Secure and Distributed Certification System Architecture for Safety Message Authentication in VANET

Tiziri Oulhaci, Mawloud Omar, Ines Harfi, Fatiha Harzine

Noname manuscript No.
(will be inserted by the editor)

Secure and Distributed Certification System Architecture for Safety Message Authentication in VANET

Tiziri Oulhaci · Mawloud Omar · Fatiha Harzine · Ines Harfi

Received: 26/05/2016

Abstract Vehicular Ad hoc NETworks (VANETs) are a burgeoning research focus, aimed at creating communication among vehicles to improve the road safety and enhance driving conditions. For such networks, security is one of the most challenging issues due to their nature of wireless transmission and high topology changing frequency. In this paper, we propose a secure and distributed certification system architecture for safety message authentication in VANET, which resists against false public-key certification. To increase the availability of the authentication service, our proposal is designed through a decentralized system, supervised by a root authority. The latter authority delegates to a set of regional certification authorities the privilege of issuing public-key certificates to the vehicles. Each regional certification authority cooperates with its subordinates RSUs to sign public-key certificates using threshold signature. The main purpose of our solution is to ensure the messages authentication while respecting the imposed constraints by the real-time aspect and the nodes mobility. We demonstrate through the practical analysis and simulation results the efficiency of our solution with comparison to other concurrent protocols.

Keywords Security · Public-key certification · Threshold signature · Safety message authentication · VANET

Tiziri Oulhaci, Mawloud Omar, Fatiha Harzine and Ines Harfi
Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes, Université de Bejaia, 06000 Bejaia, Algérie.

1 Introduction

Recently, we are witnessing to the intensive and continuous use of public transit and private vehicles by many peoples in their daily life. The harmful result of this technology is the increasing number of fatalities that occur due to the road accidents [6]. Vehicular Ad hoc NETwork (VANET) is a type of Mobile Ad hoc NETwork (MANET) that provides, using Dedicated Short Range Communication (DSRC) standards, a wireless communication between nearby vehicles forming vehicle to vehicle communication (V2V), or between vehicles and a fixed equipment next to the road, called Road Side Unit (RSU) forming vehicle to infrastructure communication (V2I) [5]. The main goal of VANET is to share the data traffic to improve the road safety and the driving conditions [2]. VANET stimulates another category of applications called non-safety applications to offer more comfort to passengers such as weather information, automated toll payment, Internet access, etc. Since the network-vehicles communicate through wireless channels, a variety of attacks can be performed. Among these, we can cite the attacks related to the data coherence, which undermine the content of messages circulating in the network by modifying them or manufacturing fake data. Moreover, a malicious entity can use a false identity or impersonate a legitimate entity to benefit from its privileges in the network. Through the eavesdropping, an attacker can collect personal information of a user from the network whose it can benefit to trace his activities and track his movements. These attacks can lead to dangerous situations for the users. Therefore, security mechanisms are required to authenticate each user before using the network and ensure the authenticity and the integrity of exchanged safety messages among the legitimate vehicles.

Several research works are proposed in the literature, which we can classify into six categories: (1) public-key based protocols, (2) secret-key based protocols, (3) group signature based protocols, (4) identity-based signature protocols, (5) group communication based protocols and (6) self-certified based protocols. These mechanisms differ in the technique used to distribute the credentials and the nodes involved in their generation and issuance. In secret-key based protocols, a prior sharing of secret-key is required between each pair of nodes, which is difficult to achieve due to the dynamic nature of the network. This method may be not suitable when broadcasting periodically the trafic data. To the same context, in group communication based protocols, the exchanged messages in the group are encrypted using a secret-key generated by the leader and shared among the group members. This method is practical for some communication scenarios. However, in the general case, it is very difficult to realize giving the high mobility of nodes (i.e. vehicles traveling in different directions and using different speeds) as well as the secret-key should be updated whenever a member leaves the group. In the mechanisms based on group signature, each member signs a message on behalf of the group using its group secret-key. The signature is then verified by other members using the group public-key. This method requires much computations, and the revocation of a group member is an inherent task. Regarding the identity-based signature based protocols, each vehicle load independently or with the trusted authorities, to generate a pseudonym and its corresponding private-key based on a master secret-key in order to sign the messages. The drawback of this method is in the use of the master secret-key to generate all the nodes private-keys. When the master secret-key is disclosed, whole the system will be compromised. This is the same issue of the self-certified signature based protocols in which the system secret-key is shared among the vehicles. Once one vehicle is compromised, the system master secret can be leaked and whole the system will be compromised. We consider that the public-key based protocols are the most appropriate in terms of security and key management in the extent that each node generates its private and public-key. However, this method requires an efficient policy of certificates management.

Our proposal is based on public-keys and signatures to authenticate the communication among the vehicles. It represents a flexible architecture for managing and issuing certificates to the vehicles by improving the availability of the authentication service. Our architecture is hierarchical and the system is supervised by a root authority and managed by a set of regional certification authorities, which are responsible for authenticating the vehicles. Each regional authority supervises a coalition of RSUs and collaborates with them when delivering certificates to the vehicles using as multisignature mechanism the elliptic curve-based threshold signature scheme [21]. The architecture of our system consists of four entities, namely the Trusted Authority (TA), which is the system root; the Regional Certification Authorities (RCAs) which are deployed in different geographic areas; the coalitions of the delegated certification authorities implanted on the RSUs; and On Board Units (OBUs), which are implanted on the vehicles. During the network initialization, each vehicle is registered by the TA and given the system parameters. Each RCA holds a private-key delivered by the TA and shared among its subordinates RSUs. The RCA cooperates with its subordinates RSUs when delivering public-key certificates to the vehicles. The secure communication among the vehicles is established through the ECDSA signatures [4]. The main purpose of our system is to provide a reliable mechanism by increasing the certification service availability and resisting against compromised RSUs. The reliability depends on the certification service availability under the compromised RSUs presence. Centralizing the certification authority individually on each RSU exposes the vehicles to the certificate falsification attack, which can be carried out by the compromised RSUs. Sharing the certification authority allows to resist considerably against this attack, and thus increasing the availability of certification service. The solution that we propose is specifically applicable for VANET regarding two main aspects. The first aspect is related to the architecture of the network, which is different to the other types of mobile networks. The architecture of VANET supports the establishment of an authoritarian certification infrastructure that is easy to deploy and secure physically. The second aspect is related to the communication mode among the vehicles that exchange an intensive data traffic needing to be authenticated through an efficient certification mechanism.

The rest of this paper is organized as follows. In Section 2, we explain the problem statement and our main contributions. In Section 3, we review the existing solutions. In Section 4, we detail the architecture and the operations of our certification system. In Section 5, we analyse the security of our certification system. The practical analysis and the simulation results are presented respectively in Sections 6 and 7. Finally, we conclude this work in Section 8.

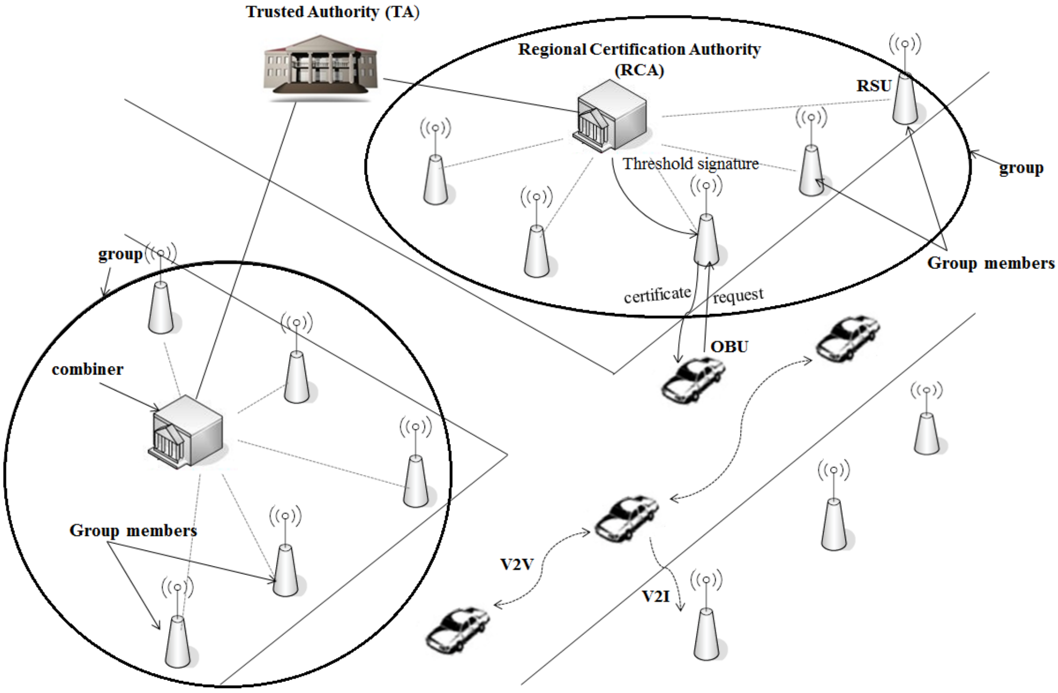

Fig. 1: Our system architecture

2 Problem statement and our contributions

The certificate management in highly dynamic networks, such as VANETs, involves two major challenges representing the main topic covered in this paper. The first problem is related to the certification service availability, which is a specific problem to the high dynamicity of VANETs. Centralizing certificate repositories on the servers could compromise the access availability, where the network is a subject of partitioning because of the mobility of the vehicles. The second challenge is related to the robustness of the certification service, regarding to how a vehicle should verify the trustworthy of the public-key certificates. This problem is due to the spontaneity nature of VANETs, which are deployed on open environments, and hence, giving the opportunity for attackers to alter or to inject trucked public-key certificates. Anterior works, as [27], [32] and [35], were specifically based on mechanisms addressing directly the robustness problem of the certification service without considering its availability. However, to the best of our knowledge, our work is the first that identifies the certification service availability problem regarding the specific constraints of VANETs.

