

SSF | Space Systems Finland Ltd
VTT | Technical Research Centre of Finland Ltd

Trusted Radionavigation via Two-Way Ranging

Ondřej Daniel (ondrej.daniel@ssf.fi)

Sami Ruponen (sami.ruponen@vtt.fi)

22.01.2020 | NAVISP INDUSTRY DAYS



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**

Minimal performance requirements for the prototype

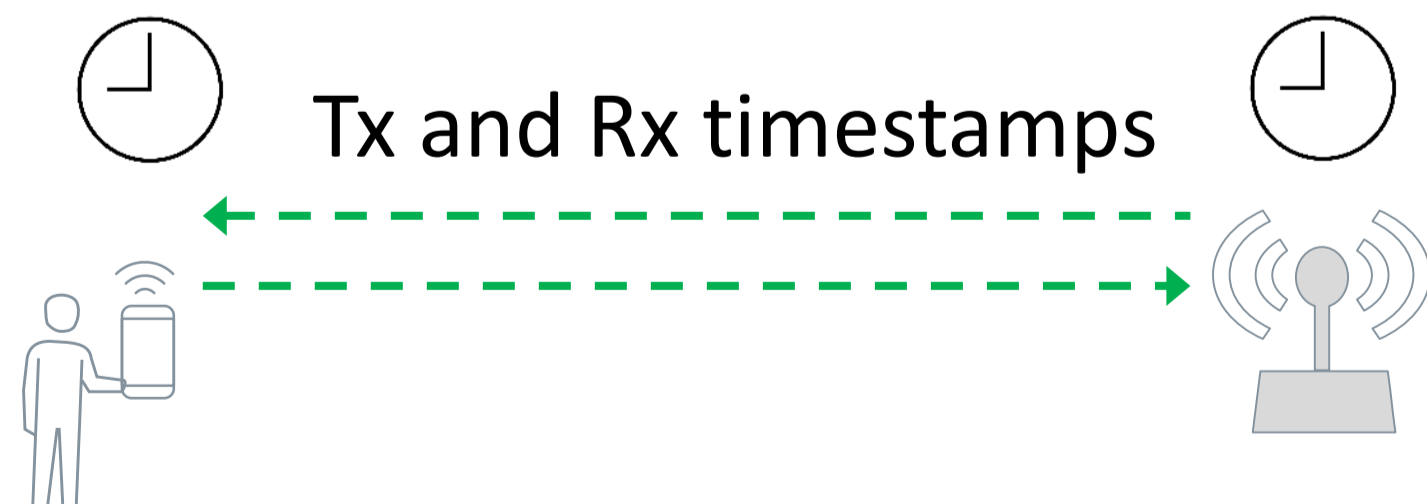
- **Time-transfer: 5 ms**
- **Authenticated ranging: 3 km**
- **Verifiable multilateration: 5 km**

Basic functions

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

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

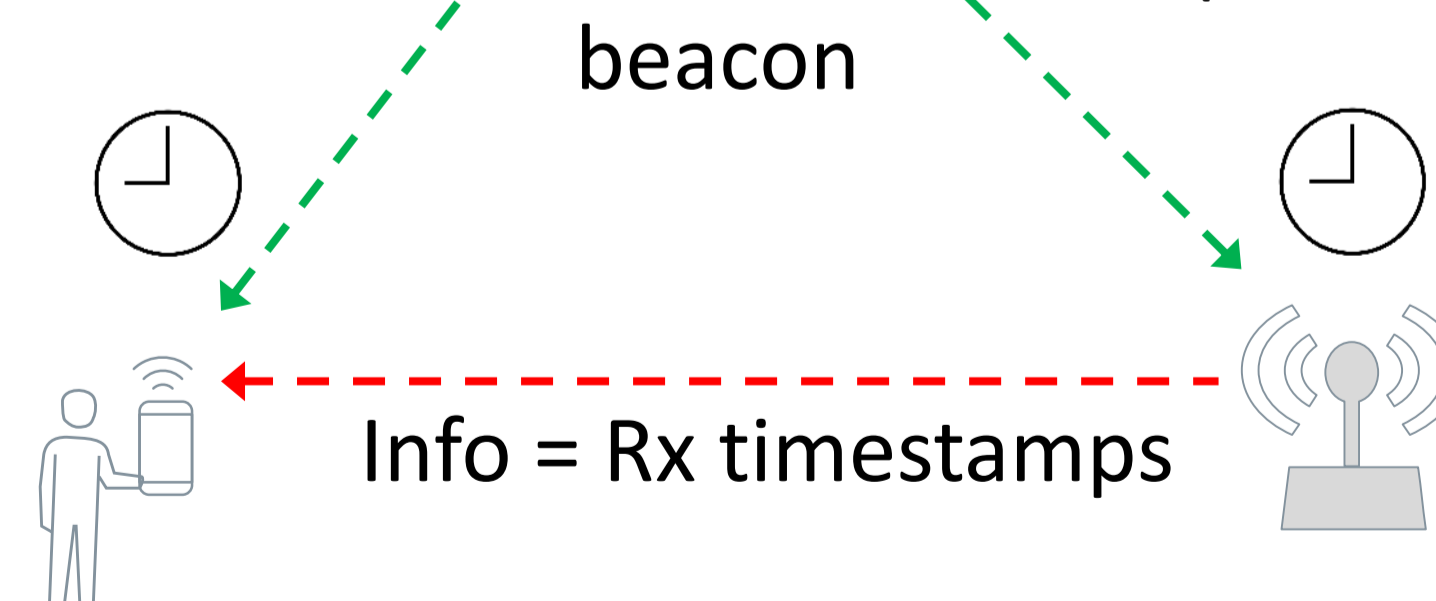
user node (slave/tag) system node (master/anchor)



