Vehicle2Vehicle Communication based on 802.11p

32. Chaos Communication Congress

Bernd Lehmann

Agenda

Introduction and Motivation

Basic Concepts

Standards
- EU and US

Security
- EU concept

What else?

Further development

Agenda

Introduction and Motivation

Basic Concepts

Standards
- EU and US

Security
- EU concept

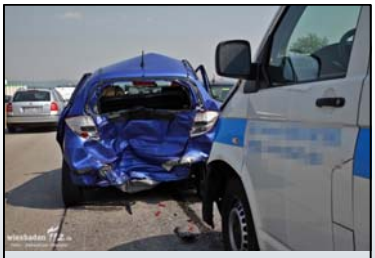
What else?

Further development

Motivation

Collision with an emergency vehicle in service

Red light violation



Crash with high velocity at the end of a traffic jam

Warning about hazardous events shall be transmitted after few milliseconds.
(hazardous areas after a turn or on crossings)

Images: Sebastian Stenzel (http://www.wiesbaden112.de/)

Motivation

- Communication range: 100 m (urban) u. 800 m (free field)
- Short distance communication
  - between Vehicles
  - between Vehicles und „Road Side Units”
- Communication latency: < 10 ms
- Transmission frequency 1-10Hz (depending on driving situation)
- Dedicated communication frequency at 5,9 GHz (Europe and USA)

Agenda

Introduction and Motivation

Basic Concepts

Standards
- EU and US

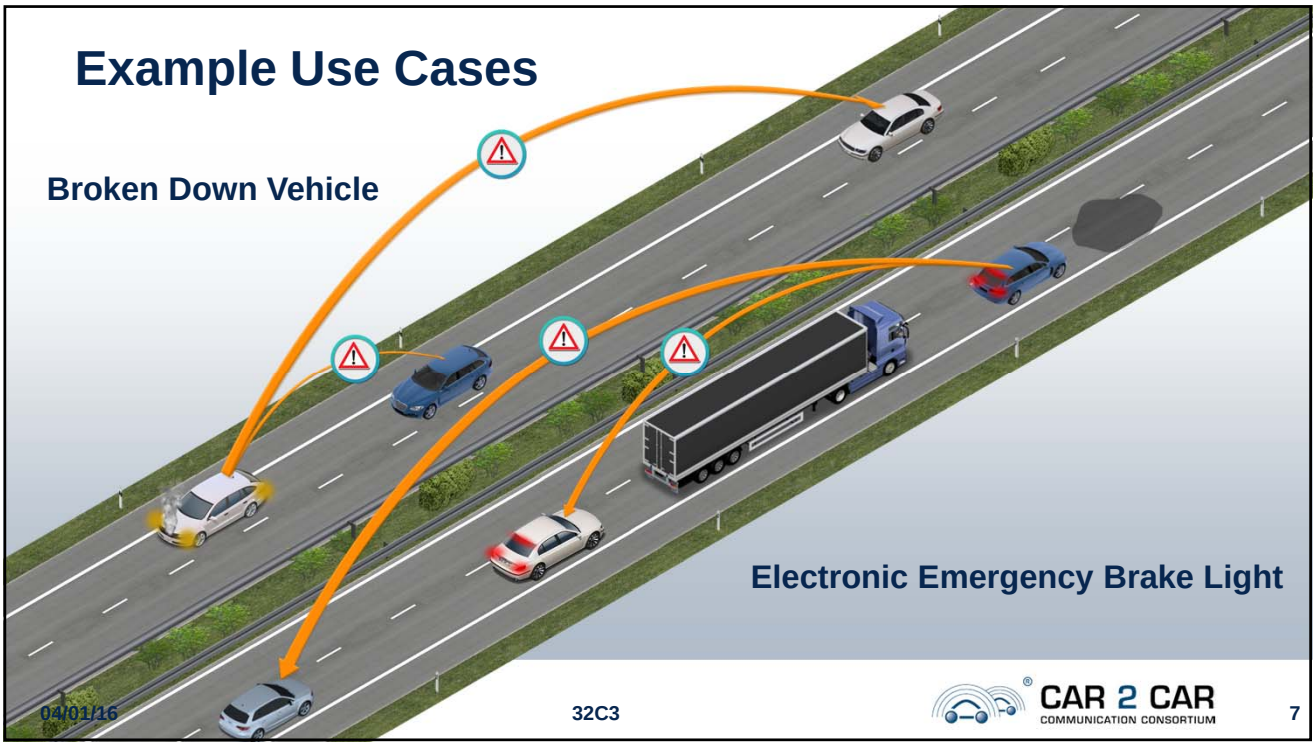
Security
- EU concept

What else?

