Vehicular Networks

Course: Network Embedded Systems

Presenter: Alexander Dethof

Date: 2015-06-12

Technische Universität Berlin

TKN

Vehicular Networks are used for …

Road Safety

Traffic Management

Infotainment

Technische Universität Berlin

TKN

Vehicular Networks challenge ...

Reliable communication

Unreliable and fast-changing environment

Mobile and dynamically moving communication nodes

Security

Technische Universität Berlin TKN

Structure

Communication Basics	Security Aspects	Standardization Efforts
• Communication Types • Routing • Addressing	• Integrity • Privacy	• CALM • C2C • COMeSafety • WAVE • DSRC

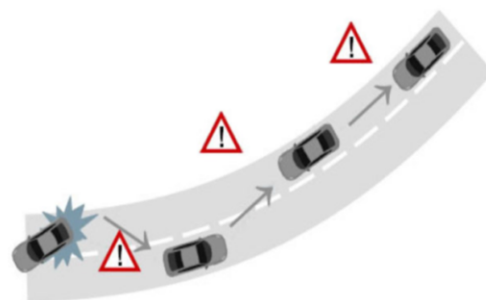
Technische Universität Berlin TKN

Communication Basics

Technische Universität Berlin TKN

Inter-vehicle communication

- Multi-hop multicast/broadcast
- Forwards messages of front vehicles
- All vehicles in forward direction are informed
- *Naïve broadcasting*
- *Intelligent broadcasting*



[2, figure 1]

Technische Universität Berlin TKN

6

Inter-vehicle communication

Naïve broadcasting

- Vehicles send broadcasts periodically
- Messages from behind are ignored
- Only front messages are forwarded
- **But:** Large message amount → collision

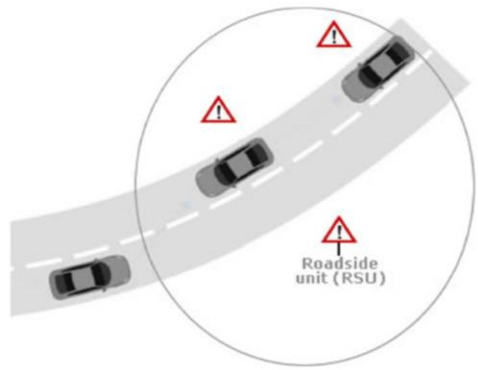
Intelligent broadcasting

- Improvement with selective forwarding
- Message will not be forwarded if the vehicle behind has sent it before
- Receiving a message of more than one source → React only on first

Technische Universität Berlin TKN

Vehicle-to-roadside communication

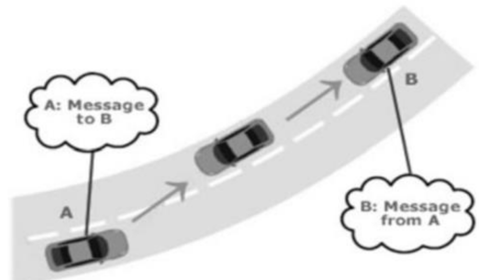
- Single hop broadcasts
- Road side units (RSUs) placed in regular (large) distances
- high data rates required for heavy traffics



[2, figure 2]

Routing-based communication

- Multi-hop unicast
- Message hops until it reaches the destination



[2, figure 3]

9

Routing

- Proactive Routing
- Reactive Routing
- Position-based Routing

Technische Universität Berlin

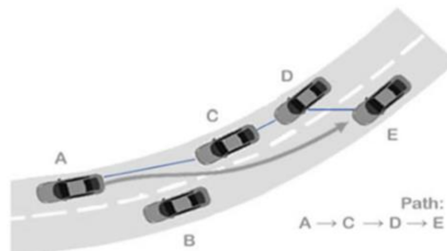
TKN

Position-based routing

- Sender may request position of receiver by a location service
- Routing decision bases on position map
- Does not require maintenance or setup information
- Several suggestions done how to move the message closer to the destination‘s positions
- Location Table (LT): Build with periodic broadcasts with own identifier and position
- If a vehicle is not in the LT, the vehicle may broadcast a request, which will be rebroadcasted, until the desired vehicle is found

