Interacting Advanced ITS Communications with Low-Power Sensor Networks*

László Virág†, József Kovács, and András Edelmayer

Systems and Control Laboratory, Institute for Computer Science and Control
Hungarian Academy of Sciences, Budapest, Hungary
{lvirag, jkovacs, edelmayer}@sztaki.mta.hu

Abstract

Recent achievements of international harmonisation and standardisation of advanced communications technologies for road vehicles and Intelligent Transportation Systems (ITS) allowed the developments of complex cooperative ITS (C-ITS) solutions by paving the way of novel ITS applications emerging from proof-of-concept designs to real industrial implementations. The Internet-of-Things (IoT) is a relatively new concept of communication, by means of which everyday physical objects will be connected to a global network (i.e., the Internet) and will be able to identify themselves to other devices in a uniform way. Based on preliminary results published by the authors, this paper provides a comprehensive idea of how the concept of IoT might converge with the C-ITS field by the assessment of a combined technology and extension of the current C-ITS standards. It also presents the results of integration of the IEEE 802.15.4 networking technology and the 6LoWPAN network protocol in the architecture and operation of ITS Station Architecture. Moreover, convergence methodologies are investigated from multiple views to identify the basic principles and requirements of the new technology for harmonised C-ITS use cases and standards. Reference implementations of the proposed approaches are presented along with the detailed verification of the concept through a road-safety V2X scenario, which was implemented by the authors as part of one of the outdoor C-ITS evaluations performed at the ITS World Congress in 2012.

Keywords: C-ITS, ITS sub-systems, IPv6, 6LoWPAN, IoT, V2X communications, C-ITS communications architecture, ITS station architecture.

1 Introduction

Cooperative systems are playing a more and more significant role in the automotive industry and in global transportation systems in general, particularly with regard to improvement of safety and energy efficiency. The next generation of Intelligent Transportation Systems (ITS) will ultimately rely on mobility technologies and cooperative communication. These new types of systems are already widely referred to as Cooperative ITS (C-ITS) systems. In the C-ITS principle a vehicle communicates with another vehicle or roadside infrastructure with the aim of achieving benefits for many areas of road safety and traffic management. Research and development of C-ITS core technology are dynamically expanding fields of applied sciences, worldwide. A number of ongoing European framework and other national and international projects are in progress (see e.g., CVIS, Safespot, ITSSv6, FOT-Net, FOTsis, Drive C2X) with the goal of developing cooperative transport and intelligent vehicle applications, and testing them in real road environments, which show this tendency clearly.

In principle C-ITS is the realisation of a generalised mobility concept where mobile entities (vehicles) can share information with each other and have access to data, either originated on-board of other vehicles, in remote data centres or embedded in the environment, in a universal way. Invaluable data characteristic to momentary traffic situations or road conditions can be provided by e.g., sensor networks deployed in the immediate vicinity of the roads. The basic idea is that making heterogeneous sensory information available for vehicles enables much faster and more reliable detection of hazardous situations on high speed roads.

Sensor networks are increasingly important technology fields, which tend to converge with C-ITS technologies. Moreover, the integrated concept of sensor networks and the Internet of Things (IoT) has shown to have obvious similarities that have been thoroughly investigated in the past years. Recall that IoT represents an enveloping concept of communication by means of which, everyday physical objects will be connected to a global network (i.e., the Internet) and will be able to identify themselves to other devices in a uniform way. IoT is visioning intelligent buildings, cities and other large IT structures in general, in which a great variety of sensors and actuators are interconnected in a complex global network. Hence the two terms are used sometimes interchangeably.

As sensor networks can be thought of as direct descendants of the enveloping concept of IoT, the generalisation of IoT to traffic and transportation systems (and to C-ITS in general) is a straightforward idea. The quality and quantity of real-time traffic data and other road condition parameters gathered from road structure sensors, as well as the access of any stationary or mobile entity in the global network of things will contribute to better and more efficient response to hazards and incidents. This will enhance management and control of the road network, and thus improve safety and efficiency.

One of the main requirements for an IoT entity (sensor node) is to have low power consumption, low price and the capability of long-term autonomous operation (in some applications up to 2-3 years is required). IoT device design methodologies, therefore, follow a simplistic approach in an attempt to get rid of unnecessary product features and functionalities to reduce power consumption and price. Communication nodes equipped with conventional high-power communication interfaces, such as WiFi or 3G/LTE, cannot satisfy the strict power and performance criteria posed by the IoT. Moreover, the communication protocols commonly used in conventional systems are inadequate to build energy efficient, well compressed and secure connection in a noisy, unreliable and varying environment.

In order to satisfy these criteria the IEEE 802.15.4 [2] standard was created, which defines the physical (PHY) and media access (MAC) layers for the subjected low-power use-cases and communication scenarios. To use this access technology for global interconnection of mobile and static entities in the C-ITS field, a network protocol compliant with existing ITS standards has to be applied.

Due to its simplicity, maturity and vast address space the version 6 of the Internet Protocol (IPv6) could serve the needs of vast number of networks. However, due to the communication overhead problems caused by its default header and data frame size, standard IPv6 may not always be used efficiently in an IoT environment where the main problem is typically to transfer a small amount of data while consuming the least possible amount of energy.

To facilitate the efficient use of the IPv6 protocol over IEEE 802.15.4 the 6LoWPAN [3] protocol family was defined, which features an efficient header compression mechanism to comply with the power requirements. Efficient routing mechanisms, such as Hierarchical Routing over 6LoWPAN (HiLow) [4], Dynamic MANET On-Demand for 6LoWPAN (DYMO-low) Routing [5], 6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD) [6], IPv6 Routing Protocol on low power and lossy networks (RPL) [7], respectively, have also been developed. In the applications of the particular routings to various ITS use-cases, several limitation criteria have to be considered. Applicability of the above protocols in the C-ITS field, therefore, has to be carefully analysed in all applications.

The ITS-S Reference Architecture (ITS-SA) has been the cornerstone of C-ITS technology harmonisation [8, 9] for years, which represents the abstraction of the ITS communication stations in the possible
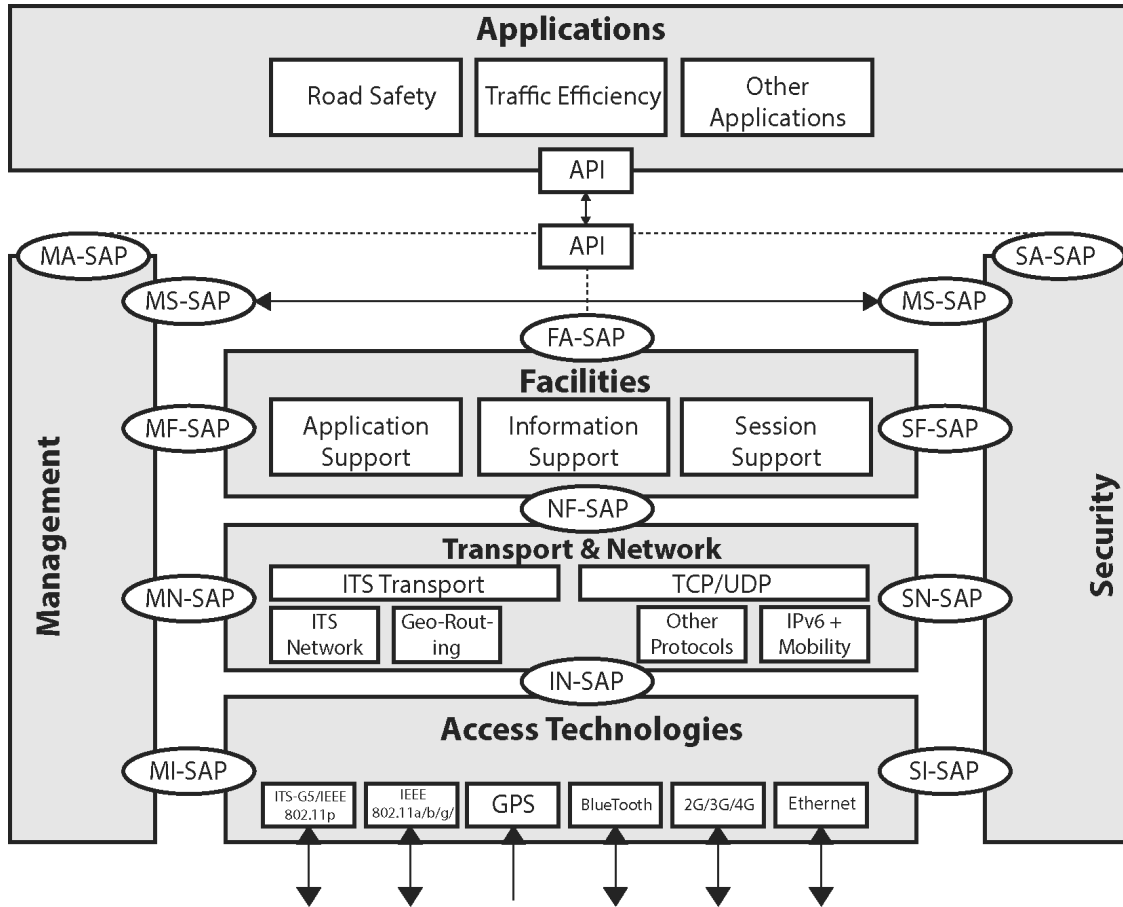
Figure 1: ITS-SA as defined by ISO 21217 and ETSI EN 302 665.

