URCA

Intelligent Transport System

VANET – Routing protocols - Facilities messages – GeoNetworking

Contents

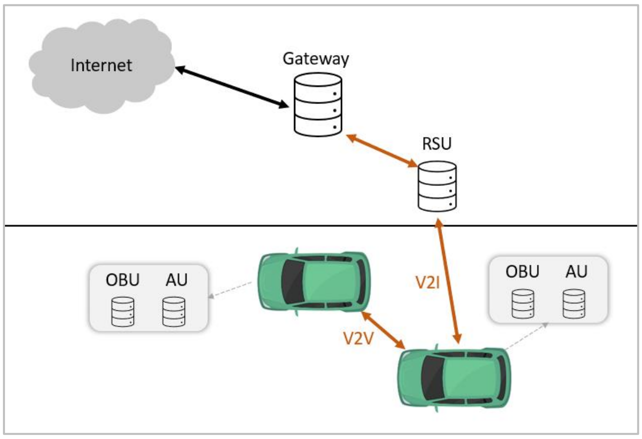
VANET and routing protocols

VANET (Vehicular ad hoc Network)

VANET is a wireless ad hoc network that provides communications among vehicles.

The goal is to provide an accident-free environment and move toward implementation of the zero-accident car by the help of vehicle area network. It shall improve road security, traffic management conditions and provide on-board infotainment (internet access, the location of free parking places, video streaming sharing).

VANETs are created by applying the principles of mobile ad hoc networks, MANETs. Indeed, vehicular Ad Hoc Networks (VANETs) are a subset of MANETs. VANETs differ from MANETs about the paths they follow, they only move on roads since MANETs could move without any restriction.



VANET main components:

-**OBU** (On Board Unit): present in a vehicle which allows the connectivity. OBU is responsible for all mobility and networking function.

-**AU** (Application Unit): present in a vehicle. It can be a dedicated device for safety applications or normal device, such as personal digital assistant. The AU decides what to do with the information coming from that communication.

- **RSU** (Roadside Unit): present on the roadsides. RS:
  - Extends the communication range of the ad hoc network,
  - Shares warnings to vehicles (low bridge warnings, accidents…),
  - Provides internet connectivity to OBUs.

Communications domains

- V2V: Vehicles communicate with other vehicles.
- V2I/I2V: communicates with an RSU.
- V2X: A mixed architecture (V2V and/or V2I)

VANET's characteristics

Routing protocols are defined and based on these characteristics:

- Predictable mobility: with VANET we can predict the mobility of vehicles. In MAGNET we make assumptions that mobility is random, but the movement of vehicles is restricted to roads.
- Large scale network
- Variable network density: although the network is very large the density can still vary a lot.
- No power limitations
- **Dynamic network topology**
- High computational ability: there can be equipped with enough sensors and computational resources such as processor memory capacity, advanced antenna…
- Security and privacy

Routing protocols

VANET is highly dynamic, although the mobility of a single vehicle can be predicted, the overall network is still quite unpredictable due to variable traffic. This can result in drop of information which leads to a poor communication.

Topology based

A protocol uses routing table which contain the information about neighbor node to router data. The problem is that information can become outdated pretty quickly.

Geographical routing protocol

Uses the actual vehicle's physical location for routing. Those protocols need extra resources (GPS). Because we are always checking the position of the destination.

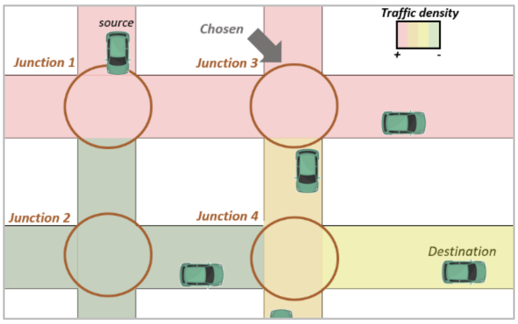
GPSR (Greedy Perimeter Stateless Routing)

It is a reactive protocol which forwards the packet to the destination's nearest neighbor (Greedy Forwarding approach) until reaching the destination. Therefore, it scales better than the topology based protocols, but it does still not consider the urban streets topology and the existence of obstacles to radio transmissions.

GSR (Geographic Source Routing)

It combines geographical information and urban topology (street awareness). The sender calculates the shorter path (using Djikstra algorithm) to the destination from a map location information. Then, it selects a sequence of intersections (anchor-based) by which the data packet has to travel, thus forming the shortest path routing. To send messages from one intersection to another, it uses the greedy forwarding approach. The choice of intersections is fixed and does not consider the spatial and temporal traffic variations. Therefore, it increases the risk of choosing streets where the connectivity is not guaranteed and losing packets.

GyTAR (Greedy Traffic Aware Routing Protocol)



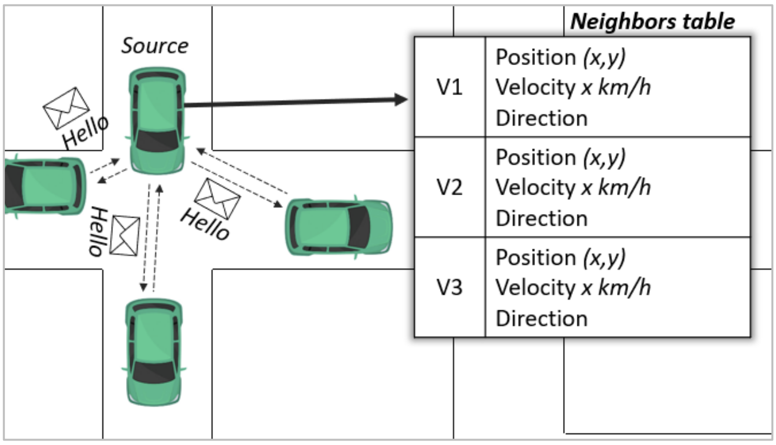
A geographical routing protocol adapted to urban environments and managing the traffic conditions. It is based on a localization system (GPS).
GyTAR aims to efficiently relay data in the network considering <u>the real time road traffic variation</u> and <u>urban environment characteristics</u>. It also considers information about vehicles <u>speeds</u> and <u>directions</u>.

1- Junction selection

Junctions through which a packet must pass to reach its destination are chosen dynamically and one by one. When selecting the next destination junction, a node looks for the position of the neighboring junctions using the map.
A score is given to each junction considering the traffic density Tj and the metric distance Dj to the destination.
The best destination junction j is then the junction with the highest score: $S(j) = \propto\times f(Tj) + \beta \times g(Dj)$

2- Forwarding data between two junctions

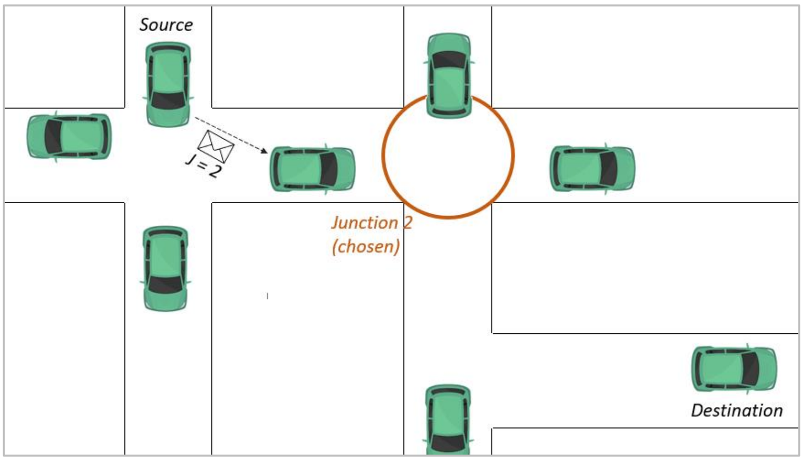
Each vehicle maintains a neighbor table in which position, velocity and direction of each neighbor vehicle are recorded. This table is updated through hello messages exchanged periodically by all vehicles.



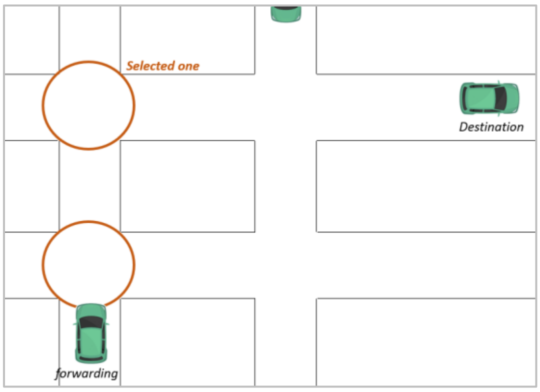
Neighbors table

V1	Position *(x,y)* Velocity *x km/h* Direction
V2	Position *(x,y)* Velocity *x km/h* Direction
V3	Position *(x,y)* Velocity *x km/h* Direction

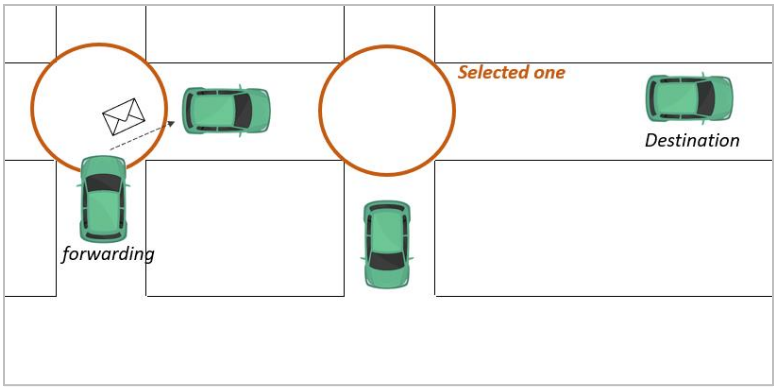
All data packets are marked by the location of this junction. Thus, when a packet is received, the forwarding vehicle computes the new predicted position of each neighbor using the recorded information (velocity, direction and the latest known position), and then selects the next hop neighbor (i.e. the closest to the destination junction)



If a packet gets stuck in a local optimum, the forwarding vehicle might be the closest to the next junction., the repair strategy is based on the idea of "carry and forward". The forwarding vehicle of the packet in a recovery mode will carry the packet until the next junction or until another vehicle, closer to the destination junction, enters/reaches its transmission range.

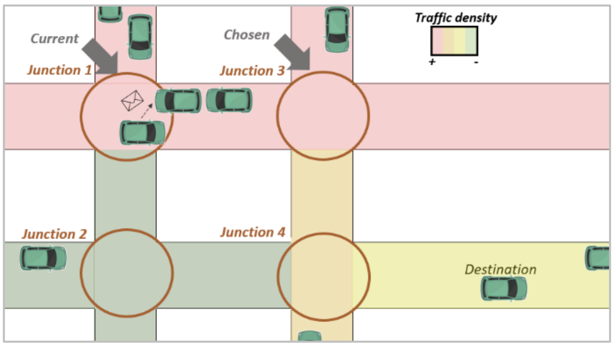


No neighbors, so goes to the next junction.



Finds a new neighbor, so sends the message.

GyTAR aims to efficiently use the network resources (wireless bandwidth) by limiting the control message overhead, and to route data packets from sources to destinations in the vehicular network with a reduced end-to-end delay and low packet loss.

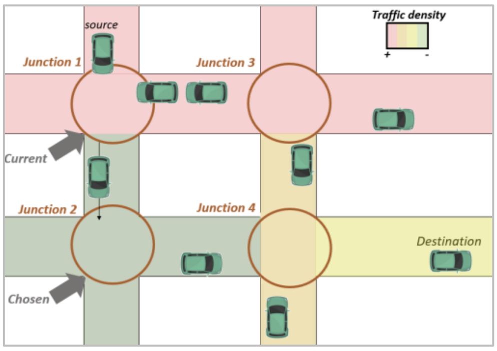


However, before selecting the next junction, **GyTAR doesn't consider the direction of vehicles**. As a result, GyTAR can select the junction which has <u>higher traffic density</u>, but vehicles move opposite to direction of destination. As a result, GyTAR suffers from local maximum problem as all the vehicles have moved away.

eGyTAR (Enhanced GyTAR Routing protocol)

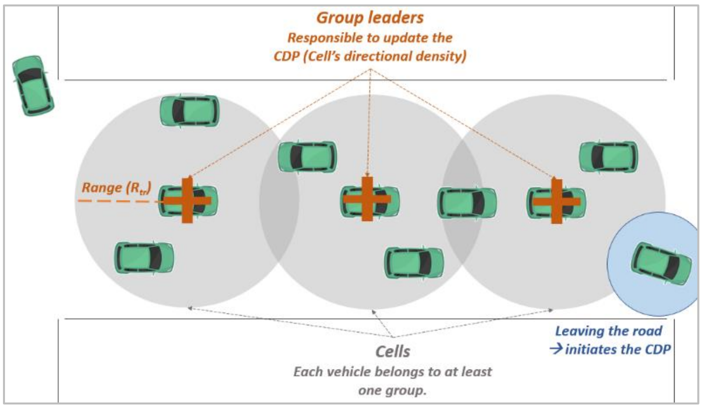
E-GyTAR protocol selects junction automatically on the basis of direction as well as density of vehicles. E-GyTAR achieves higher packet delivery ratio and lower end-to-end delay than GyTAR.

The selected junction has the higher number of vehicles moving in the direction of destination.

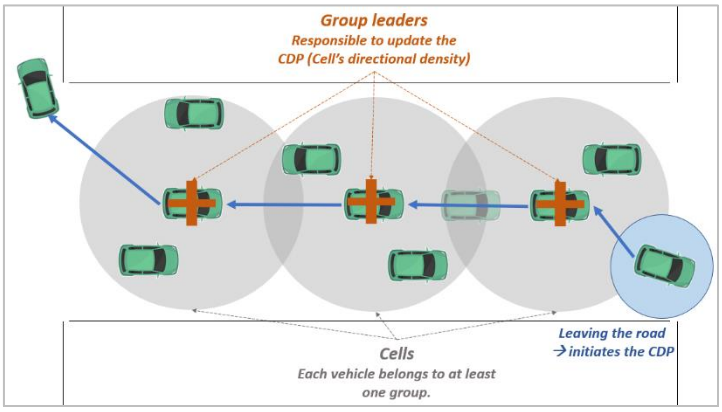


Estimate the on-road traffic density:

To estimate the on-road traffic density the road is dissected into small cell of fixed size. The vehicle which is closest to the center of the cell is selected as a group leader for that particular cell. The group leader is responsible to update the CDP by not only adding the total number of vehicles but also including the number of vehicles moving in the direction of destination in that particular cell in the CDP packet. The vehicle which is about to leave the road initiates the CDP. It will add the road ID, transmission time, list of anchors and the direction, for which the density will be calculated.