Further development

Example Use Cases

Broken Down Vehicle

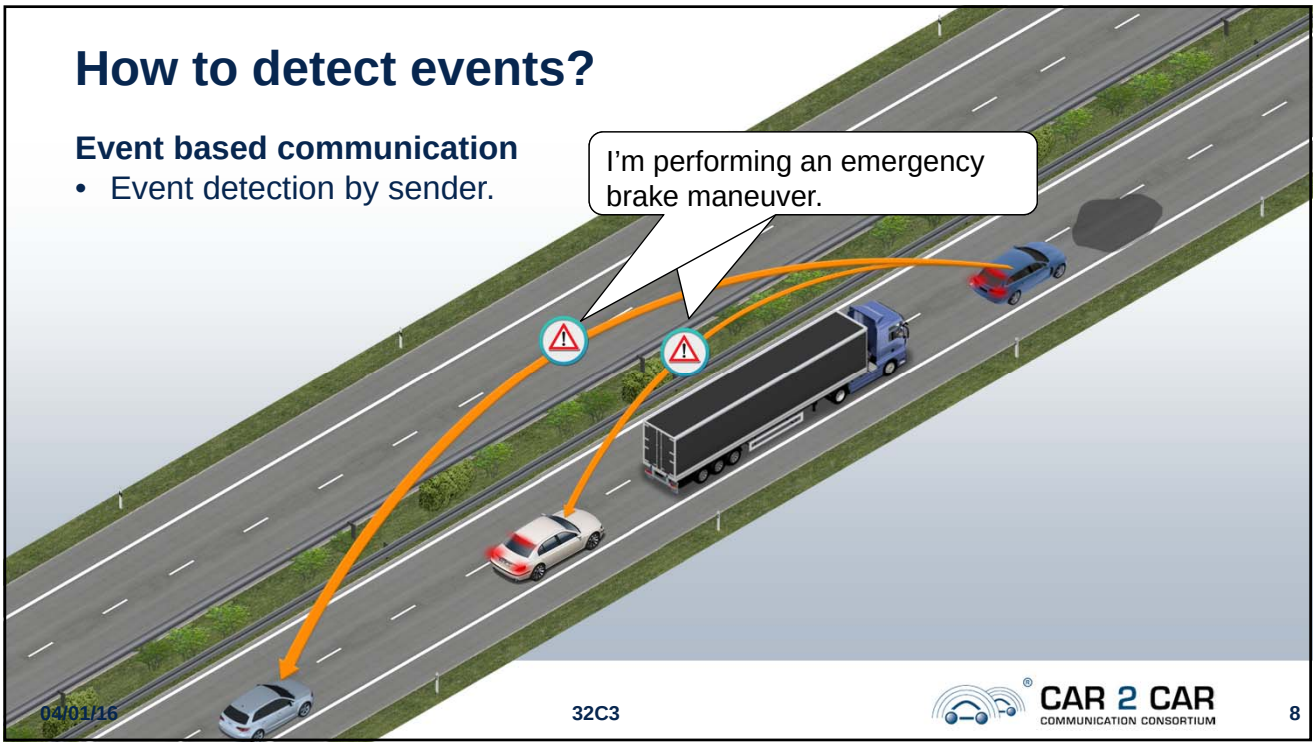


Electronic Emergency Brake Light

How to detect events?

Event based communication

- Event detection by sender.

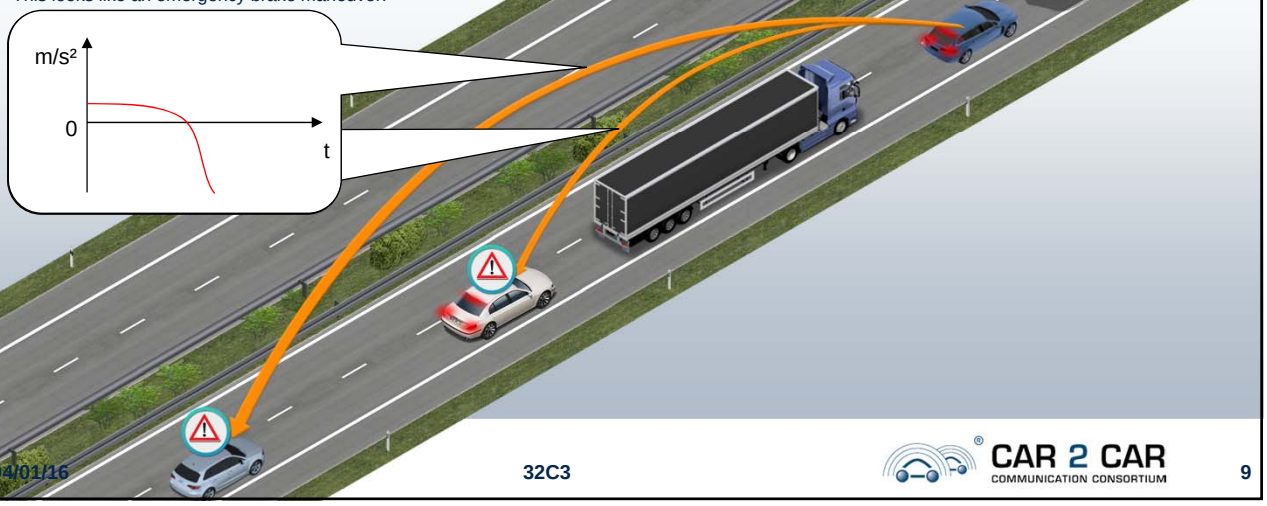


How to detect events?

