Cross-layer Identities Management in ITS Stations

Michelle Wetterwald, Fatma Hrizi, Pasquale Cataldi
EURECOM, Sophia Antipolis, France
{michelle.wetterwald, fatma.hrizi, pasquale.cataldi}@eurecom.fr

***Abstract*— Our lives are going to evolve dramatically in the coming years due to the recent explosion of mobile communications. Intelligent Transport Systems and vehicular networks are one of the resulting vertical applications that are currently being designed and standardized. They are built on the concept of the ITS station, a common reference model inspired from the OSI standard. A first set of operational tests is currently being started or executed, leading to a near future deployment and the emergence of this new type of networks. The need for a comprehensive study of the cross-layer identity management, which constitutes a fundamental element of the ITS architecture, motivated the investigation presented here. In this paper, we analyze the major requirements and constraints that are weighing on the station identity, among which are the privacy considerations and the operational compatibility with the safety applications and communications. In a second step, we define a cross-layer framework that fulfils these requirements and analyze, layer by layer, how an ITS station can be uniquely and safely identified, whether it is a moving station such as a car or a bus, or a static station such as a roadside or central station. When needed, we propose our solutions to the issues that have not yet been completely covered. Some of these proposals have been transferred into ETSI standards and will be tested in the upcoming Field Operational Tests.**

Keywords - ITS systems, Vehicular networks, ITS stations, Identity management, Geo-networking, ITS facilities.

I. INTRODUCTION

The recent spread of mobile communications has lead to the development of a whole set of new vertical applications designed to improve our daily lives with added security, flexibility and respect of the eco-system. In their domain, Intelligent Transport Systems (ITS) will use cooperative vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to provide the drivers and traffic authorities with new smart capabilities for road safety, traffic efficiency, local services or internet access. Innovation in this domain started a few years ago with several research projects such as Sevecom [1] or COMeSafety [2]. Field Operational Tests are now being conducted to execute some real-life evaluations of the designed systems and discover the remaining issues before a public deployment is started. Concurrently, standardization is setting the framework and rules to enable the compulsory interoperability of the future devices. Even though various standardization bodies (including the ETSI [3]) in Europe and around the world are considering this new area, a global agreement has been reached to work with a common framework architecture derived from the OSI (Open Systems Interconnection) model. An outline of this reference architecture is pictured in Figure 1.

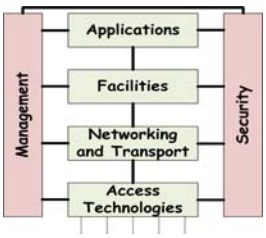

Figure 1. ITS Station Model

The centre part of the ITS station model includes the various layers for the data plane and information transfer. At the top can be found the ITS Applications, supporting the vehicles and traffic operations. Below, the Facilities layer provides the applications with common tools such as the messages management or a Local Dynamic Map (LDM) which maintains a dynamic network topology of the area around the station. Communications are then handled at the Networking and Transport layer, with specific protocols such as the GeoNetworking or more usual ones such as TCP or UDP associated to IPv6. Packets are finally forwarded to the physical network by the Access Technologies layer. On the sides, Management and Security layers provide utilities and support to the data plane layers for an enhanced operation of the station. In practice, the architecture considers a varied set of ITS stations. They can be handheld or personal devices, cars, trucks, public vehicles such as buses or trams, but also traffic lights, variable message signs, traffic monitoring centres, etc… In order to be able to communicate with one another, they must be identifiable in the network and at each layer of the architecture. It is thus needed to define a global set of identities and identifiers satisfying the various constraints of this very specific environment. It should be noted however that some of these identifiers may be reused from the technologies involved in the communication. But some recent studies have shown that the cross-layer configuration and usage of the required identifiers is not yet completely clear, even if many issues have already been addressed by the early operational tests.

