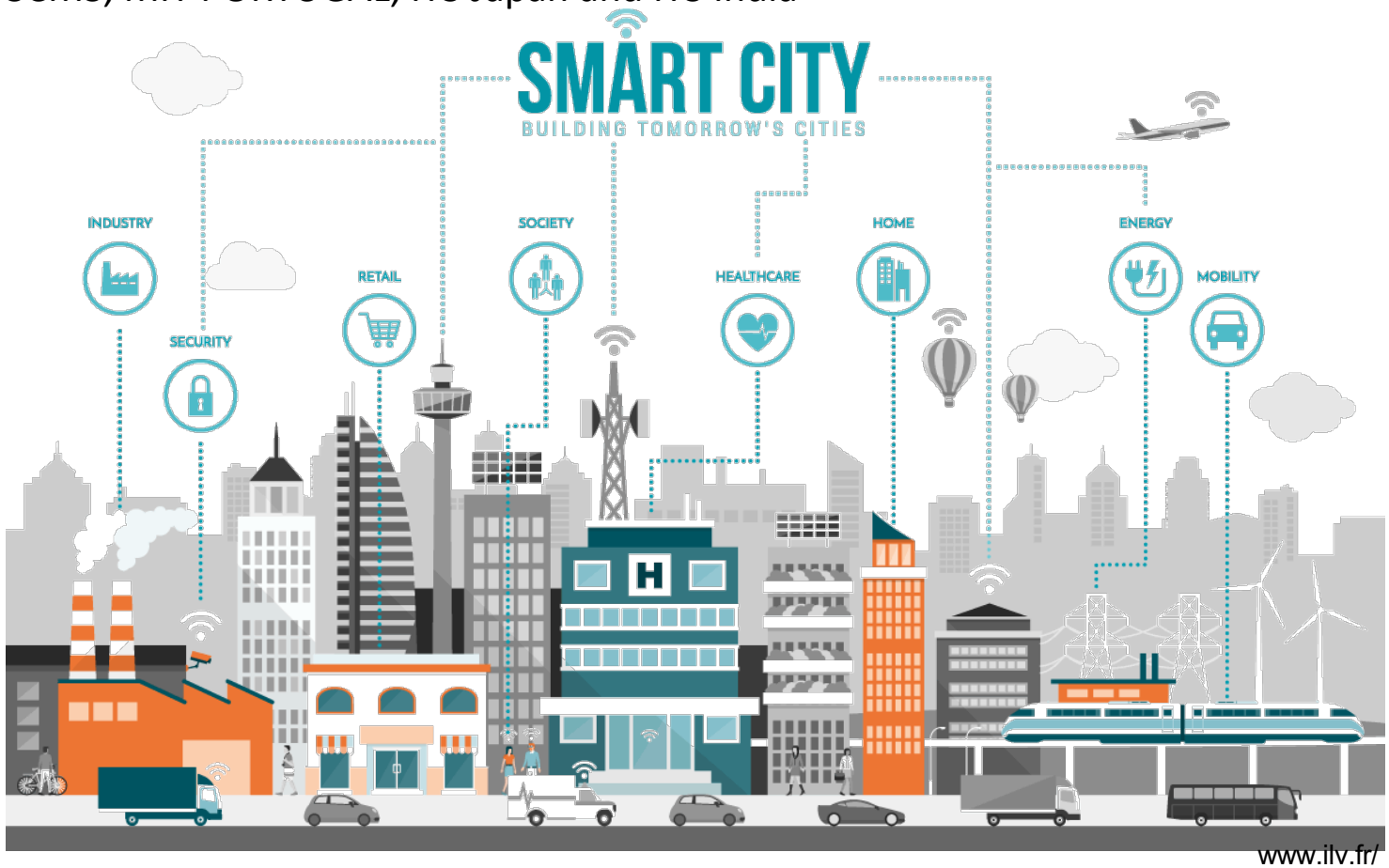
Is it that easy to detect sybil attacks in C-ITS: a position paper

Badis HAMMI

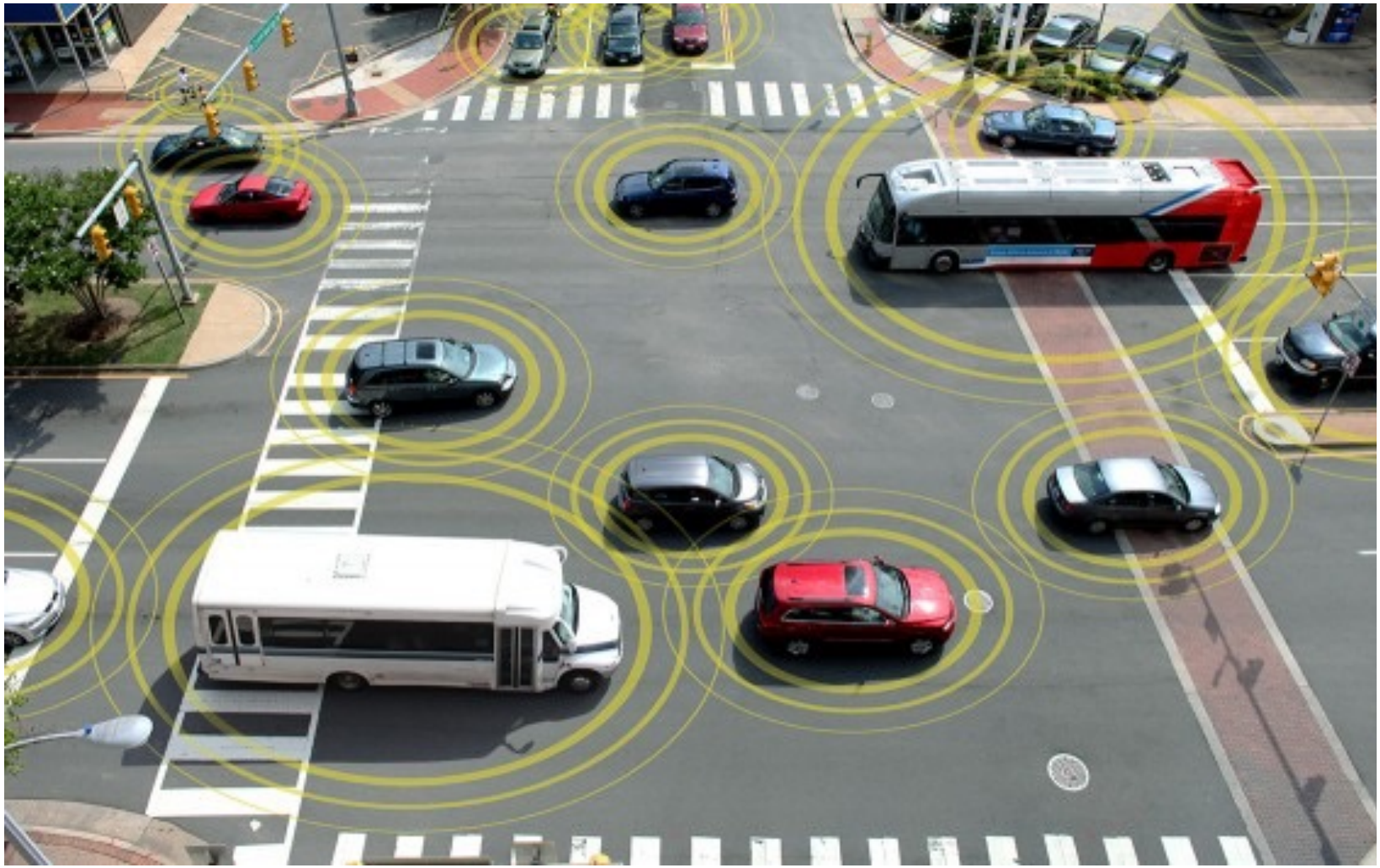
Smart cities

- Smart cities rise
- Automobile manufacturers gave more interest into Cooperative Intelligent Transportation Systems (C-ITS)
- Numerous deployment projects : SEVECOM, EVITA, PRESERVE, CORRIDOR, CVPS, California PATH, ISE, ECO-AT, SCMS, MIT PORTUGAL, ITS Japan and ITS India



