Privacy Preservation Authentication Model for a Secure Infrastructure over Vehicular Communications

https://doi.org/10.3991/ijim.v16i12.31533

Soukayna Riffi Boualam[1], Mariyam Ouaissa[2], Mariya Ouaissa[2(✉)], Abdellatif Ezzouhairi[1]
[1]Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco
[2]Moulay Ismail University, Meknes, Morocco
mariya.ouaissa@edu.umi.ac.ma

Abstract—Vehicle Ad-hoc Networks (VANET) are considered among recent wireless communication technologies. Nowadays, vehicles are no more than simple means of transport, they are endowed with a source of intelligence through their interaction with the road environment due to embedded equipment on board vehicles and integrated into stations along roads and highways. The mechanisms of security and protection of messages exchanged in VANET, thus preserving the privacy of users and satisfying the various security requirements, are a prerequisite for the deployment of vehicle networks. Increasingly, several research have been proposed to improve protocols for maintaining security and preserving privacy. This paper presents a hierarchical revocable infrastructure based privacy preservation authentication protocol for vehicles that involves authentication of each vehicle and the corresponding Road Side Unit (RSU) by a Certification Authority (CA). The proposed protocol used Elliptic Curve Diffie Hellman (ECDH) algorithm for reliable key exchange and Edwards-curve Digital Signature Algorithm (EdDSA) to speed up the execution of the authentication process especially at the key management level, message signing and verification of this signature. On the other hand, the creation of sub-lists of revoked certificates based on vehicle type makes it possible to minimize the response time by looking for a certificate if it is revoked or not. Our solution was checked by the security verification tool, Automated Validation of Internet Security Protocols and Applications (AVISPA), which indicated that it is a very secure level. Performance analysis illustrates that the protocol greatly saves computation resources.

Keywords—ITS, VANET, privacy preservation, authentication, ECDH, EdDSA

1 Introduction

Wireless networks have experienced remarkable progress in recent years, they are undeniable today. Their appearance and the advancement of communication and information technologies are giving rise to the so-called Intelligent Transport Systems (ITS). The principal aim of these systems is to make the road more efficient. Moreover, one of the main strengths of ITS is to enable a level of cooperation between participants

in the road network by equipping vehicles with wireless communication equipment. This type of wireless network refers to vehicular networks [1].

Vehicular Ad hoc Networks (VANET) [2] are a new form of Mobile Ad hoc Networks (MANET) that aim to provide communications between vehicles or with infrastructure located at roadside. These networks are described as a dynamic topology according to the addition or departure of a vehicle from the network. In these networks, vehicles are equipped with wireless short and medium range communication. Actually, the vehicles can communicate with each other with two methods, either Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I) where vehicle communicates with the equipment next to the road named Road Side Unit (RSU) [3]. VANET are used to meet the communication needs applied to transport networks to improve driving and road safety for road users.

In VANET, vehicles exchange messages and communicate with each other in a wireless environment. This situation can give rise to internal or external security attacks which can have the objective of rendering the network non-functional, of causing an accident. For that reason, the preservation of the security of information exchanged between vehicles is a crucial necessity. Communication must go through the analysis of the potential of security threats, and the design of a robust architecture capable of dealing with these threats. In this context, the implementation of vehicular networks requires an effective security mechanism in order to satisfy security requirements such as authentication, integrity and the privacy preservation of a user [4].

This paper presents a hierarchical authentication protocol with the aim of ensuring basic security requirements such as integrity, confidentiality, non-repudiation, and availability, as well as the preservation privacy of users by using an identifier or a real identifier. Firstly, our solution allows vehicles and RSUs to authenticate with the certification authority so that they are legal entities in the network. Then a mutual authentication between vehicles and RSUs makes it possible to minimize access to malicious entities in the network.

The proposed protocol combines between the symmetrical and asymmetrical approach, where the symmetrical approach used Elliptic Curve Diffie Hellman (ECDH) algorithm for reliable key exchange that is implemented in order to create and share the secret key whose objective is to ensure the security of the exchange of the parameters for the asymmetric system (Private Key/Public Key), authentication packets and vehicle certificate using Edwards-curve Digital Signature Algorithm (EdDSA). In addition, the creation of sub-lists of revoked certificates based on vehicle type makes it possible to minimize the response time by looking for a certificate if it is revoked or not.

The remainder of this paper is organized as follows: the next section details the related works. Section 3 presents the communication architecture of VANET. Section 4 describes several preliminaries used in our solution. In section 5, we propose our secure hierarchical infrastructure. The security of the designed protocol was checked by the verification tool AVISPA, in section 6. Section 7 evaluates and analyzes the performances of the existing protocols as well as our proposition. Finally, we draw our conclusion in Section 8.

2 Related works

Authentication represents an essential cryptographic mechanism that provides confidence between vehicles and infrastructures in Vehicle Ad-hoc Networks.

However, an improved authentication process will effectively detect malicious nodes and then maintain VANET security. Therefore, various authentication mechanisms that ensure protected communication in the network were suggested. In this part, we discuss them briefly.

The basic idea of the technique based on anonymous certificates is given by Raya and Hubaux [5], the authors use anonymous certificates (eg pseudonyms) to hide the real identity of users. The anonymous certificate does not include any information about the real identities of the users, but privacy may be violated because the messages contain an exchanged key which gives the possibility to track the vehicle's true identity.

The group signature is an alternative to achieve security and preserve privacy in VANETs. In this technique, a group manager is responsible for managing the group. The Members may enter or exit the group dynamically. Upon registering and joining a group, a member can sign anonymously on the behalf of the group and the recipient uses the public key to validate the signature but never will know who sent the packet. However, there are exceptional cases where the group manager may reveal the identity of a sender of any group signature. The group signing approach has emerged to overcome the disadvantage of the anonymous certificate technique. The first protocol of this technique to be implemented within vehicle networks is the Group Signature ID-based Signature protocol [6].

The authors of the paper [7] aim to guarantee the identification, authentication, non-repudiation, and integrity of the roadside unit when transmitting messages from RSU to vehicles (I2V). An identification aggregation will be carried out by several RSUs and without the intervention of a trusted third party. Their algorithm first ensures the identification of RSUs by the Elliptic Curve Diffie-Hellman's algorithm verifies that the both nearest RSU possesses the same secret key and the vehicle authenticates the signed message utilizing the Digital Signature Elliptic Curve. The ECDH-ECDSA provides a greater degree of protection even if its aggregation takes roughly 40 ms further than the basic ECDSA method.