Forwarding

- Forward by location table
- Greedy algorithm forwards than to the neighbouring vehicle in order to minimize the distance
- Forwarding must be loop-free
- Shortest-path is not useful each time, because of volatile network



[2, figure 5]

Technische Universität Berlin
TKN

Addressing

- GPS (+IPv6)
- Geographical domains with DNS
- Polygon

Technische Universität Berlin TKN

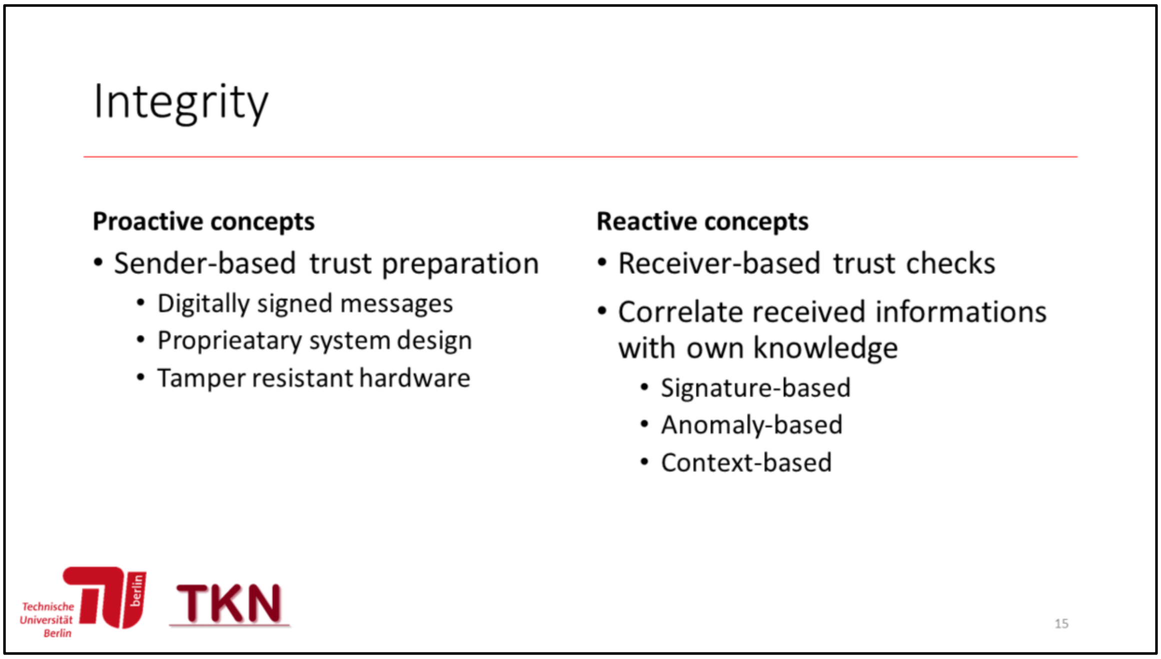
13

Several approaches are used to address the nodes in VANETs. Due to the dynamic changes in the network the idea occured to use geographical addressing methods in cooperation with logical addressing. So-called GPS addresses can be represented by closed polygons (e.g. circles) or names for sites, conties, cities, POIs (Point of Interest), … The geographical addreses can be integrated in the curent IPv6 header, but with GPS-SRC-Address and GPS-DST-Address fields. Further more a solution of using geographical domains is propsed, which encodes the position by a domain, named with some common location names nearby (city, county, …) and can be resolved via a given DNS service to IP addresses provided by base stations (e.g. RSUs) in the address zone.