www.ilv.fr/

Cooperative Intelligent Transportation Systems



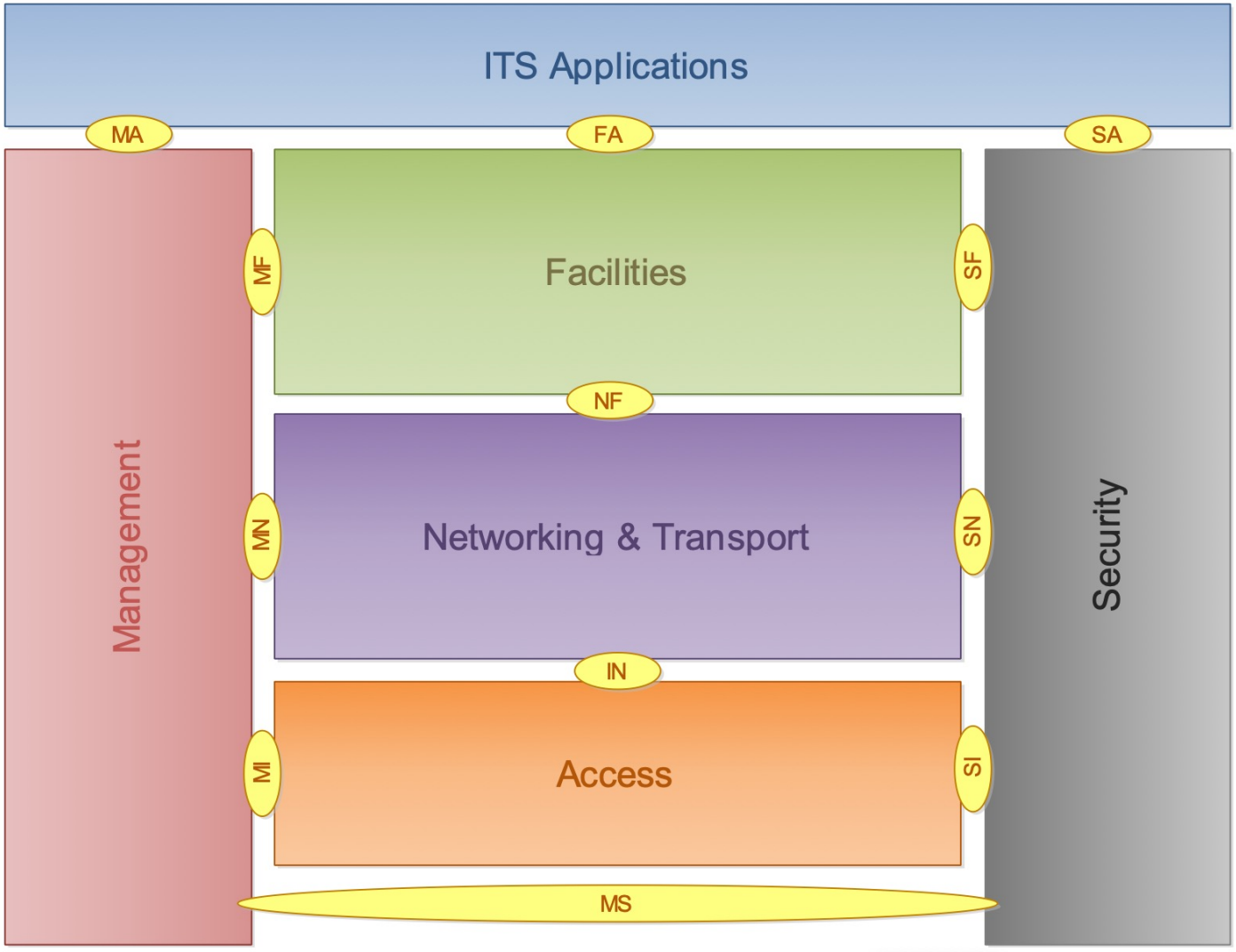
Cooperative Intelligent Transportation Systems

- **ITS applications**
  - Safety and security applications
    - BSM has the potential to prevent up to 75% of all roadway crashes [U.S. Department of Transportation, W. Whyte 2013]
  - Efficiency applications
  - Interactive entertainment applications

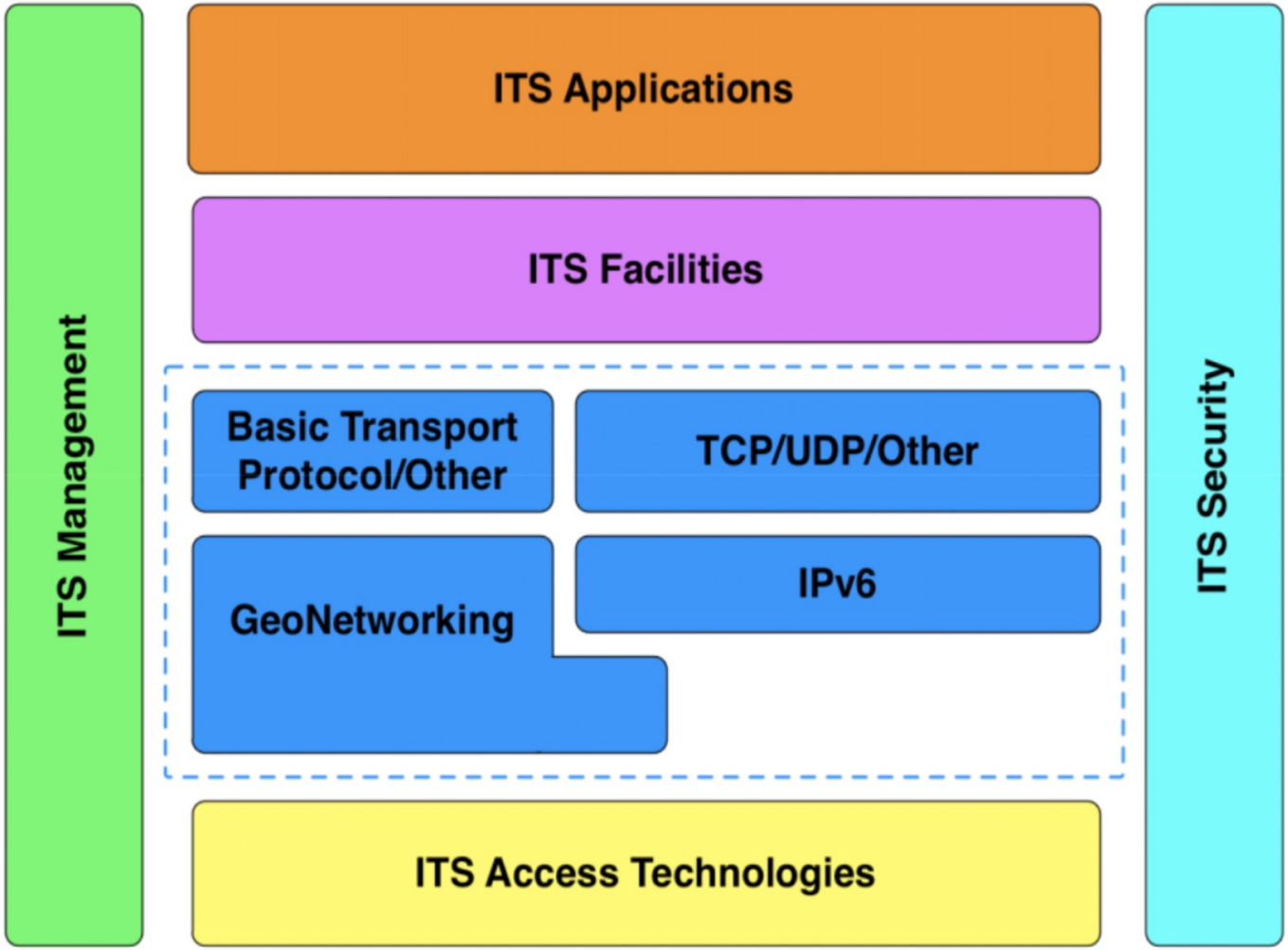
Cooperative Intelligent Transportation Systems

