A TPM-based Architecture for Improved Security and Anonymity in Vehicular Ad hoc Networks

Gilles Guette and Olivier Heen

***Abstract*— Vehicular Ad hoc Networks get increased attention by vehicle manufacturers and researchers. Their deployment requires that security and privacy issues be resolved, particularly since they rely on wireless communication.**

In this paper, we propose a TPM-based security architecture, where TPM are embedded in vehicles. We emphasize the management of cryptographic keys needed for security and anonymity of vehicles' communications. Compared to many existing solutions, our architecture requires no deployment of base stations along the roads. A special attention is paid to anonymity in order to prevent unauthorized tracking of a vehicle. Moreover, we provide a way for the authority to revoke the anonymity, as it is the case nowadays with the license plates. We discuss the robustness of this system against a compromised authority. We also indicate how the use of a portable storage device, like a USB memory stick, improves the quality of the anonymity by opportunistically binding the TPM to a security server.

I. Introduction

VANETs are highly dynamic ad hoc network with very limited access to an infrastructure [CG07], [BE04], [ZMTV02]. If base stations are sparsely deployed along the road, access to them is also of very short duration, particularly because of vehicles speed. The lack of permanently accessible network infrastructure means that decentralized architecture is necessary. In this paper, we do the assumption that the deployment of Road Side Units (RSU) will take time and that a solution working also without RSU is needed. Moreover, the applications related to passenger safety are critical. Hence, the security architecture must prevent an attacker to successfully launch an attack aiming to cause collisions.

A TPM is a hardware chip with encryption abilities. In this paper, we propose a TPM-based architecture [TCG05], [GB08] in which a TPM is embedded in each vehicle to address the problem of communication security and anonymity in VANET.

Some TPM features require from time to time connection to an external server. For this we assume a solution working without the support of RSU. We use a USB memory stick carried by the driver from a PC with an Internet connection (Home, Office) to the vehicle, as shown on Figure 1. The memory stick can store both data from the vehicle's sensors and data from the TPM such as requests for key certification.

G. Guette is with IRISA, Campus Universitaire de Beaulieu, 35042 Rennes, France. gilles.guette@irisa.fr

O.Heen is with INRIA Rennes-Bretagne Atlantique, Campus Universitaire de Beaulieu, 35042 Rennes, France. olivier.heen@inria.fr

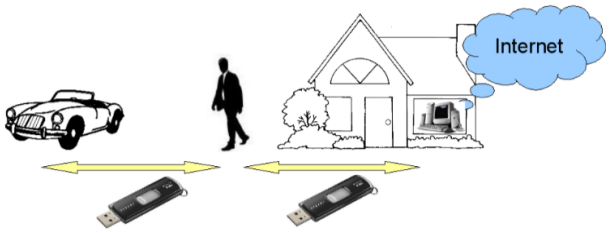

Fig. 1. The USB memory stick covers the last meters if needed.

The solution proposed in this paper is based on keys preloaded in the vehicle during the construction phase and on a protocol using the memory stick to renew the certified keys.

In section II, we present the motivations of this paper and we recall the technical environment. In section III, we present our solution and describe the communication protocols between the different components of the proposed architecture. In section IV, we describe the security of our solution as well as some quantitative considerations.

II. Motivations

The solution proposed in this paper provide **anonymous** and **secure** communication between vehicles constituting the network. In the Section II-A, we present some related work on VANET security. Then, in Section II-B, we describe briefly what is a TPM and the cryptographic material used.

A. Vehicular network security

The open nature of a VANET makes communication security a great challenge [HvL04], [PP05], [ABD+06]. In a VANET, data is broadcasted over a shared communication media: a malicious node may easily intercept, modify or inject data. Data injection can provoke collisions in a vehicular platoon [BE04] as shown on figure 2.

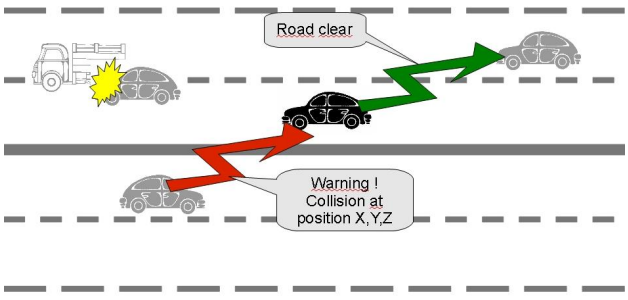

Fig. 2. An example of injection attack in a VANET.

