TITLE:

Executive Summary Report

Trusted Radionavigation via Two-Way Ranging

	FUNCTION	NAME	DATE	SIGNATURE
PREPARED BY	Senior Scientist Senior Scientist Software Engineer	Sami Ruponen Tapio Suihko Ondrej Daniel	22.06.2020	
CHECKED BY	Senior scientist	Juha Zidbeck	22.06.2020	
APPROVED BY	Project Manager	Tatjana Petkovic	22.06.2020	

REF: NAVISP1-ESR-SSF-002-00015
ISSUE: 1.1
DATE: 22.06.2020

“EUROPEAN SPACE AGENCY CONTRACT REPORT

The work described in this document was done under ESA Contract. Responsibility for the contents reside in the author or organization that prepared it”

Document Change Record

Issue and Revision number	Date	Section, pages and paragraphs affected	Modified Items / Reason for Change
1.0	05.06.2020	All	First issue of the document prepared for Final Review.
1.1	22.06.2020	 2.1 2.3 1.1	Issue updated for Final Review close-out. Implemented action FR#04, i.e., RID TWR-FR-02: "improve vulnerability of the GNSS receiver" replaced by "reduce vulnerability". Updated contract number.

Table of Contents

List of Figures

List of Tables

No table of figures entries found.

1. Introduction

1.1 Purpose and Scope

This is the Executive Summary of the NaviSp Trusted Radionavigation Two-way Ranging activity. The activity was carried out under ESA Contract No. 4000131050/20/NL/DB (initial ESA Contract Nr 4000124540/18/NL/DB).

More information on the project objectives, activities and achievement can be found in Final Report [FR].

1.2 Glossary

1.2.1 Acronyms and Abbreviations

Acronym	Description
GNSS	Global Navigation Satellite System
IMU	Inertial Measurement Unit
NLS	Non-linear Least Squares
PTP	Precision Time Protocol
RTAI	Real Time Application Interface
TWR	Two-Way Ranging
UWB	Ultra-wideband
VM	Verifiable Multilateration

1.3 References

In order to better understand this document, it should be read in conjunction with the contents of the reference documents that provide relevant background information.

[SOW]	Statement of Work ESA Express Procurement Plus -EXPRO+ Trusted Radionavigation via Two-Way Ranging, NAVISP1-SOW-ESA-002-00002
[FR]	Final Report Trusted Radionavigation via Two-Way Ranging, NAVISP1-FR-SSF-002-00018

1.4 Document Overview

Section 1 is the introduction.
Section 2 provides the executive summary of the project.

2. Executive Summary

2.1 Motivation

The main project motivation is to establish a secure wireless link, which is used for a delivery of timing information to the user and for ranging estimation. The important underlying aspect is the security of the overall solution. The wireless link is then used as a basic building block for position estimation and as a source of extra trustworthy information for a GNSS receiver to reduce its vulnerability against various GNSS attacks. We introduce and motivate each of these topics in the following subsections.

2.2 Focus and approach of the project

Secure time transfer. Many critical systems requiring reliable timing information rely on GNSS timing information. Considering the vulnerability of GNSS, there is a need for a reliable algorithm allowing establishing the time synchronization, which would rely only on the communication link among nodes. It this project we design and develop time synchronization protocol operating over commercial off the shelf technologies.

Authenticated ranging. The ability to measure the distance over a wireless channel, is naturally very similar to the time transfer. It is crucial for various applications to estimate the distances towards surrounding base stations in a secure manner. So called distance bounding concept is an emerging research area aiming to solve the vulnerability implicitly included in the traditional approach for the distance estimation. The distance bounding protocols are a class of cryptographic-based protocols that allow to securely estimate the distance between two wireless nodes. The secure estimation is assumed here as a capability of the nodes to determine an upper bound on distance among them. However, when using commercial off-the-shelf radio devices (as is the case within this project) which do not support the distance bounding concept on the physical layer, the resilience against some attacks seems to be unrealizable since the zero delay during the challenge-response operation seems to be infeasible. Distance bounding with this limitation is known as the authenticated ranging and it assumes that the users and system nodes are always trustworthy. Within this project we build the authenticated ranging function, which is then used as a basic block for position estimation.

Verifiable multilateration. Verifiable Multilateration (VM) can be understood as a logical extension of the distance bounding/authenticated ranging concept for a position estimation where the position is determined based on authenticated ranges. The actual positioning determination in VM can be performed similarly as in other positioning systems. The underlying measurement model is formed by a (possibly overdetermined) system of nonlinear equations and hence iterative techniques based on linearization are traditionally employed. In order to better cope with user's movement dynamics, a filter designed based on the Bayesian estimation approach. In this project we build the positioning system on top of the secured two-way ranging protocol and we utilize the Extended Kalman filter.

