HAL
archives-ouvertes.fr

C-ITS PKI protocol: Performance Evaluation in a Real Environment

Farah Haidar, Arnaud Kaiser, Brigitte Lonc, Pascal Urien

▶ **To cite this version:**

Farah Haidar, Arnaud Kaiser, Brigitte Lonc, Pascal Urien. C-ITS PKI protocol: Performance Evaluation in a Real Environment. WONS 2019 15 th Wireless On-demand Network systems and Services Conference, Jan 2019, Wengen, Switzerland. <hal-01978179>

HAL Id: hal-01978179
https://hal.archives-ouvertes.fr/hal-01978179

Submitted on 11 Jan 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

C-ITS PKI protocol: Performance Evaluation in a Real Environment

Farah HAIDAR[1,2,3], Arnaud KAISER[2], Brigitte LONC[1], and Pascal URIEN[3]

[1] *Renault*, Guyancourt, France, Email: name.surname@renault.com
[2] *IRT SystemX*, Palaiseau, France, Email: name.surname@irt-systemx.fr
[3] *Telecom ParisTech*, Paris, France, Email: name.surname@telecom-paristech.com

***Abstract*—In the near future, vehicles and road-side units (RSU) will communicate and cooperate by broadcasting V2X messages over the vehicular network (IEEE 802.11p). These messages are used by safety applications to improve road safety and traffic efficiency. However, those messages could also be used in a malicious way to track vehicles.**

Therefore, to guarantee drivers privacy, vehicles use pseudonym identities (or certificates) provided by a Public Key Infrastructure (PKI). During a trip, vehicles frequently change of certificates to make tracking much more difficult. They thus need to reload their certificates pool by requesting new ones to the PKI.

In this paper, we evaluate the performance of the PKI protocol regarding the reloading of certificates. We ran several tests while driving in order to quantify the number of certificates that can be reloaded from the PKI at different speeds. The obtained results show that 1) the end-to-end latency between a requesting vehicle and the PKI is non-negligible and 2) as speed increases, the number of successfully reloaded certificates decreases.

***Keywords*—C-ITS security, PKI, performance evaluation**

I. Introduction

Tomorrow's vehicles will communicate and cooperate by exchanging V2X messages in order to improve road safety and traffic efficiency.

The exchanged messages contain critical data like geographic position, speed, heading, etc. These data are directly linked to the driver's privacy because they enable vehicles tracking by eavesdropping the exchanged V2X messages. The protection of driver's privacy is a crucial element in vehicular networks as it is one of the important conditions for user's acceptance of connected vehicles. Therefore, in order to protect driver's privacy, vehicles use pseudonym certificates and frequently change them (i.e they change their digital identity) in such a way that it becomes much harder to track them. To enable frequent change of pseudonyms, vehicles use a pool of available pseudonyms (60 per week for C2C and maximum 100 per week for the European commission [1]) that has to be reloaded over time. Consequently, vehicles need to communicate with the PKI to reload their pseudonym pool.

The question of when vehicles should request new pseudonyms can be raised. For instance, is it possible for a vehicle to reload pseudonyms while driving? If yes, how many pseudonyms can be reloaded and at which speed? What is the end-to-end latency to reload one pseudonym? These are the questions we address in this paper through real experimentations.

We ran several experimentations at different driving speeds and compare the performance of two communication profiles (with and without V2X security). The obtained results show that the number of pseudonyms successfully reloaded decreases when speed increases for both profiles. The end-to-end latency is quite high and remains constant versus speed.

The remaining sections of this paper is organized as follow: section II presents the related works. Section III briefly describes the PKI while section IV details our considered use case. Section V analyses the obtained results and section VI concludes this paper.

II. Related works

To the best of our knowledge only a few papers in the literature evaluate the performance of certificates reloading in real environment.

