Extension of the ITS Station Architecture to Low-Power Pervasive Sensor Networks

László Virág, József Kovács, András Edelmayer
Systems and Control Laboratory
Computer and Automation Research Institute, Hungarian Academy of Sciences
Budapest, Hungary
e-mail: {lvirag, jkovacs, edelmayer}@sztaki.mta.hu

***Abstract* — Recent achievements in the Intelligent Transport System related research induced the need for further extensions of the newly standardized ITS Station Architecture, integrating an increasing number of emerging new technologies. In this paper preliminary results of the integration of the 6LowPAN protocols related to the use of the IEEE 802.15.4 based access technologies in the generalized ITS Station Architecture are presented. By means of this extension ITS communications open up new possibilities towards the inclusion of emerging technologies, such as the implementation of sensor networks in various safety and non-safety road and vehicle applications and the harmonization of the architecture with the principle of the Internet of Things. The proof of concept implementation of the design has been integrated into a multimodal V2X road-safety scenario, where the sensor network is attached to a roadside ITS Station using industry-grade ITS hardware and software. The results presented in this paper introduce the detailed functional evaluation of the application. By formalizing the results, provided by the functional analysis of the scenario, a feasible input is created for the standardization of the protocols in the ITS Station Architecture.**

Keywords: C-ITS systems, IPv6, 6LowPAN, IoT, V2X communication, ITS communications architecture, ITS station architecture

I. Introduction

The next generation of Intelligent Transportation Systems (ITS) will ultimately be relied on mobility technologies and cooperative communication. This new type of systems are already widely referred to as Cooperative ITS (C-ITS) systems. Research and development of C-ITS systems, and the related core technologies, are dynamically increasing fields of applied sciences, worldwide. Several ongoing and successfully terminated European framework and other international projects e.g., CVIS [1], ITSSv6 [2], FOTs [3], Drive C2X [4], Car-2-Car [5] have proven this tendency. One of the most important elements of the ITS technology harmonization process is the construction of ITS Station Architecture (SA) [6][7], which represents the abstraction of the ITS communication stations in the possible use-cases. Figure 1. illustrates the layered description of the architecture, extending the OSI network layers [8] with the management and security pane. Information exchange between each sub-layer and pane is defined by the functionality of the Service Access Points (SAPs). The presented results refer to the modification of the access layer and the transport and network layer of the SA, though, ITS SA is not in the scope of the technical discussion of this paper.

Figure 1. shows the typical access technologies used in the ITS SA, which represent the current ITS use-case concepts. However, there is another, increasingly important technology field, the Internet of Things (IoT). The main goal of IoT related technologies is to interconnect every single electronic "thing" - whether it is the smallest, simplest equipment - into a worldwide accessible network, the Internet. Several ideas have been documented in the past decade regarding the use of sensor networks and the IoT, and the standardization of the related technologies has made very good progress as well. Most of the concepts and ideas are visioning intelligent buildings, structures and cities, which are not really novel, but the global interconnection of them, based on a unifying harmonized way is definitely a pioneering step. The new mobility IP protocol i.e., IPv6 is capable to fulfill these requirements due to its simplicity, maturity and its vast address space. One of the main requirements against an IoT node are the very low power consumption, low price, long operating time (up to 2-3 years) i.e., the capability of long term autonomous operation.

IoT devices are rather simplistic and have no unnecessary features and peripherals. This is not true for communication nodes equipped with conventional communication interfaces, such as WiFi or 3G/LTE, which cannot satisfy these strict performance criteria. The communication protocols commonly used in conventional systems are inadequate or inappropriate to build a basically energy efficient, well compressed and secure connection in a noisy, unreliable and

