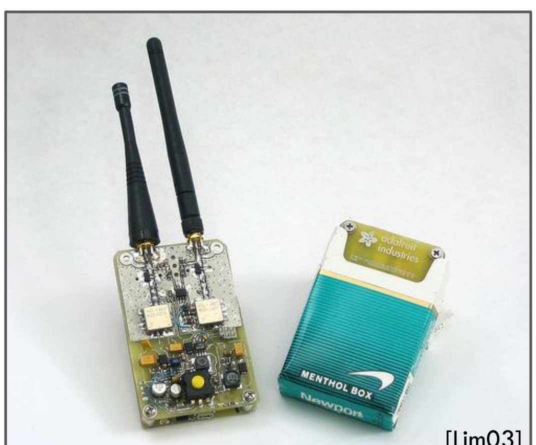


Experimental Data

THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

1. ATX wardriving campaign, 2010
   - Static and dynamic tests in deep urban multipath environments
2. Jammer characterization, 2011 [MitDou&11]
   - 18 "personal privacy device" recordings
3. Texas Spoofing Test Battery, 2012 [HumBha&12]
   - **Only** publicly-available spoofing dataset



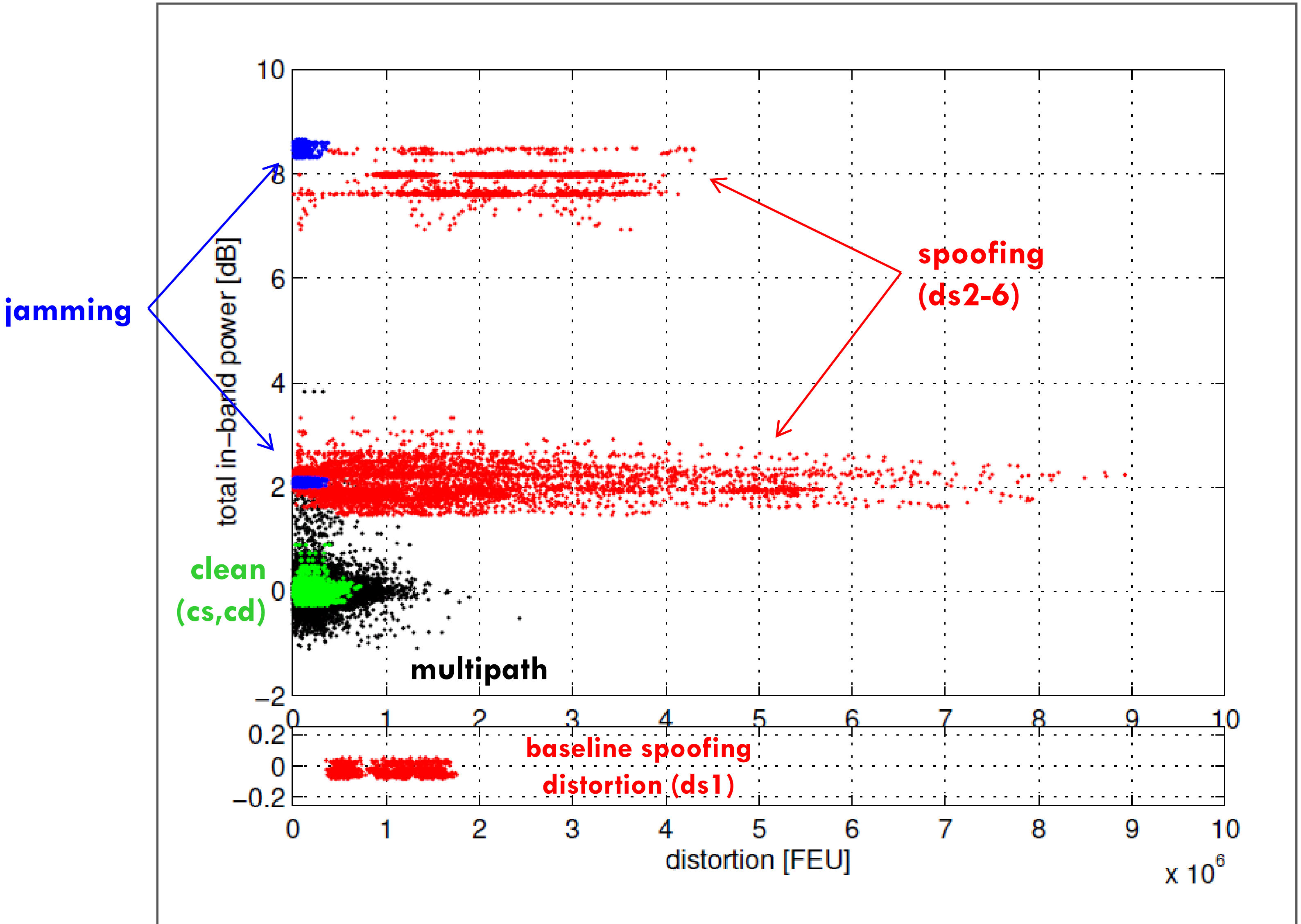


