GATEMAN Workshop
8th SESAR Innovation Days

GNSS Jammer Detection and Localization in Aviation

Philipp Richter
[TUT]

Salzburg 3rd December 2018

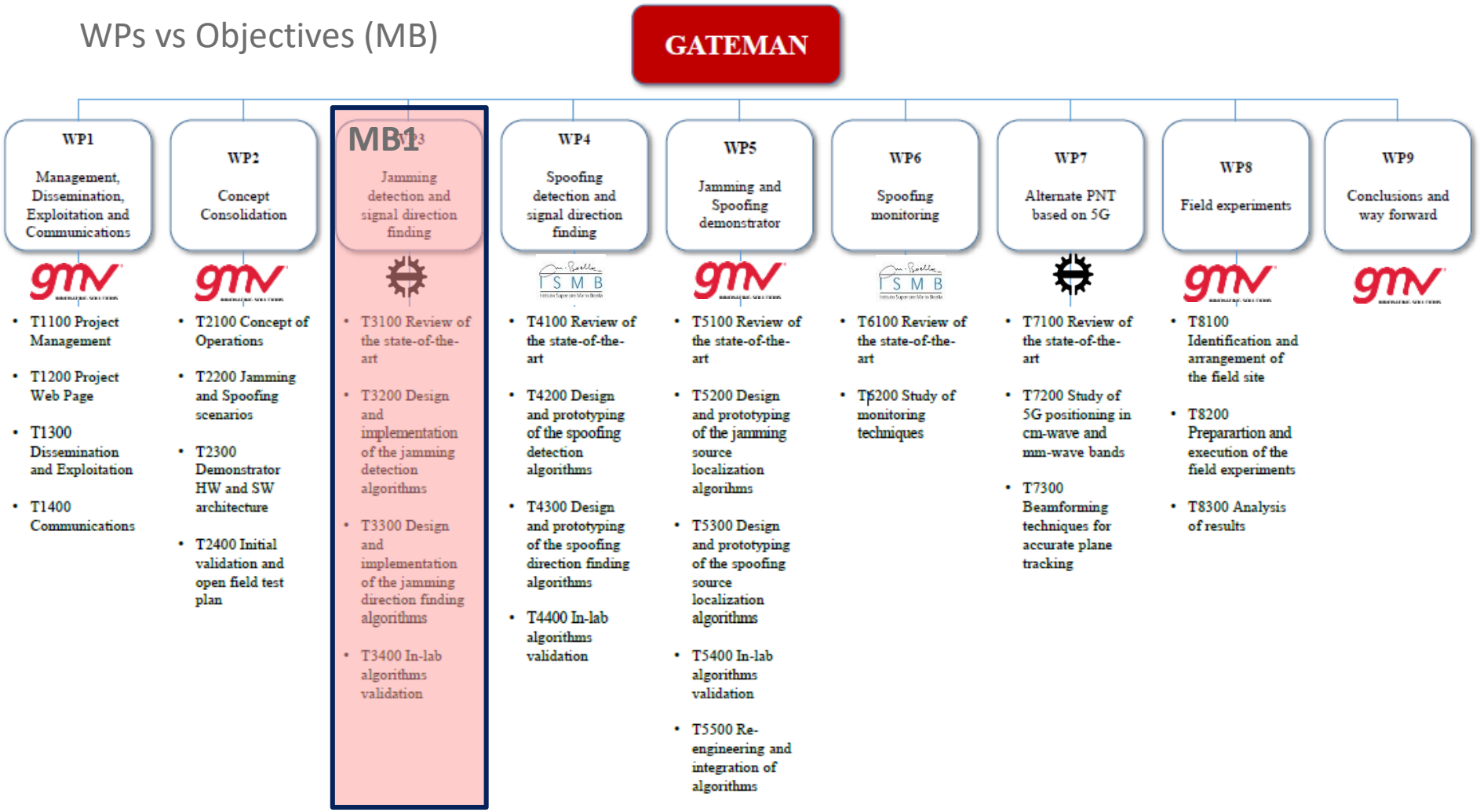
SESAR JOINT UNDERTAKING

Founding Members

EUROPEAN UNION EUROCONTROL

Context in GATEMAN

WPs vs Objectives (MB)

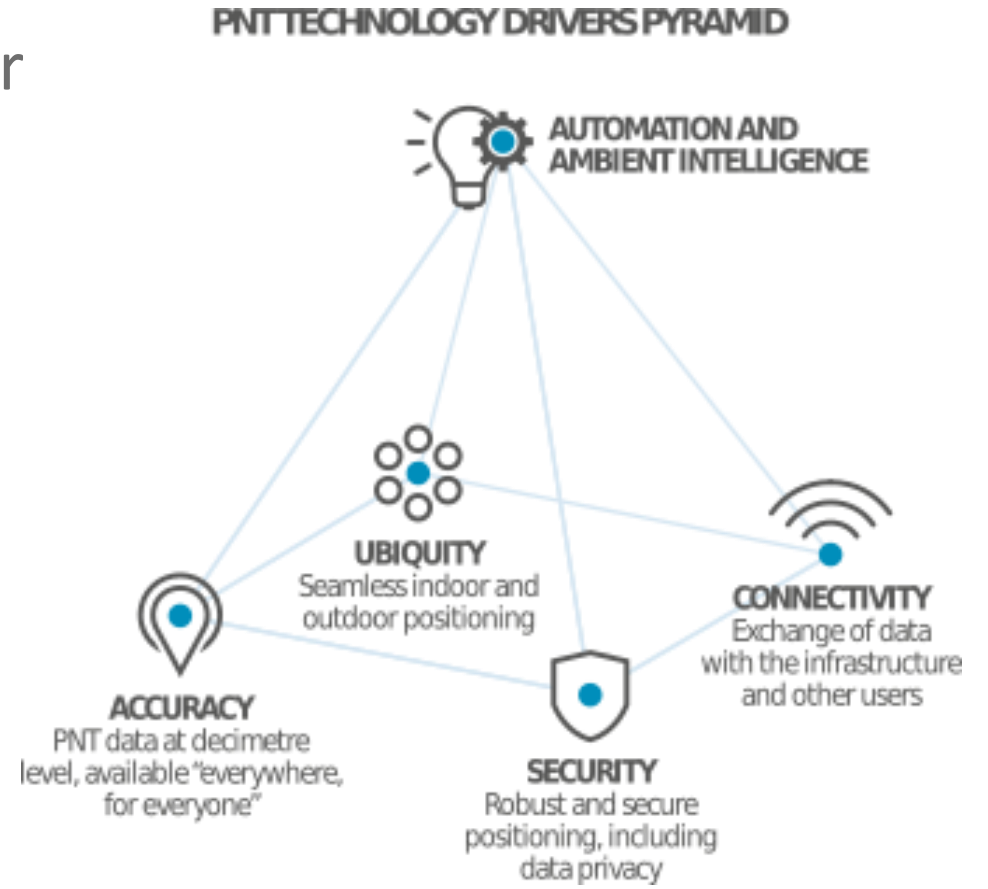


Outline

1. **Introduction**
2. Jamming
    - Jamming in the context of GNSS
    - Jamming signals
3. Jamming detection
    - Detection of signal in noise
    - Examples of detectors
    - Performance comparison of jamming detectors
    - Summary
4. Direction finding and Localization
    - Direction finding (DF) and localization of jammer
    - Angle of Arrival
    - Time Difference of Arrival / Difference Received Signal Strength
    - Frequency Difference of Arrival
    - Performance comparison of AoA and TDoA based methods
    - Summary

GNSS is ubiquitous

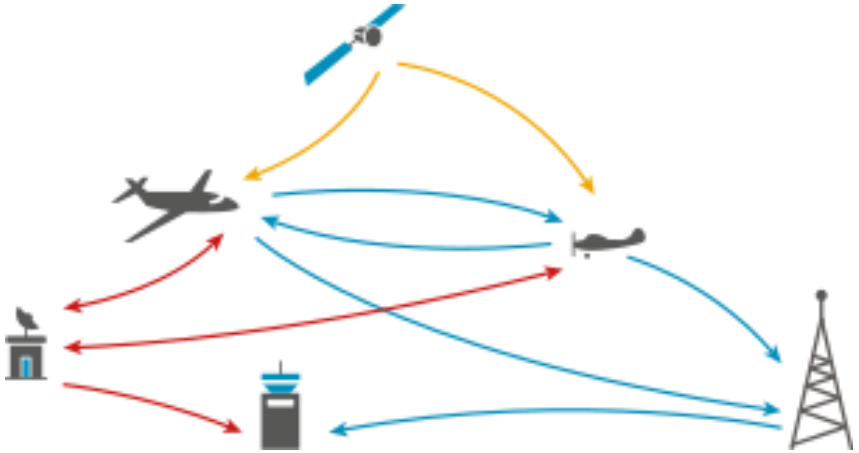
- Mass market consumer solutions
- Transport safety- and liability-critical solutions
- High precision and timing solutions



Source: Galileo Technology Report Issue 3 © European GNSS Agency, 2018

GNSS in (future) aviation

- Surveillance (ADS-B)
- Positioning and navigation
- Auto-landing
- Synthetic vision during poor visibility



Source: Galileo Technology Report Issue 3 © European GNSS Agency, 2018

Jamming

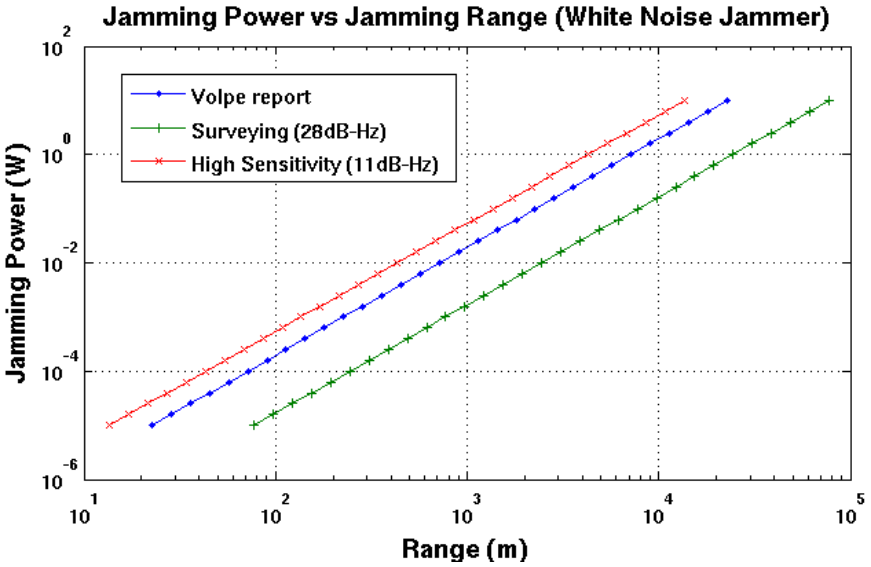
"Make (a broadcast or other electronic signal) unintelligible by causing interference."

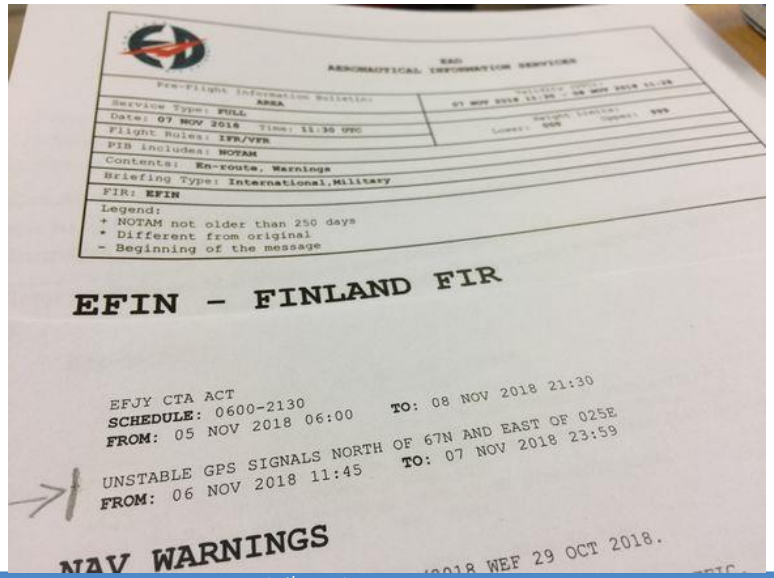
Source: https://www.jammer-store.com

Interferences							
Man-made					Channel-based		
Intentional			Unintentional		Atmospheric effects (ionopshere, troposhere, ...)	Multipaths	Fading and shadowing
Jamming	Spoofing	Meaconing/ Repeaters	Out-of-band emission	Harmonic frequencies			

Jamming

"Make (a broad- cast or other electronic signal) unintelligible by causing interference."

