# Authentication vs. Privacy within Vehicular Ad Hoc Networks

Mohamed Salah Bouassida

Laboratoire Heudiasyc UMR CNRS 6599 - Université de Technologie de Compiègne
BP 20529, 60205 Compiègne, France (Email: mbouassi at utc.fr)

*(Received Mar. 9, 2010; revised and accepted May 8, 2010)*

## Abstract

Security and protection of private user information are a prerequisite for the deployment of the vehicular network technologies. Nevertheless, the establishment of a secure communication architecture within vehicular ad hoc networks address special challenges, due to the characteristic and specificities of such environment (high dynamic and mobility of nodes, high rate of topology changes, high variability in nodes density and neighborhood, broadcast/geocast communication nature ...). Vehicular ad hoc networks (VANETs) are therefore target of several malicious attacks (internal or external), in addition to unintentional faults and errors. In this context, I present in this paper a novel security communication architecture dedicated to operate within VANETs, ensuring authentication of vehicles and revocation of intrusted ones while guarantying privacy of drivers identities. The safety and efficiency of my security architecture is validated through its formal verification using the security protocols verifier tool AVISPA (Automated Validation of Internet Security Protocols and Applications).

*Keywords: Authentication, privacy, threshold cryptography, vehicular networks*

## 1 Introduction

Vehicular ad hoc networks (VANETs) are a form of MANETs used for communication among vehicles and between vehicles and roadside equipments. In addition to the challenging characteristics of mobile ad hoc networks "MANETs" (lack of established infrastructure, wireless links, multi-hop broadcast communications, limited bandwidth ...), VANETs bring new challenges to achieve safe and secure communication architecture within such environment. Indeed, within VANET networks, nodes are characterized by high dynamic and mobility, in addition to the high rate of topology changes and density variability. Stibor *et al.* [2] evaluate the neighborhood nature of vehicular networks within a four highway lanes context (two lanes for each direction). They carried out simulations and analysis that show that the average number of potential communication neighbors is appreciatively four. In addition, in 50% of all occurrences, the maximum potential communication duration is 1 sec; in 90% of the occurrences, the upper boundary for the communication time is 5-sec.

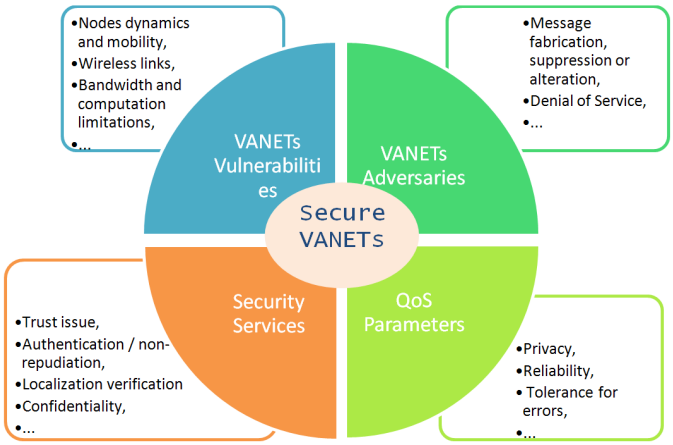


Figure 1: Securing VANETs context

VANETs are dynamic in both space and time. They offer a large flexibility. However, this flexibility associated to the vulnerability of wireless communications, require to secure data as well as the participating entities. Figure 1 summarizes the different issues to consider in order to secure communications within vehicular networks. The defenceless of VANETs due to their specificities and characteristics make them target to passive and active attacks. Passive attacks allow malicious non-authorized entities to access confidential data; whereas, active attacks can lead to the deletion or modification of messages, injection of new malicious messages, identities usurpation and consequently violation of the main security services, namely availability, integrity, authentication and non-repudiation. In addition, securing VANET communications is necessary, especially considering the high level of criticality of emergency exchanged messages. For example, from a safety perspective, a car that informs other drivers of its sudden deceleration can reduce a ten-

car pile-up to an accident, or prevent the accident entirely. The information conveyed over a vehicular network may thus affect life-or-death decisions, making fail-safe security a necessity [4] (there are 1.2 million people killed and as many as 50 million people injured in traffic accidents each year [10]).

In this context, I focus in this paper on the authentication and privacy issues. Therefore, I propose a novel security architecture within VANETs, based on three main actors (CAs: Certification Authorities, RSUs: Road Side Units [29] and OBUs: On-Board Units), which guarantees the authentication and non-repudiation of vehicles, while considering the privacy of the drivers identities, and the revocation of the malicious/untrusted participants.

To present my contributions, this paper is structured as follows. Section 2 presents the challenging issues in order to establish a secure communication architecture within VANETs. The related works in terms of security within VANETs are presented in Section 3. Section 4 describes my secure communication architecture within VANETs. In Section 5 I analyze and validate the safety of my proposal through its formal validation via the AVISPA tool. And finally, Section 6 concludes this paper and presents my future work.

## 2 Challenging Security Issues within VANETs

Considering the establishment of a secure communication architecture within vehicular ad hoc networks, several challenging issues are encountered, related to the inherent characteristics of such environment. I present hereafter these security vulnerabilities:

- The nodes dynamics and mobility. Each vehicle will have a constantly shifting set of neighbors, many of whom it has never interacted with before and is unlikely to interact with again: a specific driver is unlikely to receive multiples reports/messages from the same vehicle [4]. The high rate of topology changes is a consequence of the high dynamic of nodes, characterizing VANETs. In addition, the fast and unpredictable topology change induces a very sporadic connectivity between vehicles. Conceiving a security architecture within VANETs should take into consideration these factors.

- Wireless links. Links within VANETs are target of several malicious attacks (passive such as network sniffing or active such as messages alterations).

- Bandwidth limitation. The wireless channel can be occupied by competitive nodes for many reasons (collisions, interferences, insufficient signal strength, duration of the transmission sequence, ...).

- Trust issue. Due to the lack of fixed infrastructure within vehicular ad hoc networks, the availability of certification authorities is not guaranteed. Within such environments, the main problematic issue is to know which entities we can trust and which level of trust we can give them.

The security defenceless of vehicular ad hoc networks make them target of several malicious attacks. Authors of [4] suggest the following classes of adversaries, against the establishment of secure communications within VANETs:

- Greedy drivers: selfish drivers trying to maximize their gain by making believe a congested path to their destinations, and consequently suppress traffic by attacking the routing mechanisms. The Wormhole attack [19, 20] belongs to this category and is particularly difficult to detect and prevent. It consists of the fact that a malicious vehicle forwards the received packets to another attacker, through a private shared tunnel, by providing to the origin of a packet a best -but erroneous- route towards the destination, eliminating thus any possibility of reliable routes discovering in the network.

- Snoops: drivers attempting to profile drivers and extract their identifying information. Malicious Snoops can even track vehicle locations and determine the identities of drivers by corresponding them to the house or work sites.

- Pranksters: drivers trying to disable applications or prevent information from reaching others vehicles. Such attacks are denoted by Denial of service attacks (DoS).

- Malicious attackers: drivers deliberately attempting to make harm via the available applications within the network. Several attacks focus on damaging exchanged data between vehicles such as message fabrication, suppression or alteration. Sybil attack (Masquerade) [5]) belongs also to this category, and consists of the creation of multiple fake nodes broadcasting false information on the network.

