IEEE NCA 2024

Platelet: Pioneering Security and Privacy Compliant Simulation for Intelligent Transportation Systems and V2X





Mathias Kautz

mathias.kautz@epita.fr

https://gitlab.com/Matk3z/platelet **Badis Hammi**

badis.hammi@telecom-sudparis.eu



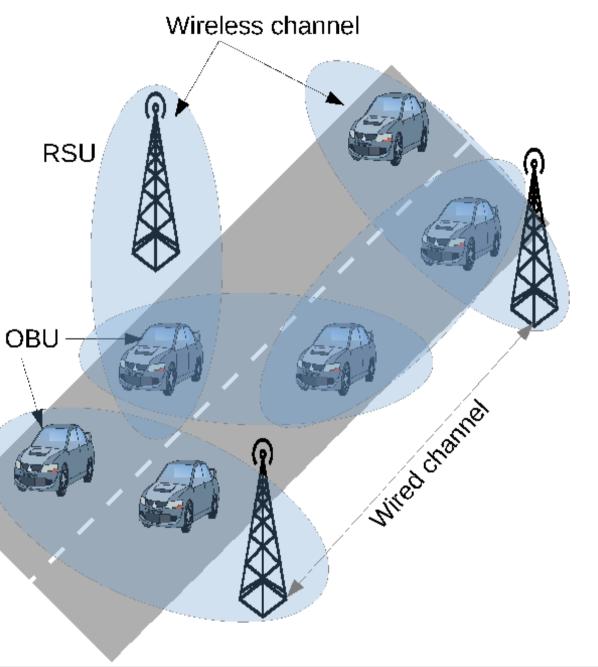
Joaquin Garcia-Alfaro

joaquin.garcia_alfaro@telecom-sudparis.eu

ITS (intelligent transportation system)

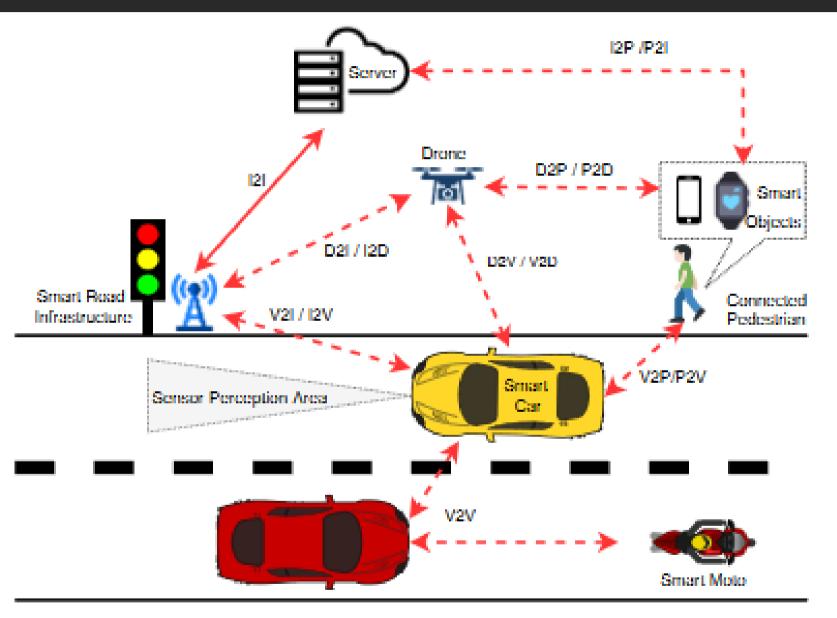
Applying new technologies to transport systems

In the context of a connected city, the presence of an inter-vehicular network is a central issue.



Simple VANET network schematic [1]

C-ITS Network



Advanced C-ITS network [3]

The network is made out of two types of nodes:

RSU nodes (road-side units)

OBU nodes (on-board units)