- **A network needs security !!!**

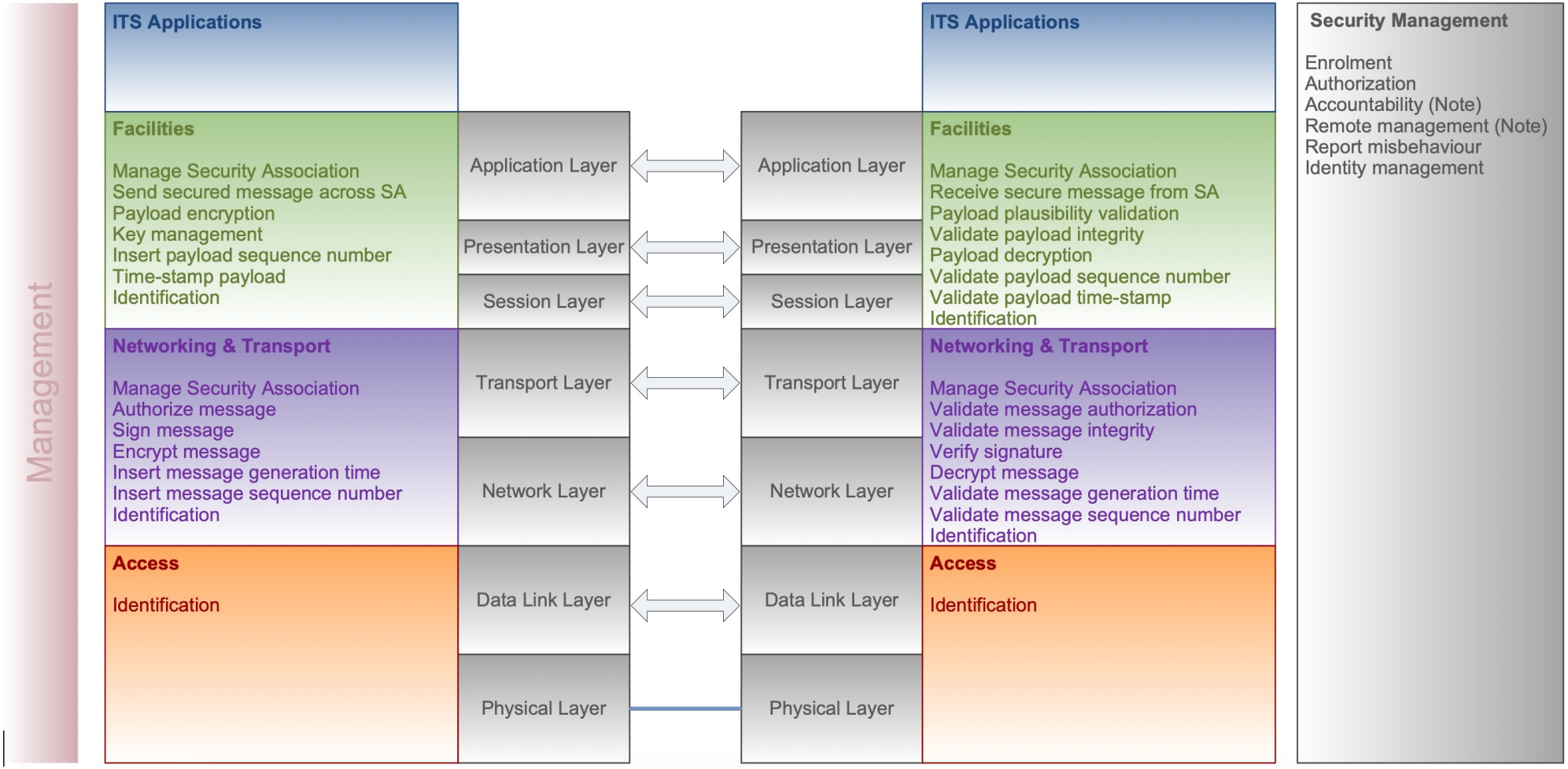
C-ITS networking architecture



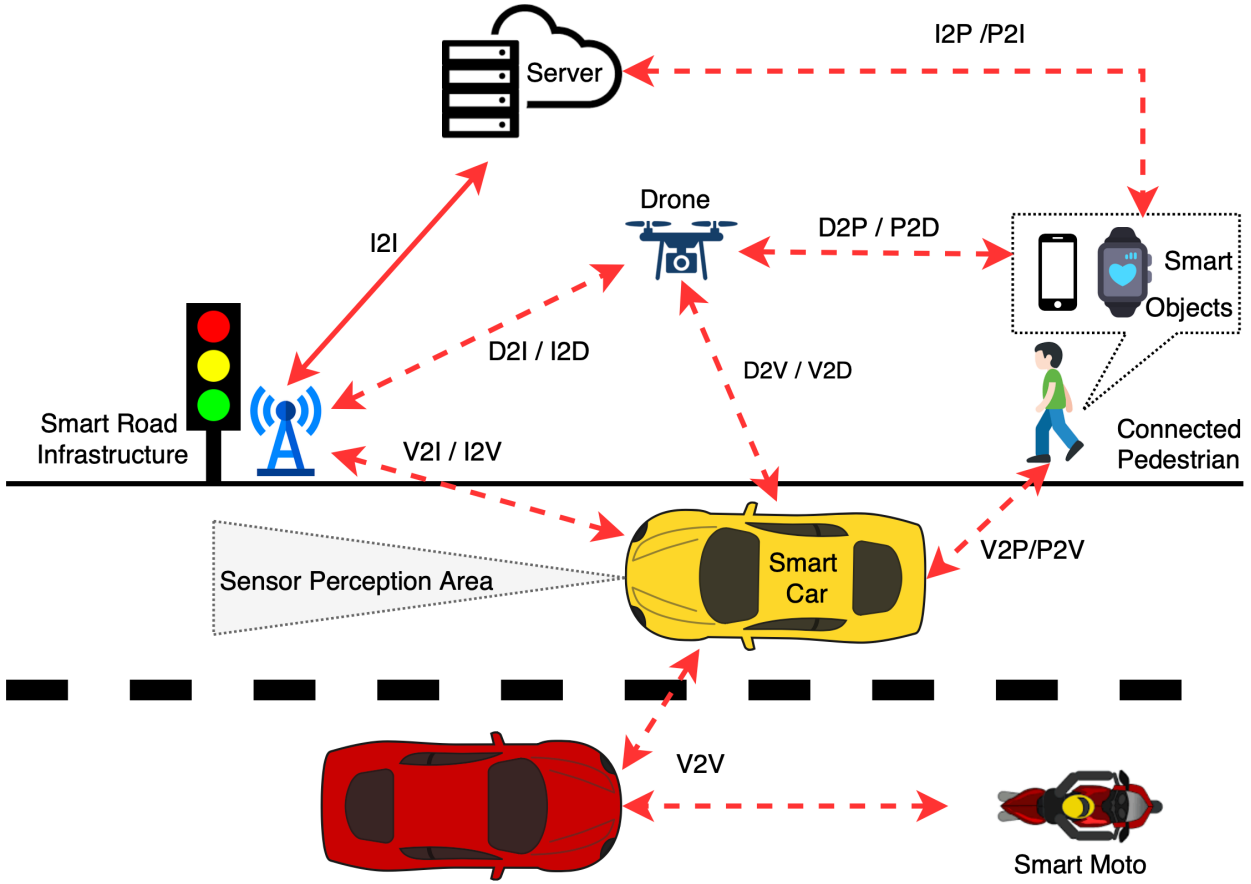
C-ITS networking architecture



C-ITS networking architecture



C-ITS Environment

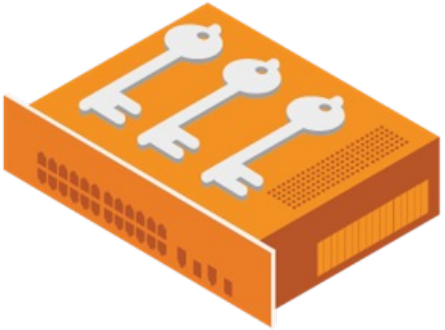


Cooperative Awareness Message (**CAM**), Decentralized Environmental Notification Message (**DENM**), Basic Safety Messages (**BSM**), Signal Phase and Timing (**SPAT**), MapData Messages (**MAP**), In Vehicle Information (**IVI**), Traffic Light Control (**TLC**)

