Evaluation of a Mobility Approach to Support Vehicular Applications Using a Realistic Simulation Framework

Nerea Toledo(✉), Marivi Higuero, Maider Huarte, and Juanjo Unzilla

University of the Basque Country, Bilbao, Spain
nerea.toledo@ehu.eus

Abstract. The connected vehicle is becoming a reality. Internet access onboard will indeed increase road safety and security thanks to the cooperative networking that it is expected among vehicles, roadside units and the Internet. Moreover, this connectivity will bring innovative driving assistance services and infotainment alike services for end users. This fact is endorsed by standardisation bodies like the ETSI or the 5G-PPP that are actively working on the definition of these innovative services and setting their requirements. The connected vehicle poses technological challenges that need to be addressed. The mobility has to be managed regardless the location of the vehicles to ensure connectivity. At the same time the required security and performance levels for the applications need to be ensured. In this paper, we present a realistic simulation framework to evaluate vehicular applications while the protocol to manage the mobility, NeMHIP, is running underneath. The simulation framework is based on the integration of the OMNeT++, SUMO, VEINS and VsimRTI simulation tools. Obtained results have been compared with the requirements defined by the 5G-PPP automotive white paper, ITU-T Y.1541 and 3GPP TS 22.105 standards with satisfactory results. Thus, we demonstrate that the NeMHIP protocol is suitable because it fulfils the requirements of the applications while it provides an essential mobility service. In addition, this work shows the validity of the simulation framework.

1 Introduction

In a very near future it is foreseeable that onboard Internet access not only for infotainment services but also for road safety assistance services will be a reality. In fact, by 2024 89 % of new cars sold are projected to include both embedded and mobile devices and ensure connectivity [10]. That is, vehicles will be connected to the Internet, to other vehicles, and to roadside units, so vehicles should rely not only on their own sensors but also on other vehicles' devices, and will cooperate with each other. This complex scenario is posing several technological challenges to the underlying communication system that need to be addressed.

From the communications point of view, a vehicle could be regarded as a cluster of mobile nodes that move together as a whole, that is, a mobile network. Vehicles equipped with several devices to measure the state of the engines,

G. Dregvaite and R. Damasevicius (Eds.): ICIST 2016, CCIS 639, pp. 709–721, 2016.
DOI: 10.1007/978-3-319-46254-7_57

machinery, etc. that are requested to provide reports to the control centre of the operation of the vehicle when referring to fleet management services; and end user devices like PDAs, smart phones, laptops, etc. brought in by the travellers are an example of scenarios where a set of nodes comprise a mobile network. Since a vehicle is constantly changing its point of attachment to the Internet one of the key technological elements that it is needed for having efficient vehicular communications is the mobility management protocol. This mobility management solution needs to guarantee the required security and efficiency levels demanded in the vehicular scenario. Consequently, the mobility management protocol we consider in this paper, the NeMHIP protocol, is the most suitable solution because it fulfils the requirements posed by this scenario as demonstrated in [24,25].

The connected vehicle will at the same time enable innovative applications to the automotive scenario to improve road safety and security and offer new services to end users. That is, services like automated overtake, emergency braking or cooperative collision avoidance together with infotainment services that demand high QoS will be possible. In fact, standardisation bodies like the ETSI or the ISO are defining the requirements of these type of services that will also pave the way to the automated driving.

In this paper, we present a simulation framework that integrates different simulation tools to have a realistic environment and evaluate the performance of different vehicular applications. We have compared obtained results with the requirements defined by the 3GPP [7], ITU-T [6] and 5G-PPP [8] standardisation bodies and demonstrate that the NeMHIP protocol is suitable because it fulfils the requirements also in a realistic vehicular simulation framework. At the same time, we show that the developed simulation framework is valid for conducting performance evaluation of vehicular applications.