Group leaders
Responsible to update the CDP (Cell's directional density)
Range (R_{tr})
Leaving the road
→initiates the CDP
Cells
Each vehicle belongs to at least one group.

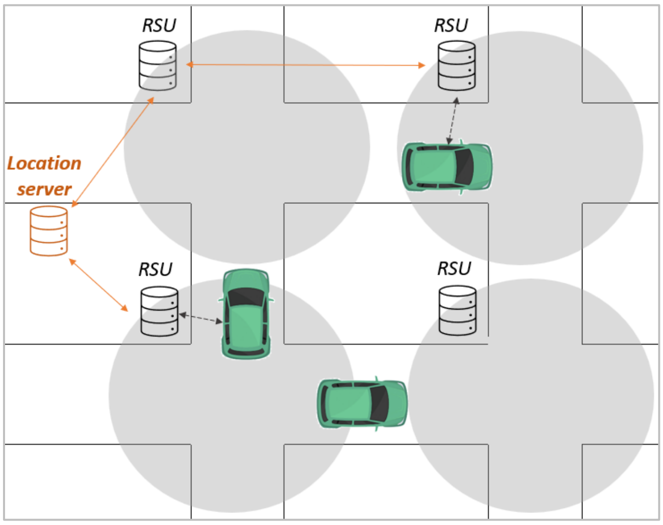
Packets travel along with these anchor to reach the other intersection. Upon receiving the CDP, the group leader updates CDP by including the total density and the directional density of the corresponding cell.


Group leaders
Responsible to update the CDP (Cell's directional density)
Leaving the road
→initiates the CDP
Cells
Each vehicle belongs to at least one group.

E-GyTAR uses the same routing mechanism as proposed in GyTAR protocol and uses the improved greedy approach to route the packets between the two involved junctions. Neighbor table is maintained by each vehicle in which it records the speed, velocity, and direction of each vehicle.

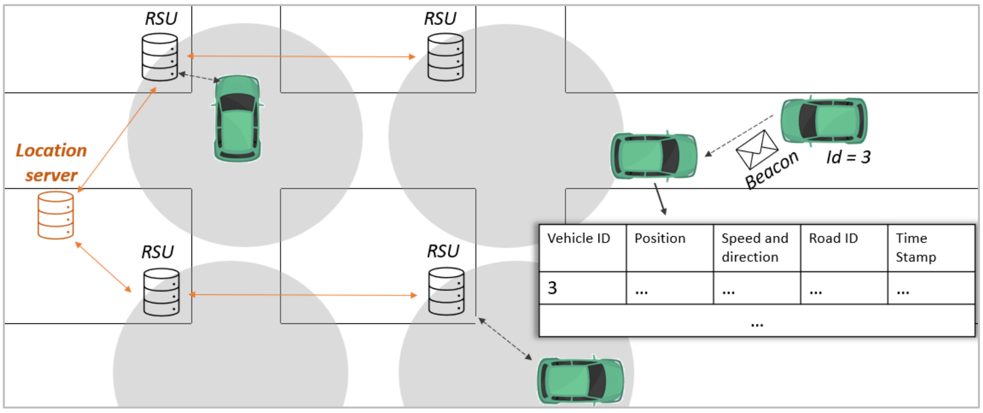
Location service algorithm (cf. An Urban location service for vehicular area networks)

A location service based on the cooperation of fixed RSUs. A vehicle finds the closest RSU to request a route to the destination. A location system is a set of distributed and interconnected RSUs through the network. Each RSU plays the role of a location server and maintains a part of all vehicles' information. This information of vehicles will be periodically shared with all other location servers. The role of a location server is not only the maintenance of vehicle information but also the participation in finding the pertinent route between two nodes.



Each location server shares its information table with all other location servers by using RSU-to-RSU communication through wired links.

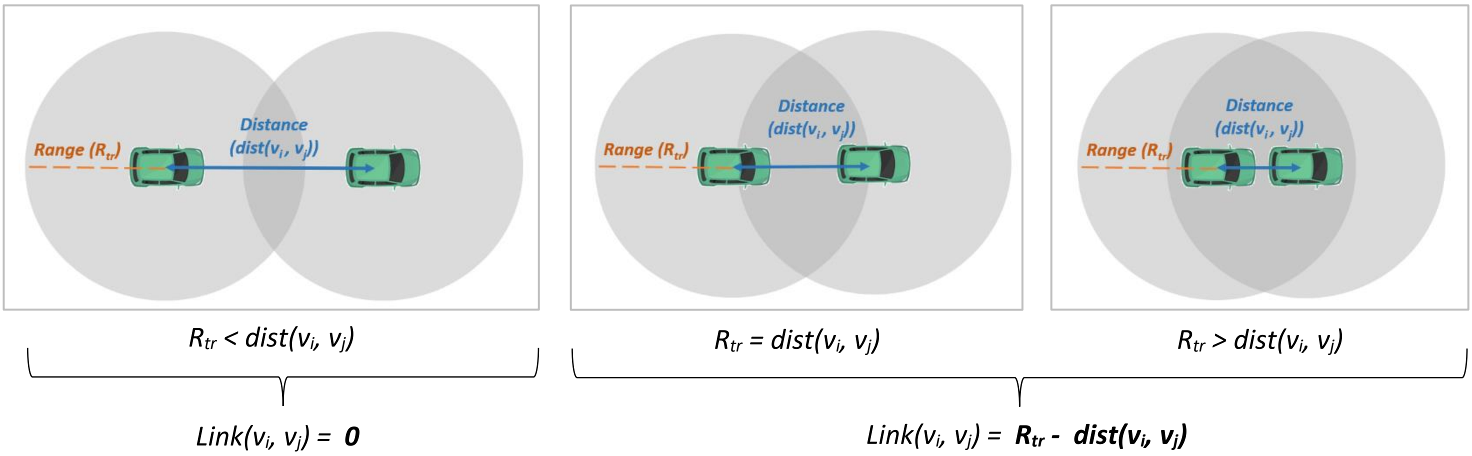
A vehicle receives vehicle beacon and puts the up-to-date information in this beacon (vehicle_id, position, speed and direction) to its information table.



Vehicle ID	Position	Speed and direction	Road ID	Time Stamp
3	...	...	...	...
...				

Link connectivity metrics

We define Link Connectivity (LC) as a metrics which measures the connectivity of a given road.


Range (R_{tr})
Distance ($dist(v_i, v_j)$)
Range (R_{tr})
Distance ($dist(v_i, v_j)$)
Range (R_{tr})
Distance ($dist(v_i, v_j)$)

$R_{tr} < dist(v_i, v_j)$ $R_{tr} = dist(v_i, v_j)$ $R_{tr} > dist(v_i, v_j)$

$Link(v_i, v_j) = \mathbf{0}$

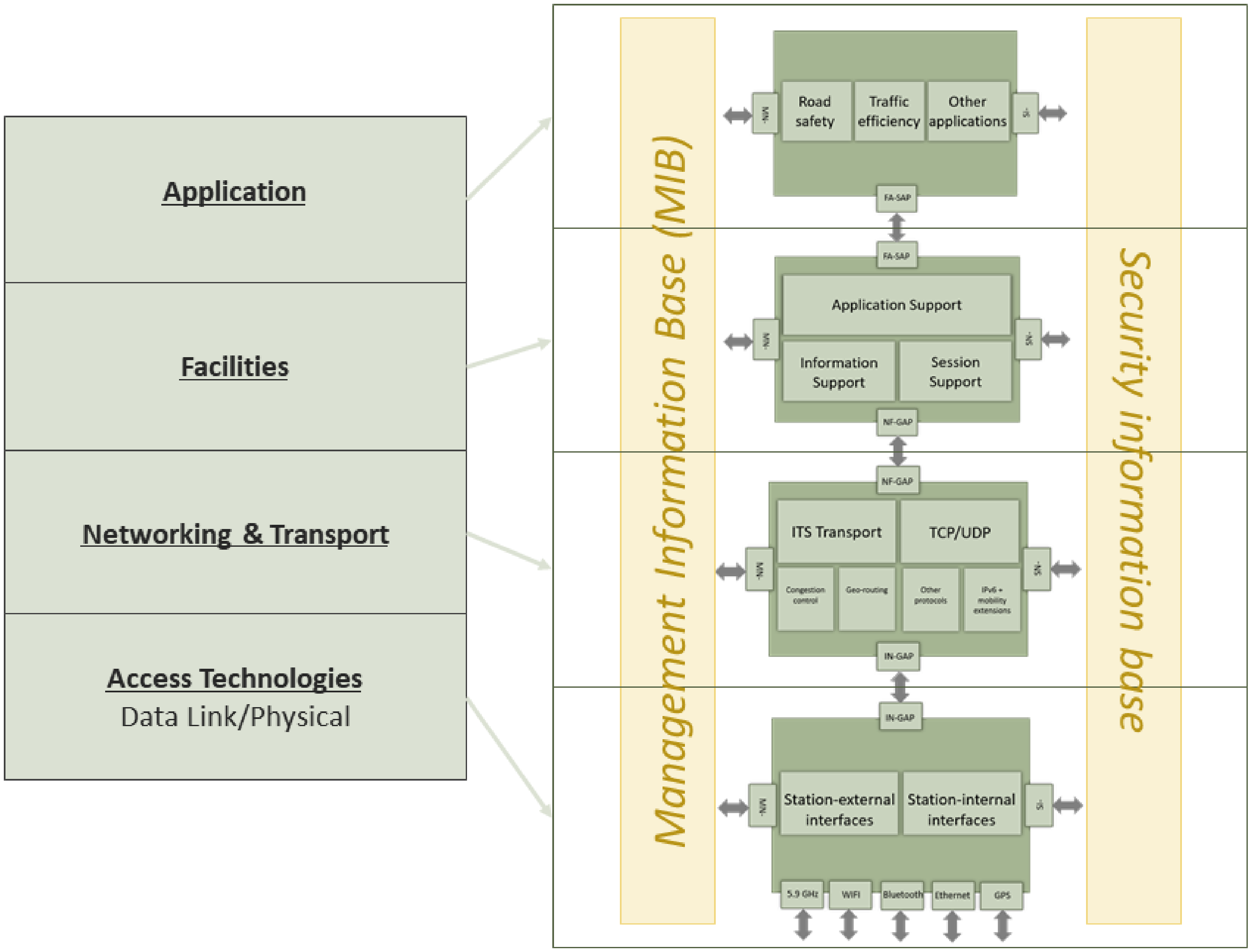
$Link(v_i, v_j) = \mathbf{R_{tr} - dist(v_i, v_j)}$

The **Mean Link** (ML) between all vehicles in the same road can be expressed as follow:

$$ML_{road} = \frac{\sum_{i=0}^{N} R_{tr} - dist(v_i, v_{i+1}))}{(N+1)}$$

The proposed metrics ML is useful to select appropriate route from a source to a destination.

ITS Station Reference Architecture



Application

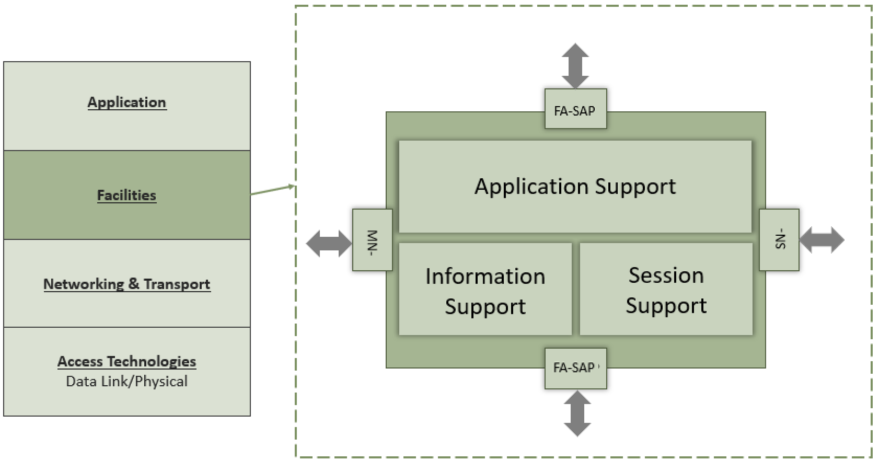
Facilities

Networking & Transport

Access Technologies
Data Link/Physical

Applicative and facilities messages

Architecture



General information

A variety of messages have been defined. However, these messages have been regionally standardized and therefore differ from country to country. In the US, they have been mostly defined by Society of Automotive Engineers (SAE). In Europe, ETSI is in charge of defining V2X messages.

CAM (Cooperative Awareness Messages)

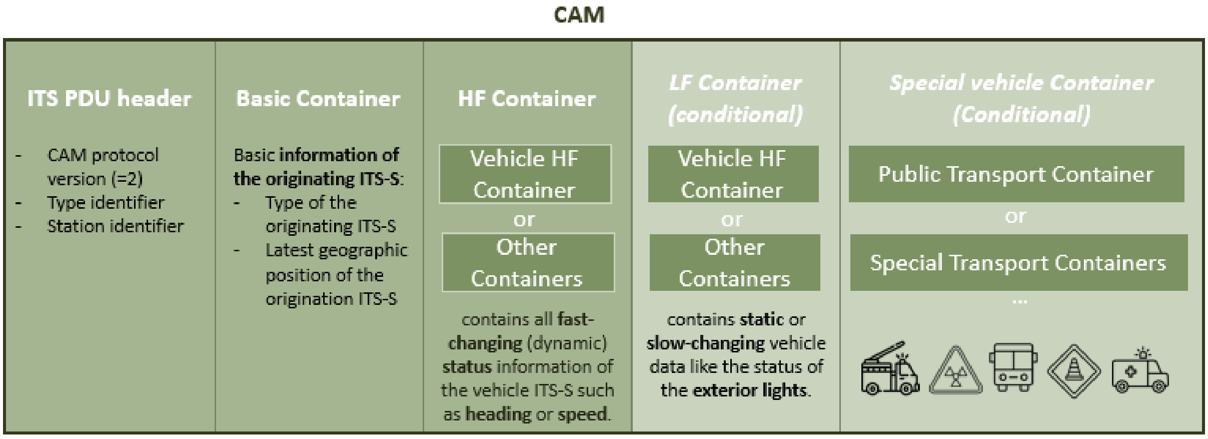
Cooperative Awareness Messages (CAMs) are messages exchanged in the ITS network between ITS-Ss to create and maintain awareness of each other and to support cooperative performance of vehicles using the road network. CAM are distributed within the ITS-G5 (802.11p) network and the GN packet transport type is Single-Hop Broadcasting (SHB).

the Cooperative Awareness Message (CAM) is the central piece of the ETSI protocol suite.