Security Aspects

Technische Universität Berlin

TKN



The integrity approaches in VANETs mainly base on common known concepts. There are two main concepts categories: *proactive concepts* and *reactive concepts*. Proactive concepts implement mechanisms in which the sender ensures that the receiver is able to trust his messages, whereas in reactive concepts the receiver verifies if the received message is trustable or not.

Proactive concepts:

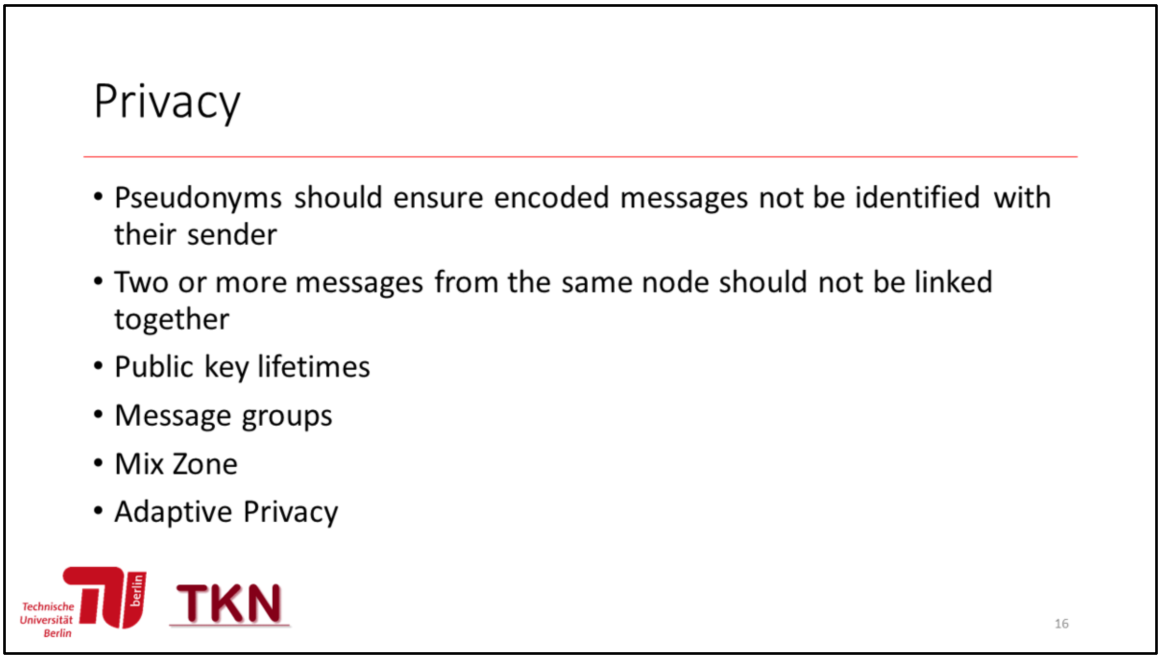
- *Digitally signed messages:* With certificate: more secure | without certificate: easier to implement
- *Proprietary system design:* e.g. non-public protocols, customized hardware, … | needs more effort to be hacked by the attacker | in order to generate a large product line quiet difficult to implement
- *Tamper resistant hardware:* Enhances the in-vehicle security

Reactive concepts:

- *signature-based:* cooperative approach to the digitally signed messages from the proactive concepts
- *anomaly-based:* system is aware of its usual behaviour and compares incoming messages if they are in order with the usual behaviour | messages out of this

behaviour are untrustable | very complex knowledge about each use-case needed to implement a reliable strategy

- *context-based: s*imiliar to anomaly-based approach but with including information of the vehicle‘s context | e.g. check if the same or a very related event has been detected on its own | constrained system description



Using cryptographic messages will enable sniffers to trace pathes of different drivers along their routes. Pseudonyms should help to abstract the message from the sender‘s origin. Further more it is requested that two consecutive messages sent from the same nodes can not be linked together.