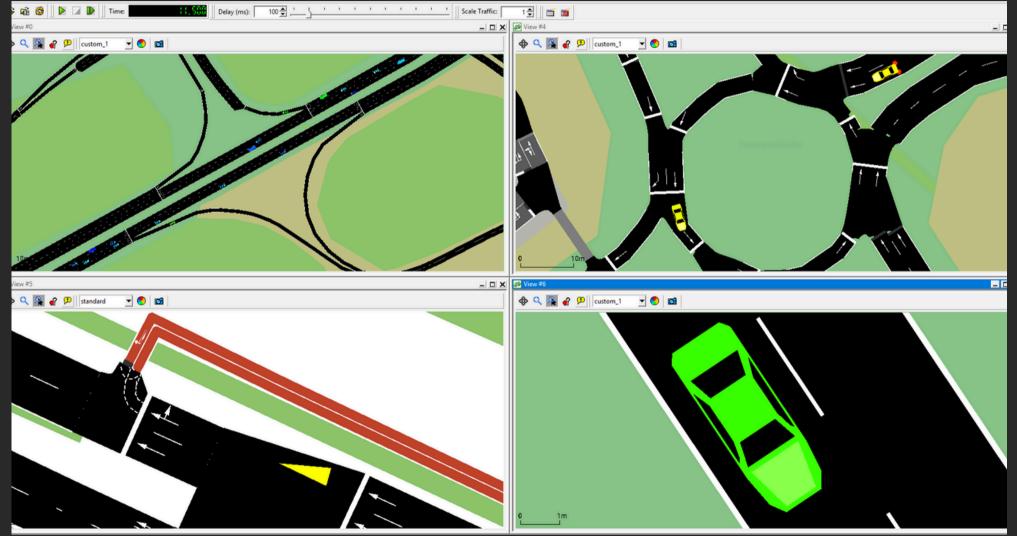
Initially **Ad Hoc**, recent solutions are increasingly based on **existing infrastructures** (cellular data, centralized servers, etc.).

V2X Network simulators

Testing on road = too expensive

Simulators are available to test these solutions in a digital environment.

Firms use **closed source** simulator but academic researchers needs **open source** simulators



SUMO simulation screen capture



State of the art

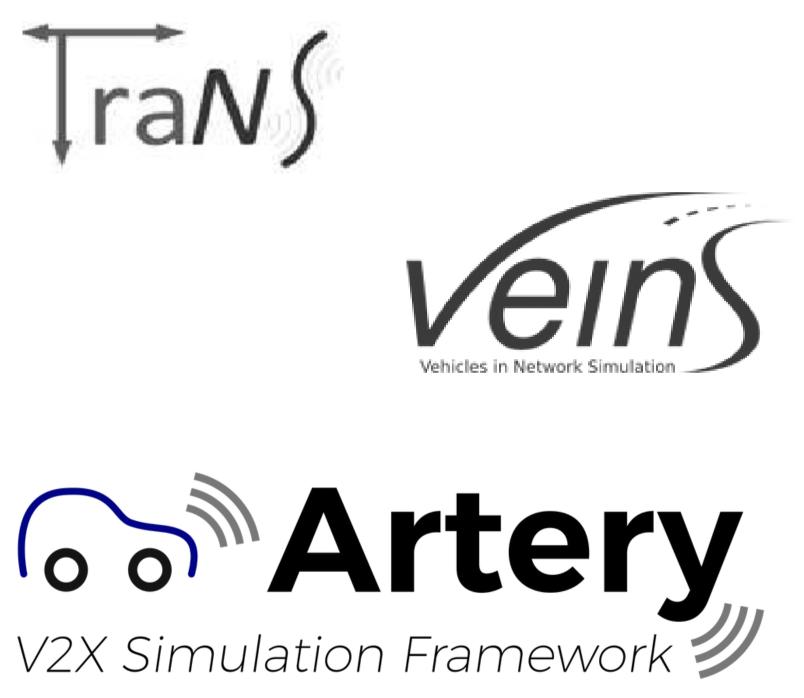
Many simulators exists but most are **ancient** and made for **older needs** of V2X network

The most recent simulator implementing the ETSI standard are **Artery and iTetris**

Artery and iTetris:

- Pros: most **efficient** platform to run ETSI simulators
- Cons: still lack consideration for **privacy** and security