The latency of pseudonym certificates reloading can be divided in two parts: 1) the latency of the embedded operations (message creation, encryption and signature) and 2) the network latency. Authors of [2] focus on the first part. They evaluate the performance of their security system using a set of performance indicators (signature/verification delays, packets signature/verification per second, pseudonym change latency). In this paper we go a step further by including the network latency and comparing two communication profiles.

In our previous work [3], we evaluated the performance of pseudonym certificates reloading by deploying an in-lab testbed and comparing two communication profiles in terms of network overhead and end-to-end latency. In this paper we extend our evaluation by conducting real experimentations while driving to get additional performance indicators such as the number of pseudonyms that can be reloaded versus speed.

III. C-ITS PKI Architecture

The PKI is a set of entities that create, manage and distribute digital certificates. We implemented a PKI

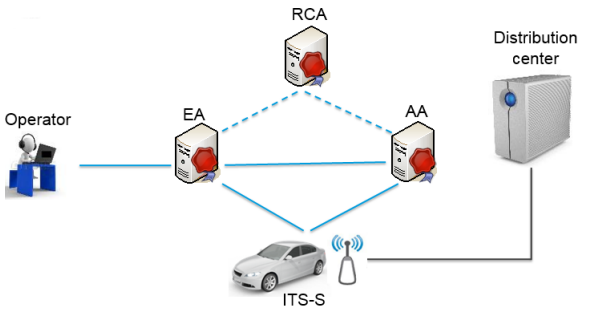


Fig. 1. PKI architecture

that is compliant with the European Telecommunications Standards Institute (ETSI). Figure 1 depicts our PKI architecture that consists of the following entities:

- **Root Certificate Authority (RCA)**: RCA is the root of trust for all certificates within the PKI hierarchy. It delivers certificates to the Enrolment Authority (EA) and the Authorization Authority (AA) to authorize them to issue certificates to Intelligent Transport System-Station (ITS-S).
- **Enrolment Authority (EA)**: EA issues one Enrolment certificate (EC) per ITS-S. EC are considered as a proof of identity, thus used to identify and authenticate ITS-S within the PKI.
- **Authorization Authority (AA)**: AA issues pseudonyms to ITS-S that are used in V2X communications.
- **Distribution Center (DC)**: provides to ITS-S up-to-date trust information necessary to validate that received information come from a legitimate and authorized ITS-S/PKI authority.
- **Operator**: registers ITS-S and updates necessary information in the EA.
- **ITS-S**: end-entity of the system that requests certificates to the PKI and communicates with other end-entities.

Basically speaking, ITS-S requests pseudonym certificates to the AA. In order to prevent that an AA links differents pseudonyms to a same requesting ITS-S (thus breaking the ITS-S privacy), ITS-S are allowed to request only one pseudonym per request. That is, in order to get 10 new pseudonyms, an ITS-S must send 10 independant requests to the AA.

IV. Use case and experimentation setup

Our considered use case is depicted in figure 2. A vehicle is within range of a RSU that provides Internet access. The vehicle has very few pseudonyms and needs to refill its pool. It thus uses the RSU as gateway forwarder to reach the PKI and requests new pseudonyms.

We evaluate the amount of pseudonyms reloaded at the following speeds (km/h): 30, 50, 70 and 90. The "in-RSU-range" detection mechanism works as follow: the vehicle sends ICMPv6 Echo Requests (or "ping") to the PKI.

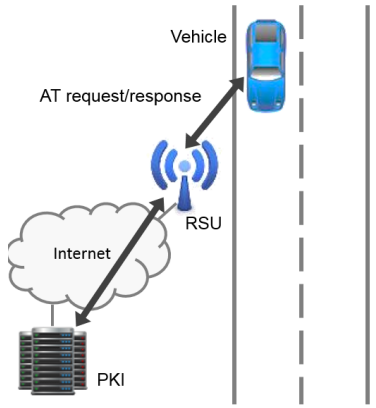


Fig. 2. Use case: pseudonyms (or AT) reloading through RSU

When the vehicle enters the range of the RSU, it receives back an ICMPv6 Echo Reply from the PKI. This response indicates that the vehicle can communicate with the PKI through the RSU. The vehicle then starts requesting new pseudonyms. When the vehicle moves out of range of the RSU (i.e. when no more new pseudonyms are received), the requesting of new pseudonyms is stopped. We configured the vehicle in such a way that it continuously requests new pseudonyms as long as it is under the RSU radio coverage.

