Formally Validated of Novel Tolling Service With the ITS-G5

Malalatiana Randriamasy, Adnane Cabani, Houcine Chafouk, Guy Fremont

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 20, 2019, accepted March 5, 2019, date of publication March 21, 2019, date of current version April 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2906046

Formally Validated of Novel Tolling Service With the ITS-G5

MALALATIANA RANDRIAMASY[1,2], ADNANE CABANI[1], HOUCINE CHAFOUK[1], AND GUY FREMONT[2]

[1]Normandy Univ, UNIROUEN, ESIGELEC, IRSEEM, 76000 Rouen, France
[2]Sanef, 92130 Issy-les-Moulineaux, France

Corresponding author: Malalatiana Randriamasy (malalatiana.randriamasy@sanef.com)

This work was supported in part by the French Road Operator SANEF and the laboratory IRSEEM-ESIGELEC. Also, it is under contract with the National Agency for Research and Technology (ANRT) under Contract 2015/1248; it has connections with the SCOOP@F project, which is co-funded by the European Commission under the CEF Programme.

ABSTRACT The arrival of the connected and/or autonomous cars offers countless opportunities for both the user and service provider. In this paper, we present a novel solution for tolling transaction using ITS-G5 technology. Specifically, it investigates how to secure tolling transactions performed with the cooperative intelligent transportation system (C-ITS) equipment and the tolling server as a trusted party. In this novel solution, we consider ITS components using the ITS-G5 technology with features specified by the European Telecommunication Standardization Institute (ETSI): RoadSide Unit (RSU), On-Board Unit (OBU), and the standardized architecture of the Electronic Fee Collection by the International Organization for Standardization (ISO). To perform the tolling transaction, a point-to-point protocol must be established between the RSU of the infrastructure and the OBU embedded in the vehicle. Therefore, we design an efficient architecture that ensures the security of exchanges is guaranteed by the security back office of the tolling server as a trusted party. From the application to the service and until its usage, some security requirements are verified: mutual authentication between all entities involved in the transaction, confidentiality, integrity, and non-repudiation of all exchanged information. The certificate usage combined with the signature process certifies the mutual authentication between each entity: the OBU with the RSU, the payer with the service provider and the RSU with the tolling server. The encryption of the messages and the verification of the signatures ensure the confidentiality, the integrity and the non-repudiation of all exchanged information. The safety and efficiency of the proposed method are validated through its formal verification using the security protocols verifier tool AVISPA (Automated Validation of Internet Security Protocols and Applications). Furthermore, the proposed architecture requires reasonable resources which will be suitable for vehicle-to-infrastructure (V2I) communications.

INDEX TERMS C-ITS, ETC, secure transaction, ITS-G5.

I. INTRODUCTION

Recent research in Intelligent Transportation System focuses on different possible use cases. Among them are the point-to-point communication between the service provider and the customers. In fact, many researches have been done and yet it is still in the process to enhance the transportation safety and to improve its related services. In this paper, we deal with the payment application with Cooperative Intelligent Transportation System (C-ITS) equipment, more specifically to exchange the Electronic Toll Collection transaction (ETC Transaction) between the RSU of the infrastructure and the OBU embedded in vehicles.

With this prospect of deployment of C-ITS in cars and on European roads, Sanef, a toll motorway operator in France, is involved in many national and European projects that aim to deploy the suitable infrastructure to welcome connected and autonoumous cars. So, one use case that can be considered is a new mean to collect toll fees on highways for the connected vehicles.

To perform the ETC system with the C-ITS equipement, it involves two main requirements: ensuring that the vehicle

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

is crossing the toll gantry or the lane, and securing the transfer of the tolling information. The first issue is dealt in our previous works [1], [2]. These works propose a method using the Kalman filtering and the Extended Kalman Filtering according to the linearity state of the kinematic model of the vehicle. In this paper, we mainly focus on our proposed approach to address the issue of the security of the transaction with the ITS-G5 technology. We propose a new secure architecture for payment application dedicated to the connected vehicles based on three main actors: RSU, OBU and the security back office of the tolling server. It guarantees mutual authentication between all entities involved in the transaction along with confidentiality, integrity and non-repudiation of all exchanged information, while considering the privacy of the drivers identities, and preventing attacks. We validate the proposed architecture as robust and secure algorithm through its formal verification using HLPSL (High-Level Protocol Specification Language).

To do, the document is organized as follow: In Section II, the context of this research is addressed by reminding the ETC system architecture [3], a brief state of art of the C-ITS and some security solutions dedicated to electronic payment. In section III, the motivation of this subject is discussed. In Section IV, we will present our method to address the issue of payment over-the-air according to our context. In Section V, we will present the process of formal validation of our method with AVISPA/SPAN tool and discuss about the advantages of this proposed approach. Conclusions and future work are given in Section VI.

II. CONTEXT OF THIS RESEARCH

A. ETC SYSTEM ARCHITECTURE

Electronic toll collection first appeared in the early eighties, in the United States (Texas) and in Europe (France in 1985, Norway in 1986, etc). The European Committee for Standardization - Dedicated Short Range Communication (CEN DSRC)[1] standard is applicable in Europe to perform this service. It occurs in the frequency band from 5795 to 5815 MHz. Figure 1 illustrates this frequency band allocation in the 5GHz band, with that of the ITS-G5 technology.

To understand how does it operate, let remind the ETC architecture model established in [3].

[1]DSRC in Europe has a different meaning than in the US.

