An Artificial Intelligence Framework for Addressing Cybersecurity Challenges in 5G-leveraged CAVs ecosystem

Center for Research & Technology Hellas (CERTH)

Information Technologies Institute (ITI)

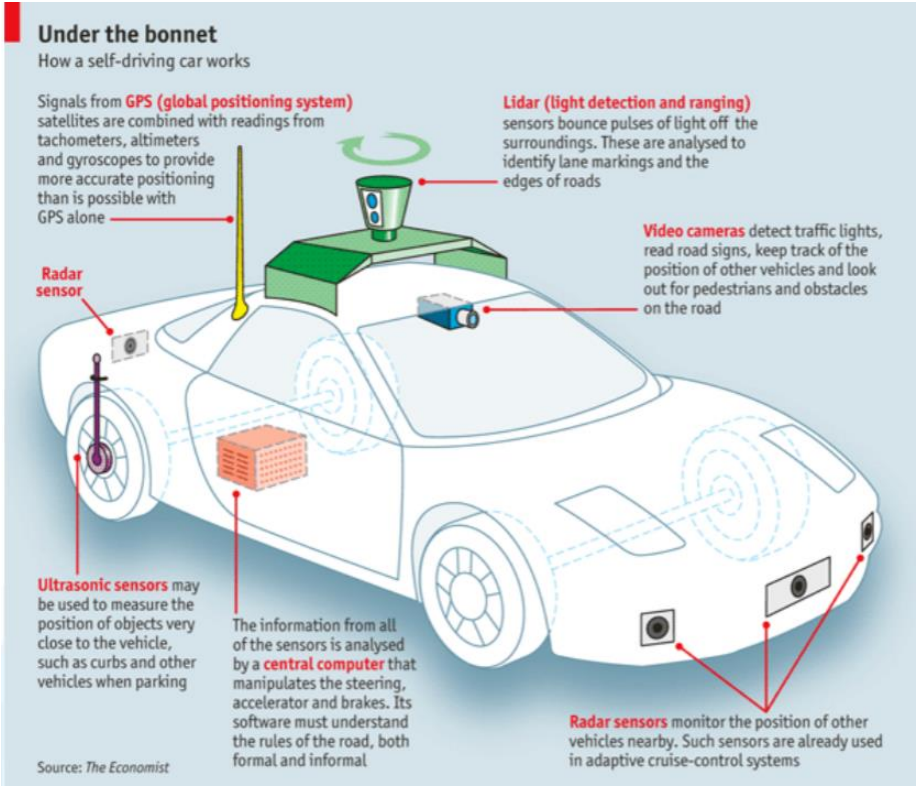
Dr. Antonios Lalas
Postdoctoral Researcher
Tel. : +30-2311-257779
E-mail : lalas@iti.gr
Web: www.iti.gr

Dr. Konstantinos Votis
CERTH/ITI Researcher Grade B'
Tel. : +30-2311-257722
E-mail : kvotis@iti.gr
Web: www.iti.gr

Presentation Outline

- Motivation & Objectives
- Cybersecurity challenges
  - Information Sharing — Intrusion Detection — Penetration Testing — Attack Mitigation
- 5G-enabled CAVs ecosystem
  - AVENUE — Autonomous Vehicles to Evolve to a New Urban Experience
  - nIoVe — A novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles
  - SHOW — SHared automation Operating models for Worldwide adoption
  - 5G-ROUTES — 5G connected and automated mobility cross-border EU trials
- Cybersecurity in 5G Connectivity
  - SANCUS — Analysis Software Scheme of Uniform Statistical Sampling, Audit and Defence Processes
- Artificial Intelligence Framework
- Future Perspectives

Ecosystem of Autonomous Vehicles



Multiple sensors

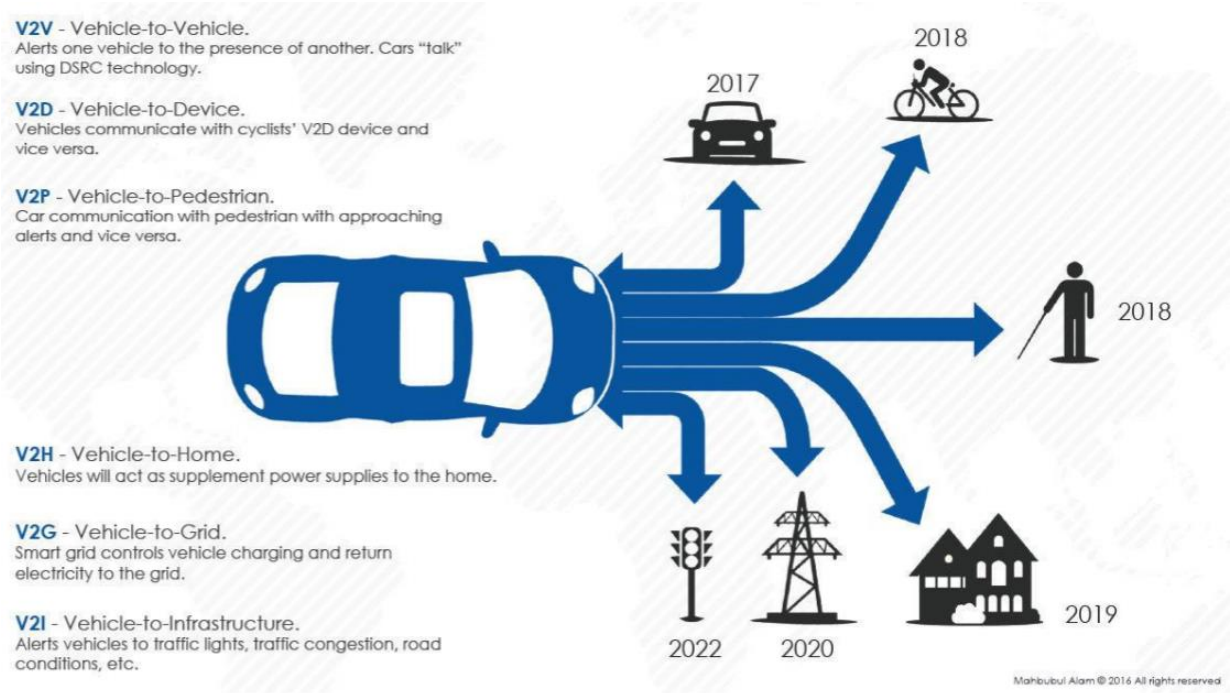
- ❑ Global Positioning System (GPS)
- ❑ Light Detection and Ranging
- ❑ (LIDAR)
- ❑ Cameras (Video)
- ❑ Ultrasonic Sensors
- ❑ Central Computer
- ❑ Radar Sensors
- ❑ Dedicated Short-Range
- ❑ Communications-Based Receiver

IoV ecosystem

Heterogeneous network architecture of IoV ecosystem includes many types of vehicular communications:

- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I)
- Vehicle-to-Network (V2N)
- Vehicle-to-Pedestrian (V2P), etc.

Automotive Technology V2X



Next Generation Dedicated Short Range Communications (DSRC) for Intelligent Transportation Systems (ITS) Vehicle Safety & Operations

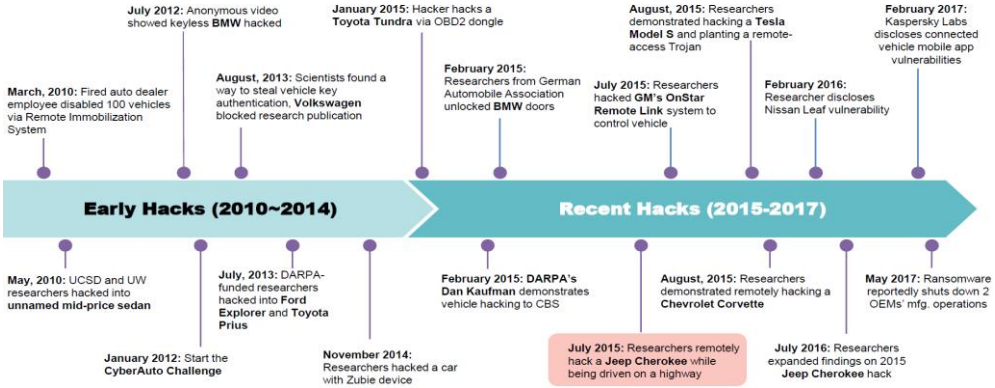
Motivation & Objectives

Today's vehicles are increasingly "connected"; there is wireless data exchange with servers, infrastructure and other vehicles.