[Lim03]

TEXBAT

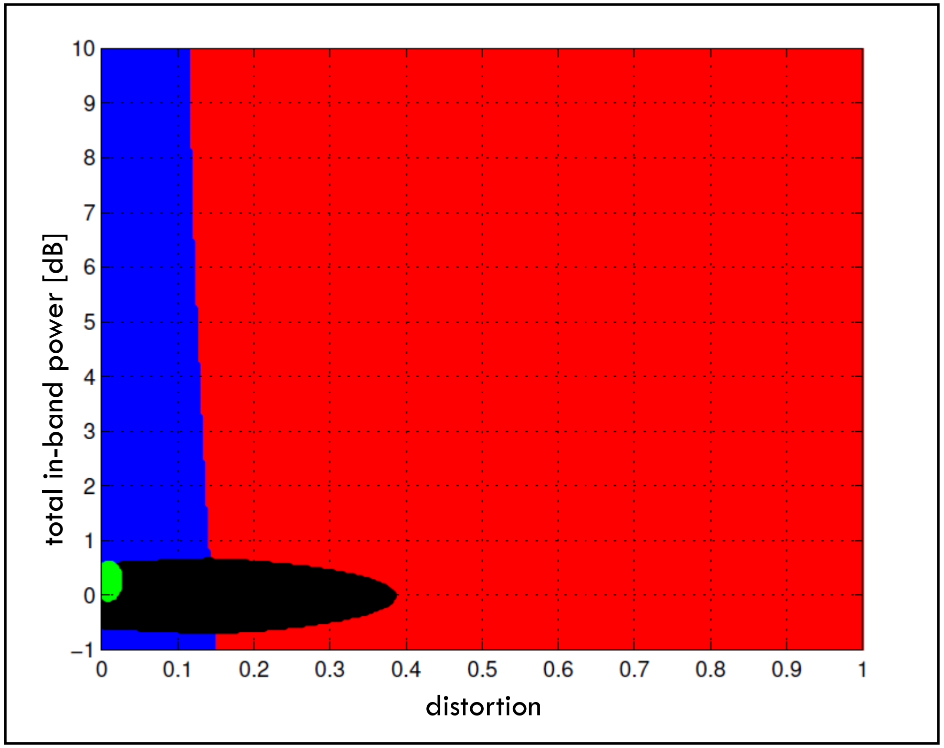
Scenario Designation	Spoofing Type	Platform Mobility	Power Adv. (dB)
1: Static Switch	N/A	Static	N/A
2: Static Overpowered Time Push	Time	Static	10
3: Static Matched-Power Time Push	Time	Static	1.3
4: Static Matched-Power Pos. Push	Position	Static	0.4
5: Dynamic Overpowered Time Push	Time	Dynamic	9.9
6: Dynamic Matched-Power Pos. Push	Position	Dynamic	0.8

