THE UNIVERSITY OF TEXAS AT AUSTIN
RADIONAVIGATION LABORATORY

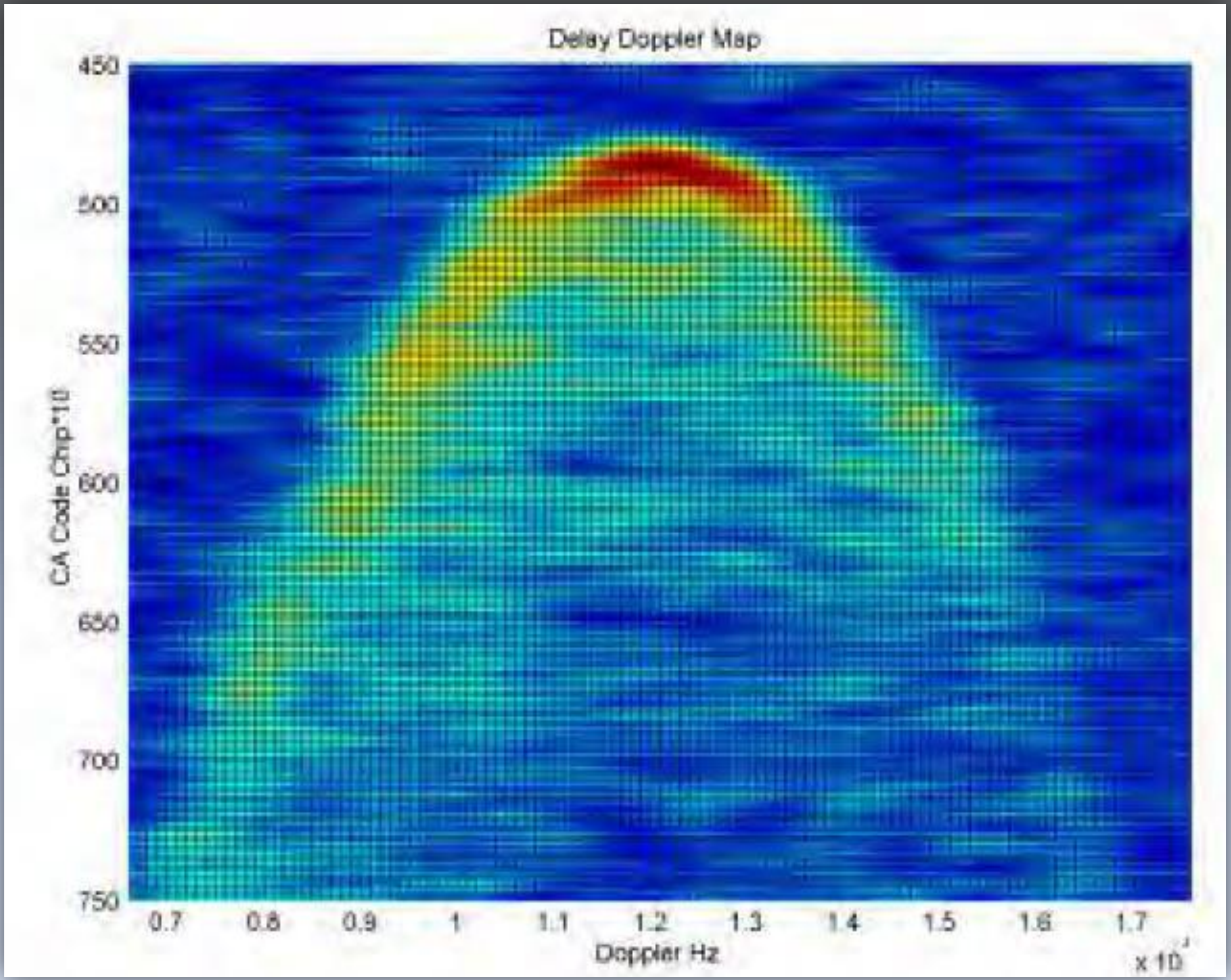
Toughening Techniques for GPS Receivers: *Navigation Message Authentication*

Todd Humphreys | Aerospace Engineering

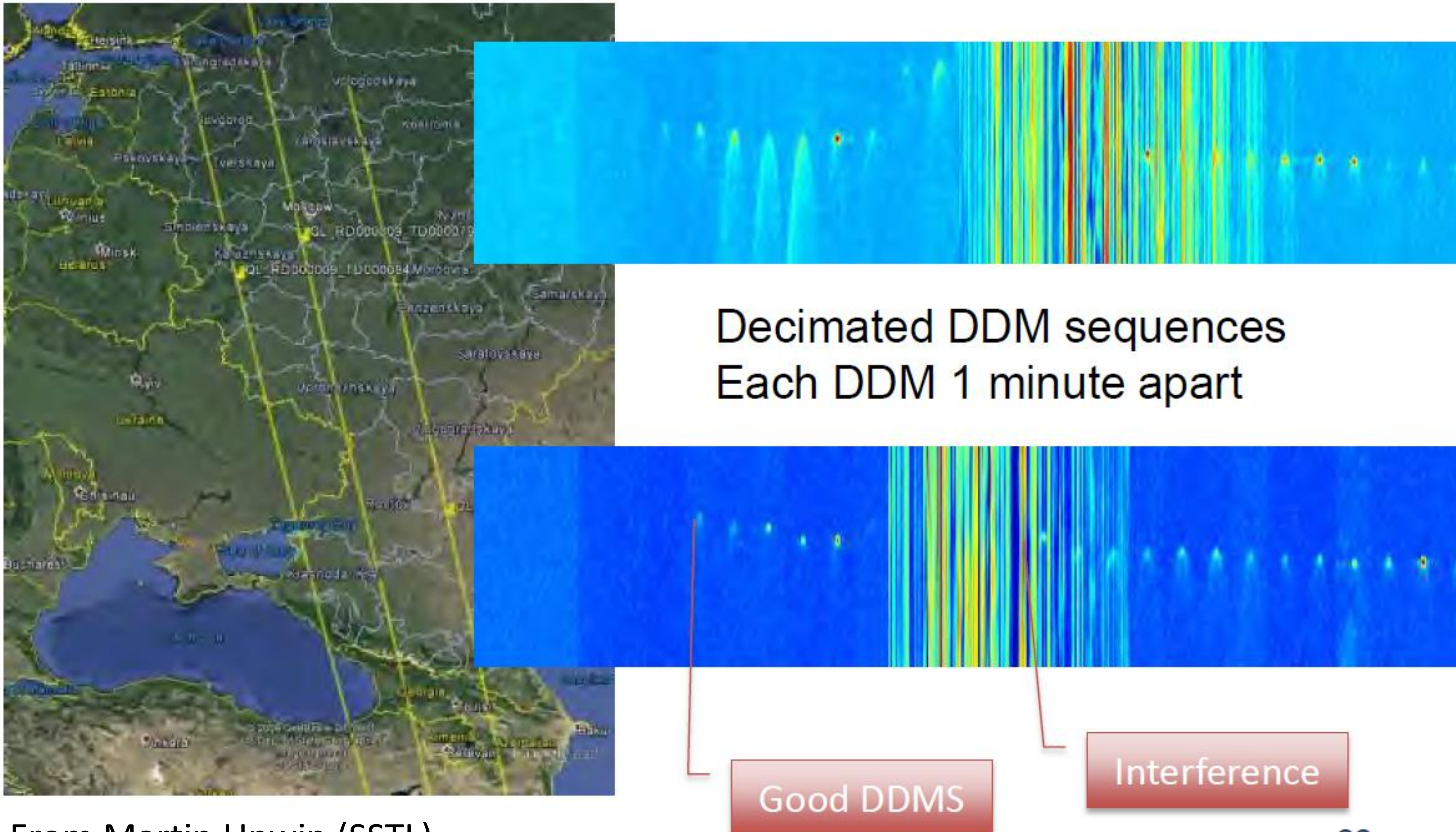
The University of Texas at Austin

PNT Advisory Board 15th Meeting | June 11, 2015

TechDemoSat-1, launched July, 2014
(SSTL, University of Surrey)



Delay-Doppler map used to measure sea state, detect ice edge, possibly measure soil moisture



From Martin Unwin (SSTL)

22

Autumn 2014: DDMs over eastern Europe exhibit striping corruption. Cause: structured interference in GPS L1 band with structure similar to C/A code. Similar patterns manifest elsewhere around globe.

