Università degli Studi di Padova

Dipartimento Matematica

Hyperloop: A Cybersecurity Perspective

Alessandro Brighente[1], Mauro Conti[1,2], Denis Donadel[1], Federico Turrin[1,3]

[1] University of Padova, [2] TU Delft, [3] Spritzmatter Srl

Workshop on Automotive Cyber Security (ACSW)
July 8, 2024

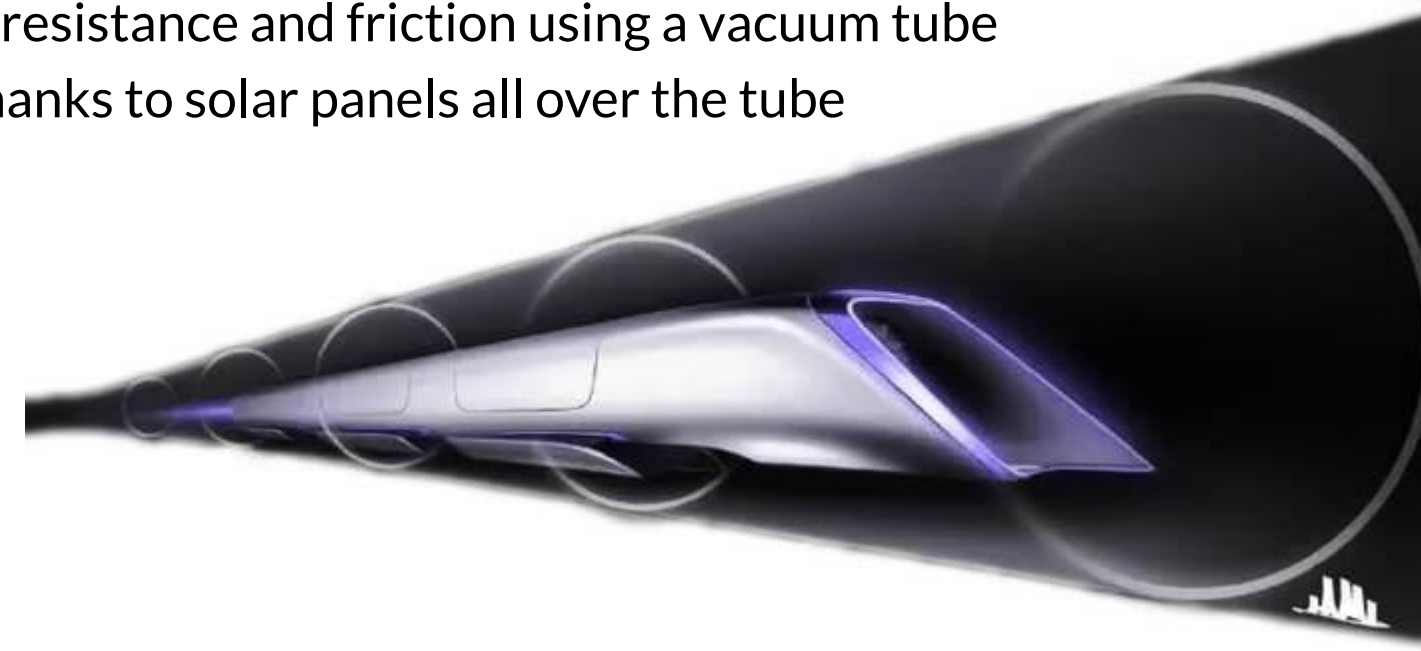
SPRITZ Security & Privacy Research Group

Index

- Introduction
- Hyperloop Infrastructures
- Communications inside a Hyperloop system
- Security issues in Hyperloop’s communication channels
- Countermeasures

