ETSI TR 102 962 V2.1.1 (2026-05)

TECHNICAL REPORT

Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS); Release 2

Reference
RTR/ITS-0078

Keywords
cellular, ITS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 5
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definition of terms, symbols and abbreviations 9
3.1 Terms 9
3.2 Symbols 9
3.3 Abbreviations 9
4 Overview 11
5 C-ITS architecture over cellular networks 11
5.1 ITS communication system architecture and ITS station reference architecture 11
5.2 System architecture of ITS using cellular infrastructure and the Uu interface 13
6 Identification and enhancements of ITS applications and related use cases 15
6.1 Introduction 15
6.2 ETSI ITS Basic Set of Applications 16
6.2.0 Introduction 16
6.2.1 Active road safety and cooperative traffic efficiency use cases 16
6.2.2 Co-operative local services and global internet services use cases 17
6.3 Support to ETSI ITS Basic Set of Applications 18
6.3.1 Introduction 18
6.3.2 Decentralized Event Notification (DEN) Service 18
6.3.3 Cooperative Awareness Service 19
6.3.4 Cooperative Adaptive Cruise Control (CACC) 20
6.3.5 Platooning 20
6.3.6 Vulnerable Road Users (VRU) protection 20
6.3.7 Collective Perception Service (CPS) 21
6.3.8 Maneuver Coordination Service (MCS) 22
6.3.9 Automated Vehicle Marshalling (AVM) 22
6.4 Example implementations and deployments 22
6.4.1 Roadwork warning 22
7 Impacts on ETSI ITS standards for cooperative ITS 23
Annex A: Cellular 4G/5G System and Technical Features Supporting ITS Services 24
A.1 Introduction 24
A.1.0 Overview 24
A.1.1 Quality of Service (priority for ITS information) 24
A.1.2 Cross border (Mobile network change) 24
A.1.3 Latency and distributed computing 24
A.2 ITS backend communications enabling interoperable C-ITS applications 25
A.2.0 Overview 25
A.2.1 Basic network architecture for information sharing among ITS backend systems 26
A.2.2 Evolved network architecture for sharing information between countries/regions 27
A.3 Security and Privacy 28
A.3.0 Introduction 28
A.3.1 System architecture and ecosystem overview 28
A.3.2 Security 29

A.3.2.1 Security within a stakeholder domain 29
A.3.2.2 Security between stakeholder domains 29
A.3.2.3 Credential handling for security domains 30
A.3.2.4 Interaction between different security domains 30
A.3.3 Privacy 30
A.3.4 Further notes on direct V2X and V2N2X 31

Annex B: ITS Message Delivery (Geocast) Solutions 32

B.1 System architecture and end-to-end message flow 32

B.2 ITS message dissemination using IoT messaging protocols, e.g. MQTT 32
B.2.1 System architecture and end-to-end message flow 32
B.2.2 Communication protocol stack 33
B.2.3 Addressability of ITS stations using cellular uplink/downlink communication 34
B.2.3.1 Server address for uplink 34
B.2.3.2 Geocast with MQTT in downlink 34
B.2.4 Security and privacy 34
B.2.5 QoS provision 34

Annex C: Numerical results for CAM and CPM load reduction using prediction error 35

History 37

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Cooperative Intelligent Transport Systems (C-ITS), e.g. as defined in Directive (EU) 2023/2661 [i.6], cover a wide range of different scenarios for road transport with entities in the infrastructure (already existent or newly to be developed), in vehicles, in portable devices, and in ITS backends. C-ITS can be implemented using communication technologies out of multiple classes and benefit from the interoperability at different ISO OSI layers. Different communication technologies may include but not be limited, e.g.:

- Direct communications, also known as ad-hoc communications, e.g. ITS-G5 standardized at ETSI and 3GPP Cellular V2X PC5 interface (LTE PC5 or NR PC5).
- Cellular network communications, e.g. the Uu interface of 3GPP UMTS (3G), LTE (4G), NR (5G), and future generations.
- Non-Terrestrial Network (NTN) communications or satellite communications.

The present document describes the framework of public cellular mobile networks and the usage of 3GPP Uu interface in C-ITS implementations. The focus of the present document is on the standardization activities in ETSI TC ITS to enable interoperability, mainly at the ITS facilities layer, among C-ITS implementations using cellular networks, as well as among C-ITS implementations using different communication technologies.

In the present document, C-ITS refers to the ITS ecosystem implementation in Europe according to the definition and requirements in Directive (EU) 2023/2661 [i.6]. When discussing cellular mobile network functions, features, and supports that are generally applicable to different ITS ecosystem implementations, including but beyond C-ITS, e.g. ITS implementation in other public and private sectors, the term ITS may be used.

1 Scope

The present document is based on an analysis of cooperative ITS (C-ITS) services using public mobile cellular networks for communications between ITS stations, in order to:

- identify related functional requirements on the ITS architecture;
- identify required amendments/modifications of existing standards on ITS, in order to enable usage of public mobile cellular networks.

The result of the investigations is illustrated in the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI TS 103 900 (V2.2.1): "Intelligent Transport Systems (ITS); Facilities Layer; Cooperative Awareness Service; Release 2".

[i.2] ETSI TS 103 831 (V2.3.1): "Intelligent Transport Systems (ITS); Facilities Layer; Decentralized Environmental Notification Service; Release 2".

[i.3] ETSI TR 102 638 (V2.1.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Release 2".

[i.4] ETSI TR 102 962 (V1.1.1): "Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)".

[i.5] ETSI TR 103 630 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Pre-standardization Study on ITS Facility Layer Security for C-ITS Communication Using Cellular Uu Interface".

[i.6] Directive (EU) 2023/2661 of the European Parliament and of the Council of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[i.7] C-Roads Platform: "C-ITS IP Based Interface Profile Version 1.7.0".

NOTE: Document "C-ITS IP Based Interface Profile Version 1.7.0" (which is part of the "Harmonised C-ITS Specifications - Release 1.7").

[i.8] AMQP: "Advanced Message Queuing Protocol".

[i.9] C-Roads Platform: "Working Group 2 Technical Aspects, Task force 2 "Service Harmonization, Common C-ITS Service and Use Case Definitions". Version 1.7.0, June 2020.

[i.10] ETSI TR 103 300-1 (V2.3.1): "Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 1: Use Cases definition; Release 2" .

[i.11] ETSI TR 103 299 (V2.1.1): "Intelligent Transport System (ITS); Cooperative Adaptive Cruise Control (CACC); Pre-standardization study".

[i.12] ETSI TS 103 324: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Collective Perception Service; Release 2".

[i.13] ETSI White Paper No. 11: "Mobile Edge Computing, A key technology towards 5G" (First edition - September 2015).

[i.14] ETSI TS 103 300-3 (V2.1.1): "Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2".

[i.15] ETSI GS MEC 030 (V2.2.1): "Multi-access Edge Computing (MEC); V2X Information Service API".

[i.16] ISO/DIS 21217(en): "Intelligent transport systems — Station and communication architecture", 2020.

[i.17] ITS America Whitepaper: "Beyond 5.9 V2X Deployment Plan", August. 2024.

[i.18] 5GAA Position Paper: "V2N2X security, privacy, and data quality", December 2024.

[i.19] 5GAA Whitepaper: "Road Traffic Operation in a Digital Age: A Holistic Cross-Stakeholder Approach", June 2025.

[i.20] 5GAA Technical Report: "Vehicle-to-Network-to-Everything (V2N2X) Communications: Architecture, Solution Blueprint, and Use Case Implementation Examples", June 2025.

[i.21] 5GAA Technical Report: "Cross-Working Group Work Items; Automated Valet Parking Technology Assessment and Use Case Implementation Description; System Architecture, Cellular Network and PC5 Direct Communication Solutions", September 2023.

[i.22] VDA Position Paper: "Requirements for automated valet parking systems", May 2023.

[i.23] Void.

[i.24] 5GAA Technical Report: "Cross-Working Group Work Item Network Reselection Improvements (NRI)", 2021.

[i.25] ETSI TS 123 501 (V19.6.0), 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 19.6.0 Release 19).

[i.26] ETSI TR 103 562 (V2.1.1): "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2".

[i.27] ETSI TS 103 882 (V2.1.1): "Intelligent Transport Systems (ITS); Automated Vehicle Marshalling (AVM); Release 2".

[i.28] IEEE™ 1609.2-2022: "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Application and Management Messages".

[i.29] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

5G System: 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE

geocast: distributing ITS message to target vehicles or end user devices in a specific geographical area

ITS backend: centralized system in the backend providing ITS services

EXAMPLE: Systems at traffic control, traffic management, ITS application suppliers, or automotive OEMs.

NOTE: A central ITS station may be part of an ITS backend.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

5GS	5G System
5QI	5G Quality of Service Identifier
AID	Application Identifier
AMQP	Advanced Message Queuing Protocol
APDU	Application Protocol Data Unit
API	Application Programming Interface
AS	Application Server
AVM	Automated Vehicle Marshalling
BI	Backend Interface
BM-SC	Broadcast Multicast Service Centre
BSA	Basic Set of Applications
BSC	Base Station Controller
BTP	Basic Transport Protocol
BTS	Base Transceiver Station
CA	Certificate Authority
CACC	Cooperative Adaptive Cruise Control
CAM	Cooperative Awareness Message
CCoC	Common Code of Conduct
CELL_DCH	Cell Dedicated Channel
CELL_FACH	Cell Forward Access Channel
CHW	Cellular Hazard Warning
C-ITS	Cooperative Intelligent Transport Systems
CPM	Collective Perception Message
CPS	Collective Perception Service
C-V2X	Cellular Vehicle-to-Everything
DATEX	Data Exchange
DENM	Decentralized Environmental Notification Message
DL	Downlink
DNS	Domain Name System
DPCH	Dedicated physical channel
DRX	Discontinuous Reception
E2E	End to End
ETWS	Earthquake and Tsunami Warning System
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network

FACH	Forward Access Channel
FQDN	Fully Qualified Domain Name
FTAP	Fast traffic access protocol
Gb/Gn	Interface between GGSN Node and Internet
GC-SAP	Geocast Client Service Access Point
GSM	Global System for Mobile Communications
HS-DSCH	High speed dedicated shared channel
HSPA	High Speed Packet Access
HTTP	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
II	Interchange Interface
IMS	Internet Multimedia Subsystem
IOO	Infrastructure Owner Operator
IoT	Internet of Things
ISI	Information Sharing Instances
ITS	Intelligent Transport Systems
IVI	In Vehicle Information
JSON	JavaScript Object Notation
LTE	Long Term Evolution
MA	Misbehavior Authority
MBMS	Multimedia Broadcast and Multicast Services
MCCH	MBMS Control Channel
MCS	Modulation and Coding Scheme
MEC	Mobile Edge Computing
MICH	MBMS Notification Indicator Channel.
MIMO	Multiple-input and multiple-output
MNO	Mobile Network Operator
MQTT	Message Queuing Telemetry Transport
MS	Mobile Station
MSA	MBMS Service Area
MSCH	MBMS Scheduling
MTCH	MBMS Traffic Channel
NR	New Radio
NTN	Non-Terrestrial Network
OEM	Original Equipment Manufacturer
OSI	Open System Interconnection
PC5	Proximity-based Communication (Interface) 5
PDCH	Physical Data Channel
PKI	Public Key Infrastructure
PoTi	Position and Time
POTI	Position and Time
QoS	Quality of Service
R&D	Research and Develoment
REST	REpresentational State Transfer
RHW	Road Hazard Warning
RLC	Radio Link Controller
RNC	Radio Network Controller
RO	Road Operator
RRC	Radio Resource Control
RTA	Road Traffic Authority
RTI	Road Traffic Information
RTT	Round Trip Time
RTTI	Real Time Traffic Information
RVO	Remote Vehicle Operation
S-CCPCH	Secondary Common Control Physical Channel
SIP	Session Initialization Protocol
SMSCB	Short Message Service Cell Broadcast
SP	Service Provider
SPaT	Signal Phase and Timing
SRTI	Safety Related Traffic Information
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLS	Transport Layer Security

TTI	Transmission Time Interval
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
UMTS	Universal Mobile Telecommunications System
URA_PCH	Utran Registration Area-Paging Channel
V2V	Vehicle to Vehicle
VAM	VRU Awareness Message
VIS	V2X Information Service
VMC	Vehicle Montion Control
VRU	Vulnerable Road User
W-CDMA	Wideband Code Division Multiple Access

4 Overview

Starting from the ITS communication architecture and considering primarily, but not exclusively, the basic set of applications identified in [i.3], a critical assessment of the applicability of mobile network access and IP unicast communication to support the described application scenarios is given in the present document. This analysis refers to technical standards developed by 3GPP for cellular mobile networks. Additional technical background provided by R&D, pilot projects, as well as commercial deployments are considered in the present document.