2 Context

Currently, there is a lot of activity on ITS and vehicular communication standardisation regarding different aspects involved in this type of communications. One of the working areas is the definition of different applications together with their requirements. In fact, the ETSI TR 102 638 standard [11] defines the Basic Set of Applications (BSA) for V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) and I2V (Infrastructure-to-Vehicle) communications. The standard defines four application classes:

1. *Active road safety.* The goal of these types of applications is to improve road safety by providing driving assistance, with cooperative awareness and/or road hazard warning applications. Example use cases of these applications are intersection collision warning, wrong way driving warning, roadwork warning, etc.
2. *Cooperative traffic efficiency.* Applications from this class are devoted to improve traffic fluidity. Thus, the defined applications are speed management and cooperative navigation, with use cases like regulatory/contextual speed limit notification or traffic information and recommended itinerary.

3. *Cooperative local services.* These type of applications provide on-demand information based on the location of the vehicles and are provided from within the ITS network infrastructure. Common use cases of these type of applications are point of interest notification or media downloading.
4. *Global Internet services.* Applications in this class provide global Internet services on commercial or non-commercial basis. Two different applications are distinguished in this class: (1) community services like fleet management; (2) ITS station life cycle management with services like vehicle software/data provisioning update. That is, these services may include Infotainment, comfort and vehicle or service life cycle management and are acquired from providers in the wider Internet.

In addition, the ETSI TS 102 637-1 [13] defines the functional requirements of the BSA, specifying different flow diagrams for the different use cases of each service class. These requirements are based on the implementation of Cooperative Awareness Message (CAM) and Decentralised Environmental Notification Message (DENM) messages that are defined at the same time in the ETSI EN 302 637-2 [18] and ETSI EN 302 637-3 [19] standards.

On the other hand, security in the ITS context is essential. In fact, the ETSI has published several technical specifications related to security: (1) the ETSI TS 102 940 [14] technical specification where an ITS communication security architecture is defined; (2) a technical specification defining ITS confidentiality services [17], pointing out that there are no mandatory confidentiality services for the application layer, and mentioning that the confidentiality in the network layer is protected using the IPsec ESP protocol; (3) a technical specification defining how to manage trust and privacy [15]; and (4) another specification defining access control [16]. Therefore, the provision of security services is regarded as critical in this scenario.

Regarding the technological strategy to provide communications it is important to take into account that a vehicle is constantly changing its location so its mobility has to be managed in order to have continuous communication without service disruption and to allow reachability to nodes onboard regardless the location of the vehicle. That is, a mobility management protocol is required for vehicular communications. The protocol considered at present by ISO and ETSI standardisation bodies in the definition of a vehicular communication architecture [12,20] for managing mobility is the NEMO BS [26] protocol. However, NEMO BS lacks of the required security support and the efficiency needed in the vehicular communications [9,22]. Because of this, we propose the use of the NeMHIP protocol as an alternative solution to manage securely and efficiently the mobility.

3 The Underlying Mobility Management Protocol: NeMHIP

The NeMHIP protocol is a novel, secure and efficient network mobility management protocol for ITS scenarios which is based on the HIP protocol [21]. HIP is

a NeMHIP defines a single security framework for protecting mobility management procedures and data exchanges, by means of the generation of independent and secret keying material in a single procedure.

HIP alike, the NeMHIP protocol consists of three different procedures: (1) the NeMHIP Registration procedure, which has the goal of ensuring the reachability of nodes onboard; (2) the NeMHIP Association Establishment procedure, which has the goal of establishing an association between a node located in the outside network like the Internet, a Correspondent Node (CN), and a node onboard, a Local or Mobile Network Node (LMN, MNN), and of agreeing upon a security context for the exchange of application data securely; (3) the NeMHIP Association Update procedure, which has the goal of maintaining the established associations when a mobility event that involves the change of the IP address takes place, or when rekeying is requested, so, it allows to maintain the communications and the reachability of nodes transparently for user applications. Next, we briefly introduce those procedures. More details can be found in [24,25].