Vehicular PKI [RH05], [RPH06], [RH07], is an approach to VANET security. It is based on a Public Key Infrastructure (PKI) and base stations along the road. Both provide support for the infrastructure, key distribution and revocation. VPKI solutions protect from car tracking using an *anonymous key set* and a *key changing algorithm*. VPKI are promising for VANET applications. However, the PKI deployment is a large-scale and potentially costly procedure. It requires large-scale testing after deployment to ensure operation under real-world VANET conditions.

Other solutions [Döt05], [GFL+07], [FFBA07] also address the problem of privacy in VANET with the help of an infrastructure and the use of pseudonyms. Here, infrastructure covers base stations and certification authorities. [FFBA07] deals with the challenges encountered when applying anonymity to a VANET and proposes a framework for pseudonymity support. A study of the impact of pseudonym changes on geographic routing in VANETs is made in [SKL+06]. All of these papers underline that supporting pseudonymity also requires changing all others *identifiers* of the protocol stack, such as IP or MAC addresses.

We believe that deploying base stations along the road is a limitation for a quick development of the vehicular ad hoc network. Most related works based on a set of keys or pseudonyms do neither discuss the overhead induced on the certificate authority nor the scalability problem induced by the huge number of needed certificates.

B. The Trusted Platform Module (TPM)

A TPM [TCG05] is a hardware module designed for secure computing and that can be integrated into many devices. TPM are now shipped with PCs; 200 million TPM-enabled PCs have been shipped by the end of 2007. A TPM requires a software infrastructure that is able to protect and store data in shielded locations. It also has cryptographic capabilities. Figure 3, taken from [TCG05], illustrates the main components of a TPM.

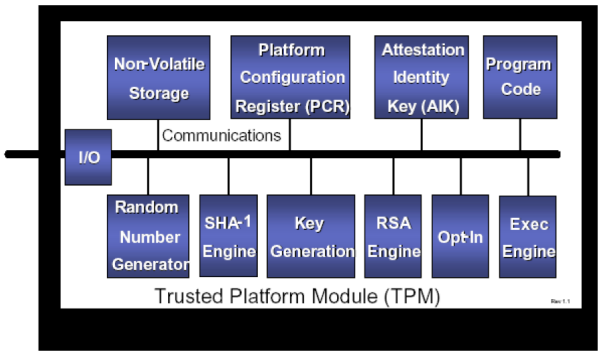

Fig. 3. Architecture of a TPM

Several keys are used by a TPM for authentication purpose and for attesting that the TPM is operating correctly. In our solution, we use essentially:

- The Endorsement Key EK: RSA key pair with a minimum size of 2048 bits. It is generated by the TPM manufacturer, is unique per TPM and is securely stored inside the TPM. The public part is available in the Endorsement Certificate.
- The Attestation Identity Keys AiK: RSA key pairs generated by the TPM. The public part is certified by a Trusted Third Party called a Privacy Certification Authority (PCA). One advantage is that AiK does not disclose the identity of the TPM.

III. An architecture to provide security and anonymity for inter-vehicular communication

The proposed solution is based on several cryptographic key pairs pre-loaded in the vehicle during the construction phase. These key pairs are used by a dedicated protocol for building cryptographic pseudonyms. Also a memory stick can be used to renew the key pairs in an opportunistic manner. The major design constraints of our solution are:

- to provide anonymity of the inter-vehicular communication and particularly to avoid the use of the same cryptographic pseudonym during a long period of time,
- to provide an authorized administrative entity the possibility to revoke the anonymity of a given message,
- to use native TPM security mechanisms,
- to keep the possibility to downgrade to standard operation if an entity does not operate correctly.

The proposed solution is based on several physical elements:

- a TPM and a memory embedded in the vehicle,
- a memory stick held by the driver and used to renew the cryptographic keys,
- an on-line server for the PCA.