PTP, FTM, and TWR operation principle

system node (AP) beacon

user node (slave) system node (master)



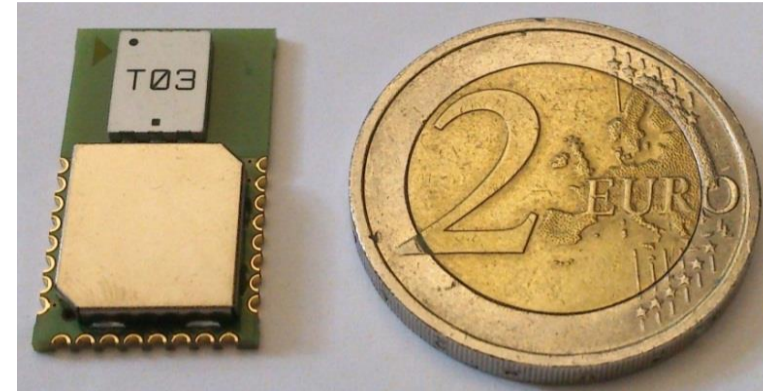
RBIS operation principle



Hardware platforms

- **UWB node platform**

- Raspberry Pi 3 model B+
- Decawave DWM1000 UWB module (DW1000 IC)

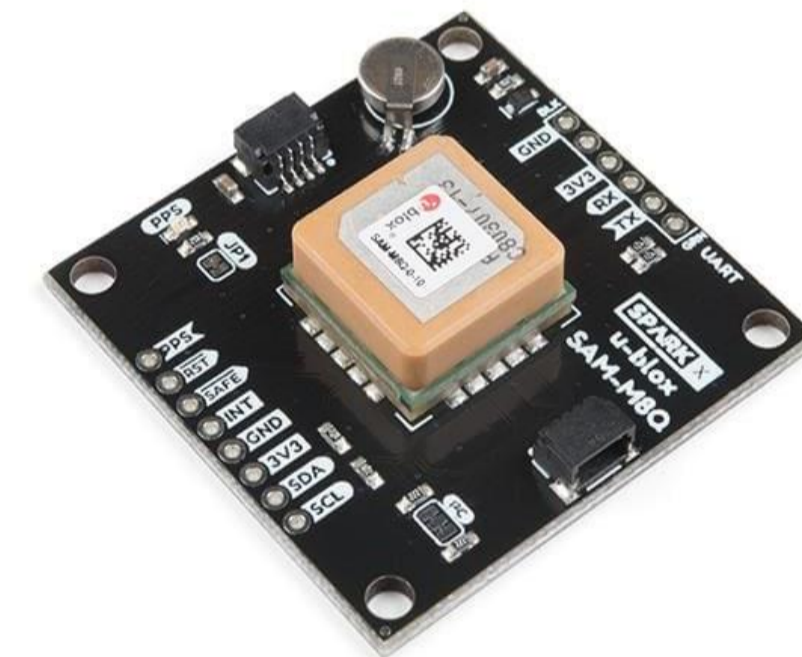
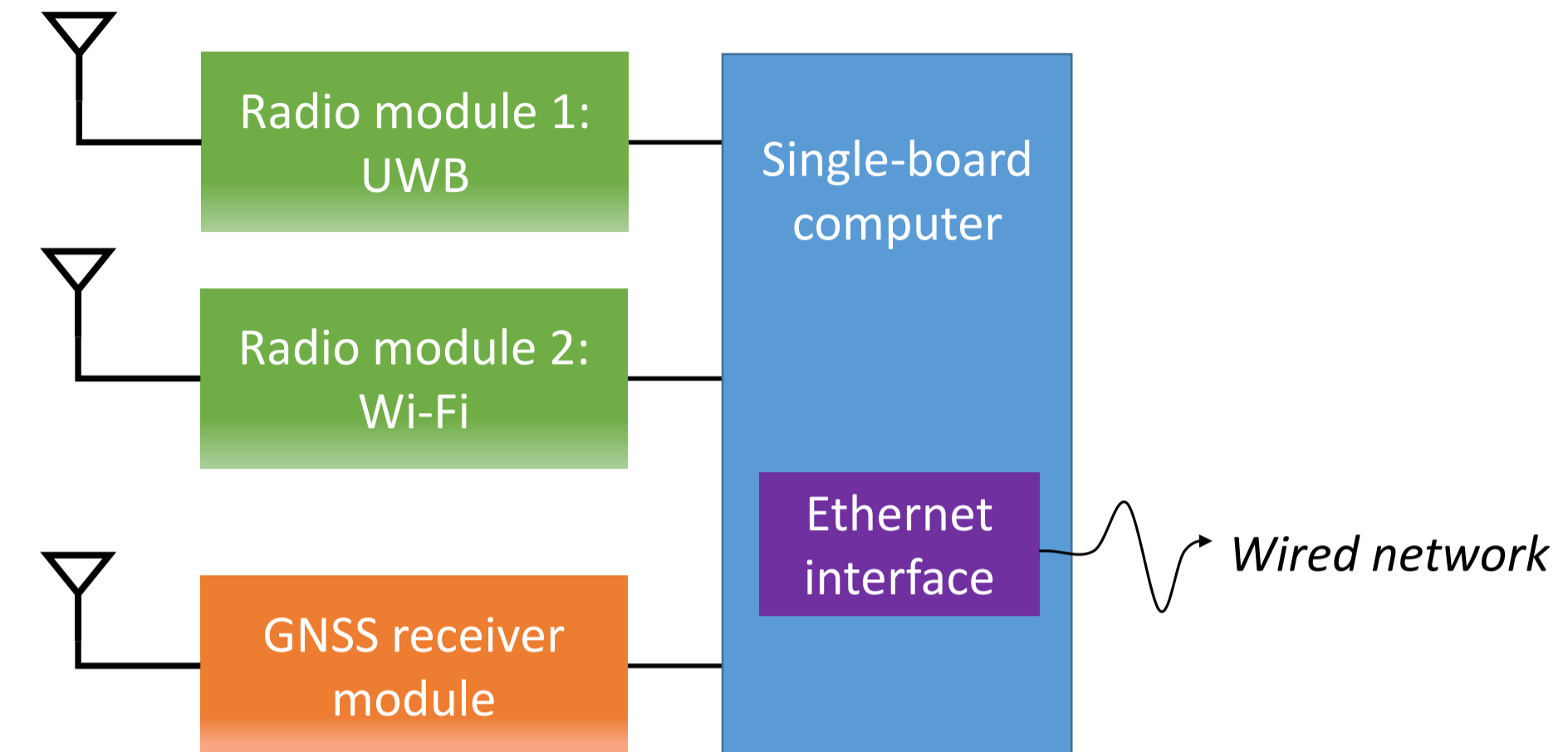


