



Vehicular Networks [C2X]

Falko Dressler and Christoph Sommer

- Inter-Vehicle Communication

Technology

Technology

- Communication paradigms and media

Wireless Communication Technologies

Infrastructure-based

Infrastructureless

Broadcast

Cellular

Short Range

Medium Range

FM Radio,
DAB/DVB,
...

GSM
2G
Cellular

UMTS
3G
Cellular

LTE /
WiMAX
4G Cell.

Millimeter,
Infrared,
Visible

802.15.1
Bluetooth

802.15.4
ZigBee

802.11
Wi-Fi

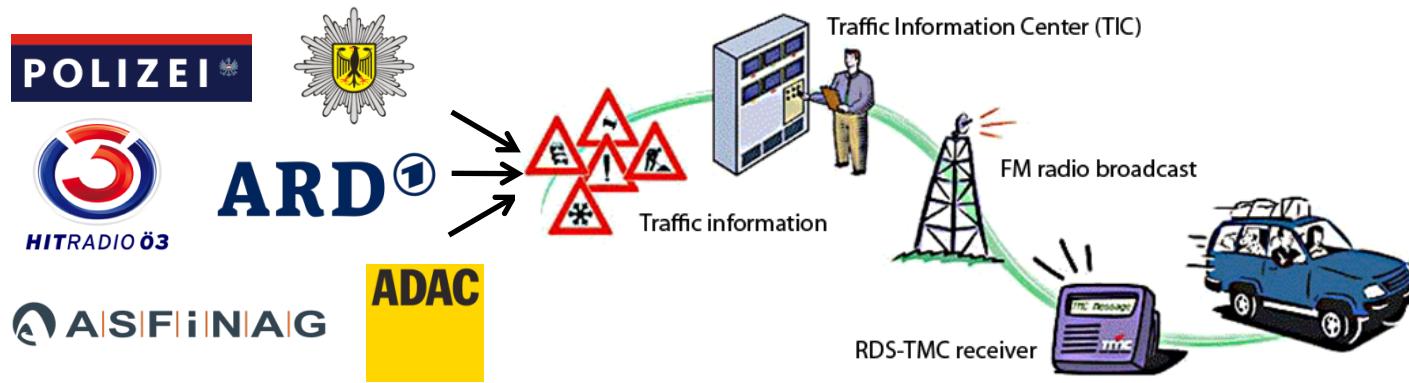
DSRC /
WAVE

[1] Dar, K. and Bakhouya, M. and Gaber, J. and Wack, M. and Lorenz, P., "Wireless Communication Technologies for ITS Applications," IEEE Communications Magazine, vol. 48 (5), pp. 156-162, May 2010

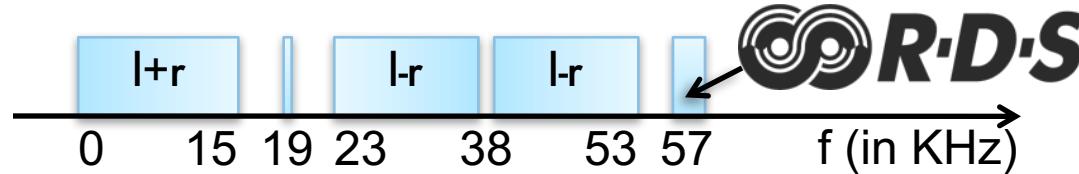
Broadcast Media

Broadcast Media

- Traffic Message Channel (TMC)
 - Central management of traffic information



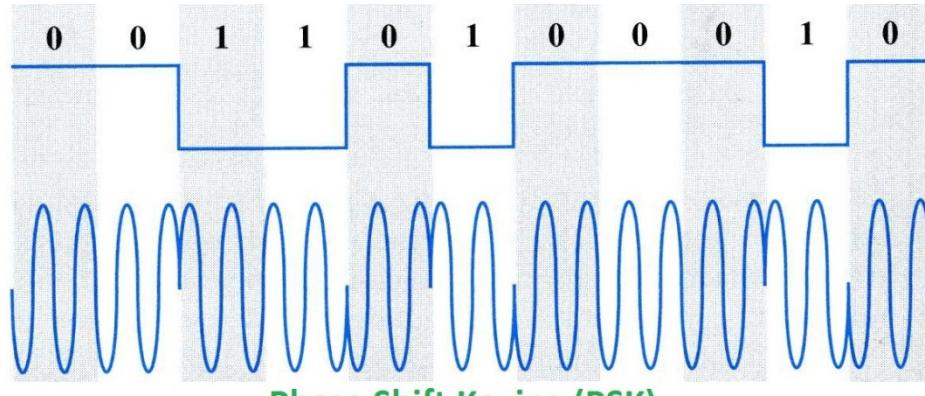
- Transmission in RDS channel of FM radio
 - BPSK modulated signal at 57 KHz, data rate 1.2 kBit/s
 - RDS group identifier 8A (TMC), approx. 10 bulletins per minute



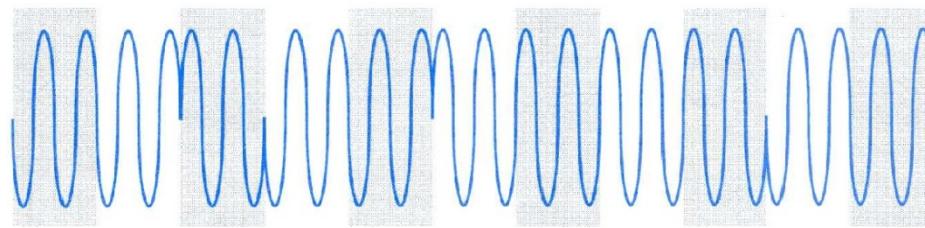
[1] ISO 62106, „Specification of the radio data system (RDS) for VHF/FM sound broadcasting in the frequency range from 87,5 to 108,0 MHz“

Broadcast Media

- Traffic Message Channel (TMC)
 - Phase Shift Keying (PSK)



Or called BPSK, uses two phases to represent 0 & 1



0 - no phase change
1 - phase change

Source: La Trobe University, Joel Sing, <http://ironbark.bendi.go.l.atrobe.edu.au/subjects/DC/lectures/7/>

Broadcast Media

■ Traffic Message Channel (TMC)

■ Contents (ALERT-C coded):

- Validity period
- Re-routing required?
- North-east or south-west?

- Spatial extent
- Code in event table

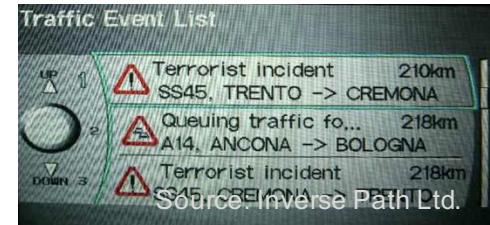
- International

■ Code in location table

- Country/region specific
- Must be installed in end device

■ No (real) security measures

101	Standing traffic (generic)
102	1 km of standing traffic
103	2 km of standing traffic
394	Broken down truck
1478	Terrorist incident
1	Deutschland
264	Bayern
12579	A8 Anschlussstelle Irschenberg

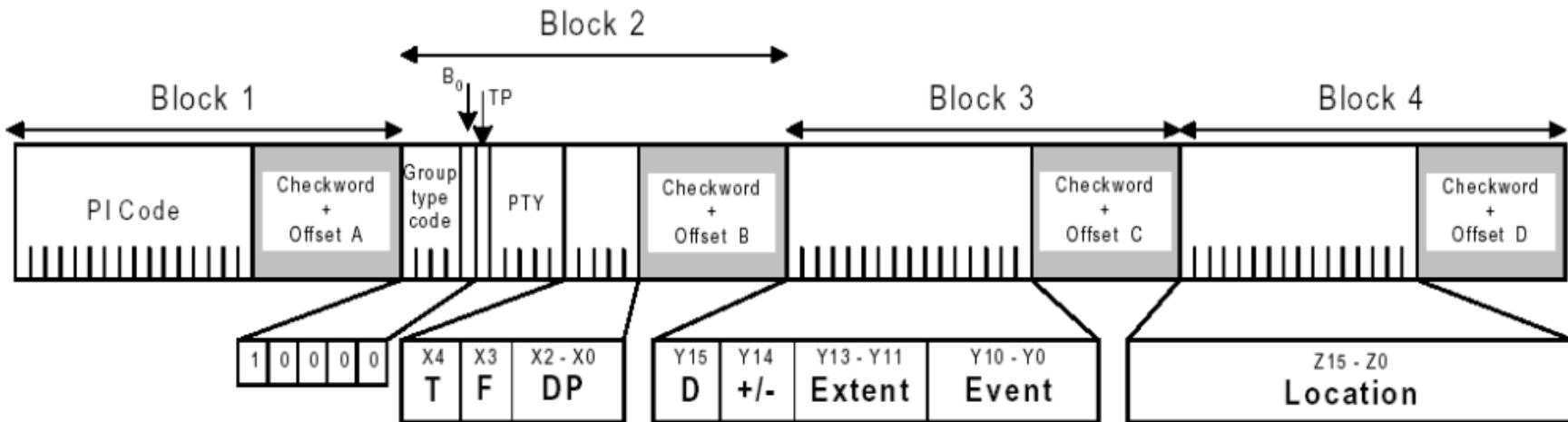


[1] ISO 14819-1, „Traffic and Traveller Information (TTI) - TTI messages via traffic message coding - Part 1: Coding protocol for Radio Data System (RDS-TMC) using ALERT-C“

[2] ISO 14819-2, „Traffic and Traveller Information (TTI) - TTI messages via traffic message coding - Part 2: Event and information codes for Radio Data System - Traffic Message Channel (RDS-TMC)“

Broadcast Media

■ Traffic Message Channel (TMC)



Source: M. Krieser, M. Buschmann: Protokollierung und statistische Auswertung von RDS/TMC Datenströmen

T = User or tuning message

F = multi-group/single-group message

DP = duration

D = re-routing flag

+/- = heading

Broadcast Media

- Traffic Message Channel (TMC)
 - Regional value added services
 - *Navteq Traffic RDS* (U.S.), *trafficmaster* (UK), *V-Trafic* (France)
 - Ex: TMCpro
 - Private service of Navteq Services GmbH
 - Financed by per-decoder license fee
 - Data collection and processing
 - Fully automatic
 - Deployment of 4000+ sensors on overpasses
 - Use of floating car data
 - Downlink from traffic information centers
 - Event prediction
 - Expert systems, neuronal networks
 - Early warnings of predicted events
 - Restricted to major roads

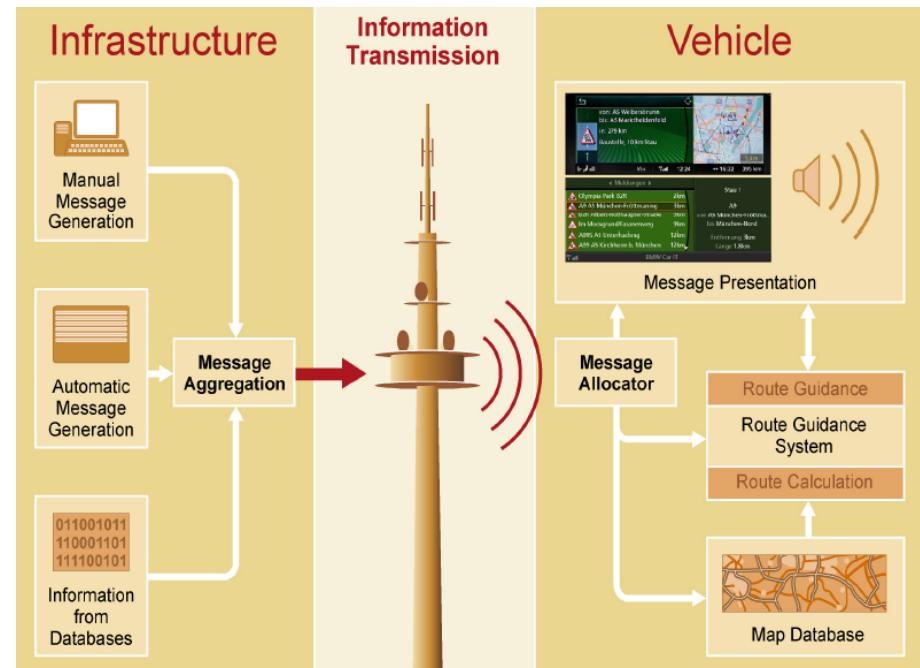
TMC PRO



Source: heise

Broadcast Media

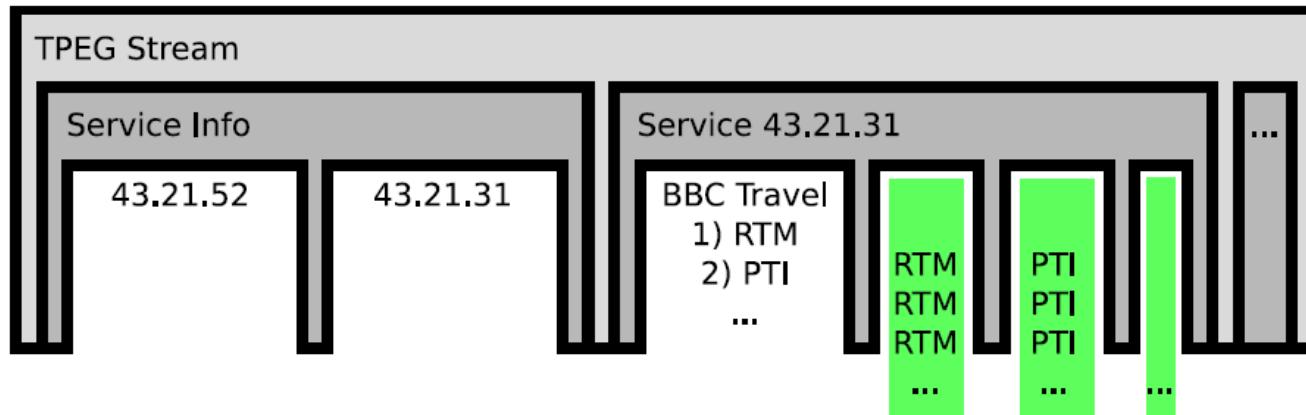
- Transport Protocol Experts Group (TPEG)
 - Planned successor of RDS-TMC/Alert-C, published April 2000
 - Principles:
 - Extensibility
 - Media independence
- Goals:
 - Built for “Digital Audio Broadcast” (DAB)
 - Unidirectional, byte oriented stream
 - Modular concept
 - Hierarchical approach
 - Integrated security



[1] ISO 18234-x, „Traffic and Travel Information (TTI) — TTI via Transport Protocol Experts Group (TPEG) data-streams“