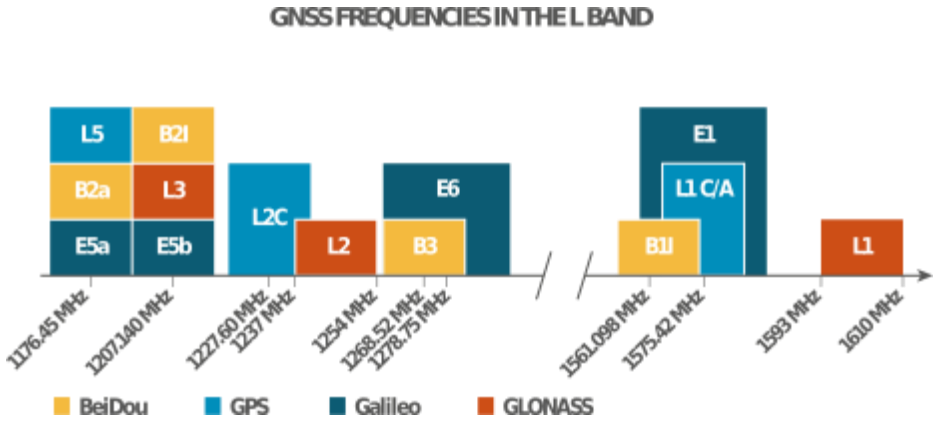




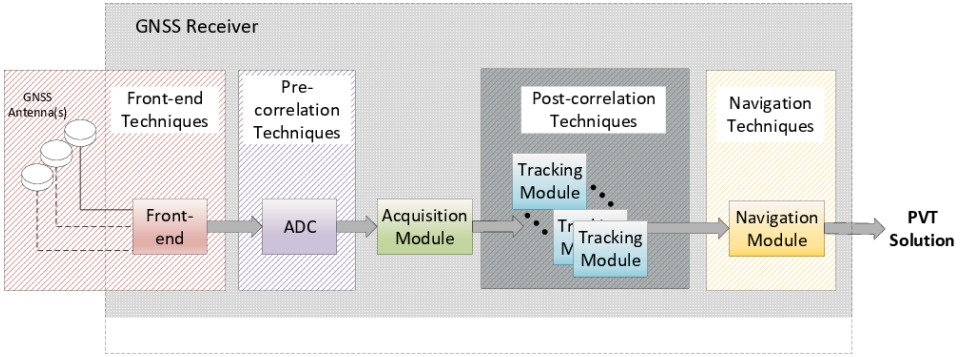
"We wanted to get this intelligence to airlines and other aviators for security reasons,"

GNSS principles

- ~20000km distance
- very low power at receiver
- DSSS sprovide robustness towards jamming



Source: Source: Galileo Technology Report Issue 3 © European GNSS Agency, 2018



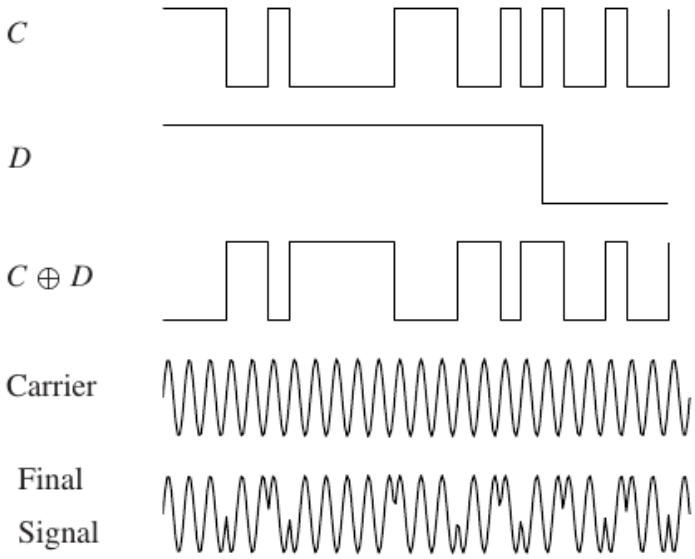
Outline

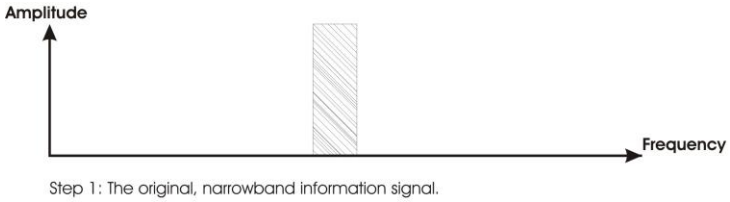
1. Introduction
2. **Jamming**
    - Jamming in the context of GNSS
    - Jamming signals
3. Jamming detection
    - Detection of signal in noise
    - Examples of detectors
    - Performance comparison of jamming detectors
    - Summary
4. Direction finding and Localization
    - Direction finding (DF) and localization of jammer
    - Angle of Arrival
    - Time Difference of Arrival / Difference Received Signal Strength
    - Frequency Difference of Arrival
    - Performance comparison of AoA and TDoA based methods
    - Summary

GNSS robustness to Jamming

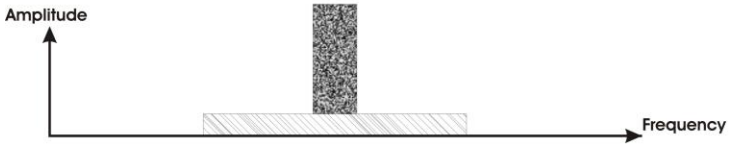
Direct-sequence Spread Spectrum system:

1. Narrowband information signal
2. Spreading with PRN code ‘C’ spreads signal’s bandwidth

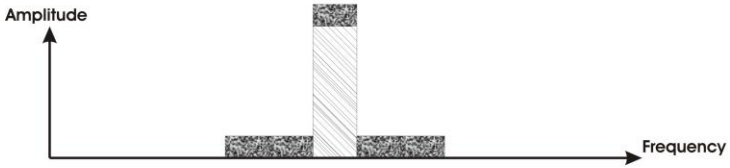




Step 1: The original, narrowband information signal.



Step 2: The information signal is spread over a wide frequency range with the spreading code and narrowband noise is added by the channel.

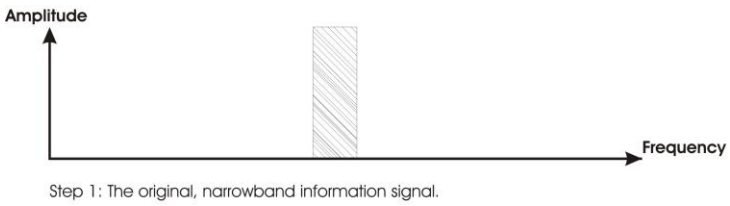


Step 3: The received signal is multiplied with the spreading code, causing the narrowband noise to be spread, and the wideband information signal to be despread.

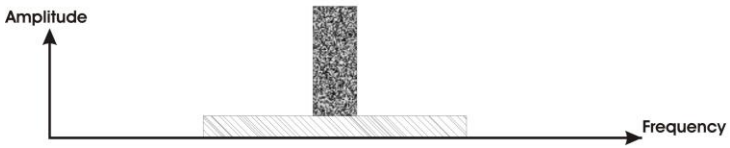
GNSS robustness to Jamming

Direct-sequence Spread Spectrum system:

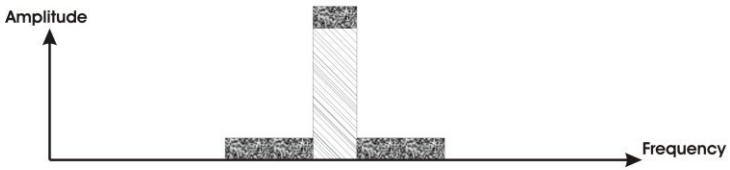
1. Narrowband information signal
2. Spreading with PRN code ‘C’ spreads signal’s bandwidth
3. Interference and noise is added during transmission
4. Despreading of signal with interferer and noise with known PRN code
5. Recovers original signal, while power of interferer and noise in actual band of signal is reduced



Step 1: The original, narrowband information signal.



Step 2: The information signal is spread over a wide frequency range with the spreading code and narrowband noise is added by the channel.

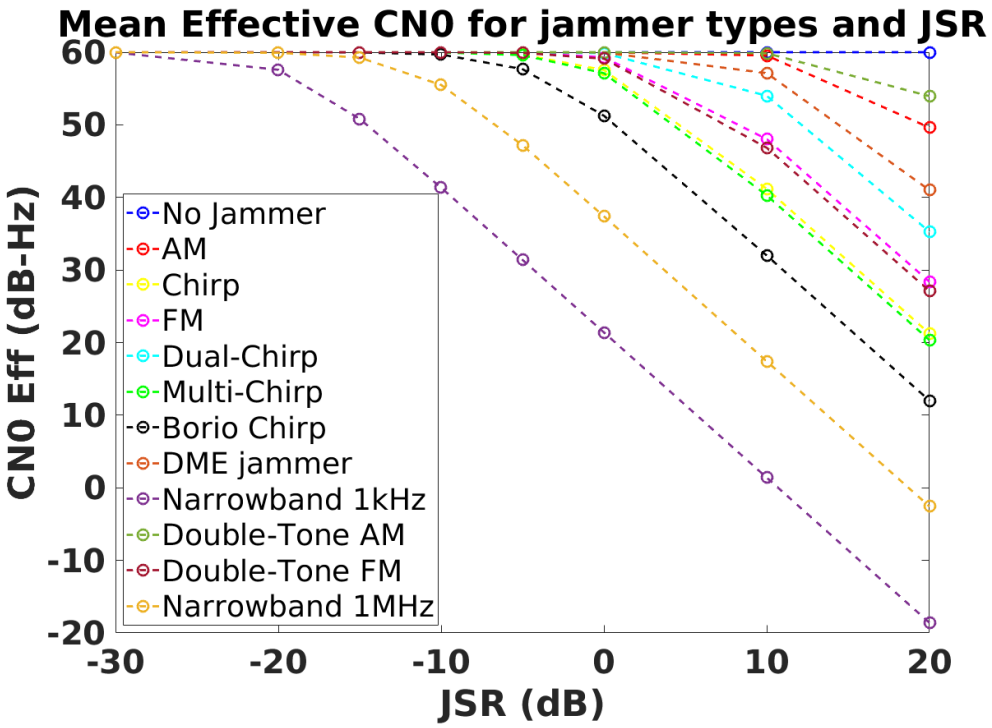


Step 3: The received signal is multiplied with the spreading code, causing the narrowband noise to be spread, and the wideband information signal to be despread.

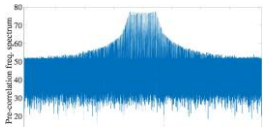
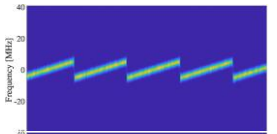
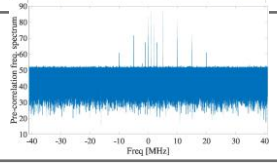
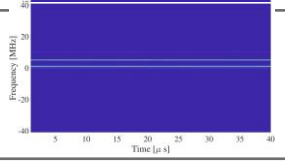
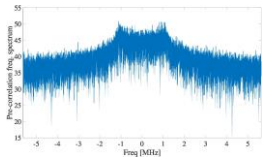
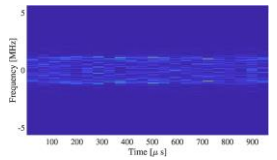
GPS process gain: 30dB

Impact of jamming on GNSS receiver

1. Low jamming power
   -> no effect
2. Medium jamming power
   -> CNR decreases
3. High jamming power
   -> acquisition & tracking *fails*



Jamming signals

Type	Comment	Spectrum	Spectrogram
Chirp	Very common, intentional		
Narrowband (CW)	Common, typ. unintentional		
NB Noise	Intentional, typ. narrowband, if wideband military		
NB Pulsed			
combinations & more complex	see STRIKE project		

Many jamming signals

- FM signal

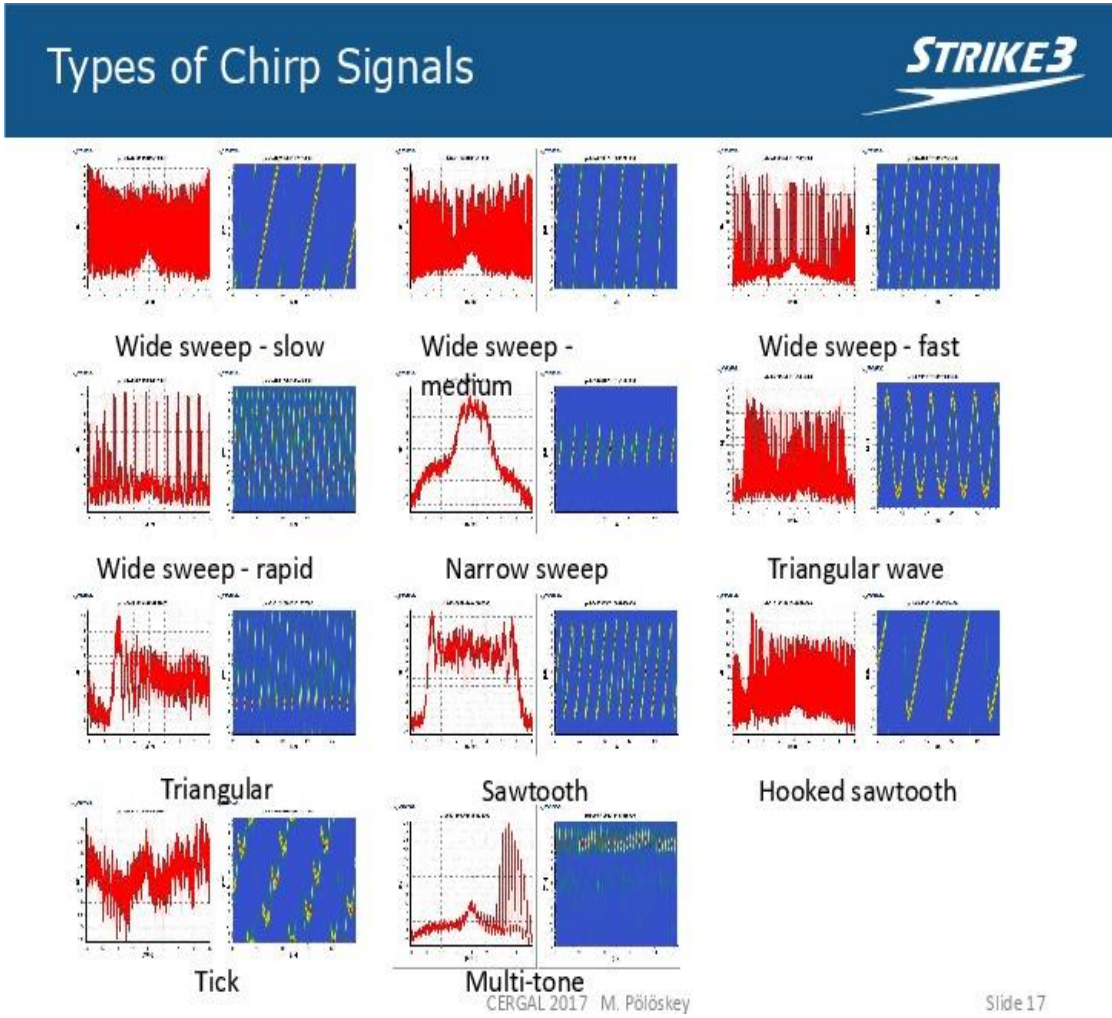
$$j(t) = \sqrt{P_J}\sin\left(2\pi f_J t + \beta\sin\left(2\pi f_J t\right)\right)$$