Examples of two use cases which benefit from CAM:

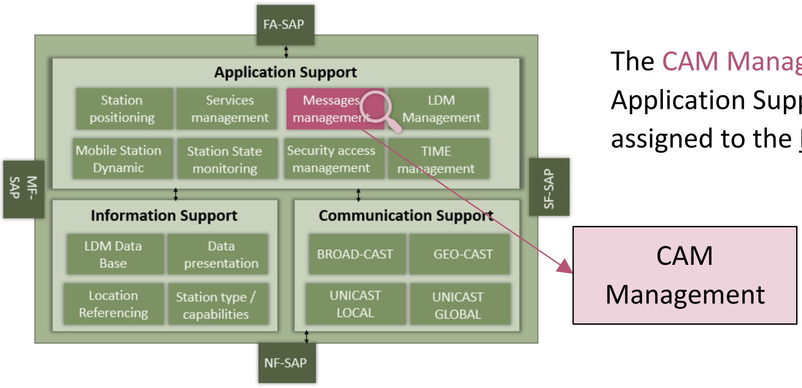
- Approaching Emergency Vehicle
- Slow Vehicle Warning

A CAM is composed of one common ITS PDU header and multiple containers, which together constitute a CAM.



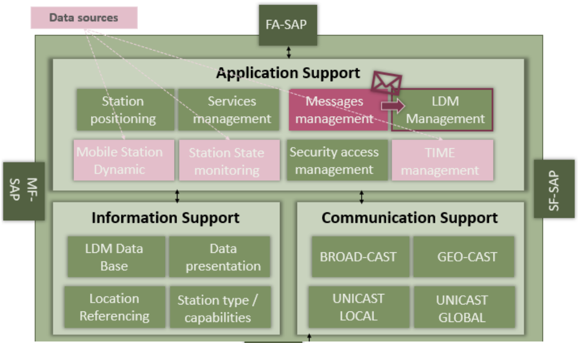
CAM

ITS PDU header	Basic Container	HF Container	*LF Container (conditional)*	*Special vehicle Container (Conditional)*
- CAM protocol version (=2) - Type identifier - Station identifier	Basic **information of the originating ITS-S**: - Type of the originating ITS-S - Latest geographic position of the origination ITS-S	Vehicle HF Container or Other Containers contains all **fast-changing** (dynamic) **status** information of the vehicle ITS-S such as **heading** or **speed**.	Vehicle HF Container or Other Containers contains **static** or **slow-changing** vehicle data like the status of the **exterior lights**.	Public Transport Container or Special Transport Containers ...



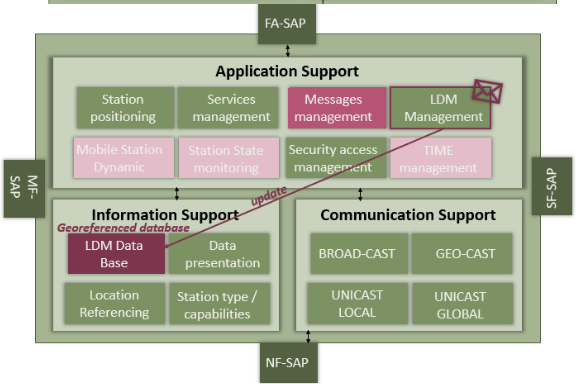
The CAM Management belongs to the Facilities Application Support and more detailed it is assigned to the Messages Management.

The CAM Management generates CAMs using as data sources the following facilities:



- Time management: provides global time reference for time stamping.
- Station state monitoring: provides current static state of ITS stations.
- Mobile station dynamic: provides real time kinematics of ITS stations.

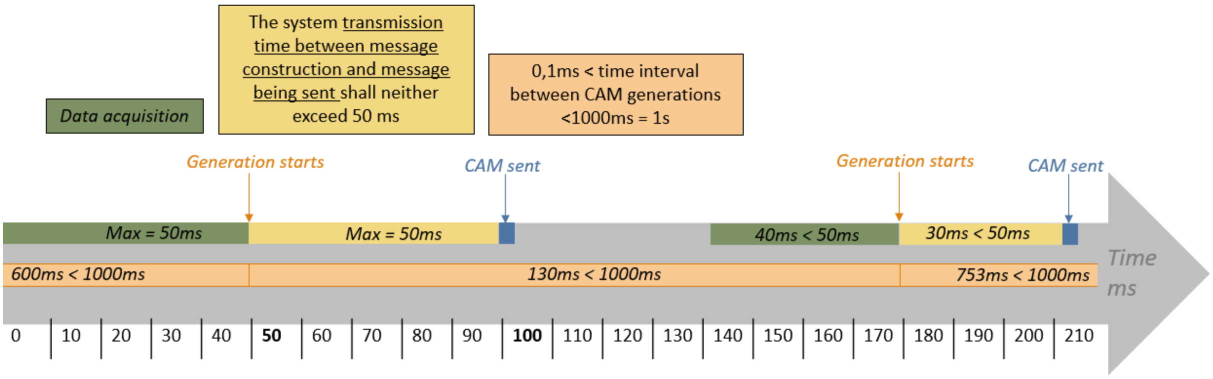
The CAM Management passes the valid CAMs to the LDM management.



LDM management, which analyses the messages and updates in real time the LDM data base. The LDM is in principle a local georeferenced database containing a C2X-relevant image of the real world.

CAMs are generated by the CAM Management and passed to lower layers according to following rules:

- Maximum time interval between CAM generations is 1 s
- Minimum time interval between CAM generations is 0,1 s

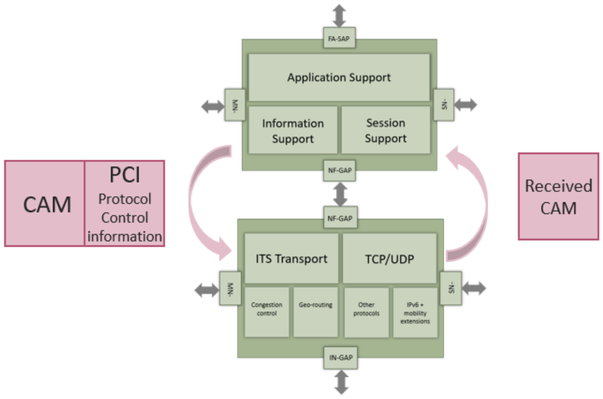

The system transmission time between message construction and message being sent shall neither exceed 50 ms

0,1ms < time interval between CAM generations <1000ms = 1s

Interface to Applications

The CAM Management is application independent. For this reason, there is no interface to applications.

Interface to the Networking & Transport layer



Message format specification

ITS Station Profiles

basicVehicle	*basicIRS*
Profile mainly used for private vehicles. This profile serves as basis for further profiles such as emergency vehicle. ***Mandatory** tagged values examples:* - vehicleType - vehicleSpeed - vehicleSpeedConfidence - heading - headingConfidence - stationLength - stationWidth - … ***Situational mandatory** tagged values examples:* - confidenceStationLength - crashStatus ***Optional** tagged values examples:* - distanceToStopLine - turnAdvice - …	The basicIRS is an ITS Roadside Station which can offer all functionality of the infrastructure. It serves as basis for more specialized profiles.

Security

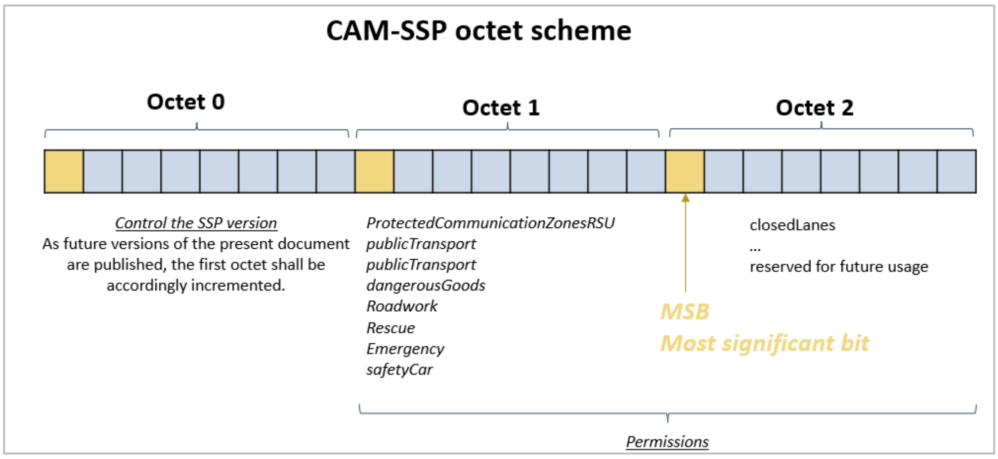
The security mechanisms for ITS consider the authentication of messages transferred between ITS-Ss with **certificates**.

A certificate indicates:

- Its holder's permissions to send a certain set of messages.
- An optionally privileges for specific data elements within these messages.

Within the certificate the permissions and privileges are indicated by a pair of identifiers:

- The ITS-AID (ITS-Application Identifier) indicates the overall type of permissions being granted.
- The SSP (Service Specific Permissions) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID.
  CAMs shall be signed using private keys associated to Authorization Tickets that contain SSPs of type BitmapSsp.



As future versions of the present document are published, the first octet shall be accordingly incremented.

An incoming signed CAM is accepted by the receiver if the certificate is valid, and the CAM is consistent with the ITS-AID and SSP in its certificate.

DENM (Decentralized Environmental Notification Message)

Decentralized Environmental Notification Messages (DENMs) are event-driven messages to inform, for instance, about a collision, road works or weather conditions.

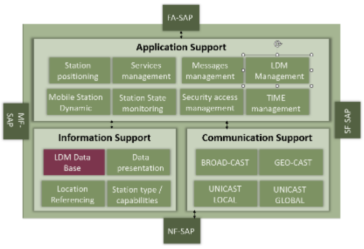
DENMs can be forwarded as long as the illustrated event is still ongoing. Typically for an ITS application, a DENM is disseminated to ITS-Ss that are located in a geographic area through communications among ITS stations.

Message termination can happen for two reasons:

- A pre-defined timer expires.
- A termination message is sent.

In order to keep messages about the event as up to date as possible, four types of messages have been defined:

- **New DENM**: the original DENM sent by a vehicle describing the event.
- **Update DENM:** is used to update event information and must be sent by the originated sender.
- **Cancellation DENM:** informs about the event termination and must be sent by the originated sender.
- **Negotiation DENM:** works like the cancellation DENM but is sent by another vehicle.

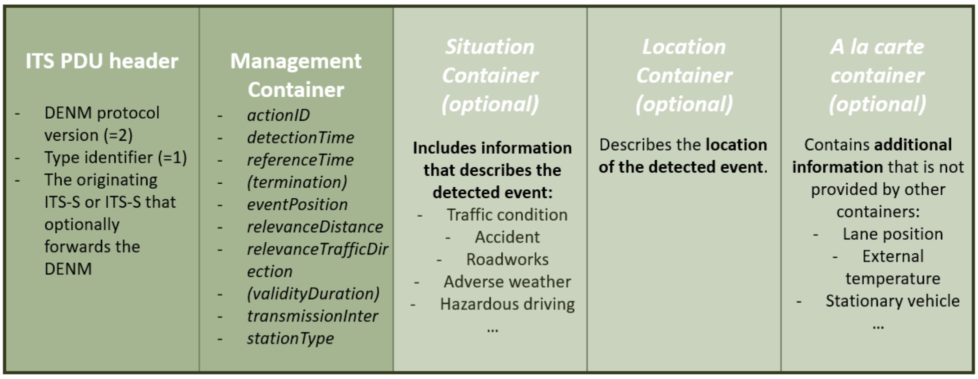


The DEN basic service is a facilities layer entity that implements the DENM protocol. The DEN basic service may interact with other facilities layer entities, in particular the Local Dynamic Map (LDM).
The DEN basic service shall provide the following sub-functions:

- Encode DENM
- Decode DENM
- DENM transmission management
- DENM reception management
- DENM Keep Alive Forwarding (KAF)

A DENM is composed of a common ITS PDU header and multiple containers, which constitutes the DENM payload.

DENM



ITS PDU header	Management Container	*Situation Container (optional)*	*Location Container (optional)*	*A la carte container (optional)*
- DENM protocol version (=2) - Type identifier (=1) - The originating ITS-S or ITS-S that optionally forwards the DENM	- *actionID* - *detectionTime* - *referenceTime* - *(termination)* - *eventPosition* - *relevanceDistance* - *relevanceTrafficDirection* - *(validityDuration)* - *transmissionInter* - *stationType*	**Includes information that describes the detected event:** - Traffic condition - Accident - Roadworks - Adverse weather - Hazardous driving …	Describes the **location of the detected event**.	Contains **additional information** that is not provided by other containers: - Lane position - External temperature - Stationary vehicle …

SPAT/MAP

The SPAT/MAP application is most relevant for cities and/or urban areas.
Intersections are often particularly dangerous because lane routing is not always intuitive, intersections can be confusing and sometimes vehicles have to yield despite green traffic lights.

Therefore 4 protocols have been standardized with a focus on intersection safety:

- **SPAT (Signal phase and timing**): will inform drivers about the current status and change of the traffic signal ahead as well as when the next signal stage change. It will also provide information about approaching traffic to optimize the signal system.
- **MAP (Map Data):** describes the topology of the intersection: the width of the road, the direction of each lane, connecting lanes, what kind of vehicles may use the lane and also what signal group the lane belongs to. The Road and lane Topology service supports continuous transmission for infinity of the MAPEM. As the MAPEM message is not changed very often in time, a stable release is stored within the ITS-S for continuous broadcast.
- **SRM (Signal Request Message):** which requests preempt or priority services for selected user groups.
- **SSM (Signal Status Messages):** which describes the internal state of the signal controller. Provides a more complete summary of any pending priority or preemption events.

ETSI also included those 4 protocols in their protocol suite. Since ETSI added the ITS PDU headers to the message, they are called Signal Phase and Timing Extended Message (SPaTEM), Map Data Extended Message (MAPEM), Signal Status Extended Message (SSEM) and Signal Request Extended Message (SREM) in the ETSI architecture.

Among potential benefits is a more optimized and environmentally friendly driving performance:

- Provides priority to selected groups like emergency vehicles and public transportation.
- Has positive effect on traffic flow.
- Minimizes the number of stops resulting in less head-tail accidents.

