Some Thoughts About VANET Security with RINA

Anis Laouiti

Telecom SudParis

Fatma Hrizi

Issat Gafsa

University of Gafsa

What is VANET?

- **Vehicular Ad hoc NETwork**

- **VANETs are emerging new technology to integrate the capabilities of new generation of wireless networks into vehicles.**

- **“A communication node on-board a vehicle is able to establish a wireless communication with other surrounding communication nodes”**

  - V2V, V2I, ….., V2X

What is VANET?

- **Goals**
  - Provide efficient vehicular communications
  - Enable a large set of Intelligent Transportation Systems (ITS) applications:
    - Improve traffic Safety on the road
    - Enhance traffic efficiency
    - Provide ubiquitous connectivity and services while on the road to mobile users

VANET Applications

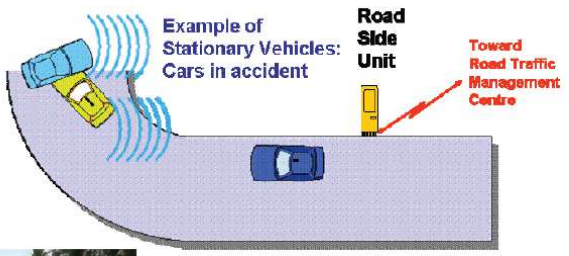
- **Three major classes**

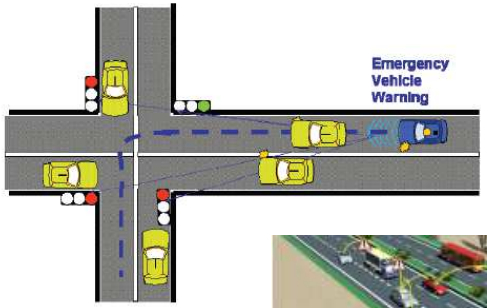
  - **Cooperative Road Safety**: Reduce accidents by warning drivers ahead of time
  - **Traffic Efficiency**: Reduce traffic jams and pollution by proposing dynamic routing and adapted speed and optimize flows of vehicles
  - **Comfort and Infotainment**: provide the driver with information support and entertainment: Location based services, Bringing Internet into cars

Non Safety

Cooperative Road Safety Applications

- **Road Hazard Warning**
  - Stationary vehicle – accident
  - Traffic condition warning
  - Collision risk warning
  - Road work warning
- **Cooperative Awareness**
  - Emergency vehicle warning
  - Motorcycle approaching indication
- **Communication Pattern / requirements**
  - Event driven
  - Low Latency: between 50ms and 100ms
  - High reliability: channel capacity/packetloss
  - High penetration rate
  - Detection capabilities of the local hazard
  - Accurate positioning capabilities
  - **Very frequent messages**
  - **Multi-hop communications**
  - **Determine Validity of Data**
  - **Ensure Integrity of Data**