Broadcast Media

- Transport Protocol Experts Group (TPEG)
 - Information types defined by “TPEG Applications”
 - RTM - Road Traffic Message
 - PTI - Public Transport Information
 - PKI - Parking Information
 - CTT - Congestion and Travel-Time
 - TEC - Traffic Event Compact
 - WEA - Weather information for travelers
 - Modular concept:



Broadcast Media

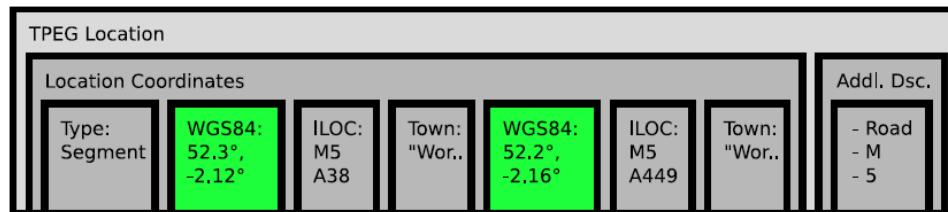
- Transport Protocol Experts Group (TPEG)
 - tpegML: XML variant of regular (binary) TPEG

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE tpeg_document PUBLIC "-//EBU/tpegML/EN"
  "http://www.bbc.co.uk/travelnews/xml/tpegml_en/tpegML.dtd">
<tpg_document generation_time="2007-09-19T07:22:44+0">
  <tpg_message>
    <originator country="UK" originator_name="BBC Travel News"/>
    <summary xml:lang="en">M5 Worcestershire - Earlier accident
      southbound between J5, Droitwich and J6, Worcester, heavy
      traffic.</summary>
    <road_traffic_message>
      <!-- ... tpeg-rtmML ... -->
    </road_traffic_message>
  </tpg_message>
  <tpg_message>
    <originator country="UK" originator_name="BBC Travel News"/>
    <summary xml:lang="en">A420 Oxfordshire - The Plain closed westbound
      at the A4158 Iffley Road junction in Oxford, delays expected.
      Diversion in operation.</summary>
    <road_traffic_message>
      <!-- ... tpeg-rtmML ... -->
    </road_traffic_message>
  </tpg_message>
</tpg_document>
```

[1] ISO 24530-x, „Traffic and Travel Information (TTI) — TTI via Transport Protocol Experts Group (TPEG) Extensible Markup Language (XML)“

Broadcast Media

- Transport Protocol Experts Group (TPEG)
 - Hybrid approach to geo-referencing: one or more of
 - WGS84 based coordinates
 - ILOC (Intersection Location)
 - Normalized, shortened textual representation of street names intersecting at desired point
 - Human readable plain text
 - Code in hierarchical location table

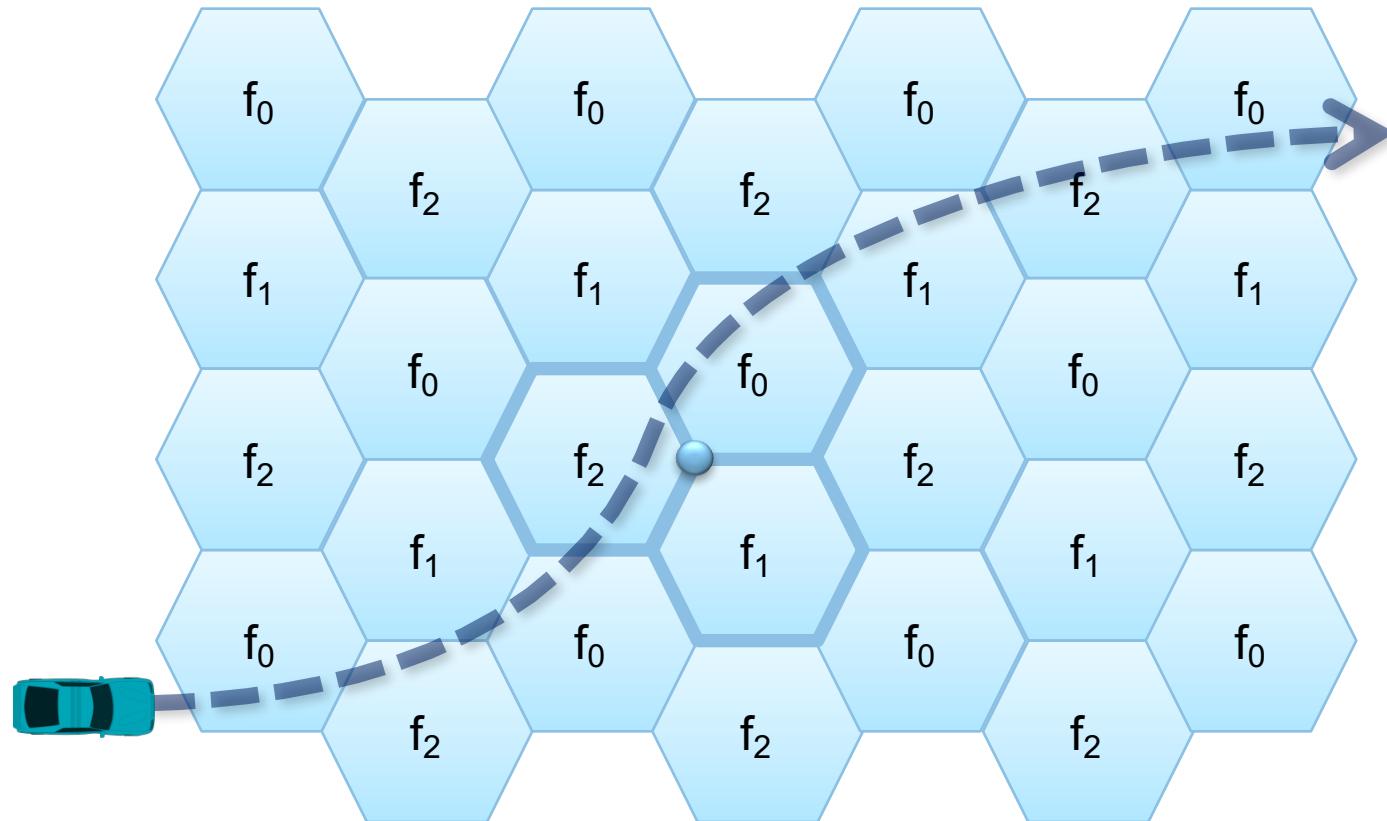


Cellular Networks

Cellular Networks

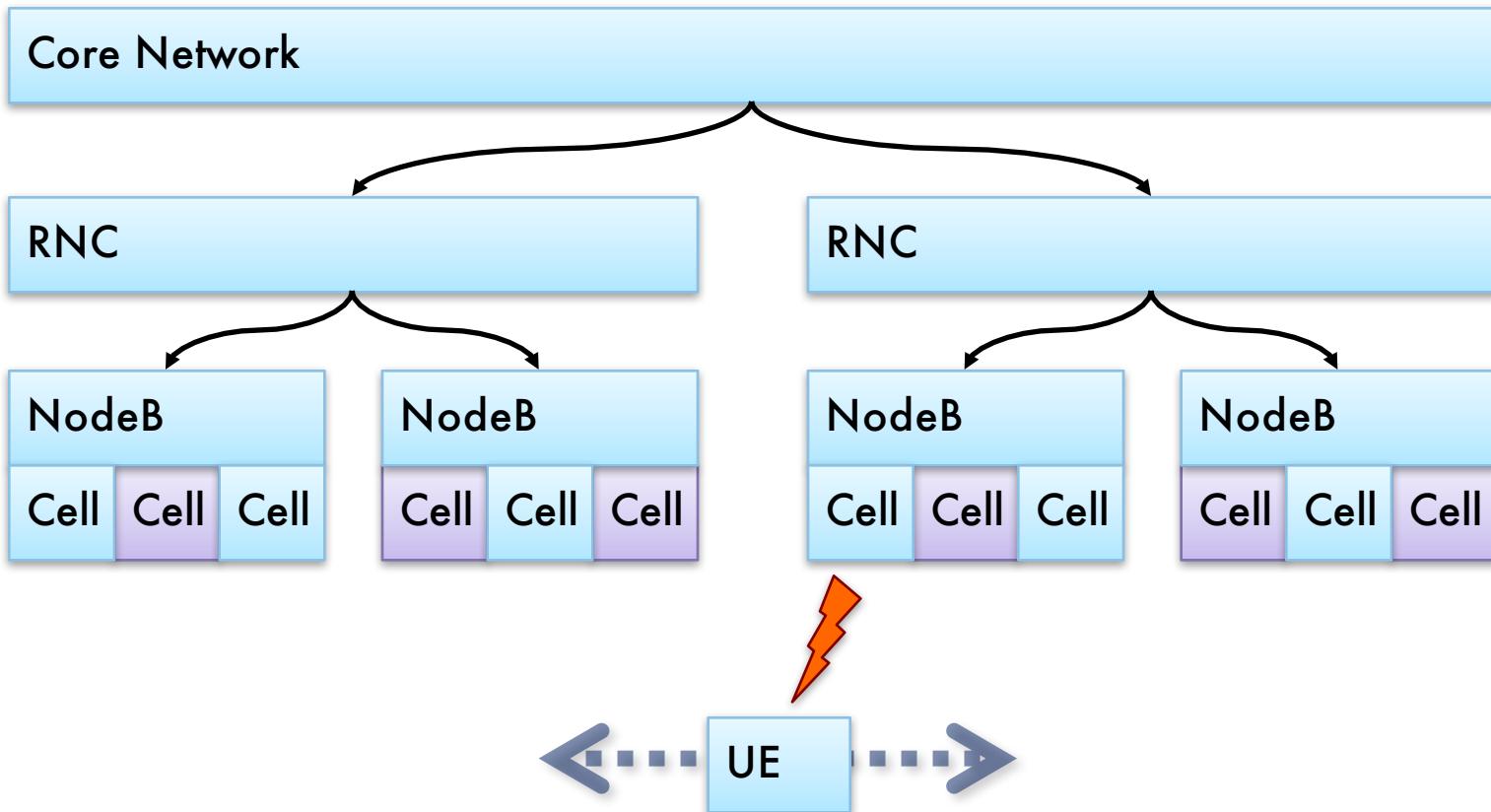
■ Concept

- Divide world into cells, each served by base station
- Allows, e.g., frequency reuse in FDMA



Cellular Networks

- Concept
 - Strict hierarchy of network components



Cellular Networks

- Can UMTS support Car-to-X communication?
 - Ex: UTRA FDD Release 99 (W-CDMA)
 - Speed of vehicles not a limiting factor
 - Field operational tests at 290 km/h show signal drops only after sudden braking (\Rightarrow handover prediction failures)
 - Open questions
 - Delay
 - Capacity
- Channels in UMTS
 - Shared channels
 - E.g., Random Access Channel (RACH), uplink and Forward Access Channel (FACH), downlink
 - Dedicated channels
 - E.g., Dedicated Transport Channel (DCH), up-/downlink

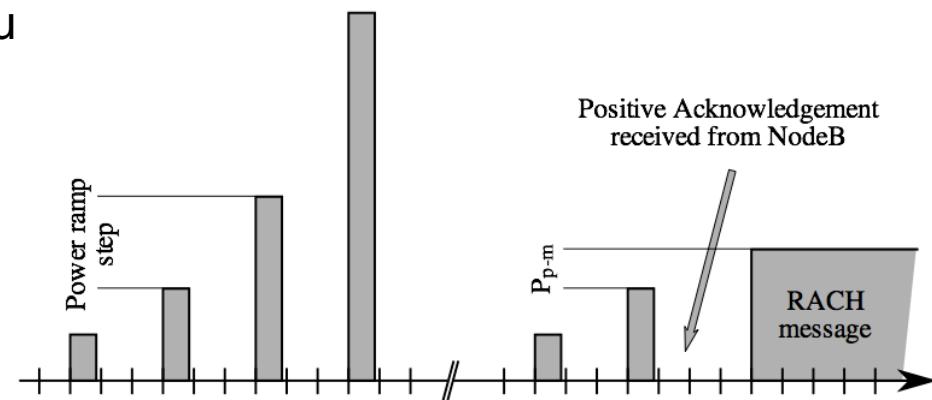
Cellular Networks

■ FACH

- Time slots managed by base station
- Delay on the order of 10 ms per 40 Byte and UE
- Capacity severely limited (in non-multicast networks)
- Need to know current cell of UE

■ RACH

- Slotted ALOHA – random access by UEs
 - Power ramping with Acqu
- Delay approx. 50 ms per 60 Byte and UE
- Massive interference with other UEs



Cellular Networks

- DCH
 - Delay: approx. 250 ms / 2 s / 10 s for channel establishment
 - Depends on how fine-grained UE position is known
 - Maintaining a DCH is expensive
 - Closed-Loop Power Control (no interference of other UEs)
 - Handover between cells
 - ...
 - Upper limit of approx. 100 UEs

Cellular Networks

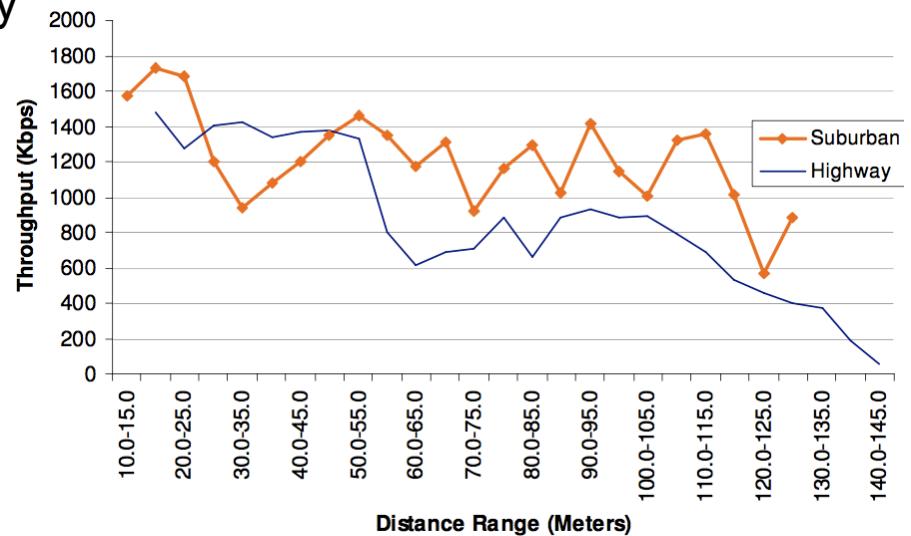
- So: can UMTS support Car-to-X communication?
 - At low market penetration: yes
 - Eventually:
 - Need to invest in much smaller cells (e.g., along freeways)
 - Need to implement multicast functionality (MBMS)
