Vehicular networks

→ VANET (Vehicular Ad-hoc Networks)

Provide safety, efficiency, traffic + road conditions, road signal alarm and local info.

OBU → communication, routing, application

RSU → processing and wireless comm modules

- ✓ Warnings
- ✓ Safety
- ✓ Efficiency
- ✓ Traffic + road conditions
- ✓ Self driving

→ Awareness and warning information

CAM (Cooperative awareness messages)

- periodic
- contain info about position and speed, ...

DENM (Decentralized Environmental Notification Msg)

- asynchronous
- info about event and station that generated the message.

Messages

→ CAM

Generated by OBU on RSU (info will change)

[delta time

[Basic container : id, position]

[High frequency container : fast-changing vehicle data (location, heading, speed)]

[low frequency container : static or low-changing data (pedals, lights, ...)]

CAM every 1 - 10 Hz.

HF container in every message, LF at max 5 Hz.

Time between CAM generation and sending < 50 ms.

→ DENM

Async messages create and maintain awareness about road event, include type, position, validity, history, ...

Type, detection time, position, type of the related station and codes identifying the type must be present.

Stationary vehicle containers.

They have a validity period to be considered up-to-date.

Terminal DENMs signal end of event.

→ VAM (vulnerable road user awareness msg)

Periodic messages to maintain awareness of the VRU and support the risk assessment.

Contain time, position, speed, heading, yaw, accel, orientation, lane, dimensions and VRU type.
(pedestrian, bycicle, animal, motorcycle)

The types can be even more distinguished. For

exaple : child pedestrian and wheelchair user have different dynamics and can help safety services.

→ CPM (cooperative perception message)

Periodic messages from sensors in a vehicle, VRU and RSUs, to broadcast info about the current environment perceived by 1+ sensors, improving awareness.

Sensor Info container : radar, lidar, camera, ...

Perceived Object container: object perceived by sensor (classification, confidence, ...)

→ SPAT (Signal Phase and Timing)

Open interface for two-way communication between traffic signal controller and mobile devices.

Current state of all lanes at intersection, priority or preemption are provided.

- intersection state

- movement state :
  - lanes set
  - current set (green, yellow or red)
  - time until signal changes.

- used with map

→ MAP

Geometric layout of intersection

Data includes number of lanes, width, attributes, offsets, reference point.

→ MCM (Maneuver Coordination Message)

Includes the intended manoeuvres and one or more trajectories

1 - 10 Hz periodic.

MCMs are expected to have advices for vehicles (ex: suggest speed or lane change)

MCMs in RSU are smaller and less frequent.

Communication Technologies

Range >200 - 400 m

Delays < 10 ms

Time for comm in range < 10 - 20 ms

Bandwidth > 10 Mb/sec

→ ITS - G5 (802.11p)

Developed for V2X.

5.9. GHz

Range: up to 1Km

Delay: < 10 ms

Time in range: 10 - 20 msec

Rate ~ 12 Mb/sec (up to 27)

Challenges:

- vehicle safety apps rely heavily on periodic broadcast of basic safety messages (vehicle pos, speed, ...)
- 300 bytes every 100 ms
- Channel congestion in dense vehicular environments.
- no QoS
- no ACK / handshake

→ Cellular V2X (LTE - based)

Based on 3GPP

5.9 GHz

Range: up to 1km

Delay < 20ms

Time: ~100 msec

Rate up to 150 Mb/sec

Defines new air interface called PC5 for V2X. It's still over the legacy LTE Uu.