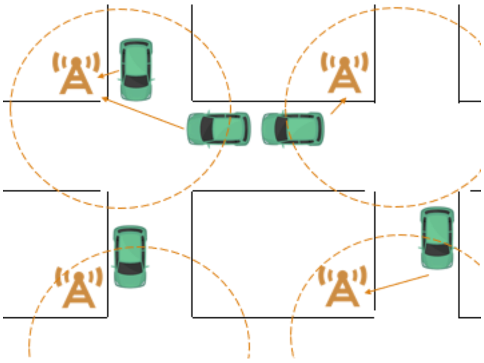
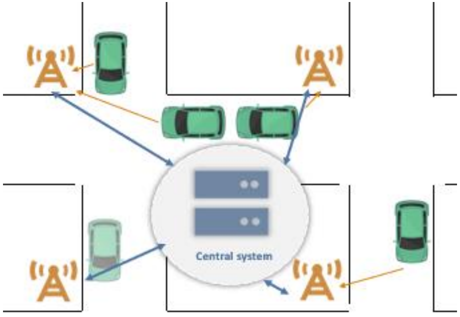
Characteristics

SPAT/MAP systems have the following characteristics:

- Concern communication between the traffic signal controller and approaching vehicles.
- Provide the driver with information about the residual signal time when approaching the intersection.
- Can be realized with centralized or local signal control, or a mix of them.
  SPAT/MAP information from a centralized system can be retrieved over cellular communication systems. The choice depends on road operator priorities related to existing and new signal control systems.

Signal control system

Fixed time *systems control systems*	***Adaptive*** *traffic control systems*
Fixed time systems give a pre-set green time to each movement in the intersection and use a pre-set cycle time. This makes it is easy to predict the signal state for a vehicle approaching in a certain direction. The challenge is mostly related to the expected travel time towards the stop line.	Even though the system might expect a certain pattern for the stages and green times, latest information might introduce alterations. Different systems allow either small or larger shifts.

Local standalone *system*	***Centralized*** *system*
The traffic controller at each intersection makes all the decisions for the next signal phase based upon local available information. 	The traffic controller at each intersection communicates with a central system receiving certain parameters that goes into the algorithm deciding the next signal phase.  An alternative for SPAT/MAP is based on centralized monitoring of signal changes and using mobile communication networks towards the users.

IVIM (Infrastructure to Vehicle Information Message)

IVIMs are used to communicate the content of static and dynamic road signs, such as (temporary) speed limits and road works warnings

An IVIM shall be disseminated to reach as many ITS-S as possible (broadcast), located in the MDA (Minimum Dissemination Area).

An IVIM shall be transmitted:

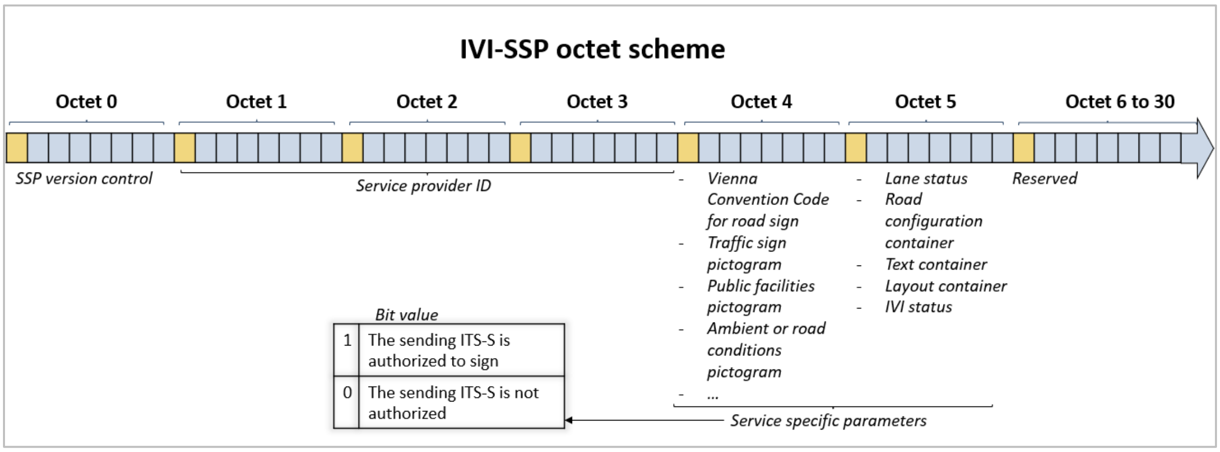
- If Applicable in time
    - *Example:* a speed limitation only valid between 8:00 and 20:00
- Due to the context as determined by the sending ITS-S
    - *Example:* speed limitation applicable in case of fog.

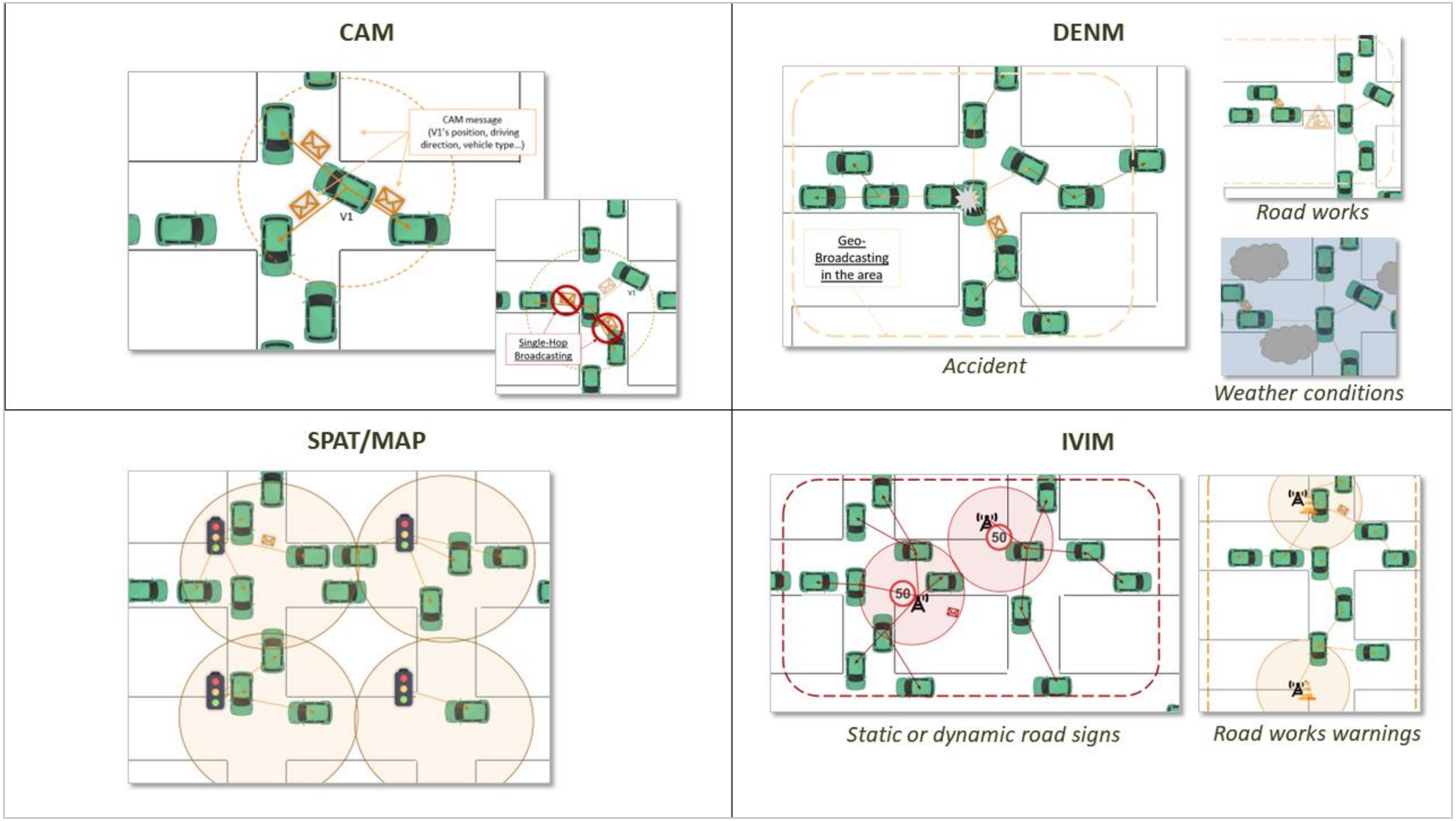
The IVIM identification is enabled with a parameter. Each time a new IVIM is generated upon an application request, a new identifier value shall be assigned by the IVI service. The identifier number is linked to the organization proving the IVI service (service provider). It enables the receiving ITS-S to differentiate IVIM messages transmitted from different service providers.

- **Trigger**: IVI service (uses IVIM) trigger refers to the process of the generation and transmission of an IVIM when the IVI service of the sending ITS-S receives an application request. The IVI service shall then generate a new message (so new identifier).
- **Update**: An IVIM content is updated by the service provider. The ITS-S application provides the update information to the IVI service at the sending ITS-S. An *update* is also used to change or add the end time to the IVIM.
- **Repetition**: In between two consequent *updates*, an IVIM shall be repeated by the IVI service of the sending ITS-S at a pre-defined repetition interval, in order that new ITS-S entering the MDA during the event validity duration may also receive the IVIM.
- **Termination**: An IVI service termination is either the ending of transmission, an application cancelation or an application negation:
    - Ending of transmission by the ITS-S originally sending the IVIM.
    - IVI service cancellation by the Service Provider originating the IVIM.
    - IVIM negation by another organization.

Security

The IVIM contains the identification of the organization originating the IVIM, e.g. the Service Provider that originated it. An R-ITS-S is only allowed to send out IVIM for a defined Service Provider. The SSP for the IVIM is defined by a variable number of octets.


IVI-SSP octet scheme
Octet 0
Octet 1
Octet 2
Octet 3
Octet 4
Octet 5
Octet 6 to 30
SSP version control
Service provider ID
- Vienna Convention Code for road sign
- Traffic sign pictogram
- Public facilities pictogram
- Ambient or road conditions pictogram
- ...
- Lane status
- Road configuration container
- Text container
- Layout container
- IVI status
Reserved
Bit value
1 The sending ITS-S is authorized to sign
0 The sending ITS-S is not authorized
Service specific parameters


CAM
CAM message (V1's position, driving direction, vehicle type...)
V1
Single-Hop Broadcasting
V1
DENM
Geo-Broadcasting in the area
Accident
Road works
Weather conditions
SPAT/MAP
IVIM
50
50
Static or dynamic road signs
Road works warnings

ITS GeoNetworking

Vehicle ITS stations are equipped with a Communication & Control Unit (CCU) that implements the ETSI communication protocol stack. The ITS ad hoc network is also formed by roadside ITS stations or Roadside Units (RSUs) that, together with CCUs, that enables decentralized inter-vehicle communications. RSUs are located alongside roads and implement the ETSI communication protocol stack, further increasing network connectivity. The ETSI TC ITS has also standardized the ETSI **GeoNetworking protocol** (GN) to forward packets in the ITS architecture.

GeoNetworking protocol is a network protocol that resides in the ITS (Intelligent Transportation System) **networking** and **transport** layer.

	Application	CAM
	Presentation	
	Session	
	Transport	BTP (Basic Transport Protocol) or GN6ASL
Beacon	Network	GeoNetworking
	Data Link	
	Physical	

The GeoNetworking protocol provides servicers to upper protocol entities.

SDU: is the "payload" of a given PDU. So, a PDU of the transport protocols is considered as SDU in the GeoNetworking protocol.

Packet structure:

~~*Secured*~~	**MAC header** MAC address (= link layer address) to define and identify the next hop of a GeoNetworking packet.	**LLC (Logical Link Control) header** Ethernet type field indicating GeoNetworking packet.	**GeoNetworking header** ★	**Optional payload** User data Beacons don't have a payload.		
Secured	**MAC header** MAC address (= link layer address) to define and identify the next hop of a GeoNetworking packet.	**LLC (Logical Link Control) header** Ethernet type field indicating GeoNetworking packet.	**GeoNetworking *basic* header**	**GeoNetworking *Secured* Packet**	**GeoNetworking *common* and *optional extended* header**	**Optional payload**

The MTU (Maximum Transmit Unit) depends on the MTU of the MTU_ALL (access layer technology) over which the GeoNetworking packet is transported.

★ GeoNetworking header

Structure

Basic header	**Common header**	**Extended header (optional)**
- **Version** of the GeoNetworking protocol. ★ - **NH** (Next header) identifies the type of header immediately following the *basic header.*	★ - **NH** - **Reserved** ★ - **HT** (header type of the GeoNetworking)	*Cf. ETSI EN 302 636-4-1 V1.3.1*

- **Reserved** - **LT** (Lifetime field) maximum time a packet may be buffered until it reaches its destination. ★ - **RHL** (Remaining hop limit) decremented by each router that forward the packet.	- **HST** (header sub-type of the GeoNetworking) ★ - **TC** (Traffic Class) represents facility layer requirements on packet transport. - **Flags** indicate whether the ITS-S is mobile or stationary. - **PL** length of the GeoNetworking payload.	

Packet descriptions

GUC	*TSB*	*SHB*	*GBC/GAC*	*BEACON*
The non-area forwarding algorithms are used to route a packet towards a destination. It is executed by a GeoAdhoc router to relay a packet to the next hop. Cf. Greedy and CBF algorithms.	Forwarder is also always a receiver.	SHB packets are not forwarded.	In GBC, a forwarder inside the target area acts also always as a receiver.	Beaconing is used to periodically advertise a GeoAdhoc router's position vector to its neighbors. A BEACON packet shall be sent periodically, advertising its GN address and its current position, speed, heading, station type, and so on, to all its direct neighbors, unless the GeoAdhoc router sends another GeoNetworking packet that carries the GeoAdhoc router's EPV. However, this beaconing algorithm generates some network overhead. The higher beacon frequency, the fresher information in the LT, but also the higher network overhead. Nevertheless, the GN standard proposes to reset the beacon timer whenever a GN packet is sent with the goal of reducing the network overhead produced by the beaconing algorithm.

