PUVEC Security Issues

Présenté par Lamia Ben Azzouz

Outline

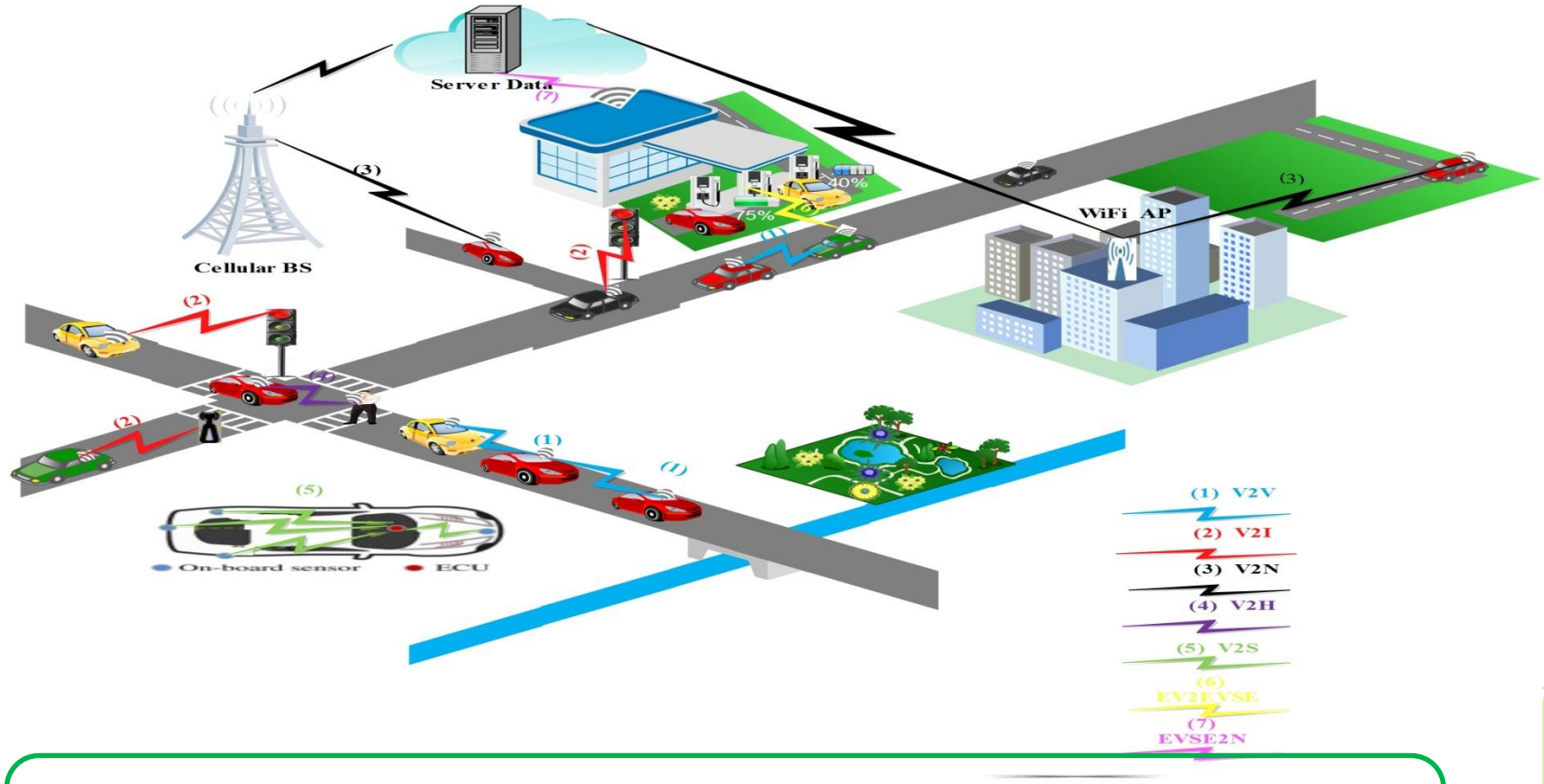
Part 1 Adaptive Security (Yosra Fraiji, Cristal, ESIGELEC)

- Vehicle communication systems
- Vulnerabilities
- Game based Adaptive security Model
- Future works

Part 2 Data Trust (Ilhem Souissi, SMART Lab, ESIGELEC)

- Data Trust in PUVEC
- Fuzzy Logic-based Speed and Energy Consumption Verification

Vehicle Communication Systems



Intra Vehicle wireless Sensor Network (V2S)

V2S Vulnerabilities

- False data injection

  battery status, temperature , etc: can affect the driver's decision , PUVEC services

- GPS deception

  false data about vehicle location

  wrong energy map

- Eavesdropping

  detect sensitive information about the vehicle (ID, position, battery status etc.)

