Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)

Gilles Guette and Ciarán Bryce

IRISA/INRIA Rennes Bretagne Atlantique
firstname.lastname@irisa.fr

WISTP'08
13-16 may 2008

agenda

1. VANET Overview
2. VANET Security
3. The Trusted Platform Module
4. The Proposed Security Architecture

VANET specificity

Vehicular Ad hoc Network

- Set of mobile nodes
- Highly dynamic and instable network
  - Two vehicles driving in opposite directions may have a connection of only a few seconds
  - In urban environments, nodes leave and join the network at each crossroad
- Few or no access to the infrastructure

VANET Specificity

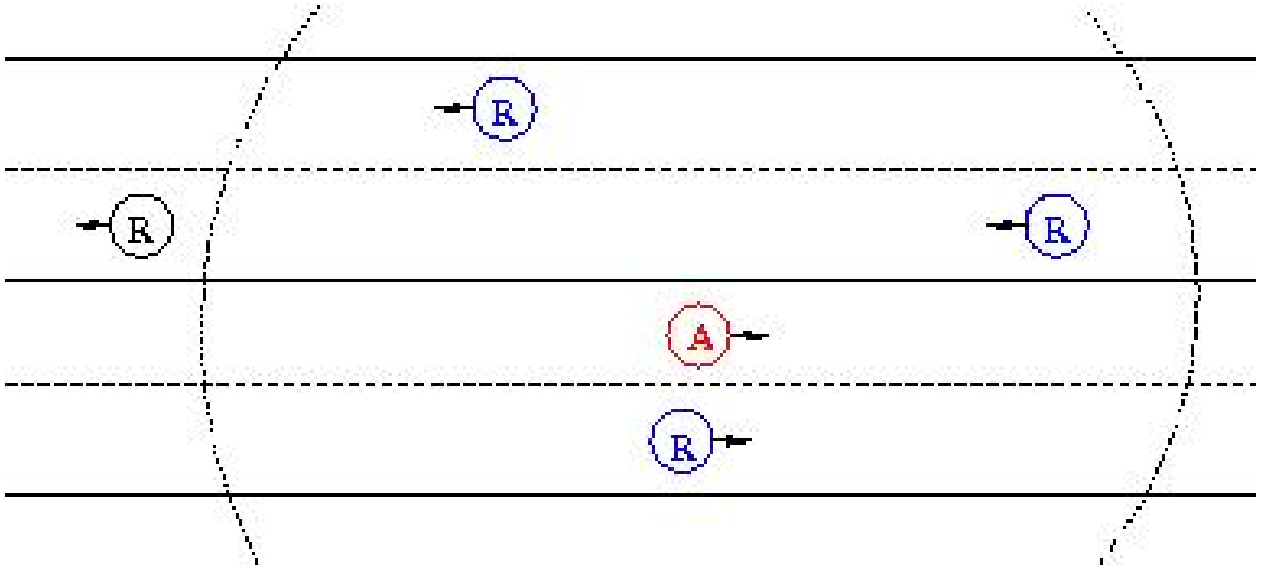
Vehicular Ad hoc Network

- Shared and unreliable communication media
- Essentially broadcasted data
- Connection time between two nodes may be very limited
- Exchanged data may influence driver behavior :
  - Slowing down in case of an accident announcement
  - Taking another direction on a traffic jam announcement
  - *etc.*

VANET Security

Attacks against VANET

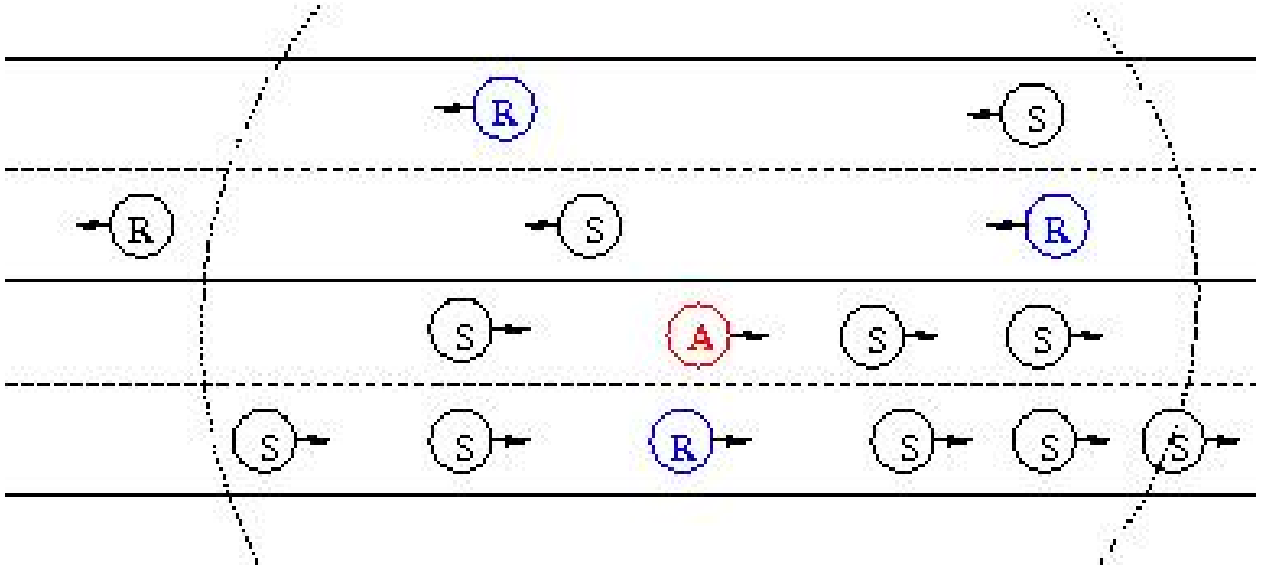
- Multiply nodes on the road : Sybil attack



