GNSS Vulnerability to Spoofing Threats and a Review of Anti-Spoofing Techniques

Ali Broumandan, Ali Jafarnia Jahromi,
Saeed Daneshmand, Gérard Lachapelle

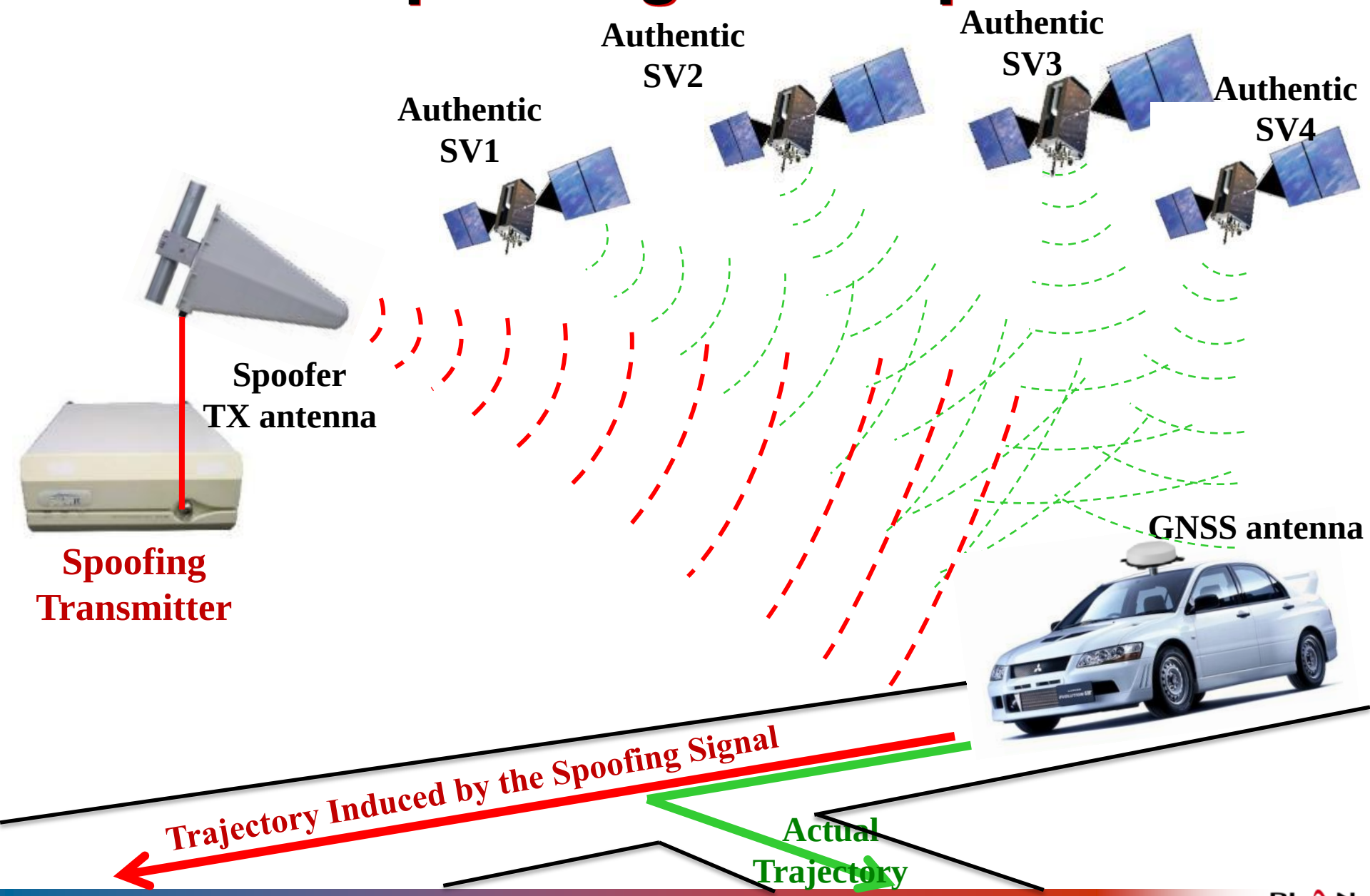
Position, Location And Navigation (PLAN) Group
Department of Geomatics Engineering
University of Calgary

ION Alberta Meeting
Friday January 24th, 2014

Outline

- Motivation and Background
- Spoofing and Anti-Spoofing Techniques
- Pre-Despreading Spoofing Detection
- Acquisition Level Analysis
- Tracking Level Analysis
- Position Level Authenticity Verification
- Synthetic Array Spoofing Detection
- Antenna Array Spoofing Mitigation
- Summary

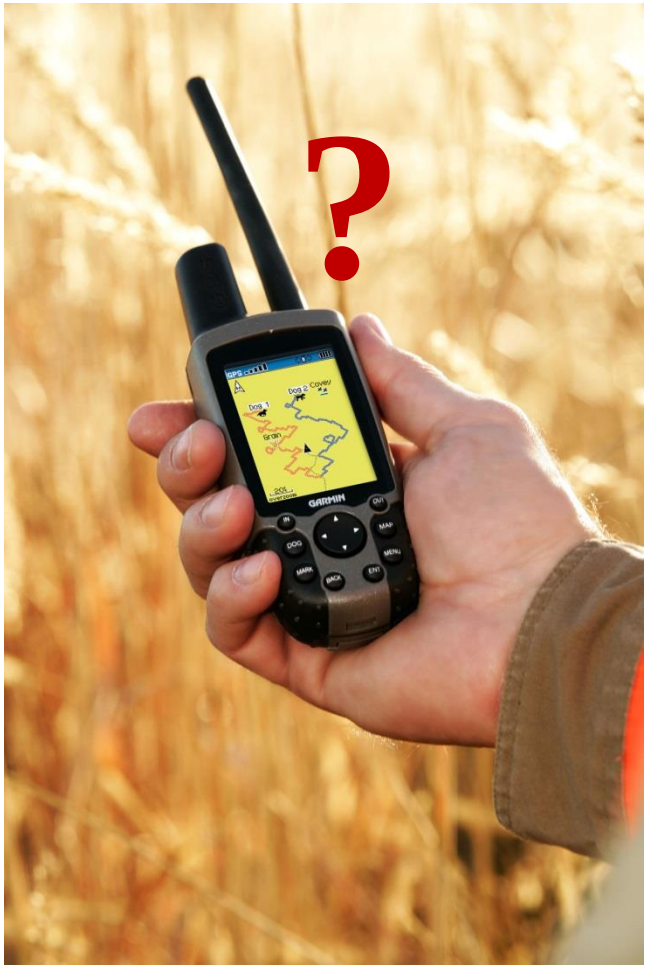
Spoofing Concept



Spoofing: A Different Type of Interference

Spoofing a deliberate interference that aims to mislead GNSS receivers into generating false PVT solution

- Spoofing signals: similar temporal and spectral characteristics to the authentic GNSS signals
- GNSS receivers are vulnerable
  - Known GNSS signal structure
  - Lack of authentication mechanism
- Spoofing is a serious threat
  - Not prohibitively costly
  - Significant motivations for spoofing due to wide-spread GNSS applications
  - Receiver is not aware of being spoofed (it is providing a PVT solution)



GPS Spoofing Headlight

- Mainstream make announcement on the vulnerability of GNSS to spoofing attack
- $80 million yacht hijacked
- Spoofing drone and UAS
- Vulnerability of timing systems

Vulnerability of Unmanned Vehicles to GPS Spoofing Attack

- Unmanned Aircraft Systems (UAS) and drones
- US congress has mandated the Security of Transportation to accelerate safety of civil unmanned aircraft systems
- Amazon is working on a new delivery system to get packages into customers' hands within 30 min using UAS

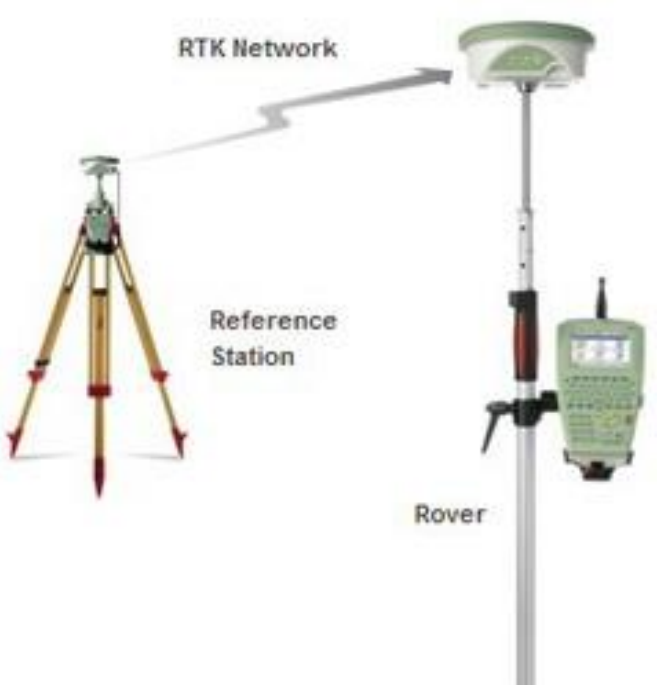
Vulnerability of Timing Systems to Spoofing Attack

- The Power Grid's Vulnerability to GPS Spoofing Attack
- Telecommunication links are using GPS time synchronization
- Stock Market time synchronization is mostly depend on civilian GPS

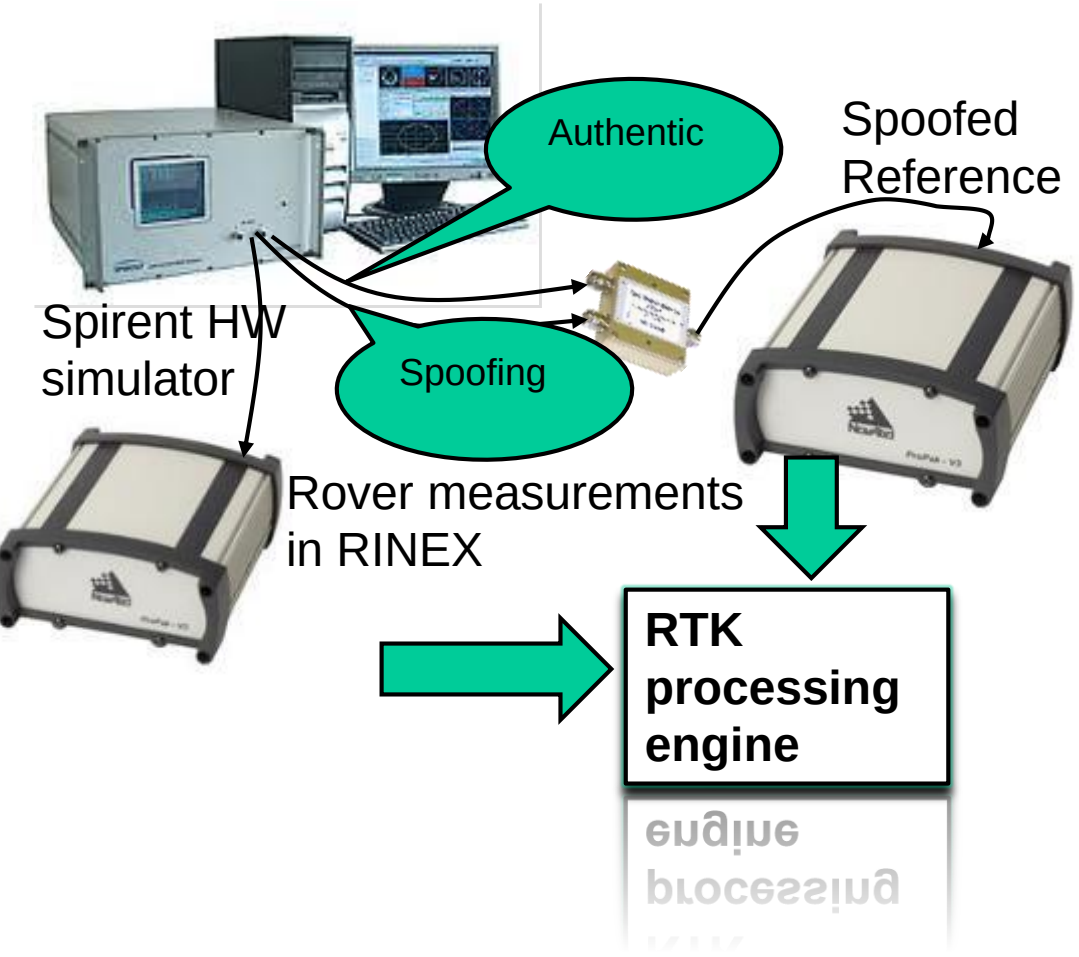
http://gpsworld.com/wirelessinfrastructuregoing-against-time-13278/