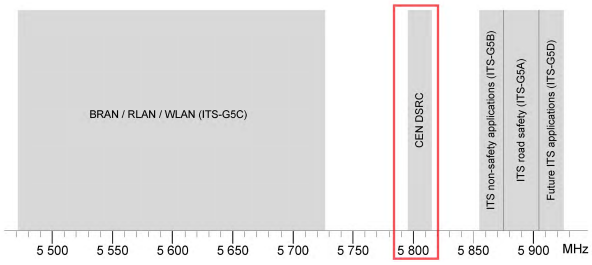


FIGURE 1. Channel allocation for the 5 GHz frequency range [4].

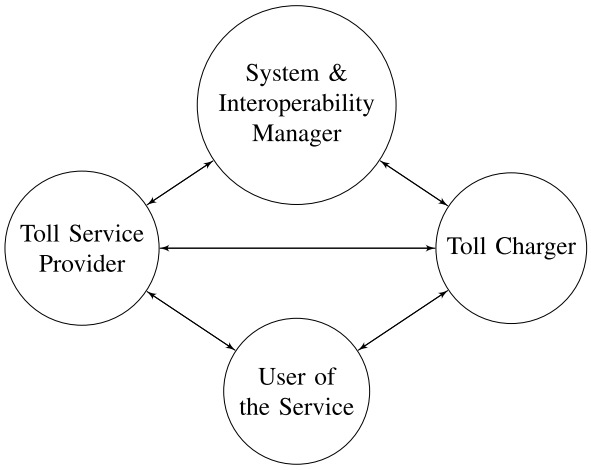


FIGURE 2. The EFC role model [3].

According to the model illustrated on Figure 2:

- The System & Interoperability Management includes the government authority of a local or of any state in case of an interoperable EFC system. It defines only the legal framework i.e. defines, maintains a set of rules of the policy of the toll collection.
- The Toll Service Provider (or Service Provision) establishes and maintains direct business relationships with all relevant Toll Chargers on behalf of the Service User and provides to the users the OBU (On-Board Unit) with the tolling application and ensures that this latter is operating correctly.
- The Toll Charging group includes all owners of road networks. The toll charging operates the toll system and may provide transport services. In France, that is the Sanef's role.
- The User of the service is the client of the Service Provision. The user does not need to procure separate tolling services for each individual Toll Charging network. A Toll Service Provision integrates all tolling services.

In France, we can distinguish the ETC system with the stop-and-go scenario and the non-stop mode with reduced speed for the majority of tolls. For these ETC with barriers, when the driver crosses the tollgates, different means of payment are provided by the motorway operator to collect toll fees: by cash, by electronic payment card, by phone through the NFC [2] or bluetooth technology [5], by DSRC equipment. For all these means, the suitable system to validate the ETC transaction is deployed in every lane. For example, for the DSRC system, in each lane, there is a DSRC beacon that can detect the vehicle in front of the tollgate with the On-Board Unit (OBU) which is placed on top of the windshield, and then perform the transaction.

As we can see in the Figure 3, only the vehicle in the coverage of the radiation pattern of the DSRC beacon can

[2]Near Field Communication

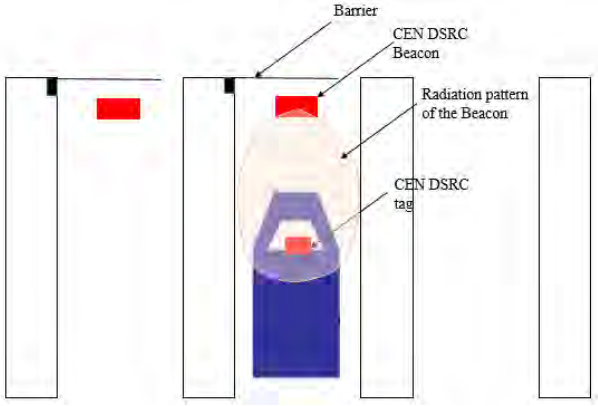


FIGURE 3. ETC system with barriers.

TABLE 1. Frequency allocation in the european union [4].

	Frequency Width [MHz]	Usage
ITS-G5D	5905 - 5925	Future ITS applications
ITS-G5A	5875 - 5905	ITS road safety related applications
ITS-G5B	5855 - 5875	ITS non-safety applications
ITS-G5C	5470 - 5725	RLAN (BRAN, WLAN)

communicate with this latter through the DSRC tag. For other ETC system using Automatic Vehicle Identification with RFID technology [3]or Automatic Number-Plate Recognition (ANPR) the same situation is found [6], [7].

B. COOPERATIVE INTELLIGENT TRANSPORTATION SYSTEM (C-ITS)

In Europe, the 5GHz frequency band is allocated for V2X communications to enable short-range and low-latency C-ITS communications. The ITS-G5 technology is based on IEEE 802.11p specifications. The table below details the frequency allocated for C-ITS in Europe.

The ITS road safety applications use the frequency band defined by ITS-G5A, with the Control Channel (CCH). The other services will use the other chanel, like Service Channel (SCH). Currently, the ITS-G5 technology permits the broadcast of the traffic messages (CAM: Cooperative Awareness Message) [8] and the events messages (DENM: Decentralized Environmental Notification Message) [9].

Other use cases are studied to ensure road safety and related services. So according to the use cases, other messages and communication profiles are specified or under reviewing, e.g. the communication system for the planning and reservation of EV energy supply using wireless network [10].

For our use case dedicated to perform specific services, the SAEM (Service Announcement Message) message [11] has been defined by ETSI organization. So, to ensure the security of communication between ITS stations, in the recents European projects like SCOOP@F or InterCor, a Public Key Infrastructure (PKI) was created according to [12]–[14] related to the broadcasting of CAM and DENM. Some results from ISE project [15] are applied in these projects.