VANET Security

Attacks against VANET

- Multiply nodes on the road : Sybil attack



VANET Security

Attacks against VANET

- Node impersonation/Taking another node identity
  - routing perturbation
  - engage the liability of another driver
  - provoking collisions while remaining “anonymous"
- Sending false information
  - to provoke collisions
  - to clear the road

VANET Security

Attacks against VANETs

- Vehicle tracking
  - Each vehicle periodically broadcasts an identifier/pseudonym and its position (GPS)
- Data eavesdropping
  - Shared communication medium
  - All vehicles in the communication range receive our messages
  - Messages, identities, pseudonyms, positions may be correlated

Cooperative driving

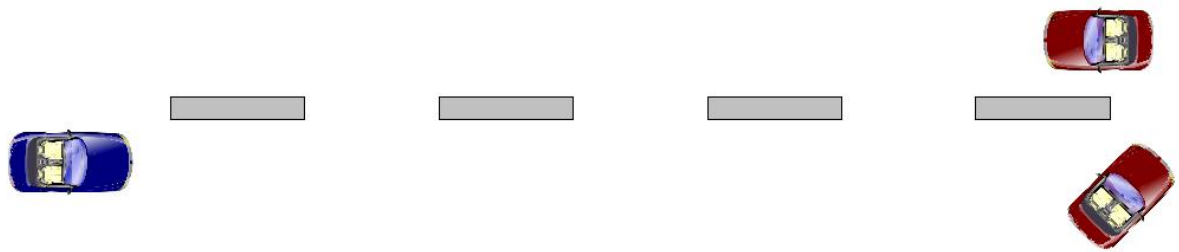
Behavior

- Data are exchanged to enhance road safety
- Messages coming from vehicles in the opposite direction give information on the road in front of you
- Event announcement can be forward by vehicle in front of you

Cooperative driving

Example

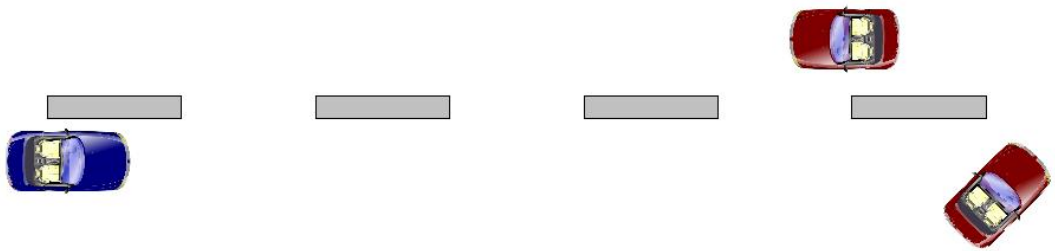
- We want to have this :



Cooperative driving

Example

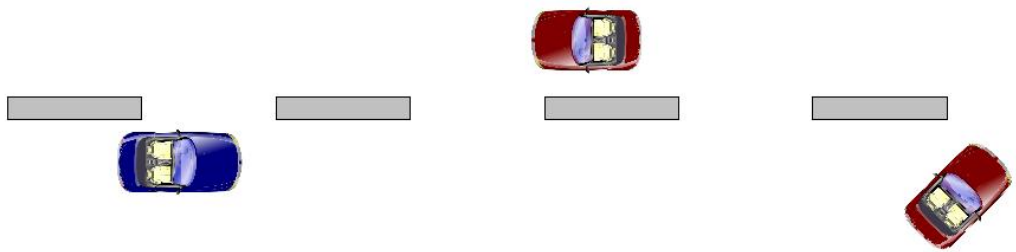
- We want to have this :