The paper [8] presents an Expedite Message Authentication Protocol (EMAP) based Hash Message Authentication Code (HMAC) for vehicular networks. The authors propose a new fast process of revocation checking to minimize the computation process and avoid overhead problems.

A new conception of Public Key Infrastructure (PKI) for the authentication process is proposed in [9]. The authors design an infrastructure PKI based symmetric encryption in order to reduce the treatment time and eliminate overhead for authentication.

Das et al. [10] offer a hierarchical protocol to reach the objectives of scalability and certification in VANET. This protocol built a structure of tree with a hierarchy of Certification Authority (CA) to operate the VANET. Authors suggest two kinds of nodes: the powerful nodes which are the certifying authorities and the leaf nodes are vehicles.

Lightweight Identity Authentication Protocol (LIAP) has proposed in [11] in order to supply a fast mutual authentication between the roadside unit and the vehicle, also to guarantee the vehicle's conditional privacy. This protocol achieves the transfer authentication process by employing a secret dynamic session mechanism and avoids the utilization of the encryption/decryption operations in the roadside unit and the vehicle.

The scheme proposed in [12] constitutes a group of vehicles and RSU through the use of self-authentication without the need of a certification authority, and uses a Group Key (GK) to improve the efficiency of certification, also the protocol selects deniable group key agreement method to avoid attacks into legal vehicles.

The authors in [13] propose a new protocol based on the complexity of two popular mathematical problems to deal with the problems existing in previous Mobile Wireless Networks (MWNs) handover authentication protocols. Security analysis illustrates that the proposed protocol is protected from various threats and can satisfy a number of security requirements. A hierarchical revocable authentication protocol based random oracle model within the Diffie-Hellman (DH) hypothesis is presented in [14]. The evaluation of the protocol shows that it saves highly computation overheads and meets the security requirements.

Our proposal is also aiming to ensure privacy and authentication in vehicular ad-hoc network. The privacy is preserved by ensuring the anonymity. In this study, we use an ECDH algorithm for reliable key exchange and EdDSA Algorithm to speed up the execution of the authentication process especially at the key management level, message signing, and verification of this signature.

3 System model

Vehicular Ad Hoc Network is a highly mobile ad hoc network integrated by ITS in order to improve traffic efficiency, minimize traffic congestion, avoid accidents and make easy access to news, information and entertainment while driving. However, recent research in vehicular networks is exploring all aspects of communication. We distinguish three modes of communication in VANET, which are vehicle to vehicle communication (V2V), vehicle to infrastructure communication (V2I) and infrastructure to infrastructure communication (I2I) [15].

- Vehicle to vehicle communication (V2V) is based on a simple inter-vehicle communication that utilizes the OBUs (On-Board Units) installed on each vehicle to communicate with each other. This communication can be established without fixed infrastructure relays.
- Vehicle to infrastructure communication (V2I) allows better use of shared resources and increases the services provided (for example data exchange, Internet access, remote diagnostics to repair a vehicle, etc.) thanks to access points deployed at the roadside. These access points are named RSU (Road Side Units) and located in certain critical sections of the road, such as traffic lights, or stop signs, in order to enhance road safety and traffic efficiency also to enjoy driving.
- Infrastructure to infrastructure communication (I2I) provides communication between RSUs or between RSU and base station. It increases the communication range and connects all vehicles in the network.

As the range of infrastructure is limited, vehicles can be used as relays to extend this distance and avoid the multiplication of base stations at each corner of the road. Therefore, the combination of the communication modes (V2V, V2I, and I2I) may achieve a very interesting and economical hybrid communication. In order to establish all these communications, VANET consists of three main components (OBU, RSU, and CA) [16] required providing communications in the network (Figure 1).

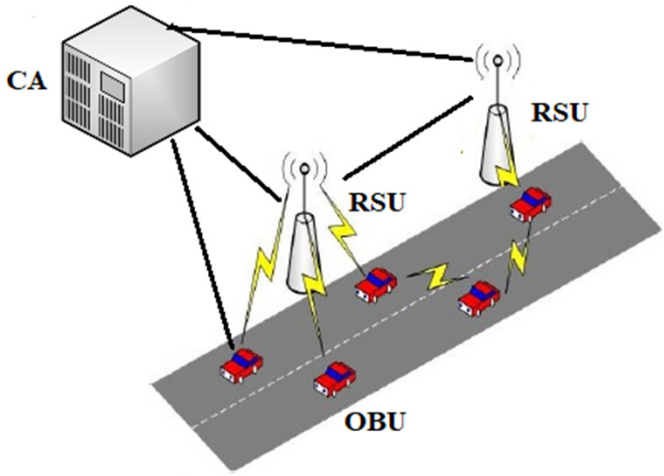

Fig. 1. Network architecture

- On-Board-Unit (OBU) is a sensor mounted in vehicles. This device provides important information to vehicle control units for automatic driving assistance. This on-board unit is used to exchange information with other OBU or with roadside units (RSU). It includes a set of high-tech hardware and software components such as GPS, radar, cameras, various sensors, and others. Its role is to ensure the location, reception, calculation, storage, and sending data over the network.
- Road Side Unit (RSU) is an infrastructure placed along roads, its main role is to inform nearby vehicles by broadcasting traffic conditions, weather, or specific road conditions (maximum speed, overtaking, etc.). They can also play the role of a base station by relaying information sent by vehicles.
- The Certification Authority (CA) represents the trusted authority in VANET. It plays the role of a server which ensures the security of the various services such as the issuing of certificates, keys distribution, and the storage of certain data. Moreover, CA maintains secure management of VANET by verifying the vehicle authentication, the user ID, and the OBU ID in order to prevent any damage to any vehicle.

4 Preliminaries

We present in this section the cryptographic algorithms that we use in our proposed; it is about Elliptic Curve Diffie-Hellman (ECDH) Protocol and Edwards-curve Digital Signature (EdDSA) Algorithm.