3.1 NeMHIP Registration

The NeMHIP Registration process is aimed at ensuring the reachability of MNNs onboard by registering them in an updated server where their identifiers and locators are stored. In the HIP architecture this server is called a Rendez-Vous server (RVS). As a result of the registration, a mapping between the identifier (HIT) and the locator (IP address) of the HIP node are stored in the RVS.

In the vehicular scenario, it is likely to have all devices switched on simultaneously. Consequently, it is interesting to think on a bulk registration. Figure 1 shows the NeMHIP Registration flow chart. In black, messages that are equal to those defined by the base HIP protocol are shown, while the message in orange (*mI2*) has been specifically designed for the Bulk Registration process.

3.2 NeMHIP Association Establishment

Whenever two HIP-aware nodes want to exchange data for the first time in a secure way, an association establishment signalling exchange takes place. By means of this exchange, both nodes agree upon a security context; that is, they agree upon the algorithms and keys to protect the messages to be exchanged. Consequently, one of the most important procedures when defining a communication protocol between a mobile network and the infrastructure is the end-to-end association establishment. In the same way as for the NeMHIP Registration procedures, the NeMHIP Association Establishment process stems from the HIP association establishment, but new parameters, packet formats and procedures have been introduced to support network mobility scenarios and to provide them with the adequate security and efficiency level.

In this protocol not only end-to-end keying material is agreed but also independent keying between the MR and the CN. That is, in this new approach a security association between the MR and the CN is established to protect

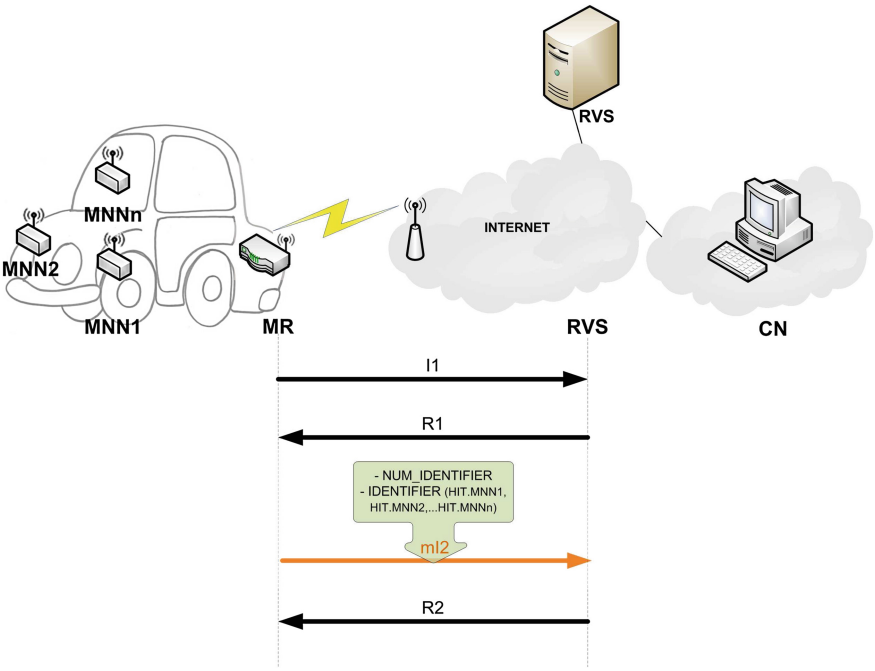

Fig. 1. NeMHIP Registration flow chart

mobility management messages as well as an end-to-end association is established between the MNN and the CN to protect user application data, both by means of a single signalling exchange. During this exchange, the MNN informs the MR about the keying material index that it will use for deriving end-to-end keys. Nevertheless, as the MR does not have knowledge of the keying material agreed upon between the CN and the node inside the moving network, end-to-end integrity and confidentiality are ensured while new end-to-end key generation can be managed by the MR, not revealing to it the keys. Figure 2 shows the NeMHIP Association Establishment flow chart and involved processing in the nodes.