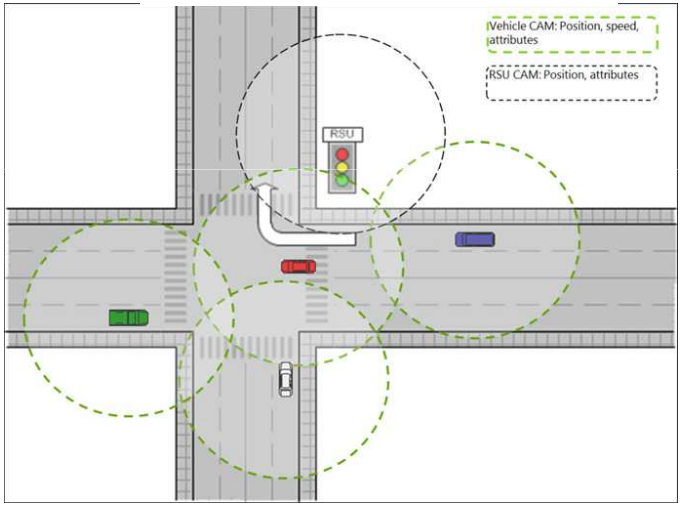




Source ETSI/ITS

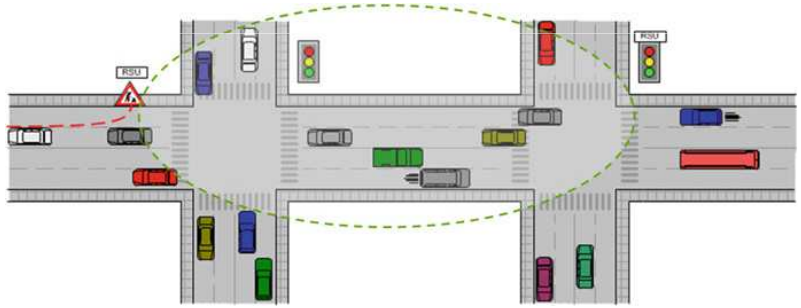
CAM: Cooperative Awareness Message

- **Real time ITS station data**
  - Vehicle type
  - Position, Movement
  - Sensor data..
- **Periodic: high frequency**
- **Application independent**
- **Broadcast**
- **Single Hop**
- **Objective:**
  - Maintain awareness to support cooperative performance of vehicles



DENM: Decentralized Environmental Notification Message

- **Event-driven: traffic event, jam…**
- **Application dependant**
- **Multi-hop Geo-Broadcast**
- **Event-related information**
  - Event type
  - Event position
  - Event detection time/duration..
- **Objective:**
  - Depending on the application, detect an event, manage its evolution and its termination

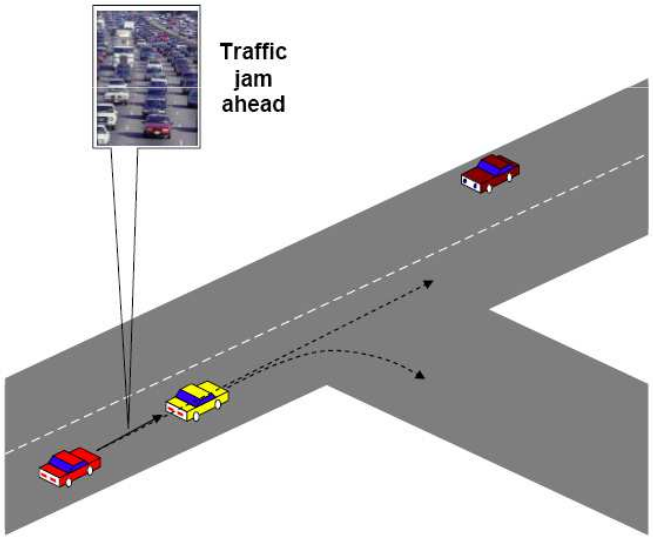


Security issues

- Security will be a crucial aspect of VANETs
- A security threat in VANET can mean not simply loss of information or transfer of funds but loss of life