use-cases. Fig. 1 illustrates the layered architecture of ITS-SA, extending the OSI network layers [10] with functionalities of management and security. Information exchange between the main entities of the architecture is defined by the functionality of the Service Access Points (SAPs). In ITS-SA the application layer is connected to lower layers via a so called API block through which facility, management and security SAP related functions become accessible.

Fig. 1 shows the typical access technologies used by the most recent C-ITS concepts, which are represented in ITS-SA. This paper deals with the modification of the access layer, as well as the transport and the network layer of the ITS-SA. Note that the ITS-SA itself is not in the focus of the article.

The combination of the aforementioned technology fields is quite a new initiative. Note that each field has cooperative goals on its own, healthcare [11], pavement management systems [12]. However, the cooperation between 'smart things' and C-ITS is still an open research topic. In order to implement a combined system there is a need for a common network protocol preceded by the feasibility analysis of various routing protocols in both the access and network layers. There are many examples of transparent IPv6 integration of IoT, see e.g., [13], but none of the approaches is capable of formalising the solution into a single, use-case independent architecture for an integrated IoT-ITS purpose. Another ITS-SA extension is introduced in [14] in which the combination of advanced, hierarchical Mobile IPv6 architecture with dynamic mobility features, distribution of the central ITS-S and context- and content-aware optimisation are assessed. Several papers [15, 16, 17, 18, 19] deal with problems assuming the coexistence of the Wireless Sensor Networks (WSN) and the C-ITS in various use-cases. Compliance

with C-ITS standards and the utilisation of general mobility concepts based on IPv6 are not in priority of discussions.

The structure of the paper is as follows. Section 2 introduces the concept of the integration of the novel IoT protocol families in the standard ITS-SA, followed by the unique idea of a decentralised extension of ITS-SA with IoT-ITS routers in Section 3. The feasibility of the proposed amendments of standardised solutions is investigated in a top-down approach in Section 4. The solution alternatives are characterised by a Proof-of-Concept (POC) implementation and its properties are discussed in Section 5. In a series of realistic experiments the performance of the new architectures were investigated, the results of which are briefly discussed and illustrated in Section 6. Section 7 defines new challenges, summarises further research directions and concludes the paper.

2   Extension of the ITS Station Architecture

The proposed adjustment of the ITS-SA, described in the following sections, integrates 6LoWPAN, LLN routing, IEEE 802.15.4 PHY and MAC functionalities which is depicted in Fig. 2. In order to ensure the appropriate configuration and maintenance of the new functionalities, e.g., header compression (HC) management for the 6LoWPAN and routing selection and configuration, extra feature blocks had to be added to the management pane. Another management block makes sure that both the MAC and PHY layer configuration for the IEEE 802.15.4 communication interface (CI) is made properly. The management blocks are connected to the transport and network layer through the Management-to-Network SAP (MN-SAP). The security pane was also extended with the network and transport layer security and authentication management for IPv6 and 6LoWPAN. Moreover, access technologies layer security features (encryption, authentication) and the respective configuration management for IEEE 802.15.4 were also added.

2.1   Access layer

In the access layer the IEEE 802.15.4 feature is added, which includes the MAC and the PHY layers of the CI. The physical layer contains several schemes of frequency allocations conforming to the different regulatory specifications all around the world.

It is also required to examine if these frequency bands interfere with one of the ITS CIs, especially in case of IEEE 802.11p and the commercial Dedicated Short-Range Communications (DSRC) microwave technologies. As IEEE 802.11p and DSRC-based technologies operate in the 5.9 GHz domain and the IEEE 802.15.4 standard defines 2.4 GHz and sub-gigahertz spectrum, further examination is not required. The applied modulation schemes and the other physical layer parameters also satisfy the necessities of the ITS world.

2.2   Transport and network layer

6LoWPAN extension and LLN routing in the transport and network layer of the ITS-SA is implemented by means of the integration of an efficient HC technique and encapsulation methods, which are commonly used in sensor network based IoT scenarios. LLN routing might be based either on RPL or any other suitable routing solutions, which satisfies the requirements of both the C-ITS and IoT needs.

2.3   Management

Management functions are subject to two major modifications in the transport and network layer and the access layer, respectively. The main objective of the transport and network layer extension is to select the
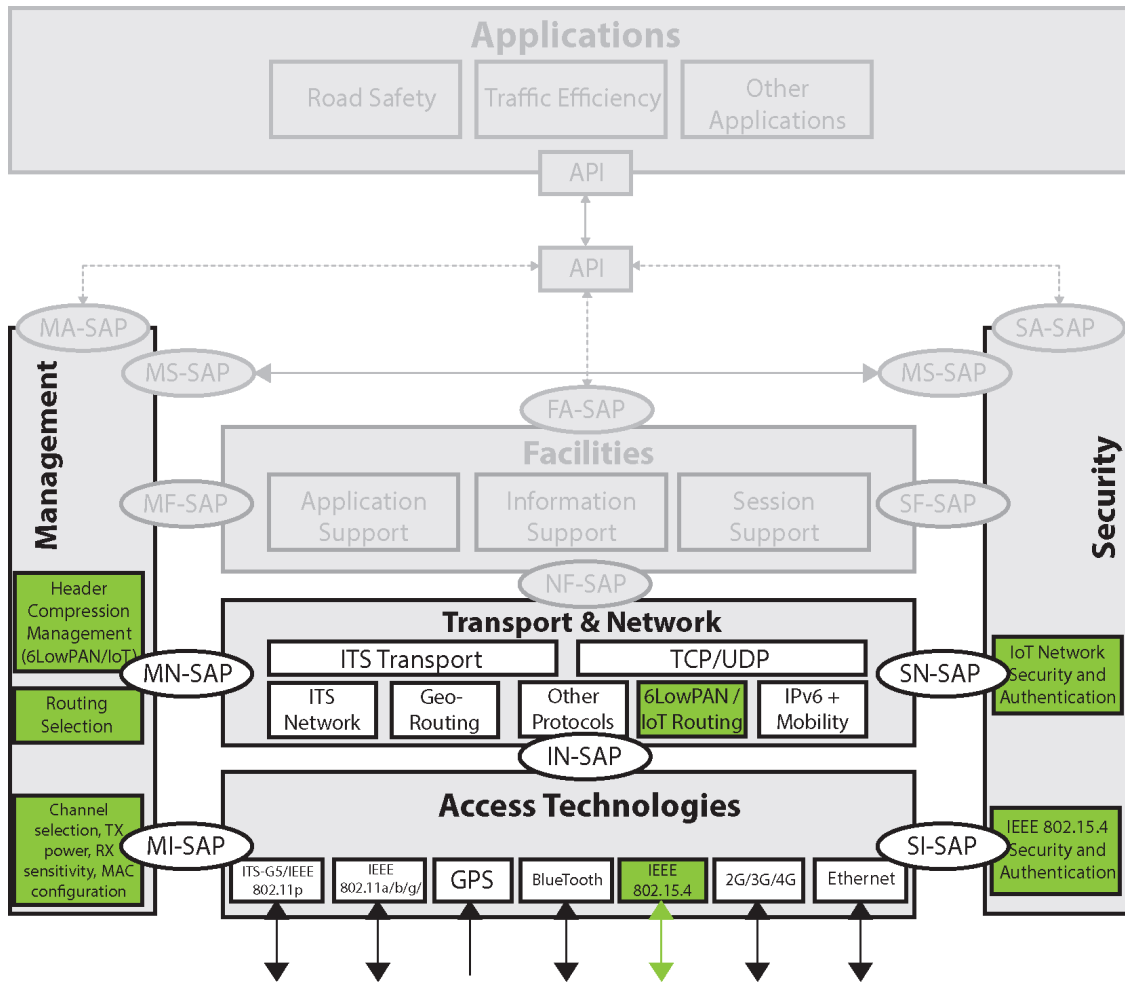
Figure 2: ITS-SA as modified and extended with IoT functionalities.