Awareness based communication

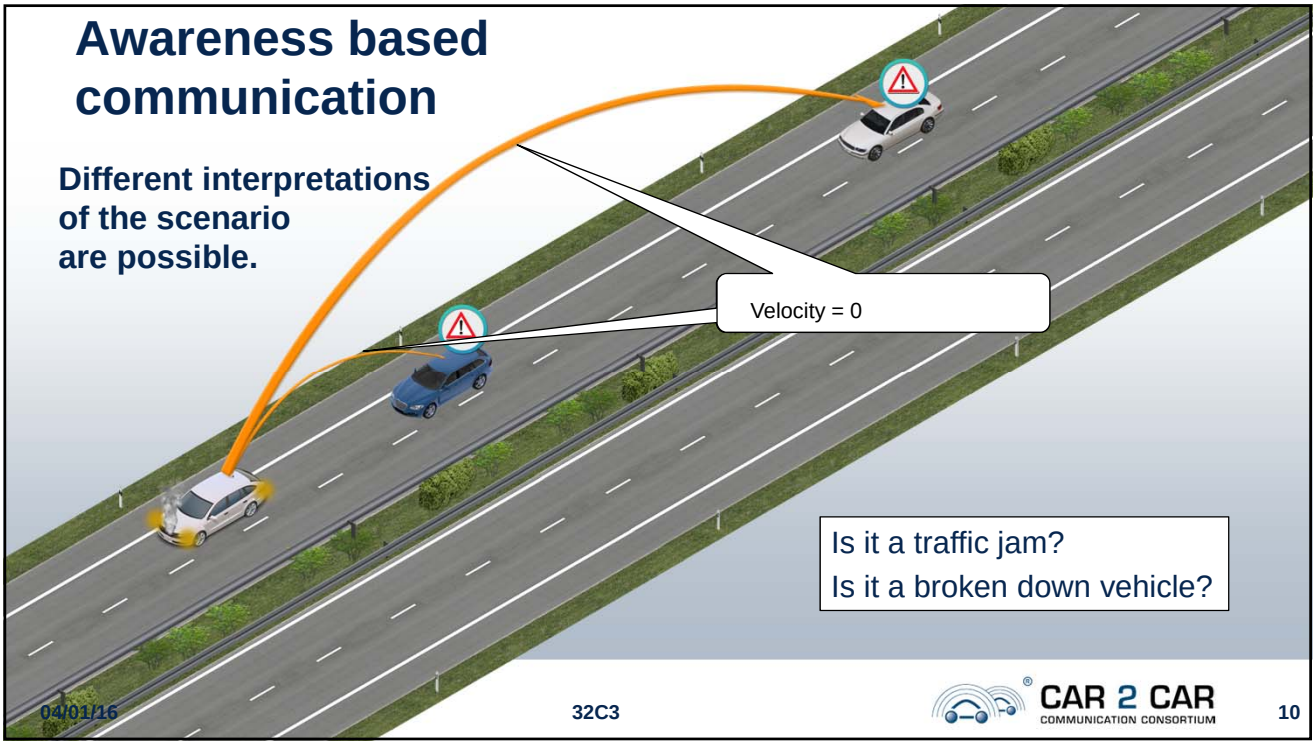
- Event detection by receiver.

This looks like an emergency brake maneuver.



Awareness based communication

Different interpretations of the scenario are possible.



Is it a traffic jam?
Is it a broken down vehicle?

Philosophy comparison

Event based	Awareness based
Message describes an event	Message describes status of a vehicle
Easy interpretation on receiver side	More complex interpretation on receiver side - Traffic jam or broken down vehicle?
One received message is sufficient	Needs to receive more than one message and track value changes
Only known use cases can be described	Data can be used for new use cases

Agenda

Introduction and Motivation

Basic Concepts

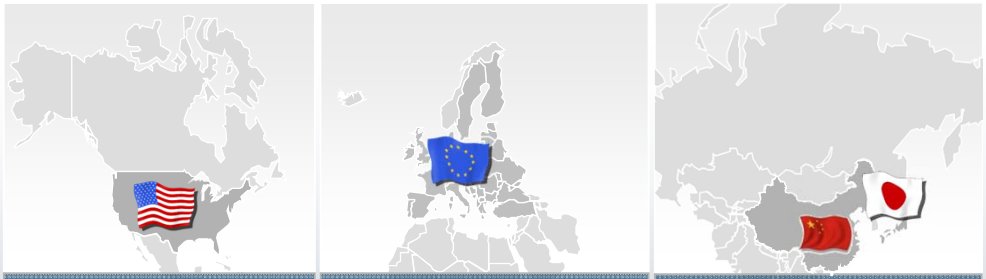
Standards
- EU and US

Security
- EU concept

What else?

Further development

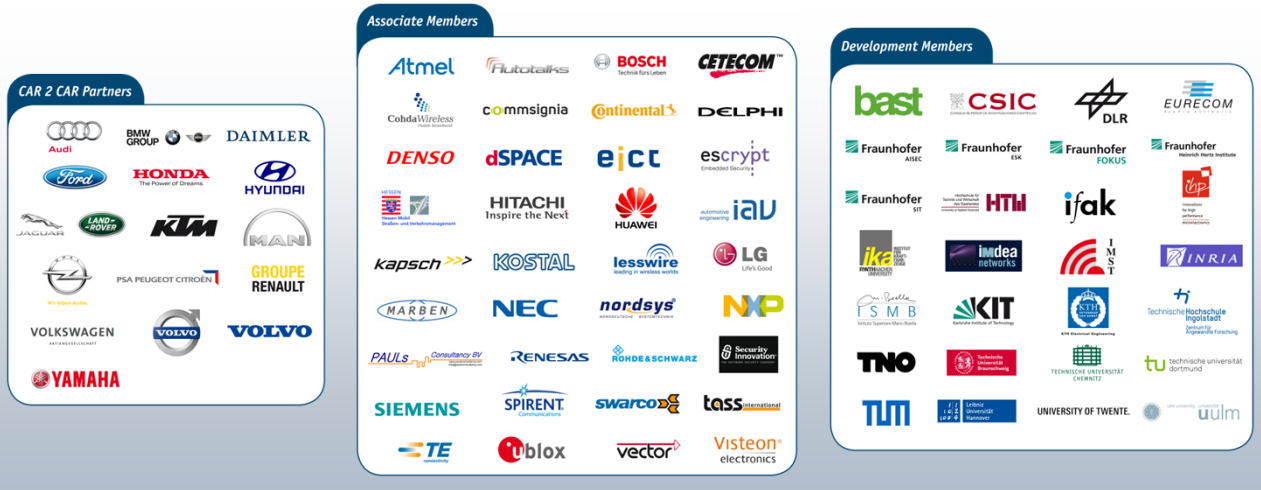
Standards



USA	Europe	Japan & China
▸ Standards by IEEE, SAE ▸ CAMP (vehicle OEM consortium) ▸ Focus on Awareness Based Communication	▸ Standards by IEEE, ETSI ▸ Car2Car Communication Consortium ▸ Focus on Event Based Communication	**Japan** ▸ ITS Info-communications Forum ▸ 802.11 on 760 MHz-Band **China** ▸ Activities started ▸ At the moment there is nothing concrete