As a result, the present document presents usage of cellular mobile networks and the 3GPP Uu interface for C-ITS.

5 C-ITS architecture over cellular networks

5.1 ITS communication system architecture and ITS station reference architecture

As shown in the example ITS station reference architecture in Figure 2 ([i.16]), different communication technologies can provide access layer connectivity service for communication among ITS stations and ITS sub-systems (see Figure 1). Cellular networks that use technologies standardized in 3GPP, where the communication interface to the User Equipment is known as the Uu interface, is one of the communication technologies and solutions providing IP unicast communication at the network layer, to support ITS services.

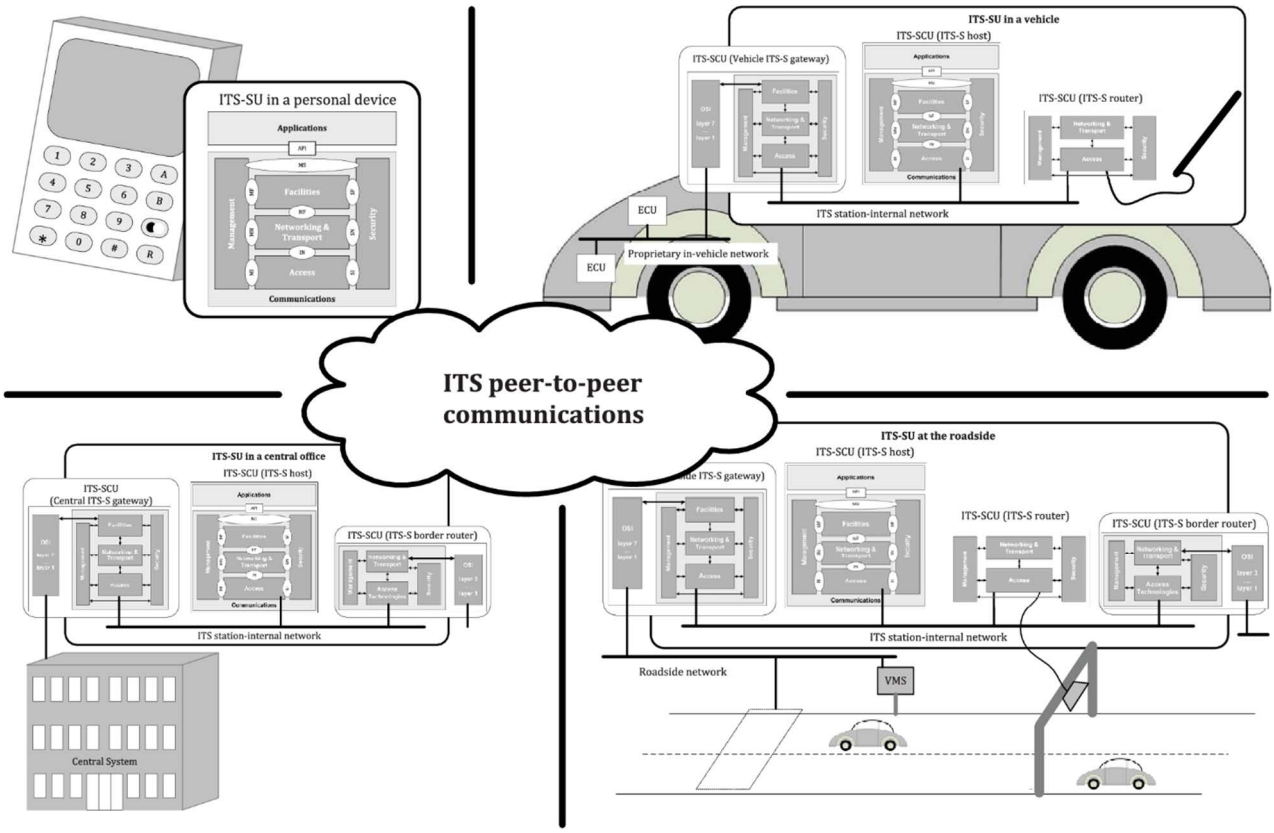


Figure 1: Illustration of ITS sub-systems [i.16]

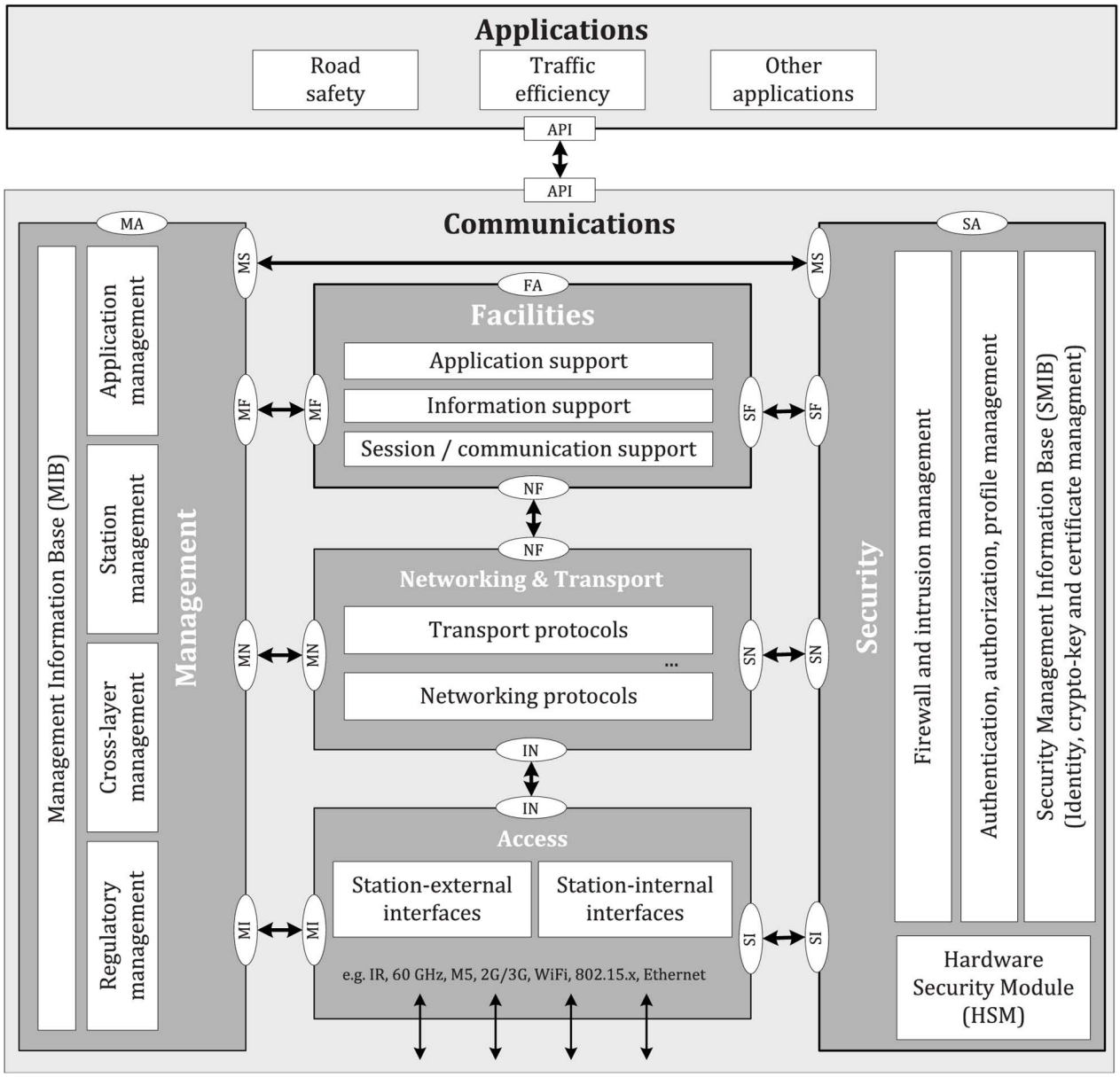


Figure 2: Examples of possible elements in the ITS station reference architecture [i.16]

5.2 System architecture of ITS using cellular infrastructure and the Uu interface

Figure 3 shows an overview of ITS using long-range cellular communication, where the dashed lines indicate links using cellular network, also referred to as long-range communication in the present document, access and solid lines show the backend connections, where ITS messages are communicated.

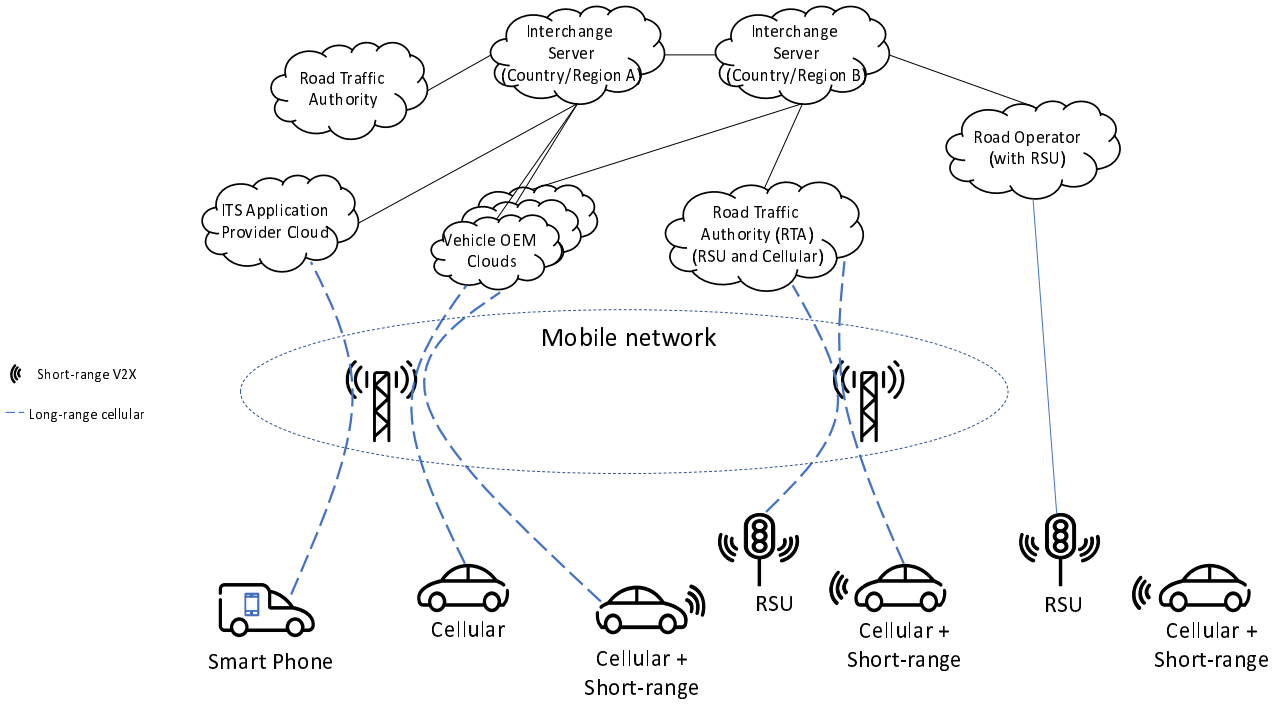


Figure 3: Overview of ITS using cellular network involving multiple service providers and backend cloud systems

As shown in Figure 3, mobile cellular networks support communication among vehicle-, roadside-, personal-, and central-ITS stations. Following ITS messages flows are supported by long-range cellular network communication:

- ITS messages are transmitted from ITS stations using the cellular User Equipment (UEs) to ITS central systems, where central ITS stations are located. In this case, cellular Uu interface is used for the uplink IP unicast communication.
- ITS messages are transmitted from the ITS central systems to ITS stations using cellular UEs. In this case, the Uu interface is used for the downlink IP unicast communication.
- ITS messages are transmitted from the ITS central systems to ITS stations using the Uu interface and downlink broadcast/multicast communication, when available.

NOTE: Due to limited deployment of cellular broadcast and multicast communication in commercial cellular networks, the present document only focuses on IP unicast uplink and downlink communications over cellular networks.

Combination of above ITS message flows enable communications among all ITS stations that use cellular UE within the coverage of mobile networks.

The cellular Uu interface does not support local direct ad-hoc communication among ITS stations that does not rely on the network infrastructure. This local direct ad-hoc communication is provided by short-range communication, e.g. the LTE-V2X sidelink, NR-V2X sidelink, or ITS-G5. Compared with short-range communication, the Uu cellular interface offers longer communication distance and end-to-end communication between vehicle-, roadside-, personal-ITS stations and the ITS central systems at the backends.