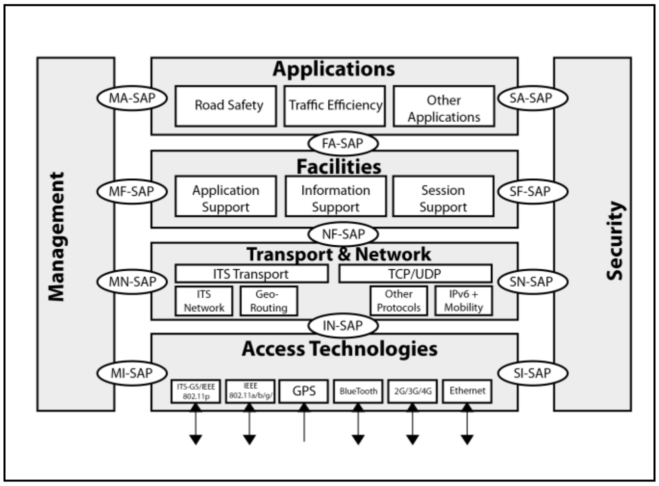

Figure 1. ITS SA defined in ISO 21217 and ETSI EN 302 665

varying environment. In order to satisfy these criteria the IEEE 802.15.4 [9] 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 novel access technology for global interconnection purposes in the ITS field, a network protocol compliant with ITS standards must be used. Due to the size and complexity of sensor networks the IPv6 would be the obvious and logical selection for network protocol, however it is not efficient. Furthermore, there is a need for intelligent and more reliable routing mechanisms. To the efficient use of the IPv6 protocol over IEEE 802.15.4 and in relation to the implementation of the IoT concept, the 6LowPAN [10] protocol family was defined. This features an efficient header compression mechanism to comply with the power requirements. In order to use intelligent and reliable routing mechanisms, such as Hierarchical Routing over 6LowPAN (HiLow) [11], Dynamic MANET On-Demand for 6LowPAN (DYMO-low) Routing [12], 6LowPAN Ad Hoc On-Demand Distance Vector Routing (LOAD) [13], IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [14] on low power and lossy networks (LLN) satisfying ITS use-cases, several limitation criteria must be considered. Applicability of the above protocols in ITS has to be carefully analyzed in all cases.

The combination of the aforementioned fields of technologies is quite a new initiative. Even though, both fields have their cooperative goals by own, e.g., in healthcare [15], pavement management systems [16], the cooperation between smart thing and C-ITS is still an open research topic. In an attempt to implement the combined system the major work items consists of the development of a common network protocol and analysis of the feasibility of various routing protocols in both the access and network layers. There are examples of transparent IPv6 integration of IoT [17], but none of them formalize the proposed solution in a single, use-case independent architecture for a combined IoT-ITS purposes.

In Chapter II the authors introduce concepts for the integration of the novel IoT protocol families in to the standard ITS SA, followed by the description of a proof-of-concept (POC) implementation and functional tests in Chapter III. Chapter IV concludes the paper and Chapter V defines new challenges and further research directions in this area.

II. Concept

A. *Integrated IoT ITS Station Architecture*

In order to eliminate the deficiencies and to integrate 6LowPAN, LLN routing, IEEE 802.15.4 PHY and MAC functionalities, the proposed adjustments of the ITS SA is depicted in the Figure 2. In the management pane further features are included to ensure the appropriate configuration and maintenance of the recently added IoT functionalities e.g., the header compression (HC) management for the 6LowPAN, routing selection and configuration. The aforementioned management blocks are connected to the Transport and Network layer through the Management-to-Network SAP (MN-SAP). A third management block is also added to the left pane to make sure both the MAC and PHY layer configuration for the IEEE 802.15.4 communication interface (CI). On the right side of the ITS-S Architecture, the Security pane is also featured respectively to the network and access layer security and authentication options of the 6LowPAN, Routing mechanisms and IEEE 802.15.4.

1) Transport and Network layer

The Transport and Network layer in the ITS-S Architecture is extended by 6LowPAN and LLN routing features. 6LowPAN extension means the integration of an efficient HC technique, which is commonly used in sensor networks based IoT scenarios. LLN routing might be based either on RPL or any other suitable routing solutions, which are able to satisfy the requirements of both the ITS and IoT.

2) Access layer

In the Access Technologies layer the IEEE 802.15.4 feature is added, which includes both the MAC and the PHY layers of the CI. The physical layer contains several schemes of frequency allocations complying with the different regulatory specifications all around the world. The functionality have to support frequency bands compliant with the international standards. Obviously, if the goal was the compliance with ETSI's regulation, the amendment in the lower layer would not need the configuration options for Japanese or US frequencies.

It is also required to examine if these frequency bands interfere to one of the ITS communication interfaces, especially in case of the IEEE 802.11p and the commercially used Dedicated Short-Range Communications (DSRC). As the IEEE 802.11p and the DSRC operate in the 5 GHz domain this requirement is satisfied since the IEEE 802.15.4 standard defines 2.4 GHz and sub-gigahertz spectrum, basically the ISM bands. The applied modulation schemes and the other physical layer parameters also satisfy the necessities of the ITS world.

