ITSNT 2018

DESIGNING AND EVALUATING NEXT GENERATION OF RESILIENCE RECEIVERS

S. Cancela, J. Navarro, D. Calle, *GMV, Spain; A. Dalla Chiara, G. Da Broi, Qascom, Italy; E. Göhler, Ifen, Germany; I. Fernández-Hernández, European Commission, Belgium; J. Simón, GSA; G. Seco, Autonomous University of Barcelona, Spain*

NOVEMBER 15, 2018

gmv INNOVATING SOLUTIONS

AGENDA

Introduction

User Terminal description

Anti-Replay Technique
- Overview
- Implementation

Validation Tests
- Attack simulation environment
- Test set-up
- Results

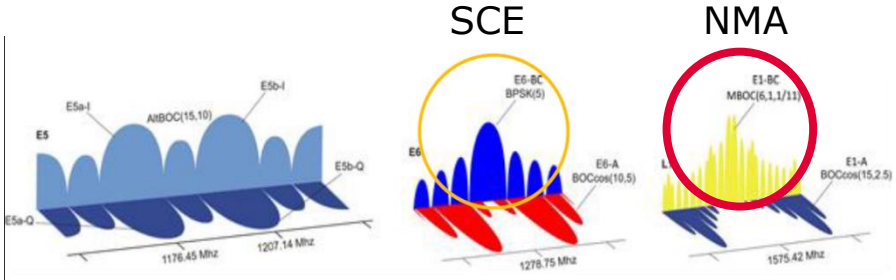
Conclusions and Way Forward

GALILEO AND RESILIENT RECEIVERS

- Galileo will provide two civil authentication services
  - Open Service Navigation Message Authentication (NMA) in E1B for receivers having the public key
  - Commercial Service authentication by spreading code encryption (SCE) in E6C for receivers having the encryption/decryption keys

- Next generation resilient receivers will use these signals in combination with other receiver resilient measures

- The main challenges are:
  - How future resilient receivers will manage cryptographic operations required for authenticated signals
  - How to optimally combine data and signal authentication with receiver-based protection measures



WHAT IS NACSET?

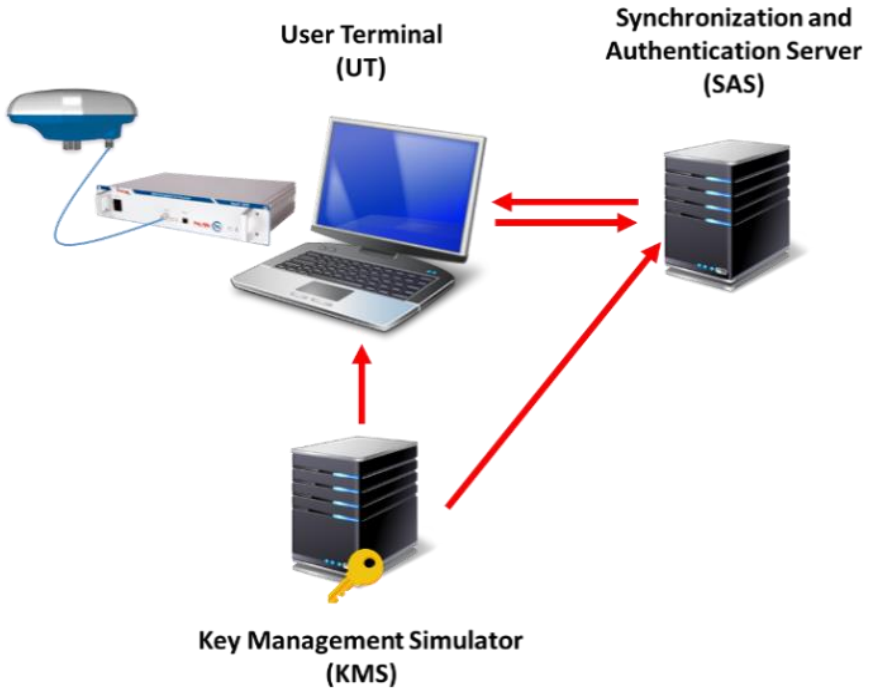
- EC started the Navigation Authentication through Commercial Service-Enhanced Terminals (**NACSET**) project in Jan 2017

Objectives:

- Develop and test a secure Key Management Simulator for the Galileo CS and OS keys
- Develop a platform resilient to malicious and spoofing attacks
  - Resilient User Terminal
    - Anti-spoofing techniques
    - Accurate Time synchronization
    - Inertial Measurements Unit (IMU)
    - Signal Authentication
  - Synchronization and Authentication Server
    - Time Synchronization provision
    - Navigation message aiding channel
    - Authentication provision (RPA, CSS)
- Keep research on Galileo to define future evolutions.