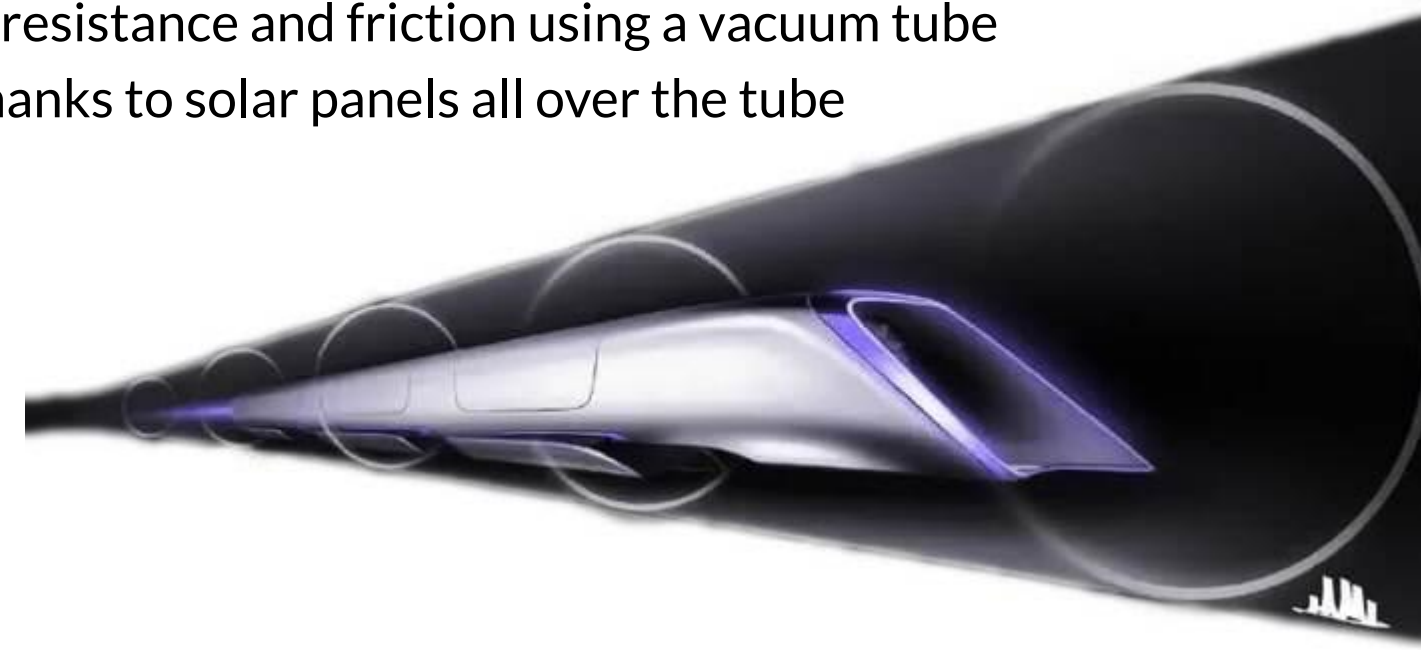
Introduction

- Introduced in 2013 by Elon Musk
- Ultra-fast train (~1200km/h)
- Mitigating air resistance and friction using a vacuum tube
- Sustainable thanks to solar panels all over the tube