> ***There is not*** *a dedicated scientific field studying the protection of Connected and Autonomous Vehicles (CAVs) against cyber-attacks and thus, the respective research endeavours are limited.*

*Over **85% of all new cars are already classed as connected**, and by 2025 there will be over 470 million connected vehicles on the roads in Europe, the USA and China alone.*

Attacks on automobile systems are **expected to increase rapidly** in the following years due to the rapid increase in connected automobile hardware & software without foundational cybersecurity principles.



Motivation & Objectives

5G networks will enable **enhanced mobile broadband (eMBB) services** – with higher data rates, lower latency, and more capacity – as well as new use cases that will generate additional revenue streams for operators.

Cellular Vehicle to Everything or C-V2X is intended to thoroughly make a 5G vehicle a part of the environment around it, making it capable of reacting to events.

Attacks on 5G infrastructure are **expected to increase rapidly** in the following years as well.

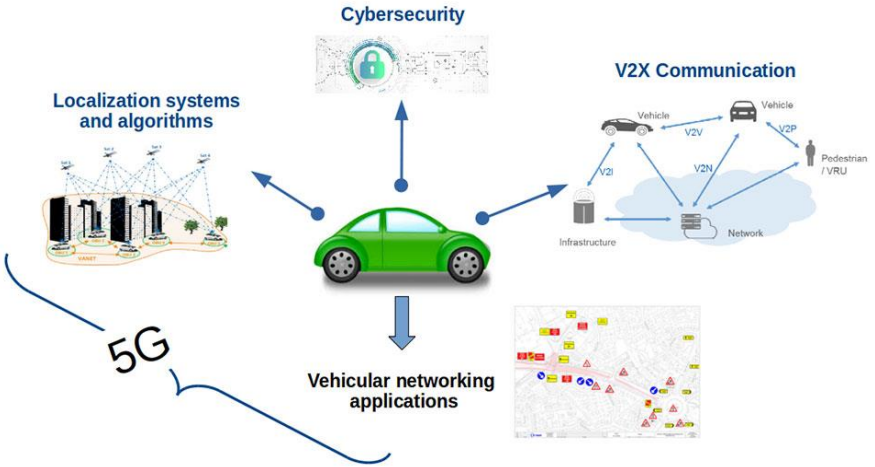
Motivation & Objectives

Motivation:

- The **cyber-protection of CAVs** is of paramount importance and appropriate tools are **urgently required**.
- **Artificial Intelligence** (AI) can effectively provide robust solutions shielding CAVs and associated 5G networks.

Objectives:

- Present the **cybersecurity challenges** in 5G-leveraged CAVs ecosystem
- Explore solutions towards a **holistic AI-enabled cybersecurity** framework

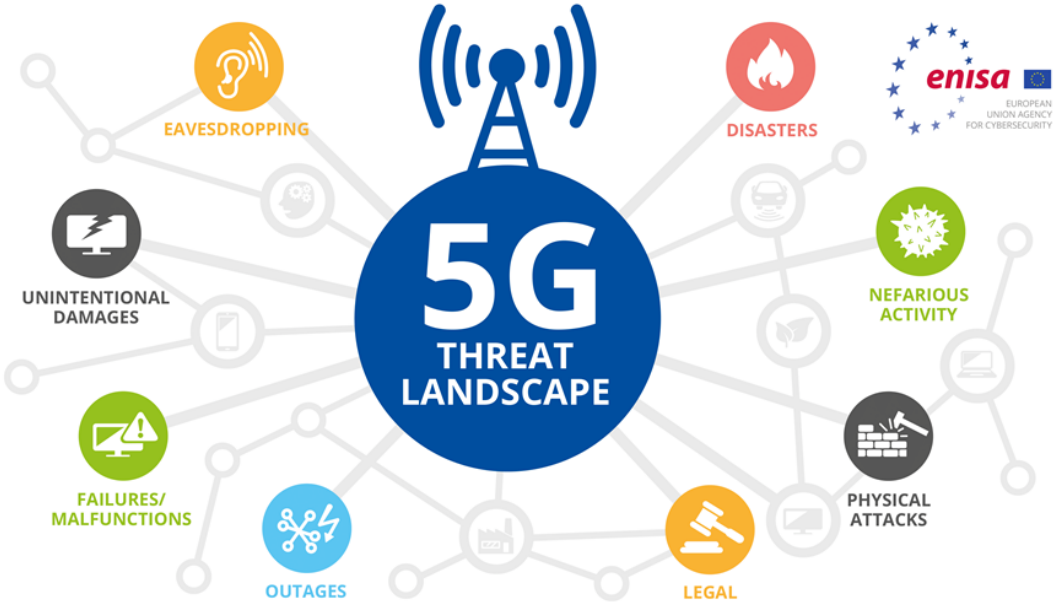


Cybersecurity Challenges

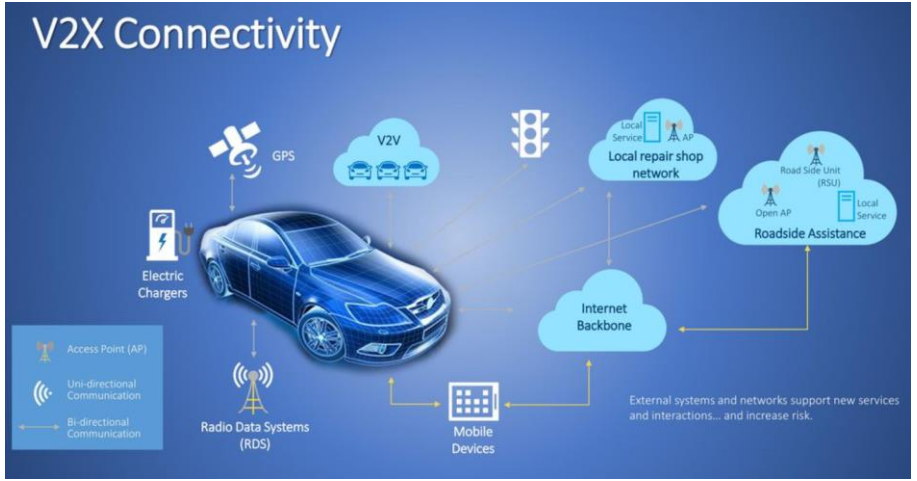
- Low level sensors essential for correct functioning of vehicle core components such as positioning, inertial measurements, engine control, tyre pressure monitoring, light detection and ranging, infrared vision systems etc.

<u>Attack vectors:</u>

- GPS spoofing
- GPS jamming
- DDoS on Engine Control Unit (ECU)
- packet injections to TPMS
- jamming and spoofing of LiDAR sensors' **data.**



Connection Infrastructure



Traditional cyber-attacks

- DoS/DDoS
- Phishing and Ransomware
- Rogue updates and Password and key attacks.