 - Main use case for UMTS: centralized services
 - Ex.: Google Maps Traffic
 - Collect information from UMTS devices
 - Storage of data on central server
 - Dissemination via Internet (⇒ ideal for cellular networks)

Infrastructureless

IEEE 802.11p

■ IEEE 802.11{a,b,g,n} for Car-to-X communication?

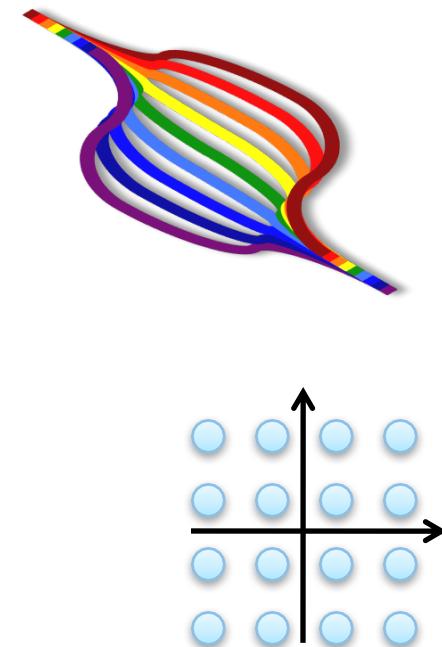
- Can't be in infrastructure mode and ad hoc mode at the same time
- Switching time consuming
- Association time consuming
- No integral within-network security
- (Massively) shared spectrum (\Rightarrow ISM)
- No integral QoS
- Multi-path effects reduce range and speed



[1] Fay Hui, Prasant Mohapatra. „Experimental Characterization of Multihop Communications in Vehicular Ad Hoc Network“. In Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005

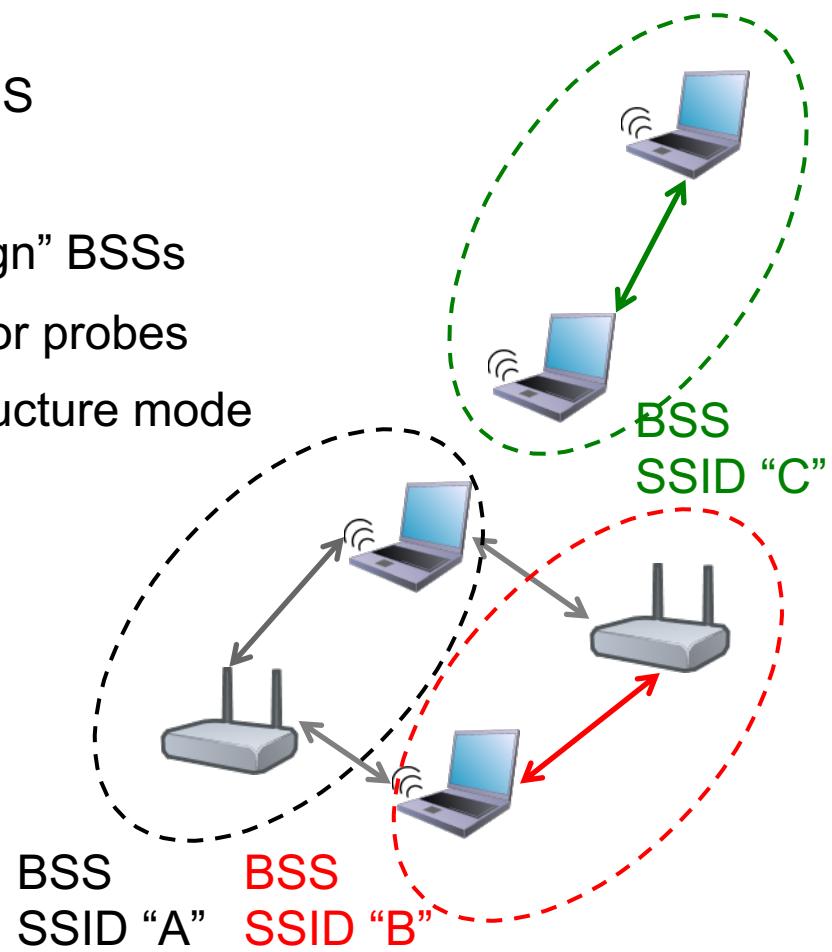
IEEE 802.11p

- IEEE 802.11p
 - PHY layer mostly identical to IEEE 802.11a
 - Variant with OFDM and 16 QAM
 - Higher demands on tolerances
 - Reduction of inter symbol interference because of multi-path effects
 - Double timing parameters
 - Channel bandwidth down to 10 MHz (from 20 MHz)
 - Throughput down to 3 ... 27 Mbit/s (from 6 ... 54 Mbit/s)
 - Range up to 1000 m, speed up to 200 km/h
 - MAC layer of IEEE 802.11a plus extensions
 - Random MAC Address
 - QoS (EDCA priority access, cf. IEEE 802.11e, ...)
 - Multi-Frequency and Multi-Radio capabilities
 - New Ad Hoc mode
 - ...



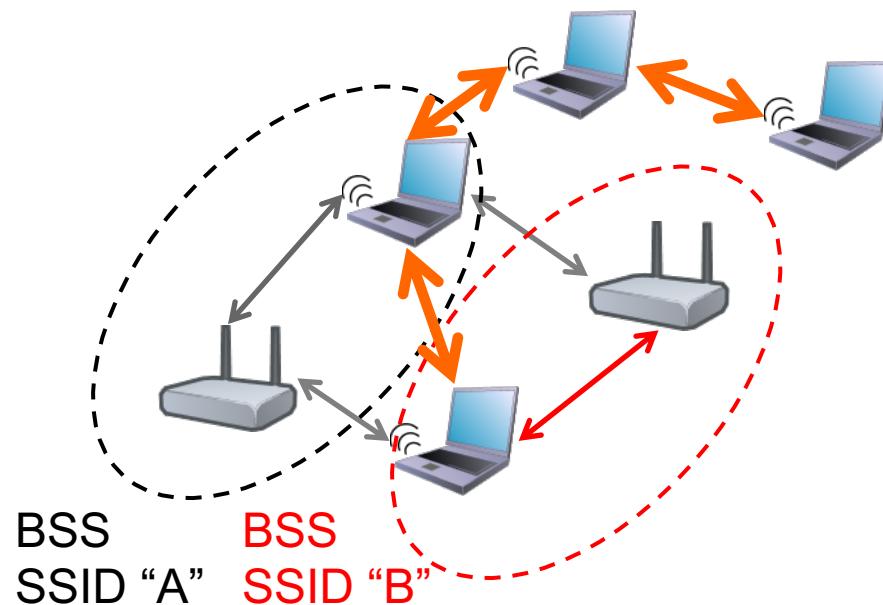
IEEE 802.11p

- Classic IEEE 802.11 Basic Service Set (BSS)
 - Divides networks into logical units
 - Nodes belong to (exactly one) BSS
 - Packets contain BSSID
 - Nodes ignore packets from “foreign” BSSs
 - Exception: Wildcard-BSSID (-1) for probes
 - Ad hoc networks emulate infrastructure mode
 - Joining a BSS
 - Access Point sends beacon
 - Authentication dialogue
 - Association dialogue
 - Node has joined BSS



IEEE 802.11p

- New: 802.11 OCB Mode
 - Default mode of nodes in WAVE
 - Nodes may always use Wildcard BSS in packets
 - Nodes will always receive Wildcard BSS packets
 - May join BSS and still use Wildcard BSS

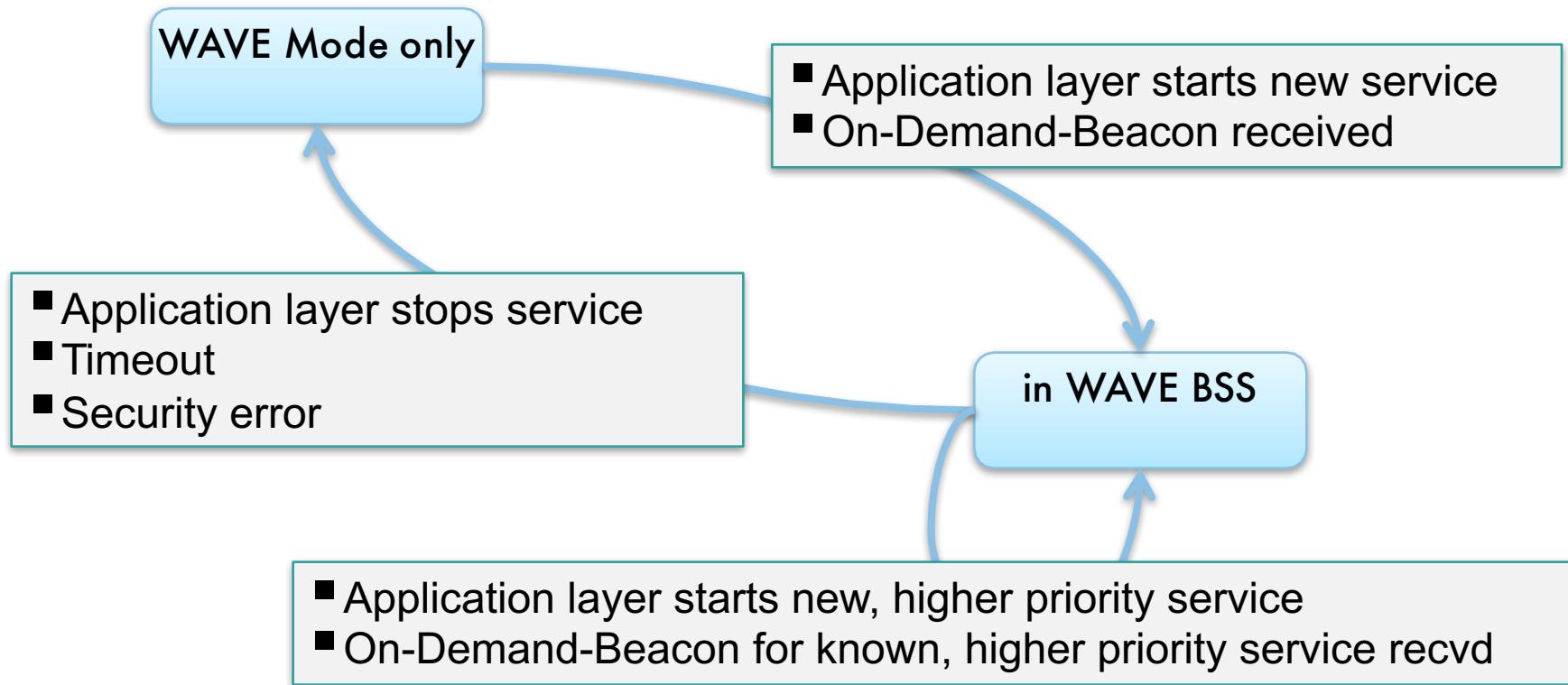


IEEE 802.11p

- New: 802.11 WAVE BSS
 - No strict separation between Host and Access Point (AP)
 - Instead, loose classification according to:
 - Equipment: Roadside Unit (RSU) / On-Board Unit (OBU)
 - Role in data exchange: Provider / User
 - No technical difference between Provider and User
 - Provider sends On-Demand Beacon
 - Analogous to standard 802.11-Beacon
 - Beacon contains all information and parameters needed to join
 - User configures lower layers accordingly
 - Starts using provided service
 - No additional exchange of data needed
 - BSS membership now only implied
 - BSS continues to exist even after provider leaves

IEEE 802.11p

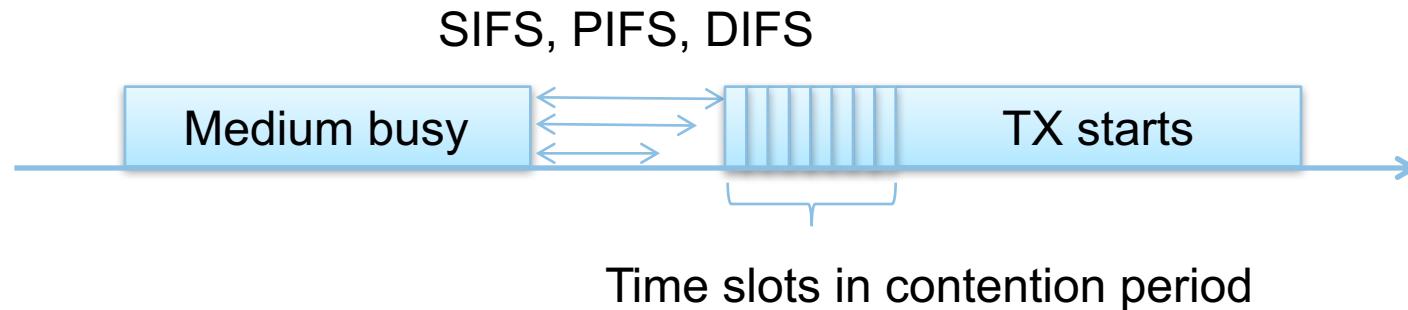
- WAVE BSS Internal state machine
 - Node will not join more than one WAVE BSS



[1] IEEE Vehicular Technology Society, "IEEE 1609.3 (Networking Services)," IEEE Std, April, 2007

IEEE 802.11p

- IEEE 802.11 Distributed Coordination Function (DCF)
 - aka “Contention Period”



- Priority access via SIFS (ACK, CTS, ...) and DIFS (payload)
- Wait until medium has been free for duration of DIFS
- If medium busy, wait until idle, then wait DIFS plus random backoff time

IEEE 802.11p

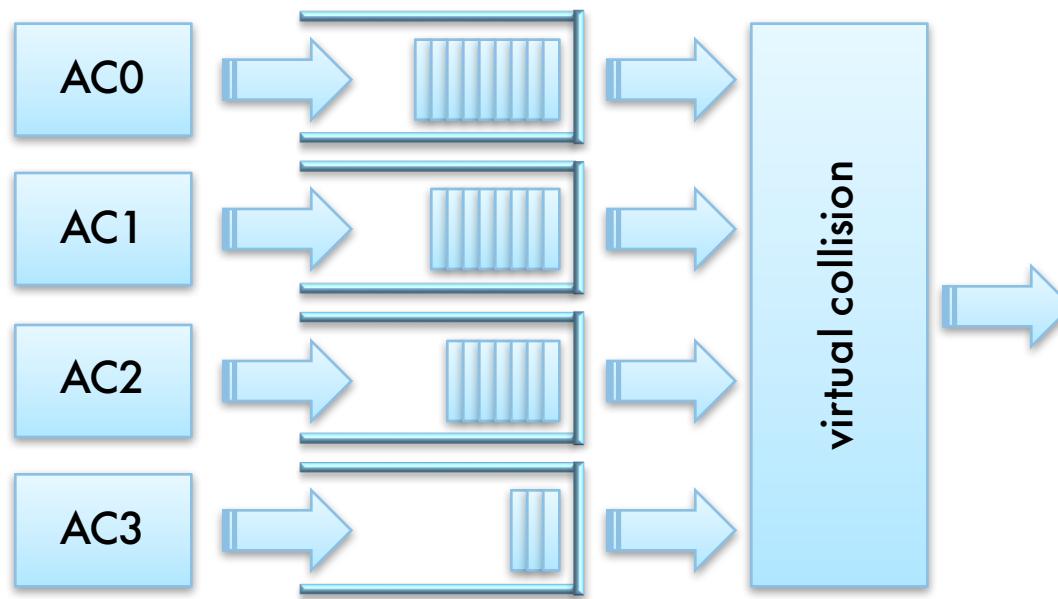
- IEEE 802.11 Distributed Coordination Function (DCF)
 - Backoff if
 - a) Node is ready to send and channel becomes busy
 - b) A higher priority queue (\Rightarrow next slides) becomes ready to send
 - c) Unicast transmission failed (no ACK)
 - d) Transmission completed successfully
 - Backoff: Random slot count from interval $[0, CW]$