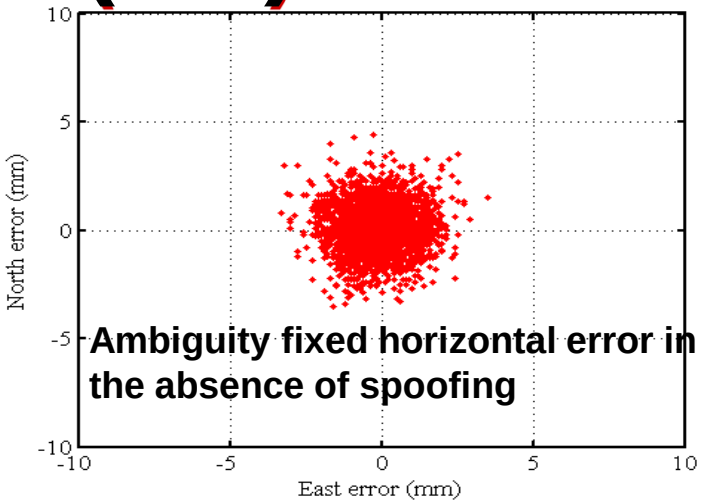
Vulnerability of RTK Application to Spoofing Attack (I/II)

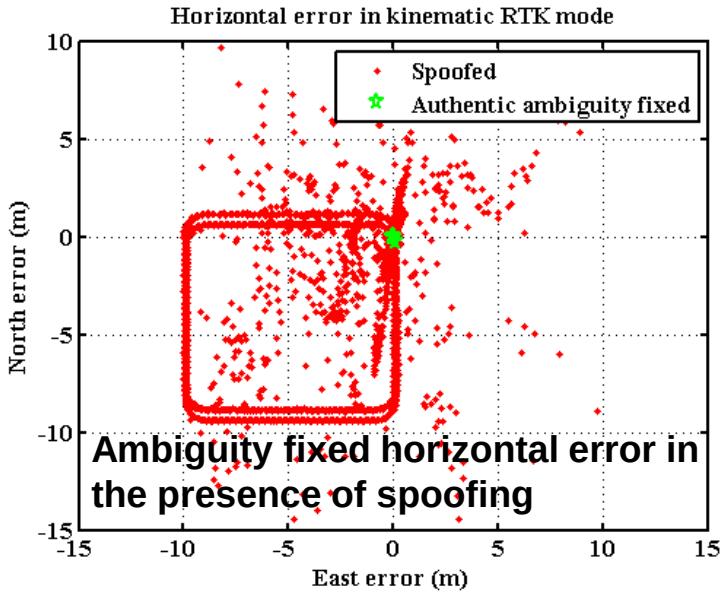
- RTK base stations are highly vulnerable to the spoofing attack
- What does to a rover position solution if the base station is spoofed?
- A two-channel hardware simulator and two NovAtel receivers in reference-rover scenario have been used to asses the spoofing vulnerability
- A spoofing attack is simulated for a RTK application where the spoofed horizontal trajectory of the base station is spoofed by 10 m



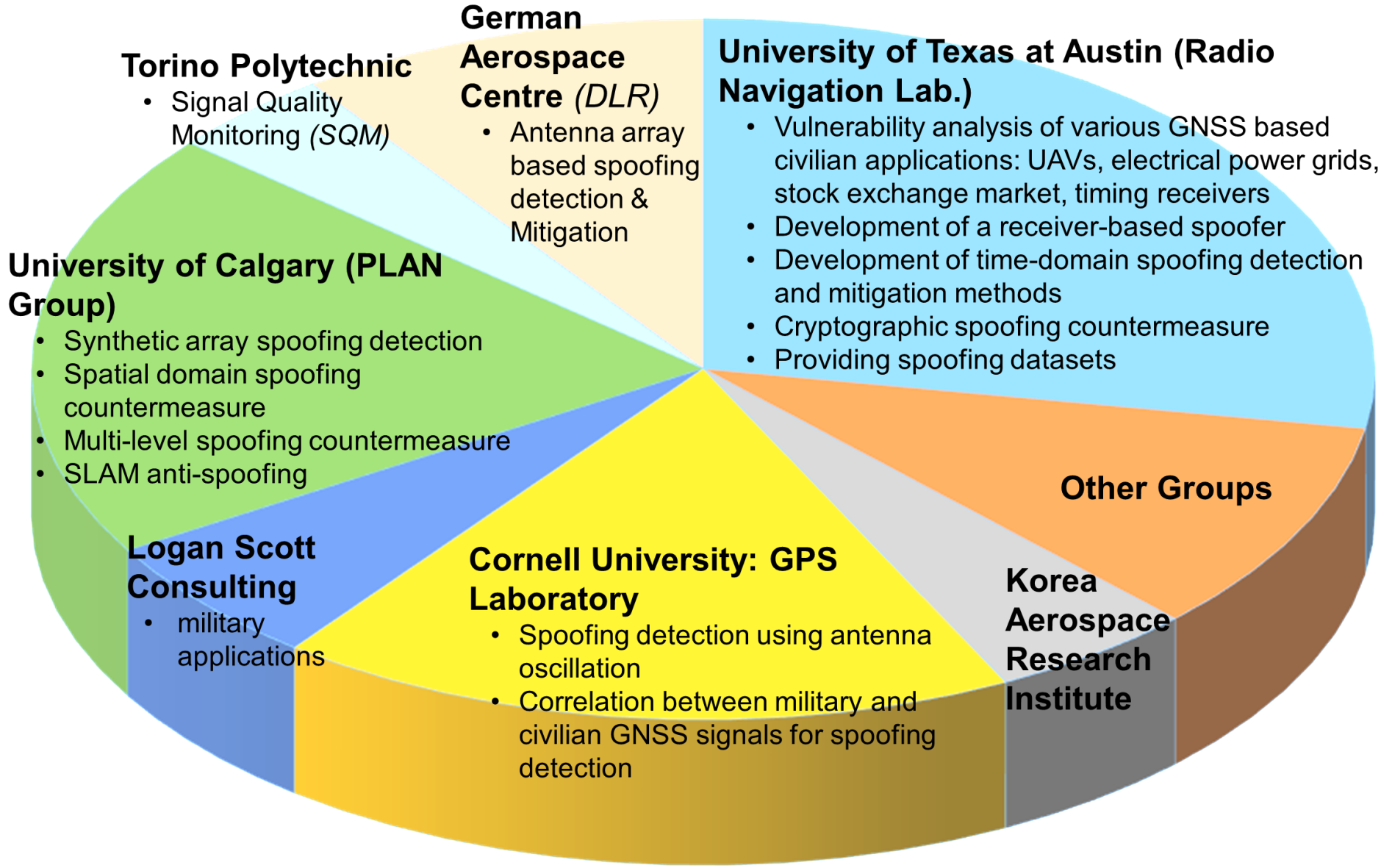
Vulnerability of RTK Application to Spoofing Attack (II/II)







Some Research Groups



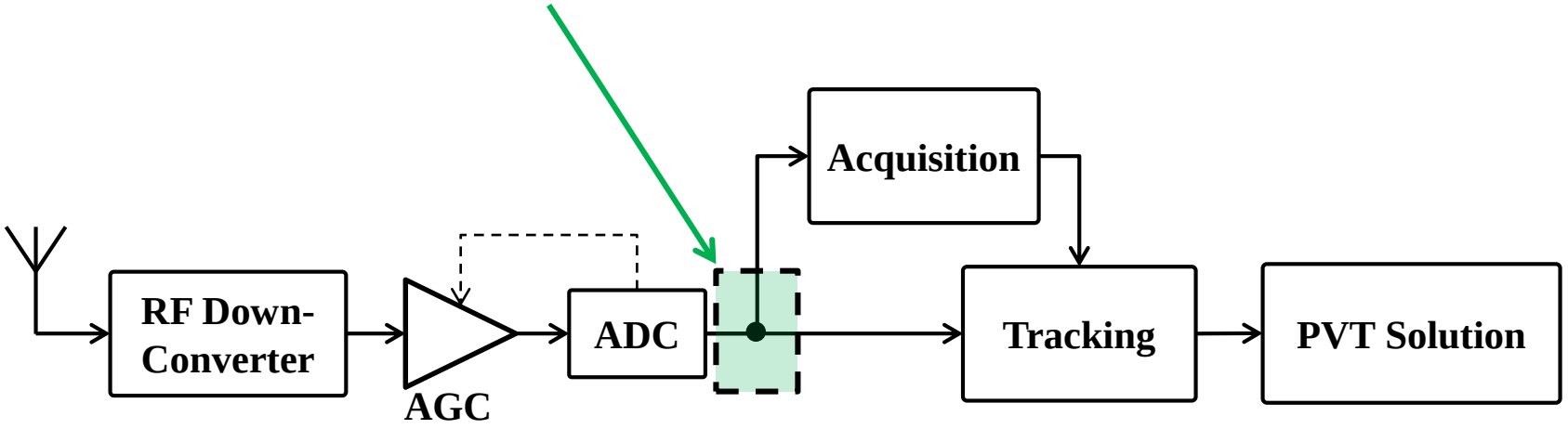
Spoofing Generation Categories

- **GPS signal generator**
  - Simplest spoofing technique but still very effective
- **Receiver based spoofer**
  - Spoofer is coupled to a GPS receiver
  - Hard to detect compared to GPS signal generator
  - Self jamming avoidance is an important issue
- **Advanced receiver based spoofer**
  - A receiver-spoofer with multiple antennas
  - Very hard to detect even for AOA estimator receivers
  - Very expensive and complex
  - Many practical implementation issues