C. SECURITY SOLUTIONS DEDICATED TO ELECTRONIC PAYMENT

With the current situation, the usage of E/M-payment[4] will reach near 726 billion transactions in 2020s according to study reports in [16]. We are facing a growing trend of using bank cards, more and more with smartphones, virtual currencies and under studies with connected objects [17]–[19].

In VANET, many studies investigate on the practices to better secure communications [20]–[22]. Indeed, wireless communications are facing numerous constraints and attacks. In [23]–[25], we can enumerate some frequent situations that face and threaten the security of wireless systems for instance attacks from insider with authorized system access. To overcome this type of attack, the trust in specific services will be established with at least the application of authentication, non-repudiation and integrity protocols.

If we have a look on the adopted method used for E/M-payments, the latest recommanded protocol is the EMV 3D-secure 2.0 (3DS 2.0), the details of this later are described in [26]. The principle ensures that the 3 domains involved in the transaction are authenticated. Let remind that the 3 domains are: the acquirer domain (the merchant and his bank), the issuer domain (the client and his bank) and the interoperability domain. In this latter, the transaction can be initiated by mobile devices or by connected equipment.

According to the context of VANET[5] and objectives of organizations specialized in security of financial transaction, it highlights the needs to authenticate all entities involved in the transactions. It permits to established a mutual trust among them while guaranteeing a positive user experience. Indeed, as a toll charger, the proposed system have to ensure that only the provided service will be billed to the clients through the service provider.

III. MOTIVATION OF THE SUBJECT

A. NOVEL TOLLING CONFIGURATION

In this vision to perform the ETC service with the ITS-G5 technology, the entities involved in the system are the connected device embedded in vehicle named the OBU and the RSU of the infrastructure. Both of them use the ITS-G5 technology. In fact, in the coming years, millions of vehicles will include a powerful communication system that will provide them with new safety and mobility services.

The real challenge for this service is to use just one RSU to interoperate with all the connected vehicles in the toll area.

[3]Radio Frequency Identification

[4]E/M-payment: electronic/mobile - payment for commerce, not mainly through the web but also through mobile devices and internet of things

[5]VANET: Vehicular Ad-hoc NETwork

So, the RSU has to ensure both a reliable vehicle location to validate the transaction in the right lane, and a secure communication during the transactions. The issue of vehicle location is already dealt in [1] and [2]. In this paper, we mainly address the security of communications issue between the RSU with the role of Toll Charger and the OBU embedded in the vehicle linked to a subscriber account.

The Figure 4 shows that the RSU handles communications between each connected vehicles to validate the transaction. Note that the range of communication for both RSU and OBU is about 1000 meters. So the transaction can occur some meters before the toll gate to avoid stopping (in case of stop-and-go situation). Therefore, it appears very important to secure the communication to avoid wireless network attacks like the eavesdropping, Man-in-The-Middle attacks, etc. In [27]–[30] they highlighted all relevant attacks for VANET and proposed some solutions to identify the measures needed to address deficiencies of the system.

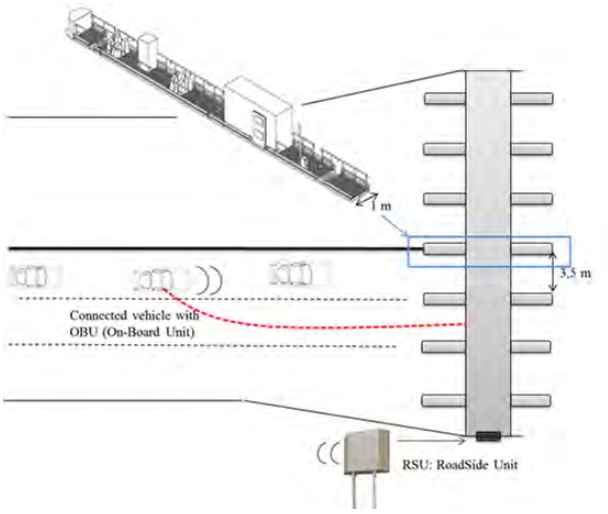


FIGURE 4. ETC system with C-ITS equipment.

For the proposed method, to limit the risks of attacks in this kind of over-the-air service and to prevent from them, we satisfy some requirements of security: ensure the integrity of the exchanged data, the authentication of each entity (subscriber, OBU, RSU, Service Provider), the non-repudiation of every action and the confidentiality.

To secure this kind of service, the following formula sums up the basis of our approach:

$$Risks = Threats \times Vulnerabilities \times Impact \quad (1)$$

Through this equation, despite of threats, we have to act preventively to mitigate it to reduce impact of risks to an acceptable level.

B. RECOMMENDED SECURITY PROPERTIES OF THE TOLLING APPLICATION USING THE ITS-G5 TECHNOLOGY

Obviously, the user will be convinced according to the reliabity of the service. The design of the secure architecture of the tolling service with the ITS-G5 technology is built under the recommandation of the standard ISO/IEC 27001 [31] added with some requirements adapted to the context of payment with C-ITS.

