LINKSFOUNDATION.COM

FONDAZIONE links
PASSION FOR INNOVATION

OSNMA decoding on software radio platforms, the experience at LINKS Foundation

Webinar on GNSS – Interference/jamming/spoofing and security

DR. BEATRICE MOTELLA
PROJECT LEADER, SPACE AND NAVIGATION TECHNOLOGIES RESEARCH AREA

11 MAY 2021

Outline

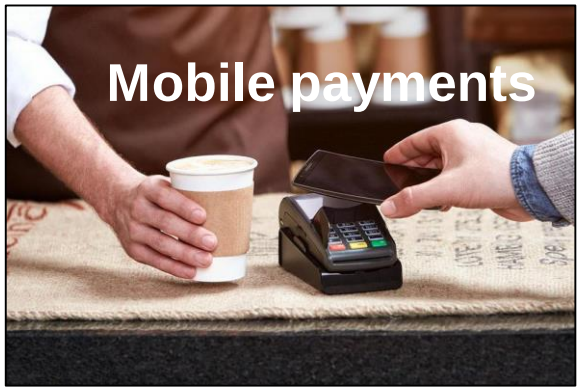
OSNMA decoding on software radio platforms

- Introduction
- Methodology and development work
- Software profiling analysis
- Conclusions and recommendations

The context

Introduction

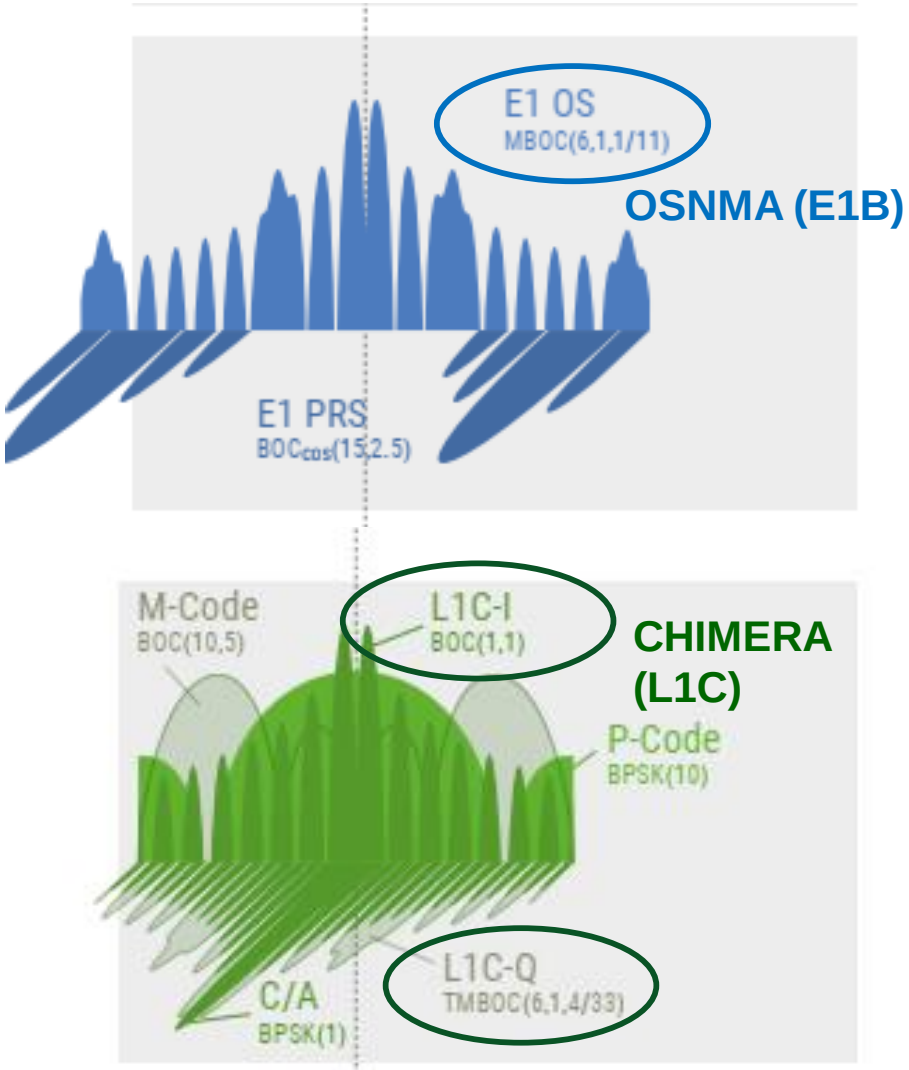
- Increase the robustness of GNSS signals is the growing need for many **safety- or liability-critical GNSS applications**
- **Authentication** goes in this direction
  It is the ability of the system to guarantee to users that they are utilizing non-counterfeit signals coming from one of the constellation satellites
- **Considered as the contribution of the system to the robustness against spoofing**