- Privacy attacks, DoS, Jamming.

Adaptive Security

a security solution/protocol:

- senses, learns the changes in the environment, device capacity, variations in the network services
- adapt security according to the changing context

Driving context information is composed of any information that describes the driving situation

position, direction, speed, traffic and weather information, etc.

PUVEC Dynamic Context

- Energy level
- processing and memory resources
- type of sensors
- traffic state
- distance to the charging stations

Game Based Adaptive Security

The solution adapts the security level according to the combination of three parameters.

- Energy level
- Traffic state
- Distance to charging station

- **Secure to Passive**

$$P_{\sigma\to\pi}(\mathrm{E, TS, DSC, TR, M\ \&P}) = \begin{cases} 1, (E_{level} - E_{cons} \le E_{threshold}) \wedge ((\mathrm{D} \le \mathrm{DCS}) \vee (V_t \le \gamma)) \\ 0, \quad \text{otherwise} \end{cases}$$

- **Passive to Secure**

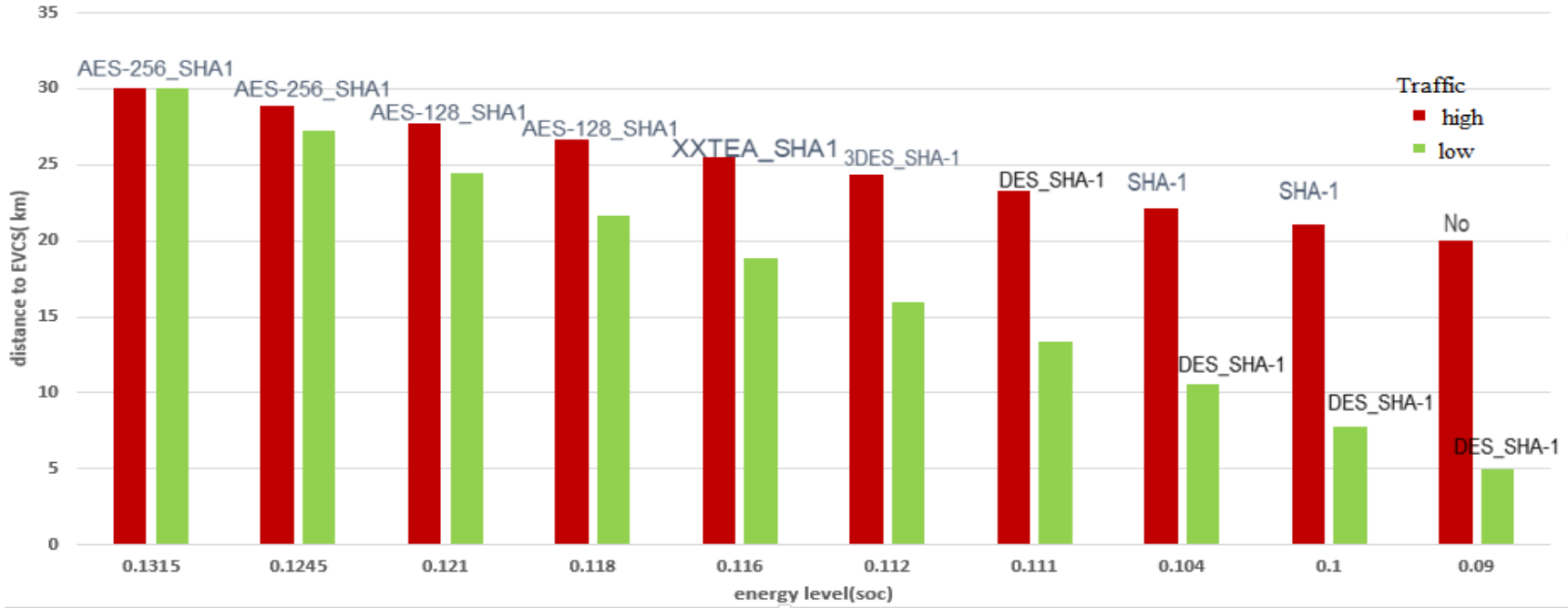
$$P_{\pi\to\sigma}(\mathrm{E, TS, DSC, TR, M\ \&P}) = \begin{cases} 1, (E_{level} - E_{cons} > E_{threshold}) \vee ((\mathrm{D} > \mathrm{DCS}) \wedge (V_t > \gamma)) \\ 0, \quad \text{otherwise} \end{cases}$$