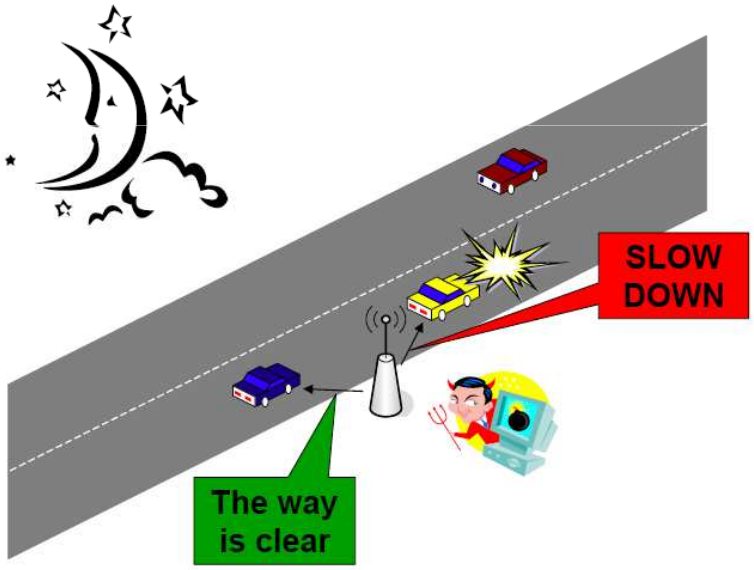
Attacks examples

- **Bugus Trafic Information**



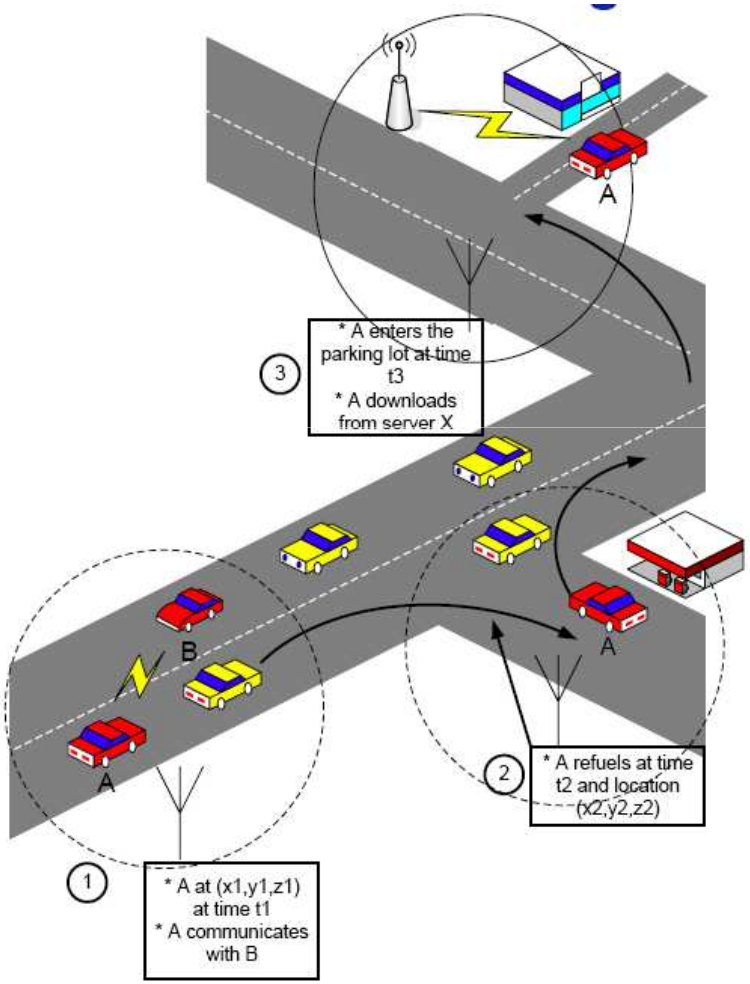
Attacker: insider, rational,active

- **Disruption of Network Operations**



Attacker: insider, malicious,active

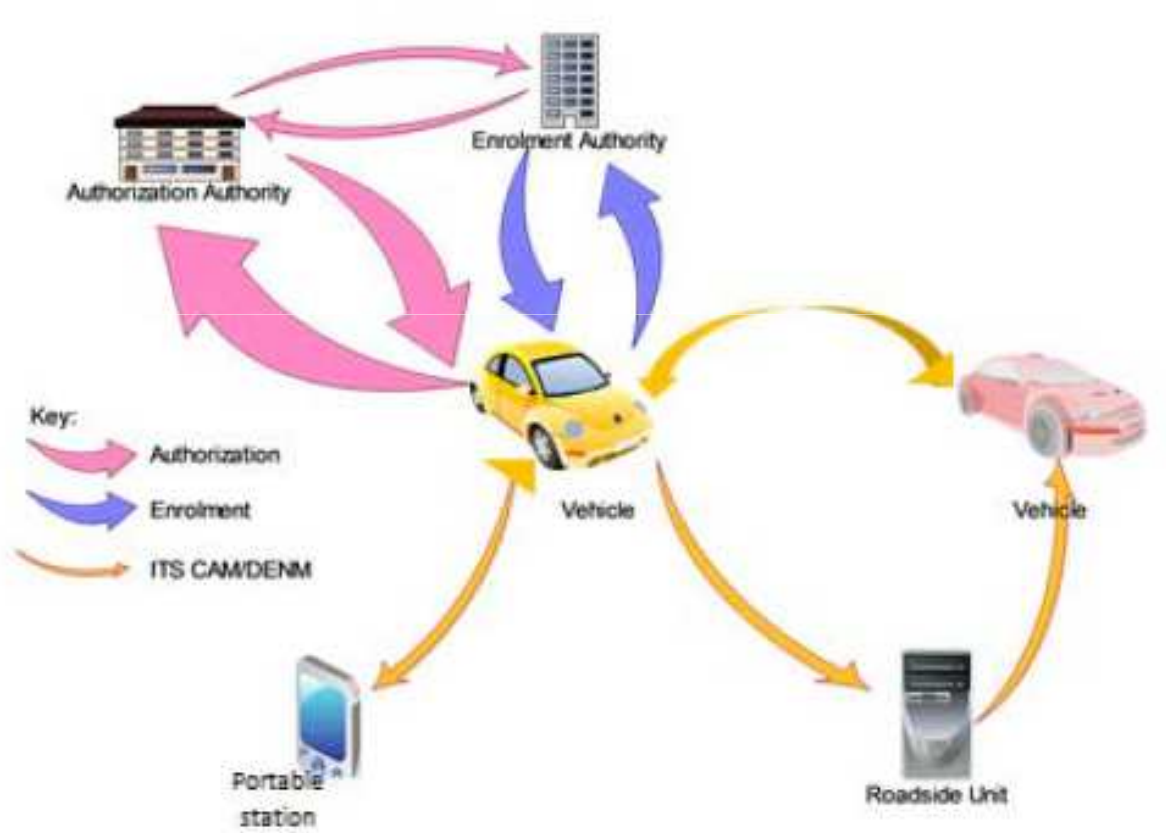
Tracking issue



Security Requirements

- **Authentication:**
  - React only to legitimate events
  - The receiver is ensured that the sender generated a message
- **Verification of data consistency**
  - Legitimate senders can send false data (attack/unintentional)
  - Can cause immense damage even fatalities
- **Availability**
  - Network should be available under jamming attacks
- **Non-repudiation**
  - Drivers causing accidents should be reliably identified
  - The sender of a message cannot deny having sent a message
- **Real-time constraints**
  - High speed means constraints on time
- **Privacy (conflicts with authentication)**
  - **Privacy of drivers against unauthorized observers**
  - **Any observers should not know any future actions of other nodes**

