
Università degli Studi di Padova – Dipartimento di Ingegneria dell'Informazione
Corso di Laurea in Ingegneria Elettronica

Relazione per la prova finale
***«Tecniche di rilevamento di attacchi di spoofing per
sistemi di navigazione ibridi GNSS-Starlink»***

Relatore: Prof. Francesco Ardizzon

Laureando: Edoardo Minardo
Matricola n.: 2109383

Padova, 23/09/2026

☐ Sistemi di Navigazione Satellitare (GNSS)

- ☐ Stima di posizione e tempo su orbite **MEO** (Medium Earth Orbit, ~20.000 km)
- ☐ Perdita di precisione in zone urbane dense, vulnerabilità ad attacchi di spoofing

☐ Segnali di Opportunità (SOP) ad Orbite Basse (LEO)

- ☐ Utilizzo di costellazioni di telecomunicazione (**Starlink**) non progettate nativamente per il posizionamento
- ☐ Maggiore potenza ricevuta e diversità geometrica
- ☐ Assenza di misure di distanza dirette (solo **Doppler**)

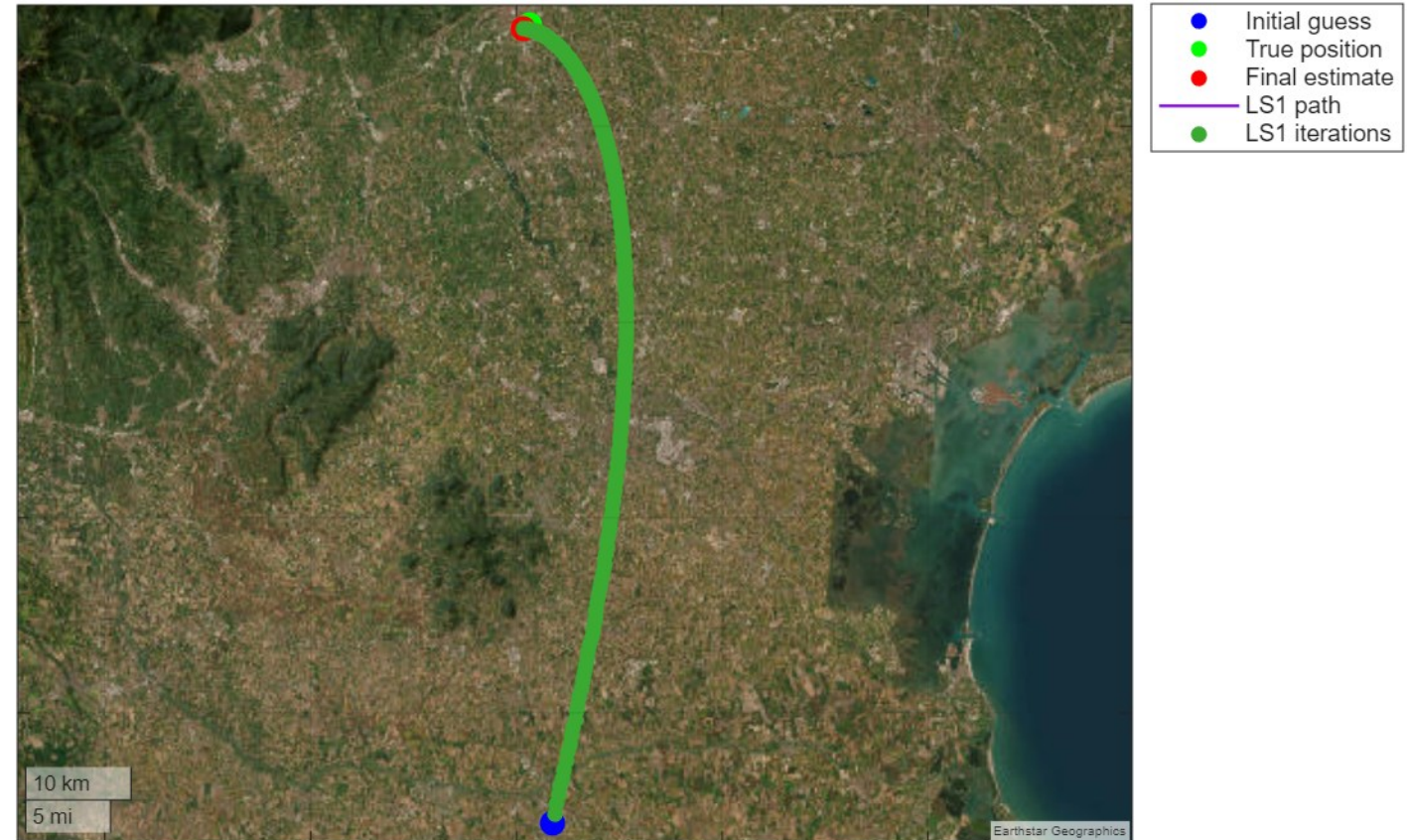
- ❑ Sviluppo di un sistema di navigazione capace di integrare misure eterogenee (**Doppler** e **pseudorange**), con ottimizzazione della matrice dei pesi
- ❑ Utilizzo dei satelliti **Starlink** per effettuare check di consistenza sul posizionamento.

