Security Issues of IPv6 Communications in Cooperative Intelligent Transportation Systems (Poster)

Jong-Hyouk Lee
INRIA, France
Email: jong-hyouk.lee@inria.fr

Thierry Ernst
Mines ParisTech, France
Email: thierry.ernst@mines-paristech.fr

***Abstract*—ETSI and ISO are completing the standardization of the building blocks of a reference communication architecture for Cooperative Intelligent Transportation Systems (ITS). Future ITS stations complying with this set of standards deployed in vehicles, at the roadside infrastructures, and within the Internet are expected to communicate with each other through a combination of ITS dedicated communication protocols and legacy Internet protocols. However, in spite of the wide adoption of IPv6 for cooperative ITS communications, relatively little attention has been paid to the security issues related to IPv6 signaling and IPv6 transport communications. In this paper, we present our position on the emerging and urgent IPv6-related security issues that occur in communications between ITS stations complying with the ITS station reference architecture under standardization within ETSI TC ITS and ISO TC204.**

I. Introduction

Cooperative Intelligent Transportation Systems (ITS) are ITS where ITS stations communicate and exchange information between themselves with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone ITS. Cooperative ITS will turn up to us with safer and more efficient driving environments as well as convenient comfort and mobility services.

Over the past few years, significant progress has been made at the standardization level in order to produce a full set of standards allowing the deployment of cooperative ITS solutions. The initial communication standards specified at the ISO TC204 level and better known as CALM and other concepts originated by the Car-to-Car Communication Consortium (C2C-CC) have been demonstrated and enhanced in the framework of a set of European projects (CVIS, SafeSpot, Coopers, GeoNet, SeVeCom). These impressive results have then been consolidated by the European COMeSafety Specific Support Action and brought back to the standards organizations. The result is the unified ITS station reference architecture [1], [2] on which is based a number of standards developed by ETSI TC ITS, CEN TC278, and ISO TC204.

The security of cooperative ITS communications has gained a lot of attraction in recent years as it is now recognized that security is not an optional but essential feature for the effective deployment of cooperative ITS: most of the potential benefits of cooperative ITS would be undermined without strongly secure communications. At the standardization level, security requirements and functionalities have been defined under the framework of the ITS station reference architecture. At the industry and academic levels, the use of pseudonyms and certificates has been well investigated within the C2C-CC and the SeVeCom European project. However, most of the security effort is being focused on securing vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) communication paths, analyzing security overhead in communications, and providing location privacy to vehicles without much consideration for other communication paths, e.g., communications between the roadside infrastructure and the control center (R2C) and between the vehicle and central management systems (V2C). In addition, the security work has mostly been focused on the 802.11p communication media and GeoNetworking without much consideration for security issues at other layers, especially at the IPv6 level, although IPv6 has been acknowledged as a master piece within the ITS station reference architecture for traffic efficiency, comfort/mobility types of and non time-critical safety types of applications [3].

The rest of this paper is organized as follows. Section II provides a brief overview of the ITS station reference architecture. Then, in the following sections, we present six security issues related to IPv6 cooperative ITS communications. For each of these issues, we present our position and explain how we think these issues could be solved. Section IX concludes this paper.

II. ITS station reference architecture overview

Cooperative ITS communications are based on ITS station reference architecture jointly specified by ETSI TC ITS and ISO TC204 [1], [2]. Fig. 1 shows this cross-layered communication architecture. It is made of four OSI-like horizontal layers, i.e., access, networking & transport, facilities, and applications layers, and two cross-layer entities, i.e., management and security entities. Service access points (SAPs) are interfaces allowing the exchange of information between different layers or entities. For instance, the SN-SAP is the SAP connecting the security entity and the networking & transport layer, whereas the MS-SAP is connecting the management and security entities. This exchange of information between layers or entities is necessary for cross-layer functions that require information from several layers for better decision making [5], for instance, selection of the best communication interface

