Thales Alenia Space
a Thales / Leonardo company

Project – 2 way communication

Final Presentation

09/11/2023

www.thalesaleniaspace.com

Schedule

Tuesday 09/11/2023	09:30 – 09:40 10’	Intro & agenda	**TASF**
	09:40 – 09:50 5’	Project Summary – Use Cases	**TASF**
	09:50 – 10:00 10’	Project Summary – Protocol & Algorithm design	**TASF**
	10:00 – 10:10 10’	Project Summary – Testbed experimentation & Security analysis	**Qascom**
	10:10 – 10:30 20’	WP4 output - Recommendations for a space-based two-way system	**TASF**
	10:30 – 10:40 10’	WP4 output - Adaptation of two-way ranging to commercial technologies	**TASF**
	10:40 – 10:50 10’	Conclusion & Way Forward	**TASF**
	10:50 – 11:30 30’	**Discussion**	

Project Summary - Reminder

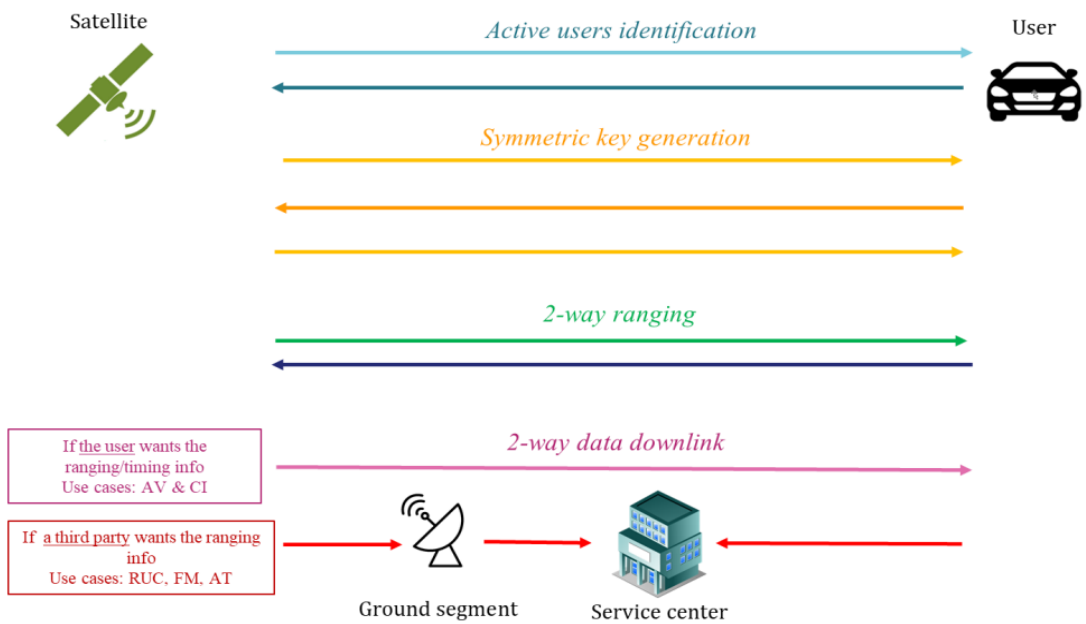
www.thalesaleniaspace.com

Use Case analysis

	Autonomous vehicle	Asset tracking	RUC	Fishing monitoring	Critical infrastructure
Nb of users (2024) Nb of users (2029)	225 k 10 M	10 k (active) 10 k (active)	10 M 10 M	25 k 50 k	25 k 25 k
Density	Specific, see [RD1]	Uniform	Specific, see [RD1]	Specific, see [RD1]	Follow pop. density
Value between two PVT verifications	10 s N/A	1 min	2 min	30 min	5 s
Mode of operation	Waypointing Bootstrapping	Waypointing	Waypointing	Waypointing	Waypointing
Pmd	10^{-7}/h	10^{-4}/h	10^{-3}/h	10^{-3}/h	10^{-5}/h
Pfa	10^{-5}/h	10^{-3}/h	10^{-5}/h	10^{-5}/h	10^{-3}/h
TTA	6 s	15mn	15 min	15 min	6 s
Ranging/Timing accuracy	10 m	25 m	100 m	100 m	240 ns (5G)
Reference environment	Light urban	Light urban	Light urban	Open sky	Light urban
Additional sensors	IMU, cameras, lidars, radars, LTE/5G positioning	RFID tags	(LTE/5G positioning)	-	(Internal clock)

