

A dramatic, dark blue sky filled with heavy, dark clouds. Multiple bright, jagged lightning bolts strike across the scene, illuminating the clouds and creating a sense of intense energy and power. The overall mood is one of awe and technological advancement.

huld

**Space software and systems
with 30 years of experience**

huld



Exceptionally highly educated and experienced people

Over 400 working years' experience in international space projects.

huld

Space applications

Onboard
Software

Ground
Processing

ISVV

Data Processing
and Instrument
Quality Tools

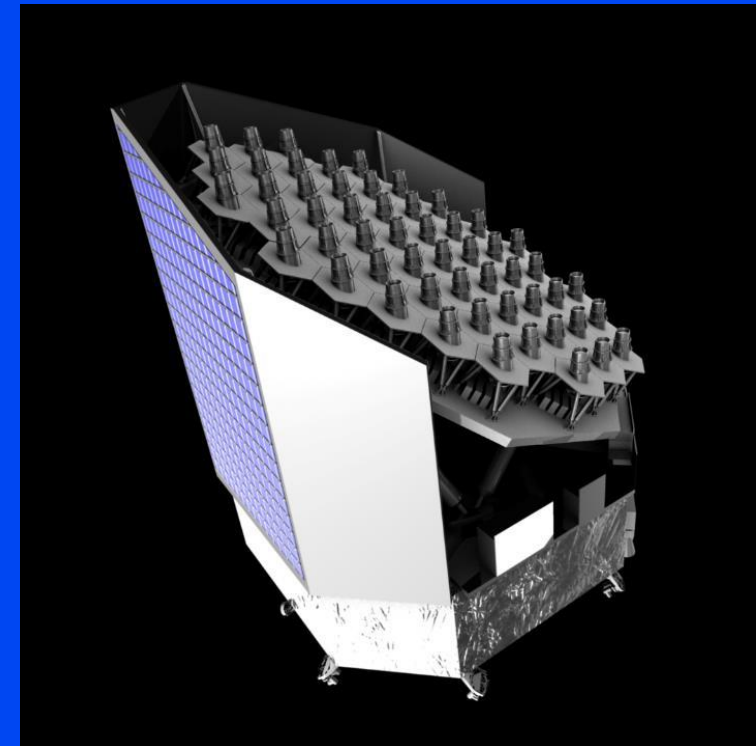
New Space

Space ML
based
Systems

huld On-Board Software Development



- 17 launched satellites carrying software designed or verified by Huld and 15 under work or waiting to be launched.
- Platform software to GOCE, Herschel, Planck and Gaia satellites.
- Latest references in application software segment are on board MetOp-SG (ROIC, SCA), ExoMars RSI, Euclid FGS, MTG FCI ICU ASW, Sentinel-4 ICU, Galileo ASW and MetOp CFSW.
- PLATO, the PLANetary Transits and Oscillations of stars mission, will be launched in 2026 to find and study exoplanets. Huld is the Spacecraft Software Prime in a consortium lead by OHB.



Ground Processing



Sentinel-4 UVN L1bPP (Airbus DS)

- Huld has developed the Level 0-1b Prototype Processor (L1bPP) that processes the raw measurements into level 1b products

Sentinel-4 UVN L1 Reference Processor (ESA)

- Huld is developing the reference processor to be used for cross-verification of the operational processor

Ground Segment as a Service (ESOC)

- Huld develops the Ground Segment Application infrastructure for SmallSats
- Cloud based service with modern UI and flexible interfaces.
- Supporting CCSDS family and CSP protocols
- Ongoing

Sentinel-5 UVNS L1bPP (Airbus DS)

- A nadir viewing push-broom spectrograph with a spectral range covering UV to short wave infrared
- SSF develops L1b prototype data processing software

MTG IQT (GMV Spain)

- Tool that allows the assessment of the geometrical and radiometric performances of the instruments on-board MTG I and S satellites

Space Trust for Maritime Activities (ESTEC)

- Huld develops Blockchain-based testbed platform for mitigation of Bunker Frauds Application
- Satellites provide metadata and protection against GNSS spoofing
- Ongoing

MTG L2PF (Thales Services SAS)

- Huld is responsible in integrating the science data processing implemented with Algorithmic Processing Elements (APEs) provided by ESA's S4 consortium onto the L2PF platform provided by Thales Services

Payload Data Acquisition and Processing (Thales)

- S5 L1B PGF software
- Huld develops and integrates S5 L1b processing into specific processing framework

OSCAR (GSA)

- Open Source Galileo GNSS receiver
- Development of open-source HW receiver for Galileo
- Ongoing

Independent Software Verification & Validation

- Galileo ISVV
 - Huld was responsible for the ISVV of five major units
 - Navigation Signal Generator Unit
 - Platform and payload Security Unit
 - Message Generation Facility
 - Integrity Processing Facility
 - Mission Support Facility
- BepiColombo ISVV
- Small-GEO ISVV
- EDRS-C ISVV
- MTG STR ISVV
- MTG SMU ISVV
- Jason (Sentinel-6) ISVV
- BIOMASS ISVV



Huld's GNSS Experience

GNSS projects since early 2000's

- Signal generators (Spectracom), pseudolites, RTK+
- ESA: EGNOS, Galileo, MetOp
- GSA: Open source GNSS receiver
- ESA R&D: IS Mask for RTK, Two-way ranging
- Consultancy: TestHouse, u-blox



Trusted Radionavigation via Two-Way Ranging

NAVISP EL1-002 ESA Contract No. 4000131050/20/NL/DB

Contractor	Huld Ltd., Finland
Subcontractor(s) (state if not applicable)	VTT Technical Research Centre of Finland Ltd (VTT), Finland
Contract Duration	From: 01.10.2018 To: 31.03.2020
Total Contract Price	450,000 EUR

Huld

NaviSp Trusted Radionavigation via Two-Way Ranging

- Project status
 - Final Review successfully completed in June 2020
- Project team:
 - Huld:
Ondrej Daniel (Tech lead), Kimmo Rautkoski, Tuomas Räsänen, Botond Sleber, Tatjana Petkovic (PM)
 - VTT:
Sami Ruponen, Tapio Suihko, Juha Zidbeck, Pekka Koskela



Content

- Introduction
- High level summary
- System architecture
- Authenticated ranging and Secure time transfer
- Security GNSS augmentation
- Feasibility study for SatCom verifiable multilateration
- Conclusion

Introduction

- Vulnerability of GNSS against malicious attacks
 - Spoofing, meaconing, jamming
- Exploration of the two-way ranging to provide security guarantees
- Considering existing wireless communication networks
- Considering commercial off-the-shelf hardware components and primarily open source software components
- Prototype development (network of nodes)

High level summary

T1: Technology Assessment & Prototype Design

T2: Point-to-Point Demonstration of Security Functions

T3: Demonstration of Security-Augmented GNSS

T4: Demonstration of Verifiable Multilateration

T5: Feasibility Study for SatCom Verifiable Multilateration

huld

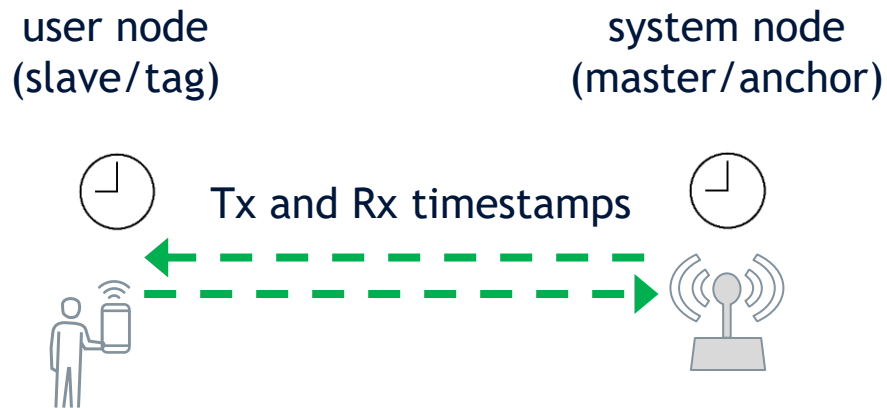
Minimal performance requirements for the prototype

- Time-transfer: 5 ms
- Authenticated ranging: 3 km
- Verifiable multilateration: 5 km

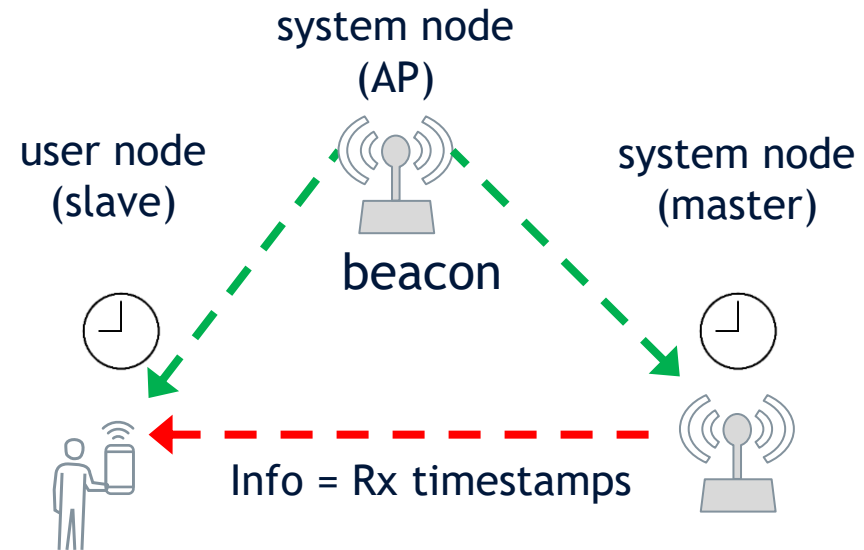
Basic functions

Given the COTS availability, opted for different solutions for the two radio technologies

Wireless system	UWB	Wi-Fi
Function		
Time transfer	Precision Time Protocol (PTP)	Reference Broadcast Infrastructure Synchronization (RBIS)
Ranging	Two-Way Ranging (TWR)	Fine Timing Measurement (FTM)