The solution involves several entities:

- the vehicle manufacturers that performs bootstrap operations,
- the driver and mechanic that can make updates,
- the administration that manage the vehicle lifecycle like sale, resale, destruction,
- the PCA.

In the Section III-A, we show how the native attestation protocol [TCG05] can be adapted to sign messages sent by the vehicles. In the Section III-B, we present a typical example of inter-vehicle communication [GB08]. In the Section III-C, we describe interactions between the TPM, the memory stick and the PCA.

A. Using a TPM for anonymous attestation

The TPM provides two modes for anonymous attestation: PCA based or DAA based (for *Direct Anonymous Attestation* [BCC04]). We use the PCA mode mainly because an authorized trusted entity may revoke the anonymity as shown in section III-D and for scalability purposes as shown in section IV-C. A solution based on DAA might be possible but this would require a dedicated study and certainly an adaptation because it is stated in the abstract of [BCC04]:

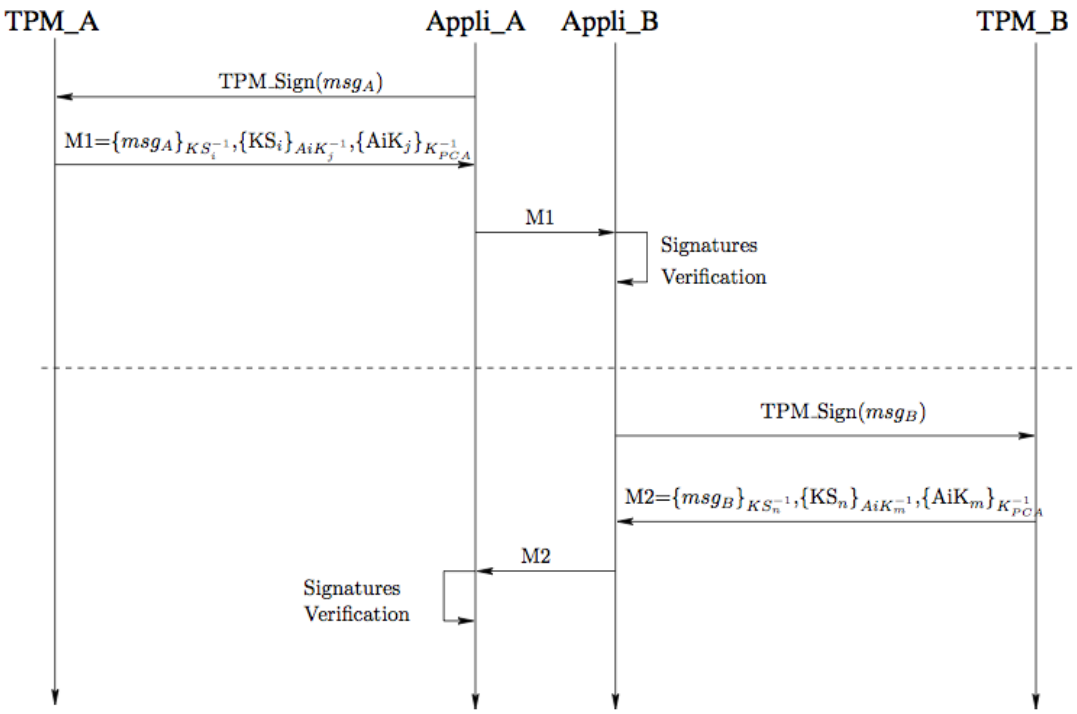

Fig. 4. Inter-vehicle communication using signed messages. The TPM is used only to sign, not to verify messages.

DAA can be seen as a group signature without the feature that a signature can be opened, i.e., the anonymity is not revocable.

We have also to face some TPM usage constraints. In TPM specification it is stated that the Attestation Identity Key AiK can not be used to sign arbitrary data. This is to avoid weakening an AiK by providing a lot of data signed by it and hence material for cryptanalysis. We must not forget that an AiK is used for identity attestation.