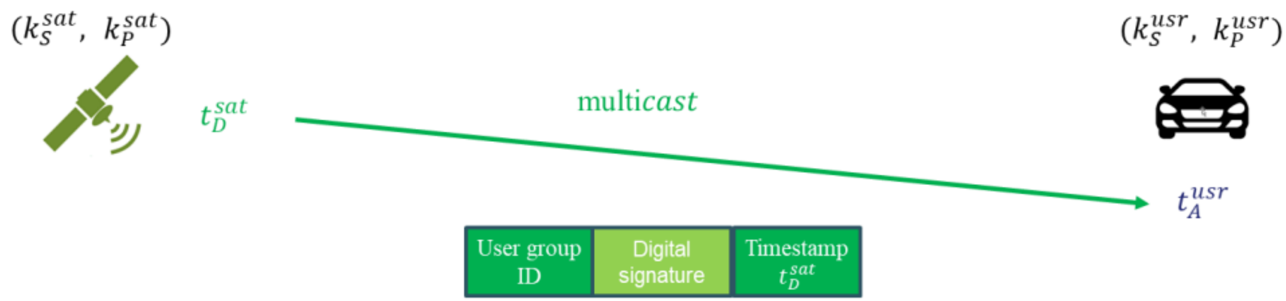
Protocol design

- Literature of Distance-Bounding protocols : robustness to Distance-Decrease attacks
  - RTT measurement robust to Distance-Decrease
  - Multi-RTT position robust to Distance-Decrease
- Tradeoff : satellite-initiated VS user-initiated
  - Satellite-initiated selected
  - Adoption of Downlink Multicast
- Protocol steps :