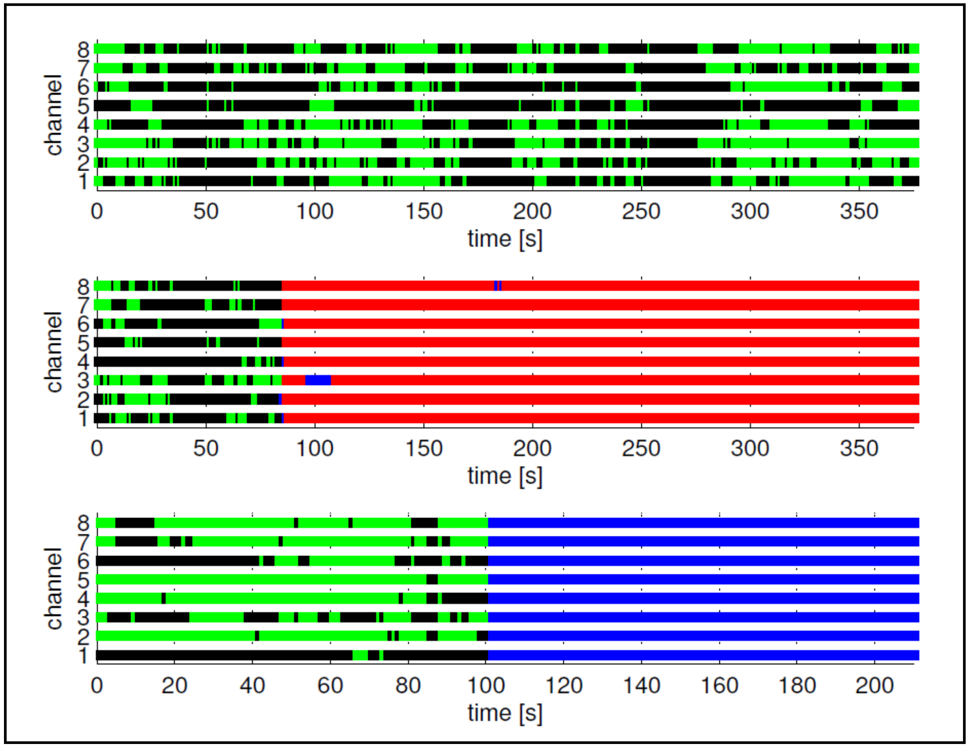
Experimental Observation Space



Decision Regions and Performance

- Attack detection within three seconds
- $P_F = 0.0044$ and $P_D = 0.999$ (overall attack vs. no-attack metrics)
- Allows for time-varying cost and prior probabilities



