Internet of Things
2016/2017

Intelligent Transportation Systems

Johan Lukkien

John Carpenter, 1982
Overview

• In four sections

  – Intelligent Transportation Systems
  – Vehicle to vehicle: safety applications
  – Vehicle to infrastructure: information applications
  – Safety, privacy and security
ITS
Guiding questions

- What are goals of ITS (Intelligent Transportation Systems)?
- How is the general structure of ITS?

- Goal:
  - Study a larger example of an IoT system.
  - Show how the different parts fit together.
Vehicles operate using networked ICT
In-vehicle networks

- **Networks of ECUs**
  - 40-80 in a modern car

- Designed for
  - cooperative behavior
  - specialist (remote) management / diagnostics

- Gateway support for *isolation*

<table>
<thead>
<tr>
<th></th>
<th>Flexibility</th>
<th>Predictability</th>
<th>Dependability</th>
<th>Bandwidth</th>
<th>Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Powertrain</td>
<td>low</td>
<td>high</td>
<td>high</td>
<td>high</td>
<td>N/A</td>
</tr>
<tr>
<td>Chassis</td>
<td>some</td>
<td>high</td>
<td>high</td>
<td>high</td>
<td>N/A</td>
</tr>
<tr>
<td>Body/Comfort</td>
<td>some</td>
<td>some</td>
<td>some</td>
<td>low</td>
<td>N/A</td>
</tr>
<tr>
<td>Telematics</td>
<td>high</td>
<td>some</td>
<td>low</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>Passive Safety</td>
<td>low</td>
<td>high</td>
<td>high</td>
<td>high</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Vehicles become parts of a larger whole

- Vehicle to Vehicle (V2V) communication
  - ad-hoc
  - collaborative applications

- Applications are distributed

- Actuation may pass by driver control
Physical organization in V2V

Moving vehicles connect ad-hoc to each other and to access points of the ambient infrastructure. **Technology:** IEEE 802.11p

Road side units (RSUs, network central devices) are connected to the Internet. The network consists of:

- **IEEE 802.16e** (WiMAX)
- **3G, 4G**
- **IEEE 802.3** (ethernet)
- **IEEE 802.11** (WiFi)

IP-based network with wide-area coverage, wireless or wired.
## V2V ad-hoc

<table>
<thead>
<tr>
<th>Bottom layer</th>
<th>Middle layer</th>
<th>Single hop (no hop)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multi hop</strong></td>
<td>(ambient infra structure)</td>
<td>(access points)</td>
</tr>
<tr>
<td><strong>Multi hop</strong></td>
<td>Most general case: moving clusters through ambient infra structure (V2I) + ad-hoc networks (V2V)</td>
<td>Moving clusters connecting to access points (V2I) + ad-hoc networks (V2V)</td>
</tr>
<tr>
<td><strong>Single hop</strong></td>
<td>Moving nodes connecting to ambient infra structure</td>
<td>Moving nodes connecting to access points</td>
</tr>
</tbody>
</table>
Multiple technologies

C2C-CC (Car2Car Communication Consortium initiated by six European car manufacturers) architecture (~2010)

IEEE 802.11p
IEEE 802.11a/b/g
Other wireless technology (full coverage)
### 3G/4G/5G

<table>
<thead>
<tr>
<th>Bottom layer</th>
<th>Middle layer</th>
<th>Multi hop</th>
<th>Single hop (no hop)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multi hop</strong></td>
<td>(ambient infra structure)</td>
<td>Moving clusters connecting to access points</td>
<td></td>
</tr>
<tr>
<td>+ ad-hoc networks</td>
<td>+ ad-hoc networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Single hop</strong></td>
<td>Moving nodes connecting to ambient infra structure</td>
<td>Moving nodes connecting to access points</td>
<td></td>
</tr>
</tbody>
</table>
A conceptual view

- Example data flows:
  - (1) gather detailed driving data to determine
    - local weather
    - road condition
  - (2) accident prevention by direct intervention
  - (3),(4) informing driver about upcoming road conditions

- Traffic management and control
  - Traffic management
  - Traffic control
  - Traffic information

- End-user applications
  - Car sharing
  - Event management

- Example data flows:
  - (1) gather detailed driving data to determine
    - local weather
    - road condition
  - (2) accident prevention by direct intervention
  - (3),(4) informing driver about upcoming road conditions

- Internet, V2I

- V2V network

- Local Control
  - In-car network

- Driver Control
  - V2V network
Guiding questions

• What are goals of ITS (Intelligent Transportation Systems)?
• How is the general structure of ITS?