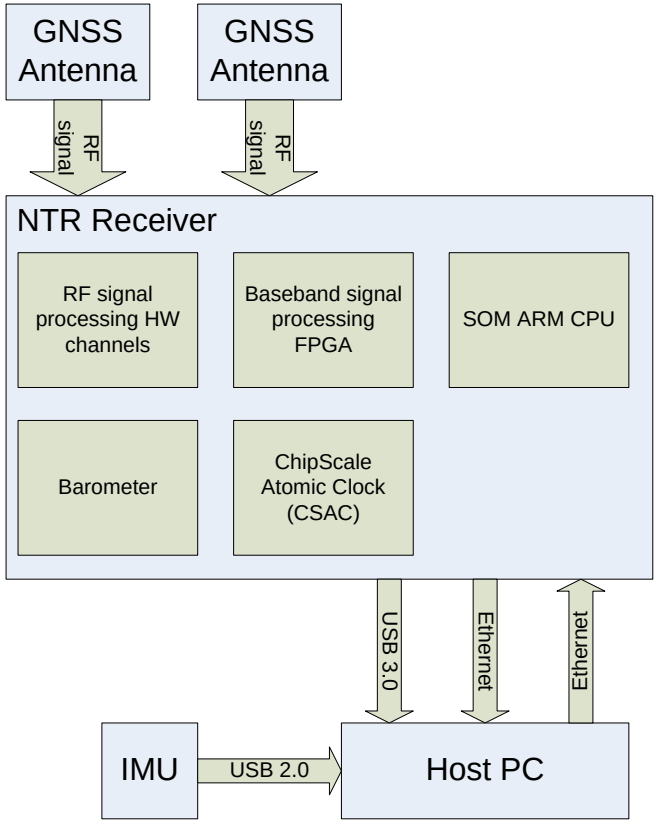
NACSET ARCHITECTURE

- **KMS:** end-to-end key management simulator of secure key management and distribution
  - NavSec Keys
  - OS Authentication keys.
- **UT:** GNSS terminal client able to perform attack detection and protection and calculate a resilient PVT
- **SAS:** Server to provide synchronization and authentication services



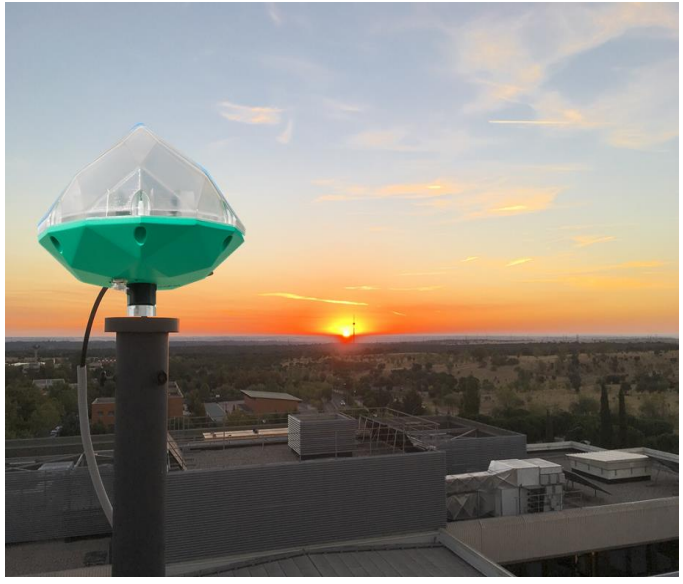
USER TERMINAL

- NavX-NTR Receiver
  - High-End GNSS Receiver
  - Support for signal encryption
  - Accurate clock evolution based on CSAC
  - Height information from Barometer
  - Dual-Antenna input
- Host-PC
  - Receiver commanding
  - Authentication Engine
  - PVT Engine
- Inertial Measurements Unit



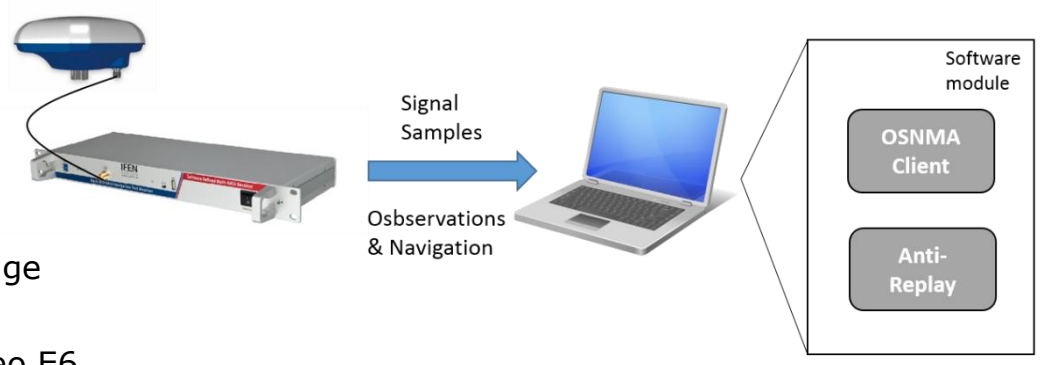
UT ANTENNA ELEMENT

Specifications	
Galileo Signals	E1, E5a, E5b, E5a+b (AltBOC), E6
GPS Signals	L1, L2
Element Distance	< λ/2 at 1591 MHz (94 mm)
Passive Gain	Elev. 90° (zenith): > 3.5 dBic Elev. 60°: > -3 dBic Elev. 15°: > -10 dBic
LNA Power Gain	~30 dB
LNA Noise factor	< 2 dB