Civil GPS spoofing has been demonstrated in the laboratory and in controlled field tests; deliberate hostile spoofing has been detected in the wild.

At present, civil GPS spoofing is a rare, minor nuisance.

But experiments demonstrate that spoofing effects can be serious, especially for critical infrastructure.

Is the threat of civil GPS spoofing serious enough to warrant a change to the GPS signal-in-space?

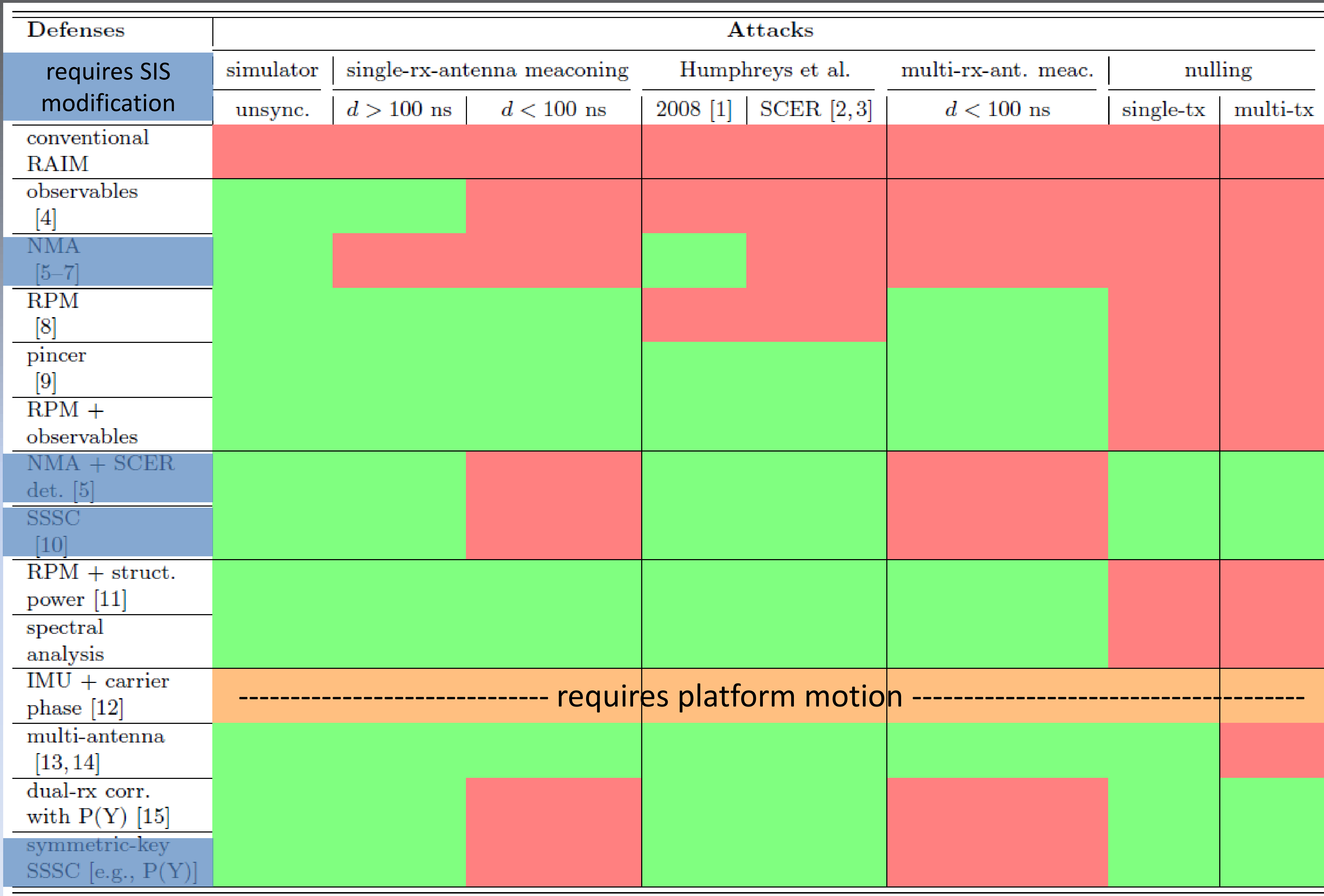
Q1: How effective are receiver-side spoofing defenses?

Q2: How effective are SIS-side spoofing defenses?

Q3: By how much would such defenses increase receiver cost?

Defenses	Attacks							
	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13,14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								

