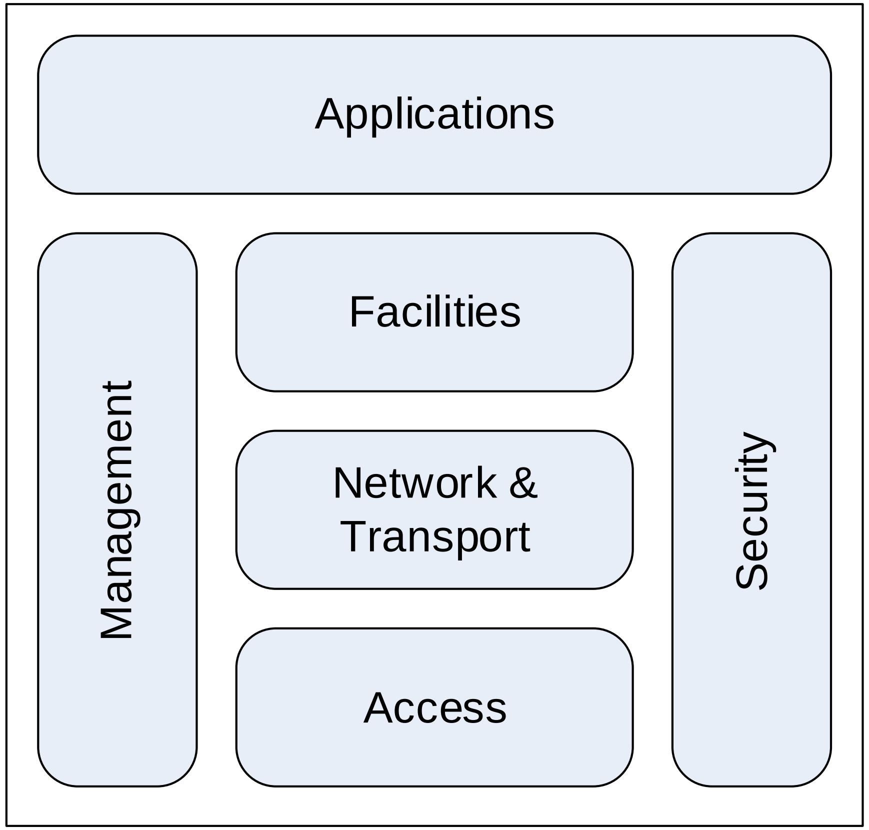
C-ITS – Key Enabling Technologies

SAMS & ITS Norway webinar 2021-01-12

Access technologies

Ola Martin Lykkja, Q-Free Norway

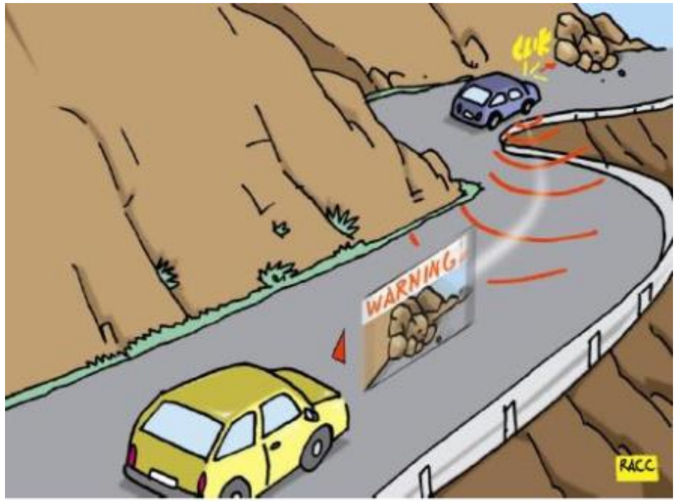
C-ITS Communication Architecture

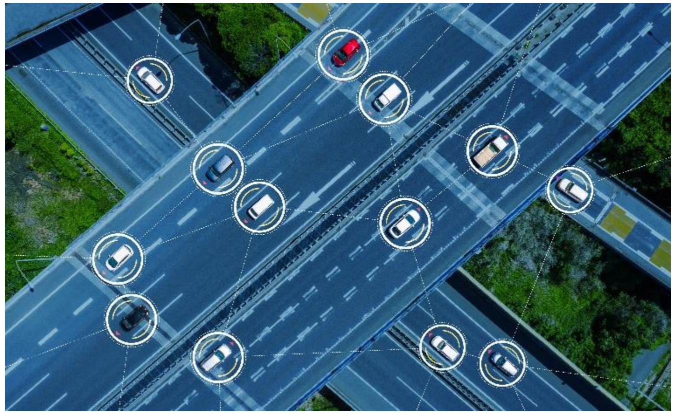


- The **Access Layer** is the lowest layers of the OSI model.
  - Communication inside the ITS station
  - External communication to other ITS stations
- Many media types and communication technologies
  - **ITS G5 / IEEE WAVE – Wi-Fi in 5.9 GHz band**
  - **Cellular V2X – LTE (sidelink/PC5) in 5.9 GHz band**
  - **Mobile networks - PLMNs (GSM, WCDMA, LTE, 5G)**
  - Infrared
  - Satellite communication
  - Ethernet
  - Fiber optic networks
  - LoRa
  - WiMax

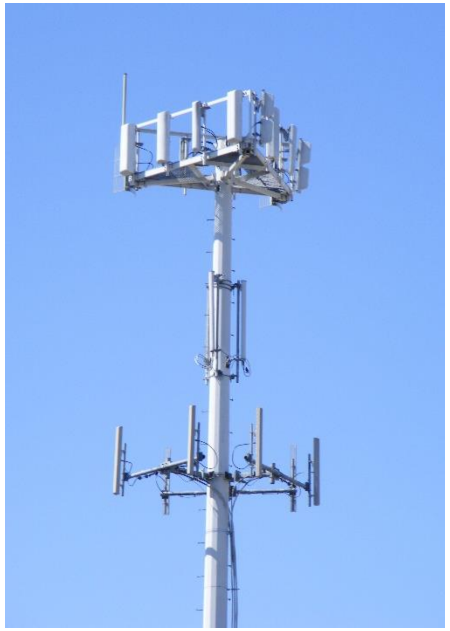
ITS G5 and C-V2X

- Medium range communication: 500 – 1000 meters
- Peer to Peer: No network infrastructure required
- V2X: Localized communications between vehicles and roadside
- Detailed standards from ETSI, CEN, ISO and IEEE
- Distinct features:
  - Communication is local and related to local events
  - Local authorities manage local information
  - No central single point of failure
  - Scales well
  - Broadcast technology