- **Wi-Fi node platform**

- 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 Receiver**

- Sparkfun SPX-15106 with u-blox SAM-M8Q GNSS module

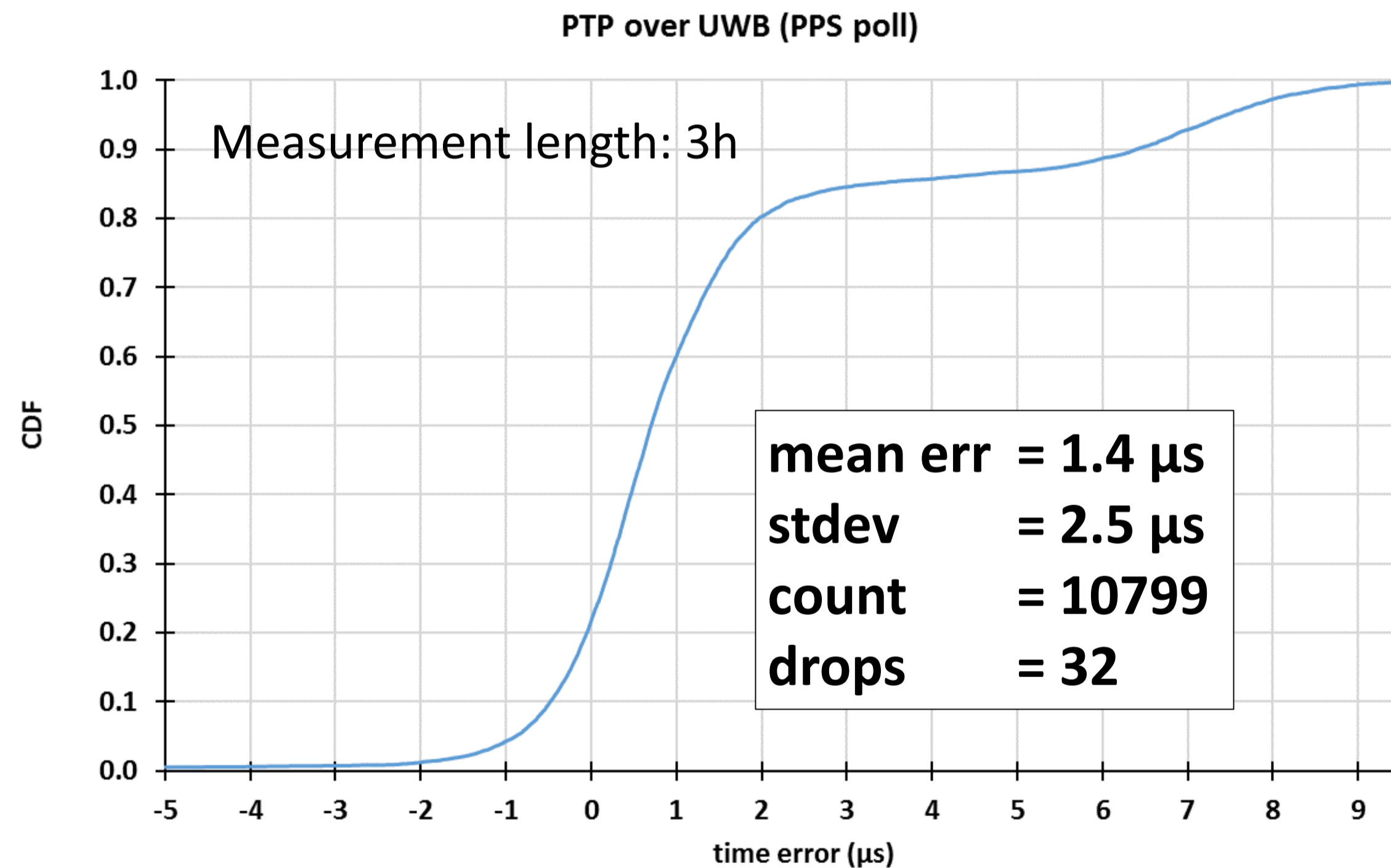


Security features

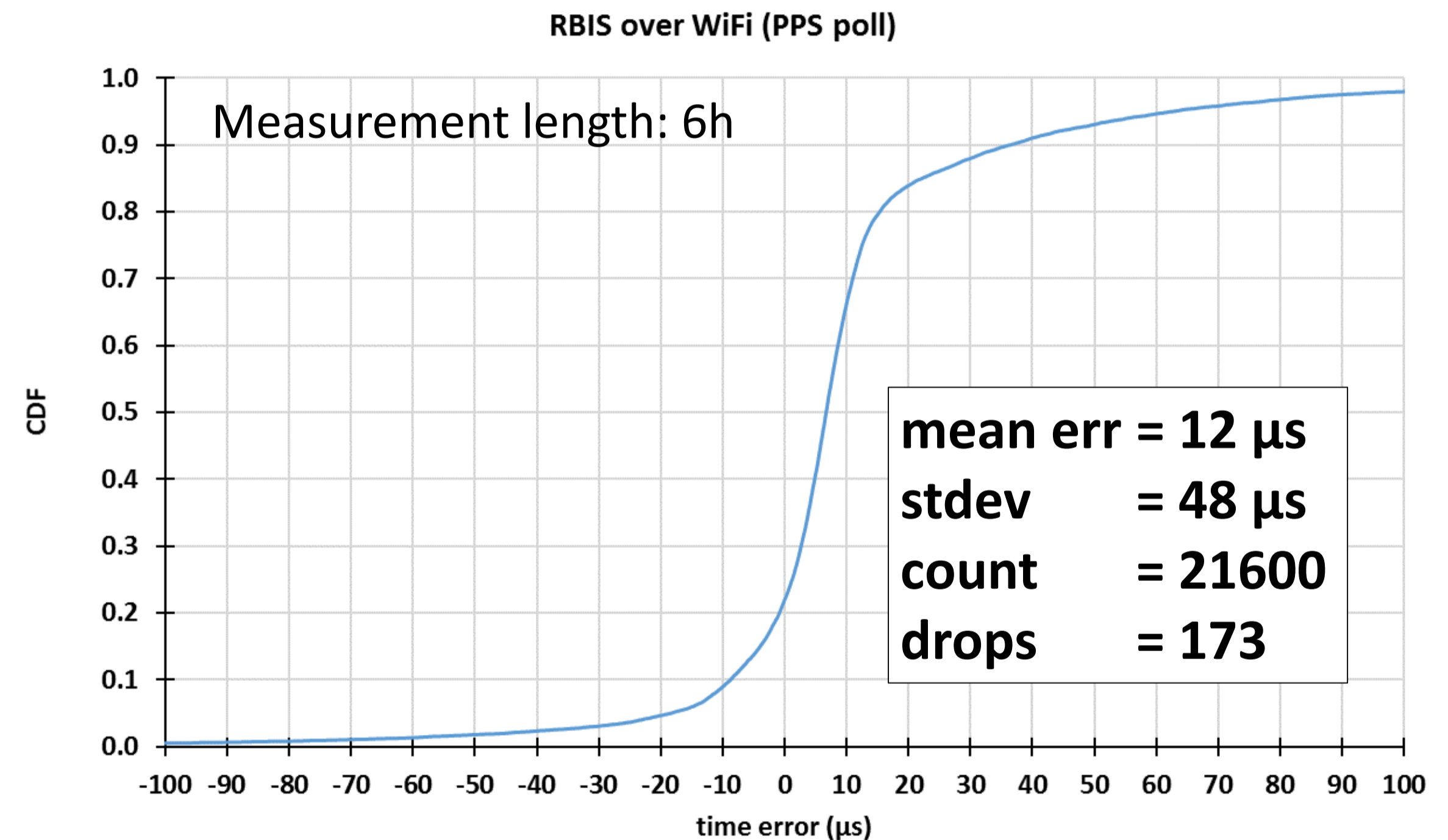
- The system and user nodes are assumed trustworthy
- Man-in-the-middle attacks are prevented by using cryptography
- Still, the system is vulnerable to message delaying, denial of service, and spying
- **PTP**
 - Added PTP message authentication to LinuxPTP – comparable to Annex K in IEEE 1588-2008 standard
 - All nodes share a set of ephemeral session keys, no key distribution protocol
- **RBIS**
 - Relies on standard Wi-Fi security (RSN)
- **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