The related authentication protocols are based on an operational architecture maintained by only one trusted authority, which is responsible to authenticate and issue credentials to the vehicles. This generates a significant computation overhead on the trusted authority, and it is hard to maintain the access to the latter because of the frequent disconnection of the vehicles. Involving each RSU independently in the authentication process can lead to dysfonctionnement when the network is exposed to the attacks with compromised RSUs. This issue is the aim of our work for which we propose a secure and distributed certification system.

In response to the challenges described above, we contribute through this work with a secure and distributed certification architecture. The availability is addressed to answer the first challenge and we propose a distributed architecture. Contrasting to the existing solutions, which centralize the certification service on the RCAs, we introduce the concept of delegation. Instead to centralize the certification service, each RCA delegates subordinates RSUs for the certificate management, and hence increasing its availability for the vehicles. The robustness is addressed to answer the second challenge and we propose a collaborative-based approach of certification in order to resist against compromised RSUs, which can deliver trucked certificates. In this context, we propose the adaptation of the threshold cryptography in the framework of certificate management for VANETs. We propose a scheme of (t, n) allowing n subordinated RSUs to share the certification service private-key. However, from only t RSUs, a vehicle could constitute the requested certificate. Hence, is hard for an attacker to compromise the certification service, in which it should compromise t separated RSUs.

In our protocol we have opted for public key cryptography to authenticate communications among vehicles. The impact of this mechanism is to facilitate the key management in the sense that each vehicle is responsible to generate its pair of secret and public key independently of other entities in the system. The RCA validates each pair of keys by issuing a certificate to the relevant vehicle. To sign the certificates, the authority uses the threshold signature. The impact of this technique is the resistance against false public-key certification. When an attacker attempting to forge the signature of a certificate, it should forge t valid partial signatures and combine them to find the signature of the certificate. The threshold signature can also increases the availability of the certification service, which is distributed on t RSUs and not supported by only one trusted entity. The threshold signature used is constructed on the two base points but other threshold signature scheme constructed on the only one point. In this case, the elliptic curve discrete logarithm problem becomes more difficult to solve while providing better security.

3 Related work

In this section, we first give an overview of security issues addressed in VANETs and then we survey the most relevant approches of certification and authentication existing from the literature.

3.1 Security issues in VANETs

There is a research effort in the framework of security in VANETs. In the following, we give a short taxonomy of works according to the supported security requirements:

- Authentication: in VANETs, It is very important to authenticate all users and messages which transit through the network. The works conducted in this context are focused to find solutions for preventing attacks (Sybil, impersonation, GPS spoofing, etc.) that undermine this goal. For example, the authors in [24] propose an approach against Sybil attack by analyzing the similarity of the informations disseminated by malicious nodes and those of its neighbors. In another works proposed in [23][33], the authors use the identity based cryptography to resist against impersonation attack.

- Availability : attacks related to the availability aim to make the network not functional and the useful informations unavailable. We can cite DoS attack, jamming attack, timing attack, etc. In [13], a distributed and robust approach is presented to defend against DoS attacks. The proposed scheme detects the fake identities of malicious vehicles with the help of consistent existing IP address information. In [14], the authors have proposed a scheme called, Hideaway Strategy, which prevent against jamming attack. This last uses the PSR (Packet Send Ratio) to determine if a network is jammed and consequently all nodes should go into silent mode.
- Confidentiality: during communications among entities of the network, outsiders are not able to understand confidential informations that pertain to each entity. We can cite some works relating to this security requirement as [15] that propose a cryptographic based access control framework for vehicles to securely exchange messages by integrating moving object modeling techniques with cryptographic policies.
- Integrity: the integrity protects against the unauthorized creation, destruction or alteration of data. It ensures that a message was not altered or delated during the transmission by a malicious node. We classify in this category the approaches that provide integrity mechanisms helping to protect information against modification, deletion or fabrication attacks. As example in [16], the authors provide methodology to dynamically re-create a new route of a message whenever a malicious node is interfaced and tries to block the transmission.
- Non-repudiation: this security requirement consists to be able to trace the origin of message or action realized in the network if necessary. In [1], the authors propose to use legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicles' real identity.

3.2 Certification and authentication approches

In what follows, we survey the most relevant certification and authentication approaches proposed in the literature in the framework of VANETs.

3.2.1 Public-key based protocols

Lu et al. have proposed an Efficient Conditional Privacy Preservation (ECPP) protocol for secure vehicular communication [35], which uses a PKI signature scheme for anonymous message authentication. A road side unit issues a short-time anonymous certificate in response to OBU's request using the identity-based group signature scheme proposed in [39]. Although ECPP provides a mechanism for conditional privacy, however it does not ensures unlink-ability of an OBU since compromised RSUs store the unchanged pseudonym for the same OBU. Furthermore, since the tracing procedure in ECPP is executed by the TA with the collaboration of RSUs, it is impossible to trace the real identity of the sender from compromised RSUs. Jung et al. have proposed a Robust and Efficient Anonymous Authentication Protocol (REA^{2}P) [32], which uses the identity-based group signature scheme proposed in [39], universal re-encryption scheme [38] and the identity based key establishment scheme [42] to assign a multiple anonymous certificates by a nearby RSU for each vehicle. These certificates are used to send authentic messages to other vehicles. Compared to ECPP, this protocol provides unlink-ability and traceability when multiple RSUs are compromised. However, in the process of the public-key certificate issuance, if the requested RSU fails, the requester vehicle will not receives its certificate. Wasef and Shen have proposed an aggregated signatures and certificates verification scheme [34], which can improve the capabilities of OBUs to simultaneously verify the signatures and public-key the senders certificates. This solution allows to reduce the loss rate and the signature verification delay. Park et al. have proposed an Efficient Anonymous Authentication Protocol (EA^{2}P) [27], which allows to optimize the computation delay, ensure efficient message verification and security requirements. To achieve this purpose, the authors have used a road side unit to issue on-the-fly public-key certificates to the vehicles. A key-insulated signature scheme is used in order to certify the vehicles anonymous public-keys. Wasef et al. have proposed an Expedite Message Authentication Protocol (EMAP) [7], which uses a keyed Hash Message Authentication Code (HMAC) to verify the revocation of vehicles instead of using the Certificate Revocation List (CRL). The key to use in calculating the HMAC is shared only among the unrevoked OBUs. For more details about the solutions proposed in the framework of this category, kindly refer to [3].

3.2.2 Secret-key based protocols

Ying et al. have used the Message Authentication Code and hash operations to authenticate messages sent among the vehicles [17]. It consists of using two-level key hash chain to sign messages. At the reception, the receiver uses the key included in the key packet to calculate the key signature and verify the signature of the received message. The drawback of this solution is the dependence on the first broadcast of the key packet, which contains the first key signature. In the event that this package will not be delivered correctly to the receiver, the latter cannot verify the messages sent from the sender. Hu et al. have proposed three authentication schemes [19]: (1) communication between vehicles and road side units, (2) one to one communication within a group, and (3) one to one communication without a group. The authors have adopted HMAC technique and symmetric encryption to sign and verify the exchanged messages among vehicles. For more details about the solutions proposed in the framework of this category, kindly refer to [30].