ITSS-R ITSS-V

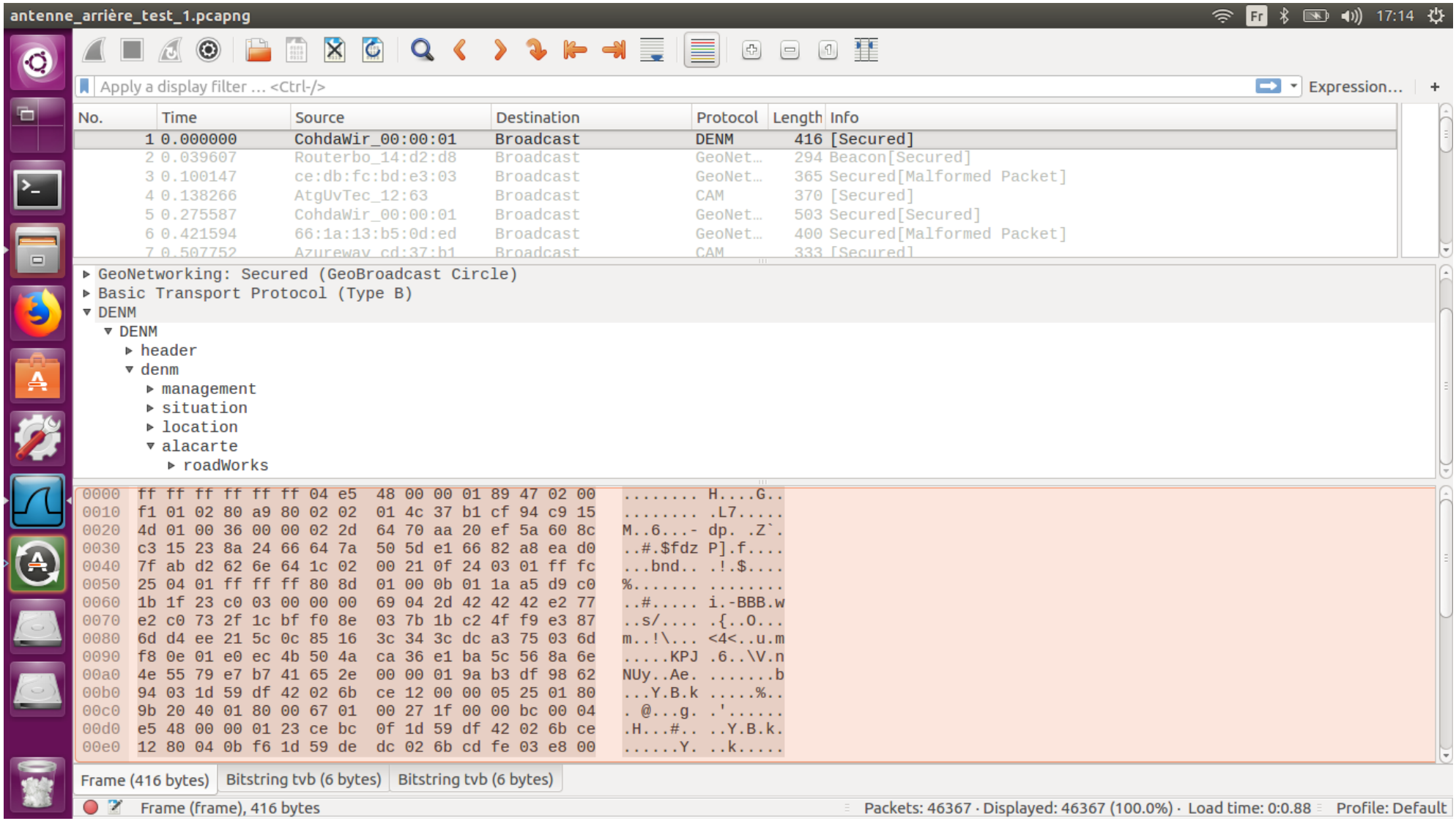

CohdaWireless


Cohda Wireless
USB
ETHERNET
VIC
12 V




Road Side Unit
On Board Unit

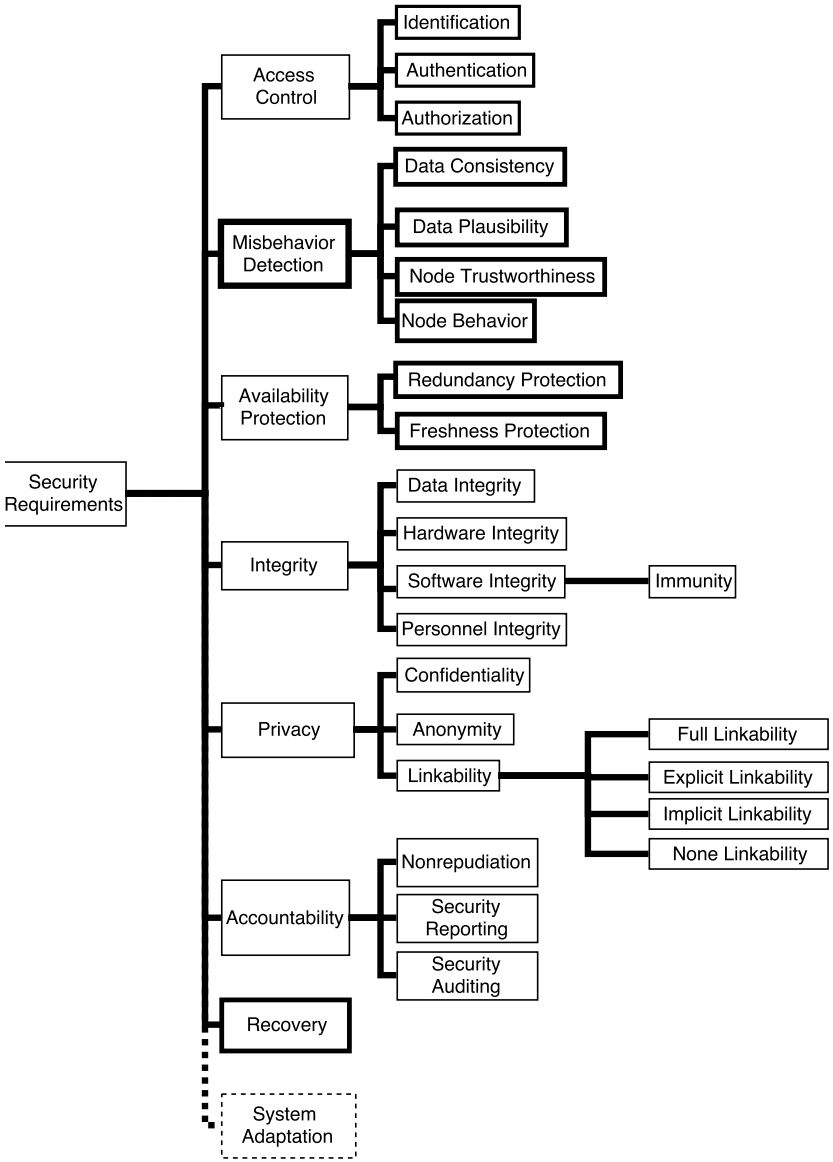
C-ITS Messages



Evolution

- C-ITS applications have evolved and become very greedy in terms of transmitted traffic and used bandwidth
- Huge amounts of data and messages are exchanged continuously, e.g., CAM, DENM and BSM
- Most of the exchanged messages contain critical data that should be confidential
- Numerous requested services require authentication to be accessed