Approaches:
- *Lifetimes*: must change simultaneously or silently, because traces still drawable with listening on consecutive messages
- *Message groups*: ensures that a vehicle in a group can only listen to the vehicle in ist group | all other vehicles outside the group are not able to listen
- *Mix Zone*: all vehicles in a specific zone share the same secret key | key is provided by RSU | public key changes automatically when leaving the zone
- *Adaptive Privacy*: User should decide the privacy factor, because higher privacy = greater communication overhead | hope to reduce the overhead | privacy as personal factor

Standardization Efforts

Technische Universität Berlin

TKN

Standards Overview

- High level standards:
  - ISO: CALM
  - IEEE 1609: WAVE
  - C2C-CC: C2C
  - ETSI, CEN: COMeSafety
- Low Level Standards:
  - IEEE 802.11p: DSRC

Technische Universität Berlin TKN

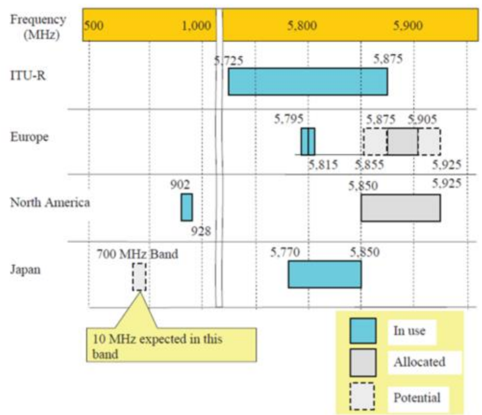
18

Across the world several standardization efforts for VANETs are in discussion. In the standardization process a bridge has to be built between the flexibility for futurous developments and the robustness, because vehicles have in general a long lifetime. Further more it is the aim to reduce the implementation costs by using common technologies, like WLAN (IEEE 802.11a).

DSRC

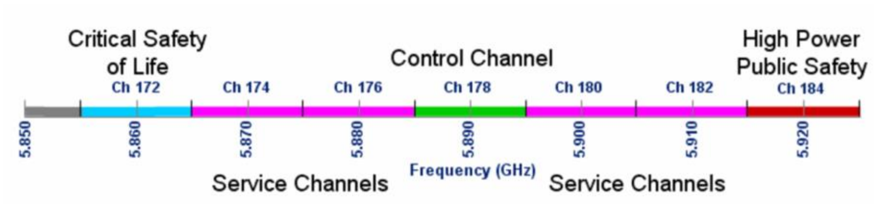
- ‘Dedicated Short Range Communication’
- High data rates at low latency
- Bases on IEEE 802.11a physical & mac layer
- OFDM: Orthogonal Frequency Division Modulation
- Adapted routing with CARAVAN and CEPEC