Connectivity specific attacks

- *physical access attacks* on OBD port or media systems
- *close proximity attacks* on keyless entry and ignition systems or signal jamming
- *remote access attacks* through radio or cellular channels

Defense Mechanisms

- Identification of knowledge gaps
- Resilience
  - Early security by design
  - R&D of cyber protective measurements
  - Monitoring
- Response
  - Development of response strategy
  - (cross border) Incident sharing
  - Fall back and recovery procedures

- Information Sharing
- Intrusion Detection
- Penetration Testing
- Attack Mitigation

CERTH/ITI In-Vehicle Services

Fleet Management

Simulation

Environment assessment

AVENUE

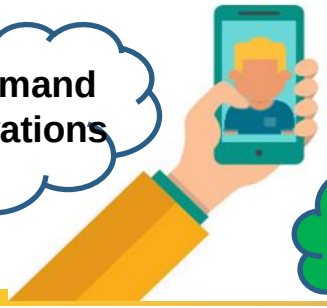
Temperature
Smoke & Dust
ENVIRONMENTAL SENSORS
Fog & Humidity
CO_2 $PM_{2.5}$
NO_2 PM_{10}
VOCs

Security & Trust

Passenger Counting

Smart Feedback

On Demand Reservations



Follow my Kid

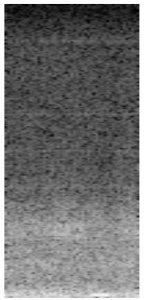
Operator cockpit Services

Real-time In-vehicle inspection

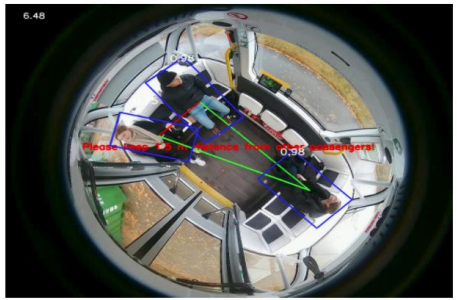
Link to Demo Video

In-vehicle security and environmental assessment

Enhance the sense of security and trust



Automated passenger presence



Follow my kid

Video Modality Status

No abnormal events are detected

Audio Modality Status

Background Noise

Event History

Video modality detected Fighting	11/23/2021 20:40:12
Video modality detected Fighting	11/23/2021 20:40:09
Video modality detected Fighting	11/23/2021 20:40:09
Video modality detected Fighting	11/23/2021 20:40:08
Video modality detected Fighting	11/23/2021 20:40:08

Automated Passenger Presence

Onboard passengers	3
Door status	-
Distance assessment	Unsafe

Environmental

AQI	45	Temperature	15.22°C
Humidity	74.77%	CO2	1361 ppm
VOC	20403 ppm	PM25	10 ppm

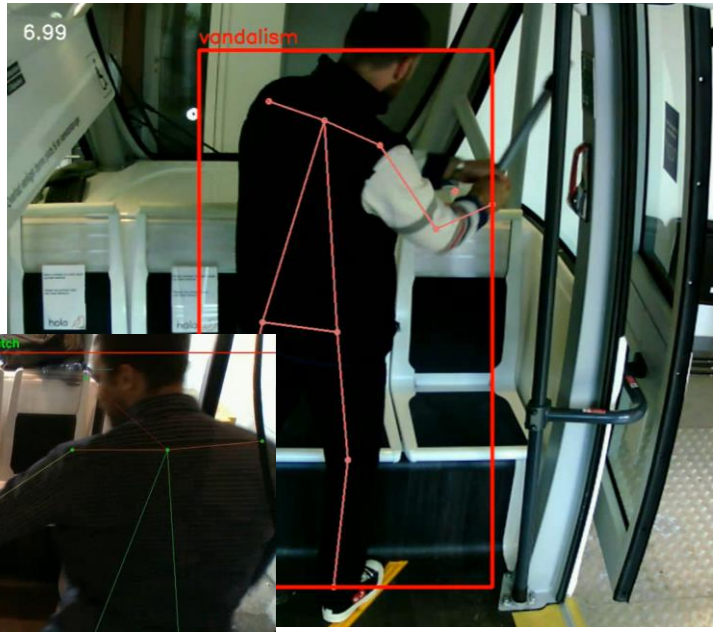
Follow My Kid Database

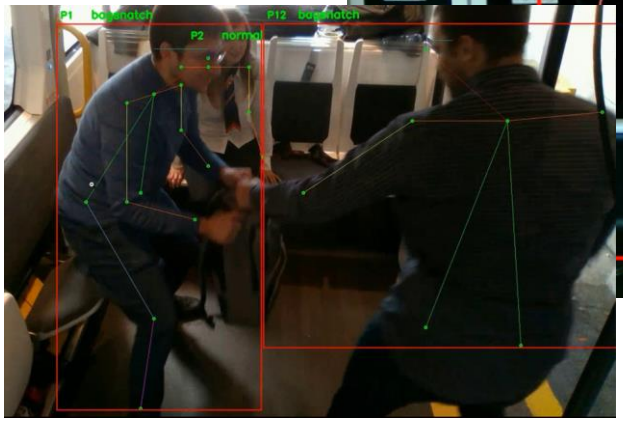
In-Vehicle Services

Enhance the sense of security and trust

- **Real-time** petty crime and abnormal event **detection**
- Red boxes indicate an **abnormal event**
- The **notification** is sent to the operator
- **Video and audio** AI-based analysis
- **5G-enabled live-streaming** if required

Deployed in Copenhagen and Geneva





Vandalism

Bag snatching

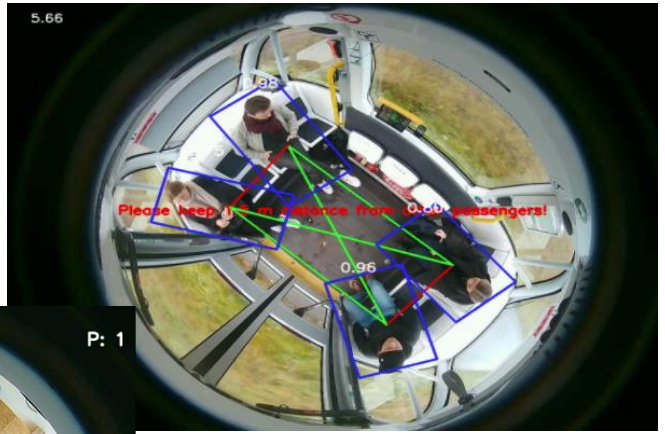
In-Vehicle Services

Automated passenger presence

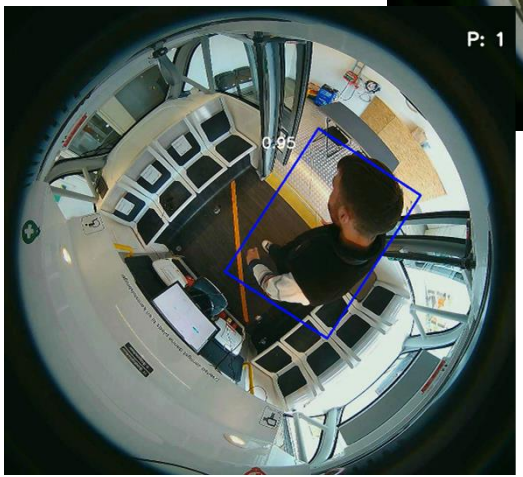
- Accurate **detection** of **passengers**
- High accuracy **proximity assessment** for new **COVID-19 regulations**
- Improved the inference time using TRT models (**250% increase** in performance)
- Red lines indicate **short distance**

