PROOF-OF-CONCEPT OF A SPACE-BASED POSITION AUGMENTATION WITH 2WAY COMMUNICATION

ESR – Executive Summary Report

Contributor	***Responsibility***
Etienne Rouanet-Labe (TAS)	Navigation algorithms engineer
Reviewer	
Ryan Jamal (TAS)	Technical responsible
Approval	
Marc Espinasse (TAS)	Project manager

CHANGE RECORDS

ISSUE	DATE	§ CHANGE RECORDS	AUTHOR
1	26/10/2023	Creation of the document	ERL

1. INTRODUCTION

1.1 Generality

This document is a shorter summary of the Summary Report document, that synthesizes the outputs of the ESA project "Proof-of-concept of a space-based position augmentation with two way communication".

1.2 Applicable & Reference documents

1.2.1 *Applicable documents*

Ref.	Reference	Title
[AD1]	ESA-TEC-SOW-018207	Proof-of-concept of a space-based position augmentation with 2WAY communication – EXPRO PLUS

1.2.2 *Reference documents*

Ref	Reference	Title
[RD1]	0005-0013334219	D101 - Report on state-of-the-art survey and use cases
[RD2]	0005-0013334207	D102 - Protocol and user equipment design
[RD3]	0003-0002935083	D201 - Design justification file
[RD4]	2WAY-TN-QAS-005	D301 - Testbed design
[RD5]	2WAY-VC-QAS-001	D302 - Validation and performance assessment report
[RD6]	0005-0017652475	D401 - Guidelines for space-based two-way ranging augmentation for PNT / Adaptation of two-way ranging to commercial technologies
[RD7]	0005-0017658798	FR - Final Report
[RD8]	0005-0017663287	SR - Summary Report

2. OBJECTIVES OF THE PROJECT

The project is centered on space-based NavCom systems for secure positioning and synchronization. In this context, the approach is using two-way protocols, which are bidirectional exchanges between a user and a gateway.

The bidirectional protocols are leveraged in order to derive secure ranging measurements, that can be transferred into a secure PNT.

The security is with respect to attacks, that can be executed either on the physical layer of the protocol, or be a join attack on the protocol data and physical layers.

The objectives of the project are :

- Design of a two-way protocol for space-based secure PNT, that allows to output secure ranging measurements
- Design algorithms for secure PNT that are based on the measurements output of the designed two-way protocol
- Demonstrate the security and performance of the designed concept, by implementation of a software testbed that simulates a space-based NavCom system that uses the designed protocol and algorithms.
- Draw conclusions on the sizing of a satellite-based two-way ranging system, and users adoption.

3. AN INCREASING NEED FOR SECURE PNT IN AN ENVIRONMENT OF GROWING THREATS

Secure PNT is an increasing demand for two categories of users :

Monitoring use cases
Reporting the positions of a fleet of trackers towards a remote end user

The monitoring use cases include :
- Road User Charging
- Illegal, Unreported, Unregulated Fishing monitoring
- Asset tracking

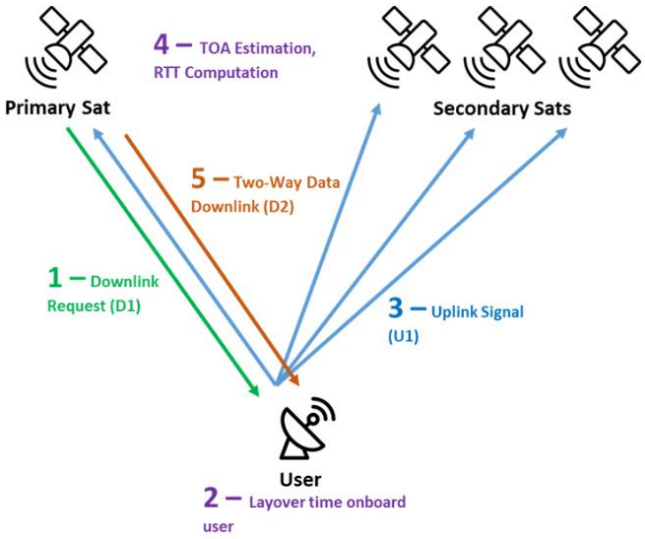
User PNT security use cases
Securing the PNT for a user co-located with its tracker

The user PNT security use cases include :

- Initial synchronization of a user for secure GNSS services (GALILEO OS-NMA / CAS, GPS CHIMERA)
- Secure Synchronization of Critical Infrastructures

A growing number of users → >20M users envisioned by 2030

4. A NEW TWO-WAY PROTOCOL FOR SECURE PNT IN A SATELLITE NAVCOM SYSTEM



A protection against Distance-Reduction attacks

The protocol was designed as Distance-Bounding, meaning that the encryption scheme protects the *Round-Trip-Time (RTT)* against Distance-Reduction attacks.

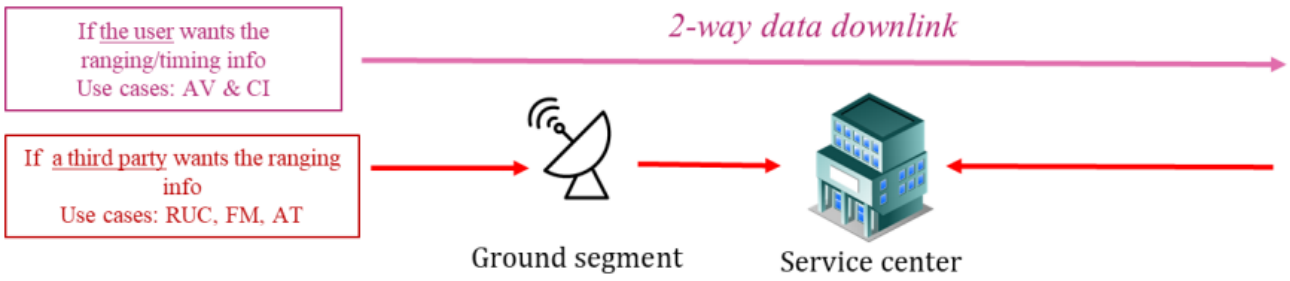
The protocol is vulnerable to Distance-Increase attacks by Record-And-Replay, but this security is handled by the PNT algorithms.