Spoofing Countermeasure Methods

Positioning	**Receiver Autonomous Integrity Monitoring (RAIM)**	Integrity Check among Different Pseudorange Measurements
	Consistency Cross Check with Other Navigation Systems	Cross check with IMU solutions, Cross check with cellular and Wi-Fi positioning solutions
Data bit	**Time of Arrival (TOA) Methods**	Monitoring the bit transition boundaries
	Navigation Message Analysis	Consistency check among satellites navigation messages
Signal Processing	**Correlation Peak Monitoring**	Signal Quality Monitoring (SQM), Monitoring the distribution of correlation peak.
	Spatial Discrimination of Spoofing Signals	Antenna Array Processing, Synthetic Antenna Arrays
	Power Based Methods	C/N_0 Monitoring, Absolute Power Monitoring, L1/L2 Power level Comparison, …

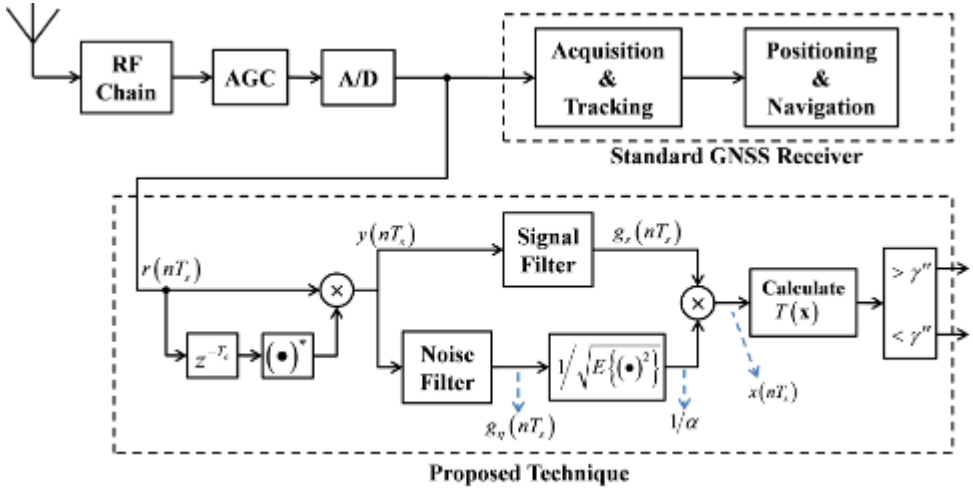
Pre-Despreading Analysis

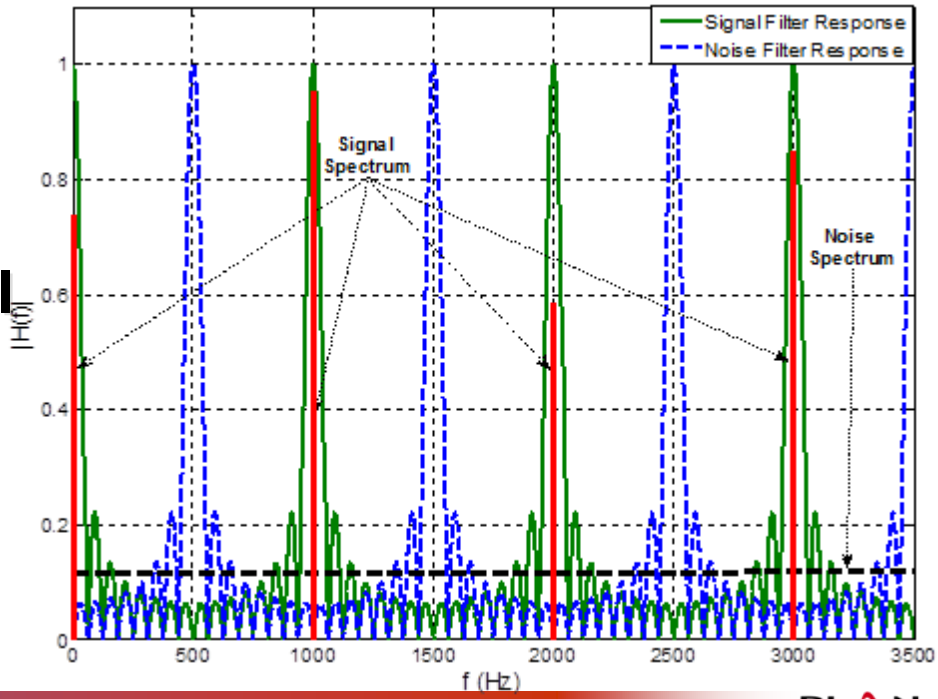


- Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2014) Pre-Despreading Authenticity Verification for GPS L1 C/A Signals. Navigation, Journal of The Institute of Navigation, in press.

Pre-Despreading Spoofing Detection

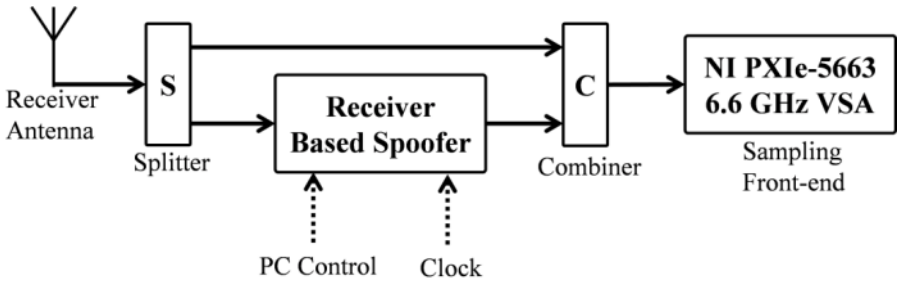
- Looking for abnormal power content of cyclo-stationary signals
- GPS L1 C/A
  - Line spectrum 1KHz spacing
  - Delay and Multiply (DAM)
- Processing method
  - Differential Doppler removal
  - Noise comb filtering
  - Signal comb filtering
  - Signal normalization
  - Spoofing detection

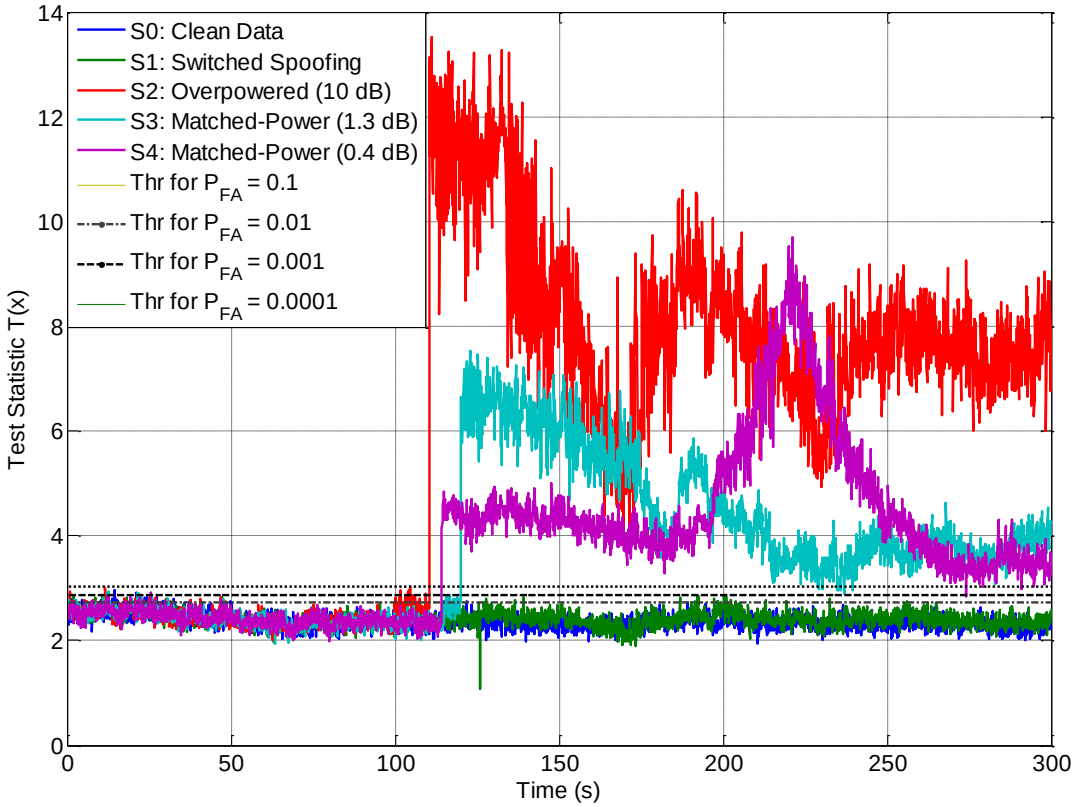




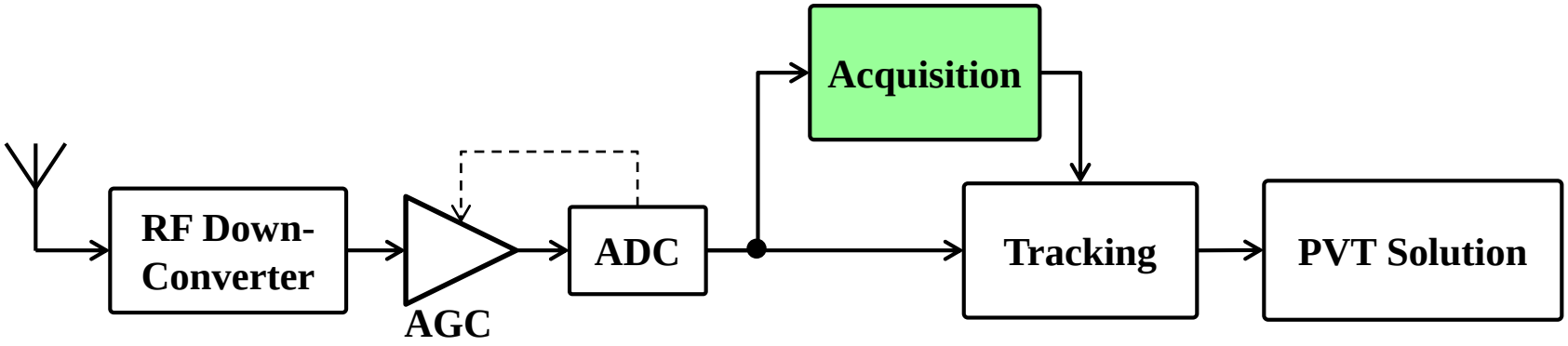
TEXBAT Data Processing

- **Spoofing datasets provided by RNL at Texas University at Austin**
- **Static spoofing scenarios**
  - **S1: Switched attack**
  - **S2: Overpowered** *(10 dB advantage)*
  - **S3: Matched Power** *(1.3 dB advantage)*
  - **S4: Matched Power** *(0.4 dB advantage)*
- **Spoofing starts after 100 s**





