A new service advertisement message for ETSI ITS environments: CAM-Infrastructure

Houda Labiod
Telecom ParisTech
houda.labiod@telecom-paristech.fr

Alain Servel
PSA
alain.servel@mpsa.com

Gérard Segarra
VICI
gerard.segarra@viciconsult.eu

Badis Hammi
Telecom ParisTech
badis.hammi@telecom-paristech.fr

Jean Philippe Monteuuis
Telecom ParisTech
jp.monteuuis@telecom-paristech.fr

***Abstract*—Collaborative Intelligent Transportation Systems are almost part of our everyday life. A C-ITS environment can provide numerous services that soon will become essential to roads' users. The latter resides in improvement of road safety, entertainment, and commercial services. However to provide such services, the C-ITS environment needs an advertisement and dissemination service of the latter. Indeed, users have to be aware of the available services in order to request them if needed. Actual standards of service announcement show their limits, especially regarding the support of several communication profiles. For this reason, this paper, describes a new service advertisement message called CAM-Infrastructure. The latter is compliant with ETSI standards and is deployed in a nationwide scale project.**

I. Introduction

In the few last years, automobile manufacturers gave more interest into Collaborative Intelligent Transportation Systems (C-ITS). Indeed, they provided numerous prototypes of vehicles equipped with sensors, dedicated computing hardware and dedicated short-range radio (DSRC) for communication with other nearby vehicles (ITSS-V)[1] or with road side infrastructure (ITSS-R). Furthermore, numerous deployment projects were achieved like SEVECOM, EVITA, PRESERVE, CORRIDORS, CVPS and California PATH.

Within an ITS environment, numerous services such as improvement of road safety, driver assistance, entertainment, and commercial services are provided. In order to achieve these latter, an advertisement and dissemination of the available services is mandatory. In a classical scenario, a service provider such as a PKI, a specific application or even a commercial ad provider sends out the service advertisement message through an ITSS-R, and nearby receiving, vehicles start to disseminate those advertisement messages by forwarding them to other vehicles in their neighborhood [6].

Numerous works and studies were proposed and conducted in the goal to provide efficient and secure service advertisement protocols. However, beyond the different organisms' architectures and requirements, only ISO and IEEE proposed standards: Fast service advertisement protocol (FSAP) described by ISO 24102-5 standard [3]; and Wave Service Advertisement (WSA) defined in IEEE 1609.3 standard [1]. Nonetheless, the latter are compatible only with architectures proposed by their respective organisms. For its part, ETSI propose Service Announcement Message (SAM), which is not yet standardized [2]. In addition, the latter is suitable only for systems using Geonetworking protocol on G5.

Our work is part of SCOOP@F project[2], a french Cooperative ITS pilot deployment project (extended to Europe) that aims at deploying C-ITS in a nationwide scale. SCOOP@F architecture relies on ETSI standards. Thus, WSA and FSAP is not compatible with our needs. Furthermore, SAM does not cover all our needs and requirements. Indeed, in multiple scenarios, we use one hop (face-to-face) advertisement, which is not compatible with SAM.

In order to remedy SAM limits, we implemented a new advertisement message called Cooperative Awareness Message Infrastructure (CAM-I). Its main advantage is that CAM-I is compliant with the CAM existing standard [5]. In this paper we describe the details of CAM-I structure and functioning.

The rest of the paper is organized as follows: Section II gives an overview of the existing advertisement standards and explain our motivation for this work. Section III details the structure of CAM-I message. Section IV describes a comparison of the proposed solution CAM-I with existing alternative messages. Finally, Section V concludes this paper and introduce our future works.

II. Related Works and motivation

Numerous research proposals and studies on services advertisement were conducted. However, since our project concerns a real nationwide deployment project, we will discuss only service advertisement standards.

IEEE propose WAVE Service Announcement (WSA), described in IEEE 1609.3 [1]. In a system implementing the latter, all stations are required to monitor the multi-channel radio Control Channel (CCH). In 1609.3 provider mode, the station transmits a WSA message on the CCH during the

[1]ITS station Vehicle

[2]http://www.developpement-durable.gouv.fr/SCOOP-F-Projet-de-deploiement.html

978-1-5090-2914-3/16/$31.00 ©2016 IEEE

CCH interval. Consequently, since all ITSS are monitoring this channel at that time, they all receive the WSA. The WSA contains a list of the services that the provider will provide during the Service Channel (SCH) interval. It also provides the SCH channel number that they will be using. The services are identified by a code number known as a Provider Service Identifier (PSID). If an ITSS in user mode receives a WSA that contains a PSID of interest, it will switch to the appropriate SCH during the SCH interval and will make use of that service [7].

