LISP-FIX Cloud Native Anomaly Detection

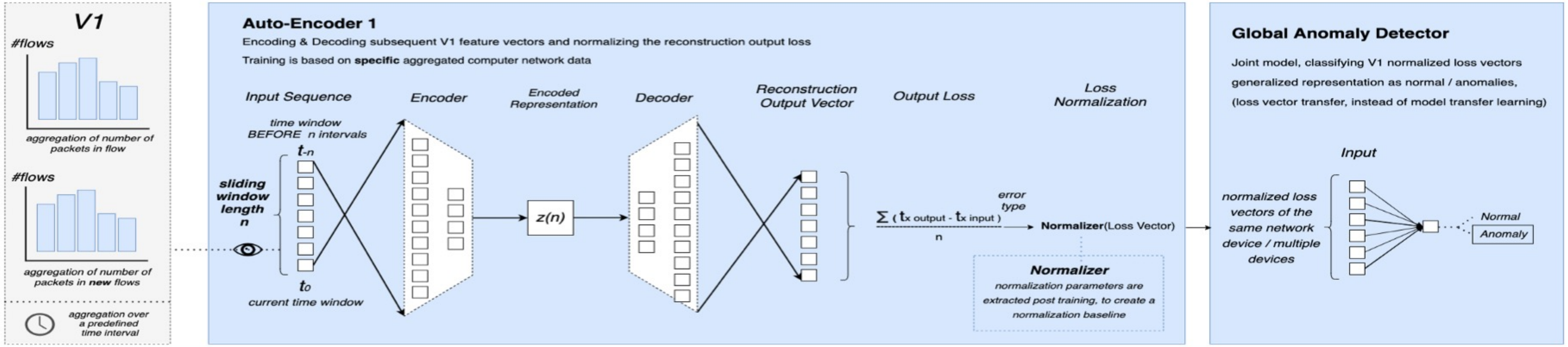
Using LISP Aggregation of IPFIX Sampling

Sharon Barkai, Dr. Aviv Yehezkel

Uniform Sampling Outperforms Probing

Auto-encoder Losses Transfer Learning, using only samples of the data

How does Uniform Small-Samples Detect App Anomalies



Method	Un-norm 18	Kitsune [10]	Norm 18	Norm 12+18
Precision	0.28	0.43	0.58	0.51
Recall	0.40	0.11	0.38	0.60
F1 Score	0.33	0.17	0.45	0.55

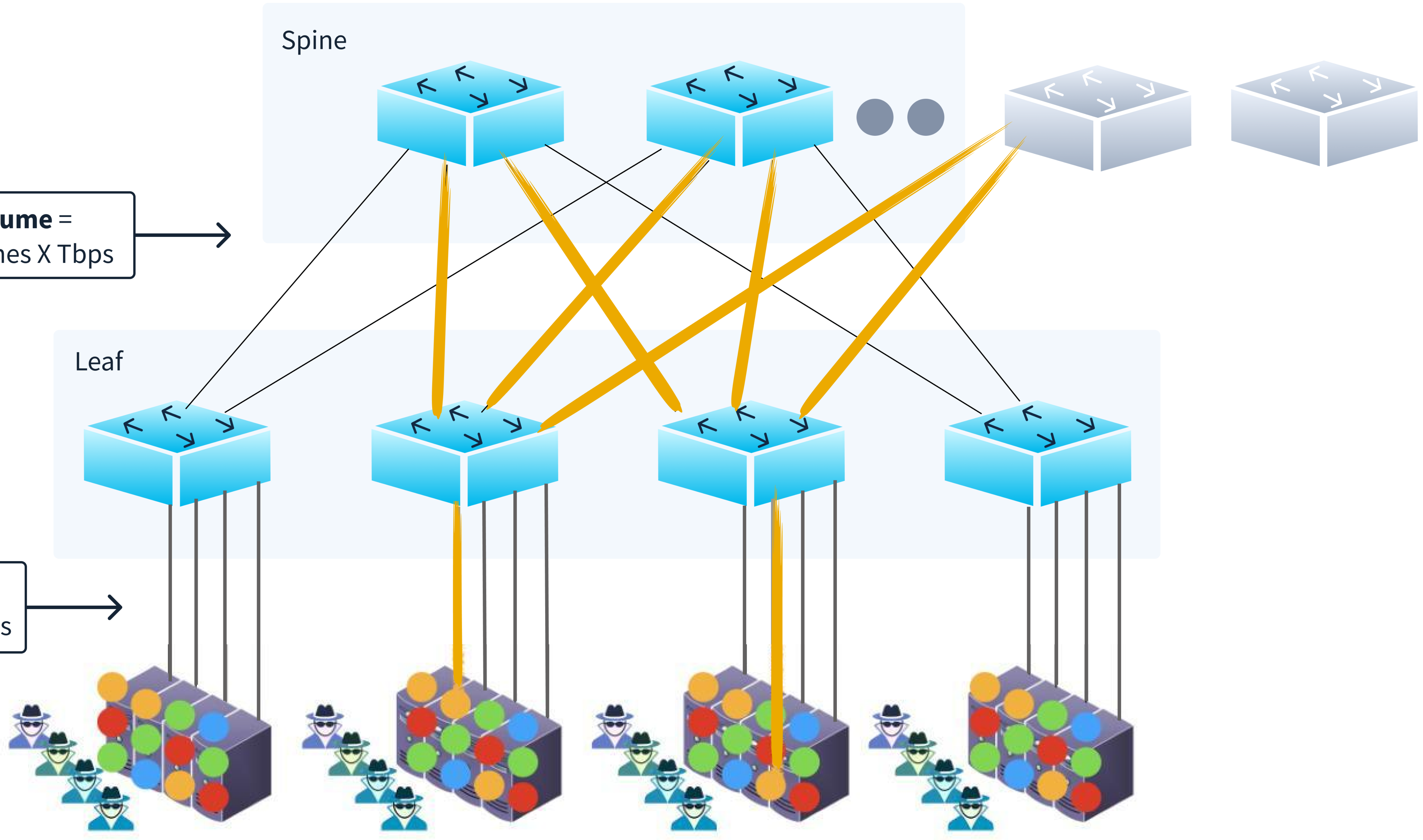
Cloud Native Flexibility → Monitoring Difficulty