- Industrial insiders: if vehicle manufacturers are responsible for securing communications within VANETs, employees can reveal confidential data to malicious entities.

## 3 Related Work

The last few years saw a research interest development on the vehicular communications technologies, focusing especially on the security and safety issues within this environment. I present in what follows existing secure communications protocols within VANETs; I summarize this state of the art in Figure 1.

- The proposal of Raya *et al.* [5], dealing with security within vehicular ad hoc networks, utilizes a public

Table 1: VANET security communications approaches (state of the art)

| Secure Communications Protocols | Functionalities | Drawbacks |
|---|---|---|
| Raya *et al.* [18] | PKI + Mobile authentication and anonymity + Data confidentiality | Large number of anonymous keys renewed by the CA |
| Wang *et al.* [23] | Based on [18] + Symmetric encryption to secure group communications for non-safety applications | Large number of anonymous keys renewed by the CA |
| Lin *et al.* [11] | RSU-aided Certification revocation + Conditional privacy preservation | Availability of TM and MM, two cryptographic encryptions for each message |
| Papadimitratos *et al.* [15, 10] | PKI + Secure communications + Privacy protection | Storage and communication overhead due to pseudonyms certification + constraining CRL broadcast process |
| Studer *el al.* [22] | Mobile authentication + Privacy (temporary anonymous certified keys) | Storage and communication overhead to update anonymous keys |

key infrastructure to ensure mobile authentication and anonymity. Each vehicle holds, via a tamper proof device, a public and private keys, in addition to others anonymous keys, certified by a specific authority (CA) and used to ensure the privacy of the initial identities. The CA can belong to the governmental transportation authorities, or simply to vehicles manufacturers. Authentication of emergency messages is ensured by signing them using private keys. Key revocation process is carried out by defining for each key a short certificate lifetime (to avoid revocation messages overhead). Hence, revealed keys could be used by malicious nodes until their expiry. Anonymous keys are renewed periodically by CAs. In addition, a vehicle should use them randomly (one key per minute) in order to face the tracking attack until discovering its identity (by associating the driver with its place of living). Because an already used key should not be re-used in the future, the number of keys become considerably large, which represents serious communication and storage overheads. In addition, the on-line availability of CAs is not ensured within vehicular networks.

Wang *et al.* propose in [11] a secure scheme for VANETs, by enhancing the proposal of Raya *et al.* [5] to be also suitable for non safety related applications (chat application for example). The basic idea of this contribution is to allow vehicles to communicate securely (ensuring the confidentiality of their exchanges) via a secret symmetric key, generated by Diffie-Hellman algorithm [30]. Communication security of a group of vehicles is also proposed, founded on a group leader responsible for the generation and the maintenance of the secret key.

Lin *et al.* address in [12] two security issues within VANETs, certificate revocation and conditional privacy preservation. A novel RSU-aided certificate revocation method (RCR) is presented, enhancing the revocation method presented in [5]. According to this method, if a certificate has been confirmed revoked by the CA, the RSU will broadcast a warning message such that all the approaching vehicles can update their lists of revoked members (CRLs). The privacy issue is based on the GSIS protocol [31], which stipulates the use of two management entities in the network: the tracing manager TM (law authority handling traffic disputes) and the membership manager MM (handling traffic regulation). Each vehicle receives from the MM a public group key (the same key destined to all vehicles) and a private one. Each sent message is signed using these two keys; the authentication of a received message using the public group key can ensure that the message was transmitted by a legal group member. In case of dispute, the misbehaving vehicle is traced, and its identity is revealed by the TM. Compared to the proposal in [5], this privacy scheme avoids constraining communication and storage overheads. However, the availability of the added entities is not addressed. In addition, the use of two cryptographic operations for signing each message is constraining within VANET, especially concerning safety or emergency notifications, which should be transmitted with the minimum delay.

- Papadimitratos *et al.* presented in [6, 7] a secure vehicular communication system, based also on a public key infrastructure. They address in their proposal identity and cryptographic key management, privacy protection and secure communications in the context of beacon exchanges, neighborhood discovery and geocast messages transmission. Each vehicle is registered with a unique long-term identity, a public and private keys and a certificate, provided by a CA. Cross certification technique is used in order to ensure authentication between vehicles registered by different CAs. Cryptographic secrets are stored within vehicles and RSUs (Road-Side Units) within a tamper-proof module, called HSM (Hardware Security Module): the cryptographic operations using secrets are carried out by this module, in order to ensure that sensitive information never leaves the physically secured equipment. Concerning anonymity, a pseudonymous authentication approach is used, described in [28]. According to this approach, each HSM generates a set of key pairs (public and private keys), and send the public keys to a CA to obtain their anonymous certificates (without identity information). Each vehicle uses at each period of time an anonymous key pair, and cannot use them after the expiry of this period. Anonymous pseudonyms refill and resolution processes are described in [6]. Note that the anonymous pseudonyms certification operations generate a storage and communication overheads, higher than generated by the proposal of Raya *et al.* [5]. Revocation of malicious nodes can be achieved via two methods. As a first solution, the CA sends securely a "Kill" message to the concerned HSM, which acknowledges the received message and deletes its memory (including all secret information it stored). If a CA does not receive an acknowledgment of a "Kill" message, it uses the second more constraining solution, which consists of broadcasting a compressed CRL (Certificate Revocation List). However, this broadcasting process is very constraining within VANETs and generates a large communication overhead.

- The authentication method presented by Studer *et al.* in [13] is based on Temporary Anonymous Certified Keys (TACKs), to ensure vehicles' privacy, while maintaining revocation of misbehaving participants. A trusted group manager, denoted by $M$, is responsible for distributing unique long-term keys to each vehicle (called group user key). $M$ maintains a history of all key/OBU pairs it has issued so that it can trace misbehaving vehicles. In addition, other trusted entities called Regional Authorities (RAs), are responsible for generating for each vehicle in their regions a TACK (public and private keys with short life-time). Nodes authenticate each other within the network using these keys. Each vehicle communicates securely with the current RA of its region (to ask for or update its TACK), by signing its sent messages with its group user key. By updating the TACKs frequently, this proposal ensures short-term linkability and long term unlinkability, in addition to the traceability and revocability of malicious nodes. However, a communication overhead is generated due to the message exchanges between RA and vehicles when updating TACKs. A storage overhead is also engendered ($M$ and RA store all the generated TACKS and manage the RL).

  In order to face DoS attacks, the same authors Studer *et al.* propose in [14], an authentication scheme based on an optimized version of the TESLA protocol [27]. However, the privacy of vehicles is not ensured in this proposal.

### 3.1 Summary

Several research works were interested in the security issue within vehicular ad hoc networks. Some works focus on secure network layer such as establishing safe routing mechanisms ([9]). Other works were interested in ensuring exchanged data correctness ([10, 18]), or localization verification ([16, 17, 8]). But the majority of existing proposals concentrates on applicative layers, to ensure basically secure exchanged data between vehicles. The most important security functionalities are ensured within existing architectures dedicated for VANETs (authentication, confidentiality, privacy ...). However, high overheads of storage and communication are more or less generated, in addition to the exclusive use of the certification authorities to generate the security keys and pseudonyms to all vehicles in the network; which make the existing approaches likely difficult to apply within real VANET environments.