4.1 Elliptic curve Diffie-Hellman (ECDH)

Elliptic Curve Diffie-Hellman is a key agreement protocol that allows two entities to create a secret key that will be used for private key operations. The public key created by each entity is shared with the other. The methods on the elliptical curves are

used to generate the secret key. We assume that Alice and Bob agree to a standard key cryptographic protocol for data exchange. It is considered that they had no contact and that the mode of communication available to them through the channel is only public. Both exchange public data or public cryptographic keys. Each of them has a private key used to generate the shared key called a public key. The two individuals agree on the same domain parameters. The steps of this protocol are as follows [17]:

- Alice and Bob choose a common elliptical curve E on a prime field Fp. They also have a base point G € E (Fp) so that the subgroup generated by G has a greater group cardinality. This determines the strength of the method involved.
- Alice chooses an integer a. It is a secret key that is not shared with anyone. This is Alice's private key. It then uses point multiplication and calculates the public key Ta = a.G and sends Ta to Bob.
- Bob also selects an integer b which becomes his private key, calculates Tb = b.G by multiplying points and sends Tb to Alice.
- Alice calculates a.Tb = a.b.G. This is done by multiplying points from Alice's secret key with Bob's shared key.
- Bob multiplies points between his private key and Alice's public key and calculates b.Ta = a.b.G. The only data that a spy can obtain concerns the elliptical curve E, the finite field Fp and the points G, a.G, b.G.

4.2 Edwards-curve digital signature (EdDSA)

Edwards-curve Digital Signature Algorithm is a digital signature method based on the Twisted Edwards curves using a Schnorr signature variant. EdDSA is a signature protocol published in 2011 by Bernstein et al. [18], it was originally intended to be used with the Curve25519 elliptical curve, but may very well be used with any other elliptical curve. A signature constructed from this protocol is a couple (R, s) and is generated from:

E: the parameters defining the elliptical curve used.
P: a point on the high-order curve.
n: the order of point P

The EdDSA key-pair consists of:

- The private key is generated from a random integer, named *seed* (which has to use a similar bit length as a curve order). The seed is first hashed, then the last few bits, corresponding to the curve cofactor are cleared, then the highest bit is cleared and the second highest bit is set.
- The public key *PubKey* is a point on the elliptic curve, calculated by the EC point multiplication: *PubKey* = *PrivKey* * P (the private key, multiplied by the generator point P for the curve).

The algorithms 1 and 2 respectively present the signature and the verification of signatures performed by this protocol.

Algorithm 1. EdDSA Signature

Inputs: the private key a, the associated public key Q, the message m
Outputs: (R, s) the signature associated with m

```
H(a, m) ← hash(a, m)
R ← H(a, m)P
H(R, Q, m) ← hash(R, Q, m)
s ← (H(a, m) + H(R, Q, m)a)[n]
return (R, s)
```

Algorithm 2. EdDSA Verification

Inputs: m a message, (R, s) the associated signature, Q the public key associated with the private key which served to sign the message.
Outputs: returns true if the signature is correct, false otherwise

```
H(R, Q, m) ← hash(R, Q, m)
U ← 8sP
V ← 8R + 8H(R, Q, m)Q
if U ≠ V then
return False
end if
return True
```

We can show that the signature produced by algorithm 1 will be validated by algorithm 2.

$$\begin{aligned} R + H(R,Q,m)\,Q &= H(a,m)\,P + H(R,Q,m)aP \\ &= (H(a,m) + H(R,Q,m)a)P \\ &= sP \end{aligned}$$

5 Proposed scheme

This section presents the description of the phases of our secure hierarchical infrastructure scheme in VANET.

5.1 Protocol description

Our solution takes place in four phases:

- The main authentication phase between the different network entities which allows VANET entities to authenticate with the CA in order to have a public key certificate for use in communication, this phase is executed at using a symmetrical approach in order to secure the authentication packets exchanged. In addition, the EdDSA algorithm for the generation of the Public/Private key pair, the generation of the signature of a message and its verification.
- The second phase is the authentication and communication phase between OBUs and RSUs, where OBUs authenticate for a second time with RSUs for the purpose to have two different keys, the first is a shared secret key for I2V or V2I communication, the other key is used for V2V communication.

- The phase of message exchange between OBUs or V2V communication, using the K_{Gi} group key issued by RSUs to encrypt the messages transmitted, and the use of the private key to sign the hash of the message in order to ensure integrity and non-repudiation, in addition, the use of certificate makes it possible to guarantee the authentication and the identity verification of the sender.
- The last phase is the revocation phase, of which the CA sends a list of revoked certificates to the OBUs. A certificate is revoked in the event that a vehicle declares the theft or loss of its private key or in the event that an RSU suspects the behavior of a vehicle. The vehicle receiving the list of revoked certificates can check the validity of a sender's certificate by searching for it in its list, in our solution we proposed to share the main list of revoked certificates to sublists according to the type (Professional, Private, Personal…) of the vehicle which is a field in the certificate, in order to reduce the response time. When a vehicle searches for a certificate whether it is revoked or not, instead of searching the entire main list, it searches only in the list corresponding to the type of vehicle.

The notations used in our proposed are illustrate in Table 1.

Table 1. The different notations used in the proposed solution

Notation	Description
C_{RSUi}, C_{OBUi}, C_{CA}	RSU_i cookie, OBU_i cookie, CA cookie
KP_{OBUi}	The OBU_i private key
$KPUB_{OBUi}$	The OBU_i public key
Enk et Dek	Encryption and decryption algorithms respectively
Hash	The hash calculated after using the hash function defined in SA
K_{OBUi}	The OBU_i's secret key
K_{CA}	TA's secret key
IDr_{OBUi}	The real OBU_i identifier
ID_{OBUi}	OBU_i pseudo identifier
Sig_{OBUi}	The digital signature of the OBU_i
H	The clock associated with the message to determine its freshness, it is the moment when the message msg is sent
$Cert_{OBUi}$	Vehicle certificate issued by CA
$Type_{OBUi}$	The type of vehicle (Professional, Public, Personal, etc.)
K_{RSUi}	The RSU_i public key
Texp	The lifetime of the certificate
ID_{CA}	The identifier of the certification authority
Sig_{CA}	The certificate signature produced by the CA private key
K_{Gi}	The group key of vehicles belonging to the same RSU_i, used for V2V communications
K_S	The session key issued by the RSU

5.2 Registration phase

In this work, we consider the same registration and authentication process is used for mutual authentication between CA → RSUs and CA → OBU. The vehicle to authenticate and to have a public key certificate must execute a series of steps:

- **Step 1.** $OBU_i \rightarrow CA$: C_{OBUi}, SA_{OBUi}.
  The OBU_i sends a message containing a cookie C_{OBUi} used to confirm that the OBUi is communicating with the CA and SA_{OBUi} presented in SA block that represents the list of algorithms cryptographic supported by OBUi.
- **Step 2.** $CA \rightarrow OBU_i$: C_{CA}, SA_{TA}, ID_{OBUi}.
  After the reception of the first message, CA responds with a message similar to the first message, which contains C_{CA} cookie with the same purpose as C_{OBUi}, SA_{CA} the type of cryptographic algorithm chosen and used in encrypted exchanges and ID_{OBUi} as a session identifier.
- **Step 3.** $OBU_i \rightarrow CA$: C_{CA}, Nonce, $\{I_{OBUi}.P\}$, ID_{OBUi}.
  The OBU_i receiving the message and checks the validity of the C_{OBUi} cookie. The OBU_i and CA agree together and publicly on an elliptical curve E (a, b, K), they choose a finite field K in (Z/pZ) and a curve elliptical and They also choose together, and always publicly, a point P located on the curve. Then the OBU_i chooses an integer I_{OBUi} and sends a message that contains a header C_{CA}, which is the same in the previous message, the point of the elliptical curve $I_{OBUi}P$ and a Nonce as a random for the design of the keys, and ID_{OBUi} its session identifier.
- **Step 4.** $CA \rightarrow OBU_i$: C_{OBUi}, Nonce, $\{I_{CA}.P\}$.
  The CA after reception of parameters and verification of the validity of C_{CA}, it generates an integer K_{CA} and returns a message which contains $I_{CA}P$. At this point, the OBU_i and CA can calculate their secret keys K_{OBUi} and K_{CA}, respectively.

$$K_{OBUi} = I_{OBUi}(I_{CA}P) = I_{CA}(I_{OBUi}P) = K_{CA} = (I_{OBUi}I_{CA})P$$

- **Step 5.** $OBU_i \rightarrow CA$: $Enk_{KOBUi}(C_{OBUi}, IDr_{OBUi}, ID_{OBUi}, Hash\{S1, S2, S3, S4\})$.
  After establishing the secret key, the OBU_i sends a message contains a header C_{OBUi}, a real identifier IDr_{OBUi}, the session identifier ID_{OBUi} plus a hash of the four previous steps using the hash function defined in SA (SHA-256) and all encrypted with the secret key (AES-128).
- **Step 6.** $CA \rightarrow OBU_i$: $Enk_{KCA}(ID_{OBUi}, Hash\{S1, S2, S3, S4\}, KPUB_{CA})$.
  Upon receiving this message and after decrypting it with the CA's secret key, the CA retrieves the IDr_{OBUi} in order to generate a certificate and returns the message with a hash of the four previous messages.
  After checking the fingerprints (the hash) sent by the two entities, these fingerprints must be the same in order to validate and confirm the agreement on the keys and the algorithm to be negotiated, by carrying out an integrity check and authenticating the messages trades. The CA public key is used to verify the signature of the latter in the certificate issued to the OBU_i.
- **Step 7.** The OBU_i requests a certificate from CA in order to communicate with the other entities in the network.

- **Step 8.** CA → OBU_i : $Enk_{KCA}(KPUB_{OBUi}, KP_{OBUi}, SigOBUi, t, Cert_{OBUi})$.
  The CA upon receiving the message of the request, checks the ID_{OBUi}, executes the EdDSA algorithm to generate the public/private key pair and the signature for the OBU_i and sends a message encrypted with its secret key which contains the pair of keys associated with the vehicle, the signature of the vehicle, and the certificate.
  The OBU_i decrypts the message, extracts the key pair, the signature and the certificate and sends a Finished message to the CA indicating the end of the authentication process.
  Upon receipt the previous message, CA sends back a Finished message to confirm the end of the process.

Figure 2 shows the different messages exchanged during the authentication phase.

The CA records in its database the information relating to the OBUi <ID_{OBUi}, IDr_{OBUi}, KP_{OBUi}, $KPUB_{OBUi}$> to use it in the event that a tracking has been launched against a vehicle in bad behavior for example, in order to obtain the true vehicle identity.

The format of a certificate:

$$Cert_{OBUi}: \{ID_{OBUi}, KPUB_{OBUi}, Type_{OBUi}, T_{exp}, ID_{CA}, Sig_{CA}\}$$

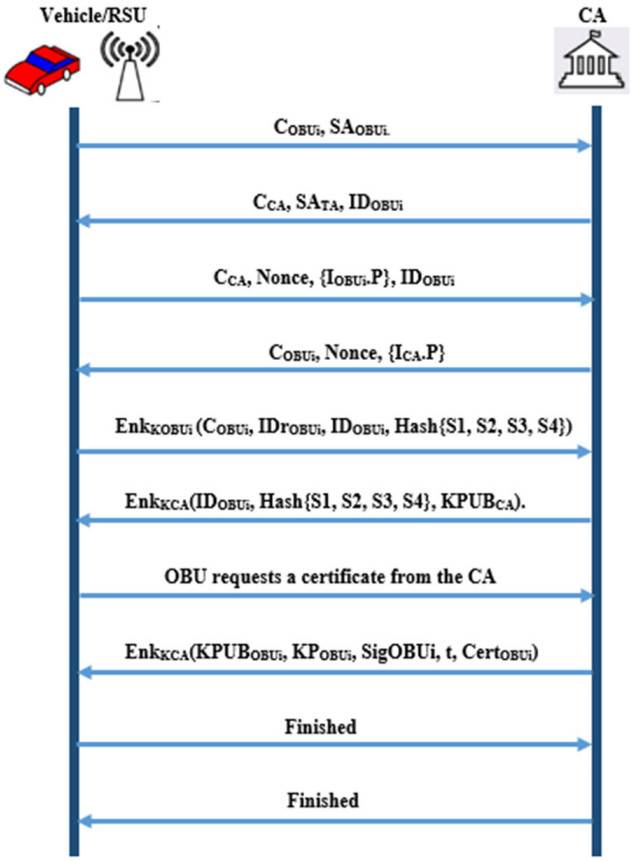

Fig. 2. Registration phase

5.3 Authentication and communication between OBU_i and RSU_i

A vehicle with a certificate issued by the CA can communicate with the other network RSUs, and this can be done after mutual authentication between the OBU_i and the RSU_i (Figure 3).