• Goal:
  – Study a larger example of an IoT system.
  – Show how the different parts fit together.
V2V
Guiding questions

• Which V2V applications are there?
• How does V2V communication and how do applications work?

• Goal:
  – Study a larger example of an IoT system.
  – Show how the different parts fit together.
V2V: goals and characteristics

• Goals
  • Safety
  • Comfort
  • Traffic efficiency

• Main characteristics
  • Very high mobility of network nodes
  • Fully distributed system
  • IEEE 802.11p (CSMA/CA) as underlying technology

• Safety applications have strict requirements on
  • Reliability
  • Delay
<table>
<thead>
<tr>
<th>Scenario and warning type</th>
<th>Scenario example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rear end collision scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>Forward collision warning</td>
<td><img src="image" alt="Forward collision warning" /></td>
</tr>
<tr>
<td>Approaching a vehicle that is decelerating or stopped.</td>
<td></td>
</tr>
<tr>
<td>Emergency electronic brake light warning</td>
<td><img src="image" alt="Emergency electronic brake light warning" /></td>
</tr>
<tr>
<td>Approaching a vehicle stopped in roadway but not visible due to obstructions.</td>
<td></td>
</tr>
<tr>
<td><strong>Lane change scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>Blind spot warning</td>
<td><img src="image" alt="Blind spot warning" /></td>
</tr>
<tr>
<td>Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.</td>
<td></td>
</tr>
<tr>
<td>Do not pass warning</td>
<td><img src="image" alt="Do not pass warning" /></td>
</tr>
<tr>
<td>Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.</td>
<td></td>
</tr>
<tr>
<td><strong>Intersection scenario</strong></td>
<td><img src="image" alt="Intersection scenario" /></td>
</tr>
<tr>
<td>Blind intersection warning</td>
<td></td>
</tr>
<tr>
<td>Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.</td>
<td></td>
</tr>
</tbody>
</table>

Source: GAO analysis of Crash Avoidance Metrics Partnership information.

from: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014
ADAS

• Equipped with a user interface these applications end up as Advanced Driver Assistance Systems (ADAS)
  – e.g. a vibrating seat or other warning

5 steps to full automation

• Currently under R&D:
  – Collaborative Adaptive Cruise Control
    • 2 or more vehicles in a platoon
  – multiple CACC: merging
C’est le Rush

https://www.youtube.com/watch?v=Johmxw3cspA
How does this work?

• It is cooperative, dynamic and ad-hoc

• Two different approaches, same network technology (IEEE 802.11p)
  – **EU**: ETSI TC ITS standards, using Geo-networking

• Essentially: vehicles emit *periodically* or *event-driven* status information
  – called *Basic Safety Messages* (BSM, US)
  – and *Cooperative Awareness Messages* (CAM, EU)
IEEE 802.11p characteristics

• Part of the full IEEE 802.11 (2800page) specification
  – enhancements for use in Vehicles
• Connect without BSS (BSS: stations with access point):
  – no association, authentication
  – just direct, ad-hoc messaging when in range
• Support prioritizing of traffic: EDCA (from 802.11e)

• Deal with high relative speeds of terminals
  – speed 3-27Mbit/s per channel, typically 6Mbit/s per channel
• UTC-based timing reference for synchronizing time accurately
• Channels in the 5.9 GHz range (~300m in free field, max 1000)
Rate-adaptation Based Congestion Control for Vehicle Safety Communications, PhD thesis Tessa Tielert

Johan J. Lukkien, j.j.lukkien@tue.nl
TU/e Informatica, System Architecture and Networking
ETSI GeoNetworking

- ETSI GN
  - Intended to work on different technologies besides IEEE 802.11p
- ITS-G5: implementation on IEEE 802.11p
  - three frequency classes
    - A: safety
    - B: non-safety
    - D: future
  - control and service channels
    - common control channel: primary channel for unsolicited traffic
  - protocols for channel switching

Johan J. Lukkien, j.j.lukkien@tue.nl
TU/e Informatica, System Architecture and Networking
23-Nov-16
ETSI GeoNetworking