3.2.3 Group signature based protocols

Zhang et al. have proposed to use a decentralized group-authentication scheme [26] to ensure the communication among the vehicles. Each group is maintained by one RSU using a group signature scheme. The group of vehicles can broadcast messages, which can be verified in the same or neighboring groups. The authors have adopted a signature scheme to reduce the time of signature and encryption. Each vehicle should be authenticated with each RSU to obtain the group secret-key, which increases the communication overhead. Kim and Song have proposed a pre-authentication method [20] improving the protocol proposed in [26]. It reduces the delay of key renewing, which takes place by vehicles in the range of each RSU. The request of the secret member key and the authentication of the vehicle are repeated in each RSU. The authors have used the communication among RSUs to exchange beforehand vehicle's information. In this way, each RSU could verify in advance the authenticity of the vehicle and issues its member secret-key in a timely manner. For more details about the solutions proposed in the framework of this category, kindly refer to [29].

3.2.4 Identity-based signature protocols

Chim et al. have proposed both Security and Privacy-Enhancing Communication Schemes (SPECS) [28]. The first consists of using a batch verification and bloom filter to verify the signatures of messages sent by the vehicles. SPECS uses a binary search to distinguish between invalid and valid signatures in the batch. However, the verification of the exchanged messages among the vehicles is performed by RSUs. Hence, the receiver cannot accept the message until it receives a notification from a nearby RSU. In the same context, Horng et al. have proposed b-SPECS+ [8], an improvement of the protocol SPECS. The protocol b-SPECS+ defends against the impersonation attack. The signatures verification is only done by the nearby RSU, which broadcasts a notification when a signature is valid. If the receiver leaves the range of RSU, it cannot be able to receive the notification. Huang et al. have proposed a pseudonym-based authentication protocol [23] to ensure the anonymity of the real identity and prevent the vehicles tracking. After registration and authentication with the Motor Vehicles Division (MVD), the vehicle collaborates with the nearby RSU to generate pseudonyms. These pseudonyms are used to send messages to other vehicles. To sign messages, the authors have used the Identity-Based Encryption (IBE) scheme [41]. Each vehicle is supposed to get one or more tokens when it joins a new RSU. Otherwise, the vehicle cannot access to the communication service in the range of this RSU. Bhavesh et al. have proposed a novel authentication protocol [12], which provides anonymity to each vehicle as per its requirement. It consists to issue a set of pseudonyms to a vehicle in the authentication of messages. Each pseudonym includes an expiration date, and hence, the level of anonymity obtained by a vehicle increases with an increased number of pseudonyms owned and decreased value of the lifetime of each pseudonym. However, the storage cost increases proportionally to the number of generated pseudonyms. The protocol proposed in [11] follows to reduce the impact of an attack by adopting a strategy of limiting the extent of damage when the tamper-proof device or RSU is compromised. This has been implemented by the vehicles distribution on groups maintained by the RSUs. Each RSU attributes the master private-key to each vehicle member to sign the traffic data. The major drawback of this solution lies in the fact that each vehicle is supposed to know the RSUs public-keys. Chim et al., in [18], were interested on the type of the broadcasted messages in the network namely, regular and urgent messages. The regular messages can be authenticated by the neighboring vehicles using HMAC and the urgent messages can be verified with the aid of nearby RSUs using the batch verification. For more details about the solutions proposed in the framework of this category, kindly refer to [30].

3.2.5 Group communication based protocols

Jesudoss et al. have proposed an authentication protocol based on group communication [9]. The protocol is not depended to any fixed infrastructure along the road. Vehicles which have the same direction, speed and able to hear emissions of each other form a group with a vehicle leader. The latter attributes the group secret-key and performs the batch verification of the broadcasted messages in the group. However, in high mobility with intermittent speeds of vehicles, it is very difficult to form and maintain the group for a long period of time. For more details about the solutions proposed in the framework of this category, kindly refer to [31].

3.2.6 Self-certified signature based protocols

Zhang et al. have proposed a privacy-preserving authentication protocol [10] which is based on the anonymous self-certified signature scheme [33]. The system consists of two entities: vehicles and the TA. Each vehicle has a public and private-keys and requests the TA to be certified. In response to each vehicle, the TA issues instead a normal certificate, a "witness" and the real identity of this vehicle is embedded. The vehicle uses its "witness" to sign messages and any vehicle which receives it along with the sender identity can recover the corresponding public-key to verify the message signature. For more details about this category, kindly refer to [36].

4 Our certification system architecture and operations

In this section, we give the description of our system. We present its architecture, and then in detail its operations.

4.1 An introduction of Elliptic Curves Cryptography (ECC)

Let $GF(P^m)$ be the finite field of P^m elements, such as p is a prime and m an integer. An elliptic curve E over $GF(P^m)$ represents a set of solutions (x, y), where $x, y \in GF(P^m)$, relating to a cubic equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with $a_1, a_2, a_3, a_4, a_6 \in GF(P^m)$, together with a special point O, called the point at infinity.

In cryptographic practice, the most used elliptic curves are the following:

1. Curves over $GF(2^m)$ with m a large integer. The cubic equation takes the form of $y^2 + cy = x^3 + ax + b$, with $a, b, c \in GF(2^m)$, $c \neq 0$, or $y^2 + xy = x^3 + ax^3 + b$, with $a, b \in GF(2^m)$, $b \neq 0$.
2. Curves over $GF(p)$ with p a large prime. The cubic equation takes the form of $y^2 = x^3 + ax + b$, with $a, b \in GF(p)$ and $4a^3 + b^2 \neq 0(\text{mod}p)$.

Given an elliptic curve E defined over $GF(p)$ and two points $G, Q \in E$. The elliptic curve discrete logarithm problem is to find the unique integer k if it exists, such that $G = kQ$. For more details about ECC, kindly refer to [40].

4.2 Architecture and assumptions

The main goals of our proposal are the following:

1. Message authentication and integrity: each vehicle in the network should be able to verify that a message is sent by a legitimate vehicle and has not been modified during its transmission.
2. The robustness: the protocol should resist against compromised RSUs which can try to deliver false public-key certificates to the vehicles.
3. The availability and the reliability: the certification service should be kept available and should be efficient in terms of delay and transmission overhead.

We illustrate in figure 1 the architecture of the proposed system. It consists of four entities which cooperate to provide the authentication of the exchanged data trafic among the vehicles. These entities have the following roles:

1. Trusted Authority (TA): is the root authority of the hierarchy, which is responsible for initializing the security parameters, registration of the network nodes and revoking the compromised entities.
2. Regional Certification Authority (RCA): is responsible for issuing public-key certificates to the vehicles within its region. The RCA cooperates with its subordinate RSUs to sign the requested public-key certificates using threshold signature. The threshold scheme is denoted by (t, n), where t represents the minimum required number of RSUs collaborating in the signature process, and n the number of RSUs supervised by the RCA.
3. RSU: it subordinates to only one RCA. It cooperates to issue public-key certificates to the vehicles by assigning a partial signature when it's requested by the RCA.
4. OBU: is a device installed in the vehicle for sharing road information with other vehicles. It also communicates with RSUs to request public-key certificates.

We assume that the TA is trusted by all the network nodes and cannot be compromised. The TA and RCAs communicate between them through a secure infrastructure-based network. We assume that each RCA is equipped with a high capacity of storage and computation and each RSU has sufficient computational ressources. Our system operates in three phases:

1. The system initialization and registration of entities: in this phase, the TA generates the system parameters and the initial credentials for each entity of the network. These parameters allow considering an entity as legitimate, which can benefice of the network services.
2. The public-key certificate deliverance: this step is performed when a vehicle requests a nearby RCA to get or renew its public-key certificate. The RCA checks the legitimacy of the vehicle and cooperates with its subordinates RSUs in order to issue the certificate using the threshold signature.
3. The safety message signature and verification: during the validity period of a public-key certificate, a vehicle diffuses the safety messages in an authenticated manner. Each message is signed and joined to the vehicle's public-key certificate. These signatures will be verified from the receiver before validating the message.

We give the detailed description of these phases in the following subsections. The used notations are summarized in Table 1.

4.3 System initialization and registration of entities

The TA chooses large prime numbers p and η, and generates an elliptic curve $E : y^2 = x^3 + ax + b(\mod p)$. $a, b \in Z_p$, are in the order of the elliptic curve and $4a^3 + b^2 \neq 0(\mod p)$. Then, the TA chooses a base point G, generates its private-key $S_{TA} \in [1, \eta - 1]$ and computes the corresponding public-key Q_{TA}, such as:

$$Q_{TA} = S_{TA} \cdot G \tag{1}$$

Finally, it chooses a hash function H and base points A and B in the order η and publishes the system parameters: $\langle Q_{TA}, A, B, p, H, \eta \rangle$.