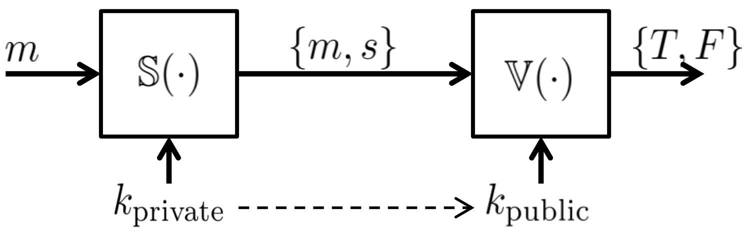


clean multipath spoofing jamming

Asymmetric Cryptographic Signal Authentication

Cryptographic Anti-Spoofing Overview

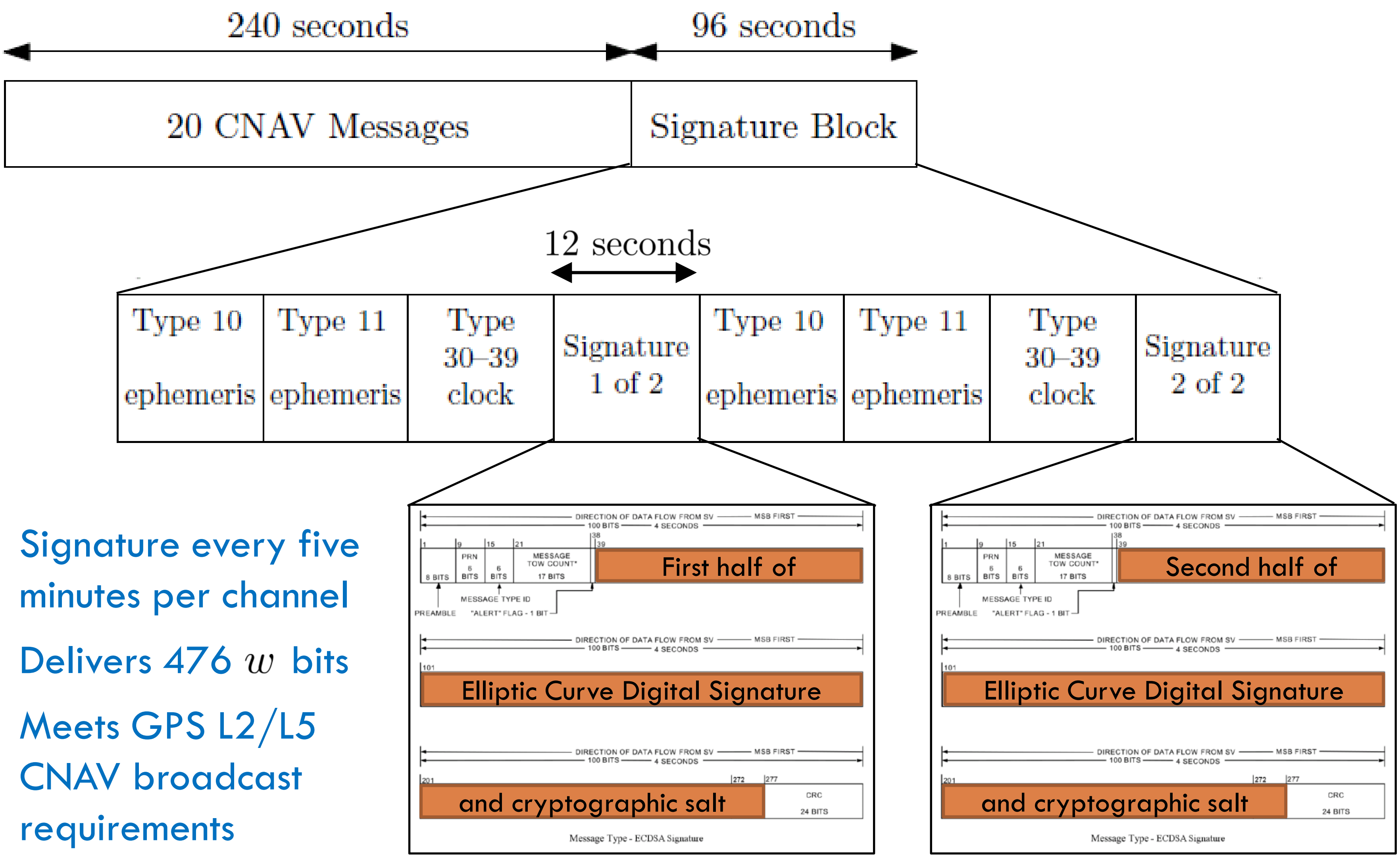
- Techniques require unpredictable bits
- Recall: security code w in security-enhanced signal model



	Cryptographic Anti-Spoofing Technique	Effective-ness	Auth. Rate	Network Conn.	Implement Time	Practical for Civil?
1	Sec. Spread Code (L1C/A)	High	Seconds	No	Years	No
2	Sec. Spread Code (WAAS)	Low	Seconds	No	Years	No
3	Nav. Msg. Auth. (L2/L5)	Med.	Seconds	No	Years	Yes
4	Nav. Msg. Auth. (WAAS)	Low	Minutes	No	Years	Yes
5	Cross Correlation of P(Y)	High	Seconds	Yes	Months	Yes
6	Military GPS P(Y) Signal	High	Real-time	No	Implemented	No