Cooperative driving

Example

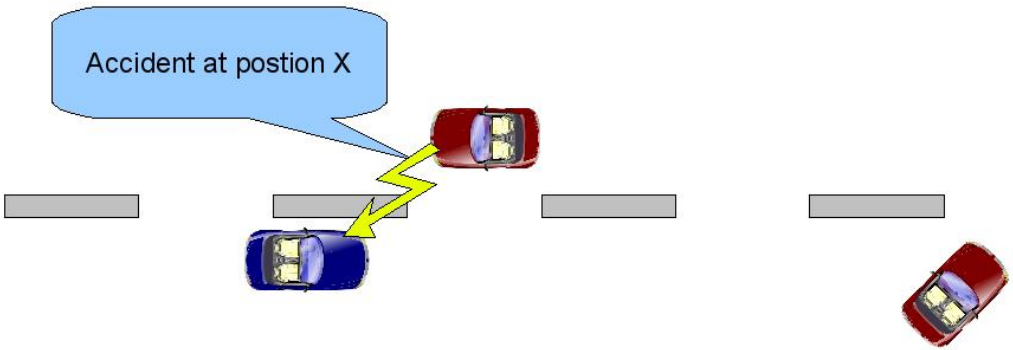
- We want to have this :



Cooperative driving

Example

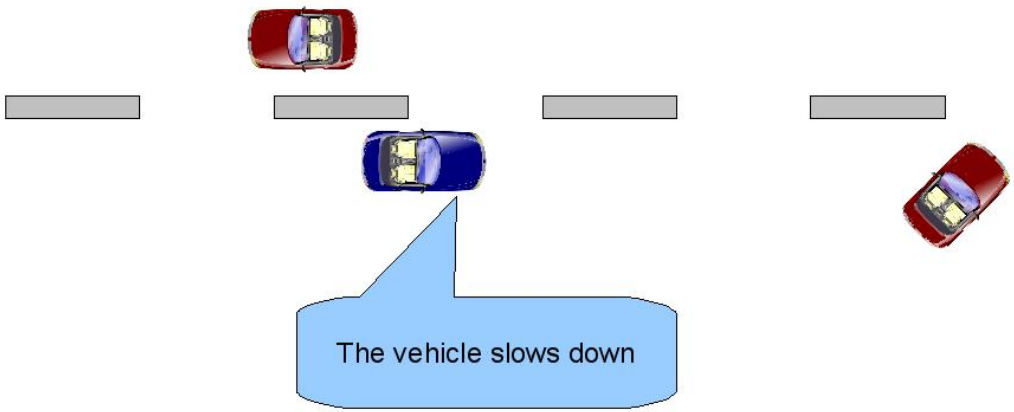
- We want to have this :



Cooperative driving

Example

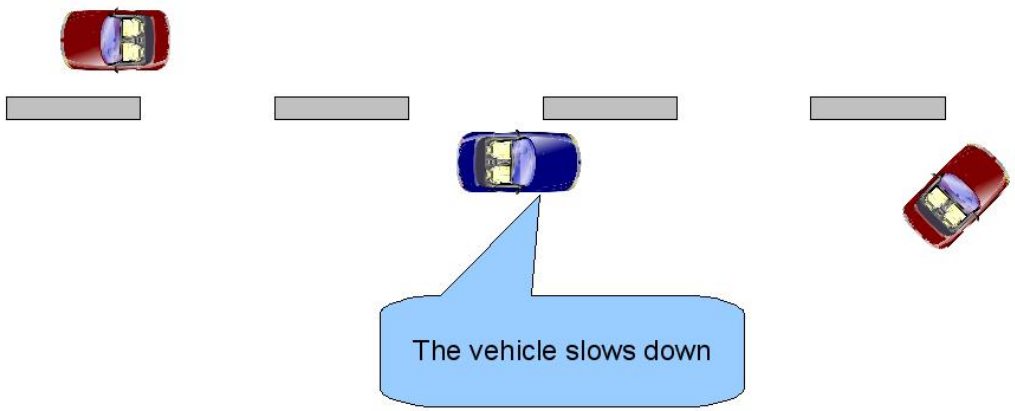
- We want to have this :



Cooperative driving

Example

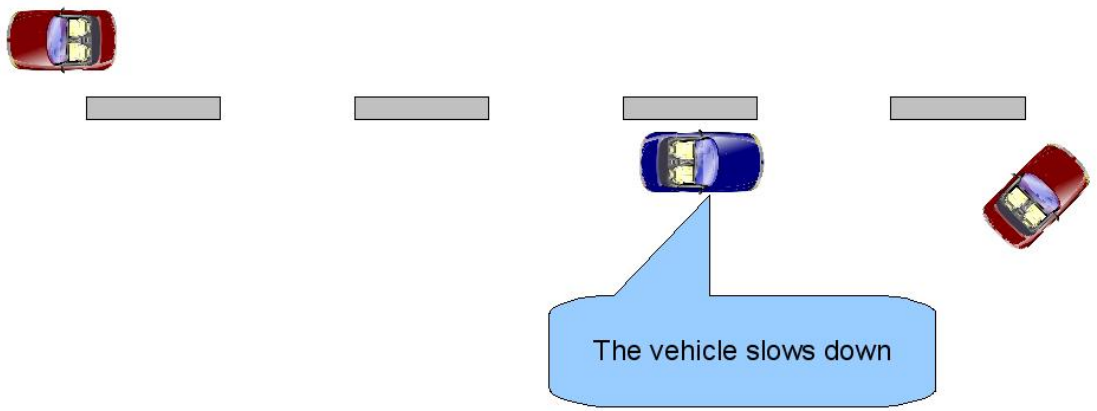
- We want to have this :