- Generic saw-tooth chirp:

$$j(t) = \sqrt{P_J}\sin(2\pi f_J t + \pi k_{up} k_J t^2 + \theta_J)$$

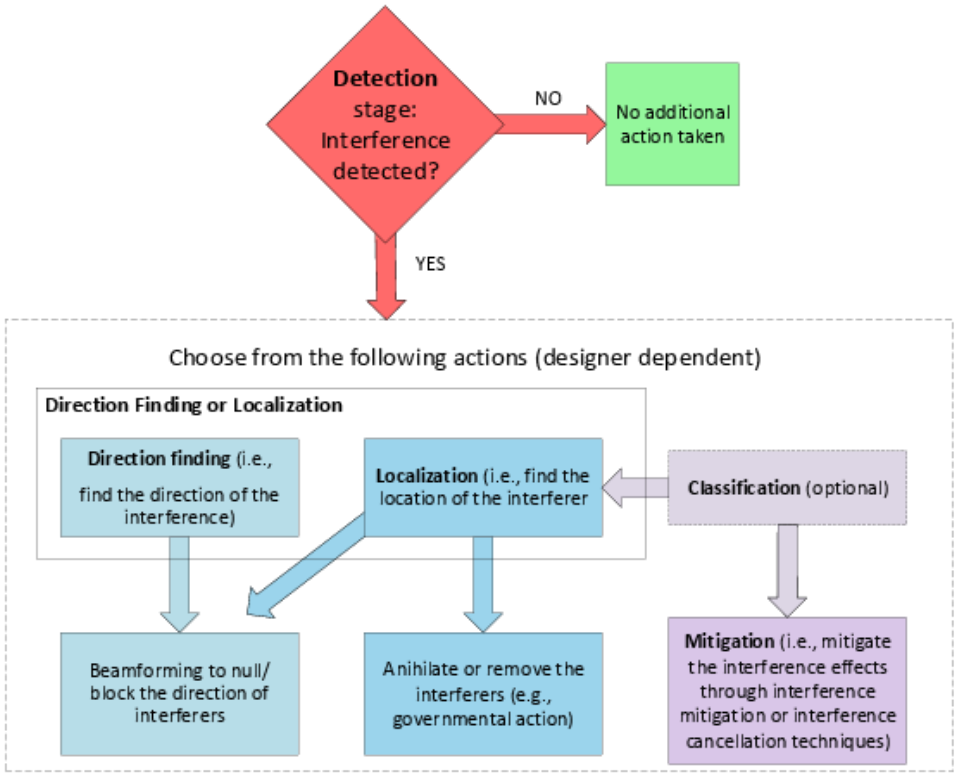
- Generic signal with frequency dependent part $f_{q(t)}$

$$j(t) = \sqrt{P_J}\sin(2\pi f_q(t) t + \theta_J)$$



Actions towards jamming

- *Detection*
- Classification
- Mitigation
- *Direction finding/ Localization*



Outline

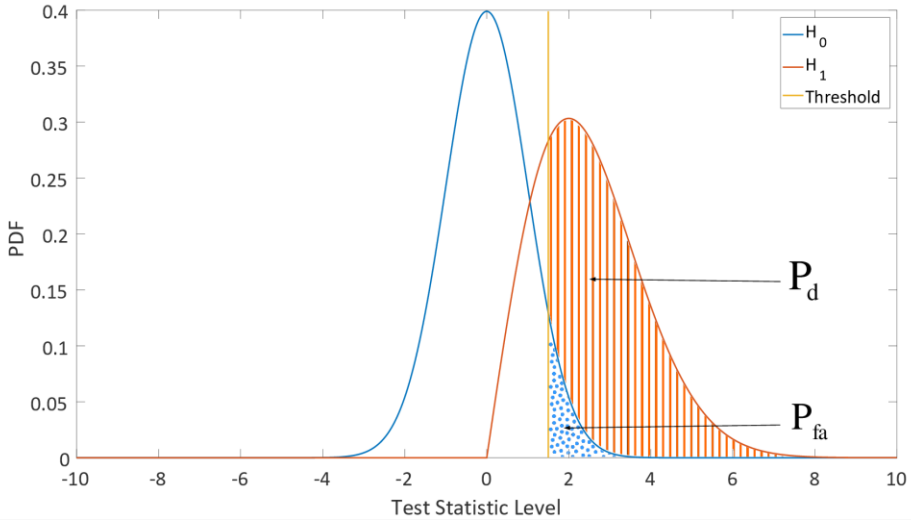
1. Introduction
2. Jamming
    - Jamming in the context of GNSS
    - Jamming signals
3. **Jamming detection**
    - Detection of signal in noise
    - Examples of detectors
    - Performance comparison of jamming detectors
    - Summary
4. Localization
    - Direction finding (DF) and localization of jammer
    - Angle of Arrival
    - Time Difference of Arrival / Difference Received Signal Strength
    - Frequency Difference of Arrival
    - Performance comparison of AoA and TDoA based methods
    - Summary

Jamming detection

Binary hypothesis testing

H0: $r(n) = s(n) + w(n)$

H1: $r(n) = s(n) + j(n) + w(n)$



Generalized likelihood ratio test:

- *Accept H1 if*

$$\frac{\max_{\theta_1} p(r|H_1, \theta_1)}{\max_{\theta_0} p(r|H_0, \theta_0)} > \gamma$$

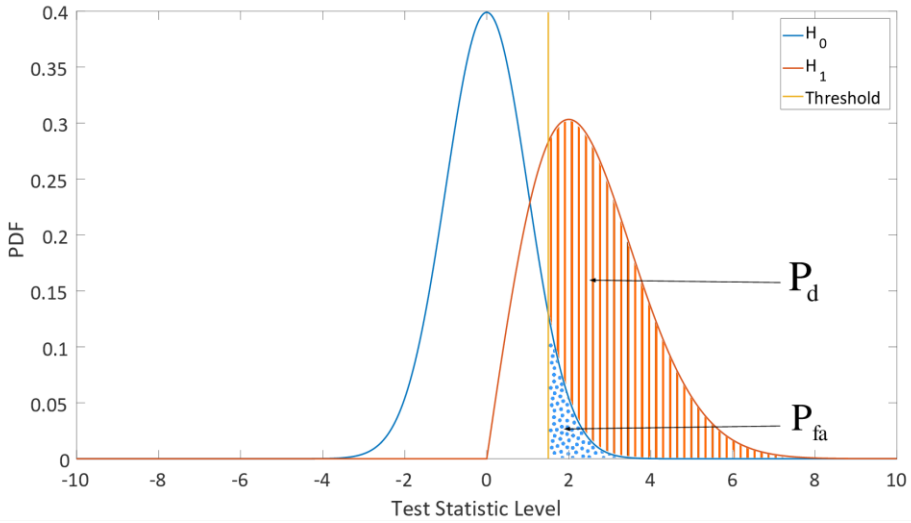
T … test statistic

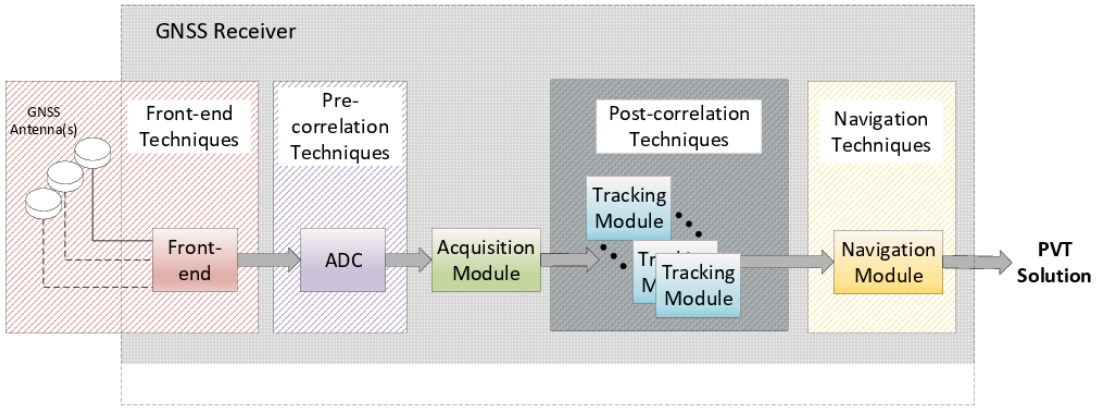
γ … detection threshold

$$P_d = \Pr(T > \gamma | H_1)$$
$$P_{fa} = \Pr(T > \gamma | H_0)$$

Jamming detection

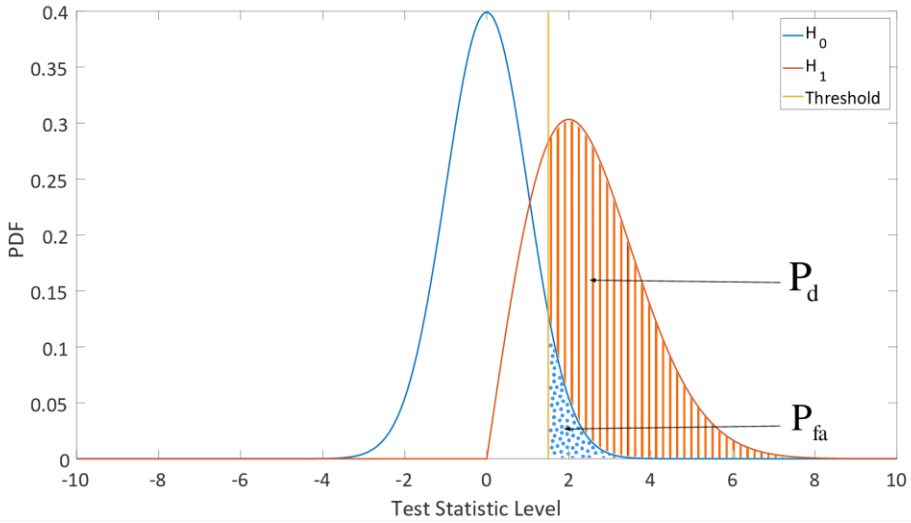
- Front-end techniques
- Pre-correlation techniques
- Post-correlation techniques
- Navigation techniques





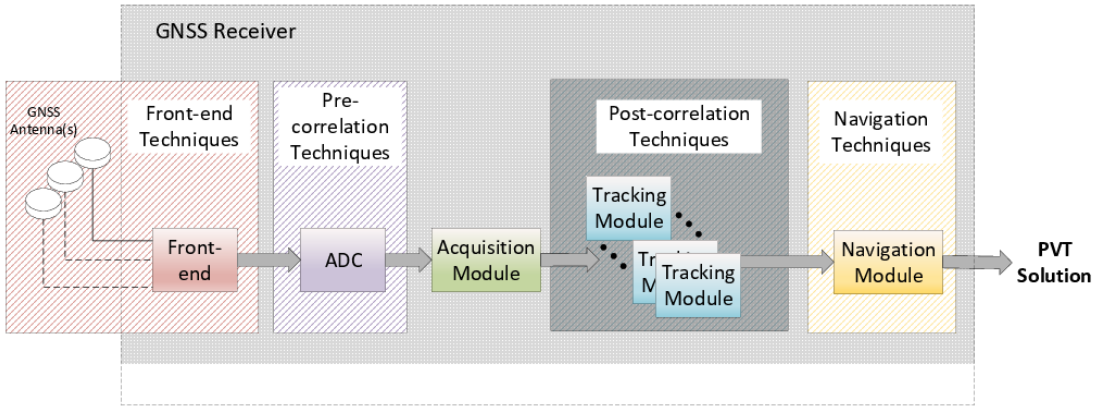
Jamming detection

- Front-end techniques
- Pre-correlation techniques
- Post-correlation techniques
- Navigation techniques