most efficient HC method and routing scheme. The 6LoWPAN is essentially an IPv6 based communication extension, which is realised by means of an efficient IPv6 header compression and encapsulation method that allow IPv6 packets to be transferred over lower layers in order to suitably fit in an IEEE 802.15.4 data packet. Prioritising algorithms are also included to provide the ability for the selection of the most effective HC and routing method according to the particular use-cases.

The interaction with the transport and network layer is achieved with the help of the Management-to-Network SAP (MN-SAP). The required configuration depends on upper layer decisions whether originated from the facility or the application layer. Monitoring of the correspondent layer activity is also a very important task. Another new component of this entity is responsible for the access control and management through the Management-to-Interface SAP (MI-SAP). This represents the channel selection, TX power and RX sensitivity setup and other physical layer properties. Furthermore, the access layer contains MAC layer functionalities as well as the new IEEE 802.15.4 additions. Thus the management pane has to support and control the MAC layer parameters accordingly. In LLN the synchronisation in the MAC layer is a very important issue, not to mention the different channel arbitration techniques and other significant MAC related processes. Detailed discussion of these features is not in the scope of this paper.

2.4   Security

Recent trends in security research and integration show a positive focus change both in IoT and C-ITS fields, which is also reflected in activities of standardisation. The security pane encloses additional functionality for both transport and network layer and the access layer. The new IoT related functionalities provide security and authentication at different levels. As 6LoWPAN is bound to IPv6 communication in the network layer, various Internet Protocol Security (IPsec) solutions can be applied from the standard IPv6 security and authentication mechanisms [20]. There could also be secure and trustful routing methods to be considered in the security pane, where the technical details of these additions are not subject of this paper.

The IEEE 802.15.4 standard defines security related functionalities, such as data confidentiality, data authenticity and replay protection. These features are configurable and both confidentiality and authenticity are defined on different levels. The encryption keys might be predefined ones or requested from a network coordinator after authentication. In reality these features are often supported by cryptographic engines implemented in hardware which are integrated into the communication interface. As a matter of fact whether it is a hardware accelerated or software implemented security and authentication solution the proper configuration and monitoring shall be placed into the Security pane along with the respective key storage and key management.

3   Decentralised implementation of the extended ITS-S with IoT-ITS Routers

In the previous section the integration of 6LoWPAN and IEEE 802.15.4 into the generalised ITS-SA has been characterised. In this section the concept of distributed implementation of the aforementioned idea, by means of the application of decentralised IoT-ITS routers is presented. The scheme of this concept is shown in Fig. 3, where the new entity, called the IoT-ITS router is defined. The IoT-ITS router is basically a 6LoWPAN border router (from the WSN point of view) complemented by features inherited from the ITS-SA, such as the management and security related ones and the corresponding SAPs.

The architecture is then split in two basic conceptual parts. On the one hand, complex and higher layer ITS stack components are left in a full featured ITS-S along with virtual representation of external functions, which will make the decentralised routing functions accessible. On the other hand, the access technology and network layer, and several security and management blocks are implemented separately in the IoT-ITS Router, which is then connected to one or more full featured ITS-S via the ITS station-internal network using USB, Ethernet or WiFi. With this solution ITS-S Hosts and ITS-S Routers along with their facilities and applications are able to reach IoT and WSN functionalities and the nodes of the sensor network. Fig. 5 depicts a roadside station where several ITS-S entities are present and connected to a separate IoT function capable ITS-S. The new decentralised design layout provides flexible means to implement the extension when involving external IoT devices in the ITS-SA.

The architecture of the newly defined IoT-ITS Router follows the conventions of the ITS-SA. The management and security panes were integrated relying on the functionalities of the corresponding 'native' SAPs in ITS-SA in interaction with the mid-layers. Green blocks in the figure represent the *actual* location of the functionalities, where they are physically located and implemented. Blue blocks are so called *virtual* entities representing the features, which are transparent management elements realised in different ITS Stations.

The virtual entities provide connection to the actual function blocks. The preferred configuration can be done either in the *actual* or in the *virtual* blocks. In the IoT-ITS Router only the transport and network layer security extension is made virtual since several network security for the IPv6 communication is
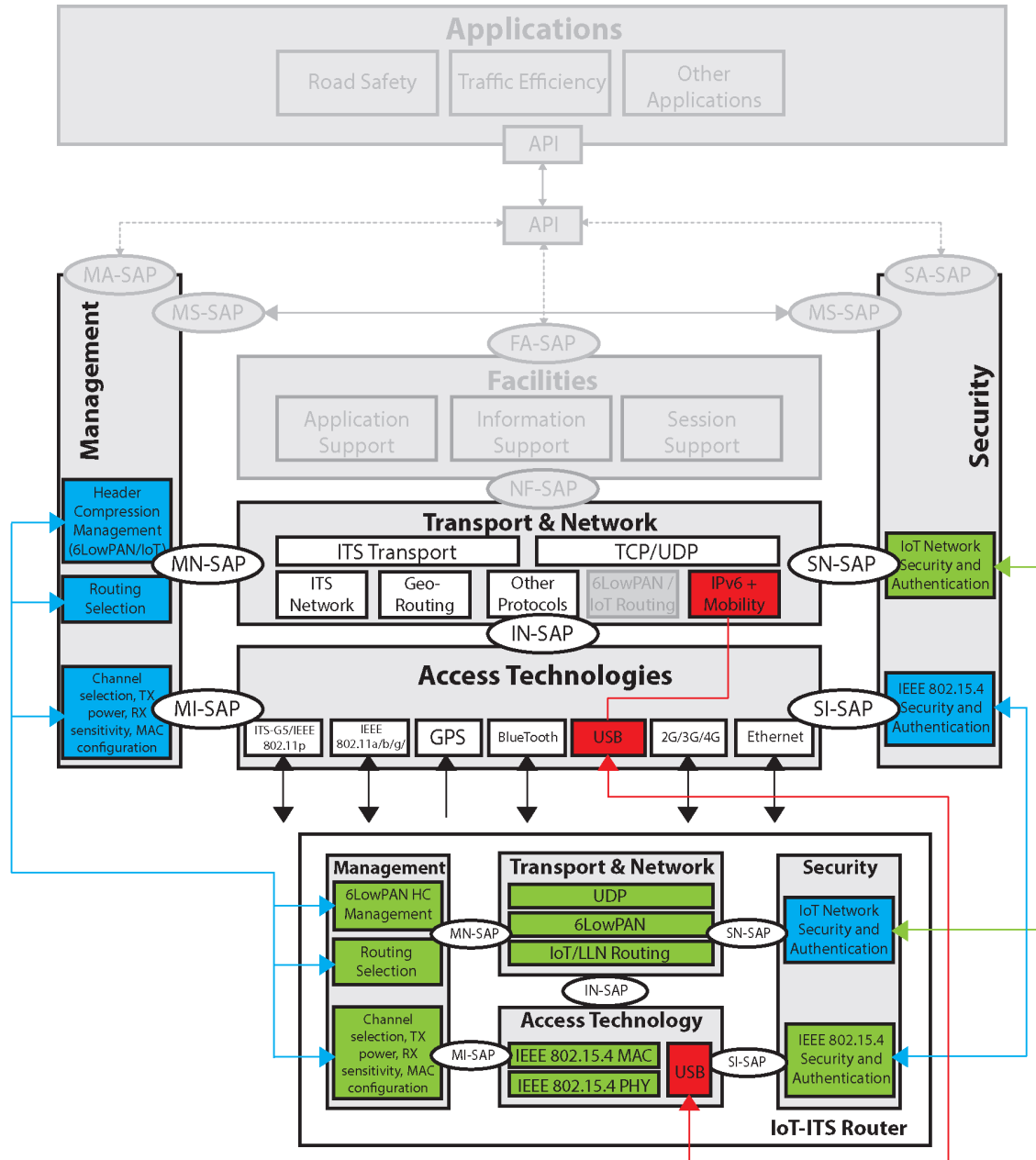
Figure 3: ITS-SA extended with external IoT-ITS Router.