Cooperative driving

Example

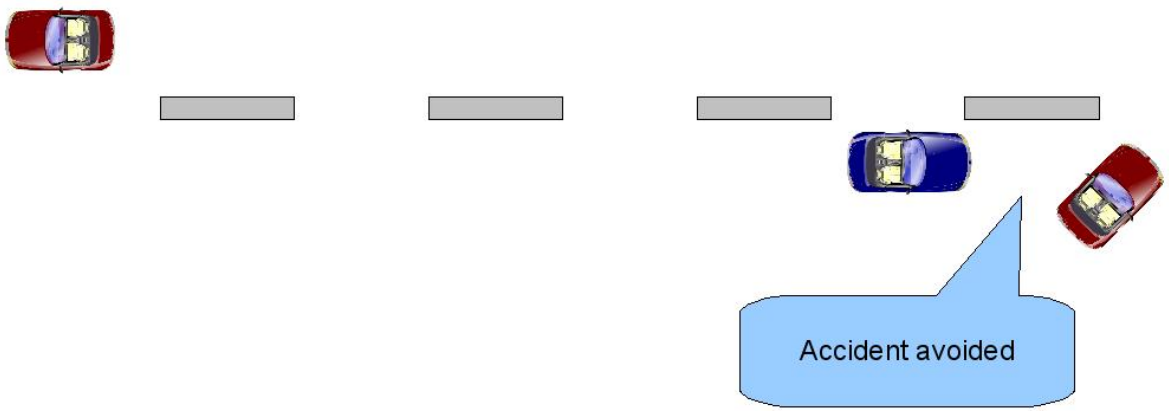
- We want to have this :



Cooperative driving

Example

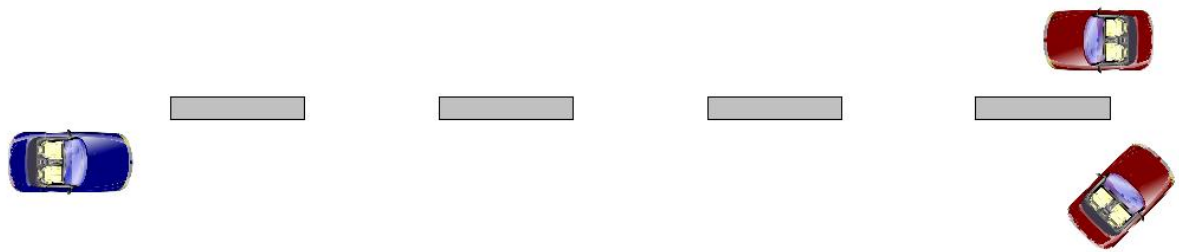
- We want to have this :



Cooperative driving

Example

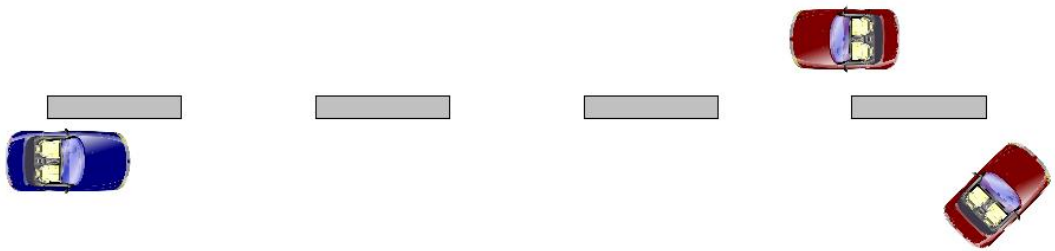
- We want to avoid this :



Cooperative driving

Example

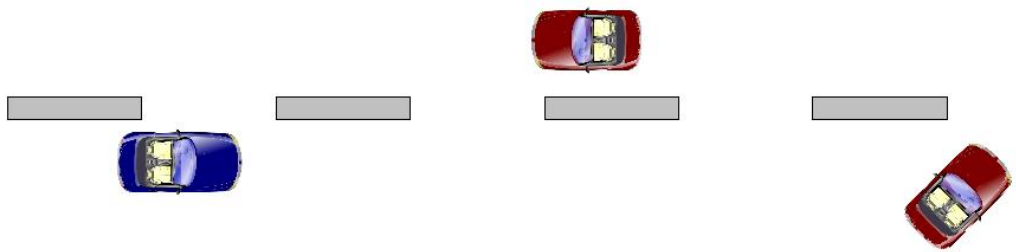
- We want to avoid this :