➡ Most detectors rely either on test statistic based on

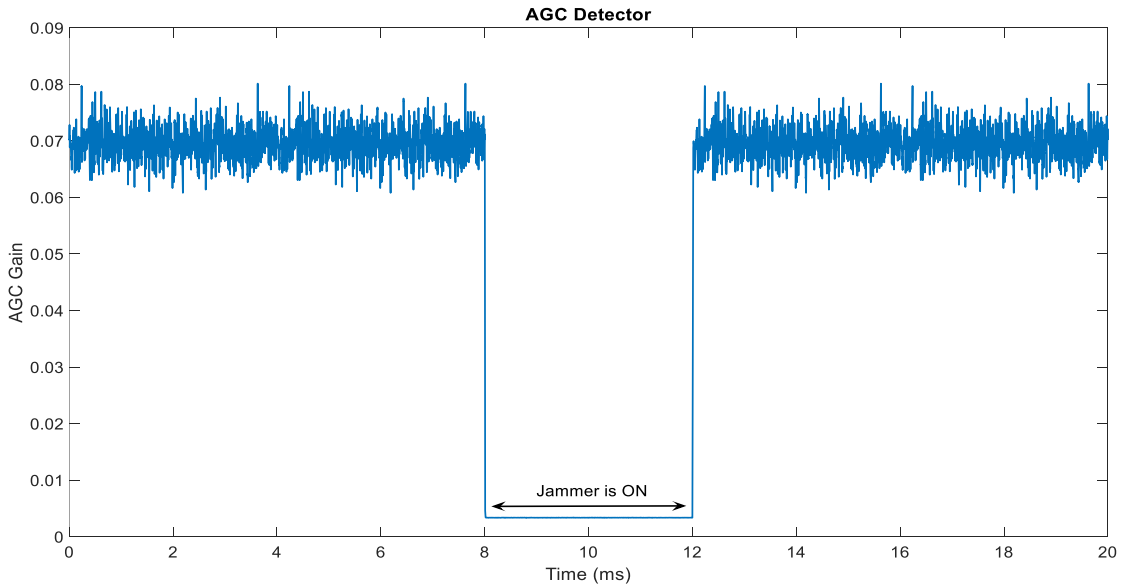
1. *Power level*
2. *Distribution of power level*



Jammer detection (cont'd)

1. Power level

Front-end ⇒ AGC level



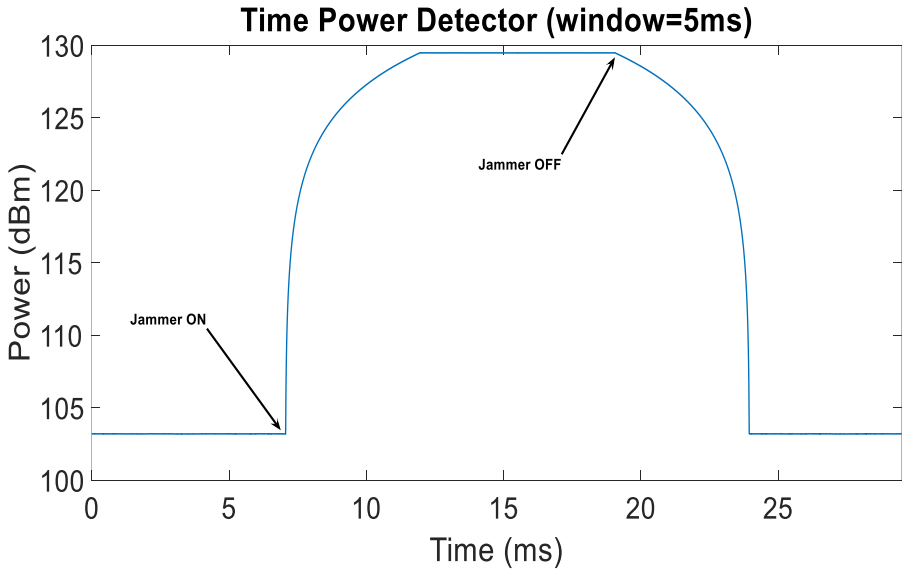
Jammer detection (cont'd)

1. Power level – time domain

Pre-correlation ⇒ time average of power, results in

Time Power Detector (TPD)

$$T = \frac{1}{JN} \sum_{\{j=1\}}^{J} \sum_{\{n=1\}}^{N} |r(n + (j-1)N)|^{2v}$$

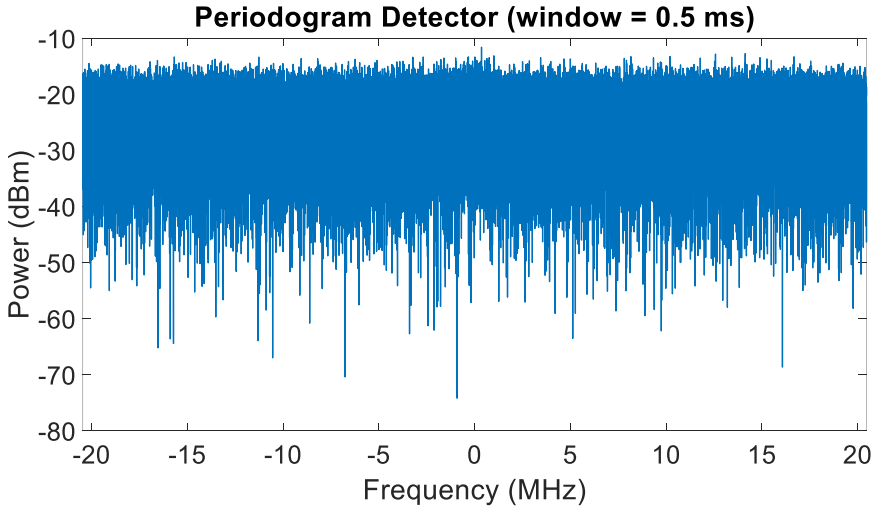


Jammer detection (cont'd)

1. Power level – frequency domain (STFT)

Pre-correlation ⇒ average of power in frequency domain, results in Frequency Power Detector (FPD)

$$T = \frac{1}{JM} \sum_{\{j=1\}}^{J} \sum_{\{k=1\}}^{M} |R(k + (j-1)M)|^{2\nu}$$



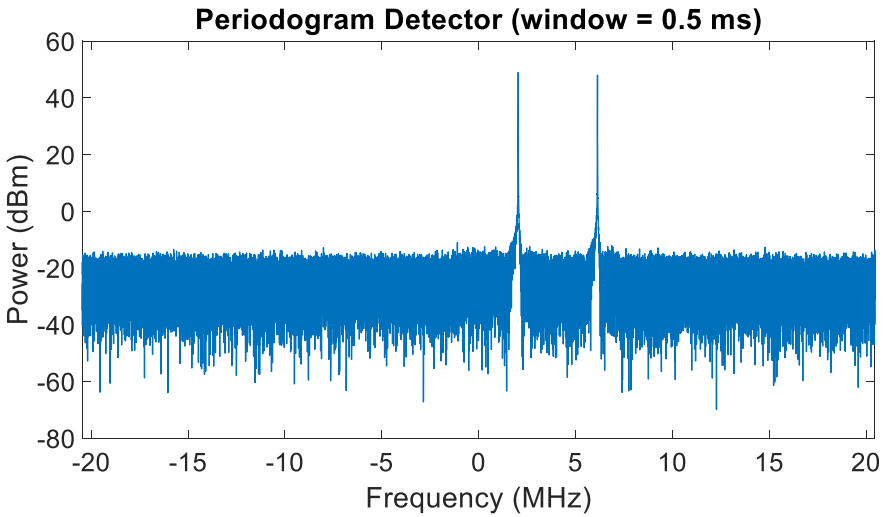
FPD test statistic without jammer at SNR=-10dB

Jammer detection (cont'd)

1. Power level – frequency domain (STFT)

Pre-correlation ⇒ average of power in frequency domain, results in Frequency Power Detector (FPD)

$$T = \frac{1}{JM} \sum_{\{j=1\}}^{J} \sum_{\{k=1\}}^{M} |R(k + (j-1)M)|^{2\nu}$$



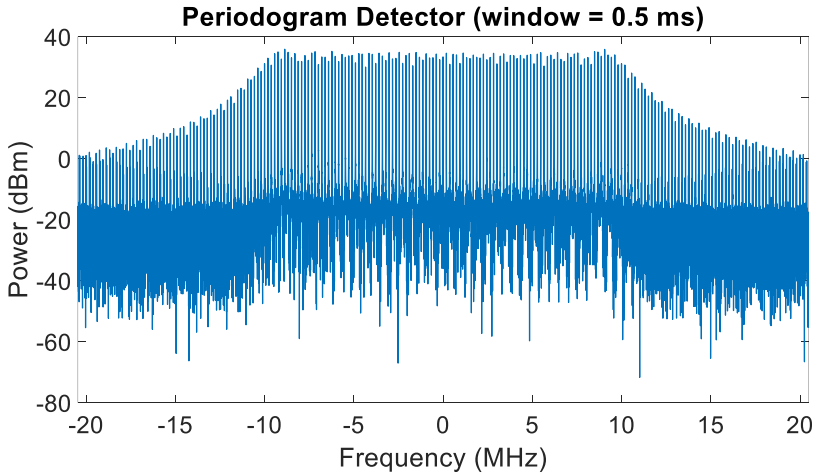
FPD test statistic with double tone jammer at SNR=-10dB

Jammer detection (cont'd)

1. Power level – frequency domain (STFT)

Pre-correlation ⇒ average of power in frequency domain, results in Frequency Power Detector (FPD)

$$T = \frac{1}{JM} \sum_{\{j=1\}}^{J} \sum_{\{k=1\}}^{M} |R(k + (j-1)M)|^{2\nu}$$



FPD test statistic with chrip jammer at SNR=-10dB

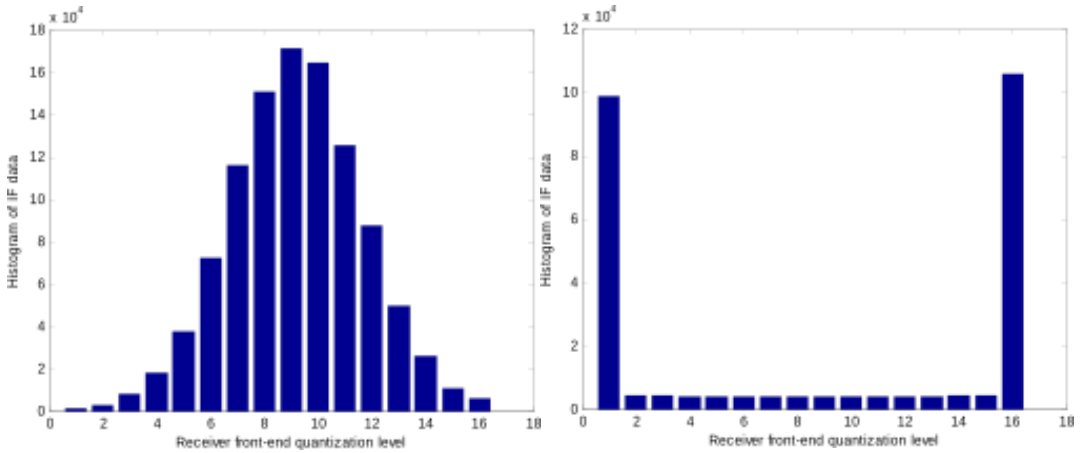
Jammer detection (cont'd)

1. Distribution of power level

Front-end ⇒ Distribution of IF data

Distribution tests for Gaussianity

- Chi-square goodness-of-fit test
- Jarque-Bera test
- Lilliefors test
- Anderson-Darling test



Histogram of IF data (4-bit) without and with strong jamming

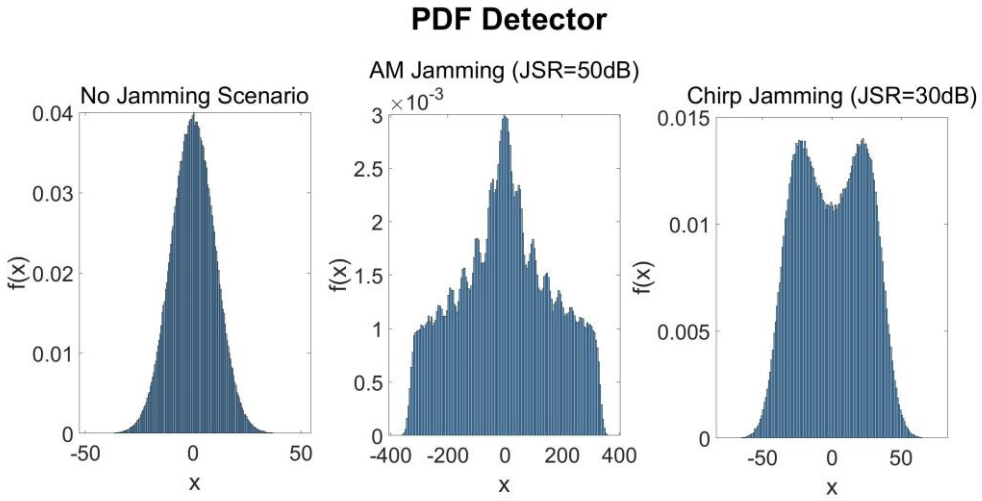
Jammer detection (cont'd)

1. Distribution of power level

Front-end ⇒ Distribution of IF data

Kurtosis detector

$$T = \frac{\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^4}{\left(\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^2\right)^2}$$



Histograms of IF data without and with different jamming

Jammer detection (cont'd)