UT SOFTWARE MODULE

- **Authentication engine:**
  - Anti-replay protection
  - Dual-antenna measures analysis
  - IMUs Hybridization
  - Clock Monitoring
  - AGC-C/N0 Monitoring
  - Galileo Open Service Navigation Message Authentication
  - Assisted signal authentication on Galileo E6



- **PVT Engine**
  - Computation of PVT using anti-spoofing indicators

ANTI-REPLAY PROTECTION

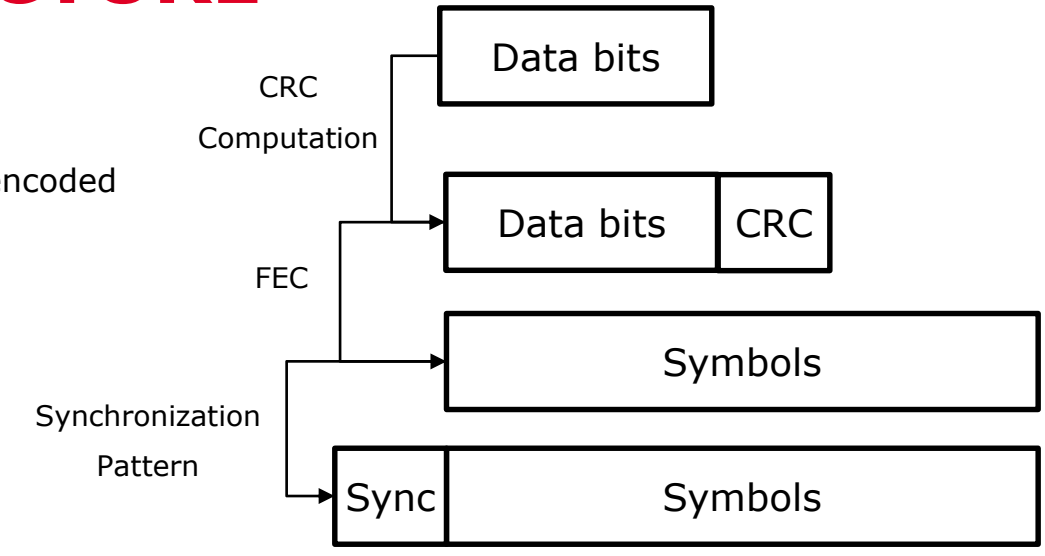
- **Anti-replay technique based on symbols unpredictability**
  - Research on literature
    - Todd E Humphreys, "*Detection strategy for cryptographic gnss antispoofing*," Aerospace and Electronic Systems, IEEE Transactions on, vol. 49, no. 2, pp. 1073–1090, 2013
    - Gianluca Caparra, Nicola Laurenti, Rigas T Ioannides, and Massimo Crisci, "*Improving secure code estimate-replay attacks and their detection on gnss signals*"," Proceedings of NAVITEC 2014, 2014
    - I. Fernández-Hernández, G. Seco-Granados, *"Galileo NMA Signal Unpredictability and Anti-Replay Protection*", ICL-GNSS 2016, 2016
  - GNSS signal stream contains data that is authenticated (NMA)
  - Data modulated includes unpredictable symbols
  - Protection against zero-delay SCER (Security Code estimation and Replay) attacks
  - Galileo Open Service Navigation Message Authentication (OSNMA) used as reference on E1B I/NAV

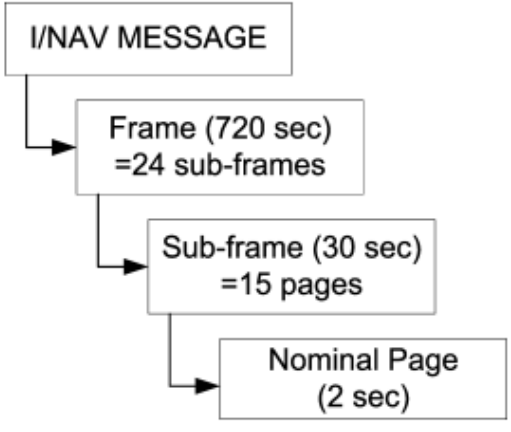
1	9	17	25	33	41	49	57	65	73	81	89	97	105	113	121	129	233
2	10	18	26	34	42	50	58	66	74	82	90	98	106	114	122	130	234
3	11	19	27	35	43	51	59	67	75	83	91	99	107	115	123	131	235
4	12	20	28	36	44	52	60	68	76	84	92	100	108	116	124	132	236
5	13	21	29	37	45	53	61	69	77	85	93	101	109	117	125	133	237
6	14	22	30	38	46	54	62	70	78	86	94	102	110	118	126	134	238
7	15	23	31	39	47	55	63	71	79	87	95	103	111	119	127	135	239
8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	...	240