 - Decrement by one after channel was idle for one slot
(only in contention period)
 - In cases b) and c), double CW (but no larger than CW_{max})
 - In case d), set CW to CW_{min}

IEEE 802.11p

- QoS in 802.11p Hybrid Coordination Function (HCF)
 - cf. IEEE 802.11e EDCA
 - DIFS \Rightarrow AIFS (Arbitration Inter-Frame Space)
 - DCF \Rightarrow EDCA (Enhanced Distributed Channel Access)
 - Classify user data into 4 ACs (Access Categories)
 - AC0 (lowest priority)
 - ...
 - AC3 (highest priority)
 - Each ACs has different...
 - CW_{min} , CW_{max} , AIFS, TXOP limit (max. continuous transmissions)
 - Management data uses DIFS (not AIFS)

IEEE 802.11p

- QoS in 802.11p (HCF)
 - Map 8 user priorities \Rightarrow 4 access categories \Rightarrow 4 queues
 - Queues compete independently for medium access



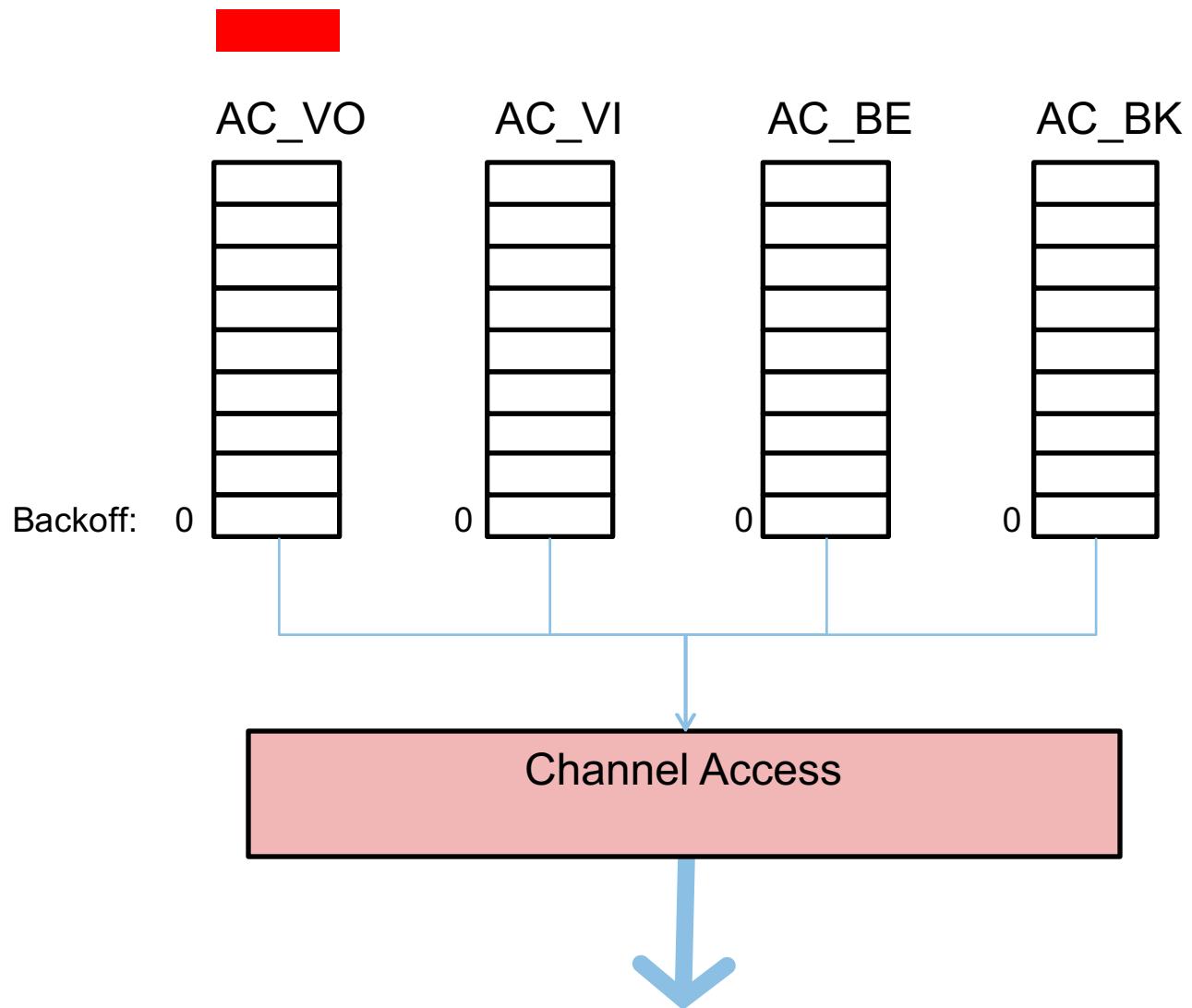
IEEE 802.11p

- QoS in 802.11p (HCF)
 - Parameterization

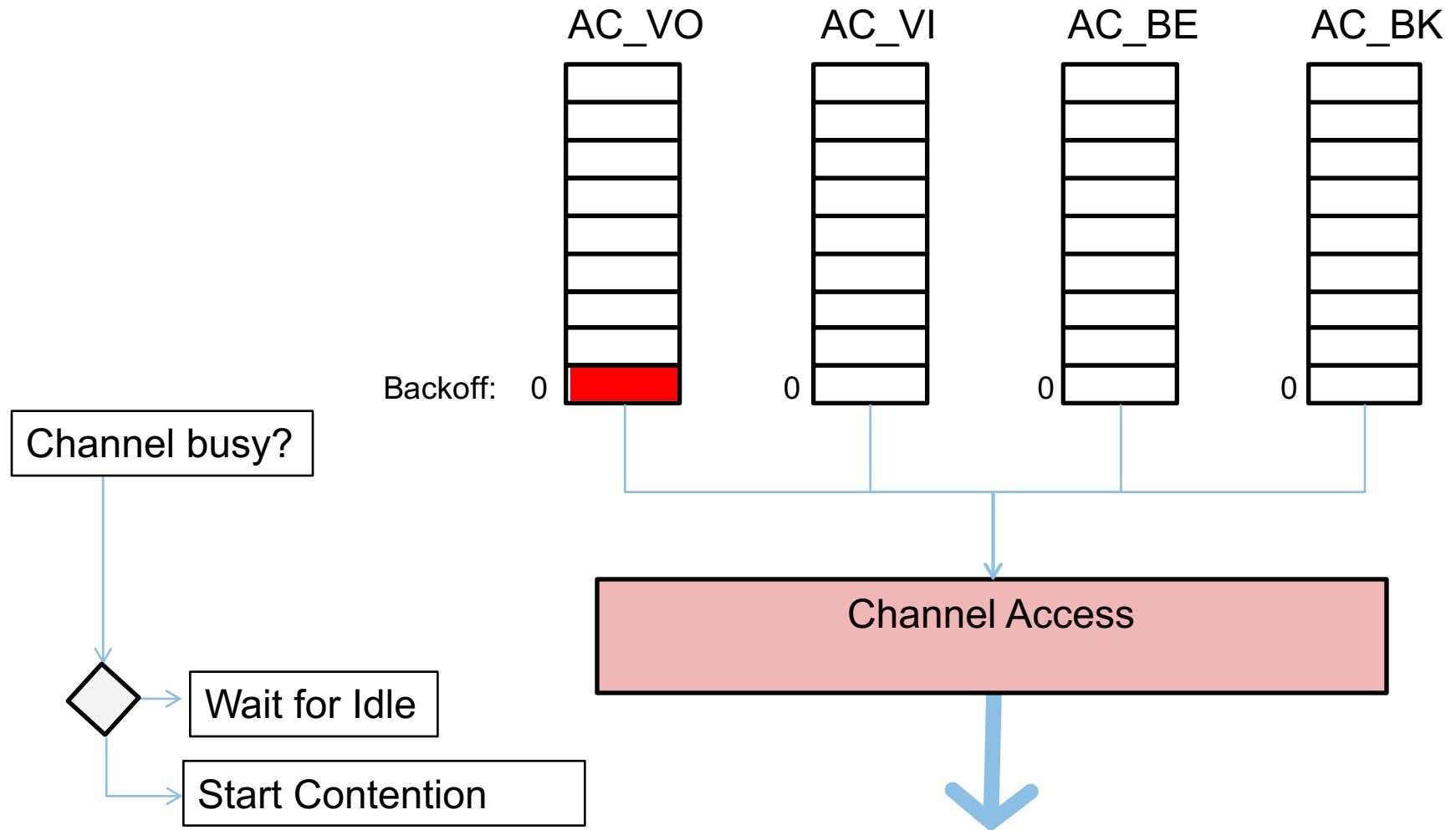
Parameter	Value
SlotTime	13µs
SIFS	32µs
CW _{min}	15
CW _{max}	1023
Bandwidth	3 .. 27 mbit/s

Parameter	AC_BK	AC_BE	AC_VI	AC_VO
CW _{min}	CW _{min}	CW _{min}	(CW _{min} +1)/2-1	(CW _{min} +1)/4-1
CW _{max}	CW _{max}	CW _{max}	CW _{min}	(CW _{min} +1)/2-1
AIFS _n	9	6	3	2

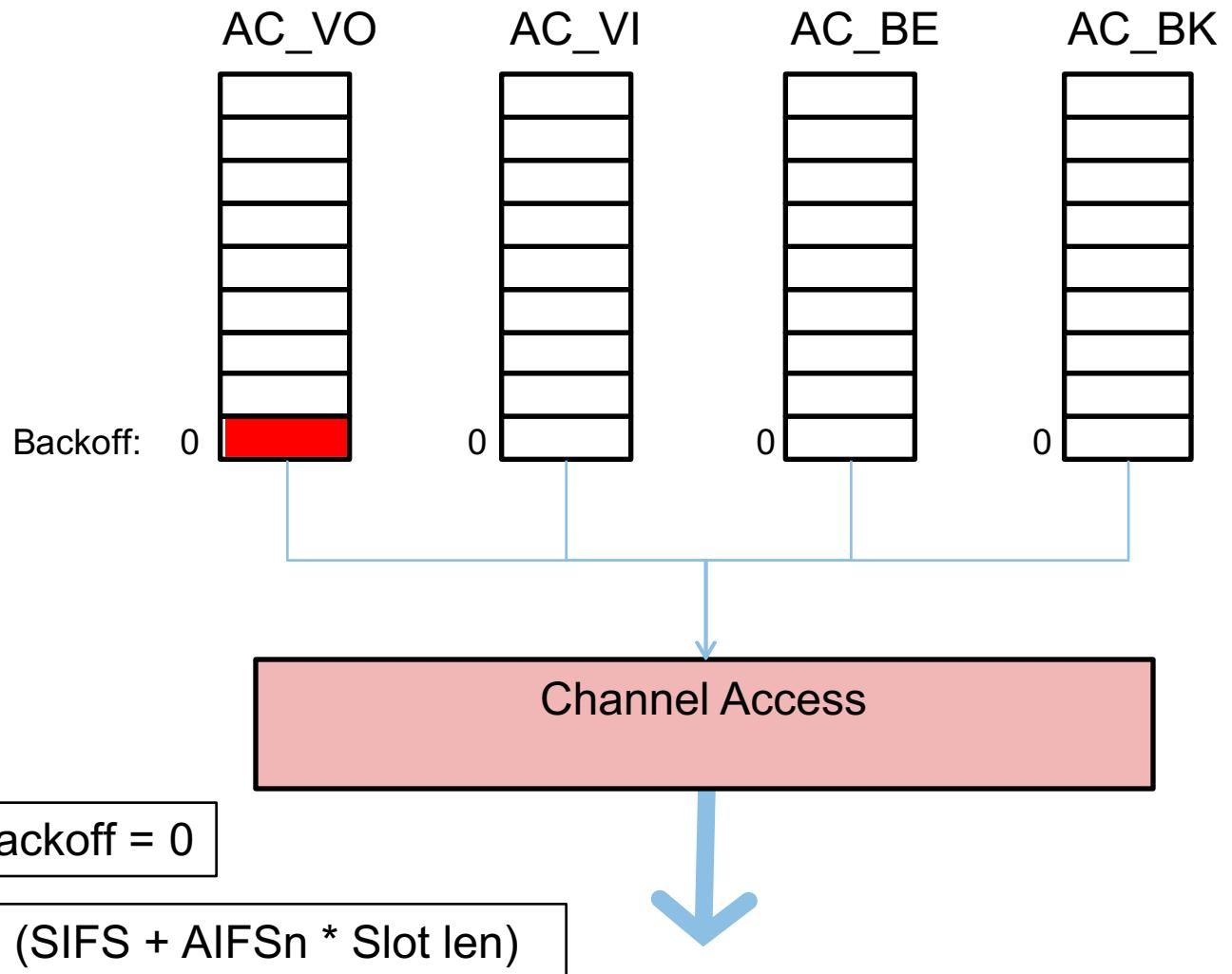
IEEE 802.11p



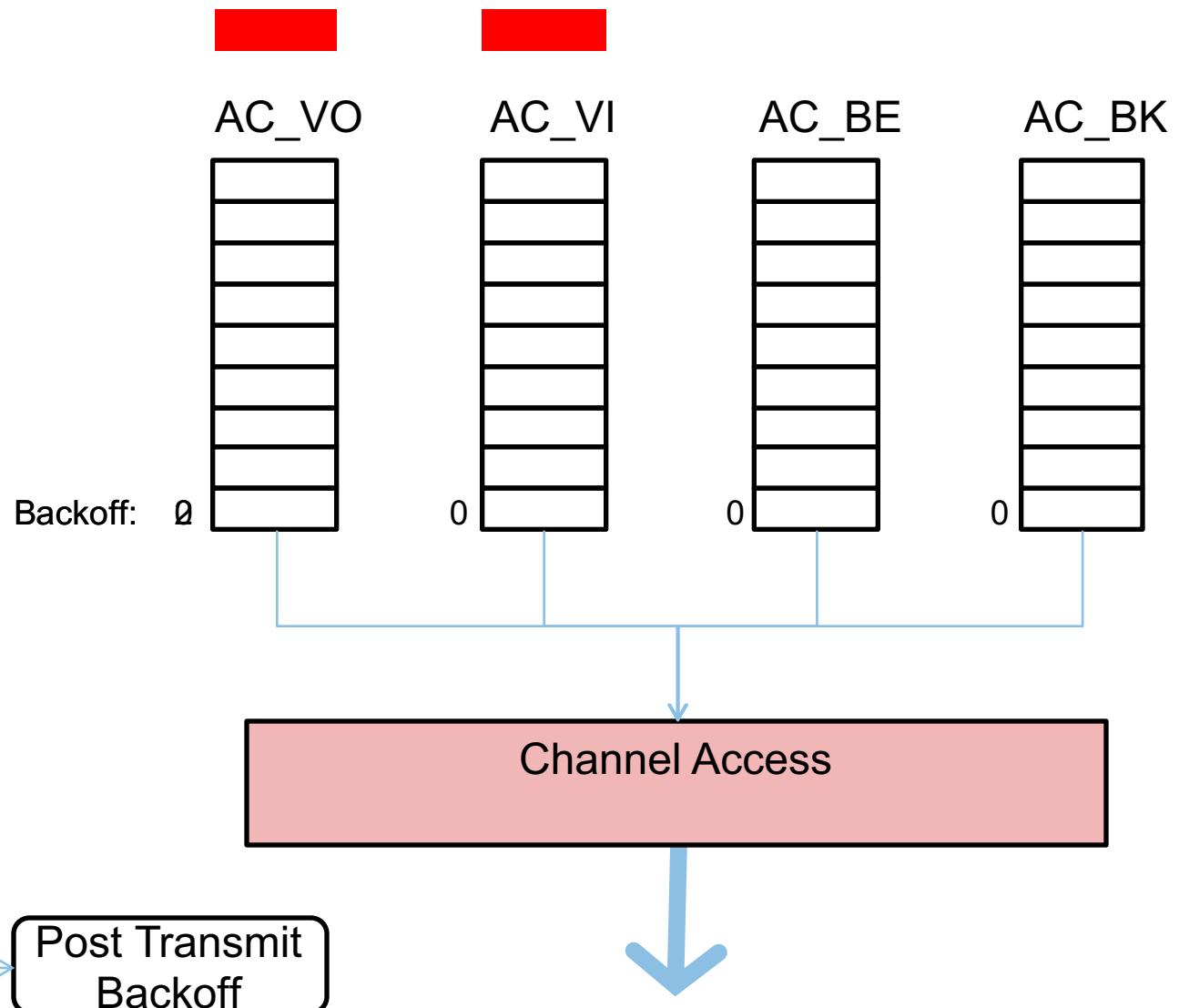
IEEE 802.11p



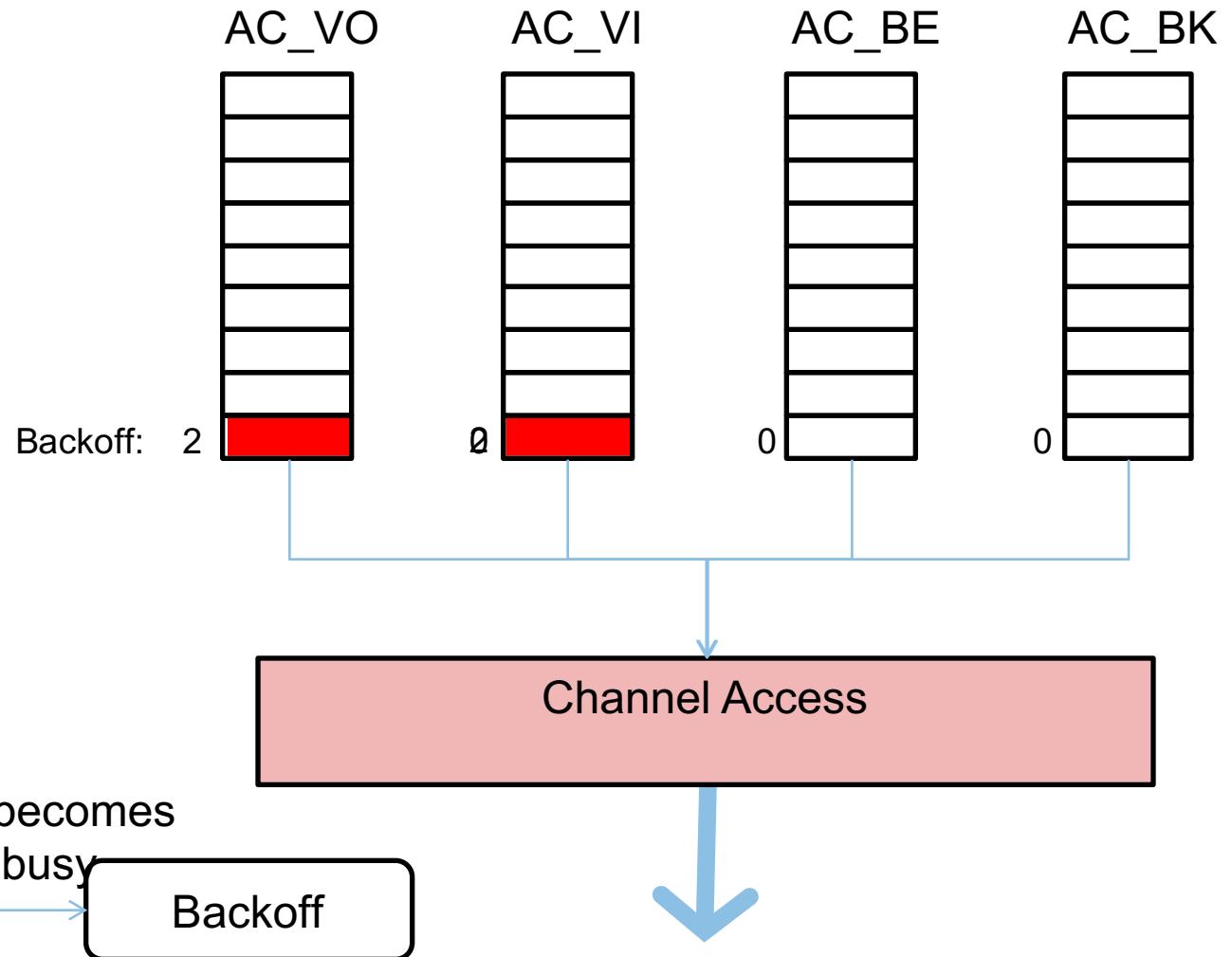
IEEE 802.11p



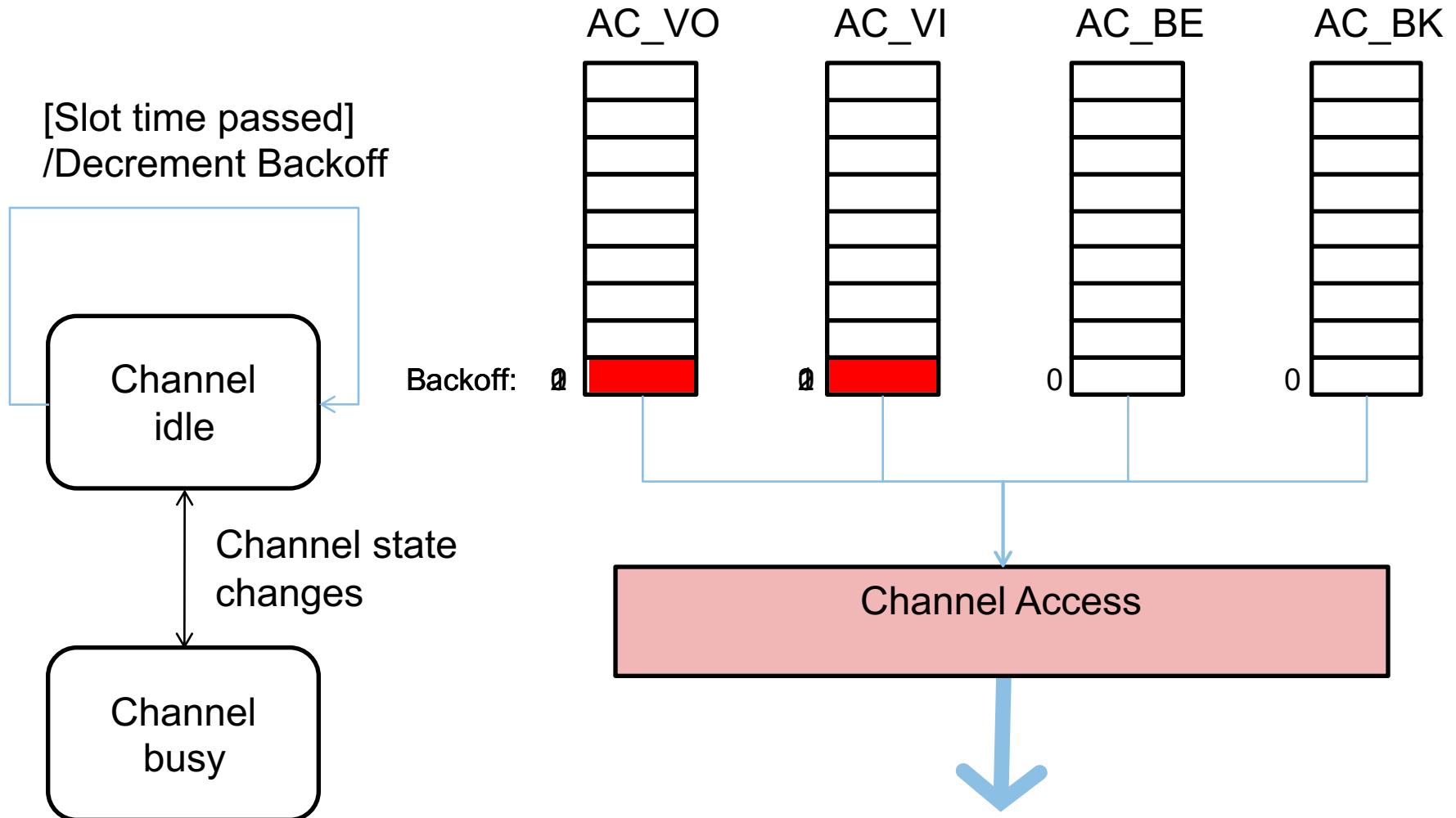
IEEE 802.11p



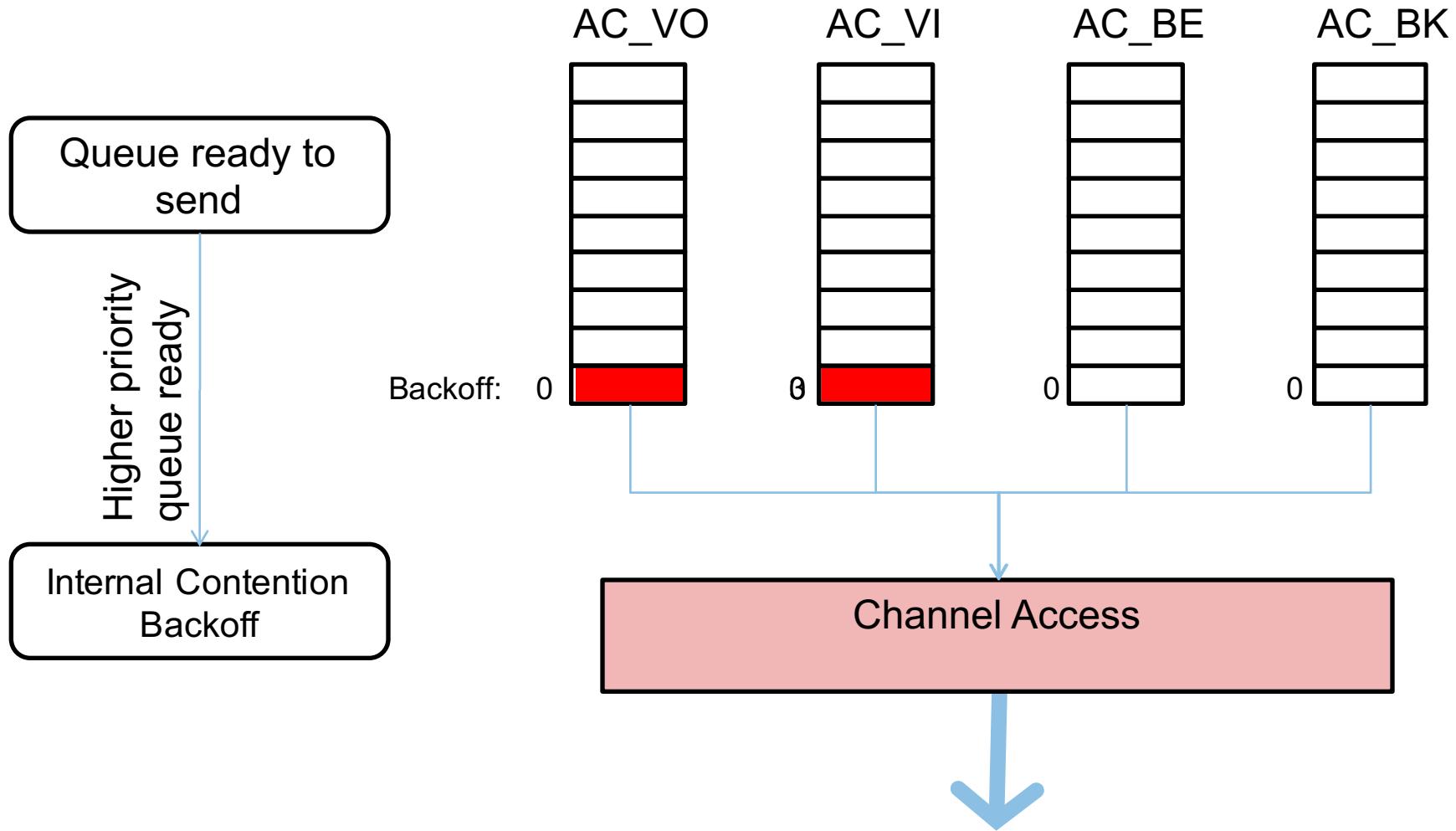
IEEE 802.11p



IEEE 802.11p



IEEE 802.11p

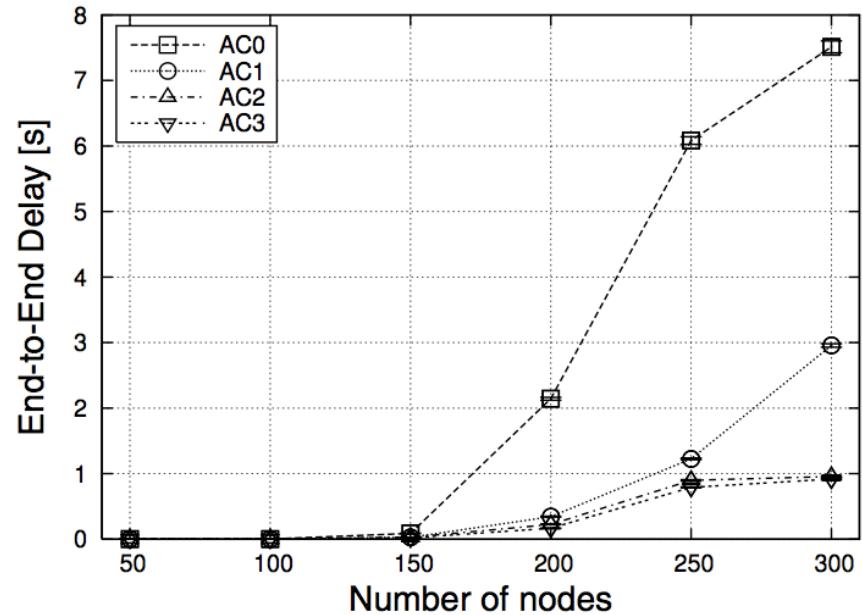


IEEE 802.11p

■ QoS in WAVE

- mean waiting time for channel access, given sample configuration (and TXOP Limit=0 \Rightarrow single packet)

AC	CW _{min}	CW _{max}	AIFS	TXOP	t _w (in μ s)
0	15	1023	9	0	264
1	7	15	6	0	152
2	3	7	3	0	72
3	3	7	2	0	56



[1] Eichler, S., "Performance evaluation of the IEEE 802.11p WAVE communication standard," Proceedings of 66th IEEE Vehicular Technology Conference (VTC2007-Fall), Baltimore, USA, October 2007, pp. 2199-2203

UMTS/LTE vs. 802.11p

- Pros of UMTS/LTE
 - + Easy provision of centralized services
 - + Quick dissemination of information in whole network
 - + Pre-deployed infrastructure
 - + Easy migration to (and integration into) smartphones
- Cons of UMTS/LTE
 - High short range latencies (might be too high for safety)
 - Network needs further upgrades (smaller cells, multicast service)
 - High dependence on network operator
 - High load in core network, even for local communication

UMTS/LTE vs. IEEE 802.11p

- Pros of 802.11p/Ad hoc
 - + Smallest possible latency
 - + Can sustain operation without network operator / provider
 - + Network load highly localized
 - + Better privacy (⇒ later slides)
- Cons of 802.11p/Ad hoc
 - Needs gateway for provision of central services (e.g., RSU)
 - No pre-deployed hardware, and hardware is still expensive
- The solution?
 - hybrid systems:
deploy both technologies to vehicles and road,
decide depending on application and infrastructure availability

Higher Layer Protocols

Higher Layer Standards: CALM

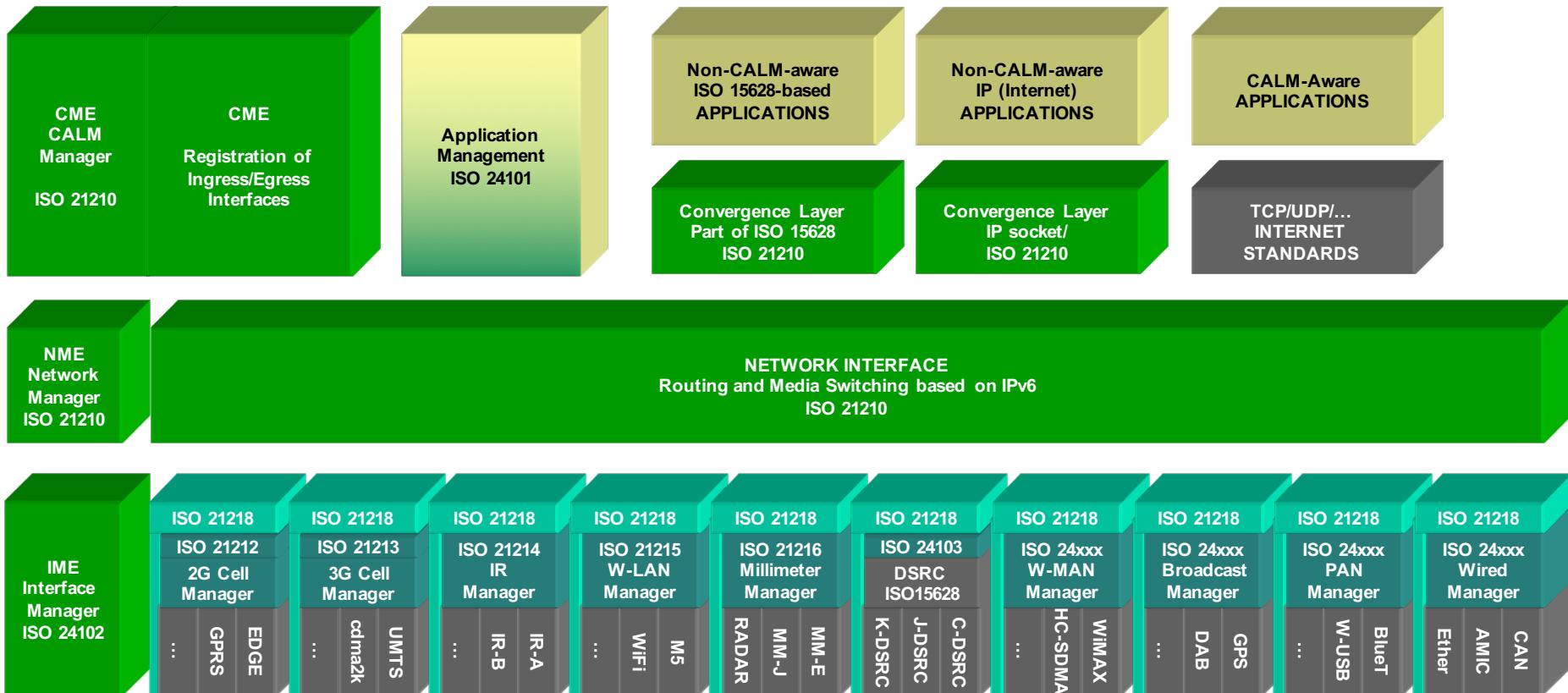
- Mixed-media communication
 - „Communications access for land mobiles“
 - ISO TC204 Working Group 16
 - Initiative to transparently use best possible medium
 - Integrates:
 - GPRS, UMTS, WiMAX
 - Infrared, Millimeter Wave
 - Wi-Fi, WAVE
 - Unidirectional data sources (DAB, GPS, ...)
 - WPANs (BlueT, W-USB, ...)
 - Automotive bus systems (CAN, Ethernet, ...)



[1] ISO 21210, “Intelligent transport systems -- Communications access for land mobiles (CALM) -- IPv6 Networking”

Higher Layer Standards: CALM

■ ISO Standards:



[1] Knut Evensen, "CALM – Architecture and Network", 5th International Conference on ITS Telecommunications (ISTS 2005), Plenary Session, Brest, June 2005

Higher Layer Standards for IEEE 802.11p

- Channel management
 - Dedicated frequency band at 5.9 GHz allocated to WAVE
 - Exclusive for V2V und V2I communication
 - No license cost, but strict rules
 - 1999: FCC reserves 7 channels of 10 MHz (“U.S. DSRC”)

Critical Safety of Life	SCH	SCH	Control Channel (CCH)	SCH	SCH	Hi-Power Public Safety
...						...
ch 172 5.860GHz	ch 174 5.870GHz	ch 176 5.880GHz	ch 178 5.890GHz	ch 180 5.900GHz	ch 182 5.910GHz	ch 184 5.920GHz

- 2 reserved channels, 1+4 channels for applications
- ETSI Europe reserves 5 channels of 10 MHz

SCH	SCH	SCH	SCH	CCH
ch 172 5.860GHz	ch 174 5.870GHz	ch 176 5.880GHz	ch 178 5.890GHz	ch 180 5.900GHz

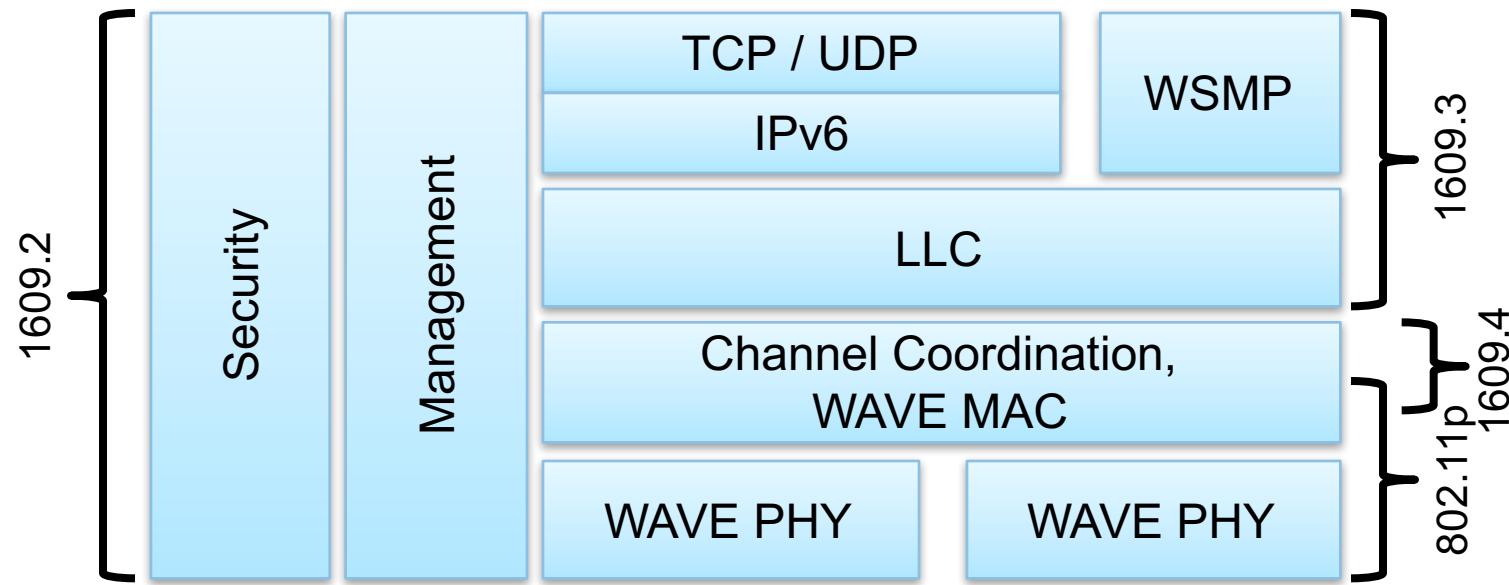
[1] ETSI ES 202 663 V1.1.0 (2010-01) : Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band

Higher Layer Standards for IEEE 802.11p

- Need for higher layer standards
 - Unified message format
 - Unified interfaces to application layer
- U.S.
 - IEEE 1609.*
 - WAVE („Wireless Access in Vehicular Environments“)
- Europe
 - ETSI
 - ITS G5 (“Intelligent Transportation Systems”)

IEEE 1609

- IEEE 1609.* upper layers (building on IEEE 802.11p)
 - IEEE 1609.1: “Operating system”
 - IEEE 1609.2: Security
 - IEEE 1609.3: Network services
 - IEEE 1609.4: Channel mgmt.



[1] Jiang, D. and Delgrossi, L., "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," Proceedings of 67th IEEE Vehicular Technology Conference (VTC2008-Spring), Marina Bay, Singapore, May 2008

[2] Uzcátegui, Roberto A. and Acosta-Marum, Guillermo, "WAVE: A Tutorial," IEEE Communications Magazine, vol. 47 (5), pp. 126-133, May 2009

IEEE 1609

- Channel management
 - WAVE allows for both single radio devices & multi radio devices
 - Dedicated Control Channel (CCH) for mgmt and safety messages
 - ⇒ single radio devices need to periodically listen to CCH
 - Time slots
 - Synchronization envisioned via GPS receiver clock
 - Standard value: 100ms sync interval (with 50ms on CCH)
 - Short guard interval at start of time slot
 - During guard, medium is considered busy (⇒ backoff)

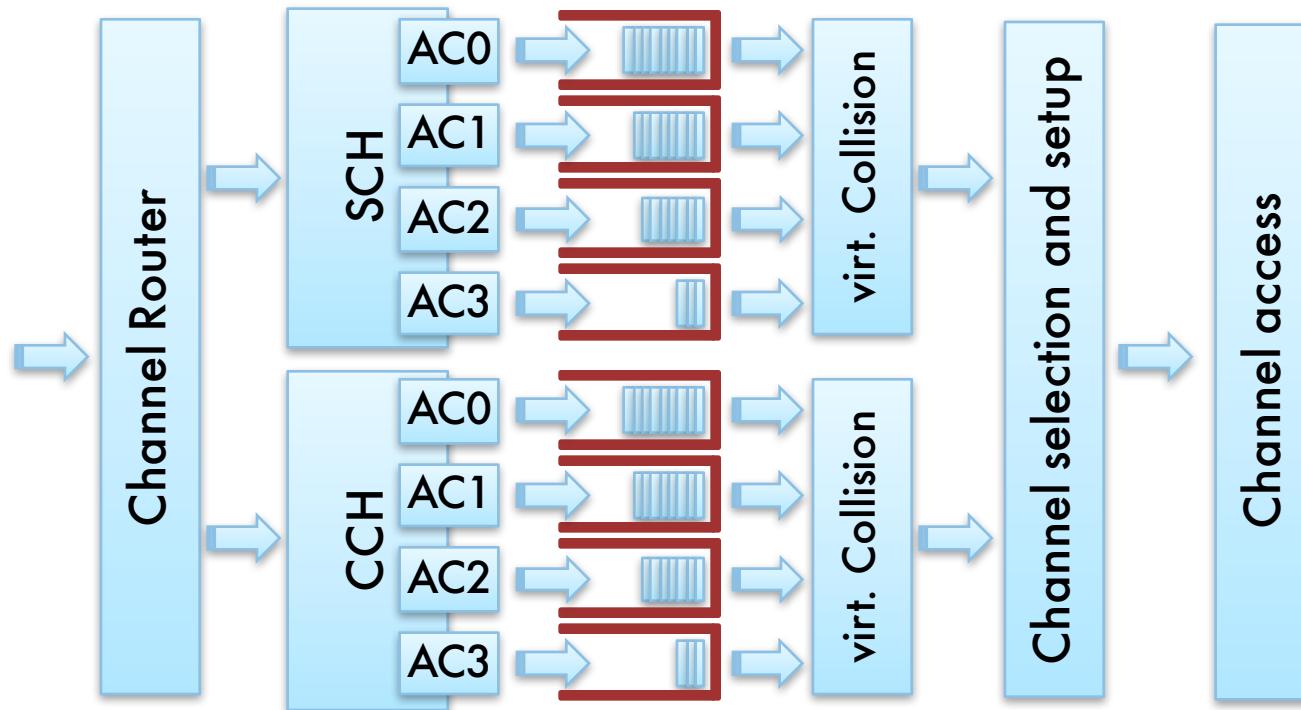


[1] IEEE Vehicular Technology Society, "IEEE 1609.4 (Multi-channel Operation)," IEEE Std, November, 2006

IEEE 1609

Packet transmission

- Sort into AC queue, based on WSMP (or IPv6) EtherType field, destination channel, and user priority
- Switch to desired channel, setup PHY power and data rate
- Start medium access

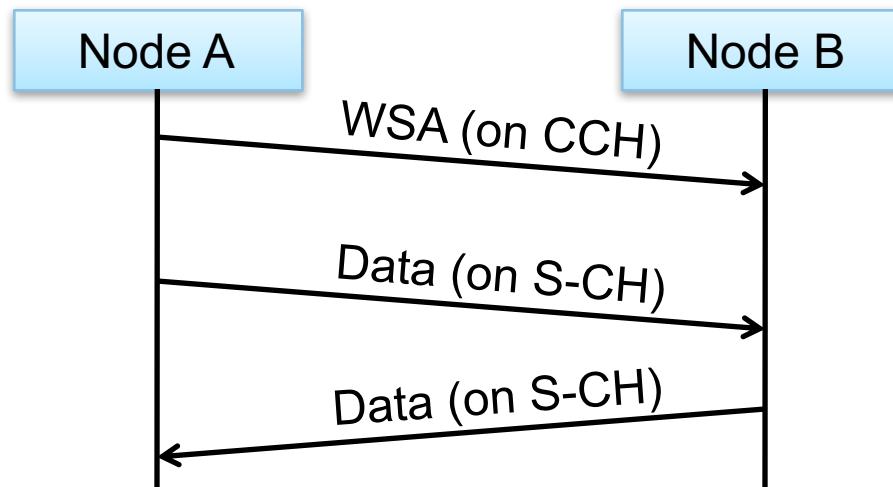


IEEE 1609

- Channel management
 - Control Channel (CCH):
 - Default channel upon initialization
 - WAVE service advertisements (WSA),
WAVE short messages (WSM)
 - Channel parameters take fixed values
 - Service Channel (SCH):
 - Only after joining WAVE BSS
 - WAVE short messages (WSM),
IP data traffic (IPv6)
 - Channel parameters can be changed as needed

IEEE 1609

- WAVE service advertisement (WSA)
 - Broadcast on Control Channel (CCH)
 - Identifies WAVE BSSs on Service Channels (SCHs)
 - Can be sent at arbitrary times, by arbitrary nodes
 - Only possibility to make others aware of data being sent on SCHs, as well as the required channel parameters to decode them



IEEE 1609

- WAVE service advertisement (WSA)
 - WAVE Version (= 0)
 - Provider Service Table (PST)
 - $n \times$ Provider Service Info
 - Provider Service Identifier (PSID, max. 0x7FFF FFFF)
 - Provider Service Context (PSC, max. 31 chars)
 - Application priority (max priority: 63)
 - (opt.: IPv6 address and port, if IP service)
 - (opt.: Source MAC address, if sender \neq data source)
 - Channel number (max. 200)
 - 1.. $n \times$ Channel Info (for each channel used in PST table)