Cellular networks support end-to-end IP-based communication, regardless of the generation of cellular communication technology and mobile communication service provider. An example of the End-to-end protocol stack for ITS applications through 3GPP LTE (4G) network is shown in Figure 4.

While communication delays can be reduced thanks to Quality of Service (QoS) within the cellular network and kept easily below a few tens of ms, the internet part of the communication path between the cellular networks and the servers may introduce significant delays and jitters in the overall communication paths. Additional network switching latency may be introduced, e.g. when vehicle ITS stations move from the coverage of one mobile operator network to another.

One possibility to reduce the length of communication paths and IP routing uncertainties is to duplicate and distribute geographically the servers or their required functions, for instance by mimicking or using Content Delivery Network concepts. The idea is even further advanced with the concept of Mobile Edge Computing (MEC). In MEC, the computing resources are directly located at the edge of cellular network under the control of the mobile operator or even at the edge of the radio access network. Consequently, OEM and ITS application servers can then directly run as close as possible to the ITS stations, taking benefits of QoS. MEC can be used for computational offloading, collaborative computing, content delivery, etc., making it a key element for the deployment of connected and autonomous vehicles. In terms of supporting ITS applications, ETSI ISG MEC has specified a V2X Information Service (VIS) and its API in [i.15], in order to facilitate interoperability in a multi-vendor, multi-network and multi-access environment.

NOTE: Mobile Edge Computing (MEC) concept has been extended to any type of IP access and is now formally named Multi-access Edge Computing (MEC) [i.13].

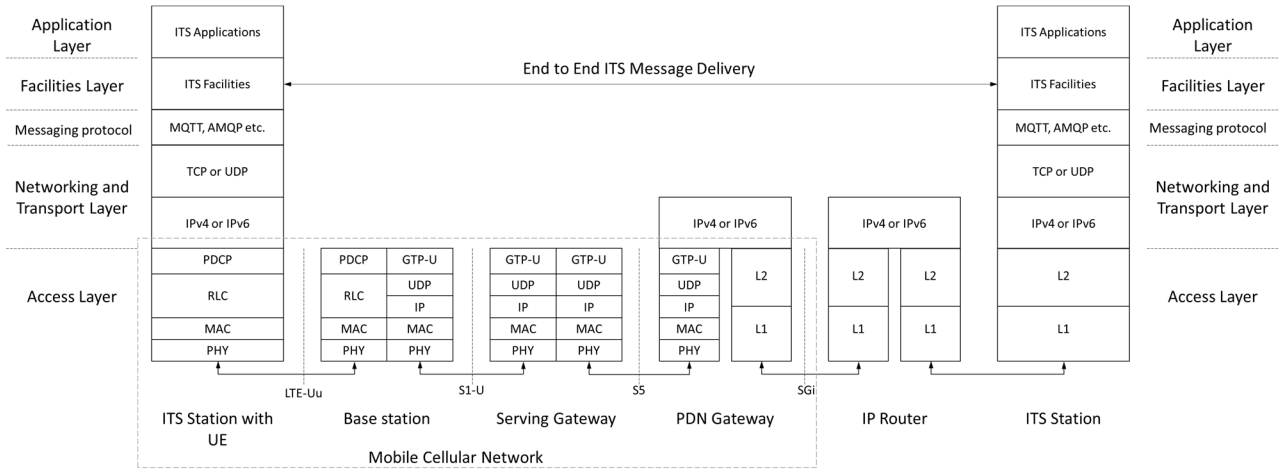


Figure 4: Example end-to-end protocol stack of wide-area communication in ITS system through cellular Uu interface

6 Identification and enhancements of ITS applications and related use cases

6.1 Introduction

This clause presents example ITS services and use cases that can be supported by cellular mobile networks. The main intention of this clause is to illustrate solution examples and capabilities of cellular network in supporting ITS services and user cases, instead of providing an exhaustive list of ITS services to be supported by cellular networks. Other ITS services that are not covered in the present document may also be supported using cellular network, as far as the corresponding communication requirements can be fulfilled. It is worth noting that ITS services and use cases described in the present document may also be supporting using other communication technologies, e.g. short-range communications, satellite communications, etc., or combination of multiple communications technologies, which may better satisfy the general road safety and/or road traffic efficiency objectives than using a single communication technology.

As an starting point, the use cases identified in [i.3] (BSA) and C-Roads [i.9] have been analysed considering these capabilities with the goal of identifying the ones that can be deployed using cellular networks. Furthermore, the present document also selects some ITS day 2 use cases that ETSI TC ITS is working on under the framework of ITS release 2 standards.

The present document analyses ETSI TC ITS specifications and reports of applications, use cases, and facilities layer functionalities, considering multiple access technologies supports, e.g. cellular network and short-range communications.

6.2 ETSI ITS Basic Set of Applications

6.2.0 Introduction

Based on the considerations in clause 6.1, applicability to cellular networks of selected use cases described in [i.3], have been identified and sorted out in the two following clauses.

6.2.1 Active road safety and cooperative traffic efficiency use cases

Table 1 shows the applicability of the active road safety and cooperative traffic efficiency related use cases to the cellular network, together with selected reference use cases following the table. It is worth noting that the types of facilities layer messages provided in Table 1 are examples.

Table 1: Analysis of cooperative road safety related use cases

Use Case Title	Facilities layer message in a cellular network	Notes
Vehicle status warnings		
Emergency electronic brake lights	N/A	
Safety function out of normal condition warning	DENM	
Vehicle type warnings		
Emergency vehicle warning	CAM and DENM	
Slow vehicle warning	CAM and DENM	
Motorcycle warning	CAM/VAM	
Vulnerable road user Warning	DENM/VAM	
Traffic hazard warnings		As cellular network gives larger coverage, DENM over cellular is more efficient in reaching far distant ITS stations.
Wrong way driving warning	DENM	
Stationary vehicle warning	DENM	
Traffic condition warning	DENM	
Signal violation warning	DENM	
Roadwork warning	DENM	
Decentralized floating car data	DENM	
Dynamic vehicle warnings		
Overtaking vehicle warning	N/A	
Lane change assistance	N/A	
Pre-crash sensing warning	N/A	
Co-operative glare reduction	N/A	
Collision Risk Warning		
Across traffic turn collision risk warning	N/A	
Merging Traffic Turn Collision Risk Warning	N/A	
Co-operative merging assistance	N/A	
Hazardous location notification	DENM	
Intersection Collision Warning	N/A	
Co-operative forward collision warning	N/A	

Use Case Title	Facilities layer message in a cellular network	Notes
Collision Risk Warning from roadside infrastructure	N/A	
Traffic Efficiency		
Regulatory/contextual speed limits	DENM	Use of DENM approach is proposed as an alternative to BSA approach that indicates use of CAM.
Traffic light optimal speed advisory	DENM	Use of DENM approach is proposed as an alternative to BSA approach that indicates use of CAM.
Traffic information and recommended itinerary	DENM	
Enhanced route guidance and navigation	DENM	
Intersection management	N/A	
Co-operative flexible lane change	N/A	
Limited access warning, detour notification	DENM	
In-vehicle signage	DENM	
Electronic toll collect		Both access technologies (direct short-range and cellular) are deployed in commercial applications.
Co-operative adaptative cruise control	See clause 6.4.2	
Co-operative vehicle-highway automation system (Platoon)	See clause 6.4.23	

- Emergency vehicle warning:

  Note that while CAM based on short-range direct communications is currently defined for implementing this use case, the related service can be enhanced with cellular networks. The position of the emergency vehicle can be used to send DENM messages to cars within the vicinity of the emergency vehicle but beyond the range supported in short range wireless communication, hence allowing the emergency vehicle faster movement.

- Signal violation warning:

  DENM handling based on Geocast (see Annex B) can be applied also to the case DENM is generated by roadside infrastructure, as given in this use case. It is worth noting that the roadside infrastructure can be connected to a fixed line infrastructure. Activation of sending DENMs over cellular networks depends on the actual importance of the event. DENM dissemination to neighboring vehicles should apply to scenarios where line of sight between vehicles and roadside infrastructure is not guaranteed.

- Roadwork Warning:

  This use case is similar to Emergency vehicle warning, but with the added feature to provide roadwork personnel with terminals (ITS stations) allowing easy placing of roadwork warning over a map managed by an application server.

6.2.2 Co-operative local services and global internet services use cases

Co-operative local services and global internet services use cases can be managed through cellular network access with or without the use of Geocast capabilities (see Annex B). The use cases are depicted in Table 2.

Table 2: Analysis of co-operative local services and global internet services use cases

Use Case Title	Support in a Cellular network
Point of interest notification	Yes
Automatic access control/parking access	Yes
Local electronic commerce	Yes
Car rental/sharing assignment/reporting	Yes
Media downloading	Yes
Map download and update	Yes
Ecological/economical drive	Yes
Instant messaging	Yes
Personal data synchronization	Yes
SOS service	Yes
Stolen vehicle alert	Yes
Remote diagnosis and just in time repair notification	Yes
Vehicle relation management	Yes
Vehicle data collect for product life cycle management	Yes
Insurance and financial Services	Yes
Fleet management	Yes
Vehicle software/data provisioning and update	Yes
Loading zone management	Yes
Vehicle and roadside infrastructure data calibration	Yes

6.3 Support to ETSI ITS Basic Set of Applications

6.3.1 Introduction

The ITS basic set of applications analysed in clause 6.2 are essentially safety applications aimed at increasing the awareness of dangerous and unexpected situations by disseminating basic status information of road users using Cooperative Awareness service or detected events by road users or the infrastructure using Decentralized Event Notification (DEN) service. Furthermore, release 2 ITS services, e.g. Collective Perception Service (CPS) and Vulnerable Road User (VRU) Awareness service, are broadening the scope of paradigm to enable road users to fulfil cooperative automated driving scenarios by exchanging more sophisticated information between the road users and road infrastructure.

The clauses below discuss the ETSI ITS services, with which cellular networks can support the release 2 applications, and the impact that cellular network communication may have on these use cases.

6.3.2 Decentralized Event Notification (DEN) Service

DEN service is related to event detection and dissemination. Support of DEN Message (DENM) [i.2] by cellular networks can bring added value in the ability to consolidate the information of numerous events that originate from ITS stations in the various relevance areas, coordinate these events, and track them in a way that allows only dissemination of useful information in the relevance areas. This added intelligence for data miming can only be centrally supported.

In addition to the business value associated with the consolidation and coordination of event-related information, this has several functional advantages:

1) Redundant uplink transmission of the event can be avoid by the originating ITS station based on the acknowledged notification of the same event on the downlink channel. This eliminates the need to repeat sending the same event again. This enhances system scalability and reduces network congestion.

2) Policies can be built in the central message dissemination functions that allow information related to events to be disseminated into an area larger than the original relevance area if warranted. The vehicle can enter the relevance area already pre-warned and increased warning levels can be assigned when approaching the position of the event.

3) For an approaching vehicle, there is no need to have a vehicle or roadside infrastructure in its vicinity to be notified of any event. The dissemination of the event is done within the cellular wide coverage.

6.3.3 Cooperative Awareness Service

Cooperative Awareness service is relevant to disseminating position, dynamics and attributes information of ITS stations, in order to improve the awareness among road users and between road users and road infrastructure. In addition to increasing the mutual awareness of road users, Cooperative Awareness Messages (CAM) [i.1] from road users can also be made available at central ITS stations, e.g. traffic control centers or ITS application servers at the backend, to support cloud-based ITS services implementations, e.g. probe vehicle data, hazard detection at central ITS stations, etc.

When a cloud server is involved in processing and/or disseminating CAM, there are two alternative ways of implementing ITS applications. As shown in Figure 5, data processing, e.g. for danger detection, can be done either on the cloud server or on the receiving vehicle. In the first case, the cloud assesses dangerous situations and delivers Downlink (DL) notifications to affected vehicles. In this case, most traffic loads are in the cellular Uplink (UL). In the second case, danger detection is done at the vehicle, after receiving the CAM messages from other vehicles relayed by the cloud. In this case, CAM traffic is generated for both cellular UL and DL. As cellular network communication can provide reliable and acknowledged message delivery between UEs and the cloud server, in both cases the cloud server can maintain the most recent or predicted status of concerned vehicles, e.g. position, speed, etc.