978-1-4673-0047-6/11/$26.00 ©2011 IEEE

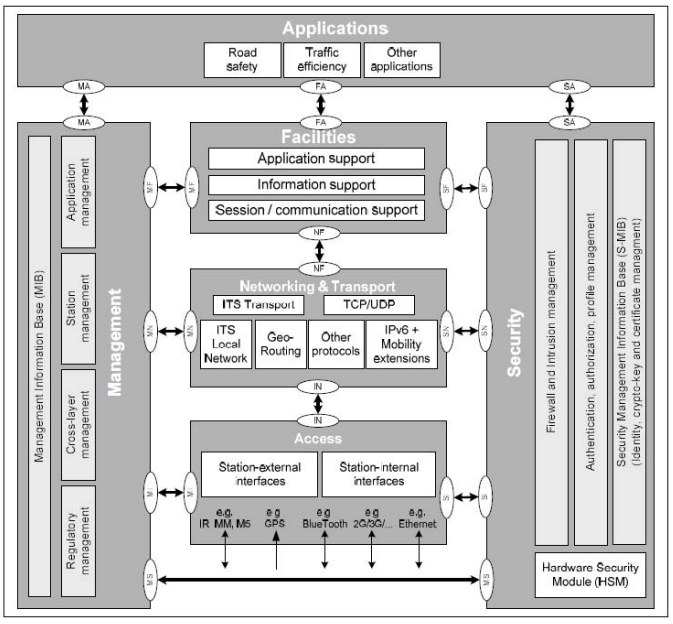

Fig. 1. ETSI/ISO ITS Station Reference Architecture.

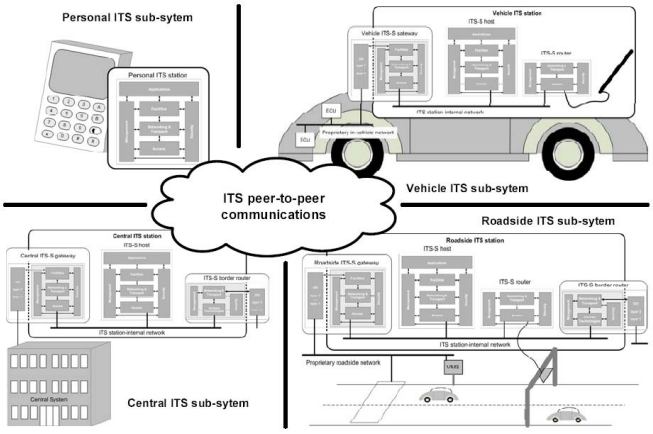

Fig. 2. Cooperative ITS Station Types.

according to application requirements (e.g., communication profiles), current media availability, and network congestion. It also simplifies security management.

As shown in Fig. 2, types of ITS stations include vehicle ITS stations (cars, buses, trucks, trains, etc.), roadside ITS stations (toll gate, gantries, electric vehicle charging station, variable message signs, etc.), central ITS stations (control center, mobility services servers, etc.) and personal ITS stations (hand-held devices, etc.). All of these ITS station types are specific instances of the ITS station reference architecture shown in Fig. 1. Each ITS station type implements a subset of the functionalities of the ITS station reference architecture (the functionalities are the building blocks depicted on the figure) according to the role it plays (does it provide or consume services?), its purposes (is this for road safety or traffic efficiency, or both?), the applications to be supported (a variety of applications or only comfort/mobility), where it is deployed, and by whom. For instance, a vehicle ITS station installed in a private car may be equipped with 802.11p and cellular interfaces, while a truck may additionally be equipped with a satellite link; similarly, a personal ITS station implemented in a PDA may only support IPv6 networking but not GeoNetworking while a vehicle ITS station would support both.

These functions may be distributed into ITS station router(s) and host(s), as shown for the vehicle ITS station on Fig. 2, or in a single ITS station node as shown for the personal ITS station. When these functions are distributed, the ITS stations router(s) and host(s) are linked through an ITS station internal network. All ITS station nodes forming an ITS station are networked and equipped with communication capabilities. They thus need to implement at least the lower layers (access layer and networking & transport layer). In addition to these layers, an ITS station host also implements the ITS dedicated facilities and application layers. For instance, the Cooperative Awareness Messages (CAMs) implemented in the facilities layer are used to disseminate presence, position, and status information of an ITS station to neighboring ITS stations [11]. The ITS station router on the other hand is not required to implement these upper layers as its role is to manage a range of communication interfaces (e.g., 802.11p, 802.11n, 3G/LTE) connecting the ITS station to neighboring ITS stations. Fig. 3 illustrates a possible implementation of the ITS station functionalities into physically distributed units. As shown, the ITS station gateway connects the proprietary in-vehicle network (e.g., CAN bus) and the ITS station internal network.