already part of the ITS-SA.

The red block is a USB CI that is not a genuine ITS CI but a standard interface for connecting the IoT-ITS Router to another ITS-S router and ITS-S host (via ITS station-internal network). Obviously, for the connection, one can use any other type of available network CIs as well, thus it can be wired or wireless LAN CI.

3.1   Access layer

The access layer is distributed into two entities. IoT-ITS Router represents an ITS-S router with reduced functionalities, and contains the new IEEE 802.15.4 PHY and MAC related features. The interconnection

with a full-featured ITS station ensured by USB CI or ITS station-internal compatible legacy CI. This method provides a transparent accessibility and intercommunication between the various layers and their function blocks via the SAPs.

3.2   Transport and network layer

The decentralised implementation is realised for the network layer as well. 6LoWPAN and LLN/IoT routing methods are not part of the original ITS station, therefore, their configuration and management need to be considered separately which will be explained in the next section. One of the most elegant methods to eliminate the necessity of these functionalities from the network layer is to use IPv6 based interfacing towards the IoT-ITS Router. Following this idea a completely transparent interconnection can be achieved between the function elements since the IoT-ITS Router is capable to handle all the required 6LoWPAN and routing tasks inside the Bounded, Secure Managed Domain (BSMD). For this purpose the IICP protocol is being developed (by ISO TC 204), which is the specification of a secure ITS station-internal management communication.

3.3   Management

The configuration and monitoring of the layers can be initiated either internally, in the IoT-ITS Router, or *remotely* from the full-featured ITS station via virtual function blocks. These blocks are equivalent to the previously introduced ones, extended with the specific interconnection options. By means of the application of this idea, both entities are aware of all the necessary information about the status of the processes and can interact with them to properly manage the ITS station.

3.4   Security

Security features consist of the same blocks as shown for the management. The network layer related options are left in the ITS-S due to efficiency reasons. Most of these security features are already part of the ITS-S concept, see e.g., IPsec and network layer authentication. The *virtual* pairs of the blocks are placed into the IoT-ITS Router architecture as depicted in Fig. 3. Security options and support are virtually represented in the full-featured ITS station since for lower layer security the methods are often bounded to the access layer.

4   Implementation archetypes and ITS sub-systems

In this section the extensions and new functionalities are discussed in view of the implementation of ITS sub-systems, in a top-down approach. An ITS sub-system is realised by the implementation of an ITS-S along with additional non ITS-SA specific features, such as e.g., in-vehicle ECU network, proprietary road-side functionalities. The distinction between ITS sub-systems comes from the context regarding their form of application. In the C-ITS world there are basically four different types of ITS sub-systems, namely vehicular ITS sub-systems, central ITS sub-systems, personal ITS sub-systems and roadside ITS sub-systems, as briefly illustrated in Fig. 4.

It is to be noted that while this paper concerns roadside extensions only, the idea is not restricted to roadside ITS stations. The proposed amendments of the ITS-SA discussed in the previous sections could be implemented for all ITS sub-systems. Detailed investigation of the feasibility of IoT and WSN extensions to ITS sub-systems is out of the scope of this paper. In a brief summary, the integration of IoT functionalities in personal and central sub-system related implementations are less relevant, but they still represent realistic applications. As a matter of fact, the implementation of this amendment in
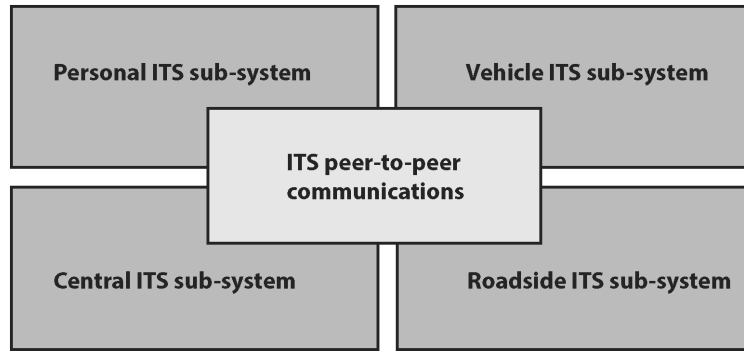
Figure 4: ITS sub-systems.

vehicular ITS sub-systems represent more important use-cases. The roadside aspect, however, plays a crucial role in view of the usability of the new technology extensions. WSNs and Low-power WSNs along the roads are already present and the need for more efficient road monitoring and status reports provided by decentralised WSN is continuously increasing.

For requirement analysis, the previously proposed methods in Section 2 and Section 3 need to be overviewed in a top-down approach in the framework of the roadside ITS sub-system architecture.

Fig. 5 shows the components of a roadside implementation as described in ISO 21217. The roadside ITS sub-system, consists of an ITS-S host, a number of ITS-S routers, ITS-S gateway and ITS-S border router. The highlighted boxes (green and blue) are special ITS stations armed with the IoT capabilities in two different roles. A typical ITS-S host is shown in the upper left corner of Fig. 5. A host device could be integrated into the vehicle as an in-dash screen or a back-seat device for entertainment or passenger information. They can also be stand-alone devices, e.g. smart phones or tablets connected via Bluetooth or WiFi. Every ITS-S router shall contain at least one communication interface to the ITS station-internal network (ingress interface), and at least one CI, as an egress interface, out of the station. The so called ITS wireless CI definition may include multiple and various types of CIs e.g., IEEE 802.11p 5.9GHz based microwave CIs, infrared CI, mobile cellular CI i.e. 3G/LTE. Different types of CIs could be distributed between several ITS-S routers.

For improved stability and for safety critical reasons multiple CIs can be installed within a single station to ensure redundant and parallel channel access, distinguishing direction or lane separation on the road. Generally an ITS-S router lacks of upper layers i.e. facility and application layers. ITS-S gateways connect ITS-S to any proprietary systems via proprietary roadside network. The gateway can be operated either as a firewall or a node which interconnects two different OSI protocol stacks that binds ITS station-internal network with other roadside proprietary networks. ITS-S gateway separates ITS-S hosts and routers from legacy roadside systems. The principle of a border router is to connect a system or station to an external network. This function is quite similar to the gateway with one exception, the purpose of a gateway is to establish a route to another closed and/or internal network while an ITS border router provides access to public networks, such as the Internet. In its extreme, any number and any combination of ITS-S routers and hosts can be included in the architecture.

Fig. 5 shows two new routing entities and one WSN representation. The green and blue boxes implement the concept of the IoT extensions discussed in the previous sections in two distinct approaches. The particular approaches were presented in Section 2 and Section 3, respectively.