Cooperative driving

Example

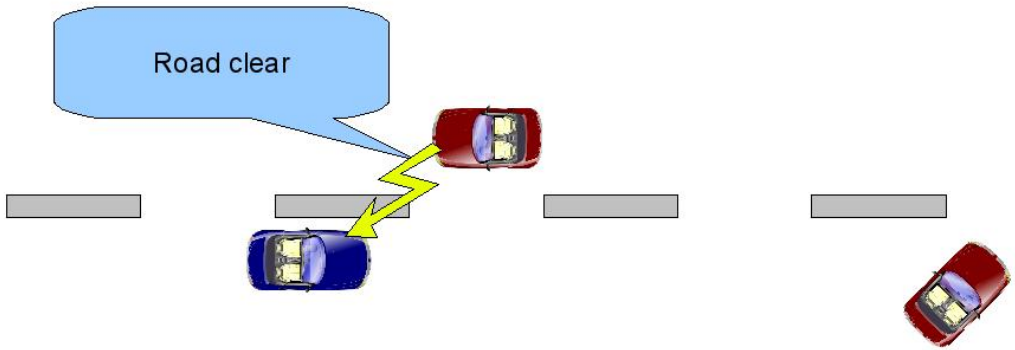
- We want to avoid this :



Cooperative driving

Example

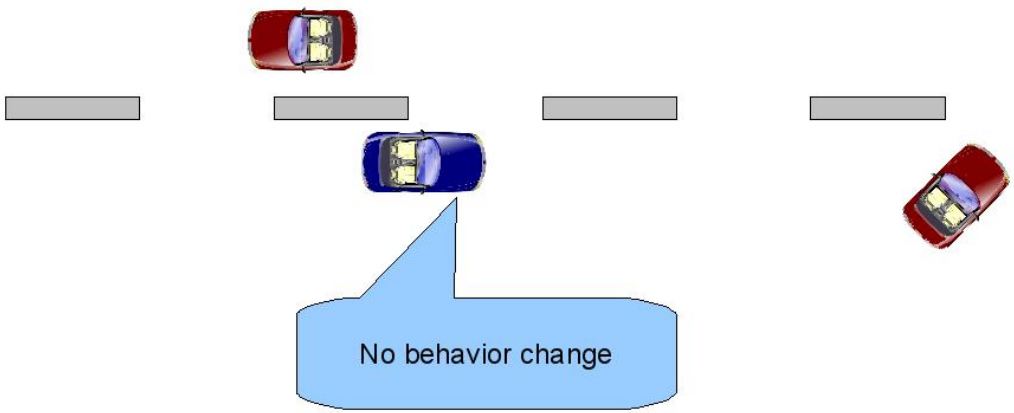
- We want to avoid this :



Cooperative driving

Example

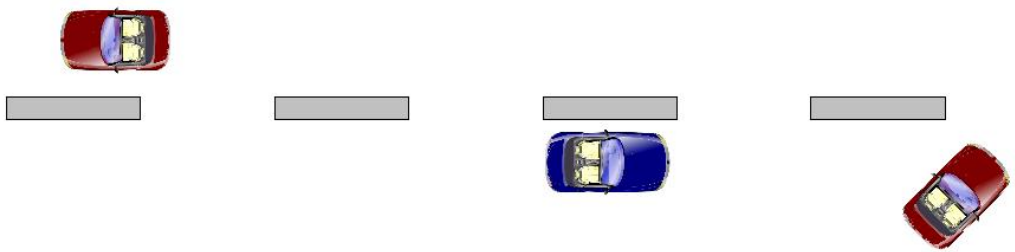
- We want to avoid this :



Cooperative driving

Example

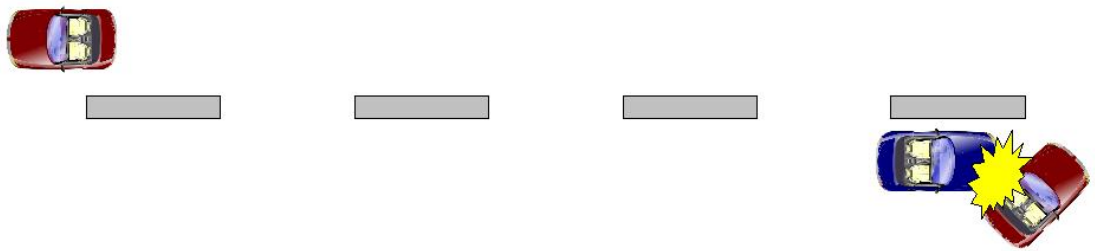
- We want to avoid this :