1	9	17	25	33	41	49	57	65	73	81	89	97	105	113	121	129	233
2	10	18	26	34	42	50	58	66	74	82	90	98	106	114	122	130	234
3	11	19	27	35	43	51	59	67	75	83	91	99	107	115	123	131	235
4	12	20	28	36	44	52	60	68	76	84	92	100	108	116	124	132	236
5	13	21	29	37	45	53	61	69	77	85	93	101	109	117	125	133	237
6	14	22	30	38	46	54	62	70	78	86	94	102	110	118	126	134	238
7	15	23	31	39	47	55	63	71	79	87	95	103	111	119	127	135	239
8	16	24	32	40	48	56	64	72	80	88	96	104	112	120	128	...	240

I/NAV PAGE STRUCTURE

- **I/NAV Data:**
  - 120 bits per page part (1 second)
  - Forward Error Coding: Convolutionally encoded in 240 symbols
  - Block interleaved 30 columns x 8 rows



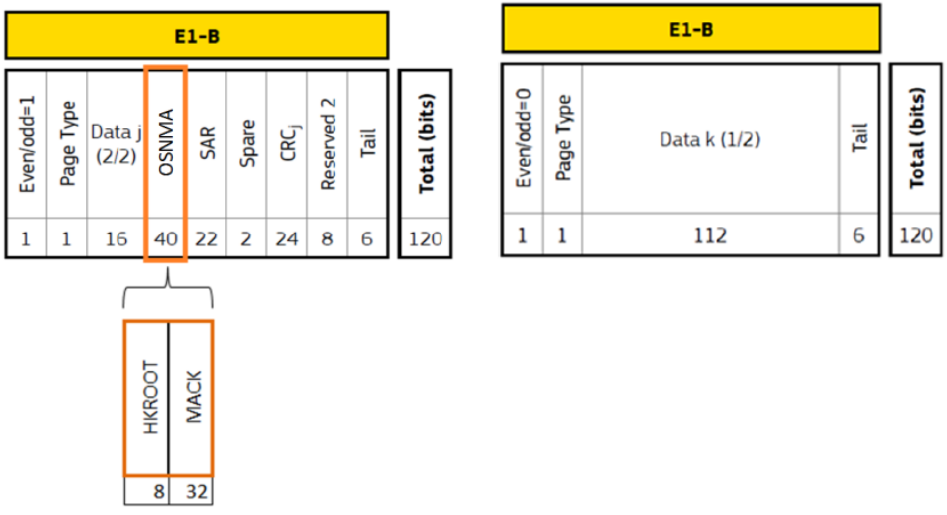


Sync.	I/NAV Page Part (even or odd) Symbols	Total (symb)
10	240	250

I/NAV Page Part (even or odd) Bits	Tail	Total (bits)
114	6	120

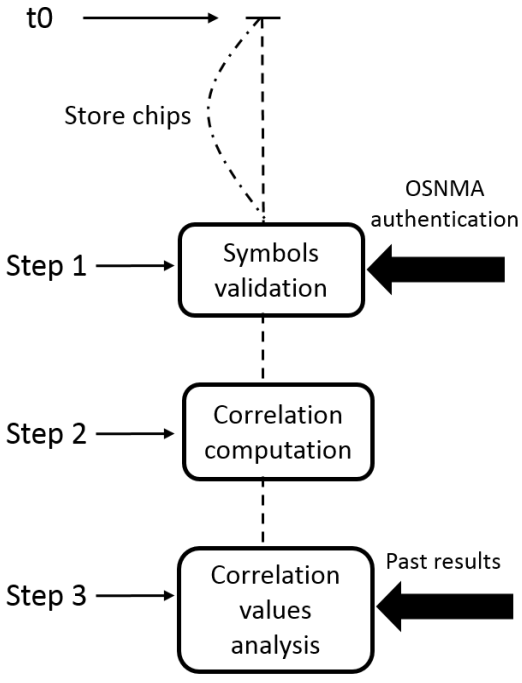
I/NAV OSNMA DATA

- **OSNMA Data:**
  - 40 bits per page (20 bits/sec rate)
  - Two types of messages:
    - Hkroot section
      - Digital Signature Messages
      - Symbols are predictable
    - MACK root section
      - Message Authentication Codes (MACs)
      - Cryptographic Keys
      - Symbols may be unpredictable
  - OSNMA data is not available in the Galileo Signal-in-Space so it is simulated inside the project.



ANTI-REPLAY IMPLEMENTATION

- **Anti-replay technique based on symbols unpredictability**
  - Continuous stream of E1B signal samples are sent from the hardware receiver to the Authentication Engine
  - N_c chips of the N_U unpredictable symbols over a given page.
  - Once symbols are authenticated, the correlation computation of the stored chips is performed
  - If a loss in correlation gain is observed, an alarm is raised.