- ETSI GN provides ad-hoc local connectivity
  - Addressing: 48bit interface address extended with station information
  - use of a location table about neighbors
    - updated by info from incoming messages
  - GN routers: role of some stations
  - Services, e.g:
    - SHB: single hop broadcast (repeated for given number of time or period)
    - unicast
    - geobroadcast: limit physical extent and limited number of hops
  - BTP: add multiplexing to the GN services
ETSI GN: Internet connectivity

- IP packets forwarded to IPv6 gateway or destination by GN protocols (services)

- Adaptation layer provides transparency
  - GN6ASL

- IPv6 of lower importance than safety applications

- Address assignment: IPv6 autoconf

AU: application unit

CCU: Communication and control unit

(draft) Vehicle to Internet communications using the ETSI ITS GeoNetworking protocol
Victor Sandonis, Ignacio Soto, Maria Calderon, Manuel Urueña

Johan J. Lukkien, j.j.lukkien@tue.nl
TU/e Informatica, System Architecture and Networking

23-Nov-16
ETSI GN: safety messages

- **CAM**: cooperative awareness messages
  - use the SHB protocol
  - repeated broadcast vehicle status in one-hop neighborhood

- **DENM**: decentralized environment notification messages
  - use the geocast protocol
  - inform about hazards and road conditions
US: WAVE/DSRC

- IEEE 1609 standardizes *Wireless Access in Vehicular Environments over Dedicated Short Range Communication*
  - 1609.1: resource management
  - 1609.2: security services
  - 1609.3: networking services (a.o. wave short message protocol)
    - broadcasting of basic safety messages
    - define channel number and power per message
  - 1609.4; multi-channel operation

- SAE J2735
  - defines the message content of WSMP
Some application examples
(US WAVE BSM ~SAE J2735)

<table>
<thead>
<tr>
<th>Apps.</th>
<th>Comm.type</th>
<th>Freq.</th>
<th>Latency</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane Change Warning</td>
<td>V2V, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>150m</td>
</tr>
<tr>
<td>Collision Warning</td>
<td>V2V, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>150m</td>
</tr>
<tr>
<td>Emergency Brake Lights</td>
<td>V2V, event-driven, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>300m</td>
</tr>
<tr>
<td>Pre-Crash Sensing</td>
<td>V2V, event-driven, P2P</td>
<td>50Hz</td>
<td>20ms</td>
<td>50m</td>
</tr>
<tr>
<td>Stop Sign Assists</td>
<td>I2V and V2I, periodic</td>
<td>10Hz</td>
<td>100ms</td>
<td>250m</td>
</tr>
<tr>
<td>Left Turn Assistance</td>
<td>I2V and V2I, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>300m</td>
</tr>
<tr>
<td>Traffic Signal Violation</td>
<td>I2V, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>250m</td>
</tr>
<tr>
<td>Curve Speed Warning</td>
<td>I2V, periodic, P2M</td>
<td>1Hz</td>
<td>1s</td>
<td>200m</td>
</tr>
</tbody>
</table>

V2V = Vehicle to Vehicle  
P2M = Point to Multipoint  
I2V = Infra structure to Vehicle

Eight high priority vehicle safety applications as chosen by NHTSA and VSCC.
VSCC – Vehicle Safety Communication Consortium of CAMP (Crash Avoidance Metrics Partnership)
Combining with Internet

Internet Apps
- TCP/UDP
- IPv6

WAVE Apps
- 1609.x
- (1,2,3)

IP packet

LLC/MAC (IEEE 802.11p with CSMA/CA)
- P1609.4

PHY (IEEE 802.11p)

WAVE (Wireless Access in Vehicular Environment) standards:
IEEE 802.11p standard and 1609.x standards
Evaluation
Concerns of safety

• What is the combined behavior of application components distributed over several vehicles?
  – agreements on and effects of actuations?
  – which situational information needs to be taken into account?
    • road condition, #passengers in other car, #vehicles in certain range, …?  
  – development and acceptance procedures for applications
    • https://blogs.nvidia.com/blog/2016/05/06/self-driving-cars-3/
    • https://www.youtube.com/watch?v=qhUvQiKec2U

• Communication from perspective of a given vehicle
  – do I know who is in my neighborhood?
    • how long does it take to know this?
  – are my messages received by vehicles in my neighborhood?
  – do I receive the messages of vehicles in my neighborhood?
  – how does this scale in function of vehicle density? of …?
Periodic Broadcast in IEEE 802.11p

\[ a_i^{(k)} \overset{\text{def}}{=} \phi_i + k \cdot T_i \]