Hybride adaptation scenario

Scenario	energy	Distance to charging station	Traffic	Security
1	$E_{level} - E_{cons} \leq E_{threshold}$	D<DCS	medium	No
2	$E_{level} - E_{cons} \leq E_{threshold}$	D<DCS	high	No
3	$E_{level} - E_{cons} \leq E_{threshold}$	D < DCS	low	No
4	$E_{level} - E_{cons} \leq E_{threshold}$	D≥ DCS	medium	Yes
5	$E_{level} - E_{cons} \leq E_{threshold}$	D≥ DCS	high	No
6	$E_{level} - E_{cons} \leq E_{threshold}$	D≥ DCS	Low	Yes
7	$E_{level} - E_{cons} > E_{threshold}$	D< DCS or D≥ DCS	low	Yes
8	$E_{level} - E_{cons} > E_{threshold}$	D<DCS or D≥ DCS	high	Yes
9	$E_{level} - E_{cons} > E_{threshold}$	D<DCS or D≥ DCS	medium	Yes

Simulation Results

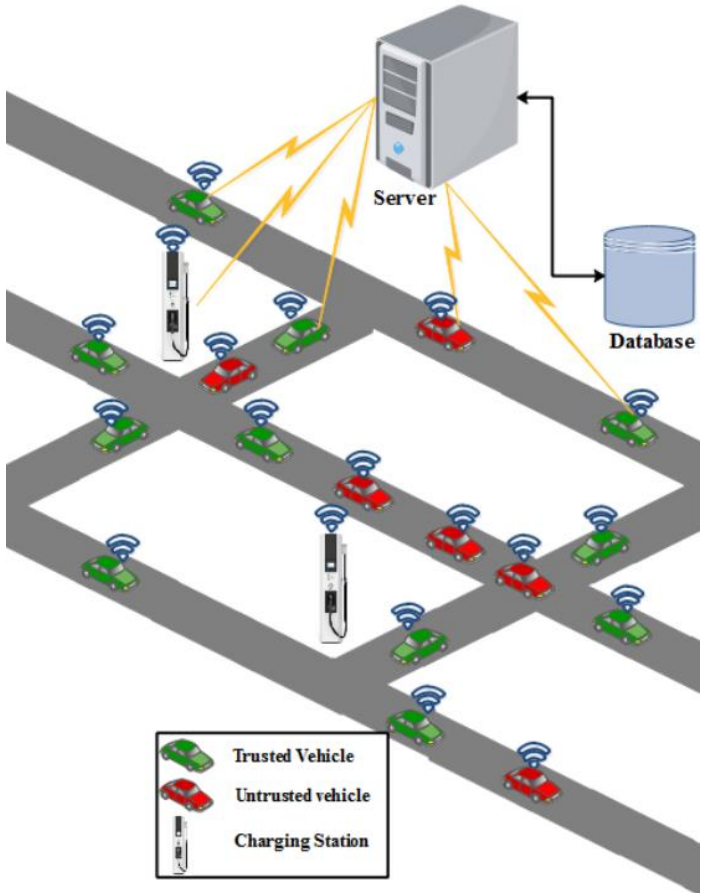
Hybrid Adaptation



Future Works

- large variety of available communication technologies
- **adaptive security policies**
  - type of available network (5G, Wi-Fi, 802.11p, etc.),
  - energy level of the battery,
  - available electric charging stations,
  - Service Awareness

