MEDIATE

A Mixed Software / Hardware Zero Trust Framework for the Cloud–Edge–IoT Computing Continuum

SIDS 2026 Workshop
in conjunction with **MDM 2026**

Authors:
Apostolos P. Fournaris*, Evangelos Haleplidis*,
Shahin Abdoul-Soukour †, Chih-Kai Huang ‡ †, Niemat Khoder †, Georgios Bouloukakis § †,
Andreas Brokalakis ¶,
Konstantinos Georgopoulos‖, and Sotiris Ioannidis‖

* Industrial Systems Institute, Greece
† **Télécom SudParis, Institut Polytechnique de Paris, France**
‡ Télécom Paris, Institut Polytechnique de Paris, France
§ University of Patras, Greece
¶ exapsys, Greece
‖ Technical University of Crete, Greece

Introduction

Motivating scenario: GNSS Spoofing in Last-Mile 4PL Delivery

Fourth-Party Logistics (4PL) orchestrates entire supply chains coordinating fleets of autonomous EVs, real-time routing, and just-in-time deliveries.

This relies on a **Cloud-Edge-IoT continuum** where sensor data (GNSS, LiDAR, cameras) drives navigation and logistics.

GNSS spoofing attack:

- A concealed radio transmitter (e.g., in a parked van 🚐) broadcasts counterfeit GNSS signals 📡 near a busy urban intersection
- The spoofed signals gradually shift calculated positions; vehicles are on a parallel street or several meters away
- In dense cities, multipath effects already degrade GNSS, making the attack harder to detect

Introduction

Motivating scenario: GNSS Spoofing in Last-Mile 4PL Delivery

Attack parameters

Transmitter range: ~100 m radius

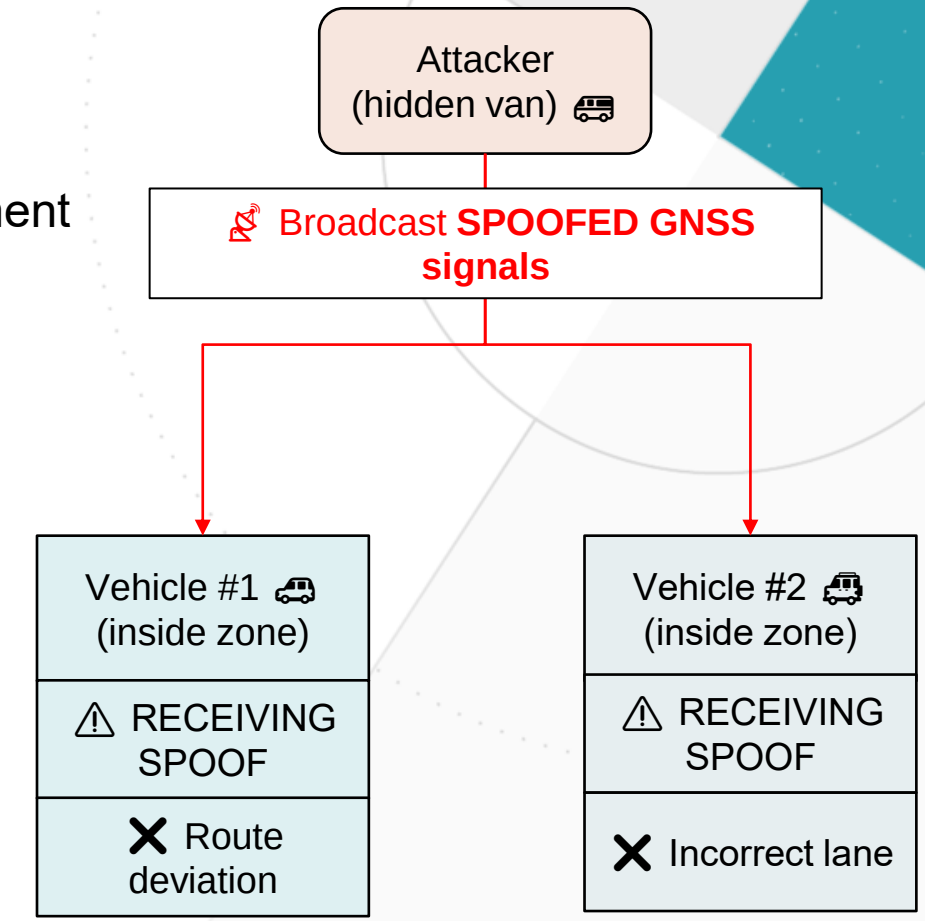
Localization error dominated by (x, y) horizontal displacement