In the first approach the IEEE 802.15.4 access technologies and 6LoWPAN network and transport layer extensions could be installed within the boundaries of an ITS station. This represents a fully functional ITS-S router or a combined ITS router-host device, which is capable of WSN interfacing. This implementation is marked in blue in Fig. 5 in the top-down analysis of the integration of ITS sub-
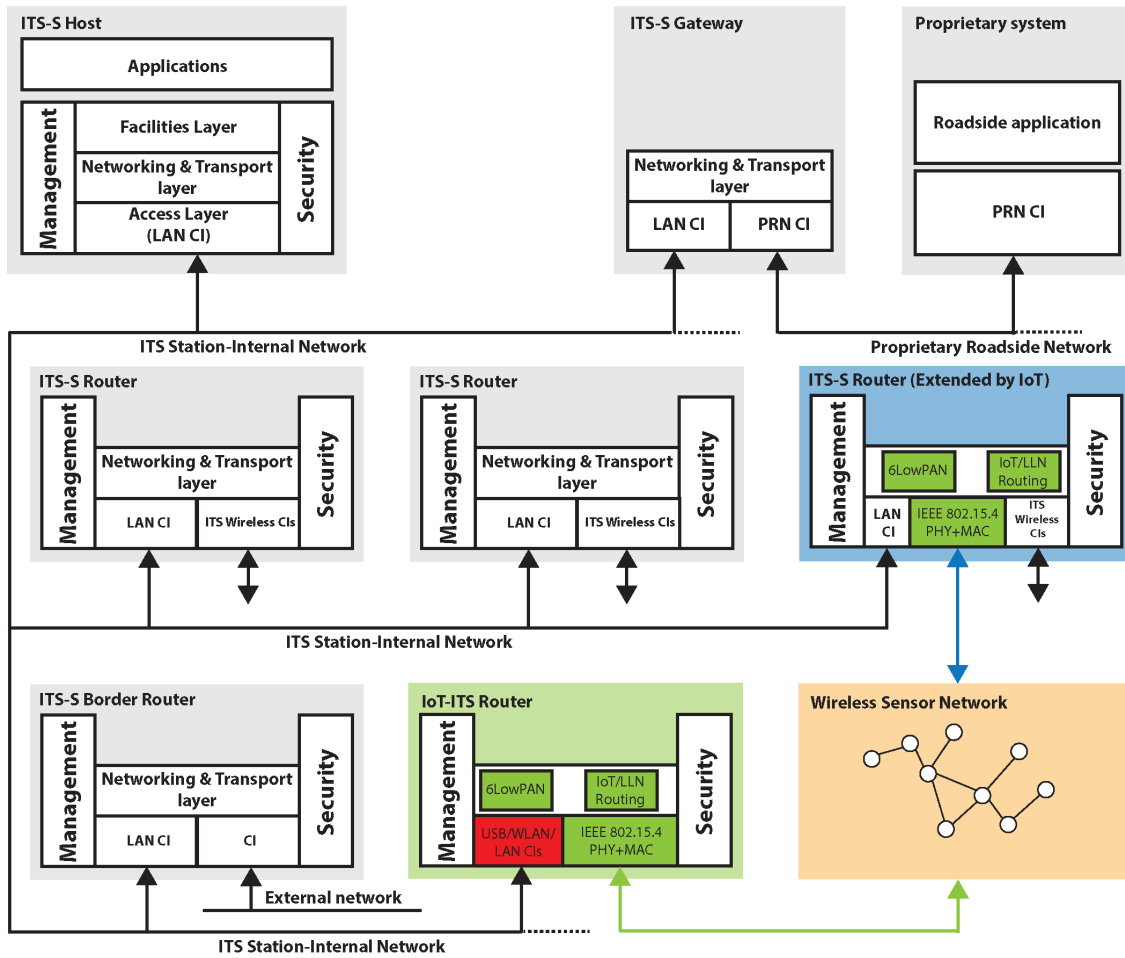
Figure 5: Amendments of ITS-S implementation at the roadside.

systems. This ITS-S router amendment contains the default ITS station-internal CI and ITS Wireless CIs. Due to the integrated WSN access this kind of ITS-S can be considered a standard ITS-S router appended with a new C-ITS legacy IEEE 802.15.4 CI. Thus the extension is capable of seamless interfacing with low-power sensor networks, which fits to the standardised ITS-S concept. This is the simplest way to implement the amendment because the extended ITS-S router includes all the new blocks, which are managed within boundary of the station. As a result, the ITS sub-system concept remains flat.

In another approach some functions are extracted and separated from the ITS-S and implemented as a standalone station (box marked in green). The advantage of the separation is to create the possibility for the connection of the IoT-ITS router to any number of linked ITS-S devices, and to all entities within a particular ITS-S, or ITS sub-stations, which are not WSN capable, via the ITS Station-Internal Network.

The red block in the green entity represents the CI to the ITS station-internal network. This new ITS-S type is close to the concept of the ITS-S gateway and the ITS-S border router since the IoT-ITS router is able to operate in both ways. Nevertheless, it was designed as a reduced functionality C-ITS device relying on virtual blocks implemented in other ITS-S routers.

Both the blue and the green box solutions are capable of low-power WSN communication by means of IEEE 802.15.4 access technologies and 6LoWPAN compatible network and transport features. It is important to note that the communication links established by the proposed solutions are bi-directional, meaning that IoT end-nodes may have access to the ITS networks or the Internet, via ITS-S gateways or

border routers, universally. Further investigation is needed to ensure security and privacy requirements.

5   POC implementation

In order to verify the feasibility of the proposed modifications, a real-life POC implementation was created. This implementation was shown on the joint ITSSv6-FOTsis demonstration event held at ITS World Congress in Vienna 2012. The system presented in Fig. 6 represents a multimodal scenario, integrating several access technologies in multiple ITS stations to demonstrate the flexibility of the combined IoT-ITS architecture in heterogeneous use-cases. The network architecture consisted of vehicle, roadside and central ITS stations, which were interconnected through different access technologies.

In the road deployment (depicted on the left side on Fig. 6) the Commsignia LGN-00-11 ITS router [21] was used as roadside unit (RSU). The RSU, which runs the ITSSv6 C-ITS software stack, was extended by the IoT-ITS router to allow seamless IPv6 access from the ITS-S towards the sensor and actuators nodes deployed along the roadside. The sensor nodes were embedded components in a wildlife crossing guard device that emits sound and light in an attempt to deter wild animals and alert the approaching vehicles on a potential safety issue. Twenty sensors were deployed along the road in a systematic structure. The communication scenario comprised of the following:

Figure 6: POC demonstration setup.
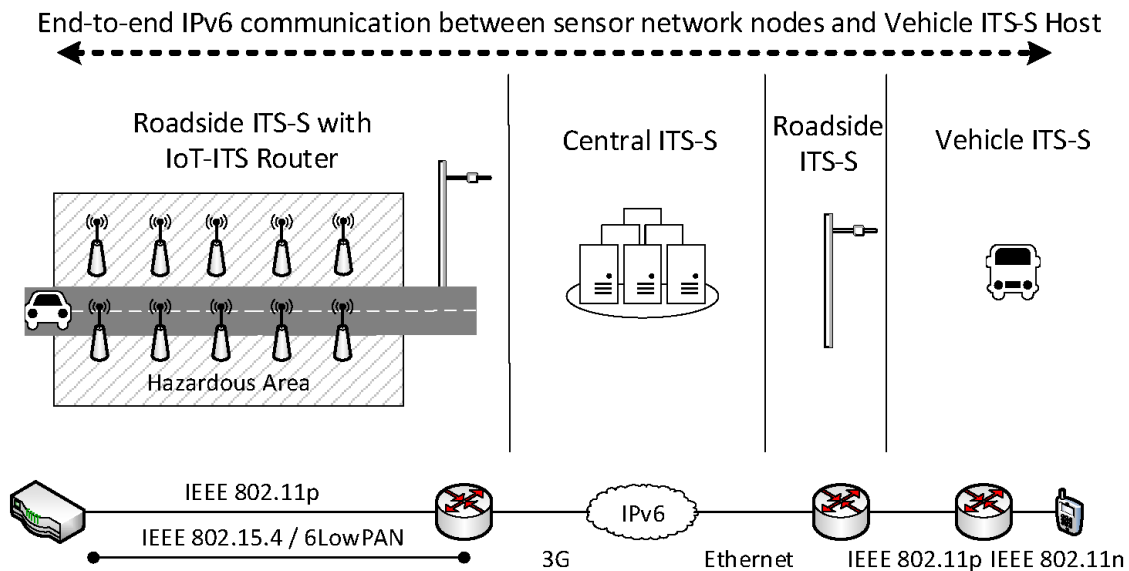
1. Vehicles commuting on the road broadcast Cooperative Awareness Messages (CAM) [22] on IEEE 802.11p radio link via periodic beaconing.