A. Communication profiles

According to ETSI standards [4], a vehicle can send a pseudonym request to the PKI using two communication profiles presented in figure 3:

1) **TIG profile**: **T**CP over **I**Pv6 over **G**5
2) **TI3G profile**: **T**CP over **I**Pv6 over **G**N6ASL over **G**N over **G**5

The difference between the two communication profiles is that TI3G provides security in the ITS G5 network between the vehicle and the RSU, whereas TIG does not provide any security. Figure 3 shows the message flow inside the vehicle to create and send a request for TIG ($1\rightarrow 2\rightarrow 3\rightarrow 4\rightarrow 9$) and TI3G ($1\rightarrow 2\rightarrow 3\rightarrow 4\rightarrow 5\rightarrow 6\rightarrow 7\rightarrow 8\rightarrow 9$) profiles.

On the other hand, a message sent using TI3G contains overhead and the RSU has to verify the request from the vehicle and sign the response from the PKI, which adds processing latency. In this paper, we evaluate these two communication profiles in term of end-to-end latency and number of pseudonyms reloaded at different speeds.

B. Protocol

Figure 4 shows the sequence diagram of the messages that are exchanged between the vehicle and the PKI through the RSU. The dotted arrows depict the additionnal operations generated when using TI3G communication profile. Basically speaking, the request is sent by the vehicle to the RSU that forwards it to the PKI and vice-versa for the response. On the PKI side, a verification is

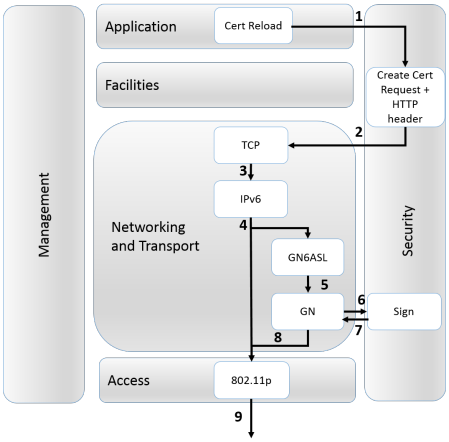


Fig. 3. Data path within ETSI ITS-S architecture when requesting a pseudonym

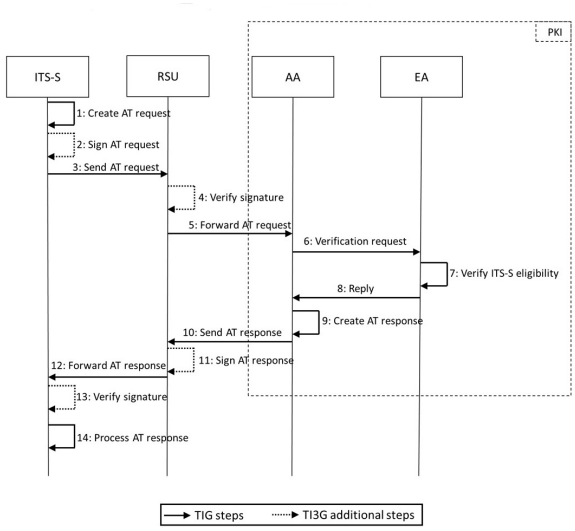


Fig. 4. Pseudonym (or AT) request/response using TIG/TI3G profile

made to ensure that the requesting vehicle is registered and authorized to request new pseudonyms, as specified by the ETSI PKI protocol [5].