We give here a long and yet non-exhaustive list of the various constraints introduced by the ITS environment on the identities management. They are mostly due to the very diverse range of ITS stations and applications. For example, safety applications imply very strict and short delays which require the identities to be easily decoded. Reliability is vital. An ITS

station may have a much longer life cycle than standard electronic devices, the set of identities must thus be wide enough to cover a very large number of objects and guarantee the uniqueness over time. Because of the wireless communications, concerns for security and privacy of the users must be addressed; they apply to all the layers simultaneously. V2V communications are performed in ad hoc mode while V2I are usually linked with some infrastructure; the networking level identities and addresses must be able to cope with both modes. In addition, some ITS stations are moving very fast, others are static, which impacts the range and geographical scope of the identities. Most of the devices, with built-in or external modems, will be multi-mode enabled, with one or several different access technologies [4]: ITS-G5 based on IEEE 802.11p, WiFi (IEEE 802.11a/b/g), cellular (GSM, GPRS, UMTS, LTE and beyond) or Ethernet. Other technologies such as digital broadcast (for example DVB or DAB), infra-red, and satellite systems could also be envisioned. All these technologies already provide their own identifiers. It is thus very important to harmonize their usage and obtain a secure and unique ITS station identification. In summary, the identifiers must be coordinated across the various layers to simplify, strengthen and streamline the transfer of packets while keeping the communications secure and reliable. Our study tried to analyze the existing status and definitions and to provide some innovative yet simple solutions when open points were encountered. Privacy and security have already been developed in details in several projects [5], so we mention them as important factors, but rather focus our work on the other constraints and on the cross-layer configuration and usage of the various identities.

This paper is organized as follows. In section II, we analyze the major constraints weighing on ITS stations identities, e.g. privacy and compatibility with safety applications. Section III is divided into three parts: the first part reviews the access technology addresses, the second part presents a comprehensive framework for the ITS-specific GeoNetwork addressing and the third part proposes an innovative scheme for identifying locally the various types of ITS stations. Finally, section IV concludes the paper with considerations on the study results.

II. CONSTRAINTS

In this section, we provide an overview of the requirements for a framework of the ITS identity management. The identifiers of an ITS station must be unique in order to individually recognize the station during the communication with peer entities in the network. In addition, they could be either updated due to privacy issues or manually configured by applications. In fact, the change of the identity might not be needed only to preserve privacy. Some applications may require a change of identity at any time. In this case, the whole system has to be able to start the procedure for a global change of identity, still ensuring the uniqueness of the identifiers. For example, to perform maintenance tests, network administrators should have high-priority access to change the identifiers of any ITS station at any time. Therefore, to trigger the update process, they need to access the system via a HMI (Human Machine Interface). Applications layer informs accordingly the Management layer which, in turn, handles the change of the identifiers. It is worth mentioning that any kind of identifiers update could lead to a potential violation of the uniqueness requirement.

A. *Privacy Considerations*

Due to the priority given to safety in vehicular communications, it is envisioned that broadcast will be the most common addressing strategy to transmit messages to the wireless medium. For instance, Cooperative Awareness Messages (CAM) are periodic messages transmitted in single hop mode. This type of messages can be seen as preventive messages in terms of safety. They convey information about the state of the sending station (identifier, position, direction, speed, etc.) which are considered as private information but could be received by anybody in the network within one hop distance. Furthermore, if a given station uses the same identifier for a long period of time, an attacker could exploit this vulnerability to conduct malicious actions, e.g. for tracking and location profiling. Therefore, the drivers' personal data need to be protected and must not be visible by unauthorized stations. A station observing the network data exchange should not be able to learn the real identity of another ITS station or know if this given station has performed, or will perform in the future, a specific task.