2 complementary transmission modes:

- Direct safety communication independent of cellular network (low latency V2X, 5.9 GHz) via PC5

- Network comms for complementary services (V2 Network in mobile operator licensed spectrum) via Uu

✓ Improved signal design → high relative speeds

✓ Improved transmission structure
✓ More efficient resource allocation
} high node densities

✓ GPS timing -> time sync

→ ITS - G5 vs Cellular - V2X

	ITS - G5	Cellular - V2X
field trials (+10y)	Yes	No
applications	V2V, V2I	V2V, V2I, V2N
latency	5ms	20ms
data rate	3-27 Mbps	150 Mbps
multimedia and cloud services support	No	Yes

↓

better for lower ranges

↓

better for higher ranges, more cars

QoS and Security

→ QoS in TCP / UDP apps

Problem with TCP: performs poorly in ad-hoc (vehicular networks, better for wire-line networks, assumes all losses are due to congestion.

It has loss detection, congestion control mechanisms.

However mobile networks have:

- mobility
- high bit error rate
- unpredictability / variability
- contention
- poor performance for long connections.

Delays cause TCP to send unnecessary Retransmissions, being more inneficient.

→ TCP Cubic

Cubic takes into account the time that has elapsed since the last congestion, allowing from faster recovery and greater throughput.

→ QUIC

It is built on top of UDP to improve performance by reducing latency.

Handshake combines negotiation of cryptographic (TLS) and transport parameters (uni and bidirectional streams, stream flow and connection flow control).

RTT: time for data packet to be sent + receive ACK of that packet.

Uses separate sequence numbers for data and packet delivery.

Lower RTT indicates better network conditions, and it's ability to manage multiple streams independently provides more accurate and responsive RTT estimation.

→ TCP Vegas

Senses congestion before any packet loss, decreasing window size.

Uses the difference between the expected rate and actual rate.

It has a modified slow-start and new Retransmission.

Note: TCP variants try to improve performance by estimating the available bandwidth or exploiting buffering capability.

↳ uses explicit route failure notifications
↳ TCP sender doubles retransmission timout
↳ avoid timeout and unnecessary retransmissions
↳ requires assistance from intermidiate nodes (to find path).

→ QoS in UDP

Trade-offs:

- intserv in multi-hop wireless network:
  - hard to estimate available resources
  - hard to do resource reservation
  - resource reservation is pinned to a route.

- diffserv " ".
  - hard to do admission control
  - hard to maintain assurances

→ QoS Routing

Essential component for QoS.

Can inform source node of bandwidth, QoS availability of destination and path

Add QoS requirements in routing metrics:

- difficult route maintenance
- overhead
- reserved resources not guaranteed
- responsive to nodes mobility

-> QoS for AODV

Adds extensions to route messages.

Node that receives can only forward if it meets QoS requirements.

Routing tables need to be updated (fields for delays, bandwidths)

Delay: maximum delay extension

list of sources requesting delay guarantees, used during route discovery

Bandwidth: similar to delay

REQ can include both

Loosing QoS: if node detects QoS cannot be maintained, generates QoS_LOST to depending nodes

Reasons: increased load of node

→ Transmission Quality (Batman)

Add local link quality in the TQ value

$$TQ = TQ(incoming) - TQ(local)$$

→ QoS for OLSR

Multi-point relays are the nodes with best QoS.

QoS depends on available bandwidth, % of nodes on other street and lane weight.

Security

→ Routing attacks

Modification: malicious nodes announces better routes than the other nodes in order to be inserted in the network.

(change route seq. number, hop count)

DOS attacks with modified routes and changes packet headers so it doesn't reach destination

Impersionation: Usurpation of the identification of another node to perform changes.

Spoofing MAC addresses, creating loops and leaving nodes unreachable.

Fabrication: generates false traffic to disturb network (false route messages, corrupting route state, routing table overflow, replay attack, black hole attack (0 metric route).

Key management

-> Symmetric cipher

- ✓ fast and secure
- ✓ longer keys -> longer security
- × requires the share of secret key
- × complex administration

-> Asymetric cipher (PKE)

- ✓ no need to share keys
- ✓ scalable and versitle
- × computationally intensive
- × certificate authority
- × confidential private keys

-> Key management in ad-hoc networks

Vulnerable mobile nodes.

Mobility induced unstable network topology

NO infrastructure to send key info to nodes.