CAMP: Crash Avoidance Metrics Partnership

C2C Communication Consortium



Source: http://www.car-2-car.org/ (11/2015)

Messages

EU

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

DENM: Decentralized Environmental Notification Message (EU)
- Event based message
- Describes an existing event (e.g. Broken down vehicle)

US

Messages

EU

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

DENM: Decentralized Environmental Notification Message (EU)
- Event based message
- Describes an existing event (e.g. Broken down vehicle)

BSM: Basic Safety Message (US)
- Awareness based message
- Contains status information about vehicles

US

Payload
SAE J2735
SAE J2945

Messages

EU

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

DENM: Decentralized Environmental Notification Message (EU)
- Event based message
- Describes an existing event (e.g. Broken down vehicle)

US

Payload
SAE J2735
SAE J2945

BSM: Basic Safety Message (US)
- Awareness based message
- Contains status information about vehicles

CAM: Cooperative Awareness Message (EU)
- Awareness based message
- Contains status information about vehicles

Messages

EU

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

DENM: Decentralized Environmental Notification Message (EU)
- Event based message
- Describes an existing event (e.g. Broken down vehicle)

US

Payload
SAE J2735
SAE J2945

BSM: Basic Safety Message (US)
- Awareness based message
- Contains status information about vehicles

CAM: Coop
- Awarene
- Contains

Also includes event flags that represents events like hard braking or disabled vehicle. Therefore the BSM is also an event based message.

Message Multiplexing

EU

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

Other messages:

- SPaT: Signal Phase and Timing
- MAP: Geometrical descriptions of e.g. intersections or work zones
- more …

Multiplexing is needed

US

Payload
SAE J2735
SAE J2945

Message Multiplexing

EU

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

BTP
ETSI EN 302 636-5-1

Other messages:

- SPaT: Signal Phase and Timing
- MAP: Geometrical descriptions of e.g. intersections or work zones
- more …

Multiplexing is needed

US

Payload
SAE J2735
SAE J2945

BTP: Basic Transport Protocol (EU)
- similar to UDP

Message Multiplexing

EU

Payload
ETSI EN 302 637-2 ETSI EN 302 637-3
BTP
ETSI EN 302 636-5-1

Other messages:

- SPaT: Signal Phase and Timing
- MAP: Geometrical descriptions of e.g. intersections or work zones
- more …

Multiplexing is needed

BTP: Basic Transport Protocol (EU)

- similar to UDP

No dedicated header in the US messages

- Implicit convention: First element of the payload in the US is an enumeration which indicates the message type.

US

Payload
SAE J2735 SAE J2945

Message Routing

EU

Payload
ETSI EN 302 637-2 ETSI EN 302 637-3
BTP
ETSI EN 302 636-5-1

How to send messages?

- Who is interested in this message?
- How to address them?

US

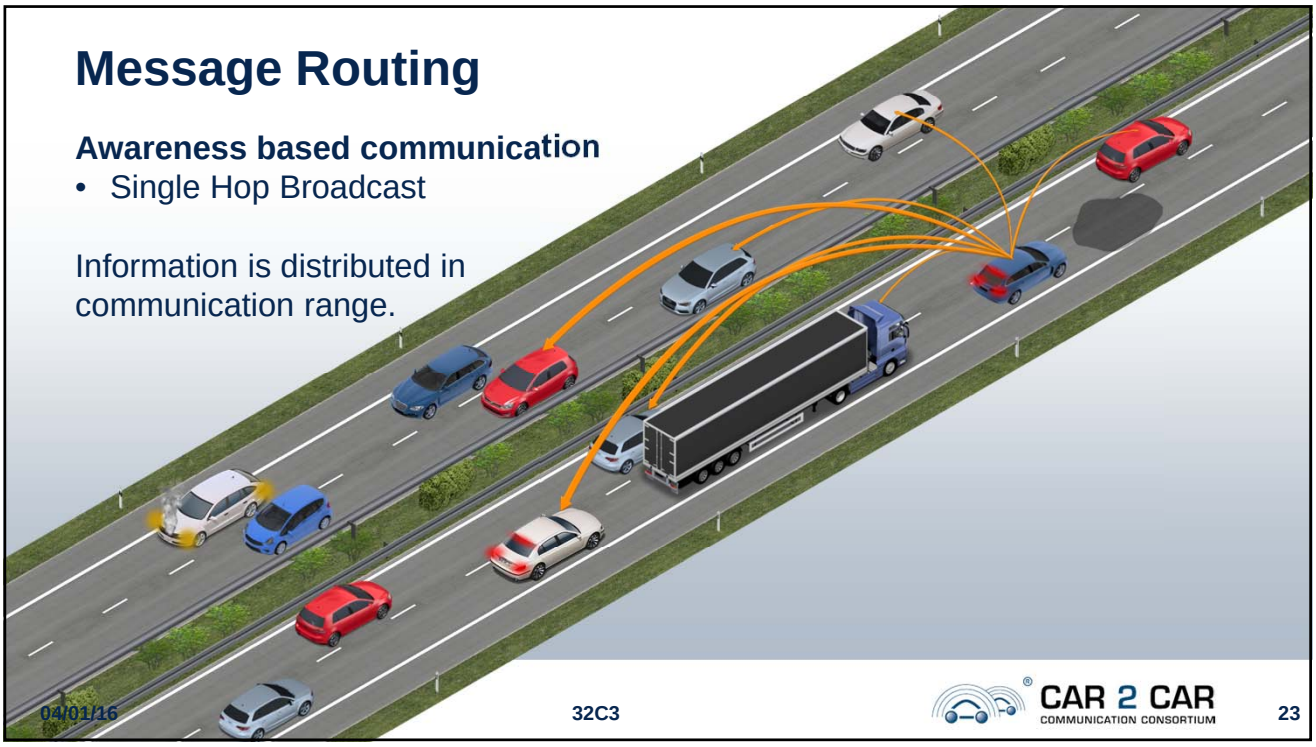
Payload
SAE J2735 SAE J2945

Message Routing

Awareness based communication

- Single Hop Broadcast

Information is distributed in communication range.