  - Challenging to sniff and store everything
  - Unlicensed frequency band at 5.9 GHz
- Disadvantage
  - If there are no peers nearby, there is no one to talk to.



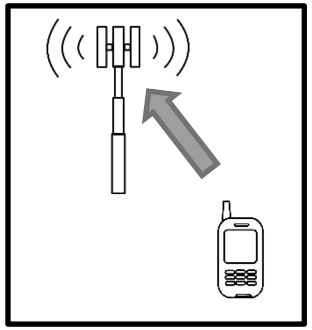


Mobile networks – 2G - 3G - 4G - 5G - 6G

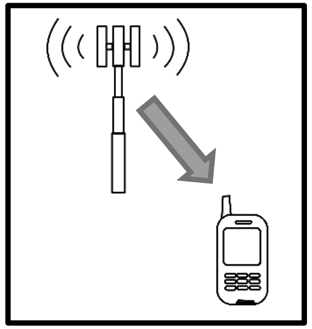


- The offer internet connectivity to C-ITS stations
  - TCP/IP, HTTP, WebServices, MQTT, AMQP, WebSockets, etc.
- Not a broadcast technology, but server-to-peer messages
  - 3G and LTE has broadcast features standardized, but they never become a hit.
- Coverage and bandwidth provided by the Telecom companies
  - Where it is economically feasible
  - Large bandwidth requires smaller cells and more infrastructure
- Distribution challenge
  - Communication is no longer local and other means must be used to ensure that local messages reach relevant users.
  - Facebook and twitter and google gives me local information, so this can’t be hard
    - If you care about privacy, it gets a lot harder
  - Typically a publish-subscribe architecture is used: I am in Oslo downtown, please give me relevant information
- For road-operators it is infrastructure-less, the infrastructure is “free”, payed by the users (drivers).