Vehicles affected only while inside the spoofed zone

Consequences

- ❌ Missed delivery time-slots
- ❌ Traffic flow disruption
- ❌ Increased collision risk

→ This single-point vulnerability exposes a deeper problem: the entire Cloud-Edge-IoT stack lacks a unified security model.



Introduction

Computing Continuum

Cloud, Edge, and IoT have converged into a single, decentralized computing continuum[1,2] to handle:

- Increasing data generation and real-time analytics demands
- Decentralized processing across multi-tier infrastructures

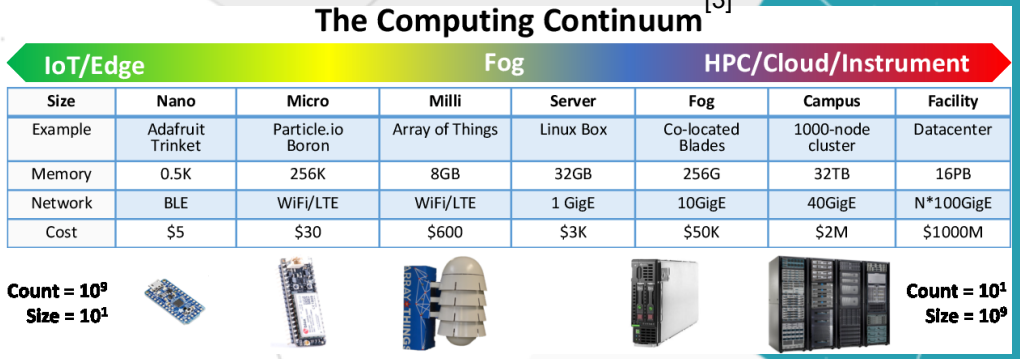
Why security is harder now?

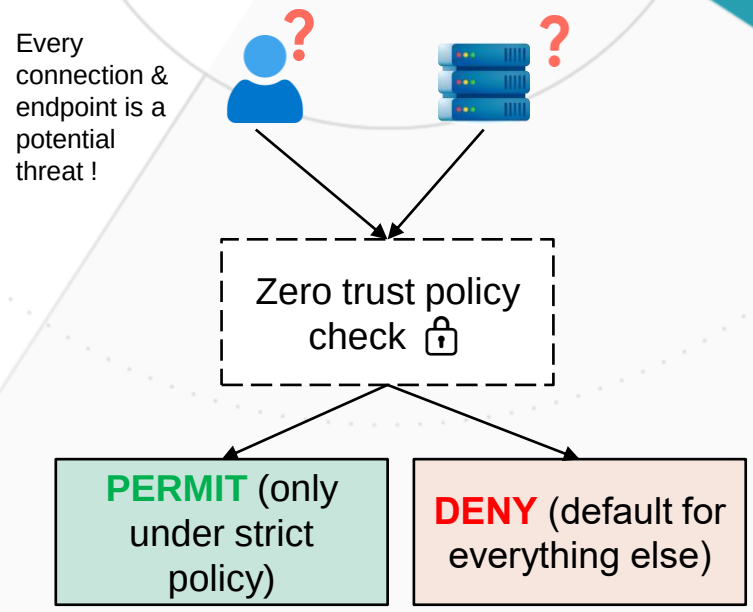
Traditional perimeter-based security is obsolete, attacks can enter at the IoT layer, propagate through the Edge, and corrupt Cloud decisions.

Zero Trust[4] secures such systems by treating every connection and endpoint as a potential threat:

- Deny by default → access is blocked unless explicitly granted
- Grant only under strict, continuously verified policy

The Computing Continuum[3]





[1] P. Gkonis et al., "A Survey on IoT-Edge-Cloud Continuum Systems: Status, Challenges, Use Cases, and Open Issues," Future Internet, 2023.