A satellite-initiated two-way protocol for reduced system complexity

The choice of a satellite-initiated protocol allows the use of Downlink multicast, which prevents the transmission of a synchronized Downlink message for each user Uplink request.

The secure ranging measurements are estimated onboard the satellites of the two-way constellation.

Two modes of PNT transmission



Depending on the nature of the use case, the RTT / PNT information is transmitted via two datalinks :

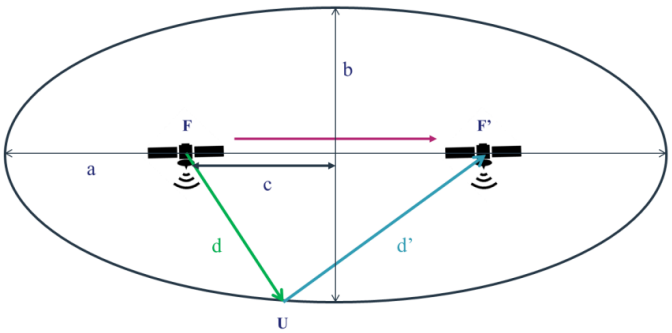
- Monitoring : the satellite measurements must transit through the ground segment where the tracker position is computed, before transmission to the remotely connected user via Terrestrial Networks.

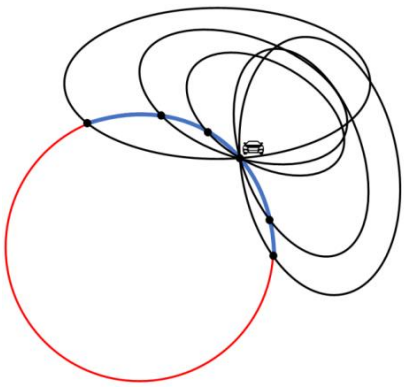
- User PNT security : the satellite measurements are directly downlinked to the user via a satellite Downlink, the user then computes its position.

5. NEW RTT-BASED ALGORITHMS FOR SECURE POSITIONING AND SECURE SYNCHRONIZATION

An innovative geometry-based secure positioning concept for space systems

The algorithm is based on a multi-RTT scheme. The security is ensured by considering the RTTs as upper bounds of the corresponding round-trip distances.

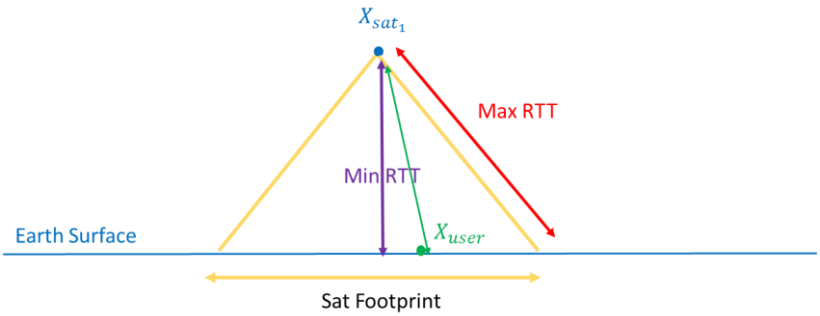




The altitude information is essential to solve the position, thus this concept is dedicated to users located on the ground.

A secure synchronization algorithm without need for user position information

The security is assured by the verification of the RTT value within the footprint of the satellite.



The accuracy of the output synchronization information is of the order of a few nanoseconds in a nominal case, but the range of the uncertainty for security corresponds to the difference between the maximum and minimum RTT values within the satellite footprint.

6. A FLEXIBLE TESTBED FOR SECURITY PROOF OF THE CONCEPT AND OPTIMIZATION OF TWO-WAY NACVOM SYSTEM PARAMETERS

Demonstration of the security of the concept

Spoofing attacks on the two-way signals were implemented in a software testbed for verification of the performance and security of the two-way protocol and PNT algorithms.

The testbed demonstration is complemented by a theoretical analysis of the threats on the two-way secure PNT concept by an independent team.

Optimization of two-way system parameters

The testbed allows tuning a wide range of system parameters :

- RF parameters : Uplink / Downlink frequencies, waveform, transmission power, antenna gains, integration time
- Constellation parameters : number of satellites, altitude, number of plans
- Demand parameters : number of simultaneous Uplink signals received

The service KPIs are output : accuracy / availability / security.

The testbed allows to assess various system designs and draw recommendations on system sizing.

7. PROMISING PROSPECTS FOR TWO-WAY BASED SATELLITE NAVIGATION SYSTEMS

Identified growing needs for secure PNT → 20M users by 2030

A new PNT concept based on two-way ranging proven as secure against a wide range of attacks

A PNT performance in line with the identified user expectations

Order of magnitude of compliant system size : 450 satellites at 2000km

A range of envisioned improvements for performance optimization :

- *Online selection of primary satellite*
- *Extension of the PNT concept to multi-epoch*
- *In-orbit demonstration of the concept / performance*

END OF DOCUMENT