Cooperative driving

Example

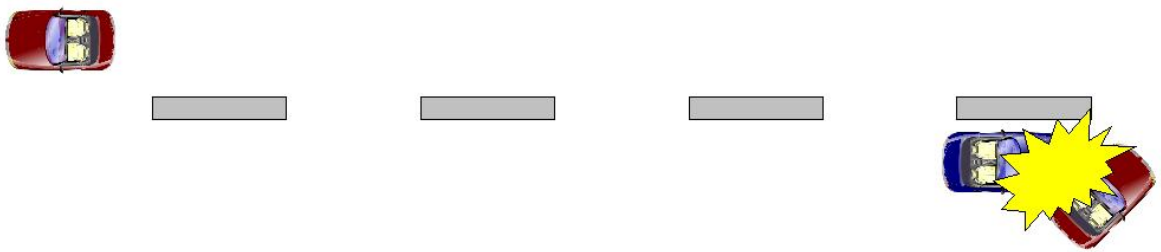
- We want to avoid this :



Cooperative driving

Example

- We want to avoid this :



Cooperative Driving

Security needs

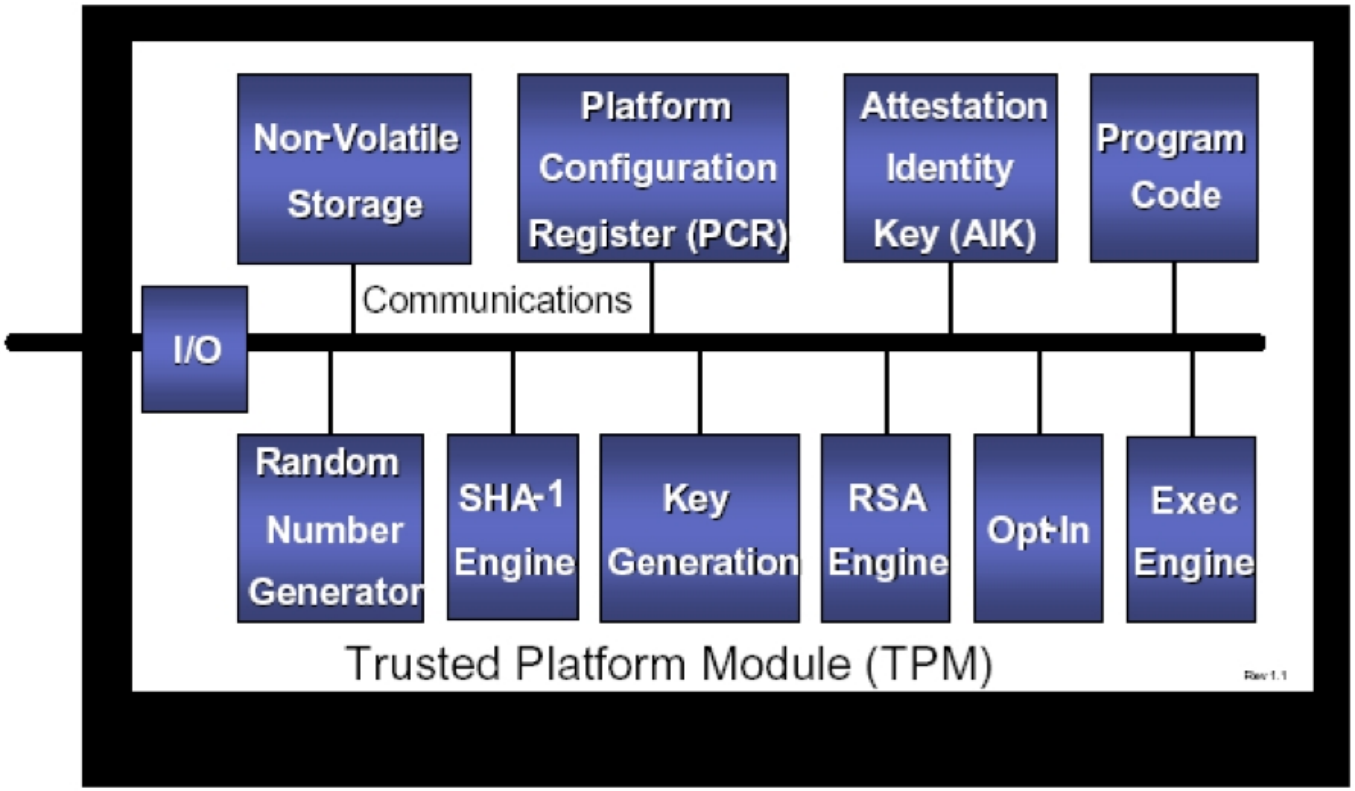
- We need :
  - to protect sent messages from modification (forged message)
  - to know if a message is sent by a real node (sybil attack, forged message)
  - to protect the node identity/pseudonym (node impersonation)
  - to find the responsible driver of an accident (liability)

The Trusted Platform Module

TPM overview

- Secure piece of hardware with cryptographic capabilities
- Able to protect and store data in shielded location
- Provides solutions to our problems
  - Able to generate RSA keys and verify signatures
  - Able to provide integrity measurement and integrity reporting
  - Able to store credentials