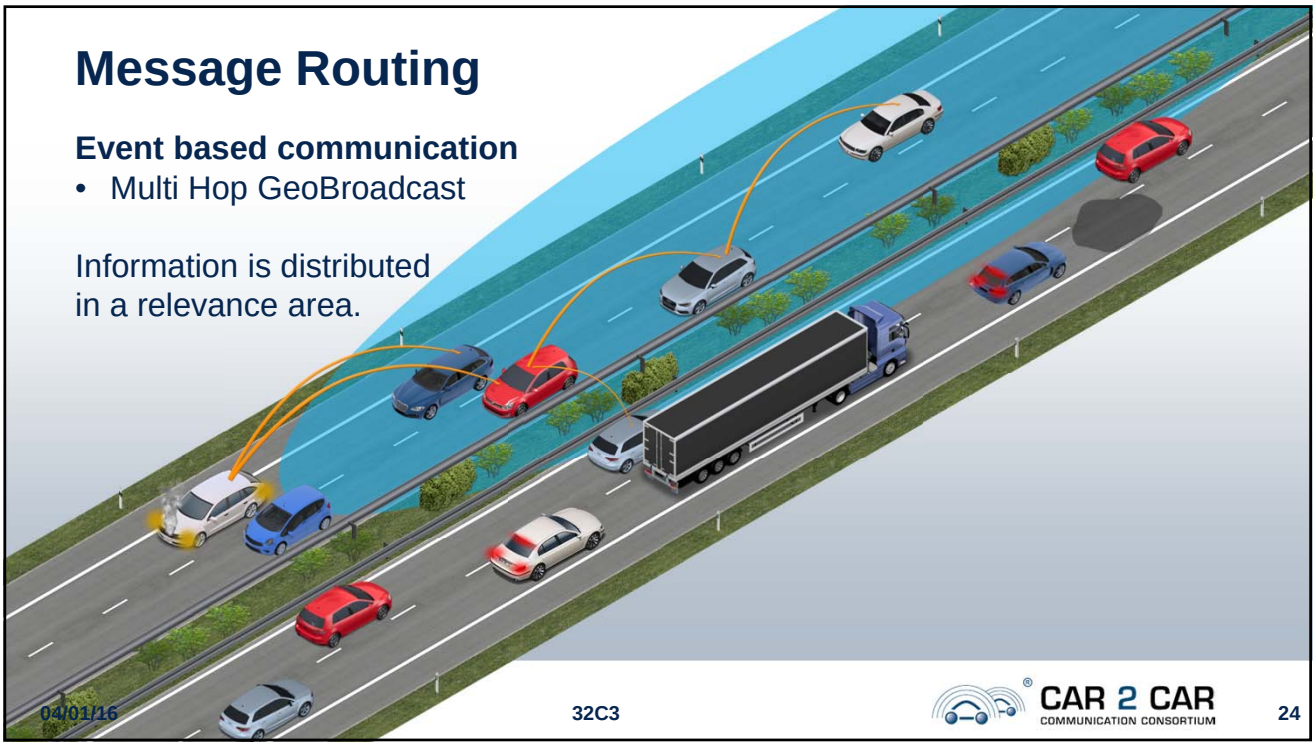


Message Routing

Event based communication

- Multi Hop GeoBroadcast

Information is distributed in a relevance area.



Message Routing

EU

US

How to send messages?

- Who is interested in this message?
- How to address them?

Awareness based messages

- Single Hop Broadcast

Event based messages

- Multi Hop GeoBroadcast

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

BTP
ETSI EN 302 636-5-1

GN-ExtendedHeader
ETSI EN 302 636-4-1

GN-CommonHeader
ETSI EN 302 636-4-1

GN-BasicHeader
ETSI EN 302 636-4-1

GN: GeoNetworking
- Geographical Routing of Messages
- Supports **Single Hop Broadcast**, **Multi Hop GeoBroadcast** and **more**

Payload
SAE J2735
SAE J2945

Message Routing

EU

US

How to send messages?

- Who is interested in this message?
- How to address them?

Awareness based messages

- Single Hop Broadcast

Event based messages

- Multi Hop GeoBroadcast

Payload
ETSI EN 302 637-2
ETSI EN 302 637-3

BTP
ETSI EN 302 636-5-1

GN-ExtendedHeader
ETSI EN 302 636-4-1

GN-CommonHeader
ETSI EN 302 636-4-1

GN-BasicHeader
ETSI EN 302 636-4-1

GN: GeoNetworking
- Geographical Routing of Messages
- Supports **Single Hop Broadcast**, **Multi Hop GeoBroadcast** and **more**

WSMP: WAVE Short Message Protocol
- Single Hop Broadcast

Payload
SAE J2735
SAE J2945

WSMP-Header
IEEE 1609.3

Communication technology

EU

Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

LLC+SNAP

- US-Ethertype:
  0x88DC = WAVE Sort Message Protocol (WSMP)
- EU-Ethertype:
  0x8947 = GeoNetworking (GN)

IEEE 802.11p

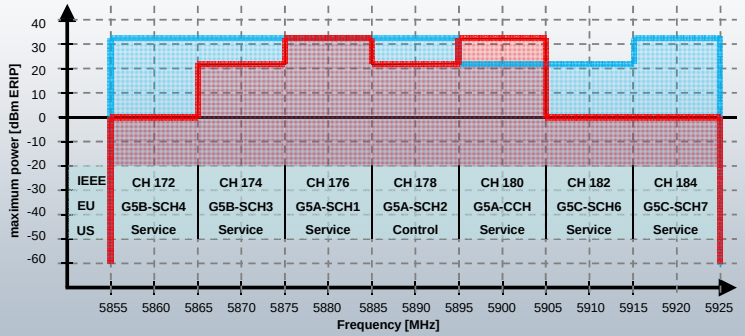
- dot11OCBActivated = true
- Outside the Context of BSS (OCB)
  - No Access Point
  - No authentication service
  - No association service
  - No confidentiality service
  - No …