C. Test environment

The experimentations were conducted on the test track "Val d'or" located at Versailles-Satory (France) and using our vehicle prototype. The vehicle is provided by RENAULT and the model is a MEGANE COUPE as depicted in figure 5. Figure 6 depicts a satellite view of the test track. We equipped the test track with one RSU depicted by the red antenna. The green line shows the radio coverage of the RSU (about 940 meters) whereas the red line shows the road segment which is out of the coverage of the RSU. We equipped our prototype vehicle with an on-board unit (OBU), a Samsung tablet, a Raspberry Pi that provides an in-vehicle Wi-Fi access point (to connect the tablet with the OBU), and two IEEE

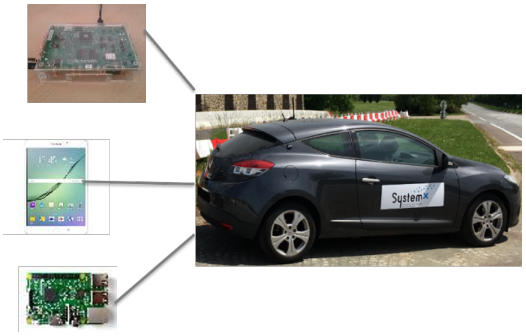


Fig. 5. In-vehicle equipments



Fig. 6. Versailles-Satory test track (green line = RSU coverage)

802.11p antennas that we placed on the vehicle's roof. The list of hardwares/softwares and the configuration of the antennas are presented in table I.

OBU	Hardware	RENESAS R-Car E2 board
		Antenna with gain +9dBi
	Software	IEEE 802.11p driver
		V2X communication stack
		V2X security stack
		Pseudonym reloading application
RSU	Hardware	RENESAS R-Car E2 board
		Antenna with gain +6dBi
	Software	IEEE 802.11p driver
		V2X communication stack
		V2X security stack
PKI	Hardware	DELL Latitude 3330
	Software	ISE PKI [6]
Config	ITS G5 channel	CCH(180)
	OBU radio power (incl. antenna gain)	+33 dBm e.i.r.p
	RSU radio power (incl. antenna gain)	+33 dBm e.i.r.p
	RSU radio coverage	940 meters

TABLE I
HARDWARE AND SOFTWARE CONFIGURATIONS

V. Results and analysis

We conducted the experimentations as follow: we did two track laps for each speed (30, 50, 70 and 90 km/h) and for each communication profile (TIG and TI3G), resulting in a total of 16 laps. The main objectives of these experimentations are 1) to demonstrate the correct behaviour of the system in a realistic environment and 2)

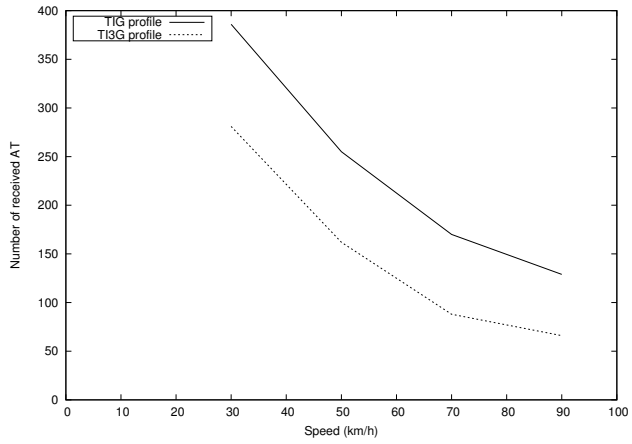


Fig. 7. Number of pseudonyms (or AT) reloaded versus speed for both communication profiles