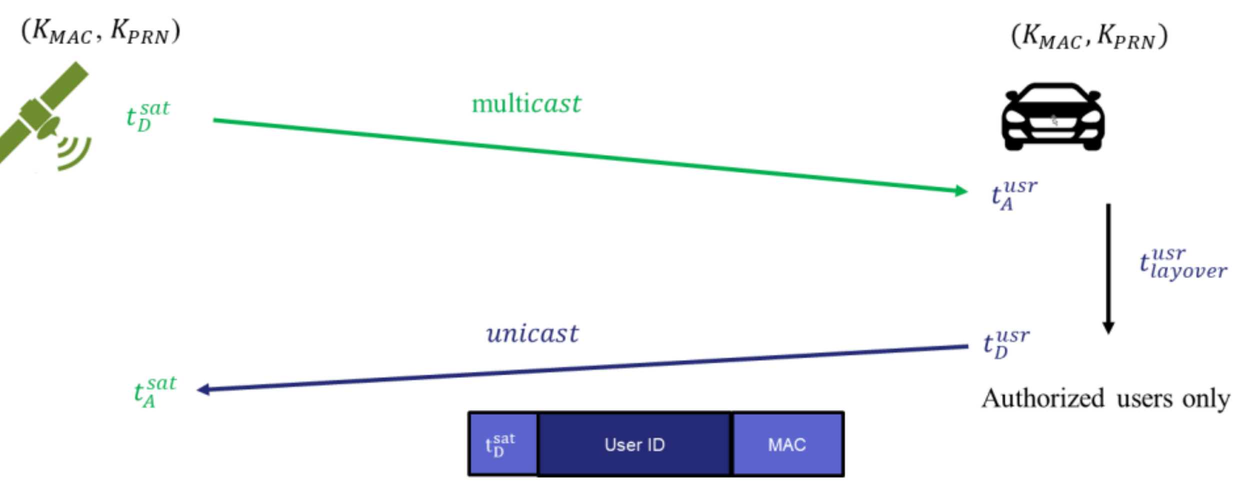


Protocol design – Two-Way Exchange

- Downlink request



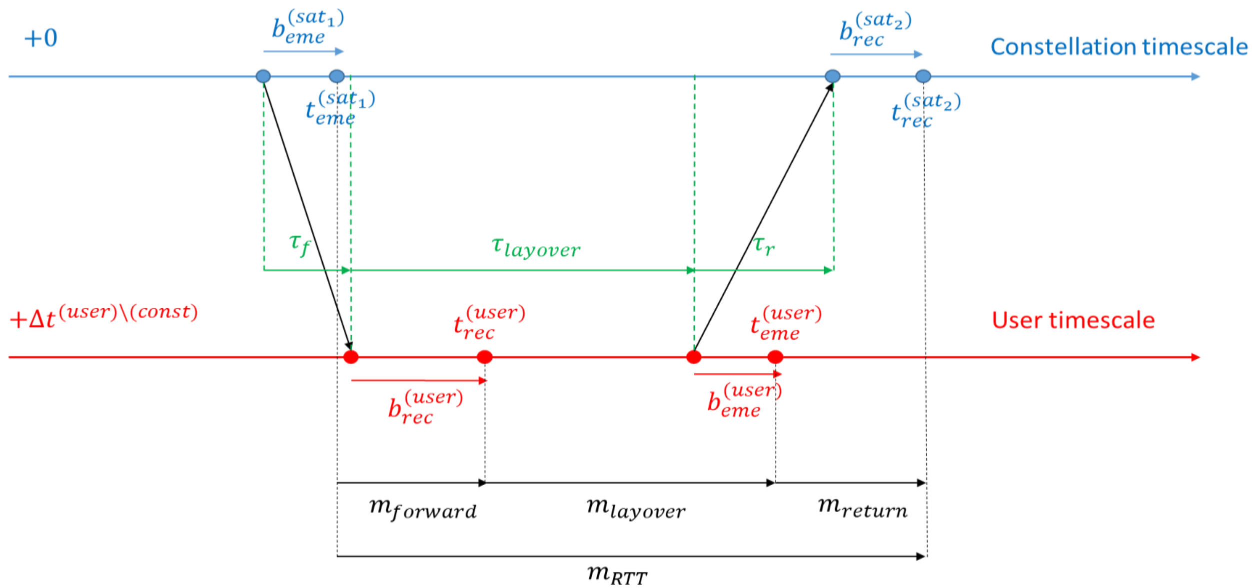
- Uplink response



- Signal : 1Mcps, BPSK, Encrypted Spreading code

Measurements output of protocol

- Overview of two-way protocol measurements

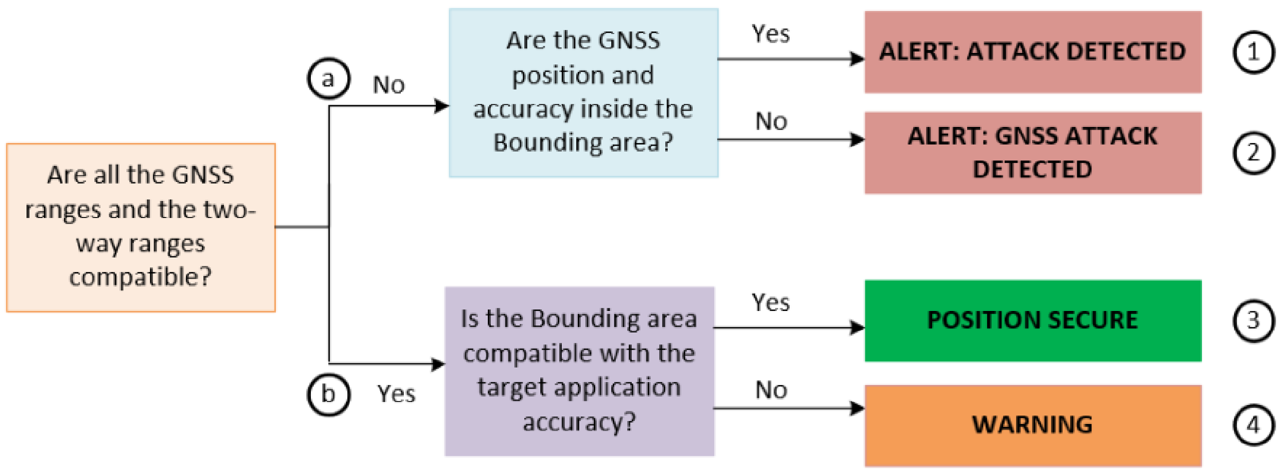


- 2 measurements :
  - RTT : $m_{RTT} = t_{rec}^{sat} - t_{eme}^{sat}$
  - Synchro : $m_{sync} = \frac{1}{2}(t_{rec}^{user} - t_{eme}^{sat} + t_{eme}^{user} - t_{eme}^{sat}) - \delta\tau_{forward\backslash return}$