Security and privacy requirements



- Integrity
- Authentication
- Non repudiation
- Privacy (no tracking)
- Authorization
- Confidentiality (some use cases)

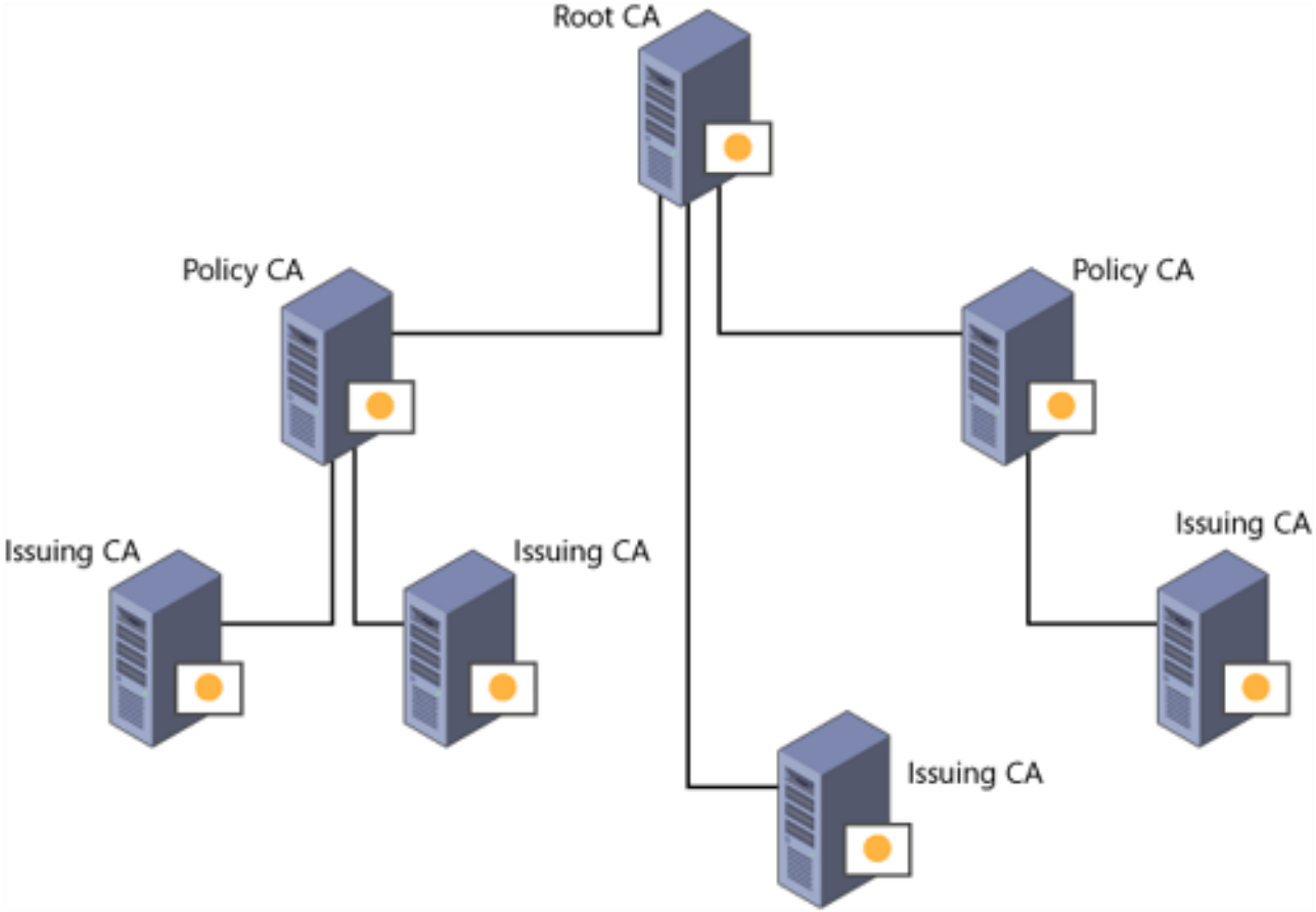
Public Key Infrastructure

- **Public Key Infrastructure**
  - Set of authorities, policies and procedures
  - Manages public-key mechanisms
  - Binds public keys with respective identities of entities
  - Binding is established through a process of registration and issuance of certificates
  - Creates, manages, distributes, uses, stores, and revokes certificates