Packet handling – source operations

	GUC	*TSB*	*SHB*	*GBC/GAC*	*BEACON*
Create GN-PDU with packet header.					
Check whether the entry of the PV for DE in its LocT is valid.	If not, invoking the location service.				
Check no neighbor exists (LocT does not contain a LocTE with the IS_NEIGHBOUR flag set to TRUE). Packet buffered in the …	UC forwarding packet buffer.	BC forwarding packet buffer.	BC forwarding packet buffer.	BC forwarding packet buffer.	
Execute the forwarding algorithm ▲	0 UNSPECIFIED 1 **GREEDY** 2 **CBF**			**Selection procedure**	
If `itsGnSecurity` Enabled : - Send a service primitive SN-ENCAP.request					

- Process the service primitive SN-ENCAP.confirm					
Optional Repetition interval parameter in GN-DATA.request is set: - Save the packet. - Retransmit the packet with a period in Repetition interval until the maximum repetition time of the packet is expired.					
Execute media-dependent procedures. If the communication profile parameter of GN-DATA.request is: - UNSPECIFIED: omit this operation - ITS-G5: ETSI TS 102 636-4-2 [5]					
Pass the GN-PDU to the LL protocol entity via the IN interface and set the destination address to the broadcast address of the LL entity.					
Initialize the timer for the periodic transmission			Reset the beacon timer		If it expires cf. p.43

GeoAdhoc router receives a LS Request GN_ADDR field in the LS Request header does not match its GN_ADDR → procedure = TSB

Packet handling – Forwarder operations

	GUC	*TSB*	*GBC/GAC*
Basic header processing			
Common header processing			
Function F(x,y) ▲			F(x,y) < 0: - 0 UNSPECIFIED - 1 **GREEDY** F(x,y) ≥ 0: - 0 UNSPECIFIED - 1 **SIMPLE**
Execute DPD ▲	If greedy or unspecified		
Execute DAD			
Check if the LocTE exists ▲			
Check the DE LocTE (cf. p. 50-51)			
Flush packet buffers ▲			
Decrement the RHL value ★			
Check no neighbor exists	Packet buffered in the UC forwarding packet buffer.		
Execute forwarding algorithm. ▲	0 UNSPECIFIED 1 GREEDY 2 CBF		**Selection procedure**
Execute media-dependent procedures.			
Pass the GN-PDU to the LL protocol entity via the IN interface and set the destination address to the broadcast address of the LL entity.			

GeoAdhoc router receives a LS Request packet and the Request GN_ADDR field in the LS Request header does not match its GN_ADDR → procedure = GUC

Packet handling – receiver operations

	GUC	*SHB*	*BEACON*
Basic header processing	▨	▨	▨
Common header processing	▨	▨	▨
Function F(x,y)			
Execute DPD ▲	▨		
Execute DAD	▨	▨	▨
Update the PV in the SO LocTE		▨	▨
Update the PDR in the SO LocTE ▲		▨	▨
Set the IS_NEIGHBOUR flag of the SO LocTE to TRUE		▨	▨
Check if the LocTe (SO) exists ▲	▨		
Flush packet buffers ▲	▨	▨	▨
Pass the GN-PDU to the upper protocol entity by means of a service primitive GN-DATA.indication	▨	▨	

NH Next Header field

Basic header

★

0	ANY (unspecified)
1	Common header
2	Secured Packet 1- Execute the SN-DECAP service. 2- Process the service primitive SN-DECAP.confirm. 3- Report a. SUCCESS b. !=SUCCES i. If constant = 0 → discard ii. If constant = 1 → Pass the payload to the upper protocol entity (GN-DATA.indication)

Common header

★

0	ANY (unspecified)
1	BTP-A (interactive packet transport)
2	BTP-B (non-interactive packet transport)
3	IPv6

H(S)T Header (Sub) Type

★

0	ANY
1	BEACON
2	**GEOUNICAST**
3	GEOANYCAST
4	**GEOBROADCAST**
5	TSB
6	LS

Most common

In ***geo-unicast***, the destination of the packet is a node located at a specific position. The packet is forwarded hop by hop towards the position of the destination and delivered to that specific node. **GREEDY** or **CBF** algorithm.

With ***geo-broadcast*** delivery, a packet targets all nodes inside a specific geographic area. The *geo-broadcast* packet is first forwarded like a *geo-unicast packet* (using the **GREEDY** forwarding algorithm) until it reaches the target zone. Then, the *geo-broadcast* packet is delivered to all nodes within the destination area by **SIMPLE** flooding. The packet is first geo-routed to a target geographic zone, and then delivered to all nodes located inside the destination area.

TC Traffic Class

Represents facility layer requirements on packet transport. Default value is set by the GN protocol constant.

SCF (Store Carry Forward)	**Channel Offload**	**TC ID**
Indicates whether the packet shall be buffered when no suitable neighbor exists.	Indicated whether the packet may be offloaded to another channel.	Cf. media-dependent part

RHL Remaining Hop Limit

Forwarders decrement RHL by one.

- If RHL = 0 discard the packet
- If RHL > 0 update the field of the basic header

1	- Packet Transport Type in the GN-DATA.request is SHB. - Header type is 1 → BEACON.
Value of MHL (Maximum hop limit)	From service primitive GN-DATA.request.
GN protocol constant	GN protocol constant `itsGnDefaultHopLimit`

DPD Duplicate packet Detection

A GeoAdhoc router may receive multiple copies of the same packet. Reasons for packet duplications may be the forwarding of the packet from multiple GeoAdhoc routers, routing loops, misconfiguration or replay of packets from misbehaving GeoAdhoc routers. In order to control the forwarding of duplicate packets, the GeoNetworking protocol uses mechanisms for duplicate packet detection (DPD) based on sequence number.

A GeoAdhoc router maintains a duplicate packet list DPL(GN_ADDR, list with sequence numbers and counter that indicates how often the packet with a particular sequence number has already been received from the source) for every entry in its LocT.

PDR Packet Data Rate

Packet rate and geographical area size control is executed in the GeoNetworking forwarding process. A GeoAdhoc router shall maintain the Exponential Moving Average (EMA) of the packet data rate PDR for every LocTE.

$$PDR = \beta \times PDR_{t-1} + (1-\beta) \times x_t$$

Geographical area size control

If the geographical area size carried in a GBC or GAC packet exceeds the maximum value specified in the GN protocol constant `itsGnMaxGeoAreaSize`, the GeoNetworking packet shall not be sent by the source and shall not be forwarded by the forwarder.

Flush packet buffer (SO LS packet buffer and SO UC forwarding packet buffer)

- If LS_pending(SO) is TRUE:
    - forward the stored packets and remove them from the SO LS packet buffer
    - Set LS_pending(SO) to false
- If the UC forwarding packet buffer for SO is not empty, flush UC forwarding packet buffer and forward the stored packets.

Forwarding algorithm

The procedure utilizes the function F(x,y) in order to determine whether the GeoAdhoc router is located inside, at the border or outside the geographical target area carried in the GeoBroadcast or GeoAnycast packet header.

F(x,y):

- =1 → for x=0 and y=0 (at the center point)
- >0 → inside the geographical area
- =0 →at the border of the geographical area
- <0 outside the geographical area

Returns:

- The broadcast LL address BCAST
- The LL address of the next hop NH_LL_ADDR
- 0 →the packet is buffered.
- -1 → the packet is discarded.

Types

	GUC	*TSB*	*SHB*	*GBC/GAC*	*BEACON*	*LS request*	*LS reply*
Basic header	■	■	■	■	■	■	■
Common header	■	■	■	■	■	■	■
SN	■	■		■		■	■
Reserved	■	■		■		■	■
SO PV (long position vector containing the position of the source)	■	■	■	■	■	■	■
DE PV (short position vector containing the position of the destination)	■						■
Midia-dependent data	■		■				
GeoAreaPos Latitude (latitude for the center position of the geometric shape, micro degree)				■			
GeoAreaPos Longitude (longitude for the center position of the geometric shape, micro degree)				■			
Distance a (radius, meters)				■			
Distance b (meters)				■			
Angle (of the geometric shape, degrees)				■			
Reserved				■			
Request GN_ADDR (network address for the GeoAdhoc router entity)						■	

Address

Every GeoAdhoc router shall have a unique GeoNetworking address. It identifies the communicating entities.

To ensure the uniqueness of GeoNetworking address, DAD Duplication Address Detection, is applied.

GeoNetworking address format:

M 1 bit Manually (1) or initial (0) address	ST 5 bits Identify the ITS-S type (tram, cyclist…)	Reserved 10 bits	MID 48 bits Represents LL_ADDR (access layer address)

DAD Duplicate address detection

1- Upon reception of a GeoNetworking packet, the router compares:
   a. Its local GN_ADDR and GN_ADDR of the so carried
   b. Its local link layer address (in the MID field) with the sender link layer address

If a conflict is detected the protocol shall request a new MID field.
In case the MID changes the MAC address should also be changed

Address configuration

Auto-address configuration

`itsGnLocalAddrConfMethod` set to 0.

Managed address configuration

`itsGnLocalAddrConfMethod` set to 1.

With managed address configuration, the ITS Networking Layer Management entity is responsible for providing the MID field of the GeoAdhoc router address GN_ADDR.

The update of the MIB field of the local GN_ADDR may be triggered by:

- The GeoAdhoc router
  The router should use GN-MGMT.request
  then ITS GN-MGMT.response
- The ITS Networking Layer Management entity.
  Unsolicited GN-MGMT.response

Anonymous address configuration

`itsGnLocalAddrConfMethod` set to 2.

This method allows for configuration of anonymous addresses controlled by the security entity.

At startup, the GeoAdhoc router shall execute:

1- Subscribe to the IDCHANGE-SUBSCRIBE service provided by the security entity.
2- SN-IDCHANGE-SUBSCRIBE.confirm
3- SN-IDCHANGE-EVENT.indication
4- SN-IDCHANGE-EVENT.response

Security and privacy

- Digital signatures
- Encryption
- Consistency and plausibility checks
- Hop counts
- Lifetime
- Geo area
- Data rate
- Pseudonyms (anonymous address)
- Cryptographic protection (constant `itsGnSecurity`)

LOCT Location Table

Local data structure contains information about other ITS-S. Entries are added with a lifetime constant. Due to the high mobility of vehicles in the VANET, the LT information may become obsolete quickly, so every LT entry has a lifetime. An entry is removed when the lifetime expires. The LT entry lifetime also has an impact on the performance of the GN protocol.

- GeoNetwork address
- LL address of the ITS-S
- Type of ITS-S
- Version of the GeoNetworking protocol
- PV (Position Vector)
- Flag LS_PENDING indicating that a LS (Location service) is in progress
- Flag LS_NEIGHBOUR indicating that the GeoAdhoc router is in direct communication range, is a neighbor.
- DPL (Duplicate Packet List)
- TST (Timestamp)
- PDR (Packet Data Rate) as EMA (Exponential Moving Average)

Check LocTE

Doesn't exist	*Exists*
- Create PV(SO) in the LocT. - Set the IS_NEIGHBOUR flag to false. - Update PDR(SO) in the LocT.	- Update PV(SO) with the SO PV fields of the GUC Extended header - Update PDR(SO) in the LocT

EPV Ego Position Vector

Contains at least:

- POS_EPV: geographical position
- S_EPV: speed
- H_EPV: heading
- TST: when POS_EPV was generated
- PAI_EPV: accuracy of the geographical position

Updated with a frequency of the GN protocol constant.

For position update, the ITS Networking and Transport Layer Management entity shall send an unsolicited GN-MGMT.response with the EPV parameter.

PV Short and Long Position Vectors

The position vector update is executed in the GeoNetworking forwarding process when a PV in a LocTE is updated by PV carried in a GeoNetworking packet header. The algorithm ensures that always the newer PV is used indicated by the timestamp that is contained in the PV.

Long Position Vectors	*Short Position Vectors*
- GN_ADDR: network address for the GeoAdhoc router entity - TST (Timestamp) in milliseconds at which time latitude and longitude of the ITS-S were acquired by the router. - Lat - Long	- GN_ADDR: network address for the GeoAdhoc router entity - TST (Timestamp) in milliseconds at which latitude and longitude of the ITS-S were acquired by the router. - Lat

- PAI: Position accuracy indicator - S: speed - H: heading of the GeoAdhoc router	- Long

SN Sequence Number

Each GeoAdhoc router shall maintain a local sequence number that determines the Sequence Number (SN) field of the next GeoNetworking packet to be transmitted.

$$SN(P) = (SN(P)+1) \%SN\_MAX$$

Single hop does not carry SN. *Examples:* Beacon, SHB.

LS Location Service

To discover the position of another ITS station, for instance when sending a geo-unicast packet to a destination that is not in the LT, the source node uses the Location Service (LS). The location service is used if a GeoAdhoc router needs to determine the position of another GeoAdhoc router. The location service is based on the exchange of control packets between GeoAdhoc routers.

LS packet buffer

The LS buffer is used to store packets while the LS resolves the geographic position of a destination node.

GeoAdhoc router shall queue a GeoNetworking packet in a LS packet buffer for the sought destination **until the LS is completed.**

- *Queued at the tail.*
- *Head Drop*: When buffer overflows, packets from the head of the queue are removed and the new packet is queued at the tail.
- *Flushed*: when the LS is completed
- *Discard*: when queuing time exceeds the packet lifetime (LT field) or LS does not complete.
- *Send:* LT field is reduced by the queuing time in the LS packet buffer.

LS packet handling

LS request

When a source has a T/GN6-SDU to send and has no position vector information for the destination address, the source shall invoke the location service and shall execute the following operations:

- Check whether a LS for the sought GN_ADDR is in progress, i.e. the flag LS_pending is set TRUE
- Create a GN-PDU with T/GN6-SDU as payload and a TSB packet header
- If `itsGnSecurity` Enabled :
    - Send a service primitive SN-ENCAP.request
    - Process the service primitive SN-ENCAP.confirm
- Execute media-dependent procedures.
- Start a timer T_{LS, GN_ADDR}.
- Initialize the LS retransmit counter for the GeoAdhoc router GN_ADDR RTC_{LS, GN_ADDR} to 0
- Add a LocTE for the sought GN_ADDR and set the flag `LS_pending` to TRUE.
- Pass the GN-PDU to the LL protocol entity via the IN interface and set the destination address to the Broadcast address of the LL entity.