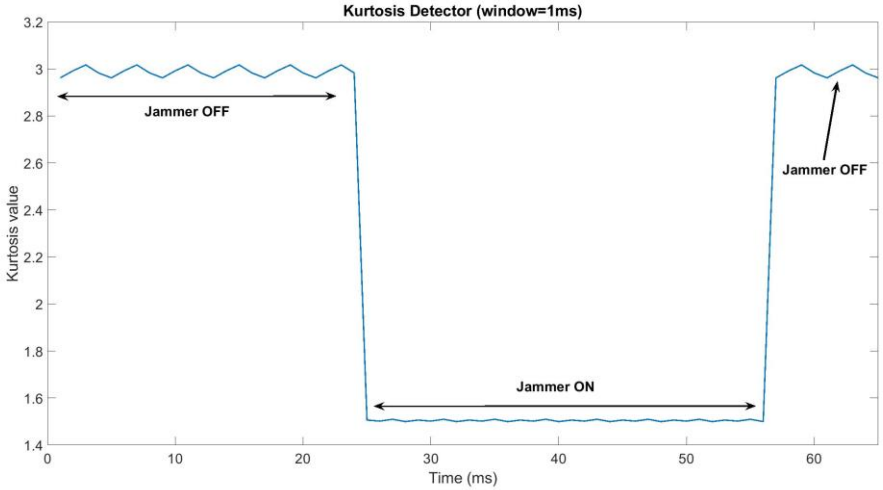
1. Distribution of power level

Front-end ⇒ Distribution of IF data

Kurtosis detector

$$T = \frac{\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^4}{\left(\frac{1}{N}\sum_{n=1}^{N}(r(n)-\mu_r)^2\right)^2}$$

$T \approx 3$ for Normal distributions



Jammer detection (cont'd)

Filtering (jamming mitigation in frequency domain)

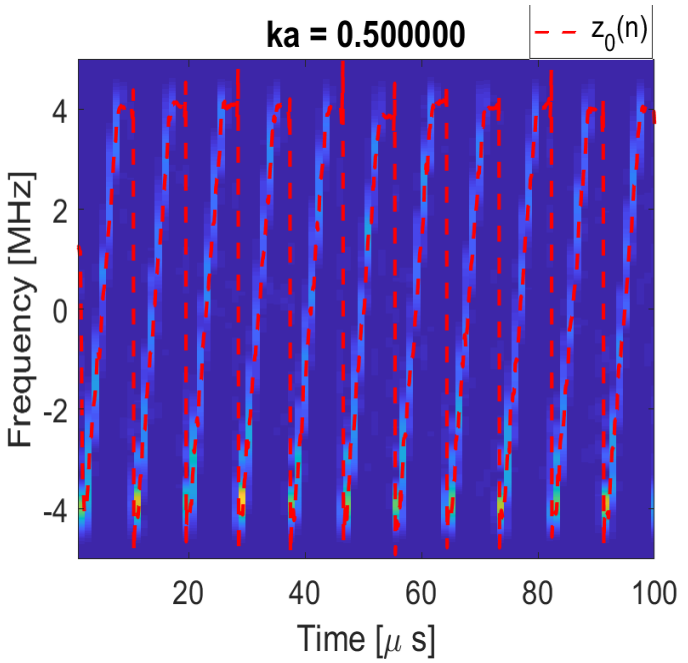
Pre-correlation ⇒ IIR filtering

Notch filter

$$H_n(z) = \frac{1 - z_0(n)z^{-1}}{1 - k_a z_0(n)z^{-1}}$$

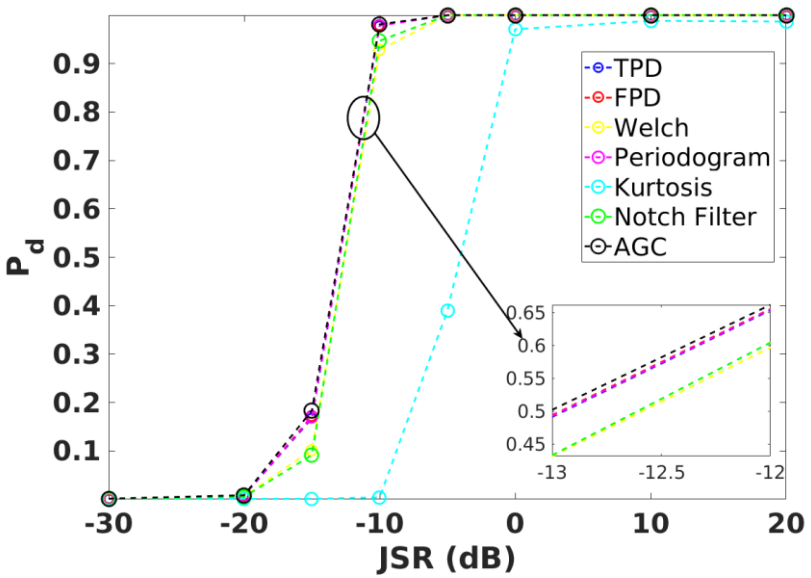
$|z_0(n)|$ as test statistic

$$T = \frac{1}{N}\sum_{n=1}^{N} |z_0(n)|$$

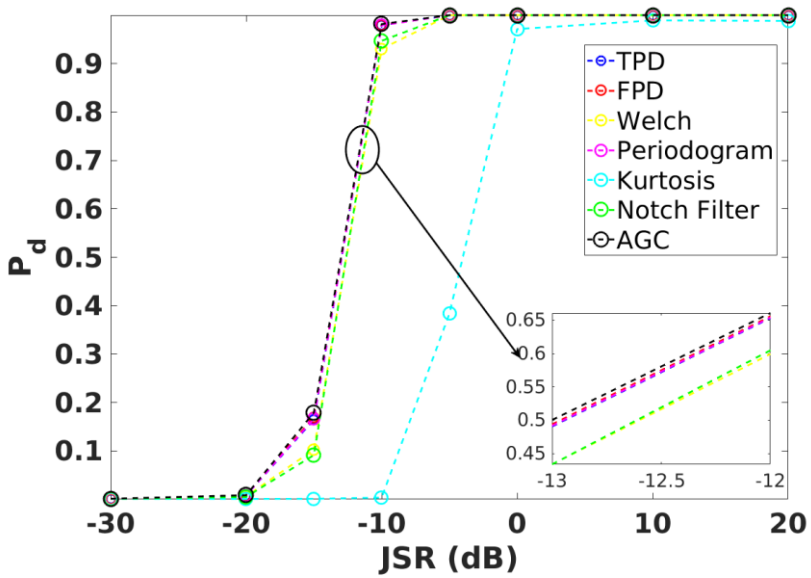


Comparison of jamming detectors

Single AM-tone

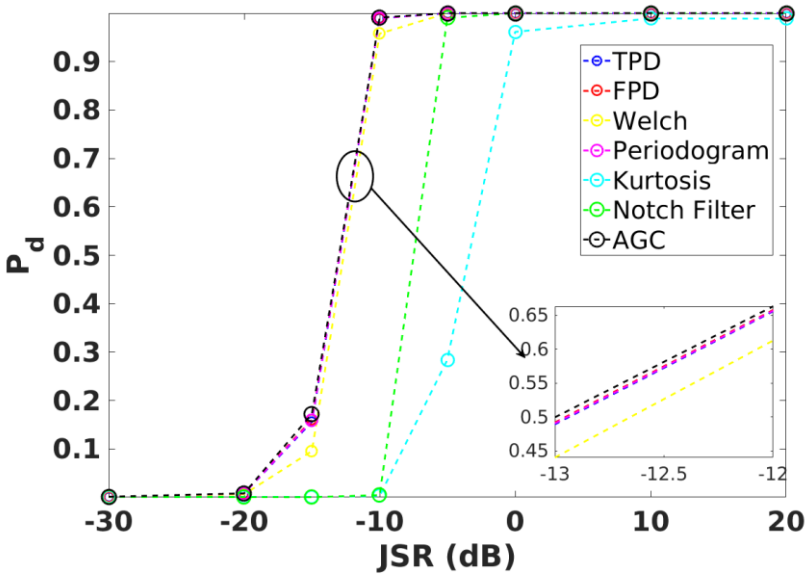


Single FM-tone

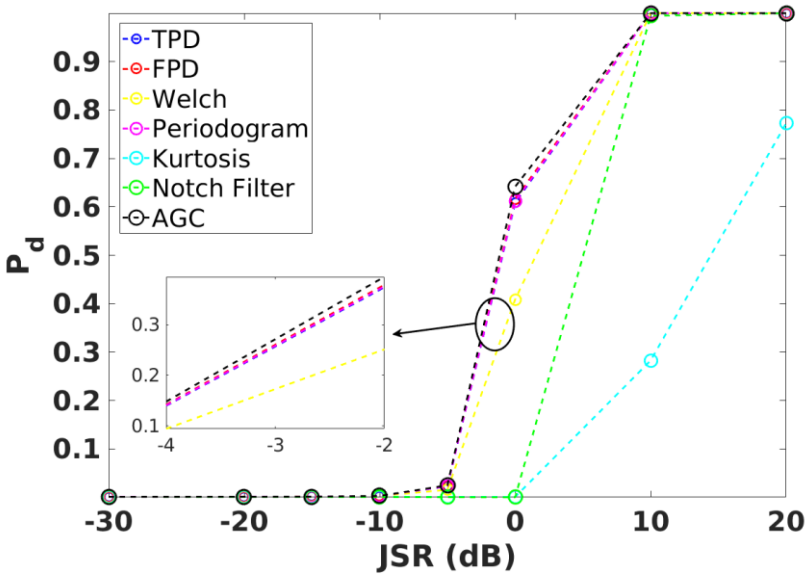


Comparison of jamming detectors

Single Chirp

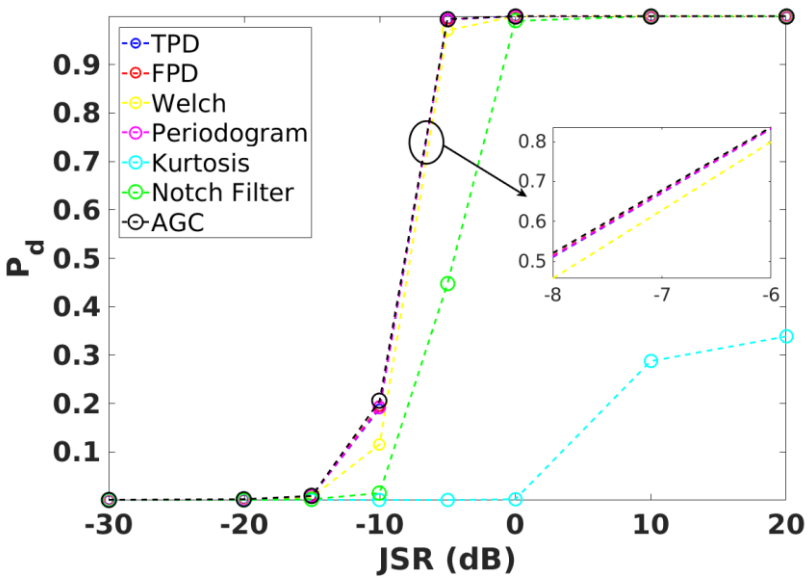


Dual Chirp

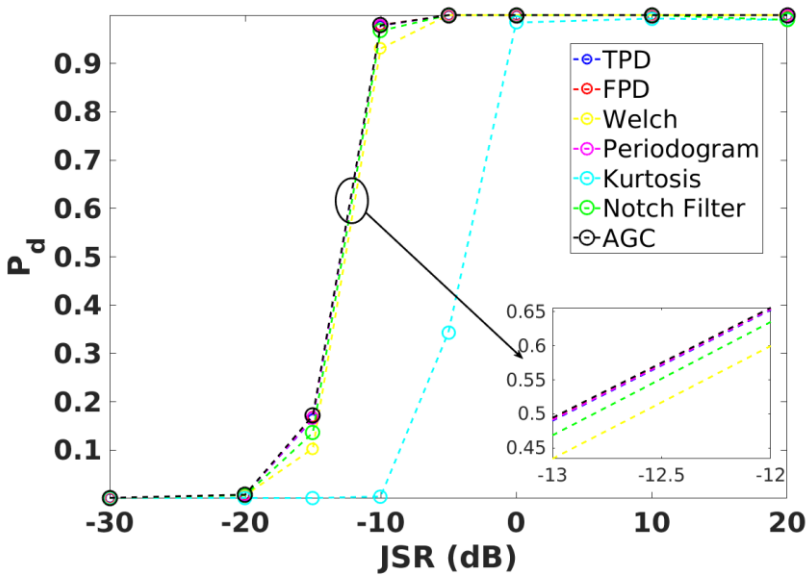


Comparison of jamming detectors

Multiple Chirps

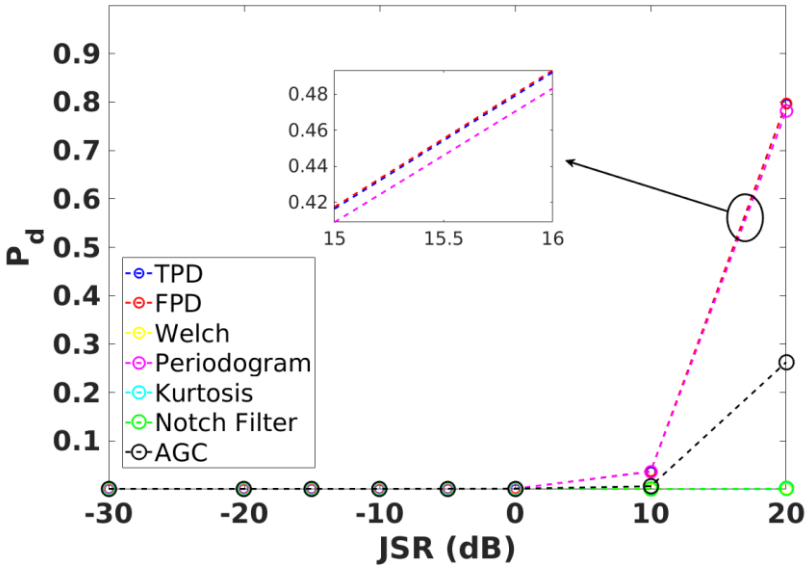


Fast Chirp

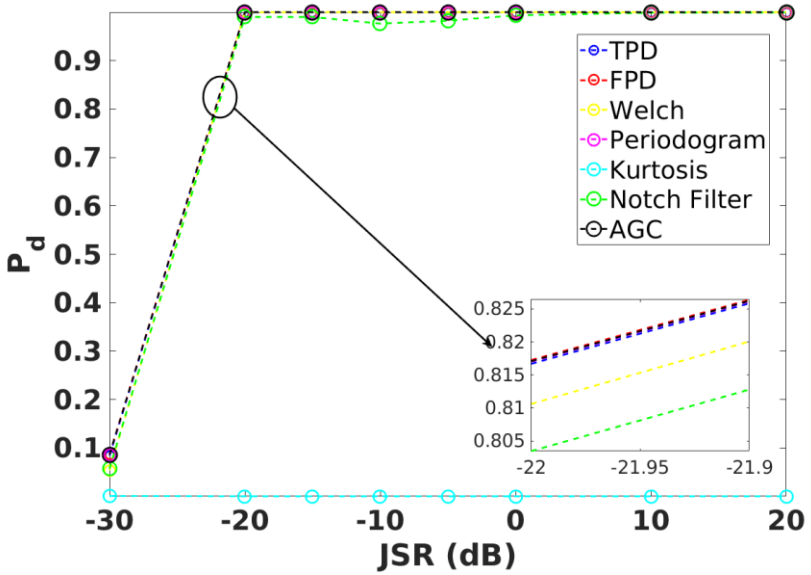


Comparison of jamming detectors

Narrowband pulse (DME-like)