DSRC Standard

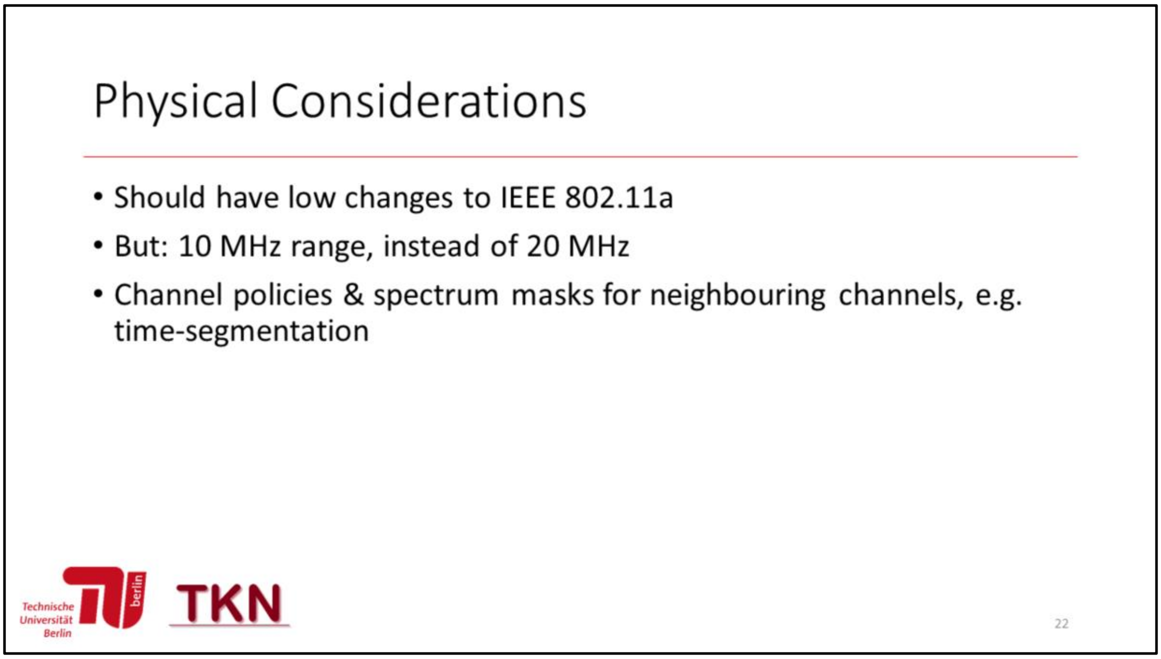


[3, figure 1]

DSRC Channels



[1, figure 2]

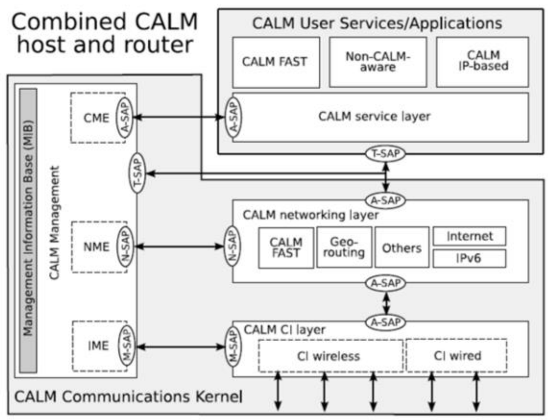


The DSRC standard origins in the IEEE 802.11a standard. In order to reduce costs, the physical layer should have only small changes. The most impactful change is the reduction of the channel width from 20 MHz to 10 MHz. The reason for this are a reduction of Doppler spreads (because of fast-moving nodes) and RMS delay spread which has been measured in several studies. Usually the delay spread is avoided by using gurad intervals. But in vehicular networks it as been measured that this interval has to be enlarged from 0.8µs to 1.6µs. Therfore the channel width has been reduced. Unfortunatly this means also a reduction of the channels capacity by half, but in further studies it was measured that the Doppler spread and the RMS delay spread has been reduced too.

Further more to avoid channel cross-interferences of neighbouring nodes (e.g. on a motorway), special channel policies have been adapted.

CALM

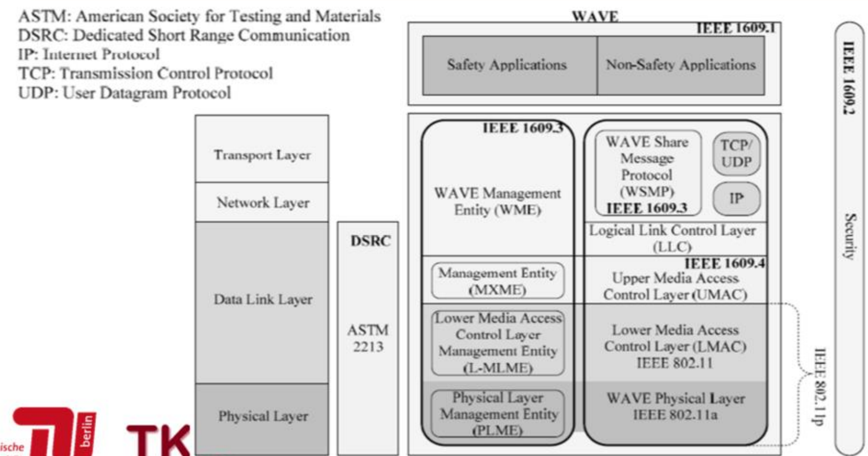
Continous air interface for long and medium distance