3) Management

The Management pane contains two major amendments according to the Transport and Network layer and to the Access layer. On behalf of the Transport and Network layer

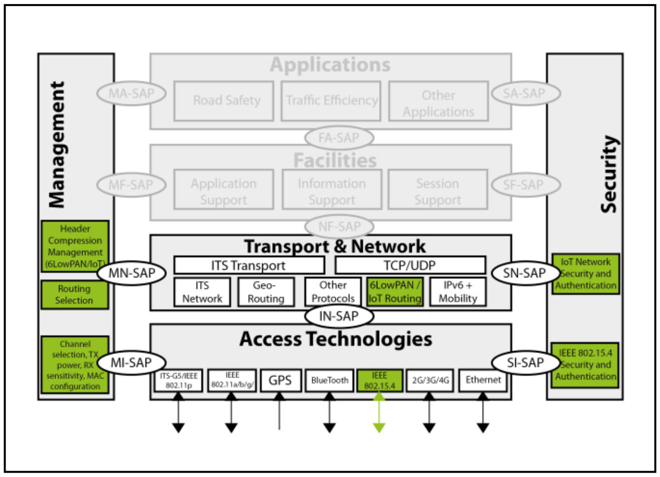

Figure 2. Integrated IoT ITS-S Architecture

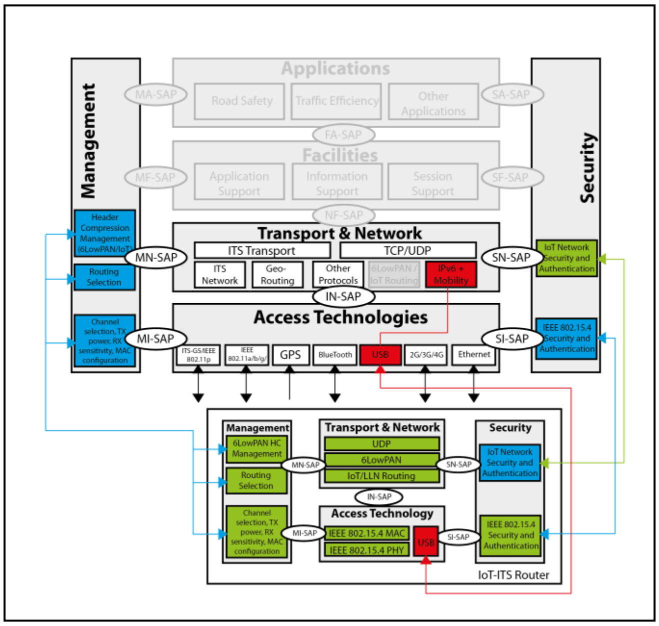

Figure 3. ITS-S Architecture with IoT-ITS Router

extensions the main objective is to select the most efficient HC method and routing scheme. The 6LowPAN is essentially an IPv6 based communication extension, in which the IPv6 header is compressed for efficient data transfer in the lower layer e.g., to suitably fit into an IEEE 802.15.4 based data packet. Different prioritizing algorithms are included to this block to provide the ability to select the most effective HC and routing method according to the use-case.

The interaction with the Transport and Network layer is achieved by means 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 the correspondent layer is also a very important feature of this extension. 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. The access layer also contains MAC layer functionalities as well as the new IEEE 802.15.4 block. Thus the management pane has to support and control the MAC layer parameters as well. Monitoring the MAC layer parameters is also an essential section in this block. In a LLN network the synchronization in the MAC layer is a very important, not to mention the different channel arbitration techniques and other significant MAC processes.

Detailed introduction of these features are out of scope of this paper but the correspondent section of the management pane, which is responsible for their control, is aware of it.

4) Security

Recent trends of research show a positive focus change both in IoT and ITS. In fact, this field of ITS communications becomes more and more important and several research and standardization activities pay attention to improve communication security. The security pane encloses additional functionality blocks for both Transport and Network layer and for Access layer. The new IoT related functionalities provide the possibilities of security and authentication on different levels. As 6LowPAN is bound to IPv6 communication in the network layer, various Internet Protocol Security (IPsec) solutions can be applied or merged from the IPv6 security and authentication prospects [18]. Nevertheless, with specific modifications and restrictions a feasible amendment can be achieved. The discussion of these additions is not scope of this paper. There could also be secure and trustful routing methods, which should be considered in the security pane.

The IEEE 802.15.4 standard, which is one of the new extensions in the ITS-S Architecture, defines security related functionalities as data confidentiality, data authenticity and replay protection. These options are configurable and both confidentiality and authenticity have different levels or can be turned off. The encryption key or keys might be predefined ones or requested from a network coordinator after authentication. In reality these features often supported by hardware cryptographic engines 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 supervising shall be placed into the Security pane.