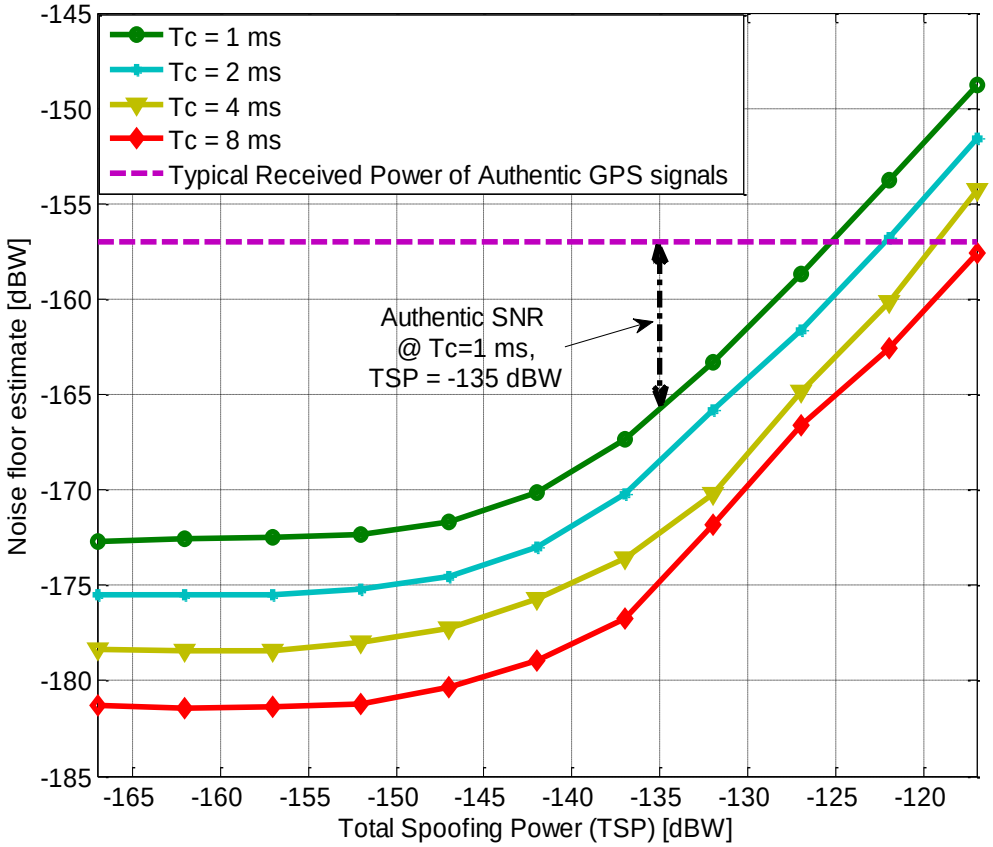
Acquisition Level Analysis



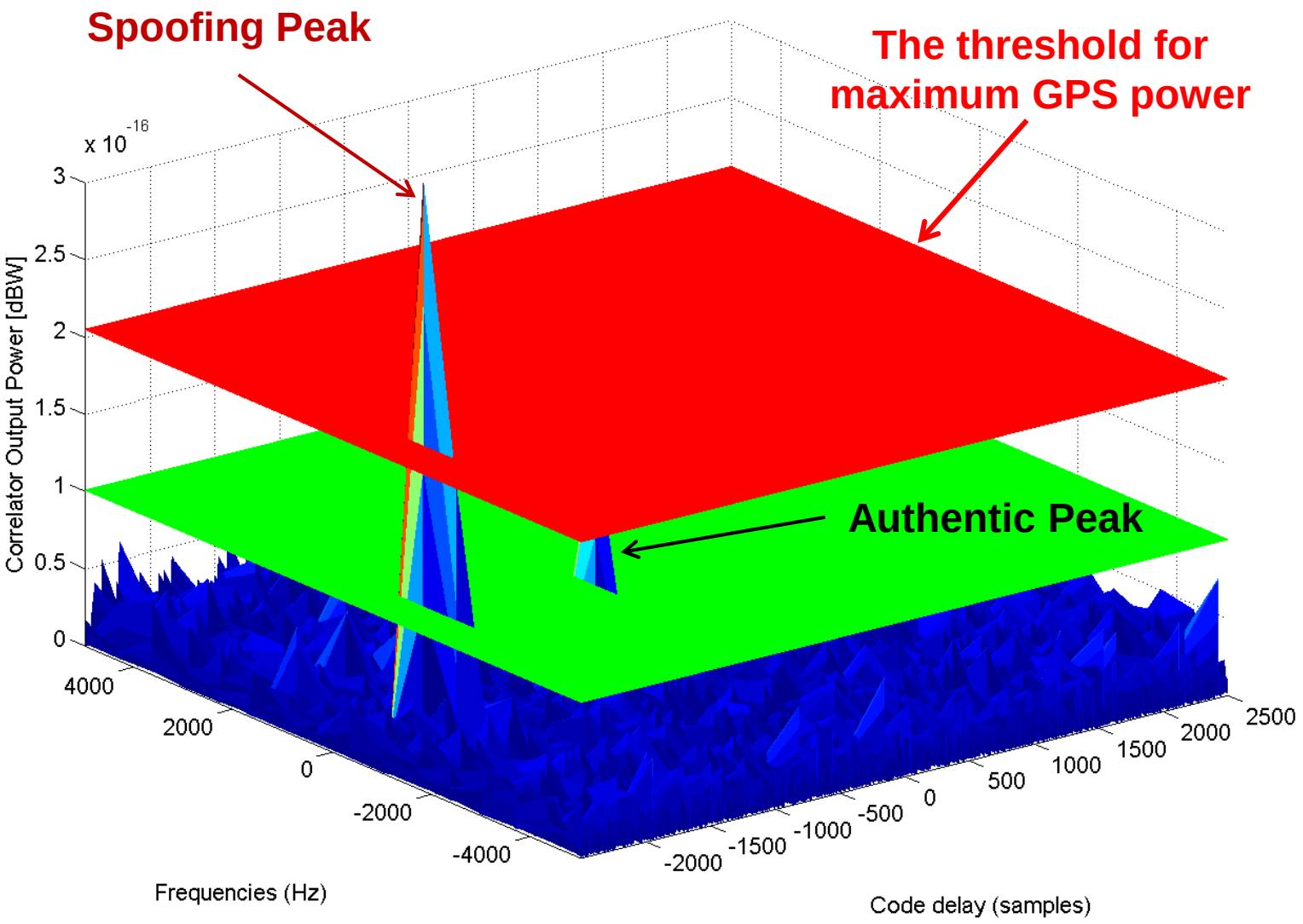
- Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012) *GPS Spoofer Countermeasure Effectiveness based on Using Signal Strength, Noise Power and C/No Observables*. International Journal of Satellite Communications and Networking, 30:181–191, DOI: 10.1002/sat.1012.
- Nielsen, J., V. Dehghanian and G. Lachapelle (2012) Effectiveness of GNSS Spoofing Countermeasure based on Receiver CNR Measurements. International Journal of Navigation and Observations, vol. 2012, Article ID 501679, 9 pages, 2012. doi:10.1155/2012/501679.
- Dehghanian, V., J. Nielsen and G. Lachapelle (2012) GNSS Spoofing Detection Based on Receiver C/No Estimates. Proceedings of GNSS12 (Nashville, TN, 18-21 Sep), The Institute of Navigation, 10 pages.

Acquisition Vulnerability to Spoofing

- Additional fake correlation peaks
  - Potentially misdirects the acquired PRN set, code delay and Doppler estimate
- Receiver noise floor increase
  - Generated by the cross correlation between spoofing PRNs and local replicas
  - Spoofing acts as a wide-band interference
  - Affects all the PRNs