The behavior of IPv6 for all types of ITS stations has been specified by ISO in [4]. In the most general and advanced case, an in-station IPv6 network is linking a communication device (ITS station router) and other devices (ITS station hosts), e.g., IP sensors, navigation systems, and nomadic devices in the case of a vehicle ITS station. However, the few security studies applying to IPv6 in cooperative ITS have so far considered only one single IPv6 address per vehicle although each vehicle should form an IPv6 subnetwork of its own. ISO is therefore considering the most general case where an IPv6 prefix is allocated to each vehicle. This generalization simplifies mobility management.

Suppose now that a vehicle ITS station is changing its attachment point from one network (a roadside ITS station) to another network (another roadside ITS station). This network-level handover results in updating the location information, i.e., the new transient IPv6 address obtained from the current access network is provided to a home agent (HA) that maintains the location of the vehicle ITS station and forwards the traffic bound to the vehicle ITS station to its current transient IPv6 address. As the vehicle ITS station, or more specifically, the vehicle ITS station's router detects its network point of attachment, it can promptly send a router solicitation (RS) message to quickly receive a router advertisement (RA) message including the network prefix in the new access

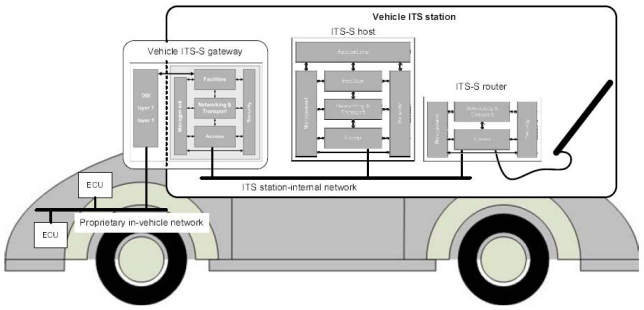

Fig. 3. Distributed ITS Functionalities in a Vehicle ITS Station.

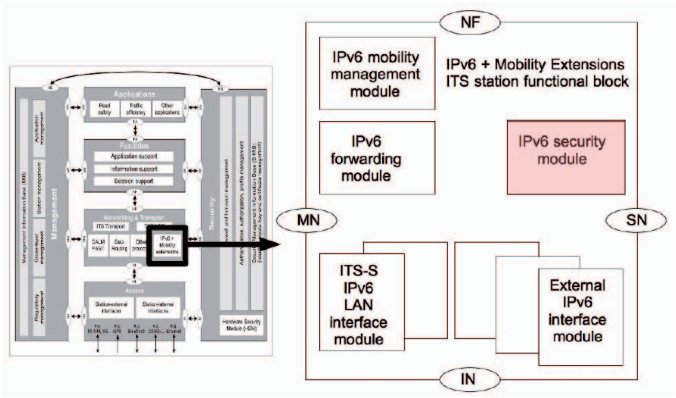

Fig. 4. IPv6 Security Module in the IPv6 Protocol Block.

network. Then, the vehicle ITS station's router immediately generates its new transient IPv6 address, better known as the Care-of Address (CoA), based on the network prefix and sends a binding update (BU) message carrying the CoA to the HA for location update, without waiting an unsolicited RA message periodically sent from the roadside ITS station's router. During this handover process, access layer parameters (e.g., link status) and network layer parameters (e.g., IPv6 address configuration status) are provided to the management entity which is then able to determine what is the best available path for a given communication flow. The management entity then instructs the IPv6 protocol block by providing routing rules through the MN-SAP. The IPv6 protocol block then applies these rules to the IPv6 forwarding table.

The IPv6 security module shown in Fig. 4 is in charge of securing IPv6 communications (i.e., IPv6 dedicated mobility signaling and user traffic). It does the following actions:

- it communicates with the security entity through the SN-SAP;
- it communicates with other modules in the IPv6 protocol block;
- it enables the security protocols for the required security services; and
- it reports available IPv6 security capabilities to the security entity through the SN-SAP.

III. Security Decision: Management Entity vs. Security Entity

In this section, we discuss a potential decision making conflict between the two management and security cross-layer entities, when routing and security functions are applied simultaneously.