3.3 NeMHIP Association Update

The core of the mobility support of the NeMHIP protocol is the association update process described in this section. Commonly, an established NeMHIP association will be updated when the MR changes its point of attachment to the Internet. This scenario often gives rise to drastically change link characteristics like throughput or delay. These changes may lead to packet reordering and packets falling outside the ESP anti-replay window [23] and therefore, to packet discarding. Consequently, whenever a host changes its locator the NeMHIP SA has to be renewed.

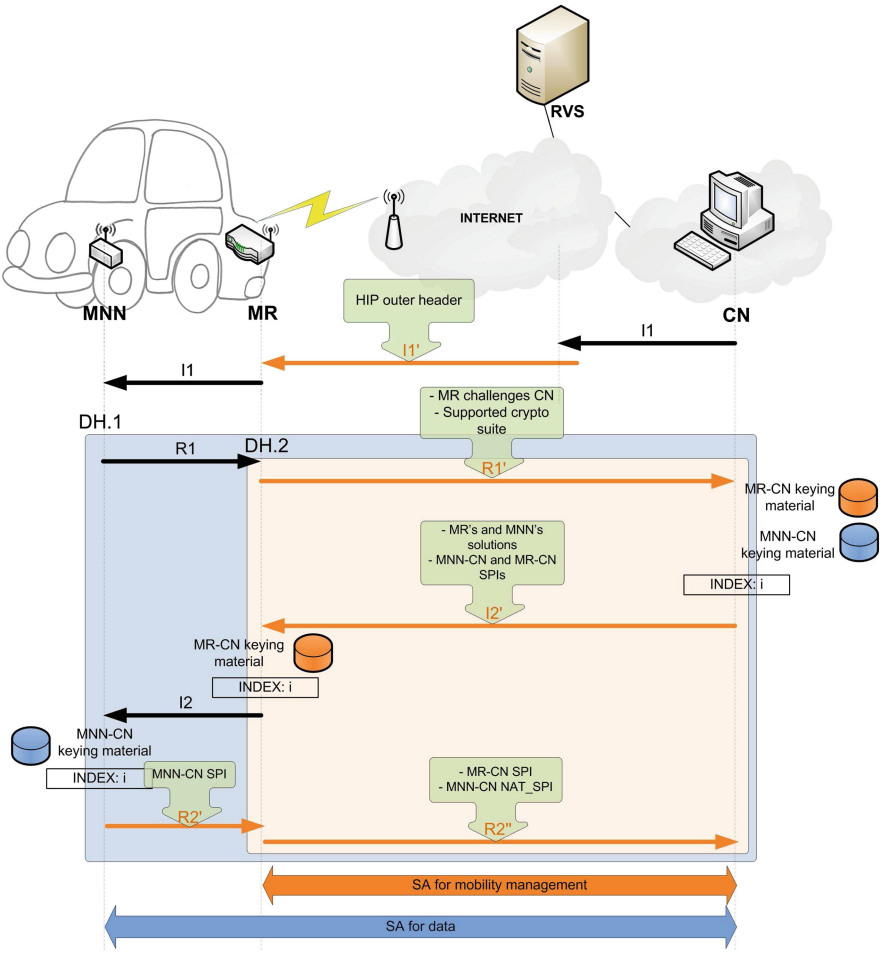

Fig. 2. NeMHIP Association Establishment

Following the same design approach as the other NeMHIP procedures, the NeMHIP Association Update procedure also stems from the HIP update procedure, but new messages and parameters have also been introduced. Figure 3 shows the update signalling exchange caused by the MR.