Galileo and GPS civil authentication

❖ Introduction

GPS and Galileo systems are proposing evolutions of their legacy civil signals to include features of authentication



➢ **Galileo Open Signal Navigation Message Authentication**

- designed for the E1 Galileo band
- availability of the full service expected soon

➢ **GPS Chips-Message Robust Authentication – Chimera**

- solution suitable for the GPS L1C signal
- its first experimental version will be broadcast by the Navigation Technology Satellite 3 (NTS-3)

Picture reworked from: Orolia, Skydel, The GNSS Spectrum. September 2019
Available at: https://www.orolia.com/documents/gnss-spectrum

Motivation of the work

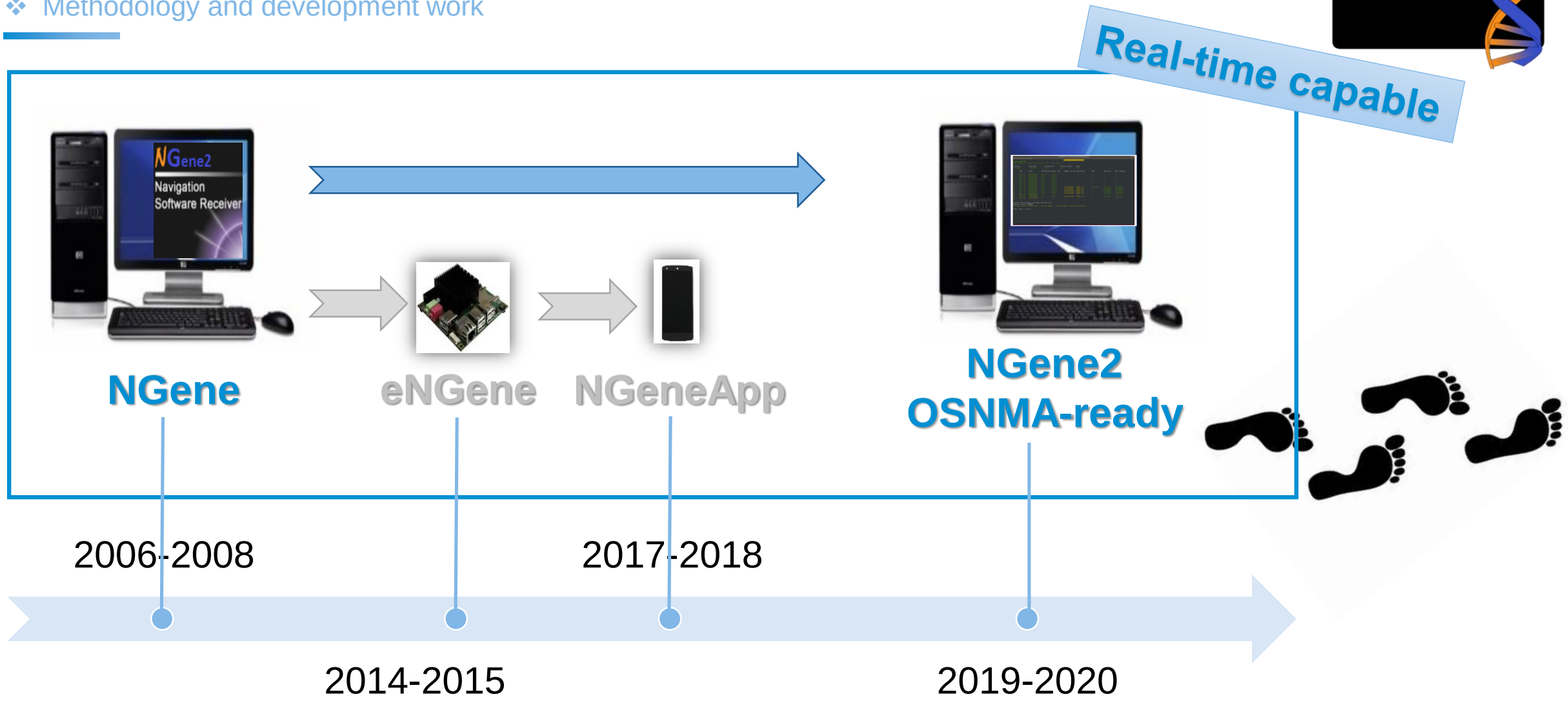
❖ Introduction

- **No OSNMA-ready commercial receivers were available on the marketplace**, so the only way to test this new service is to go for an ad-hoc, proprietary implementation

- **Goal**: implementation of the OSNMA functionalities in a complete GNSS fully software receiver