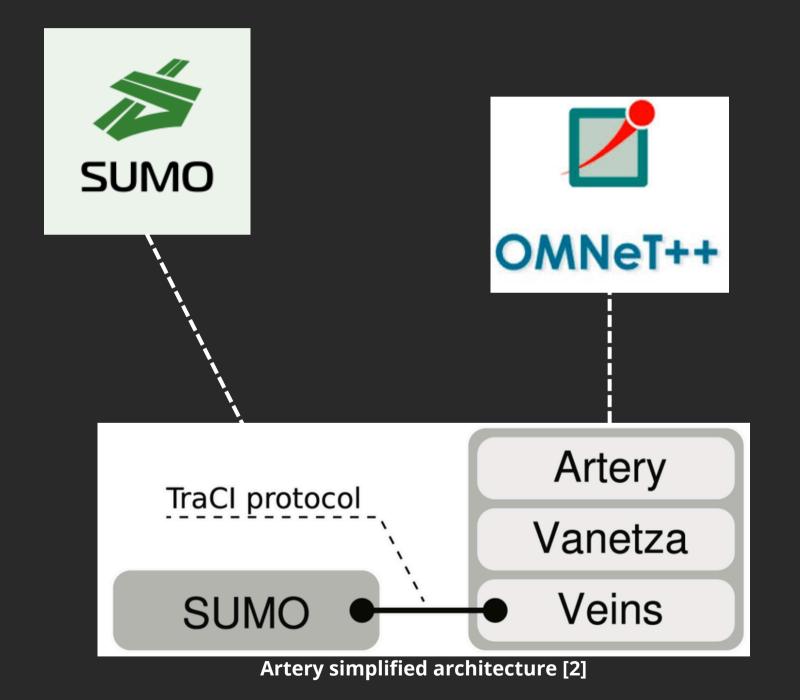




State of the art

| Simulator | Traffic simulation | Network simulation | ETSI- compliant | IEEE- compliant | 5G and Beyond compatible | Signature implemen- tation | Certificate renewal | pcap logging | EC and PC implemen- tation | Certificate pool imple- mentation |
|-----------|---|---|--|---|--|---|--|---|---|---|
| TraNS | Image: A set of the set of the | ✓ | × | × | × | × | × | × | × | × |
| GrooveSim | 1 | Image: A set of the set of the | × | Image: A set of the set of the | × | × | × | × | × | × |
| iTETRIS | Image: A set of the set of the | Image: A set of the set of the | Image: A set of the set of the | × | Image: A set of the set of the | × | × | × | × | × |
| Veins | Image: A set of the set of the | Image: A set of the set of the | × | Image: A set of the set of the | Image: A second s | × | × | × | × | × |
| Artery | Image: A set of the set of the | Image: A set of the set of the | Image: A set of the set of the | × | Image: A set of the set of the | Image: A set of the set of the | × | × | Image: A set of the set of the | × |
| Platelet | Image: A set of the set of the | ✓ | Image: A second s | × | Image: A set of the set of the | Image: A set of the set of the | Image: A second s | Image: A set of the set of the | Image: A set of the set of the | Image: A set of the set of the |

Artery's architecture



- Omnetpp: Network simulator
- SUMO: Traffic simulator
- Vanetza: Library implementing the ETSI standard used heavily inside Artery and Platelet

Based on SUMO and Omnetpp Most advanced ETSI based ITS simulator

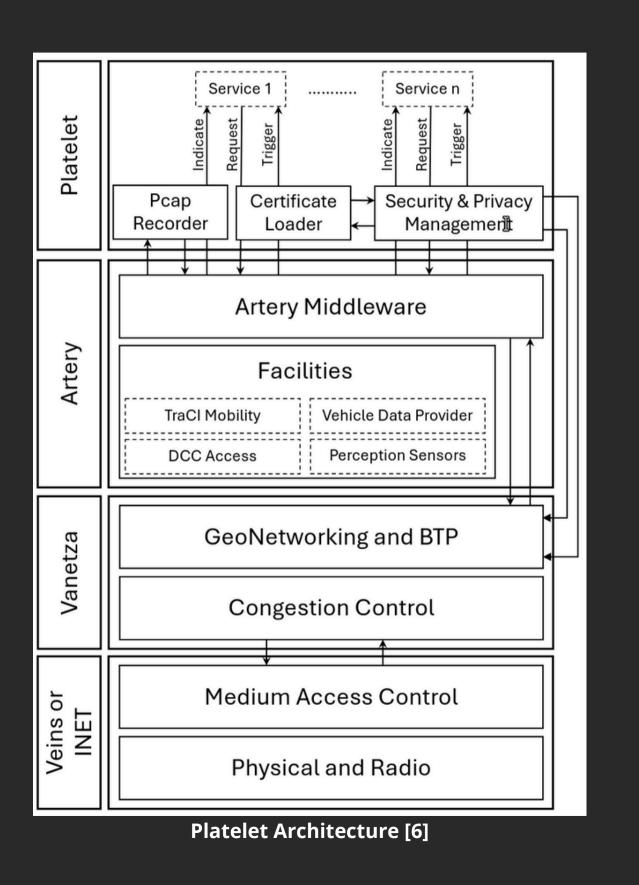
Platelet

First simulator to implement proper security and privacy management

Two new components:

- to send secured messages

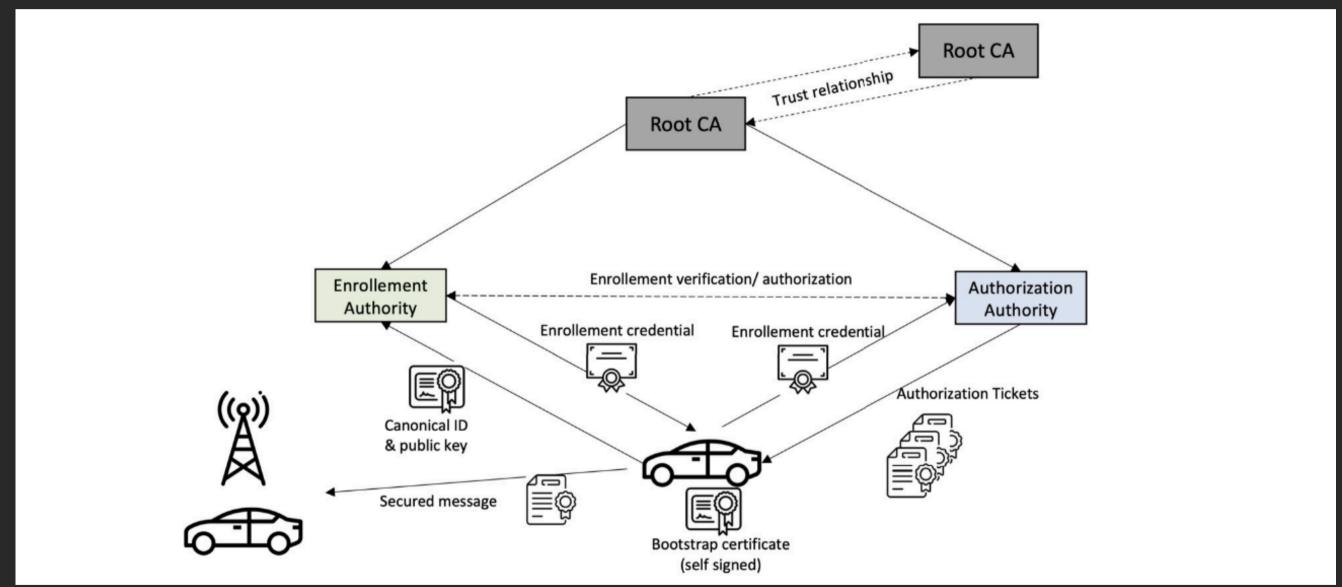
A **fully integrated** standalone app to manage secured scenarios



• A pcap recorder allowing for easier verification of completed scenarios

• A proper **certificate loader** allowing vehicles

PKI, security and privacy managment



Generic ETSI PKI architecture [12]

StaticCertificateLoader

Artery has no certificate loading module

This Loader works by loading a stack of pre generated certificate and distributing them during the simulation