- **Step 1.** $RSU_i \rightarrow OBU_i$: (ID_{RSUi}, $KPUB_{RSUi}$, $Cert_{RSUi}$)
  The RSU_i periodically broadcasts a message that includes its ID_{RSUi} identity, its K_{RSUi} public key and its CertRSUi certificate issued by the CA, this certificate allows the OBU_i to verify the validity of the RSU_i public key. By intercepting this message, a OBU_i retrieves the public key from the RSU_i and sends a series of authentication and secret key generation messages following the ECDH algorithm.
- **Step 2.** $OBU_i \rightarrow RSU_i$: $Enk_{KPUBRSUi}(C_{OBUi}, I_{OBUi}.P, Cert_{OBUi})$.
  The OBU_i sends a first message containing a C_{OBUi} cookie to fight against DoS attacks and $I_{OBUi}P$ (point of the elliptical curve generated using ECDH algorithm) thus its $Cert_{OBUi}$ certificate issued by the CA.
- **Step 3.** $RSU_i \rightarrow OBU_i$: $(C_{OBUi}, C_{RSUi}, I_{RSUi}.P, [I_{OBUi}.P, I_{RSUi}.P, ID_{OBUi}]Enk_{KPRSUi})Enk_{PUBOBUi}$.
  The RSU_i when receiving the first message from OBU_i, decrypts (C_{OBUi}, $I_{OBUi}.P$, $Cert_{OBUi}$)$KPUB_{RSUi}$ using its private key KP_{RSUi} and checks the validity of the certificate of OBU_i $Cert_{OBUi}$. The RSU_i then sends a message which contains its signature, the C_{OBUi} vehicle cookie and its C_{RSUi} cookie, where the ID_{OBUi} is a pseudo identifier used to protect user privacy.
- **Step 4.** $OBU_i \rightarrow RSU_i$: $(C_{RSUi}, [I_{OBUi}.P, I_{RSUi}.P, ID_{RSUi}]Enk_{KPOBUi})Enk_{KPUBRSUi}$.
  The OBU_i checks the signature $[I_{OBUi}.P, I_{RSUi}.P, ID_{OBUi}]KP_{RSUi}$ using the public key of the RSU_i and checks the C_{OBUi}. If the cookies are different it can directly interrupt the communication because it perceives that it is exchanged with a malicious entity. Otherwise, it continues the exchange by sending his signature $[I_{OBUi}.P, I_{RSUi}.P, ID_{RSUi}]$ KP_{Vi} and the C_{RSUi}. Similarly for the RSU_i, when it receives the message it first checks the C_{RSUi} cookie if it is valid, it decrypts the signature.

At this time, the OBU_i and the RSU_i can calculate the symmetric and shared secret key K_S, used for communications between an OBUi and an RSU_i. In addition to this key, the RSU_i generates another K_{Gi} key for vehicles after successful authentication. This key will allow vehicles to communicate with each other in the same coverage area of the RSU_i.

The RSU_i communicates with neighboring RSUs to obtain their group keys (V2V communication key). At the same time as the delivery of the K_{Gi} key to the Vehicles, it sends the keys of the neighboring RSUs obtained as well as their identifiers (a set of keys). Consequently, the OBU_i will have a list of group keys from neighboring RSUs in addition to that of its RSU_i. When receiving a message from an OBU_j, the OBU_i retrieves the identifier of the RSU_j in order to determine the corresponding key for decryption.

The use of two different keys for I2V communication and V2V communication, ensures confidentiality especially at the level of I2V communication, because the use of a group key causes certain drawbacks, for example, an OBU_i requesting service with an RSU_i encrypts its request with the group key, and in the case that an OBU_j receives this information, it can decrypt the message and know its content, which violates the confidentiality of the message. However, with the use of the secret key, the OBU_i can send a request and only the RSU can decrypt it using its key shared with the OBU_i, thus preserving the concept of confidentiality.

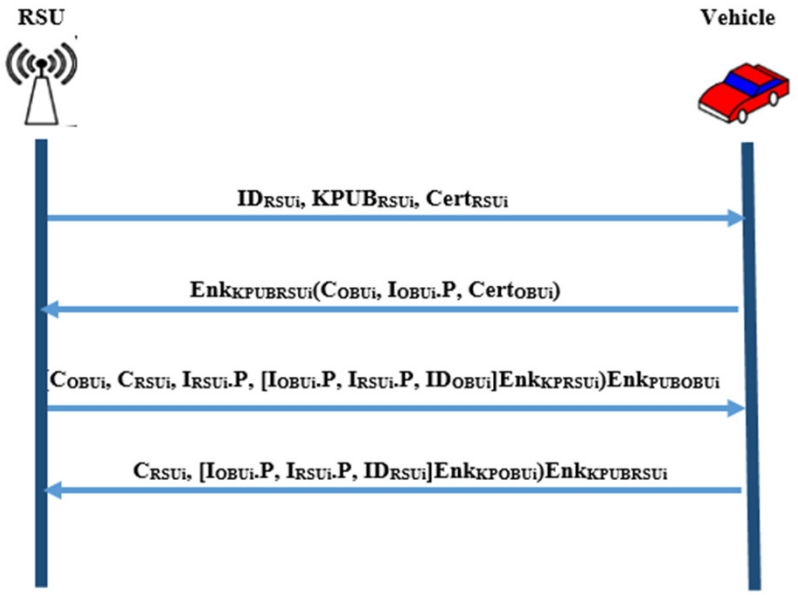

Fig. 3. Authentication and communication between OBU_i and RSU_i

5.4 Communication between vehicles

To send messages to other vehicles, the OBU_i encrypts the message with the K_{Gi} key delivered by its RSU_i, signs the message content using the EdDSA algorithm with its private key and sends its certificate with the adding of a parking meter (Clock) for the message freshness (Figure 4).

$$OBU_i \rightarrow OBU_j: (ID_{OBUi}, Cert_{OBUi}, Data(Msg,h), Sig_{OBUi}(Hash(Data))Enk_{KGi}, ID_{RSUi}$$

When receiving a message, the OBU_j checks the RSU_i identifier, retrieves the corresponding key and decrypts the message with the K_{Gi} key corresponding to the RSU_i identifier. It verifies the sender's signature using the EdDSA algorithm and the time interval between the current moment and the moment when the OBU_i sent the message. This interval must not exceed a predefined threshold (Ex. 300ms). In addition, it checks the validity of the certificate for the current date. If the certificate is not valid, it ignores the message otherwise the message is accepted. The sender's current position can be added to the sent message in order to avoid replay attacks, where message receivers including the RSU can compare between the sender's current position and the position to which he sent the message in order to deduce whether this entity is malicious or not.

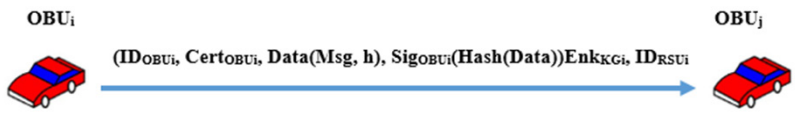

Fig. 4. Communication between vehicles

5.5 Revocation

A vehicle whose behavior is detected to be abnormal, for example misconduct or the sending of false safety messages, etc., is marked malicious. The RSUs are responsible for this task and inform the CA to die whether or not their certificate is revoked. In addition to its behavior, a vehicle may lose its private key, or its key may be stolen. So in these cases, the vehicle certificate must be revoked and registered in the Certificate Revocation List (CRL) revoked certificate list in order to inform the RSUs and vehicles belonging to the VANET. As illustrated in Figure 5.