  - ✓ able to process in real-time the Galileo signal, including the OSNMA bits
  - ✓ exploiting the Software-Defined-Radio (SDR), providing the highest level of flexibility to easily add new features or algorithms and speeding up the prototyping process

NGene receiver family

- Methodology and development work



NGene2 software receiver

❖ Methodology and development work

NGene2 real-time software receiver

- Supports the L1/E1 **GPS/EGNOS/Galileo signals** elaboration chain
- Supports several L1/E1 USB front-ends
- **Two usage modes**
  - Real-time from USB front-end
  - Post-processing from file
- **Two processing modes**
  - Raw samples processing mode
  - Navigation message bits processing mode
- Enabled to process the E1 OS I/NAV message **OSNMA bits**

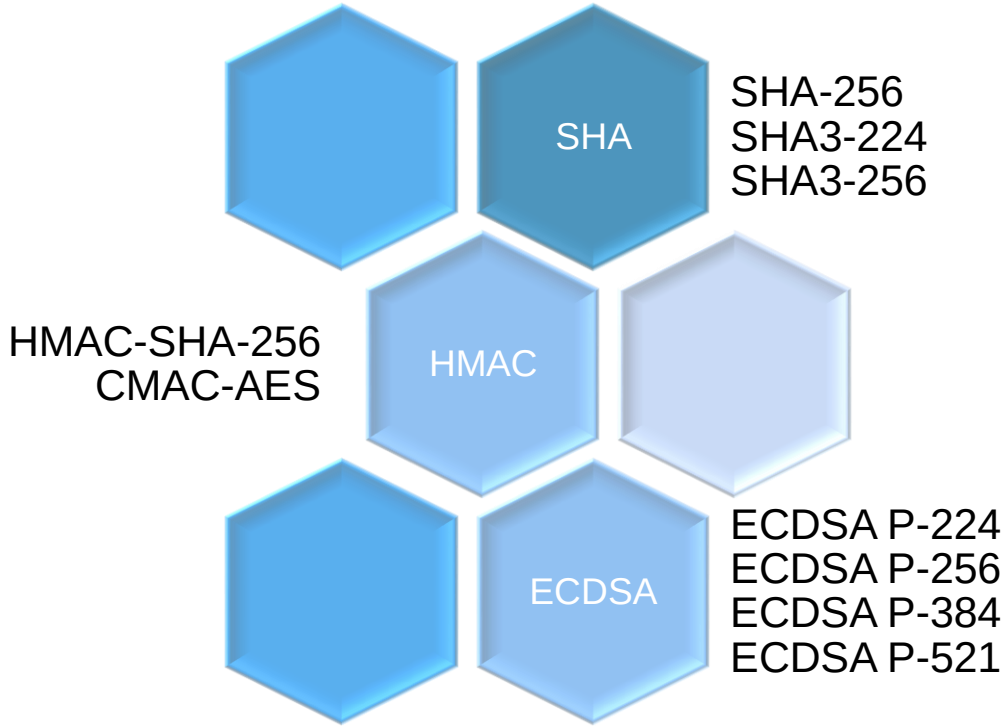
B. Motella, M. Troglia Gamba, M. Nicola, "A real-time OSNMA-ready software receiver," *Proceedings of the 2020 International Technical Meeting of The Institute of Navigation*, San Diego, California, January 2020, pp. 979-991