B. Distributed extension of the ITS-S Architecture with IoT-ITS Router

In the previous chapter the integration of 6LowPAN and IEEE 802.15.4 into the ITS-S Architecture has been introduced. In this section the concept of distributed implementation of the aforementioned idea is presented. The schematic of this concept is shown in Figure 3. At first glance the architecture might look more difficult and more complex than in the previous section. The new design, however, has better properties to realize and verify existing ITS and IoT platforms, proving the concept and predict the efficiency of the system. In this architecture a new entity was defined, the IoT-ITS Router, which is basically a 6LowPAN Border Router (BR) armed with ITS features such as the management pane, security pane and SAPs. This kind of distribution is not new in the ITS field since the different layers and their functionalities, the various CIs can be placed into different and locally separated but connected ITS-S Routers and ITS-S Hosts. This distribution is depicted by Figure 5, in which the IoT extension is connected to a full-featured ITS-S Router. With this solution the ITS-S Host and its facilities and applications can reach the IoT ITS-S functionalities and the sensor network node.

1) IoT-ITS Router

All the new functions in the Transport and Network layer and Access Technologies layer are included by IoT-ITS Router is shown in Figure 3. This is the concept of connecting the desired functionalities with an external router entity, which satisfies the ITS-S Architecture specific requirements. In other words the new IoT-ITS Router Architecture follows similar conventions in its architecture

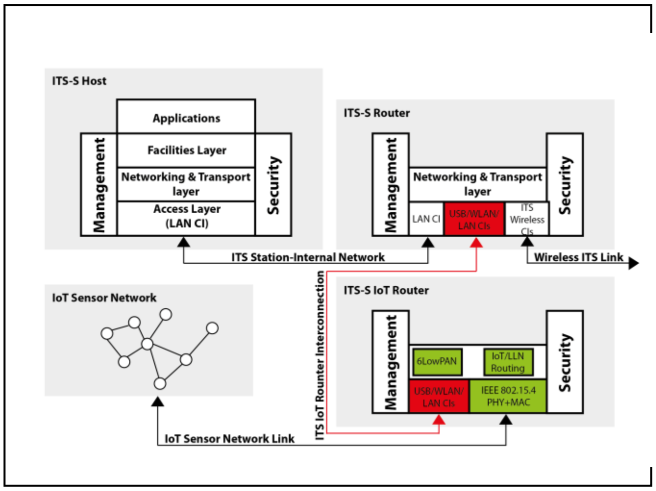

Figure 5. IoT-ITS Router in the distributed ITS Station Architecture

as the ITS-S Architecture. Compatible Management and Security panes were integrated with the analogous SAPs in interaction with the various mid-layers.

Green blocks in the figure represent the real location of the functionalities, depicting where the functionality should operate in the reality.

Blue blocks are so called "virtual" representations of the features which are basically transparent management elements realized in different ITS Stations. The virtual blocks provide the necessary amendments on other ITS entities and create the connection between the actual function blocks. Thus preferred configuration can be done either in the real block or in the virtual one. Accordingly, in the IoT-ITS Router only the Transport and Network layer security extension is virtual since network level security for the IPv6 communication is already part of the ITS-S Architecture. This method does not prevent either the addition of new functionalities locally.

The red block in the IoT-ITS Router is a USB CI that is not a genuine ITS CI but a viable interface for connecting this router to another ITS router and host. This CI could be any other network CIs as well e.g., wired or wireless LANs.

2) *Access layer*

The Access layer is distributed into two entities. IoT-ITS Router represents an ITS 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. This kind of method provides a transparent reachability and intercommunication between the various layers and their function blocks between the entities via the SAPs.

3) *Transport and Network layer*

The aforementioned distribution is true for the network layer as well. 6LowPAN and LLN/IoT routing methods are not part of the original ITS station though their configuration and management need to be considered as the next chapter will explain. 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. Thus a completely transparent interconnection can be achieved since the IoT-ITS Router is able to take care of all the required 6LowPAN and routing tasks inside its boundaries.

4) *Management*

The configuration and monitoring of above layers can be initiated internally in the IoT-ITS Router and "remotely" from the full-featured ITS station via virtual function blocks. These blocks are equivalent with the previously introduced ones extended with interconnection options. In this way, both entities are aware of all the necessary information about the status of the processes and can interact to properly manage the global ITS station.