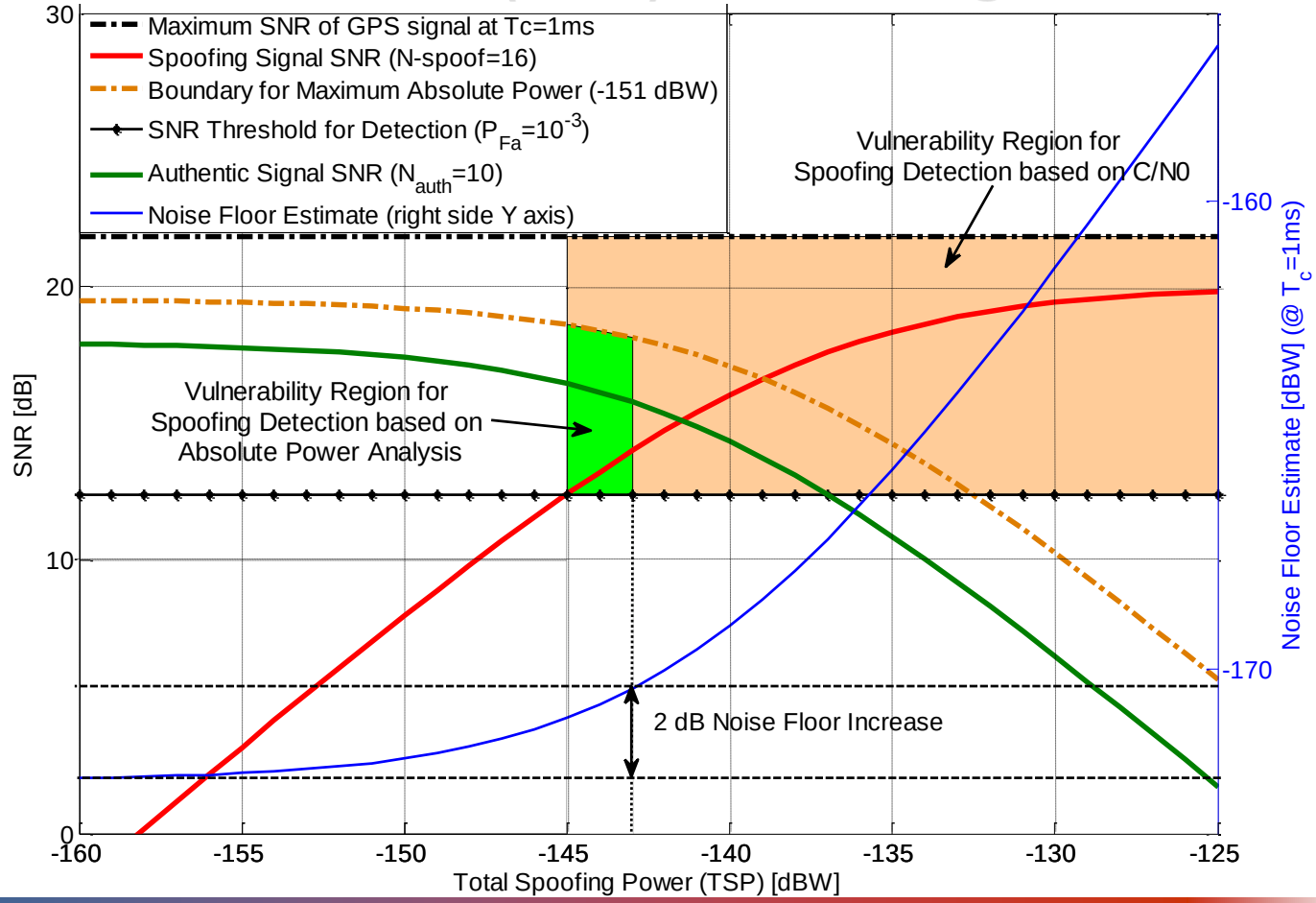


Multiple Thresholds in CAF

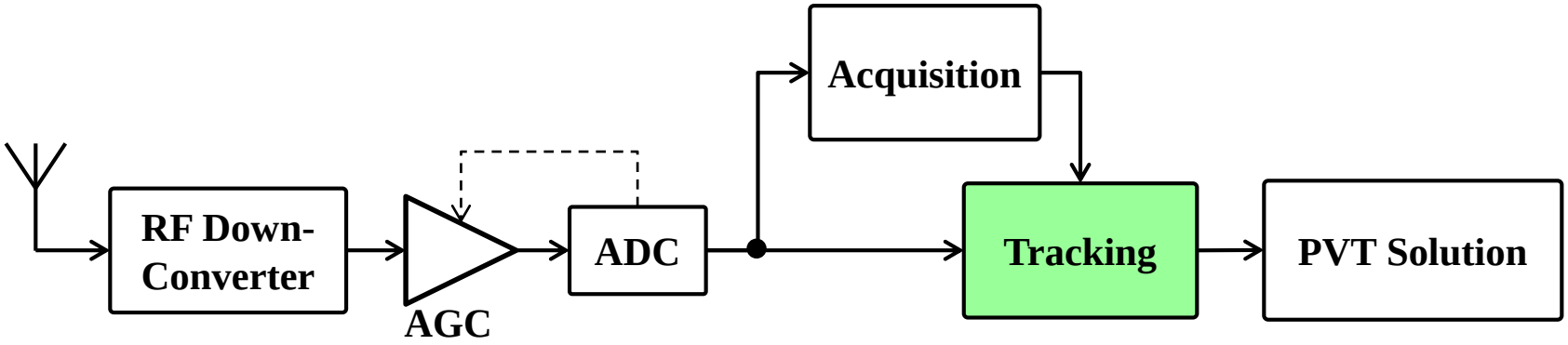


SNR vs. Absolute Power Monitoring

- **Absolute power monitoring**
  - **Signal level monitoring, Noise level monitoring**
- **Signal to Noise Ratio (SNR) monitoring**



Tracking Level Analysis



- Jafarnia-Jahromi, A., T. Lin, A. Broumandan, J. Nielsen and G. Lachapelle (2012) Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver. International Technical Meeting, Institute of Navigation, 30Jan-1Feb, Newport Beach, CA, 11 pages.
- Jafarnia-Jahromi, A. (2013) GNSS Signal Authenticity Verification in the Presence of Structural Interference. PhD Thesis, Report No. 20385, Department of Geomatics Engineering, University of Calgary

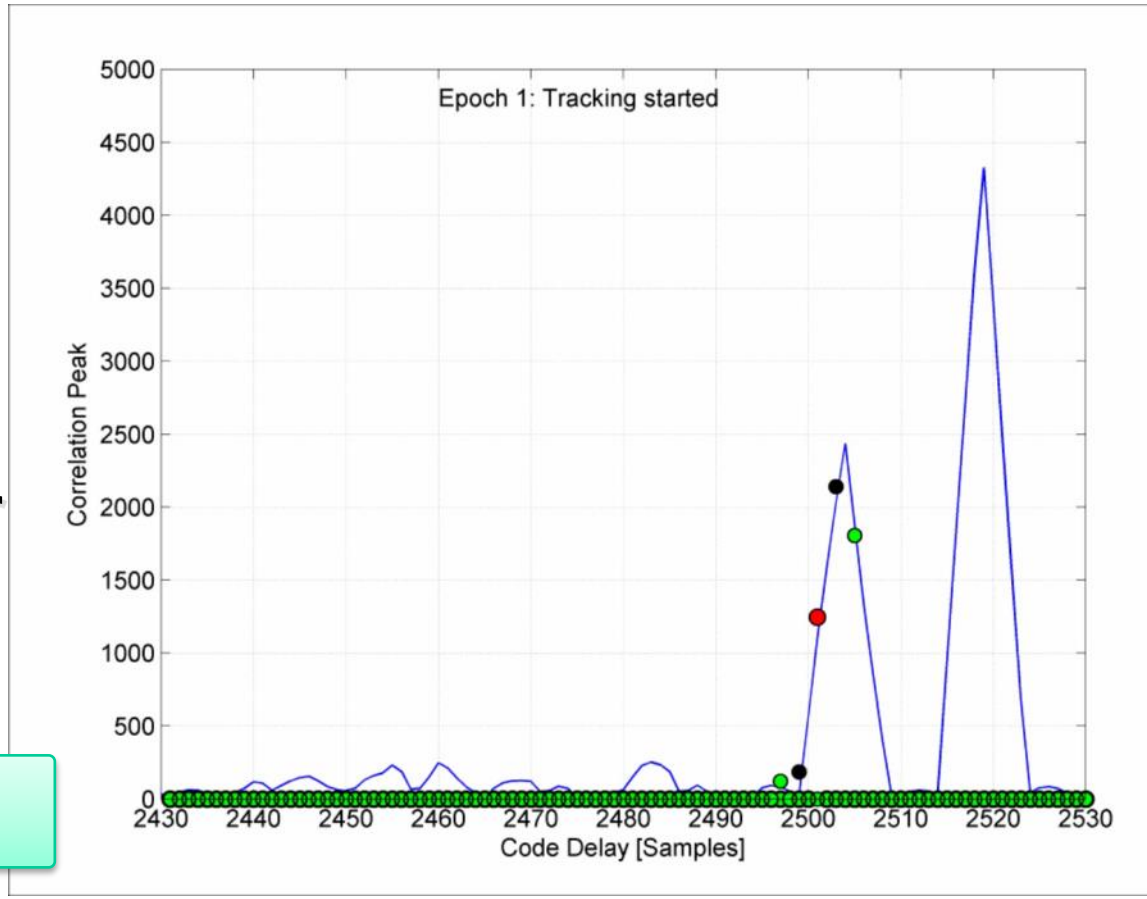
Spoofing Attack on Tracking Receivers

- **Tracking receiver**
  - **Focused on tracking authentic correlation peaks**
  - **Less vulnerable to non-aligned spoofing peaks**
- **Spoofer lifts-off the tracking point of the receiver**
- **Two categories:**
  - **Consistent Doppler**

$$\Delta f_l^{a,s}[k] = -f_{RF}\,\Delta\dot{\tau}_l^{a,s}[k]$$

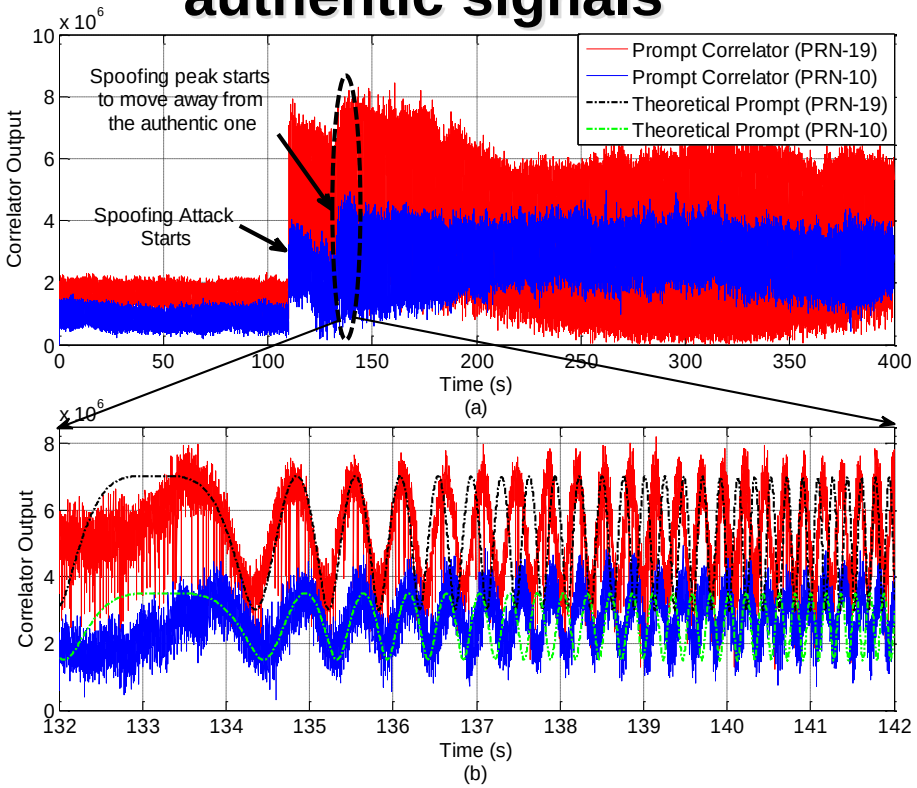
  - **Locked Doppler**

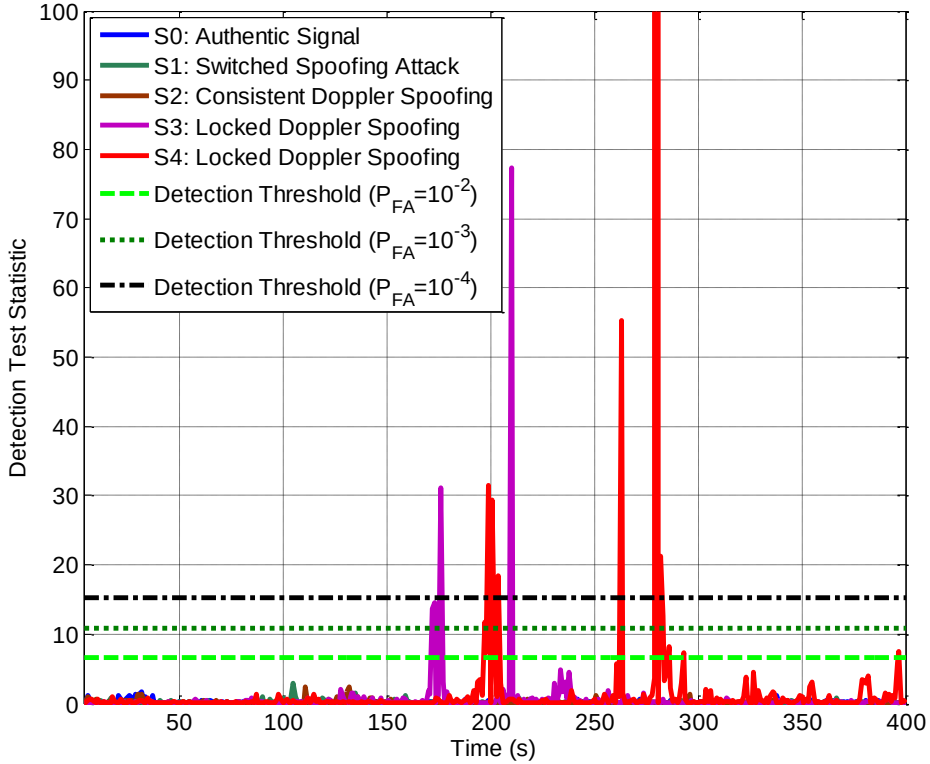
$$\Delta f_l^{a,s}[k] = 0 \rightarrow \Delta\varphi_l^{a,s}[k] = \Delta\phi_{l,0}^{a,s}$$