US

Payload SAE J2735 SAE J2945
WSMP-Header IEEE 1609.3
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Frequency allocation for ITS

- Federal Communications Commission (FCC)
- European Commission (EC)
- Technology (e.g. 802.11p) is not fixed



US dBm ERIP for Private OBU (FCC 03-324)

EU dBm ERIP (ETSI EN 302 663 V1.2.1, European Commission 2008/671/EC)

CCH: Control Channel
SCH: Service Channel

Agenda

Introduction and Motivation

Basic Concepts

Standards
- EU and US

Security
- EU concept

What else?

Further development

Security and Privacy

EU

SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Requirements
- Authenticated senders
- Protect privacy of drivers
- Prevent message manipulation
- Prevent replay attacks
- …

US

Security-Payload IEEE 1609.2
Payload SAE J2735 SAE J2945
Security IEEE 1609.2
WSMP-Header IEEE 1609.3
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Security and Privacy

EU

SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Requirements

- Authenticated senders
- Protect privacy of drivers
- Prevent message manipulation
- Prevent replay attacks
- …

Security and Privacy

EU

SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

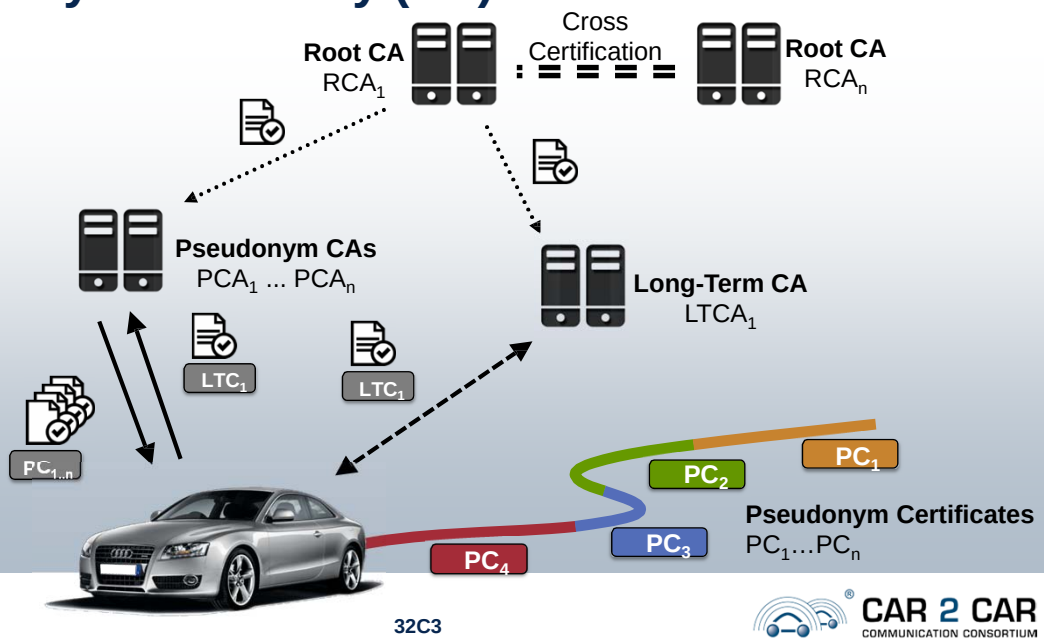
Requirements

- Authenticated senders
- Protect privacy of drivers
- Prevent message manipulation
- Prevent replay attacks
- …

Use of certificates

- But this is a unique Identifier!
- Privacy?
- Pseudonym Certificates (PC)
- Long Term Certificates (LTC)

Security and Privacy (EU)



Security and Privacy

EU

SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Pseudonym change

- Valid for one week
- >= 20 pseudonyms valid at the same time
- Pseudonym change …
  - At engine start
  - Every 10 to 30 minutes
- Upon changing the pseudonym, a random new pseudonym is chosen
- It is not allowed to use the same pseudonym twice successively

- This will be defined in the Basic Standard Profile of the C2C-CC
  - Unfortunately not yet published and still in the process of definition
  - Car2Car Communication Consortium (https://www.car-2-car.org/)

Security and Privacy

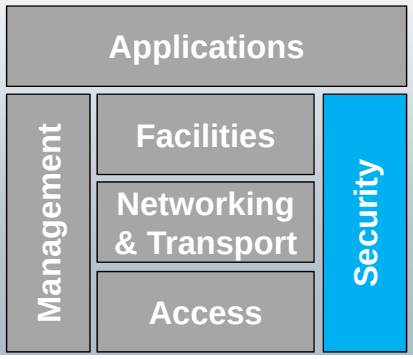
EU

SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Pseudonym change

- What is affected by a pseudonym change?

ETSI ITS G5 Stack



Security and Privacy

EU

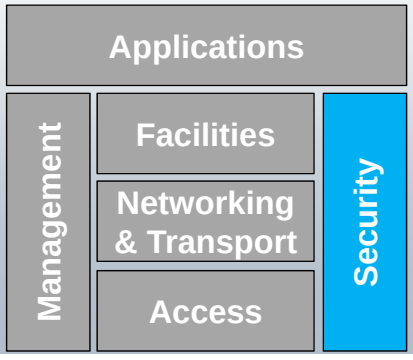
SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Pseudonym change

- What is affected by a pseudonym change?