In this standard [31], it mainly recommends the compliance to the ISMS (Information security management system). First, it consists in the application of the D.I.C.T. rules:

- Disponibility [D] or Availability: Information is said to be available when it is accessible and usable under specific conditions (authorized entities, etc). The unavailability of information may be due to its destruction or erasure, or to a malfunction of the equipment, services or processes supporting it.
- Integrity [I]: Integrity of information ensures that it is not modified in an undesired or uncontrolled manner. Integrity guarantees the completeness, accuracy and technical adequacy of the information.
- Confidentiality [C]: Only authorized persons can access to required ressources, treatments or equipment. We have to comply with the GDPR (General Data Protection Regulation) recommendation for the confidentiality of personal data (according to the Data-processing Law n° 78-17 of 6th January 1978 supplemented by the Law n° 2018-493 of 20th June 2018). Indeed, the confidentiality can be expressed as another safety factor to preserve anonymity, as we can see on the security protocol for road safety communication [12].
- Traceability [T]: Traceability is the fact of having elements to provide evidence of processing carried out in relation to a resource: typically the traceability of the treatments, their date, how they were done, and the entity responsible for the treatment. The traceability will permit to exploit these collected logs, for instance to search for causes of system incidents.

Added to these requirements, we consider these following criteria as important conditions to fullfill:

- Authentication: here our architecture proposes an authentication in every level: not only for the client but also for the RSU of the infrastructure and the back office (BO) of the service provider. Later in the document, as a notation, we will designate this BO of the service provider as *server*.
- non-repudiation: indeed, because of payment service, every transaction will be validated as proof of act (crossing the toll area).
- managing the personal data: due to exchange of state message to perform the transaction, it is crucial to define the scope of the use of these data, the conditions of storage of these latter. For our case, we dealt in [1] and [2] the reasons we use it.

IV. PROPOSED METHOD

The proposed method to ensure secure communication to perform the ETC service influences on every stages: the installation of the tolling application on the OBU, subscription of the

user to the service provider and mainly during the crossing of the toll area. Indeed, the critical exchanges take place between the RSU and the OBU through a secure channel protected with the TLS protocol through the ITS-G5 technology.

A. SUBSCRIPTION & REGISTRATION

For the future road tolling with the ITS-G5 technology, the vehicle equipped with the tolling application can be driven by its owner or/and also by different peoples (e.g.: rental car, etc.). So one of the requirements to use the service is that the payer entity should be subscribed with an ETC Service Provider. This subscription shall give access to the service on the whole of the countries that contract the interoperability of the concerned service. Then, he connects with his account on the toll application of the vehicle.

- During the user subscription, the user defines the process for him to connect to the toll application (E.g.: login/password, fingerprint, etc.). By saving these information, the back office of the security part of the Toll Service Provider generates the certificate associated to this subscriber and the relative public key. Then, when connecting the account the private key relative to the public key associated to the certificate will be computed and stored carefully. Indeed, it is not recommended to transmit the private keys to keep them safe: they need to be stored and handled carefully, and no copies should be distributed.
- Also, the RSU dedicated to perform the service should be registered to the back office of the security part of the toll service provider. For the registration of the RSU, the UID[6] of the road operator and the toll station where will be installed the RSU should be provided. For the RSUs of the same road operator, the certificate with key pair can be the same to better optimize resources in the OBU. For the registration of the OBU, it will occur during the installation of the tolling application in the vehicle system. The car registration number or/and the Unique Identifier (UID) of the ITS equipment should be provided. By saving these information, the back office of the security part of the Toll Service Provider delivers the certificate with the associated public key to the ITS station.
- Then the ITS station will compute and store the private key associated to the public key of the delivered certificate. It is recommended to use a specific container like SSM (Software Secure Module) or HSM (Hardware Secure Module) to store the private key and to perform the cryptographic signature process.
- When the payer entity connects his account to the toll application of the vehicle (by introducing login/password or/and fingerprint) with the car registration number, the OBU will sign this information with its private key. Then, it will be sent to the security part of the Toll Service Provider in order to be checked. By this way, both the OBU and the payer entity are authenticated and associated when crossing the toll area. After the validation of credentials information, the back office will send the certificate and public key associated to the payer entity, the public key of his service provider and all the public keys of the RSU of all road operators in order to be able to communicate and to authenticate them later.

[6]UID: unique Identifier

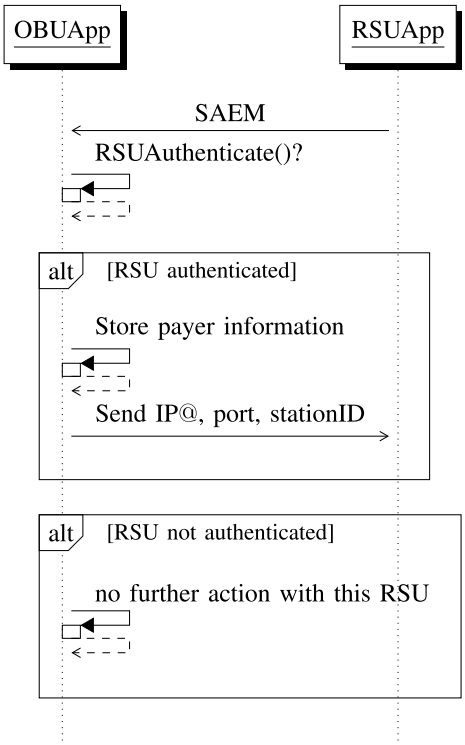


FIGURE 5. RSU authentication as a Payee.

B. WHEN APPROACHING & CROSSING TOLL GATES

- Authentication of the Payee entity by RSU:
  The RSU dedicated to tolling service broadcasts a regular message to announce the tolling station and tolling service (Service Announcement Message [11], e.g. 1 message per second) signed with its private key according to [12].
  The OBU that can apply to the service should authenticate the RSU with the public key of this latter (already stored in the OBU). This step authenticates the RSU. If everything is OK, the OBU will extract the payee entity (RSU) information like IP address to communicate with this RSU later. Indeed, for our use case ''payment through the ITS-G5 technology'', we will not use the CCH (Control CHannel) dedicated for road safety use cases, instead we use the SCH1 (Service CHannel). We can see on Figure 5 the exhange information between the RSU and the OBU to check the authentication of the RSU as mandated by the service provider.
- Authentication of the OBU:

TABLE 2. CAM definition [8].