\( k : k^{\text{th}} \text{ message} \)

\( \phi_i = \text{initial phase (or offset) with respect to a common zero} \)

\( T_i : \text{period} \)

- **Defer**: waiting until channel is free; **Bf**: backoff; **AIFS**: see Networks
- For broadcast, randomization in back-off process is limited
- Point-to-point techniques for solving hidden node problems do not work
  - MAC layer acknowledgement
  - RTS/CTS
Case study: scalability of periodic broadcast

- When the number of vehicles increases, message collisions will increase as well
- Nodes will suffer losses through Near Neighbor and Hidden Node effects

Questions:
- what are effects on reliability, delay and fairness?
  - fairness: all vehicles taking the same loss?
- what is the impact of HN, NN?
- what is the impact of the phase, and of changes therein?
- what are relevant metrics?

From: Model, Analysis, and Improvements for Inter-Vehicle Communication Using One-Hop Periodic Broadcasting Based on the 802.11p Protocol, T.Batsuuri, R.J.Bril, J.J.Lukkien
How to setup the simulation?

- Two ‘independent’ parts:
  - Simulate vehicles, and vehicle movement
  - Simulate communication
    - how detailed should this be?

- Vehicle movement
  - idealized, parameterized
  - or real-world traces?
Highway model

Total path length is 3000m.
The inter-vehicle distance is changed to have different densities.
Metrics

- **Successful Message Ratio (SMR)** – the fraction of vehicles in Communication Range that receive a broadcast message.
  - Example: if a network has vehicles with 10 neighbors on average and on average 7 receive the message then SMR=70%
  - SMR is also defined per vehicle and per message

- **First Delay (FD)** – the longest interval in which no message is successfully delivered between two vehicles since they established a link (i.e. a delay to discover each other)

- **No Message Interval (NoM)** – the longest interval in which no message is successfully delivered in a link
Results: overall SMR vs. Vehicle Density (VD)

- minSMR: all phases equal
- maxSMR: optimal scheduling
- no HN: single broadcast domain
- significant losses at low densities

SMR ~ 78%

VD = 48
CDF of vehicles by its SMR

- CDF: Cumulative Distribution Function
  - $y\%$ vehicles have at most $x\%$ SMR
- Some vehicles have SMR of 15%, and some of 100%
  - unfair!
- Ideal case: all the same
First Delay (60 simulated seconds)

- Most vehicles see each other within 100ms
- Some vehicles never see each other

52644 links are established (~36000 links between vehicles traveling in opposite directions, ~17000 links for the same direction)
CDF of NoMessage Interval

- y% links have up to x seconds NoM
- Most NoMs are short
- However, a positive number of NoMs is larger than 10s
Possible adjustments

\[ a_i^{(k)} \overset{\text{def}}{=} \phi_i + k \cdot T_i + \text{jitter} \]

\( k : k^{th} \) message

\( \phi_i = \text{initial phase (or offset) with respect to a common zero} \)

\( T_i : \text{period} \)

- **Elastic:**
  - randomize the phase every \textit{er} (elastice rate) messages
    - appears to improve fairness

- **Jitter:**
  - give a jitter of \textit{AJ} msec (Activation Jitter) to the arrival moment
    - appears to improve long delays
Two solutions into one: SMR

- Neither Jitter nor Elastic changes SMR!
- Combined: best results
- MD: multi-domain
- Choice of er=6, AJ=20 based on experimentation
Two solutions into one

- Neither Jitter nor Elastic changes SMR!
Two solutions into one

- Neither Jitter nor Elastic changes SMR!
- Combined: best results

![Graph showing CDF of links vs. NoM (seconds)]
Guiding questions

- Which V2V applications are there?
- How does V2V communication and how do applications work?

- Goal:
  - Study a larger example of an IoT system.
  - Show how the different parts fit together.
V2I
Guiding questions

• How does V2I communication work and how is it used?
• Who are stakeholders in ITS?
• Which V2I applications are there?

• Goal:
  – Study a larger example of an IoT system.
  – Show how the different parts fit together.
V2I communication

- On-board-units (OBUs) manage (IP-based) connections with back-offices
  - via IEEE 802.11p: not likely
  - 3G/4G/5G
- Less time-critical applications
V2I applications examples

• Users (drivers):
  – traffic guidance
  – road warnings
  – car sharing
  – event management
  – parking support
  – predictive maintenance

• Government
  – road management
  – traffic management
  – vehicle behavior?
  – traffic violations?