I present in the next section my novel security architecture within vehicular ad hoc networks, aiming to resolve the drawbacks described above, while ensuring the authentication and the privacy of the participating vehicles.

## 4 Secure Communication Architecture within VANETs

To present my contributions, I start by giving an overview of my novel security architecture objectives in terms of authentication and privacy. Then, I identify the main actors of this architecture. And finally, I detail the different functionalities of my security architecture.

### 4.1 Security Architecture Objectives

From one hand, each driver should be bounded to a single identity, in order to prevent Sybil or other spoofing attacks [4]. The authentication service allows entities within VANETs to prove their identities towards nodes communicating with them; whereas the non-repudiation service

ensures that an entity transmitting a message in the network cannot deny sending it. When an entity is detected malicious within the network, its revocation should be immediately carried out, by deactivating its tamper-proof security device TP-DS, in the charge of the corresponding CA and the RSUs.

In the other hand, the privacy of drivers against unauthorized or malicious attackers observers should be guaranteed [5]. Indeed, the identity of the source of a transmitted message should not be revealed. In addition, if drivers uses pseudonyms when they communicate within VANETs, malicious nodes should not be able to trace their trajectories, by associating vehicles to driver's houses or work offices (long-term unlinkability). However, vehicles need to reveal their identities to some other entities in the network in order to prove their authorization to access defined groups (short-term linkability). Additionally, certification authorities should be able to extract message source identities in order to revoke malicious and untrusted entities.

The privacy concept of drivers identities is opposite to the authentication and the non-repudiation security services. The challenging issue is therefore to find the best tradeoff between these concepts.

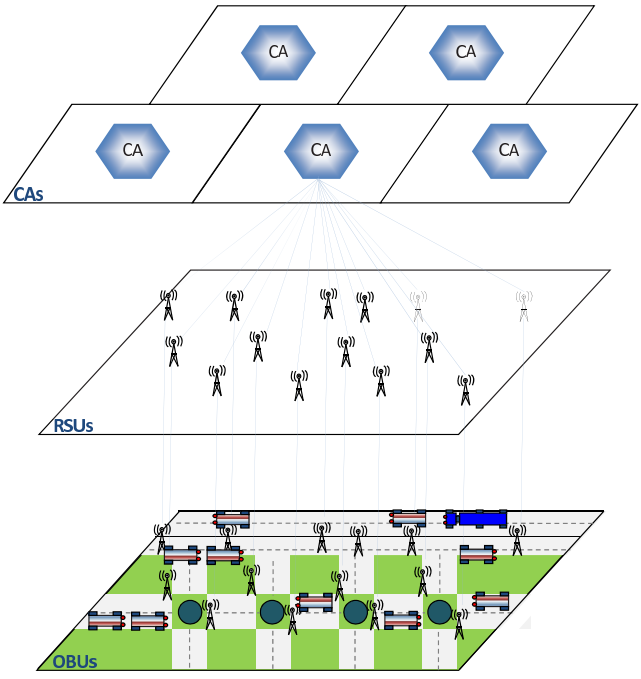


Figure 2: Security schema within VANET

## 4.2 Security Architecture Actors

The principle idea of my security architecture within vehicular ad hoc networks is to allow vehicles and infrastructure equipments to communicate (V2V and V2I) in a secure and anonymous manner, dealing with the characteristics and vulnerabilities of such environment, while facing eventual malicious attacks. Three types of actors are considered by my security architecture within VANETs (cf. Figure 2):

- **Certification Authorities (CAs):**

  These entities represent the trust establishments. They are responsible for providing for each vehicle and RSU a personal certificate, off-line, allowing it to prove its identity when communicating with other participants. A CA is also in charge of revoking certificates of untrusted and malicious nodes. It is responsible for establishing the security requirements within its region. Moreover, CAs cooperate to ensure inter-regions security (when vehicles move between regions managed by different CAs).

- **RSU (Road Side Units):**

  The RSU entities participate to the security architecture of the vehicular ad hoc network; they are delegated by the corresponding CA to carry out some security functionalities as detailed in Section 4.3.3. Within rural environments (where the number of available RSUs may be insufficient), I propose an adaptation of my security architecture in Section 4.3.6.

- **Vehicles or OBUs (On-Board Units):**

  There exist different types of vehicles within VANETs (e.g. police car, firemen vehicle, personal car, official car . . . ); the type of a vehicle defines precisely which applications and exchanged information the vehicle is authorized to access. In addition, I assume that each vehicle is equipped with a Tamper-Proof Security-Device (that I denote by TP-SD). The TP-SD is a physically secure equipment, responsible for ensuring the confidentiality of the sensitive and personal information of the ego vehicle, such as its private key, and to execute all the cryptographic operations that the vehicle needs to operate, in order to participate to the secure vehicular network. The physical damage of the TP-SD implies an immediate destruction of all the information stored on it.

## 4.3 Security Approach Description

After having defined the framework of my security architecture within VANET, its actors and objectives, I detail in this subsection the different functionalities of my architecture in the following order: vehicles' certification, pseudo certification delegation to the RSUs, privacy of the drivers' identities, securing inter-vehicular communications, de-anonymity and revocation procedures and finally the adaptation of my security architecture within rural environments.

### 4.3.1 Vehicles' Certification

The certification authority is responsible for generating and providing for each vehicle a certificate (Cert), com-

posed of the following parameters (cf. Figure 3).

| Certificate Composition |
| --- |
| $Identity\_Holder$, $Pub\_Key\_Holder$, $Type\_Holder$, $Life\_Time$, $Id\_CA$, $Signature\_CA$ |

Figure 3: Vehicle certificate composition

1) Identity_Holder: unique identity of the vehicle (physical address + random nonce for example) and identity of the vehicle's owner;
2) Pub_Key_Holder: public key of the vehicle;
3) Type_Holder: type of the vehicle (professional, police, personal ...);
4) Life_Time: duration of the certificate's validity;
5) Id_CA: identifier of the certification authority;
6) Signature_CA: signature of the certificate, generated by encryption with the private key of the CA.

In addition, the CA affords for each vehicle (in a secure off-line manner) the private key Priv_Key_Holder, corresponding to its public key Pub_Key_Holder. Each vehicle in the network can thus prove its identity, certified by the trusted authority CA.

#### 4.3.2 Pseudo Certification Delegation to the RSUs

Within an ad hoc network, having only one certification authority of a PKI (Public Key Infrastructure) represents a security defenceless. Indeed, its availability is not ensured during secure communications between nodes. The threshold cryptography [21, 22] proposes a more flexible and efficient approach: the new key management service having the configuration (n,t+1) consists of n special nodes, called servers or MOCAs (Mobile Certificate Authorities), available in the ad hoc network, and sharing the ability to generate certificates for the others nodes. The private key $k$ of all the certification service is divided into n shared secrets ($s1$, $s2$ ... $sn$); one secret being known by only one server. Figure 4 illustrates this configuration. t+1 valid partial signatures are required to construct a valid complete one.