Container	Data elements
ITS PDU header	Protocol version
	Message ID
	Station ID
	Generation delta time
Basic Container	Station Type
	Reference Position
High Frequency Container	Heading
	Speed
	Drive Direction
	Vehicle Length
	Vehicle Width
	Longitudinal Acceleration
	Curvature
	Curvature Calculation Mode
	Yawrate
	Steering wheel angle
	Lateral acceleration
	Vertical acceleration
Low Frequency Container	Vehicle Role
	Exterior Lights
	Path history

After the RSU authentication step, the OBU will send to the RSU a specific message that contains the payer information and its certificate with public key. The message will be signed with the private key, and encrypted with a symmetric session key. This latter is computed according to a prior convention of key exhanged through TLS protocol. By this way, only the RSU and the OBU can decrypt the message. The parameter ITSStationID-CAM retrieved from emitted CAM of the vehicle is sent among the payer information message (see Table 2), it permits to associate the vehicle and the transaction. In fact, in [1] and [2], to better locate the vehicle until it crosses the toll gate, the RSU uses the content of this message.

The RSU will forward the message to the Back Office of the security part of the service provider. This latter will check if the OBU information is not blacklisted (obviously associated to a revoked certificate). If all goes well, the Back Office of the security part of the service provider will send to the RSU an OK response signed by the private key of this security back office as a trusted party. The public key of the OBU, the ITSStationID-CAM and the IP address of the OBU will be temporarily stored on the RSU. The RSU will send to the OBU an acceptance response to benefit the service. The message will be encrypted with the EPuK(OBU). The OBU will decrypt the message and will fix static its ITSStation-IDCAM until the vehicle crosses the tollgate. By this time, the RSU can begin the geolocation process of the OBU. We can see on Figure 6 the exchange information between involved entities to validate the eligibility of an OBU to the service.

- Authentication of the Payer entity (subscriber of the service):

When the vehicle equipped with the OBU is about 100 meters before the tollgate, the RSU requests the OBU to send the payer information. The concerned OBU will only decrypt it. The OBU will send to the RSU a specific message that contains the payer information called PAN (Personal Account Number), the message should be signed with its private key, and encrypted with the symmetric session key.

The RSU decrypts this latter. Then, the RSU will send the content to the Back Office of the security part of the ETC service provider. This latter will check if the PAN is not blacklisted in other words, not present in the CRL (Certificate Revocation List). If all goes well, the Back Office of the security part of the service provider checks the subscriber information and will send an OK response to the RSU with a computed token signed with its private key, and the public key of the payer, eventually the car registration number (For our case, we do not send the car registration number). The RSU should temporarily store these information and just forward the signed token to the OBU. The message should be encrypted with the session key.

When receiving the message, the OBU has to check the signature of the token with the public key of the back office service provider already stored in his account. If this verification goes well, the OBU will send to the RSU the same token signed with his private key. The RSU will check the signed token with the public key temporarily stored. If the signature is authenticated, the RSU will wait until that the vehicle crosses a virtual position which is positioned in front of the barrier, or under the toll gantry. At this time, the RSU will send the acknowledgement message to completely validate the transaction.

We can see on the Figure 7 the process of subscriber's authentication and payment when crossing the toll gantry.

We can see on the Figure 8, 9 the toll configuration where the PAN is requested and where the transaction is achieved. Here, the border area to request PAN in each direction are placed in the way that the vehicle will be sure to cross the toll gantry.

The achievement of the transaction will trigger on the RSU the command to notify the central toll plaza server about the vehicle in the concerned lane. The central toll plaza server will send command to the concerned lane to perform the last checks (vehicle class, etc) and to open the barrier. If everything is OK, the RSU will send a notification to the OBU that the vehicle can pass. The driver will be notified by one beep or by a display on his HMI. At the same time, the back office of charging of the ETC service provider will book the transaction related to this payer. By this time, the RSU should stop the geolocation process of the concerned vehicle, and the OBU should change its ITSStationIDCAM according to [12].

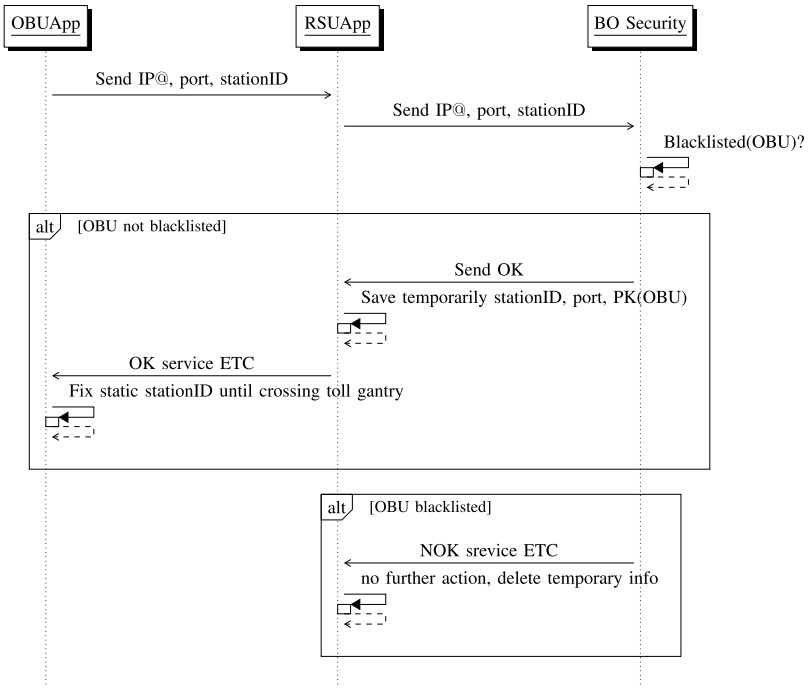


FIGURE 6. OBU authentication for eligibility to the service.