• Manufacturers
  – maintenance info
  – warranty evidence
  – performance
Data?
New functions, new sensors!

- Safety
- Comfort, Convenience
- Driver assist
- Traffic management

(pictures from the Internet)
Stakeholders & concerns for V2I

- **End-Users**
  - *manufacturers*:
    - obtain continuous operational data
  - *government*:
    - obtain data about road usage & conditions & traffic,
    - regulations, certification, standards
  - regular users:
    - user apps, safer driving
    - secure data sharing, privacy

- **Application developers**
  - facilities for creating and selling applications
    - safety & data driven applications

- **Infra structure providers**
  - data storage, data access (cloud)
  - connectivity provisioning (telecom)

- **Platform maintainers**
  - system integration, facilitating (*enabling*) other stakeholders
  - standardization of equipment, software stacks

- **Car (component) manufacturers**
  - access to data
  - responsible for implementations within vehicles
  - rules and regulations, standards

- **Owner(s) of business case(s)**
  - all, except perhaps the end-users
  - overall architecture must support business cases

Johan J. Lukkien, j.j.lukkien@tue.nl
TU/e Informatica, System Architecture and Networking

23-Nov-16
Stakeholders & scenarios

- Analogy: the smartphone market
  - *enabled* by platform provisioning, both hardware and software (apps, app store)

- Each stakeholder has *scenarios*, which are (sets of) interactions in relation to the system

- System components have *life cycles*

- Stakeholder positions are important, and influence the system architecture
  - *example*: just imagine government would define all apps and let these develop by invited parties

- Scenario examples
  - *regulations*:
    - testing & certification of safety apps
    - data protection
  - *app programming*: app life cycle of development, testing, certification, and:
    - deployment in store, loading
    - deployment into vehicles
  - *car manufacturer*: process of data generation, collection, access to data
Example: how do manufacturers get data?

- Built into the WAVE stack
  - This means that such data would be exchanged between RSU and OBU
    - and then transported onwards
- SAE J2735 specifies applications:
  - **Basic Safety Messages** transmitted periodically as broadcast via WSMP
  - **Road side warnings**
  - **Probe data** (history data) reporting vehicle state
    - ‘floating car data’
- Circumventing user consent issues
Current trends

• Experimental systems and projects in consortia
  – vehicle to cloud
  – CAN bus to cloud

• Individual parties recording data from vehicles, either proprietary or via service provider
  – fleet owners
  – manufacturers

• Problem: enabling third parties (app developers)

• Effect: groups of vehicles connected to a ‘group owner’

• VIBe project:
  – pursue a unifying API
  – focus on electric vehicle applications
Outline of VIBe vision
Logical organization

- Preferred: user consent / control:
  - joining a group
  - decide data transmitted

- Plus collection / access policies:
  - access only data that is required by an APP
Concluding

• Gathering vehicle data is similar to gathering data for an app in a smart phone

• Current tendency for vehicles:
  – recording data not under control of the user
    • owner and manufacturer do this
  – gather all available data (and use later)
    • rather than a user selecting to join an app (or group)

• Required:
  – further analysis and protection of stakeholder positions
  – changes in the architecture as a consequence
Example: regulation is required

- What will the government do if large databases are available, even if they cannot access them in principle?
- What will happen with large hacks?
Guiding questions

- How does V2I communication work and how is it used?
- Who are stakeholders in ITS?
- Which V2I applications are there?

Goal:
- Study a larger example of an IoT system.
- Show how the different parts fit together.
Privacy, Safety and Security
Guiding questions

- What are safety and privacy concerns and what role plays security?
- What are current solutions?

Goal:
- Study a larger example of an IoT system.
- Show how the different parts fit together.
Privacy, Safety, and Security

- **Privacy**: control over personal information

- **Safety**: freedom from danger or risk on injury resulting from recognized but potentially hazardous events

- **Security**: regulating access to (electronic) assets according to some policy
  - *policy*: allowed and disallowed actions
  - *security mechanisms*: can be regarded as enforcing the policy

- Privacy and safety restrictions result in *security policies*
  - *security for privacy and security for safety*

- In addition: security for protection of the business case
  - *security for the business case*, quite often an *availability concern*
Example requirements

• Safety:
  – safety violations by malicious external parties must be prevented (e.g. by a policy of forbidding certain actions)
  – safety must be maintained while executing regular functions (functional safety)

• Privacy:
  – personal data must remain under control of the owner
  – vehicle must not be tracked

• This leads to Common Criteria, to classification of functions and the development process (ISO 26262), and to certification

• We look at some examples
Security to protect safety in BSM

• A vehicle could perform a (physical) action upon receiving certain messages. This response must be on good grounds, and safe.
  – authentication: does this message really come from
    • that particular car?
    • the car left behind me?
  – authorization: what is allowed
    • by this party?
    • by this message?
  – integrity: was this message not tampered with?