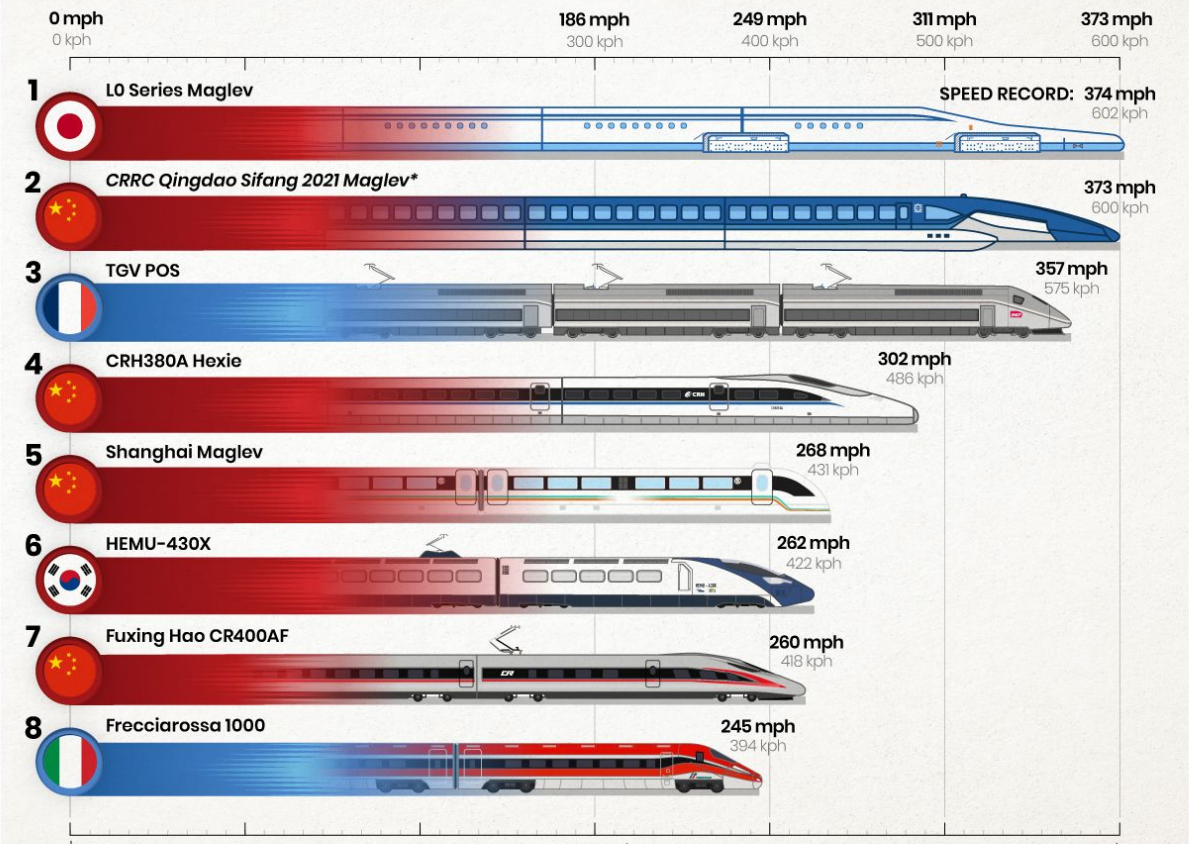


Introduction

- Introduced in 2013 by Elon Musk
- Ultra-fast train (~1200km/h)
- Mitigating air resistance and friction using a vacuum tube
- Sustainable thanks to solar panels all over the tube