A. Lack of synchronization in decisions

The management entity is constantly monitoring the status of the interface and provides new routing rules to the IPv6 protocol block which updates its forwarding table accordingly. However, this is not synchronized with the security entity that may also request the IPv6 protocol block to apply specific security services to outgoing packets.

Let us consider a vehicle ITS station changing its point of attachment from a public wireless local area access network to a 3GPP cellular access network. IPsec is the recommended means to secure IPv6 location update signaling in the public wireless local area network [6], [7], whereas a shared-key-based authentication is used for IPv6 location update signaling in the 3GPP radio access network to minimize signaling overhead and improve handover performance [8]. Note that the size of the BU message, which is sent over a wireless link, is significantly increased as the IPsec ESP tunnel mode is applied [7]. Suppose that the management entity detects the new link from the access layer and is informed by the IPv6 protocol block that an IPv6 path is up and operational through the new access network (i.e. a NEMO tunnel has been established between the MR and the HA over the 3GPP access network). Should the management entity instruct the IPv6 protocol block to switch from IPsec to the shared-key-based authentication at the same time it instructs the IPv6 protocol block to divert the traffic (possibly all flows or only some of them if there are multiple available paths) from the public wireless local area network to the 3GPP access network ? If so, how does the management entity know the available security protocols for IPv6 location update signaling? Even if the management entity is able to access the list of the available security protocols, how does it assess if a security protocol properly works for the currently attached network? Moreover, IPv6 dedicated security protocols such as IPsec for IPv6 location update signaling and user traffic, shared-key-based authentication for location update signaling, SeND [9] for securing the neighbor discovery protocol [10], etc. are protocols belonging to the networking & transport layer, or more precisely to the IPv6 protocol block [4]. Should the management entity make a decision for enabling or disabling an IPv6 dedicated security protocol when required?

B. Our proposition and potential solution

As seen in the previous section, the ITS station reference architecture allows informative parameters residing in each layer/entity to be exchanged via the SAPs.

We propose that the security entity is in charge of security related decisions, i.e., which security services (authentication, access control, confidentiality, integrity, and location privacy support) are activated or deactivated at the IPv6 security

module in the IPv6 protocol block, while the IPv6 security module executes the actual IPv6 dedicated security protocols whenever required.

The security entity does not need to be aware about the actual IPv6 dedicated security protocols implemented at the level of the IPv6 security module. It just needs to know what are its capabilities. In other words, there are features implementing required security services at the IPv6 security module. For instance, upon reception of an activation command for a specific security service via the SN-SAP from the security entity, the IPv6 security module shall enable an IPv6 security protocol complying to the requested security service.

Let us consider again the vehicle ITS station changing its point of attachment from a public wireless local area network to a 3GPP radio access network. In this case, the security entity is not able to directly activate the shared-key-based authentication for IPv6 location update signaling, instead of IPsec. The security entity should thus request the IPv6 security module via the SN-SAP to deactivate the confidentiality security service for IPv6 location update signaling. This deactivation command sent from the security entity to the IPv6 security module results in switching from IPsec to the shared-key-based authentication. Note that the shared-key-based authentication presented in [8] does not support the confidentiality security service, but it supports authentication and integrity.

We also suggest that the security entity provides related informative parameters to the management entity and other layers via SAPs if requested, while the security entity makes security related decisions based on informative parameters obtained from the management entity and other layers via SAPs

IV. Single ITS functionality vs. Distributed ITS functionalities

As indicated in Section II and shown in Fig. 3, the ITS station's functionalities can be implemented into a single physical unit or in physically distributed units, i.e., ITS station router(s), host(s) and gateway(s).

A. No consideration for the router-host split model

The security work recently achieved at the ETSI, i.e., ITS security services and architecture [12], assumes that the vehicle and roadside ITS stations are mostly formed as a single physical network unit comprising all the ITS functionalities of host and router. The C2C-CC security working group also considers all ITS station functionalities are implemented into a single physical unit. This assumption was taken as it simplifies and minimizes the complexity of the security design. However, such a security design only considering the single unit approach does not cover all cases and is thus broken when it is applied to ITS stations implementing the ITS station host and router functionalities separately.