In this phase, we are proposing a new strategy for managing CRLs, in order to improve the response time to search for the validity of a certificate. We will proceed by dividing the main CRL into several sub-CRLs based on the type cited in the public key certificate. For example, one under CRL for professional vehicles, one under CRL for private vehicles … etc.

When updating these sub-CRLs, the revoked certificate will register in a sub-list according to its type and when an OBU_i wants to verify the certificate it will not need to browse the entire main list, it searches in the sub-list corresponding to the type of OBU_j certificate.

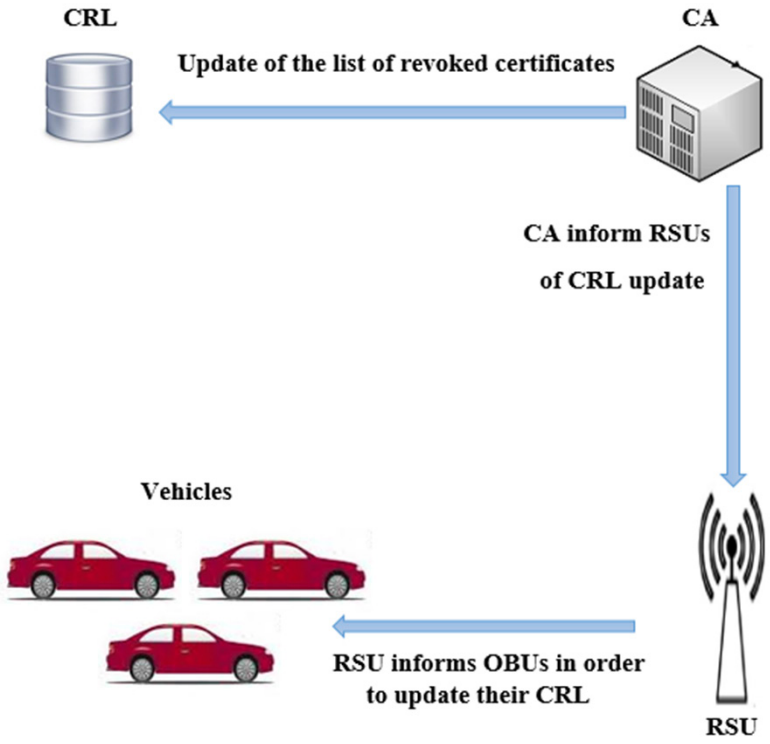

Fig. 5. The different steps of the revocation phase

6 Security analysis

In this section, we analyze the security analysis and the formal verification to illustrate that our model can reach the security objectives and requirements.

6.1 Analysis of security requirements

- **Mutual authentication between the CA and the OBUs and between the CA and the RSUs:** it is ensured by the authentication process where the OBU authenticates with the CA (and the CA authenticates with the OBU) and ensures that the latter is the entity it claims by using cookies, in order to issue a public key certificate for the OBU.
- **Mutual authentication between RSUs and OBUs:** it is carried out in the second phase of the solution, where OBUs and RSUs exchange a series of messages in order to authenticate each other and obtain a secret key, this secret sharing is carried out using the ECDH algorithm.
  In addition to this key, the RSU generates a group key K_{Gi} for all the OBUs in its zone, which is used for V2V communication.
- **Negotiating and choosing a cryptographic policy:** it allows an algorithm to be easily excluded in the event of vulnerability, in order to replace the cryptographic policy used by a new policy supported by the two entities. To remedy the vulnerability of an algorithm, we can define a duration during which a user can authenticate, and in case the defined threshold is exceeded we will change the cryptographic policy used.
- **Confidentiality of authentication packets:** our solution ensures the confidentiality of authentication packets, by encrypting them using the secret key shared between OBUs and CA.
- **Protection against replay attacks:** the use of nonce as random events in order to ward off replay attacks, where the malicious replaying entity cannot be able to calculate shared secrets.
- **Protection against Denial of Service (DoS) attacks:** the use of cookies allows our solutions to remedy denial of service attacks. Malicious OBUs generally start by spoofing the addresses of other OBUs, then massively sending authentication requests in order to exhaust CA resources, or using the latter as an amplifier or attack relay to OBUs from which they initially usurped their address. Therefore, the exchange of cookies during the authentication phase is essential, so that the CA server does not reserve its resources, only if, the OBU returns the CA cookie, to confirm that it is in use. exchange with the alleged entity, which limits this type of attack.
- **The confidentiality of the exchanged packets:** is ensured by encrypting the exchanges with the secret key K_S in V2I or I2V communications and with the group key K_{Gi} in V2V communications.
- **Non-repudiation:** the signature makes it possible to verify the identity of the sender of this fact, each message exchanged in the VANET must be signed with the private key of the sender. This key is generated by the CA and OBUs after successful authentication, the verification of this signature is done with the sender's public key and the use of the EdDSA algorithm. Signing allows the receiver of a message to authenticate the identity of the sender and to ensure non-repudiation.
- **Privacy Preservation:** the use of pseudo identifiers or real vehicle identifiers allows users to preserve their private lives by exchanging messages anonymously. These pseudo identifiers are issued by the CA during the authentication process.

- **Availability:** DoS attacks aim to exhaust the resources of a server and make the server inaccessible, the use of cookies makes it possible to counter these types of attacks and therefore to ensure server availability.
- **Integrity:** the hash functions ensure data integrity, in our solution, the hash of the four messages sent in step 5 and step 6 messages makes it possible to verify the integrity of these exchanges.

6.2 Formal verification

We used the AVISPA (Automatic Validation of Internet Security Protocols and Applications) [19] tool to provide a formal modular and expressive language to specify the protocols and their security properties. It integrates different back-end which uses a variety of automatic machine analysis techniques namely, On-the-fly Model-Checker (OFMC), CL-based Attack Searcher (CL-AtSe), SAT-based Model-Checker (SATMC) and Tree-Automata-based Protocol Analyzer (TA4SP).

The primary goal of our proposed scheme is to verify that it can provide a reliable key exchange between the entities of the VANET in order to secure the registration, authentication, and data transfer phases by using back-end servers.