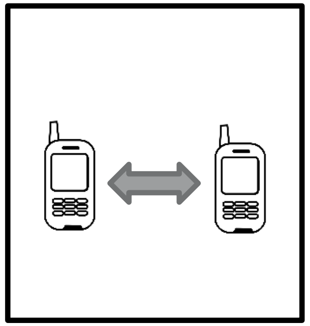
Cellular V2X: It is LTE! – It is sidelink!



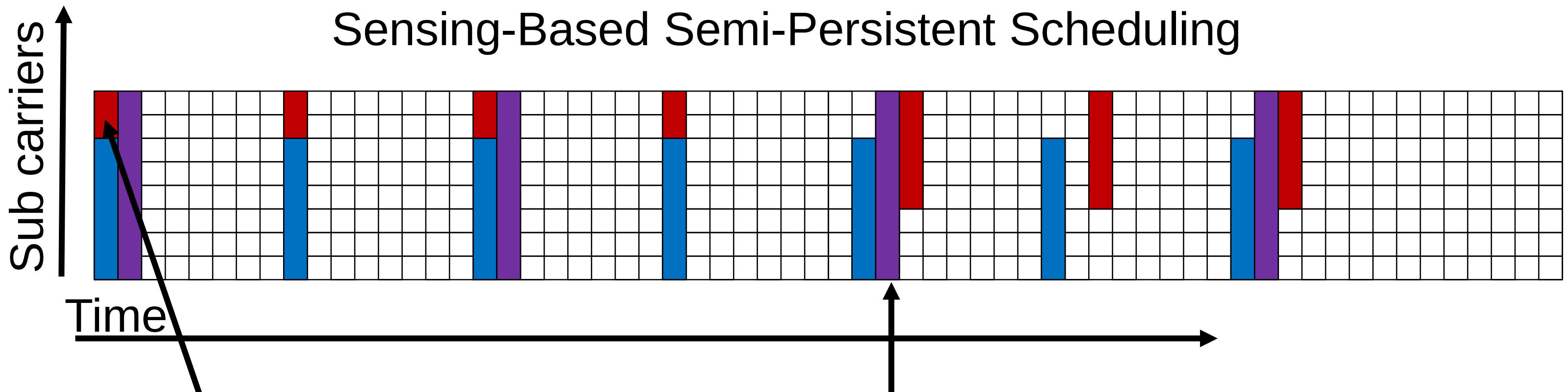
Uplink
Send data to the network



Downlink
Receive data from the network



Sidelink
No network – Phone to phone
PC5 interface is used
Mode 4.



Red ITS station has negotiated with others to send small frames at high rate. Later red wants to send a large frame

Purple ITS station has negotiated with others to send large frames at low rate.

For this to work a global time-base (UTC) synchronized to microsecond level is needed for time and phase. GNSS is used.