4 Evaluation Scenario

In this section, the developed simulation framework to evaluate the performance of vehicular applications is described. We have selected the OMNeT++ [3] simulation tool as the communication simulator, the SUMO [2] traffic simulator to simulate the traffic of vehicles, a framework that merges these two simulation

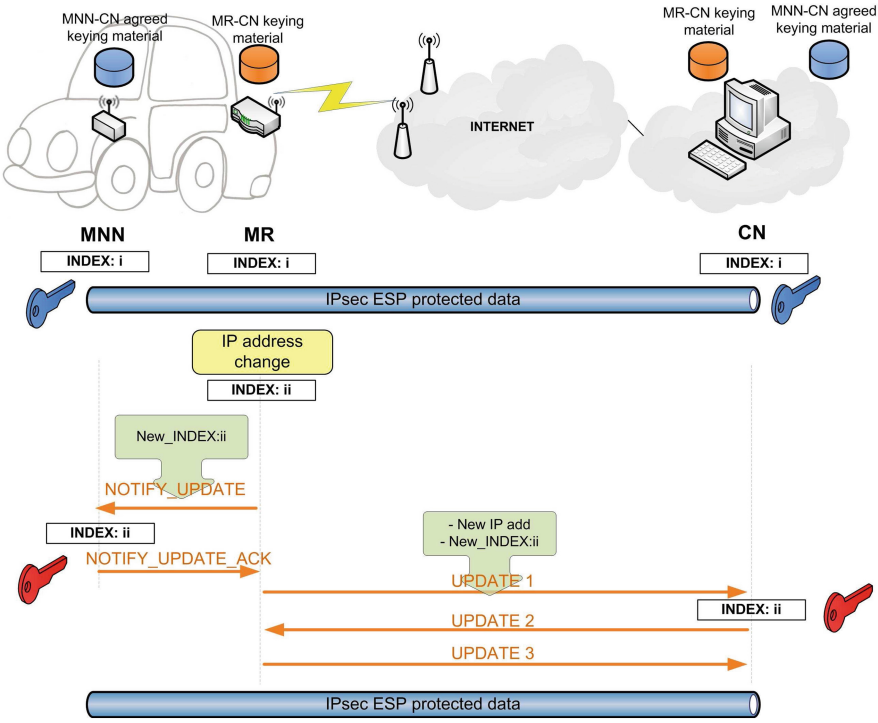

Fig. 3. NeMHIP Association Update caused by the MR

tools named VEINS [4], and the VSimRTI [5] tool to dynamically simulate the vehicular applications. Figure 4 shows the simulation framework.

More precisely, this simulation framework runs on a Ubuntu 12.04 operating system, where we have OMNeT++ 4.4.1, SUMO 0.21.0, VEINS 2.2 and VSimRTI 0.13.4 simulation tools integrated.

4.1 Analysed Vehicular Applications

Although there is a variety of vehicular applications available for vehicular communications, we have selected three different applications because they have different QoS requirements and are expected to be common in the near future. These applications are based on the CAM and DENM messages defined by the ETSI standards [18,19]. We next describe these vehicular applications.

1. *Emergency braking.* The goal of this application is to control the emergency braking of a vehicle. This application sends messages periodically and warns about an emergency braking if necessary. In order to avoid possible accidents, this application demands minimum end-to-end delay. This application sends a notification periodically (every 2 s).

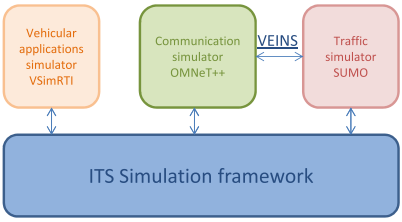

Fig. 4. Developed simulation framework

2. *A real-time webcam conversation.* This application sends periodically video traffic. The real-time nature of this application requests also minimum end-to-end delay to maintain its conversational characteristic.
3. *Weather forecast notification.* This application does not demand stringent QoS requirements but it is desired to have minimum packet loss and a minimum end-to-end delay is suggested.