Each server generates a partial signature of a node's certificate, and sends it to the concerned node, which needs at least $t+1$ partial signatures to generate its complete one.

The maximal number of compromised servers at any period of time must be equal to t: with t compromised servers, each entity is still able to generate a valid signature. Zhou *et al.* make the assumption that ($n >= 3t + 1$) [21]. Each node is also able to verify the validity of a partial signature (PS) sent by a server. A PS is rejected if it is revealed erroneous. The choice issue of

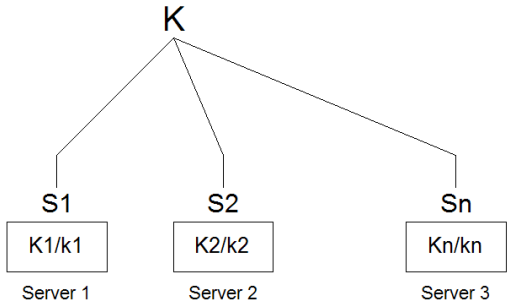


Figure 4: Threshold cryptography concept

the parameter $t$ is detailed in [22]. The higher the parameter $t$, the higher the security level against eventual malicious attacks. However, a high value of $t$ increases the communication overhead.

In the context of my security architecture within VANETs, in order to ensure the privacy of their identities, communicating vehicles do not use their certificates (containing their real identities), nor their public and private keys. They exploit for this purpose temporary pseudonyms certificates, that I denote by Pseudo_Cert. For the generation of the Pseudo_Cert to all the vehicles, I take advantage of the threshold cryptography technique, in the following manner: the concept of threshold cryptography is used to share the private secret of the CA between RSUs; a defined number of these new trusted entities can therefore cooperate to produce for each vehicle a Pseudo_Cert, allowing it to communicate securely without revealing its identity.

Let's consider a $(n, t+1)$ configuration of the threshold cryptography technique; $n$ represent all the RSUs located in the region of the corresponding CA, and $t + 1$ represent the minimum number of RSUs required to produce a pseudonym certificate for an applicant vehicle. Note that any group of $t+1$ RSUs are able to produce a pseudonym certificate. Figure 5 illustrates the generation process of Pseudo_Certs; in the illustrated example, $t$ is equal to 2.

#### 4.3.3 Privacy of the Drivers Identities

Before applying for a pseudonym certificate Pseudo_Cert, each vehicle generates a pair of keys (public denoted by Pseudo_Pub_Key and private noted Pseudo_Priv_Key). The Pseudo_Cert generated by the group of $t + 1$ RSUs, corresponding to a Pseudonym key pair, is composed as shown in Figure 6.

To obtain a $\frac{1}{t+1}$ part of its pseudonym certificate, a vehicle communicates securely with a RSU. I present in Figure 7 this communication exchange (a message M encrypted with a key k is denoted by $\{M\}k$).

Two parameters characterize the pseudonym certification process, the choice of their values should be carried out by real tests and measurements, and adaptable to the VANET environment (considering the density of RSUs on roads):

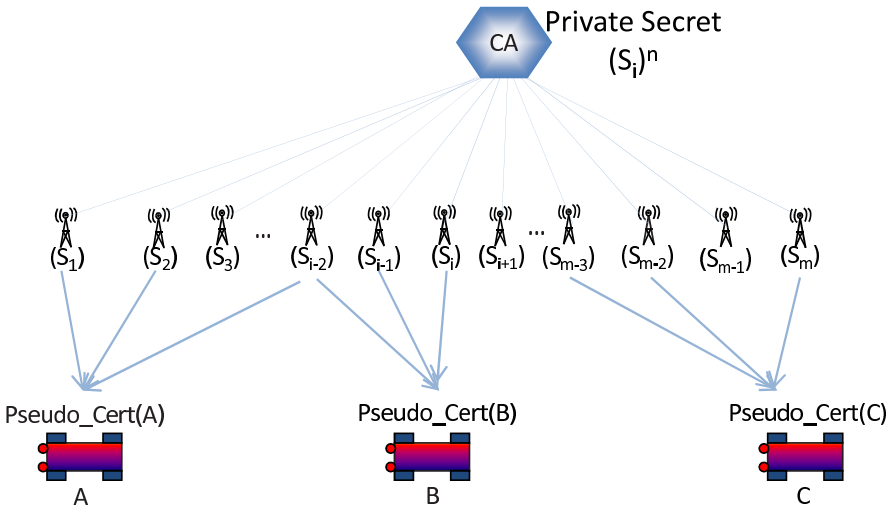


Figure 5: Pseudonyms generation by RSUs

| **Pseudo Certificate Composition** |
|---|
| $Pseudo\_Pub\_Key\_Holder$, $Type\_Holder$, $Life\_Time$, $Id\_CA$, $Signature\_CA$ |

Figure 6: Vehicle pseudo certificate composition

| **Pseudo – Cert Generation Procedure** |
|---|
| $vehicle\ v \longrightarrow RSU$ : **(Certif_Request)** $\{Cert_v, old\_Pseudo\_Cert_v, Seq\_Num\}Pub\_key_{RSU}$<br><br>$RSU \longrightarrow vehicle\ v$ : **(Certif_Answer)** $\{Part\_Pseudo\_Cert_v\}Pseudo\_Pub\_key_v$, $\{Seq\_Num\}Priv\_Key_{RSU}$ |
| $vehcile\ v$ : $Combination\ of\ t+1\ received\ Part\_Pseudo\_Cert$ and generation of $Pseudo\_Cert_v$ |

Figure 7: Pseudo certificate generation procedure

- The minimum number $(t + 1)$ of RSUs, acting as servers, required for the generation of a Pseudo_Cert. A high value of $t$ enhances the security level of the certificate generation process (a maximum of $t$ compromised RSUs cannot compromise the VANET security), but generates a higher communication overhead.
- The duration of a Pseudo_Cert: a vehicle should update its pseudonym certificate each fixed period of time. A life time of five to ten minutes for each pseudonym is acceptable to ensure a high level of privacy, without generating a constraining communication overhead.

To allow vehicles to communicate securely since they join a vehicular network (at the bootstrap), the CA may provide for each vehicle, in addition to its certificate, its first pseudonym certificate (associated with a pseudonym key pair). During a secure communication session, each vehicle can prepare in advance its "next" pseudonym certificate. The number of prepared Pseudo_Certs is fixed to one, to consider de-anonymity and revocation issues, treated below.

**Advantages**

1) Privacy is ensured because vehicles will never use their identities when communicate with other nodes. A RSU does not hold the conversion Cert $\leftrightarrow$ Pseudo_Cert. A RSU knows which vehicles communicate with it, to obtain pseudonym certificates, but cannot know actor identities of inter-vehicular communications.

2) No regular communication between vehicles and CAs are required, vehicles communicate regularly with

RSUs in a secure manner. The availability of certification authorities issue is thus resolved. Moreover, the tolerance for errors is also guaranteed in the phase of pseudonym certificates generation.

3) A vehicle belonging to a certification region, managed by a CA, can obtain Pseudo_Certs from RSUs belonging to other certification regions with different CAs (cross authentication mechanism is possible with the assumption that RSUs can acquire the identities of others CAs).