The Trusted Platform Module



The Trusted Platform Module

TPM overview

- A vehicle can trust another if the latter can demonstrate that it can be trusted (not tampered, verifiable software, *etc.*)
- The embedded credentials can be signed by the manufacturer (responsibility of the embedded devices)
- Credentials and Attestation Identity Keys may be updated during the technical review of the vehicle
- The TPM is used to check embedded software and the signed information that may be received

Exploiting the TPM for Use Case Security

TPM use

- At the first boot, the TPM measures embedded application
- The TPM stores this measurement in a dedicated register
- The TPM can check that the application code has not been modified by a malicious person
- Modified applications cannot access to secure material such as keys or stored values

Exploiting the TPM for Use Case Security

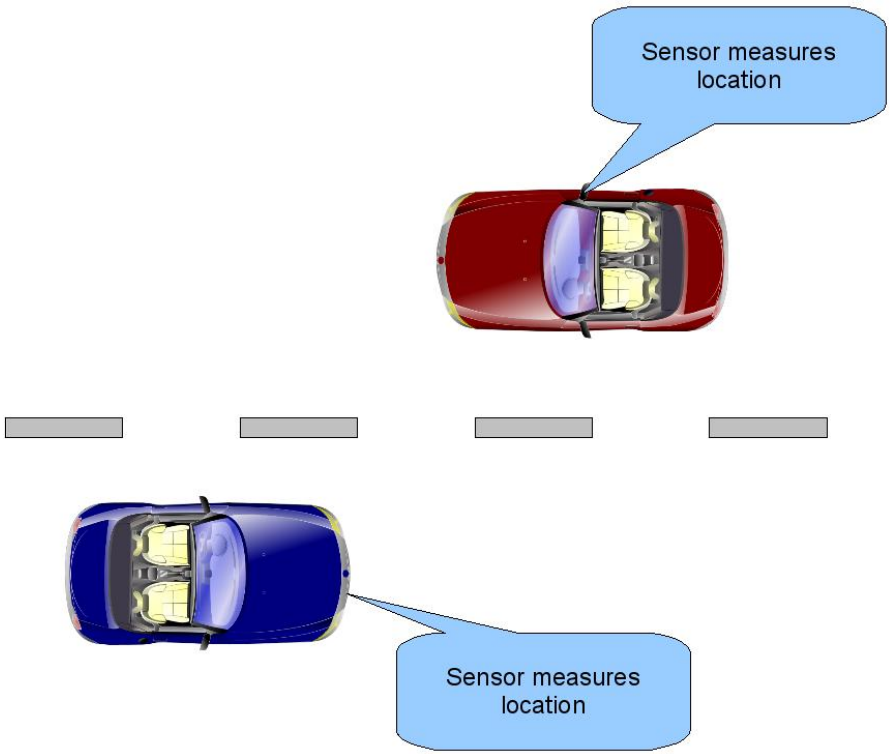
Some features of TPM

- Auto-measuring
  - Some measured data can be protected by the TPM : acceleration, speed, tire denseness
  - Data useful in vehicle platoon scenario
- Challenge-Response protocol
  - Car that are close together should possess same data : location, temperature, *etc.*
  - Cars can challenge each other to detect some measurement errors, or erroneous sensors