4.2 Developed Evaluation Scenario

With the goal of analysing the aforementioned ITS applications, an evaluation scenario that approximates as much as possible to a real scenario has been developed. Because of this, we have selected an urban scenario that implies a variety of velocities, different directions and routes of vehicles, variations in the number of connections to be established, etc. More precisely, we have defined a circular route in the city centre that lasts 16 min and with a maximum speed of 50 km/h. For the sake of simplicity and with the goal of analysing the impact of the number of LMNs and the underlying NeMHIP protocol, this study considers a single vehicle. The left side of Fig. 5 shows the route of the vehicle. In order to have a real urban scenario, we have introduced the map of the city of Bilbao (Spain) which is shown in the right side of Fig. 5 provided by the OpenStreetMap tool [1] in the SUMO simulation tool. This way, we can simulate a realistic scenario with real routes that vehicles follow.

Fig. 5. The route of the vehicle in Bilbao city centre and the map of the city of Bilbao obtained from OpenStreetMap

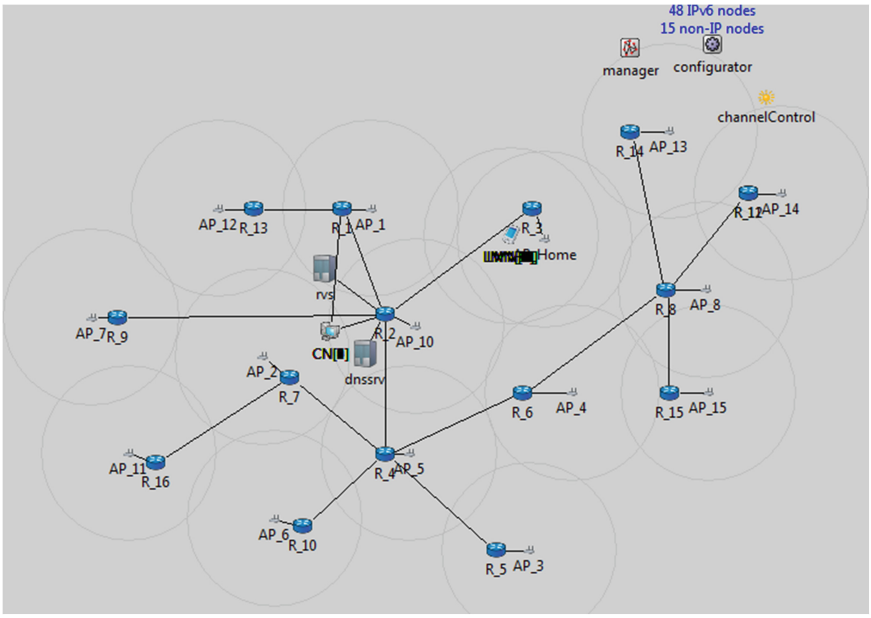

Fig. 6. Network topology defined in OMNeT++

Once the vehicle and its route are defined, it is necessary to configure the OMNeT++ simulator, that is, the communications simulator. More specifically, we have configured a network with 15 WiFi APs, several routers, a DNS server, the mobile network (vehicle), the communication endpoint (CN) and a RVS, and we have placed them as shown in Fig. 6.

5 Results and Discussion

This section shows the obtained results for each of the vehicular applications analysed. In order to evaluate the performance of the applications, we have considered four different scenarios in terms of number of LMNs onboard: 1 LMN, 5 LMNs, 10 LMNs and 20 LMNs. For each of the scenarios we have conducted 30 simulations following the central limit theorem. This way, we obtain the mean value and the limit values for 90 %, 95 % and 99 % confidence intervals. For the three applications (emergency braking, a real-time webcam application and weather forecast notification) we have analysed the mean end-to-end delay of the packets and compare obtained results with the ITU-T and 3GPP standards, which point out that it should be preferably <150 ms and 400 ms at most, as well as with a recent White Paper published by the 5G-PPP where future vehicle communications and enabling technologies are outlined. Figures 7 and 8 show the results obtained for the emergency braking application and for the weather warning application respectively.