[4, figure 2.2]

WAVE (with DSRC)

Wireless Access in Vehicular Environments



[2, figure 4]

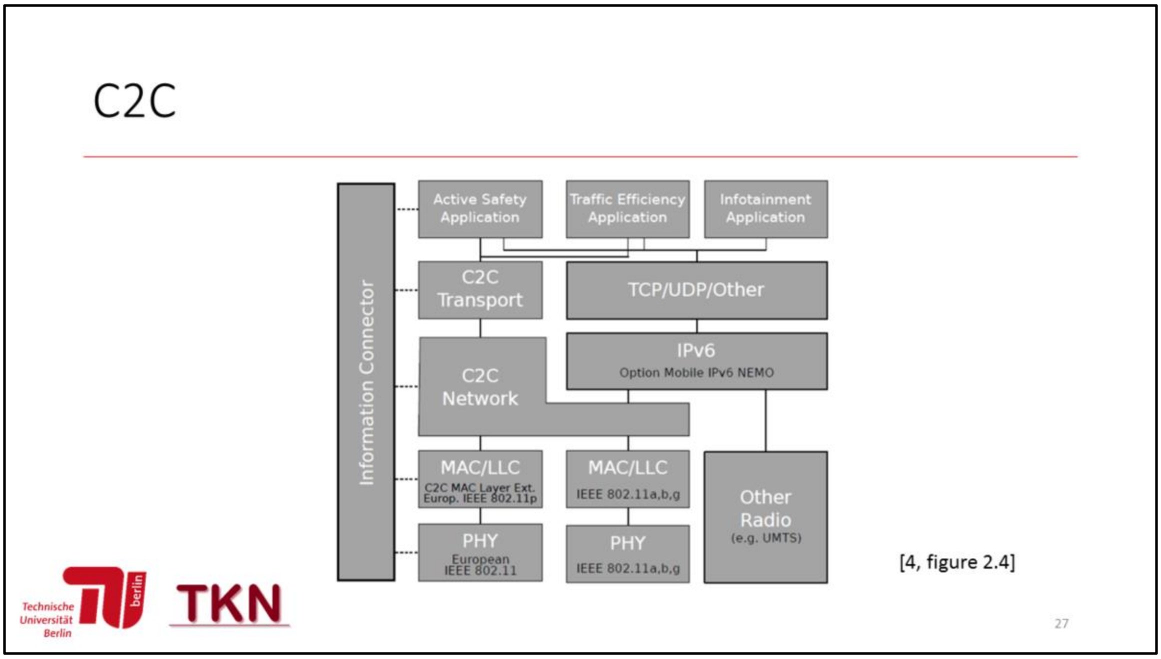
WAVE – MAC Purposes

- Low MAC overhead → simplifying BSS operations
- Also too expensive for non-safety applications
- New BSS type introduced: WBSS (WAVE BSS)