2. By receiving and processing CAM/DENM messages the RSU obtained the position and calculated the distance profile of the vehicles entering the hazardous area.

3. When the roadside ITS-S detected that a vehicle was approaching the predefined geographical area around the dangerous zone it distributed a warning message to the sensor nodes, commanding them to activate the wildlife crossing guard devices. Parallel to this action, the RSU sent alerts to the central ITS-S via the 3G/LTE link.

4. When the central ITS-S received the information about the presence of vehicles in the dangerous zone it decided to broadcast a warning to all roadside ITS-S in the vicinity of the relevant area.

5. The 'Wildlife Crossing' alert messages obtained from the central ITS-S through the roadside ITS-S, were forwarded to vehicles located in the dangerous zone via IEEE 802.11p.

6. The messages were finally relayed from the vehicle ITS-S router to the onboard ITS-S host, which had an HMI implemented on a smart-phone/tablet application. The road safety application also included the sensor data management unit through which each sensor node was made accessible via the end-to-end IPv6 link provided by the extended ITS-SA.

The implemented POC system provided not only road safety warnings to other ITS stations, regardless of the access technology in use, but allowed nodes residing under the supervision of other ITS stations to query either sensor node individually via IPv6 connection since all nodes were addressable using global IPv6 addresses.

6   Experimental evaluation

In a current laboratory work program we aim to collect experience with the design, implementation and operation of the proposed architecture extension. For the verification of the performance in this section round trip time (RTT) measurements for the respective ITS-SA modifications are presented. Model INT and model EXT represent integrated and distributed extensions of the ITS-SA according to Fig. 2 and 3, respectively. The tests were made in laboratory environment using a reference network which consisted of the low-power sensor network (12 nodes) and other ITS-S entities.

Additionally, packet delivery ratio measurements were done between two ITS stations. In this scenario we measured the packet delivery rate between a vehicle onboard unit (OBU), or mobile router (MR), moving on road by constant velocities, and a stationary RSU. These tests were performed on real road segment in real traffic situation. This test provided the maximum ITS-S coverage as well, parameterised by vehicle speeds.

Based on the validation results the model INT and model EXT can be compared with each other in a more complex system, in which other restrictions and design assumptions are to be made.

During the RTT measurements the test network consisted of two ITS-S devices: one of them operated as MR, while the other as RSU. The equipment were Commsignia's LGN-20-00 ITS routers equipped with IEEE 802.11p communication interface along with GPS, WiFI, 3G wireless interfaces. The radio parameters were configured as follows: centre frequency 5.900 GHz, bandwidth 10 MHz, TX power 27 dBm, maximum RX sensitivity and normal MAC priority. The RSU was equipped with 6LoWPAN BR connecting 12 sensor nodes in a 6LoWPAN network. Two types of BR, an externally connected device and an integrated one corresponding to model EXT and model INT were used, respectively. The external BR was a custom designed device based on Atmel ATmega128RFA1 MCU + USB-to-Serial functionalities running a modified version of Contiki OS. The connection of BR to the RSU was made of Ethernet over serial line. The integrated BR was based on Atmel AT86RF232 RF chip interconnected with the RSU via SPI line. The necessary IEEE 802.15.4 and 6LoWPAN layer functionalities were implemented on chip and partially in the Linux OS operated on the LGN-20-00. All sensor nodes were operated under a modified version of Contiki OS.

Based on the above equipment setup and test scenarios full IPv6-based end-to-end data transfers were accomplished and the RTT between the MR and every single sensor nodes were measured. RTT between the MR and the RSU was assumed independent of vehicle (MR) speed. The architecture of the sensor net was configured in a chain-like structure in which every single node could be reached via hop-by-hop
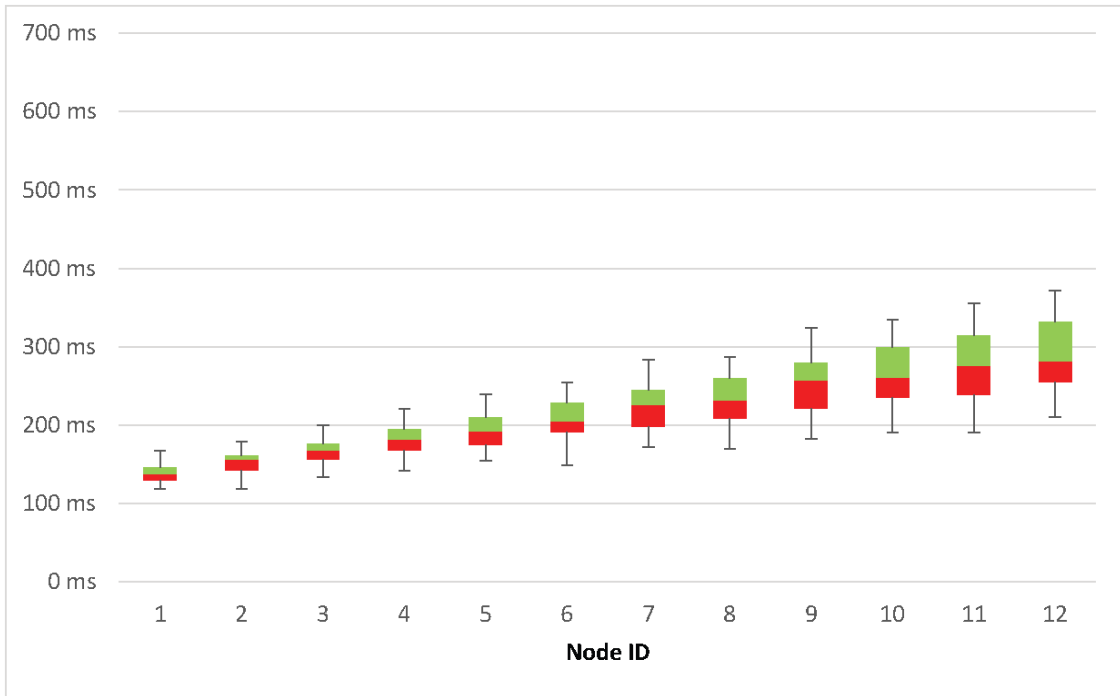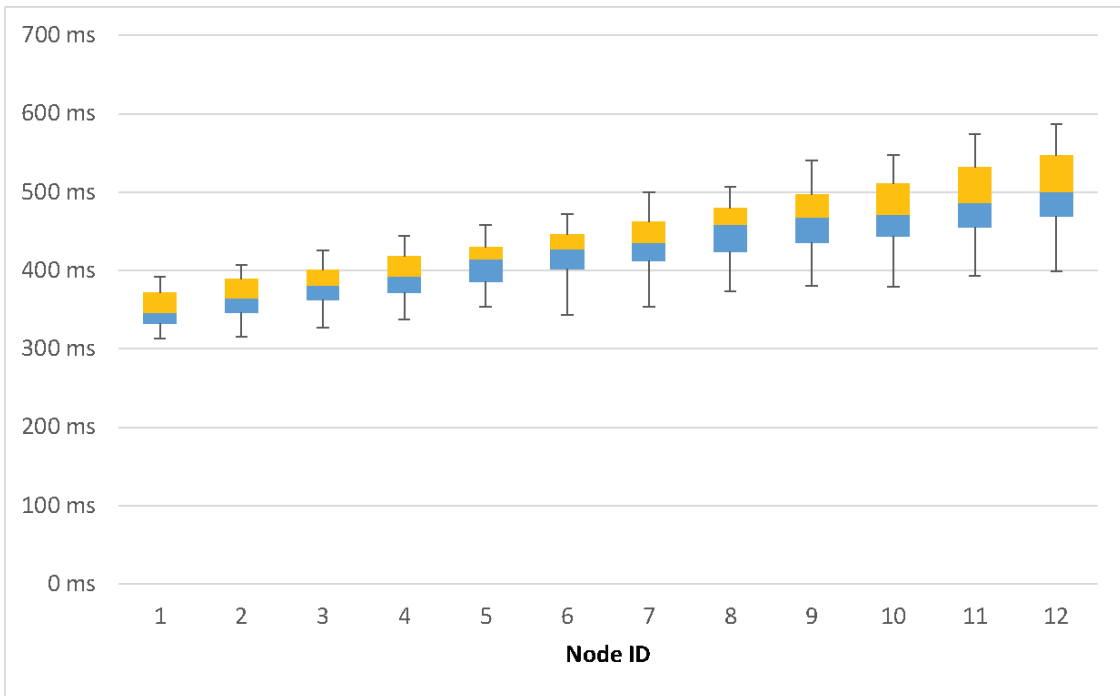
Figure 7: RTT for model INT.