Probing Any Process on Any Server, Any to Any Rack Links is Hard

Probing Volume =
Racks X # Spines X Tbps

Probing Volume =
Racks X # Servers per Rack X 10Gbps

Complexity and Attack Surface



Uniform Sampling Problem

Monitoring Links or Servers is Difficult

1

Link Probing

- Any specific link is hard only captures a fraction of per cloud native application behavior
- All the links is impossible due to sheer volume, a 50 rack segment = 100s of Tbps

2

Server Agents

- Increases complexity and attack surface by orders of magnitude
- Agents can and have brought attackers right into the OS soft belly

3

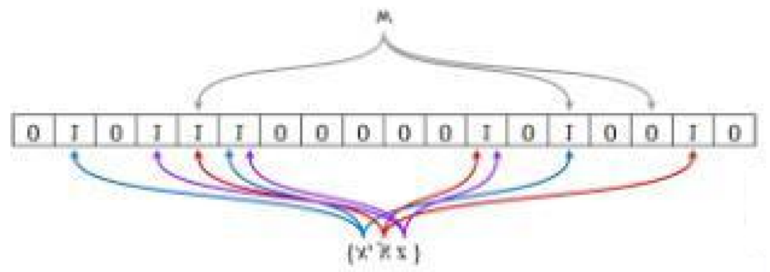
Default IPFIX

- Switch based sampling aggregation will result in random mix of applications traffic, none of the partitions will likely have Uniform Sampling of any of the Apps.