Security requirements

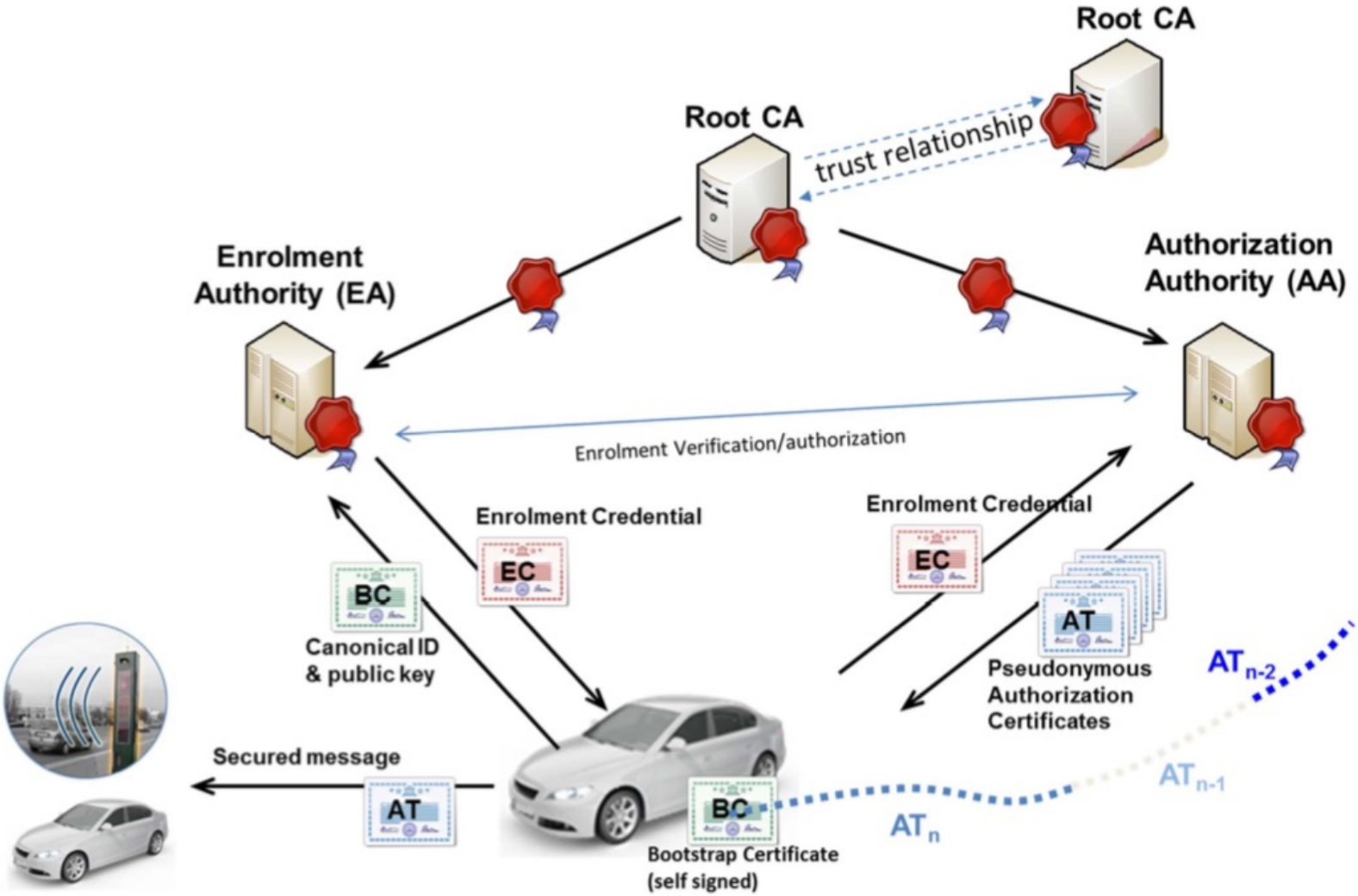
Requirement	Mechanism/Algorithm
Confidentiality	Encryption (ECIES)
Authentication	Certification (PKI), Signature (ECDSA)
Integrity	Signature (ECDSA)
Non repudiation	Signature (ECDSA)
Privacy	Certificate change
Authorization	SSP