4) In case of detection of malicious entities, identities of untrusted vehicles can be revealed (cf. Section 4.3.5).

#### 4.3.4 Security of Exchanged Communications

To address the authentication issue of the exchanged messages between vehicles, the appropriate cryptographic mechanisms should be chosen. To ensure data confidentiality and nodes authentication, symmetric cryptographic mechanisms induce less overhead per sent message than asymmetric techniques. However, asymmetric operations are most suitable for vehicular safety applications [5]. Indeed, safety messages are typically stand alone and should be sent as fast as possible, without a key agreement phase, required for symmetric authentication techniques. The non repudiation service is additionally guaranteed with this type of cryptographic operations. Therefore, the digital signature operation is chosen for authentication and non repudiation services. I present in Figure 8 the format of a message broadcasted by a vehicle $A$, and the security operations carried out at the side of its neighbors.

| **Message Exchange between Vehicles** |
|---|
| $vehicle\ A \longrightarrow \forall Neighbors\ v:\ Pseudo\_Cert_A,$ $DATA = (Message\_Content, Seq\_Num),$ $\{Hash(DATA)\}Pseudo\_Priv\_key_A$ |
| $Neighbor\ v: Authentication\ of\ Pseudo\_Cert_A$ $and\ the\ signature\ of\ DATA$ |

Figure 8: Secure communication between vehicles

The authentication of the pseudonym certificate of $A$ by the neighbor vehicle $v$ implies that node $v$ knows the identity of the CA which created the certificate of node $A$. Otherwise, if the two entities belong to different certification regions, a cross authentication mechanism is needed (vehicles can ask RSUs for the identity of other certification authorities, to be able to authenticate messages sent by vehicles certified in other regions).

#### 4.3.5 De-Anonymity and Revocation

A vehicle whose behavior is detected untrusted is labelled malicious. The RSUs are responsible for this task: investigate suspect behaviors and inform CA to decide the revocation of the malicious entities.

Because vehicles do not reveal their real identities when communicating within VANETs (by using Pseudo_Certs), a de-anonymity phase is required before each revocation procedure. Hence, this phase consists of associating to an untrusted pseudonym certificate (Untrusted_Pseudo_Cert) its real certificate (Untrusted_Cert). The de-anonymity operation requires the cooperation of all the RSUs of the certification region, in the following manner: the RSU which affects the malicious label to a Pseudo_Cert will send this certificate to the other RSUs of its group (RSU_Group). Before the expiry of Untrusted_Pseudo_Cert (with short lifetime), the concerned vehicle will try to obtain a new Pseudo_Cert, and thus will include in its pseudonym certificate request the Untrusted_Pseudo_Cert, in addition to its identity Untrusted_Cert. The RSU receiving this request will thus know which certificate is corresponding to the untrusted pseudonym and inform CA to decide the revocation.

The revocation operation at the side of the CA consists of the transmission of a secure "Kill" command to the tamper proof security device of the malicious node, encrypted with the private key of the CA. At the automatic destroying of the TP-SD of the untrusted vehicle, an acknowledgement message is sent to the CA. In case of fail of this operation, the CA broadcast the Kill command to its RSUs, and in a final step to other CAs (which will reiterate the revocation procedure in their respective certification regions). A revocation list (RL) containing the certificates of the banished vehicles is maintained by CAs and RSUs. This list is constructed and updated locally by each actor, at the reception of a Kill command of a vehicle. At the reception of the revocation acknowledgment message relating to a vehicle M, the CA inform the RSUs of its region and the other CAs (if they were notified concerning the revocation of M) about this reception, in order to update their local revocation lists.

I summarize in Figure 9 the message exchanges between VANET actors to revoke a malicious vehicle M.

**Detection of a malicious Pseudo_Cert:** As presented above, the operation of detection of a malicious Pseudo Certificate can represent a vulnerable point of security. Indeed, if a single RSU can be responsible for the detection of a malicious vehicle in the network, a malicious RSU (untrusted) can blacklist all vehicles communicating with it. The detection of an untrusted vehicle in the network by more than one RSU ($\geq 2$) can thus resolve this problem. Reputation mechanisms can also be used at the side of the CA to affect to each RSU in its domain a reputation level, and thus be able to detect and revoke malicious RSUs.

#### 4.3.6 Security Architecture within Rural Environments

Within rural environment, the density of RSUs may decrease, making difficult the establishment of a security architecture based on these entities. In addition, the on-

| **Revocation Procedure** |
|---|
| $RSU_i$ : *Detection of a malicious* $Pseudo\_Cert_M$<br>$RSU_i \longrightarrow RSU\_Group$ :<br>$\{Pseudo\_Cert_M, Seq\_Num\}TEK\_RSU$<br><br>$Vehicle\ M \longrightarrow RSU_j$ : **(Certif_Request)**$\{Cert_M$,<br>$Pseudo\_Cert_M, Seq\_Num\}Pseudo\_Priv\_key_M$<br><br>$RSU_j \longrightarrow CA$ :<br>$\{Cert_M, Seq\_Num\}Priv\_Key\_RSU_j$<br><br>$CA \longrightarrow M$ : **Kill Command**<br>$\{Cert_M\}Priv\_Key_{CA}$ |
| *IF M not yet revoked*<br>$CA \longrightarrow RSU\_Group$ : **Kill Command**<br>$\{Cert_M\}Priv\_Key_{CA}$<br>$RSU\_Group \longrightarrow M$ : **Kill Command**<br>$\{Cert_M\}Priv\_Key_{CA}$ |
| *IF M not yet revoked*<br>$CA \longrightarrow \forall CAs$ : **Kill Command**<br>$\{Cert_M\}Priv\_Key_{CA}$ |

Figure 9: Revocation procedure

line availability of the certification authority CA is not guaranteed. To address this challenge, let's consider the possibility to affect to special vehicles the role of server nodes (sharing the CA private secret), in addition to the available RSUs. These vehicles (police car for example) should have enhanced characteristics in term of physical security and computation power. As for RSUs using the threshold cryptography, police car participating to the generation of a pseudonym certificate will just generate a part of this certificate: they are not be able to discover which real identity is hidden behind a defined pseudonym certificate.

### 4.4 Summary

I detailed in this section my novel security architecture dedicated to operate within vehicular ad hoc networks. I identified in a first step the main actors of my architecture. Then, I presented the different procedures and functionalities of my secure communication architecture while establishing the message exchange protocols necessary to provide both authentication and privacy of vehicles. Therefore, I showed that by using pseudo certificates generated via the cooperation of several RSUs, the overhead of communications and management of anonymous keys at the side of a CA is avoided (contrary to several other security architectures within VANETs such as [5, 11, 13]). In addition, the operations of de-anonymity and revocation of malicious vehicles in VANETs shun the constraining CRL broadcast processes, used for example in [6, 7]. Finally, the confidentiality of inter-vehicular communications are ensured by a unique cryptographic operation, on the opposite of [12] which requires two cryptographic encryption and decryption operations for this purpose.

The correctness and the validity of my contributions are verified in the next section using the AVISPA tool.

## 5 Analysis and Validation

Considering the high sensitivity and reliability context of vehicular applications, including for example emergency message notification suggesting deceleration or stop of vehicles, I undertake a safety analysis of the different procedures of my security architecture within VANETs. This analysis allows to validate my specifications and guarantee the required security services. I use for this purpose the AVISPA security verifier tool that I present hereafter.