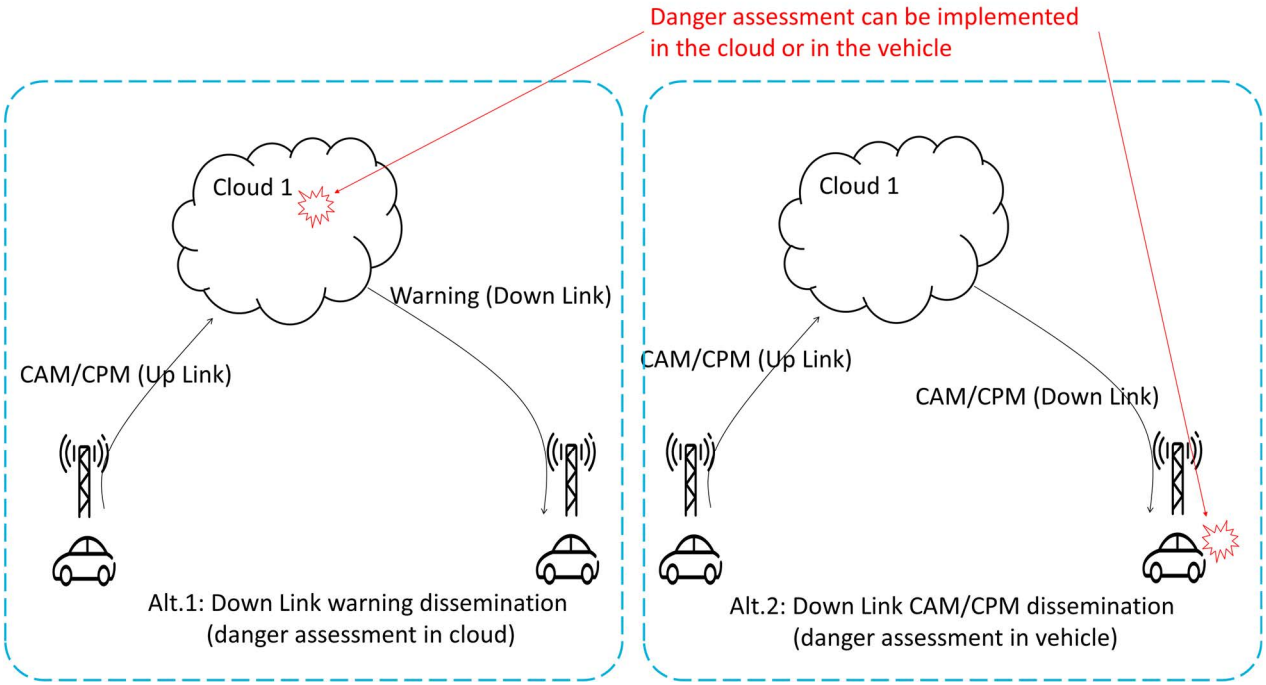


Figure 5: Examples of two alternative ways of processing CAM/CPM in the cloud

ETSI TS 103 900 [i.1] defines the procedure for periodic CAM transmission with a frequency with a frequency of 1 Hz to 10 Hz depending on congestion control and mobility of the transmitting ITS station. This periodic transmission procedure generates high traffic load to the cellular network, as studied in [i.4], and causes high spectrum demand and energy consumption at ITS stations.

One example solution for this issue is to use other transmission frequency lower than the prescribed minimum value 1 Hz, when CAM are transmitted using the cellular Uu interface unless any safety concern is caused by this change. Additionally, a trigger for transmitting the CAM can be introduced based on the prediction error, which is the deviation between ITS station's actual position and the predicted position based on its last transmitted CAM. When the prediction error exceeds a predefined threshold, a new CAM is transmitted. The threshold can be configured depending on the applications using the information conveyed by CAM and the evaluated safety impact to the application, i.e. any deviation from the prediction value that may have safety impact to the receiving ITS station will trigger the transmission of CAM immediately. This way, a higher threshold, i.e. larger acceptable errors, gives larger load reductions, while a lower threshold enables more accurate status information at the receiving stations without compromising the safety constraint. As an example, Annex C presents numerical results of the proposed CAM trigger rule using prediction error, which can achieve significant load reduction in cellular uplink.

Therefore, applicability of CAM to cellular networks should be intended for selected applications and areas/vehicles, based on mechanisms allowing network control of its activation/deactivations and related generation rules. It is proposed to specify CAM generation rules in [i.1] using configurable parameters for the maximum and minimum transmission frequencies of CAM, instead of the prescribed absolute values in the standard unless any safety concern is caused by this change. So that implementation of different ITS ecosystems may configure the value of CAM transmission frequency to fit their specific needs, e.g. for the prediction error-based CAM generation rules, as described in Annex C.

6.3.4 Cooperative Adaptive Cruise Control (CACC)

CACC is an automated driving assistance application that adjusts automatically vehicle speed to keep a target time gap with a target vehicle while keeping a minimum safety distance with it. CACC makes use of data received from other vehicle ITS-Ss and/or from roadside ITS-Ss via ITS network [i.11].

Cellular networks may provide advantage of advanced controllability, e.g. elaborated management of CACC strings including dynamic joining and leaving vehicles and string break-up.

6.3.5 Platooning

Platooning is an automated driving assistance application that enables vehicles to form a platooning group and performs lateral and longitudinal controls of vehicles. Vehicle platooning applications can be used in order to improve fuel efficiency and safety for goods transport. The potential social and environmental benefits of vehicle platooning have been largely proven.

Cellular networks may provide advantages of advanced controllability, e.g. more elaborate management of platooning group operations such as creation, joining and leaving and platoon break-up.

6.3.6 Vulnerable Road Users (VRU) protection

In the Release 2 application deployment phase, VRUs are expected to play a more active role in announcing their presence whenever necessary and detect risky situations, hence they will contribute to further increase in road safety. VRUs can announce their individual presence by transmitting VRU Awareness Messages (VAMs) in the same way that vehicles announce their presence by transmitting CAMs. However, in consideration of the dynamic characteristics of VRUs which are different from vehicles, VRUs can be considered grouped in certain situations and clustered VAMs can be sent by the cluster leader instead of many individual VAMs. The clustering method is specified in ETSI TS 103 300-3 [i.14] along with the clustering operations such as creating, joining, leaving and breaking up of the cluster to reduce the use of bandwidth.

Cellular networks can provide the advantages of increased coverage and advanced controllability, e.g. more elaborate management of VRU clusters, with appropriately tailored triggering conditions, message generation rules and clustering scheme, and mechanisms of delivering VAMs to selected areas, and so on.

A combined operation of day-1 and day-2 services can be supported by using both a short range communication and a long range communication. A roadworker warning can be considered as one of such use cases. The RTA is generally in charge of scheduling all road constructions within its jurisdiction. The Road Traffic Authority (RTA) should ensure the safety of roadworkers who can be exposed on a road under construction. The RTA can generate DENM containing information of a road construction e.g. geolocation, area, duration, start time and end time and transmit DENM to a roadside infrastructure via a secure path. The roadside infrastructure can broadcast DENM to approaching vehicles via short range communication. Vehicles equipped with the short range communication can notice roadworkers in their path, before arriving at the point. It can be a basic operation of day-1 service with a short range communication. It should be also considered the case when the RTA may not be able to manage all road constructions which depend on the road condition dynamically and unexpectedly in real world situations. Also, it might cause unexpected latency when the RTA should manage a lot of road constructions in a short time frame. If the roadworker can send VRU awareness message to make approaching road users (e.g. vehicles, bicycles, or motorcycles) aware of their existence on a road by using day-2 VRU Basic service, the roadworkers can be protected even when the roadwork warning message was not provided by the RTA because of any unexpected reasons described above. Furthermore, if the roadworker's device is connected to the cellular networks and can send VRU awareness message via the cellular networks, even road users not equipped with the short range communication can also receive those messages via the cellular networks. Figure 6 depicts a combined operation of day-1 and day-2 services by using both a short range communication and a long range communication.

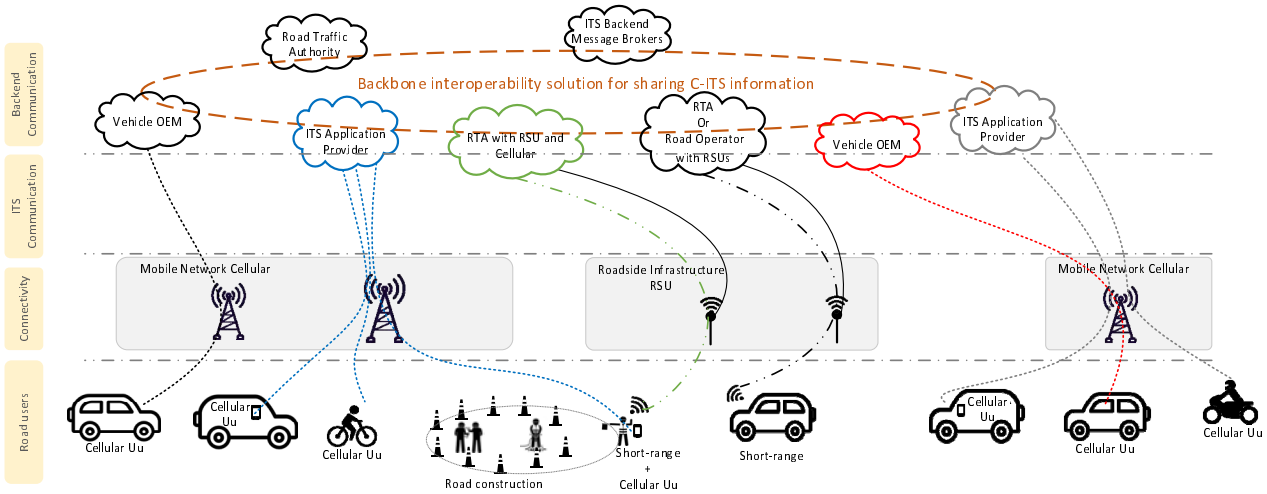


Figure 6: Roadworker warning via short-range communication and cellular Uu

With regard to the active roadworks use case, more detailed indications are described in Annex H of ETSI TS 103 300-3 [i.14]. More use cases supporting the operations/provisions of day-1 services and day-2 services particularly related to the VRU Basic service are described in ETSI TR 103 300-1 [i.10].

6.3.7 Collective Perception Service (CPS)

The V2X system will be extended to additionally permit vehicles and roadside infrastructure to share information of objects detected by on-board sensors such as cameras, lidars and radars. The detected information is conveyed via Collective Perception Messages (CPMs) and enables receiving vehicles to be aware of objects that are not V2X capable and would otherwise not be locally detectable (e.g. standing VRUs behind a corner in intersection areas, or vehicles behind a truck on interurban roads) [i.12].

Cellular networks can provide an advantage of increased coverage with appropriately tailored triggering conditions and message generation rules, and mechanisms of delivering CPMs to selected areas, and so on.

In use cases of CPS described in [i.26], ITS central systems that include central ITS stations can receive and transmit CPM. Particularly, use cases of CAM Information Aggregation described in clause 4.1.4 of [i.26] require the ITS central system to process and fuse information in the received CAM and CPM and disseminate the processed and integrated information in form of CPM to relevant road users.

Like the case of CAM discussed in clause 6.3.3, the high generation frequency of periodic CPM, e.g. 1 Hz or higher, at road users impose high traffic load to the cellular network. As cellular networks can provide reliable and acknowledged message delivery, there is no need to improve communication reliability by repeating messages. When communicating via the cellular Uu interface, road users should trigger CPM generate only according to the update of message content. To further reduce the CPM generation rate, prediction error-based message generation rules, as described in Annex E, can also be defined for CPM. Unlike CAM, the generating station of CPM predicts the status and locations of perceived objects or free space, instead of its own status. Effects in reducing the traffic load of periodic message generation like the numerical results shown in Annex C can be expected for CPM.

Therefore, it is proposed to specify CPM generation rules using configurable parameters for the maximum and minimum transmission frequencies of CAM, instead of the prescribed absolute values in the standard unless any safety concern is caused by this change. So that implementation of different ITS ecosystems may configure the value of CPM transmission frequency to fit their specific needs.

6.3.8 Maneuver Coordination Service (MCS)

Coordination can be beneficial in case a vehicle's planned trajectory is in conflict with the planned trajectory of another vehicle. MCS allows both vehicles to exchange information of their planned and desired trajectories, which enables a negotiation to resolve the conflict. Through the use of the MCS, a number of cooperative automated driving use cases can be supported such as Cooperative Merging, Cooperative Lane Change, Cooperative Overtaking, etc.

Cellular networks may provide advantages of increased range and advanced controllability, e.g. more scalable and elaborate coordination for larger number of vehicles and larger area.