After running this specification with OFMC and CLAtSe backends, we can conclude that the proposed scheme can accomplish our goal and can resist those malicious attacks, such as replay attacks, secrecy attacks, and DoS attacks under the test of AVISPA. The outputs of the model checking results are shown in Figure 6.

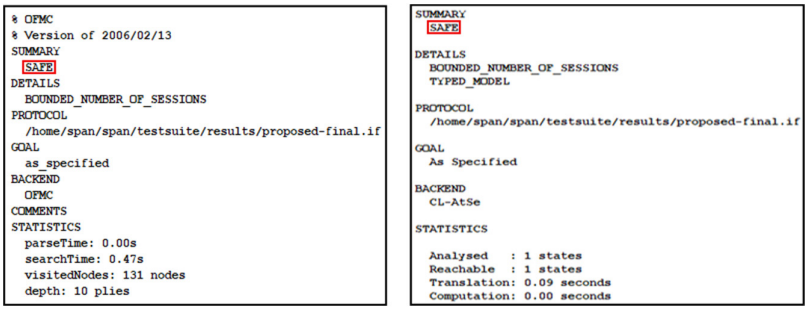

Fig. 6. Results reported by the OFMC and CL-AtSe back-ends

7 Performance evaluation

This section evaluates the performances of our authentication protocol with other existing protocols according to security and computation overhead.

7.1 Comparison of security performance

We have compared the security protocols performance of existing authentication protocols with our protocol. As shown in Table 2, the proposal can provide the most comprehensive security performance and check the security level.

Table 2. Security performance comparison

Security Features	[10]	[11]	[12]	[13]	[14]	Proposed Scheme
Mutual authentication	No	Yes	Yes	Yes	Yes	Yes
Provides message confidentiality	No	No	Yes	Yes	Yes	Yes
Provides message integrity	No	No	Yes	Yes	Yes	Yes
Providing non-repudiation	No	No	Yes	No	No	Yes
Privacy Preservation	No	Yes	No	Yes	Yes	Yes
Resistance against the DoS attack	No	No	No	No	No	Yes
Resistance against the replay attack	No	Yes	No	Yes	Yes	Yes

7.2 Computation overhead

This part evaluates the computation cost required by related protocols and our scheme, in this context we choose to use the rational arithmetic C/C++ library (MIR-ACL) [20] installed on a computer with a 3.2G HZ CPU and 8G of memory in order to calculate the execution time of such single operations using in existing and proposed protocols [21]. Table 3 illustrates the operations and their computation overheads.

Table 3. Computation overhead of single operation

Operations	Description	Time (ms)
PM	Point Multiplication	2.258
BP	Bilinear Pairing	6.443
H	Hash (SHA-256)	0.021
EXP	Exponentiation in Bilinear Group	3.212
ENC	AES-128 Encryption	0.902
DEC	AES-128 Decryption	7.357
MM	Modular Multiplication	1.657
MP	Modular Square Root	2.942
MTP	Map-to-Point Hash Function	2.258
SING/VER	Signature/Verification EdDSA	3.21

The overheads are the sum of the time consumed on both the vehicle and the RSU's side. Table 4 indicates the operation numbers of the computation overheads for the existing protocols [12–14] and the proposed protocol. We demonstrate the computation cost for OBU and RSU in Figure 7. It is observed that the proposed protocol is faster than the protocols adopted in [12–14], the reason is that the choice of lightweight operations to make the mutual authentication.

Table 4. Comparison of computation overheads

Protocols	Operation Numbers		
	Vehicle's Side	RSU's Side	Total (ms)
[12]	PM + 2MTP + 5BP	2BP + 4MTP	48.352
[13]	4PM + 5H + 2EXP	3BP + 5H + 2EXP	41.419
[14]	7PM	7PM	30.95
Our	2ENC + DEC + SING/VER + 2PM	ENC + 2DEC + SING/VER + PM	27.971

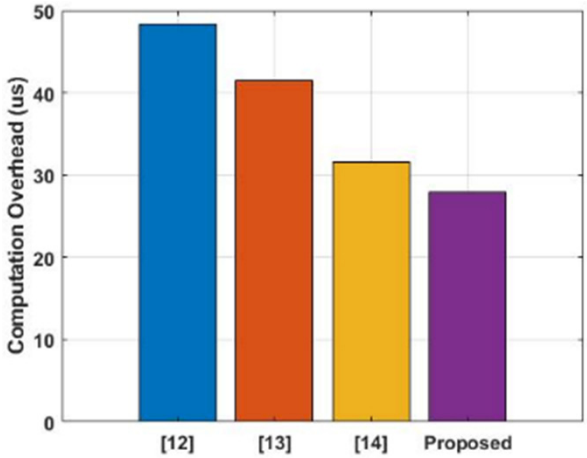

Fig. 7. Computation cost of different schemes

8 Conclusion

The security of vehicular networks is a prerequisite for their deployment, the fact that these networks are a category of wireless networks and the importance of the information exchanged which can endanger the lives of users, the security of these networks does not stop to receive particular interest from research communities in academic and industrial circles. Among the problems that have arisen in these networks is the problem of privacy preservation of users. Our solution allows vehicles (OBUs) and RSUs to authenticate with the certification authority so that they are legal entities in the network. This authentication faces attacks such as denial of service attacks and replay attacks using cookies and nonce, respectively. In addition, double authentication between OBUs and RSUs makes it possible to minimize access to malicious entities in the network. Also, the use of a symmetric key during V2I and V2V communication makes it possible to reduce the calculation time and the verification time compared to other protocols using the asymmetric approach. The use of the EdDSA algorithm makes it possible to speed up the execution of the authentication process, especially at the level of key management, message signature, and verification of this signature. On the

other hand, the creation of sub-lists of revoked certificates based on vehicle type makes it possible to minimize the response time by looking for a certificate if it is revoked or not. In summary, our solution ensures basic security requirements such as integrity, confidentiality, non-repudiation, and availability, as well as the preservation of users' privacy by using the real identifier.