Security augmented GNSS receiver. The secure time transfer function and the authenticated ranging functions are used as a source of trustworthy additional information supporting the GNSS receiver on the user node. The receiver can exploit this information in order to extend its level of resilience against various GNSS attacks. This leads to a concept of security augmented GNSS receiver, which is also implemented within the scope of this project.

Feasibility study for satellite based two-way ranging system. In the final part of the project we investigate whether (and under what conditions/parameters) it is feasible and reasonable to consider the authenticated two-way ranging protocol between a terrestrial user node and a satellite-based system. Within this task, we evaluate what benefits such a solution might bring to the end users and we address the technical obstacles, which need to be overcame.

2.3 System overview

The overall system developed within the project consists of a set of mutually communicating nodes. We distinguish among so called *system nodes*, which are statically located on fixed and known positions, and *user nodes*, which are mobile. All nodes can communicate with each other. The nodes exchange information in order to accomplish the following tasks:

- authenticated two-way ranging,
- secure time transfer,
- secure augmentation for GNSS based positioning, and
- positioning based on verifiable multilateration technique.

An overview of the considered system is depicted in Figure 1. There is the user node which is connected to the network. The local clock of the node is time-wise synchronized to the network via the secure time transfer protocol (the network itself is supposed to be synchronized to GNSS time). The node can estimate the distance towards surrounding nodes via the authenticated ranging protocol. Both these protocols are built on top of a short-range and long-range wireless communication standards, which are in this case UWB and Wi-Fi, respectively.

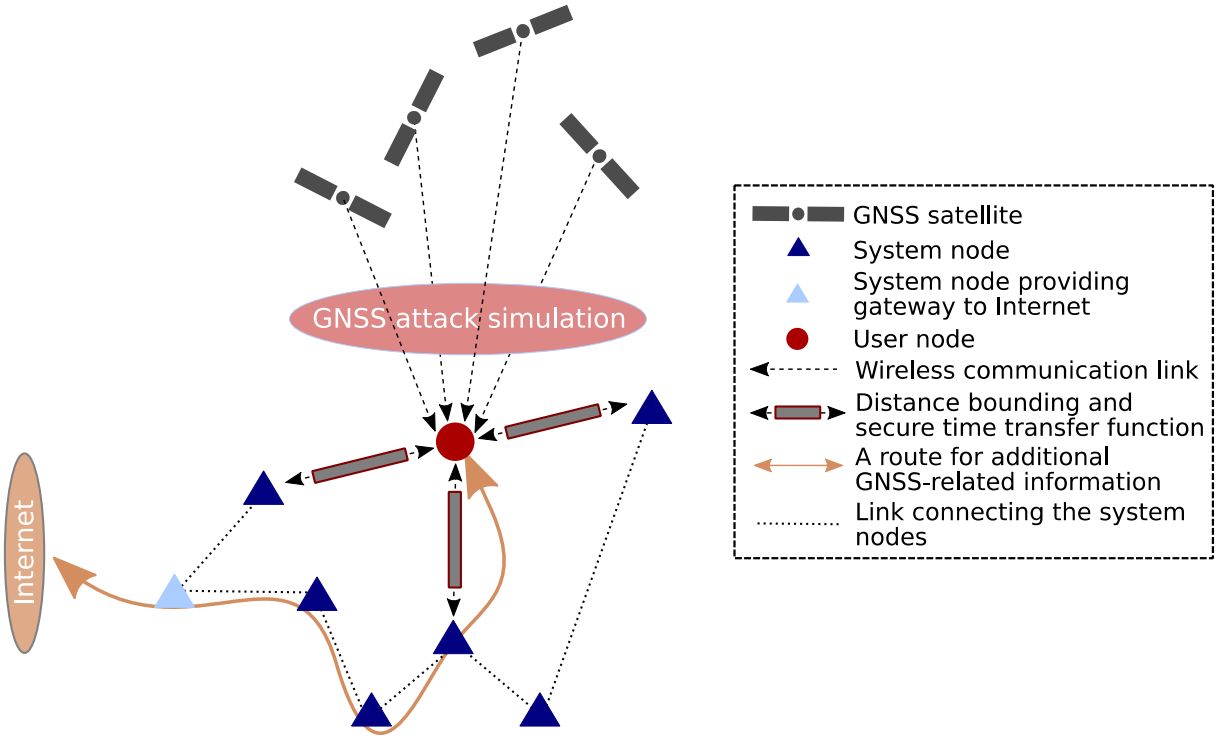

Figure 1: System overview of the secure GNSS-augmentation concept

Moreover, the user node is equipped by an inertial measurement unit (IMU) and commercial off-the-shelf GNSS receiver. In this project we aim to reduce vulnerability of the GNSS receiver with respect to various attacks. In principle, there are several approaches how to deal with the vulnerability. Within this project, we provide an extra a priori information to the various parameter estimators (such as estimators of the delay, frequency) employed by a GNSS receiver with an aim of limiting a search space over which the individual parameters are sought for, hence increasing robustness against various attacks. Moreover, we compare the outcomes of the GNSS receiver with additional information (such us distance from the two-way ranging protocol and readings from IMU) in order to detect the GNSS attack.