ThalesAlenia Space
a Thales / Leonardo company

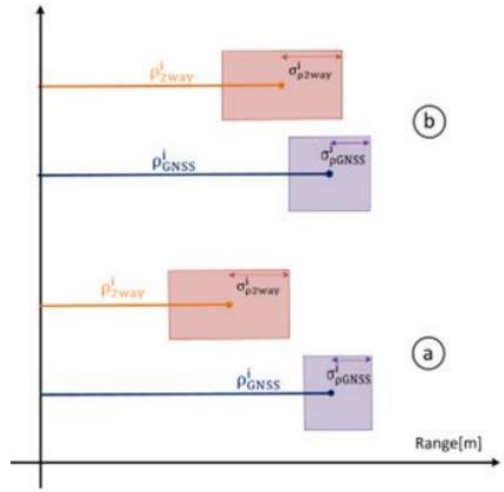
Position verification algorithm design

- Multi-RTT Snapshot Algorithm based on DB protocol
- Single primary satellite → Common focus of ellipsoids
- Two-Step Approach

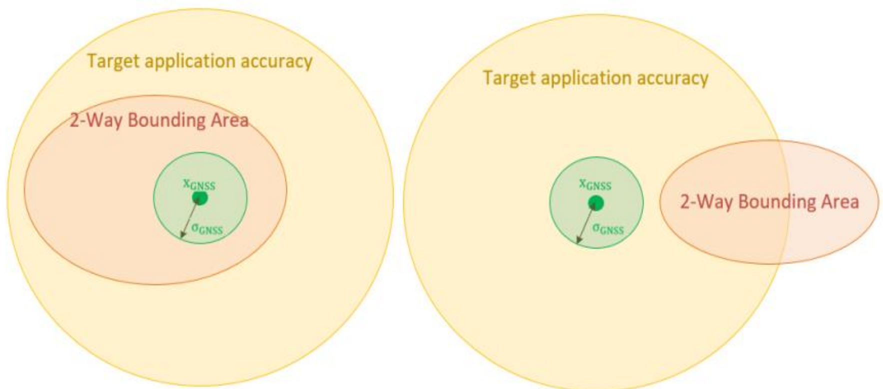


Position verification algorithm design

- Step 1 : position verification – Measurements consistency at reported position



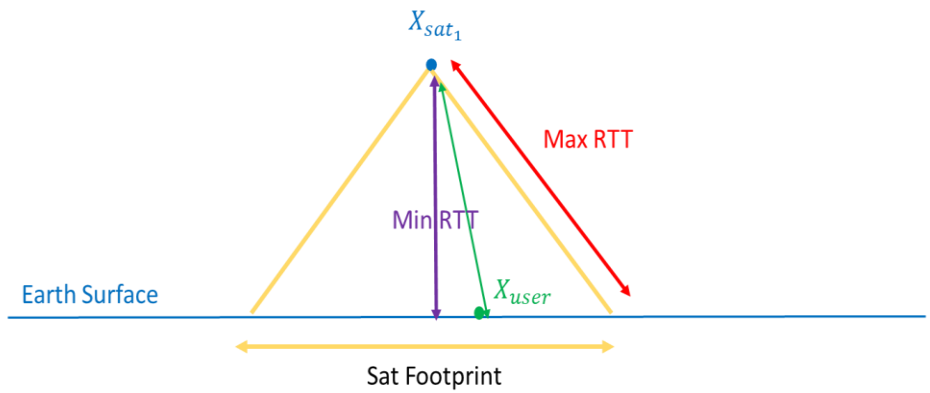
- Step 2 : position computation – Computation of independent bound based on Distance-Bounded RTT