LS request re-transmission

If the source node does not receive a LS reply packet, it continues sending LS request packets each LS retransmission interval until it receives a LS reply packet or the retransmission counter reaches the maximum LS retransmissions. If the timer $T_{LS,\ GN\_ADDR}$ expires the source shall execute the following operations:

- Check the retransmit counter $RTC_{LS,\ GN\_ADDR}$
    - RTC < maximum number of LS retransmissions set by the GN constant
        - re-issue a LS request packet
        - re-start the time $T_{LS,\ GN\_ADDR}$
        - increment the retransmit counter $RTC_{LS,\ GN\_ADDR}$
    - RTC ≥ maximum number of LS retransmissions set by the GN constant the router:
        - Remove the pending packets for the sought GN_ADDR from the LS packet buffer
        - Remove the LocTE for the sought GN_ADDR

LS reply

When the source node receives the LS reply packet, it creates a new entry in the LT for the destination node, which will be valid until its lifetime expires. If the source receives a LS Reply packet for the sought GN_ADDR, the source shall execute:

- Basic header processing
- Common header processing
- Execute DPD
- Update PV
- Update PDR
- Flush the LS packet buffer
- Flush packet buffers
- Set the flag LS_pending for the sought GN_ADDR to false
- Stop the timer $T_{LS,\ GN\_ADDR}$
- Reset the re-transmit counter $RTC_{LS,\ GN\_ADDR}$

LS forwarding

Cf. ***Packet handling – Forwarder operations*** part.

LS destination operations

On reception of a LS Request packet, the GeoAdhoc router shall check the Request GN_ADDR field. If this MID field matches the MID field of its GN_ADDR, the GeoAdhoc router shall execute:

- Basic header processing
- Common header processing
- Execute DPD
- Execute DAD
- Check LocTE(SO)
- Create a GN-PDU with a GUC packet header
- Forwarding algorithm
- Optional Security profile
- Execute media dependent procedures
- Pass the GN-PDU to the LL protocol entity via the IN interface and set the destination address to the LL address of the next hop LL_ADDR_NH

Forwarding packet buffer

The GN protocol defines multiple packet buffers: A LS buffer, a unicast buffer, a broadcast buffer and a CBF buffer (used if CBF is enabled).

To temporarily keep packets in a GeoAdhoc router **during the forwarding process**. A GeoAdhoc router shall maintain the following forwarding packet buffer:

- UC forwarding packet buffer GUC packets per GN_ADDR.
- BC forwarding packet buffer to buffer TSB, GBC dans GAC packets.

The unicast and broadcast buffers are useful to store geo-unicast and geo-broadcast packets when the forwarding algorithm fails finding a valid neighbor to route the packet towards the destination. These buffers are flushed when the LT is updated with information about packets' destination, so packets can be forwarded. Storing packets into buffers avoids dropping them when there are no valid neighbors due to temporal disconnections among nodes of the VANET, which is more likely in low density scenarios.

Those two buffers work the same way as LS packet buffer.

Non-area forwarding algorithm

It is used to route a packet towards a destination. It is executed by a GeoAdhoc router to relay a packet to the next hop.

GF Greedy forwarding algorithm

The GeoAdhoc router uses the location information of the destination carried in the GN packet header and selects one of the neighbors as the next hop.

The algorithm applies the most forward within radius (MFR) policy, which selects the neighbor with the smallest geographical distance to the destination, thus providing the greatest progress when the GN packet is forwarded.

Returns:

- The LL address of the next hop NH_LL_ADDR
- 0 → the packet is buffered.

If no suitable neighbor exists, the packet has reached a local optimum and the result '0' is returned indicating that no forwarder could be found.

CBF Contention Based Forwarding algorithm.

A receiver decides to be a forwarder of a GN packet. This is contrary to the sender-based forwarding scheme where the sender determines the next hop.

The CBF algorithm utilizes timer-based re-broadcasting with overhearing of duplicates in order to enable an implicit forwarding of a packet by the optimal node. With CBF, the GeoAdhoc router broadcasts the GN packet.

All neighbors, which receive the packet, process it: those routers with a positive progress buffer the packet in the CBF packet buffer and start a timer with a timeout that is inversely proportional to the forwarding progress of the GeoAdhoc router.

Upon expiration of the timer, the GeoAdhoc router re-broadcasts the GN packet. Before the timer expires, the GeoAdhoc router may receive a duplicate of the packet from a GeoAdhoc router with a shorter timeout, i.e. with a smaller distance to the destination. In this case, the GeoAdhoc router inspects its CBF packet buffer, stops the timer and removes the GN packet from the CBF packet buffer.

Returns:

- The broadcast LL address BCAST
- 0 →the packet is buffered.
- -1 → the packet is discarded

Area forwarding algorithm

The area forwarding algorithms assume that the sender of the data packet is located inside or at the border of the target area. If this is not the case, the packet can be transported from the sender towards the target area using non-area forwarding algorithms.

Simple geo-broadcast forwarding algorithm

The packet is re-broadcasted.

returns:

- The broadcast LL address BCAST

Contention based

Like the non-area contention-based forwarding algorithm, with the area contention-based forwarding (CBF) algorithm, a receiver decides to be a forwarder of a GN packet. But the definition of the distance is different from the non-area CBF algorithm, where the distance is the forwarding progress between the GeoAdhoc router's local position and the destination position.

Returns:

- The broadcast LL address BCAST
- The LL address of the next hop NH_LL_ADDR
- 0 →the packet is buffered.
- -1 → the packet is discarded

Advanced

Includes mechanisms from the Greedy Forwarding (GF) algorithm and the area contention-based forwarding (CBF) algorithm. As such it is both sender-based and receiver-based. It also includes further enhancements of CBF to improve the efficiency and reliability. At the source, the algorithm selects the next forwarder from its location table, forwards the packet to the neighbor with the greatest progress (GF) and additionally enters CBF mode.

1- CBF is used to deal with uncertainties in terms of reception failure caused by mobility of ITS-S, fading phenomena and collisions on the wireless medium.
2- In order to minimize the additional forwarding delay introduced by CBF, CBF is complemented with the selection of one specific forwarder, referred to as next hop, at the sender
3- The efficiency of CBF is improved by choosing potential forwarders only from a specific sector of the circular forwarding area; i.e. GeoAdhoc routers located inside the sector (defined by an angle and the maximum communication range) refrain from retransmission of the packet (sectorial backfire).
4- The reliability of the dissemination process is increased by a controlled packet retransmission scheme within the geographical target area.

In order to increase the reliability of the dissemination process by controlled packet retransmission, a GeoAdhoc router in CBF mode maintains a counter for the number of re-transmissions for a packet. This counter is incremented every time this packet is received. When the number of re-transmissions for this packet reaches a threshold, the GeoAdhoc router stops contending for the packet. By this mechanism, the packet is allowed to be re-transmitted several times for better reliability, but the data overhead is controlled.

Returns:

- The broadcast LL address BCAST
- The LL address of the next hop NH_LL_ADDR
- 0 →the packet is buffered.
- -1 → the packet is discarded.

GeoNetworking data services

The GN data service primitives allow entities of ITS transport protocols to send and receive PDUs via the GN_SAP.

GN-DATA.request

It is used by the ITS transport protocol entity to request sending a GeoNetworking packet. Upon reception of the service primitive GN-DATA.request, the GeoNetworking protocol delivers the GeoNetworking packet to the LLC protocol entity via the IN_SAP.

GN-DATA.confirm

It is used to confirm that the GeoNetworking packet was successfully processed in response to a GN-DATA.request. For the reception of the primitive, no behavior is specified. The ResultCode parameter specifies whether the service primitive GN-DATA.request is:

- accepted
- rejected due to
  - maximum length exceeded if the size of the T/GN6-PDU exceeds the GN protocol constant `itsGnMaxSduSize`
  - maximum lifetime exceeded if the lifetime exceeds the maximum value of the GN protocol constant `itsGnMaxPacketLifetime`
  - repetition interval too small, if the repetition interval is smaller than the GN protocol constant `itsGnMinPacketRepetitionInterval`
  - unsupported traffic class
  - geographical area exceeds the maximum geographical area size in the GN protocol constant `itsGnMaxGeoAreaSize`
  - unspecified reasons if the service primitive GN-DATA.request cannot be accepted for any other reason.

GN-DATA.indication

Indicates to an upper protocol entity that a GeoNetworking packet has been received

GeoNetworking management services

The GN management service primitives allow the ITS Networking & Transport Layer Management entity to update position, time and GeoNetworking address of the GeoAdhoc router.

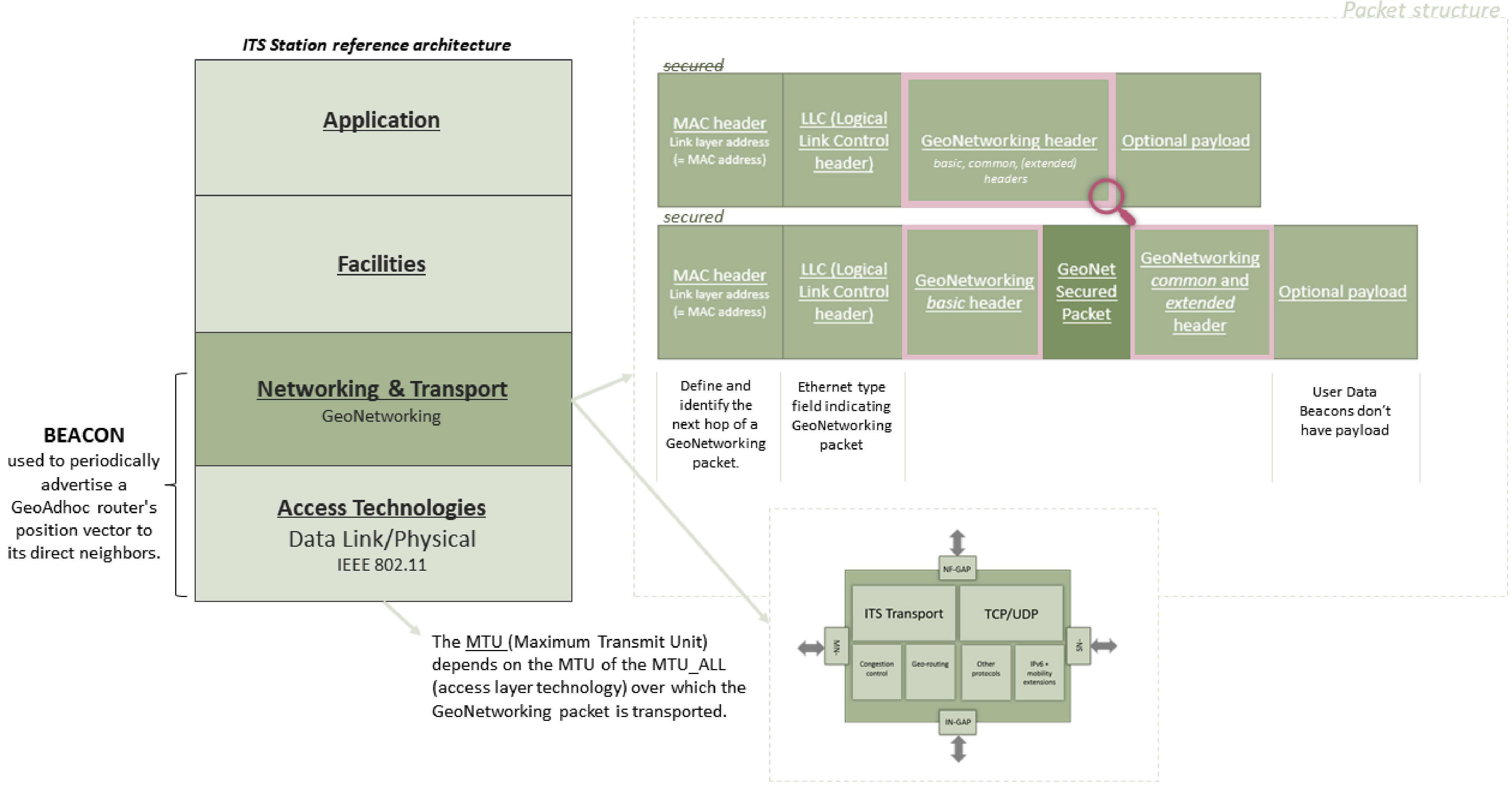
GN-MGMT.request

Generated by the GeoNetworking protocol at the initialization phase in order to request management information, i.e. time, position vector, GeoNetworking address, TC mapping. After receiving the service primitive GN-MGMT.request, the ITS Networking & Transport Layer Management entity is in charge of providing the GeoNetworking entity with the requested management information.

GN-MGMT.response

Generated by the ITS Networking & Transport Layer Management entity to indicate an update of management information, i.e. time, position vector, GeoNetworking address and TC mapping. The service primitive can be triggered upon reception of a GN-MGMT.request primitive or can be generated unsolicited, i.e. without a service primitive GN-MGMT.request.

GeoNetworking protocol



ITS Station reference architecture

Application

Facilities

Networking & Transport
GeoNetworking

Access Technologies
Data Link/Physical
IEEE 802.11

BEACON
used to periodically advertise a GeoAdhoc router's position vector to its direct neighbors.

The MTU (Maximum Transmit Unit) depends on the MTU of the MTU_ALL (access layer technology) over which the GeoNetworking packet is transported.