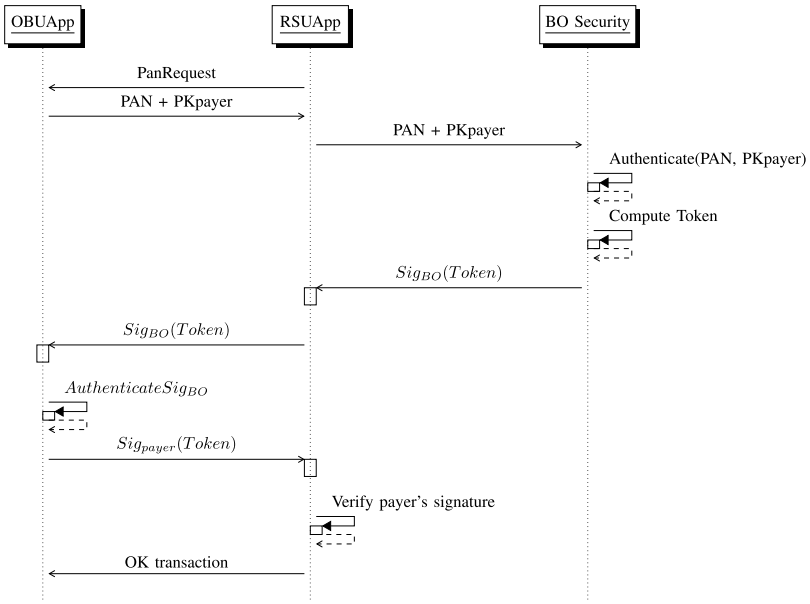


FIGURE 7. Subscriber's authentication for the ETC service.

- For the payer entity, when he will disconnect his account on the vehicle, the key pair related to his account should be deleted from this car.

To ensure the integrity of exchanged data, we apply the hash function SHA256. For the key transfer, we use secured protocol as HTTPS between each ITS stations and the Back office of security of the Toll Service Provider. The security functions such as generating digital signature, encryption / decryption use the ECDSA algorithm with 256 bits as key length. The signature of messages, the encryption, and the decryption functions satisfy the requirements for authentication, confidentiality and non-repudiation.

V. DISCUSSIONS

A. VERIFICATION OF SECURITY PROTOCOL USING AVISPA

Evaluating the robustness of the approach is an important stage to prove its effectiveness on preventing disruption to the normal operation. Also, it ensures that no attack could

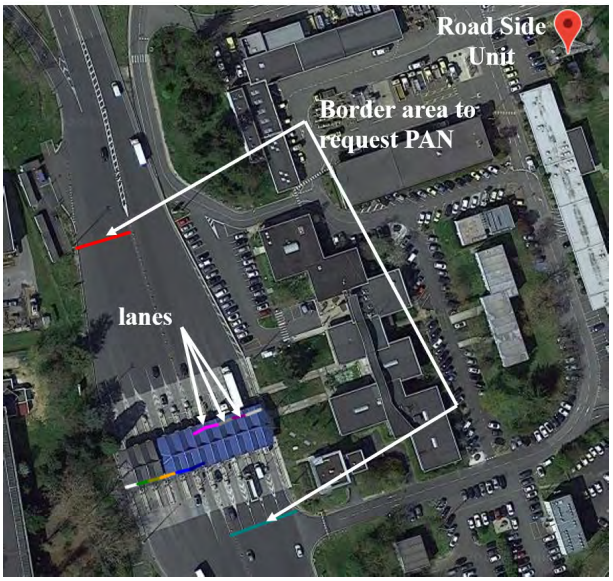


FIGURE 8. Relevant zones.

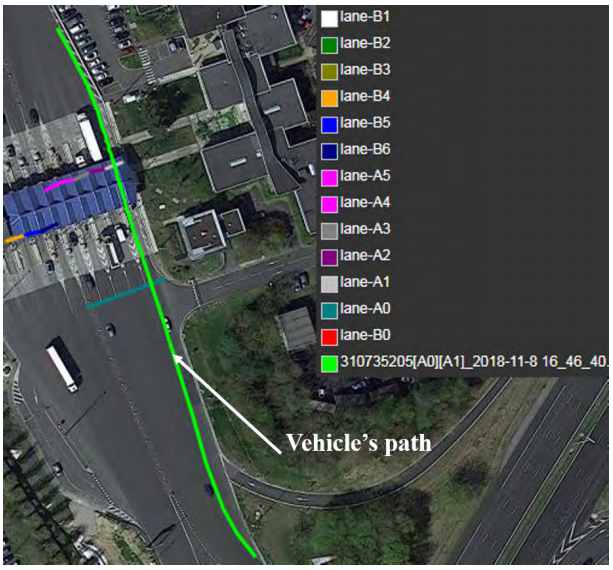


FIGURE 9. Configuration of the toll area.