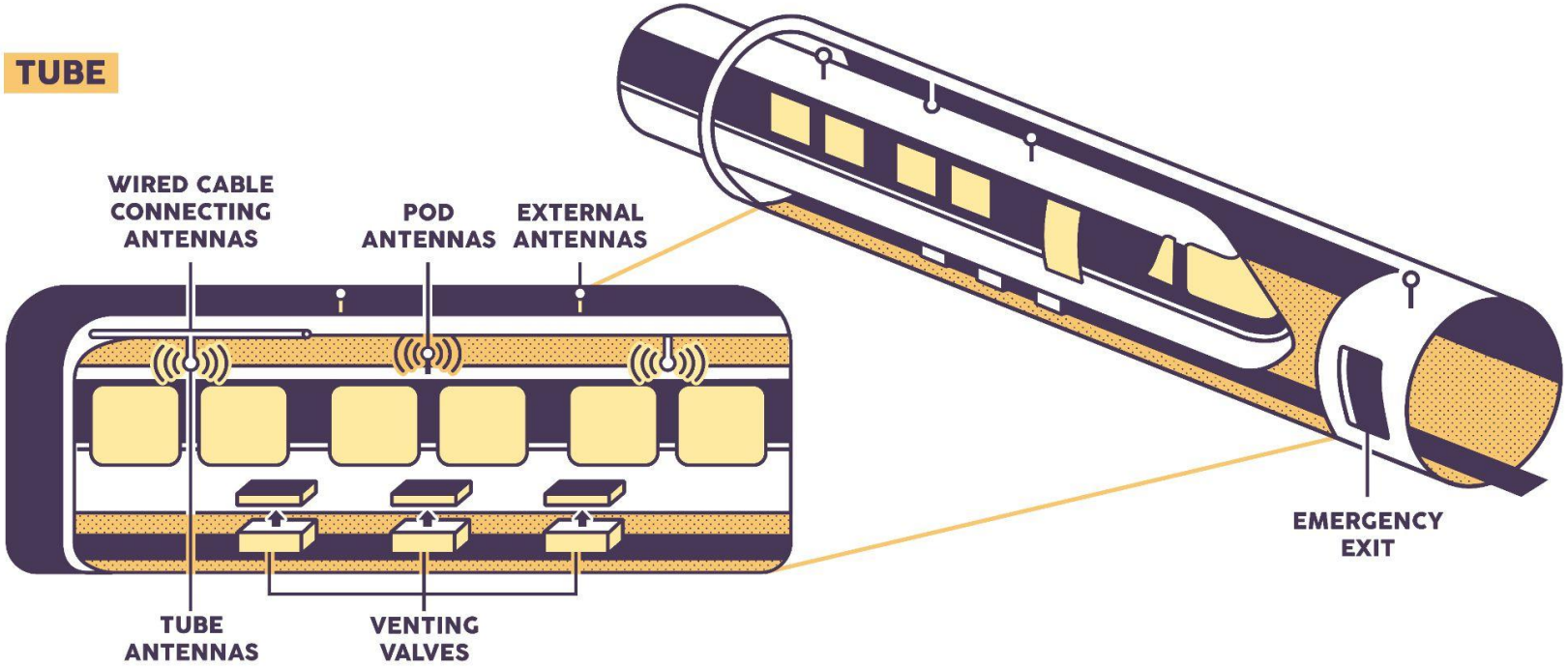
Similar vehicles



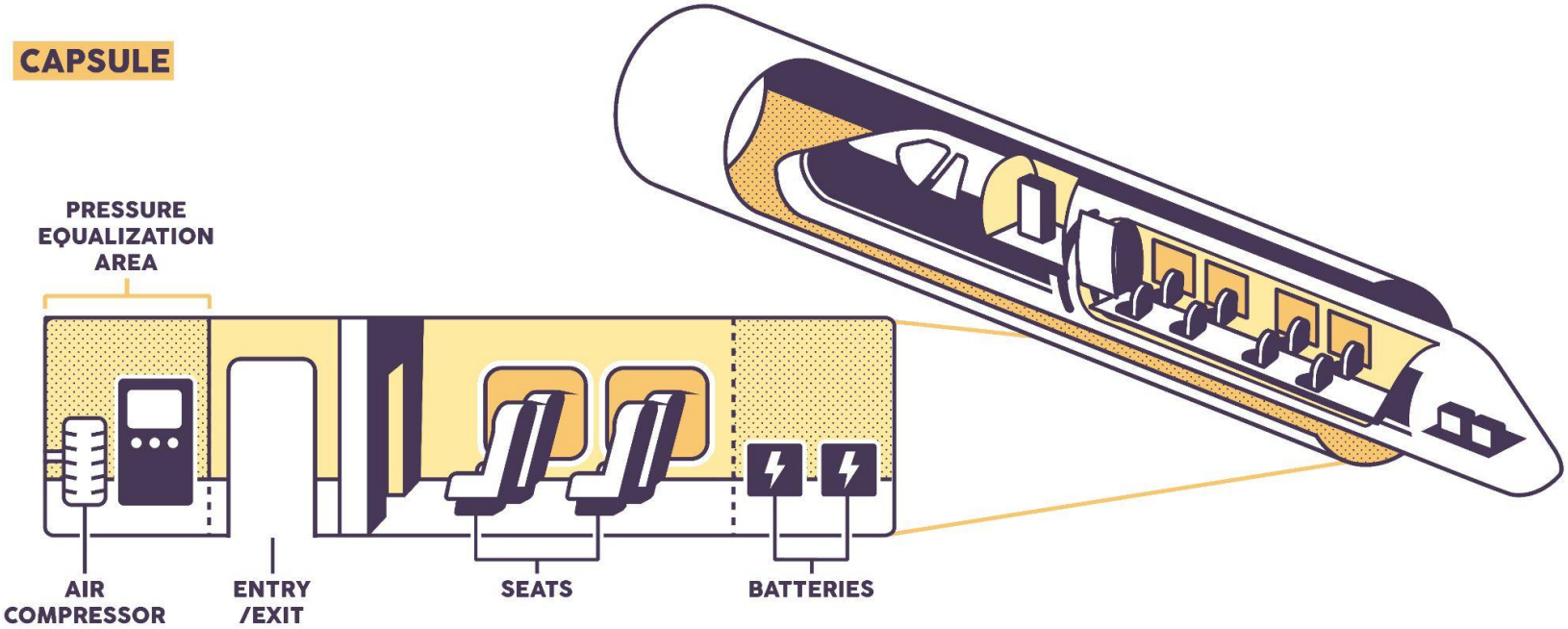
Related works?