ESS

Synchronization Algorithm design

- Computation of maximum possible spoofing delay introduced

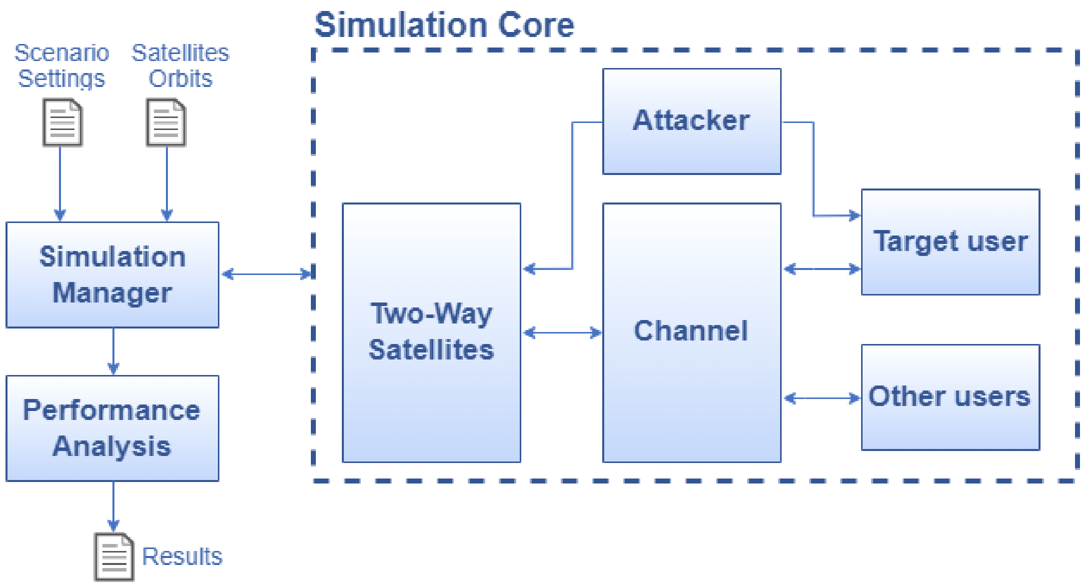


- Unknown user position : Uncertainty on computed desynchronization depends on altitude

- Known user position : The RTT can be checked with exact theoretical value

Two-Way Ranging Simulator

- Development of a Matlab simulator
  - Simulation of both positioning and time transfer
  - Compute the KPIs on a single *target user*
  - Simulation of attacks
    - Man in the Middle attack (SCER, Distance Increase)
    - Distance Fraud attacks
    - GNSS attacks



UNCLASSIFIED - COMMERCIAL IN CONFIDENCE

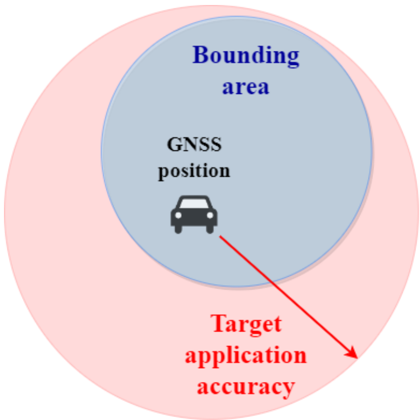
Experimentation Plan

- Preliminary simulations
  - Description
    - test several short simulations;
    - tune the parameters having the higher impact on the KPIs
  - Goals
    - assess the sensitivity of the KPIs with respect to the tuned parameters
    - define a baseline nominal scenario and a baseline attack scenario

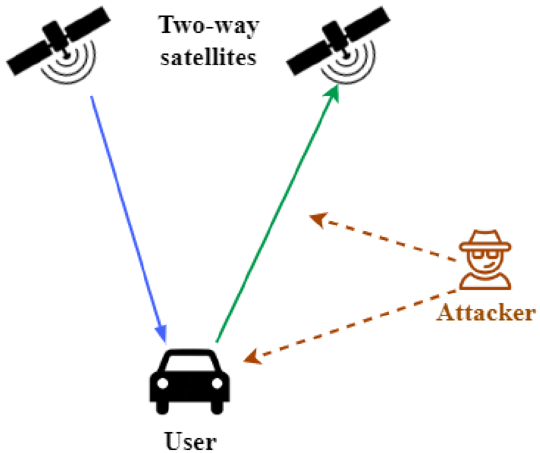
- Long simulations:
  - Description
    - increase the simulation duration;
    - test the baseline scenarios and tune the most interesting parameters
  - Goal
    - derive statistically meaningful KPIs

Experimentation Plan

- Nominal scenarios
  - Goal
    - Authenticate the user GNSS position (positioning mode)
    - Authenticate the clock bias (time transfer mode)
    - Tune key parameters
    - Extract KPIs



- Attack scenarios
  - Goal
    - Detect the attack



Qascom
Trust is Nice, Control is Better.