There is a known technique to overcome this problem [KS07]. As an AiK is authorized to sign the data and keys generated by the TPM, the TPM generates a new key called *Key Signing*, and then certifies it with an AiK. This creates a certifying chain that authenticates the Key Signing.

One negative side effect is that AiK or *Key Signing* may represent vehicle identifiers. Thus, to respect our anonymity constraint, it is important to change the AiK and *Key Signing* frequently.

In the following, $\{x\}_K$ denotes x encrypted by K and $\{x\}_{K^{-1}}$ denotes x signed by K^{-1}.

B. Inter-vehicular communication

The Figure 4 shows inter-vehicle communications using our solution. When the vehicle A wants to send a message msg_A to the vehicle B, the application running on A inserts the current date and time into the message, and then sends a query `TPM_Sign(msg`$_A$`.date)` to the TPM of A. The TPM of A returns the signed message: $\{msg_A.date\}_{KS_i^{-1}}$, together with the certificates needed for verification: $\{KS_i\}_{AiK_j{}^{-1}}, \{AiK_j\}_{K_{PCA}^{-1}}$.

The application running on A sends both the signed message and the cryptographic material to B. Note that data can be broadcasted. On receipt, the application running on the vehicle B verifies the certificates and signatures. The only public key that B has to know is the public key of the PCA. We can note here that the TPM of the vehicle B is not solicited to verify signatures.

The application can also check the date and time of the message and compare it to the current date and time of its vehicle. This optional check can easily eliminate some trivial replay attack cases, such as when the received date is clearly inferior to the current date.

To provide a good quality of anonymity, it is necessary to periodically change the *Key Signing* used and therefore by extension the AiK used. This prevents the possibility of car tracking. Therefore, we should ensure that the TPM owns a sufficient number of AiK. The quantitative aspects are discussed in IV-C.

C. Interaction between the TPM and the PCA

During a communication, the TPM uses one of its AiK chosen in a finite set of certified AiK.

This AiK will certify the key used to sign the message. For better anonymity the AiK used should not be traceable. It must be changed frequently.

Nevertheless, the set of certified AiK available is not infinite, it should be renewed.

Interactions with the PCA described on the figure 5 allows the certified AiK renewal. This appears :

- when a new vehicle is built, the manufacturer inserts new signed AiK in the memory embedded in the