WSA is only compatible with architectures that deploy IEEE WAVE communication stack. Thus, this solution does not fit needs of SCOOP@F project which relies on ETSI architecture.

ETSI propose Services Announcement Message (SAM), which represents an ITS message that advertises available services. SAM is broadcasted from a ITSS-R on G5's channel CCH using the Geonetworking protocol. Within a SAM, an ITSS-R must provide some specific information such as the list of the available services, the type of target for each services and the communication profile. More specifically, the available services are a list of Service-IDs. The target of the service has the value (All) or a Community-ID (CID) which associates a specific group of ITSS to an ID. The communication profile is identified by a Communication Profile Identifier (CPID).

However, SAM solution is suitable only for systems using Geonetworking protocol on G5, which relies on broadcast of messages. The latter does not suits to SCOOP@F needs, in which it exists scenarios where ITSS-V communicate with ITSS-R in one hop comminication using IP protocol. To remedy these limits and to achieve SCOOP@F needs, we propose a new service advertisement message called CAM-I, compliant with ETSI CAM standard [5].

III. A NEW MESSAGE FOR SERVICES ADVERTISEMENT: CAM-I

A. Global structure

In ETSI architecture, periodic messages called CAM are diffused continuously. In our solution, the available services are advertised via the periodic broadcasting of a specific CAM message by the ITSS-R, called CAM-Infrastructure (CAM-I) message. The latter has almost the same structure as a CAM message sent by an ITSS-V.

As described in [5], a CAM is composed of one common ITS PDU header and multiple containers. The ITS PDU header is a common header that includes the information of the protocol version, the message type and the ITSS ID of the originating ITSS. For an ITSS-V a CAM shall comprise one basic container and one high frequency container, and may also include one low frequency container and one or more other special containers: (1) Basic container: includes basic information related to the originating ITSS. (2) High frequency container: contains highly dynamic information of the originating ITSS. (3) Low frequency container: contains static and not highly dynamic information of the originating ITSS. (4) Special vehicle container: contains information specific to the vehicle role of the originating vehicle ITSS.

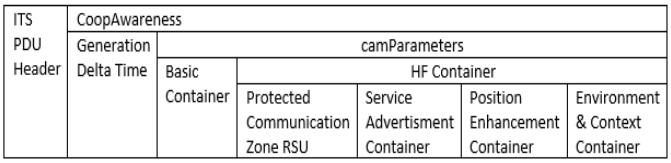

Figure 1: CAM-I structure

As indicated in the CAM standard [5], all CAMs generated by an ITSS-R shall include a basic container and optionally more containers. Consequently, the proposed CAM-I is composed of an ITS PDU Header, a basic container and a High Frequency container composed of 4 containers. Described by Figure 1, CAM-I structure is similar to the one of CAM. Its header (ITS PDU Header) and Basic Container are compliant with the standard ETSI EN 302 637-2 [5]. The ITS PDU header includes the protocol version, the message type, the ITSS-R identifier of the originating ITSS-R. In addition, a generation delta time of the message is included. The Basic Container includes the following fields: (1) The type of the emitting station (ITSS-R): 15; (2) The geographic position of the ITSS-R. While the PDU header and the low frequency are the same as in CAM, we modified the High Frequency (HF) container. More specifically, we defined a HF Container composed of the following containers: (1) Service Advertisement Container; (2) Position Enhancement Container; (3) Environment & Context Container; (4) Protected Communication Zone RSU Container.

Table I describes the structure of the three last containers. Service Advertisement container is detailed in next section.

B. Service Advertisement Container

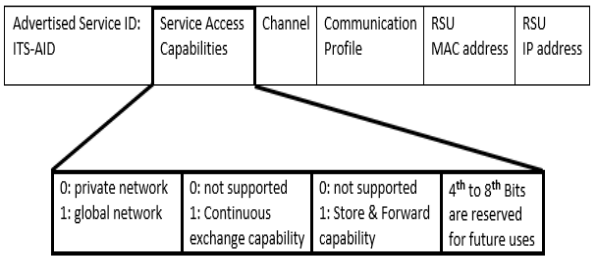

Figure 2: Service Advertisement Container structure

As described by Figure 2, Service Advertisement Container includes the following fields:

(1) Advertisement Service ID: this byte provides the ID of the advertised service.