Deployed in Copenhagen and Geneva

AVENUE



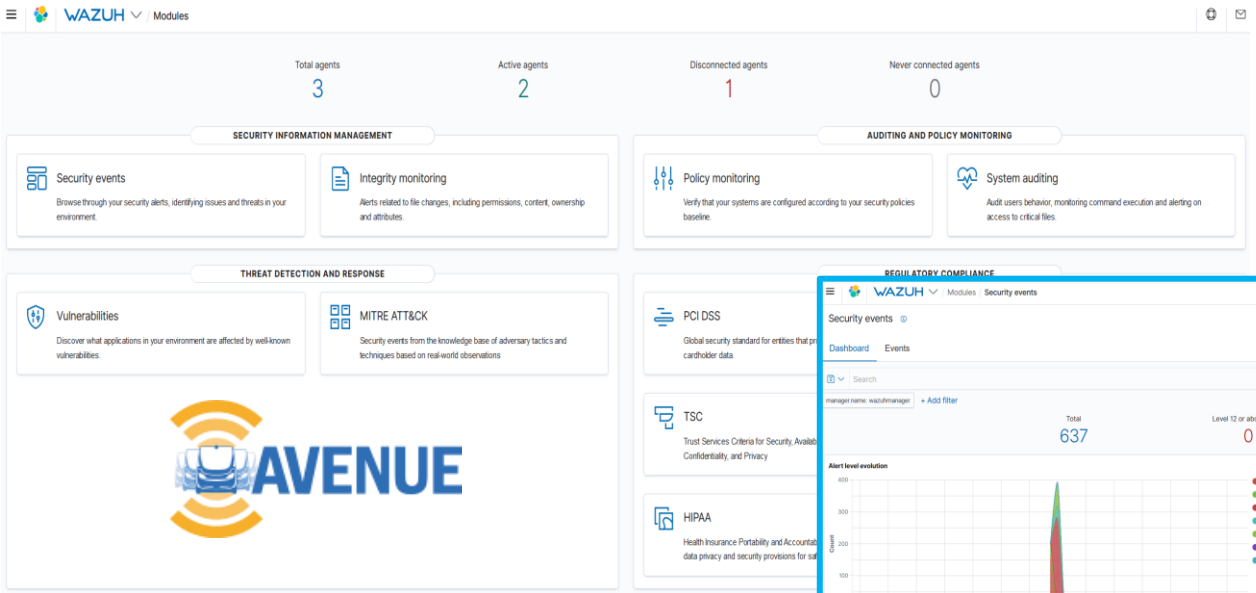
Proximity Assessment



Passenger Counting

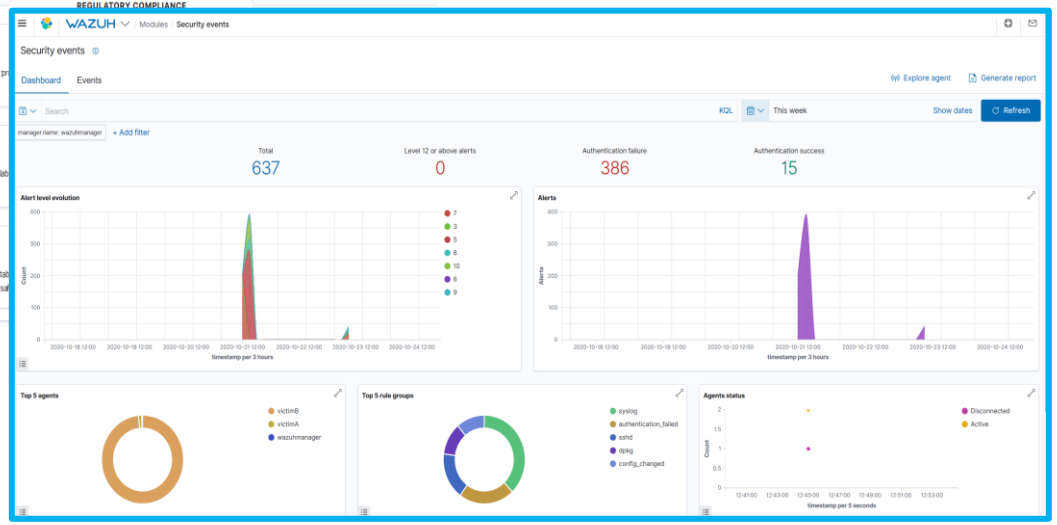
In-vehicle Services Demo

SIEM solution for AVs



General dashboard

Monitoring of security events



Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, and other event and contextual data sources.

Visual Analytics Suite

Data streams from the CAVs connected devices and network are **send to the cloud** for analysis and visualization. VAS aims to assist the human analysts to **visually spot attacks** and their causes.

Main features:

- Analysis and visualization of the input data → Interactive graphs generation for analytic reporting to end-users
- AI algorithms application for anomaly detection → Visualization of their results for threat detection on the entire fleet
- Alerts for possible cybersecurity attacks → Threats detection and identification
- Enrich the pool of shared known threats
- Basis for applying mitigation strategies
- Active monitoring of the CAV fleet

nIoVe

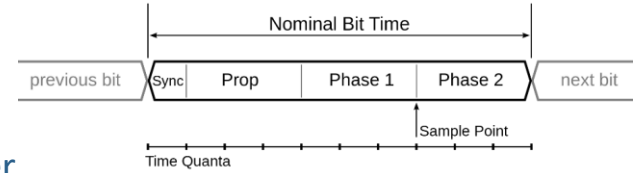
Visual Analytics Suite

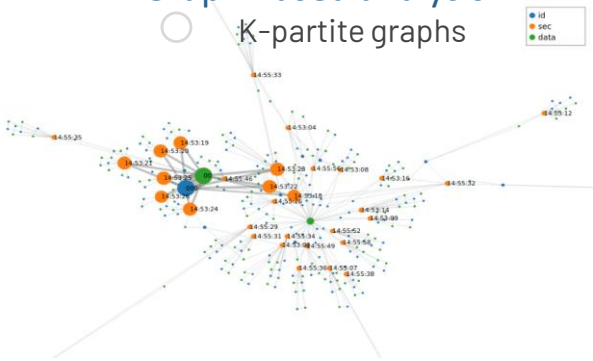
Data from the CAV network are collected and stored for analysis regarding anomaly detection and prediction of forthcoming attacks.

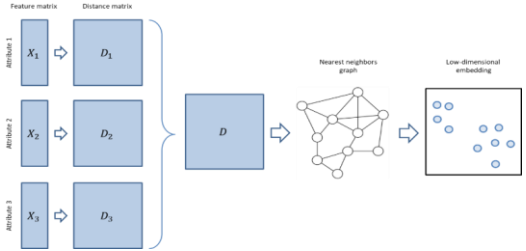
nIoVe

Algorithms:

- CAN bus analyser
  - Decision trees
- Camera Stream analyser
  - AI (LSTM networks)
- Graph Based analysis
  - K-partite graphs



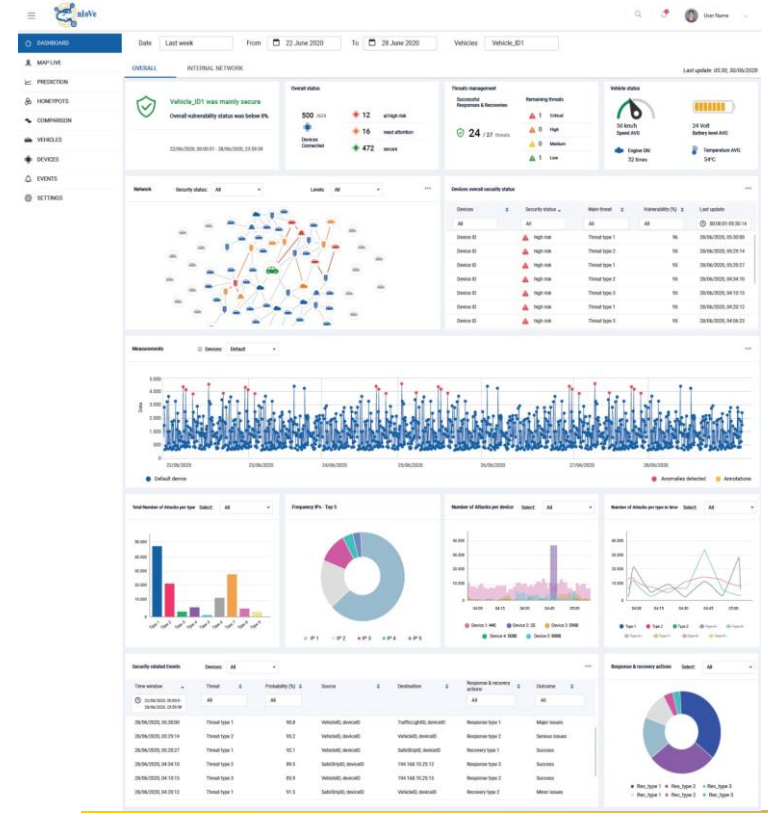


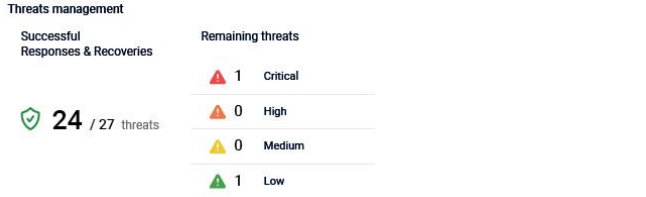


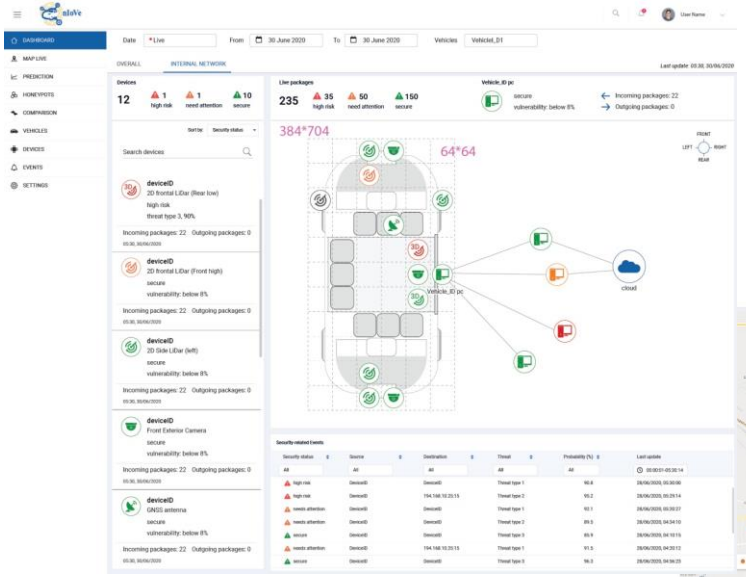
CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