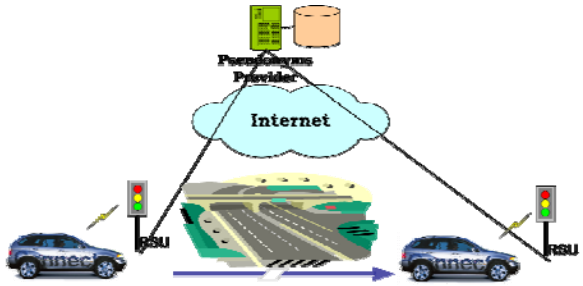

Figure 2. Pseudonyms list retrieval

One possible approach that can be applied is the use of a short-term identity or “pseudonym”. Each ITS station is assigned a pseudonym that is used instead of its long-term identity in the communication process. Pseudonyms are defined as security certificates utilized for signing and encrypting messages. Therefore, they need to be retrieved from a trusted pseudonyms provider as illustrated in Figure 2. ITS stations first obtain a list of pseudonyms from the provider. Then, when all the pseudonyms are consumed, a new connection to the provider should be established in order to retrieve a new list. This mechanism is handled by the Security layer. All the retrieved pseudonyms are provided to the Management layer which is responsible of assigning identifiers to each layer. Pseudonyms must be updated periodically, using a strictly regular or irregular period, in order to avoid malicious tracking of the station The frequency of update should be high enough to guarantee a high level of privacy. Many projects have been working on defining appropriate mechanisms to generate and update pseudonyms. For instance, Sim^{TD} [5] proposed to set a high frequency to change pseudonyms. As a complement, an interface to the applications is also provided to block the update in case of critical situations where the modification of pseudonyms may be considered as a source of

danger. Pseudonyms generation and update is still a topic that needs to be further studied. In addition, to design a reliable identity management entity that would constitute a fundamental building block of future ITS architecture, other constraints need to be considered.

B. Applications and Communications

In the previous section, we assumed that the higher the frequency of pseudonyms update, the better we ensure privacy. Nonetheless, the performance of applications and the communication requirements must be considered as well. From a communication point of view, the change of ITS stations' identity (and especially the frequent update for privacy purposes) influences the performance of the networking and routing protocols. For instance, network beacons, containing identity and position information, are sent periodically. If an ITS station changes its pseudonym too often, neighbours may store in their location table many entries corresponding to the same ITS station. The same problem should be considered in the case of the LDM which stores the dynamic knowledge of the environment surrounding an ITS station at the Facilities layer. In fact, if the change of pseudonyms is not handled correctly, the LDM could record a higher number of surrounding stations because it will consider a message received from a station that just changed its identifier as belonging to a new station. This rather inaccurate description of the station neighbouring environment may worsen the performance of the applications that exploit the information collected by the LDM. A possible solution to the identity problem in the LDM is the use of algorithms based on movement prediction for correlating the identities of one hop distant stations.

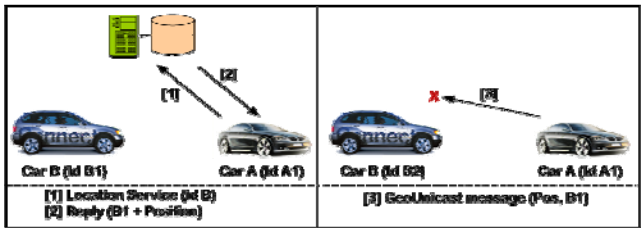

Figure 3. Issue for unicast communications

Another issue is related to the unicast communications. To send a unicast message, if the position information of the destination is not provided, an ITS station needs to trigger a location service request as depicted in Figure 3. Assuming that the request has been correctly received by the destination station, this latter will send a location service reply with the needed information. Once the reply is received, the source will send the unicast message. However, it could happen that in the meantime, the destination has changed its identity. In that case, the source will never know that the destination has acquired another identifier. One possible solution could be to block the identity update during the end-to-end communication. An attacker could exploit this vulnerability to conduct a Denial of Service (DoS) attack in order to prevent the station from changing its identifiers. The second solution that can be considered is to allow an overlap of the ITS station identifiers. This means that, after updating its identity, an ITS station continues to monitor the messages containing the previous identifier for a limited time before switching definitely to the new one. Upon the reception of a message with the former identifier, the station sends back a message to its correspondent indicating the new identifier.