Figure 8: RTT for model EXT.

communication. In other words, every single node represents different architectural level in the sensor network.

RTT values to both models were calculated according to Eq. (1) that sums up the most important
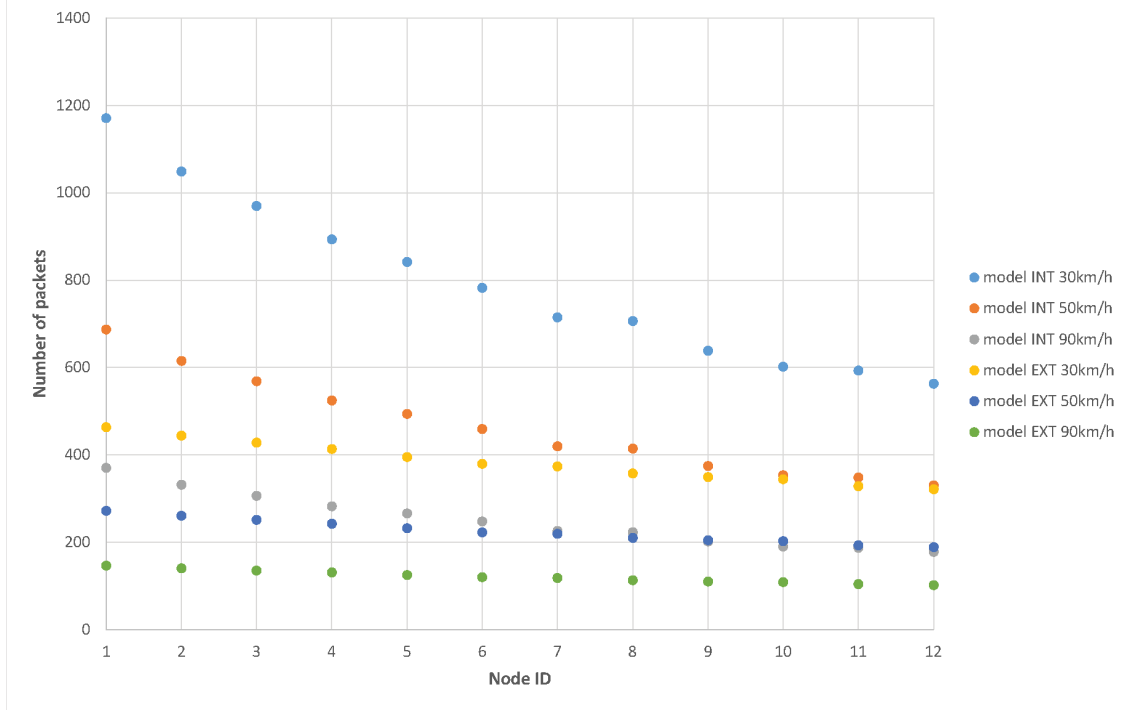
Figure 9: Maximum number of deliverable packets between MR and individual sensor nodes in function of architecture model and vehicle speed.

delays between the end nodes. RTT_n is the overall delay from the MR to the node number n.

$$RTT_n = 2 * \left[\Delta_{802.11p} + \Delta_{RSU_{proc}} + \Delta_{BR_{proc}} + \sum_{i=1}^{n} \Delta_{s_i} \right] + \Delta_{dcycle} \quad (n = 1, \ldots, 12) \quad (1)$$

$\Delta_{802.11p}$ represents the delay of the IEEE 802.11p channel itself and the total of processing delays of the radio SoC. RTTs of model INT and model EXT differ in the delays $\Delta_{RSUproc}$ and Δ_{BRproc} due to the different interconnection schemes. We obviously assume bigger delays in case of model EXT. The delay $\sum_{i=1}^{n} \Delta_{s_i}$ equals to the transmission delay from the BR to the node n of the sensor net. With the inclusion of the dummy value Δ_{dcyle} we model the delay time in the application layer caused by the sensor node application processing, when determining the value of a physical entity (temperature, light, pressure). In our tests a homogeneous sensor net (containing a multitude of identical temperature sensors) was used and Δ_{dcyle} was assumed constant 50 ms as a worst case value.

Fig. 7 and 8 show the Box-and-Whisker charts of the RTT values for model INT and model EXT, respectively. In the course of each measurement scenario 1.000 data packets were sent from the MR to every single node and then, received back correspondingly.

Due to the external BR function processing and the extra transfer time between the RSU and the BR the results are as expected. RTT of model EXT shows higher delay values than model INT. However, the unsubstantial difference suggest that both model application could provide adequate solution in the extension of the ITS-SA when the inclusion of data from sensor networks to C-ITS is required.

The main goal of the next series of validation tests was to find out whether the proposed architecture extensions are capable of serving dynamic communication scenarios in which sensor nodes are attempted to be reached from on-board systems of moving vehicles. Using the test network characterised above a moving MR was used along with the sensor network whose nodes were deployed and evenly distributed

Figure 10: Packet delivery ratio between MR and individual sensor nodes in function of architecture model and vehicle speed.

along the road in 50 m distances, linearly.

PDR measurements with bi-directional packet transfer at variable MR speed (30, 50 and 90 km/h) between the MR and the RSU were performed. Fig. 10 depicts the successful packet delivery rate along with the 802.11p radio coverage which is around 1.280 m, radially. Note that the experiments were made in good visibility conditions. The steep slope at 1.280 m is due to the radio characteristic at the border of the line of sight of reception.

The maximum amount of successfully distributed data packets can be calculated based on Fig. 10, and from the RTT values obtained for the whole IEEE 802.11p coverage between the MR and a particular sensor node. These values can be estimated in the whole coverage from Fig. 9 which contains the values of the maximum number of deliverable data packets for various speed and architecture extension models assuming the radio links in the sensor network are considered ideal compared to the radio link between the ITS-S's. By this consideration Fig. 10 may characterise the end-to-end communication properties and the packet reception probability between the MR and the nodes in the sensor network. Moreover, since the nodes in this linearly chained network topology represent 12 different hop levels (depth of network), the results can be directly generalised to sensor networks with more complex topology where the depth of network is less or equal to 12.

7   Conclusion and future works

This paper dealt with the theory and practice of the modification of the standardised ITS-SA to low-power sensor networks, and the interfacing with the concept of IoT in general, with using IEEE 802.11p based access technologies. Two approaches for the extension were discussed. One of the approaches integrated sensor technology access in the ITS station architecture, profoundly, while the other assumed the application of external IoT routers attached to any type of ITS stations in a closely coupled architecture. The latter idea was implemented as a separate router (the border router) in an embedded platform

realising the interfaces defined by the extended ITS-SA. The feasibility of the implementation was successfully verified in the frame of a real-life test scenario of the official demonstration program of ITS World Congress 2012 in Vienna.

The successful implementation of the technology showed the usefulness of the integration of IoT functionality in ITS communication use-cases and demonstrated the functionality in several safety and non-safety C-ITS communication scenarios.