- Lack of official documentation
- Expensiveness of testing
- Mostly related to infrastructure and design problem

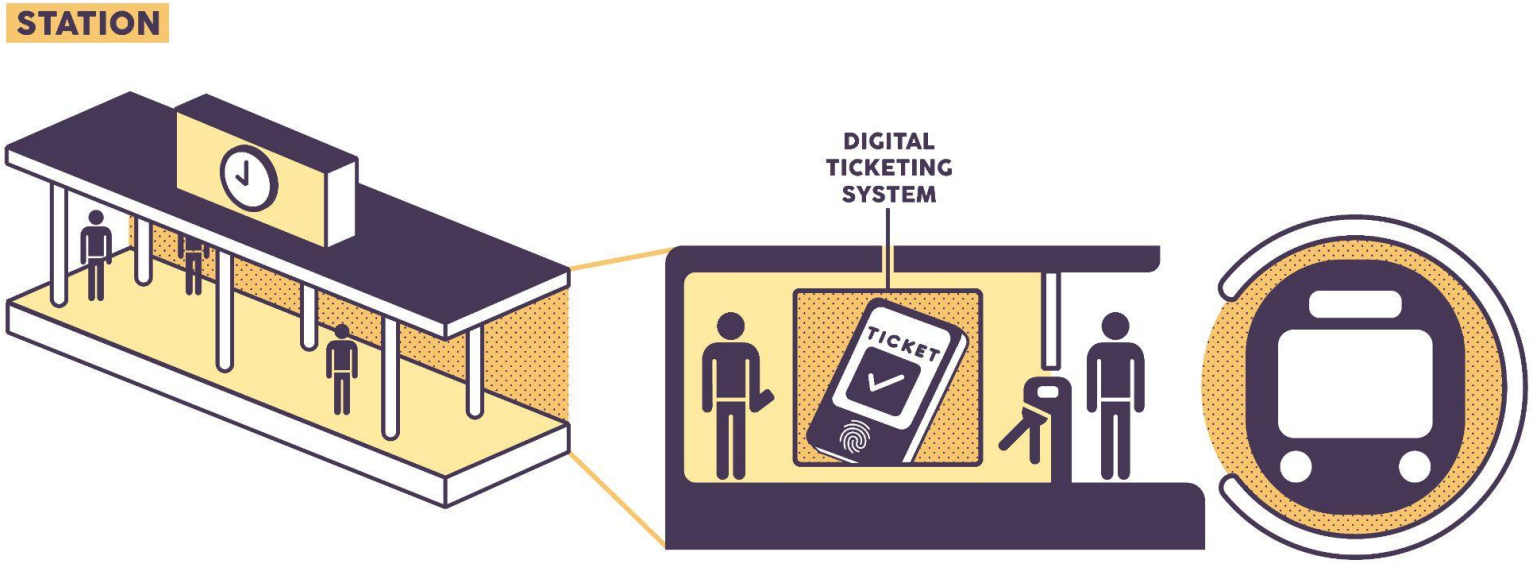
Physical Infrastructure



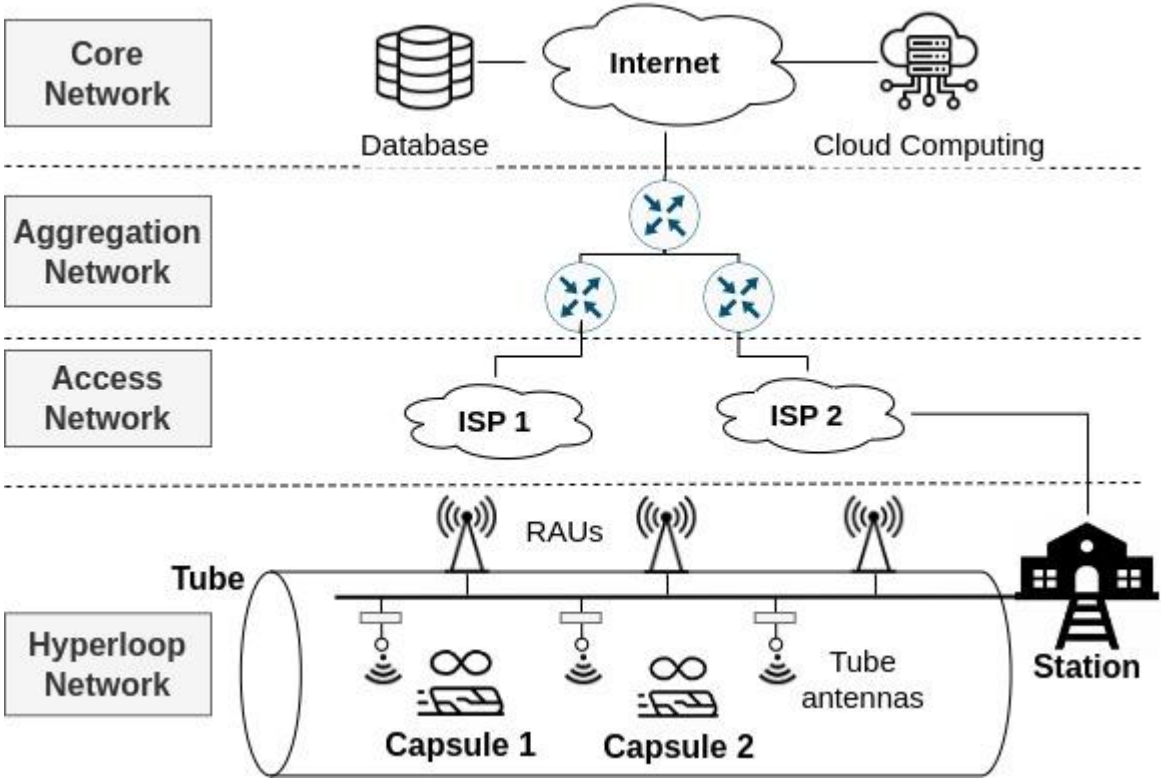
Physical Infrastructure



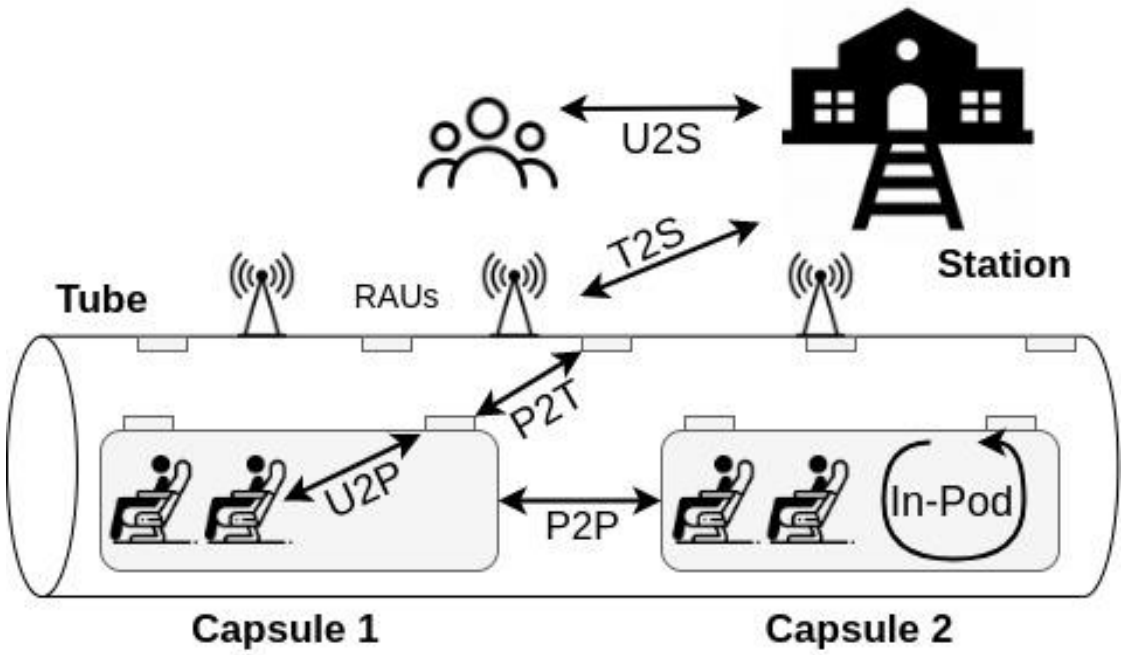
Physical Infrastructure



Network Infrastructure