 - Data rate (fixed or minimum value)
 - Transmission power (fixed or maximum value)
 - (opt.: WAVE Routing Announcement)

[1] IEEE Vehicular Technology Society, "IEEE 1609.3 (Networking Services)," IEEE Std, April, 2007

IEEE 1609

- WAVE service advertisement (WSA)
 - Provider Service Identifier (PSID) defined in IEEE Std 1609.3-2007

0x000 0000	system	0x000 000D	private
0x000 0001	automatic-fee-collection	0x000 000E	multi-purpose-payment
0x000 0002	freight-fleet-management	0x000 000F	dsrc-resource-manager
0x000 0003	public-transport	0x000 0010	after-theft-systems
0x000 0004	traffic-traveler-information	0x000 0011	cruise-assist-highway-system
0x000 0005	traffic-control	0x000 0012	multi-purpose-information system
0x000 0006	parking-management	0x000 0013	public-safety
0x000 0007	geographic-road-database	0x000 0014	vehicle-safety
0x000 0008	medium-range-preinformation	0x000 0015	general-purpose-internet-access
0x000 0009	man-machine-interface	0x000 0016	onboard diagnostics
0x000 000A	intersystem-interface	0x000 0017	security manager
0x000 000B	automatic-vehicle-identification	0x000 0018	signed WSA
0x000 000C	emergency-warning	0x000 0019	ACI

IEEE 1609

- WAVE Short Message (WSM)
 - Header (11 Byte)
 - Version (= 0)
 - Content type: plain, signed, encrypted
 - Channel number (max. 200)
 - Data rate
 - Transmission power
 - Provider Service Identifier (Service type, max. 0x7FFF FFFF)
 - Length (max. typ. 1400 Bytes)
 - Payload

IEEE 1609

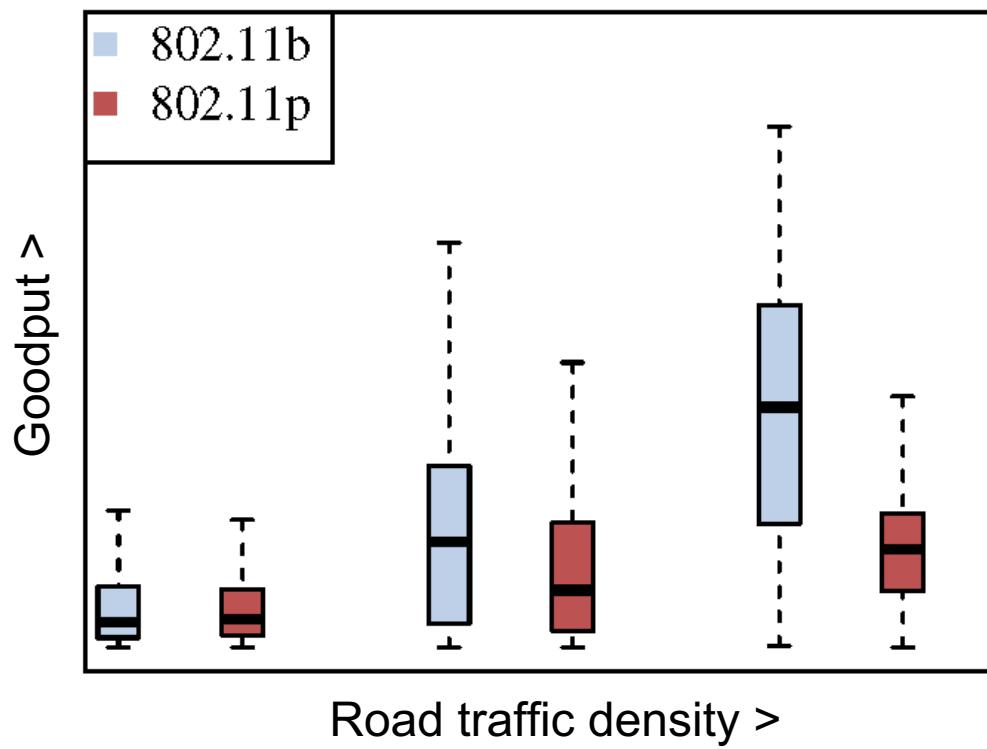
- IP traffic (UDP/IPv6 or TCP/IPv6)
 - Header (40+n Byte)
 - Version
 - Traffic Class
 - Flow Label
 - Length
 - Next Header
 - Hop Limit
 - Source address, destination address
 - (opt.: Extension Headers)
 - Payload
- No IPv6-Neighbor-Discovery (High overhead)
- All OBUs listen to host multicast address,
all RSUs listen to router multicast address

IEEE 1609

- Channel quality monitoring
 - Nodes store received WSAs, know SCH occupancy
 - Received Channel Power Indicator (RCPI) polling
 - Nodes can send RCPI requests
 - Receiver answers with Received Signal Strength (RSS) of packet
 - Transmit Power Control (TPC)
 - Nodes can send TPC requests
 - Receiver answers with current transmission power and LQI
 - Dynamic Frequency Selection (DFS)
 - Nodes monitor transmissions on channel (actively and passively)
 - If higher priority third party use (e.g., RADAR) is detected, nodes cease transmitting

Drawbacks of Channel Switching

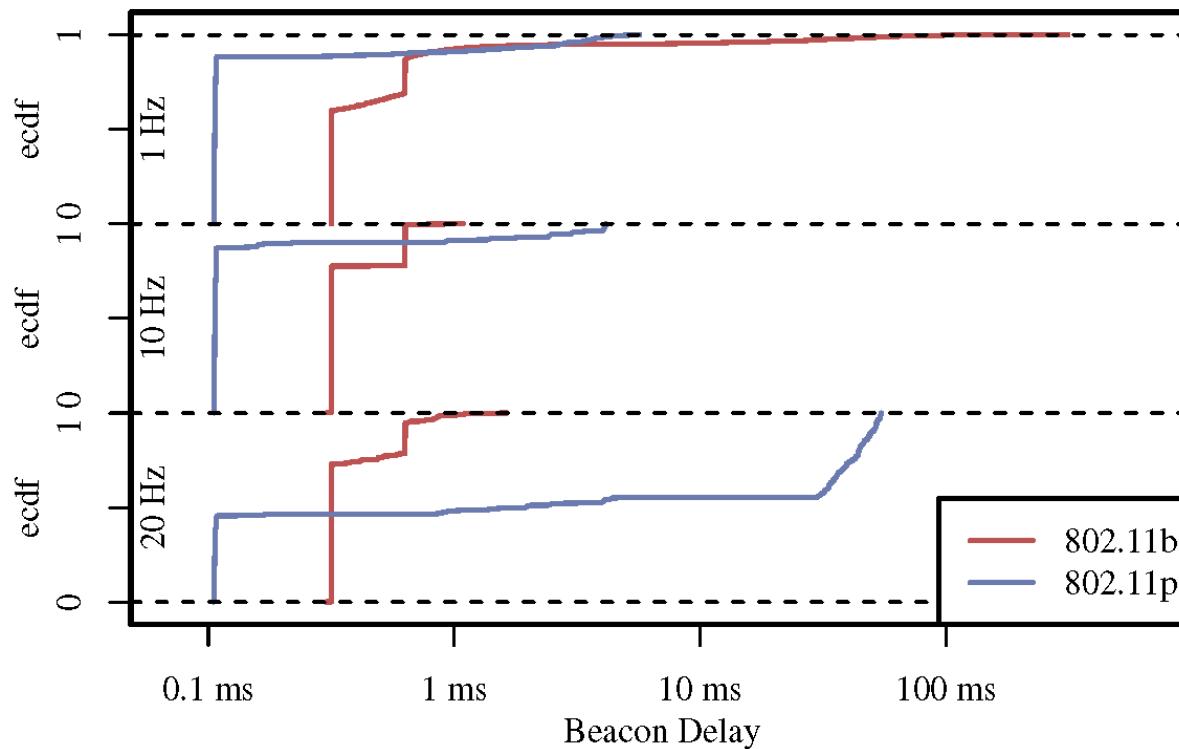
- 1) Goodput
 - User data must only be sent on SCH, i.e., during SCH interval
⇒ goodput cut in half



[1] David Eckhoff, Christoph Sommer and Falko Dressler, "On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation," Proceedings of 75th IEEE Vehicular Technology Conference (VTC2012-Spring), Yokohama, Japan, May 2012.

Drawbacks of Channel Switching

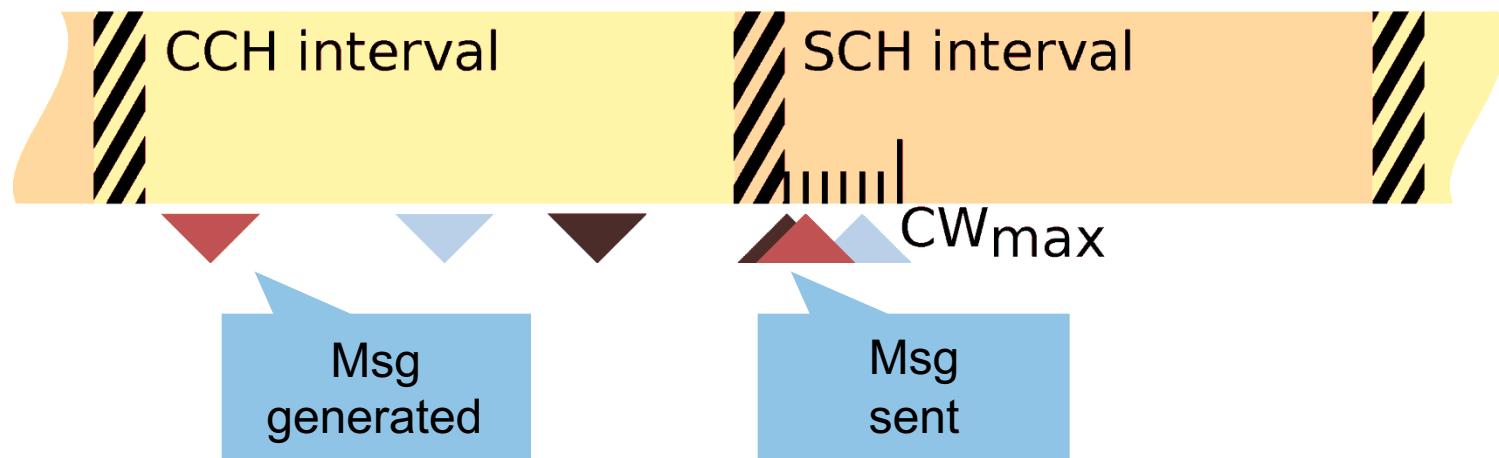
- 2) Latency
 - User data generated during CCH interval is delayed until SCH intv.



[1] David Eckhoff, Christoph Sommer and Falko Dressler, "On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation," Proceedings of 75th IEEE Vehicular Technology Conference (VTC2012-Spring), Yokohama, Japan, May 2012.

Drawbacks of Channel Switching

- 3) Collisions
 - Delay of data to next start of SCH interval
 - ⇒ increased frequency of channel accesses directly after switch
 - ⇒ increased collisions, packet loss



[1] David Eckhoff, Christoph Sommer and Falko Dressler, "On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation," Proceedings of 75th IEEE Vehicular Technology Conference (VTC2012-Spring), Yokohama, Japan, May 2012.

IEEE 1609

- Security in WAVE
 - Nature of WAVE messages mandates trust between nodes