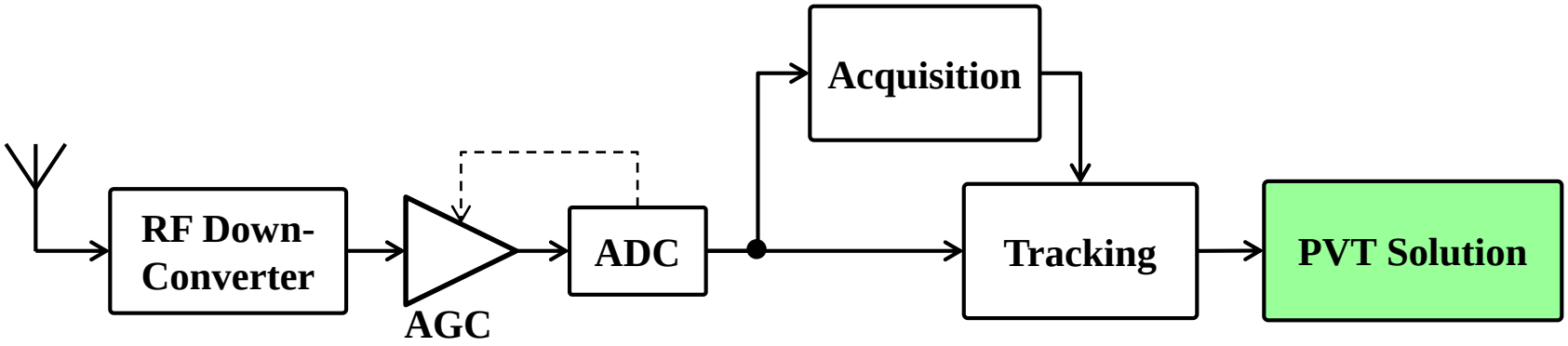
Spoofing Countermeasure during Tracking

- **Consistent Doppler:**
  - Amplitude fluctuations due to the interaction between spoofing and authentic signals
- **Locked Doppler:**
  - Consistency check between PLL and DLL loop filter outputs





Position Level Analysis



- Jafarnia-Jahromi, A., S. Daneshmand, A. Broumandan, J. Nielsen and G. Lachapelle (2013) PVT Solution Authentication Based on Monitoring the Clock State for a Moving GNSS Receiver, Proceedings of the European Navigation Conference (ENC2013), April 23-25, Vienna, Austria, 11 pages.

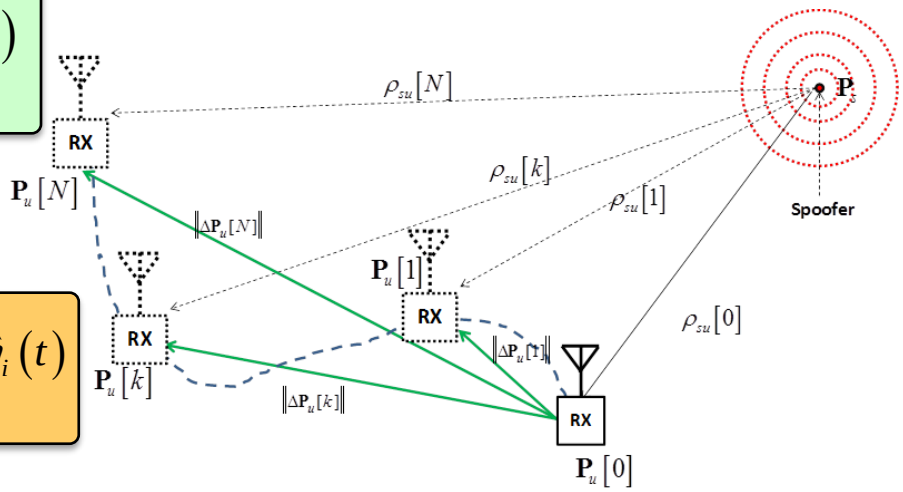
Position Level Authenticity Verification

- **Authentic pseudorange**

$$PR_i(t) = \underbrace{\rho_i(t)}_{\text{Specific to } PRN_i} + cdt_i(t) + \underbrace{c\,dT_u(t)}_{x(t)\text{: Common among all PRNs}} + \eta_i(t)$$

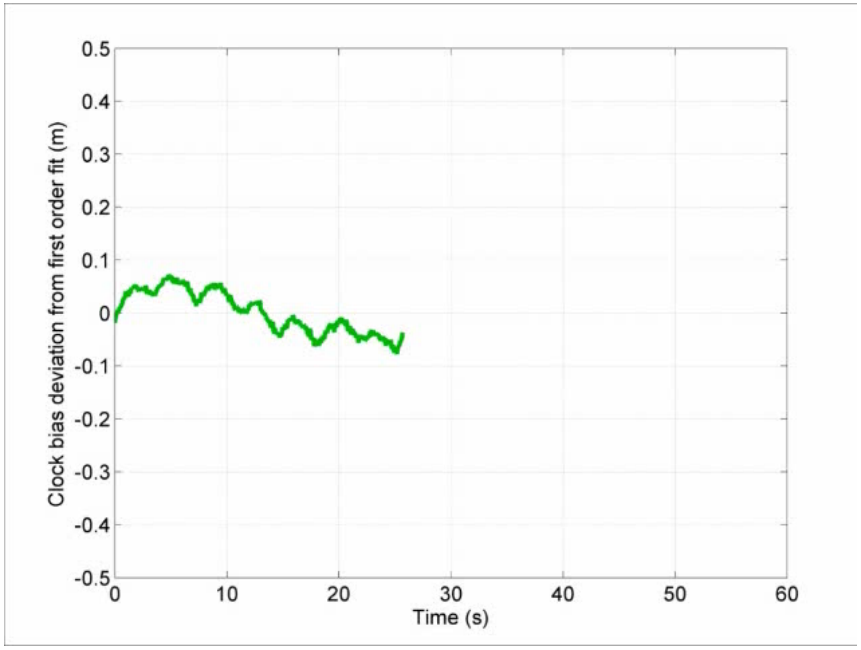
- **Spoofed pseudorange**

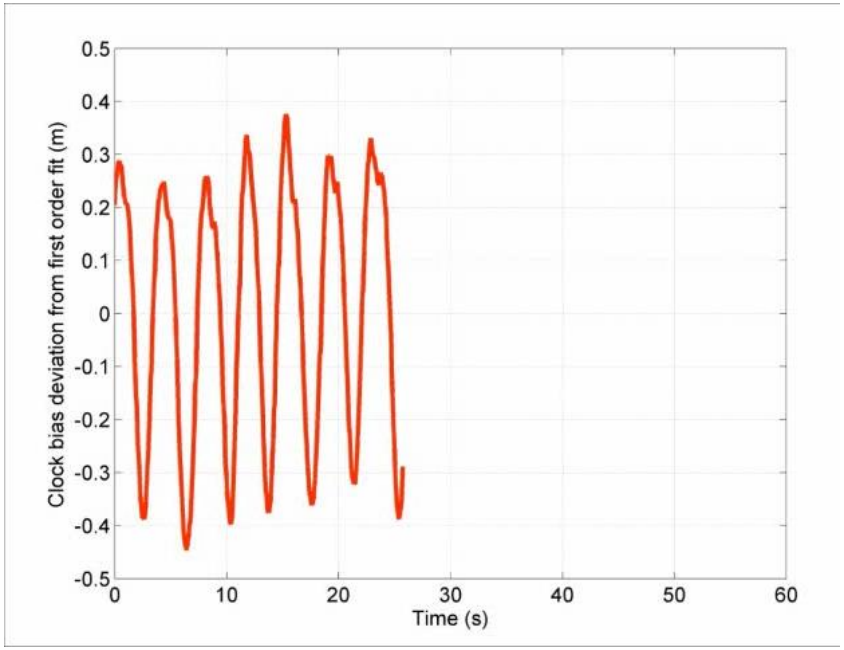
$$\hat{PR}_i(t) = \underbrace{\hat{\rho}_i(t) + cd\hat{t}_i(t)}_{\text{Specific to } PRN_i} + \underbrace{c\,dT_u(t) + \rho_{su}(t) - c.dT_s(t)}_{\hat{x}(t)\text{: Common among all PRNs}} + \hat{\eta}_i(t)$$



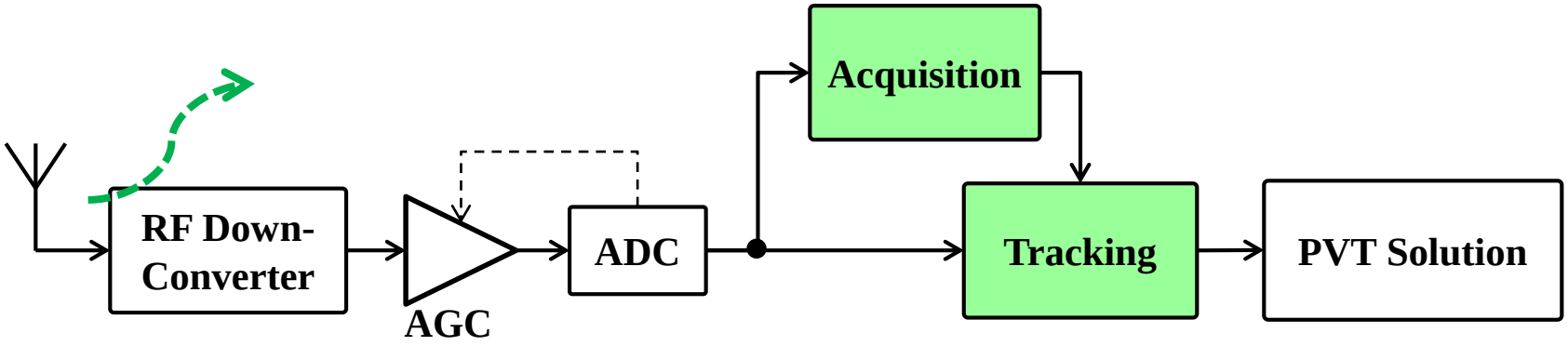
- **Spoofing Detection (the idea)**
  - Receiver motion causes pseudorange variation
  - All spoofing PRNs coming from the same source
  - Common spoofer-user range (ρ_{su}) variation
  - Clock state will be affected for a spoofed PVT solution