penetrate our architecture even in the presence of intruders in the network regarding our over-the-air context. Performing different attacks on our approach is the best way to evaluate its robustness. In this context, different tools are proposed by the litterature: AVISPA/SPAN [32], CryptoVerif [33] and Proverif [34], etc. In this paper, we decide to use the AVISPA/SPAN tool: in fact, some comparison studies about different cryptographic verification tools highlight the effectiveness of AVISPA/SPAN among other tools [35]. We present in this subsection the formal verification of the authentication stage between the payer, the back office of the toll service provider as a server and the RSU. To do, we use the HLPSL specification according to [32] and [36]. We present the parameters of the simulation and the results

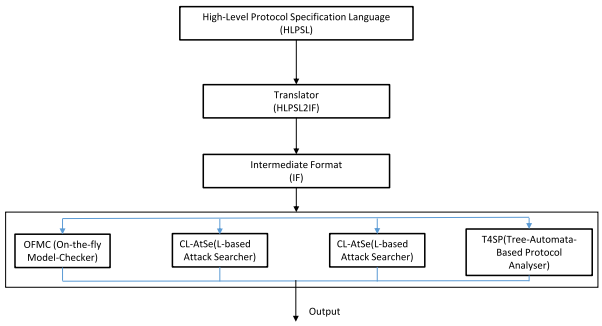


FIGURE 10. Architecture of the AVISPA tool [37].

during the process of crossing toll gate. Obviously, evaluating occurance of attacks during the exchanges of transaction is relevant to be validated. Before specifying this scenario with the HLPSL language, we will briefly present the tool.

1) AVISPA DESCRIPTION

AVISPA [32]
(Automated Validation of Internet Security Protocols and Applications) is a push-button tool that takes as input HLPSL specifications. It permits the analysis of large-scale Internet security-sensitive protocols and applications. And SPAN, the Security Protocol ANimator for AVISPA, helps in interactively buiding Message Sequence Charts (MSC) of the protocol execution. We can see on the Figure 10 the architecture of this modular tool.

A protocol in HLPSL is automatically translated into the rewrite based formalism IF (Intermediate Format). The IF language will be analysed by the back-ends of AVISPA. Each back-end implements one specific analysis technique. In fact, the AVISPA toolkit offers several backends for analyzing a HLPSL specification: OFMC (On-the-Fly Model-Checker), ATSE (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model-Checker) and TA4SP (Tree Automata tool based on Automatic Approximations for the Analysis of Security Protocols). Our method is verified with the OFMC back-end. It builds the infinite tree defined by the protocol analysis problem in a demand-driven way. It can be employed not only for efficient falsification of protocols (i.e. fast detection of attacks), but also for verification (i.e. proving the protocol correct) for a bounded number of sessions [38]. So it is suitable to test the robusteness of our proposed procedure.

2) HLPSL SPECIFICATION

Firstly, we will identify the participating entities (called roles), their initial knowledge and the exchanged messages between them. For our case, we have to define three roles: RSU, OBU, the payer and the back office of the service provider as a server. Also, in the implementation, we suppose that the communication between the RSU and OBU is secure, hence, a convention of a symmetric key is already shared to cypher all exchanges. We can see in the Table 3, the parameters used in the specification.

TABLE 3. Parameters in the HLPSL specification.

Parameter	Description
PKr	Public Key of the RSU
PKp	Public Key of the Payer
PKs	Public Key of the server
SK	Symmetric Key between the RSU and OBU
token_rs(respectively _ ps, _ ss)	token signed by the RSU(respectively by payer, by server)

```
%RSUDemo%
role rsu (R, V, S: agent,
        SK: symmetric_key,
        PKr, PKs: public_key,
        Panrequester,Ackok: message,
        Snd, Rcv: channel(dy))
played_by R def=
local State: nat,
        Pan: message,
    Token:text,
        PKp: public_key
init State:=0
transition
0.State=0 /\ Rcv(start)
  =|> State':=2
  /\ Snd({{Panrequester}_inv(PKr)}_SK)
1.State=2 /\ Rcv({{Pan'}_inv(PKp')}_SK)
  /\ secret({Pan'}_inv(PKp'), pan)
  =|> State':=4
  /\ Snd({{Pan'}_inv(PKp')}_PKs)
2.State=4
  /\ Rcv({{Token'}_inv(PKs).PKp.Pan}_PKr)
  =|> State':=6
  /\ Snd({{Token'}_inv(PKs)}_SK)
  /\ secret({Token'}_inv(PKs).
  PKp.Pan, token_ss,{S,R,V})
  /\ request(R,S, token_rs, Token')
  /\ witness(S,V, token_ps,Token')
3.State=6 /\ Rcv({{Token}_inv(PKp)}_SK)
  =|> State':=8
  /\ Snd({{Ackok}_inv(PKr)}_SK)
  /\ secret({Token}_inv(PKp),
                token_ps,{R,V})
end role
```

FIGURE 11. Role of the RSU tolling application.

```
%OBUDemo%
role obu(R,V,S: agent,
         SK: symmetric_key,
         PKr, PKp, PKs: public_key,
         Pan: message,
         Snd, Rcv: channel(dy))
played_by V def=
local
        State: nat,
        Panrequester,Ackok: message,
    Token: text
init State:=1
transition
1. State=1
  /\ Rcv({{Panrequester'}_inv(PKr)}_SK)
  =|> State':=3
  /\ Snd({{Pan}_inv(PKp)}_SK)
  /\ secret(Panrequester',panrequester,{R,V})
2. State=3
  /\ Rcv({{Token'}_inv(PKs)}_SK)
  =|> State':=7
  /\ Snd({{Token'}_inv(PKp)}_SK)
  /\ secret({Token'}_inv(PKs), token_rs,
    {R,V})
  /\ request(V, S, token_rs,
    {Token'}_inv(PKs))
  /\ witness(V,R, token_ps,{Token'}_inv(PKp))
3. State =7
  /\ Rcv({{Ackok'}_inv(PKr)}_SK)
  =|> State':=9
  /\ secret({Ackok'}_inv(PKr),ackok,{V,R})
end role
```