Checks the authenticity and integrity of the certificate while loading it







PcapItsRecorder

Pcap: packet recording file format

There was **no recorder** previously in the project

Thanksfully! A **packet reader** exists inside wireshark

| | | | | Ľ | Intitleo | i - sp | 9-1 | - Inv | estig | jati |
|--------------|--------------------|----------------|---------------|------------|----------|----------|------|----------|----------|------|
| e | sp9-1 | ٢ | admir | . ~ | | | | | | |
| Wiresh | nark | Pivot | from I | Pan | oran | na | | | | |
| Eile I | diti | ew <u>G</u> | o <u>C</u> ap | ture | Ana | alyz | e | Stat | istic | s |
| | | ۲ | | | X | 6 | 9 | • | (| |
| l !(er | f.types. | type = | = MET/ | N) | | | | | | |
| No. | Tim | e | | | | | | Sou | rce | |
| | 5 202 | | | | | | | | | |
| | 5 202 | | | | | | | | | |
| | 5 202 | | | | | | | | | |
| | 5 202 5 202 | | | | | | | | | |
| 136 | 5 202 | 0-03-1 | 1 00:4 | 15:2 | 5.213 | 057 | 7 | 10. | 9.1 | 31 |
| 136 | 5 202 | 0-03-1 | 1 00:4 | 15:25 | 5.213 | 059 | 9_ | 10. | 9.3 | 7. |
| 136 | 5 202 5 202 | 0-03-1 | 1 00:4 | 15:25 | 5.213 | 060 | 0 | 10. | 9.3 | 7. |
| 136 | 5 202 | 0-03-1 | 1 00:4 | 15:25 | 5.213 | 060 | θ | 10. | 9.6 | 5. |
| | 5 202 | | | | | | | | | |
| | 5 202 | | | | | | | | | |
| 136 | 5 202 | 0-03-1 | 1 00:4 | 15:2: | 5.213 | 001 | 4 | 10. | 9.1 | .31 |
| | ne 1: 6 | | | | e (4 | 872 | bit | ts), | 66 | 99 |
| | ensible | | | | 1.04 | | 0.5 | 107 | | |
| | ernet I .10 Vir | | | | | | | | | |
| ▶ 802 | 10 Vin | tual | LAN, P | RI: | 0, DI | ET: | 0. | ID: | 14 | 1 |
| ▶ Inte | ernet F | rotoc | ol Ver | sion | 4, 5 | Src | : 10 | 9.9. | 68. | . 6 |
| | nsmissi | | | | | | | | | |
| | BIOS Se | | | | | | | | | |
| SMB2 | 2 (Serv | er Me | ssage | Bloc | k Pro | oto | col | ver | rsid | on |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| 0000 | | c5 04 00 0e | | | | 01 02 | | | 05 46 | |
| 0010 | | 0a 09 | | | | 44 | | e5 | | |
| 0030 | 9b ac | 3c 22 | 7b 54 | 88 | 18 | 21 | d8 | bc | 68 | 0 |
| 0040 | | dd 5f | | | | 81 | | 00 | | |
| 0050 | | 40 00 | | | | 00 | | 01 | | |
| 0060 | | 00 00 | | | 00 | | | 00 00 | | |
| 0080 | | 00 00 | | | | 00 | | 00 | 00 | θ |
| 0090 | 00 01 | 01 00 | 00 00 | 00 | 00 | 00 | 00 | 58 | 00 | b |
| 0000 | | 00 00 | | | | | | | 82 | |
| 00b0 00c0 | 0a 01 53 50 | 01 a2 00 03 | 82 0 | | | | | 8e 00 | | |
| 0000 | | 00 9e | | | | 00 | | 00 | | |
| 00e0 | | 00 68 | | | | | | 00 | | |
| 0 🛛 | wires | hark_U | ntitled | 64a6 | 583ad | r-dd | b9- | 4a1 | 3-b | 16 |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | 0 Er | ndi |

11

Wireshark interface

e Technology Ltd. EndaceVision™ is a trademark of Endace Technology Ltd. Wireshark® is a trademark of the Wireshark Foundation.

| Dst: 10.9.68.247 53, Dst Port: 445, Seq: 1, Ack: 1, Len: 531 | | |
|---|--|------------------|
| 2) | | |
| | | |
| | | |
| | | |
| | | |
| 00.03.00 | | |
| 00 01 90 ····a·· 00 20 06 ·····E··G4F@·· | | |
| bd 22 ea ·\··D··· D····"· | | |
| 00 01 01 ···<"{X·· !··h···· | | |
| 0f fe 53 VS | | |
| 00 00 00 MB@ | | |
| 00 41 ca ······A· | | |
| 00 00 00 ·····a· ···· | | |
| 00 19 00 | | |
| 01 00 00 ······ | | |
| af a0 030 | | |
| 4 4 5 4 5 4 5 4 5 4 5 5 4 5 5 5 5 5 5 5 | | |
| 00000e0 SP····· | | |
| 0 00 00 10 ···h···· v··· | | |
| | | Y |
| i-06f2ba9be1b3.pcap_20200430210728_DHwFdW.pcap | Packets: 136558 · Displayed: 136558 (100.0%) | Profile: Default |