- Each identifier has to be changed
  - MAC-Address
  - Pseudo Identifier

ETSI ITS G5 Stack



Security and Privacy

EU

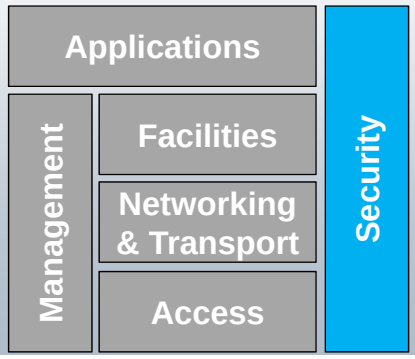
SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

Pseudonym change

- What is affected by a pseudonym change?

- Each identifier has to be changed
  - MAC-Address
  - Pseudo Identifier

ETSI ITS G5 Stack



Security and Privacy

EU

SecurityPayload ETSI TS 103 097
Payload ETSI EN 302 637-2 ETSI EN 302 637-3
BTP ETSI EN 302 636-5-1
GN-ExtendedHeader ETSI EN 302 636-4-1
GN-CommonHeader ETSI EN 302 636-4-1
Security ETSI TS 103 097
GN-BasicHeader ETSI EN 302 636-4-1
LLC+SNAP ISO/IEC 8802-2:1998
MAC IEEE 802.11

- Long Term Certificates are valid for several years. Depends on the vehicle manufacturers.

- Elliptic Curves for all certificates:
  - ECDSA 256
  - NIST Curve

- Standards are currently discussed with the “Bundesamt für Sicherheit in der Informationstechnik (BSI)”
  - Changes are expected
  - Brainpool instead of NIST
  - Curves should be exchangeable but will be ECDSA 256 to be able to use the same hardware acceleration
  - Algorithms for Root Certificate and LTC don’t have to be Elliptic Curves

Agenda

Introduction and Motivation

Basic Concepts

Standards
- EU and US

Security
- EU concept

What else?

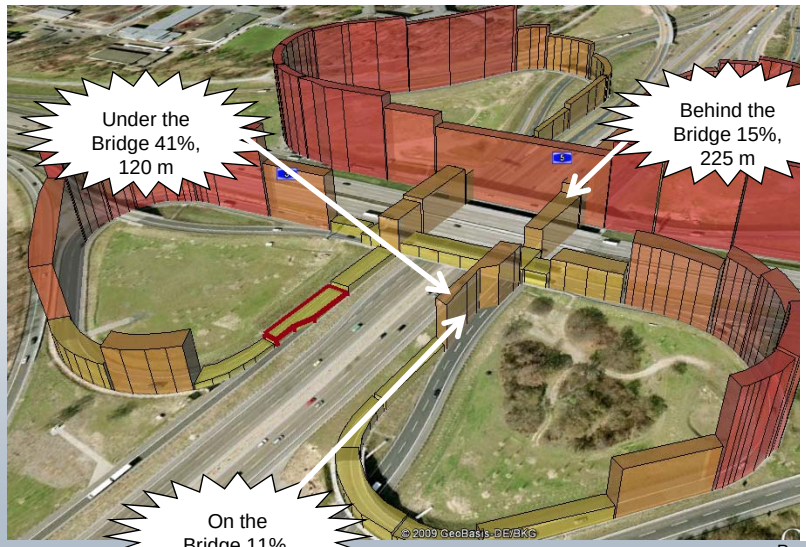
Further development

Conclusion

Summary
- Communication part of V2V Communication is standardized
- Includes security and privacy considerations

Work on additional standards
- Additional the quality and meaning of information in the messages has to be specified for the applications.
  - Minimum accuracy
  - Triggering conditions
  - Value interpretation
  - …
- **EU:** C2C-CC Standard Profile, C2C-CC Triggering conditions
- **US:** Minimum Performance Requirements

Challenges



- How many communication nodes can the wireless channel support?
- Is the communication range enough at high relative speeds?
- Environmental influence of communication?
- Coexistence with tolling stations (ETSI TS 102 792).
- …

Result: http://www.simtd.de/ Map: http://www.google.de/

Tools

IEEE 802.11p

- The Czech Technical University in Prague is working on upstreaming OCB support to the Linux Kernel.
- MAC, LLC+SNAP
- At the moment only supports ath9k
- https://ctu-iig.github.io/802.11p-linux/

Upper Layer for the European Standards

- GeoNetworking, BTP, CAM, DENM
- Security Header can be interpreted, but signing or verifying not yet supported
- https://github.com/riebl/vanetza

Agenda

Introduction and Motivation

Basic Concepts

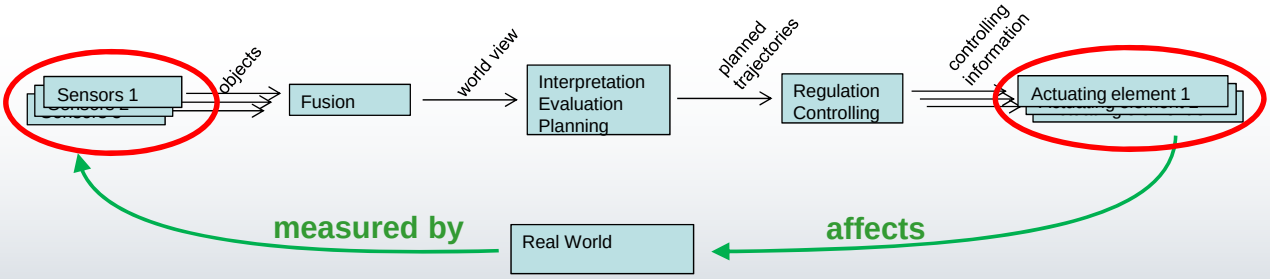
Standards
- EU and US

Security
- EU concept

What else?

Further development

V2V is an additional sensor … or is it more?