2.4 Achievements

We were able to successfully design and develop the overall system described in the previous sections. Nodes share the same hardware and software architecture; whether a node is configured as the user or system node is selected solely by the software configuration. The conceptual hardware architecture of a node is depicted in Figure 2, the software architecture is shown in Figure 3. During the development we focused on a clear definition of interfaces among various system parts.

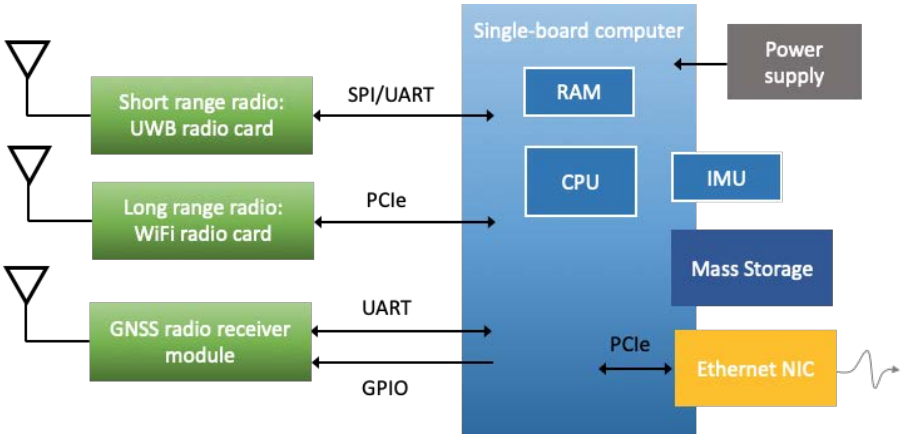

Figure 2: Node platform components

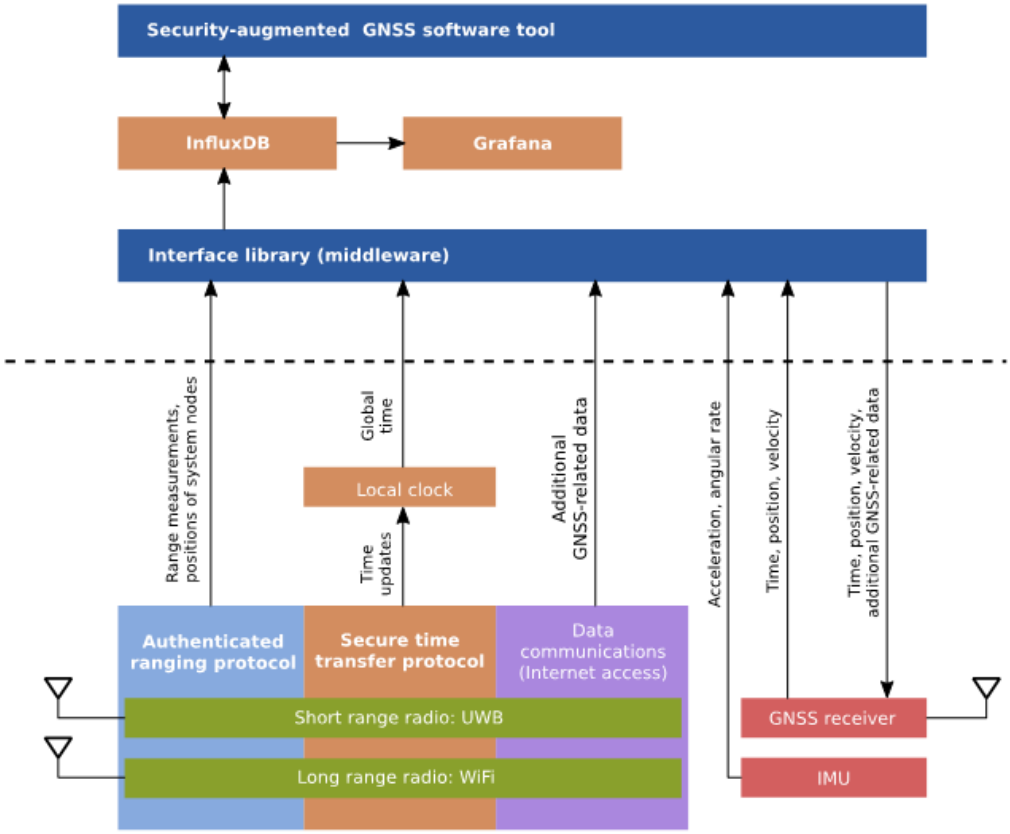

Figure 3: User node software architecture

The secure time transfer and authenticated ranging protocols were implemented differently for each of the radio technologies, as shown in Table 2. Probably the most difficult task was to achieve the high accuracy of timing and synchronization (needed for proper function of the secure time transfer and two-way ranging protocols). In particular, there is no support for any kind of timestamps in the Wi-Fi driver. Therefore, reception timestamp support had to be added in the interrupt routine of the Wi-Fi driver. Unfortunately, the latency in entering an interrupt routine in the normal Linux kernel is high, which undermines timestamping accuracy. Therefore, the kernel had to be augmented by patching it with real-time properties by using the Real Time Application Interface (RTAI) package.

Table 2: Functions vs. wireless technologies

Wireless system / **Protocol**	*Wi-Fi*	*UWB*
Secured time transfer	Reference Broadcast Infrastructure Synchronization (RBIS)	Precision Time Protocol (PTP)