Comparison between ITS G5 and Cellular-V2X

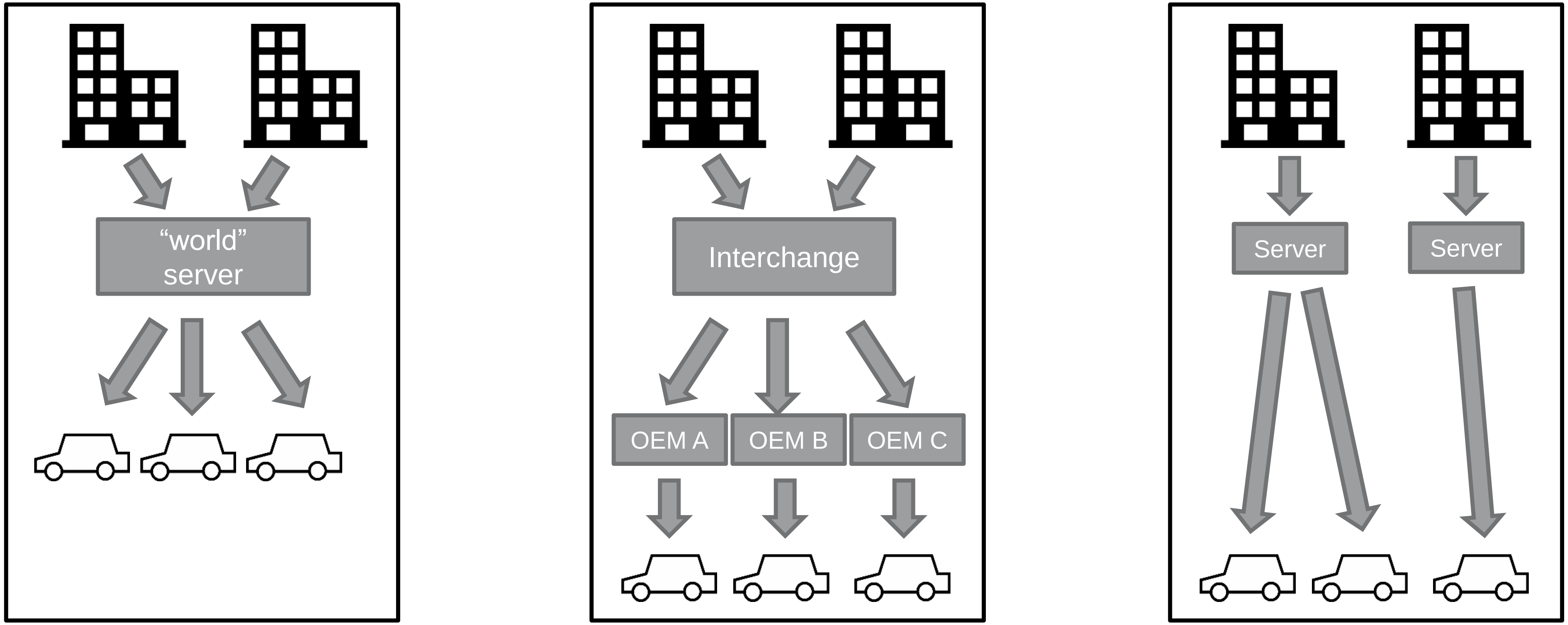
ITS G5 / IEEE 802.11p (or OCB mode)

- Based on Wi-Fi technology
- Carrier-sense multiple access with collision avoidance (CSMA/CA)
- Cannot use 100% of the bandwidth
- No concept of time.
- No pre-allocation of talk time
- Mixing of large of small frames
- Old technology, patent free, many chipsets
- Polite guests at a cocktail party

Cellular-V2X

- Based on LTE technology
- Time-slot based
- Can in theory use all bandwidth
- In “normal” LTE, the base station (eNodeB) coordinates time. In C-V2X, each peer must have precise time, typically from a GNSS receiver.
- Talk time and time slots are allocated using *Sensing-Based Semi-Persistent Scheduling.*
- Assumes that all frames has equal size
- New technology, few chipsets
- Dinner guests at a wedding with a strict toastmaster.

Distribution architectures for C-ITS over mobile networks



Many architectures are possible!
Open vs proprietary communication, proof or origin of events, scalability, privacy, financial models.