Narrowband noise (1MHz)



Summary jamming detection

- AGC and TPD are *simple* and most *reliable* detectors
- Short and narrow band pulse are hard to detect
- Detection thresholds must be found and set

Jammer Type	Minimum JSR needed to be able to detect the jammer in at least 50% of cases with the best detector [dB]
AM	<-30
FM	-20
Chirp	-20
Dual-chirp	0
Multi-chirp	-10
Fast chirp	-10
NB	<-30 dB

Outline

1. Introduction
2. Jamming
    - Jamming in the context of GNSS
    - Jamming signals
3. Jamming detection
    - Detection of signal in noise
    - Examples of detectors
    - Performance comparison of jamming detectors
    - Summary
4. **Direction finding and Localization**
    - Direction finding (DF) and localization of jammer
    - Angle of Arrival
    - Time Difference of Arrival / Difference Received Signal Strength
    - Frequency Difference of Arrival
    - Performance comparison of AoA and TDoA based methods
    - Summary

Direction finding (DF) and localization

Observables for localization

- Phase
- Time
- Frequency
- Power

➢ Jamming signal characteristics and parameters are unknown

$$j(t) = \sqrt{P_J}\sin(2\pi f_q(t)t + \theta_J)$$

$f_{q(t)} = ?$

$t = ?$

$\theta_J = ?$

$P_j = ?$

➢ Typical methods (ToA, RSS, FoA) are *not* applicable

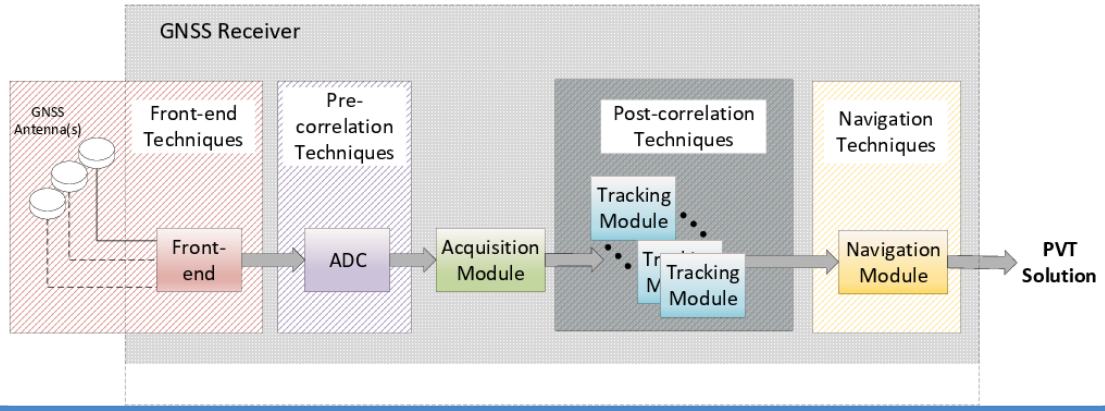
➢ *Differential methods required*

Jammer Direction finding (DF) and localization

Observables for jammer localization

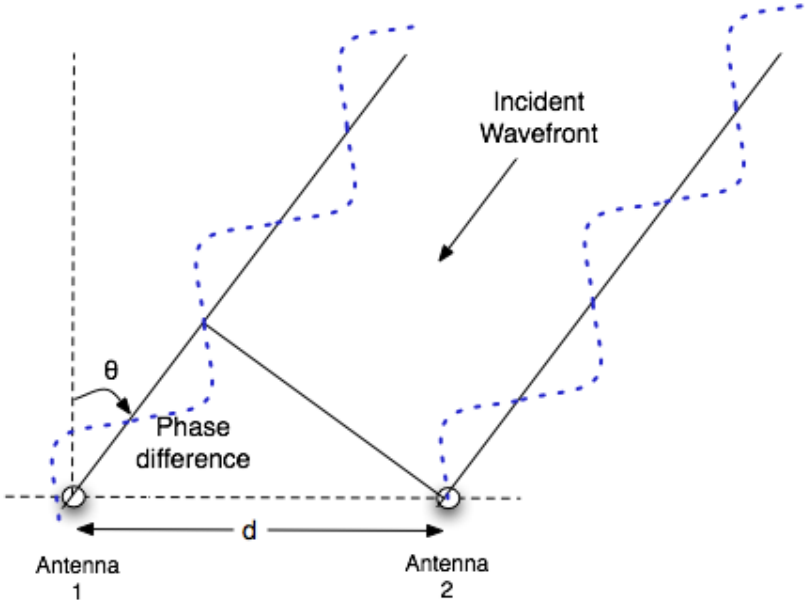
- ❑ AoA (phase difference
- ❑ TDoA (time difference)
- ❑ DRSS (power difference)
- ❑ FDoA (frequency difference)

1. Measurements at *2 antennas*
2. Measurements at *2 positions* at different time (signal parameter constant during that time)



Estimation of AoA

- **AoA (phase difference)**



AoA: estimate from spatial spectrum of signal at different antenna elements

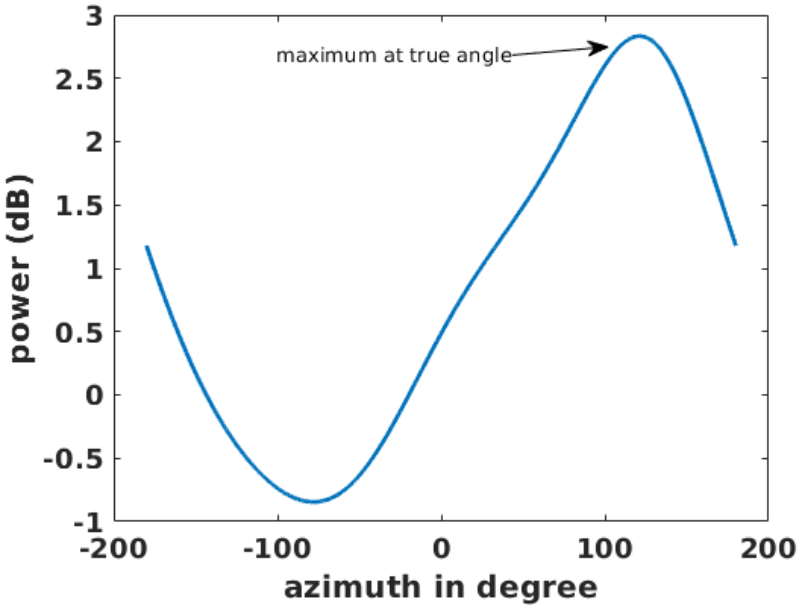
$$P(\theta) = \frac{1}{a(\theta)^H R^{-1} a(\theta)}$$

(Capon method)

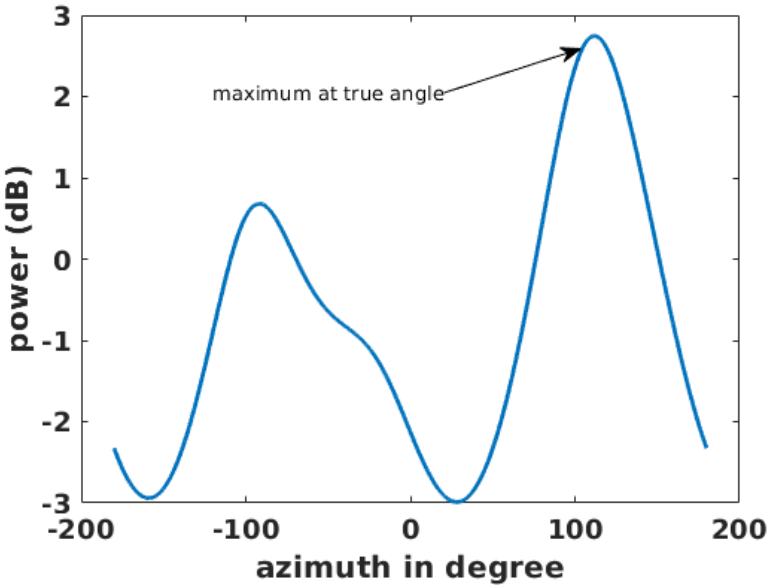
- *Multiple antennas as antenna array*
- *Requires antenna array calibration*

Estimation of AoA -- Spatial Spectrum

Capon method with 3 element antenna array



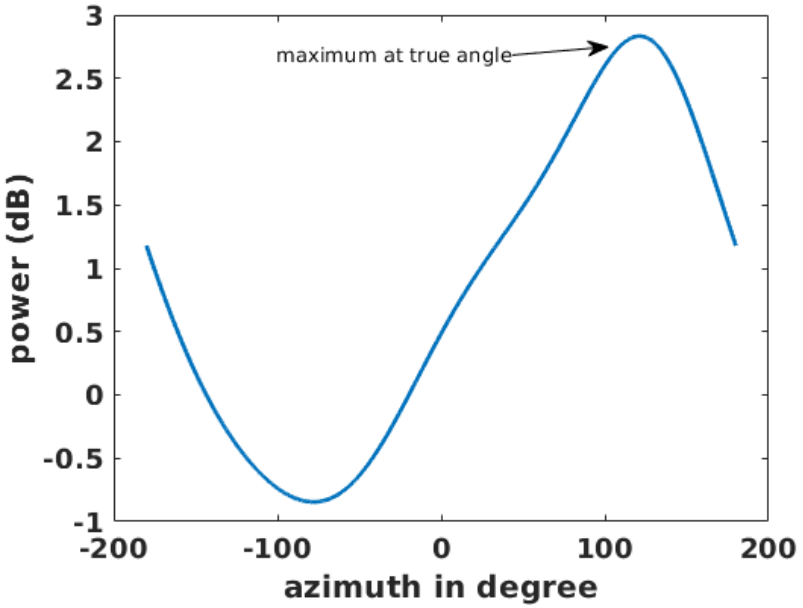
Interelement spacing: 1m



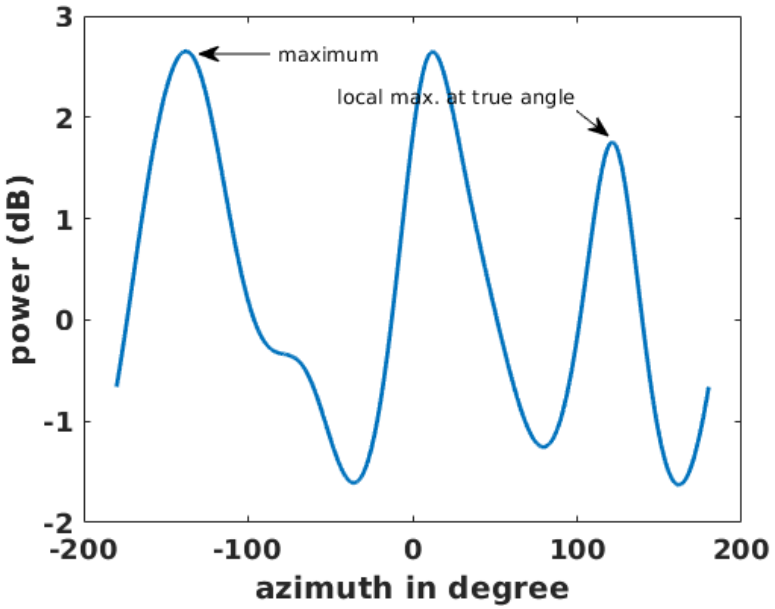
Interelement spacing: 2m

Estimation of AoA -- Spatial Spectrum

Capon method with 3 element antenna array



Interelement spacing: 1m



Interelement spacing: 3m

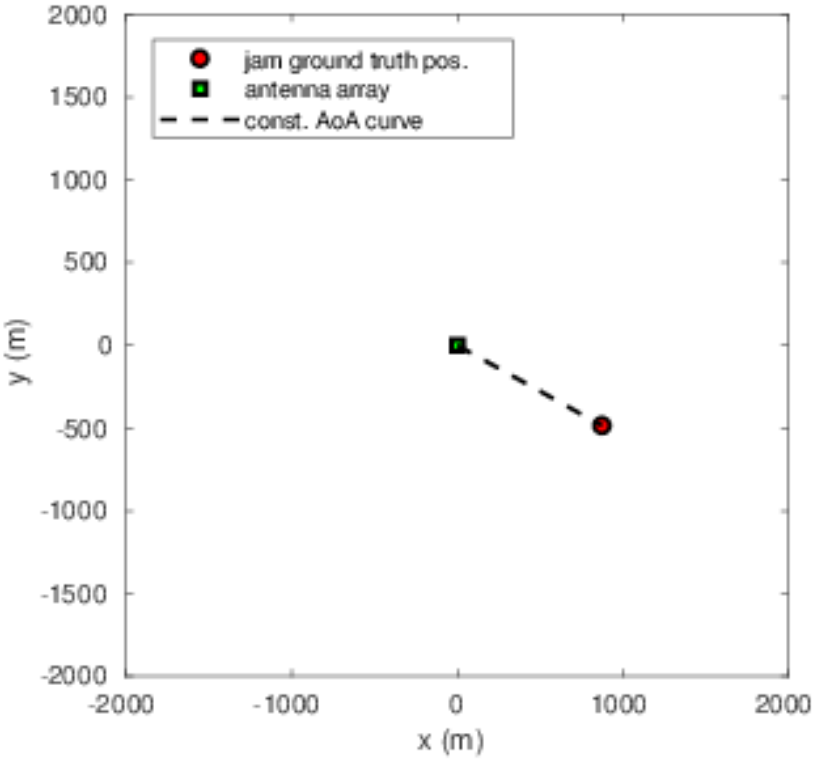
❖ Ambiguities can be avoided with small interelement distances