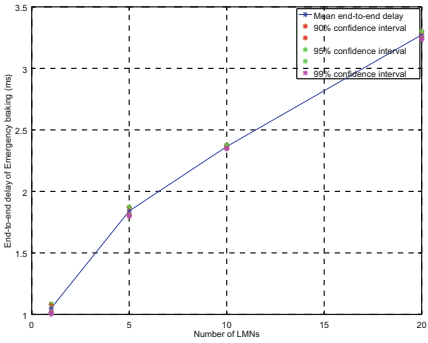

Fig. 7. End-to-end delay of the emergency braking application

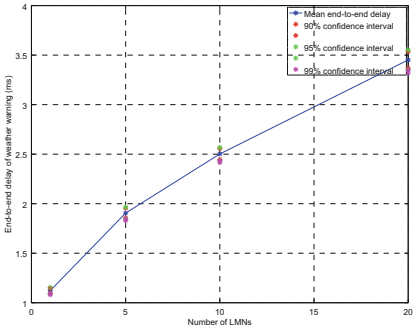

Fig. 8. End-to-end delay of the weather warning application

Obtained results show that with the increase in the number of LMNs the end-to-end delay of the applications increase but it is still less than 4 ms. In the 5G Automotive Vision white paper [8] Key Performance Indicators (KPIs) for vehicle applications are defined. More precisely, although this white paper describes different use cases the emergency braking is not described but other use cases like automated overtake, cooperative collision avoidance or high density platooning are introduced and the defined maximum end-to-end delay is set to 10 ms. Although this value is restrictive due to the nature of the automotive context, we still fulfil the recommendation.

Apart from evaluating *Active Road Safety* type of application by means of the emergency braking and weather notification applications, we have also analysed a *Global Internet Services* type of application, infotainment in this case, by evaluating the end-to-end delay of a real-time webcam conversation. Figure 9 shows obtained results.

As can be regarded, the obtained values for end-to-end delay webcam conversation and also for the other two applications fully satisfy the ITU-T Y.1541 recommendation which points out that the end-to-end delay should be 100 ms at most, and with the 3GPP TS 22.105 which establishes this value in 150 ms.

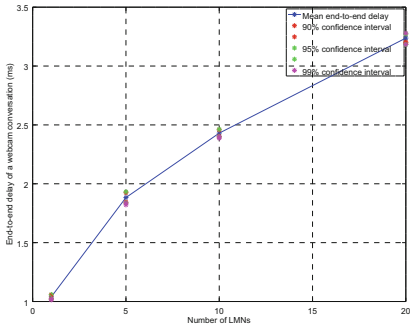

Fig. 9. End-to-end delay of the real time webcam conversation

Consequently, the end-to-end delay can be considered negligible while the impact of the introduction of a novel protocol such as NeMHIP does not involve any additional delay.

6 Conclusions

The connected vehicle is expected to be a reality in the near future. This capacity of being vehicles connected with other vehicles, roadside units or the Internet will increase road safety and security thanks to innovative cooperative applications that will assist driving and offer new services to the users. However, at present this complex scenario poses technological challenges that need to be addressed.

In order to guarantee the demanded safety and security level in the automotive scenario, vehicular applications need to satisfy stringent performance and security requirements.

In this paper we present a realistic simulation framework based on the OMNeT++, SUMO, VEINS and VsimRTI simulation tools to evaluate new vehicular applications. More specifically, we have evaluated an emergency braking application, a weather forecast notification application and a real time webcam conversation application. This way, we have checked a variety of applications each with different QoS demands. Since the vehicle is a moving network, its mobility has to be managed securely and efficiently. Because of this, we have selected the NeMHIP protocol to manage the mobility and include it in our simulation framework as a key enabler of the always connected vehicle.

Obtained results demonstrate that the end-to-end delay of the analysed applications fulfils the ITU-T Y.1541 and 3GPP TS 22.105 recommendations, and even more stringent requirements recently defined in the 5G Automotive Vision white paper by the 5G-PPP. Consequently, we demonstrate that the NeMHIP protocol is suitable because it fulfils the mentioned requirements even in using a realistic simulation framework and that the developed simulation tool is a valid framework for evaluating new vehicular applications.