For instance, let us consider a bus which provides Internet connectivity to passengers and in which the ITS station functionalities are splitted into an ITS station router and multiple ITS station hosts. A dedicated ITS station host sends CAMs to neighboring ITS stations via the ITS station router. The current ETSI/ISO security work does not define any means for 1) protection against threats from the ITS station internal network; or 2) security association between the ITS station host sending CAMs and the ITS station router forwarding the CAMs to neighboring ITS stations. Note that the ITS station router also provides Internet access to personal ITS stations carried by the passengers and connected to the ITS station internal network. Accordingly, a passenger can be an eavesdropper as he secretly listens to the messages sent on the ITS station internal network from the ITS station host or other passenger's personal ITS station. He can even easily perform a spoofing attack as he successfully masquerades as another person by falsifying messages and thereby gaining an illegitimate privilege, e.g., message redirection.

B. Our proposition and potential solution

As the work for securing ITS communications was still in its infancy, it was understandable to take the simplest case as a starting point for a security threat analysis. The security threat analysis, however, must cover all possible and identified deployment scenarios as its purpose is to serve as a basis for building the ITS security services and architecture. The current security threat analysis for cooperative ITS conducted by ETSI [13] should thus be extended to address this ITS station architectural issue — single and distributed cases — and then the ETSI specification of ITS security services and architecture [12] should be updated.

In order to prevent attacks from the ITS station internal network in the distributed case, the ITS station internal network should be protected by means of access network authentication or access control mechanisms as the ones widely deployed in wireless local area networks and 3GPP radio access networks. For instance, the EAP authentication framework [14] can easily be deployed to provide access network authentication. An easiest deployment scenario is where ITS station nodes and legacy devices implementing the EAP peer functionality in the ITS station internal network are authenticated with certificates or passwords by the ITS station router acting as the authenticator and EAP authentication server. A scalable deployment scenario is where the ITS station router acts as the authenticator and the ITS station nodes and legacy devices implementing the EAP peer functionality are authenticated by the remote EAP authentication server, which is likely deployed at the central ITS station. In the former scenario, access network authentication is limited to the ITS station nodes and legacy devices registered to the local EAP authentication server, i.e., ITS station router, whereas any ITS station node and legacy device registered to the remote EAP authentication server are authenticated in the latter scenario [15].

In a configuration where the ITS station router only implements the routing capabilities such as GeoNetworking [16], IPv6 with mobility extensions [4], e.g., NEtwork MObility (NEMO) [17], over the access layer, ITS dedicated messages such as CAMs or legacy Internet application's messages would

be generated at an ITS station host. This means that in the distributed case such messages generated from the ITS station host are forwarded by the ITS station router. However, as the messages are encrypted or signed by the ITS station host, the ITS station router cannot process the secured messages without a security association (i.e., information about the used algorithm, key, etc) configured with the ITS station host. We thus suggest that 1) the ITS station router should have the security association with the ITS station host for at least decrypting or verifying the access layer and networking & transport layer headers of the packets; or 2) the ITS station host should encrypt or sign only the payload part of the packet, not the entire packet. It allows the ITS station router to examine the message for forwarding. Note that in the second suggestion case the ITS station router should make secure the access layer and networking & transport layer headers of the packets when it forwards them. Accordingly, a security association between the ITS station host and router or a layered message security is required for a proper forwarding/routing at the ITS station router when the ITS station router only implements the routing capabilities. Note that the layered message security is vulnerable unless the ITS station internal network is secure.

V. Security Credential Management

Security credentials such as cryptographic keys, certificates, and pseudonyms are required in security related operations. For instance, a key pair consisting of a public key and a private key with an associated certificate is required in SeND [9] for securing the neighbor discovery protocol [10]. In this section, we discuss the security credential management.

A. Security credential transmission from the security entity

As indicated in Section II and illustrated in Fig. 4, IPv6 dedicated security protocols such as IPsec, shared-key-based authentication, SeND, etc. are implemented in the IPv6 security module of the IPv6 protocol block. The current ETSI specification of ITS security services and architecture [12] defines that the security credentials for all communication layers are managed by the security entity and those credentials are kept in the security entity. Note that SeVeCom, a completed EU-funded project focusing on vehicular communication security, also suggested that the security credentials are securely maintained in a hardware security module wherein security operations are performed [18]. In other words, the IPv6 protocol block would not be able to request to the security entity (via the SN-SAP) any security credentials necessary for IPv6 dedicated security protocols.