Real-life performance tests performed on an experimental scenario revealed that both categories of the proposed architecture extensions can provide adequate solution to the inclusion of sensory data, obtained from sensor networks as part of C-ITS deployments of the future, in a very transparent way.

Reconsideration of the implementation of various SAPs and the intercommunication between IoT capable blocks and conventional building blocks is an essential part of the future work. Additionally, station-internal management in a standardised way, e.g., with IICP is a very important issue, which is to be implemented either within the BSMD of an ITS-S or between internal stations. The application of the concept of virtual communication interfaces (VCIs) can be an effective means to the integration of IoT devices in any similar communication architectures.

Although the POC demonstration scenario focused on the extension of the roadside ITS router, the generalised idea of extended ITS SA permits the utilisation of more general IoT concepts and application frameworks. The authors plan to extend their research towards more general IoT use-cases, where mobility is considered, proving the applicability and accessibility of rapidly varying sensor networks in vehicular environments for a safer and more economical transport in the future.

8   Acknowledgement

References

[1] L. Virág, J. Kovács, and A. Edelmayer, "Extension of the ITS Station Architecture to Low-Power Pervasive Sensor Networks," in *Proc. of the 27th International Conference on Advanced Information Networking and Applications Workshops (AINA'13 Workshops), Barcelona, Spain.* IEEE, March 2013, pp. 1386–1391.

[2] IEEE, "Standard for Local and Metropolitan Area Networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE, 2011, iEEE 802.15.4-2011.

[3] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," IETF RFC 6282, September 2011, http://www.ietf.org/rfc/rfc6282.txt.

[4] K. Kim, S. Yoo, S. D. Park, J. Lee, and G. Mulligan, "Hierarchical Routing over 6LoW-PAN (HiLow)," IETF Internet-draft (work in progress), June 2007, http://tools.ietf.org/html/draft-daniel-6lowpan-hilow-hierarchical-routing-01.

[5] K. Kim, G. Montenegro, S. Park, I. Chakeres, and C. Perkins, "Dynamic MANET On-demand for 6LoW-PAN (DYMO-low) Routing," IETF Internet-draft (work in progress), June 2007, http://tools.ietf.org/html/draft-montenegro-6lowpan-dymo-low-routing-03.

[6] K. Kim, S. D. Park, G. Montenegro, S. Yoo, and N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)," IETF Internet-draft (work in progress), June 2007, http://tools.ietf.org/html/draft-daniel-6lowpan-load-adhoc-routing-03.

[7] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, March 2012, http://www.ietf.org/rfc/rfc6550.txt.

[8] ISO, "Intelligent transport systems – Communications Access for Land Mobiles (CALM) – Architecture," ISO TC204 WG16, April 2010, iSO 21217:2010(E).

[9] ETSI, "Intelligent Transport Systems (ITS); Communications Architecture," ETSI, September 2010, eTSI EN 302 665 V1.1.1 (2010-09).

[10] ISO, "Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model," ISO, November 1994, ISO/IEC 7498-1.

[11] Rohokale, V. M., Prasad, N. R., and Prasad, R., "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," in *Proc. of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE'11), Chennai, India*. IEEE, Feburary-March 2011, pp. 1–6.

[12] A. Ghose, P. Biswas, C. Bhaumik, M. Sharma, A. Pal, and A. Jha, "Road condition monitoring and alert application: Using in-vehicle smartphone as internet-connected sensor," in *Proc. of the 2012 IEEE International Conference on the Pervasive Computing and Communications Workshops (PERCOM'12 Workshops), Budapest, Hungary*. IEEE, March 2012, pp. 489–491.

[13] A. J. Jara, M. A. Zamora, and A. F. Gómez-Skarmeta, "Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things," *Mobile Information Systems*, vol. 8, no. 3, pp. 177–197, 2012.

[14] "A Distributed Dynamic Mobility Architecture with Integral Cross-Layered and Context-Aware Interface for Reliable Provision of High Bitrate mHealth Services," in *Proc. of the 3rd International Conference on Wireless Mobile Communication and Healthcare (MobiHealth'12), Paris, France, LNICST*, vol. 61. Springer-Verlag, November 2012, pp. 369–379.

[15] H. Tao, W. Liu, and S. Ma, "Intelligent transportation systems for wireless sensor networks based on ZigBee," in *Proc. of the 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering (CCTAE'10), Chengdu, China*, vol. 2. IEEE, June 2010, pp. 396–399.

[16] K. Selvarajah, A. Tully, and P. Blythe, "ZigBee for Intelligent Transport System Applications," in *Proc. of Road Transport Information and Control - RTIC 2008 and ITS United Kingdom Members' Conference, Manchester, UK*. IET Publication, May 2008, pp. 1–7.

[17] G. Owojaiye and Y. Sun, "Focal design issues affecting the deployment of wireless sensor networks for intelligent transport systems," *IET Intelligent Transport Systems*, vol. 6, no. 4, pp. 432–432, 2012.

[18] V. Verma, R. Choudhari, S. Singh, A. Singh, T. Mishra, and P. Srivastava, "Intelligent transport management system using sensor networks," in *Proc. of the 2008 IEEE Intelligent Vehicles Symposium (IV'08), Eindhoven, The Netherlands*. IEEE, June 2008, pp. 991–996.

[19] J. Xiangyu and W. Chao, "The Security Routing Research for WSN in the Application of Intelligent Transport System," in *Proc. of the 2006 IEEE International Conference on Mechatronics and Automation (ICMNA'06), Luoyang, Henan, China*. IEEE, June 2006, pp. 2318–2323.

[20] J. H. Lee and T. Ernst, "Security issues of ipv6 communications in cooperative intelligent transportation systems (poster)," in *Proc. of 2011 IEEE Vehicular Networking Conference (VNC'11), Amsterdam, The Netherlands*. IEEE, November 2011, pp. 284–290.

[21] "Commsignia LGN-00-11 multimodal V2X communication platform," Web page, Last Visited April 2013, http://www.commsignia.com.

[22] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," ETSI-TS, March 2011, eTSI TS 102 637-2 V1.2.1 (2011-03).

Laszló Virág is a research associate at Institute for Computer Science and Control, Hungarian Academy of Sciences (MTA SZTAKI), Budapest, Hungary. He is currently pursuing his PhD in Computer Science and Information Technology at the Széchenyi István University, Győr. He received his MSc in 2008 from the Budapest University of Technology and Economics (BUTE) in electrical engineering at the Department of Automation and Applied Informatics. He was involved in several automotive and embedded projects in the past years, such as in the European FP6 CVIS, ITSSv6 FP7 projects. Now he is working on ITS communication related tasks and examine the possibilities of the integration of the concept of the Internet of Things into the ITS world.

József Kovács (MSc) is a research associate at Institute for Computer Science and Control, Hungarian Academy of Sciences (MTA SZTAKI), Budapest, Hungary. He is a PhD student in Computer Science and Information Technology at the Széchenyi István University, Győr. He received his MSc degree in Information Technology at Budapest University of Technology and Economics (BUTE). His main interest is communication protocol research and development for vehicular (VANET) and ad-hoc sensor networks. In the past years he participated in several mobility related research projects with special focus on the use of Mobile IPv6 protocols, non-IP V2X protocols and performance analysis of VANETs. Currently he is lead developer at MTA SZTAKI, working on C-ITS research projects.

András Edelmayer (DSc) is a research advisor at Institute for Computer Science and Control, Hungarian Academy of Sciences (MTA SZTAKI), Budapest, Hungary. He holds engineering degrees in mechanical and electrical engineering, specialised in control and computer sciences, communications and information technologies. He holds scientific degrees from universities (PhD) and degrees obtained from the Hungarian Academy of Sciences (CSc,DSc). He owns the academic degree Dr. Habil and is a full professor at many universities. He was the principal investigator in many control and IT related projects in the past 25 years. He has been working in fault detection and various topics of dependable dynamical systems for more than 20 years. His latest research interest is in intelligent vehicle communications technology and cooperative communication. He is the author of more than 70 technical papers in refereed journals and conference proceedings. He served on several conference program committees as member or chair.