Validation results – time transfer



PTP over UWB



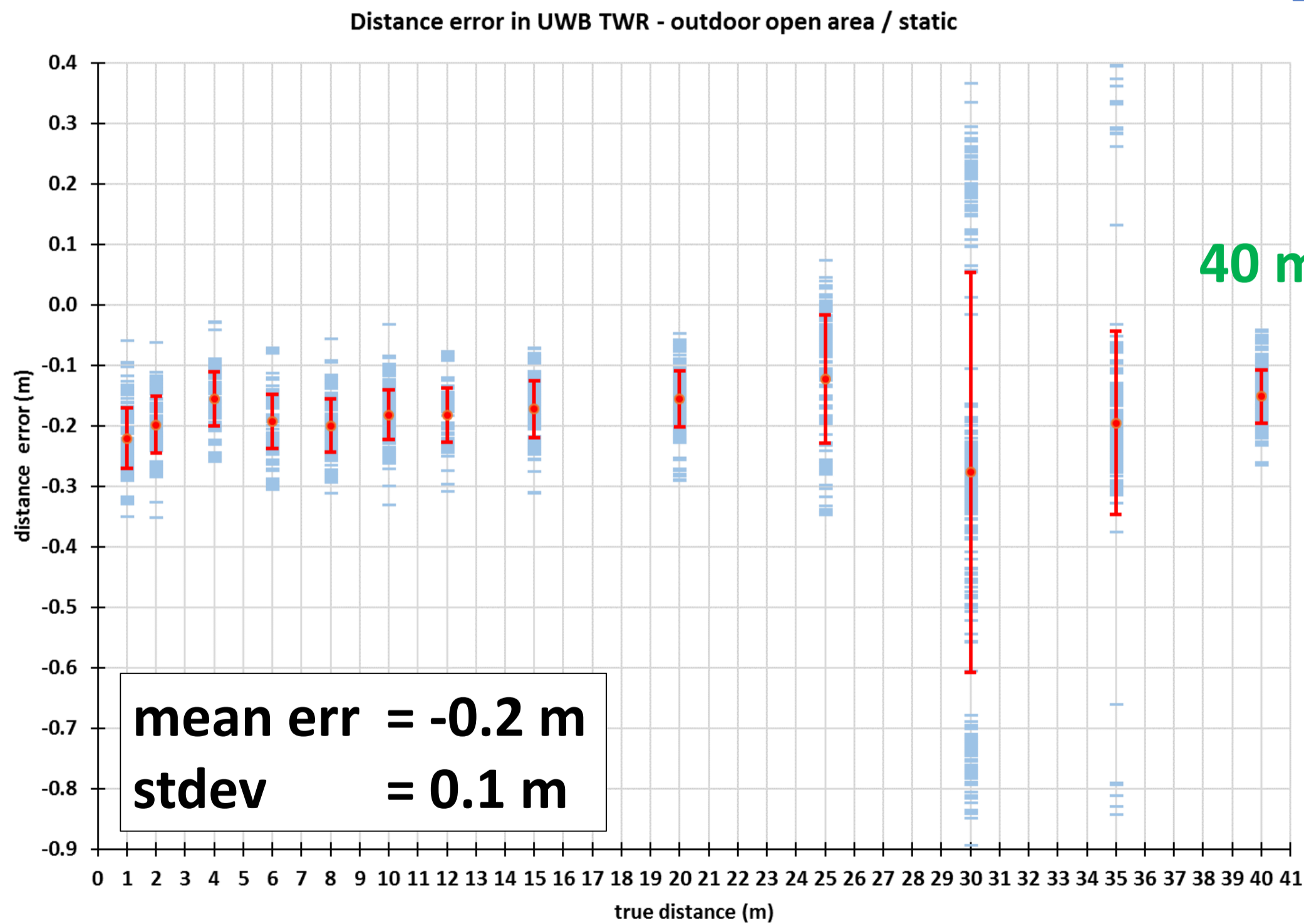
RBIS over Wi-Fi



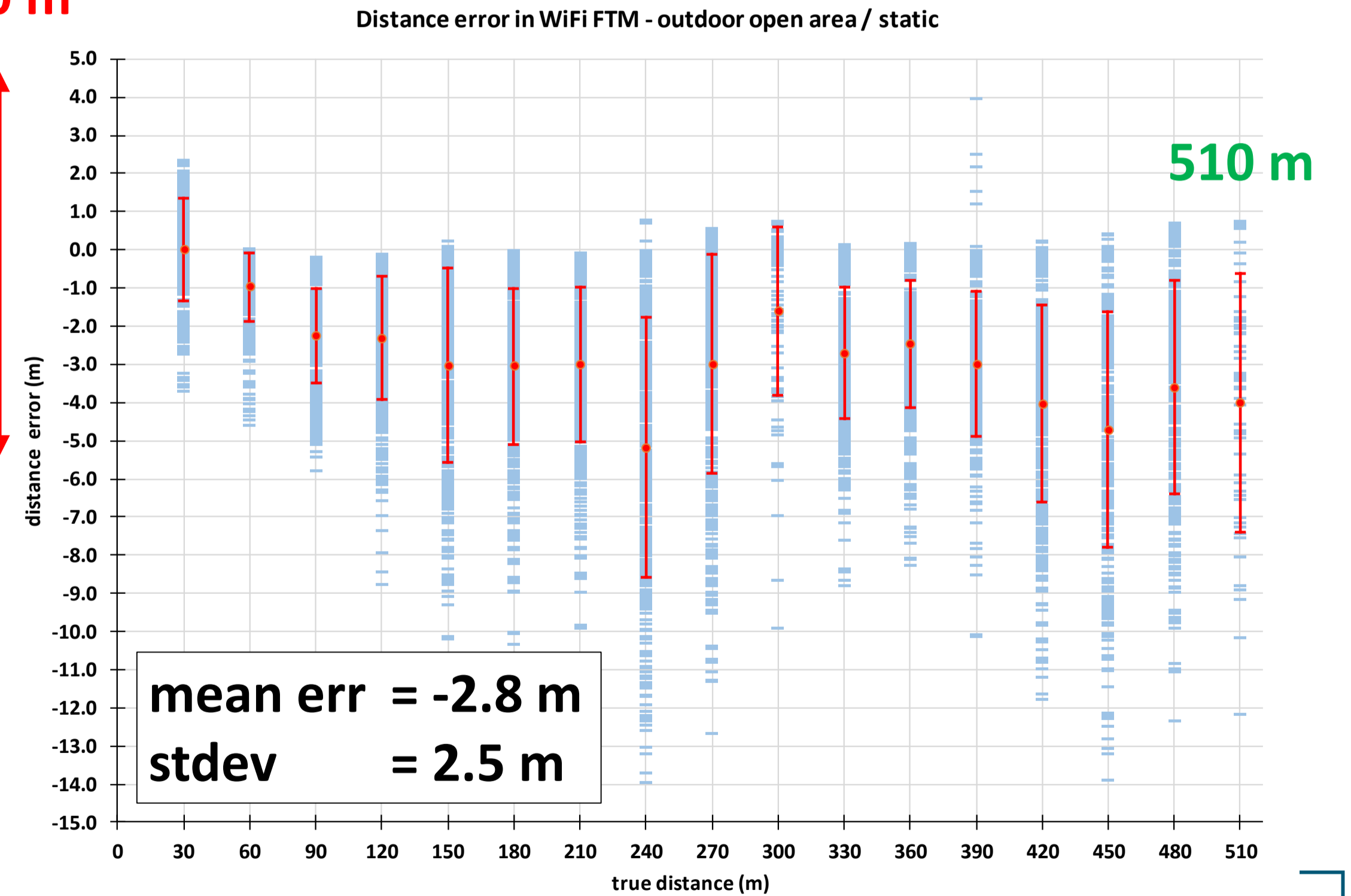
Validation results – ranging

		Environment	
		Short range (UWB)	Long range (WiFi)