 - Ex: Green wave for emergency vehicles
 - Security is built into WAVE (IEEE 1609.2)
 - WAVE can transparently sign, verify, encrypt/decrypt messages when sending and receiving
 - Ex: WSA → Secure WSA
 - Authorization of messages needed
 - By role: CA, CRL-Signer, RSU, Public Safety OBU (PSOBU), OBU
 - By application class (PSID) and/or instance (PSC)
 - By application priority
 - By location
 - By time

[1] IEEE Vehicular Technology Society, "IEEE 1609.2 (Security Services)," IEEE Std, July, 2006

IEEE 1609

- Certificates
 - Encryption is useless without authentication
 - Alice \Leftrightarrow Eve \Leftrightarrow Bob
 - Eve can pretend to be Alice,
replace K^+_A with own key K^+_E
 - Solution: use Trusted Third Party (TTP) and certificates
 - TTP signs (Name, Key) tuple, vouches for validity and authorization:
“Alice has Public Key K^+_A , may participate as OBU until 2019”
 - not: “~~whoever sends this packet is Alice~~”
 - not: “~~whoever sends this packet has Public Key K^+_A~~ ”
 - Send K^+_A together with certificate vouching for tuple

IEEE 1609

■ Implementation in WAVE

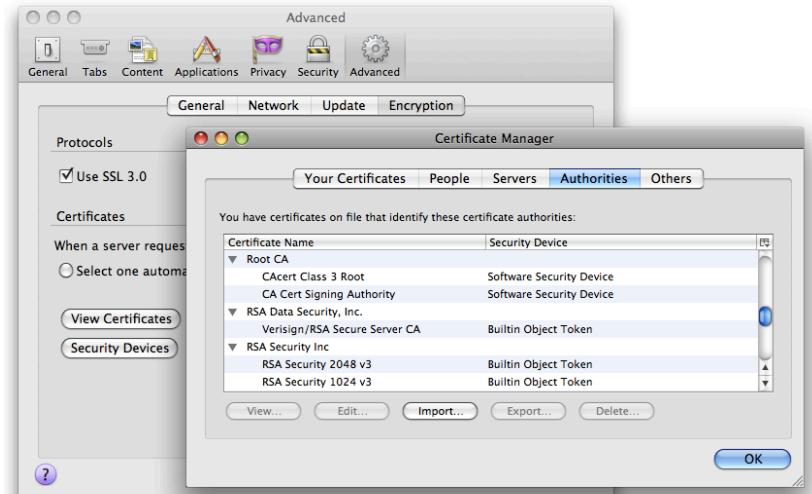
■ Certificate signature chains

- Root certificate \Rightarrow certificate \Rightarrow certificate \Rightarrow payload
- Root certificates pre-installed with system
- Other certificates cannot be assumed to be present

■ Nodes must download certificates along with signed message

- Include chain of certificates
- ...or SHA-256 of first certificate in chain

(if receiver can
be assumed to
have all required
certificates)



IEEE 1609

- Implementation in WAVE
 - X.509 formats too large \Rightarrow new WAVE certificate format
 - Version
 - Certificate
 - Role (RSU, PSOBU, OBU, ...)
 - Identity (dependent on role)
 - Restrictions (by application class, priority, location, ...)
 - Expiration date
 - Responsible CRL
 - Public Keys
 - Signature
 - New: Restriction by location
 - e.g.: none, inherited from CA, circle, polygon, set of rectangles
 - Public Key algorithms (motivated by key size):
ECDSA (NIST p224), ECDSA (NIST p256), ECIES (NIST p256), ...

IEEE 1609

■ Complete packet format of a WSM:

Length	Field		
1	WSM version		
1	Security Type = signed(1)		
1	Channel Number		
1	Data Rate		
1	TxPwr_Level		
4	PSID		
1	PSC Field Length		
7	PSC		
2	WSM Length		
1	WSM Data	signer	type = certificate certificate
125		unsigned_wsm	message flags application_data
2			transmission_time
32			latitude
8		transmission_location	longitude
4			elevation_and_confidence
4			r
3		signature	s
28			ecdsa_signature
28			

Ex: Signed WSM of an OBU,
Certificate issuer is known

⇒ next slide

IEEE 1609

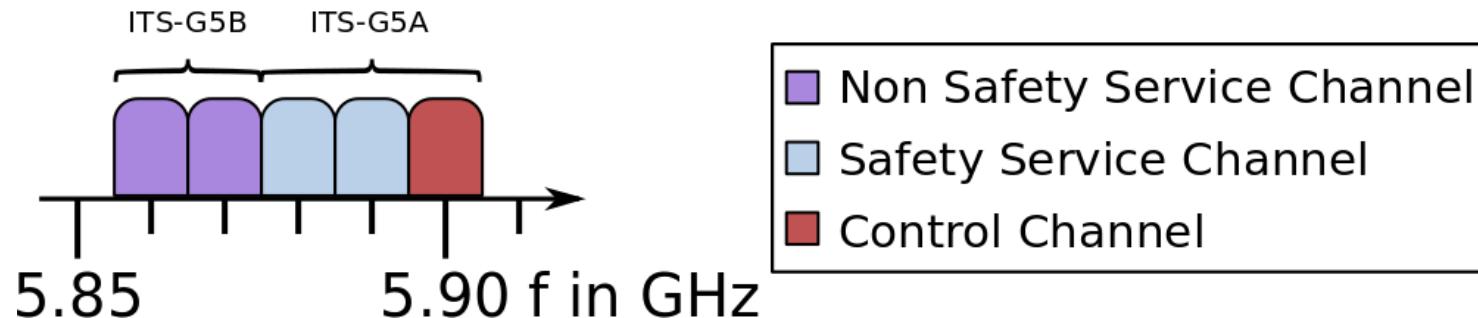
- Complete packet format of a WSM (certificate part):

Length	Field		
1	certificate_version = 1		
1	unsigned_certificate	subject_type = obu_identified	
8		signer_id	
1		scope	subject_name length
8			subject_name
2			applications
1			length of applications field
4			type = from_issuer
4		expiration	
4		crl_series	
1		public_key	length of public key field
1			algorithm = ecdsa nistp224..
29			public_key
32	signature	ecdsa_signature	r
32			s

ETSI ITS G5

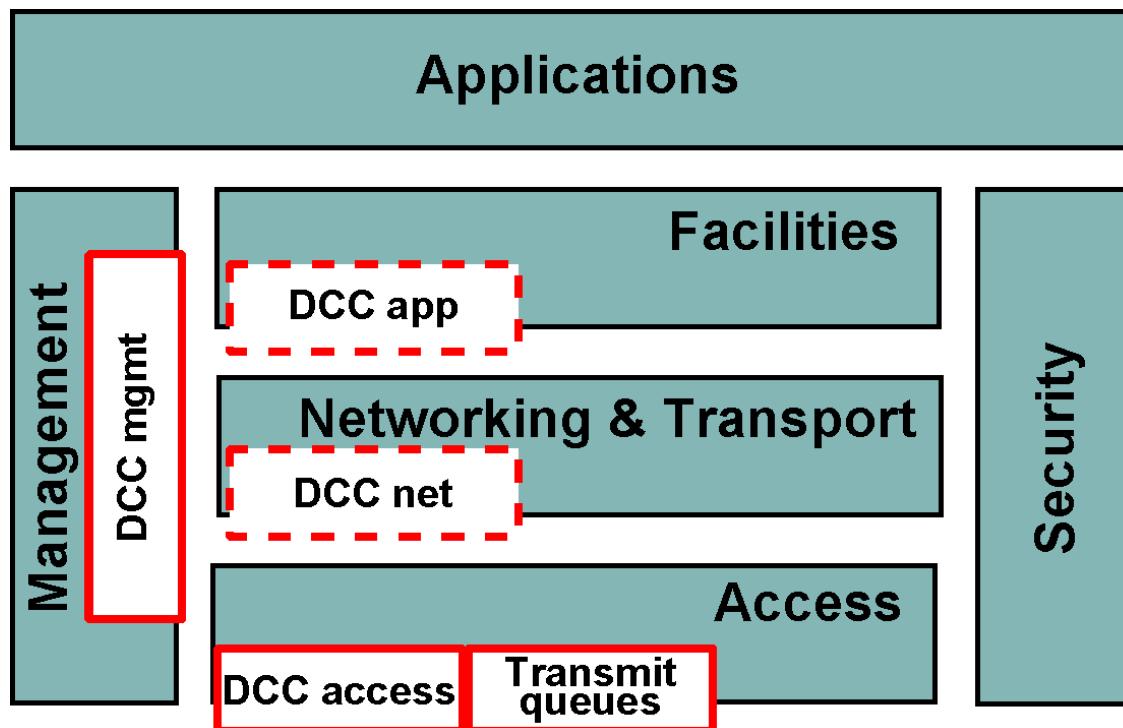
■ Motivation

- European standardization effort based on IEEE 802.11p
- Standardization to include lessons learned from WAVE
- Different instrumentation of lower layers
- Different upper layer protocols
- Different channel assignment
 - ITS-G5A (safety)
 - IST-G5B (non safety)



ETSI ITS G5

- Protocol stack
 - PHY and MAC based on IEEE 802.11p
 - Most prominent change:
cross layer Decentralized Congestion Control (DCC)



ETSI ITS G5

- Channel management
 - Multi radio, multi antenna system
 - No alternating access