Packet structure

~~secured~~

MAC header
Link layer address (= MAC address)

LLC (Logical Link Control header)

GeoNetworking header
basic, common, (extended) headers

Optional payload

secured

MAC header
Link layer address (= MAC address)

LLC (Logical Link Control header)

GeoNetworking *basic* header

GeoNet Secured Packet

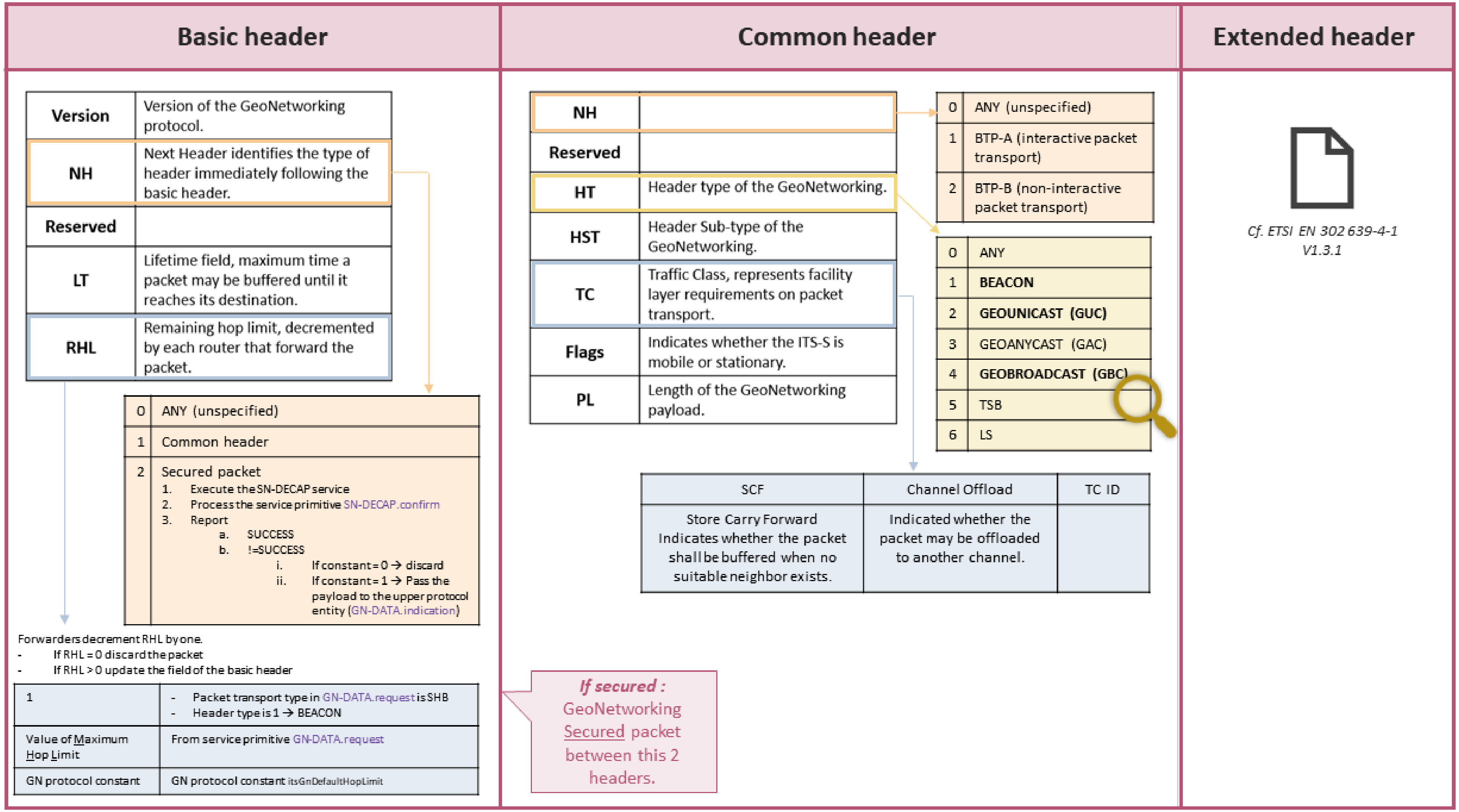
GeoNetworking *common* and *extended* header

Optional payload

Define and identify the next hop of a GeoNetworking packet.

Ethernet type field indicating GeoNetworking packet

User Data
Beacons don't have payload



Basic header

Version	Version of the GeoNetworking protocol.
NH	Next Header identifies the type of header immediately following the basic header.
Reserved	
LT	Lifetime field, maximum time a packet may be buffered until it reaches its destination.
RHL	Remaining hop limit, decremented by each router that forward the packet.

0	ANY (unspecified)
1	Common header
2	Secured packet 1. Execute the SN-DECAP service 2. Process the service primitive SN-DECAP.confirm 3. Report a. SUCCESS b. !=SUCCESS i. If constant = 0 → discard ii. If constant = 1 → Pass the payload to the upper protocol entity (GN-DATA.indication)

Forwarders decrement RHL by one.

- If RHL = 0 discard the packet
- If RHL > 0 update the field of the basic header

1	- Packet transport type in GN-DATA.request is SHB - Header type is 1 → BEACON
Value of Maximum Hop Limit	From service primitive GN-DATA.request
GN protocol constant	GN protocol constant itsGnDefaultHopLimit

Common header

NH	
Reserved	
HT	Header type of the GeoNetworking.
HST	Header Sub-type of the GeoNetworking.
TC	Traffic Class, represents facility layer requirements on packet transport.
Flags	Indicates whether the ITS-S is mobile or stationary.
PL	Length of the GeoNetworking payload.

0	ANY (unspecified)
1	BTP-A (interactive packet transport)
2	BTP-B (non-interactive packet transport)

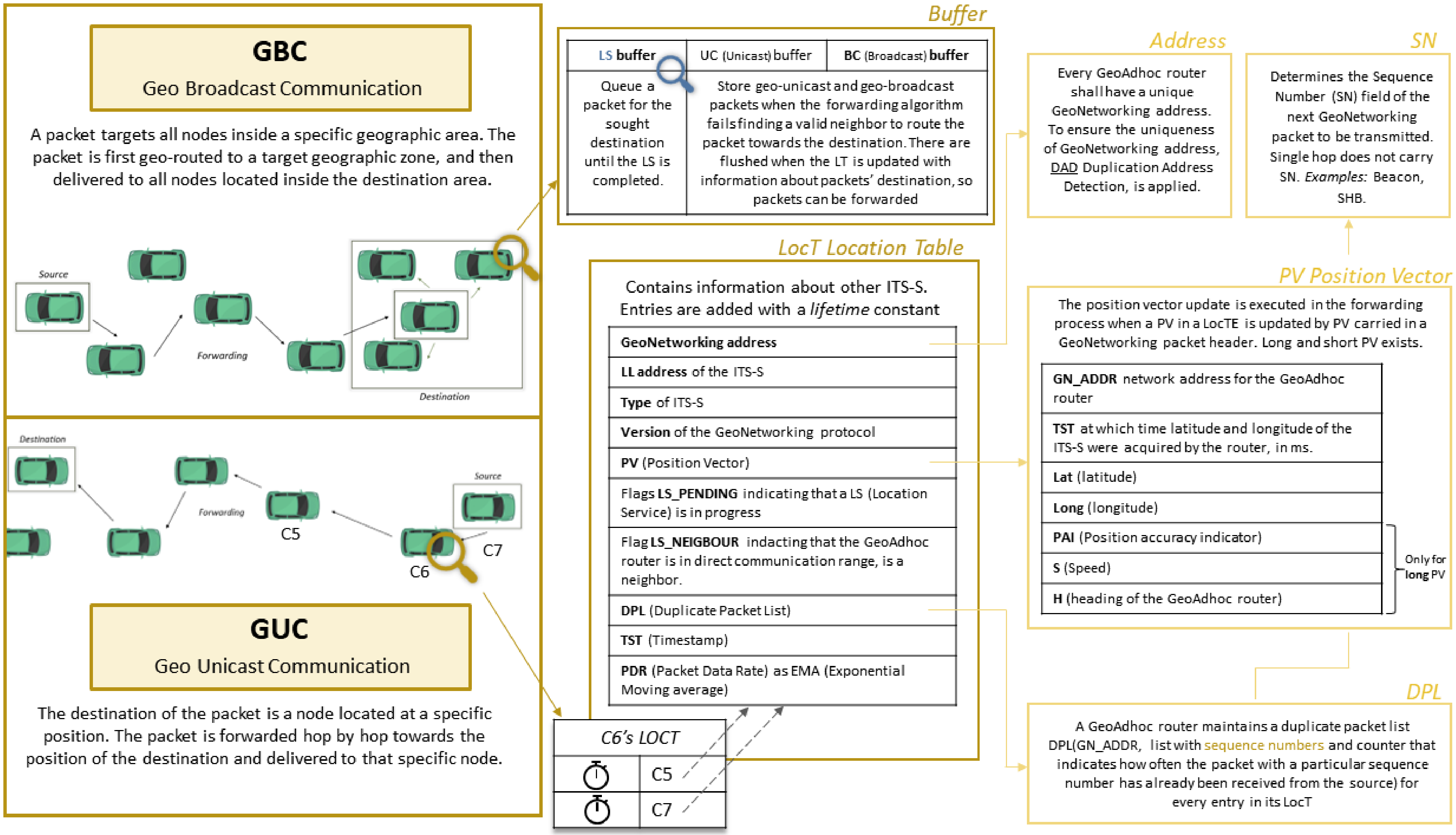
0	ANY
1	**BEACON**
2	**GEOUNICAST (GUC)**
3	GEOANYCAST (GAC)
4	**GEOBROADCAST (GBC)**
5	TSB
6	LS

SCF	Channel Offload	TC ID
Store Carry Forward Indicates whether the packet shall be buffered when no suitable neighbor exists.	Indicated whether the packet may be offloaded to another channel.	

If secured : GeoNetworking Secured packet between this 2 headers.

Extended header

Cf. ETSI EN 302 639-4-1 V1.3.1



GBC

Geo Broadcast Communication

A packet targets all nodes inside a specific geographic area. The packet is first geo-routed to a target geographic zone, and then delivered to all nodes located inside the destination area.

GUC

Geo Unicast Communication

The destination of the packet is a node located at a specific position. The packet is forwarded hop by hop towards the position of the destination and delivered to that specific node.

Buffer

LS buffer	UC (Unicast) buffer	**BC** (Broadcast) **buffer**
Queue a packet for the sought destination until the LS is completed.	Store geo-unicast and geo-broadcast packets when the forwarding algorithm fails finding a valid neighbor to route the packet towards the destination. There are flushed when the LT is updated with information about packets' destination, so packets can be forwarded	

LocT Location Table

Contains information about other ITS-S. Entries are added with a *lifetime* constant

GeoNetworking address
LL address of the ITS-S
Type of ITS-S
Version of the GeoNetworking protocol
PV (Position Vector)
Flags **LS_PENDING** indicating that a LS (Location Service) is in progress
Flag **LS_NEIGBOUR** indacting that the GeoAdhoc router is in direct communication range, is a neighbor.
DPL (Duplicate Packet List)
TST (Timestamp)
PDR (Packet Data Rate) as EMA (Exponential Moving average)

C6's LOCT	
⏱	C5
⏱	C7

Address

Every GeoAdhoc router shall have a unique GeoNetworking address. To ensure the uniqueness of GeoNetworking address, DAD Duplication Address Detection, is applied.

SN

Determines the Sequence Number (SN) field of the next GeoNetworking packet to be transmitted. Single hop does not carry SN. *Examples:* Beacon, SHB.

PV Position Vector

The position vector update is executed in the forwarding process when a PV in a LocTE is updated by PV carried in a GeoNetworking packet header. Long and short PV exists.

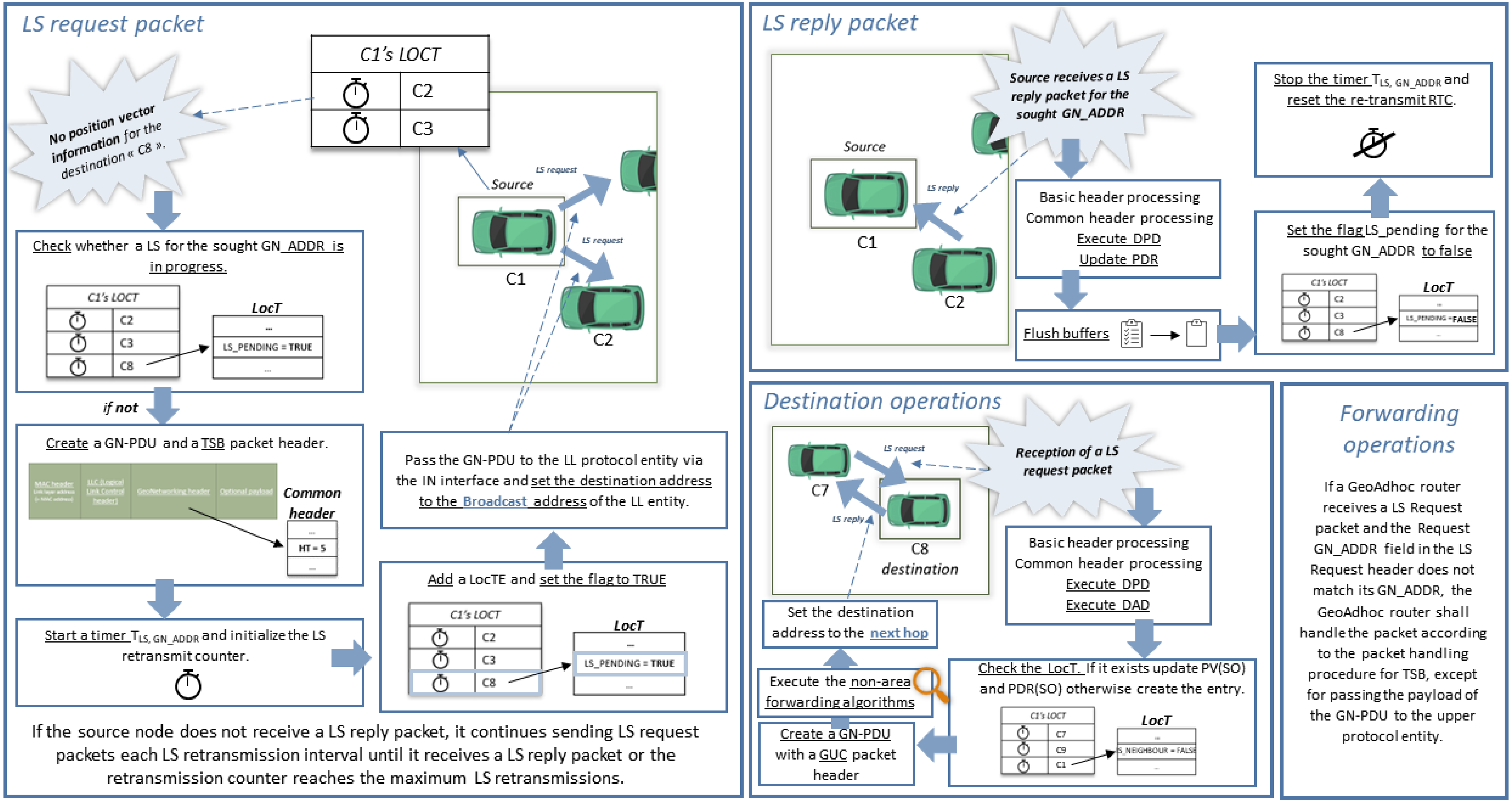
GN_ADDR network address for the GeoAdhoc router	
TST at which time latitude and longitude of the ITS-S were acquired by the router, in ms.	
Lat (latitude)	
Long (longitude)	
PAI (Position accuracy indicator)	Only for long PV
S (Speed)	
H (heading of the GeoAdhoc router)	

DPL

A GeoAdhoc router maintains a duplicate packet list DPL(GN_ADDR, list with sequence numbers and counter that indicates how often the packet with a particular sequence number has already been received from the source) for every entry in its LocT

Location Service

To **discover the position** of another ITS station, for instance when sending a geo-unicast packet to a destination that is not in the LT, the source node uses the Location Service (LS). Based on the exchange of control packets between GeoAdhoc routers.



LS request packet

No position vector information for the destination « C8 ».

Check whether a LS for the sought GN_ADDR is in progress.

if not

Create a GN-PDU and a TSB packet header.