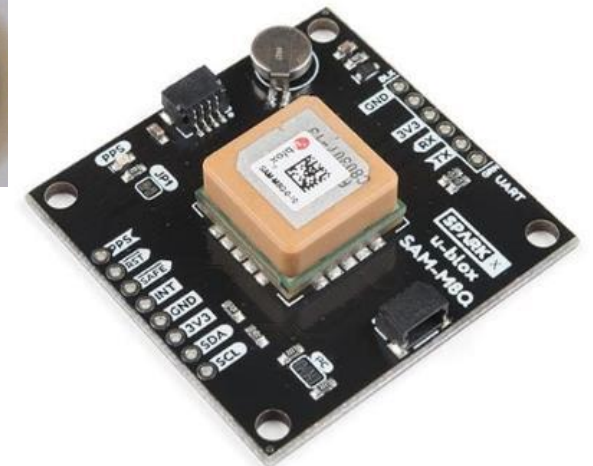
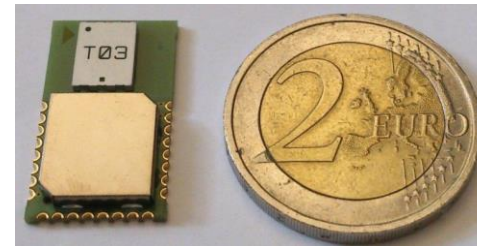
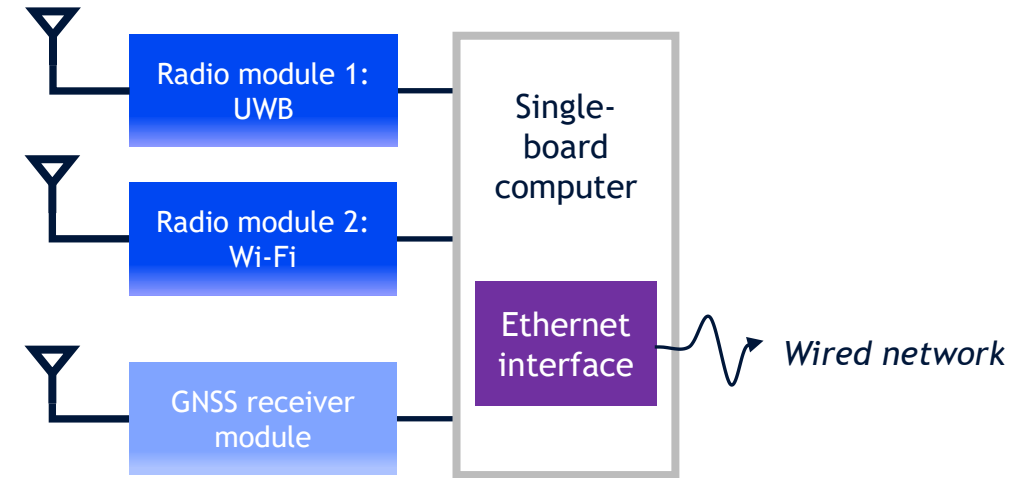
PTP, FTM, and TWR operation principle



RBIS operation principle

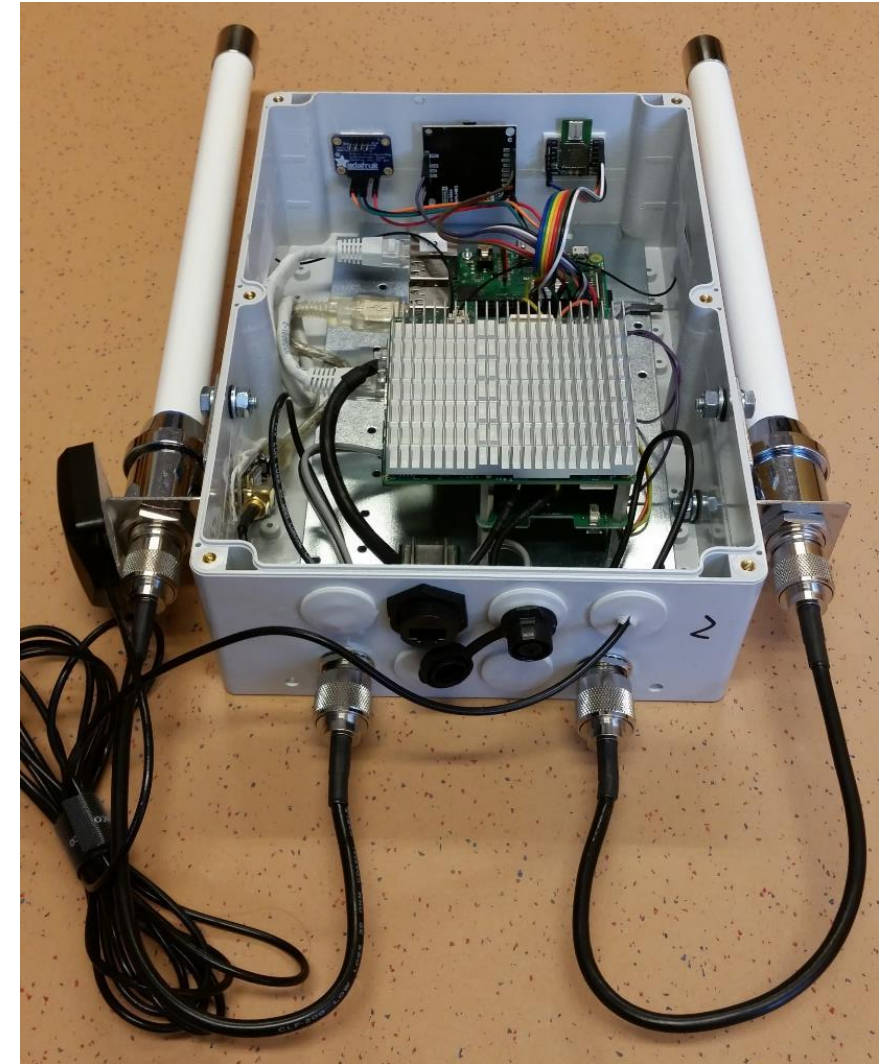
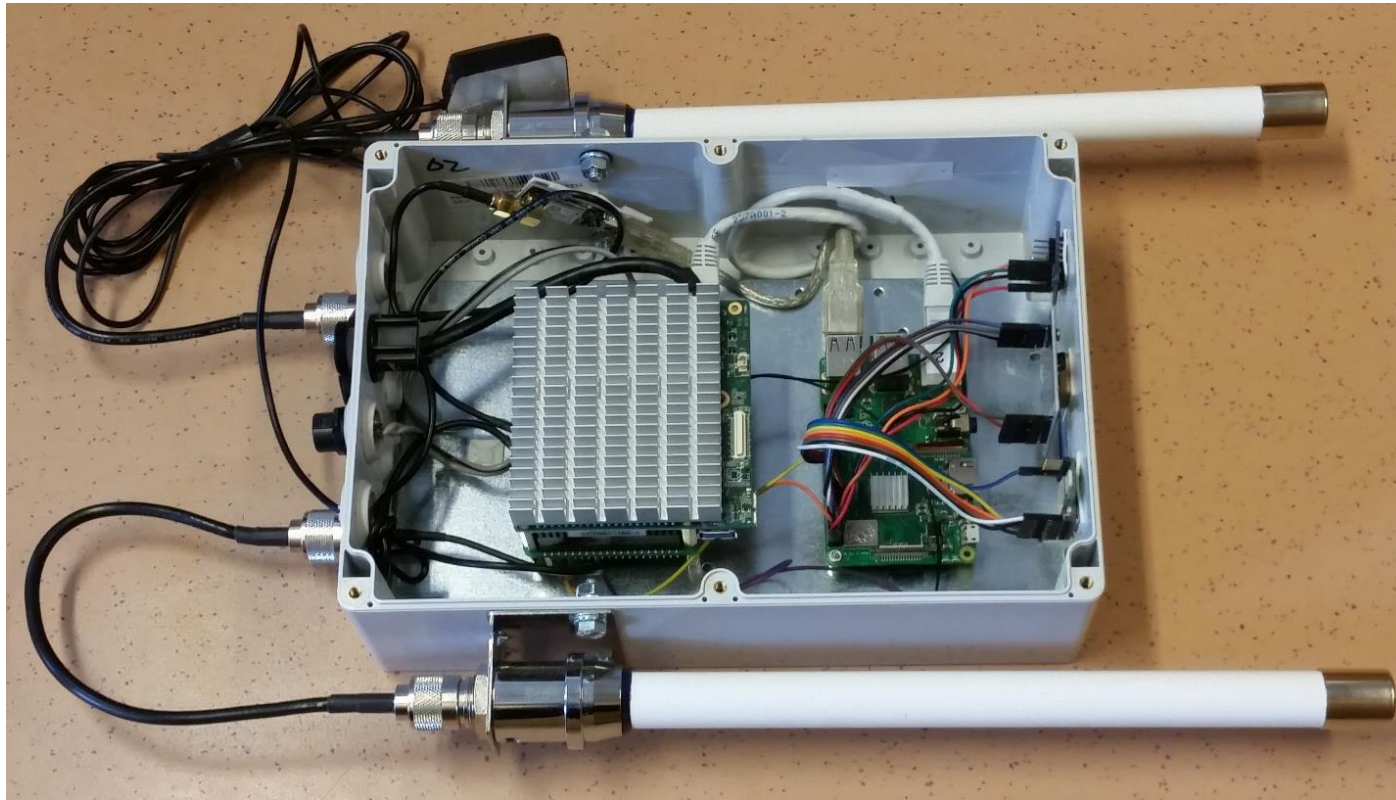
Hardware platforms - components

- UWB node platform
 - Raspberry Pi 3 model B+
 - Decawave DWM1000 UWB module (DW1000 IC)
- Wi-Fi node platform
 - AAEON UP2 model UP-APLC2-A10-0232, equipped with 1.1 GHz Intel Celeron N3350 SoC
 - Mikrotik R11e-5HnD, using the Atheros AR9580 chip
 - Wi-Fi mesh, long range (omni-antenna connectors)
 - Intel 8260NGW
 - FTM, short range (Molex film type sticker antenna)
- GNSS Receivers
 - Sparkfun SPX-15106 with u-blox SAM-M8Q GNSS module
 - u-blox M8T (only in one user node)
- IMU
 - Adafruit BNO055 (only in one user node)