The problem of the identity changes has to be opportunely solved because it could lead to wrong and potentially dangerous behaviours of certain applications. For instance, a high frequency of identity updates may influence ITS event-based safety applications. For instance, if a vehicle A detects an accident, it will send a safety message with pseudonym A1. Neighbour B receives this message and takes care of forwarding it with the pseudonym A1 as source identifier. Then, the source changes its pseudonym to A2 and transmits new messages with the identifier A2. In this way, another vehicle could receive two different safety messages with different pseudonyms but originally triggered by the same source and, consequently, the vehicle would detect two safety events.

We tried to list some of the applications and communications constraints regarding the ITS station identity definition. But still, there are cases that we have not mentioned and that could also be considered.

III. CONFIGURATION AND USAGE OF IDENTITIES

According to the reference architecture described in section I, the ITS station identity is globally handled by the Management layer. When needed, this layer must define and store the related identifiers, then ensure that all the data plane layers are using valid values, especially in the case of vehicles which need to preserve the user privacy. The identifiers can also be made available on request to the Network Management functions, using the ITS station MIB description.

A. Access Technology Addresses

An ITS station may include one or more network interfaces, providing access to the network. These modems use well defined technologies which already provide their own identification methods. In the case of vehicular communications, the most popular access technology is the 802.11p amendment of the IEEE 802.11 standard. Same as Ethernet, WiFi (IEEE 802.11) and WiMax (IEEE 802.16), this technology is based on a globally unique MAC address identifier, 48 bits long. Specific mechanisms exist to use it for building upper layer protocols identification such as the host part of the IPv6 address. This identifier is used in clear as source address in the outgoing frames and as destination in case of unicast communications, so it may need privacy protection in the case of an end-user terminal. On the other hand, other technologies such as the cellular, which comply with the 3GPP standards, the Digital Broadcast, the satellite systems or the infra-red, do not work with MAC addresses. In the case of cellular systems, the IMSI (International Mobile Subscriber Identity), identifies the user of the mobile device. Other identities are assigned on a temporary basis by the network. 3G systems and beyond may allocate an IP address to the user equipment. For example, in LTE, the equipment receives a unique interface identifier from the network to which it is attached. This identifier is later used to auto-configure the IPv6

address. Therefore a cellular access can be operated in the ITS station without requiring an address similar to the MAC address. Similar considerations can also be drawn for the other listed technologies. However, the 48-bit identifier may be needed when the MAC address is used to build the identifier for an ITS-specific upper layer entity (e.g. the GeoNetworking). It is generally admitted that a random 48-bit identifier is generated and the upper layer is responsible to guarantee the uniqueness requirement in the network.

To sum up, when the ITS station is initialized or when a new modem is inserted, the Management entity retrieves the Layer2-Id (MAC address or any other identifier) from the network interface and stores it internally. If needed, in the case of an identifier different from a MAC address, the Management entity generates randomly a MAC address. It also generates all the identifiers such as the EUI-64 or the GeoNetwork address needed by the ITS station, and provides them on request to the upper layers. In the case where privacy is activated, it ensures that a new temporary MAC address is built at the same time as the station pseudonym is changed and provides it to the relevant network interfaces, such as the IEEE 802.11p interface where it will replace the original MAC address. In all other procedures, the modem uses its own identifier in a way identical to that originally planned. There is no differentiation in the identity management at Access Technologies layer between fixed and mobile ITS stations.

B. GeoNetwork Address

ITS communications are based on ITS-specific protocol functionalities such as GeoNetwork protocol. IP-based protocol stacks are also considered especially in case of V2I and I2V communications. For instance, applications that require an internet connexion, e.g. entertainment services, will need to use the IP stack. Moreover, IPv6 could be integrated with GeoNetworking in order to exploit V2V communications with IP forwarding, providing extended functionalities to the ITS architecture. In that case, IP packets are encapsulated in GeoNetwork packet and forwarded using V2V links until they reach their destination.

In this paper, we are mainly interested in the definition of the GeoNetwork address, and in the next sections, we give more details about the format and configuration of this address. Regarding the other protocols, the existing specifications can still be used for the identification of stations at the network layer. For instance, the TCP/IP stack uses standard IPv6 addresses for communications.