M. Troglia Gamba, M. Nicola, B. Motella, "Computational Load Analysis of a Galileo OSNMA-Ready Receiver for ARM-Based Embedded Platforms," *Sensors* 2021, 21, 467. https://doi.org/10.3390/s21020467

Receiver Upgrade

❖ Methodology and development work

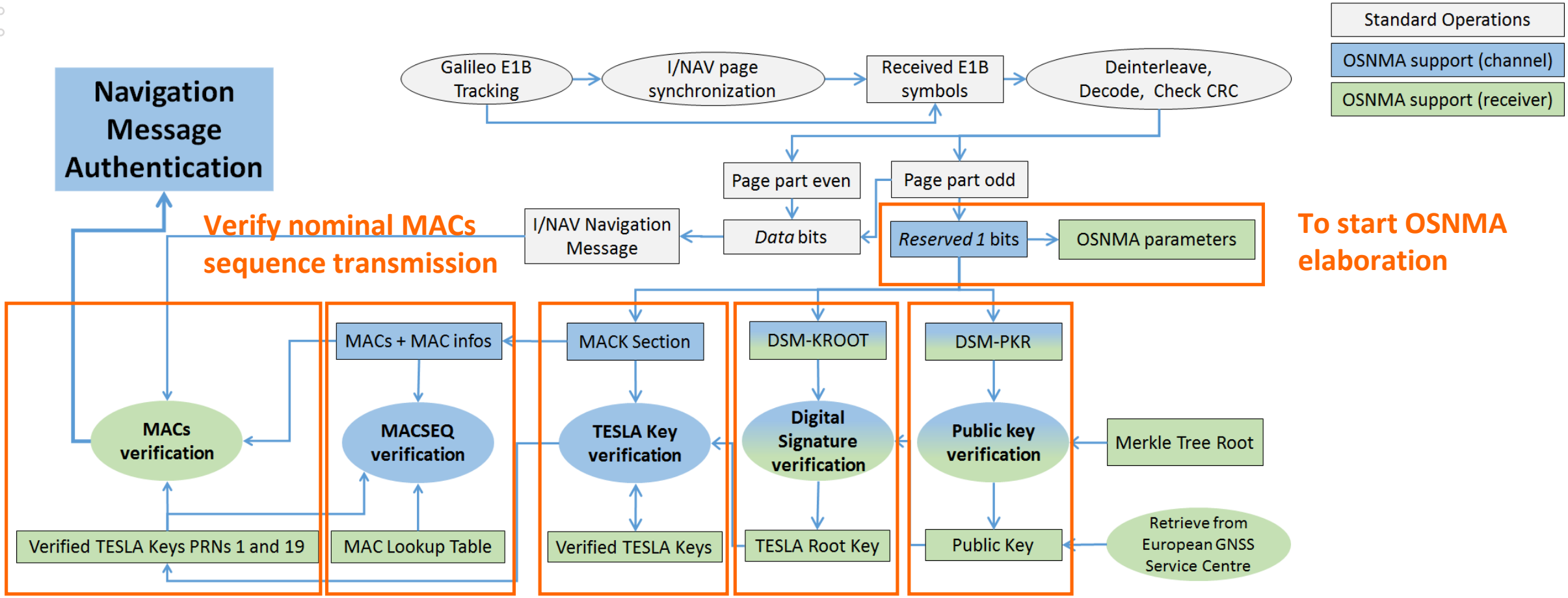
- **OSNMA support** included in NGene2 according to the ICD specifications
- Development performed on a standard desktop PC with Ubuntu 18.04 LTS OS using Eclipse IDE and GCC compiler
- **OpenSSL 1.1.1 library** used for the cryptographic functions
- Five main functionalities developed:
  1. **Digital Signature verification**
  2. **TESLA key verification**
  3. **MAC verification**
  4. **MACSEQ verification**
  5. **Public key verification**



European Commission, Galileo Navigation Message Authentication Specification for Signal-In-Space Testing – v1.1. grow.ddg3.j.1(2018)1670062. October 2018.