hld

Hardware platforms - node assembly

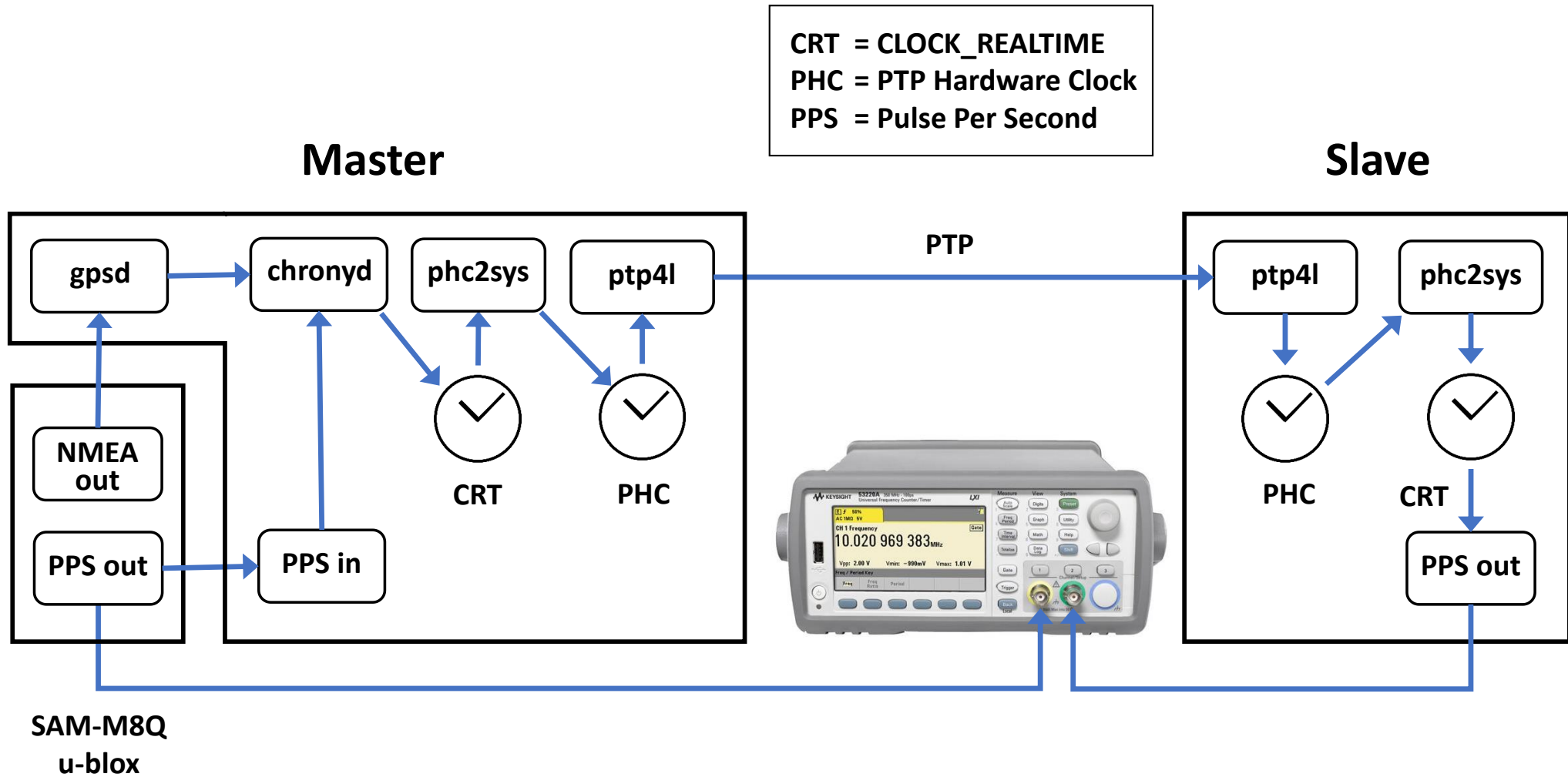




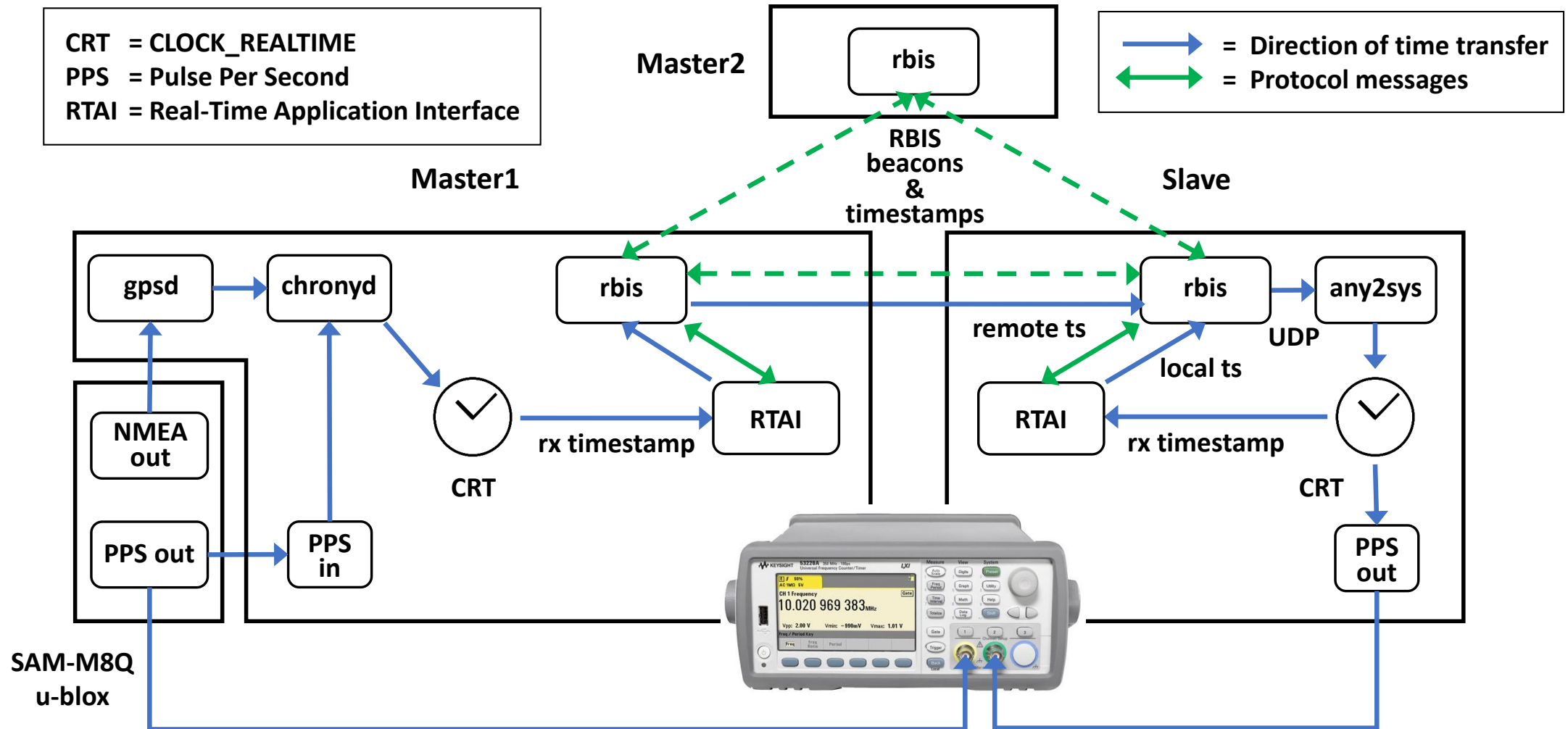
Security features in time transfer and ranging

- The system and user nodes are assumed trustworthy
- Man-in-the-middle attacks are prevented by using cryptography
- Still, the system is vulnerable to message delaying, denial of service, and spying
- PTP
 - Added PTP message authentication to LinuxPTP - comparable to Annex K in IEEE 1588-2008 standard
 - All nodes share a set of ephemeral session keys, no key distribution protocol
- RBIS
 - Relies on Wi-Fi security based on IEEE 802.11i standard (Robust Security Network)
- TWR
 - Message authentication (HMAC-256 truncated to 128 bits) and replay protection (sequence numbers)
 - PKI-based key delivery by using HTTPS - session keys derived from a master key by using HKDF
- FTM
 - Based on Intel's firmware that does not expose the HW timestamps, and lacks security
 - The FTM security solution is being standardized in IEEE P802.11 Task Group AZ

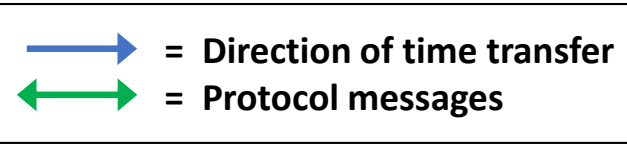
Time transfer validation - PTP over UWB measurement setup



Time transfer validation - RBIS over Wi-Fi measurement setup

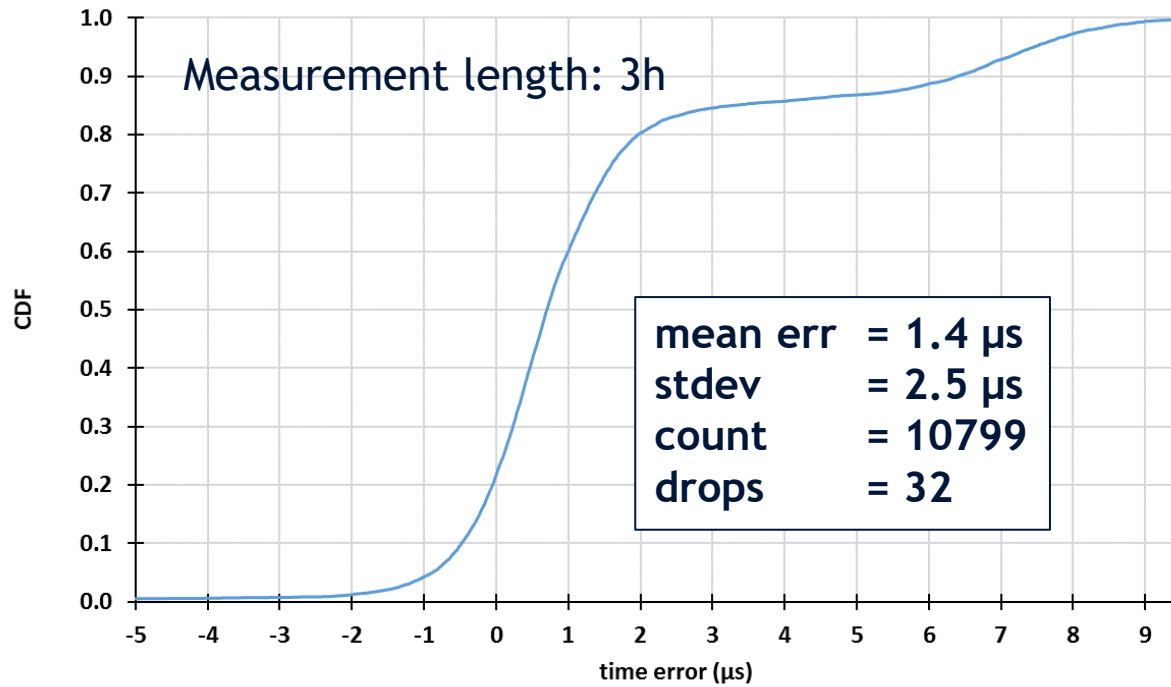


SAM-M8Q
u-blox



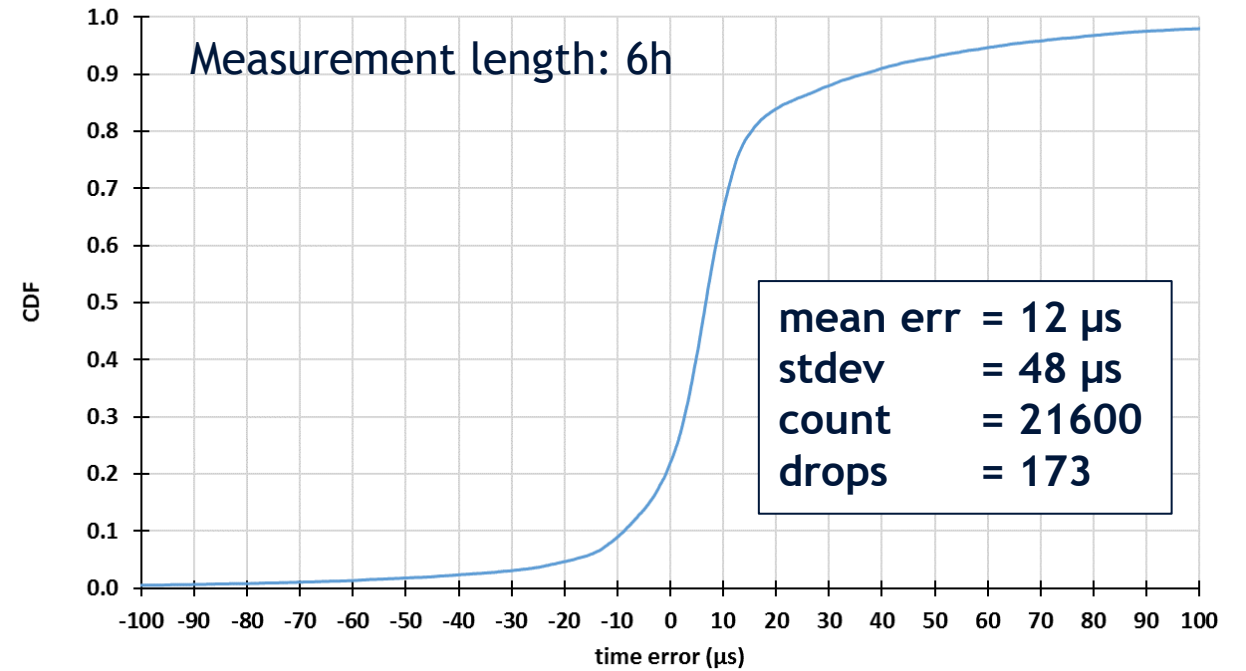
Time transfer validation - results

PTP over UWB (PPS poll)