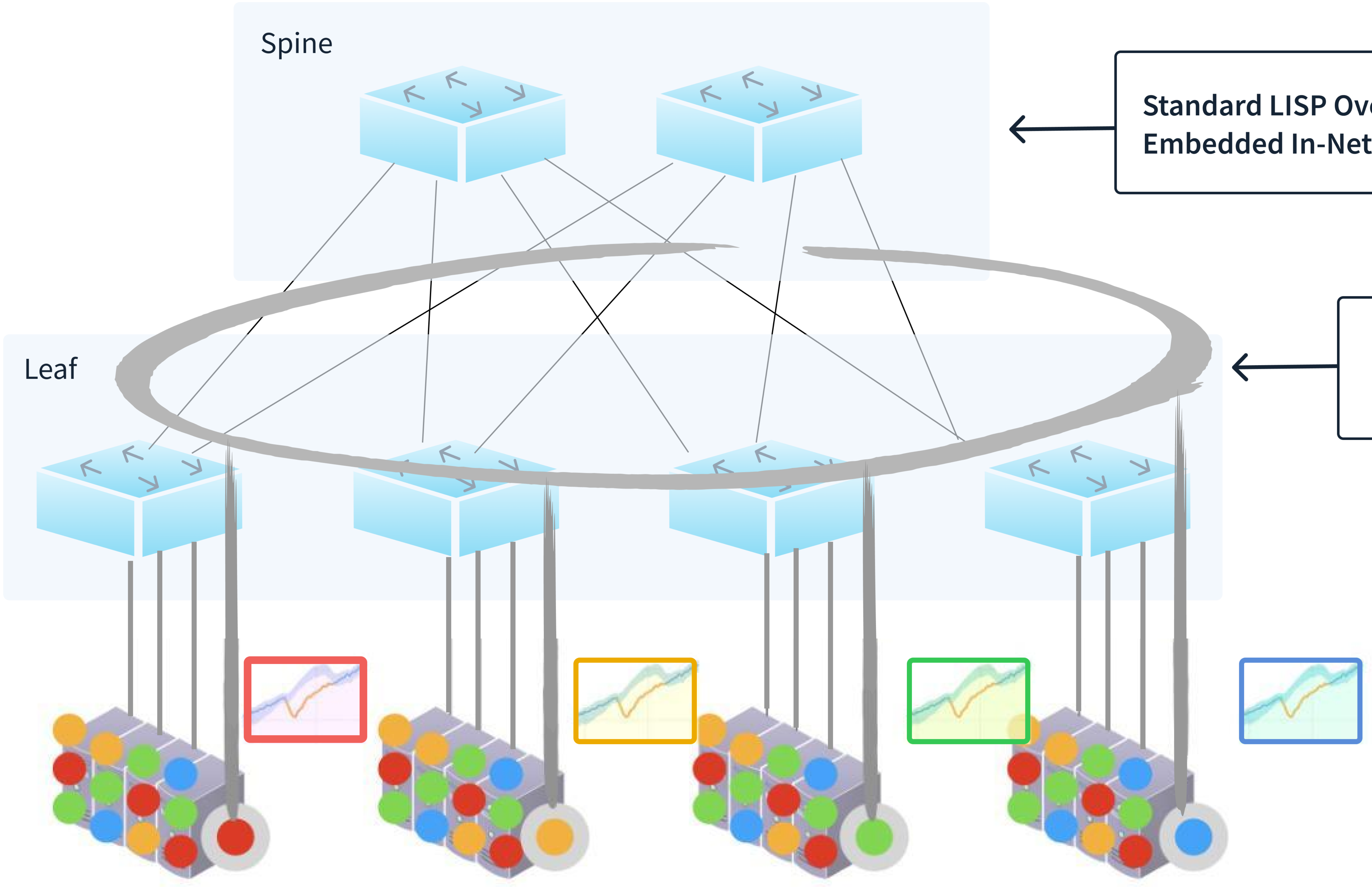
Logical IPFIX aggregation per application can Solve Uniform Sampling

App Samples Aggregated On Cyber CFN

Standard Sample Steering → Realtime Uniform Sample per App



IPFIX + LISP-FIX Algorithmic EID Steering Of Samples from Switch/Vswitch exporters



Standard LISP Overlay Embedded In-Network

EID Auto Encoders Detect Anomalies at Any Scale

Next-Gen Sampling Analysis

Normalized Uniform Small Samples per Application

- Latest AI technology can instantly detect anomalies
  - Based on <u>normalized uniform **small** samples</u> of application traffic.
  - Proven in Gbps size sites, municipalities, hospitals
  - Sampling simulations provides higher accuracy than probes

- **<u>We therefore:</u>**
  - Add LISP-CFN overlay to standard IPFIX sampling
  - LISP-FIX in switches steers built-in sampling export
  - Records are aggregated by dedicated encoders per app

Method	Un-norm 18	Kitsune [10]	Norm 18	Norm 12+18
Precision	0.28	0.43	0.58	0.51
Recall	0.40	0.11	0.38	0.60
F1 Score	0.33	0.17	0.45	0.55

Reducing 100Tbps to Tbps samples to Gbps partitions
Each partition is a uniform sample of the cloud native application