### 5.1 Security Oriented Verification in AVISPA

AVISPA [24] is a push-button tool for automated verification of Internet security-sensitive protocols and applications. Built upon independently developed modules (cf. Figure 10), AVISPA takes as input a security problem specification which includes one protocol and the security property to be satisfied. The specification is expressed in HLPSL (High Level Protocol Specification Language). Nevertheless, the architecture of AVISPA is so flexible that the tool may be used for any language convertible to IF (Intermediate Form).

A security problem modelled in HLPSL is automatically translated into the rewrite based formalism IF. An IF specification describes an infinite-state transition system amenable to formal analysis. The IF language acts as an interface between the protocol specification in HLPSL and the back-ends of AVISPA. Each back-end implements one specific analysis technique. Upon completion, AVISPA outputs one analysis result stating whether the input problem was solved or not. When no attack was found the protocol may be considered as safe. The result is valid for the environment considered in that verification experiment.

#### 5.1.1 The HLPSL Language

HLPSL is an expressive, modular, role-based, formal language that enables specification of control flow patterns, data structures, alternative intruder models, complex security properties, and various cryptographic primitives along with their algebraic properties. The HLPSL semantics is based on Lamport's Temporal Logic of Actions (TLA). A protocol specification in HLPSL is expressed in terms of roles. HLPSL uses basic roles to represent the roles played by each participant and composed roles to represent basic roles scenarios. Basic roles are two by two independent. They get initial information from parameters, and communicate with other roles via channels. The actions performed by a basic role are modelled by transitions which describe how the role state changes depending

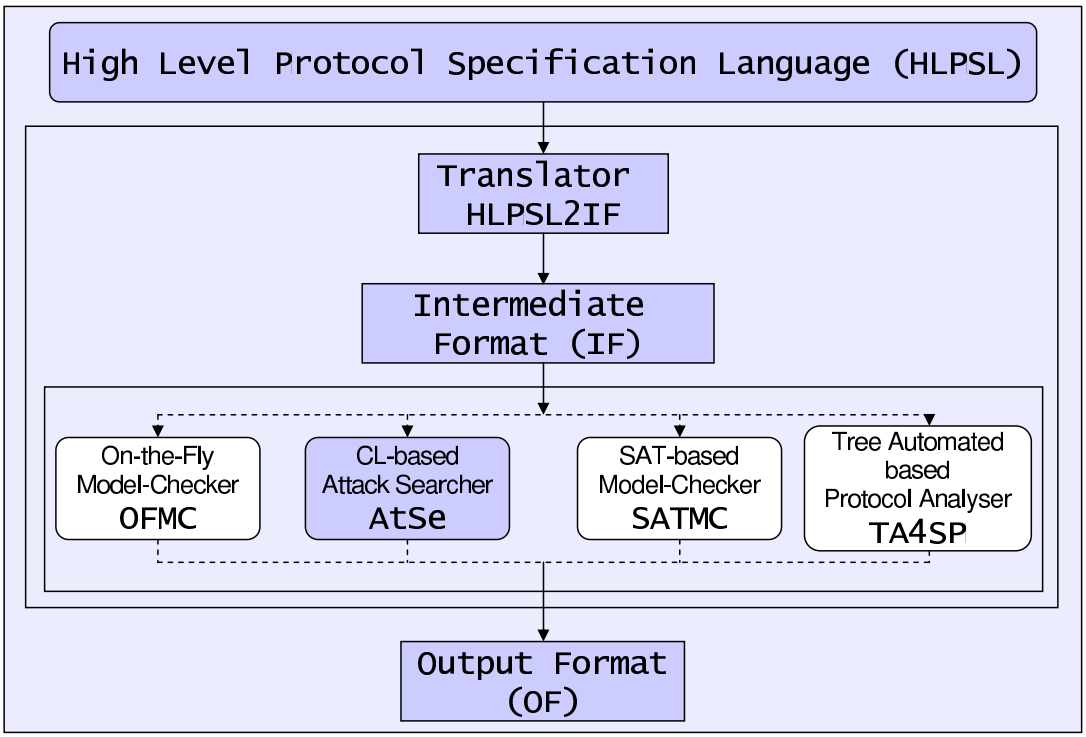


Figure 10: Architecture of the AVISPA tool

on events and facts. On the other hand, composition roles combine other roles, either in parallel or in sequence.

#### 5.1.2 Verifiable Security Properties

The AVISPA toolkit offers several backends for analyzing a HLPSL specification. The Constraint-Logic-based Attack Searcher (CL-AtSe) backend was used to verify my security architecture. CL-AtSe enables verification of various security properties, such as secrecy, authentication, fairness, and non-repudiation. The list is not exhaustive, since CL-AtSe can verify any state-based security property, including LTL formulas.

#### 5.1.3 The CL-ATse Backend

The Constraint-Logic-based Attack Searcher (CL-AtSe) takes as input the IF translation of the protocol specification. It uses rewriting and constraint solving techniques to identify all the reachable states of the participants and to state whether an attack does exist or not. Further, CL-AtSe enables security property specification using algebraic properties. It also analyzes constraints such as typing, inequalities, and shared sets of knowledge. It can obtain results for a large number of protocol sessions. Its flexibility and optimization facilitate integration of additional deduction rules and operator properties. For all these reasons, I decided to use CL-AtSe to verify my security architecture within VANETs.

### 5.2 Verification of the Security Framework using AVISPA

We successfully validated the different functionalities of my security approach within VANETs. I present in this subsection the verification of the revocation procedure. Before specifying this scenario with the HLPSL language, I identify the participating entities (called roles), their initial knowledge and the exchanged messages between them.

#### 5.2.1 Roles and Initial Knowledge

I identify four roles participating to a revocation scenario: a suspect vehicle "$Suspect$", two RSUs denoted by $RSU1$ and $RSU2$ and the corresponding $CA$. Figure 11 illustrates the messages exchange between these entities. Figure 2 shows the initial knowledge of these four roles.

#### 5.2.2 HLPSL Specification

I specify hereafter the HLPSL specification of the four roles of the proposed scenario. The first role corresponds to the RSU1; this entity detects the presence of a suspect vehicle within its range, defined by a pseudonym certificate (Pseudo_Cert_Suspect), and starts the revocation procedure by transmitting the pseudonym certificate to the group of RSUs.

```
role member1 (Suspect, RSU1, RSU2, CA: agent,
              TEK_RSU:symmetric_key,
              Seq_Num_RSU1:nat,
```