- ❑ Sviluppo del codice in **MATLAB**, simulando inizialmente il modello di navigazione con solo GNSS, per poi progettare e sviluppare un **solutore ibrido**
- ❑ **Testing** e analisi comparativa tra il caso nominale e diversi scenari di attacco, individuando con quali pesi il sistema è più sensibile.

Navigazione basata su soli satelliti Starlink (**LEO**): Misure Doppler

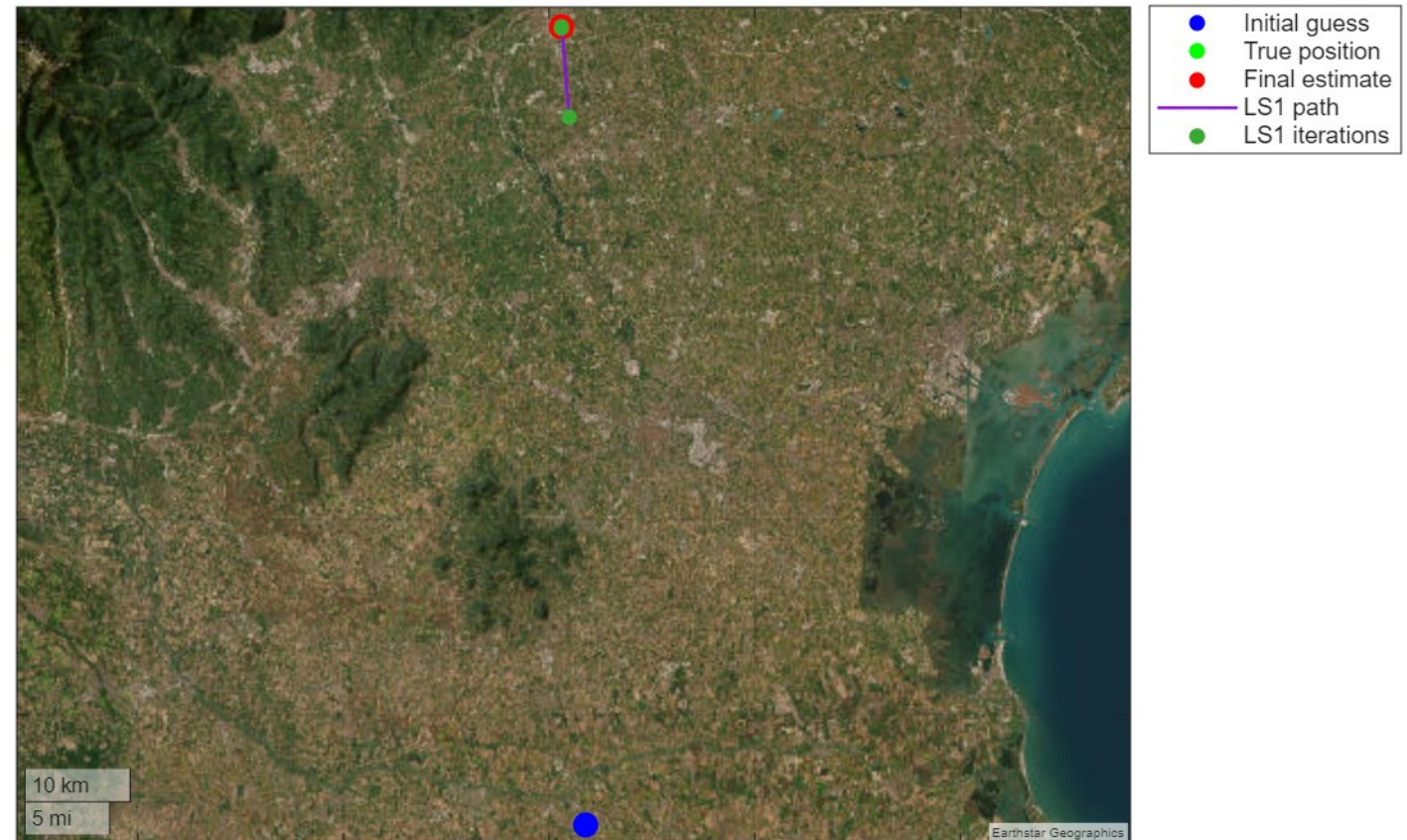
Risolutore ai minimi quadrati (LS) partendo da un punto iniziale arbitrario