Start a timer $T_{LS,\ GN\_ADDR}$ and initialize the LS retransmit counter.

Add a LocTE and set the flag to TRUE

Pass the GN-PDU to the LL protocol entity via the IN interface and set the destination address to the Broadcast address of the LL entity.

If the source node does not receive a LS reply packet, it continues sending LS request packets each LS retransmission interval until it receives a LS reply packet or the retransmission counter reaches the maximum LS retransmissions.

LS reply packet

Source receives a LS reply packet for the sought GN_ADDR

Basic header processing
Common header processing
Execute DPD
Update PDR

Flush buffers

Set the flag LS_pending for the sought GN_ADDR to false

Stop the timer $T_{LS,\ GN\_ADDR}$ and reset the re-transmit RTC.

Destination operations

Reception of a LS request packet

Basic header processing
Common header processing
Execute DPD
Execute DAD

Check the LocT. If it exists update PV(SO) and PDR(SO) otherwise create the entry.

Create a GN-PDU with a GUC packet header

Execute the non-area forwarding algorithms

Set the destination address to the next hop

Forwarding operations

If a GeoAdhoc router receives a LS Request packet and the Request GN_ADDR field in the LS Request header does not match its GN_ADDR, the GeoAdhoc router shall handle the packet according to the packet handling procedure for TSB, except for passing the payload of the GN-PDU to the upper protocol entity.

Non-area forwarding algorithm

It is used to route a packet towards a destination. It is executed by a GeoAdhoc router to relay a packet to the next hop.

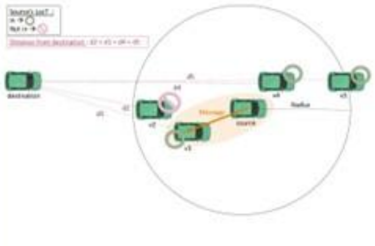
GF Greedy

The GeoAdhoc selects one of the neighbors as the next hop.

The algorithm applies the most forward within radius (MFR) policy, which selects the neighbor with the smallest geographical distance to the destination, thus providing the greatest progress when the GN packet is forwarded.

Returns:

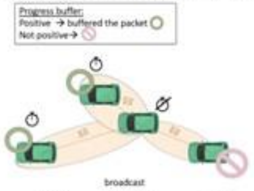
- The LL address of the next hop
- 0 → the packet is buffered



CBF

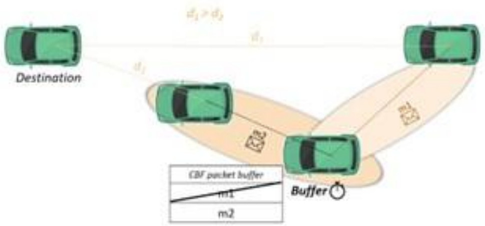
Contention based forwarding

A receiver decides to be a forwarder of a GN packet. With CBF, the GeoAdhoc router broadcasts the GN packet.



All neighbors, which receive the packet, process it: those routers with a positive progress buffer the packet in the CBF packet buffer. Upon expiration of the timer, the GeoAdhoc router re-broadcasts the GN packet.

Before the timer expires, the GeoAdhoc router may receive a duplicate of the packet from a GeoAdhoc router with a shorter timeout, i.e. with a smaller distance to the destination. In this case, the GeoAdhoc router inspects its CBF packet buffer, stops the timer and removes the GN packet from the CBF packet buffer.



Area forwarding algorithm

The area forwarding algorithms assume that the sender of the data packet is located inside or at the border of the target area. If this is not the case, the packet can be transported from the sender towards the target area using non-area forwarding algorithms.

CBF

Like the non area contention-based algorithm, but the definition of the distance is different.

Simple geo-broadcast

The packet is re-broadcasted.

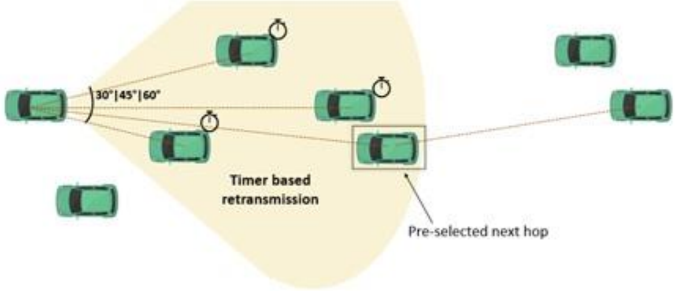
Advanced

CBF is used to deal with uncertainties in terms of reception failure caused by mobility of ITS-S, fading phenomena and collisions on the wireless medium.

In order to minimize the additional forwarding delay introduced by CBF, CBF is complemented with the selection of one specific forwarder, referred to as next hop, at the sender

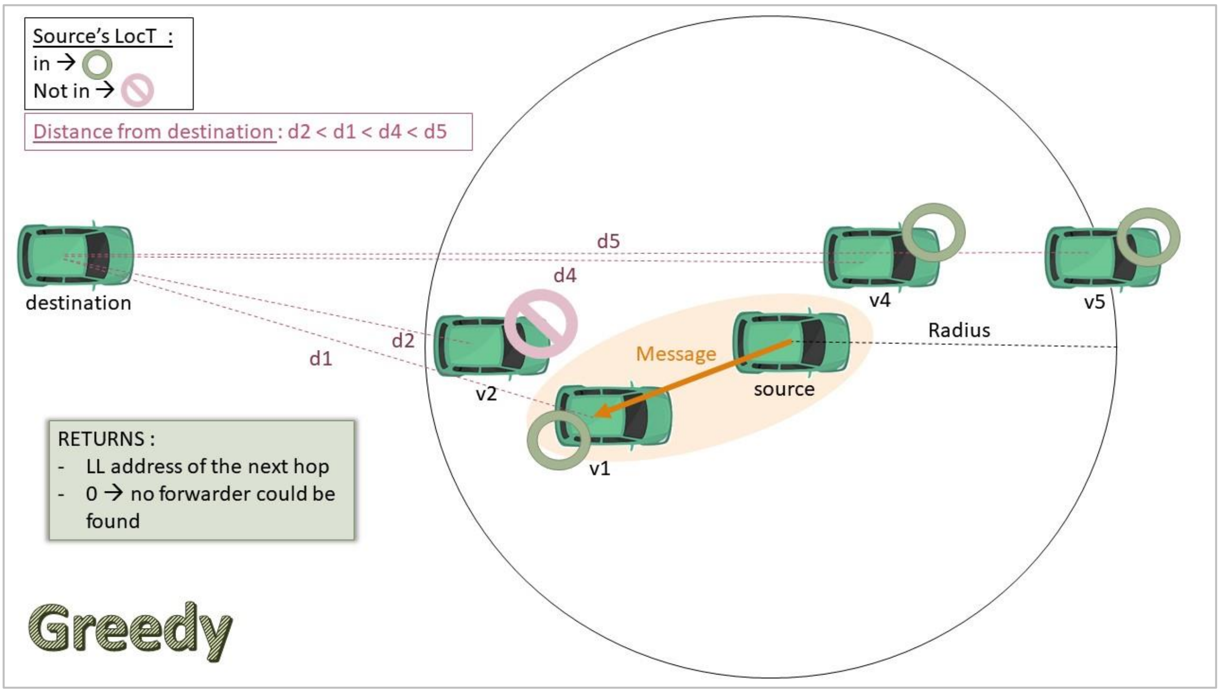
The efficiency of CBF is improved by choosing potential forwarders only from a specific sector of the circular forwarding area; i.e. GeoAdhoc routers located inside the sector (defined by an angle and the maximum communication range) refrain from retransmission of the packet (sectorial backfire).

The reliability of the dissemination process is increased by a controlled packet retransmission scheme within the geographical target area



Zoom sur ces algorithmes ci-après

Non-Area forwarding algorithm



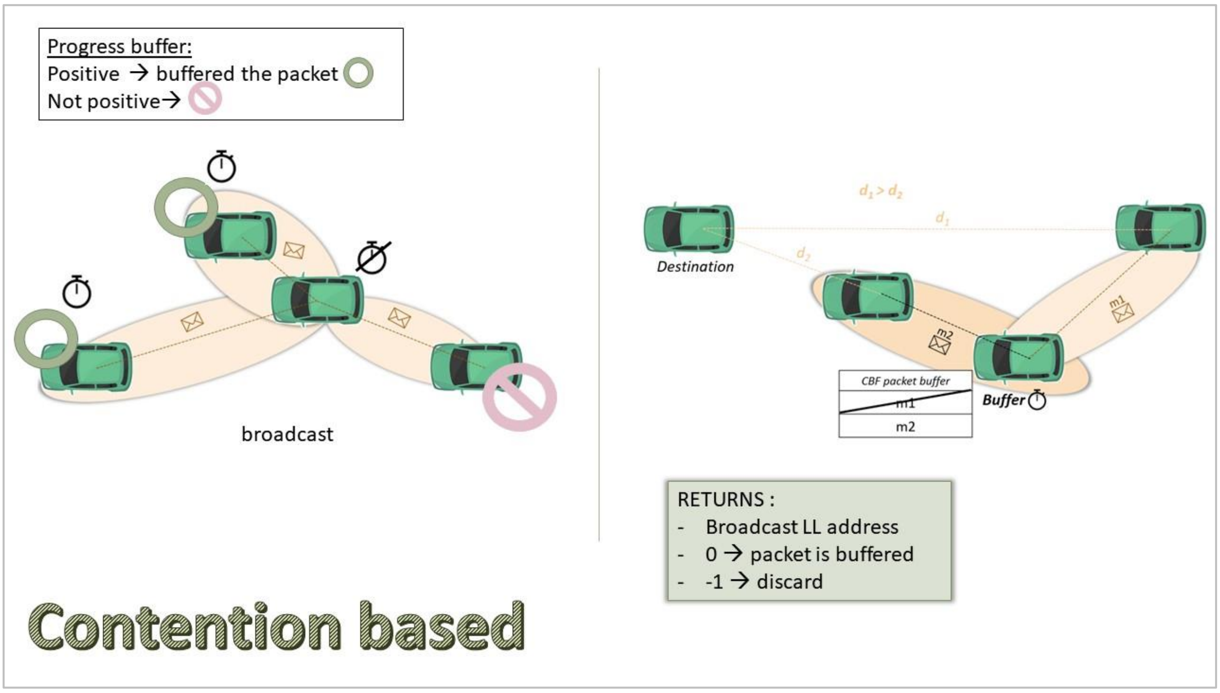
Source's LocT :
in → ○
Not in → 🚫

Distance from destination : d2 < d1 < d4 < d5

RETURNS :

- LL address of the next hop
- 0 → no forwarder could be found

Greedy



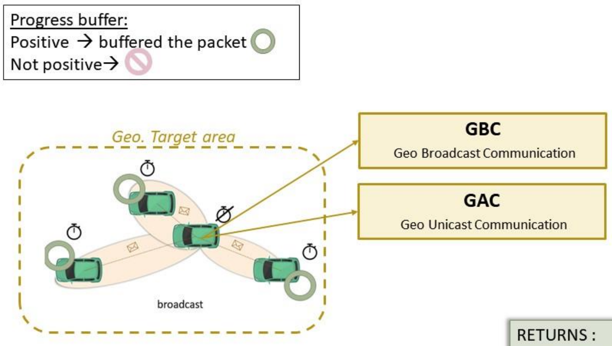
Progress buffer:
Positive → buffered the packet ○
Not positive → 🚫

RETURNS :

- Broadcast LL address
- 0 → packet is buffered
- -1 → discard

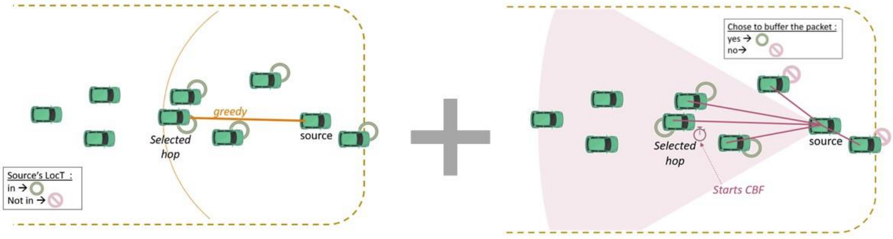
Contention based

Area forwarding algorithm


Progress buffer:
Positive → buffered the packet ○
Not positive→ ⃠
Geo. Target area
broadcast
GBC
Geo Broadcast Communication
GAC
Geo Unicast Communication

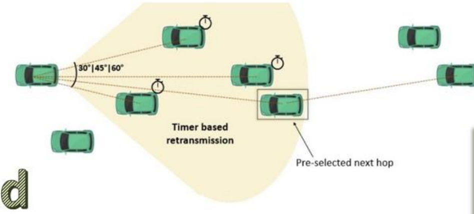
RETURNS :
- Broadcast LL address
- 0 → packet is buffered
- -1 → discard
- LL address of the next hop

Contention based



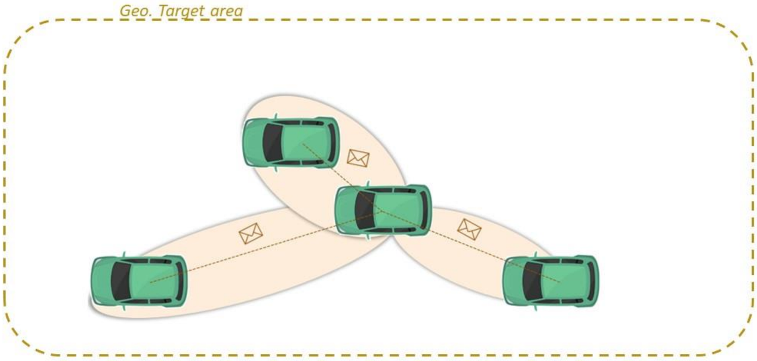
GF

CBF



RETURNS :
- The LL address of the next hop
- The broadcast address
- 0 → packet is buffered
- -1 → packet is discared

Advanced



RETURNS :
- Broadcast LL address

Simple

Bibliography

(hyperlinks)

- (PDF) GyTAR: improved greedy traffic aware routing protocol for vehicular ad hoc networks in city environments (researchgate.net)
- (PDF) An urban location service for vehicular area networks (researchgate.net)
- TS 102 637-2 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service (etsi.org)
- EN 302 637-2 - V1.4.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service (etsi.org)
- Signal Phase And Timing - MAP_v1.1_published_April2016.pdf (randolphtoom.com)
- TS 103 301 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services (etsi.org)
- (PDF) Analysis of V2X Performance and Rollout Status with a Special Focus on Austria (researchgate.net)
- EN 302 637-3 - V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service (etsi.org)