9 References

[1] S. Chavhan, D. Gupta, B.N. Chandana, A. Khanna, and J.J. Rodrigues, "IoT-based context aware intelligent public transport system in a metropolitan area," *IEEE Internet of Things Journal*, vol. 7, no 7, pp. 6023–6034, 2019. https://doi.org/10.1109/JIOT.2019.2955102

[2] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommun. Syst*., vol. 50, no. 4, pp. 217–241, 2012. https://doi.org/10.1007/s11235-010-9400-5

[3] M. Houmer, M. Ouaissa, M. Ouaissa, and M. Hasnaoui, "SE-GPSR: Secured and enhanced greedy perimeter stateless routing protocol for vehicular ad hoc networks," *International Journal of Interactive Mobile Technologies (iJIM)*, pp. 48–64, 2020. https://doi.org/10.3991/ijim.v14i13.14537

[4] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors*, vol. 19, no. 16, 3589, 2019. https://doi.org/10.3390/s19163589

[5] M. Raya, A. Aziz, and J.P. Hubaux, "Efficient secure aggregation in VANETs," In Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks, pp. 67–75, 2006. https://doi.org/10.1145/1161064.1161076

[6] X. Lin, X. Sun, P.H. 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. https://doi.org/10.1109/TVT.2007.906878

[7] A. Bendouma and B.A. Bensaber, "RSU authentication by aggregation in VANET using an interaction zone," In Proceedings of IEEE International Conference on Communications (ICC), pp. 1–6, 2017, IEEE. https://doi.org/10.1109/ICC.2017.7997017

[8] V. Vijayabharathi and P.S.K. Malarchelvi, "Implementing HMAC in expedite message authentication protocol for VANET," In Proceedings of International Conference of Information Communication and Embedded Systems (ICICES), pp. 1–5, 2014, IEEE. https://doi.org/10.1109/ICICES.2014.7033753

[9] S.C. Sakhreliya and N.H. Pandya, "PKI-SC: Public key infrastructure using symmetric key cryptography for authentication in VANETs," In Proceedings of IEEE International Conference Computational Intelligence and Computing Research (ICCIC), pp. 1–6, 2014, IEEE. https://doi.org/10.1109/ICCIC.2014.7238326

[10] A. Das, D.R. Chowdary, and A. Rai, "An efficient cross authentication protocol in VANET hierarchical model," *Int. J. Mob. Adhoc Netw*., vol. 1, no. 1, pp. 128–136, 2011.

[11] J. S. Li and K.H. Liu, "A lightweight identity authentication protocol for vehicular networks," *Telecommunication Systems*, vol. 53, no. 4, pp. 425–438, 2013. https://doi.org/10.1007/s11235-013-9706-1

[12] M. Han, L. Hua, and S. Ma, "A Self-Authentication and Deniable Efficient Group Key Agreement Protocol for VANET," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 7, pp. 3678–3698, 2017. https://doi.org/10.3837/tiis.2017.07.021

[13] D. He, D. Wang, Q. Xie, and K. Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," *Science China Information Sciences*, vol. 60, no. 5, 052104, 2017. https://doi.org/10.1007/s11432-016-0161-2

[14] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in VANET," *IET Information Security*, vol. 14, no. 1, pp. 99–110, 2019. https://doi.org/10.1049/iet-ifs.2019.0249

[15] A.K. Goyal, G. Agarwal, and A.K. Tripathi, "Network architectures, challenges, security attacks, research domains and research methodologies in VANET: A survey," *International Journal of Computer Network and Information Security*, vol. 10, no. 10, pp. 37–44, 2019. https://doi.org/10.5815/ijcnis.2019.10.05

[16] N. Kaibalina and A.E.M. Rizvi, "Security and privacy in VANETs," In Proceedings of IEEE 12th International Conference on Application of Information and Communication Technologies (AICT), 2018, pp. 1–6, IEEE. https://doi.org/10.1109/ICAICT.2018.8747100

[17] A.P. Fournaris, I. Zafeirakis, C. Koulamas, N. Sklavos, and O. Koufopavlou, "Designing efficient elliptic curve Diffie-Hellman accelerators for embedded systems," In IEEE International Symposium on Circuits and Systems (ISCAS), 2015, pp. 2025–2028, IEEE. https://doi.org/10.1109/ISCAS.2015.7169074

[18] D.J. Bernstein, S. Josefsson, T. Lange, P. Schwabe, and B.Y. Yang, "EdDSA for more curves," Cryptology ePrint Archive, 2015.

[19] AVISPA Project, http://www.avispa-project.org/

[20] MIRACL Library, http://www.shmus.ie/index.php

[21] P. Wang, Y. Liu, and S. Lv, "An improved lightweight identity authentication protocol for VANET," *Journal of Internet Technology*, vol. 20, no. 5, pp. 1491–1504, 2019.

10 Authors

Soukayna Riffi Boualam is currently a Professor at Specialized Institute of Applied Technology. She received her engineer's degree in Network and Telecommunications in 2016. She is a PhD student at ENSA, Sidi Mphammed Ben Abdallah University Fez, Morocco. Her research interests include Network, Telecommunications, Internet of Things and Routing Protocols.

Mariyam Ouaissa is a Professor/Trainer and Researcher Associate. She is a Ph.D. in Computer Science and Networks graduated in 2019, at the Laboratory of Modelisation of Mathematics and Computer Science, from Moulay Ismail University, ENSAM, Meknes, Morocco. She is a Networks and Telecoms Engineer, graduated in 2013 from National School of Applied Sciences Khouribga. Her main research topics are IoT, M2M, WSN, Vehicular Networks, Cellular Networks. She is mainly working on M2M congestion overload problem, security and the resource allocation management. She has published more than 20 research papers. She is a Editor in several books (Springer, De Gruyter, RGN Publications …) and Guest Editor in several special issues of journals (IGI Global, River Publishers, EAI Publisher, RGN Publications …).

Mariya Ouaissa is currently a Professor at Institute Specializing in New Information and Communication Technologies, Researcher Associate and practitioner with industry and academic experience. She is a Ph.D. graduated in 2019 in Computer Science and Networks, at the Laboratory of Modelisation of Mathematics and Computer Science from ENSAM-Moulay Ismail University, Meknes, Morocco. She is a Networks and Telecoms Engineer, graduated in 2013 from National School of Applied Sciences Khouribga, Morocco. Dr. Ouaissa has made contributions in the fields of information security and privacy, Internet of Things security, and wireless and

constrained networks security. Her main research topics are IoT, M2M, D2D, WSN, Cellular Networks, and Vehicular Networks. She has published over 20 papers (book chapters, international journals, and conferences/workshops), 8 edited books, and 5 special issue as guest editor.

Abdellatif Ezzouhairi received the M.Sc and the PhD degrees in Mobile computing from Ecole Polytechnique Montreal Canada. He worked as an adjunct researcher at the Mobile Computing and Networking Research Laboratory (LARIM) Chair Ericsson Canada. He is now a Professor at ENSA Fez Morocco. His interests: NGN integration, mobility and sensor/MANET.

Article submitted 2022-04-08. Resubmitted 2022-05-13. Final acceptance 2022-05-13. Final version published as submitted by the authors.