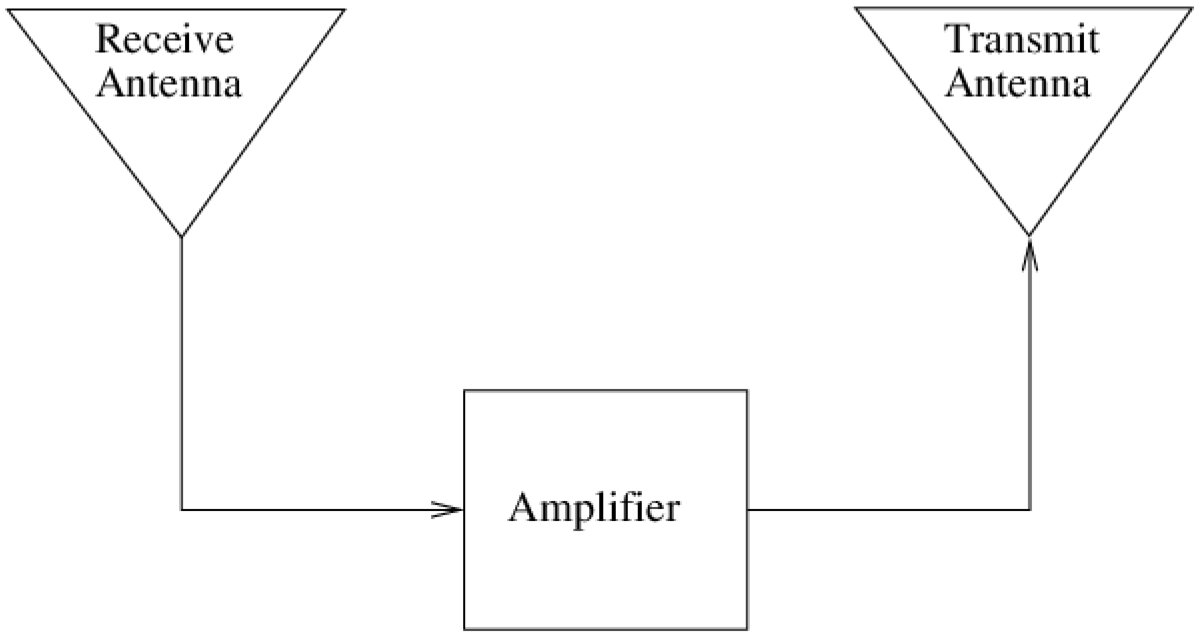

Defenses
Attacks
simulator
single-rx-antenna meaconing
Humphreys et al.
multi-rx-ant. meac.
nulling
unsync.
$d > 100$ ns
$d < 100$ ns
2008 [1]
SCER [2, 3]
$d < 100$ ns
single-tx
conventional RAIM
observables [4]
NMA [5–7]
RPM [8]
pincer [9]
RPM + observables
NMA + SCER det. [5]
SSSC [10]
RPM + struct. power [11]
spectral analysis
IMU + carrier phase [12]
multi-antenna [13, 14]
dual-rx corr. with P(Y) [15]
symmetric-key SSSC [e.g., P(Y)]
Increasing cost of attack
Increasing receiver-side cost of defense


Defenses
Attacks
requires SIS modification
simulator
single-rx-antenna meaconing
Humphreys et al.
multi-rx-ant. meac.
nulling
unsync.
d > 100 ns
d < 100 ns
2008 [1]
SCER [2, 3]
d < 100 ns
single-tx
multi-tx
conventional RAIM
observables [4]
NMA [5–7]
RPM [8]
pincer [9]
RPM + observables
NMA + SCER det. [5]
SSSC [10]
RPM + struct. power [11]
spectral analysis
IMU + carrier phase [12]
------------------------------ requires platform motion ------------------------------
multi-antenna [13, 14]
dual-rx corr. with P(Y) [15]
symmetric-key SSSC [e.g., P(Y)]

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								

Inexpensive (< $5k) COTS signal simulator/record-and-replay devices enable low-cost unsynchronized spoofing and meaconing

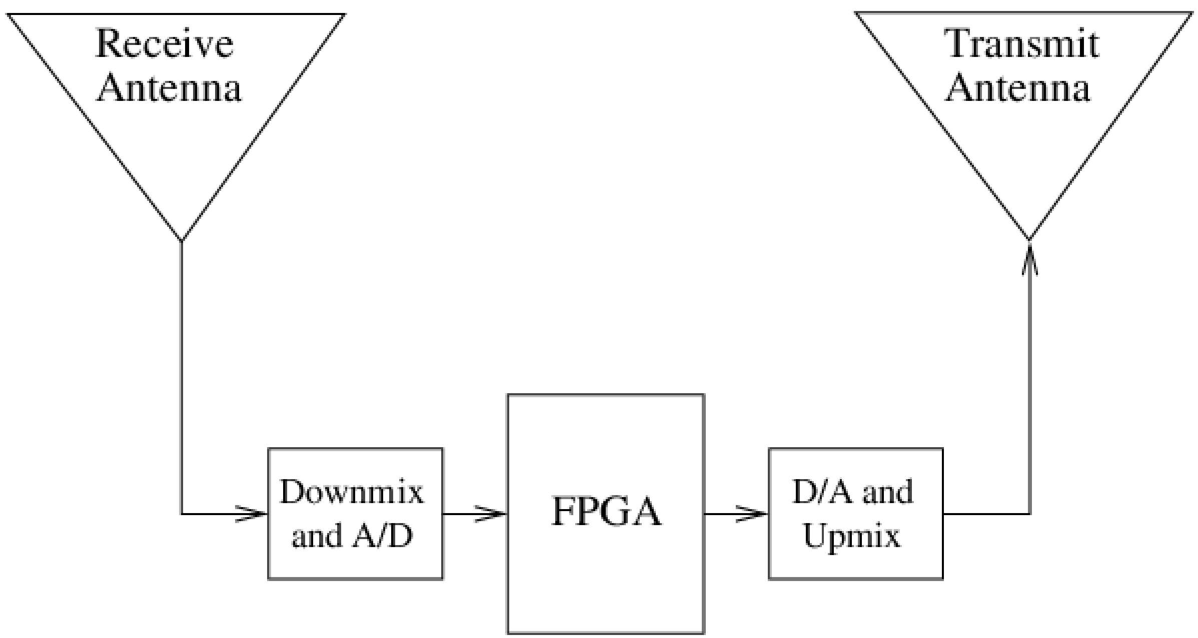
Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13,14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



Synchronized (d < 100 ns) meaconing possible with a simple setup:
rx antenna → amplifier → tx antenna