Notation	**Description**
H	Hash function
S_{TA}, Q_{TA}	The TA secret and public keys
ID_{RCA_i}	The RCA$_i$ identity
ID_{RSU_j}	The RSU$_j$ identity
F_i, G_i	The threshold functions of the RCA$_i$ group
$\langle \rho_0^{(i)}, \varrho_0^{(i)} \rangle$	The RCA$_i$ secret-key
Y_i	The RCA$_i$ public-key
$\langle \rho_j^{(i)}, \varrho_j^{(i)} \rangle$	The RSU$_j$ secret-key
Y_j	The RSU$_j$ public-key
RID_{V_k}, PID_{V_k}	The vehicle V_k real and pseudo identities
γ_k	The V_k implicit certificate
PrK_k, Q_k	The V_k long-term secret and public keys
SK_k, PK_k	The V_k short-term secret and public keys
ζ_k	The V_k public-key certificate
T	The public-key certificate validity period
$(P)_x$	The x coordinate of the point P
$\|$	Concatenation operation
$+$, $-$, $\cdot$	Elliptic curve addition, substruction and multiplication

Table 1: Notations

4.3.1 Registration of RCAs and RSUs

The TA generates for each RCA$_i$ a unique identifier ID_{RCA_i} and two secure threshold functions, denoted by F_i and G_i. The latter functions are used to generate the RCA$_i$'s group private-key X_i and the corresponding public-key Y_i, such as:

$$X_i = \langle \rho_0^{(i)}, \varrho_0^{(i)} \rangle = \langle F_i(0), G_i(0) \rangle \tag{2}$$

$$Y_i = \rho_0^{(i)} \cdot A + \varrho_0^{(i)} \cdot B \tag{3}$$

sends X_i to the RCA$_i$ through a secure channel and publishes $\langle ID_{RCA_i}, Y_i\rangle$ as public parameters.

For each RSU$_j$, the TA generates a unique identifier ID_{RSU_j} and affects it to the group maintained by the nearby RCA$_i$. Then, it generates the RSU$_j$'s representative index $I_j \in [1, n]$ and through the threshold functions F_i and G_i, computes the RSU$_j$'s private-key X_j and the corresponding public-key Y_j, such as:

$$X_j = \langle \rho_j^{(i)}, \varrho_j^{(i)}\rangle = \langle F_i(I_j), G_i(I_j)\rangle \tag{4}$$

$$Y_j = \rho_j^{(i)} \cdot A + \varrho_j^{(i)} \cdot B \tag{5}$$

sends X_j to the RSU$_j$ through a secure channel and publishes $\langle ID_{RSU_j}, Y_j\rangle$ as public parameters.

4.3.2 Registration of vehicles

When a vehicle V_k joins the network for the first time, it should be registered by the TA to get its pseudo-identity and its implicit certificate. These parameters will be used to authenticate itself to the RCA when it requests for a public-key certificate. The TA uses the hash function H to generate the V_k's pseudo-identity, denoted by PID_k, such as: $PID_{V_k} = H(RID_{V_k})$, where RID_{V_k} denotes the V_k's real identity. Then, it generates random integers α, $\beta \in [1, \eta - 1]$ and computes:

$$\gamma_k = \alpha \cdot A + \beta \cdot B \tag{6}$$

$$PrK_k = \Big(H(\gamma_k \| PID_{V_k}) \cdot (\alpha + \beta) + S_{TA}\Big) \bmod \eta \tag{7}$$

$$Q_k = H(\gamma_k \| PID_{V_k}) \cdot \gamma_k + Q_{TA} \tag{8}$$

where Q_k, PrK_k and γ_k represent, respectively, the vehicle V_k's long-term public-key, long-term private-key and implicite certificate. Finally, the TA sends $\langle PID_{V_k}, \gamma_k, PrK_k, Q_k\rangle$ to the vehicle V_k through a secure channel. The private-key PrK_k is used to sign each request sent by the vehicle to the RCA in order to get or renew its public-key certificate. The RCA computes the public-key Q_k from the implicit certificate γ_k and verifies the signature validity of the vehicle request.

4.4 Public-key certificate deliverance

Each vehicle V_k could submit a request to the nearby RCA to get or renew its public-key certificate. It chooses a validity period T and a base point G_k, generates its own short-term private-key $SK_k \in [1, \eta - 1]$ and computes the corresponding short-term public-key PK_k, such as:

$$PK_k = SK_k \cdot G_k \tag{9}$$

The vehicle V_k authenticates itself to the RCA using its long-term private-key PrK_k by generating the signature $\langle r, s \rangle$ of the certification request $\langle PID_{V_k}, PK_k, \gamma_k, T \rangle$. To calculate the signature, it selects a random number $\mu \in [1, \eta - 1]$ and computes:

$$r = (\mu \cdot A)_x \bmod \eta \tag{10}$$

$$s = \mu^{-1} \cdot \left(H(PID_{V_k} \| PK_k \| \gamma_k \| T) + r \cdot PrK_k \right) \bmod \eta \tag{11}$$

Finally, it sends $\langle PID_{V_k}, PK_k, \gamma_k, T, r, s \rangle$ to the RCA through the nearby RSU. Upon receiving the request, the RCA verifies the authenticity of the vehicle V_k by computing its long-term public-key Q_k, such as:

$$Q_k = H(\gamma_k \| PID_{V_k}) \cdot \gamma_k + Q_{TA} \tag{12}$$

The computed public-key is used to verify the validity of the signature $\langle r, s \rangle$. To do this, the RCA computes:

$$\lambda = s^{-1} \cdot \left(H(PID_{V_k} \| PK_k \| \gamma_k \| T) \cdot A + r \cdot Q_k \right) \bmod \eta \tag{13}$$

and verifies if $\lambda_x = r \bmod \eta$. If it holds, then the signature is valid and the RCA issues the vehicle V_k's public-key certificate ζ_k.

Each RCA$_i$ supervises a set of n RSUs and it cooperates with t RSUs to generate a public-key certificate using threshold signature. The RCA$_i$ broadcasts the certification request to its subordinating RSUs. Upon receiving the request, each RSU$_j$ chooses randomly two numbers r_{j_1} and $r_{j_2} \in [2, \eta - 1]$, computes and sends to the RCA$_i$ the point P_j, such as:

$$P_j = r_{j_1} \cdot A + r_{j_2} \cdot B \tag{14}$$

Upon receiving P_j, the RCA$_i$ computes $e = H(ID_{RCA_i} \| PID_{V_k} \| PK_k \| T \| R_x)$, selects t RSUs and responds with $\langle R, e, L_j \rangle$, such as:

$$R = \sum_{j=1}^{t} P_j \bmod p \tag{15}$$

$$L_j = \prod_{\ell=1,\, \ell \neq j}^{t} \frac{I_\ell}{I_\ell - I_j} \tag{16}$$

Then, each RSU$_j$ computes and sends to the RCA$_i$ the partial signature $\langle S_{j_1}, S_{j_2} \rangle$, such as:

$$S_{j_1} = \left(r_{j_1} + e \cdot \rho_j^{(i)} \cdot L_j \right) \bmod (p - 1) \tag{17}$$

$$S_{j_2} = \left(r_{j_2} + e \cdot \varrho_j^{(i)} \cdot L_j \right) \bmod (p-1) \tag{18}$$

and sends $\langle S_{j_1}, S_{j_2} \rangle$ to the RCA$_i$. The latter verifies the partial signature validity of each RSU$_j$ by verifying the equality:

$$Q_j = S_{j_1} \cdot A + S_{j_2} \cdot B - e \cdot Y_j \cdot L_j \tag{19}$$

If at least one partial signature is not valid, the RCA$_i$ selects another alternative set of t RSUs and reiterates the process. Otherwise, if all the partial signatures are valid, then the RCA$_i$ computes the vehicle V_k's public-key certificate complete signature σ_k, such as:

$$\sigma_k = \langle e, S_1 = \sum_{j=1}^{t} S_{j_1} \bmod p, S_2 = \sum_{j=1}^{t} S_{j_2} \bmod p \rangle \tag{20}$$

Finally, the RCA$_i$ sends the public-key certificate $\zeta_k = \langle ID_{RCA_i}, PID_{V_k}, PK_k, T, \sigma_k \rangle$ to the vehicle V_k through the t participating RSUs. Upon receiving the public-key certificate, the vehicle V_k verifies the signature validity using the RCA$_i$'s public. It computes:

$$Z = S_1 \cdot A + S_2 \cdot B - e \cdot Y_i \tag{21}$$

and verifies if:

$$e = H(ID_{RCA_i} \| PID_{V_k} \| PK_k \| T \| Z_x) \tag{22}$$

4.5 Safety messages signature and verification

During the validity period T of a public-key certificate ζ_k, the vehicle V_k diffuses the safety messages in an authenticated manner. Each message must be signed and joined to the public-key certificate ζ_k. To generate the message M's signature $\langle r, s \rangle$, the vehicle uses its short-term secret-key SK_k. It selects a random number $\mu \in [1, \eta - 1]$ and computes:

$$r = (\mu \cdot A)_x \bmod \eta \tag{23}$$

$$s = \mu^{-1} \cdot \left(H(M) + r \cdot SK_k \right) \bmod \eta \tag{24}$$

and broadcasts $\langle M, r, s, \zeta_k \rangle$ using its maximal power range. Upon receiving the message, each neighbor vehicle verifies the public-key certificate ζ_k validity using the issuer RCA public-key. If the signature is invalid, the message is ignored. Otherwise, its verifies the validity of the message M's signature. To perform that, it extracts the vehicle V_k's short-term public-key PK_k through the joined public-key certificate ζ_k, computes:

$$\lambda = s^{-1} \cdot \left(H(M) \cdot A + r \cdot PK_k \right) \bmod \eta \tag{25}$$

and verifies if $\lambda_x = r \bmod \eta$. If it holds, then the signature is valid, and the safety message M is accepted. We note that in case of security problem, the TA is able to trace the origin of the message by extracting from the public-key certificate ζ_k the vehicle V_k's pseudo-identity PID_{V_k} and recovers its real identity RID_{V_k}.