→ Self-organized public key management (SOPKM)

Users issue certificates based on personal acquaintance (certificates stored and distributed by users themselves)

Has a repository for updated and expired certs.

Public keys and public-key certs:

If a user u believes that a given public key k_v belongs to a user v, then u can issue a public-key certificate in which k_v is bound to v with the signature of u. (and validity)

Each certificate is stored at least twice: by the issuer and the user.

Updating repositories:

Exchanging certificates between nodes, where each node multicasts its certificate graphs to it's physical neighbours (hash of ids).

Users share public keys when they meet.

A user who wants to find the public key of other has to find the chain of valid public key certificates leading to that user.

Revocation

Certificates can be explicitly revoked or implicity (expiration)

Malicious users

Certificate exchange mechanisms allows nodes to virtually gather all certificates

They cross-check the user-key bindings in the certificats to detect inconsistencies.

→ Self-securing ad-hoc wireless networks (SSAWN)

Achieve high security scenario.

High access ratio

Efficient communication

localized trust model : an entity is trusted if any k trusted entities claim so within a time period. (usually among 1-hop neighbors).

shared secrets: use of RSA. Use of Public key and Global Secret key (SK).

SN is used to sign certificats for all nodes and can be verified by the well-known public key.

Each node has a part of the secret.

- By collecting k partiall certificates, combines them together to generate the full new certificate
- Nodes without valid certificates are denied from acces to the network.

Reputation appraaches

Explore reliability of each node:

- how node handles packet forwarding
- level of trust
- reputation information exchanged periodically among neighbours

Routing and comms through high rep. nodes.

Protect network traffic from misbehaving nodes and minimize interaction.

There are friendly, selfish and bad nodes.

→ Reputation

Combination of first-hand reputation (neighbours) and second-hand reputation (info from neighbours).

Probability of well-transmitted packets.

Deviation test to detect false reports.

- Trust value : α

T = trustworth

NT = non-trustworthy

$$\alpha = \frac{T}{T+N}$$

- Merge first and second-hand reputation:

Reputation of node B seen by A is the first-hand rep plus the trust factor of second-hand rep of B seen by C (and others second-hand reps).

$$R_{AB} = F_{AB} + \alpha F_{CB}$$

- normal operation of network

. Choice of nodes to form a path uses the reputation of nodes

- Choice of nodes to join certificate graph user reputation. (+)

- Choice of nodes to get the very pairs or very pairs user reputation (+).

- Reputation of nodes can change over time.

Mobile Edge Computing

- Concept in 5G
- Brings cloud closer to network edge
- Traffic redirecting and low latency.
- Provides services to enhance apps with context information.
- Facilitates running apps at the right location and time.

→ Edge and Cloud

- Edge computing devices depend on network access to the cloud to receive machine learning stuff.
- They need to send sensor and data to cloud.
- Strong bandwidth requirements → 5G to 6G
- Low latency
- Massive ammount of nodes.

→ MEC: Mobile Edge Apps

. Run as VMs
. consume and provide edge services
. have rules about DNS and resources
. assisted by mobility info
. may be relocated to other mobile edge host.

→ MEC: Mobile Edge Platform

. environment for apps discover, consume and offer edge services
. configures DNS
. provides mobile edge services
. provides access to persistant storage
. controls data-plane in SDN.

→ MEC: Mobile Edge Orchestrator

. maintains overall view of system and mobile edge hosts (resources, services, topology)
. on-boards app packages
. triggers app start and termination
. triggers app relocation

Note: MEC is envisioned as promising tools to deliver better Quality of Experience for immersive AR apps.

Key enabler for IoT and mission critical vertical solutions.

Enables apps to be deployed and run in virtualized env.

Enables autonomous networks and systems.

6G

Self-organization

P2P relationships

Ubiquous 3D coverage (space, terrestrial, undersea)

Thing-to-thing communication (Intelligent IoT).