| ۲ | | २ 🔍 🎹 | |
|----------|-------------------------|-------------|---|
| | | | Expression + |
| | Destination | Protocol | Length Info |
| 130.154 | 10.9.130.12 | SSL | 1514 Continuation Data |
| 17.7 | 10.9.17.158 | TCP | 78 56618 → 443 [ACK] Seq=1 Ack=33936 Win=64668 Len=0 TSval=380779482 TSecr=38076… 🚃 |
| 17.198 | 10.9.17.6 | TCP | 1514 80 → 51623 [PSH, ACK] Seq=61220 Ack=1 Win=7228 Len=1436 TSval=380779479 TSecr |
| 34.170 | 10.9.34.6 | TCP | 1514 80 → 32993 [PSH, ACK] Seq=53133 Ack=1 Win=7228 Len=1436 TSval=4195746565 TSec |
| 66.162 | 10.9.66.4 | TCP | 1514 80 → 50884 [PSH, ACK] Seq=10053 Ack=1 Win=7228 Len=1436 TSval=3715746337 TSec |
| 131.167 | 10.9.131.13 | TCP | 1514 80 → 60887 [PSH, ACK] Seq=22977 Ack=1 Win=7228 Len=1436 TSval=3235746081 TSec |
| 37.5 | 10.9.37.196 | TCP | 78 49772 → 443 [ACK] Seq=1 Ack=87068 Win=64668 Len=0 TSval=4195746576 TSecr=4195 |
| 37.7 | 10.9.37.200 | TCP | 78 [TCP Dup ACK 136383#5] 34509 - 443 [ACK] Seq=1 Ack=31593 Win=64668 Len=0 TSva |
| 65.176 | 10.9.65.11 | TCP | 1514 80 → 55786 [PSH, ACK] Seq=25320 Ack=1 Win=7228 Len=1436 TSval=3715746347 TSec |
| 18.12 | 10.9.18.204 | TCP | 78 46572 → 80 [ACK] Seq=1 Ack=33936 Win=64668 Len=0 TSval=380779503 TSecr=380771 |
| 37.13 | 10.9.37.159 | TCP | 78 57036 → 8313 [ACK] Seq=1 Ack=4309 Win=64668 Len=0 TSval=4195746589 TSecr=4195… 💳 |
| 131.167 | 10.9.131.13 | TCP | 1514 80 → 60887 [PSH, ACK] Seq=24413 Ack=1 Win=7228 Len=1436 TSval=3235746091 TSec… |
| 09 bytes | captured (4872 bits) on | interface 1 | |