Operating conditions	static	open area	
		urban	
	pedestrian	open area	
		urban	
vehicular		open area	
		urban	

1 m 10 m



TWR over UWB



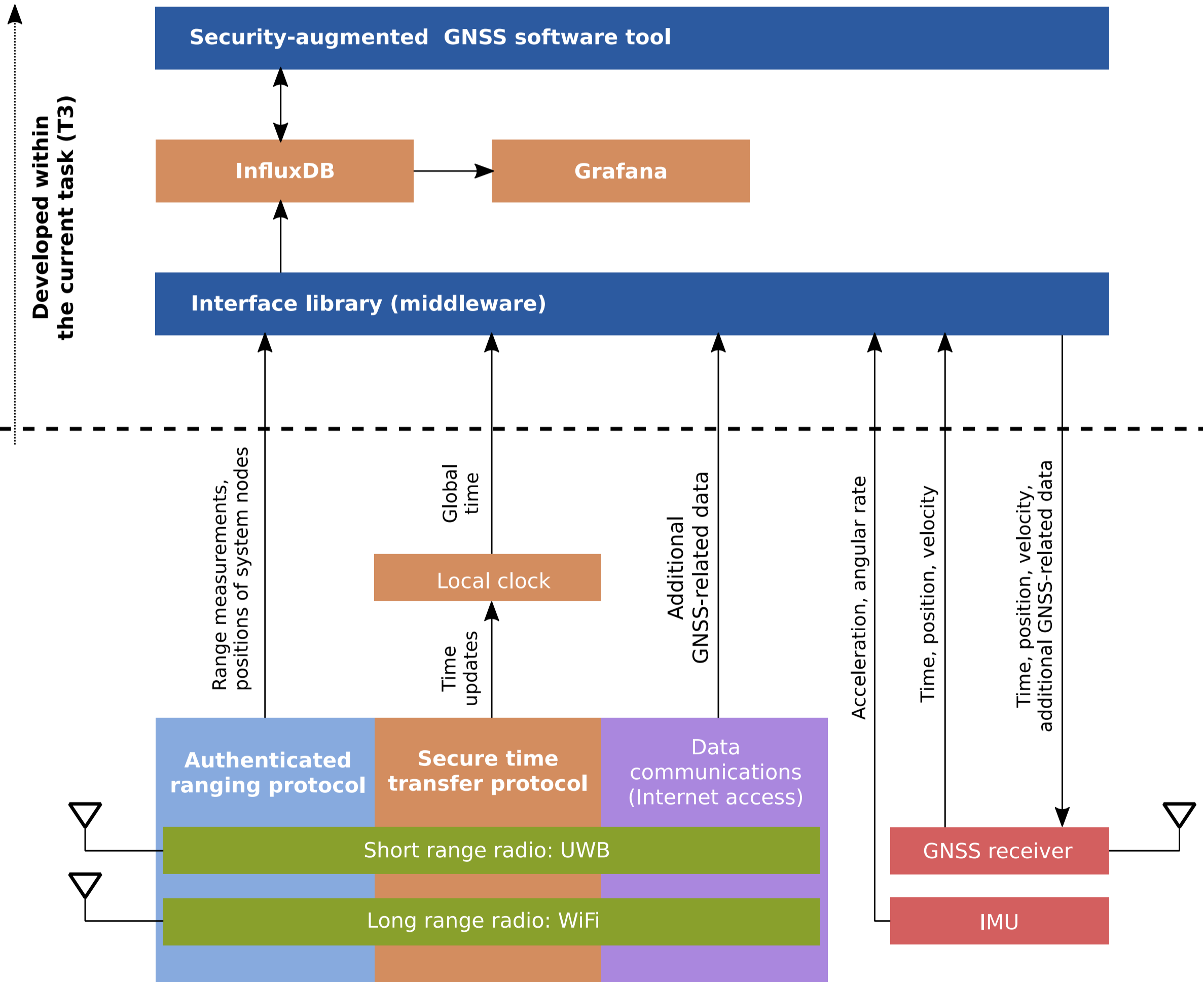
FTM over Wi-Fi



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)