Variable delay requires:
downconversion → A2D → FPGA → D2A → upconversion

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								

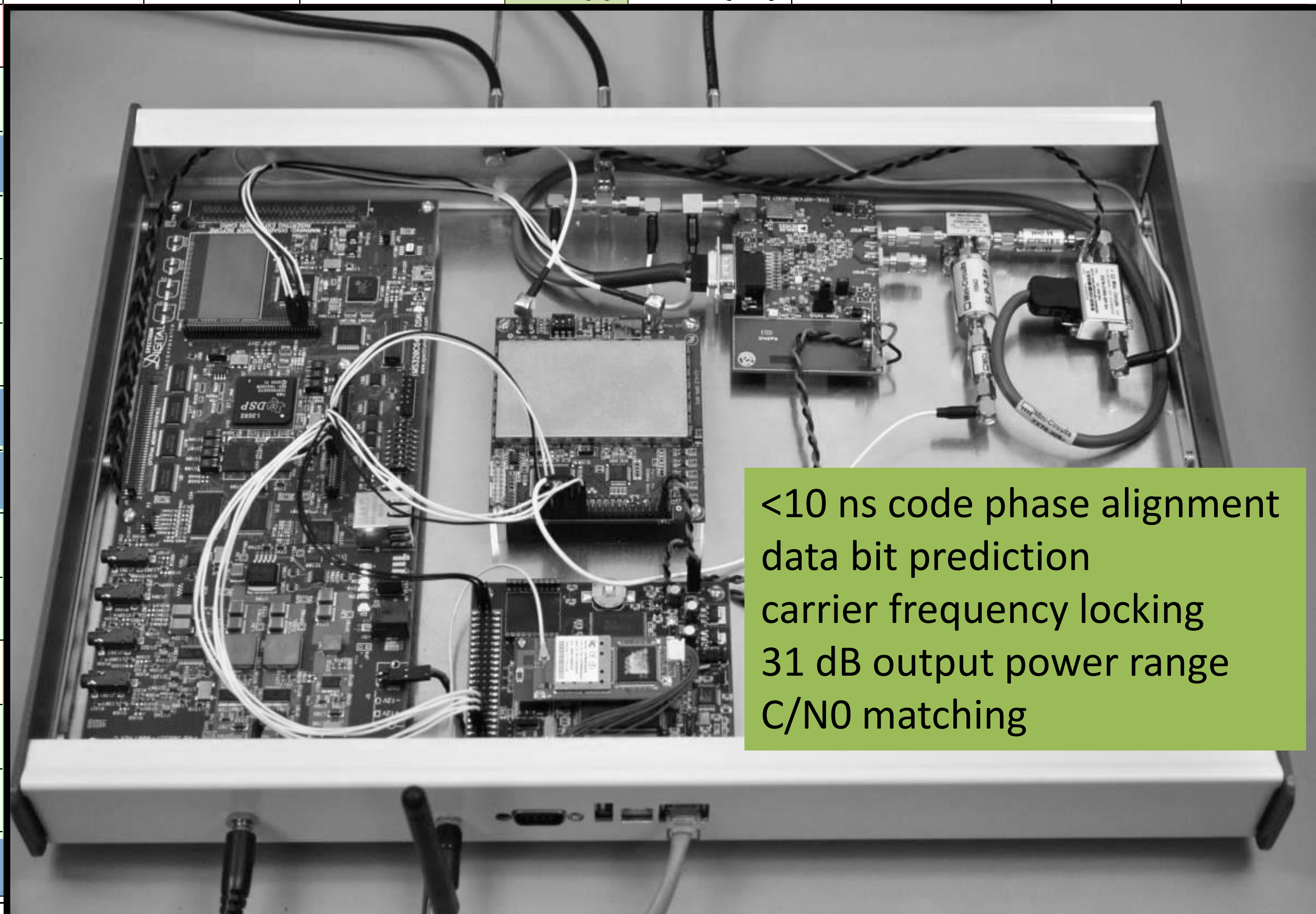


Synchronized (d < 100 ns) meaconing possible with a simple setup:
rx antenna → amplifier → tx antenna

Variable delay requires:
downconversion → A2D → FPGA → D2A → upconversion

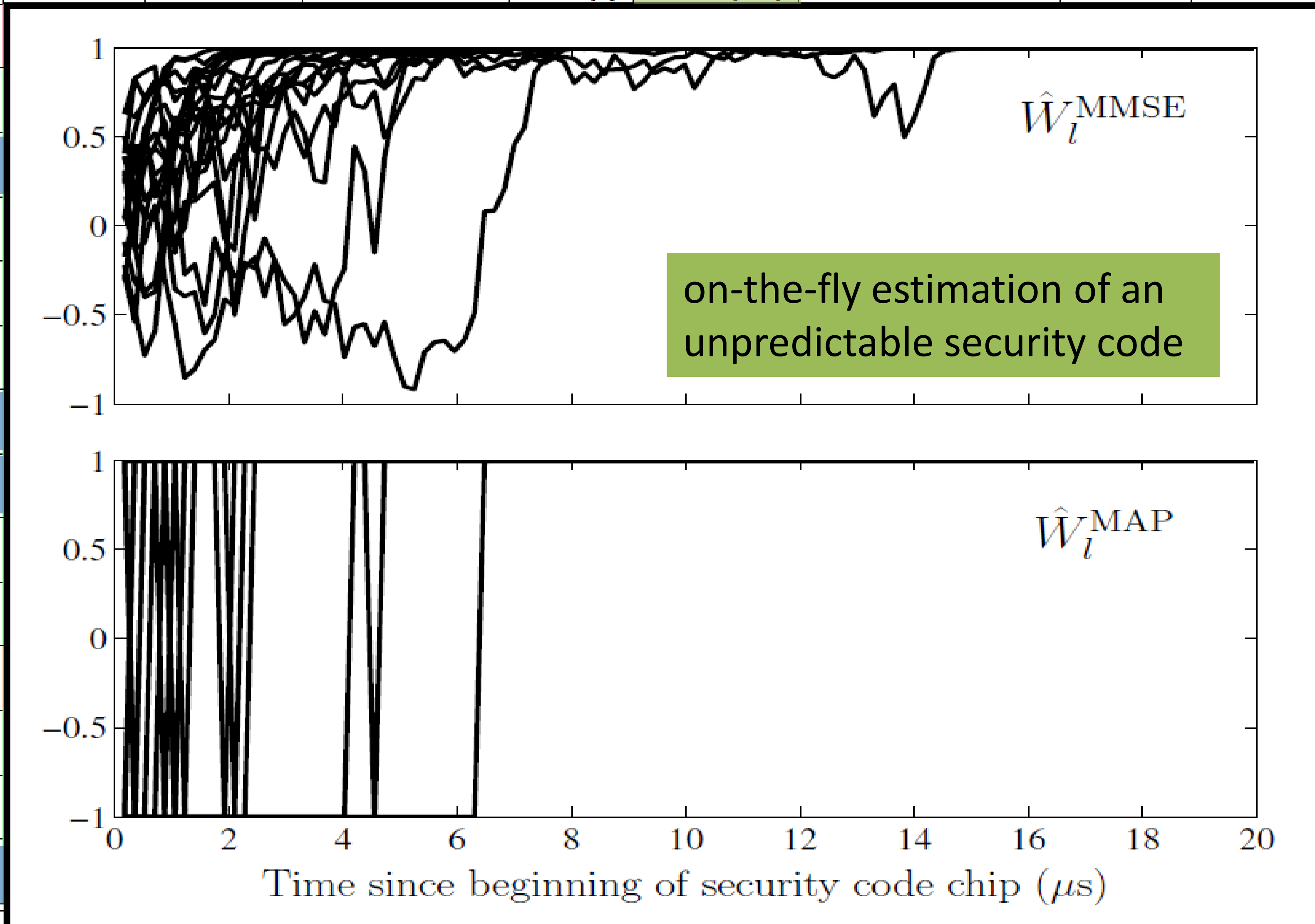
requires SIS modification

Defenses	Attacks							
	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								

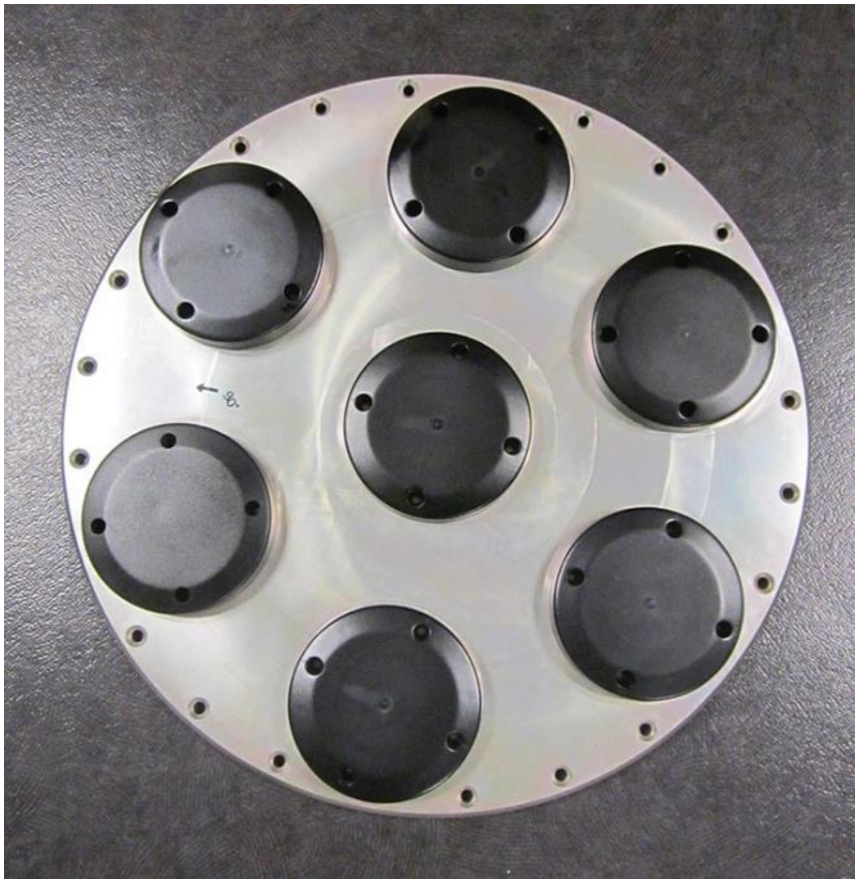


<10 ns code phase alignment
data bit prediction
carrier frequency locking
31 dB output power range
C/N0 matching