6.3.9 Automated Vehicle Marshalling (AVM)

Automated Vehicle Marshalling (AVM) [i.27] in the context of road traffic, means that individual or multiple unoccupied vehicles of several kinds are automated driven in the lower velocity range. The AVM entity in the Facilities layer is a broad Vehicle Motion Control (VMC) functionality supporting Remote Vehicle Operation (RVO) in the low-speed domain and it is an entity within the ITS ecosystem. As specified in Annex E of ETSI TS 103 882 [i.27], AVM service can be implemented using secured IP unicast communication on top of cellular network-based communication.

6.4 Example implementations and deployments

6.4.1 Roadwork warning

A Road Traffic Authority (RTA) is generally in charge of scheduling all road constructions within its jurisdiction. The RTA should ensure the safety of roadworkers who can be exposed to a road under construction. The RTA can generate DENM containing information of road construction e.g. geolocation, area, duration, start time and end time and transmit DENM to a roadside infrastructure via a secure path. The roadside infrastructure can broadcast DENM to approaching vehicles via short range communication. Vehicles equipped with short range communication can notice roadworkers in their path, before arriving at the point. It can be a basic operation of day-1 service with short range communication.

It should be also considered the case when the RTA may not be able to manage all road constructions which depend on the road condition dynamically and unexpectedly in real world situations. Also, it might cause unexpected latency when the RTA should manage a lot of road constructions in a short time frame. If the roadworker can send VRU awareness message to make approaching road users (e.g. vehicles, bicycles, or motorcycles) aware of their existence on a road by using day-2 VRU basic service, the roadworkers can be protected even when the roadwork warning message was not provided by the RTA because of any unexpected reasons described above.

Furthermore, if the roadworker's device is connected to the cellular networks and can send VRU awareness message via the cellular networks, even road users not equipped with the short range communication can also receive those messages via the cellular networks if available. Figure 7 depicts a combined operation of day-1 and day-2 services by using both a short range communication and a long range communication. With regard to the active roadworks use case, more details are described in Annex H of ETSI TS 103 300-3 [i.14].

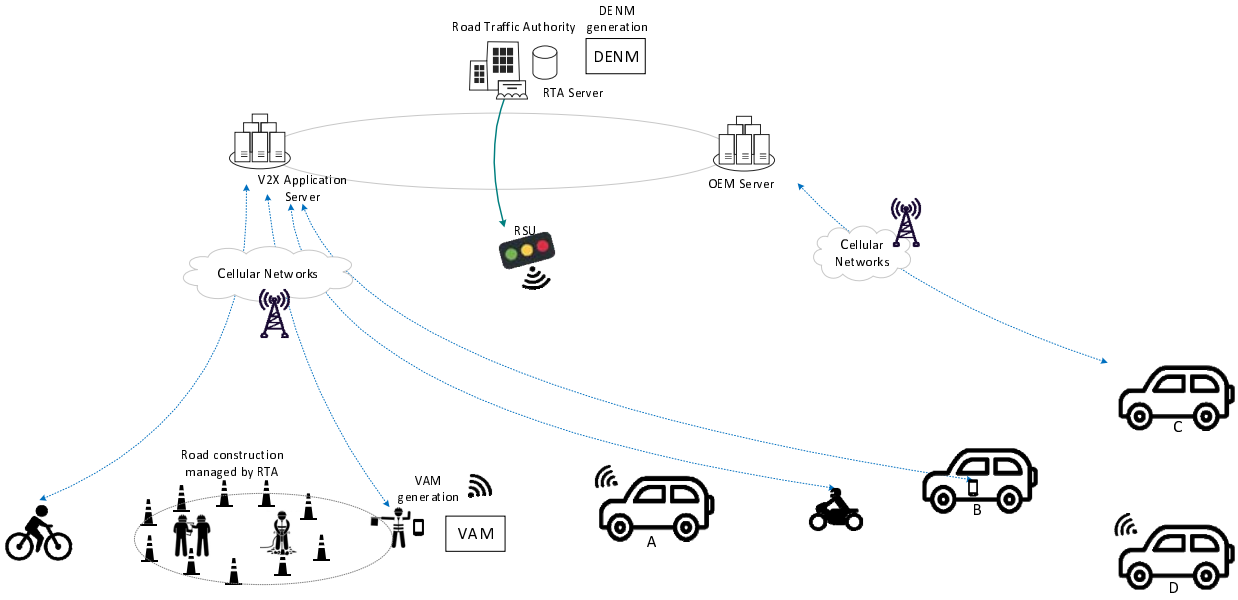


Figure 7: Roadwork warning using both short-range communication and cellular networks

7 Impacts on ETSI ITS standards for cooperative ITS

As shown in Figure 4, the protocol stack of the ITS station using cellular network communications is based on IP unicast communication, which uses protocols and standards from different standardization organizations. In most cellular network-based C-ITS implementations, standards developed in ETSI TC ITS are mostly used at the Facilities layers, e.g. CAM, DENM, CPM, VAM, AVM, POTI, as well as functional safety related standards, etc., while transport, network, and access layer standards are developed in other standardization bodies, e.g. IETF, ISO, and 3GPP. From the security and privacy perspective, IP unicast communication employs solutions different from short-range direct communications, as elaborated in clause A.3.

To enable cellular mobile network support, as well as other communication technology support, to ETSI facilities layer services, the following requirements should be fulfilled when developing ETSI facilities layer standards:

- The ETSI ITS facilities layer standards should be developed to work with different lower layer technologies and protocols, e.g. the ITS facilities layer message should be able to be conveyed using the TCP/IP protocols stack as well as BTP/GeoNetworking protocol stack, without extra implementation effort (e.g. protocol encapsulation) for any protocol stack.

- The ETSI ITS facilities layer standards should be developed to work with different security technologies and protocols, e.g. the ITS facilities layer message should be able to work together with TLS/DTLS security as well as IEEE 1609.2 [i.28] security solutions, without extra implementation effort for any security solution.

- For above reasons, ETSI ITS facilities layer standards should avoid any requirement or parameter setting that is designed for the purpose of being exclusively supported by a specific lower layer protocol stack or security solution. The focus of facilities layer standards should be fulfilling the functional and interoperability requirements of the relevant services or applications.

Annex A: Cellular 4G/5G System and Technical Features Supporting ITS Services

A.1 Introduction

A.1.0 Overview

The Uu interface works without any special handling in cellular networks nor is any special interaction with the cellular networks needed for basic communication, i.e. vehicles and smartphones can just use the cellular connection as a normal IP connection with the ordinary subscription to any Mobile Network Operator (MNO). However, there are standardized features in mobile networks that potentially can be used to optimize for C-ITS as described below. These features would however incur a cost for the MNOs.

A.1.1 Quality of Service (priority for ITS information)

Mobile networks can be configured to identify certain traffic flows based on the IP five tuple (IP addresses, port numbers, protocol). This can be used to provide quality of service and priority for ITS information over normal Internet traffic in case of high load in the mobile network.

3GPP defined QoS mechanisms and network slicing solutions are elaborated in the context of V2X and C-ITS communication with details in Annex E of the 5GAA V2N2X Technical Report [i.20]. ETSI TS 123 501 [i.25] (Table 5.7.4-1) defines the 5G Quality of Service Identifier (5QI) in terms of the QoS performance targets, e.g. packet delay budget, packet error rate, etc.

A.1.2 Cross border (Mobile network change)

When changing serving MNO an interruption in connectivity usually occurs due to reselection of frequency and attachment to new serving MNO. This interruption can be substantially reduced or eliminated by features available in cellular networks, however these features need to be activated between MNOs.

The interruption time is relative to the configuring effort needed, how to reduce or even eliminate the interruption time is described in [i.24].

A.1.3 Latency and distributed computing

Cellular networks of today provide low latency, a common performance is around 20 - 40 millisecond to reach a server on Internet, so C-ITS day 1 and 1,5 use cases can be supported. For C-ITS information exchange, 'car to backend to car' latency has been shown to be in the range of 50 - 150 ms when using (early version of) LTE [i.4]. However, the latency is strongly dependent on the implementation and the design of the Geocast function and protocol translation, which may add 1 - 2 seconds to the latency. For future use cases, e.g. related to autonomous vehicles, a lower latency may be needed, this can be achieved by placing equipment to provide hosting of needed applications (e.g. compute and storage) in the MNO and by that reduce the latency added by transport and Internet. In a cellular radio network, User Equipment (UEs) are put into 'inactivity' state on the radio interface when no traffic for certain time (configurable by MNO), this to optimize battery consumption and to maximize the number of UEs that can be served, this result in some additional latency when UEs are brought back to connected state again. However, this additional latency can be eliminated since a vehicle in operation does not suffer from battery constraints it can be in connected mode, thus remove the radio connection establishment latency, i.e. no radio sleep modes necessary.

A.2 ITS backend communications enabling interoperable C-ITS applications

A.2.0 Overview

Figure A.1 shows an overview of some implementation models for C-ITS services. Different implementation models provide the same C-ITS services using different communication solutions and backend systems. Interoperability of services among different implementation models is an essential requirement of C-ITS.

NOTE 1: Not all variants of implementation models are shown in Figure A.1. These examples show the most probable models for deploying C-ITS services and explain the interoperability requirement from an end-to-end point of view.

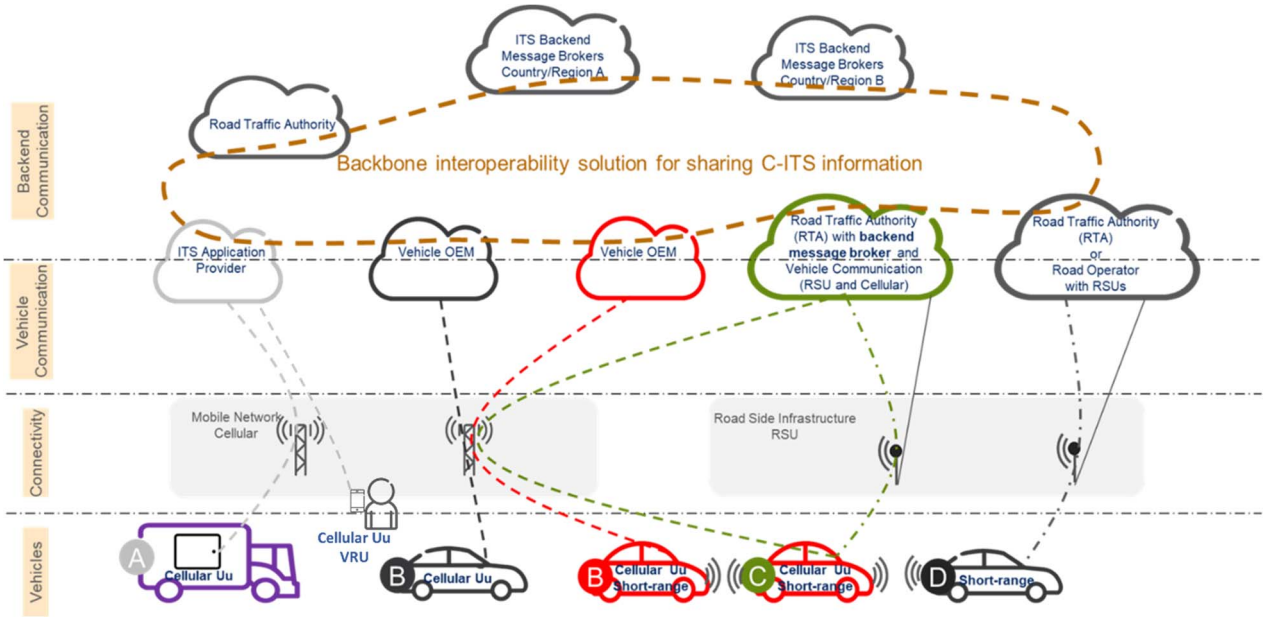


Figure A.1: Overview of implementation models for C-ITS services

Implementation models shown in Figure A.1 include (from left to right):

1) Implementation model A is to include additional communication devices in the C-ITS ecosystem, e.g. smartphones and navigators. In this scenario, the devices communicate with their application. This communication path to the devices may be used by Road Traffic Authorities/road operators in agreement with application providers. In this case, the application providers and the road traffic authority/road operator are the trusted actors.

NOTE 2: This type of device may be used outside vehicles as well, e.g. by vulnerable road users.

2) Implementation model B is to use the OEM and its existing connection to its vehicles for C-ITS services. This communication path to vehicles may be used by Road Traffic Authorities/road operators in agreement with OEMs. In this scenario, the OEM and the road traffic Authority/road operator are the trusted actors.

3) Implementation model C is to have a dedicated connection from vehicles to Road traffic Authorities for C-ITS, either using cellular and/or short-range communication via roadside infrastructure. In this scenario, the Road traffic Authority is the trusted actor.