1) GeoNetwork address format

To ensure a reliable performance for communication protocols, the GeoNetwork address must be globally unique. It is mainly used to identify the packet originator, forwarders and the unicast destination. As depicted in Figure 4, the GeoNetwork address is divided into two parts. The last field corresponds to the MAC address. The first 16 bits contain some static information that is related to the ITS station. When considering privacy, the GeoNetwork address should be updated periodically and at the same time as the other identifiers (corresponding to other layers) are changed. Accordingly, in each update, the last two fields, i.e. S_CC and M_ID, must be modified and derived from the selected pseudonym.

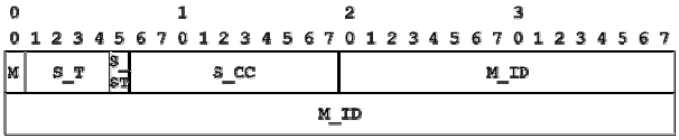

Figure 4. GeoNetwork Address Format

The different fields of the GeoNetwork address are described as follows.

M: This bit allows identifying manually-configured GeoNetwork addresses. M is set to 1 if the address is manually configured. Otherwise, it is equal to 0. It could be useful for some network protocols.

S_T: The ITS Station Type is defined on 4 bits. The first bit is reserved to classify the ITS stations into two categories: mobile and fixed stations. The second part is used to define a set of types for each category. For example, a fixed station can be a traffic light or a variable message sign, and a mobile station can be a car, a motorbike or a bus.

S_ST: The ITS Station Sub-Type is specified on 1 bit in order to differentiate between public and private ITS stations. For instance, for public transport vehicles, such as buses, it is set to 0. For private cars, it will contain a 1.

S_CC: The ITS station Country Code, defined in 10 bits, indicates the country from where the ITS station is originated. The allocation of ITS station Country Codes follows the ITU-T standard [7].

M_ID: This field corresponds to the access layer address. Commonly, 802.11p MAC layer is used in case of GeoNetworking. However, an ITS station may have multiple modems (see section III.A). The 48-bit 802.11p MAC address is then used by default. If the station does not contain an 802.11p modem, a random 48-bit address is built.

The first 16 bits of the GeoNetwork address provide additional information that can be used in some GeoNetwork protocols. For example, the S_T and S_ST fields can be exploited in the forwarding decision. In the case of an emergency vehicle, needing a higher priority than normal vehicles when travelling through traffic-signal-controlled roads, it can help disseminate the data with shorter delays.

2) GeoNetwork address configuration and update

At start-up, the Management layer is responsible for providing the GeoNetworking layer with the identifier that will be used in the communication phase. Nevertheless, an ITS station should be able to receive non-unicast messages even if it does not own a GeoNetwork address. This allows the ITS station to be aware of its vicinity even though it does not want to communicate and to send messages. Once it decides to enter the communication phase, the ITS station should obtain its initial GeoNetwork address from the management layer.

As we outlined in section II, due to privacy reasons, the GeoNetwork identifier should be updated almost periodically. Applications can also have an access to change the

GeoNetwork address. In both cases, the Management layer is in charge of informing the GeoNetworking layer of the update.

However, it is worth noting that even in the case where privacy is preserved, fixed stations e.g. Road Side Units (RSU) should use their initial or long-term GeoNetwork address. Only mobile ITS stations need to update their GeoNetwork address.

The configuration of the GeoNetwork address does not guarantee its uniqueness. Our proposal is that every ITS station should execute periodically a duplicate address detection algorithm to verify the uniqueness requirement. The algorithm is described as follows:

- Upon reception of a network BEACON, each ITS station checks if there are duplications by comparing the last field of its own GeoNetwork address, M_ID, to the BEACON's one.
- If a conflict is detected, the GeoNetworking protocol should request a new GeoNetwork address from the Management layer indicating duplicate address as the reason.