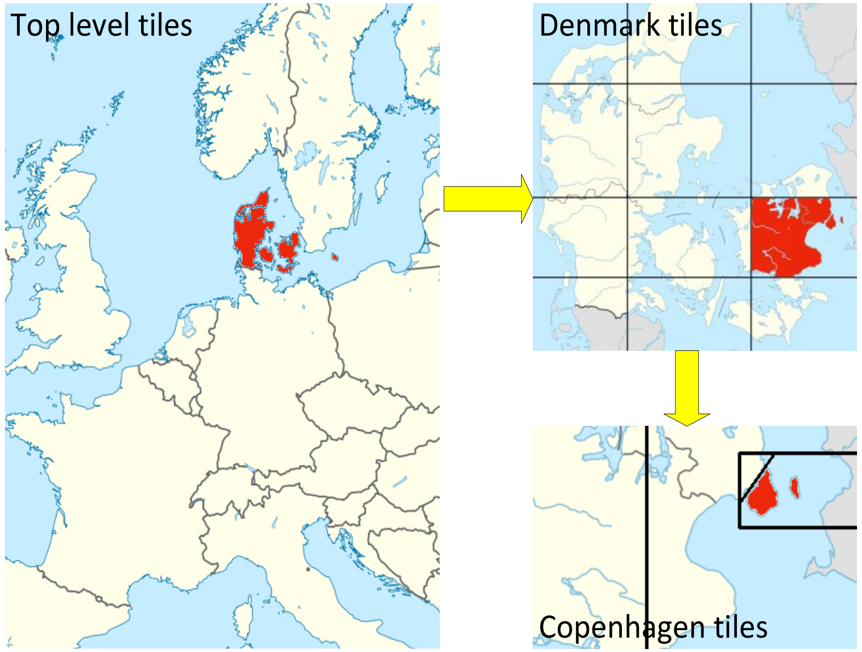
Privacy issues

- ITS G5 message dissemination makes it hard to do large scale data collection.
  - There is no central server to wire-tap.
  - There is no user/account registry.
  - There is no passwords.
- TCP/IP based architectures *may* be designed with the same principles
- It is very easy, for many reasons to fall in the ‘I just want to utilize the rich data’ trap.
- In practice, it is hard (impossible) to anonymize travel location data (See NRK articles about mobile apps).
- Mandatory use of mobile phone network (LTE) will create records in the mobile core network, in addition to the server logs.
- One possible solution is to divide the world (country) into tiles, where a vehicle ITS station can subscribe anonymously, without any user name or registration to traffic information based on coarse location.

Tile concept

- Vehicle ITS station subscribes to messages relevant for a tile.
- One tile server may handle one infrastructure operator.
- Tiles may be small or large depending on traffic and infrastructure density
- Hierarchical tile structure
- Tile border may follow administrative borders
- Tiles may overlap
- One tile may have zero or many messages
- Anonymous users may access the tile server, it has only public information.

- Most messages correspond to ITS messages
(DENM, IVI, MAP), some is meta-data (tile definitions)



Security issues

- In a V2X scenario, the sender signs the message with his private key.
  - The signature protects the payload (e.g. CAM, DENM, IVI) message and the GeoNetworking header.
  - The receiver can verify the signature and detect if the payload (and network header) is genuine.
  - This is unambiguously described in ETSI and IEEE standards.
  - Role-based security
  - Security domain is tightly governed by EC/JRC with the European C-ITS Security Policy.
- In a scenario where the message is sent over TCP/IP, this is not clear.
  - Typically HTTPS/TLS is used to protect the communication channel
  - X.509 certificates are used, they are not in the EC C-ITS trust domain.
- Recent developments!
  - TLS 1.3 is updated with RFC 8902 and together with ISO 21177 it allows C-ITS certificates in TLS.
  - This brings HTTPS/TLS into the same trust domain as C-ITS
- Protocol conversion (or gateway) challenges
  - GeoNetworking signing must be opened and rewritten to be forwarded over internet (and vice versa).
  - No end-to-end signatures

Summary

	ITS G5	C-V2X	Mobile networks
Bandwidth	Limited	Limited	Unlimited in urban, Limited in rural
Latency	Low	Low	Medium (low in 5G)
Technology maturity	Mature	Infancy	Mature
Standardized all layers	Yes	Yes	No
Security/Signatures	Well-defined	Well-defined	Not well-defined
RSU deployment cost	Road operators	Road operators	Telecom users
Privacy	Good	Good	Service provider decide
Tunnel operation	Yes	No (GNSS needed)	Yes
Range	500 m	500 m	Needs mobile coverage
RF band allocation	Unlicensed at 5.9	Unlicensed at 5.9	Licensed, 450-26000 MHz
SIM card / mobile subscription	No	No	Yes
Trust / certificate standards	C-ITS	C-ITS	X.509 (but soon C-ITS)

Ola Martin Lykkja, Q-Free, Oslo Norway

ola.Lykkja@q-free.com

HEADQUARTERS
Q-FREE ASA

Strindfjordvegen 1
7053 Ranheim
Norway

Postal Address
Pob 3974 Leangen
7443 Trondheim
Norway

Tel.:+47 73 82 65 00
Fax:+47 73 82 65 01

info@q-free.com
www.q-free.com

twitter.com/qfreeasa
linkedin.com/qfreeasa

Bank: Nordea Bank Abp, filial i Norge
ACC. No.: 6402.05.33518

Register of business
enterprises NO 935 487 242