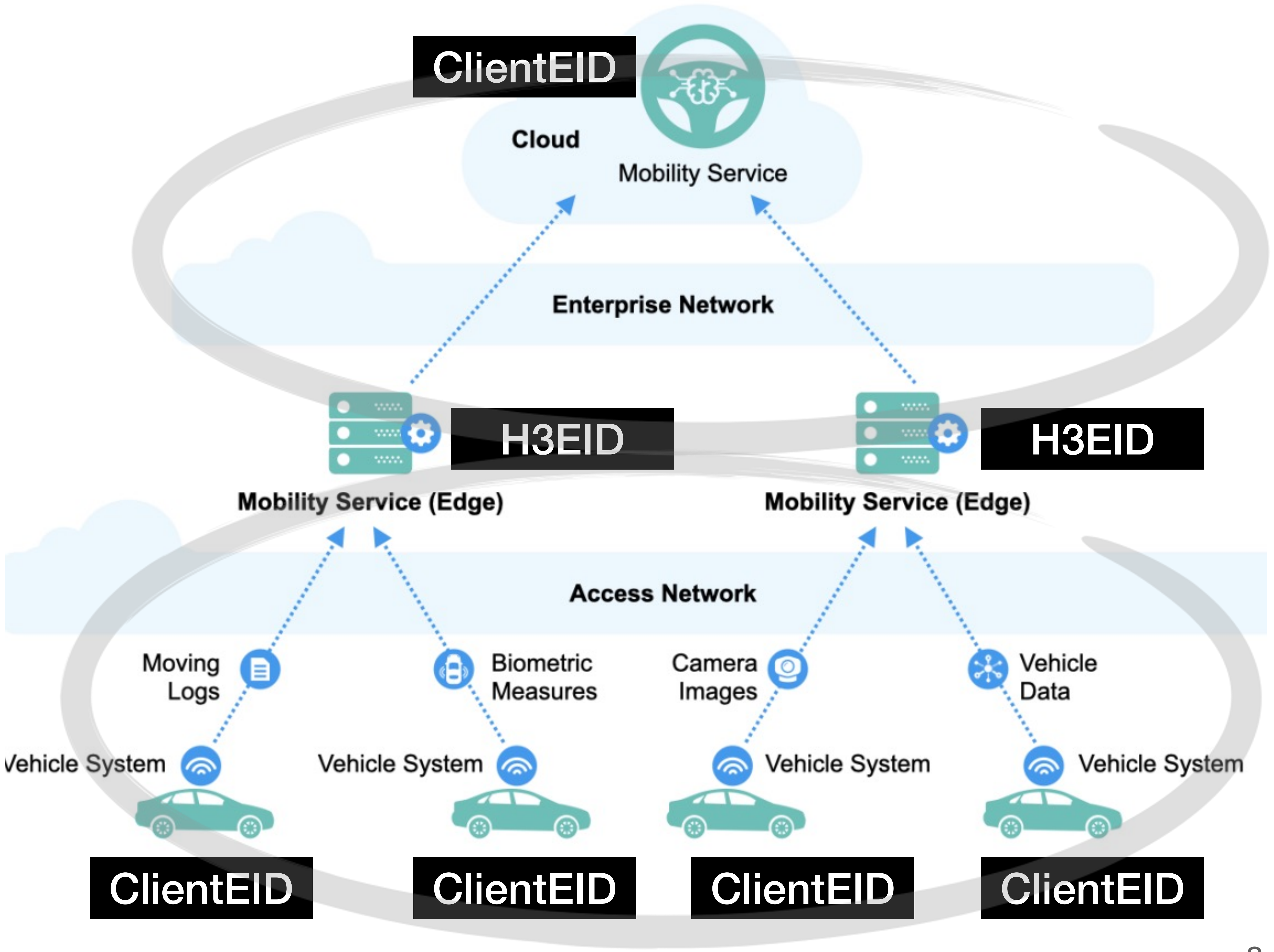
LISP-NEXAGON Parking Detection Deployment

