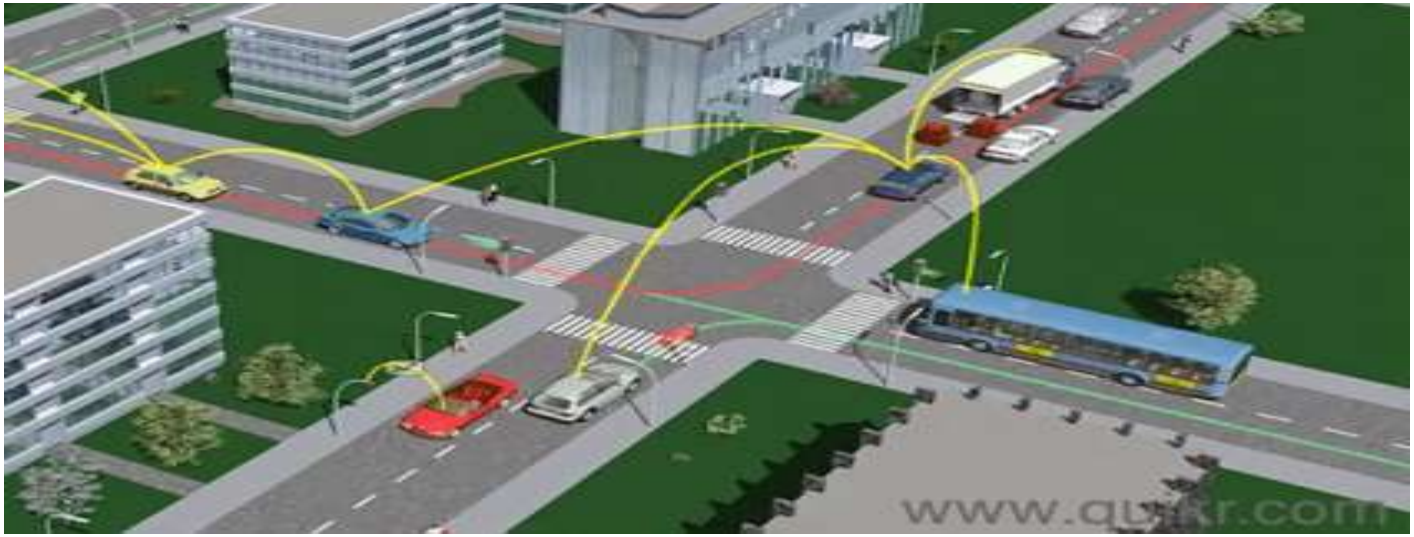
Driving for Big Data?

Privacy Concerns in Vehicular Networking

Eckhoff & Sommer



UNIK4750
Angélique Colle

- A call for a stronger emphasis on privacy in networked vehicules
  - Vehicules communicate with each others, roadside infrastructure etc.
  - A huge amount of information can be collected, and exploited.
  - Privacy protection is not integrated in developing and testing new vehicular network technologies.

Strategical aspects

- Safety versus privacy
  - Safety usually surpasses privacy when up against each other
- The amount of data and what it may imply at a later stage
  - Traffic supervision both by roadside units or other vehicules who may forward broadcasted messages later.
- Privacy, and how it should be resolved, is mentioned, but not actually addressed
- Retrofitting privacy will not work