PTP over UWB

RBIS over WiFi (PPS poll)



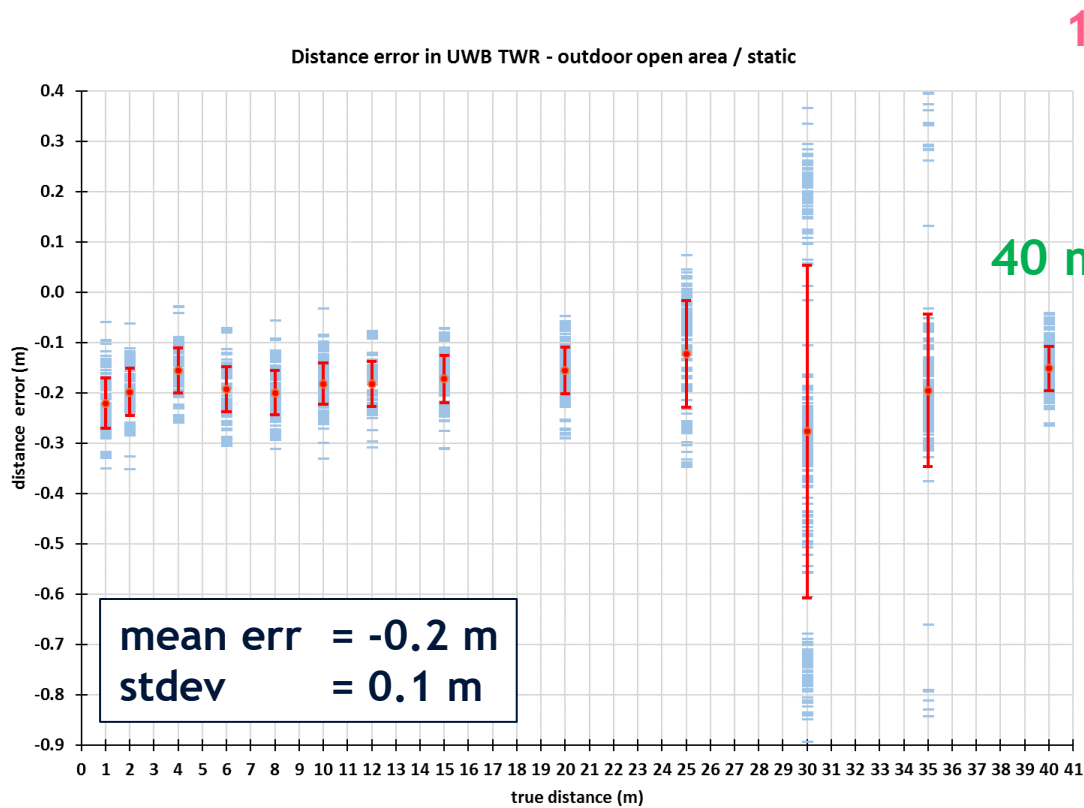
RBIS over Wi-Fi

hld

Ranging validation - outdoor measurement setup with UWB

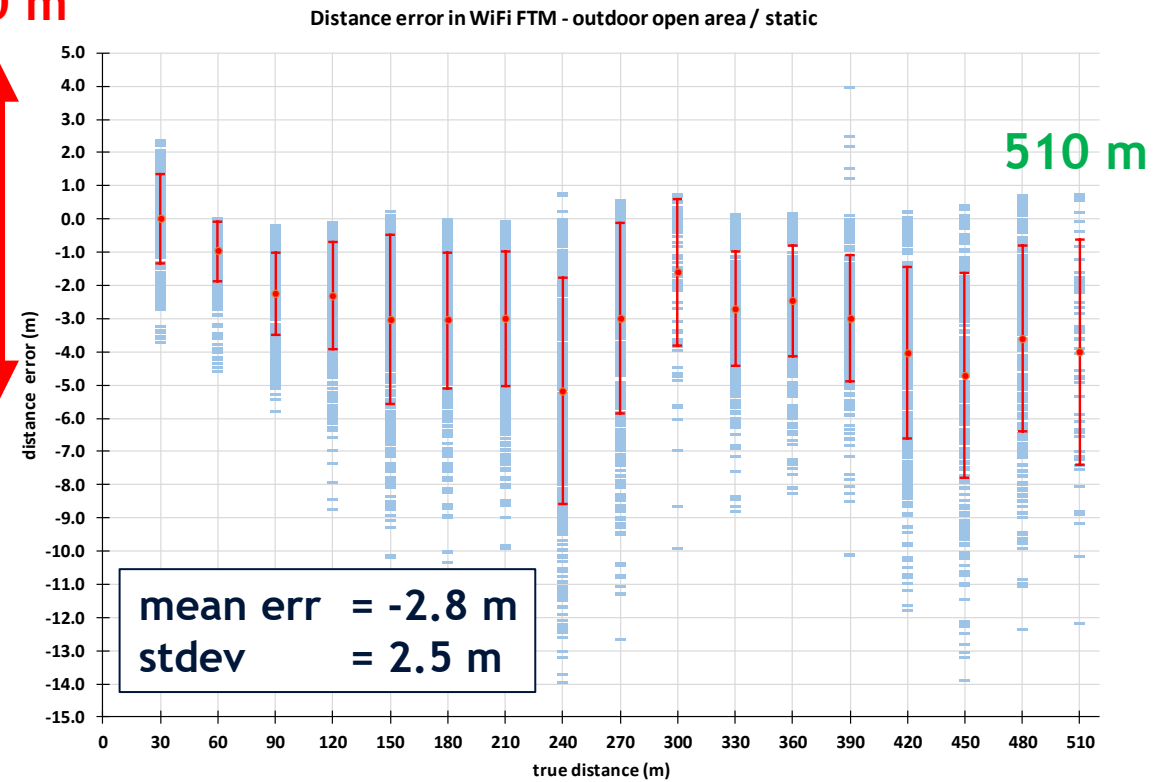


Ranging validation - results (outdoor open area)



TWR over UWB

1 m 10 m

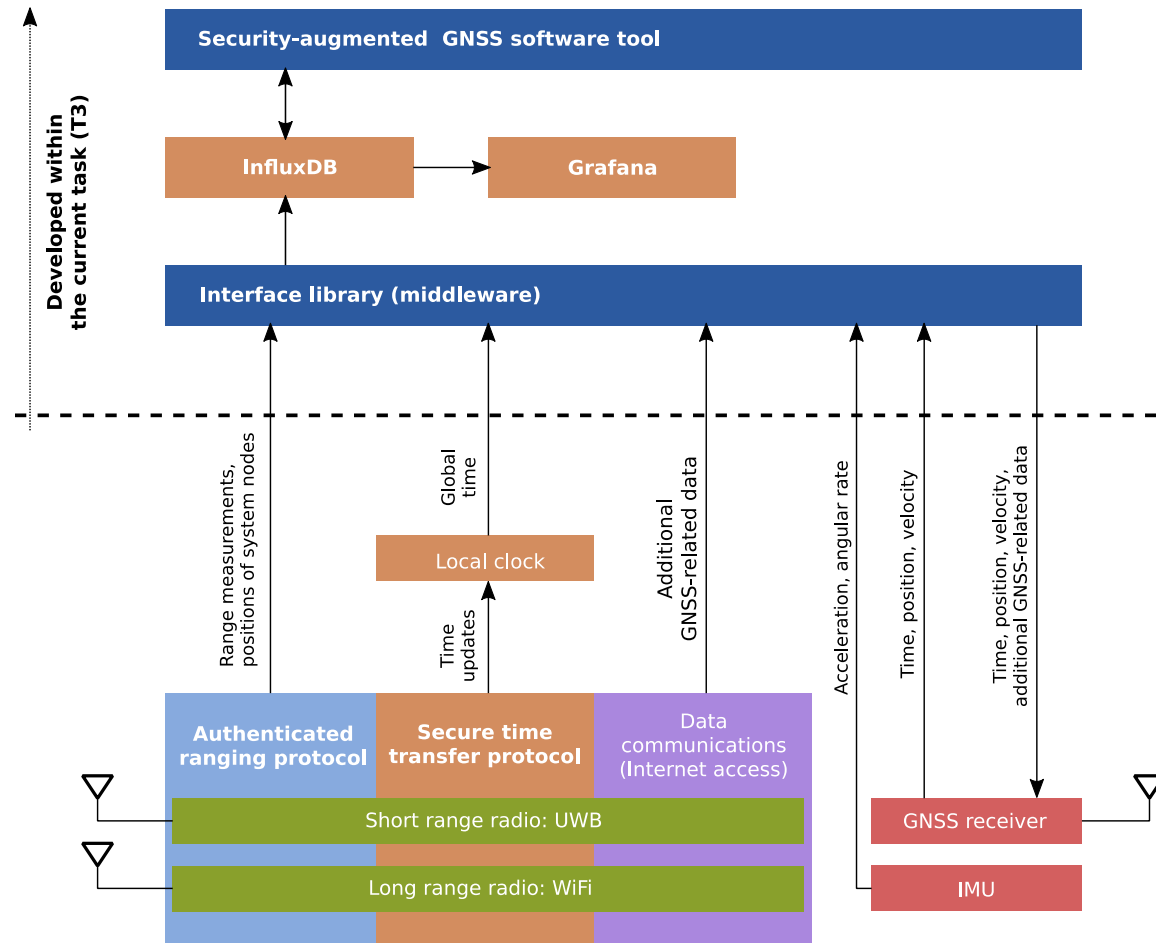


FTM over Wi-Fi

Security GNSS augmentation

- **Commercial off-the-shelf GNSS receiver considered**
 - u-blox M8Q
- **Augmentation methods**
 - Loosely coupled: GNSS receiver used as a black box
 - Tightly coupled: GNSS receiver is provided with additional trustworthy inputs
- **Functionality build on top of**
 - Authenticated ranging protocol
 - Secure time transfer protocol
 - Inertial measurement unit (IMU)