B. Our proposition and potential solution

As we presented in previous sections, the current ETSI specification of ITS security services and architecture has been developed without considering all possible and identified deployment scenarios as well as IPv6 dedicated security protocols. If we follow the current approach where the security related operations are only performed in the security entity while the security credentials are only maintained in the security entity or the hardware security module, the IPv6 dedicated security protocols should be implemented at the level of the security entity, not in the IPv6 protocol block. This must be not happen because it will break the cross-layered communication architecture concept. In addition, since the IPv6 dedicated security protocols are subject to be modified or replaced as new security protocols appear, it will also break modularity and increase the development complexity of the security entity.

To solve this problem, we propose to utilize the SN-SAP for transmitting required security credentials from the security entity to the IPv6 protocol block. For instance, when a protection to the neighbor discovery protocol [10] is needed, the IPv6 protocol block, or more specifically, the IPv6 security module would request necessary security credentials to the security entity via the SN-SAP. Another example is a pseudonym[1] change at the IPv6 layer. Suppose that a vehicle ITS station is required to change its pseudonym to preserve location privacy. In this case, a new pseudonym should be provided from the security entity via the SN-SAP in order to generate a new IPv6 address based on the new pseudonym. We will further discuss about the pseudonym change at the IPv6 layer in Section VII.

VI. Broadcast vs. Others Communication Modes

ITS stations will not only have a broadcast communication capability, but will also have various communication capabilities. Especially, IPv6 provides connection-oriented (session-based) communication in a multihop communication manner.

A. One-sided consideration for communication modes

The dissemination of ITS station presence, position, and status information for safer and more efficient driving environments is one important goal of cooperative ITS communications, particularly for the automotive industry. Most of the security work achieved in the context of cooperative ITS communication is thus about securing broadcast messages, which are supported by the access layer and delivered to neighboring ITS stations in the radio range. In other words, security for one-hop broadcast messages has been widely studied, but no comprehensive security study for other communication modes has been conducted. Particularly, GeoNetworking [16], which is a protocol designed for geographical addressing and routing, introduces new communication modes, while IPv6 also provides different modes of communication other than broadcast. Table I shows the ITS communication modes supported at each layer/protocol of the ITS station reference architecture. Note that some communication modes for GeoNetworking, e.g., beaconing message, have been omitted since those are not relevant from the viewpoint of IPv6.

Since broadcast is a connectionless mode of communication, i.e., no pre-communication establishment for data communication is required, a security association is also not required before a message is sent. Accordingly, a dominant security

[1]The pseudonym is a temporary identifier only used in communications for a short period of time and changed regularly. Two consecutive temporary identifiers are not linkable.

TABLE I
ITS COMMUNICATION MODES AT EACH LAYER/PROTOCOL

Layer/Protocol	Communication Mode
IPv6	Unicast, Multicast, Anycast
GeoNetworking	GeoUnicast, GeoBroadcast, GeoAnycast
Access (IEEE 802.11p)	Broadcast

approach for broadcast is to use a PKI structure and carry the security association (i.e., certificate) directly in the message. Note that the attached certificate in the message identifies how the message is protected and allows security assertions for authenticity, integrity, authority, etc. However, such an approach, i.e., most of existing security protocols for cooperative ITS communication, cannot be directly applied to other ITS communication modes. For instance, IPv6 unicast communications are not only connectionless (UDP), but can also be connection-oriented (TCP which supports flow control, congestion control, and error correction). If the security association is carried for every single packet on connection-oriented communication, it is obviously inefficient and would increase message size, increase packet loss rate, decrease throughput, and so on.

In order to further improve V2V and V2R communications, multihop communication has been considered more recently. In both GeoNetworking and IPv6, intermediary nodes are relaying messages to their final destination. As messages are forwarded by intermediate ITS stations (nodes) to the final destination in a multihop communication manner, it is important to ensure end-to-end security and reliable forwarding/routing.

B. Our proposition and potential solution

For securing IPv6 communications, we propose to use IPsec with IKEv2. IPsec provides secure IPv6 communication by authenticating and encrypting each message, while IKEv2 allows to establish a dynamic security association between two ITS stations. However, how IPv6 communications are protected over V2V and V2R communication environments has been not been studied yet. For instance, the use of IPv6 over GeoNetworking has been specified at ETSI [19], but no means of protection has been defined although IPsec combined with IKEv2 is available. Furthermore, a security mechanism for GeoNetworking has not yet been defined nor a threat analysis for GeoNetworking been conducted.