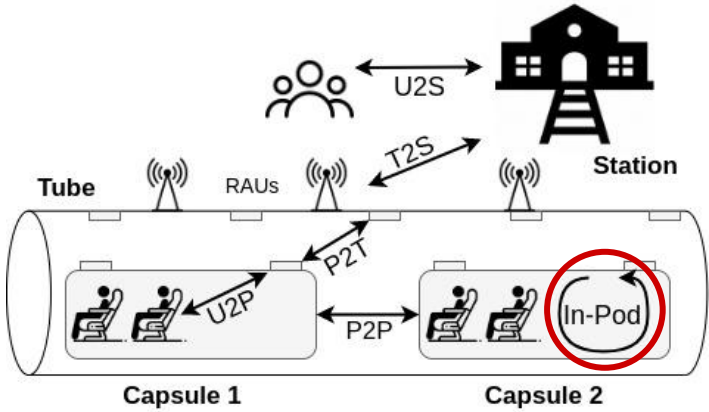


Communications inside Hyperloop



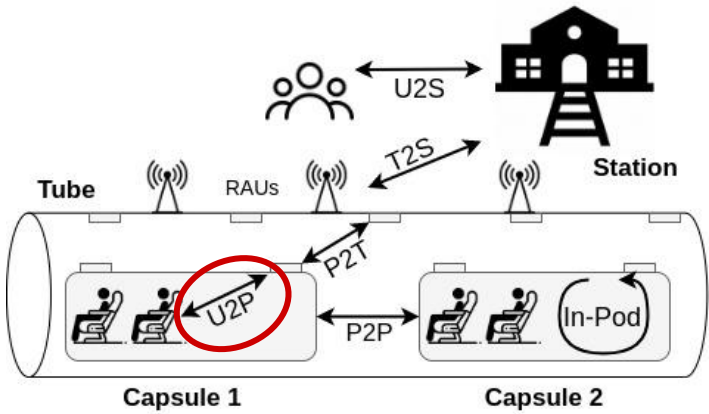
In-Pod Security

- Similar to in-vehicle networks
  - An attacker may directly connect to the internal network e.g., via Ethernet ports
- Levitation in managed on pod may be tampered with
- Users may DoS the pod through the legitimate connection if proper connection limits are not imposed



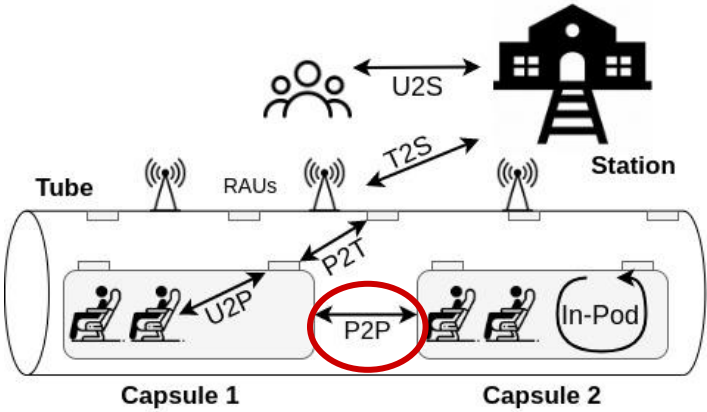
User-To-Pod Security

- Infotainment:
  - DoS can prevent or slow down other user's connection
  - Attacking other users through credentials leakages
- U2P may be used as an entry point to the other communication channels