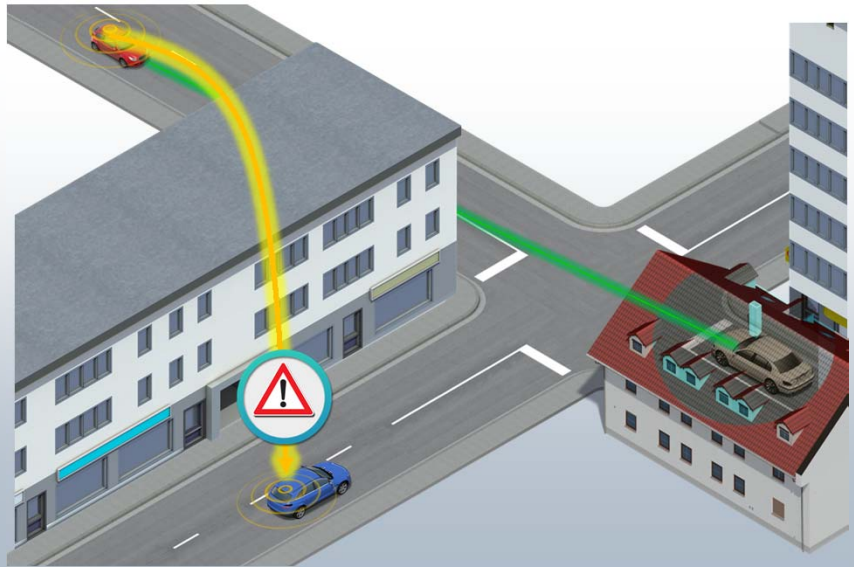


A V2V communication unit is like a radar?

Yes
- Same type of information. (Speed and position of other Objects)

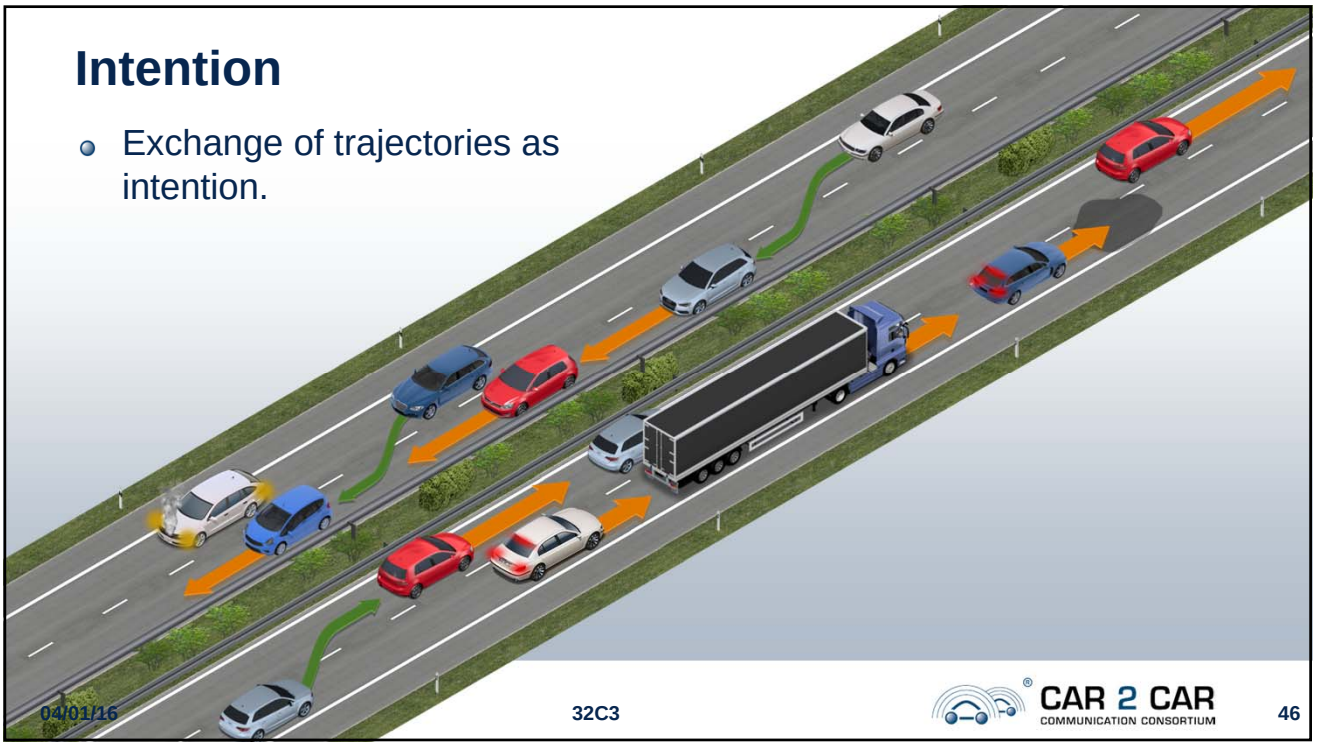
No
- No own measurement. Depends on the information of the sending vehicle.
- Complex data.
- Influence of other vehicles

Collective Perception



Intention

- Exchange of trajectories as intention.



Questions?

bernd[dot]lehmann[at]volkswagen[dot]de

Backup

Next mobile communication standard: 5G

- Technical
  - Not standardized yet!
  - Only requirements and promises known, but drawbacks unknown.
- Which layer?
  - Only physical layer?
  - Is security included?
- Functional safety
  - One more stakeholder
  - Depending on solution one more component
- Privacy
  - Mobile Network Operators (MNOs) forced by legislation to track user
- Cost
  - Business model

Talk Goals

- Idea/Concepts
- Insights into the V2V technology (basic system)
- Standards
- Security and privacy (EU)
- Further development of the technology

Remarks

- Everything is based on standards which are developed jointly together with many stakeholders
- A lot of evaluation was done in public funded projects
- No product information from vehicle manufacturers