5) *Security*

The Security pane contains the same blocks as it was shown before. The network layer related options are left in the full-featured ITS station due to efficiency consideration Most of these security features are originally part of the ITS-S concept e.g. IPsec and different network layer authenticity procedures. The virtual pair of this block can be placed into the IoT-ITS Router architecture as it can be seen in Figure 3.

Security options and support are virtually represented in the full-featured ITS station since the methods often bounded to the access layer. Thus realizing this in the IoT-ITS Router is the efficient approach.

III. POC Implementation

In order to verify the feasibility of the above-introduced architecture, a POC real-life implementation was created which became important part of the demonstration scenarios at the Intelligent Transport Systems World Congress, Vienna 2012. The system presented in Figure 4. describes 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 via different access technologies. On the left side of Figure 4. a road segment deployment is depicted, where the Commsignia LGN-00-11 [19] roadside unit was installed running the ITSSv6 ITS software stack. On this network node the ITS hardware and software architecture was extended by a IoT-ITS Router to allow seamless IPv6 connection towards the sensor nodes deployed along the roadside. Each sensor node

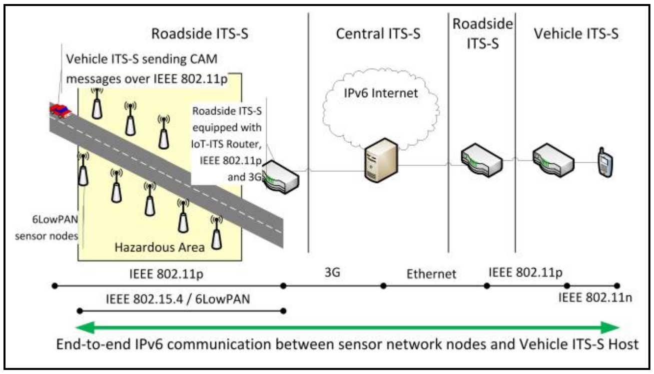
Roadside ITS-S
Central ITS-S
Roadside ITS-S
Vehicle ITS-S
Vehicle ITS-S sending CAM messages over IEEE 802.11p
IPv6 Internet
Roadside ITS-S equipped with IoT-ITS Router, IEEE 802.11p and 3G
6LowPAN sensor nodes
Hazardous Area
IEEE 802.11p
3G
Ethernet
IEEE 802.11p
IEEE 802.11n
IEEE 802.15.4 / 6LowPAN
End-to-end IPv6 communication between sensor network nodes and Vehicle ITS-S Host

Figure 4. Validation Network Architecture

was interfaced with a wildlife crossing guard device, which emit sound and light in an attempt to deter wild animals and alert the approaching vehicles on a potential safety issue. The operation of the demonstration scenario comprised of the following actions:

1. Vehicles on the road periodically send Cooperative Awareness Messages (CAM) [20] on the IEEE 802.11p radio link.
2. The roadside ITS-S obtains the position of the vehicles by processing the received CAM messages and calculates the distance of the vehicle to the hazardous area (sensors deployed along the road segment).
3. When the Roadside ITS-S detects that a vehicle is inside the predefined geographical area around the dangerous zone it distributes a warning message to the sensor nodes, commanding them to activate the wildlife crossing guard devices. Parallel to this action, the roadside also alerts the central ITS-S via the 3G link.
4. The Central ITS-S receives the information about the vehicles and alert status changes and may decide to broadcast a warning to all Roadside ITS-S in the relevant area (operated by FOTsis [21] in the congress demonstration launch area).
5. Vehicles in the area receive the alert messages forwarded by the Central ITS-S through the Roadside ITS-S via IEEE 802.11p.
6. The messages are finally relayed from the Vehicle ITS-S Router to the in-vehicle ITS-S Host, which is a HMI implemented on a smart-phone/tablet application. The applications also include a management interface through which each sensor is accessible via the end-to-end IPv6 link provided by the extended ITS architecture.

The implemented system not only provides road safety warnings to other ITS stations, regardless of the access technology in use, but allows nodes residing in other ITS stations to query each sensor node individually via IPv6 connection since all of the nodes have both global and link-local IPv6 addresses.

This POC setup verified the concept of the ITS-S Architecture extension with IoT functionalities because the distributed Roadside ITS-S router and the IoT-ITS Router were successfully integrated into the reference demonstration in Vienna. The proposed and implemented features and their management facilities were positively functional and interconnected between the distributed ITS Stations.