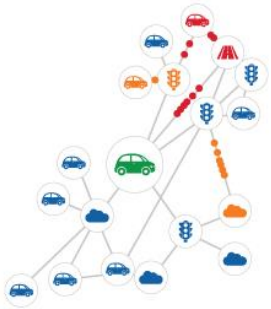
Information Technologies Institute

Visual Analytics Suite Interfaces



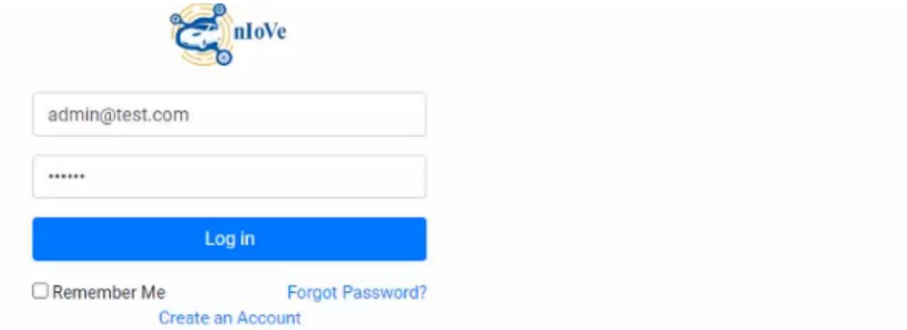






nIoVe

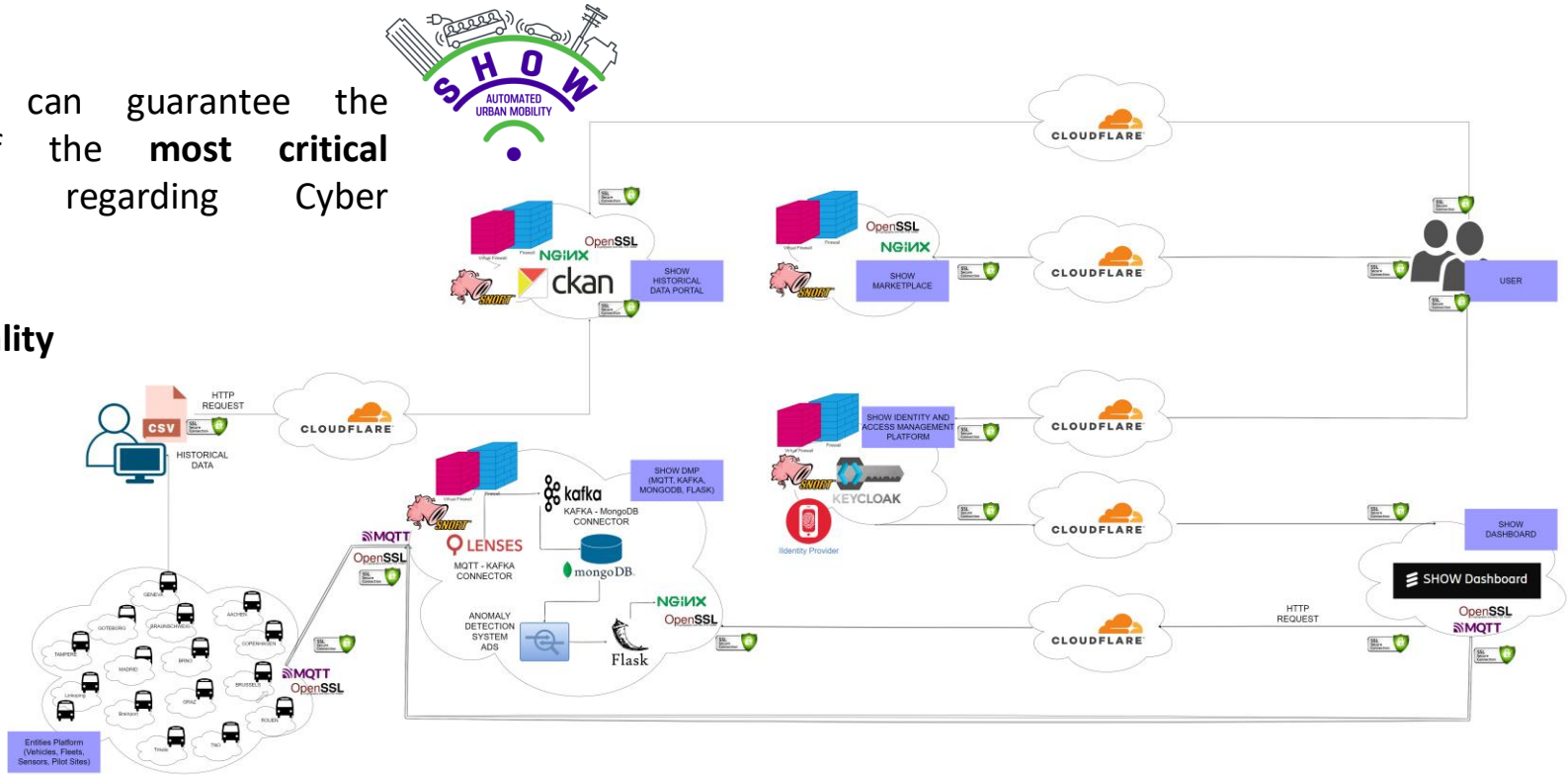
Visual Analytics Suite Demo



CAVs Ecosystem Cyber Security

The system can guarantee the fulfilment of the **most critical requirements** regarding Cyber Security (**CIA**):

- **Confidentiality**
- **Integrity**
- **Availability**



Attack Implementation

The SHOW system has been tested to popular cyber attacks:

- **Denial Of Service and Distributed Denial of Service attack (DOS/DDOS):**

Result: In some cases the server response time increased from 10ms to 140ms.

Attack:
- Python libraries
- Hping3
- Cloud Virtual Machines

Defense:
- CLOUDFLARE
- SNORT
- IDS

- **Man In The Middle (MITM) or SPOOFING:**

RESULT: SSL/TLS encrypts the messages in transit.