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								

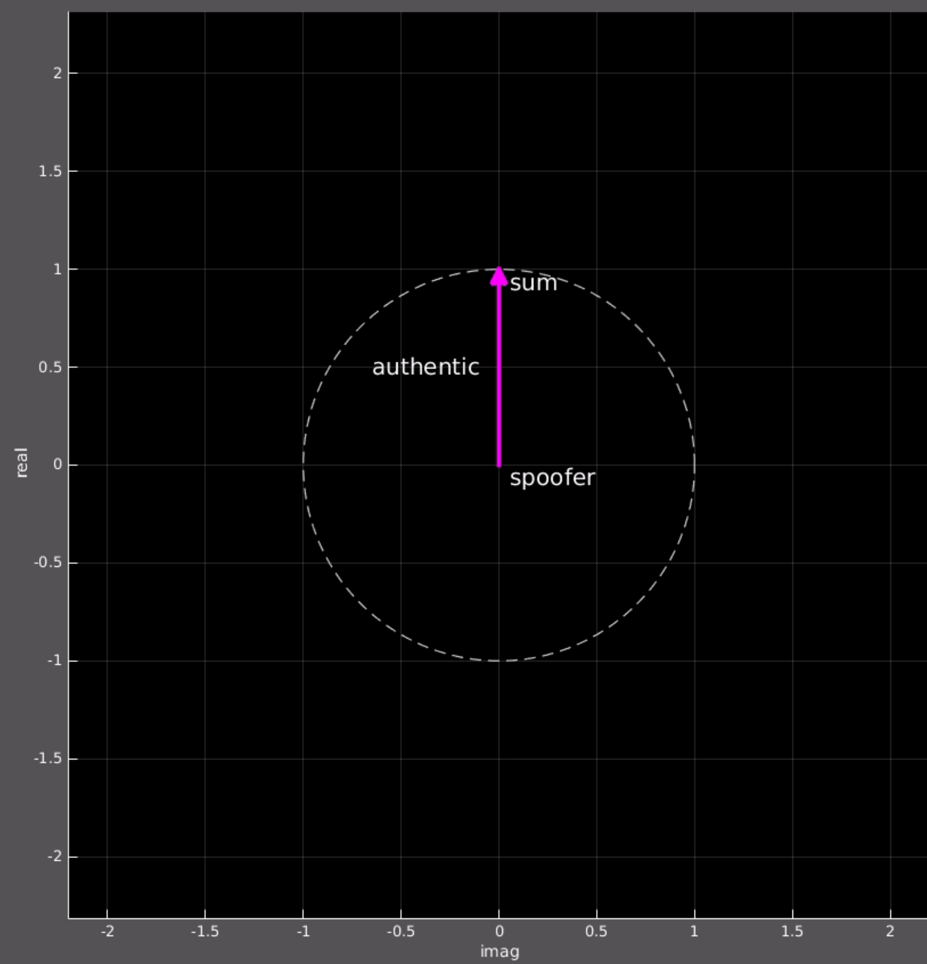


Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13,14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



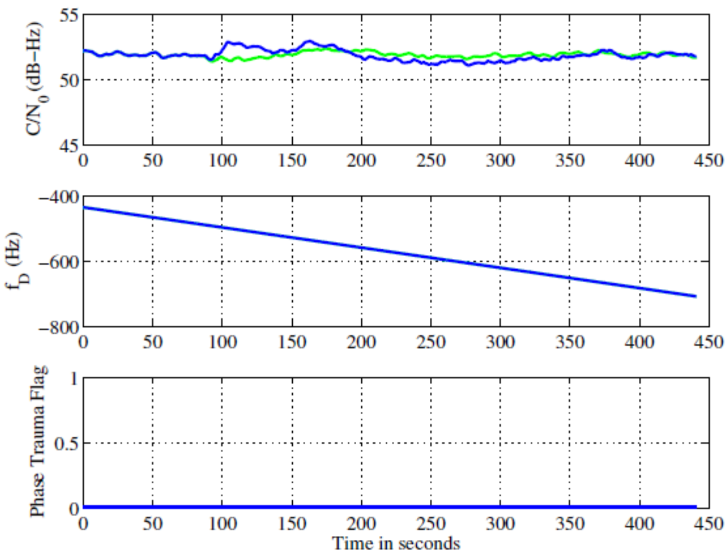
Each antenna's RF signal is independently digitized. The resulting complex digital streams are weighted and summed to achieve simultaneous beam steering toward any number of SVs. The SV-specific signals are time-shifted and summed to create the false signal ensemble.

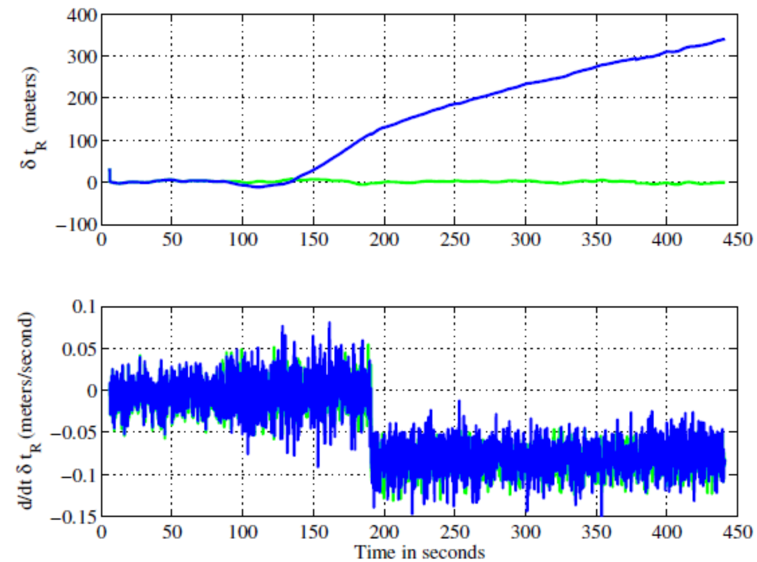
Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13,14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



A nulling attack annihilates the authentic signal with an antipodal spoofing signal. Thereafter, no vestige of the authentic signal remains to interact with further spoofing. The attack can begin instantaneously at a data bit boundary or emerge gradually as shown by the phasor interaction in the video.