WAVE BSS

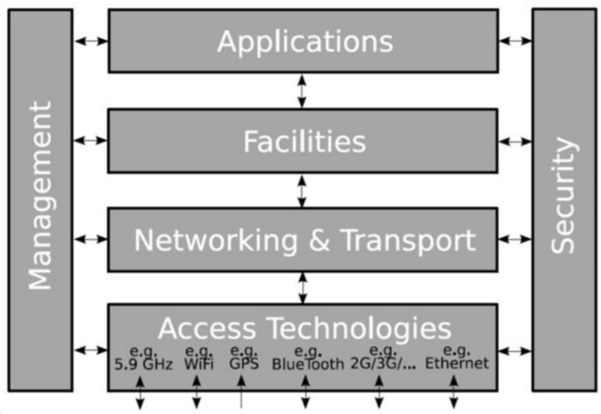
- BSS of WAVE stations
- Common BSSID
- Initialized via WAVE advertisment
- Includes all information to join
- Receiver can join without any further interaction
- Leave WBSS by stopping sending and receiving frames with BSSID
- One station can only be part of one WBSS
- Should not be part in any other (I)BSS or do scanning or MAC authentification
- WBSS without members does not exist
- Wildcard BSSIDs possible, independent if it is part of WBSS or not

Technische Universität Berlin TKN



Integration of the American WAVE standard into the European CALM standard with application-dependent network stacks.

COMeSafety



[4, figure 2.5]

Technische Universität Berlin TKN

28

The European COMeSafety standard unites the C2C and CALM standard. In difference to the European C2C and American WAVE standard, the network stacks are not separated by applications. But therefore a facilities and orthogonal security layer is added. The facilities layer provides commonly requested information and methods which can be used by applications from the upper layer. The security layer is an orthogonal pane to access security functionalities from each layer in the network stack.

Thanks for your attention!

Sources

[1] D. Jiang, L. Delgrossi. Mercedes-Benz Research & Development North America, Inc. "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments". IEEE. 2008

[2] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan. "Vehicular ad hoc networks (VANETS): status, results and challenges". Springer Science+Business Media. 2010

[3] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil. "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions". IEEE Communications Surveys & Tutorials. Vol. 13. No. 4. 2011

[4] Felix Schmidt-Eisenlohr. "Interference in Vehicle-to-Vehicle Communication Networks - Analysis, Modeling, Simulation and Assessment". Dissertation. Karlsruher Institut für Technologie. Fakultät für Informatik. Tag der mündlichen Prüfung: 09.02.2010

Questions?

Technische
Universität
Berlin

32

DSRC Standards

ARIB: Association of Radio Industries and Businesses
CEN: European Committee for Standardization
ASTM: American Society for Testing and Materials
OBU: On-Board Unit
RSU: Road Side Unit
ASK: Amplitude Shift Keying
PSK: Phase Shift Keying
OFDM: Orthogonal Frequency Division Multiplexing

Table 1 DSRC standards in Japan, Europe, and the US

Features	JAPAN (ARIB)	EUROPE (CEN)	USA (ASTM)
Communication	Half-duplex (OBU)/Full duplex (RSU)	Half-duplex	Half-duplex
Radio Frequency	5.8 GHz band	5.8 GHz band	5.9 GHz band
Band	80 MHz bandwidth	20 MHz bandwidth	75 MHz bandwidth
Channels	Downlink: 7 Uplink: 7	4	7
Channel Separation	5 MHz	5 MHz	10 MHz
Data Transmission rate	Down/Up-link 1 or 4 MBits/s	Down-link/500 Kbits/s Up-link/ 250 Kbits/s	Down/Up-link 3-27 Mbits/s
Coverage	30 meters	15–20 meters	1000 meters (max)
Modulation	2-ASK, 4-PSK	RSU: 2-ASK OBU: 2-PSK	OFDM

[2, table 1]

Technische Universität Berlin

TKN

Proactive routing protocols

- All nodes are periodically update with information about the network
- Updates occur regardless of network load, bandwidth constraints and network size
- Often inefficient for vehicular networks, because of fast network changes

Technische Universität Berlin TKN

Reactive routing protocols

- Implement route determination on demand
- Maintain only routes which are in use
- Leads to a reduction of network load
- More suitable due to low amount of routes used by vehicles

Technische Universität Berlin TKN