Lenta convergenza (centinaia di iterazioni) con errore di posizionamento **~600m**.



Navigazione **simulata** a partire da satelliti GNSS (**MEO**): Misure di Pseudorange

Convergenza veloce con poche iterazioni, **errore nullo** se non aggiunto artificialmente.

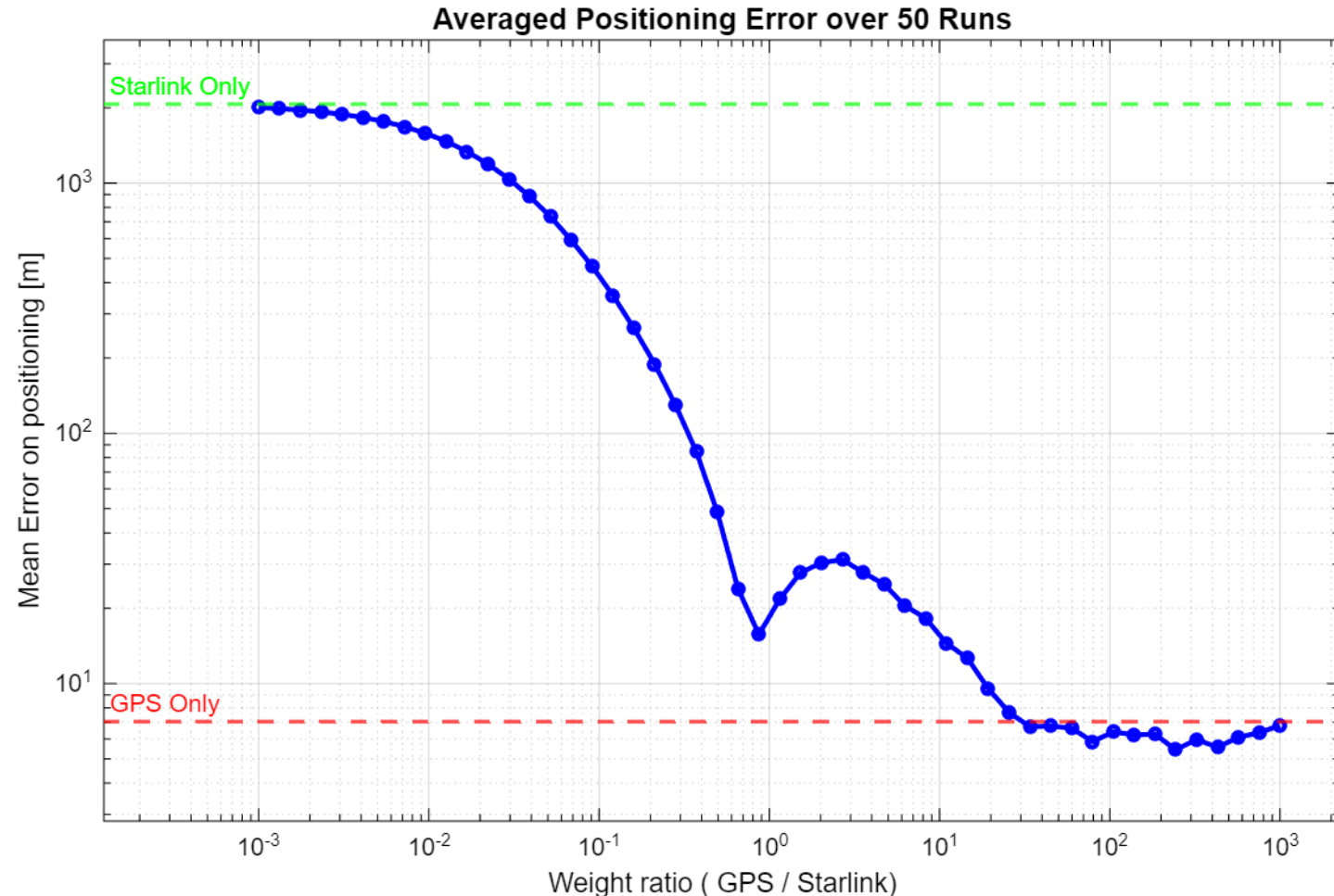


Manteniamo il tipo di segnale originale di entrambe le sorgenti utilizzando il metodo dei **Minimi Quadrati Pesati (WLS)**:

$$\mathbf{H}_{\rho f} = \begin{bmatrix} \mathbf{H}_{\rho p} & 0 \\ \mathbf{H}_{fp} & \mathbf{H}_{fv} \end{bmatrix}$$