4.6 Computational complexity

The computational complexity of the initialization phase is $O\big((e+1)\log(\eta)\big)$, where e represents the total number of the RCAs, RSUs, and OBUs in the system. The computational complexity of the public-key certificate deliverance phase is $O\big(n_r(t+2)\log(\eta)\big)$, where n_r represents the number of requests sent by the vehicles in order to obtain the certificates. The computational complexity of the signature and verification phase is $O\big(f\log(\eta)\big)$, where f represents the number of diffused messages in the network. Indeed, the complexity does not change in the case of sporadic traffic. This does not depend on traffic behavior, but it depends on the parameter e in the initialization phase, on the parameter n_r in the certificate deliverance phase, and on the parameter f in the signature and verification phase.

5 Security analysis

5.1 Fake public-key certification

We consider two types of adversaries: compromised RSUs and external malicious entities. The external malicious entities have no way to take part in issuing fake certificates. Indeed, to be able to generate a partial signature, the malicious entity should be subordinated of a regional certification authority and has its private share corresponding to the threshold signature scheme. Compromised RSUs represent threat because they are an internal entities. A compromised RSU may issue several types of false certificates: (1) a certificate that binds a public-key PK_i to a vehicle V_j instead of the vehicle V_i in order to trick other vehicles to believe in this fake binding, (2) a certificate that binds a vehicle V_j to a fake public-key, or (3) it can invent a number of vehicle pseudo-identities and public-keys and bind them by appropriate certificates. Our proposal resists against bindings described in (1), (2), and (3). Indeed, if a compromised RSU intends to invent a fake binding, it should exist a least other $t-1$ partial signatures corresponding to this false binding. However, to do that a compromised RSU should collect, beside its private share, at least $t-1$ private shares from other RSUs, signs t partial signatures and combines them to generate the signature of the fake certificate. Therefore, our solution resists against the fake public-key certification that can be launched by compromised RSUs.

5.2 Message integrity and authentication

The authenticity of a vehicle and the integrity of the safety messages are ensured, respectively, by verifying the vehicle certificate signature and the vehicle message signature. This allows to prove that the vehicle holds a valid short-term key pair corresponding to its pseudo-identity. An attacker may attempt to impersonate a legitimate vehicle by forging the signature of its certificate. In order to show the robustness of our protocol against the forgery attack, we analyze the following scenario. Suppose the attacker eavesdrops the exchanged traffic on the network and collects the public system parameters $\langle Q_{TA}, A, B, p, H, \eta\rangle$. Suppose also that the attacker is given from a challenger the pseudo-identity PID_{V_k} of a vehicle V_k, the RCA$_i$'s public-key Y_i and its identity ID_{RCA_i}. The attacker chooses randomly SK as its short-term secret-key, chooses a base point G, computes the corresponding short-term public-key $PK = SK \cdot G$ and sends PK to the challenger. The latter asks the attacker to pick and sign a random message M on behalf of V_k to produce $\sigma = \langle r, s\rangle$. The challenger also generates a valid period T and asks the attacker to sign $\langle ID_{RCA_i} \| PID_{V_k} \| PK \| T\rangle$ in order to produce the signature $\sigma' = \langle e, S_{j_1}, S_{j_2}\rangle$ of the vehicle's certificate ζ_k. Finally, the attacker sends σ and σ' to the challenger. The attacker's advantage depends to the validity probability of both signatures namely, σ and σ'. The signature scheme should be secure against forgery attack if the latter probability is negligible. To forge a valid signature σ', we assume that the attacker randomly selects a point Z, intending to compute e following $Z = (Z_x, Z_y)$. Hence, the attacker computes $e' = H(ID_{RCA_i} \| PID_{V_k} \| PK \| T \| Z_x)$ and derives the signature $\langle e, S_{j_1}, S_{j_2}\rangle$ from A, B and Y_j, and tries to solve the equation $S_{j_1} \cdot A + S_{j_2} \cdot B - e' \cdot Y_i = (Z_x, Z_y)$. Such solutions of the unknown numbers S_{j_1}, S_{j_2} depend on the elliptic curve discrete logarithm problem, and it is infeasible in reasonable computational time. Therefore, the attacker cannot forge a valid signature of a certificate even if he intercepts some important information for its generation from the network thus, the attacker's advantage is negligible.

6 Practical analysis of our certification system

In this section, we evaluate the hardware performance required to put in the practice our system. Indeed, each vehicle maintains a set of security parameters and exchanges safety messages with the other vehicles. Thus, two important performance parameters are involved: the storage and the transmission.

6.1 Storage requirement

The safety message $\langle M, \sigma_M, \zeta_i\rangle$ is diffused periodically by each vehicle. The message M includes the vehicle's position, its current time, its direction, its speed, its acceleration/deceleration and its traffic current events with $|M| = 100$Bytes. However, the size of the M's signature (σ_M) depends on the prime curve size. The public-key certificate ζ_i size varies according to the hash function and the prime curve size. In figure 2, we present the evolution of the public-key certificate size in function of three hash functions in the NIST elliptic curves over prime fields. Since each message sent in the network is joined to the sender public-key certificate, we evaluate, as shown in figure 3, the evolution of the safety message size in function of the prime curve size.

Each vehicle maintains a long-term private-key, a long-term public-key, an implicit certificate, a short-term key pair and a public-key certificate delivered by the RCA. In figure 4, we illustrate the storage requirement in each OBU according to the prime curve size and