Handheld Circular Motion





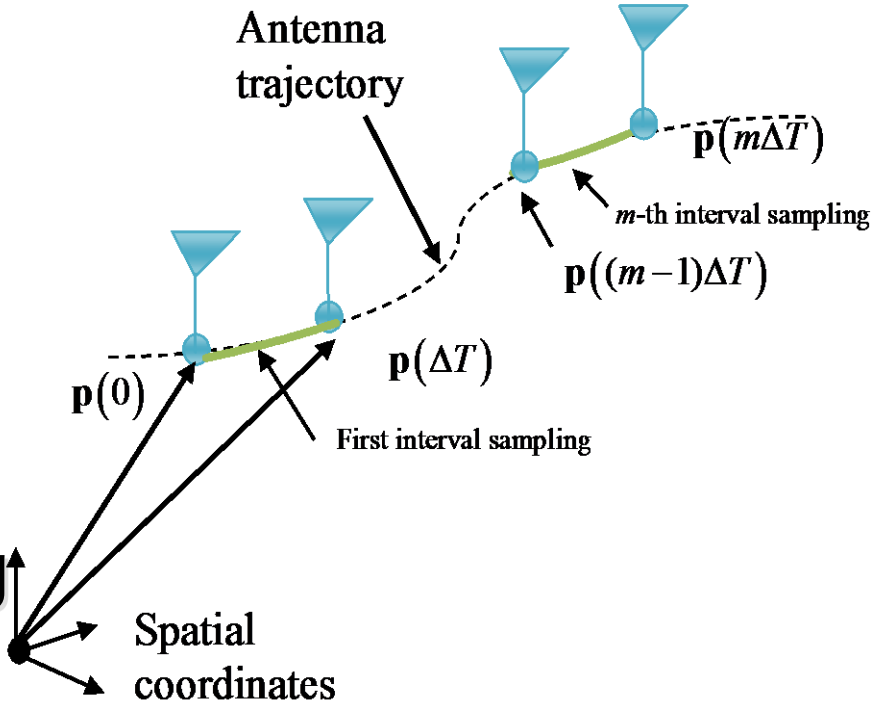
Synthetic Array Processing



- Broumandan, A., A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen and G. Lachapelle (2012) GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation. Proceedings of IEEE/ION PLANS 2012, Session B3, Myrtle Beach, SC, 24-26 April, 9 pages.
- Nielsen, J., A. Broumandan and G. Lachapelle (2011) GNSS Spoofing Detection for Single Antenna Handheld Receivers. NAVIGATION, 58, 4, 335-344.

Synthetic Array Processing

- **Spatial correlation coefficient is a metric to discriminate spoofing**
- **The processing interval is divided into *M* subintervals**
- $A_i^A(\mathbf{p}(t),t)$ **and** $A_i^S(\mathbf{p}(t),t)$ **are assumed constant during each subinterval**
- **The detection problem can be developed as**

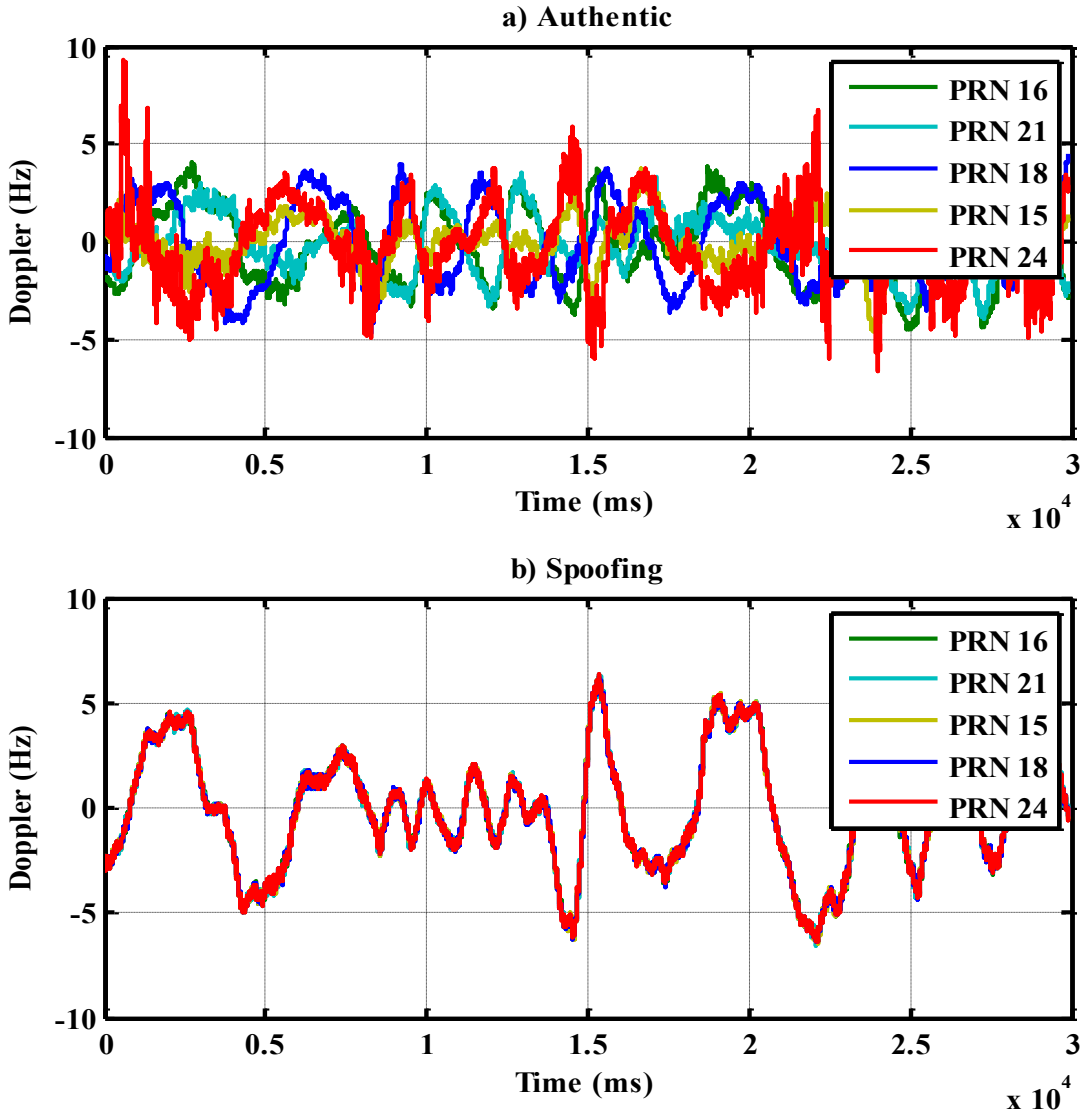


$$\mathbf{x}_i = \begin{cases} \mathbf{a}_i^S \times \boldsymbol{\alpha}_i^S + \boldsymbol{\eta}_i^S = \boldsymbol{\Lambda}_i^S + \boldsymbol{\eta}_i^S & H_1 \\ \mathbf{a}_i^A \times \boldsymbol{\alpha}_i^A + \boldsymbol{\eta}_i^A = \boldsymbol{\Lambda}_i^A + \boldsymbol{\eta}_i^A & H_0 \end{cases}$$

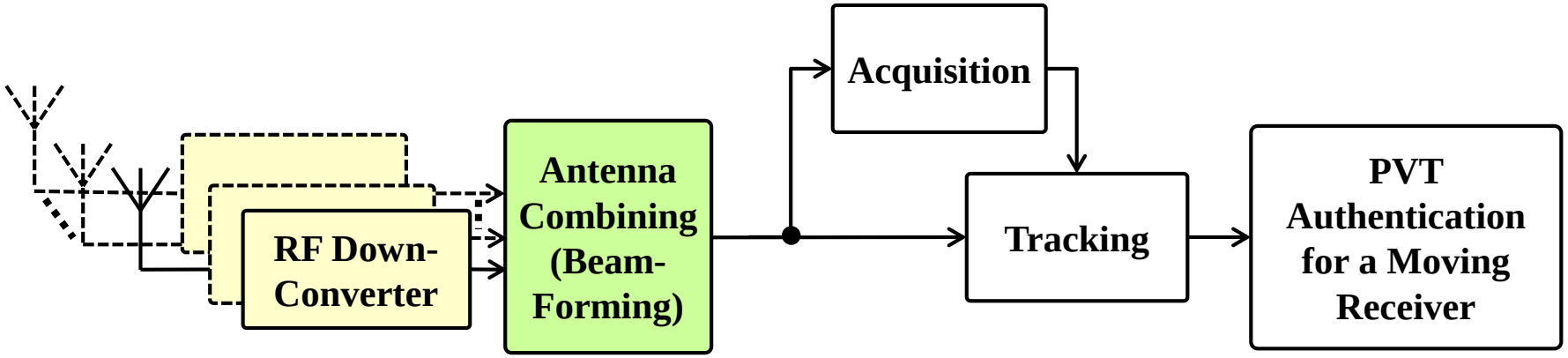
$$\rho_{ij} = \frac{E\left[\mathbf{x}_i \mathbf{x}_j^H\right]}{\sqrt{E\left[\mathbf{x}_i \mathbf{x}_i^H\right]}\sqrt{E\left[\mathbf{x}_j \mathbf{x}_j^H\right]}}.$$

Spoofing Discrimination based on Doppler Pairwise Correlation

- Measured Doppler due to the antenna motion for the authentic and spoofing signals
- Authentic Doppler values are uncorrelated while the spoofed ones are correlated



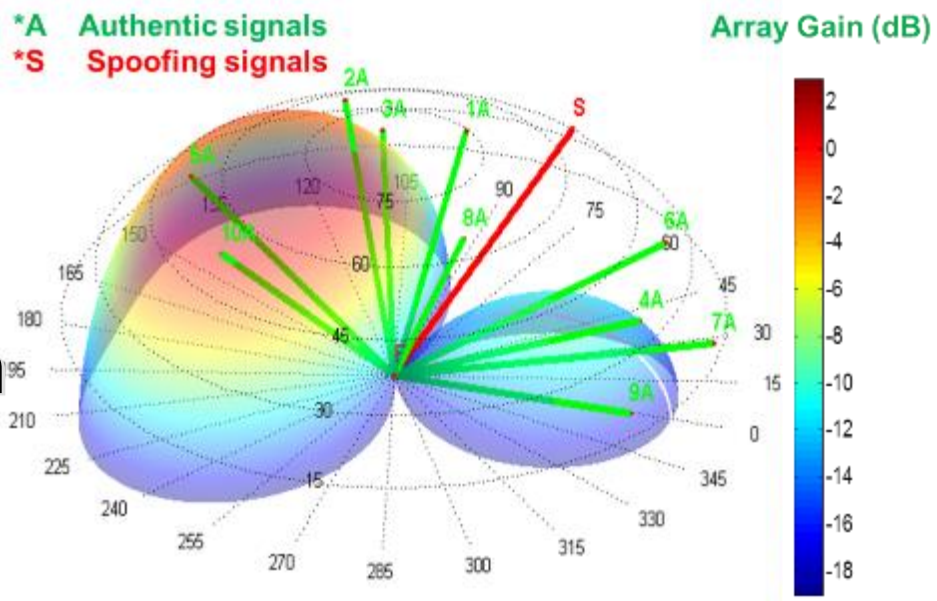
Antenna Array Processing



- Daneshmand, S., A. Jafarnia Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle (2013) GNSS Spoofing Mitigation in Multipath Environments Using Space-Time Processing, Proceedings of the European Navigation Conference (ENC2013), April 23-25, Vienna, Austria 12 pages.
- Daneshmand, S., A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle (2012) A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array. Proceedings of GNSS12 (Nashville, TN, 18-21 Sep), The Institute of Navigation, 11 pages.
- Daneshmand, S, A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle (2011) A Low Complexity GNSS Spoofing Mitigation Technique Using a Double Antenna Array. GPS World, 22, 12, 44-46.