4) Implementation model D is that road traffic authorities or Road operators use roadside infrastructure to communicate with vehicles. In this scenario, the Road traffic Authority and/or the Road operator are the trusted actors.

The 'Backbone' sharing C-ITS information consists of interconnected trusted actors, e.g. C-ITS actors. Here, C-ITS information refers to information for enabling C-ITS services at C-ITS stations.

What is not shown in Figure A.1 is the combination of using model B and model D, i.e. a vehicle using its cellular long-range communication to connect to its OEM and having short-range capabilities to communicate with roadside infrastructure.

Vehicles in Figure A.1 may directly exchange C-ITS information by using short-range V2V communication without relying on infrastructure and backend systems.

Figure A.1 illustrates hybrid solutions for deploying C-ITS services. On the one hand, "hybrid" means C-ITS information, in the form of standardized ITS messages, can be sent via short-range communication, or via cellular long-range communication, or both. On the other hand, "hybrid" also means C-ITS information can be conveyed using cellular infrastructure and backend systems in either standardized or proprietary message formats, i.e. that can be the case for implementation model B, where an OEM is responsible for conveying the information in a proprietary format between its backend system and its vehicles.

Depending on implementation models and evolution of the ecosystem, additional actors may be present in the future. For example, it is likely that public safety organizations can join to provide information about emergency vehicles such as fire trucks and ambulances, and parking companies can join to announce parking possibilities, etc.

Furthermore, the EU Commission have in Delegated Regulation 2015/962 [i.29] specified that DATEX II should be used e.g. for Real Time Traffic Information (RTTI) and Safety Related Traffic Information (SRTI).

Therefore, it is important to have an architecture that allows different implementation models, evolution, scalability and easy ways to join the ecosystem, while maintaining interoperability of C-ITS services. This objective can be fulfilled by ensuring interoperability in backend systems by using industry standards to interconnect backend systems.

Interoperability and scalability of using communication between backend systems are the focuses of this clause.

A.2.1 Basic network architecture for information sharing among ITS backend systems

For easy understanding, in the present document, Service Provider refers to OEM or ITS application provider backend system, to be differentiated from the backend systems of providers of road infrastructure (e.g. Road Traffic Authority (RTA) and Road Operators (ROs)).

In the basic scenario, exemplified in Figure A.2, service providers typically operate in one country/region and share information with its clients on vehicles or mobile devices located in that country/region. The service provider connects to entities in ITS backend systems in the relevant country to consume or provide information e.g. to an RTA/RO. The service provider may operate in additional countries/regions and connect directly to the relevant actors in those countries/regions for information sharing. To facilitate this information sharing among ITS backend systems an Interface/protocol named **Backend - Interface (BI) and the interchange entity** are introduced.

The BI protocol uses AMQP to convey information such as DENMs, IVI as payload. Information carried in payload is identified with metadata (called AMQP properties). This metadata can be used to filter out information. Examples of metadata are message types and relevance area for event, e.g. based on Quadtree tile concept.

Interchange entities are AMQP brokers with additional functionality to federate information between various data sources and consumers. The concept of interchange and federation is further elaborated in clause A.2.2.

Communication uses standard AMQP [i.8] methods with publish and subscribe between clients and AMQP brokers. The use of AMQP for C-ITS has been profiled in [i.7]. According to the profile, events are published by producers including metadata for the event and are pushed to consumers that are subscribing to information identified with the metadata. This facilitates that no tight interaction is required by the participating actors.

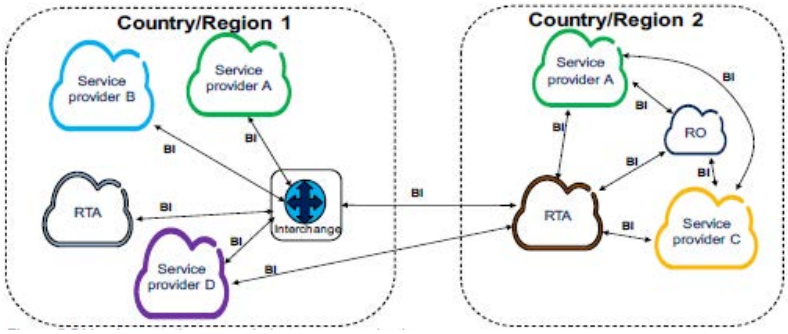


Figure A.2: Basic network architecture for C-ITS information sharing among ITS backend systems

Figure A.2 exemplifies two different approaches of using the BI interface for connecting ITS backend systems:

- Country/region 1 is using an interchange entity that interconnect ITS backend systems. The interchange entity provides publish/subscribe mechanisms to facilitate information sharing between the ITS backend systems, e.g. information received from the RTA is distributed to all service providers that have subscribed to the information. The replication is handled by the interchange entity without extra efforts at the RTA.
- In country/region 2, ITS backend systems interconnect with direct (logical) connections and provides publish/subscribe mechanisms to share information among them, i.e. service providers connect directly to RTA and RO for information sharing. Also, RTA and RO are interconnected to share information. In this scenario, an RTA would have to replicate and send information to all subscribing actors individually on the direct connections.

Figure A.2 further exemplifies potentially different interconnection strategies using the BI interface among Service providers, e.g. OEMs and ITS application providers:

- Service provider A' has multiple backend systems in several regions/countries. Each backend instance is connected to other relevant ITS backend systems, including the interchange entity. This is a common approach for many OEMs, where a vehicle connects to the 'best' OEM backend instance depending on its location.
- Service provider B' is active in one country/region and its backend is interconnected with the Interchange entity in that country/region.
- Service provider C' has a backend instance in region/country 2 and is directly connected to RTA and RO in that country/region. To share information with service provider A about events in country/region 2, an additional direct connection is established between the service providers A and C.
- For service provider D' to enable information sharing with its clients in both country/region 1 and country/region 2, its backend instance in one region/country 1 needs to connect to the interchange entity in country/region 1, as well as to the RTA in country/region 2. The specified common BI interface simplifies the connections to different ITS backend systems.
- There is also a BI established between RTA in in country/region 2 and Interchange entity in country/region 1 for information exchange.

A.2.2 Evolved network architecture for sharing information between countries/regions

In this scenario countries/regions are interconnected to share information for clients moving around in Europe, e.g. service providers have clients located in multiple countries/regions. This country/regional interconnection is to avoid a service provider creating and maintaining connections to many information sources/consumers e.g. to many RTAs/ROs, as well as to avoid the RTAs/ROs interacting with many service providers. To facilitate this, Interchange entities and an Interface/protocol to federate information between Interchange entities are introduced. This interface/protocol is named **Interchange Interface (II)**, which is the federation interface between Interchange entities. The II protocol can serve as look-up entity to inform consumers about where to find the data source or can function as an entity that fetches the information on behalf of the data consumer. The II control plane protocol uses HTTP REST principles with information JSON encoded.

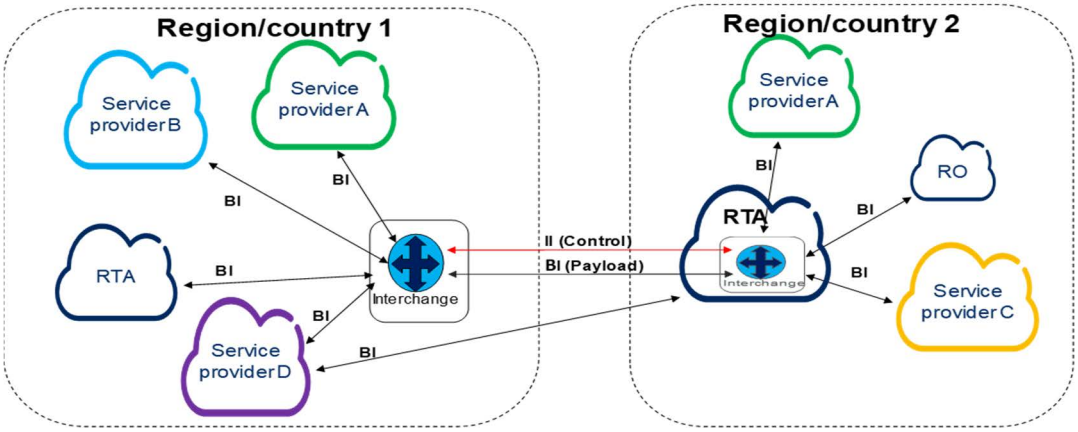


Figure A.3: Evolved architecture for country/region information sharing

Figure A.3 illustrates the evolved network architecture scenario with the II interface between countries/regions. Compared with Figure A.3, an interchange entity is introduced in region 2 to reduce the number of direct connections between ITS backend systems and to support sharing of information between countries/regions.
To exemplify, with the II interface, service provider B connected in country/region 1 can get information for country/region 2 without needing a direct connection to information sources in country/region 2. Same for service provider C, which can get information related to country/region 1 and supply that information to its clients located in country/region 1.

A.3 Security and Privacy

A.3.0 Introduction

In many cases, both direct short-range (direct V2X) and cellular network communications (V2N2X) can be used for the same or similar automotive and ITS applications, noticing different applications characteristics. However, the system architecture and application implementation and operation details when using mobile network communication and interconnected backend systems are fundamentally different from when using direct short-range communication, as explained in clause 5.2. This leads to different ways of handling the security and privacy requirements when using different communication technologies. Related discussions can also be found in other contexts like ITS America [i.17]. This clause provides an overview on how security and privacy are maintained when using cellular mobile networks and backend communications, based on the recently published 5GAA whitepaper V2N2X Security, Privacy, and Data Quality [i.18].

A.3.1 System architecture and ecosystem overview

The system architecture and ecosystem overview of ITS using cellular networks and backend communications for ITS applications is illustrated in Figure A.4 (Source: 5GAA), including system components and interfaces. More information about important operational steps and functions that are needed for the eco-system to support ITS services, e.g. the 'governance', the 'eco-system initialization', as well as other 'key functions' in the run time operation of an ITS application can be found in the corresponding 5GAA whitepaper [i.19] and technical report [i.20]. As summarized in clause 5.2, compared to direct short-range communications, the cellular network-based implementation achieves interoperability at the application and service level, instead of at the radio level. Geo-referencing is used to address ITS stations in the relevance area, thanks to standard IP and message queuing protocols, as explained in Annex B.

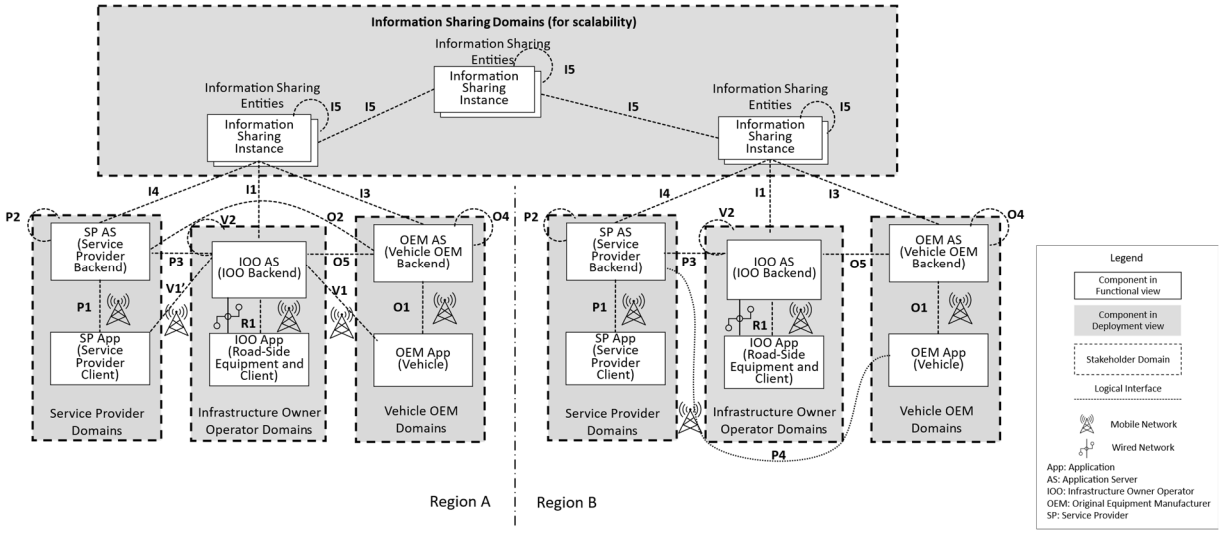


Figure A.4: Applied application layer architecture of ITS using cellular network and backend communications (Source: 5GAA [i.19])

At the bottom of Figure A.4, there are stakeholder domains of Service Providers (SPs), Infrastructure Owner Operators (IOOs) and automotive OEMs. Within the respective domains, as the domain owners, the corresponding stakeholders take the full responsibility. In Figure A.4, multiple instances of SP, IOO, OEM domains are connected to different Information sharing Instances or directly with each other, to illustrate example setups in two regions. The 'Information Sharing Domain' on top of these stakeholder domains is to enable data sharing among the stakeholders. Within the 'Information Sharing Domain' there can be multiple interconnected 'Information Sharing Instances' forming a decentralized system. Usually, one 'Information Sharing Instance' is responsible for a state, region, or country. The 'Information Sharing Domain' can also provide data federation, meaning that one stakeholder domain connected to the 'Information Sharing Domain' can obtain information published by another connected stakeholder domain.