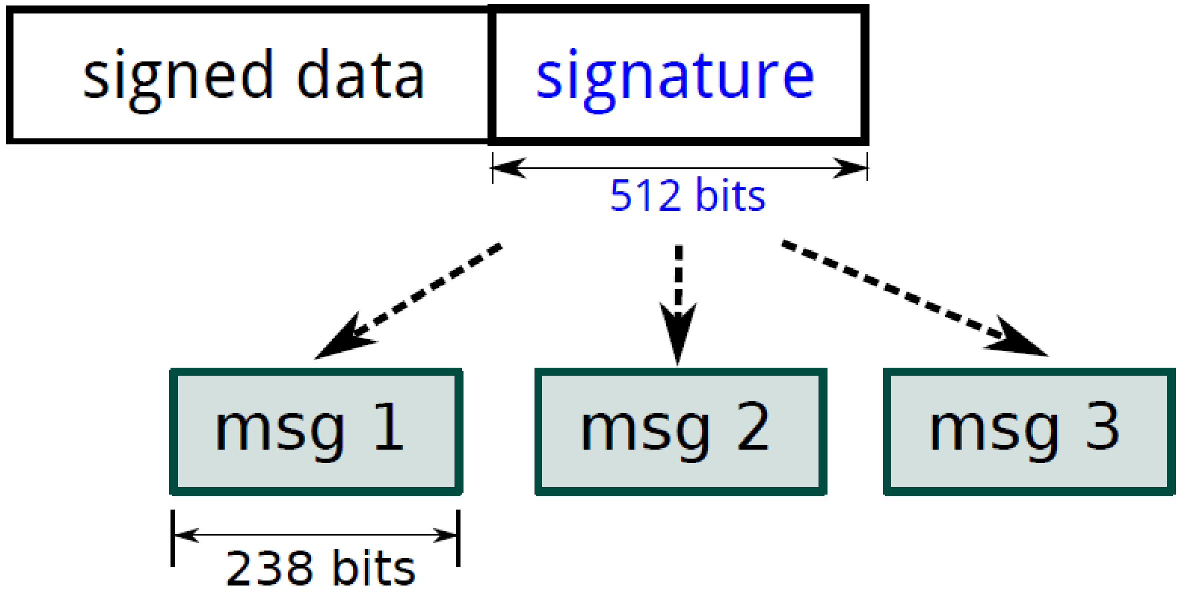
Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								





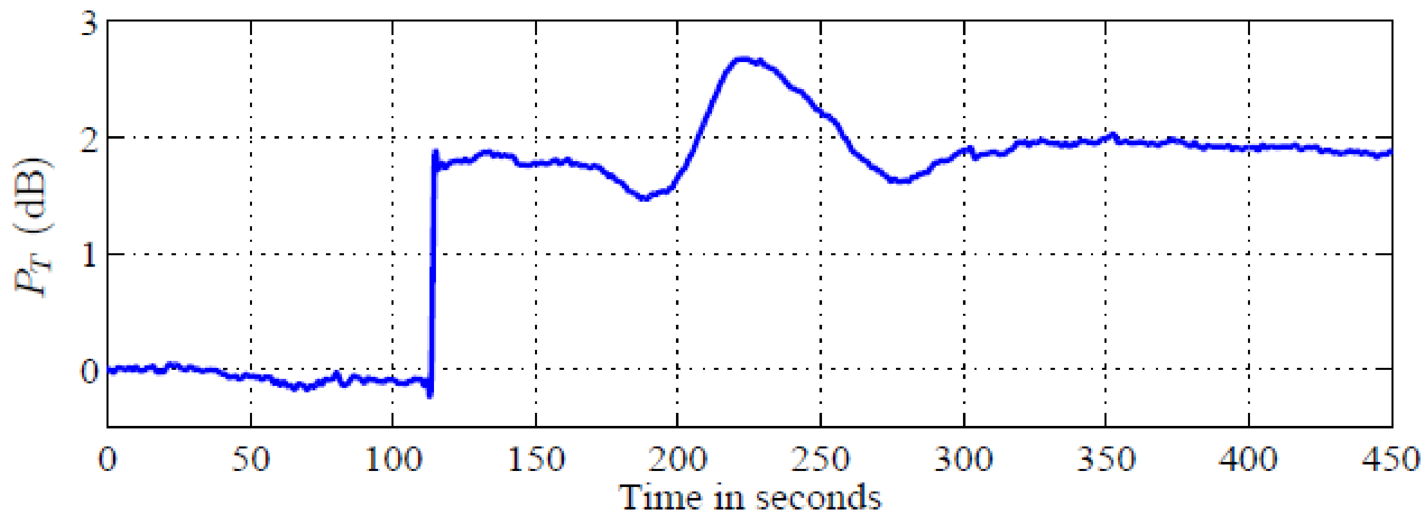
Standard GNSS pseudorange, Doppler, carrier phase, and signal strength observables can be analyzed to detect a spoofing attack. Detection is more powerful for static receivers.

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



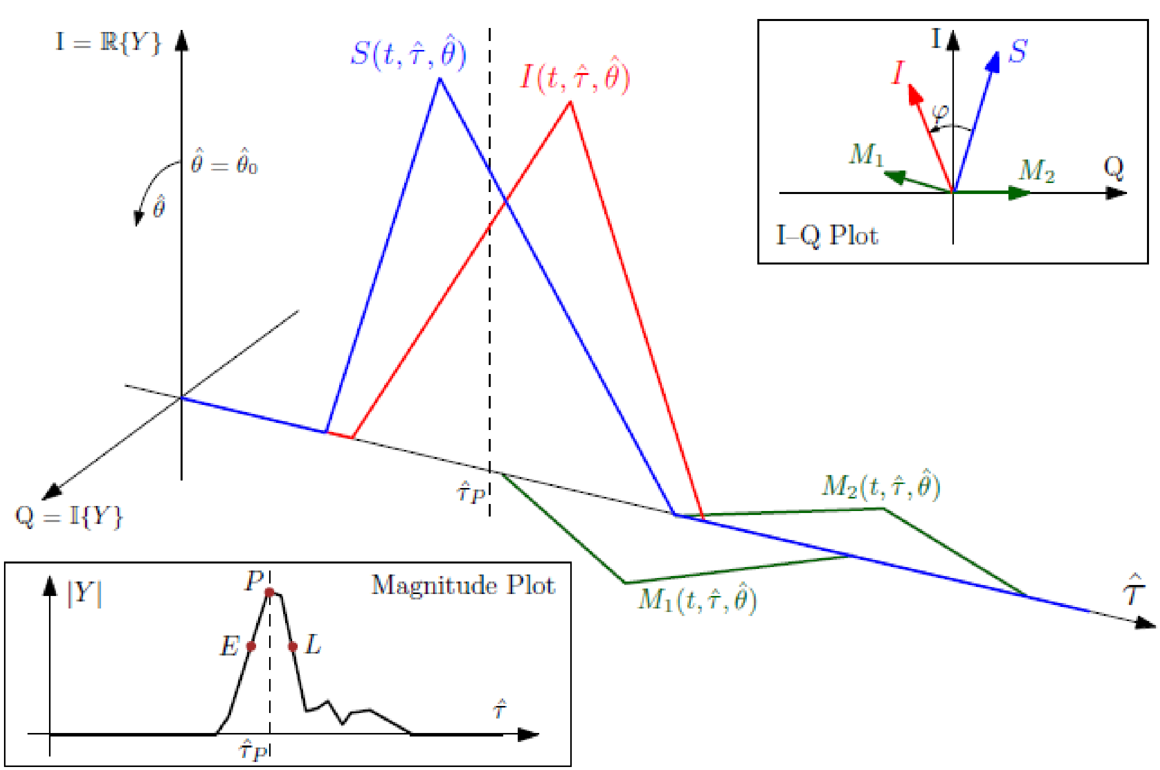
Signatures interleaved within navigation data stream. Authenticates origin of data. No need for secret keys to be stored in the receiver.