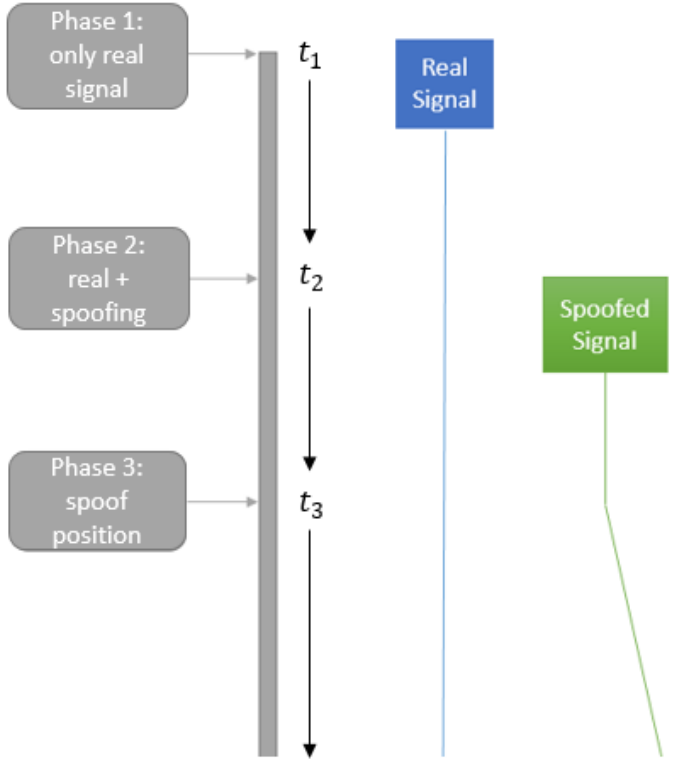


SCER ATTACK SIMULATOR

- **SCER simulator components**
  - HackRF One
    - Needed to convert to RF the GNSS baseband signal data streams generated and replay it with the antenna.
  - Software Module
    - Galileo E1 and GPS L1 signal sample generation
    - OSNMA data generated by means of the Commercial Service Demonstrator (CSDemo) platform developed in the frame of the AALECS, project managed by the European Commission.
    - Zero delay attack simulated
      - Generation of two signals:
        - Trusted signals with no chip errors
        - Spoofed signal aligned with the trusted signal and with chip errors

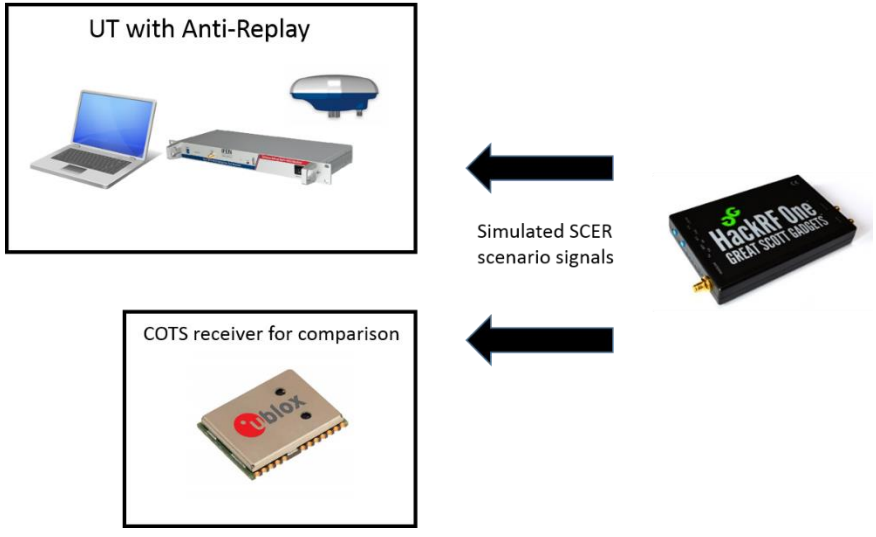
SCER ATTACK DETAILS

- **SCER simulation definition**
  - Three phases
    - Phase 1: Only the signal without spoofing is generated, this simulate the real signal. The receiver tracks only this real signal.
    - Phase 2: The spoofing signal perfectly aligned with the real signa simulating a theoretical perfect zero delay.
    - Phase 3: After configurable time, when the receiver tracks the spoofing signal, the spoofing signal starts delaying the signal to spoof the receiver position



TEST SET-UP AND CONFIGURATION

- **Test set-up**
  - NACSET User Terminal with Anti-Replay protection implemented
  - COTS Receiver used for comparison: u-Blox M8T
- **SCER attack configuration**



Phase	Duration	Notes
Phase 1	60s	Real signal simulating position in LLH: (40.59º, -3.7º), 806 m
Phase 2	20s	Both spoofing signal and real simulate position (40.59º, -3.7º), 806 m with one chip delay
Phase 3	60s	Spoofing signal deviate receiver position in a linear trajectory.