[2] A. Ullah et al., "Orchestration in the Cloud-to-Things Compute Continuum: Taxonomy, Survey and Future Directions," Journal of Cloud Computing, 2023.

[3] Beckman, Peter H. et al. "Harnessing the Computing Continuum for Programming Our World." Fog Computing (2020)

[4] V. Stafford, "Zero Trust Architecture," NIST special publication, 2020.

Problem

The Core Gap

❌ No framework brings Zero Trust to the continuum as a whole.

⚠ A robust model that extends **deny-by-default** across the entire Cloud-Edge-IoT continuum remains unrealised [5–7].

Existing solutions[8] often focus on **isolated layers** (e.g., only Cloud or only IoT), leaving:

- **Gaps** in end-to-end security
- **Blind spots** for cross-layer attacks (like the GNSS spoofing)

4PL demands a **unified, cross-layer framework** that combines:

- Coordinated mitigation across Cloud, Edge, and IoT
- Dynamic policy enforcement (real-time, context-aware)
- Lightweight monitoring

[5] C. Liu et al., “Dissecting Zero Trust: Research Landscape and its Implementation in IoT,” Cybersecurity, 2024.

[6] J. M. B. Murcia et al., “Decentralised Identity Management Solution for Zero-Trust Multi-Domain Computing Continuum Frameworks,” Future Generation Computer Systems, 2025.

[7] D. Rosendo et al., “Distributed Intelligence on the Edge-To-Cloud Continuum: A Systematic Literature Review,” Journal of Parallel and Distributed Computing, 2022.

[8] Biswajit Sarkar, et al., A sustainable random paradigm of centralized multi-customized facility with fourth-party logistics (4PL) and cleaner production with remanufacturing, Journal of Cleaner Production, 2025,

Related works

Orchestrating the Continuum

- **Kubernetes** and its lightweight variant **K3s** are widely used for managing containerized applications across cloud and edge.
- Federation frameworks like **Karmada** and **UnBound**[9] enable multi-cluster management and multi-tenancy.

Dynamic Access Control

- The **Usage Control** (**UCON**)[10] model and its extensions (SoNeUCONABC[11], UseCON[12], UCON+[13]) introduce continuous, context-aware, and relationship-based access control, supporting dynamic and distributed environments.

Decision Support

- **Multi-Objective Reinforcement Learning** (MORL)[14] is leveraged for optimizing defense strategies in complex, multi-objective settings.

⚠ No unified zero-trust framework addressing all continuum layers simultaneously

The need a unified, cross-layer zero-trust framework that combines coordinated mitigation, dynamic policy enforcement and lightweight monitoring deployed right next to each asset.

[9] C.-K. Huang, et al., “UnBound: Multi-Tenancy Management in Scalable Fog Meta-Federations,” in IEEE/ACM International Conference on Utility and Cloud Computing, 2024.

[10] J. Park, et al., “The UCONABC Usage Control Model,” ACM Transactions on Information and System Security, vol. 7, no. 1, 2004.

[11] L. Gonz´ alez-Manzano et al., “SoNeUCONABC, an Expressive Usage Control Model for Web-Based Social Networks,” Computers & Security, vol. 43, 2014