Authenticated ranging	Fine Timing Measurement (FTM)	Two-Way Ranging (TWR)

Moreover, we developed an application implementing secure features reducing the vulnerability of a GNSS receiver with respect to attacks. In general, the application compares various parameters from the receiver with corresponding information obtained from the network of from IMU. There are the following checks implemented: ephemeris check, clock correction parameters check, orientation check, position check, distance check, time check, consistency check, and verifiability check. The application also implements the verifiable multilateration feature; an example of positioning based on UWB is illustrated in Figure 4 (left). More details about the application can be found in [FR].

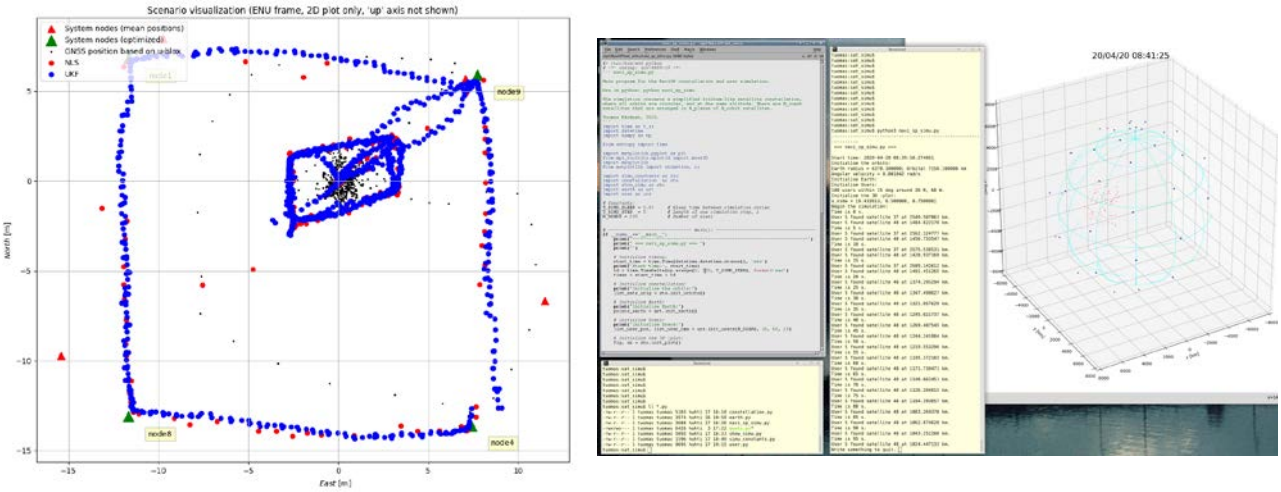

Figure 4: Position estimation based on two-way ranging measurements from UWB (left) and a snapshot of the simulator developed within the scope of the project (right)

Finally, we conducted a theoretical analysis and feasibility study of satcom based system, which would provide to its terrestrial users the secure time transfer and authenticated ranging functionality. The most important issue related to the system is its scalability (over the number of terrestrial users) since the communication is bidirectional. To provide reasonable conclusions about the system parameters, we developed a simulator considering real satellite constellations. A snapshot of the simulator is shown in Figure 4 (right).

Distribution

Nr	Destination
1	ESA

(End of the document)