C. *Application-level Identity*

The identification of a station at layers higher than network is a topic that has not gained much attention yet. In fact, as standardization bodies have not yet defined the identification at Facilities layer, field operational tests are not concerned by this problem because the number of ITS stations used during the tests is small and ad hoc solutions can easily be implemented. Nonetheless, the identification of a station is still an important problem that has to be addressed before the introduction of vehicles with ITS capabilities on the consumer market. In fact, while low layers identifiers are dependent on the network and access technologies, Facilities layer identifiers should indicate the source and the destination stations of a message disregarding the way it is delivered on the network.

Figure 5. ITS station types with the corresponding S_T field values of the Facilities station identifier.

Currently four bytes have been dedicated to the identification of ITS stations at the Facilities layer. While the size of this identifier is clearly not large enough to univocally identify all the stations in the global ITS network, the requirement of uniqueness of the identities still has to be satisfied. Fortunately, most of the information that stations exchange has only local relevance and most of the communications are performed between ITS stations that are geographically close. As a consequence, the same identifiers can be reused at different and far away locations.

In this paper we present a new proposal to assign the identifiers of ITS stations at the Facilities layer. In our approach we distinguish identifiers according to the type of stations. We propose to assign the first two bits of the identifier, namely S_T, according to the station type. The advantage of using the S_T field is that different identification rules specifying the content of the remaining bits of the identifier could be applied to the different types of stations. Figure 5 pictures the four types of ITS stations that are generally considered. In the following paragraphs, we discuss the format of the identifier for each type of station separately.

1) *Central ITS Station Identifier*

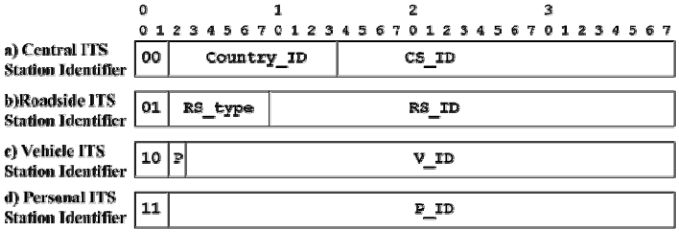

Figure 6. Application-level identifiers.

Figure 6a shows the identifier of the central stations. These stations have the station type field S_T, set to 00. Since they should be univocally identified in the entire ITS network, the assignment of their identifiers should be managed by national or international authorities. Moreover, central stations will not be required to change their identifier since they have to be reachable from any station in the network.

In order to identify the central stations geographically, the identifier also contains a 10-bits field, named Country_ID, which indicates the location of the central station. The country IDs are specified according to the ITU recommendations [7]. The advantage of using the Country_ID field is that some services can be dedicated for specific areas. Finally, the 20-bits CS_ID field represents the actual identifier of the central stations that is assigned by the international authority. This identifier is not periodically updated and remains the same as long as the central station is registered to the authority list.

2) *Roadside ITS Station Identifier*

Roadside stations in ITS networks are very important in that they allow mobile stations to access advanced services. In general, these services are only relevant locally. Therefore, the identifiers do not have to be globally unique. As we can observe in Figure 6b, the *S_T* field is set to 01. Moreover, a 6-bits field, *RS_type*, indicates the type of roadside station that is transmitting a message, while the other three bytes are assigned to the roadside station ID (*RS_ID*). Since roadside stations are useful not only as communication relays, but also for traffic efficiency and safety services, no identifier update is generally required, although updates can still be performed for specific reasons, for instance for maintenance purposes.

3) *Vehicle ITS Station Identifier*

Figure 6c depicts the format of a vehicle's identifier. For this type of stations the *S_T* field is set to 10. Since the number

of vehicles exceeds the capacity of the identifier, stations in vehicles will be uniquely identified only locally and not globally. Vehicles in a same location should not have the same identifier. Moreover, identifiers will be periodically updated through the use of pseudonyms in order to increase the security of the system and avoid that an observer be able to learn whether a specific station performed or will perform in the future a certain action.