Receiver Block Diagram

❖ Methodology and development work



Test setup

❖ Software profiling analysis

- **OSNMA functions profiling** performed in terms of:
  - memory requirements
  - functions call rate and execution times
- **Testbed executed on:**
  - two standard desktop PCs
  - 60 h total running time
- **Profiling tools**
  - Standard profiling not suitable for an accurate profiling
  - Home-made profiling procedure specifically set up

	Parameter	Value	
OSNMA parameters	NS	36	
	NB_KROOT	7	
	NMACK	2	
	HF	SHA-256	
	MF	HMAC-SHA-256	
	KS	96 bits	
	MS	10 bits	
	MACLT	26	
	MO	0 (No offset)	
	ADKD	{0,2,3,4,11,12}	
	NB_PKR	13	
	NPKT	ECDSA P-224	
	DSMs Sequence	{DSM-KROOT, DSM-PKR, DSM-KROOT}	
	D_KROOT	Short	Long
		32m 11s	1d 6h 32m 11s
General parameters	Number of Galileo Satellites	7	
	Galileo PRNs	{5,6,7,14,24,25,26}	
	NavMsg Length	1 h	

Platform	Platform 1	Platform 2
Board	Dell Optiplex 9010 Desktop PC	Dell Precision T1700 Desktop PC
Processor	Intel® Core™ i7-3770	Intel® Xeon® E3-1270 v3
Base frequency of the processor	3.40 GHz	3.50 GHz
Cores	8	
Memory	8 GB DDR3	16 GB DDR3
Operative System	Ubuntu 18.04.3 LTS (64 bit)	

Results

- Software profiling analysis

	Intel® Core™ i7-3770			Xeon® E3-1270 v3		
	Call rate (Hz)	Mean value (µs)	Standard deviation (µs)	Estimation accuracy (%)	Mean value (µs)	Standard deviation (µs)	Estimation accuracy (%)
TESLA key verification (one step)	13,60	0.71	0.01	1.77	0.61	0.02	2.87
MAC verification	2,62	10.89	0.20	1.87	7.85	0.21	2.66
MACSEQ verification	0,27	8.74	0.20	2.26	5.84	0.18	3.11
Digital Signature verification	0,03	345.53	4.07	1.18	134.82	1.51	1.12
Public key verification	0,01	3.50	0.12	3.43	2.76	0.08	3.08