Key Performance Indicators (KPIs)

- System availability – A_{system}
  - percentage of iterations the system authenticates the user
- Target application availability – $A_{targetApp}$
  - percentage of times the system authenticates the user within the target application period
- Probability of false alarm – P_{fa}
- Misdetection probability – P_{md}

Testbed Configuration – Nominal Scenario

- Main tuned parameters:
  - User equipment transmitting power P_{UE}
  - Time between user requests $\mathrm{T_{req}}$
  - Scheduling rule $\mathrm{M_{scRule}}$
  - Bandwidth (uplink and downlink) B_w
  - Target position accuracy $\mathrm{x_{acc}}$
  - LEO satellite constellation SV_{const}

Constellation name SV_{const}	#sat	Satellite altitude [km]
a)	900	1200
b)	300	1200
c)	375	2000
d)	450	2000

  - Number of simultaneous Uplinks for the selected simulations : 100

Positioning Mode – Nominal Scenario

- Results Long Simulations (6h duration):
  - No false alarms: P_{fa}= 0%
  - Baseline scenario:
    - A_{system}= 43%
    - $A_{targetApp}$= 92%

#ID	M_{scRule}	T_{req}[s]	P_{UE}[W]	B_w[MHz]	x_{acc} [m]	A_{system} [%]	$A_{targetApp}$ [%]	P_{fa} [%]
1	1	10	1	2	100	42.82	92.16	0
2	Inf	10	1	2	100	37.29	91.24	0
3	Inf	10	1	1	100	26.12	78.17	0
4	Inf	5	1	2	100	42.06	100.00	0
5	1	5	1	2	100	42.29	99.01	0
6	Inf	20	1	2	100	28.15	53.27	0
7	1	20	1	2	100	44.26	78.42	0
8	Inf	25	1	2	100	5.45	10.20	0
9	1	25	1	2	100	40.51	60.33	0
10	Inf	10	1	2	25	21.85	71.00	0

Testbed Configuration – Attack Scenario

- 4 types of simulated attacks:
  - GNSS attack;
  - GNSS + Man In the Middle (MIM) attack;
  - Distance Fraud (DF) attack;
  - Distance Fraud + GNSS attack

- Tuned parameters:
  - Distance between the true and the spoofed position $d_{spoofed}$
  - Uncertainty on the layover time T_{layStd}

Positioning Mode – Attack Scenarios

- **GNSS attacks**
  - always detected
  - incompatibility between authentic ranges and spoofed position
- **GNSS + MIM, DF, GNSS + DF attacks**
  - detected with low std of the layover time → incompatibility between spoofed ranges and spoofed position
  - $P_{md} = 7.02$ with higher uncertainty on layover time → looser compatibility checks → two-way ranges can be compatib

#ID	Attack type	$d_{spoofed}$ [m]	T_{layStd} [ns]	P_{md} [%]
1	GNSS	500	0.289	0
2	GNSS	150	0.289	0
3	GNSS + MIM	500	0.289	0
4	GNSS + MIM	150	0.289	0
5	GNSS + MIM	150	289	7.02
6	DF	500	0.289	0
7	DF	150	0.289	0
8	GNSS + DF	500	0.289	0
9	GNSS + DF	150	0.289	0

Time Transfer Mode – Nominal Scenario

- System availability:
  - Impacted by:
    - Elevation mask angle → 30°
    - Constellation altitude → 4 tuned constellations
  - $A_{targetApp} = 100\%$

Constellation name	#sat	Satellite altitude [km]
a)	900	1200
b)	300	1200
c)	375	2000
d)	450	2000

#ID	SV_{const}	Satellite altitude [km]	δ_c^{max}[ms]	A_{system} [%]
1	a)	1200	2.7	100
2	b)	1200	2.7	100
3	c)	2000	3.8	100
4	d)	2000	3.8	100

Time Transfer Mode – Attack Scenario

- MIM Distance Increase attack
  - $\delta_c > \delta_c^{max} \rightarrow$ attack always detected
- Distance Fraud attack
  - $\delta_c > \delta_c^{max} \rightarrow$ attack always detected