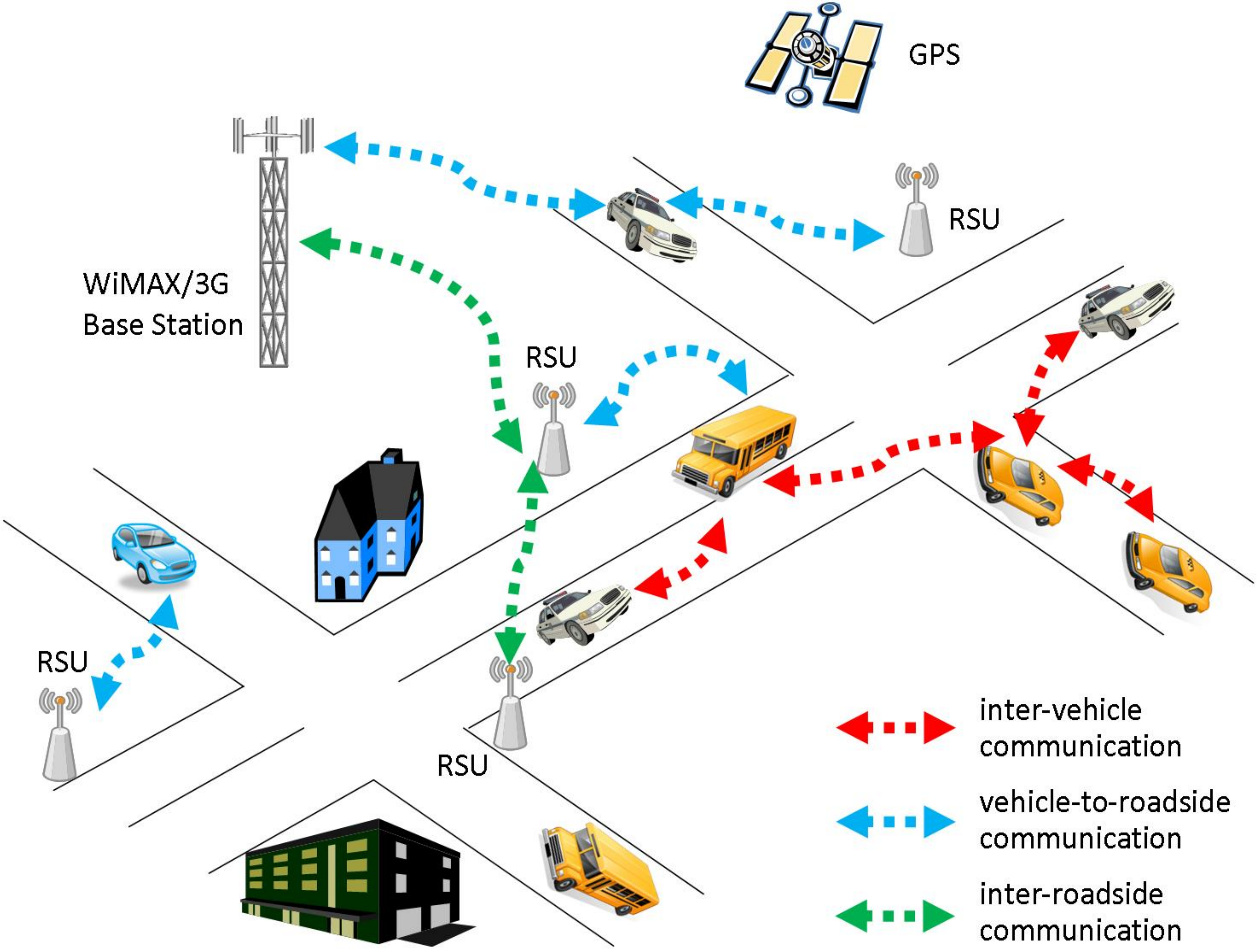
Practical aspects

- The authors call for three things:
  - An understanding on how privacy provisions affect other applications related to safety and comfort
  - Measurement of privacy protections in simulations already in use for performance testing/evaluations
  - Meaningful privacy metrics in order to convince decision makers

Key findings

- Pseudonyms/public-key infrastructure:
  - Preinstalled certificate (base identity) used only to request pseudonyms from a CA. Used to sign and send messages over wireless channel.
  - Problem: drivers can be reidentified
    - Pick up signed messages at different locations.
  - Counter measure: a pool of pseudonyms
    - How: drivers use a different pseudonyms for each message
    - Problem: may pose a problem for other applications (confusion)
    - Counter: pseudonym-changing strategies
      - No suggestion on how this should be done – problematic
      - Occasional change of pseudonyms has been deemed insufficient if a malicious actor witness the change.
  - Signing authority have the ability to resolve the base identity.
  - Accountability in case of hit-and-run, stolen vehicules etc.
  - Reality: Approaches to solve the resolving of pseudonyms may never be deployed due to the need for «*law enforcement access under appropriate circumstances*» (IEEE 1609.2 – 2013)

- Users may not, themselves, be able to turn off some of the networked devices because of mandatory implementations etc.
  - Ex. eCall
- Broadcasting of unencrypted messages
  - Some messages have to be readable to everyone, such as awareness messages, and thus have to be unencrypted – polling.
    - Ex. AIS on boats
  - Contain detailed information on the vehicule’s position, speed information etc.
  - When used to inform other vehicules on hazards along the road, it may include sequence numbers.


GPS
WiMAX/3G
Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

- System operators, providers, authorities may detect any sort of traffic offense, by checking steering wheel, exterior lights, direction etc.
- Counter: coopertaion of mutiple institutions to resolve a pesudonym.

Strengths and weaknesses

- Future technology
- Short summary
- Easy to read
- Focus on pseudonyms
- Weaknesses of suggestions proposed in IEEE 1609.2-2013 and ETSI 102941-v.1.1.1 (IEEE WAVE and ETSI ITS G5)
- Raises a dilemma that is known, safety/privacy, but may not be sufficiently focused on when manufacturers develop and politicians suggests new legislations