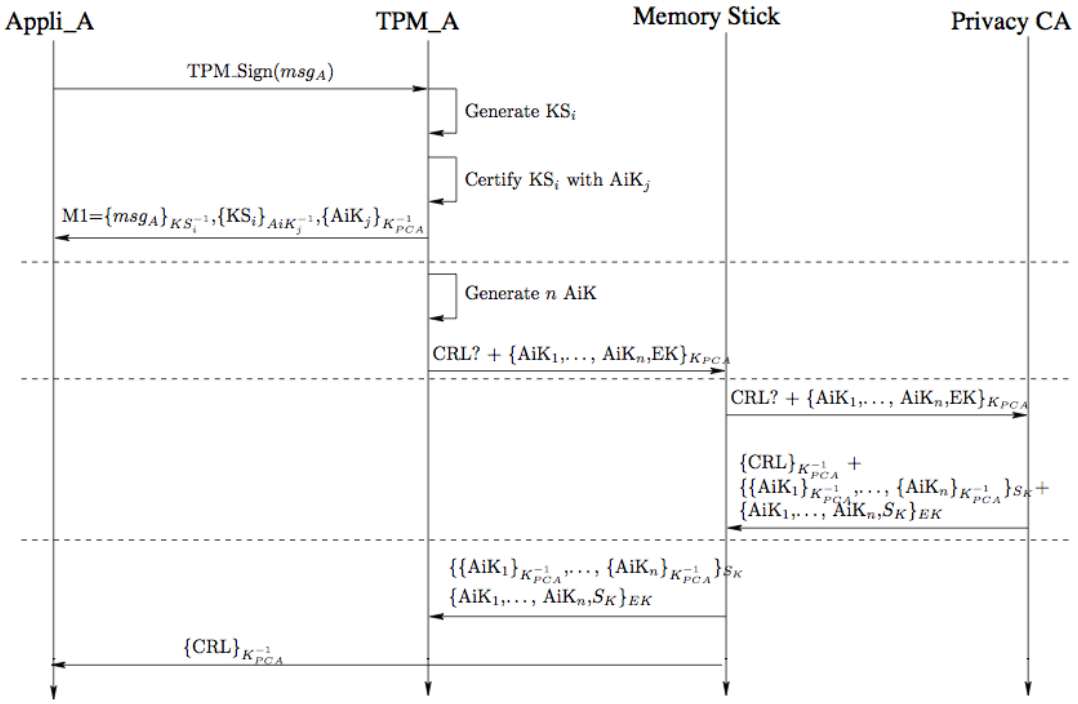

Fig. 5. Interactions between the elements of our architecture. Data in the memory stick are either public data like a CRL or encrypted data like AiK.

vehicle.

- during the lifecycle of the vehicle new certified AiK can be requested.
- when the vehicle is sold, the standard command `TPM_OwnerClear` clears the existing AiK and launch a query to obtain new AiK.

The memory stick is used by the driver to carry the AiK certification requests between the vehicle and any Internet connected device. Then the AiK certification requests is transmitted to the online PCA. It is also used to carry the signed AiK and the revocation list back to the vehicle.

If the driver never uses the memory stick, then the AiK are never renewed. Only the preloaded AiK contribute to the anonymity. In this case, the system behaves at worst as a standard communication system and the quality of the anonymity may decrease with time.

When a vehicle is on the road, its TPM uses its Key Signing to sign messages sent to other vehicles. When a Key Signing has been used during a certain distance or time or has signed a given number of messages, the TPM uses another Key Signing. When the number of available Key Signing reaches a given threshold the TPM creates a certifying request for new AiK. The EK certificate is added at the end of the AiK set. This request is encrypted with the PCA public key and then stored in the memory stick.

When the memory stick will be connected to the Internet, the request will be forwarded to the PCA. Then, the PCA will verify the request and the EK certificate and certifies the AiK. The PCA will also keep in memory a link between the AiK it has just certified and the EK. This link is needed when the authorized authority has to revoke the anonymity of a message.

The response of the PCA containing the certified AiK is encrypted with a session key S_K chosen by the PCA. Then the set of AiK is concatenated to the session key and encrypted by the EK previously received and added to the response. Finally the response is stored in the memory stick.

This particular use of the session key and the EK is needed to respect the TPM specification. Hence the TPM will give the session key to the application if it has successfully verified that the received AiK are the correct ones. The session key is encrypted with the public part of the EK. Thus, only the TPM with the corresponding private part can retrieve the session key and eventually decrypt the certified AiK.

D. Anonymity revocation

Adding anonymity in the inter-vehicle communications must not prevent the authorities to catch the attacker in given situations. This is important for the deployment of a realistic solution. We believe in particular that a solution without a trap will not be accepted in the automotive world when the driver engages its liability. We can underline that current registration systems offer exactly this type of feature. The registration provides anonymity for everyone and only one entity can associate the license plate number with the identity of the driver.

We introduce an additional parameter noted α in the certificate of an AiK. This setting allows an authority who knows the secret K_{auth}^{-1}, to retrieve the information j related to the vehicle. This information is the number of the vehicle in a database or its registration number. Thus, the certificate

of the i^{th} AiK provided by the PCA has the form:

$$\{AiK, \alpha\}_{K_{PCA}^{-1}} \text{ with } \alpha = \{j, i\}_{K_{auth}}$$

Several points are important with α:

- The i parameter increases the possible values of α thus an observer cannot say if two values α and α' are owned by the same vehicle j.
- The key K_{auth} used to create α is not public; only the entity authorized to create the α knows this key, in our case this is the PCA.
- The key K_{auth}^{-1} needed to revoke anonymity is not a public one; only the trusted third party must know this key; this is not necessarily the PCA.

E. Key revocation

Two types of keys can be revoked in our model, AiK and EK.

When the PCA is informed of a compromised AiK it simply updates the revocation list accordingly. We use an opportunistic revocation mechanism: the vehicle request and obtains the revocation list via the memory stick.