Exploiting the TPM for Use Case Security

Example

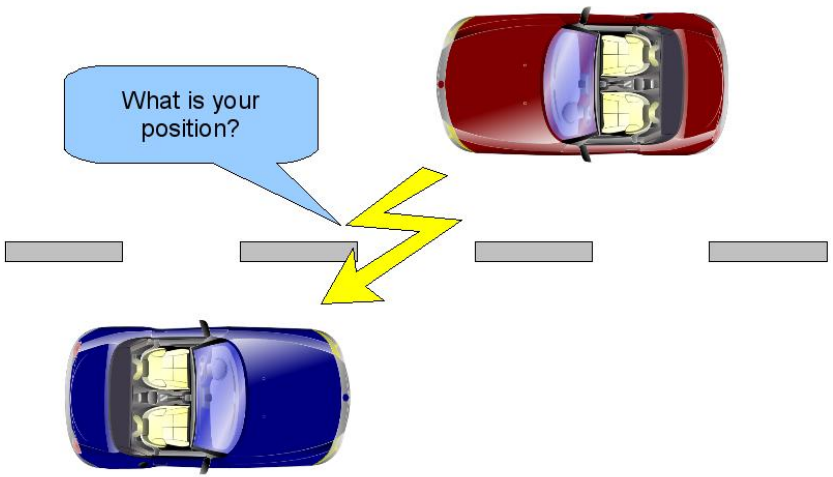
- Challenge-Response protocol



Exploiting the TPM for Use Case Security

Example

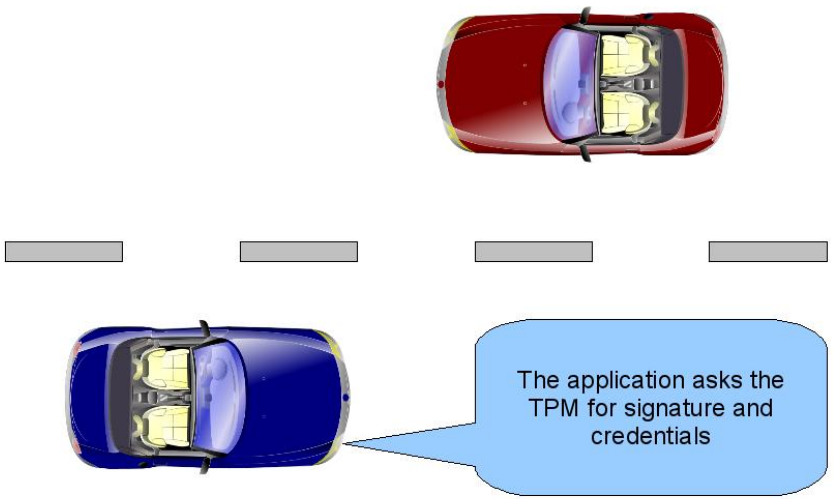
- Challenge-Response protocol



Exploiting the TPM for Use Case Security

Example

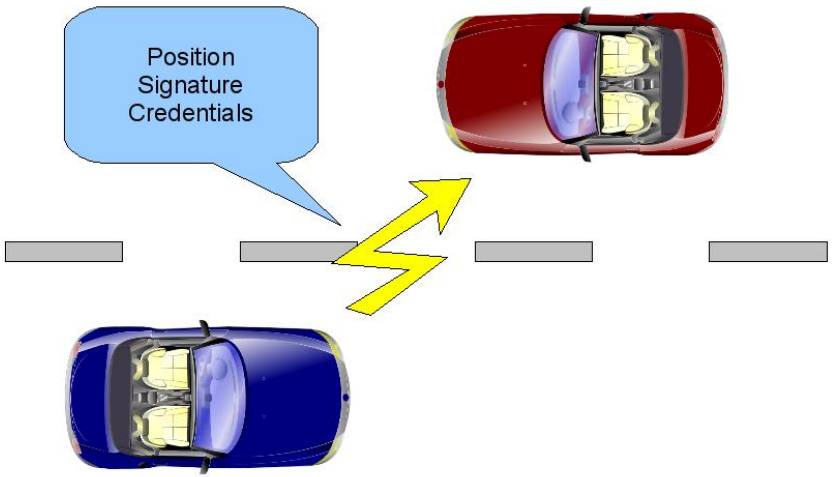
- Challenge-Response protocol



Exploiting the TPM for Use Case Security

Example

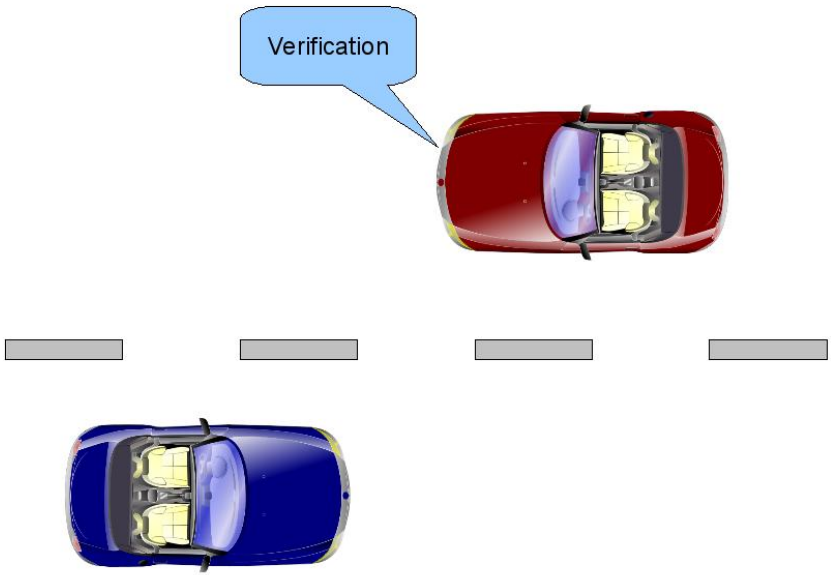
- Challenge-Response protocol



Exploiting the TPM for Use Case Security

Example

- Challenge-Response protocol



Conclusion and future work

Conclusion

- Vehicular Ad hoc Networks need security
- Trusted Platform Modules seem to provide solutions :
  - to detect attacks and protect cryptographic and application data
  - to enhance VANET security

Conclusion and future work

Future work

- Investigate the TPM management and the deployment model
- How to update the application code
- How to enhance the way certificates are handled