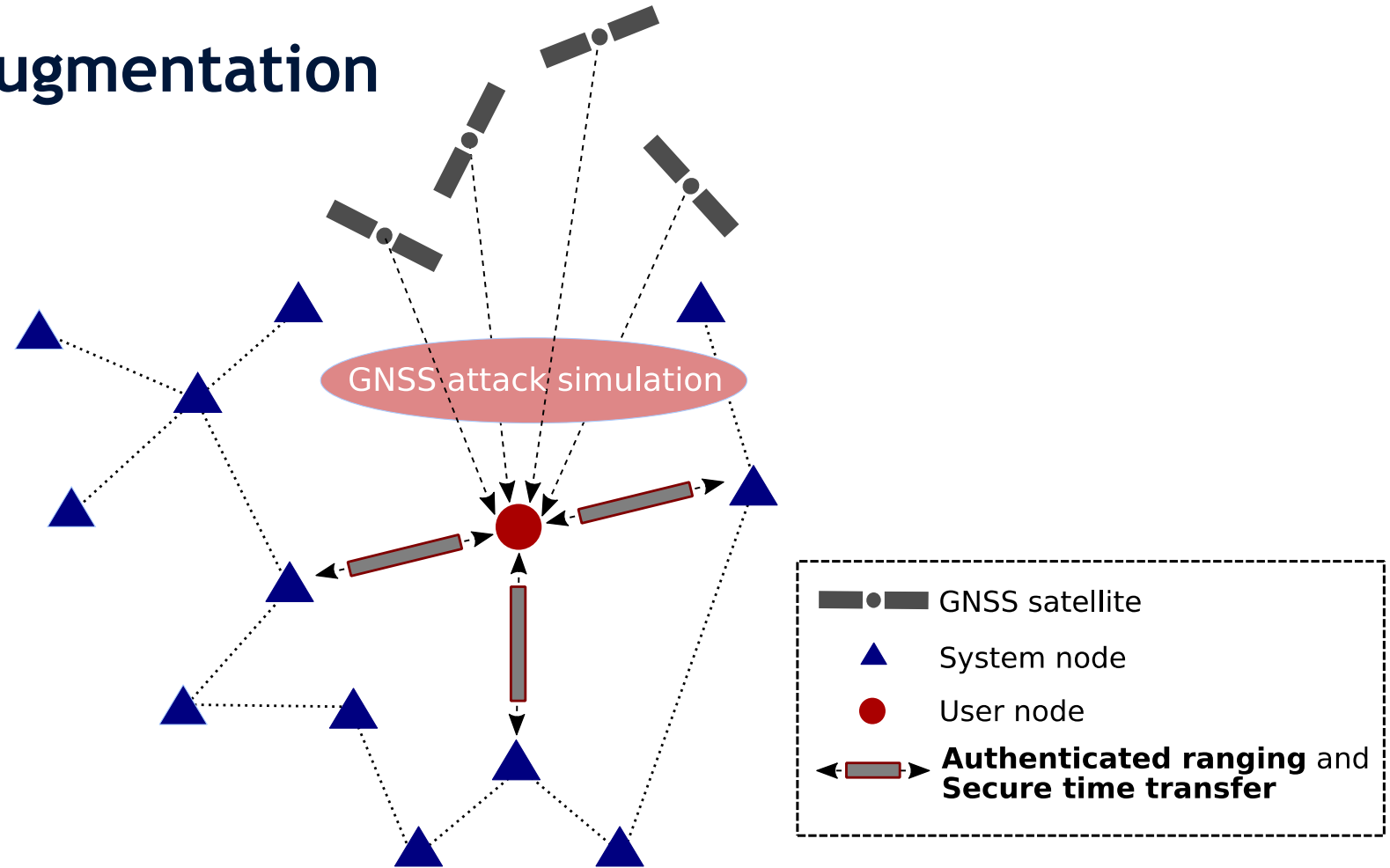
Security GNSS augmentation



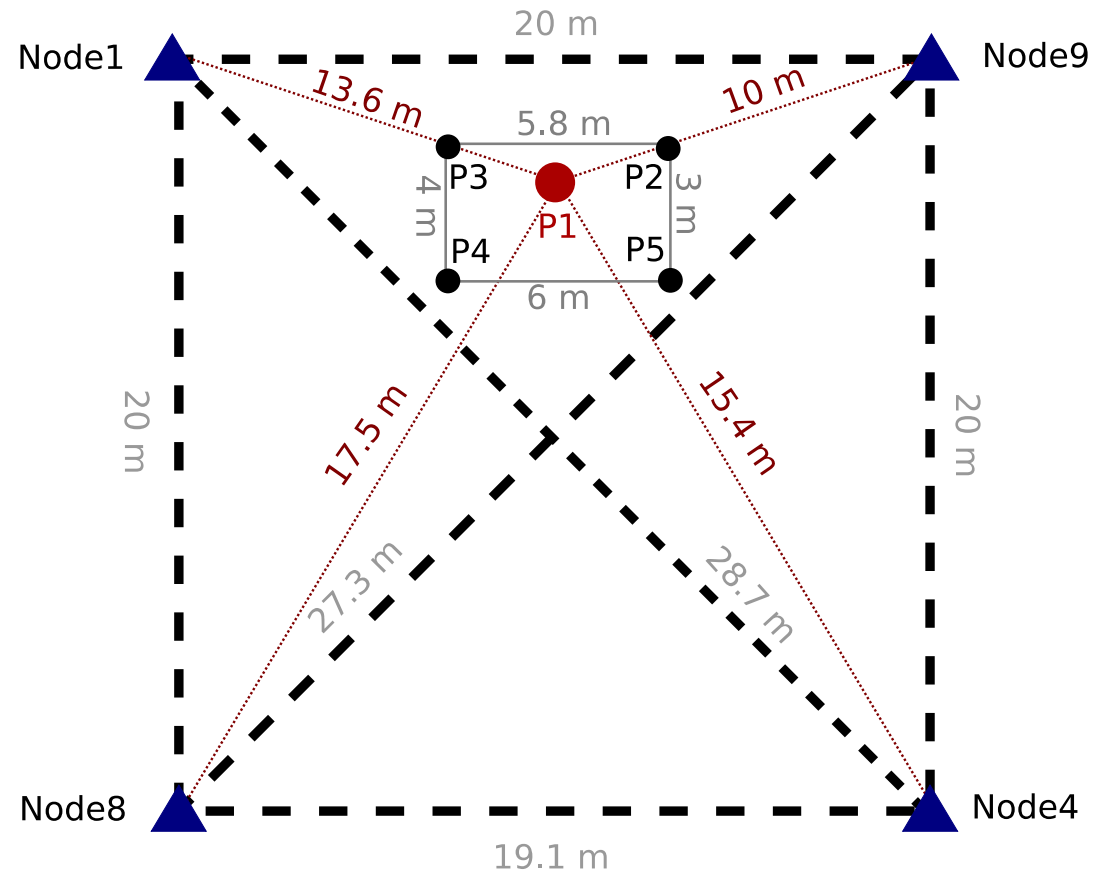
Security GNSS augmentation

- Position (and distance) check: TWR-based versus GNSS-based position (and distance) estimates
- Time check: System time versus time from GNSS receiver
- Orientation check: IMU-based orientation versus orientation calculated from GNSS observations
- Ephemeris check: Ephemeris from sky versus assisted GNSS service
- Clock correction parameters check: Clock correction parameters from sky versus assisted GNSS service
- Consistency check: Searching for a discrepancy among GNSS pseudorange measurements
- Verifiability check: Checking that TWR based position lies inside a pyramid/triangle formed by system nodes

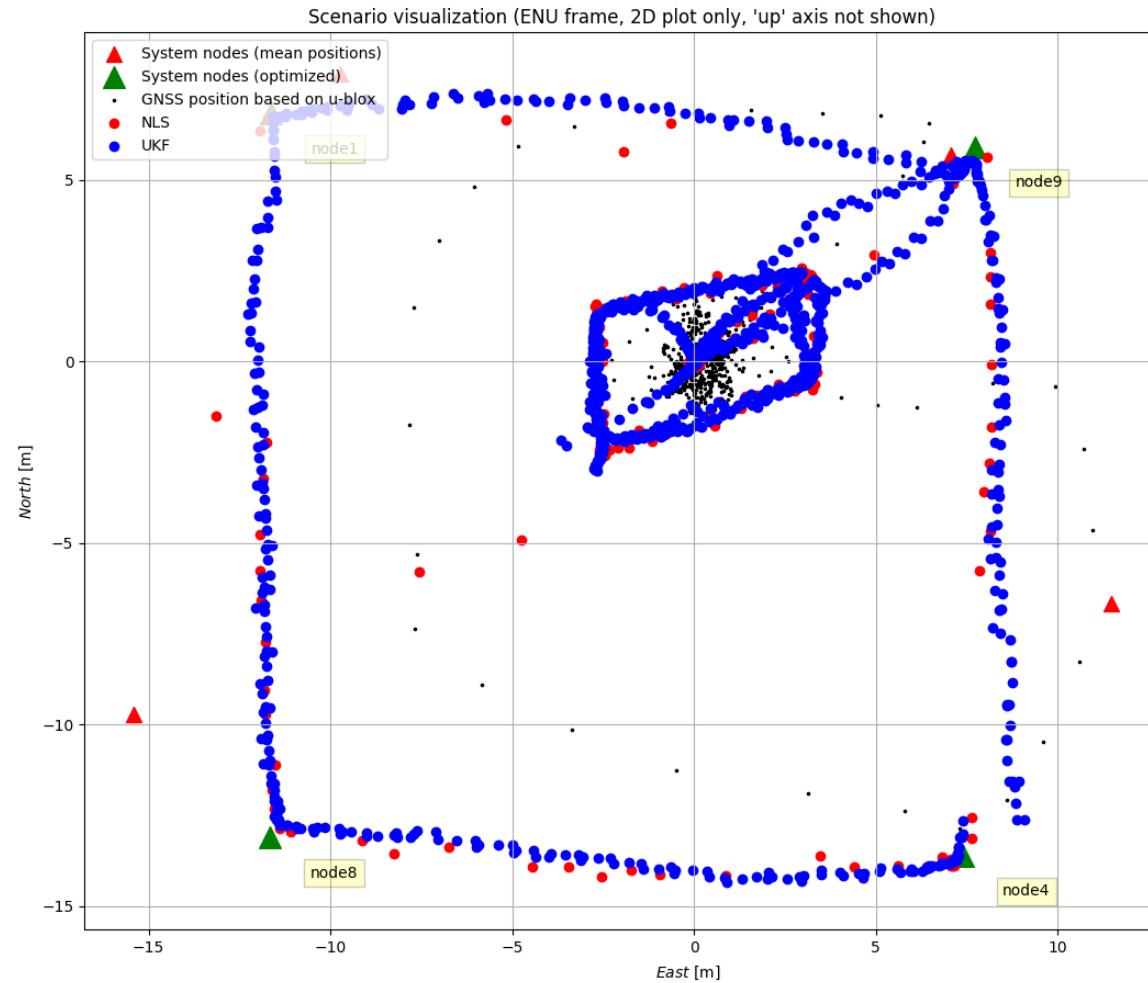
Security GNSS augmentation



Verifiable multilateration (demonstration)