When the PCA is informed of a compromised EK, this means that the primary function of the corresponding TPM is no longer fulfilled. In this case the PCA revokes all the AiK associated with the EK. The PCA places the EK in the revocation list and keep the information locally in order not to certify further AiK for this TPM.

Note that it would be more difficult to revoke the *Key Signing* because the PCA has no knowledge of these keys. However it is not necessary to directly revoke a compromised *Key Signing*, it is sufficient to revoke the AiK that signed it.

If the driver never uses the memory stick, then the revocation list is never provided to the vehicle. Thus, the vehicle may unnecessary verify some messages crafted with revoked keys.

IV. Security analysis

In this section we discuss the security of our solution against an attacker that can read, write or intercept messages. In particular, the attacker can manipulate the inter-vehicle communications, intra-vehicle communications between the TPM and its application, communications with the memory stick and Internet communications.

A. Protocol modelization

We used the tools AVISPA [ABB+05] and SPAN [SPA] to prove two properties of our protocol:

1) the session key shared by the PCA and the TPM remains secret,
2) the AiK exchanged between the PCA and the TPM through the memory stick remains secret, until their first use in an inter-vehicular message.

Note that property 2 is not mandatory for the security of the overall protocol. Nevertheless, property 2 allows using the memory stick without any security assumption: the memory stick can be lost, copied, or modified without any other consequences on the protocol that a loss of data. The stolen data remains not understandable and useless for the attacker.

An output of the SPAN tool is presented on Figure 6 and the HLPSL code is provided online at `www.irisa.fr/celtique/Olivier-Heen/IEEEVNC-Annex.hlpsl`. The part of AVISPA that is used for our verification is proven complete. This means that when the protocol is found safe according to the security goals, then it is safe for an unbounded number of sessions.

The steps 1 to 4 are a query for AiK certification. The steps 5 to 7 are the answer of the PCA. The steps 8 to 11 are a typical message signature request and message signature. Note that the step 9 is not mandatory for the good execution of the protocol, although it is not false either. This is just one possible execution step, as selected by the simulator which does not necessarily choose the shortest possible session.

B. Anonymity revocation analysis

With the solution proposed in III-D, an authorized entity can revoke the anonymity of a particular message. Indeed, a message produced by one AiK is as follows:

$$\{msg\}_{KS^{-1}}, \{KS\}_{AiK^{-1}}, \{AiK, \alpha\}_{K_{PCA}^{-1}}$$

Any entity receiving such a message can easily find α. But only the entity that owns K_{auth}^{-1} can find the parameter j by deciphering $\alpha = \{j, i\}_{K_{auth}}$.

A collaboration is required between the entity that found j and the PCA to bind j to the identity of the vehicle's owner. This collaboration is essential to prevent a single compromised authority from revoking the anonymity. So, it requires a corruption of the two authorities for breaking the anonymity in an unauthorized manner and for retrieving the identity of a particular TPM owner. Indeed, the PCA can only bind an AiK to an EK, and the authorized entity can only bind an EK and thus a TPM to the identity of its owner.

C. Quantitative aspects

The quality of anonymity clearly increases with the number of certified AiK in the TPM. A direct approach would be to use an AiK for a short period of time or a short distance, and then removed it immediately.

For example, if a vehicle uses the same AiK along 500 meters, and if this vehicle travels 25,000 km per year, then 50,000 certified AiK per year are needed. In other words, for this vehicle, the TPM should generate 50,000 AiK that the PCA must certify.

A quick estimation shows that this approach is not well suited compared to certification time. Indeed, based on 2 million of new vehicles per year in France, the PCA should be able to certify $6.10^9 AiK$ per month. This exceeds the current rate of the certification authority, in the order of 2.10^6 from IBM source [BGA+07] of estimated signature time with dedicated hardware.