C-ITS PKI



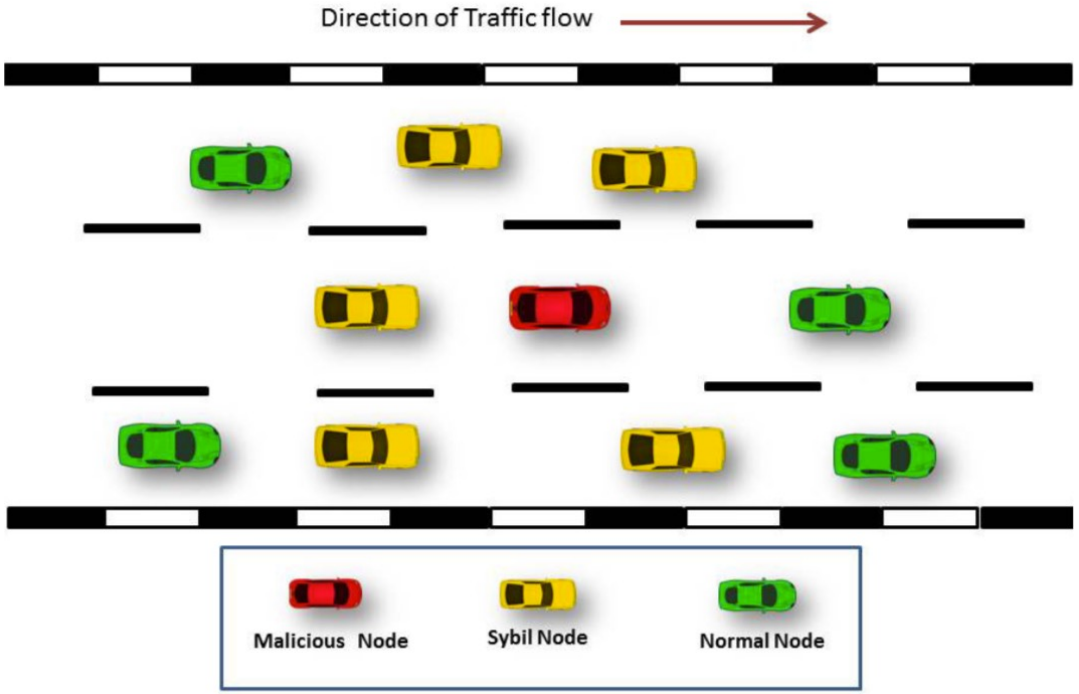
Design of a traditional PKI

C-ITS PKI



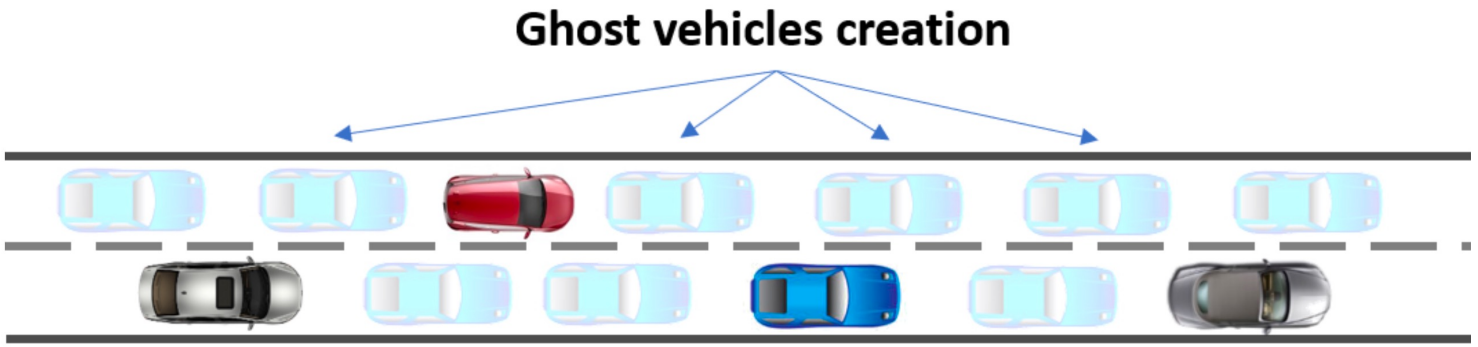
Design of a C-ITS PKI

Sybil attack

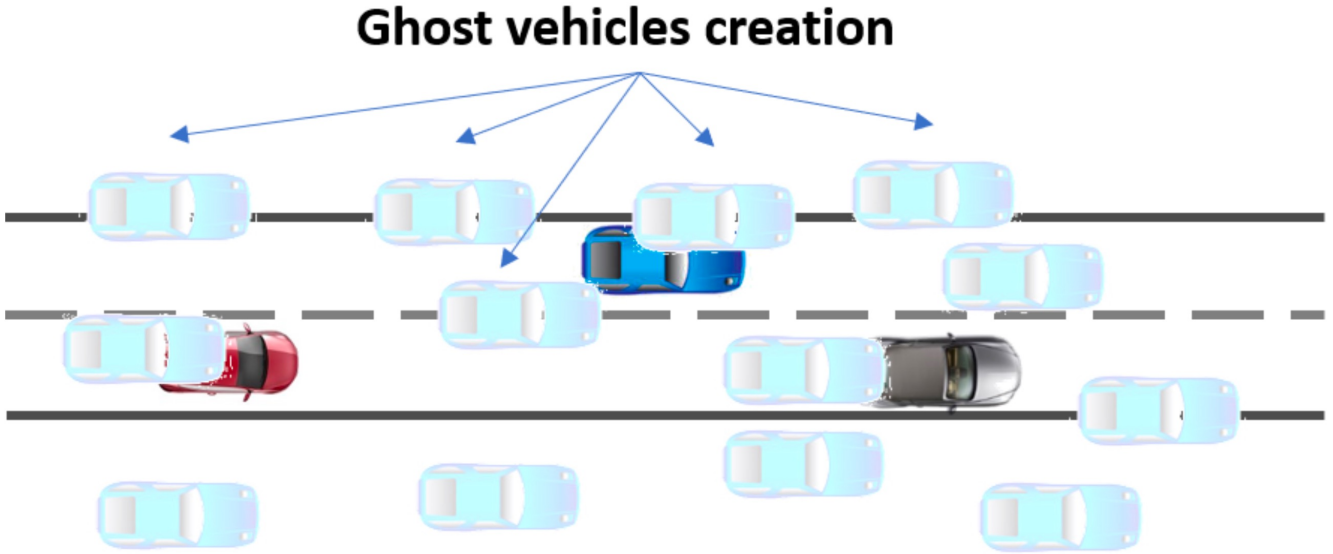


- The attacker node creates different virtual nodes (also called sybil ghosts) in order to have a certain influence on the network's decisions especially in voting based protocols and applications
- The creation of the sybil ghosts is performed by creating different messages using different fake identities and different fake locations

Sybil attack



Sybil goals : (a) Traffic congestion



Sybil goals : (b) Denial of Service

Contribution

- Research requirements
- State of the art review regarding the requirements defined
- Recommendations for a research methodology that can be considered in future works
  - Provision of one dataset for an urban scenario and another dataset for a highway scenario
  - Provision of network model
  - Provision of attack models (three realistic attack scenarios)