However, not all the vehicles are subject to privacy constraints and need a periodical update of their identifier. This is for example the case of public vehicles such as buses or emergency vehicles. In the identifier the 1-bit field *P* indicates whether a station is public (field set to 1) or private (0). The knowledge of the type of vehicle can be exploited at application layer by some services, for example to send a help request to a police car in the area. The rest of the identifier is dedicated to the local ID of the vehicle, *V_ID* and is the field that may be changed by means of pseudonyms.

4) Personal ITS Station Identifier

The last class of ITS stations represents the vast class of personal stations, such as handheld devices. In this case the S_T value is set to 11 while the rest of the identifier is dedicated to a local identifier, shown in Figure 6d, which will be periodically updated.

It is important to note that duplications of the identifiers can locally occur also at Facilities layer. In this case we propose to use a duplication detection algorithm similar to the one that was presented in Section III-B. The only difference will be that the messages to be considered for the detection are the CAM messages, instead of the network beacons

Another important remark is about communication between stations that are far from each other, for example vehicles belonging to different but confining cities. In this case, from a theoretical point of view the communication can be performed without the infrastructure (assuming that there is a V2V communication path between the two stations). However, in practice, the communication shall pass through the infrastructure. In fact, apart from channel considerations, not only the stations' identifiers may change during the communication and generate some problem, but there could also be a station on the V2V path that has the same identifier as one of the two communicating vehicles.

Finally, the last topic to be considered is how to identify applications that are running at the top of the ITS stations. In this case, simple port addressing can be performed, similarly to what is done in computer networks. Since we can assume that privacy is not an issue anymore at this layer, no specific rules have to be defined.

IV. CONCLUSION

This paper presented a framework for the management of cross-layer identification in the future ITS stations. After analyzing the various constraints specific to this new vertical application, we defined and proposed solutions for ensuring the unique identification of the ITS-specific or existing entities at each layer and allowing them to communicate efficiently in the ITS network. We could highlight that some issues have not yet been fully specified. For instance, the frequency of update of identifiers for privacy reasons is still not clearly defined. For this topic and others similar that were found during this study, some simple yet effective solutions were proposed. However, we realized that the current addressing scheme is not fully optimal. A redundancy between MAC and GeoNetworking layers could be perceived. When the protocols used are IPv6 over GeoNetworking over IEEE 802.11, the 48-bit MAC address is used three times in three different headers. This is the price to pay for the openness and the flexibility of the system. Our framework is based on existing standards. It improves them because we investigated systematically all the layers and components of the ITS Station and provided a clear direction for each of them, flexible yet easily deployable. The proposal regarding the GeoNetwork addressing was submitted to the ETSI standardization group and included in a Technical Specification. The next step is to start the deployment of this new framework in real systems. Several Field Operational Tests (FOTs) are currently under way or being prepared where these solutions will be tested. They will provide in the coming months some feedback for further improvements on addressing and identification of the ITS stations.

ACKNOWLEDGMENT

This work has been partly funded by the European Commission through FP7 ICT Project iTETRIS: An Integrated Wireless and Traffic Platform for Real-Time Road Traffic Management Solutions (No. FP7 224644). The authors wish to acknowledge the Commission for their support.

REFERENCES

[1] SeVeCom project : http://www.sevecom.org

[2] European ITS Communication Architecture Overall Framework, COMeSafety project, http://www.comesafety.org .

[3] ETSI TC-ITS, http://www.etsi.org/WebSite/Technologies/IntelligentTransportSystems.aspx

[4] ETSI EN 302 665 V1.0.0, "Intelligent Transport Systems (ITS); Communications Architecture" (2010-03)

[5] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper" ; Workshop on Standards for Privacy in User-Centric Identity Management, Zurich, Switzerland, July 2006.

[6] Sim^{TD} project: http://www.simtd.de

[7] "COMPLEMENT TO ITUT RECOMMENDATION E.212 (11/98)", Annex to ITU Operational Bulletin No. 741 – 1.VI.200; http://www.itu.int/ITUT