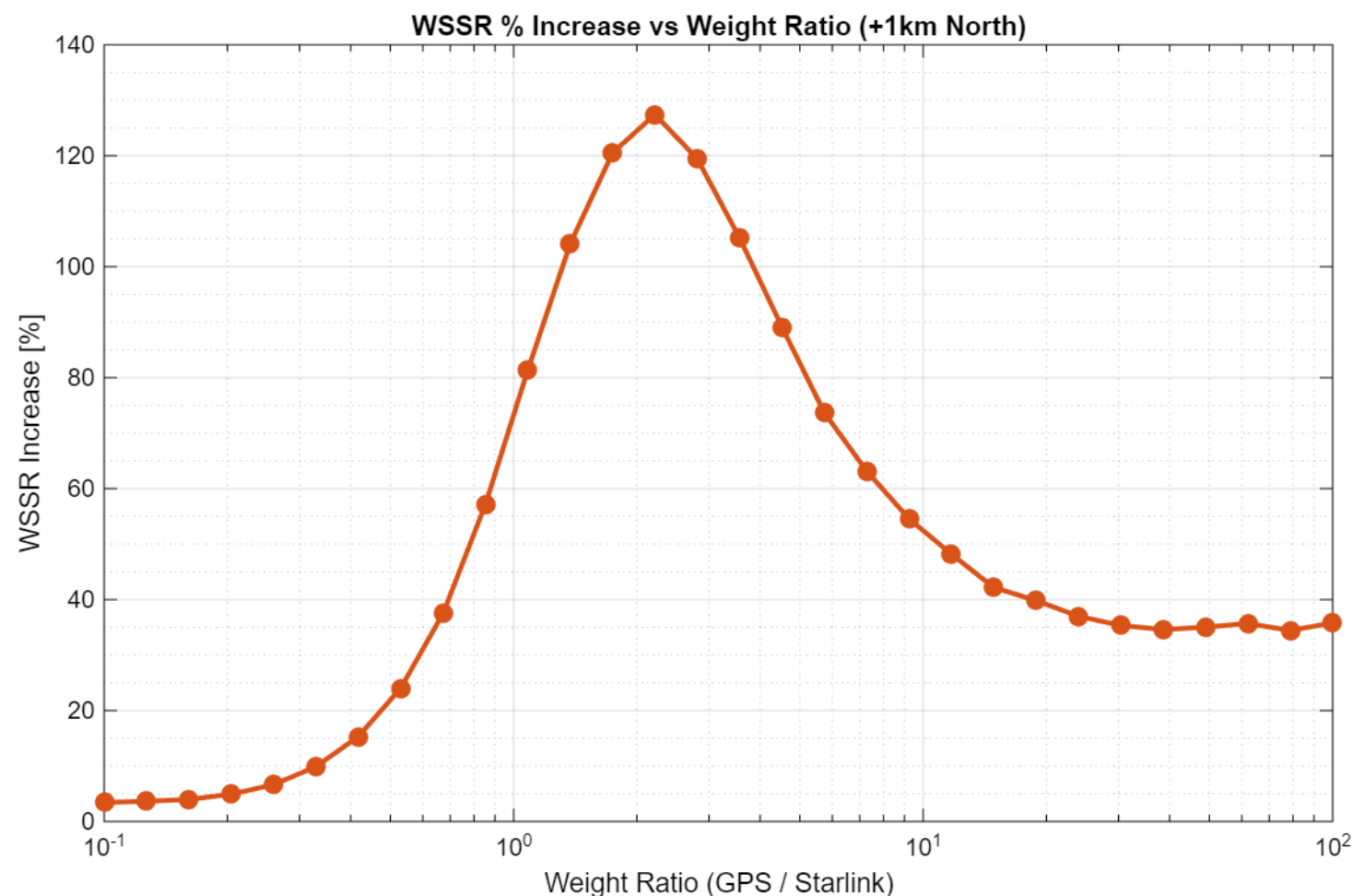
$$\hat{\delta \vec{\theta}} = (\mathbf{H}_{\rho f}^H \mathbf{W}_{\rho f} \mathbf{H}_{\rho f})^{-1} \mathbf{H}_{\rho f}^H \mathbf{W}_{\rho f} [\delta \vec{\rho}, \delta \vec{f}_d]^T$$

con una precisione variabile rispetto alla matrice dei pesi assegnata.



Per verificare se riusciamo a rilevare un attacco misuriamo il **Weighted Sum of Squared Residuals (WSSR)** su un posizionamento «attaccato» comparandolo ad uno attendibile.

N.B.: il **Weight Ratio** si riferisce a quello usato per calcolare il WSSR, non il posizionamento