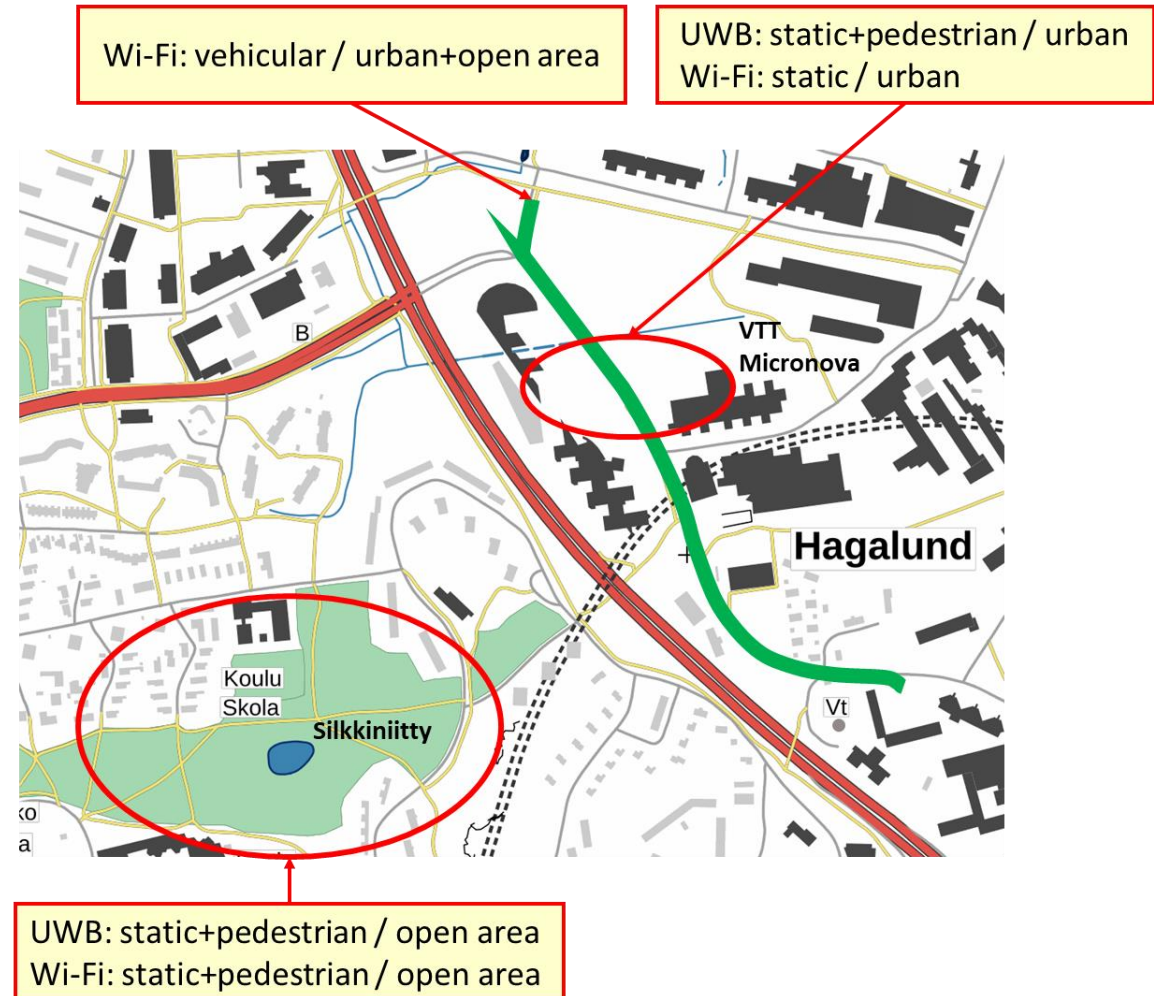


Verifiable multilateration (demonstration)



Verifiable multilateration (validation) - scenarios and testing areas

		Environment	
		Short range (UWB)	Long range (Wi-Fi)
Wireless system	Operating conditions	static	open area urban
		pedestrian	open area urban
	vehicular		open area urban

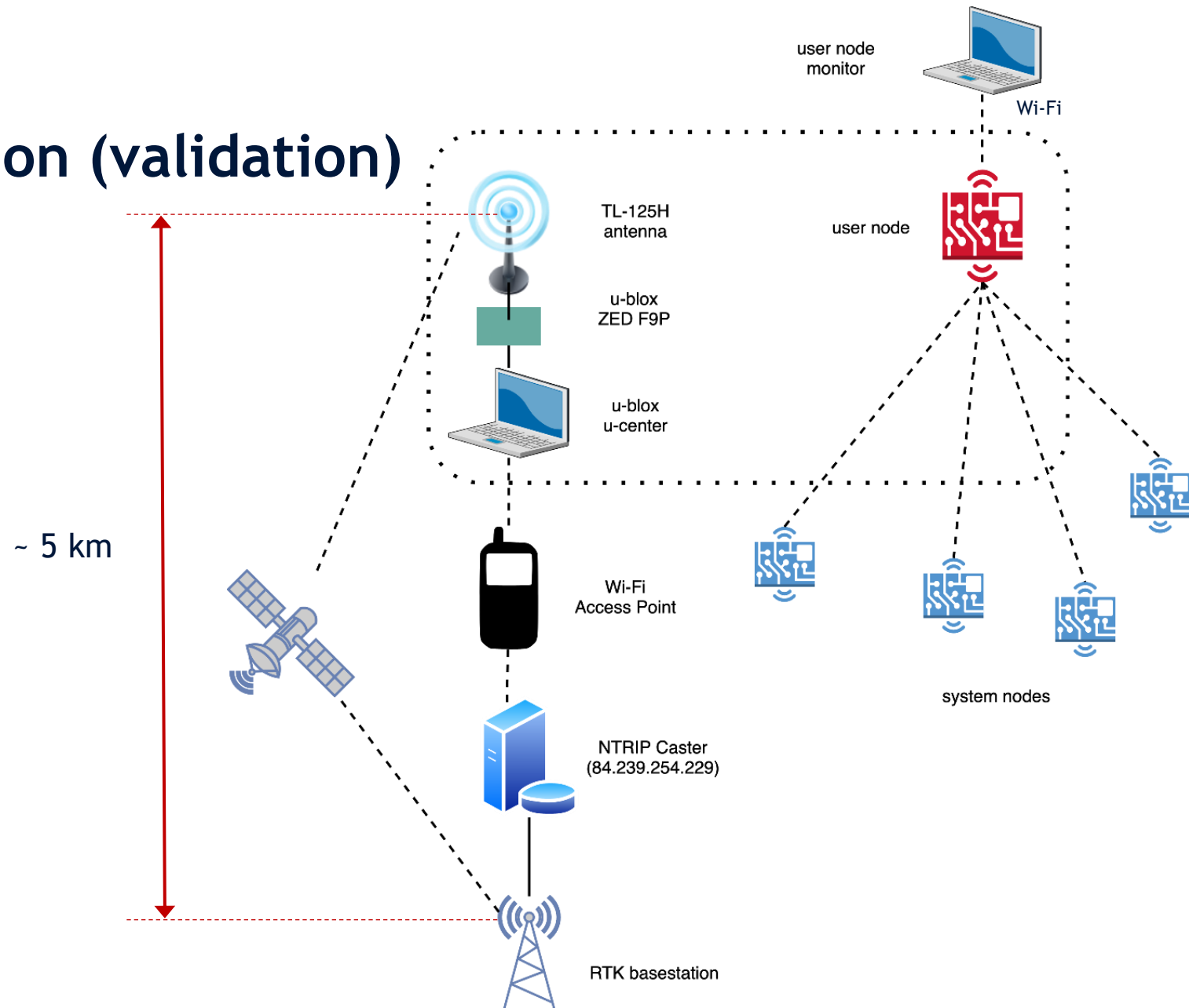


Verifiable multilateration (validation) - Silkkiniitty park

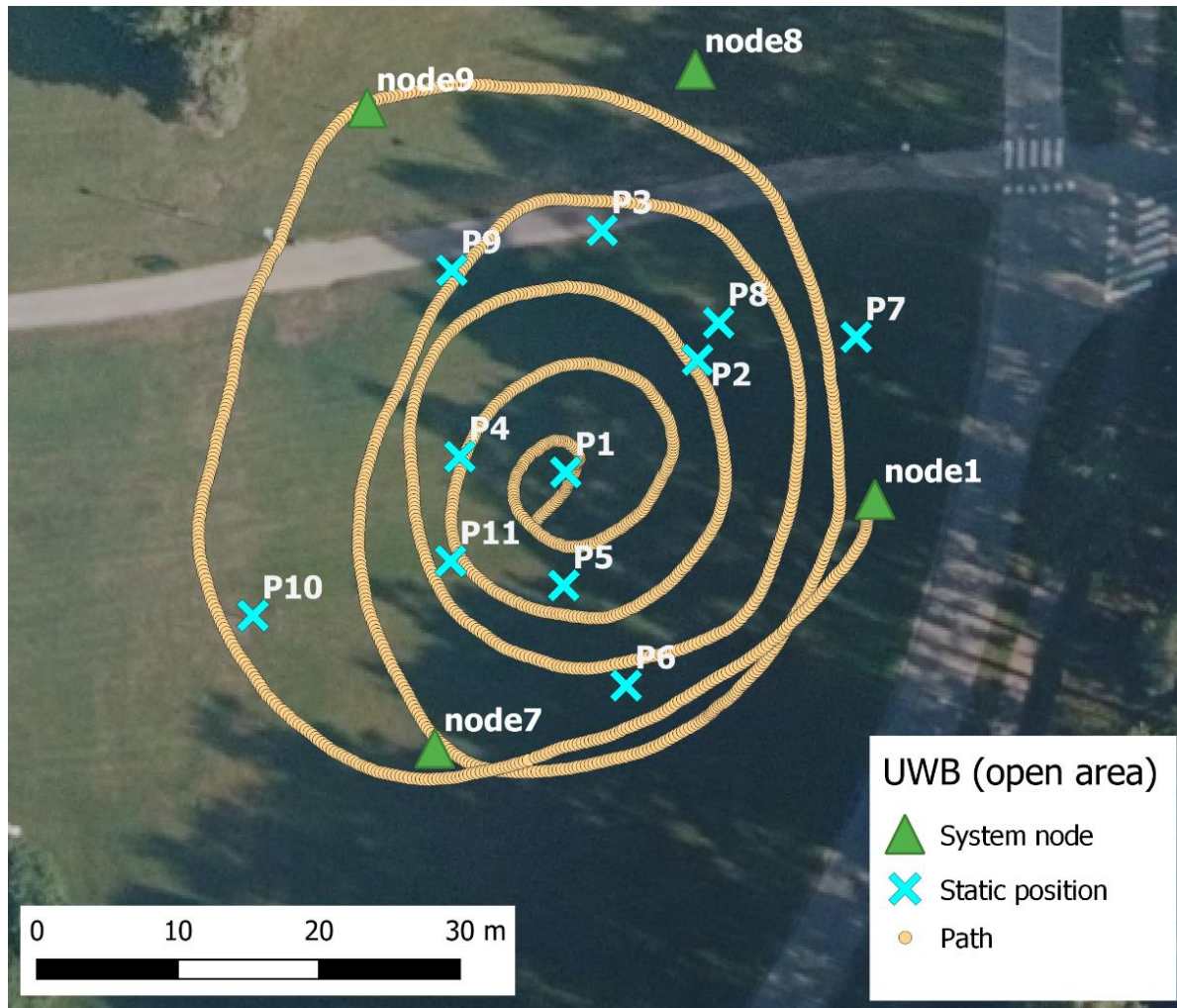


Verifiable multilateration (validation)