(2) Service Access Capabilities (SAC): The second byte details access capabilities to (1) a private network such as a network of the road operator that offers an access reserved to its staff, or (2) to a global network like Internet. The choice of

Container	Data Elements	Type	Size in Bytes	Description
ITS PDU Header	Protocol version	same as in [5]		Version 1
	Message ID	same as in [5]		CAM
	Station ID	same as in [5]		ITSS-R identifier
Generation Delta Time	Generation Delta Time	same as in [5]		
Basic Container	Station Type	same as in [5]		ITSS-R
	Reference Position	same as in [5]		Accurate position of the ITSS-R established at installation time
Protected Communication Zone RSU Container	Data elements for Toll collect protection	same as in [5]		for tolling collection
Position Enhancement Container	GPS Position Delta Latitude	same as in [5]		Optional, enable to correct positioning error by comparing the RSU accurate position with the given RSU GPS position
	GPS Position Delta Longitude	same as in [5]		Same as for GPS Latitude
	GPS Position Delta altitude	same as in [5]		Same as for GPS Latitude
	Satellite constella-tion locally available	Integer	1 byte	Enable the use of correction if the vehicle detects the same satellite constellation
	Trace leading to the ITSS-R	same as in [5]		Enable the improvement of the vehicle position and the computation of the time window for RSU exchange
Environment and context container	local mete-orological data	Binary	1 byte	Provide local meteorological data for environmental characterization
	Road envi-ronment	Integer	byte	Provide the road environment type in which the RSU is positioned
	Traffic condition	Integer	1 byte	Provide the current traffic condition

Table I: Global Structure of the proposed CAM-I

access policy for SCOOP@F vehicles depends on the global access policy selected by each road operator. In SAC:

- The first bit indicates if a private access or a global access is available. If it is equal to 1, then the ITSS-R provides access to a private network and if it is equal to 0 ITSS-R provides access to a global one.
- The second bit, when having the value 1, it indicates the capacity of the ITSS-R to establish a continuous exchange with a remote server via the private/ global network. If it has the value 0, then the ITSS-R does not possess this capacity.
- The third bit, when it is equal to 1, it indicates the capacity of the ITSS-R to store locally a message and to transmit it as soon as possible towards a remote server (store and forward) via the private/ global network, as soon as this one is available. If this bit has the value 0, the ITSS-R does not possess this capacity.
- The bits N° 4, 5, 6, 7 and 8 are reserved for a future usage.

(3) Channel: This field contains the channel used for communication
(4) Communication Profile (CP): The fourth byte indicates the communication profile.
(5) RSU MAC Address (RM: This field indicates the MAC address of the ITSS-R.
(6) RSU IP Address (RIP): This field indicates the IP address of the ITSS-R. If IPv4 is supported the field contains the IPv4 address of the RSU. If IPv6 is supported the field contains the IPv6 address of the RSU. If both IPv4 and Ipv6 are supported, the field contains both addresses.

CAM-I messages are encoded in ASN.1 UPER encoding and integrated as the payload of a secured message compliant with the structure described in the standard ETSI TS 103097 [4]. For security purposes, the secured message is signed using the private key of the sender through Elliptic Curve Digital Signature Algorithm (ECDSA). The secured message contains also a field named ITS Application ID (AID). The latter describes the type of message transported by the secured message and its value should belongs to a standardized list defined by ISO organism. The latter is broadcasted via CCH channel with a frequency f as follows : $1\ hertz \leq f \leq 10\ hertz$. this frequency is chosen according to the environment and context needs. As for CAM messages and in compliance with ETSI 103097 standard, for each second, the first sent message contains the sender's certificate. For the rest, just the digest of the certificate, computed using SHA 256 algorithm is sent. Detailed ASN.1 structure of the advertisement container is described by Listing 1.