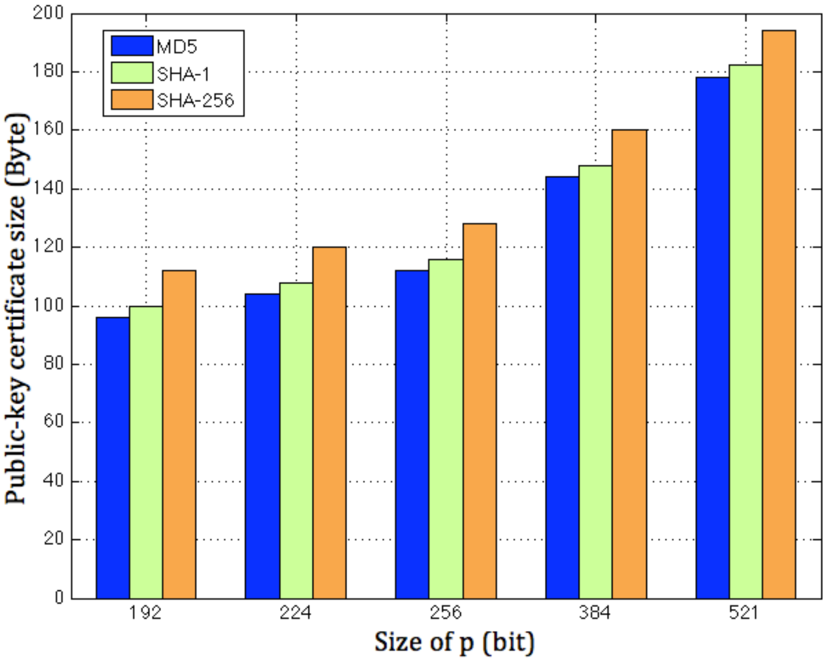

Fig. 2: Public-key certificate size

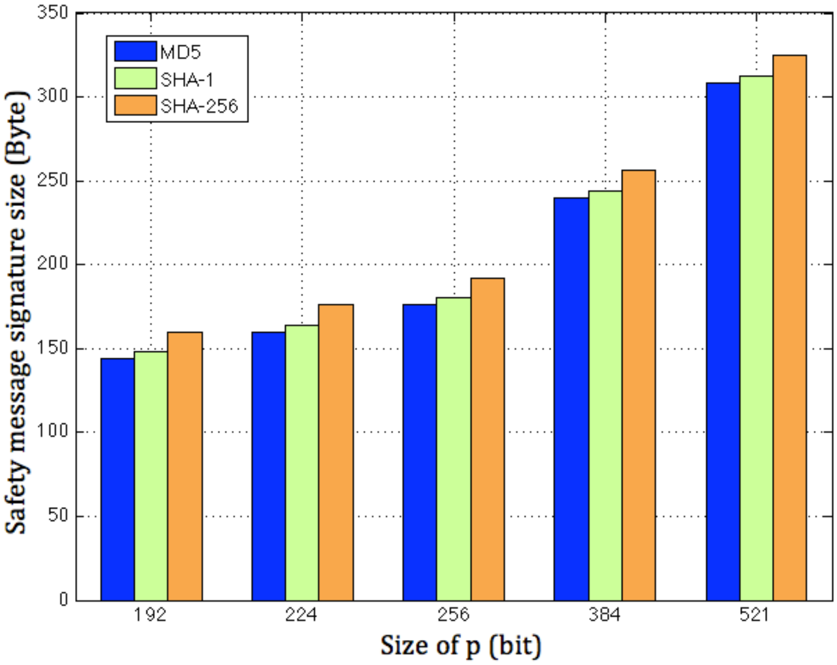

Fig. 3: Authentication message size

the hash function used in the certification process. For example, in the worst case with $|p| = 512$bits, just approximately 0.7KBytes of memory capacity is required in each OBU.

Indeed, the hash function is used only in the safety message signature and the certification process. The generated hash value does not affect considerably both the safety message signature and the certificate sizes. According to the obtained results, we note a slight gap between the public key certificate size, the safety message signature size and the storage requirement according to the used hash function. The results demonstrate that our protocol is flexible and the storage requirement is independent of the hash function technique. Moreover, we note that our system has no constraints in terms of storage requirements according to the actual development of technology. For example, with the highest size of p, the stockage capacity needed is only about 200Bytes.

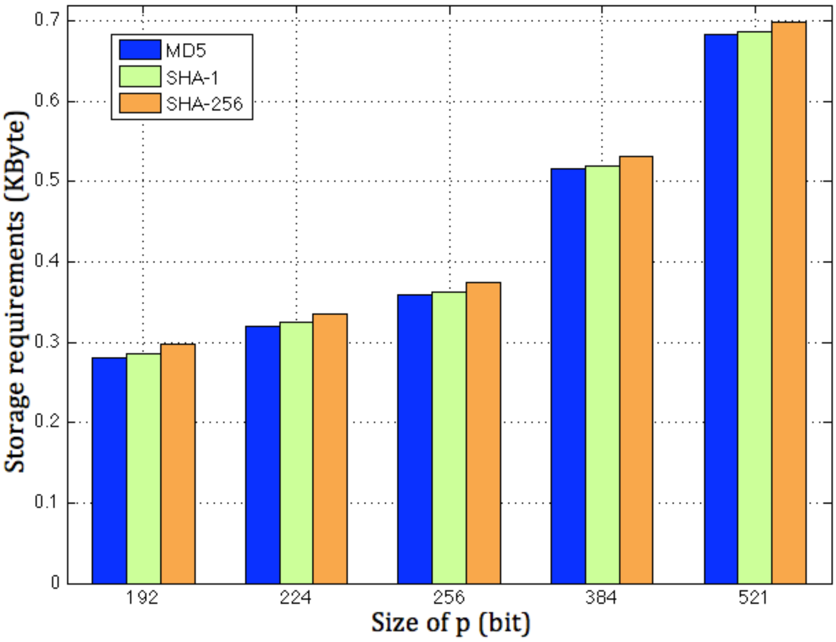

Fig. 4: Storage requirement

6.2 Transmission requirement

The system throughput in VANETs is the bandwidth currently demanded by vehicular communication in the communication channel [25]. It can be calculated in Mbps as [37]:

$$2^{-17} \times w \times rt \times m \tag{26}$$

where w is the number of vehicles in the transmission range, rt is the messaging rate per vehicle, and m is the total message size. According to the DSRC standards, each vehicle sends the message with a time interval from 100ms to 300ms and the minimal data rate is 6Mbps, two scenarios are considered:

- Scenario 1: a highway with 6 lanes (3 in each direction) of 3m each. We assume a uniform presence of vehicles with an inter-vehicle space of 30m. Vehicles in movement transmit messages every 300ms over a 300m communication range. We consider a vehicle located in the middle of the highway, which corresponds to a maximum of received messages, this vehicle can hear 120 vehicles per 300ms. In figure 5, we illustrate the transmission speed required according to the vehicle number and the prime curve size. In the worst-case, where all the vehicles contend for the channel, for $|p| = 521$bits, the system throughput is 2.5Mbps (< 6Mbps).

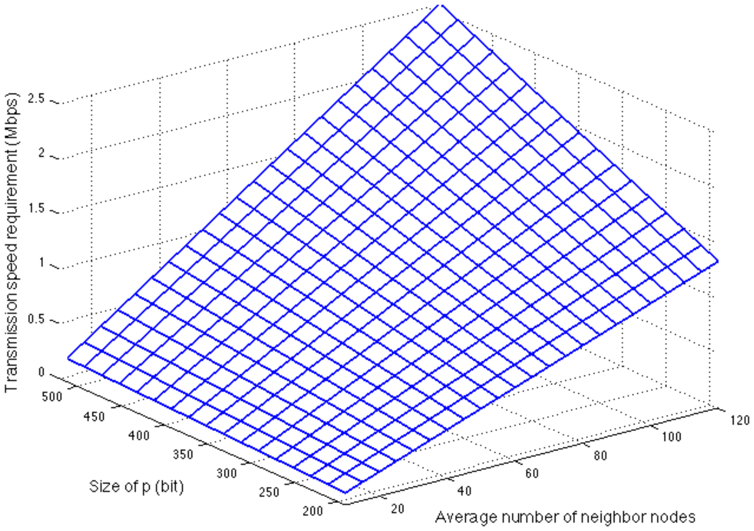

Fig. 5: Transmission requirement for the first scenario

- Scenario 2: we consider the same highway as in the previous case but this time vehicles are very slow or stopped, spaced by 5m. Each vehicle transmits a safety message over a range of 15m every 100ms. In this case, a vehicle can hear at most 36 other vehicles per 100ms. As shown in figure 6, for $|p| = 521$bits, the system throughput 2.5Mbps (< 6Mbps).

7 Performance evaluation

In this section, we analyze the performances of our system. We perform a comparison with other authentication signature-based protocols to underline the efficiency and the suitability of our solution. The performance analysis given here is focusing on the certification and message verification successful rate.

7.1 Simulation model

We have implemented the simulations using Matlab environment [43]. We have simulated a vehicular ad-hoc network with $N = 400$ vehicles moving on a highway road of 12km supervised by a set of RSUs. Each vehicle moves with a speed of 80km/h and diffuses every 300ms a safety message of size 100Bytes. The vehicles and RSUs are configured with a wireless communication range of 300m and a bandwidth of 6Mbps. Our simulator estimates if

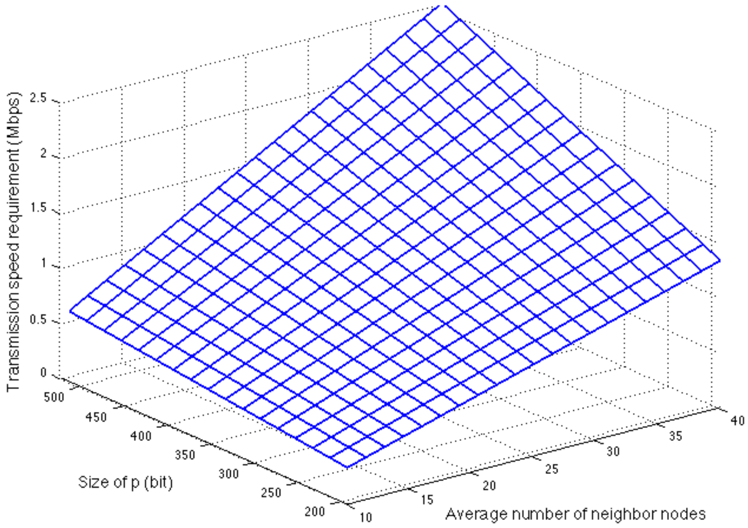

Fig. 6: Transmission requirement for the second scenario

a radio link exists among the vehicles (respectively among the vehicles and RSUs) according to the distance that separates them. We assume that the vehicles are homogeneous and have the same hardware characteristics and processing capabilities. The certification requests arrive to the RSUs following a Poisson law with an average inter-arrival between requests of $\lambda = 5$s under a simulation period of 2000s. We have evaluated two important metrics: (1) the certification success rate, which represents the pourcentage of successful certification requests, and (2) the message verification rate, which is calculated as follows [18]:

$$\frac{1}{N}\sum_{k=1}^{N}\frac{m^{(k)}}{m'^{(k)}} \tag{27}$$

where $m^{(k)}$ is the total number of messages that are successfully verified by the vehicle V_k and $m'^{(k)}$ represents the total number of the received messages by the vehicle V_k. We compare our protocol with three authentication signature-based protocols, namely ECPP [35], REA^{2}P[32] and EA^{2}P [27]. The latter protocols are described in Section 3.