Estimation of Position from AoA

- **AoA (phase difference)**

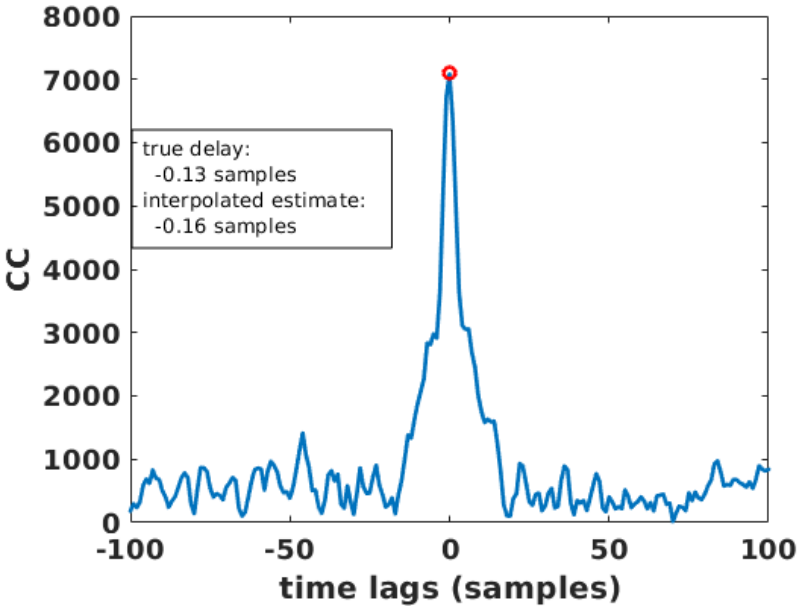
$$\theta = \arcsin \frac{\Delta\phi_{12}}{d} \frac{c}{2\pi f_c}$$

- **Triangulation** to compute position with a *pair of AoAs,* from typically *two different* locations



Estimation of TDoA

- **TDoA (time difference)**



CC function for double chirp signal

TDoA: estimate from cross-correlation function of signal at different antennas

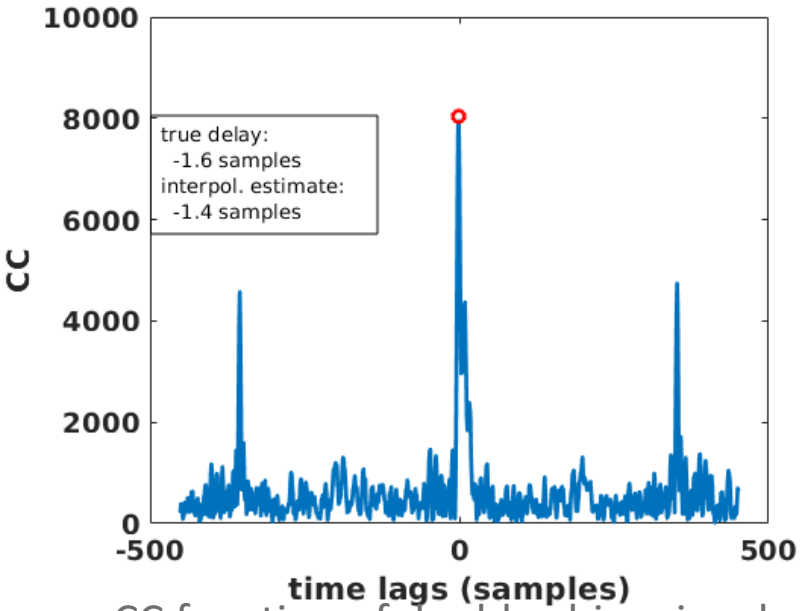
$$\hat{R}_{r_1 r_2}(\tau) = \int_{-\infty}^{\infty} \Psi_g(f) G_{r_1 r_2}(f) \mathrm{e}^{j2\pi f \tau} df$$

$$G_{r_1 r_2}(f) = \int_{-\infty}^{\infty} R_{r_1 r_2}(\tau) e^{-j2\pi f t} \, \mathrm{d}\tau$$

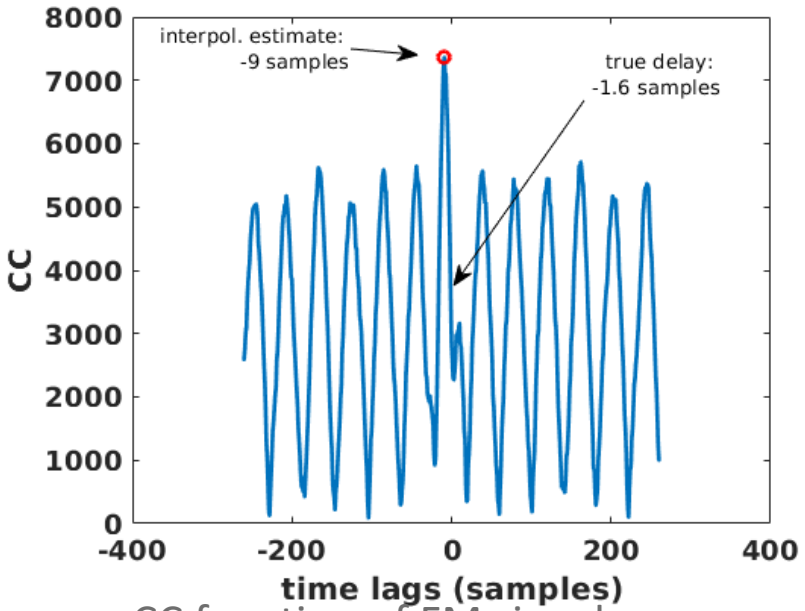
- *Time synchronized antennas*
- *Interpolation of CC func. to get sub sample time resolution*

Estimation of TDoA – CC function

Cross-correlation function for different signal types



CC function of double chirp signal



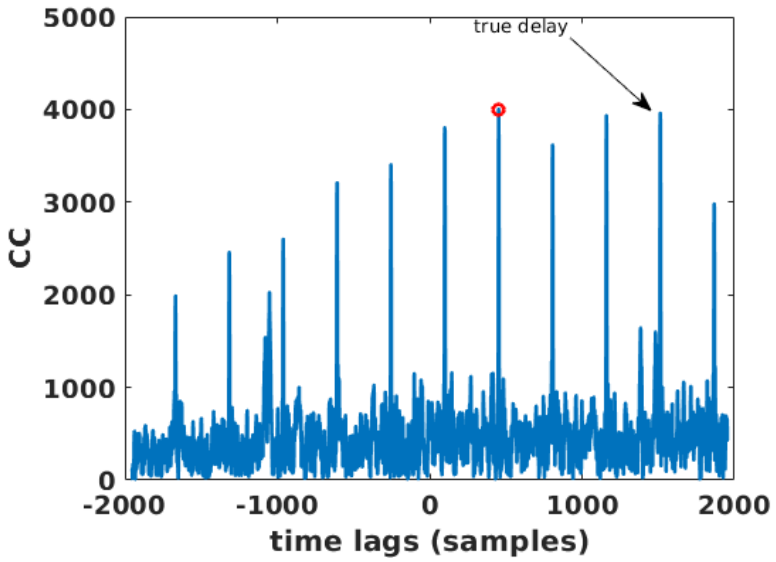
CC function of FM signal

55m delay error

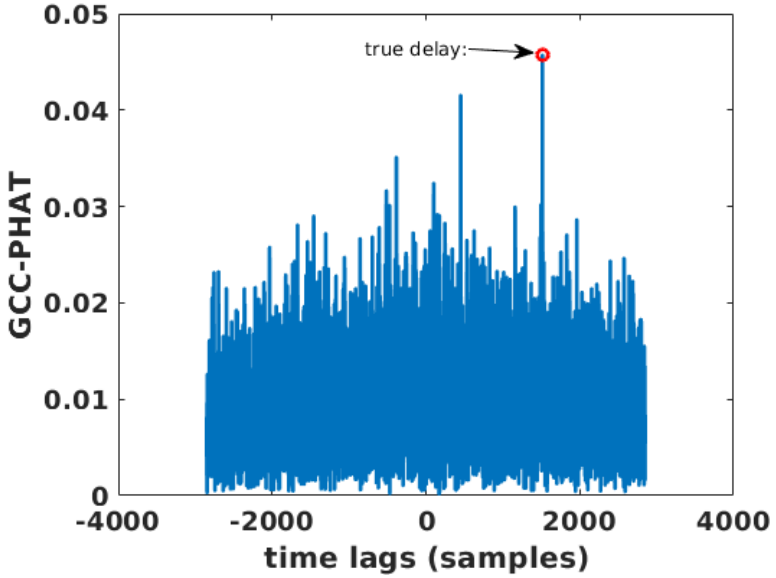
❖ *Accuracy of CC function depends on bandwidth of signal*

Estimation of TDoA – CC function

Cross-correlation function for large baseline



CC function of double chirp signal



GCC-PHAT function of double chirp

8 km delay error

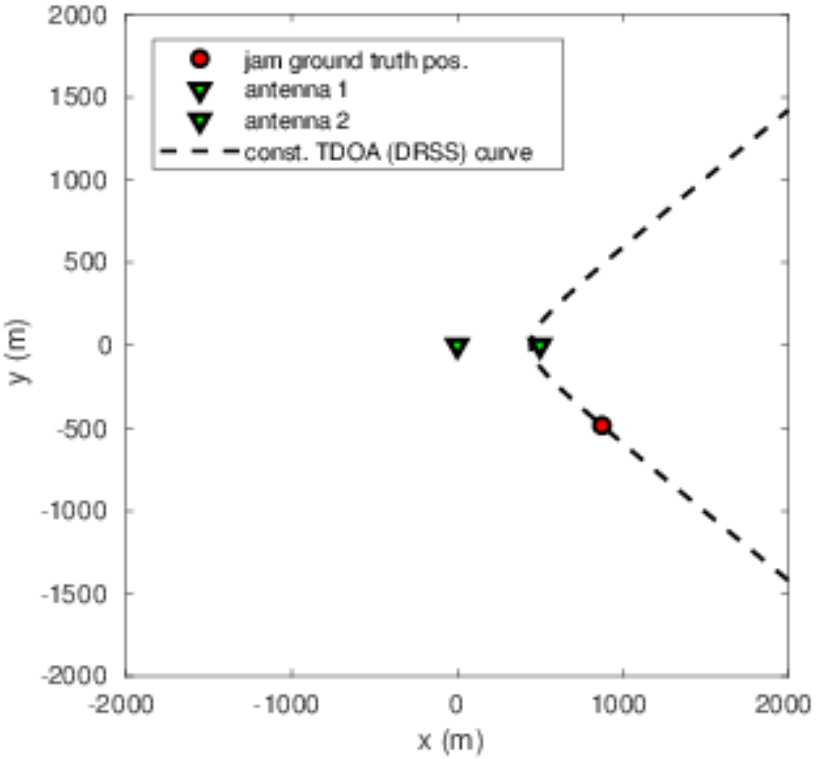
❖ *Different types of transforms for CC funct. -> different performance*