VII. PSEUDONYMS AT THE IPV6 LAYER

In this section, we discuss the use of a set of pseudonyms and its relation with IPv6 addresses.

A. Use of pseudonyms

For location privacy support, the approach adopted at ETSI is to utilize a set of pseudonyms with an appropriate changing scheme. Pseudonyms are temporary identifiers used in communications for a short period of time and changed regularly, e.g., random 48 bits for the MAC address at the access layer. A pseudonym P_1 is only used for a short period t_{P_1} and then changed to a new one P_2 for the next short period t_{P_2}. Since P_1 and P_2 are not linkable, observers are only able to link either messages associated with P_1 over t_{P_1} or messages associated with P_2 over t_{P_2}.

The change of identifiers for location privacy must indeed happen across the entire communication stack. In other words, if a vehicle ITS station implementing IPv6 over GeoNetworking changes its pseudonym, which is 48 bits long, the whole MAC address at the access layer is replaced by the new pseudonym, while the GeoNetworking address and IPv6 address must also be changed. As presented in [19], the rightmost 48 bits of the GeoNetworking address, which correspond to the MAC address, are changed when the pseudonym is changed.

B. Our proposition and potential solution

For the IPv6 layer, we propose to generate the rightmost 64 bits of the IPv6 address, i.e., interface identifier, based on the pseudonym. By this way, the leftmost 64 bits of the IPv6 address, i.e., network prefix, are changed when the mobile router (MR), i.e., vehicle ITS station's router, changes its attachment point, while the rightmost 64 bits of IPv6 address are changed when the pseudonym is changed.

At the IPv6 layer, the pseudonym change should be triggered by either the movement (network-level handover from one roadside ITS station to another one) or the pseudonym lifetime expiration. As the MR changes its attachment point, it generates its new address, i.e., CoA, based on the network prefix provided from the new network. However, if the MR continuously uses its interface identifier for the address generation, the MR's movement is tracked as observers link the previous address's interface identifier and the new address's interface identifier. Accordingly, whenever the MR changes its attachment point from one network (one roadside ITS station) to another network (another roadside ITS station), the pseudonym change is required.

Also, the pseudonym must be changed when the current pseudonym's lifetime has expired. However, because the pseudonym change causes an address change at the IPv6 layer, it results in performing the duplicated address detection procedure and location update to its HA even if the MR still remains attached at the same roadside ITS station. The pseudonym change caused by the lifetime expiration thus decreases the overall performance of the MR as it yields time-consuming procedures and significant signaling over the air interface. Accordingly, it is highly recommended to develop a pseudonym change scheme that considers both location privacy and performance.

VIII. IDENTITY INFORMATION AT THE IPV6 LAYER

In this section, we discuss identity information at the IPv6 layer and show why the use of pseudonym is not enough and additional protections are required for location privacy.

A. Identity information

The MR, i.e., vehicle ITS station's router, can be tracked with the following identity information:

- Home address (HoA): It is a permanent IPv6 address assigned to the MR. This address is not changed during the vehicle ITS station's travel.

- Mobile Network Prefix (MNP): It is a permanent IPv6 network prefix assigned to the vehicle ITS station and used to configure the IPv6 address of all ITS station nodes on the ITS station internal network.
- Care-of Address (CoA): It is a transient IPv6 address only valid at the current location of the vehicle ITS station, i.e., the current point of attachment of the MR. This address is changed when the MR changes its attachment point.

The HoA and MNP are considered as identifiers, whereas the CoA is considered as a locator. As presented in Section VII, the CoA is changed as the pseudonym is changed so that it is not traceable. However, as the HoA and MNP are included in location update signaling, i.e., BU and BA messages between the MR (of the vehicle ITS station) and the HA (of the central ITS station), the observers can identify the MR by examining location update signaling. In other words, the use of pseudonym at the IPv6 layer is not enough and additional protections are required for location privacy.

To protect location update signaling from such eavesdroppers, the IPsec ESP tunnel mode [7] is recommended. However, in spite of the confidentiality protection of the IPsec ESP tunnel mode, it creates a new identity information allowing to identify a given ITS station. In IPsec, a security parameters index (SPI), which is 32 bits, is used to identify the established security association with the source address and is not changed during the IPsec protection. Since the SPI is sent in cleartext, it is the identity information and can be used by the observers to track the MR. Note that the SPI is required in both AH and ESP packets.