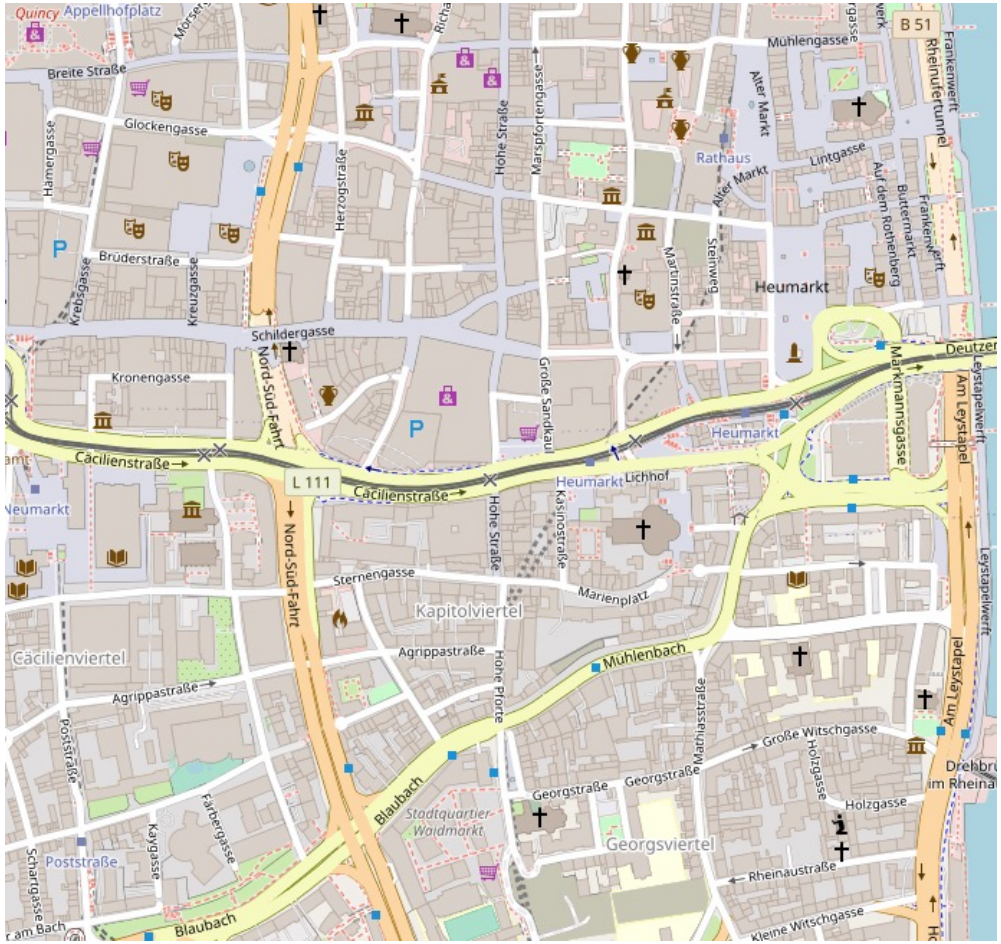
Contribution: Research requirements

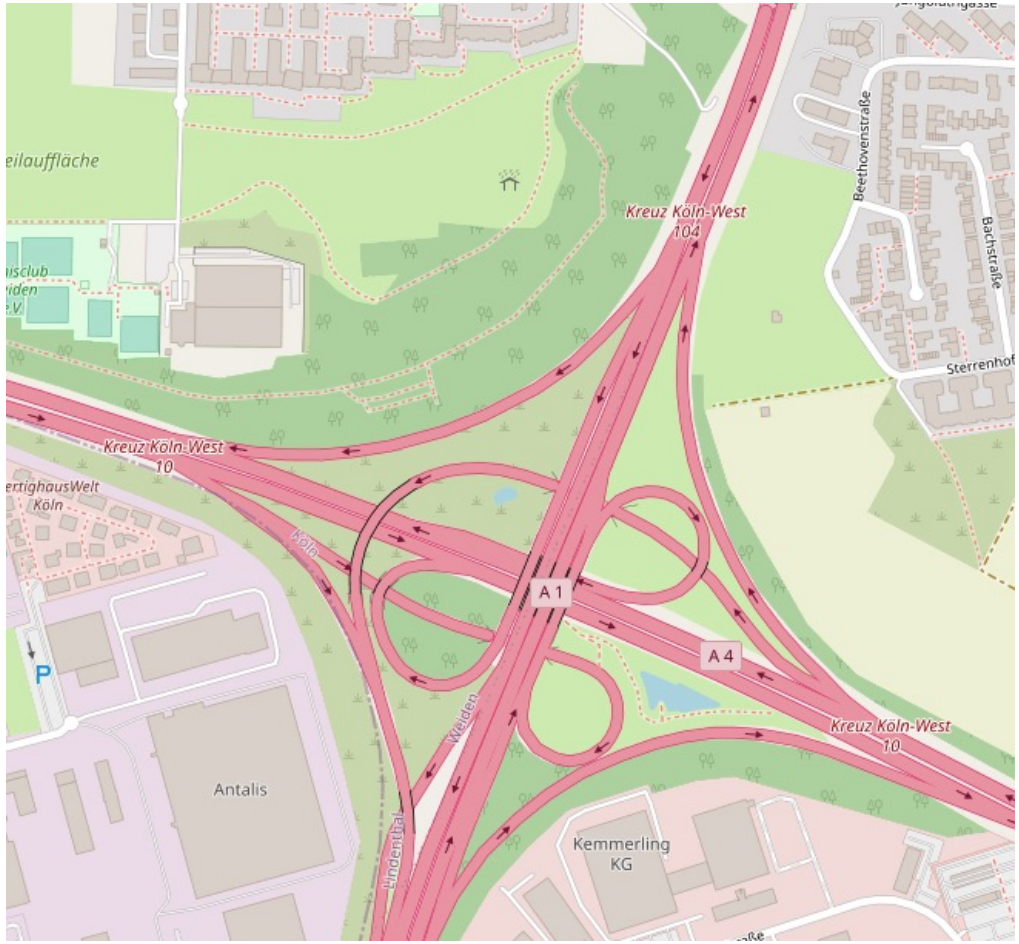
- The proposal of a sybil detection solution that requires the complete modification of the messages structures or their replacement by other structures cannot be considered
- The proposal of a solution that requires a new security architecture or security mechanisms different from the standards cannot be considered
- An approach that relies on a station's history or assumes that a station does not change its identity multiple times during a journey, cannot be considered
- If the history of the vehicle must be considered in the detection process, the linkage of the different PCs must be provided by the Linkage authority while adhering to the PKI disclosure policies

Contribution: State of the art analysis

- Scalability issues
- Do not meet privacy and non-tracking requirements
- Do not satisfy the requirements of current standards (formats of messages, security, and PKI architecture)
- Limited evaluations where only few use case scenarios (such as single lane) were tested

Contribution: recommendations: Network model

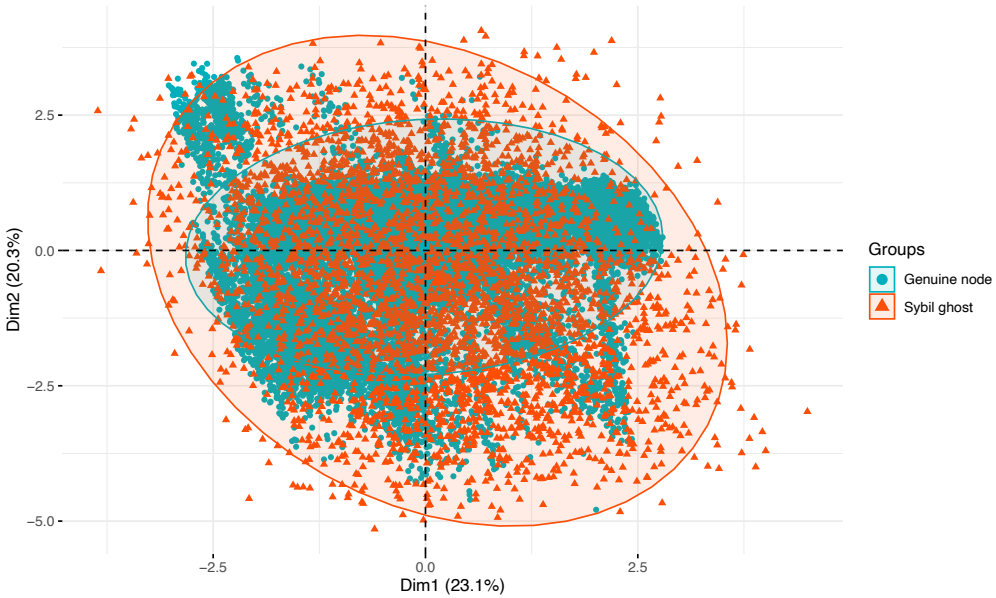




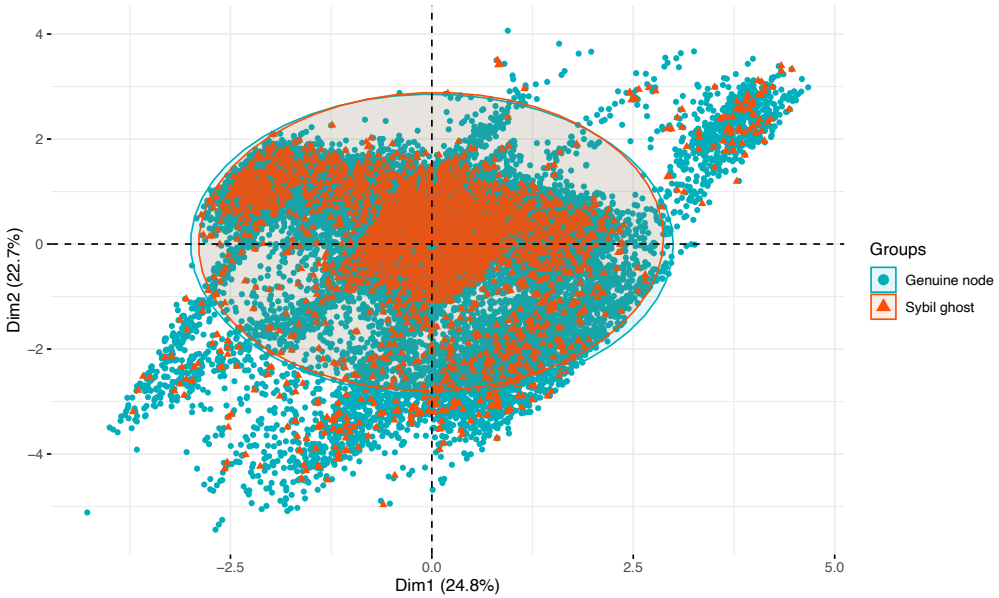
Contribution: recommendations: Attack scenarios

- Sybil scenario with random values
  - Chosen locations from other messages
- Sybil scenario with static values
- Sybil scenario with replayed values

Attack scenarios: statistical characterization



Random scenario



Replayed scenario

Conclusion

- A **position paper** is an essay that presents an arguable opinion about an issue – typically that of the author or some specified entity. Commonly, such a paper will substantiate the opinions or positions put forward with evidences from an extensive objective discussion of the topic.

Future works

- The proposal of a sybil detection approach that cope with different needs and requirements
- The proposal of a fully distributed sybil detection approach that can address scalability issues