A.3.2 Security

A.3.2.1 Security within a stakeholder domain

Within their own stakeholder domain, a SP, IOO, or OEM is fully responsible for its service and need to meet the requirements of security, privacy, and data quality, etc. The Application Server (AS), i.e. the backend system, and the 'App' and the end user device are operating according to a standard client-server concept over cellular networks. This means security solutions specified by 3GPP are applied, including authentication, encryption etc, though this is provided by the mobile network operators and transparent to the domain owner, but such 3GPP network security features do offer increased security level against attacks and risks to the communication system. Since the communication between AS and App is crucial for ITS application operation and business, it is also protected at the application layer or transport layer using state-of-the-art technology, e.g. Transport Layer Security (TLS). The implementation details of the security solution in a stakeholder domain are decided by the domain owner.

A.3.2.2 Security between stakeholder domains

Figure A.4 shows a number of interfaces between stakeholder domains, i.e. P2, V2, O4, O2, O5, P3, P4, V1. These interfaces may be based on bilateral agreement between stakeholders. Figure A.4 also shows a number of interfaces between stakeholder domains and Information Sharing Domain, i.e. I2, I3, I4, as well as the I5 interface between the 'Information Sharing Instances'. Such interfaces are used when an eco-system for information sharing is established. Participants need to agree on a Common Code of Conduct (CCoC), related contractual conditions, and to pass related authentication and verification, etc., before joining the eco-system as a trusted actor.

If an 'App' (client) in one stakeholder domain needs to communicate with an Application Server (AS) in another stakeholder domain, this is always performed under control by the 'App's (client) backend system. For example, an OEM backend may allow an OEM App in a vehicle to establish a connection to a SP AS. In such case, an agreement should have been established between the stakeholders. Security credentials, AS address information, etc. need to be exchanged between the backend systems prior to the connection establishment between the OEM App and the SP AS. An example for such setup is Automated Valet Parking/Automated Plant Marshalling ([i.21] and [i.22]).

Technically, these communication interfaces are using standard IP technology and security methods, such as TLS with standard X509 certificates, mutual authentication and operate in client-server fashion. The key aspect in this relationship is that everyone involved knows the other party it is communicating with, i.e. knows the responsible entity/entities if security or data quality is compromised. When Information Sharing Instances (ISIs) are used, additional functions monitor behaviour.

A.3.2.3 Credential handling for security domains

The AS entities used for communicating with other stakeholders are separated from the stakeholder internal domain and therefore use different certificates for related communications, keeping the internal security domain isolated from the external security domain.

In the initial stages/rollout of the solution - or indeed if only a limited number of stakeholders establish backend communication links for information sharing - bilateral agreements may be used, and security credentials (e.g. X509 certificates) can be provided by either party. However, as the ecosystem of interconnected actors in a V2N2X solution scale up and begin to use ISIs, then it is reasonable and helpful to employ one or a few common Root Certificate Authorities (CAs) to create common trust anchor(s) for backend communications, i.e. leverage standard IT technology and CAs and create a trust domain with a dedicated PKI for the ecosystem. Common trust anchor(s) can help to align efforts, avoiding individual solutions on each connection, thus allowing greater flexibility, e.g. redirecting stakeholder connections to other actors using the same trust anchor, which in turn optimizes the data path to a data source. Redirects like this could prove useful when large amounts of data are involved or more time critical data needs to be transferred, such as Signal Phase and Timing (SPaT) data.

Furthermore, for scalability and operational reasons, intermediate CAs could be used to issue and distribute the X509 certificates to the approved actors. Depending on the trust model agreed, the X509 certificates could be used for signing shared information to help trace the originator. Alternatively, trust may instead be based on agreements among actors, complemented by technical measures such as adding an actor identifier to the shared information, applying validation steps for shared information and logging, and other approaches to further ensure traceability.

A.3.2.4 Interaction between different security domains

If a stakeholder is a trusted actor in the V2N2X domain, in which stakeholders adhere to a Common Code of Conduct signs and respect the contractual terms regarding data quality, security, validation, etc., and if the stakeholder is also enrolled in the short-range direct communication domain, adhering to the rules applying to that domain, the stakeholder can act as a bridge between the domains. This means stakeholders receiving a message via direct communication can verify the quality and take responsibility for the information before sharing it with other interconnected backend systems, or via the Information Sharing Domain. If stakeholders obtain information from interconnected backend systems or the Information Sharing Domain and intend to forward it with direct communication, the stakeholder can create a message according to the standard used in the direct communication domain.

NOTE: It is up to the owners of the interacting security domains to decide, whether and how the ITS messages should be signed using ITS digital certificates. In case signing messages with ITS digital certificates is needed in the respective domain, clauses 4.4.1 and 4.4.2 in ETSI TR 103 630 [i.5] provide examples of how the message can be signed. It is worthy mentioning that signing message is independent from, and can be considered as extra security method to, the security solutions described in clauses A.3.2.1 to A.3.2.3 of the present document.

A.3.3 Privacy

Privacy should be governed by contracts and the agreed CCoC, complemented with technical measures. **For communication within a stakeholder domain**, e.g. between an SP AS and the SP App or between an OEM AS and the OEM App, privacy is protected by security measures subject to the decision of the respective party - e.g. using TLS connections for integrity and confidentiality to prevent leakage of sensitive private information. In this case, user consent for the AS whether and how to handle personal data need to be in place as part of user acceptance to access the services.

For communication with and in the Information Sharing Domain, secured connections (e.g. based on TLS) are used for I1, I3, I4, I5 interfaces between authorized and trusted actors, see Figure A.4, to ensure the integrity and confidentiality of the communication. Additionally, for the actual information (payload data) conveyed, before an AS transmits any data in the Information Sharing Domain, it should ensure that the data does not contain personal data e.g. by applying data anonymisation methods. This means if the payload contains personal data, e.g. the data is based on received information from an SP App or OEM App, the AS should remove any private information before transmitting it. Therefore, for V2X use cases which do not require personal information, communication in the backend systems is fully anonymized, because personal information stays only with the party the user has subscribed to, that is service providers and/or OEMs.

If identity information is required by the V2X use case, the AS may use its identification for the anonymized data, e.g. insert a default identifier for the AS. In many cases, an AS improves payload data quality by analysing and fusing multiple inputs from individual SP Apps or OEM Apps. In such cases, it would be normal and common practice for the AS to use its identity to transmit the processed data instead of using individual identification of the SP Apps or OEM Apps.

For V2X use cases requiring two-way communication, e.g. for requesting traffic signal priority and receiving a response, to protect the privacy of the actual requesters, the requesting AS can act as a proxy for the actual requesters. The proxy can allocate temporary identifiers associated with the actual requesters and use the temporary identifiers in the request response message. When receiving a response, the AS can map back to the actual requester. In this way, the personal data of the actual requester is protected.

A.3.4 Further notes on direct V2X and V2N2X

While direct V2X relies on certificate and signatures to verify the authenticity of messages, V2N2X can use different or additional models, including models based on agreements and trust among interconnected actors and complemented by standard IP-based security mechanisms to establish secure data exchange sessions. Direct V2X and V2N2X can use different trust mechanisms; in both cases, the trust mechanisms needs to be suited to establishing the reliability and authorization of the source of an incoming communication to a level that meets the requirements of the receiver. For both modes of communication, it is anticipated that there will be some form of credentialing of sending systems by an authority or service provider, that establishes the performance and security capabilities of the system and requires ongoing cybersecurity management of the system. The requirements for these credentials may differ between the direct and network settings based on other factors, such as the ability of the rest of the system to mitigate risks from malicious senders, but those requirements are expected to be somewhat uniform across the different modes of communication.

It is recommended that both V2N2X and direct V2X application designs consider the possibility that false or malicious data is received (and potentially acted upon) by the receiver, even if there are countermeasures in place to reduce the chance that this happens. If receivers can receive false data and identify it as such, either before or after making use of it, then the application design is recommended to consider how the reception of the false data can be reported to some responsible authority. In the direct V2X case this is known as "misbehavior reporting" and the system security architecture includes a Misbehavior Authority (MA) which collects reports of observed false or malicious data. In the V2N2X case, the appropriate mechanism might be an interface to the service provider which could be defined as part of the application profile for V2N2X, or V2N2X receivers could also report to the same MA if appropriate.

With V2N2X, privacy can also be based on user consent as part of user agreements to access the services, potentially further governed by contracts, complemented with technical measures to anonymize end users.

Annex B:
ITS Message Delivery (Geocast) Solutions

B.1 System architecture and end-to-end message flow

The high-level functional architecture for ITS message delivery solution using cellular infrastructure is illustrated in Figure B.1.

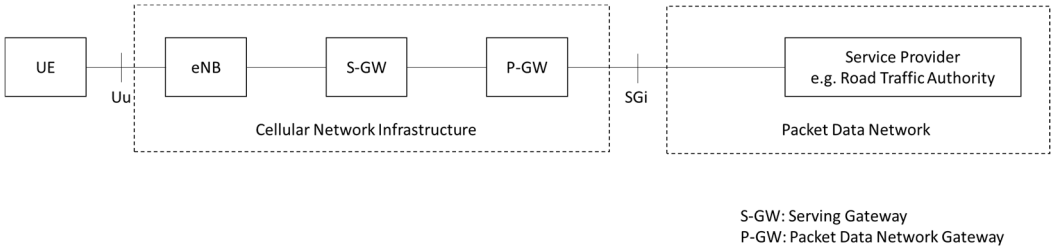


Figure B.1: High level functional architecture of ITS message delivery via LTE cellular network

Following this architecture, ITS message generated at the UE is transmitted via the Uu interface uplink and the cellular network infrastructure to the service provider, which operates the V2X application server in the packet data network. In this context, the packet data network can be Internet or any dedicated IP networks, e.g. Road Traffic Authority networks. The ITS message from the service provider is sent using downlink communication to the UE in the reverse direction.

B.2 ITS message dissemination using IoT messaging protocols, e.g. MQTT

B.2.1 System architecture and end-to-end message flow

Solutions using IoT messaging protocols, e.g. MQTT, follow the same high-level functional architecture for ITS message delivery, as shown in Figure B.1. Following this architecture, ITS message generated at the vehicle ITS station is transmitted via the Uu interface and the cellular network infrastructure to the service provider, which operates the V2X application server in the packet data network. The ITS message from the service provider is sent using downlink communication to the UE in the reverse direction.

The IoT messaging protocols are introduced for addressing specific receiver ITS stations, e.g. by realizing the GeoCast feature. Figure B.2 shows the architecture at the messaging protocol level for a solution using the MQTT protocol for ITS message dissemination.