7.2 Results

We have performed three experiments comparing the performance of our protocol with ECPP, REA^{2}P and EA^{2}P. We have considered the presence of a set of malicious RSUs. A malicious RSU could be a compromised RSU or an external attacker. It could alter the certification request forwarding and/or generate fake public-key certificates. It performs the attack following a probability p_a, i.e., the probability of a honesty behavior performed by a malicious RSU is $1 - p_a$. In the first experiment, we have varied the percentage of malicious RSUs from 0% to 90% with an attack probability $p_a = 0.9$ while observing the certification success rate. In the second experiment, we have varied the attack probability p_a of malicious RSUs from 0.1 to 0.9 with a percentage of 10% of malicious RSUs while observing the certification success rate. In the third experiment, we have measured the messages authentication success in function of time. Due to the close convergence of the protocols ECPP and EA^{2}P in terms of certification policy, the results of successful certification rate of the two protocols are presented on the same curve. However, the protocols use different policies of safety messages signature and verification. Table 2 and Table 3 show the measures used in the simulations considering the same security measures and cryptographic operation time presented in [27].

Mesure	**Value**
Bilinear pairing operation time	4.5ms
Point multiplication operation time	0.6ms

Table 2: Cryptographic operation time

Mesure	**Our protocol**	**ECPP**	**REA^{2}P**	**EA^{2}P**
Certificate generation time	16.8ms	34.8ms	31.2ms	20.4ms
Certificate verification time	1.8ms	18.9ms	17.1ms	2.4ms
Message signature verification time	1.2ms	1.28ms	1.28ms	1.2ms

Table 3: Protocol execution time

In figure 7 (a), we illustrate the certification success rate of the protocols in function of the percentage of malicious RSUs in the network. We note that the successful rate of the protocols ECPP, REA^{2}P and EA^{2}P decreases rapidly by increasing the percentage of malicious RSUs. However, the performance of our protocol remains stable at 100% until a rate of 70% of malicious RSUs. Regarding the protocols EA^{2}P, REA^{2}P and ECPP, when a vehicle requires a public-key certificate, it solicits one RSU and if the latter is compromised it can issue a fake public-key certificate, which affects considerably the successful rate of certification, especially the protocol REA^{2}P since each RSU issue multiple public-key certificates to both. In our protocol, the public-key certificates are issued using threshold cryptography. The operation is performed with the collaboration of a set of t RSUs to deliver the partial public-key certificates. The signatures are verified and combined by the regional certification authority, which allows the elimination of the fake signatures, and hence maintaining a high successful rate. In figure 7 (b), we illustrate the certification success rate of the protocols in function of the attack probability. Compared to the protocols EA^{2}P, REA^{2}P and ECPP, the attack probability does not affect the efficiency of our protocol, where the certification process avoid all the false signatures irrespective of the intensity of the attacker. In figure 8, we illustrate the messages authentication success rate of the protocols in function of time. We note that our protocol verifies an average of 89% of the received safety messages. However, EA^{2}P verifies about 73%, REA^{2}P average 31% and ECPP only 13%, which are much lesser than our protocol. Fewer messages are lost in the case of our protocol compared to ECPP, REA^{2}P and EA^{2}P. This is due to the execution rapidity of the signature verification process, and hence, treating a maximum number of messages before being ignored in the next round of diffusion (period of 300ms).

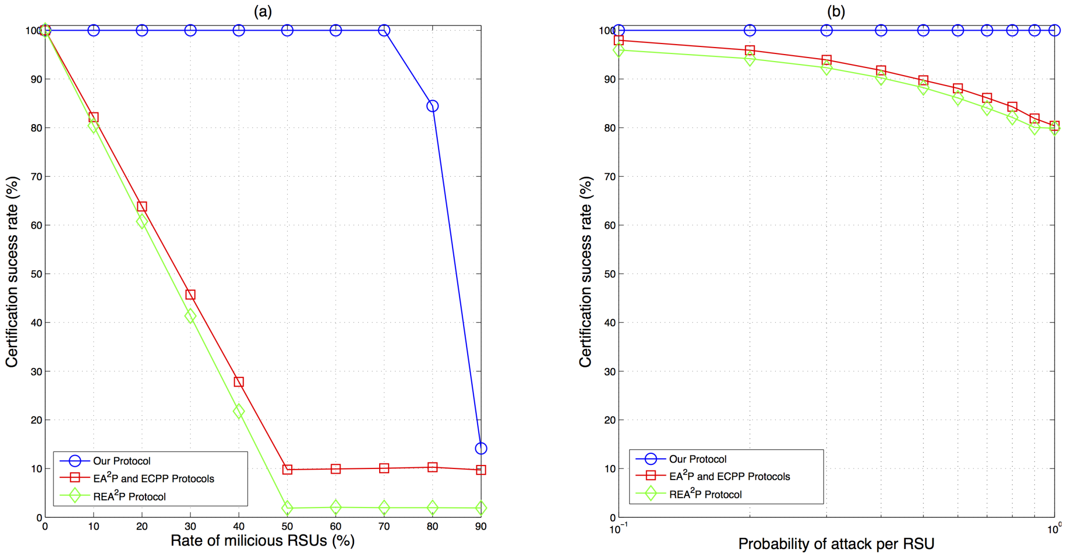

Fig. 7: Certification success rate in function of (a) the compromised RSUs rate, and (b) the probability of attack per compromised RSU (our protocol with $t = 10$)

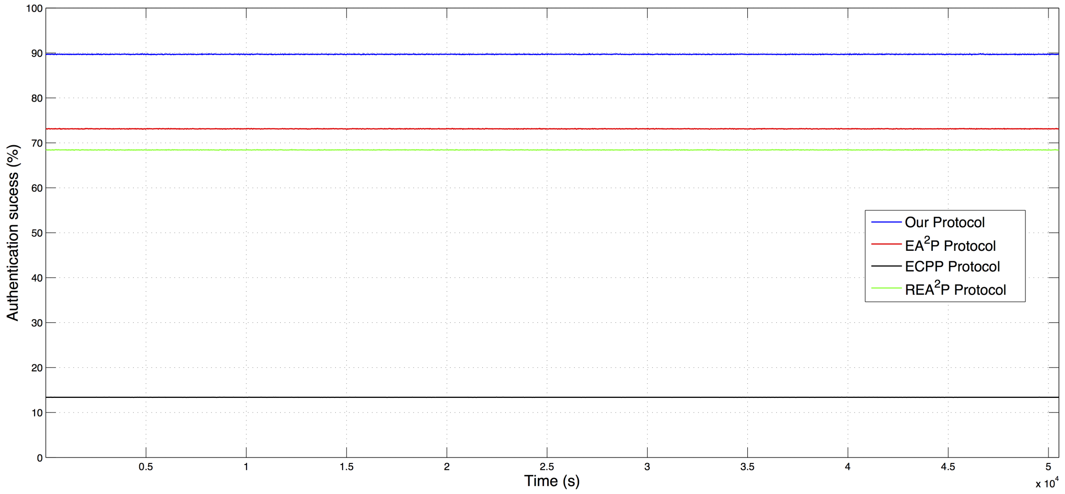

Fig. 8: Message authentication success

8 Conclusion

In this paper, we have focused on the authentication protocols in VANETs. We have presented the related works, where we have classified them regarding the signature mechanisms of the safety messages. Then, we have proposed a certification system, which uses public-key based signature to authenticate the communication among vehicles. The architecture of the proposed system is hierarchical, supervised by a trusted root authority. The latter supervises the regional certification authorities, which are responsible for authenticating the vehicles when the latter request public-key certificates. Each regional authority manages a set of RSUs and collaborates with them to sign public-key certificates to the vehicles using threshold encryption. The concept of threshold cryptography is introduced in order to resist against compromised RSUs that may issue false public-key certificates to cheat the service of certification. Through a practical analysis, we have discussed the hardware performance required to put in a real practice our system. Finally, the simulation results show the robustness of our proposal with comparison to other concurrent solutions.

