Vehicular communication and applications: who depends on whom?

Natalya An, Tristan Gaugel, Jens Mittag, Till Neudecker, Marcel Revfi, Hannes Hartenstein

Avizienis, Laprie, Randell, Landwehr paper

DEPENDABILITY

THREATS
- FAULTS
- ERRORS
- FAILURES

ATTRIBUTES
- AVAILABILITY
- RELIABILITY
- SAFETY
- CONFIDENTIALITY
- INTEGRITY
- MAINTAINABILITY

MEANS
- FAULT PREVENTION
- FAULT TOLERANCE
- FAULT REMOVAL
- FAULT FORECASTING
Vehicular communication system

„Good enough dependability?“*

Vehicular networking applications

… a personal view …

*Thanks to Ravi Sandhu: Good enough security, 2003
A look back …

1. Vehicular communication system
2. Rear End Collision Avoidance, Virtual Traffic Lights
3. „Good enough dependability?“ … for what?

Vehicular networking applications
PROMETHEUS:
Dabbous and Huitema (1988)

![Diagram showing merging lanes scenario with $V_2$ and $V_1$]

<table>
<thead>
<tr>
<th>Merging lanes scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypothesis</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Max. deceleration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Messages</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>5 Hz</td>
<td>1+n</td>
</tr>
<tr>
<td>Connection phase</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Synchronization</td>
<td>2 Hz</td>
<td>10</td>
</tr>
<tr>
<td>Emergency</td>
<td>10 Hz</td>
<td>50</td>
</tr>
<tr>
<td>Total</td>
<td>2 – 10 Hz</td>
<td>14 – 64</td>
</tr>
<tr>
<td>Maximum transmission delay</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A look back … 802.11p-driven research

- Periodic beacons, emergency notifications:
  - Almost nothing to be done for networking protocols …
  - One hop broadcasts

- Metrics:
  - Packet (frame) reception probability, inter-reception time …

- Influencing factors:
  - Everything that influences the radio channel, car maneuvers, vehicular traffic …

- Controlling communication:
  - Rate control, power control, combination thereof …

- Our “final word” on this (so far):
Work referenced on previous slide assume there is a bunch of vehicular networking applications with roughly sketched requirements (like: 10 beacon messages per second ought to be enough for anybody …)

“VANET: Is 95% Probability of Packet Reception safe?” Natalya An et al., ITST, Saint Petersburg, Russia, 2011

“Ideal” procedure: start with specification of application, determine requirements for the communication system, check whether (or better: under which conditions) the communication system can meet the requirements.
Co-design “blueprint”

Rear-End Collision Avoidance*

- Dependability attribute: safety
- Considered dependability threats:
  - Unpredictable driver behavior
    - Variable reaction time and braking intensity
  - Unreliable communication
    - Variable packet inter-reception times
- Not considered dependability threats:
  - Human-Machine-Interface
  - Fail-safety against hardware, software failure, or other external effects
- Considered means: Fail-safety, i.e. system incorporates features for automatically counteracting the effect of an anticipated possible source of failure (from Merriam-Webster dictionary)
- Performance: impact on vehicular traffic density and on channel load?

N. An et al. Balancing the Requirements for a Zero False Positive/Negative Forward Collision Warning, WONS, Canada, 2013
Application “continuously” calculates the warning distance $D_W$ (and $D_{AB}$)

How to make it fail-safe?

- Against unpredictable driver behavior
  - Account for a worst driver (reaction time, braking intensity)
  - Account for disobedient driver

- Against unreliable communication
  - Account for the worst change of $v_{LV}$ during packet inter-reception time (IRT)
Unpredictable driver behavior

Reaction Time
- Log-normal distribution
  - mean = 1.3s and deviation = 0.74s

Braking Intensity
- Truncated Gaussian distribution with
  - mean = -0.6g,
  - deviation = 0.1g,
  - max = -0.8g and min = -0.3g

Unreliable communication

- Account for a worst case during inter-packet reception (IRT)

- Typical* scenarios
  - Lead Vehicle Stopped (LVS)
  - Lead Vehicle Moving (LVM)
  - Lead Vehicle Decelerating (LVD)

*LVM, IRT = 0.2s

“Uncertainty quantification”

Means for dependability (fail-safety)

- Bound IRT (with high probability, say 99.99%)
  - larger IRT → larger uncertainty about LV → larger warning (automatic braking distances) → reduced traffic density → less load on radio channel
  
  → Requires realistic model for IRT (e.g., of probability of reception) and detection of the radio condition

- Bound reaction time and braking intensity by automatic braking for those drivers who do not meet the bounds
  
  → “Automation level” (ratio of drivers’ population deprived of vehicle control)
Performance: traffic efficiency & channel load

- Generated drivers’ population (250000 driver profiles)
- Lead Vehicle Decelerating
  - $v_{LV} = 100\text{km/h}$, $a_{LV} = -0.6g$
  - $v_{FV} = 130\text{km/h}$