References

1. OpenStreetMap. https://www.openstreetmap.org/
2. Simulator for Urban Mobility. http://sumo-sim.org/
3. The OMNeT++ Network Simulator. http://omnetpp.org/
4. Veins Simulator. http://veins.car2x.org
5. VSimRT Smart Mobility Simulation. http://www.dcaiti.tu-berlin.de/
6. ITU-T Y.1541. Network Performance Objectives for IP-Based Services (2006)
7. 3GPP TS 22.105 v7.1.0 (2006–12). Technical Specification Group Services and Systems Aspects; Services and service capabilities (Rel. 11) (2013)
8. 5G-PPP: 5g-ppp white paper on automotive vertical sector. Technical report, The 5G Infrastructure Public Private Partnership (2015)
9. Petrescu, A., Olivereau, A., Janneteau, C.: Threats for Basic Network Mobility Support (NEMO threats), January 2004
10. Analysis Mason: Connected cars: worldwide trends, forecasts, and strategies 2014–2024. Technical report (2014)
11. European Telecommunications Standards Institute: ETSI TR 102 638 V1.1.1 (2009–06), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions. Technical report, ETSI (2009)
12. European Telecommunications Standards Institute: ETSI EN 302 665 (2010). Intelligent Transport Systems (ITS): Communications Architecture. Technical report, ETSI (2010)
13. European Telecommunications Standards Institute: ETSI TS 102 637-1 V1.1.1 (2010–09), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions; Part 1: Functional Requirements. Technical report, ETSI (2010)
14. European Telecommunications Standards Institute: ETSI TS 102 940 V1.1.1 (2012–06), Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. Technical report, ETSI (2012)
15. European Telecommunications Standards Institute: ETSI TS 102 941 V1.1.1 (2012–06), Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. Technical report, ETSI (2012)
16. European Telecommunications Standards Institute: ETSI TS 102 942 V1.1.1 (2012–06), Intelligent Transport Systems (ITS); Security; Access Control. Technical report, ETSI (2012)
17. European Telecommunications Standards Institute: ETSI TS 102 943 V1.1.1 (2012–06), Intelligent Transport Systems (ITS); Security; Confidentiality services. Technical report, ETSI (2012)
18. European Telecommunications Standards Institute: ETSI TS 302 637-2 V1.3.1 (2014–09), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Technical report, ETSI (2014)
19. European Telecommunications Standards Institute: ETSI TS 302 637-3 V1.2.2 (2014–11), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specification of Decentralized Environmental Notification Basic Service. Technical report, ETSI (2014)
20. International Standardization for Organization: ISO-21217-CALM-Architecture. Intelligent Transport Systems - Communications access for land mobiles (CALM) - Architecture. Technical report, ISO (2010)

21. Nikander, P., Gurtov, A., Henderson, T.R.: Host Identity Protocol (HIP): connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks. IEEE Commun. Surv. Tutorials **12**(2), 186–204 (2010)
22. Jung, S., Zhao, F., Wu, S.F., Kim, H., Sohn, S.: Threat Analysis on NEMO Basic Operations, July 2004
23. Kent, S.: IP Encapsulating Security Payload (ESP). RFC 4303, December 2005
24. Toledo, N., Bonnin, J.M., Higuero, M.: Performance evaluation of user applications in the its scenario: an analytical assessment of the nemhip. J. Netw. Comput. Appl. **36**, 1324–1336 (2013)
25. Toledo, N., Higuero, M., Huarte, M., Matias, J., Jacob, E., Unzilla, J.J.: A proposal to contribute to its standardization activity: a valuable network mobility management approach. Comput. Stand. Interfaces **36**(3), 465–479 (2014)
26. Devarapalli, V., Wakikawa, R., Petrescu, A., Thubert, P.: Network Mobility (NEMO) Basic Support Protocol. RFC 3963, August 2005