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13,14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



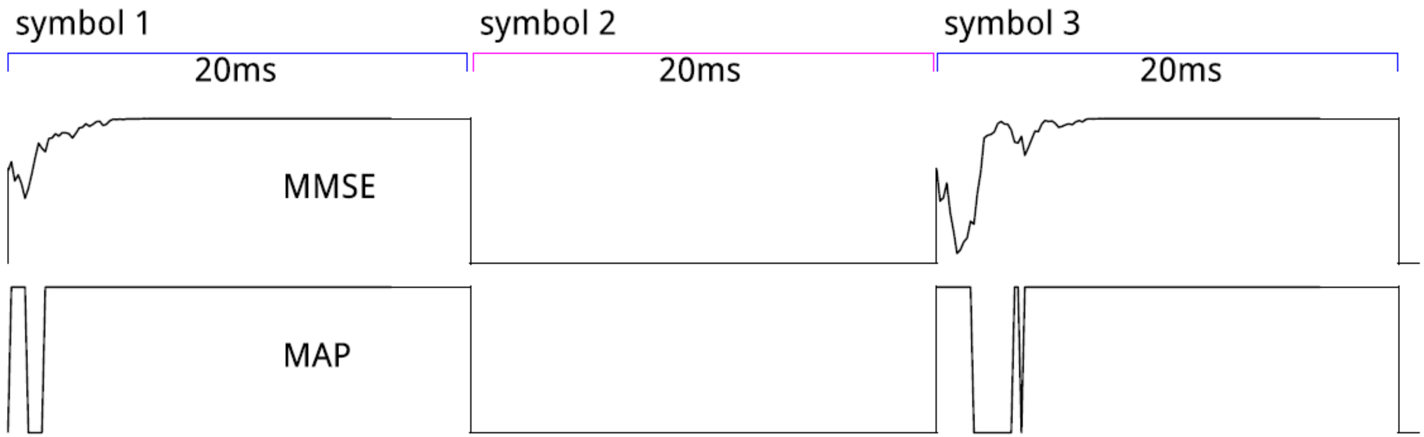
Received power monitoring: continuous measurement of the total in-band received power. Requires access to automatic gain control instantaneous setpoint.

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



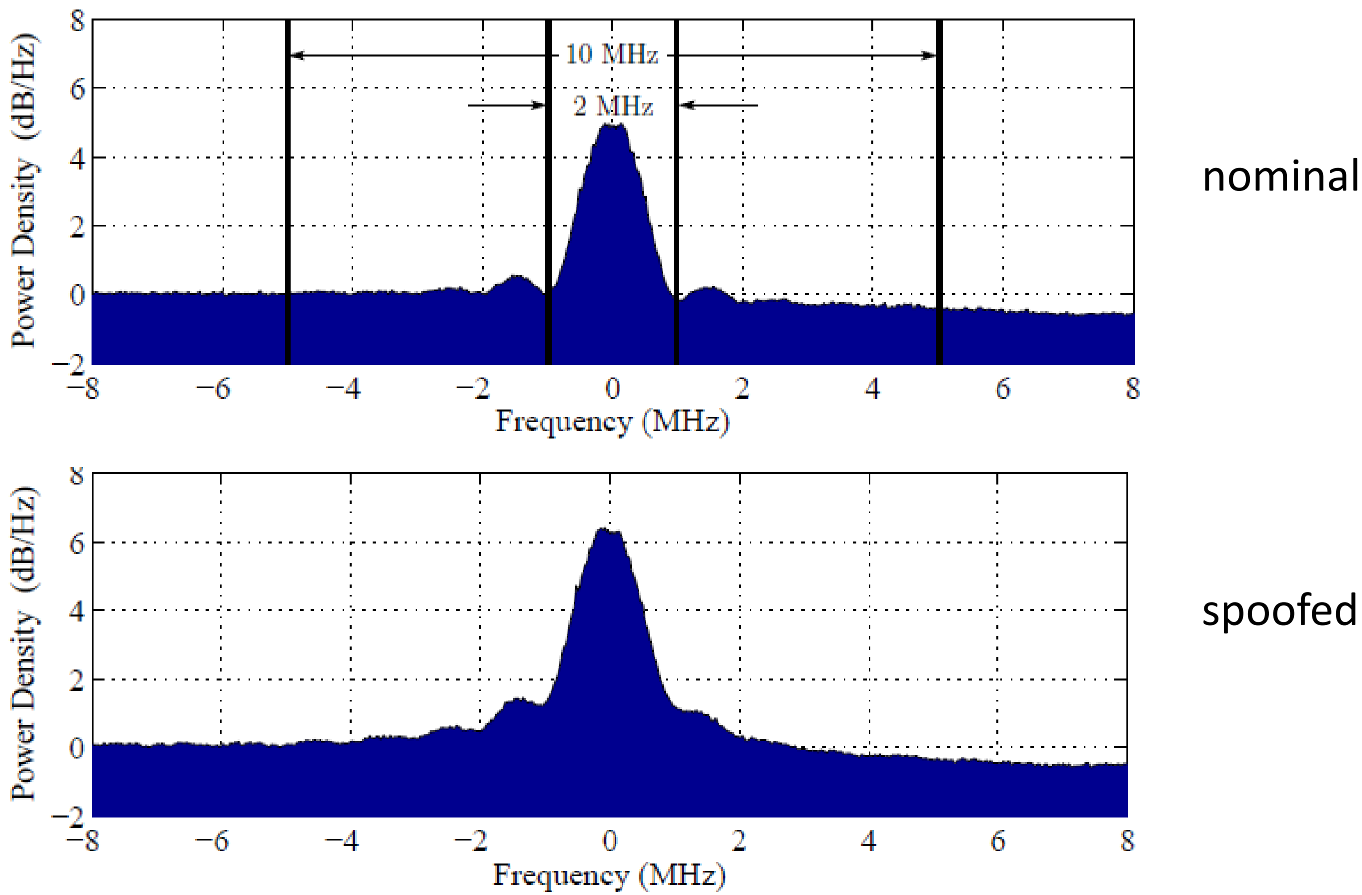
The Pincer defense: Exploit the attacker's difficulty in preventing distortion when spoofing signals are approximately power-matched to authentic signals; amounts to trapping the spoofer between (1) a received power monitor, and (2) a distortion monitor.

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



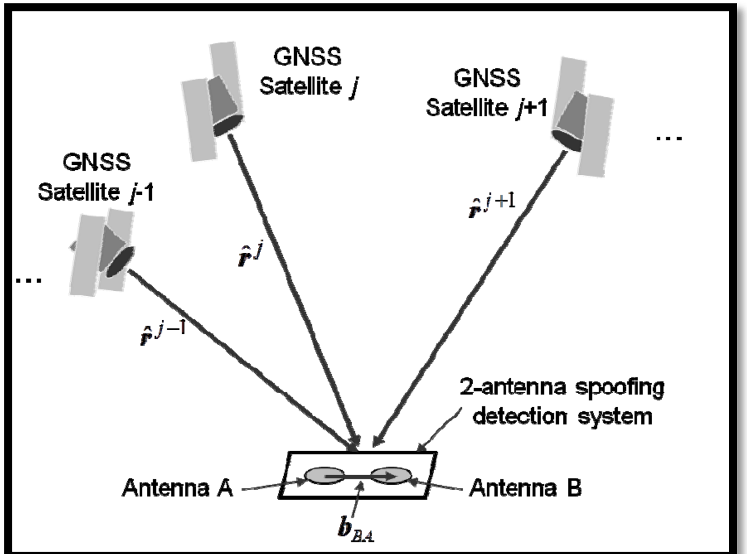
NMA + SCER detection exploits the attacker's inability to accurately estimate the security code chip values during the first few microseconds after an unpredictable transition.