Estimation of Position from TDoA

- **TDoA (phase difference)**

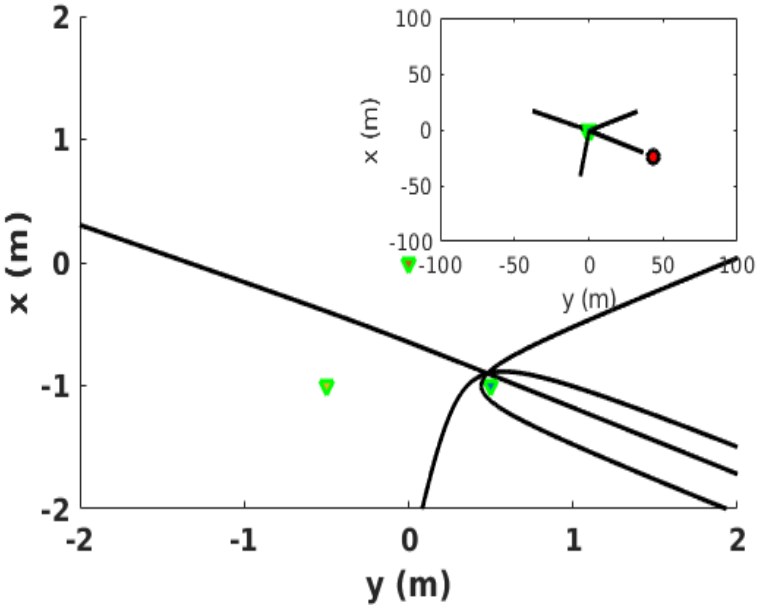
$$r_1 = \Delta\tau_{12} c + r_2$$

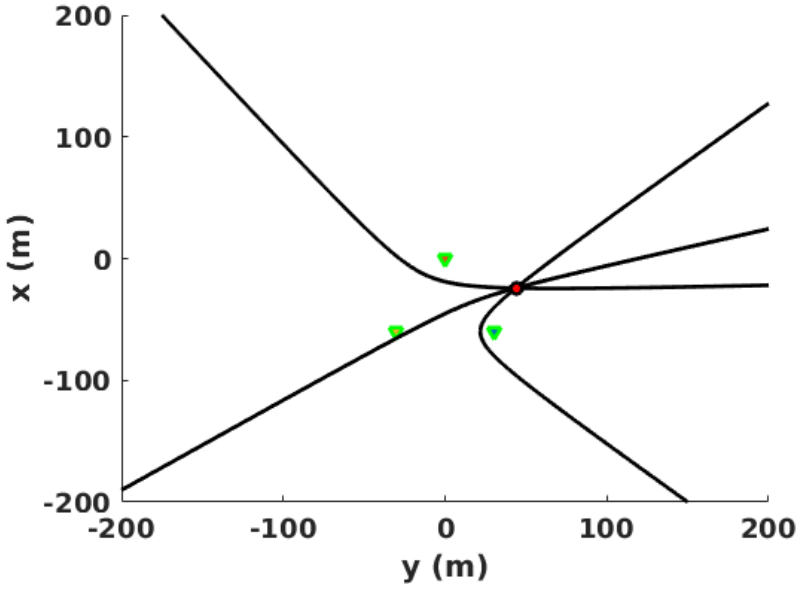
- **Trilateration** to compute position with a *pair of TDoAs* ,
  from *3 antennas* with *large baseline*, but also from 2 antennas at *different location*



❖ *Three antennas can provide position estimate*

Estimation of Position from TDoA

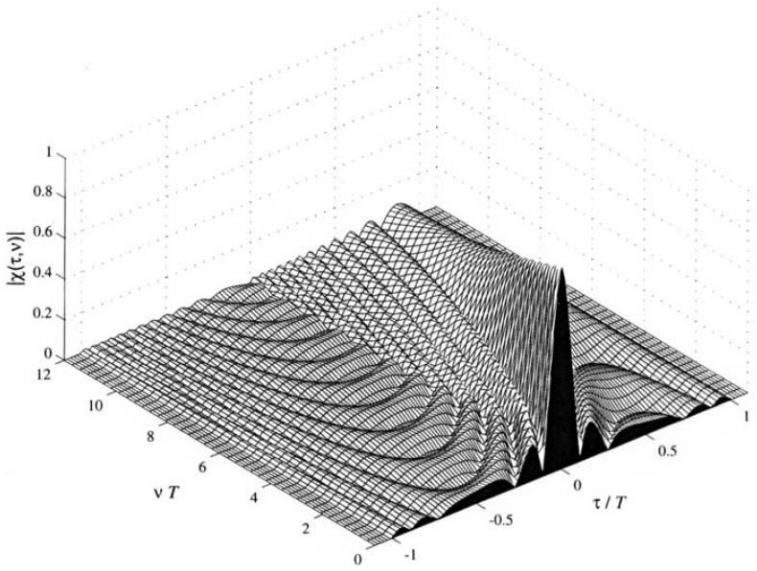




❖ *Antenna baseline crucial parameter determining geometry*

Estimation of FDoA

- **FDoA/DD (frequency difference / Doppler difference)**



CAF single Chirp pulse

FDoA: compute Cross-Ambiguity Function (CAF) function of signals at different antennas, estimate DD from CAF

$$A(\tau, f_D) = \int_0^T s_1(t) s_2^*(t+\tau) \exp(2\pi j f_D t)\, dt$$

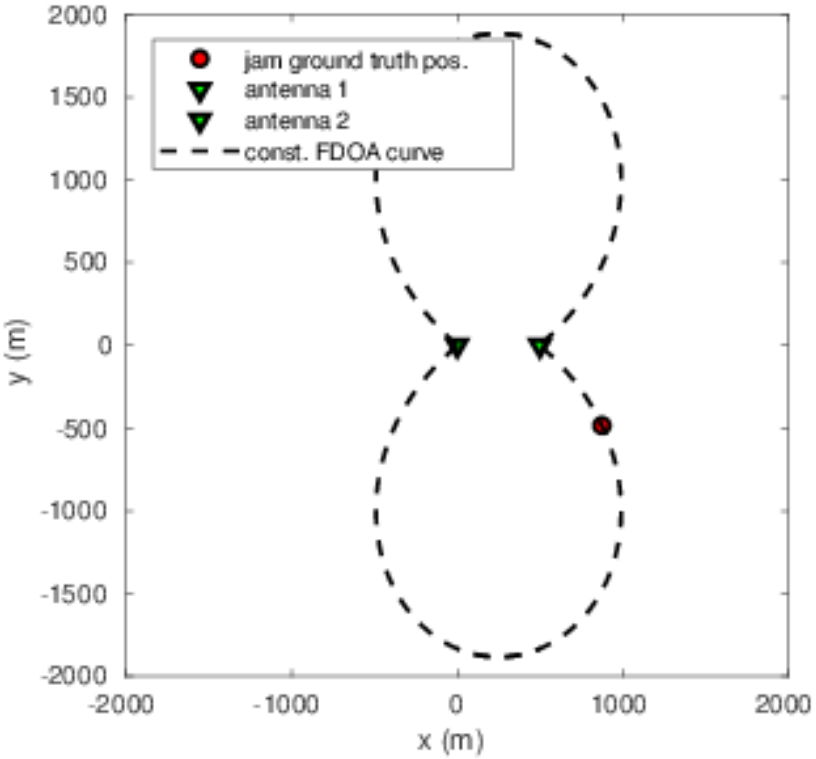
- *Frequency & time synchronized antennas and knowledge about centre frequency*
- Receiver and/or transmitter in motion

Estimation of Position from FDoA

- **FDoA/DD (frequency difference/Doppler difference)**

$$\theta_1 = \alpha_{v,1} + \arccos \frac{-\frac{\Delta f_{12} c}{f_c} + v_{r,2}}{\|v_1\|}$$

- Trilateration to compute position with pair of FDoAs, from *3 antennas* with *large baseline*, but also from 2 antennas at *different location*

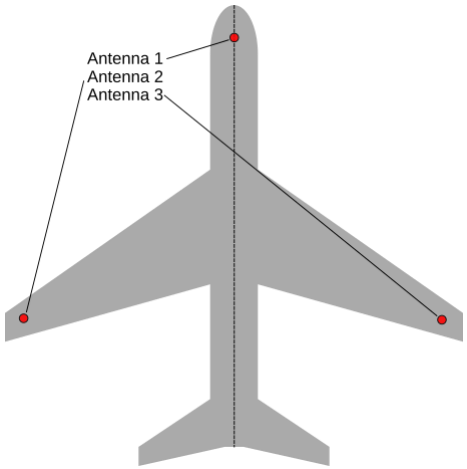


❖ *Time and frequency synchronized antennas and estimate of centre frequency*

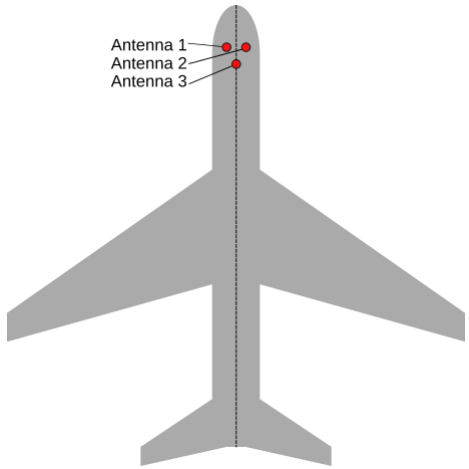
Jammer DF/localization scenario

- Jammer at 1000m distance at 119°
- Capon spectrum estimator (MVDR)
- cross-correlation function with phase transform (GCC-PHAT)
- linearized LS for TDoA based positioning

Large baseline (60m—10km) - TDoA

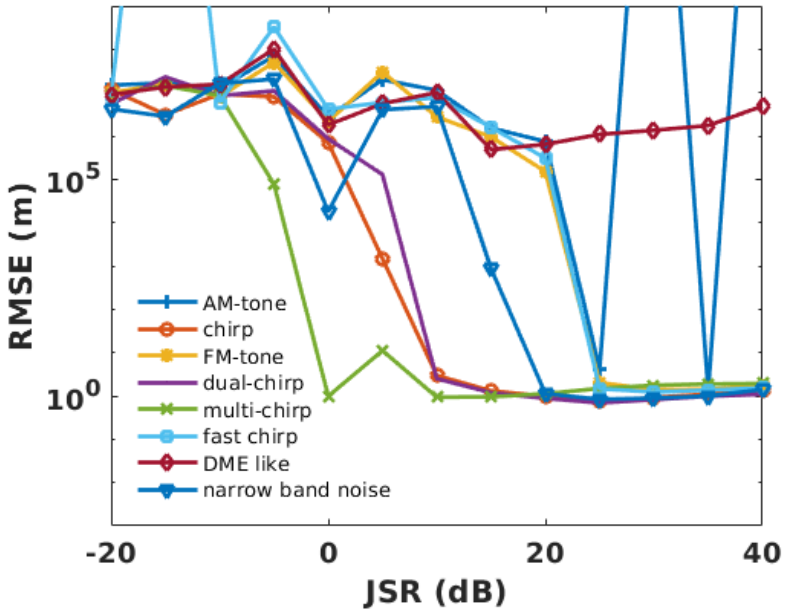


Small baseline (1m)- AoA

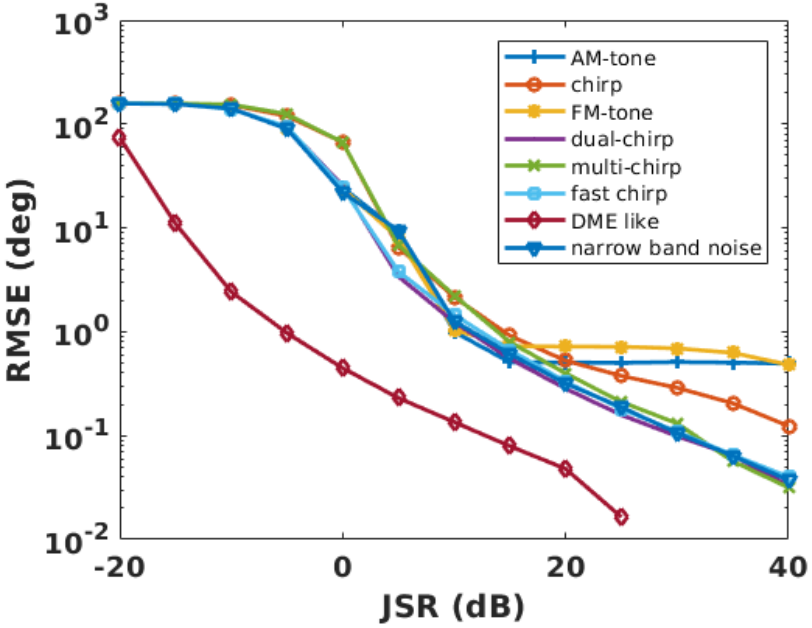


Jammer DF/localization results

Positioning using TDoA



Direction finding (AoA)



Assumptions / errors sources

- Antenna array calibration perfectly calibrated
- Narrowband signal and far field assumed for AoA model
- Receiver location/aircraft position perfectly known

Summary jammer DF/localization

AoA

- Antennas as array, array requires calibration
- Antenna elements closely spaced
- Narrowband signals (more complex for wideband signals)
- At least 3 elements for unambiguous DF

  - bearing only
  - 2D Positioning with 2 AoAs from different array locations

Summary jammer DF/localization

TDoA

- Synchronized antennas
- Antennas spacing in the order of receiver—emitter distance
- Wideband signals (not working for very narrowband signals)
- Interpolation of CC function for improved time resolution
- Less complex than AoA and FDoA

- Large antenna baseline for distant emitter
- 2D Positioning with 2 TDoAs from different array locations

Summary jammer DF/localization

FDoA

- Time & frequency synchronized antennas
- Narrowband signals
- Accurate FDoA are difficult to obtain
- More complex than TDoA and AoA

  - 2D Positioning with 2 FDoAs from different array locations

GATEMAN

Thank you very much for your attention!

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No [number]

SESAR JOINT UNDERTAKING

Founding Members

EUROPEAN UNION EUROCONTROL