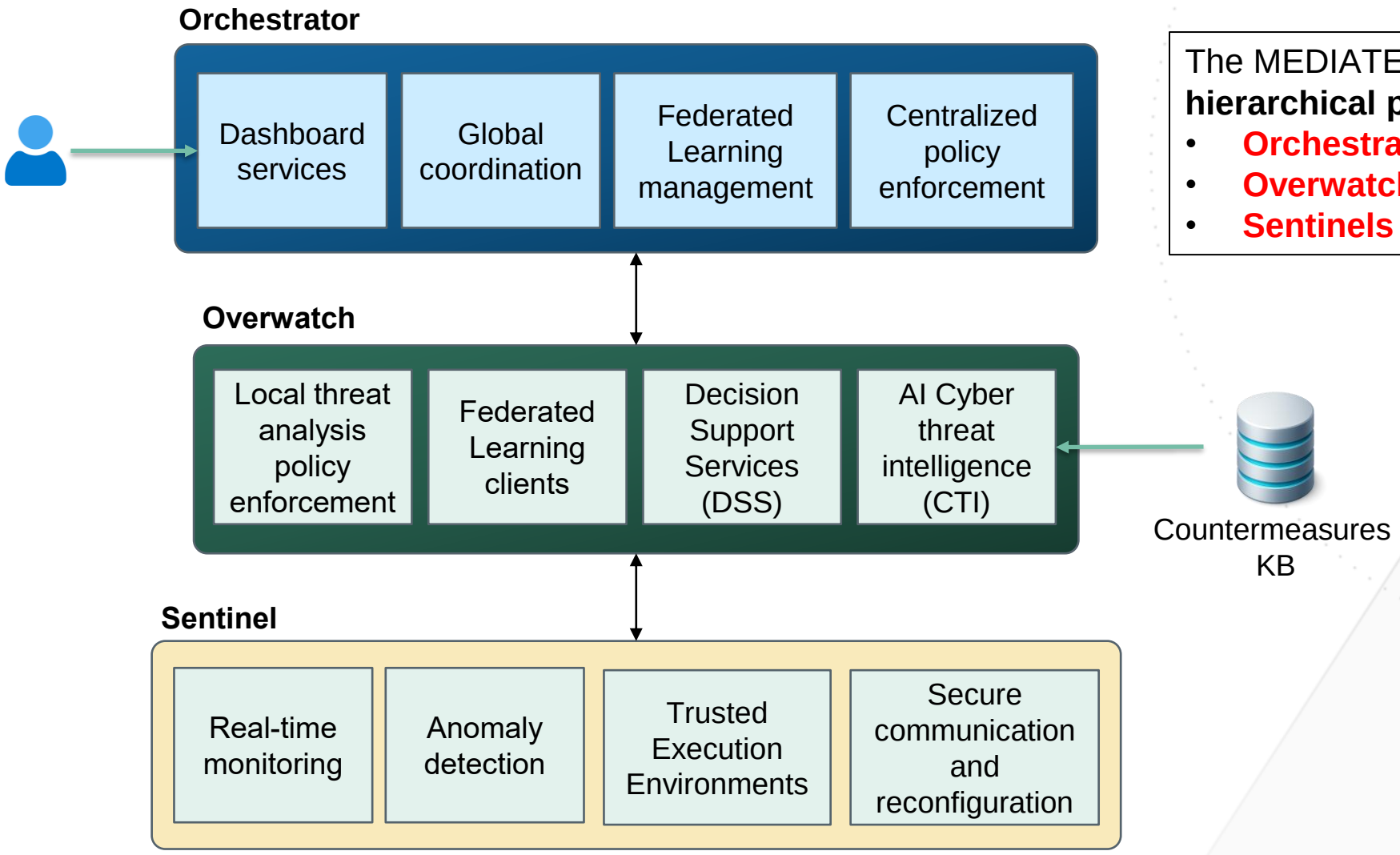
[12] C. Grompanopoulos, et al., “A use-based approach for enhancing UCON,” in International Workshop on Security and Trust Management. Springer, 2012, pp. 81–96.

[13] A. Hariri, et al., “Ucon+: comprehensive model, architecture and implementation for usage control and continuous authorization,” in Collaborative Approaches for Cyber Security in Cyber- Physical Systems. Springer, 2023, pp. 209–226.

[14] L. Zhang et al., “Multi-Objective Reinforcement Learning - Concept, Approaches and Applications,” Procedia Computer Science, vol. 221, 2023.