ETSI: ITS Security functional model

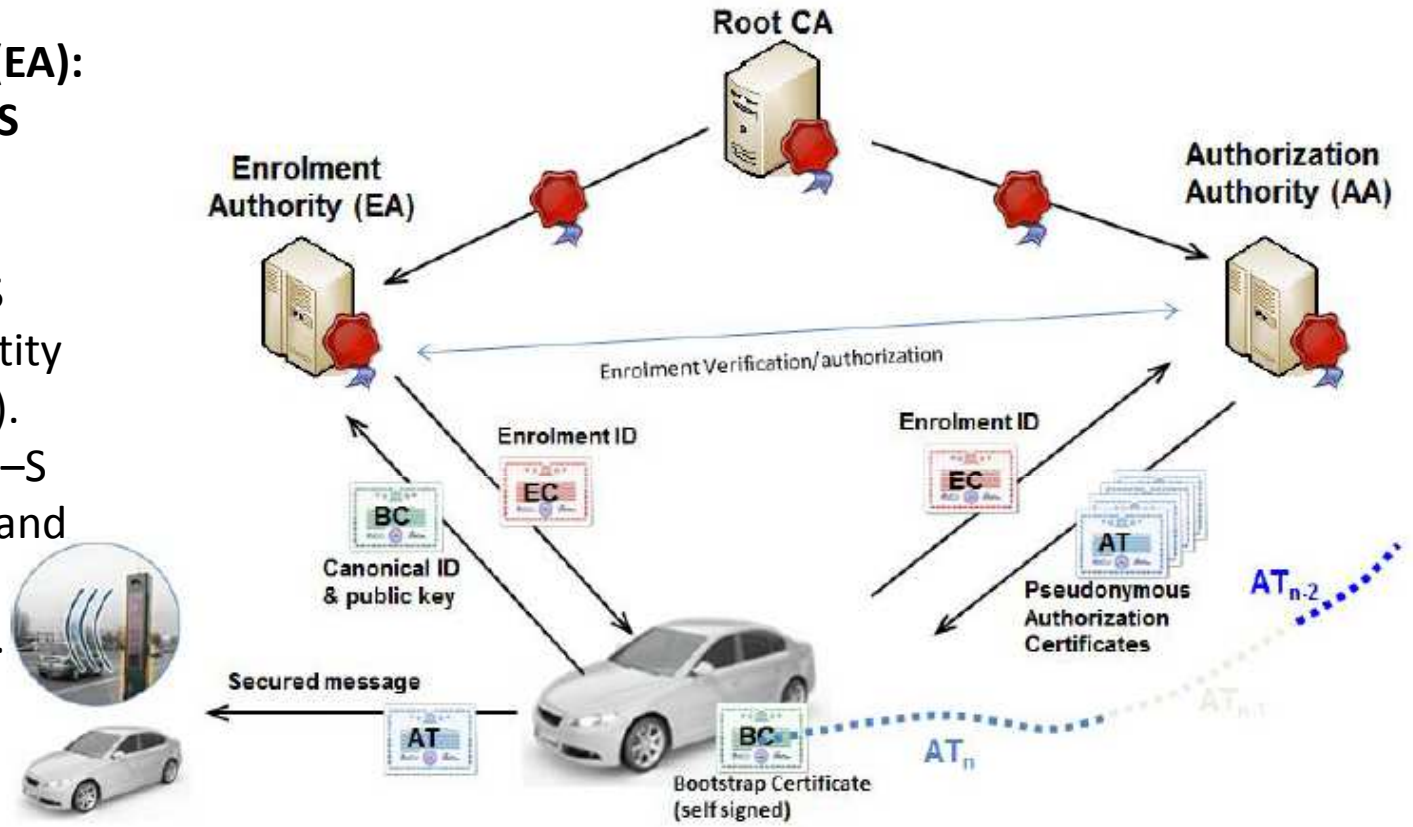


ETSI: ITS Security functional model

- **Enrolment**
  - Use of long-term certificates for identification and accountability (Enrolment Certificates)
- **Authorization**
  - Use of short-lived, anonymized certificates for V2V/V2I (Authorization Tickets/Pseudonyms certificates)
- **Privacy problem**
  - Cryptographic certificates allow tracking of vehicles
- **Solution**
  - Users privacy is protected by a pseudonym scheme
    - Changing frequently the pseudonym certificates
    - Tracking is made more difficult

ETSI: ITS trust model (PKI)

Enrolment Authority (EA): Validates that an ITS–S can be trusted.
It issues an enrolment identifier for the ITS–S and a proof of its identity (Enrolment certificate). the EA provides an ITS–S with an enrolment ID and related enrolment certificate (long term).



Authorization Authority (AA): An ITS–S may apply for specific services and permissions. These privileges are denoted by means of authorization tickets (AT). The AA provides the ITS–S with multiple pseudonyms and the related authorization tickets (short term), to be used in V2X communication.

Some thoughts about VANET Security with RINA

- **CAM and DENM messages (carrying geographical information) are exchanged in broadcast manner**

- **Privacy /tracking issues**

- **RINA**
  - is secure by design
  - Enrolment phase by design
  - Management system already integrated by design
  - But, how to deal with privacy in case of VANET ?

Some thoughts about VANET Security with RINA

- Communication architecture will be organized by area, sub region, region, Global
- Similar to ETSI, we propose to assign several pseudonyms to each vehicle to insure privacy within a DIF/DAF
- The management DIF will be in charge of such task during the enrolment phase

Some thoughts about VANET Security with RINA