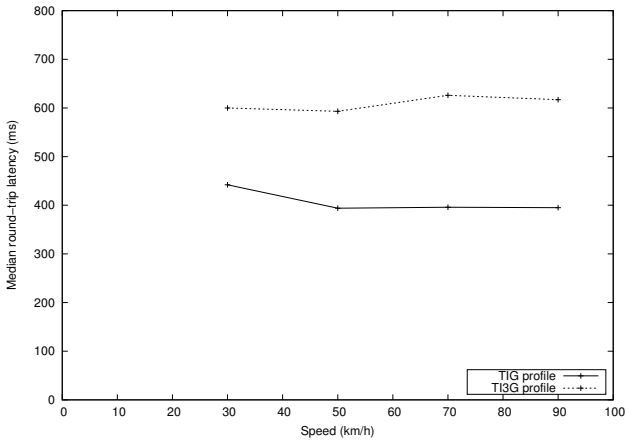


Fig. 8. Pseudonyms reload median end-to-end latency versus speed

to evaluate the system performance in terms of number of pseudonyms reloaded and the end-to-end latency.

A. Number of pseudonyms reloaded

Figure 7 shows the number of pseudonyms successfully reloaded from the PKI versus the speed of the vehicle. The presented values are the sum of the two laps for each speed. We first observe that the number of pseudonyms successfully reloaded decreases as speed increases, following an exponential shape. This result was expected as the faster the vehicle moves, the less time it remains under the RSU radio coverage, thus the less time it has to reload new pseudonyms. Second, we also observe that both curves have the same shape and the gap between them remains constant when speed increases. The gap is explained by the additional security processing required by the TI3G profile. Apart from the gap, the similar shape of both curves shows that the speed has the same impact on the performance, no matter what communication profile is used.

B. End-to-end latency

Figure 8 depicts the median end-to-end latency of the pseudonym request/response for both profiles versus speed. We observe that the end-to-end latency is always shorter when using TIG profile. This was also observed during our in-lab experimentations and is explained by the additional security processing required by the TI3G profile. Also, the median end-to-end values remains roughly constant versus speed, i.e. the speed has no impact on the time required to successfully reload a pseudonym. Finally, the median end-to-end latency is roughly half a second to reload one pseudonym, which is quite high, especially for a highly mobile network.

VI. Conclusion and future works

In this paper we evaluate the performance of pseudonyms reloading in a realistic environment. We compare two communication profiles: with and without the V2X security using different speeds (30 to 90 km/h).

The obtained results in terms of end-to-end latency show that requesting pseudonyms is always shorter when using TIG profile but remains still high (about half a second). As we expected, the speed has an impact on the number of reloaded pseudonyms as the faster a vehicle moves, the less time it has to reload new pseudonyms.

Future works include a performance evaluation and comparison with the integration of a Hardware Security Module (HSM) that accelerates cryptographic operations (and thus decrease the end-to-end latency), and evaluating the protocol under a congested ITS G5 network (high density of vehicles).

Acknowledgments

This research work has been carried out in the framework of the Technological Research Institute SystemX, and therefore granted with public funds within the scope of the French Program *Investissements d'avenir*.

References

[1] ETSI TR 103 415, "Intelligent Transport Systems (ITS); Security; Prestandardization study on pseudonym change management ," 2018.

[2] Rim Moalla, Brigitte Lonc, Gerard Segarra, Marcello Laguna, Panagiotis Papadimitratos, Jonathan Petit , Houda Labiod, "Experimentation with the PRESERVE VSS and the Score@F system," in *Transport Research Arena*, 2014.

[3] Farah Haidar, Arnaud Kaiser and Brigitte Lonc, "On the performance evaluation of vehicular PKI protocol for V2X communications security," in *IEEE Vehicular technology Conference (VTC)*, 2017.

[4] ETSI TS 102 940, "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management," June 2012.

[5] ETSI TS 102 941, "Intelligent Transport Systems (ITS); Security; Trust and privacy management," March 2018.

[6] J.P. Monteuuis, Badis Hammi, Eduardo Salles, Houda Labiod, Remi Blancher, Erwan Abalea, Brigitte Lonc, "Securing PKI Requests for C-ITS Systems," in *International Conference on Computer Communication and Networks (ICCCN)* , 2017.