Attack:
- MQTT
- WHIRESHARK

Defense:
- SSL/TLS
- OPEN SSL
- CLOUDFLARE

- **NETWORK DISCOVERY TOOLS:**

RESULT: NMAP failed to find any vulnerabilities

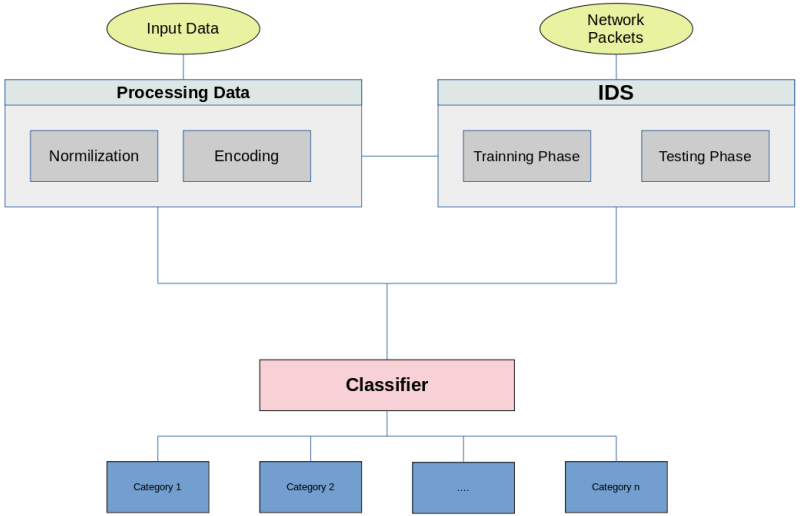
Attack:
- NMAP

Defense:
- CLOUDFLARE
- NGINX

AI-enabled Anomaly Detection

Intrusion Detection System (IDS)

- **Analyzes Internet traffic** in form of network packets, inserted into the AI model to detect hostile activity.
- The IDS has been **trained in a predefined data set** in order to configure the weights for the neural networks.
- IDS is able to **classify the respective network package** into hostile and benign. Hostile packets will be blocked while others will be allowed to communicate with the server.



Machine learning uses techniques for:

- Pattern recognition
- Anomaly detection
- Dynamic data analysis
- Statistical analysis

Machine learning algorithms

- SVM (Support Vector Machine)
- CNN (Convolutional Neural Nets)
- LSTM(Long Short Term Memory)
- Transformers

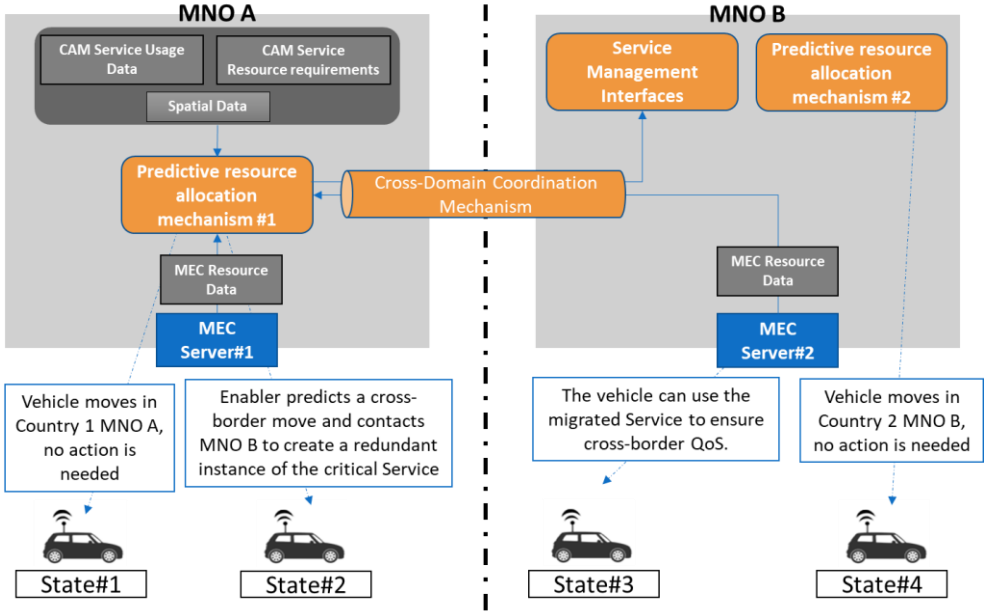
Predictive resource allocation of V2X related network functions using AI algorithms

Problem

- Automotive services have **stringent requirements** related to low latency and reliability.
- These can be met using edge resources i.e. by deploying components of the E2E services as close as possible to the network edges. However, edge resources are finite.

Solution

- The proposed mechanism uses two SotA AI mechanisms, to:
  a) initially **predict future vehicle location** and then
  b) **support the optimal positioning of the VNFs** related to V2X services in the available MEC servers.
- In the context of the existing project it **predicts the need for cross-border VNF placement** to ensure **service continuity** and **satisfy** stringent **resource requirements** by pre-emptively requesting resources.



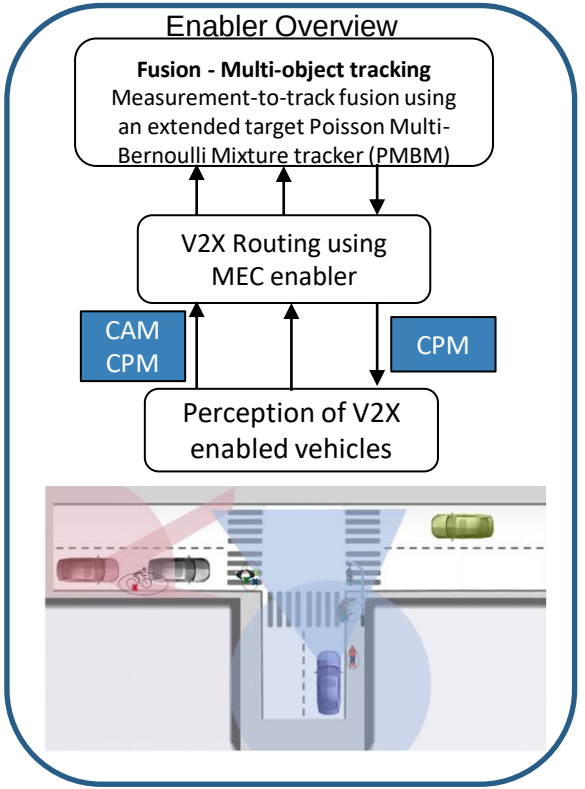
5G Localization for Vulnerable Road User protection

Problem

- Protect Vulnerable Road Users, utilizing connected road users perceptions to achieve better localization i.e. A multiple object tracking problem.
- High accuracy is required under a time constraint in publishing fused perception.

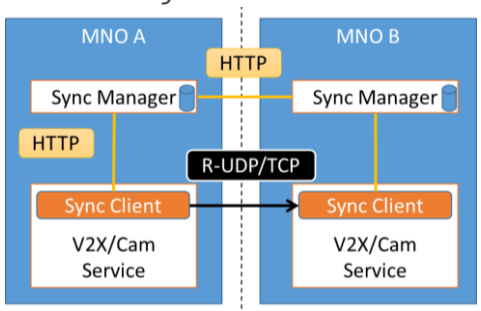
Solution

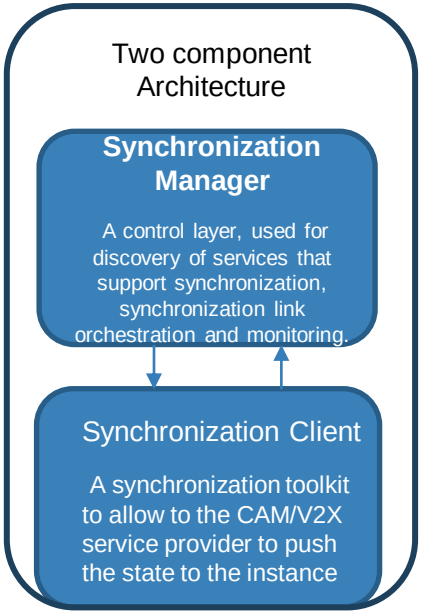
- A **centralized fusion sensor for Intelligent traffic system (ITS) messages has been developed**.
- It uses ML to perform **Multi-object tracking** by fusing VRU related spatial data transmitted from the V2X-enabled road users: **Sub-meter accuracy positioning for** VRUs in the region is achieved.
- Scenarios of Line-of-Sight and no Line-of-Sight are supported for both Connected & non-Connected VRUs.
- CPM and CAM messages are used as inputs while clutter is expected and misdetections are taken into account.
- Accuracy < 0.5m and a latency ~ 500ms (required for calculations) is achieved.