Parameter	Value
Sampling frequency	8192000 Hz
Threshold	40 % maximum correlation loss from the mean.
Unpredictable symbols	32 per page
Chips to be correlated per unpredictable symbol.	10 at the beginning of the symbol

TEST SCENARIOS

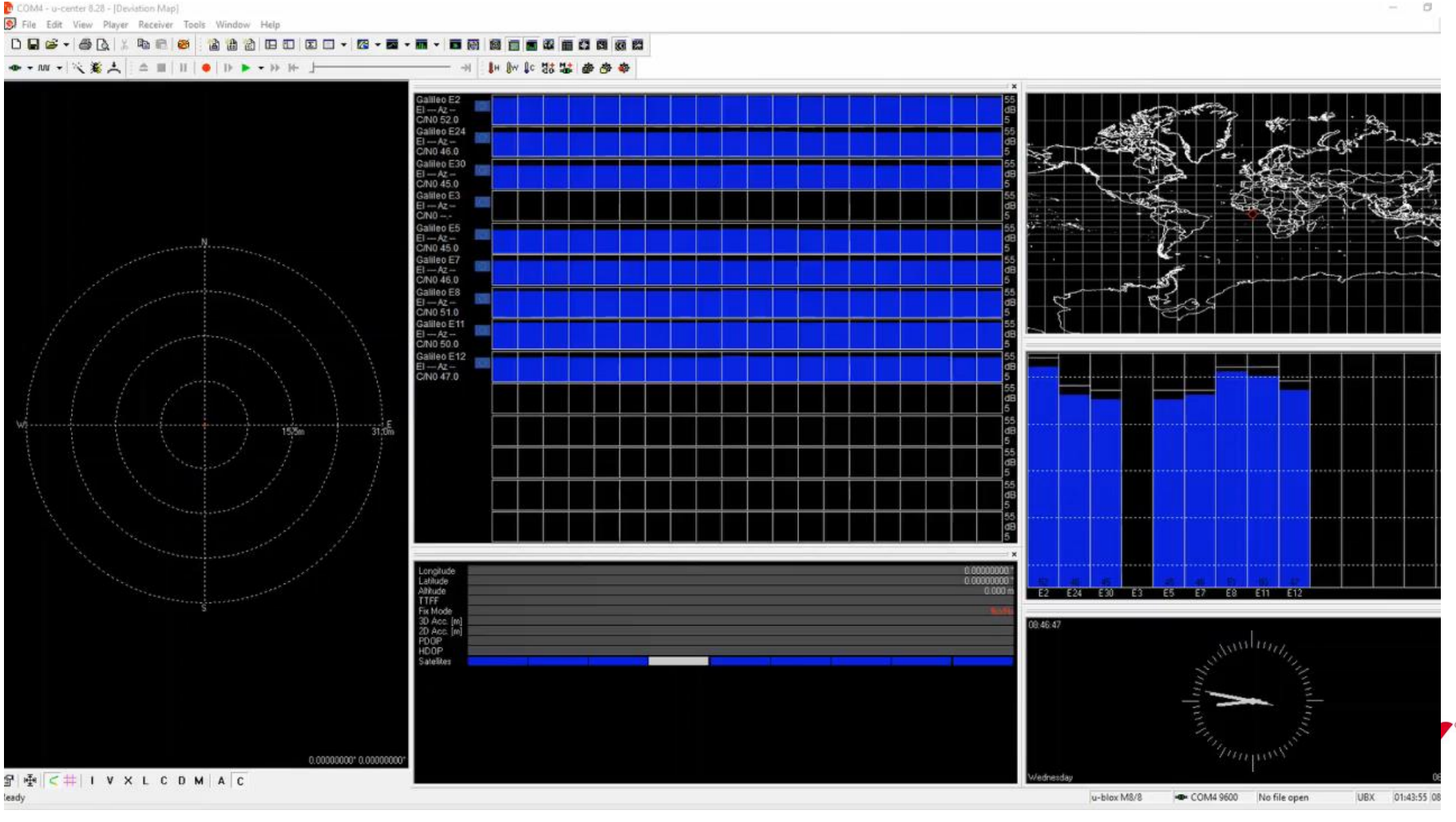
- **Test attack profiles**

  - Reference attack: Pseudorandom errors are introduced in the estimation of the unpredictable symbols (50% of chip errors at the beginning of each symbol) and no modification of the signal power is done.