#ID	Attack type	Link	δ_c [ms]	P_{md} [%]
1	MIM - DI	Uplink	3.85	0
2	MIM - DI	Downlink	3.85	0
3	DF	Uplink	3.85	0

Recommendations for a space-based system dedicated to two-way

www.thalesaleniaspace.com

Constellation geometry

- Testbed showed that essential parameters are :
  - Number of satellites in visibility instantaneously
  - Primary satellite elevation
  - Geometric diversity between secondary satellites

- Retained constellations
  - ≥450 satellites / ≥2000km altitude
  - Hypothesis : random selection of primary satellite

- Promising constellations : MEO + LEO
  - Primary satellites at MEO → High elevation (+ No UL budget problems)
  - Secondary satellites at LEO → Low elevation

- Possible adaptation of protocol for constellation optimization

  ➔ Selection of primary satellite at user level

  - Better geometry → Reduction of constellation size
  - Simplification of allocation plan

Payload Design – Satellite onboard computation needs

- Recall of session rate for 1200km satellite

	Total nb of active users in 2029 (k)	Tx duration (s)	Tx period (min)	Nb of signals simultaneously transmitted in a sat footprint
Autonomous vehicles (bootstrapping)	700	1.2	8h	44
Road user charging	70		15	93
Asset tracking	10		10	20
Fishery monitoring	50		30	33
Critical infrastructures	25		5	100
TOTAL	**855**			**290**
Target				**280**

- Extrapolation to 2000km altitude → 384 /s

- Main operations performed onboard
  - Acquisition / Demodulation of 384 AUI Uplinks /s
  - Acquisition / Demodulation of 384 Uplink responses /s

→ 1 Versal Core Processing board (50W)

Payload Design – Satellite Downlink transmission power

- Downlink Data Stream
  - Downlink requests → 460bps (1 request each 1.2s)
  - Two-Way Data Downlink → 61.6kbps ***- 268b per user of AV / CI***

- Downlink Budget analysis
  - Omni-directional transmission within the footprint

    → **100W Transmission Power**

- Two-Way Data Downlink is unicast → Use of SDMA w DL Beamforming
  - 7 beam – uniform power accross beams

    → **14W Transmission Power**

- Beamforming allows
  - Sufficient UL demodulation probability under Intra-syst. Interference
  - Reduced DL transmission power

Payload Design – Tentative payload Size / Weight / Power

- Estimated required power for 2 scenarios
  - Omnidirectional Downlink Transmission
  - Downlink SDMA

		Power consumption - Omni (W)	Power consumption – Beamforming (W)
Rx GNSS		10	10
2 way	Processing : - 1 Versal core processing board - 1 timing board	50	50
	RF : - 1 Front-end RF Tx (100W / 15W RF) - 1 Front-end RF Rx	200	30
	Filtering	0	0
Margin (%)	20	56	18
	Total	336	108

- Benchmark Solution → GOMSpace 16U
  - 12U Payload size
  - 80W-150W Average power

→ 16U estimated for beamforming solution

→ Towards micro-satellite (80kg) for Omnidirectional DL

Recommendations on revisit time

- Revisit time = max. duration between 2 station visibilities

- Revisit time dimensioning for
  - Compliance to TTA requirement for remote users
  - Required onboard memory (secondary)

- Revisit time dimensions TTA of monitoring use cases
  - Information transits through ground segment
  - Target TTA value : 15mn → Asset tracking / IUU Fishing / RUC

- Target revisit time depends on ISL in system design
  - No ISL → Revisit time = 15mn
  - ISL → 15mn = transit time through ISL to ground segment

- Estimated onboard memory needs
  - 52kbps memory input
  - 47Mb for 15mn revisit time

Recommendations on satellite footprint

- 2000km, 30° elevation mask
  - ➔ Fp area 14M km² - ***460 simultaneous Uplinks interferring***
  - ➔ Number of users above system capacity assessed in testbed

- Beamforming (7 beams), 30° elevation mask
  - ➔ Beam area 1.9M km² - ***70 simultaneous Uplinks interferring per beam***
  - ➔ Number of users coherent with capabilities demonstrated in testbed

- Elevation mask of 30° considered due to environmental conditions of most use cases