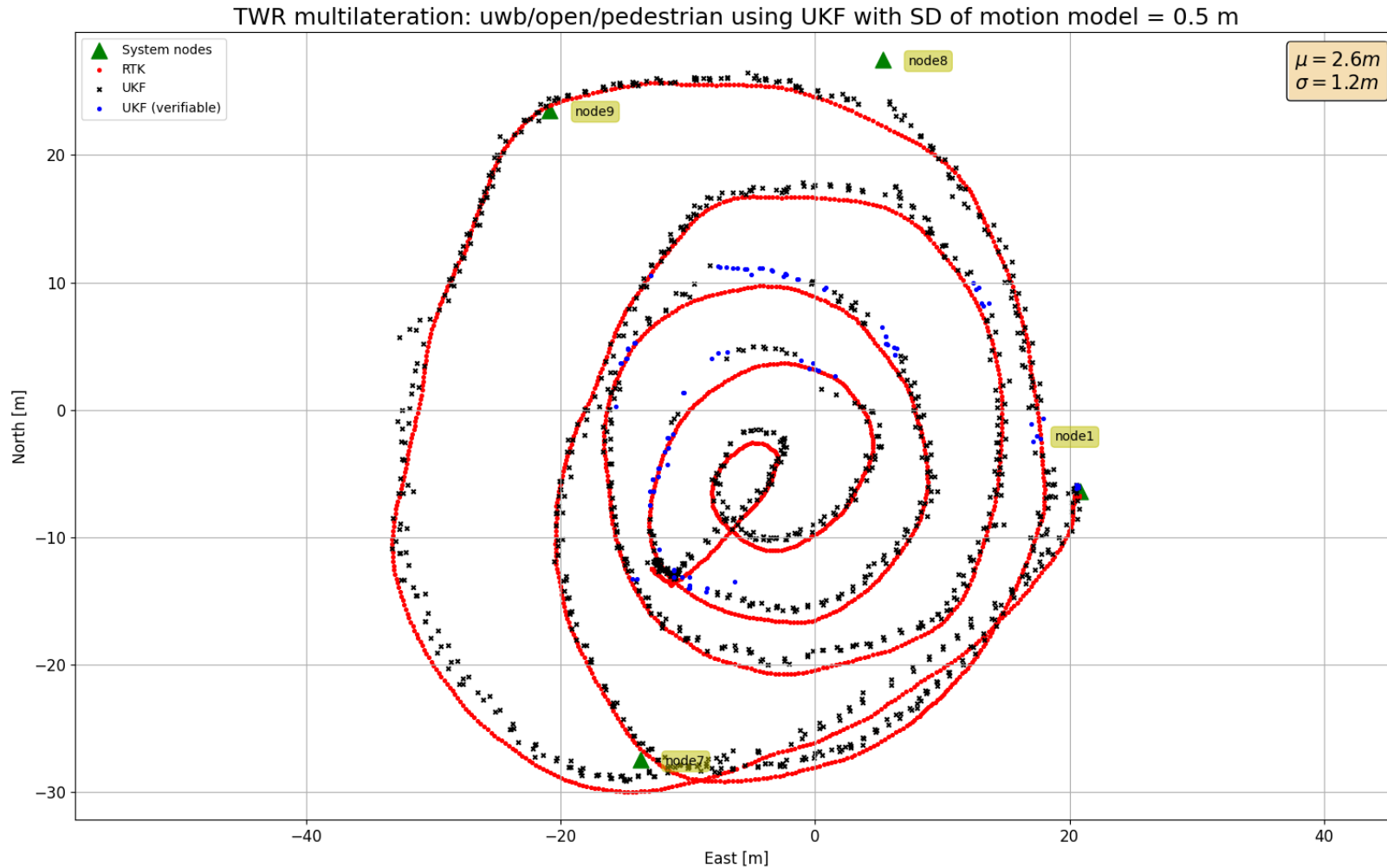
Measurement setup



Verifiable multilateration (validation) - UWB open area scenario

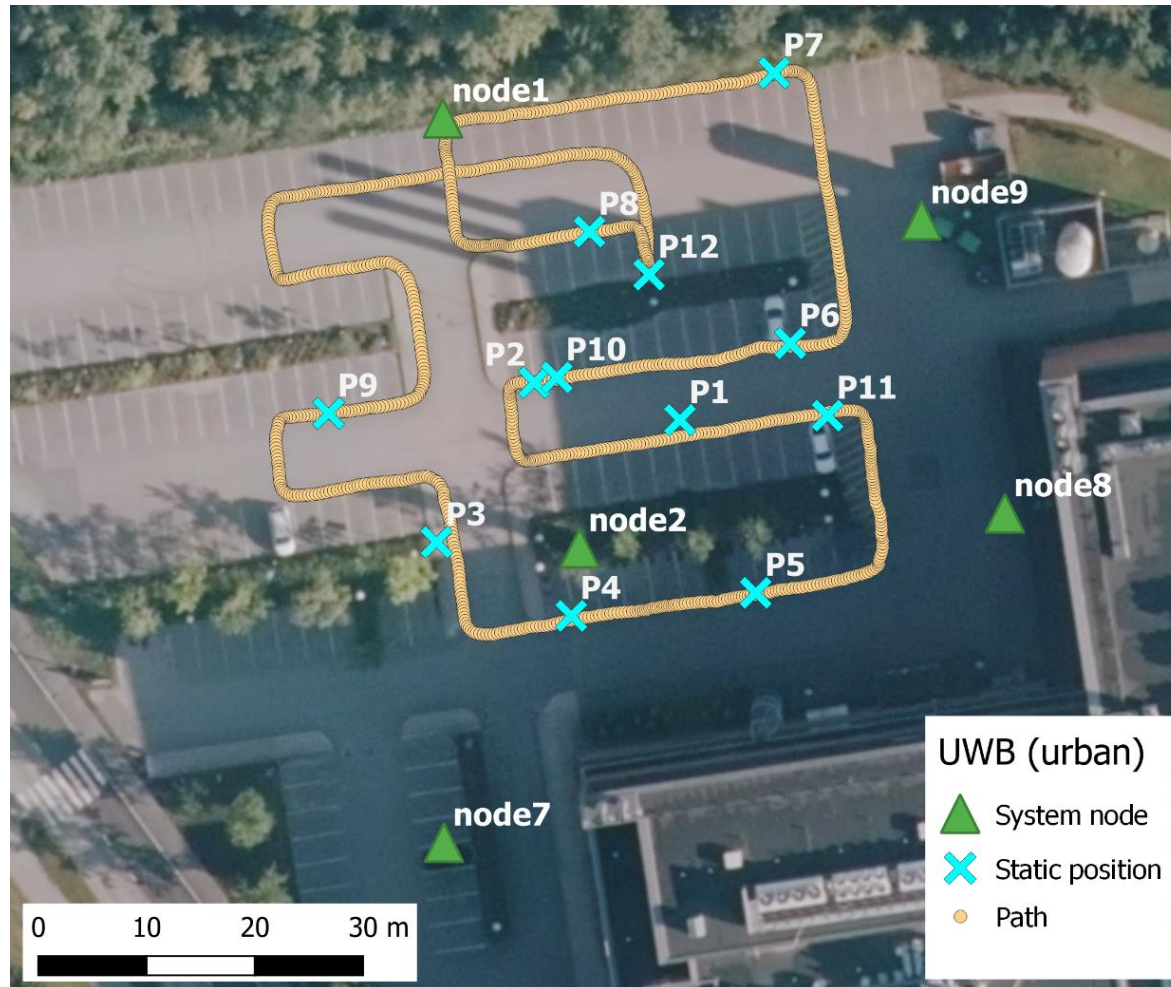


Verifiable multilateration (validation) - UWB open area pedestrian



RMSE (m)	2D	3D
Static	0.8	1.4
Pedestrian	1.7	3.0

Verifiable multilateration (validation) - UWB urban scenario

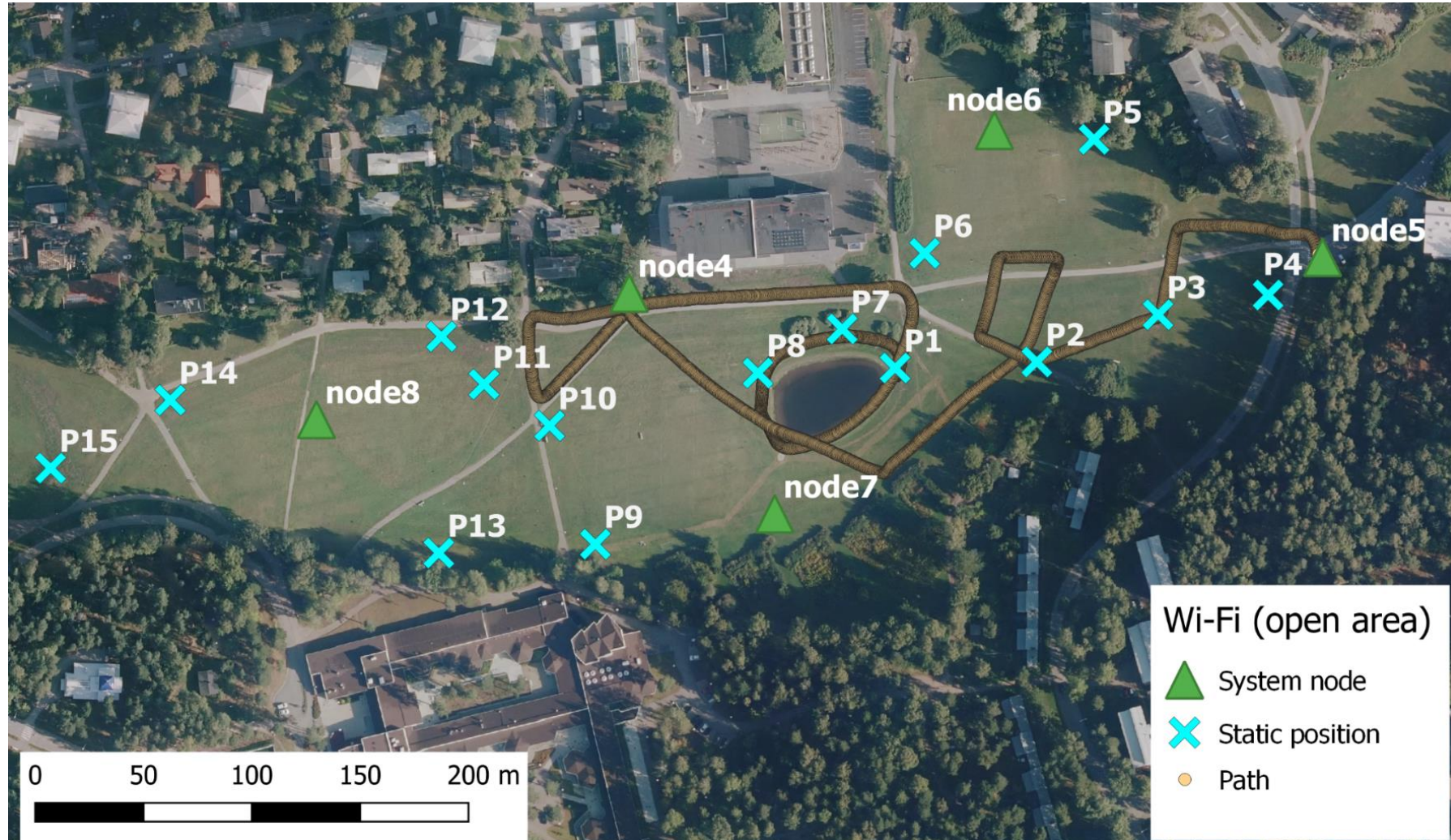


Verifiable multilateration (validation) - UWB urban pedestrian



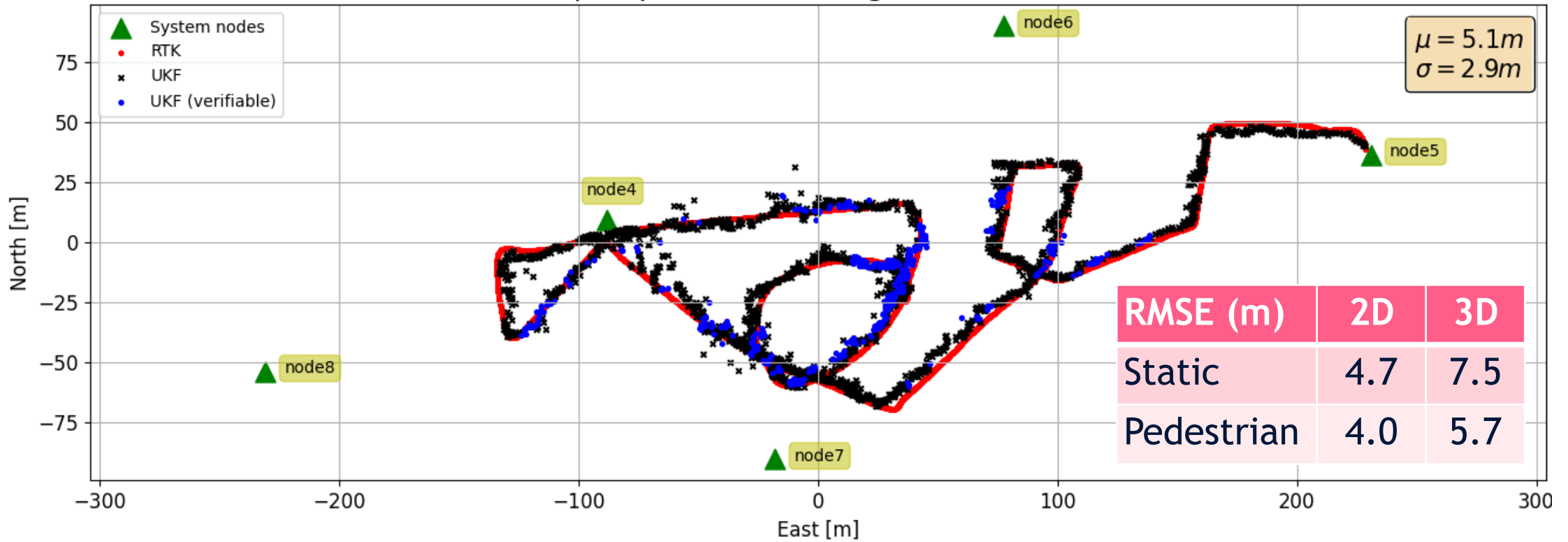
RMSE (m)	2D	3D
Static	0.6	2.0
Pedestrian	1.7	3.9

Verifiable multilateration (validation) - Wi-Fi open area scenario

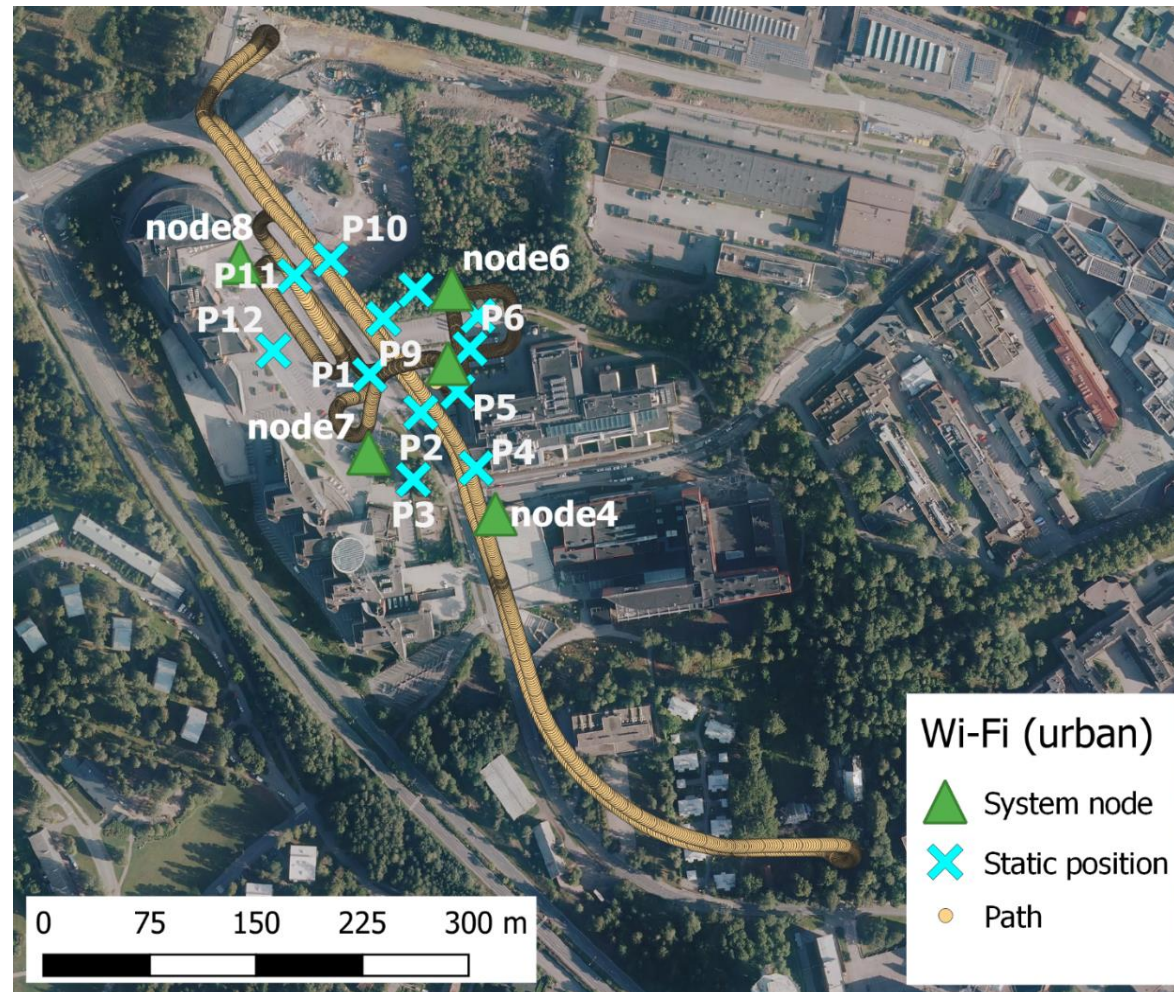


Verifiable multilateration (validation) - Wi-Fi open area pedestrian

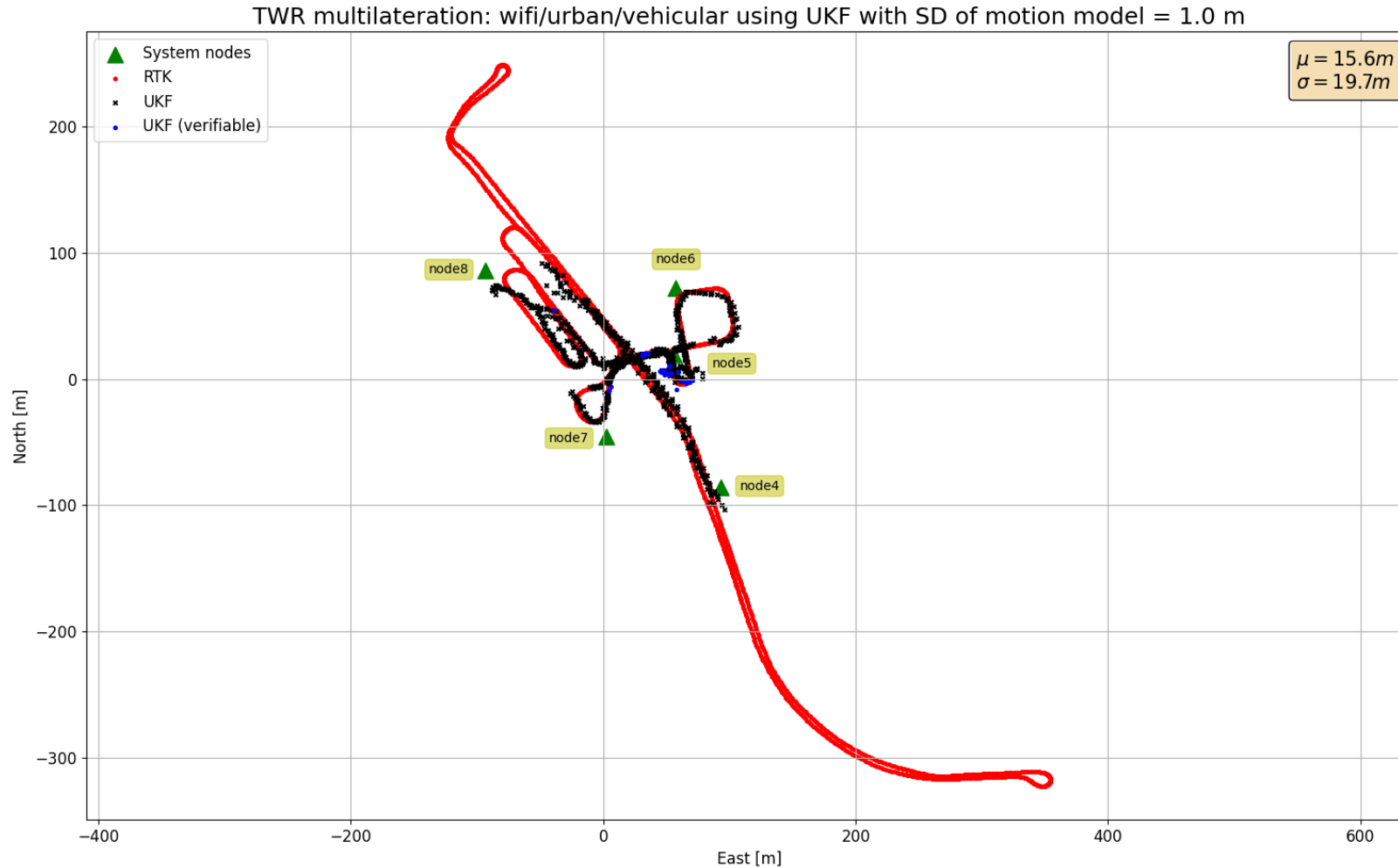
TWR multilateration: wifi/open/pedestrian using UKF with SD of motion model = 1.0 m



Verifiable multilateration (validation) - Wi-Fi urban scenario



Verifiable multilateration (validation) - Wi-Fi urban vehicular



RMSE (m)	2D	3D
Static	3.7	8.3
Vehicular	9.7	15.2

Feasibility study on SatCom verifiable multilateration

- Design of a SatCom system providing
 - positioning capabilities in the verifiable manner and
 - secure time transfer
- Land-mobile terminal can communicate with satellites
 - via a network of terrestrial base stations or
 - directly.
- Main focus on
 - Scalability and service availability
 - Physical and link layers
- Study is driven by outcomes from the previous tasks

Suggestions for Future Work

- Timestamping capability needed in HW as well as support in SW and drivers
 - Vendors need to implement and provide necessary HW APIs for timestamping and security features
- Authentication and security features need to be addressed in respective standardisation bodies for (wireless) communication and protocols
 - e.g. IEEE, Wi-Fi Alliance
- External aiding of additional trustworthy information to GNSS receivers need to be addressed by the manufacturers
 - Especially with respect to the technical details on internal usage of this information

hld

Conclusion

The project objectives have been achieved and some performance related requirements even exceeded. The prototyping work done within the project has paved the way for further development phases. Some parts will be probably optimized or redesigned, but the overall ideas and principles will remain for the future development.

huld

Beyond tomorrow