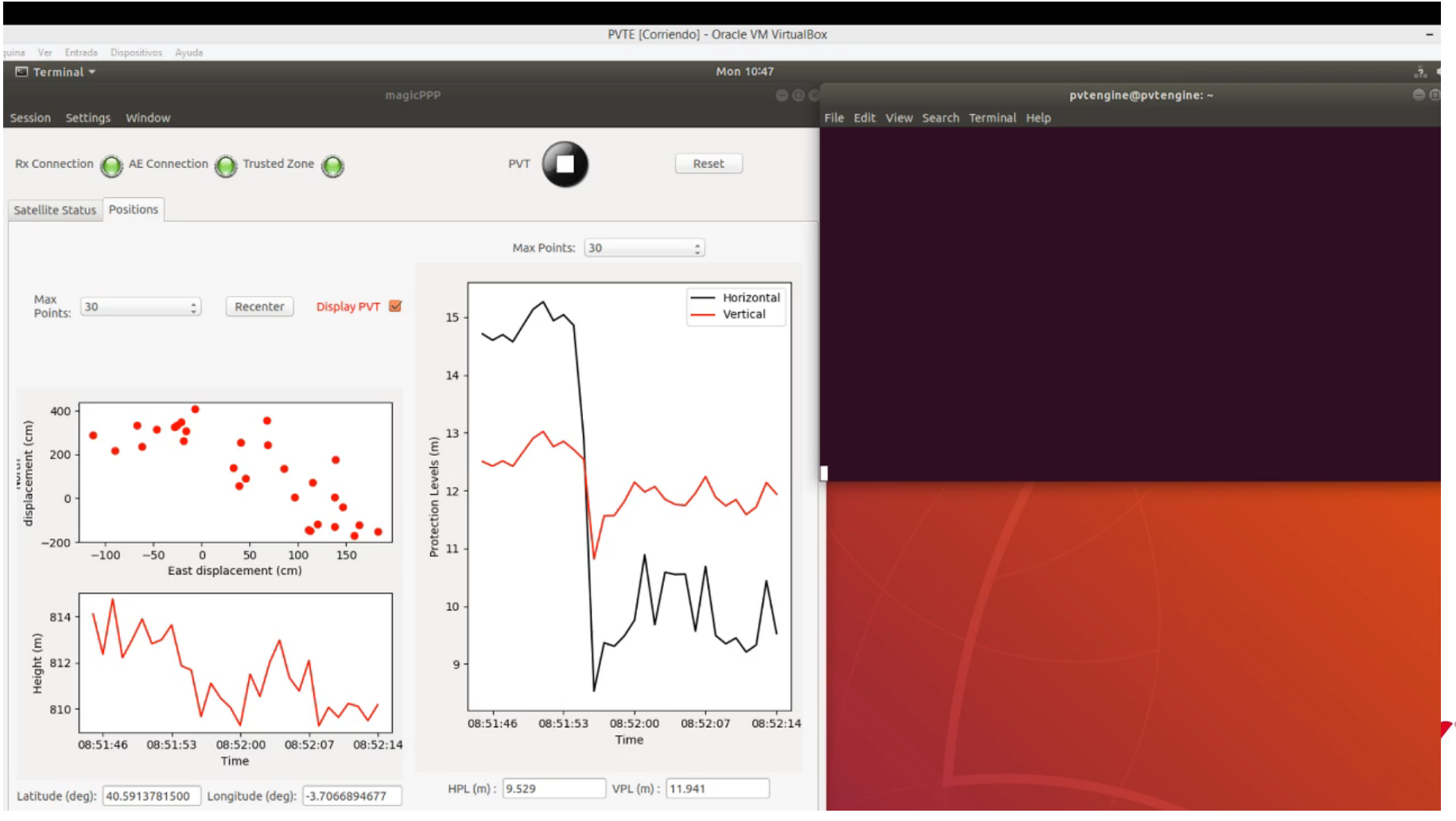
  - Intermediate attack: low error rate in the estimation of the unpredictable symbols (30% of chip errors at the beginning of each symbol) and no modification of the signal power is done.

  - High-power attack: low errors rate in the estimation of the unpredictable symbols (30% of chip errors at the beginning of each symbol) and modification of the signal power per symbol to mask the errors in the estimation process.