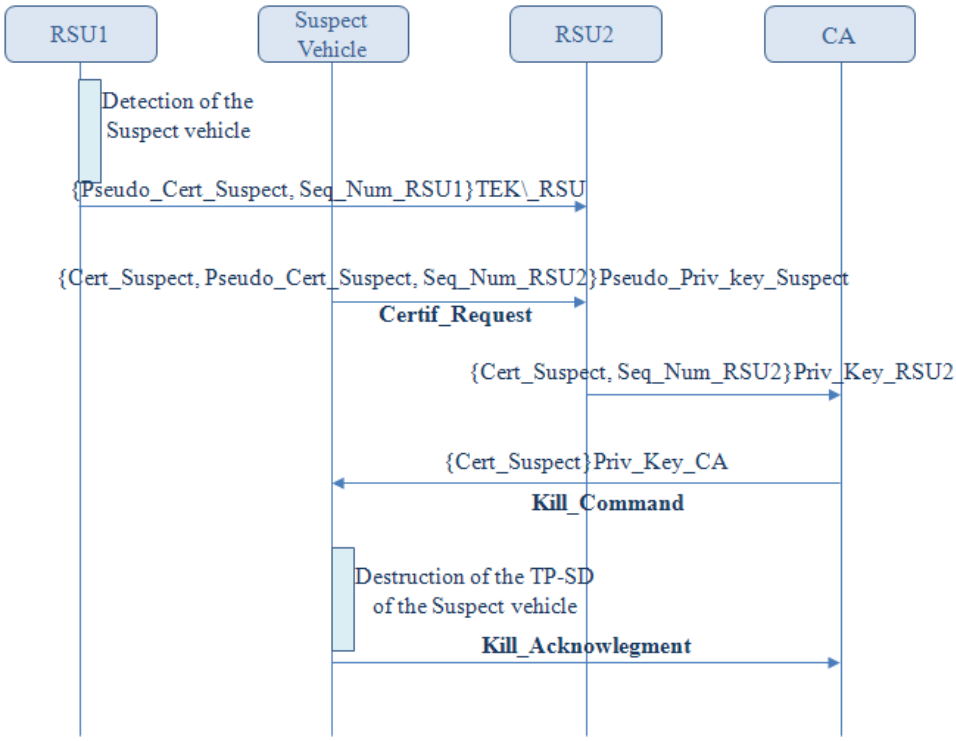


Figure 11: Scenario of revocation procedure

Table 2: Initial knowledge of the AVISPA roles

| Initial_Knowledge | |
|---|---|
| $RSU1$ | $TEK\_RSU, Seq\_Num\_RSU1, Pseudo\_Cert\_Suspect$ |
| $Suspect\_Vehicle$ | $Seq\_Suspect, Pseudo\_pub\_key\_suspect, Cert\_Suspect, Pseudo\_Cert\_Suspect$ |
| $RSU2$ | $TEK\_RSU, Pub\_Key\_RSU2$ |
| $CA$ | $PUB\_CA, Kill\_Command$ |

```
        Pseudo_Cert_Suspect:text,
        Snd, Rcv: channel(dy))
  played_by RSU1 def=
  local State: nat
  const id1: protocol_id
  init State:=0
  transition
  step1. State=0 /\ Rcv(start)
     =|> Snd({Pseudo_Cert_Suspect.Seq_Num_RSU1}
         _(TEK_RSU))
     /\  secret(Pseudo_Cert_Suspect,id1,{RSU1,RSU2})
     /\  State':=1
end role
```

The second role is corresponding to the suspect vehicle, detected by RSU1. In order to update its pseudonym certificate, this vehicle sends to RSU2 a Certif_Request message. At the reception of a Kill command sent by the CA, the TP-SD equipment of the suspect vehicle is immediately destroyed and all the sensitive elements it contents are damaged.

```
role member2  (Suspect, RSU1, RSU2, CA: agent,
          Seq_Suspect:nat,
          Pseudo_pub_key_suspect:public_key,
          Cert_Suspect,Pseudo_Cert_Suspect:text,
          Snd, Rcv: channel(dy))
   played_by Suspect def=
   local State: nat,
         PUB_CA: public_key,
         Kill:text
   const id2,id3: protocol_id
   init State:=0
   transition
   step1. State=0 /\ Snd({Cert_Suspect.Pseudo_
       Cert_Suspect.Seq_Suspect}_inv(Pseudo_pub_
       key_suspect))
      =|> witness(Suspect,RSU2,id2,Seq_Suspect)
      /\  State':=1
   step2. State=1 /\ Rcv({Kill'.Cert_Suspect'}
       _inv(PUB_CA'))
      =|> request(Suspect,CA,id3,Kill)
      /\  State':=2
end role
```

The third role is played by RSU2. It is responsible for notifying the real certificate of the suspect vehicle to the CA, after receiving the Certif_Request of this vehicle. This operation corresponds to the de-anonymity of the suspect entity.

```
role member3  (Suspect, RSU1, RSU2, CA: agent,
              TEK_RSU:symmetric_key,
```

```
              Pub_Key_RSU2: public_key,
              Seq_Num_RSU2:nat,
              Snd, Rcv: channel(dy))
    played_by RSU2 def=
    local State: nat,
          Pseudo_Cert_Suspect,Cert_Suspect:text,
          Pseudo_pub_key_suspect:public_key,
          Seq_Num_RSU1,Seq_Suspect:nat
    const id1,id2,id4: protocol_id
    init State:=0
    transition
    step1. State=0 /\ Rcv({Pseudo_Cert_Suspect'.
        Seq_Num_RSU1'}_(TEK_RSU'))
       =|> secret(Pseudo_Cert_Suspect,
        id1,{RSU1,RSU2})
       /\  State':=1
    step2. State=1 /\ Rcv({Cert_Suspect'.
        Pseudo_Cert_Suspect'.Seq_Suspect'}
        _inv(Pseudo_pub_key_suspect'))
       =|> request(RSU2,Suspect,id2,Seq_Suspect)
       /\  State':=2
    step3. State=2 /\ Snd({Cert_Suspect.
        Seq_Num_RSU2}_inv(Pub_Key_RSU2))
       =|> witness(RSU2,CA,id4,Cert_Suspect)
       /\  State':=3
end role
```

The CA is represented by the fourth role; the revocation of the suspect vehicle detected by RSU1 is in charge of this entity. At the reception of the certificate of the malicious node, sent by RSU2, the CA sends a Kill command to the concerned entity.

```
role member4 (Suspect, RSU1, RSU2, CA: agent,
              PUB_CA: public_key,
              Kill:text,
              Snd, Rcv: channel(dy))
       played_by CA def=
       local State: nat,
             Cert_Suspect:text,
             Seq_Num_RSU2:nat,
             Pub_Key_RSU2:public_key
       const id3,id4: protocol_id
       init State:=0
       transition
       step1. State=0 /\ Rcv({Cert_Suspect'.
           Seq_Num_RSU2'}_inv(Pub_Key_RSU2'))
          =|> request(CA,RSU2,id4,Cert_Suspect)
          /\  State':=1
       step2.State=1 /\ Snd({Kill.Cert_Suspect}
           _inv(PUB_CA))
          =|> witness(CA,Suspect,id3,Kill)
          /\  State':=2
end role
```

To verify the correctness of the specified scenario, I define the following security properties, considered as the goals of the verification phase: the confidentiality of the communications between RSUs (denoted by id1) and the mutual authentication between the RSU2, the CA and the suspect vehicle (id2,id3,id4).

```
goal
    secrecy_of id1
    authentication_on id2,id3,id4
end goal
```

Other composed roles are also included within the HLPSL specification of the specified scenario (session and environment roles).