- Beamforming hypothesis requires antenna area of :
  - 0.73m² for considered L-band hypothesis
  - 0.17m² for retained S-band in ELCANO dedicated to Two-Way

➔ Preferred solution : shifting to higher frequency band (S-band) and have a satellite multi-antenna

Envisioned Way Forwards – System sizing

- Study the extension to **multi-epoch** of the Distance-Bouded RTT positioning / position verification
  - Extend positioning concept to multi-epoch
    - Possible use of IMU
    - Relax attack hypotheses (LOCFIT)
  - Extend position verification concept to multi-epoch
    - Verification of sequence of positions (LOCFIT)

➔ Enable two-way positioning with smaller constellations

- Study of **LEO + MEO** constellations
  - Assessment of two-way positioning performance with LEO + MEO
  - Cost Analysis / Optimization

Envisioned Way Forwards – System sizing

Protocol improvements (ELCANO)

- Enable online selection of primary satellite at user level
  - Simultaneous Downlink transmission on all satellites
  - Satellite ID information in return Uplink

➔ Better geometries and position availability

- Random selection of session (ALOHA Uplink Multiple Access)
  - Reduce allocation plan complexity
  - Avoid an Active Users Identification phase

➔ Reduced UL / DL datarates

➔No need for allocation plan

- Adaptations of the waveform (single-PRN DL/UL)

- **Followup activity** : Perform security analysis of this concept

Adaptation to commercial technologies

www.thalesaleniaspace.com

Study Logic

- The protocol designed in the context of the study i
  - No existing system / user device for this protocol

- Study possibility to use standardized protocol as a support for two-way
  - Derive requirements for a protocol that supports two-way
  - Identify candidate protocols
  - Derive modifications of the associated user device

- Protocols considered
  - LoRa CSS
  - LoRa LR-FHSS
  - Argos
  - Nb-IoT
  - LTE-M
  - VDES
  - E-SSA
  - 5G NR

Requirements for a protocol that supports two-way

- R1 – Bidirectional communication
- R2 – Wide-band for Uplink & Downlink
  - Def : >2MHz bandwidth (derived from testbed result)
- R3 – Secure physical layer
  - Def : Short symbols for robustness to SCER, >1µs length
- R4 – Waveform robust to LEO Doppler
- R5 – No reliance on user position / synchronization
- R6 – Communication with multiple satellites

Benchmark protocols wrt requirements

- LoRa CSS
  - Vulnerable physical layer (Long symbols)
  - Doppler pre-compensation (initial pos. / sync. necessary)
  - Single-satellite communication
- Nb-IoT
  - Narrow-Band (200kHz max)
  - Doppler pre-compensation (initial pos. / sync. necessary)
  - Single-satellite communication
- LTE-M
  - Doppler pre-compensation (initial pos. / sync. necessary)
  - Single-satellite communication
- Argos
  - Narrow-Band (50kHz)
  - Vulnerable physical layer (long symbols)

Benchmark protocols wrt requirements

- LoRa LR-FHSS
  - Narrow-Band (Max. 488Hz baseband BW)
  - Vulnerable physical layer (Long symbols – 325bps max)
- VDES
  - Narrow-Band (Max. 150kHz)
  - Vulnerable physical layer (Symbol duration >5ms)
- E-SSA
  - Doppler pre-compensation (initial pos. / sync. necessary)
  - Single-satellite communication
- 5G NR
  - Doppler pre-compensation (initial pos. / sync. necessary)
  - Single-satellite communication

Adaptation of commercial user devices

- No standardized protocol supports the designed two-way protocol

- Operations performed at tracker level
  - Cryptographic operations :
    - key exchange with KMI
    - verification of DL request signature
    - UL response MAC generation
    - UL / DL Encrypted PRNs generation
  - Active users identification ping reception
  - Acquisition / demodulation of Downlink request
  - Precise control of Layover time between DL / UL
  - Transmission of Uplink response

- No identified COTS performs these operations

➔ Perspective in prototyping user device

Envisioned way forward

Point : Difficulty to overlay Two-Way on standardized protocol / existing COTS

- Consolidate protocol output of ELCANO project

- Consolidate complexity assessment of user segment
  - Transmission power reasonable
  - Still to be analyzed for constraints imposed by accurate layover time

- Implement first prototypes of user devices