Based on the framework of this work, we are considering to adresse the challenge of privacy. Indeed, an attacker may try to collect the information of a user from the network such as its pseudonyms, which can be used to trace his activities and/or track his movements. Therefore, we propose to contribute by designing a new system which satisfies the unlinkability. Moreover, we aim to extend our protocol by incorporating an efficient mechanism of public-key certificate revocation. We will further evaluate the performances of our protocol on a large scale of VANET and implement a prototype for a real practice.

Acknowledgment

This work was carried out in the framework of research activities of the laboratory LIMED, which is affiliated to the Faculty of Exact Sciences of the University of Bejaia.

References

1. J. Li, H. Lu and M. Guizani. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, Num. 4, Pages 938–948, 2015.
2. M. N. Mejri, J. Ben-Othman and M. Hamdi. Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communication*, Vol. 1, Num. 2, Pages 53–66, 2014.
3. V. Vijayalakshmi, M. Sathya, S. Saranya and C. Selvaroopini. Survey on various mechanisms for Secure and Efficient VANET communication. *International Conference on Information Communication and Embedded Systems*, 2014.
4. S. Karati, A. Das, D. Roychowdhury, B. Bellur, D. Bhattacharya and A. Iyer. New algorithms for batch verification of standard ECDSA signatures. *Journal of Cryptographic Engineering*, Vol. 4, Num. 4, Pages 237–258, 2014.
5. R. G. Engoulou, M. Bellaïche, S. Pierre and A. Quintero. VANET security surveys. *Computer communications*, Vol. 44, Pages 1–13, 2014.
6. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti and H. Zedan. A comprehensive survey on vehicular Ad hoc network. *Journal of Network and Computer Applications*, Vol. 37, Pages 380–392, 2013.
7. A. Wasef and X. Shen. EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE transactions on mobile computing*, Vol. 12, Num. 1, Pages 78–89, 2013.
8. S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li and M. K. Khan. b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET. *IEEE transactions on information forensics and security*, Vol. 8, Num. 11, Pages 1860–1875, 2013.
9. A. Jesudoss, S. V. K. Raja and S. H. Park. GRAS: A Group Reliant Authentication Scheme for V2V communication in VANET. *Systemics, cybernetics and informatics*, Vol. 11, Num. 6, Pages 47–52, 2013.
10. J. Zhang, W. Zhen and M. Xu. An Efficient Privacy-preserving Authentication Protocol in VANETs. *9th International Conference on Mobile Ad-hoc and Sensor Networks*, 2013.

11. B. Liu and L. Zhang. An Improved Identity-based Batch Verification Scheme for VANETs. *5th International Conference on Intelligent Networking and Collaborative Systems*, 2013.
12. B. B. N, S. Maity and R. C. Hansdah. A Protocol for Authentication with Multiple Levels of Anonymity (AMLA) in VANETs. *27th International Conference on Advanced Information Networking and Applications Workshops*, 2013.
13. K. Verma, H. Hasbullah and A. Kumar. Prevention of DoS Attacks in VANET. *Wireless Personal Communications*, Vol. 73, Num. 1, Pages 95–126, 2013.
14. I. K. Azogu, M. T. Ferreira, J. A. Larcom and H. Liu. A New Anti-Jamming Strategy for VANET metrics-directed security defense. *International Conference - Globecom - Vehicular Netwok Evolution*, 2013.
15. S. Karumanchi, A. Squicciarini and D. Lin. Selective and Confidential Message Exchange in Vehicular Ad Hoc Networks. *Chapter Book on Network and System Security of the series Lecture Notes in Computer Science*, Vol. 7645, Pages 445–461, 2012.
16. M. U. Farooq, M. Pasha, K. U. R. Khan, M. U. H. Atif. An Advanced Security and Data Integrity Protocol for Vehicular Ad-Hoc Networks. *Advanced Materials Research*, Vols. 403–408, Pages 994–1001, 2012.
17. B. Ying, D. Makrakis and H. T. Mouftah. Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Applications*, Vol. 36, Num. 5, Pages 1352–1364, 2012.
18. T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li. MLAS: Multiple level authentication scheme for VANETs. *Ad Hoc Networks*, Vol. 10, Num. 7, Pages 1445–1456, 2012.
19. C. Hu, T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li. Efficient HMAC-based secure communication for VANETs. *Computer Networks*, Vol. 56, Num. 9, Pages 2292–2303, 2012.
20. J. Kim and J. Song. A Pre-authentication Method for Secure communication in Vehicular Ad Hoc Networks. *8th International Conference on Wireless communication, Networking and Mobile Computing*, 2012.
21. W. Yun and L. Dianjun. An Efficient Threshold Signature Scheme Based on the Elliptic Curve Cryptosystem. *International Conference on Computer Science and Electronics Engineering*, 2012.
22. M. S. Al-kahtani. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). *6th International Conference on Signal Processing and Communication Systems*, 2012.
23. D. Huang, S. Misra, M. Verma and G. Xue. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE transactions on intelligent transportation systems*, Vol. 12, Num. 3, Pages 736–746, 2011.
24. J. Grover, M. S. Gaur, V. Laxmi and N. K. Prajapati. A Sybil Attack Detection Approach using Neighboring Vehicles in VANET. *International Conference on Security of information and networks*, 2011.
25. A. K. K. Aboobaker. Performance Analysis of Authentication Protocols in Vehicular Ad hoc Networks (VANET). Technical report, Department of Mathematics, Royal Holloway, University of London, Egham, England, 2010.
26. L. Zhang, Q. Wu, A. Solanas and J. D. Ferrer. A Scalable Robust Authentication Protocol for Secure Vehicular communication. *IEEE transactions on vehicular technology*, Vol. 59, Num. 4, Pages 1606–1617, 2010.
27. Y. Park, C. Sur, C. D. Jung and K. H. Rhee. An Efficient Anonymous Authentication Protocol for Secure Vehicular communication. *Journal of information science and engineering*, Vol. 26, Pages 785–800, 2010.
28. T.W. Chim, S.M. Yiu, L. C. K. Hui and V. O. K. Li. SPECS: Secure and privacy enhancing communication schemes for VANETs. *Ad Hoc Networks*, Vol. 9, Num. 2, Pages 189–203, 2010.
29. H. Xiong, Z. Guan, J. Hu and Z. Chen. Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview. *Computer and Information Science*, Applied Cryptography and Network Security, Dr. Jaydip Sen (Ed.), InTech, DOI: 10.5772/34675, 2010.
30. M. Al-Qutayri, C. Yeun and F. Al-Hawi. Security and Privacy of Intelligent VANETs. *Computer and Information Science*, Security and Privacy of Intelligent VANETs, Computational Intelligence and Modern Heuristics, Al-Dahoud Ali (Ed.), InTech, DOI: 10.5772/7815, 2010.
31. M. Riley, K. Akkaya and K. Fong. A survey of authentication schemes for vehicular ad hoc networks. *Security and Communication Networks*, Vol. 4, Num. 10, Pages 1137–1152, 2010.
32. C.D. Jung, C. Sur, Y. Park and K. H. Rhee. A Robust and Efficient Anonymous Authentication Protocol in VANETs. *Journal of communication and networks*, Vol. 11, Num. 6, Pages 607–614, 2009.

33. T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li. Security and privacy issues for inter-vehicle communication in VANETs. *In Proceedings of 6th Annual IEEE communication Society Conference on SECON Workshops*, 2009.
34. A. Wasef and X. S. Shen. ASIC: Aggregate Signatures and Certificates Verification Scheme for Vehicular Networks. *Global Telecommunication Conference*, 2009.
35. R. Lu, X. Lin, H. Zhu, P. H. Ho and X. Shen. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular communication. *In Proceedings of IEEE Infocom*, 2008.
36. J. K. Liu, M. H. Au and W. Susilo. Self-generated-Certificate Public Key Cryptography and certificateless signature/encryption scheme in the standard model. *2nd ACM symposium on Information, computer and communications security*, ACM, 2007.
37. M. Raya and J. P. Hubaux. The security of vehicular ad hoc networks. *Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks*, 2005.
38. P. Golle, M. Jakobsson, A. Juels and P. Syverson. Universal reencryption for mixnets. *In Proceedings of CT-RSA, LNCS 2964*, 2004.
39. D. Boneh and H. Shacham. Group signatures with verifier-local revocation. *In Proceedings of the 11th ACM conference on Computer and communication Security*, 2004.
40. H. Darrel and V. Scott. Guide to Elliptic Curve Cryptography. *Springer Professional Computing Publishing Company Incorporated*, Book, 2003.
41. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. *In Proceedings of 21st Annual International Cryptology Conf. Adv. Cryptology*, 2001.
42. U. M. Maurer and Y. Yacobi. A non-interactive public-key distribution system. *Designs, Codes, and Cryptography*, Vol. 9, Num. 3, Pages 305–316, 1996.
43. http://www.mathworks.com/