Proposed framework: MEDIATE

ARCHITECTURE → A Three-Layer Hierarchy



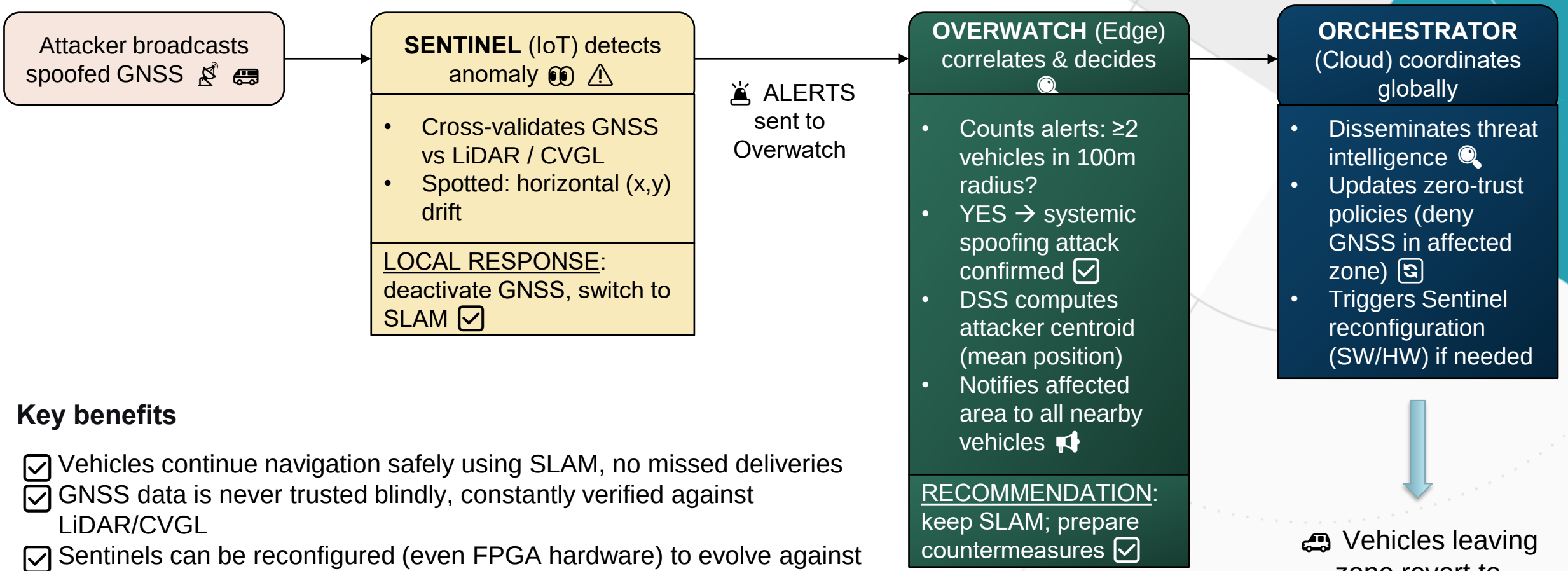
The MEDIATE architecture is organized as a **hierarchical pyramid**:

- **Orchestrator** at the cloud layer
- **Overwatch** modules at the edge
- **Sentinels** deployed at the IoT layer

Proposed framework: MEDIATE

How does the MEDIATE hierarchy stop the attack?

The three layers act in real-time coordination → from local detection to fleet-wide response.



Key benefits

- ☑ Vehicles continue navigation safely using SLAM, no missed deliveries
- ☑ GNSS data is never trusted blindly, constantly verified against LiDAR/CVGL
- ☑ Sentinels can be reconfigured (even FPGA hardware) to evolve against new spoofing variants
- ☑ Federated Learning keeps vehicle data decentralized, only model updates shared

CVGL: Cross-View Geo-Localization
SLAM: Simultaneous Localization and Mapping

Conclusion

MEDIATE → A unified, adaptive, and reconfigurable Zero Trust framework for the entire Cloud–Edge–IoT continuum.

Zero Trust	*Deny by default* → access granted only under strict, continuously verified policy
AI & FL	AI-driven threat intelligence + Federated Learning for privacy-preserving, distributed defense
HW/SW Reconfigurability	Sentinels adapt to evolving threats → software updates or even FPGA hardware reconfiguration

Future work: Implement and validate MEDIATE's core components in complex, real-world 4PL environments.

THANK YOU

For more information about MEDIATE European project
https://mediate-horizon.eu/

Link to our paper

This paper is supported by the Horizon Europe project MEDIATE under grant agreement number 101168465.