The neighbor discovery protocol is protected by SeND. However, as the SeND protection relies on the public key cryptography, the public key of the sender is attached in every messages. Accordingly, the public key included in messages is the identity information.

B. Our proposition and potential solution

Eavesdroppers can identify a given ITS station by collecting SeND protected messages with the same public key. In order to prevent this threat, we suggest to change the public key regularly. This is a similar approach with the use of pseudonym certificate introduced in [18].

As the SPI is used to identify the established security association for the IPsec protection, the change of SPI results in re-establishing the security association that causes packet loss or delayed transmission. A potential solution should randomize the SPI and synchronize it between end-to-end communication peers, while minimizing the frequency of the security association re-establishments.

As an MR (of vehicle ITS station) uses IPv6 communications, the location and movement of the MR can be revealed by the identity information such as HoA, MNP, CoA, SPI in IPsec, and public key in SeND. It leads us to protect not only IPv6 address related identity information, but also to protect the identity information generated in securing IPv6 communications.

IX. Conclusions

In this paper, we have discussed emerging and urgent security issues related to IPv6 communications in the context of cooperative ITS communication complying with the ITS station reference architecture. We have presented our views on the identified issues and identified possible solutions which require further work. The intend of this paper is to raise a debate on such issues and to serve as an input to ETSI TC ITS and ISO TC204 standardization activities. In the meantime, the ITSSv6 FP7 European project is tasked to deliver an enhanced specification and implementation of the IPv6 protocol block of the ITS station reference architecture. This particularly includes features to secure IPv6 communications.

Acknowledgment

This work has been supported by the ITSSv6 (IPv6 ITS Station Stack for Cooperative ITS) FP7 European project (http://www.itssv6.eu) under European Commission Grant 270519. Figs.1, 2, 3, and 4 are extracted from [2], [4].

References

[1] ISO/FDIS 21217: “Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture”, January 2010.
[2] ETSI EN 302 665: “Intelligent Transport Systems (ITS); Communication Architecture”, v1.1.1, September 2010.
[3] T. Ernst, “The Information Technology Era of the Vehicular Industry”, *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 36, no. 2, pp. 49–52, April 2006.
[4] ISO 21210: “Intelligent transport systems — Communications access for land mobiles (CALM) — IPv6 Networking”, January 2011.
[5] ISO/FDIS 24102, “Intelligent transport systems — Communications access for land mobiles (CALM) — Management”, July 2010.
[6] J. Arkko, V. Devarapalli, and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, *IETF RFC 3776*, June 2004.
[7] V. Devarapalli and F. Dupont, “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture”, *IETF RFC 4877*, April 2007.
[8] A. Patel, K. Leung, M. Khalil, H. Akhtar, and K. Chowdhury, “Authentication Protocol for Mobile IPv6”, *IETF RFC 4285*, January 2006.
[9] J. Arkko, J. Kempf, B. Zill, and P. Nikander, “SEcure Neighbor Discovery (SEND)”, *IETF RFC 3971*, March 2005.
[10] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, “Neighbor Discovery for IP version 6 (IPv6)”, *IETF RFC 4861*, September 2007.
[11] ETSI TS 102 637-2: “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service”, v1.1.1, April 2010.
[12] ETSI TS 102 731: “Intelligent Transport Systems (ITS); Security; Security Services and Architecture”, v1.1.1, September 2010.
[13] ETSI TR 102 893: “Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)”, v1.1.1, March 2010
[14] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, “Extensible Authentication Protocol (EAP)”, *IETF RFC 3748*, June 2004.
[15] B. Aboba, D. Simon, and P. Eronen, “Extensible Authentication Protocol (EAP) Key Management Framework”, *IETF RFC 5247*, August 2008.
[16] ETSI TS 102 636-4-1: “Intelligent Transport System (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media Independent Functionality”, v1.1.1, June 2011.
[17] V. Devarapalli *et al.*, “Network Mobility (NEMO) Basic Support Protocol”, *IETF RFC 3963*, January 2005.
[18] P. Papadimitratos *et al.*, “Secure Vehicular Communication Systems: Design and Architecture”, *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, November 2008.
[19] ETSI TS 102 636-6-1: “Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols”, v1.1.1, March 2011.