Enabler: Low-Latency Cross-Border Synchronization Mechanism for Seamless CAM Service Delivery

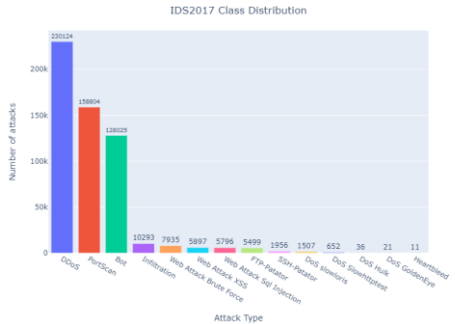
- **Objectives:**
  - To deliver seamless cross-border /cross-MNO CAM services by relocating the state of the CAM service from the serving to the visited network.
- **Solution:**
  - Provided Solution has achieved real time synchronization requirements:
  - A Synchronization Manager as a python Flask service.
  - A Synchronization Client as a C++ Library is able to:
    - Provide real-time eventual or P2P synchronization.
    - Automatically coordinate with the synchronization Manager
- Synchronization Utilizes Delta encoding, Coordination through serialized structured data & RPC calls, Compression (optional)



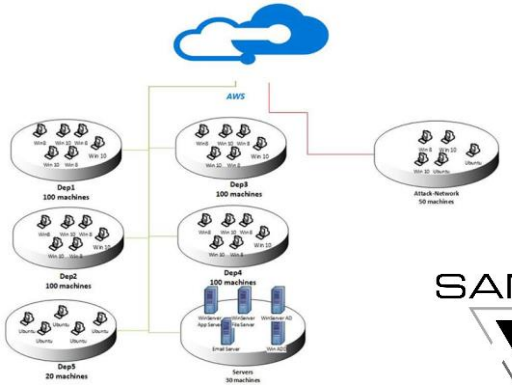


Datasets for 5G-tailored IDS

- **CIC-IDS-2017**[1] dataset contains **benign** and **common attacks traffic**, while it
  - Contains the abstract behaviour of 25 users based on the HTTP, HTTPS, FTP, SSH, and email protocols
  - Includes the most common attacks based on the 2016 McAfee report, such as Web based, Brute force, DoS, DDoS, Infiltration, Heart-bleed, Bot and Scan
  - Used among the literature for **5G research**



- **CID-IDS-2018**[2] dataset is **derived from an attacking infrastructure** that includes 50 machines and a victim organization that has 5 departments of 420 machines and 30 servers. The dataset includes the captures network traffic and system logs of each machine.
  - The simulated protocols are HTTP, HTTPS, SMTP, POP3, IMAP, SSH, and FTP.
  - Used among the literature for **5G research**



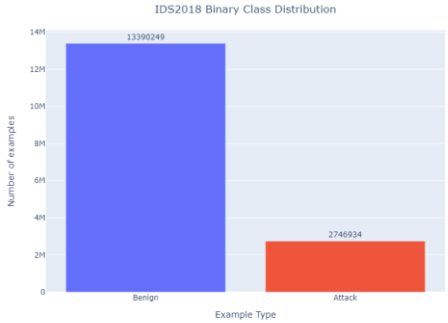
SANCUS

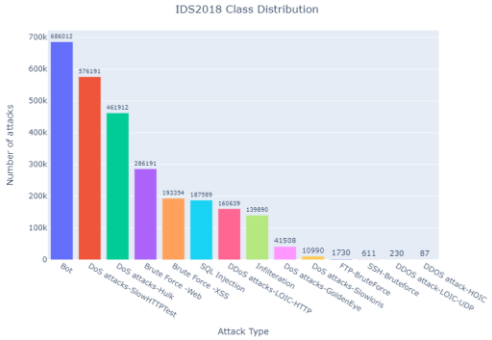
[1] https://www.unb.ca/cic/datasets/ids-2017.html
[2] https://www.unb.ca/cic/datasets/ids-2018.html

Datasets for 5G-tailored IDS

- **USTC-TFC2016** [3] dataset contains
  - **ten types** of **malware traffic** collected from real network environment by CTU researchers from 2011 to 2015, and
  - **ten types** of **normal traffic** collected using IXIA BPS, which is a kind of professional network traffic simulation equipment

- **CID-IDS-2017** fused with **CID-IDS-2018** dataset
  - **77 total features** common for both datasets, namely Destination Port, Idle Min, Flow IAT Mean, Packet Length Min
  - **TCP** and **UDP** traffic, and
  - **14 types** of **malware traffic** per dataset



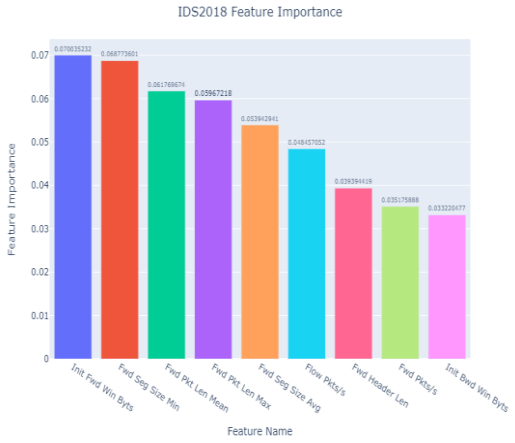


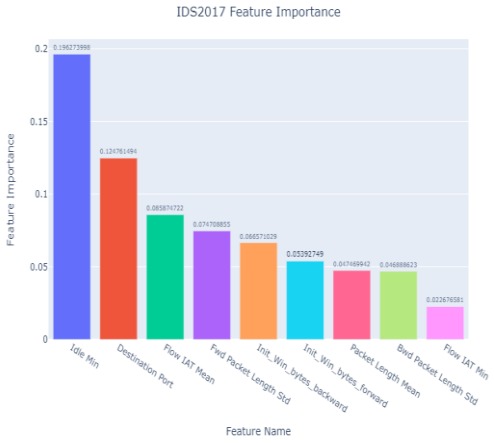
[3] https://github.com/echowei/DeepTraffic/tree/master/1.malware_traffic_classification/1.DataSet(USTC-TFC2016)

Feature Extraction & Pre-processing

- **Feature-based Models**:

1. **Use** CIC-Flow-Meter for the extraction of 80 statistical network traffic features such as Duration, Number of packets, Number of bytes, Length of packets, etc.
2. **Clear redundant records**, i.e., discard attack samples that appear less than 1%
3. **Discard extra features**, namely Forward Header Length, Protocol, Timestamp





SANCUS

Feature Extraction & Pre-processing

- **Image-based Models:**

Using **Wang et al.**'s designed a tool, called **USTC-TK2016**, .pcap files are converted into images in the following manner:

1. **Traffic split**: If representation type is Flow + All or Session + All, output data format is pcap. If representation type is Flow L7 or Session + L7, output data format is bin
2. **Traffic cleaning**: Perform traffic anonymization/sanitization and empty/duplicated files removal
3. **Image generation**: Trim all files to uniform length and convert them to grayscale images

SANCUS

Architectures

Non-Symmetric Stacked Autoencoders

- The core of this algorithm consists of stacked auto-encoders featuring non-symmetrical multiple hidden layers

Convolutional Stacked Autoencoders

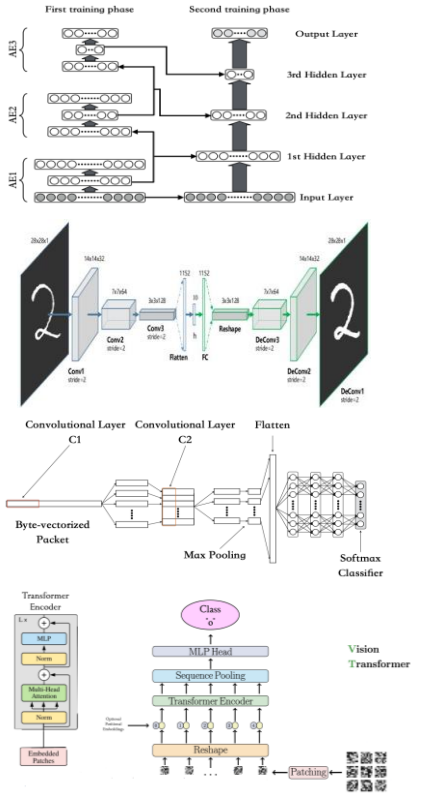
- Same concept as fully connected stacked autoencoders, but tailored to processing images by deploying convolutional networks

1D-CNN

- 1D-CNNs can capture spatial dependencies between adjacent features in network packets that may lead to discriminative patterns for every class of attacks/normal traffic.