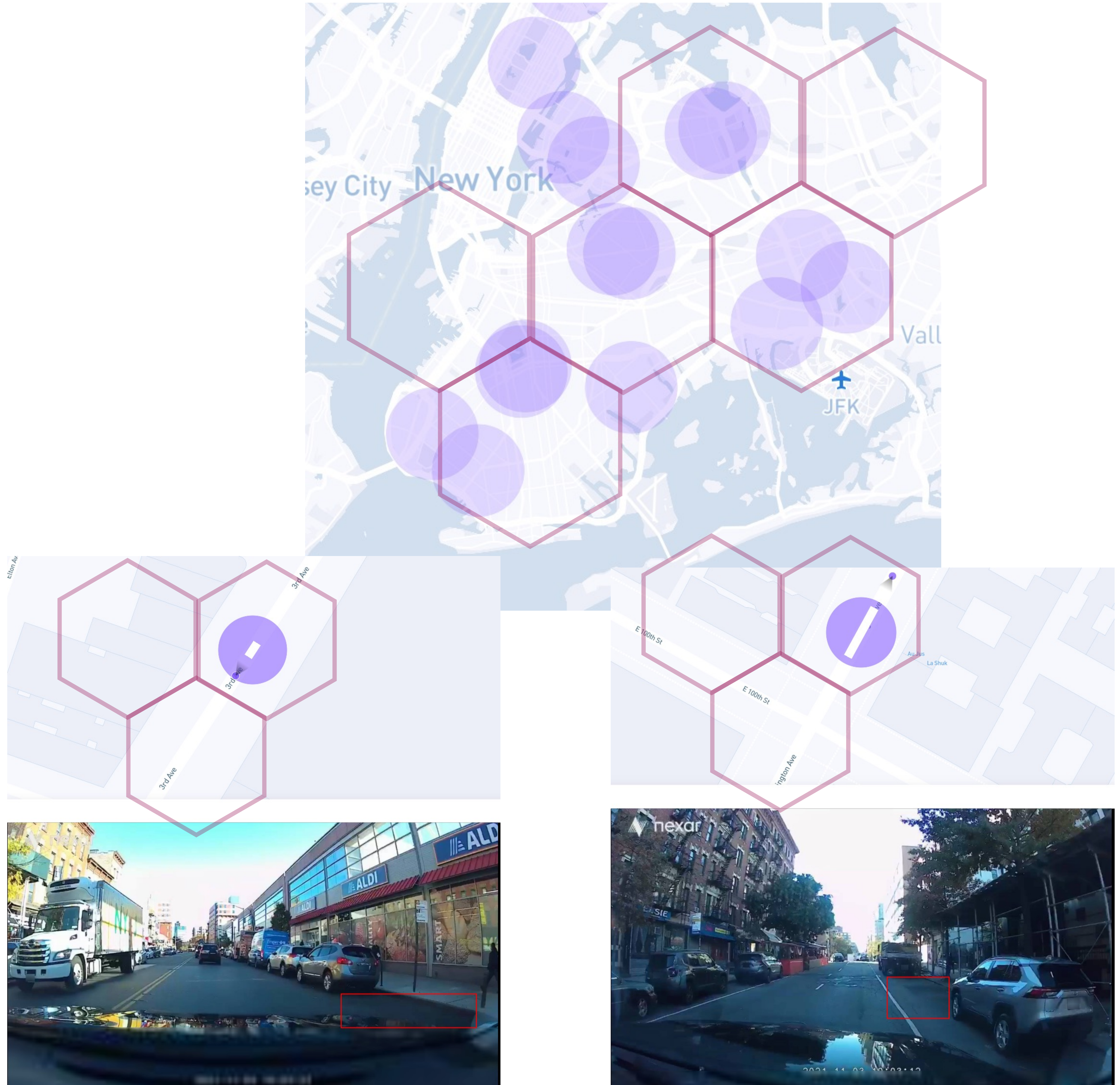
NYC Nexar, Tokyo AECC

Sharon Barkai

Scale & Spectrum of AECC Architecture

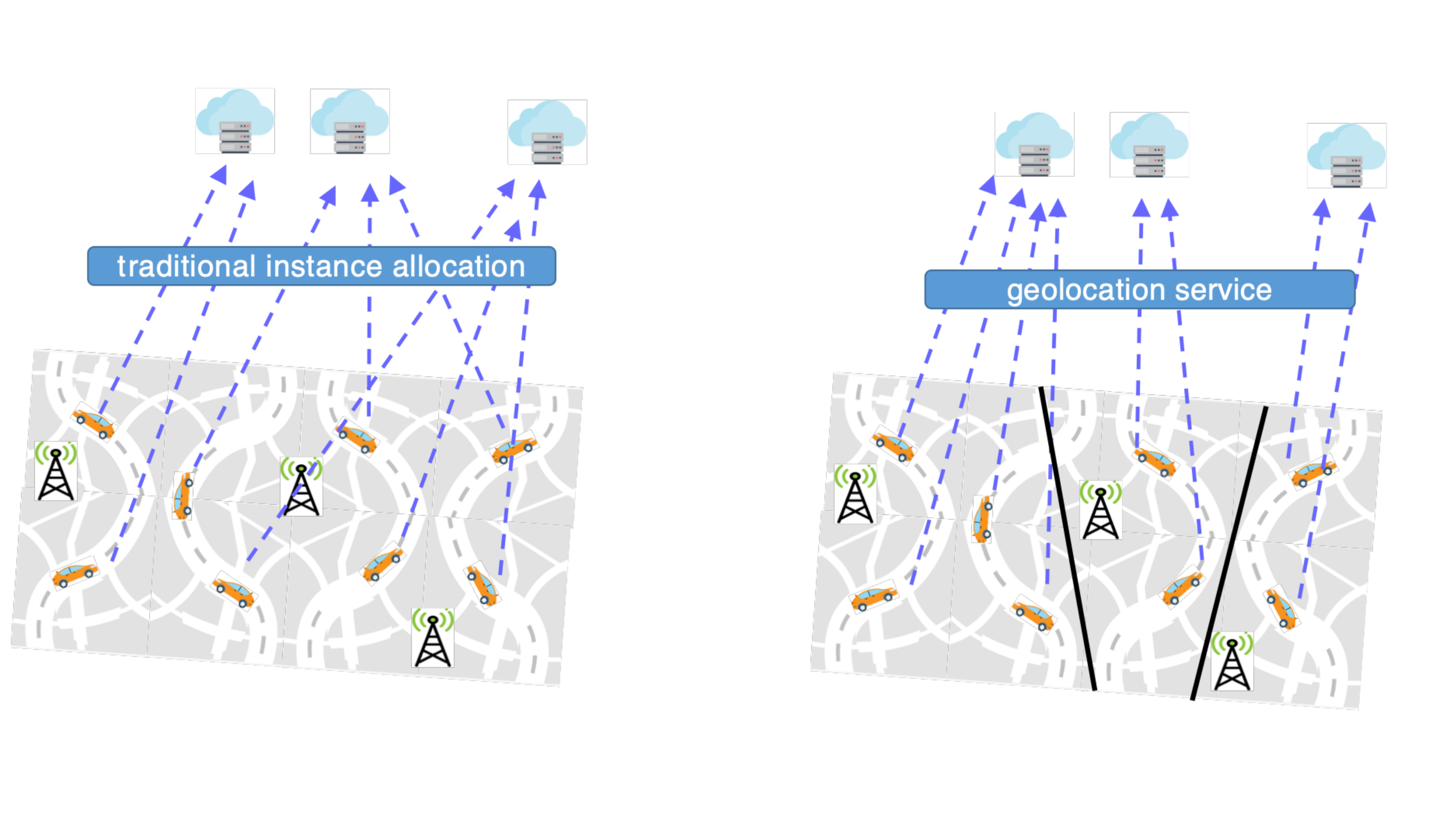
Using Hierarchy and Layering





The Geolocation Service Key-Issue

To Utilize a Geospatial Area: Vehicle-to-Service Uploads Are Consolidated



Non-Random Association Between Vehicles and Geolocation Service Instance

Client-Service association challenges:

1. Transparent re-resourcing per traffic density in Geolocation Service Area
2. Geoprivacy of vehicles uploading or subscribing to Geolocation Service
3. Seamless geospatial context-switching for vehicles while driving between areas
4. Identity preservation while toggling between carriers while in a service area

Solving Scale and Use-Case Spectrum

By Leveraging LISP Layering / LISP-Nexagon Hierarchy

<u>Crowd-Scaled Concurrency, Throughput, Latency</u>

- Uploads partitioned to H3EIDs, scale connected cars and coverage areas
- LISP Signal-Free Propagation form H3EIDs is O(changes) not O(uploads)
- Edges RLOCs pre-allocated per latency to mobile carriers IP Anchors

<u>Layering Protections</u>

- Transparent resource reallocation of H3EIDServices per road traffic (H3EID)
- Seamless geospatial context switching without mobile resolutions (H3EID)
- Multi-carrier ID preservation and IP geoprivacy of Vehicle systems (V-EID)

Thank You