Listing 1: ASN1 definition of the Service Advertisement Container

```
ServiceAdvertismentContainer ::= SEQUENCE {
  advertisedServiceItsAid
      AdvertisedServiceItsAid,
  serviceAccessCapabilities
      ServiceAccessCapabilities,
  channelUsedByTheAdvertisedService
      ChannelUsedByTheAdvertisedService,
```

```
  communicationProfileUsedForTheService
      CommunicationProfileUsedForTheService,
  rsuMacAddress RsuMacAddress,
  rsuIpAddress RsuIpAddress
  }
AdvertisedServiceItsAid ::= INTEGER(0..
    4294967295)
ServiceAccessCapabilities ::= BIT STRING {
  globalNetwork (0),
  continuousExchangeCapability (1),
  storeForwardCapability (2)
  } (SIZE(8))
ChannelUsedByTheAdvertisedService ::=
    ENUMERATED {
  cch(0),
  sch1(1),
  sch2(2),
  sch3(3),
  sch4(4),
  sch5(5),
  sch6(6)
  }
CommunicationProfileUsedForTheService ::=
    ENUMERATED {
  btpgeonet(0),
  tcpipv4(1),
  tcpipv6(2)
  }
RsuMacAddress ::= OCTET STRING (SIZE(6))
RsuIpAddress ::= CHOICE {
  rsuipv4Andv6Address Ipv4Andv6,
  rsuiPv4Address IPv4Address,
  rsuiPv6Address IPv6Address
  }
Ipv4Andv6 ::= SEQUENCE {
  rsuiPv4Address IPv4Address,
  rsuiPv6Address IPv6Address
  }
```

C. Security material for CAM-I users

in order to use CAM-I service, the ITSS-R should have the authorization to use it. The latter is provided within its certificate. Indeed, ETSI certificates contains (1) a field called ITS AID, which includes the list of the services that the station is authorized to access and use; and (2) a field called ITS AID Service Specific Permissions (SSP), which indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. more precisely, the SSP is a field that includes the different authorized options for each ITS AID. SSPs for CAM-I message are defined using 3 bytes and include three main advertised services: (1) ITSSs' provisioning with certificates from PKI; (2) upload of logs generated by ITSSs; and (3) Data Exchange with specific applications.

IV. Comparison of CAM-I with existing alternatives

In this section we produce, through Table II, a comparison of the proposed CAM-I with WSA and SAM .

Criterion	WSA	SAM	CAM-I
Compatible architectures	IEEE	ETSI	ETSI
Average Packet size			
Advertising channel	CCH	CCH/SCH (A verifier pour SAM)	CCH
Advertised service channel	Any SCH (except CH 172)	SCH2-SCH4	Any SCH
Message emission Frequency	$1\ Hz \leq f$	$1\ Hz \leq f \leq 10\ Hz$	$1\ Hz \leq f \leq 10\ Hz$
security mechanism	Digital Signature: ECDSA	Digital Signature: ECDSA	Digital Signature: ECDSA
access control	MAC layer	MAC layer	MAC layer NACS[3]
Communication profile (Access; Network; Transport)	WAVE+LLC WMSP/IPV6 WMSP/TCP/UDP	G5 GEONET/BTP/	G5 GEONET/IPv6 BTP/TCP/UDP

Table II: Comparison of advertisement services

V. Conclusion and future work

In this paper we have proposed a new message for service advertisement in Intelligent Transportation Systems' environments called CAM-I. The latter is compliant with the existing ETSI CAM standard and is more flexible to support several communication protocols. CAM-I was implemented in SCOOP@F project and support three advertised services: (1) ITSSs' provisioning with certificates from PKI; (2) upload of logs generated by ITSSs; and (3) Data Exchange with specific applications.

For our future works, at short term we plan to study the impact of this solution on the network's overhead and the study of its evolution regarding the infrastructure scalability. For long term perspectives, we plan to submit CAM-I proposal to ETSI organism in the goal to standardize it.

References

[1] Ieee standard for wireless access in vehicular environments (wave) – networking services. *IEEE Std 1609.3-2016 (Revision of IEEE Std 1609.3-2010)*, pages 1–160, April 2016.

[2] Draft ETSI DTS – 102890-2: Intelligent Transport Systems (ITS), Facilities Layer Function, Part 2: Services Announcement . February 2010.

[3] ISO 24102-5 Intelligent transport systems — Communications access for land mobiles (CALM) — ITS station management - Part 5: Fast service advertisement protocol (FSAP). July 2013.

[4] ETSI TS 103 097 V1.2.1: Intelligent Transport Systems (ITS), Security header and certificate formats. June 2015.

[5] ETSI EN 302 637-2 V1.3.2: Intelligent Transport Systems (ITS), Vehicular Communications. Basic Set of Applications, Part 2: Specification of Cooperative Awareness Basic Service. November 2014.

[6] Suk-Bok Lee, Gabriel Pan, Joon-Sang Park, Mario Gerla, and Songwu Lu. Secure incentives for commercial ad dissemination in vehicular networks. In *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '07, pages 150–159. ACM, 2007.

[7] T. Weil. Service management for its using wave (1609.3) networking. In *2009 IEEE Globecom Workshops*, pages 1–6, Nov 2009.