Vision Transformer

- Transformers are an emerging DL technique that has been proven superior to RNNs and the rest of the state-of-the-art techniques in speech applications.



Indicative Results

IDS2018

Model	Accuracy	Precision	Recall
RF	0.986	0.981	0.938
NSAE	0.982	0.978	0.931
CSAE	0.981	0.976	0.929
1D-CNN	0.973	0.969	0.925

IDS2017

Model	Accuracy	Precision	Recall
RF	0.985	0.979	0.931
NSAE	0.984	0.982	0.929
CSAE	0.984	0.981	0.928
1D-CNN	0.977	0.965	0.922

Some Details:

- Accuracy scores derived from the test set (**25%**)
- By keeping the **IP** feature, there is a risk for the network to be IP biased
- **Binary** classification is performed

Conclusions:

- **More data** must be utilized for real world applications
- **Random Forest** classifier outperforms neural architectures, but the latter achieves better metrics on unseen data

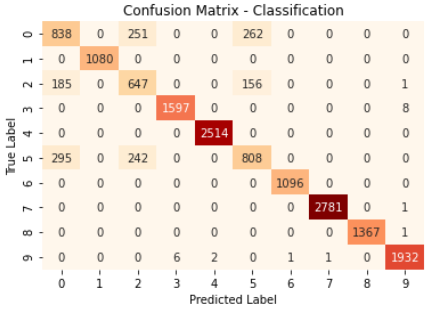
SANCUS

Indicative Results

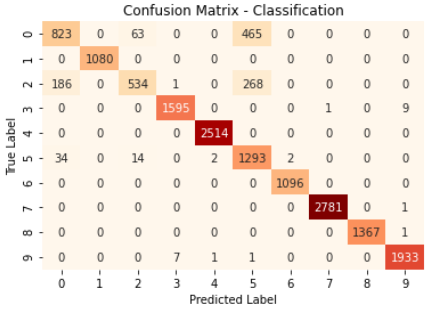
The **results** of the ViT compared to a CNN implementation are the following:

Method	Accuracy Scores
CNN	0.91
Vision Transformer	0.93

CNN Confusion Matrix



ViT Confusion Matrix



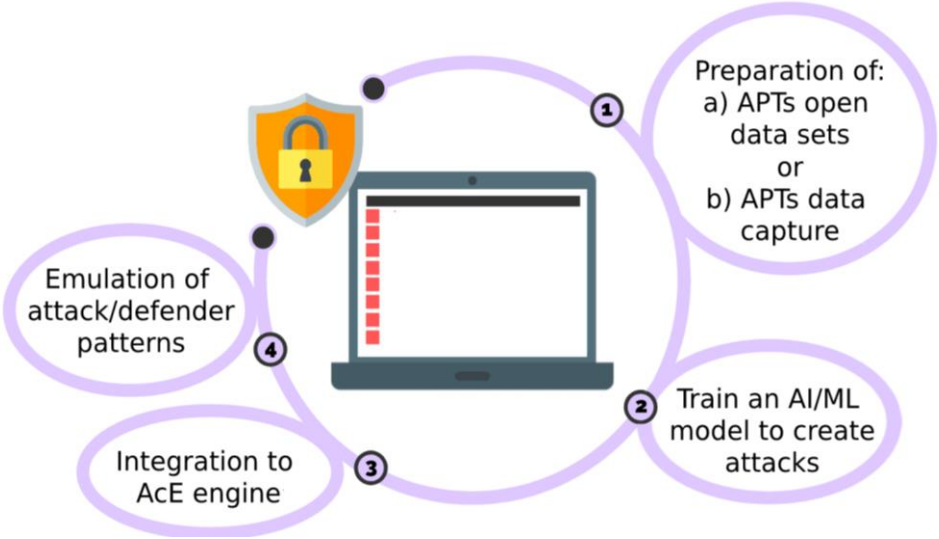
Conclusions:

- **ViT model performs better** than CNN, with the same number of trainable parameters
- ViT's self attention mechanism seems to **improve the model's predictive capability** on unseen data

AI-enabled Penetration Testing

Attack configuration and emulation engine mechanism (AcE)

SANCUS



Future Perspectives

- Combination of different approaches towards a **holistic Artificial Intelligence Cybersecurity Framework** that involves:
  - Intelligent information sharing
  - Intrusion detection system
  - Automated Penetration Testing
  - Attack mitigation mechanisms
- Fine-tuning of derived AI-models to provide **tailored solutions to 5G connectivity in CAVs** ecosystem
- Extension of the proposed approach to **6G infrastructure and related use cases**

SANCUS

Related skills and competences

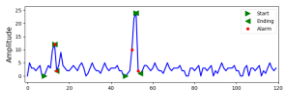
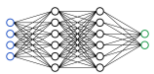
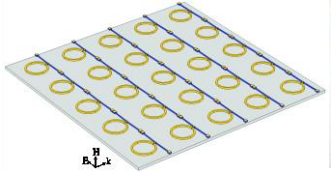
- Technologies
  - **Artificial Intelligence and Analytics**
  - **Blockchain technologies and smart contracts**
  - **Data Security and Privacy**
    - Design/implementation/operation of data management systems with security/privacy functions
  - **Operational Incident Handling and Digital Forensics**
    - Digital forensic processes and workflow models; Digital forensic case studies; Incident forecasting
    - Anomaly detection using machine learning; Decision support for incident detection/prediction
    - Information Sharing, Threat Detection and Intelligence
  - **Artificial Intelligence and Machine learning** for near Real-time Abnormal events identification
  - **Software and Hardware Security Engineering**
    - Intrusion detection and honeypots; Malware analysis; Security documentation, Blockchain
  - **Security Measurements**
    - Security analytics; Validation and comparison frameworks for security metrics, SIEM

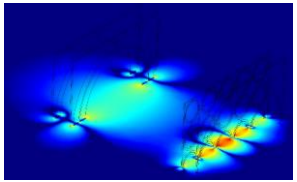
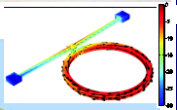
Member & active contributor of ECS EUROPEAN CYBER SECURITY ORGANISATION 6G SNS IA

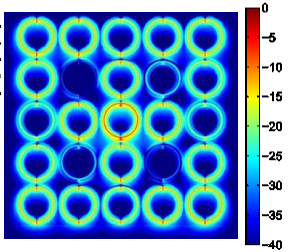
Research interests

- Technology areas
  - **IoT and THz communication technologies**, **5G/6G networks**, **Cybersecurity**, **Autonomous vehicles, Anti-Drone**, **eHealth**, navigation technologies, cloud/edge and computing technologies, distributed ledger technologies (blockchain), (semantic) interoperability
  - **Data, visual and audio analytics**, **multiphysics simulation**, data mining, **machine and deep learning**, federated and swarm learning, explainable AI, **neuromorphic computing**, virtual and augmented reality, image processing, computer and cognitive vision, human computer interaction, data anonymization
  - system integration, mobile and web applications, hardware design and development, **smart materials (metasurfaces)**, **wireless power transfer** technologies, **photonics**, smart grid technologies and solutions, social media analysis.

- SNS Domain:
  - **AI-powered Cybersecurity** in 5G networks
  - **Cloud/Edge computing** with artificial intelligence
  - **State synchronization** for data-centers/cloud/5G
  - AI application in **Physical Layer/Neuromorphic computing**
  - AI application in **Photonic Integrated circuits (PICs)**
  - **Reconfigurable Intelligent Surfaces (RIS)**
  - Design and **multiphysics simulation** of **metasurfaces**
  - **Simulation tools** (FDTD, FEM, Ray tracing)
  - Metamaterial-based **Wireless Power Transfer, Antennas, Filters**
  - **5G Testbed (core & RAN) & several verticals** (industry, health, autonomous vehicles)
  - **Smart home** infrastructure & **EMF exposure** prediction



Thank you! … Any Questions?

Dr. Antonios Lalas
Postdoctoral Researcher
Tel. : +30-2311-257779
E-mail : lalas@iti.gr
Web: www.iti.gr

Centre for Research & Technology Hellas
Information Technologies Institute