Part 2 : Data Trust

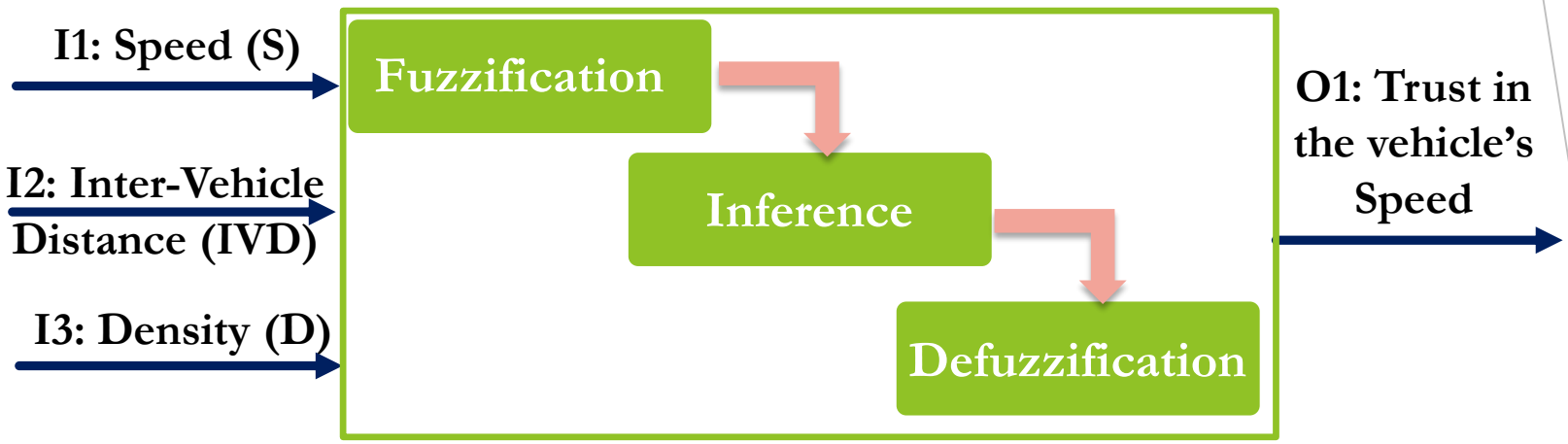


only trusted energy information are considered .

Assumptions:

- Only trusted messages in terms of position are handled during the verification process.
- speed has a great impact on the energy consumption for EVs.

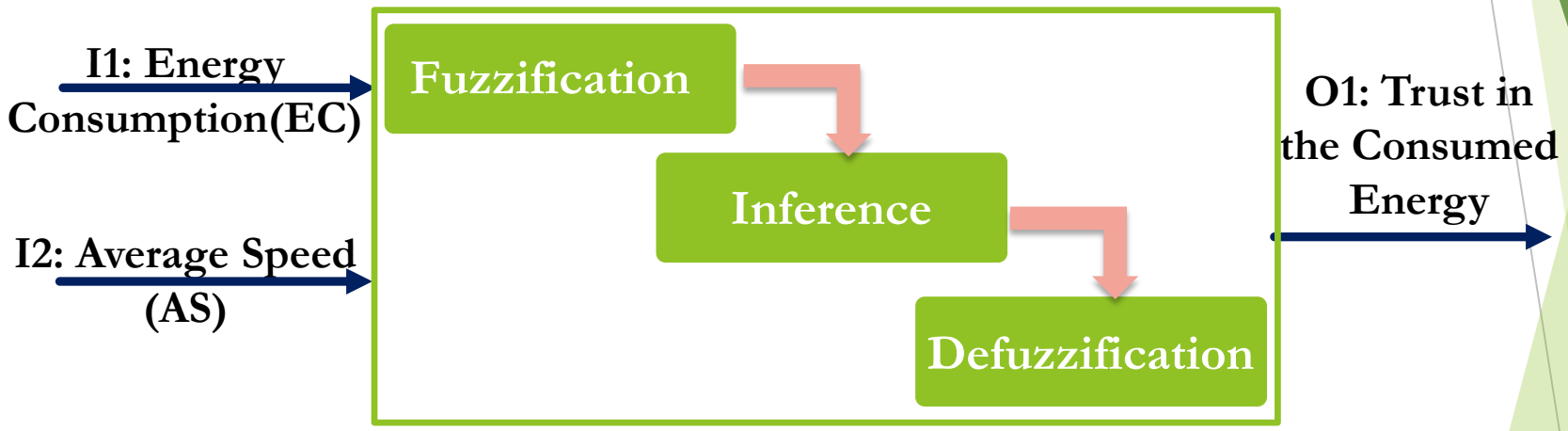
Fuzzy Logic-Based Speed Verification



To trust the **speed**:

- should not exceed the maximum allowed speed per lane ($S \geq 0$ and $S \leq Smax + \Delta$)
- should be proportional to the inter-vehicle distance.
- should be proportional to the traffic density.

Fuzzy Logic-Based Energy Consumption Verification



To trust the **Energy Consumption**:

- should be proportional to the Vehicle's speed.

Futur Works

- Trust the position.

- Consider the vehicle's type (e.g. police car, ambulance, etc.).

- Integrate other methodologies (e.g. the vehicle reputation).

THANK YOU