Highest call rate

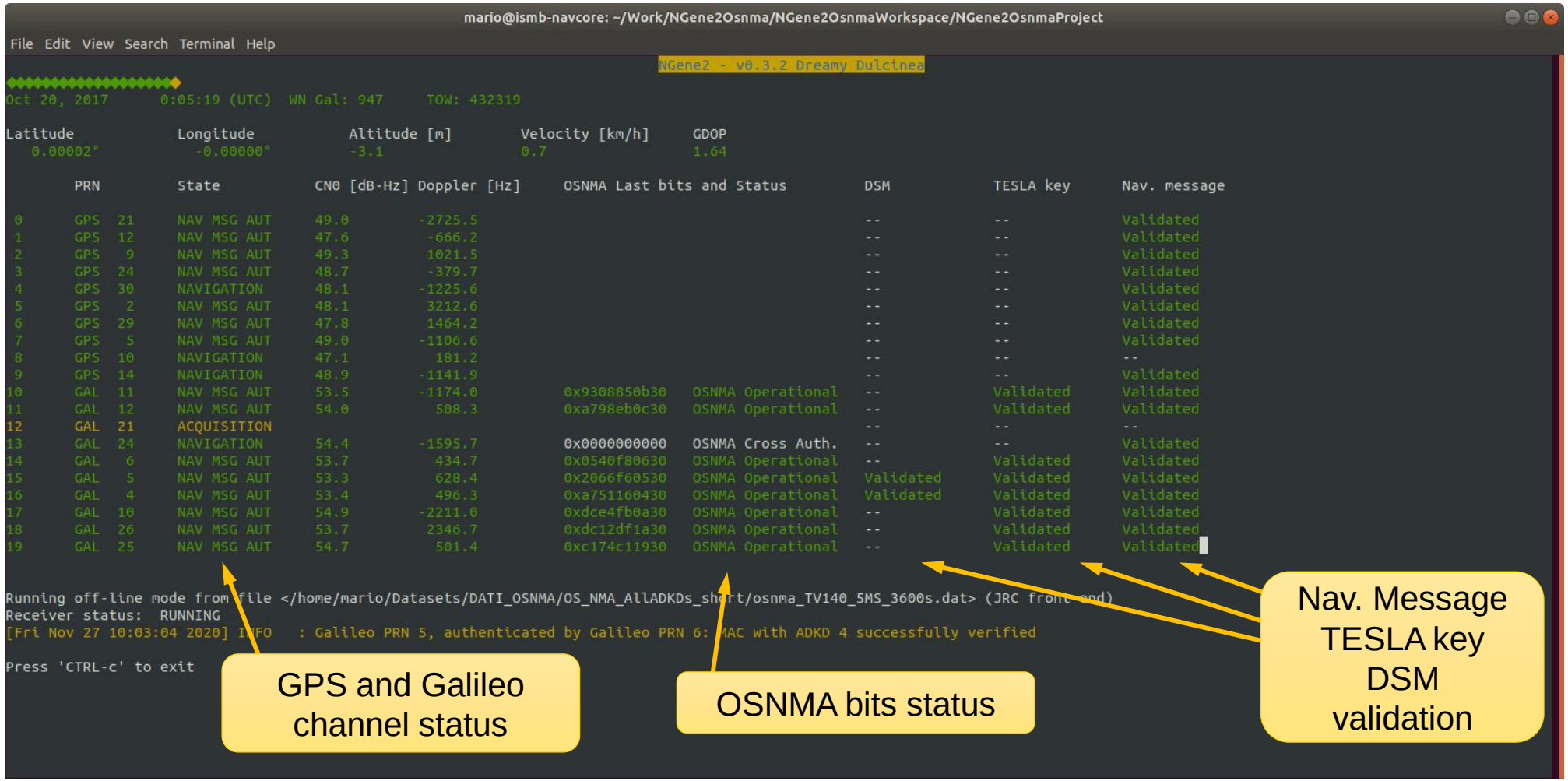
Lowest call rate

Reduced execution times on Xeon®

Additional memory usage negligible w.r.t. the original version of the RX

NGene2 software receiver

- Software profiling analysis



Recommendations for the RX Implementation

❖ Conclusions and recommendations

- **Perform the parse of DSM section both on system and satellite basis**
  - The DSM offsetting allows to speed up the reception of DSM joining together OSNMA bits from different satellites → good for first authentication latency reduction
  - Cross-check with DSM from single satellites might increase robustness
- **Continuously monitor the validity of DSM sections** for an early detection of spoofing attacks
- Perform a **consistency check** between the **received signal time** and the **RX clock**
  - Galileo System Time is used in the TESLA key (and MAC/MACSEQ) verification

Conclusions

Conclusions and recommendations

- **NGene2** → implementation of a new **fully SW OSNMA-ready GNSS receiver**
- Profiling analysis OSNMA functions
  - **Compatibility** between the computational burden requirements posed by a **real-time SDR architecture** and the computational power available in standard PCs
- **eNGene** → Real-time ARM-based SW receiver (Linux)
  - Implemented on ODROID-X2, but compatible with more recent ARM-based embedded platforms

November 2020 - April 2021: NGene2 used to support the Joint Research Centre of the EU Commission in the testing phase of the OSNMA Galileo signal

FONDAZIONE links

PASSION FOR INNOVATION

Dr. Beatrice Motella

Project Leader, Space and Navigation Technologies research area

Beatrice.motella@linksfoundation.com

linkedin.com/in/beatrice-motella-5a6b9b13b/

FONDAZIONE LINKS
Via Pier Carlo Boggio 61 | 10138 Torino
P. +39 011 22 76 150
LINKSFOUNDATION.COM