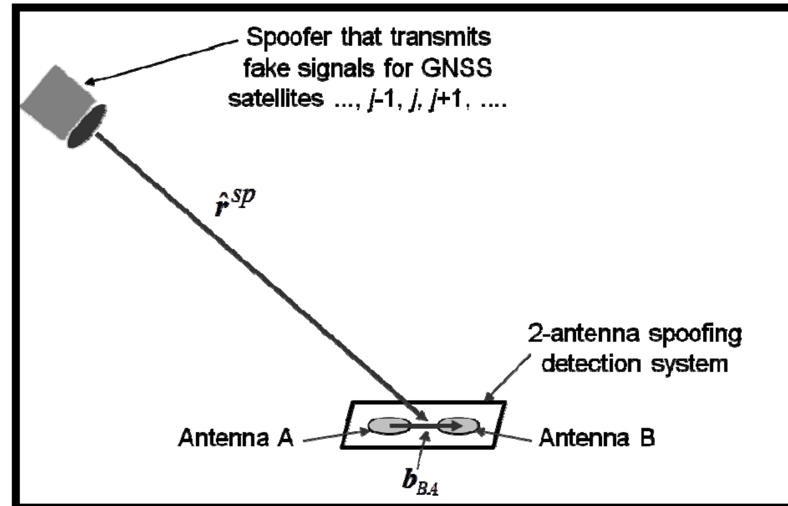
Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								



Power spectrum analysis is valuable diagnostic for all types of RFI

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2, 3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]								
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								





Psiaki et al., 2014

Spoofing signal arriving from a single spatial direction are easily distinguished from spatially diverse authentic GNSS signals.

Defenses	Attacks							
requires SIS modification	simulator	single-rx-antenna meaconing		Humphreys et al.		multi-rx-ant. meac.	nulling	
	unsync.	$d > 100$ ns	$d < 100$ ns	2008 [1]	SCER [2,3]	$d < 100$ ns	single-tx	multi-tx
conventional RAIM								
observables [4]								
NMA [5–7]								
RPM [8]								
pincer [9]								
RPM + observables								
NMA + SCER det. [5]								
SSSC [10]								
RPM + struct. power [11]								
spectral analysis								
IMU + carrier phase [12]	---------------------------- requires platform motion ------------------------------------							
multi-antenna [13, 14]								
dual-rx corr. with P(Y) [15]								
symmetric-key SSSC [e.g., P(Y)]								

NMA + SCER detection offers substantial PNT security at low cost

NMA has been advocated for over a decade:
Scott (2003) [10]
Internal MITRE memoranda
Wesson (2012) [5]
Kerns (2014) [6]

No surprise that Europe is moving forward with NMA on Galileo [7]

NMA on Galileo

Basic Design

- To be included on E1B open service
- High rate: 20 security bits per second avg.
- Based on TESLA (keys successively revealed after use period)

Status

- Draft blueprint complete
- Over-the-air testing took place in summer 2014
- Journal paper forthcoming

NMA on GPS

May 2015: The University of Texas completed a 2-year contract with the GPSD to develop a blueprint for NMA on GPS.

Basic Design

- Targeted to CNAV on L2C and L5
- Low rate: <1 security bit per second avg.
- Hybrid of TESLA and digital signature scheme (e.g., ECDSA, BLS)

Status

- Draft blueprint complete
- Optimized scheduling across constellation
- Receiver demonstrates NMA + SCER det.
- Journal paper forthcoming

NMA on GPS L2C and L5

Case For

- Low cost to user (software update)
- Substantial improvement in PNT security for GPS users worldwide; patches a serious vulnerability in civil GPS

Case Against

- Narrow uplink pipe leads to long time between authentication (9 minutes; compare Galileo at 10-20 seconds)
- Response from industry: “If it’s not on L1, it’s not much use.”
- Bad time to be adding requirements to OCX

Recommendations

1. Implement NMA on WAAS quadrature channel; provide example for other SBAS. Much higher SBAS data rate (250 bps) will support short time between authentication.
2. Digitally sign GPS LNAV data, then broadcast signatures over WAAS quadrature channel: cross authentication.
3. Encourage GNSS mfrs. to adopt simple receiver-autonomous defenses such as Pincer.
4. Plan for NMA on L1C.

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the ION GNSS Meeting*, (Savannah, GA), Institute of Navigation, 2008.

[2] T. E. Humphreys, "Detection strategy for cryptographic GNSS anti-spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[3] T. E. Humphreys, D. P. Shepard, J. A. Bhatti, and K. D. Wesson, "A testbed for developing and evaluating GNSS signal authentication techniques," in *Proceedings of the International Symposium on Certification of GNSS Systems and Services (CERGAL)*, (Dresden, Germany), July 2014. (available at `http://radionavlab.ae.utexas.edu/testbed`).

[4] V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection based on receiver C/N_0 estimates," in *Proceedings of the ION GNSS Meeting*, (Nashville, Tennessee), Institute of Navigation, 2012.

[5] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.

[6] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Proceedings of the IEEE/ION PLANS Meeting*, May 2014.

[7] I. F. Hernandez, V. Rijmen, G. S. Granados, J. Simon, I. Rodriguez, and J. D. Calle, "Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service," in *Proceedings of the ION GNSS+ Meeting*, 2014.

[8] D. M. Akos, "Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC)," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 4, pp. 281–290, 2012.

[9] K. D. Wesson, T. E. Humphreys, and B. L. Evans, "Receiver-autonomous GPS signal authentication based on joint detection of correlation profile distortion and anomalous received power," 2014. (in preparation).

[10] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the ION GNSS Meeting*, pp. 1542–1552, 2003.

[11] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Pre-despreading authenticity verification for gps l1 c/a signals," *Navigation*, vol. 61, no. 1, pp. 1–11, 2014.

[12] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Position, Location and Navigation Symposium-PLANS 2014, 2014 IEEE/ION*, pp. 1232–1239, IEEE, 2014.

[13] M. L. Psiaki, B. W. O'Hanlon, S. P. Powell, J. A. Bhatti, K. D. Wesson, T. E. Humphreys, and A. Schofield, "GNSS spoofing detection using two-antenna differential carrier phase," in *Proceedings of the ION GNSS+ Meeting*, (Tampa, FL), Institute of Navigation, 2014.

[14] M. H. Castañeda, M. Stein, F. Antreich, E. Tasdemir, L. Kurz, T. G. Noll, and J. A. Nossek, "Joint space-time interference mitigation for embedded multi-antenna gnss receivers," 2013.

[15] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

THE UNIVERSITY OF TEXAS AT AUSTIN

RADIONAVIGATION LABORATORY

radionavlab.ae.utexas.edu