### 5.2.3 Validation

The validation of my protocol specification, using the CL-Atse back-end, produces the following output:

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
GOAL
  As Specified
BACKEND
  CL-AtSe
```

The result of the AVISPA tool presented above shows that the scenario corresponding to the revocation procedure is correct, as it is specified. I obtained the same successful result with the specification of the other procedures of my security architecture within VANETs.

## 6 Conclusions and Future Work

Security within vehicular ad hoc networks is a very important issue; its development is required for the large deployment of this kind of networks. I focus in this paper on this problematic: I proposed a novel security architecture within VANETs, establishing an efficient tradeoff between authentication and privacy of drivers identities. My security architecture makes use of the threshold cryptography technique in order to share the certification capacity of vehicles to road side units (RSUs), while ensuring the privacy of the drivers identities by employing pseudonym certificates; the de-anonymity and revocation of untrusted entities are also guaranteed by my security architecture. These policies ensure authentication and non-repudiation of vehicles, while improving the availability of the certification authorities within VANETs (delegated to the RSU cooperations) and the tolerance for errors during the pseudonym certification communication phase. I validated the safety of my security architecture using the AVISPA security protocols verifying tool, and showed its correctness and applicability within VANETs.

As future work, I envisage to implement my security architecture within VANETs, and carry out real tests and measurements on the experimental platform of my research team.

## References

[1] Y. Zang, "Study on Message Dissemination Algorithms for Cooperative Danger Warning Applications

Based on Inter-Vehicle Communications", *COMNETS*, 2008.

[2] L. Stibor, Y. Zang, and H.J. Reumerman, "Neighborhood evaluation of vehicular ad-hoc network using IEEE 802.11p", *The 8th European Wireless Conference*, pp. 5, Paris, France, 2007.

[3] E. Minack, "Evaluation of the influence of channel conditions on Car2X communications", Chemnitz University, November 2005.

[4] B. Parno and A. Perrig, "Challenges in securing vehicular networks", *Workshop on Hot Topics in Networks (HotNets-IV)*, 2005.

[5] Raya Maxim and Hubaux Jean-Pierre, "The Security of Vehicular Ad Hoc Networks", *3rd ACM workshop on Security of ad hoc and sensor networks (SASN)*, Alexandria, VA, USA, 2005.

[6] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.P. Hubaux, "Secure vehicular communication systems: design and architecture", *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100-109, 2008.

[7] F. Kargl, P. Papadimitratos, L. Buttyan, M. Miller, E. Schoch, B. Wiedersheim, T. Thong, G. Calandriello, A. Held, A. Kung, and J.P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges", *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110-118, 2008.

[8] J.H. Song, W. S. Wong, and C. M. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks", *GLOBECOM*, pp. 806-810, 2008.

[9] S. Eichler, F. Dötzer, C. Schwingenschlögl, J. Eberspächer, and F.J. Fabra Caro, "Secure Routing in a Vehicular Ad Hoc Network", *60th Vehicular Technology Conference*, Los Angeles, USA, 2004.

[10] N. W. Lo and H. C. Tsai, "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks", *Eurasip Journal on Wireless Communications and Networking*, article in press, 2009.

[11] N. W. Wang, Y. M. Huang, and W. M. Chen, "A Reputation System for Traffic Safety Event on Vehicular Ad Hoc Networks", *Computer Communications*, vol. 31, pp. 2827-2837, 2008.

[12] X. Lin, R. Lu, C. Zhang, H. Zhu, P.H. Ho, and X. Shen, "Security in Vehicular Ad Hoc Networks", *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88-95, 2008.

[13] A. Studer and E. Shiand B. Fan and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs", *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09)*, pp. 1-9, 2009.

[14] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication", *Proceedings of the 6th Embedded Security in Cars Workshop (ESCAR)*, 2008.

[15] A. Studer, M. Luk, and A. Perrig, "Efficient Mechanisms to Provide Convoy Member and Vehicle Sequence Authentication in VANETs", *3rd International Conference on Security and Privacy in Communication Networks (SecureComm'07)*, 2007.

[16] M. S. Bouassida, G. Guette,d M. Shawky, and B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET", *International Journal of Network Security*, vol. 9, no. 1, pp. 22-33, 2009.

[17] M. S. Bouassida and M. Shawky, "Localization Verification and Distinguishability Degree in Wireless Networks using Received Signal Strength Variations", *7th International Symposium on Communications and Information Technologies ISCIT*, 2007.

[18] P. Golle, and D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs", *First ACM Workshop on Vehicular Ad Hoc Networks*, pp. 29-37, 2004.

[19] Y. Chun Hu, A. Perrig, and D. Johnson, "Packet Leashes: A defense against Wormhole Attacks in Wireless Ad Hoc Networks", Report Research, TR01 - 384, Rice University Department of Computer Science, 2002.

[20] P. Michiardi and R. Molva, "Ad hoc Network Security", *ST Journal of System Research*, vol. 4, no. 1, 2003.

[21] L. Zhou and J. Haas, "Securing Ad Hoc Networks", *IEEE Network*, vol. 13, no. 6, pp. 24-30, 1999.

[22] S. Yi and R. Kravets, "Key Agreement for Heterogeneous Ad Hoc Networks", Report Research, University of Illinois at Urbana-Champaign, Department of Computer Science, 2002.

[23] V. Legrand, "Etablissement de la Confiance et Reaux Ad Hoc - Le Germe de Confiance", Report Research, EDIIS, Laboratoire CITI, INRIA ARES, 2003.

[24] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Drielsma, P. Heam, J. Mantovani, S. Modersheim, D. Von Oheimb, M. Rusinowitchh, J. Santiago, M. Turuani, L. Vigano and L. Vigneron, "The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications", *17th International Conference on Computer Aided Verification (CAV'05)*, pp. 281-285, 2005.

[25] H. Ragab Hassen, A. Bouabdallah, H. Bettahar, and Y. Challal, "Hi- KD: Hash-based hierarchical Key Distribution for Group Communication", *IEEE-INFOCOM*, 2005.

[26] M. S. Bouassida, I. Chrismen,t and O. Festor", "Group Key Management in MANETs", *International Journal of Network Security*, vol. 6, no. 1, pp. 67-79, 2008.

[27] A. Perrig, R. Canetti, D. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol", *RSA CryptoBytes*, vol. 5, pp. 2002, 2002.

[28] G. Calandriello, P. Papadimitratos, J. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET", *Proceedings of the fourth*

*ACM international workshop on Vehicular ad hoc networks*, pp. 19-28, 2007.

[29] F. Bai, H. Krishnan, V. Sadekar, G. Holl, and T. Elbatt, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective", *Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2006.

[30] W. Diffie and M.E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644-654, 1976.

[31] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, 2007.

[32] I. Ingemarson, D. Tang, and C. Wong, "A conference key distribution system", *IEEE Transactions on Information Theory*, 1982.

**Mohamed Salah Bouassida** is a CNRS researcher at the HEUDIASYC laboratory in France. He has a Ph.D. and master degree from Henry Poincaré University, Nancy France, within the MADYNES research team in the LORIA laboratory (in 2006 and 2003 respectively). His main research interests are around ad hoc and vehicular networks, and include localization, security of group communications, establishment of group key management protocols, congestion control and dynamic geocast routing.