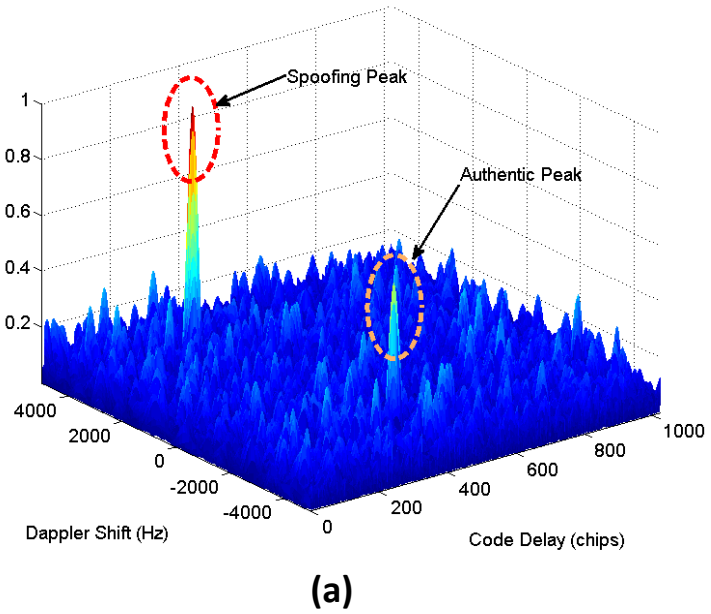
Antenna Array Processing

- **Each Signal has Specific Spatial Signature Vector (SSV)**
- **Spoofer spatial detection**
  - **Authentic signals**
    - ✓ **Different SSVs**
  - **Spoofing signals**
    - ✓ **All PRNs coming from the same source**
    - ✓ **The same SSV**
- **Spoofing mitigation**
  - **Spatial filtering (Null Steering)**

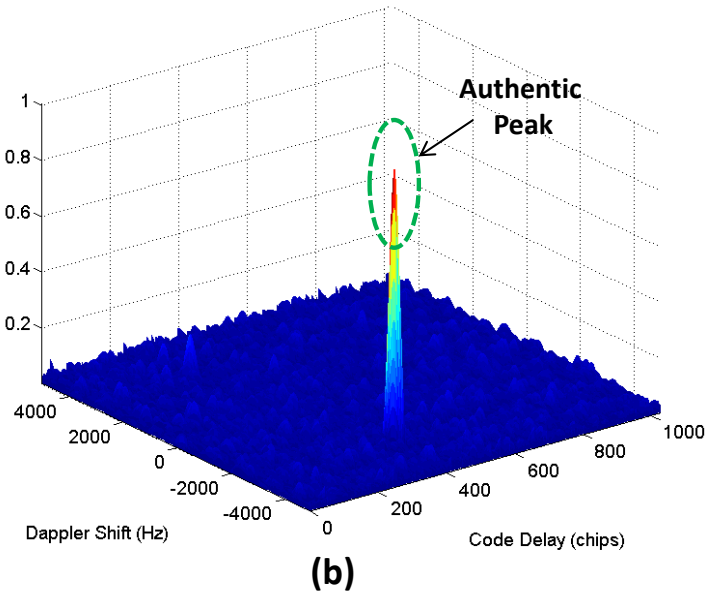


Nullifying Spoofing Signals

- Real-time operation
- Low computational complexity
- Pre-despreading operation
- Applicable for both civilian and military signals
- Array antenna considerations
  - No need for array calibration
  - Small antenna separation



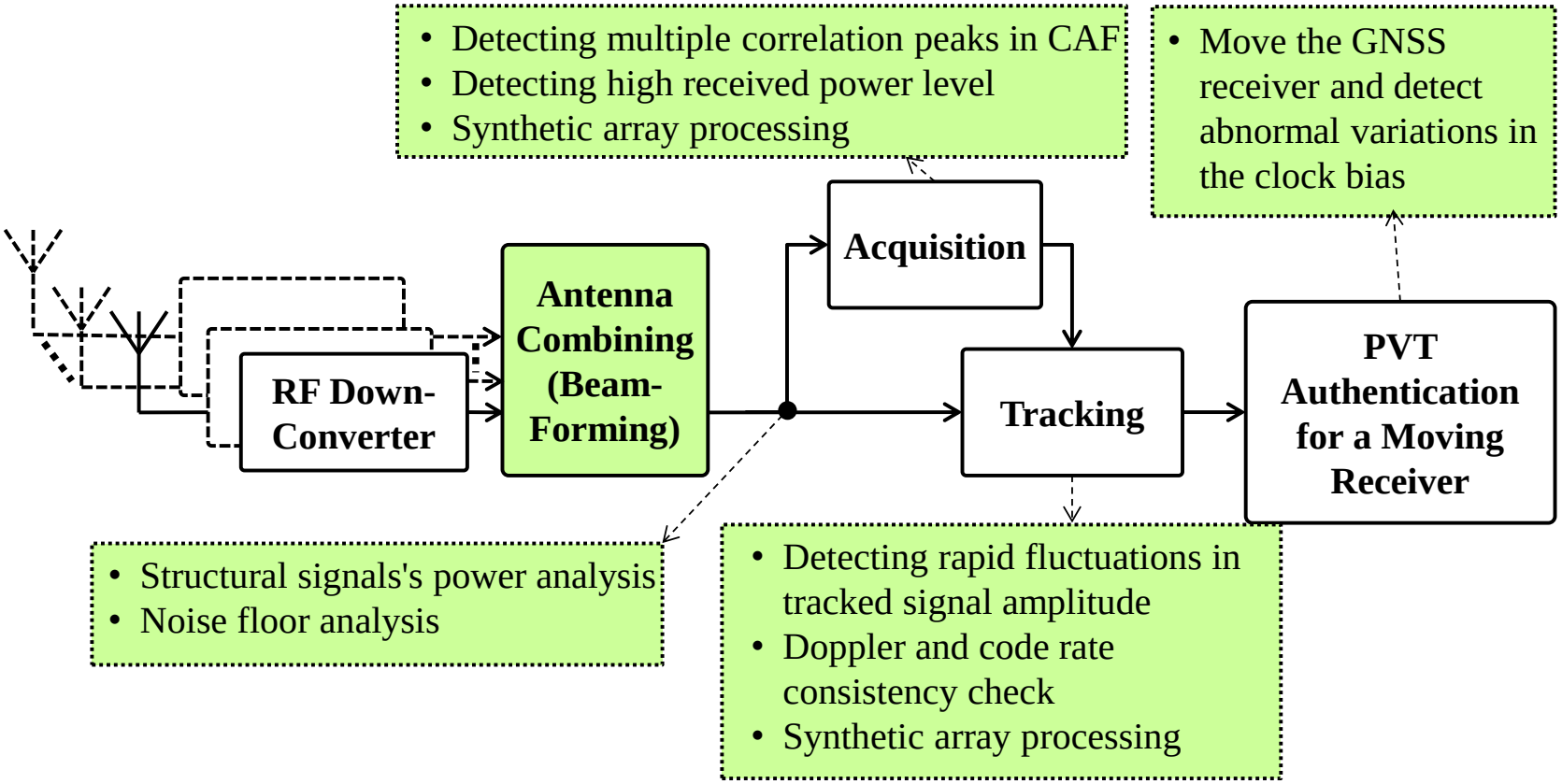
(a)



(b)

Summary

- **A possible structure of a stand-alone anti-spoofing GNSS receiver**
- **Increased resistance against spoofing signals**



References (1/2)

- http://plan.geomatics.ucalgary.ca/project_info.php?pid=26
- Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2014) Pre-Despreading Authenticity Verification for GPS L1 C/A Signals. Navigation, Journal of The Institute of Navigation, in press.
- Jafarnia-Jahromi, A. (2013) GNSS Signal Authenticity Verification in the Presence of Structural Interference. PhD Thesis, Report No. 20385, Department of Geomatics Engineering, University of Calgary
- Jafarnia-Jahromi, A., S. Daneshmand and G. Lachapelle (2013) Spoofing Countermeasures for GNSS Receivers – A Review of Current and Future Research Trends. Proceedings of Fourth Internantional Colloquium on Scientific and Fundamental Aspects of the Galileo Programme, Prague, 4-6 Dec 2013, 8 pages.
- Jafarnia-Jahromi, A., S. Daneshmand, A. Broumandan, J. Nielsen and G. Lachapelle (2013) PVT Solution Authentication Based on Monitoring the Clock State for a Moving GNSS Receiver, Proceedings of the European Navigation Conference (ENC2013), April 23-25, Vienna, Austria, 11 pages.
- Daneshmand, S., A. Jafarnia Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle (2013) GNSS Spoofing Mitigation in Multipath Environments Using Space-Time Processing, Proceedings of the European Navigation Conference (ENC2013), April 23-25, Vienna.
- Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012) GPS Vulnerability to Spoofing Threats and a Review of Anti-Spoofing Techniques. International Journal of Navigation and Observations, vol. 2012, Article ID 127072, 16 pages, 2012.
- Broumandan, A., A. Jafarnia-Jahromi, V. Dehgahanian, J. Nielsen and G. Lachapelle (2012) GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation. Proceedings of IEEE/ION PLANS 2012, Myrtle Beach, SC, 24-26 April, 9 pages.

References (2/2)

- Jafarnia-Jahromi, A., A. Broumandan, J. Nielsen and G. Lachapelle (2012) GPS Spoofer Countermeasure Effectiveness based on Using Signal Strength, Noise Power and C/No Observables. International Journal of Satellite Communications and Networking.
- Nielsen, J., V. Dehghanian and G. Lachapelle (2012) Effectiveness of GNSS Spoofing Countermeasure based on Receiver CNR Measurements. International Journal of Navigation and Observations, vol. 2012, Article ID 501679, 9 pages, 2012.
- Dehghanian, V., J. Nielsen and G. Lachapelle (2012) GNSS Spoofing Detection Based on Receiver C/No Estimates. Proceedings of GNSS12 (Nashville, TN, 18-21 Sep), The Institute of Navigation, 10 pages.
- Jafarnia-Jahromi, A., T. Lin, A. Broumandan, J. Nielsen and G. Lachapelle (2012) Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver. International Technical Meeting, ION, 30Jan-1Feb, Newport Beach, CA, 11 pages.
- Nielsen, J., A. Broumandan and G. Lachapelle (2011) GNSS Spoofing Detection for Single Antenna Handheld Receivers. NAVIGATION, 58, 4, 335-344.
- Daneshmand, S., A. Jafarnia-Jahromi, A. Broumandan and G. Lachapelle (2012) A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array. Proceedings of GNSS12 (Nashville, TN, 18-21 Sep), The Institute of Navigation, 11 pages.
- Daneshmand, S, A. Jafarnia, A. Broumandan and G. Lachapelle (2011) A Low Complexity GNSS Spoofing Mitigation Technique Using a Double Antenna Array. GPS World, 22, 12, 44-46.
- Nielsen, J., A. Broumandan and G. Lachapelle (2010) Spoofing Detection and Mitigation. GPS World, 21, 9 (September), 27-33.