TEST COTS RECEIVER RESULTS

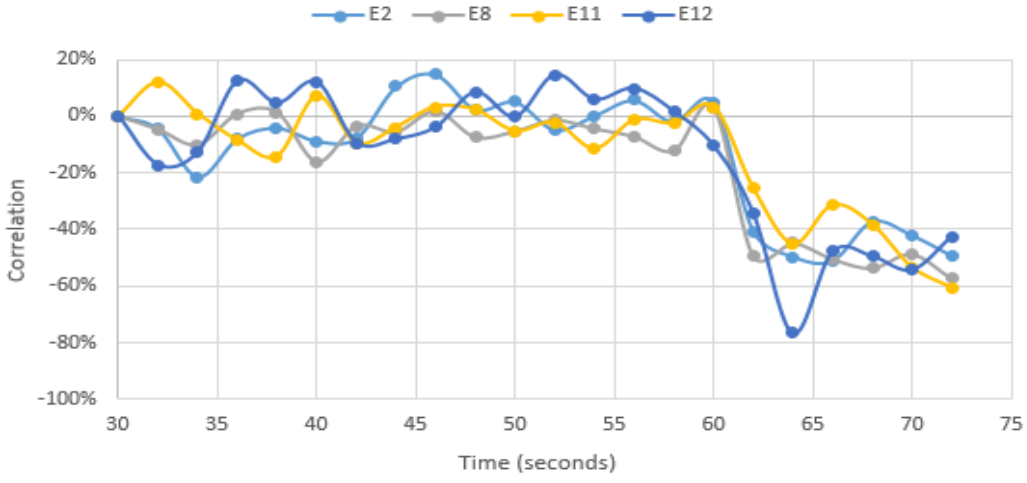


USER TERMINAL TEST RESULTS



TEST RESULTS: REFERENCE ATTACK

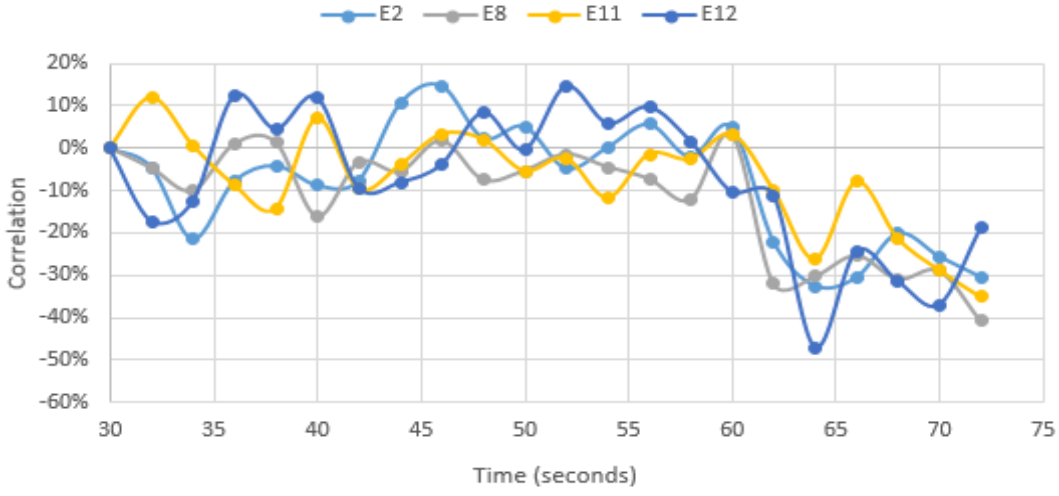
- Clear loss of correlation gain as soon as the spoofing attack starts
- Attack is detected almost immediately
- Considered pessimistic for the spoofer (success rate of 0.5 in the estimation



	E02	E08	E11	E12
Reference attack	-45%	-51%	-42%	-51%

TEST RESULTS: INTERMEDIATE ATTACK

- Less clear loss of correlation gain
- Still able to detect the attack and stops computing the positioning solution.
- More realistic rate of success for the estimation of the symbols

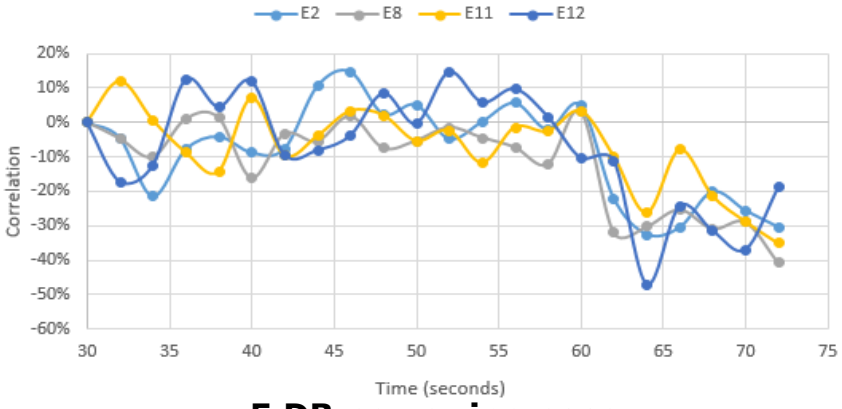


	E02	E08	E11	E12
Intermediate attack	-27%	-31%	-21%	-28%

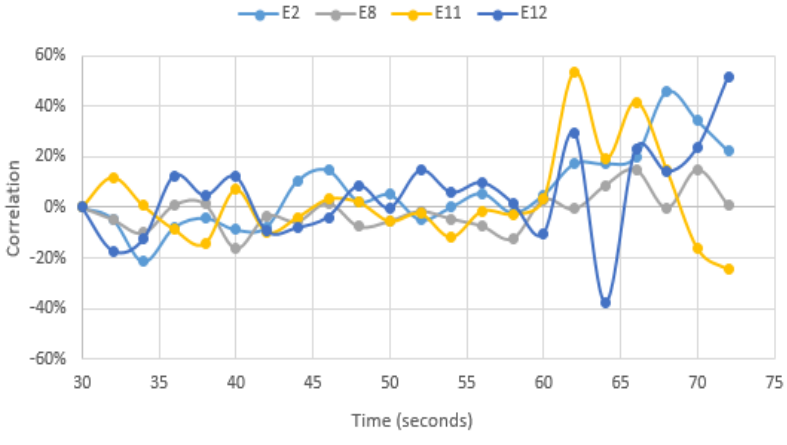
TEST RESULTS: HIGH-POWER ATTACK

- 3 DB increase
  - The correlation variation is more subtle than in the previous cases but a general correlation gain loss can be identified.
- 5 DB increase
  - The NACSET receiver is unable to clearly detect the attack, as it is quite difficult to propose a firm decision based on the correlation values.

3 DB power increase



5 DB power increase



	E02	E08	E11	E12
High-power attack (3dB)	-19%	-29%	-21%	-25%

	E02	E08	E11	E12
High-power attack (5dB)	26%	6%	15%	17%

CONCLUSIONS AND WAY FORWARD

- Implementation of a solution for protecting against zero delay SCER attacks has been described and tested against a simulated attack.
- Technique behaves well against standard zero-delay SCER attacks
- Combination with other signal-related indicators (AGC, C/N_0,…)
- Proving the technique with real SIS and in harsher environments
- Refine the statistical analysis to work in those environments
- Characterize the probability of false alarm and time to alert

www.gmv.com

THANK YOU

www.facebook.com/infoGMV

@infoGMV