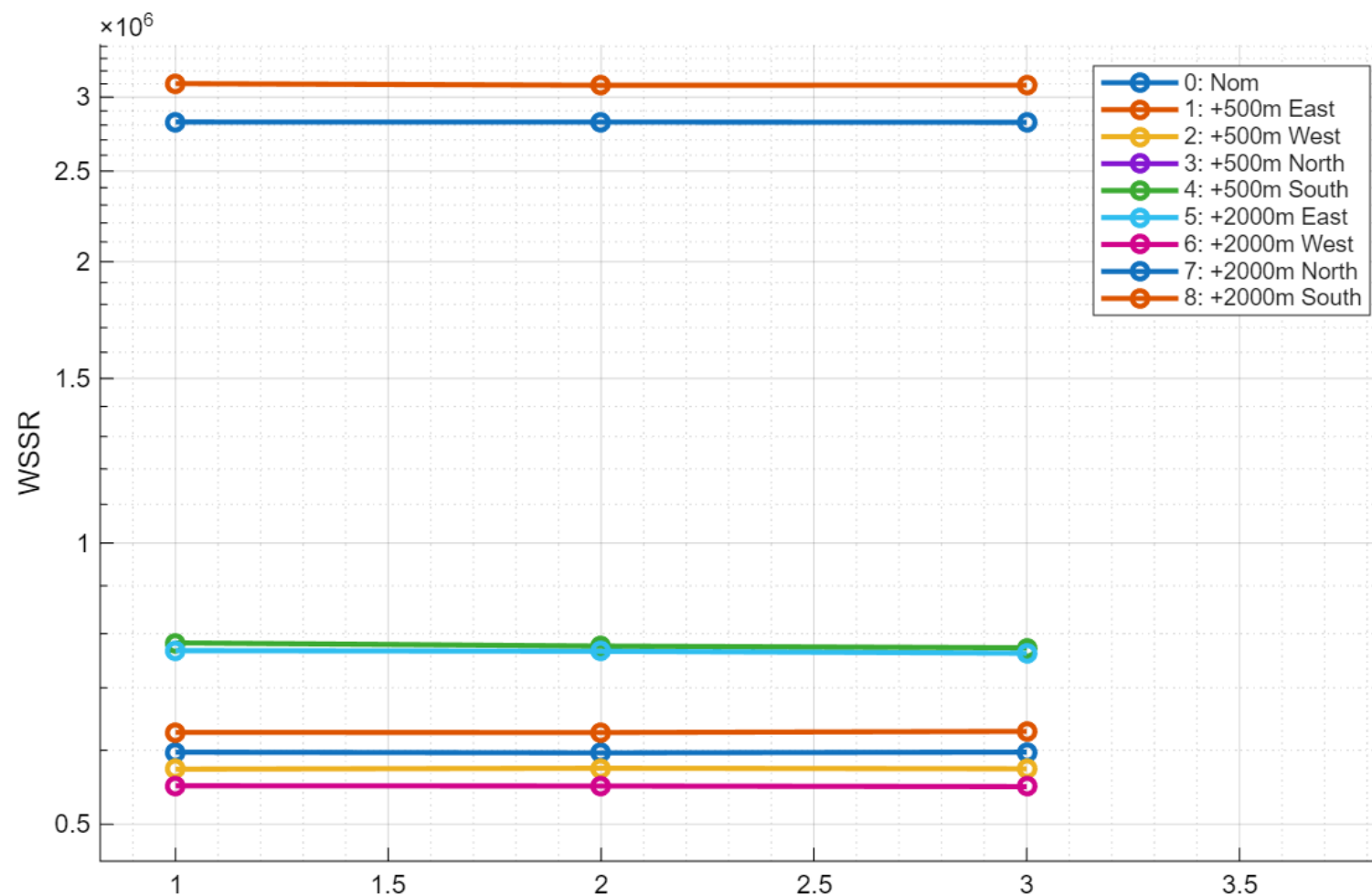


RILEVAMENTO SPOOFING

Analizziamo vari scenari d'attacco con punti di partenza diversi, osservando come cambia il WSSR in base all'attacco.

Gli attacchi verso **nord/sud** sono molto evidenti,

si nota invece che simulando l'attacco verso **ovest** il WSSR **diminuisce** rispetto al caso nominale.



- ❑ È possibile rilevare attacchi di spoofing sul GNSS integrando la costellazione Starlink in un'architettura WLS
- ❑ Si può definire un range di valori di WSSR all'infuori del quale si stabilisce di essere attaccati. Questo dipende dall'efficacia del sistema Starlink (più accurato = range più ristretto).