• Further concerns regarding safety:
  – are messages really delivered (and not lost or jammed)?
  – functional safety
    • maintain safe and responsive behavior while executing normal functions
Security to protect privacy in BSM

• Communication might reveal sensitive information
  – location of vehicle, one could track it
  – driver identity, number of passengers
  – driving behavior

• Security mechanisms might add to this
  – e.g. the signing of messages reveals the signature

• Hence:
  – policies for data handling, certification of those policies
    • e.g. collect only anonymous data, forbid vehicle tracking (by the government) in mandatory services
  – requirements on security mechanisms so they don’t unveil details

Johan J. Lukkien, j.j.lukkien@tue.nl
TU/e Informatica, System Architecture and Networking
Requirements on security

• Interoperable
• Process-able in real-time and limited in size (bandwidth)
• Identity-free
• Non-repudiation (sender cannot deny having sent a message)

• Scalable
  – local: few hundreds of vehicles
  – global: millions of vehicles
• Extensible, towards other applications of V2x communication
Proposal (US)

- Use Public Key Infrastructure to sign messages
  - authentication, integrity & non-repudiation

- **Certificate** associates public and private key
  - decryption using the public key demonstrates:
    - that the sender knows the private key, which is associated with an identity by an authority
    - and that the message was not altered

- Complex extensions to deal with the specific concerns of these applications
  - intermittent connectivity, anonymity
    - provide several temporary identities (pseudonyms)
  - small size keys and certificates: ECQVIC / ECDSA
    - though these require 10 times more processing power
System outline

• Security Credentials Management System

• Comparison: basic PKI versus V2x design

• Main idea:
  – give a vehicle several pseudonyms, valid for a limited period

• However, the driver’s phone will be logged into google et al. ....

from: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014

Johan J. Lukkien, j.j.lukkien@tue.nl
TU/e Informatica, System Architecture and Networking
Security within the vehicle
Increasing wireless connections … and vulnerabilities

- hacking *without* altering the electronics

https://www.youtube.com/watch?v=OobLb1McxnI
The drill…

• Attach a module to the CAN bus in order to send and receive control messages and connect to a wireless transceiver

OR

• Hack into the car via the Internet with the same effect

• Reverse engineer the messaging of this type of car

• Control the car via remote access
What to do about this?

- **Protect CAN bus**
  - admission control for new CAN devices
  - CAN message signing and encryption
  - … but who has the keys?

- **Physical separation** – make harmful influence from new components physically impossible

- **Policy separation**
  - implement policies that restrict behavior in certain modes
    - e.g. no remote access while driving
    - software update only under specific circumstances, e.g., in a car shop
    - (expose certain behavior while being examined ;‐)

- **Self monitoring** – intrusion detection
What about privacy?

- Adopt policies about what to collect, communicate, store, e.g.,
  - collect only anonymous data
  - forbid vehicle tracking in mandatory services (e.g. road side)
  plus certification of these policies, access tracing, accounting, auditing

- A radically different approach to managing data
  - a personal data store where data about a person is stored under his control
    - no storage in private repositories of companies
    - in fact, avoid that data leaves a managerial domain
Next Generation Vehicle OS...
Guiding questions

• What are safety and privacy concerns?
• What are current solutions?

• Goal:
  – Study a larger example of an IoT system.
  – Show how the different parts fit together.
Concluding

• This example has all characteristics of an IoT application
  – complex physical platform
    • distributed
    • managerial domains – vehicle user, owner, road owner etc.
  – short and long ‘cycle’
    • short: safety applications
    • long: applications on top of collected data
  – domains with different criticality and timing requirements
    • and corresponding applications
  – data traversing managerial domains
    • from vehicle via infra structure to cloud
  – concerns of security, privacy
    • lack of control over data
    • security for both privacy an safety