[HeiKne&07B]; **1**- [Sco03]; **2**- [LoEng10]; **3**- [Sco03], [PozWul&04] [WulPoz&05], [WesShe&12], [Hum13]; **4**- [LoEng10]; **5**- [PsiHan&12], [PsiOha13]; **6**- [BarBet&06]

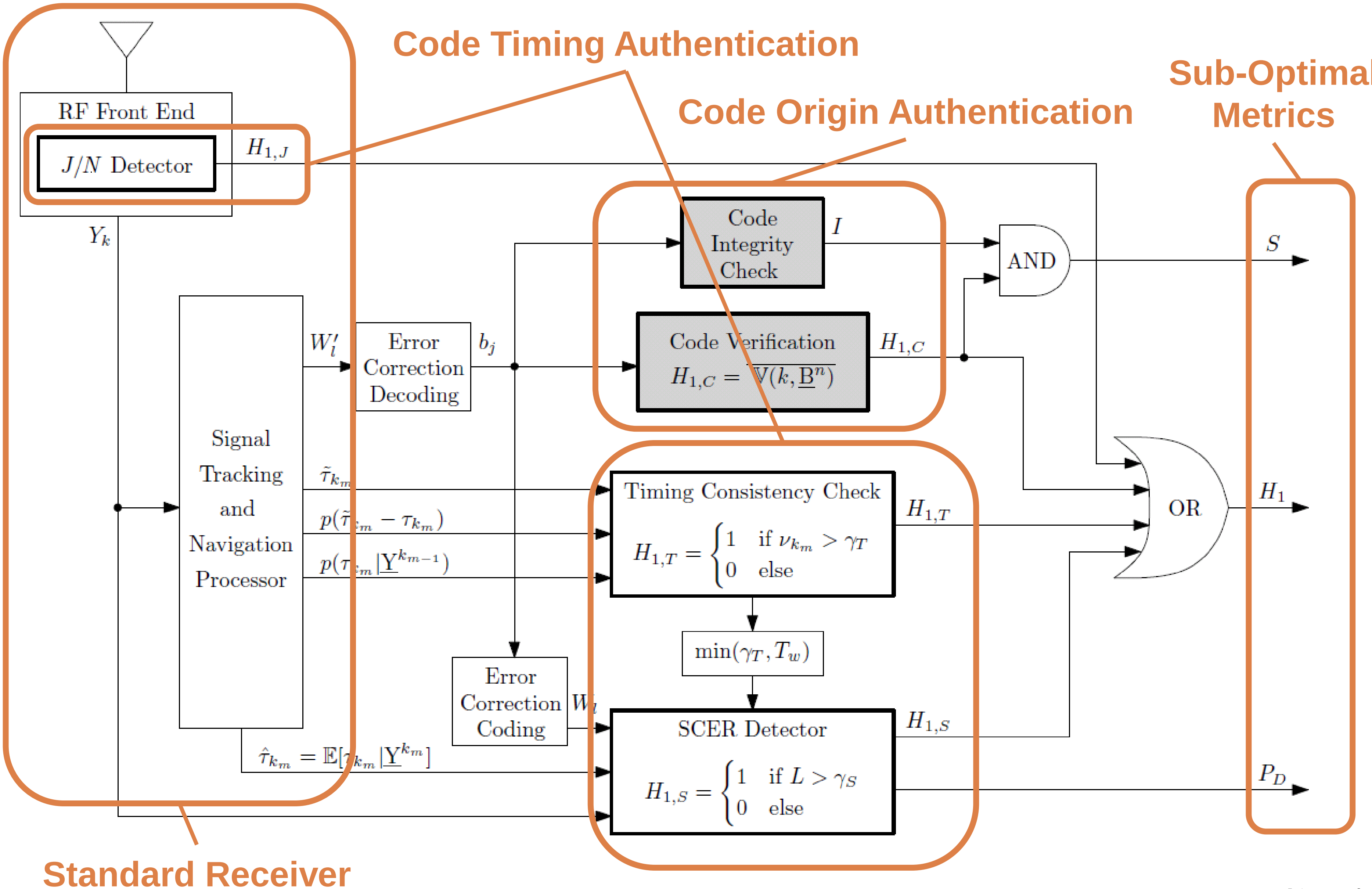
NMA on GPS L2/L5 CNAV



- Signature every five minutes per channel
- Delivers 476 w bits
- Meets GPS L2/L5 CNAV broadcast requirements

[WesRot&12]

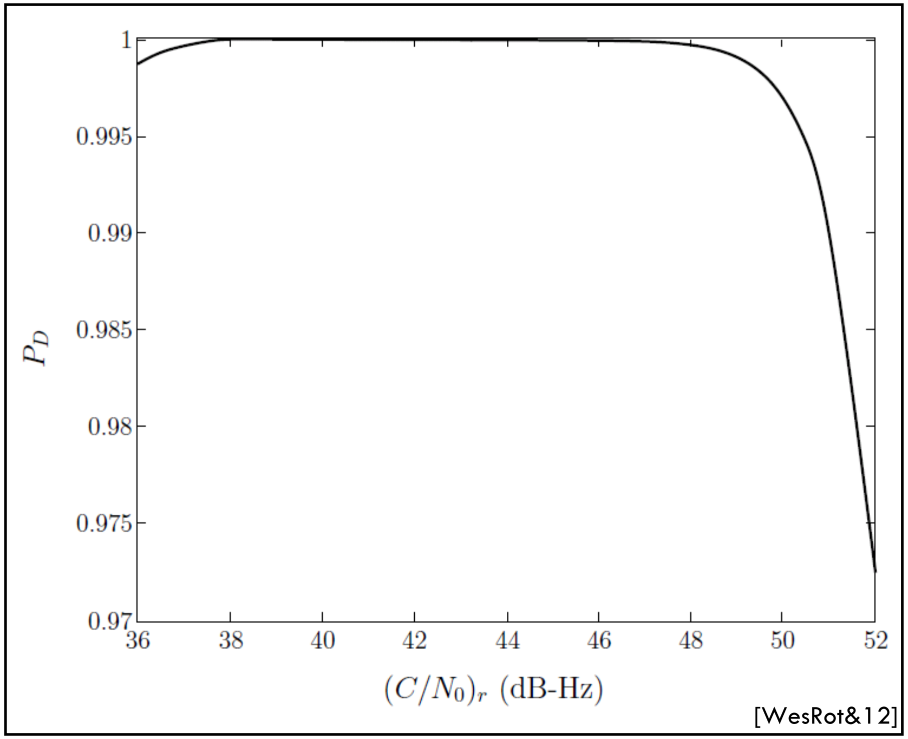
How to Authenticate NMA Signals?



[WesRot&12]

How Effective is this Proposed Defense?

- Challenging SCER attack
  - Spoofer has 3 dB carrier-to-noise ratio advantage
  - Received spoofed signals 1.1 times stronger than authentic signals
  - Spoofer introduces timing error of 1 µs
  - False alarm probability for SCER detector is 0.0001



[WesRot&12]

NMA is highly effective

"Secure Navigation and Timing Without Local Storage of Secret Keys"

theory
technology
policy

Probabilistic Anti-Spoofing Framework

- Explain insufficiency of traditional data authentication
- Establish necessary security checks across network layers

GPS Spoofing Detection via Composite Hypothesis Testing

- Explain and exploit power–distortion tradeoff
- Illustrate composite hypothesis testing strategy against simulated and experimental data

Asymmetric Cryptographic GNSS Signal Authentication

- Develop backward compatible authentication scheme
- Propose practical and effective strategy to embed public key signature in GPS L2 or L5 CNAV message

Case Study: Secure Navigation for Aviation

[for closed door session due to time constraints]