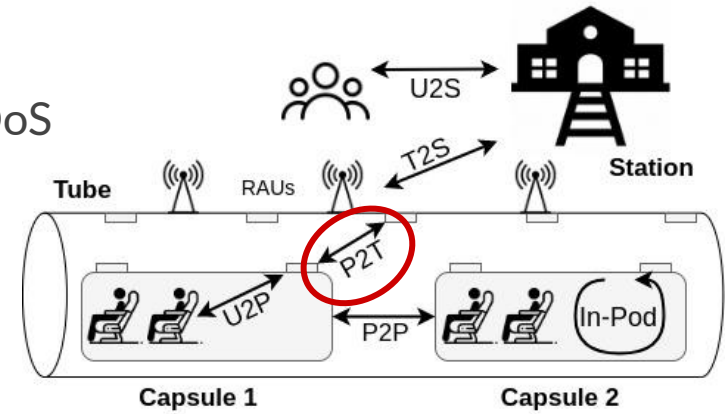
Pod-to-Pod security

- Pods can be attached/detached
- Similarities with vehicle platoons
- MitM to modify speeds can cause collisions
- DoS/flooding can delay critical messages
- Location spoofing can create crashes and dangerous behaviors



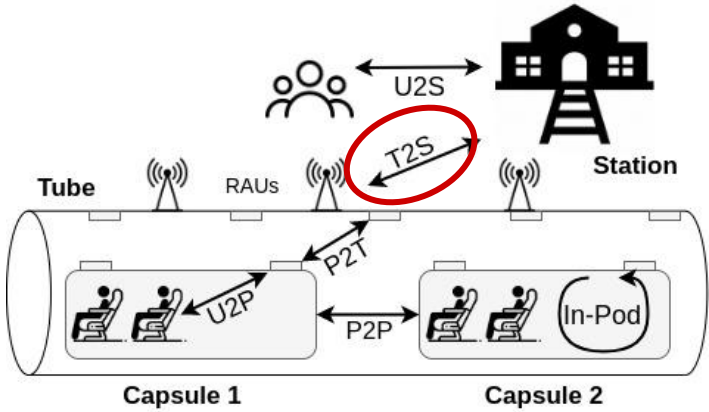
Pod-to-Tube Security

- MitM attacks can interfere with critical systems such as the pressurization of the tube
- Spoofing a pod location can create inconsistencies or hide pods
- DoS can impact the Internet connection of all the pod's users
  - The fast handover process can be a target for DoS
- Tampering with communication to stop charge or overcharge of the pod's batteries



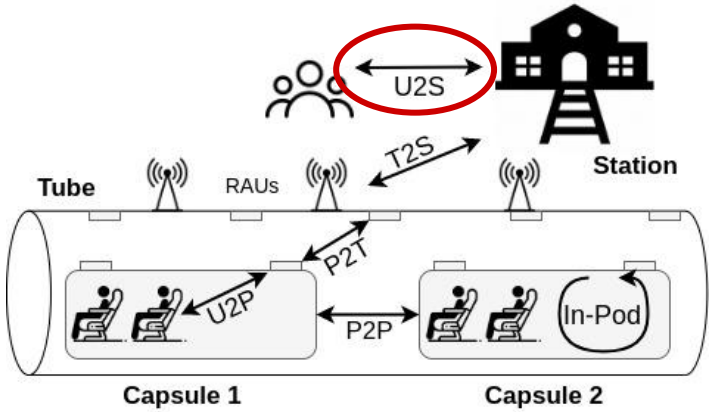
Tube-to-Station Security

- Critical connection which needs to manage high traffic amounts
- DoS can generate delays with impacting consequences
- This connection controls physical parameters such as the pressurization
  - Tampering with it can have harmful consequences
- Due to the tube length, physical tampering should be considered



User-to-(Devices in the)-Station Security

- Mainly inherited from common train systems
- Privacy leakages (user profiling)
- Frauds (e.g., bill another purser for a ticket)



Countermeasures

- Consider Hyperloop a critical infrastructure
  - Adopting best security practices and standards
- Adapt standards for railways systems
  - CEN-CENELEC
- General security standard (e.g., ISO 27000, IEC 62443)
- Automotive security standards (e.g., AUTOSAR)

Future directions

- Apply this research to real implementations
  - Complete testbeds
  - Standardized technologies
- Joint Technical Committee 20 is working on standardizing Hyperloop
  - CEN/CLC/TR 17912:2023
  - Up to now, a list of related standards and a roadmap for standardization
  - Are they considering security?

denis.donadel@phd.unipd.it
donadelden.github.io

Images credits: Upata (Elisa Turrin)