 - ⇒ Circumvents problems with synchronization
 - ⇒ No reduction in goodput
 - Direct result of experiences with WAVE
 - One radio tuned to CCH
 - Service Announcement Message (SAM)
 - Periodic:
Cooperative Awareness Messages (CAM)
 - Event based:
Decentralized Environment Notification Message (DENM)
 - Addl. radio tuned to SCH
 - User data

ETSI ITS G5

- Medium access
 - Separate EDCA systems
 - Different default parameters:

Parameter	AC_BK	AC_BE	AC_VI	AC_VO
CW _{min}	CW _{min}	(CW _{min} +1)/2-1	(CW _{min} +1)/4-1	(CW _{min} +1)/4-1
CW _{max}	CW _{max}	CW _{max}	(CW _{min} +1)/2-1	(CW _{min} +1)/2-1
AIFS _n	9	6	3	2

- *Contention Window* – less distance to lower priority queues
 - ⇒ less starvation of lower priority queues

ETSI ITS G5

- Cooperative Awareness Message
 - Periodic (up to 10Hz) safety message
 - Information on state of surrounding vehicles:
 - Speed, location, ...
 - Message age highly relevant for safety
 - Need mechanisms to discard old messages
 - Safety applications rely on CAMs:
 - Tail end of jam
 - Rear end collision
 - Intersection assistance...
 - Sent on CCH
 - Generated every 100ms .. 1s, but only if
 $\Delta\text{angle} (>4^\circ)$, $\Delta\text{position} (>5\text{m})$, $\Delta\text{speed} (>1\text{m/s})$

ETSI ITS G5

■ CAM format

Length[byte]	Field	
1	messageId (0=CAM, 1=DENM)	
8	generationTime	
4	StationId	
1	StationCharacteristics	mobileITSStation
1		privateITSStation
1		physicalRelevantITSStation
8+8+4	ReferencePosition	Longitude/Longitude/Elevation
4		Heading
32+4		Streetname/RoadSegment ID
1		Position/Heading Confidence
1	CamParameters	vehicleType
2+2		Length/Width
4		Speed
2		Acceleration
1		AccelerationControl (break, throttle, ACC)...
1		exteriorLights
1		Occupancy
1+1		crashStatus/dangerousGoods

ETSI ITS G5

- Decentralized Environmental Notification Message (DENM)
 - Event triggered (e.g., by vehicle sensors)
 - Hard braking
 - Accident
 - Tail end of jam
 - Construction work
 - Collision imminent
 - Low visibility, high wind, icy road, ...
 - Messages have (tight) local scope, relay based on
 - Area (defined by circle/ellipse/rectangle)
 - Road topology
 - Driving direction

ETSI ITS G5

■ DENM format (excerpt)

Length[byte]	Field	
1	messageId (0=CAM, 1=DENM)	
6	generationTime	
4	Originator ID	Who sent this?
2	Sequence Number	
1	Data Version	Is this an update on a situation?
6	Management	Expiry Time
1		Is this still valid?
1		Frequency
1		When can I expect an update?
1		Reliability
1		Should I trust a single notification?
1		Does this cancel an earlier notification?
1	Situation	CauseCode
1		SubCauseCode
1		Severity
4	LocationContainer	Situation_Latitude
4		Situation_Longitude
2		Situation_Altitude
4		Accuracy
N-40		Relevance Area

ETSI ITS G5

- Service Announcement
 - Message on Control Channel to advertise services offered on Service Channels
 - Channel number
 - Type of service
 - ...
 - Similar to WAVE Service Announcement (WSA)
 - Receiver can tune (its second radio) to advertised channel

ETSI ITS G5

- Security and privacy
 - No published specification (yet)
 - Kerberos or WAVE-like PKI
 - Restrict participation to authorized vehicles
 - Sign messages
 - Limit V2I and I2V traffic where possible
 - Use pseudonyms to protect privacy
 - Use base identity (in permanent storage) to authenticate with infrastructure
 - Infrastructure generates pseudonym for vehicle

Main Takeaways

- Broadcast Media
 - TMC, TPEG
- UMTS
 - Channels, Pros / Cons
- DSRC/WAVE lower layers
 - 802.11p vs. old 802.11: commonalities and differences
 - HCF (EDCA QoS)
- IEEE 1609.* upper layers
 - Channel management
 - Security / Certificates
- ETSI ITS G5
 - Channel management
 - Message types
 - Commonalities and differences wrt. IEEE 1609.*