It is therefore necessary to reuse AiK to get a realistic trade-off between certification time and anonymity. With

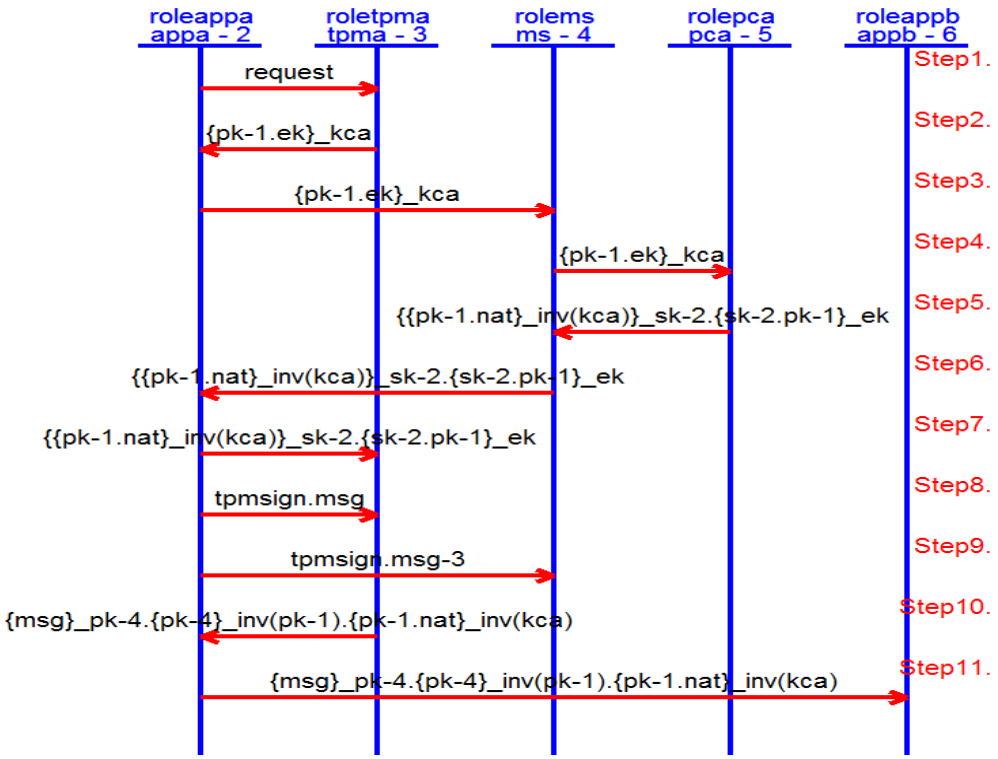

Fig. 6. A SPAN execution diagram of our protocol. The full specification is available at `www.irisa.fr/celtique/Olivier-Heen/IEEEVNC-Annex.hlpsl`

2 million vehicles a year in France and a rate of around 2.10^6 certified AiK produced the trade-off is around a few thousands of certified AiK by new vehicle. This set of AiK can then be completed by our protocol using the memory stick. Thus, adding around 100 AiK per vehicle per month, we have a low overhead on the PCA while allowing the partial renewal of AiK. Compared to the time of certification, the size of the AiK set is not a problem: the size of a single AiK is the size of a 2048 bits key pair. The current flash memories, with gigabytes at low cost, offer more space than necessary.

D. Incentive applications

The quality of the anonymity can be improved by a renewal of the AiK in a vehicle. Our solution is designed so that the AiK can be renewed without any security assumption on the communication channel. According to the available technologies, the renewal can rank from:

1) no renewal, if the driver ignores this possibility.
2) opportunistic renewal using a memory stick.
3) regular renewal using a GSM, is the driver is willing to pay for it.
4) continuous renewal, if many base stations are available.

The second possibility is a good compromise until many base stations are deployed. There are many incentives for encouraging the driver to use the memory stick. For instance collecting vehicle related data on the memory stick: fuel consumption, distance travelled and statistics on the driving behaviour, GPS updates, etc. Such data are useful in computer applications like statistics or driving improvement. Each time the driver connects its memory stick into a PC, this can be the opportunity obtain new certified AiK.

In addition, regular maintenance operations of the vehicle may also be the opportunity for a partial renewal of the AiK.