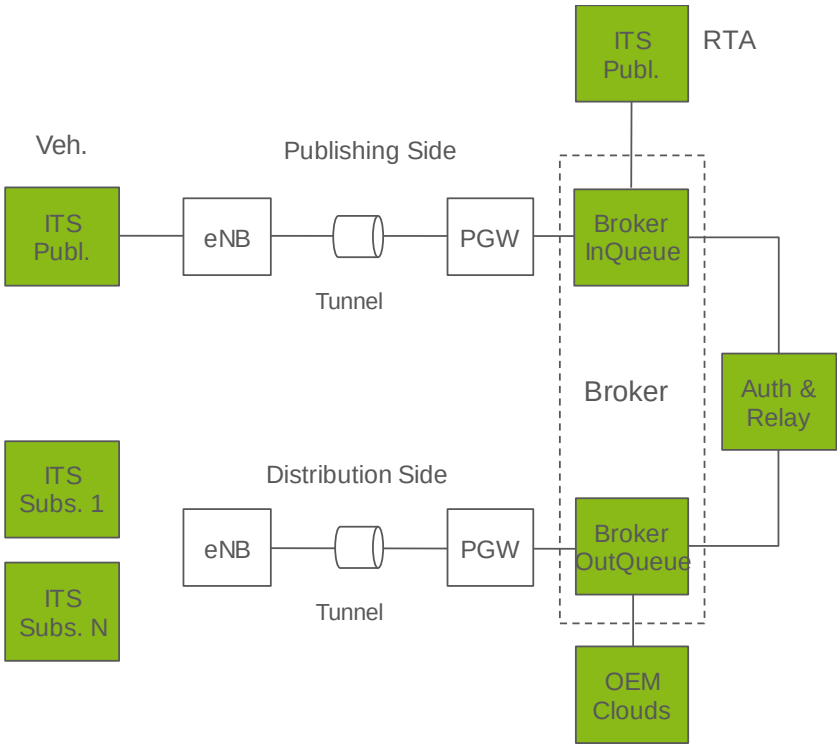


Figure B.2: The architecture of using MQTT protocol for ITS message dissemination

The architecture is separated between publisher side and distributor side. The Auth & Relay function replicates and forwards messages from the input queue, i.e. "Broker InQueue" function, to the correct output queue(s), i.e. "Broker OutQueue" function, of the broker. Only the Auth & Relay function can distribute messages to subscribers, to prevent miss-use and spam attacks. There are many different output queues in the "Broker OutQueue" function. Each output queue is identified by a unique MQTT topic. Note, the MQTT topic may contain information indicating the relevant geographic area.

ITS stations, which can be vehicles or RTA servers, can inject messages into the system. The Auth & Relay function is subscribed to the InQueue and decides (upon message reception), whether the message is trustworthy and whether the message should be forwarded for distribution or rejected.

ITS stations, which are interested in receiving messages for certain relevance areas need to subscribe to the corresponding queue that is associated with the relevance area. An ITS station may subscribe to one or more output queues. OEM clouds may also act as subscribers to the output queues.

B.2.2 Communication protocol stack

Figure B.3 shows the protocol stack for MQTT based solutions. The MQTT protocol operates on top of the TCP/IP protocol stack. Transport Layer Security (TLS) is used to provide secure end-to-end communication between the vehicle ITS station and the MQTT message broker at the ITS service provider. ITS messages at the facilities layer are conveyed as the payload of the MQTT protocol.

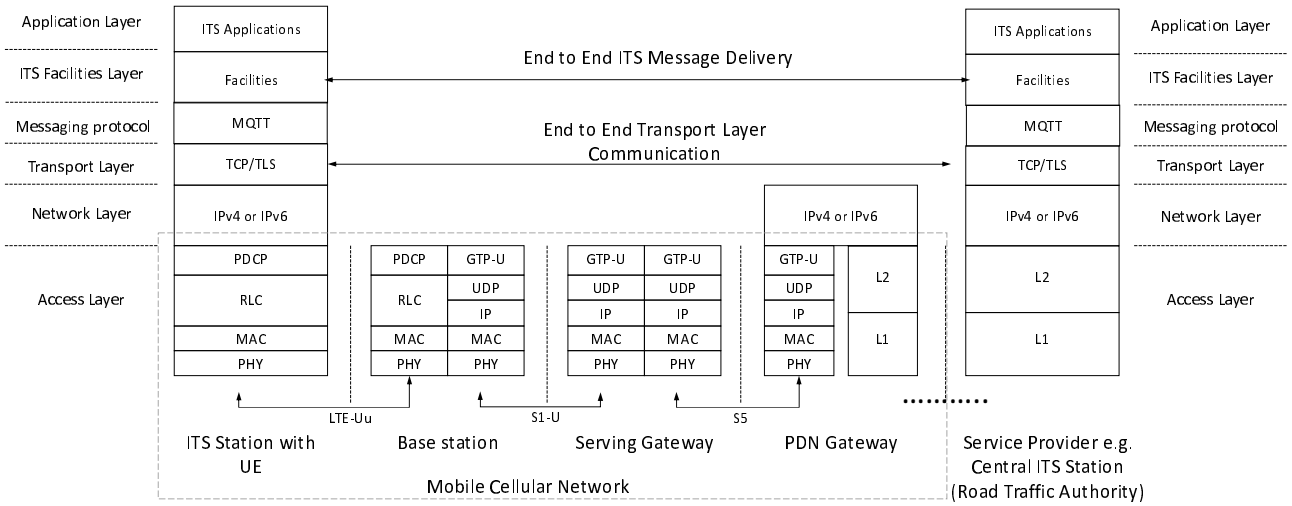


Figure B.3: End-to-end protocol stack for MQTT based solutions

B.2.3 Addressability of ITS stations using cellular uplink/downlink communication

B.2.3.1 Server address for uplink

To use C-ITS services via the Uu interface, ITS stations are pre-configured, e.g. in the V2X application client software, with IP addresses or FQDN(s) of the V2X application servers. When the configuration contains FQDN(s), the ITS stations need to perform DNS resolution to obtain the IP addresses of the servers.

B.2.3.2 Geocast with MQTT in downlink

One way of realizing Geocast with the MQTT protocol is to include geographical information about the relevant area in the MQTT topic. ITS stations can subscribe to different output queues identified by the topics. The ITS station determines the MQTT topic based on its current location and subscribes to the corresponding queue. Messages related to the geographical area are delivered to all ITS stations who have subscribed to the corresponding queue.

NOTE: This solution requires all ITS stations to follow a standard indexing system for geo maps, e.g. QuadTree map.

B.2.4 Security and privacy

The MQTT protocol operates on top of TCP/IP protocol. TLS is used to establish secure communication between vehicle ITS stations and the MQTT message broker at the V2X application server.

Message level authentication according to the EU C-ITS certificate policy may be supported by encapsulating the signed ITS messaged into the payload of MQTT protocol. (See clause A.3.)

B.2.5 QoS provision

In addition to the QoS mechanism defined in 3GPP (see clause A.1.1), the MQTT protocol provides QoS features supporting reliable message delivery at the messaging level.

Annex C:
Numerical results for CAM and CPM load reduction using prediction error

This annex introduces a trigger for transmitting the CAM based on the prediction error, which is the deviation between ITS station's actual position and the predicted position based on its last transmitted CAM. When the prediction error exceeds a predefined threshold, a new CAM is transmitted. The threshold can be configured depending on the applications using the information conveyed by CAM. A higher threshold, i.e. larger acceptable errors, gives larger load reductions, while a lower threshold enables more accurate status information at the receiving stations.

Figure C.1 and Figure C.2 show the normalized channel load of unlink communication, i.e. the load of CAMs transmitted from vehicles to the cloud using the cellular Uu interface. Following three trigger conditions are considered:

1) the transmitting station follows the CAM generation protocol specified in [i.1].

2) the transmitting station follows the same CAM generation protocol as 1) except that the 1 Hz minimum transmission frequency constraint is disregarded.

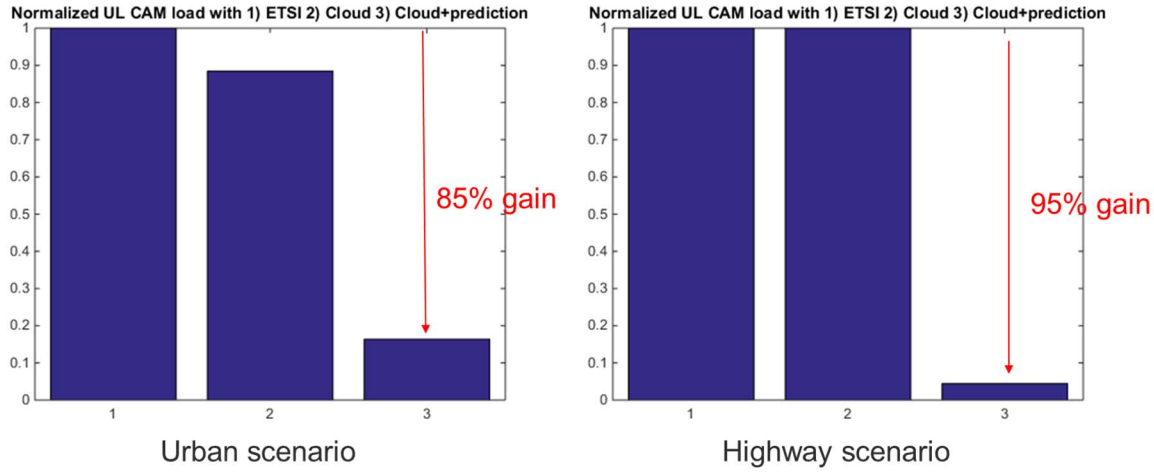
3) uses the prediction error trigger rule on top of 2). Linear prediction is used for deriving the numerical results in 3):

$$s'(t) = s(t_0) + v(t_0) \cdot (t - t_0)$$

$s'(t)$ is the predicted position at time t. t_0 is the timestamp of the latest CAM. $s(t_0)$ and $v(t_0)$ are the position and velocity vectors signaled in the latest CAM. If the prediction error exceeds the threshold t_{err}, i.e. $\|s'(t) - s(t)\| > t_{err}$, a new CAM is generated immediately. Figure C.1 and Figure C.2 show the results of $t_{err} = 1\ m$ and $t_{err} = 0{,}1\ m$, respectively. Table C.1 provides detailed scenario settings.

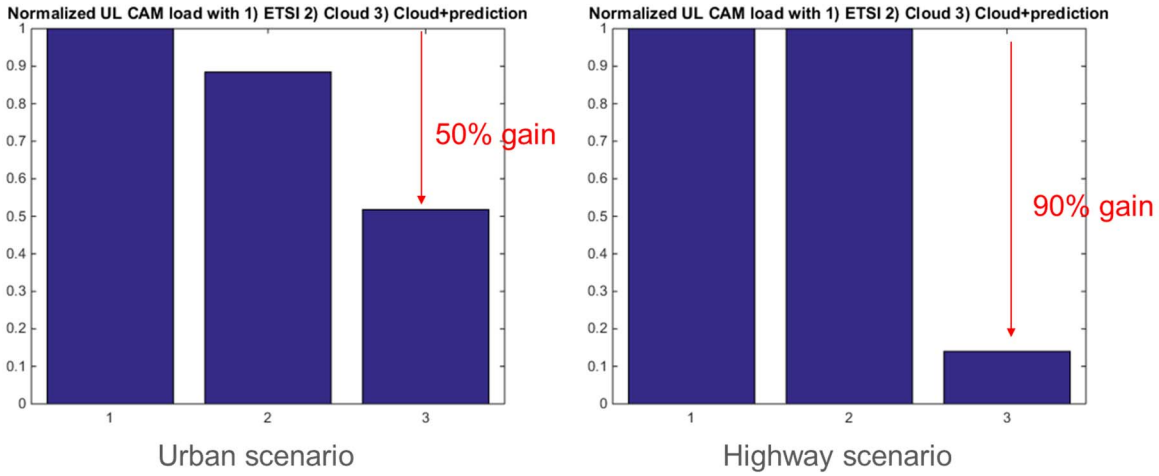
All results are normalized according to the channel load result of 1). Table C.1 provides detailed parameters setting for obtaining numerical results.

It can be observed that up to 85 % and 95 % UL channel load reduction can be achieved with prediction error threshold $t_{err} = 1\ m$, in urban and highway scenarios, respectively. Even with $t_{err} = 0{,}1\ m$, up to 90 % UL traffic load can be saved in the highway scenario.



NOTE: 1) CAM generation rules in [i.1];
2) CAM generation rules in [i.1] without the minimum 1 Hz CAM frequency requirement;
3) CAM generation based on prediction error (t_err=1 m).

Figure C.1: CAM traffic load for cellular uplink communication



NOTE: 1) CAM generation rules in [i.1];
2) CAM generation rules in [i.1] without the minimum 1 Hz CAM frequency requirement;
3) CAM generation based on prediction error ($\boldsymbol{t_{err} = 0,1\ m}$).

Figure C.2: CAM traffic load for cellular uplink communication

Table C.1: Settings for Urban and Highway scenarios

Urban scenarios	Highway scenarios
¼ of vehicles are static ¼ of vehicles at 30 km/h with acceleration $1\ m/s^2$ ¼ of vehicles at 30 km/h with acceleration $-1\ m/s^2$ ¼ of vehicles at 50 km/h	¼ of vehicles at 100 km/h ¼ of vehicles at 100 km/h with acceleration $1\ m/s^2$ ¼ of vehicles at 130 km/h with acceleration $-1\ m/s^2$ ¼ of vehicles at 130 km/h
Vehicles follow linear trajectories	Vehicles follow linear trajectories
NOTE: Velocity based CAM trigger rules in [i.1] is not modeled.	

History

Version	Date	Status
V1.1.1	February 2012	Publication
V2.1.1	May 2026	Publication