IV. Conclusion

In this paper we reviewed the current status of the ITS standardization activities regarding to the integration of IoT functionality in the ITS Station Architecture. To facilitate this process, two methods of development were introduced: one of them integrates IoT standards in the ITS station, completely, while the other incorporates existing IoT routers with any ITS station in a coupled architecture. The latter approach was implemented in an embedded computational platform, realizing the interfaces defined by the extended ITS Station Architecture. The feasibility of the implementation was 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 shows the presence of IoT functionality in ITS communication use-cases as a relevant building block for several safety and non-safety scenarios, granting the support for taking further steps towards an integrated standard.

V. Future work

After the successful functional verification of the integrated technology, several aspects of the performance need to be further evaluated. Reconsideration of the implementation of various SAPs that outline the shared interfaces of the standards is an ongoing work item.

Although the above introduced scenario described the extension of a Roadside ITS router, the extended ITS Station architecture does not restrict the usage of IoT applications to the roadside. The authors plan to extend their research with IoT use cases, where excess mobility is considered, proving the applicability of rapidly varying sensor networks in vehicular environments.

Acknowledgement

This work was supported by the European collaborative research project ITSSv6 and partly by the project TÁMOP-4.2.2.C-11/1/KONV-2012-0012: Smarter Transport – IT for cooperative transport systems, which is supported by the Hungarian Government and co-financed by the European Social Fund., which are gratefully acknowledged by the authors.

The authors would also like to express their gratitude to all ITSSv6 and FOTsis partners for the efforts that have been made during the joint ITSSv6-FOTsis demonstration project at ITS World Congress in Vienna, where the subjected solutions were thoroughly validated.

References

[1] “Cooperative Vehicle-Infrastructure Systems.” [Online]. Available: http://www.cvisproject.org.

[2] “IPv6 ITS Station Stack.” [Online]. Available: http://itssv6.eu.

[3] “Field Operational Tests.” [Online]. Available: http://www.fot-net.eu.

[4] “Drive C2X.” [Online]. Available: http://www.drive-c2x.eu.

[5] “Car 2 Car Communication Consortium.” [Online]. Available: http://www.car-to-car.org/.

[6] ISO, “ISO 21217:2010 Intelligent transport systems – Communications access for land mobiles (CALM) – Architecture.” 2010.

[7] ETSI, “ETSI EN 302 665 V1.1.1 Intelligent Transport Systems (ITS); Communications Architecture.” Sep-2010.

[8] ISO, “ISO/IEC 7498-1 Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.” Nov-1994.

[9] IEEE, “IEEE Std 802.15.4TM-2011 IEEE Standard for Local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).” 2011.

[10] J. Hui and P. Thubert, “RFC 6282 Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,” Sep-2011. [Online]. Available: http://www.ietf.org/rfc/rfc6282.txt.

[11] IETF, “Hierarchical Routing over 6LoWPAN (HiLow) - Draft,” Jun-2007. [Online]. Available: http://tools.ietf.org/html/draft-daniel-6lowpan-hilow-hierarchical-routing-01.

[12] IETF, “Dynamic MANET On-demand for 6LoWPAN (DYMO-low) Routing - Draft,” Jun-2007. [Online]. Available: http://tools.ietf.org/html/draft-montenegro-6lowpan-dymo-low-routing-03.

[13] IETF, “6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD) - Draft,” Jun-2007. [Online]. Available: http://tools.ietf.org/html/draft-daniel-6lowpan-load-adhoc-routing-03.

[14] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander, “RFC 6550 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” Nov-2012. [Online]. Available: http://tools.ietf.org/html/rfc65500.

[15] V. M. Rohokale, N. R. Prasad, and R. Prasad, “A cooperative Internet of Things (IoT) for rural healthcare monitoring and control,” in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, 2011, pp. 1–6.

[16] 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 *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, 2012, pp. 489–491.

[17] 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.

[18] J.-H. Lee and T. Ernst, “Security issues of IPv6 communications in Cooperative Intelligent Transportation Systems,” in *Vehicular Networking Conference (VNC), 2011 IEEE*, 2011, pp. 284–290.

[19] “Commsignia LGN-00-11 multimodal V2X communication platform.” [Online]. Available: http://www.commsignia.com.

[20] ETSI, “ETSI TS 102 637-2 V1.2.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service.” Mar-2011.

[21] “European Field Operational Test on Safe, Intelligent and Sustainable Road Operation.” [Online]. Available: http://www.fotsis.com.