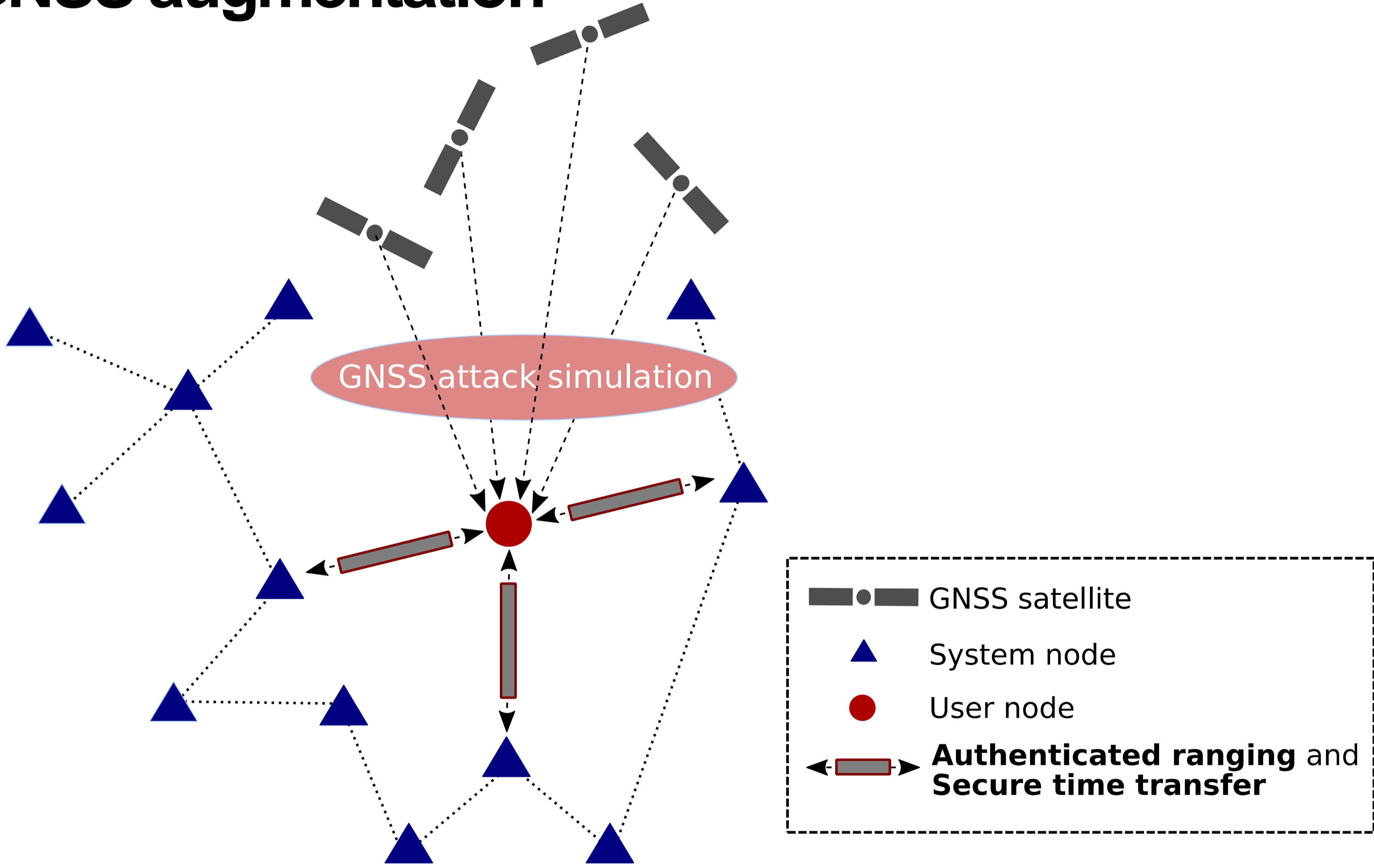
Security GNSS augmentation



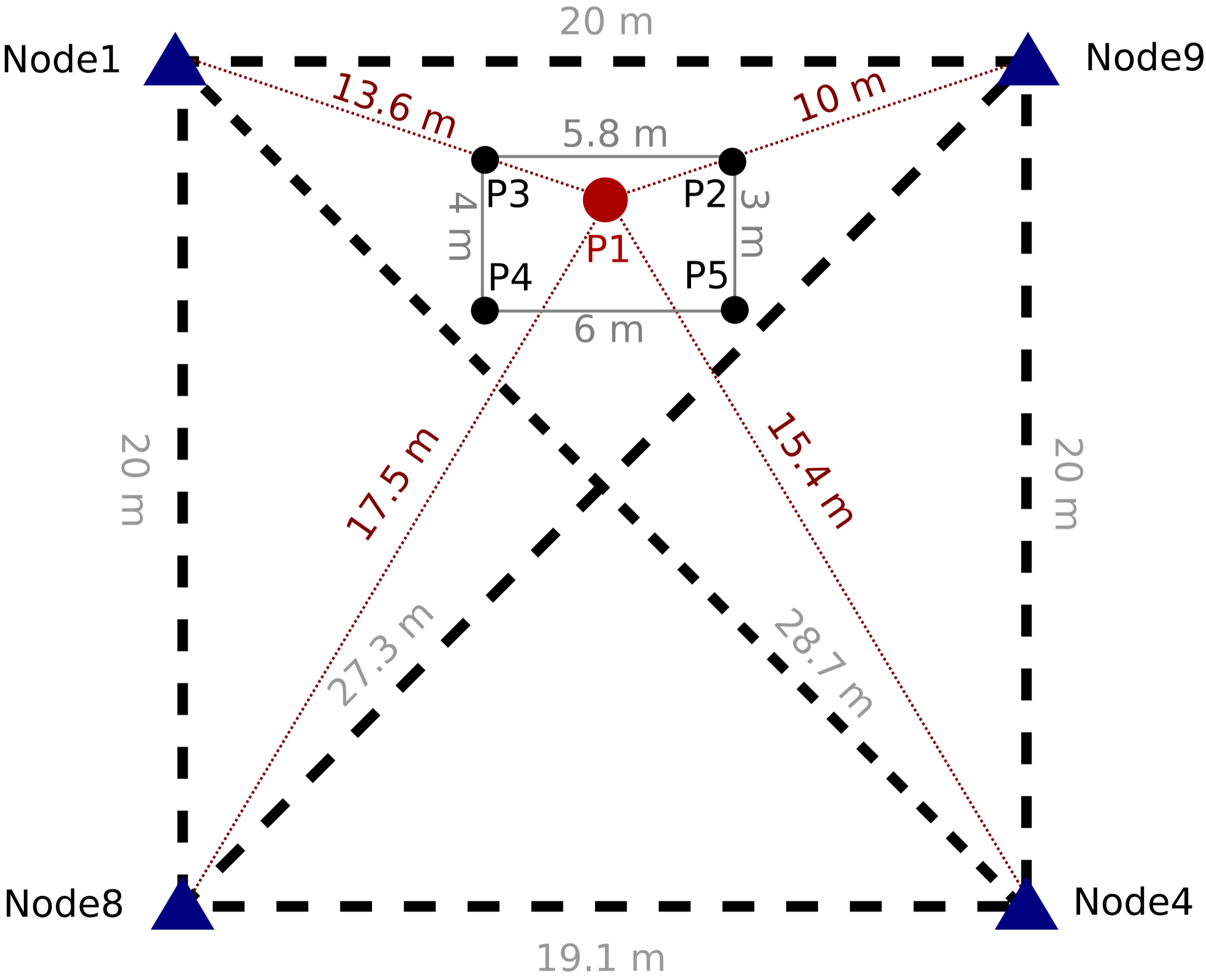
Security GNSS augmentation

- **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

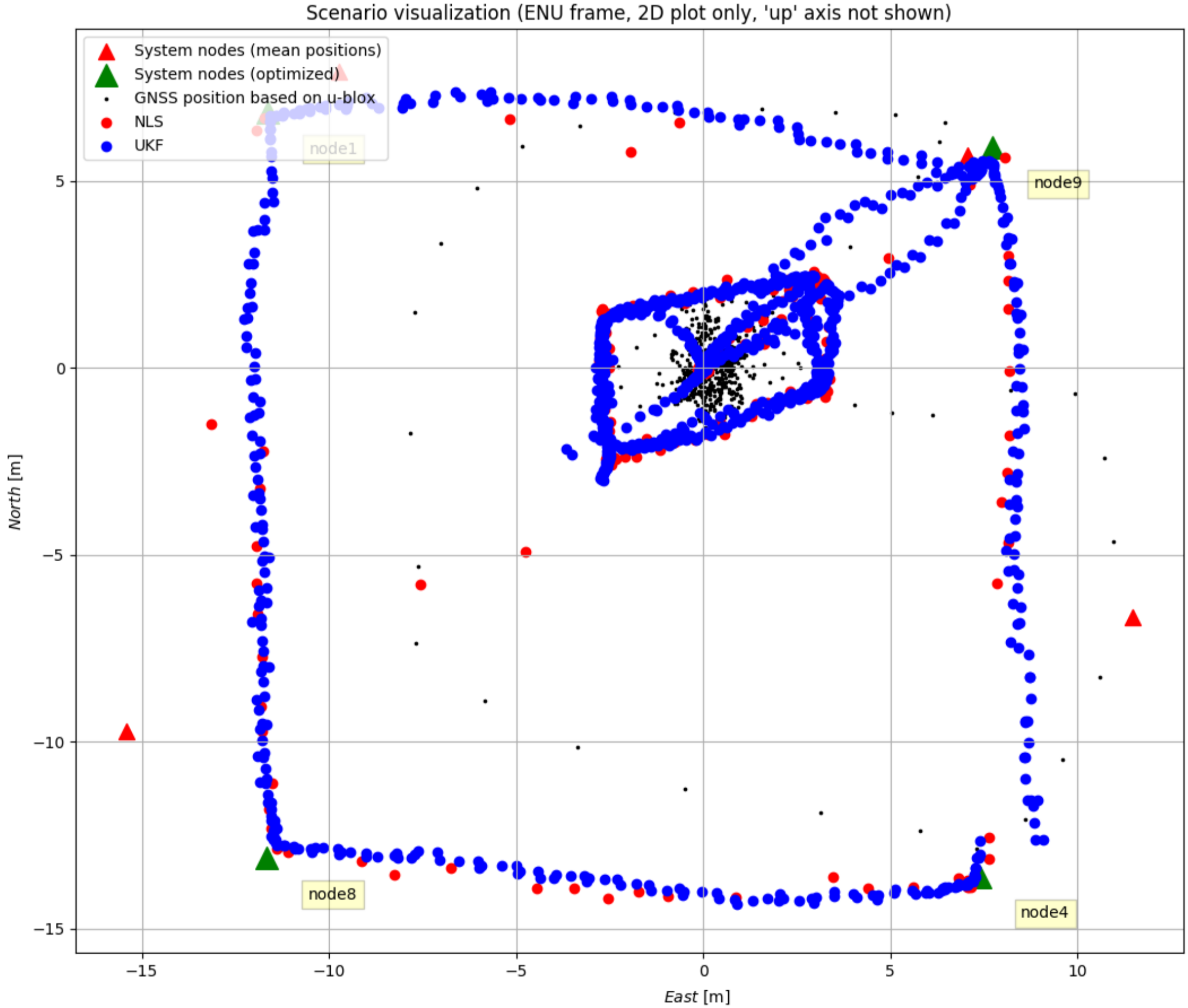
Security GNSS augmentation



Verifiable multilateration



Verifiable multilateration



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**

Conclusion

- **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
- **Upcoming activities:**
 - Analysis of data from measurement campaigns
 - Preparation of the feasibility study on SatCom verifiable multilateration