- Impact on traffic efficiency
- 802.11p performance “okay” under given model assumptions
More details can be found in:

Designing Fail-Safe and Traffic Efficient 802.11p-based Rear-End Collision Avoidance, N. An, J. Mittag, H. Hartenstein
IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, December 2014
Vehicular Visible Light Communications

Transmitter: LED lights

Receiver: Off-the-shelf cameras

"N-version programming"

1010

Virtual Traffic Lights (VTL)

Concept and notion follows Ferreira et al. (2010), assumptions:

- 100% VTL equipment ratio
- GPS with sufficient precision, road topology maps available
- Drivers are compliant and non-distracted
- Vehicles are able to sense existence of other vehicles in front (using sensors or line-of-sight communication)

**Dependability threats**: no assumptions on the reliability of NLOS communication are made
Design of VTL

**Dependability attribute**: safety $\rightarrow$ reliable consensus, consistency

- Consistency requires at most one VTL Leader at time per intersection
- When to establish a new VTL instance?
  - Model requires information from all approaching roads
  - VTL leader has highest unique ID among approaching vehicles
  - Only first vehicle (Cluster Leader) on each road segment is a possible VTL leader

**Dependability means**: fallback mechanism

- Handling no traffic light information case
  - Braking begins at $D_{safe}$ in case of no information by design
  - Fallback option: First come, first served all-way-stop

How to be sure? $\rightarrow$ Formal verification
Verification (PROMELA/SPIN)

- Model Checking: Search for invariant violations
  - Implement VTL model in PROMELA (http://dsn.tm.kit.edu/english/vtl.php)
  - Define invariant: **There exists one traffic light information set so that each vehicle either has this information or no information**
  - Automatic model checker (SPIN) checks if invariant holds true for all possible protocol runs
  - Exhaustive or partial (*Bitstate hashing*) search possible
  - Challenge: no support of floating point units
Verification Results

<table>
<thead>
<tr>
<th>Vehicles</th>
<th>Roads</th>
<th>States</th>
<th>Memory</th>
<th>Time</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>267,441</td>
<td>34.7 MB</td>
<td>1.37 s</td>
<td>Exhaustive</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>5.42E+09</td>
<td>216 GB</td>
<td>7.2 h</td>
<td>Exhaustive</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1.91E+10</td>
<td>256 GB</td>
<td>18.8 h</td>
<td>Bitstate, h=115</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>&gt; E+11</td>
<td>256 GB</td>
<td>14 d</td>
<td>Bitstate, incomplete</td>
</tr>
</tbody>
</table>

- No violations found
- Bitstate verification for scenario with 4 vehicles reached cluster’s two week computation time limit
  - State space explosion with number of vehicles
  - Optimization & decomposition could allow verification of larger scenarios

- Output: Verified (for shown scenarios) failsafe VTL model
- What about traffic efficiency? → next slide
Performance: Average Travel Time

![Graph showing performance metrics with trade-offs between safety and efficiency.](image)

- FCFS
- VTL, verified
- CTL
- CTL sync
- VTL, optimized, SL = (1 - 10\(^{-1}\))
- VTL, optimized, SL = (1 - 10\(^{-11}\))

Virtualsource11p model

Tradeoff safety ↔ efficiency
More details can be found in:


and for a visualization:

http://dsn.tm.kit.edu/english/misc_vtl.php
And there are many interesting papers around:

See, e.g.,


- Cooperative vehicle-to-vehicle active safety testing under challenging conditions, M. Sepulcre, J. Gozalvez, J. Hernandez, Transportation research part C: emerging technologies 26, 233-255, 2013

- ...
A look back …

1. Vehicular communication system
2. „Good enough dependability?“
3. … for what?

Vehicular networking applications

Rear End Collision Avoidance, Virtual Traffic Lights
A broader view on dependable vehicular communication (1)

- Vehicles as parts of the “Internet of Things”
- Architecture, security, performance → I(o)T management aspects
Trip planning

Dependability seen from the multi-modal traffic perspective
- include walking, biking, trains etc.
Dependability attribute: reliable travel times
Dependability threats: many, including strike actions …
Dependability means:
- Disruption management
- Proper planning per mode of traffic
- …

More of an information systems topic?
Discussion, challenges, conclusions (1)

- **Network performance**
  - Challenge: many driving situations

- **Awareness**
  - Challenge: appropriate level of abstraction?
  - Clarification of dependability attributes, threats and means under study

- **Application performance**
  - Challenge: will data be available?
  - Challenge: human factors and/or many driving situations

Improvement of (fault) models and awareness concepts
Discussion, challenges, conclusions (2)

Look at vehicular communications from the perspective of dependable vehicular applications.

- What is the desired/achievable level of dependability?
  - Risk management
  - Tradeoffs (like in the field of security)
  - Inter-disciplinary

- Benefit: Gives communication and networking metrics a “real world meaning”

- Challenge: Hard to validate