Untitled - sp9-1 - Wireshark - Endace Vision^{TI}

Investigations

& Wireshark Profile |44 Previous 100 MB Next 100 M

Manager

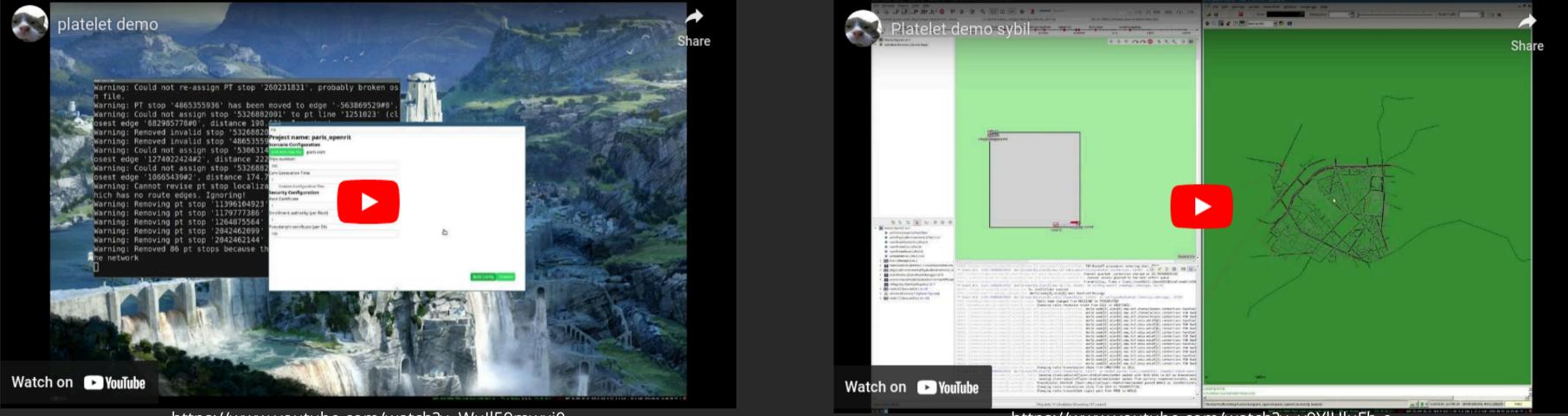
• •

Telephony Wireless Tools Help

ion - Endace Vision™

ſ

Demo



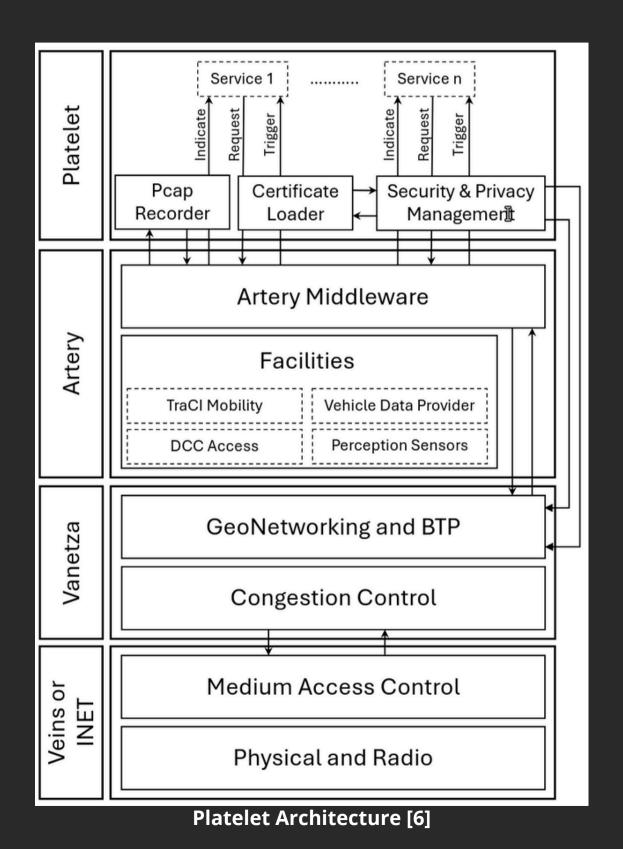
https://www.youtube.com/watch?v=Wull59mwxi0

https://gitlab.com/Matk3z/platelet

https://www.youtube.com/watch?v=v9YlUluFh-o

12

To conclude



There was no simulator implementing **security** and **privacy** management allowing for unrealistic scenarios

Platelet allow for **secured** scenarios simulation and provides more component to **facilitate** it

To make researcher's life **easier** we centralized tools in a single **GUI app**

Bibliography

 Mukesh Saini, Abdulhameed Alelaiwi, Mathias K, Badis H, Joaquin G, 2024, Platelet: ightarrowAbdulmotaleb El Saddik, 2015, How Close are Pioneering Security and Privacy We to Realizing a Pragmatic VANET Solution? Compliant Simulation for Intelligent Transportation Systems and V2X A Meta-Survey

- R. Riebl, H. Gunther, Christian Facchi, L. Wolf, ightarrow2015, Artery: Extending Veins for VANET applications ullet
- Badis H, Jean-Philippe M, Jonathan P, 2022, PKIs in C-ITS: Security functions, architectures and projects: A survey
- Agachai S, H.W. Ho, 2017, Smarter and more ightarrowconnected: Future intelligent transportation system
- Jonathan P, Florian S, Michael F and Frank K, 2014, Pseudonym Schemes in Vehicular Networks: A survey

- - Artery Documentation, http://artery.v2xresearch.eu/
- Omnet++ documentation, https://omnetpp.org/ documentation/
 - Vanetza documentation, https://
 - Institut européen des normes de Institut européen des normes de Institut européen des normes de
 - télécommunications, ETSI TS 103 096 télécommunications, ETSI EN 302 637-2 télécommunications, ETSI TS 102 940 14

www.vanetza.org/