V. Conclusion

In this paper, we show a way to use a TPM component embedded in vehicles to improve security and anonymity of VANET communications. Nevertheless, this use is not a direct one. It requires special operations such as establishing opportunistic communication with the PCA, using short term keys to sign message, and adding a parameter to revoke anonymity if authorized. In our solution, the link with the PCA is enforced by a memory stick. This device requires the intervention of the driver and can be an obstacle to the deployment of the solution. We make no assumption about the security of the opportunistic link between the vehicle and the network. Hence, we can consider the use of any other link such as a 3G phone in the car that connects to the PCA *via* a GSM communication. One might also consider a wireless communication module in the vehicle starting key, and the appropriate module connected to the home PC. So when the key is in the vehicle, it communicates with the TPM and when it is close to the PC connected to the Internet, it communicates with the PCA.

Finally, it is possible that the DAA algorithm (*Direct Anonymous Attestation*) now integrated in the TPM could be adapted to the VANET context. This algorithm could be

well suited because it does not need a certification authority. On the other hand it complicates certain operation like the anonymity revocation. A dedicated study is necessary.

The authors are grateful to Thomas Genet and Nicolas Prigent for useful comments.

REFERENCES

[ABB+05] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santos Santiago, M. Turuani, L. Viganò, and L. Vigneron. The AVISPA Tool for the automated validation of internet security protocols and applications. In K. Etessami and S. Rajamani, editors, *17th International Conference on Computer Aided Verification, CAV'2005*, volume 3576 of *Lecture Notes in Computer Science*, pages 281–285, Edinburgh, Scotland, 2005. Springer.

[ABD+06] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller. Attacks on Inter-Vehicle Communication Systems - An Analysis. In *3rd International Workshop on Intelligent Transportation*, pages 189–194, 2006.

[BCC04] E. Brickell, J. Camenisch, and L. Chen. Direct Anonymous Attestation. In *ACM Conference on Computer and Communication Security (CCS)*, pages 132–145, 2004.

[BE04] J. Blum and A. Eskandarian. The Threat of Intelligent Collisions. *IT Professional*, 6(1):24–29, January-February 2004.

[BGA+07] P. Bari, M Gasparovic, H. Almeida, G. Detro, D. Druker, M. Gnirss, JF. Jiguet, and M. Raicher. *Security on z/VM*. IBM Redbooks, 2007.

[CG07] M. Conti and S. Giordano. Multihop ad hoc networking: The theory. *IEEE Communications Magazine*, 45(4):78–86, 2007.

[Döt05] F. Dötzer. Privacy Issues in Vehicular Ad Hoc Network. In *Workshop on Privacy Enhancing Technologies*, pages 197–209, 2005.

[FFBA07] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar. Support of Anonymity in VANETs - Putting Pseudonymity into Practice. In *IEEE Wireless Communications and Networking Conference*, pages 3402–3407, 2007.

[GB08] G. Guette and C. Bryce. Using TPMs to secure Vehicular Ad hoc Networks (VANETs). In *Workshop on Intormation Theory and Practices*, pages 106–116, 2008.

[GFL+07] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch. Security Architecture for Vehicular Communication. In *Workshop on Intelligent Transportation*, 2007.

[HvL04] JP. Hubaux, S. Čapkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security and Privacy*, 2(3):49–55, May-June 2004.

[KS07] N. Kuntze and A. U. Schmidt. Trusted Ticket Systems and Applications. In *IFIP sec: New Approaches for Security, Privacy and Trust in Complex Environments*, pages 49–60, 2007.

[PP05] B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. In *Fourth Workshop on Hot Topics in Networks*, 2005.

[RH05] M. Raya and JP. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21, 2005.

[RH07] M. Raya and JP. Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[RPH06] M. Raya, P. Papadimitratos, and JP. Hubaux. Securing Vehicular Communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, 13(5):8–15, 2006.

[SKL+06] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos. Impact of pseudonym changes on geographic routing in vanets. In *European Workshop on Security in Ad-hoc and Sensor Networks*, pages 43–57, 2006.

[SPA] A Security Protocol Animator for AVISPA (SPAN). `http://www.irisa.fr/lande/genet/span/`.

[TCG05] Trusted Computing Group. TPM Main Specification. Main Specification Version 1.2 rev. 85, Trusted Computing Group, February 2005.

[ZMTV02] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security Issues in a Future Vehicular Network. In *European Wireless*, pages 270–274, 2002.