FIGURE 12. Role of the OBU tolling application.

```
%Server%
role server(R, V, S: agent,
        PKr, PKp, PKs: public_key,
        Pan: message,
        Snd, Rcv: channel(dy))
played_by S def=
local State: nat,
Token: text
init State:=1
transition
0. State=1 /\ Rcv({{Pan}_inv(PKp)}_PKs)
        =|> State':=5 /\ Token':=new()
        /\
    Snd({{Token'}_inv(PKs).PKp.Pan}_PKr)
        /\ witness(S,V, token_ss,{Token'}
                _inv(PKs).PKp.Pan)
end role
```

FIGURE 13. Role of the server.

The used notations are enumerated below:

- {message}_K denotes the message is ciphered/signed by the key K
- inv(PK) means the private key associated to the public key PK
- the primed variable that is within the reception channel means that we bind the variable to whatever is received

We can see on the Figures 11, 12, 13, 14, 15 and 16 respectively the definitions of the RSU role, the OBU role, the server roal, the session role and the environment of the verification and the objectives of the specified protocol.

After defining the participants' role, we present the session and the environment of the execution of the crossing the toll area scenario. The result of the simulation of the OFMC attacks on our protocol is shown in the Figure 18. We have successfully validated the robustness to the attacks of the proposed method to secure the toll transactions between the C-ITS equipment and the trusted party of the service provider. Let us remind that this protocol has been implemented and tested in real situation.

B. ADVANTAGES OF OUR PROPOSED PROCEDURE

In our approach, we clearly mention why the shared certificate with key pair is created. Here, the Back Office of the Toll Service Provider is the trusted party that can deliver the certificates of all involved entities and can authenticate

```
role session(
  R,V,S: agent,
  SK: symmetric_key,
  PKr, PKs, PKp: public_key,
  Panrequester,Pan,Ackok:message)
def=
local Snd,Rcv: channel(dy)
composition
  rsu(R,V,S, SK, PKr, PKs, Panrequester,
  Ackok, Snd, Rcv)
  /\ obu(R,V,S,SK, PKr,PKp,PKs,Pan,
  Snd, Rcv)
  /\ server(R,V,S, PKr, PKp,PKs,Pan,
  Snd, Rcv)
end role
```

FIGURE 14. Definition of the process session.

```
role environment() def=
const
  r, v, s: agent,
  panrequester,token_rv, token_rs,
  token_ps, token_ss: protocol_id,
  kr, kp, ks, ki: public_key,
  ackok,pan,panreq: message,
  k: symmetric_key
intruder_knowledge=
  {r,v,s, ki, kr, kp,inv(ki)}
composition
  session(r,v,s, k, kr,ks,kp,panreq,pan,
  ackok)
end role
```

FIGURE 15. Definition of the process environment.

```
goal
  secrecy_of panrequester,pan, token_ss,
  token_ps, token_rs, ackok
  authentication_on token_ps, token_rs,
  token_ss
end goal
environment()
```

FIGURE 16. Definition of the protocol goal.

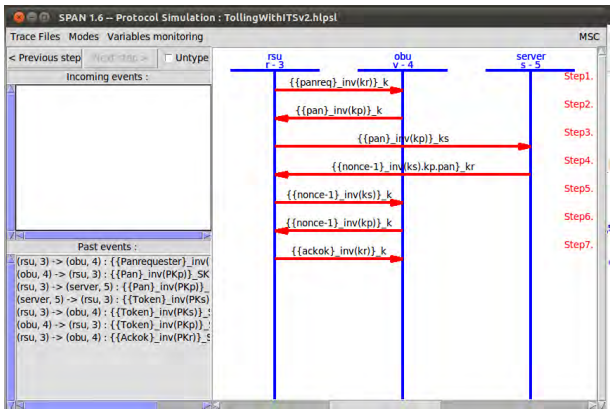


FIGURE 17. The monitor of the protocol simulation tool.

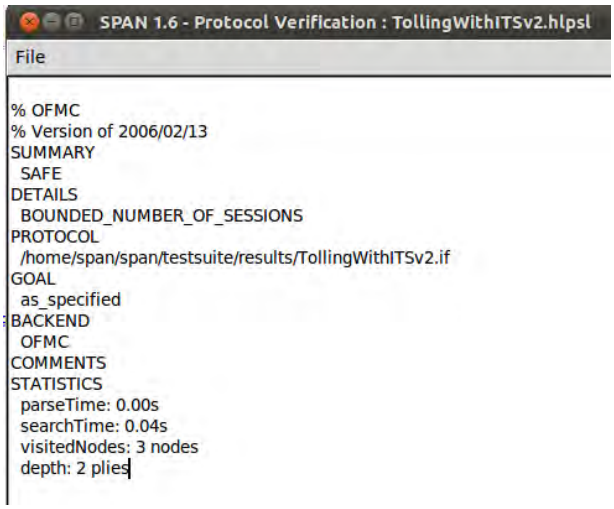


FIGURE 18. Result of simulation.

all subscribers, all OBUs with installed toll application and all RSUs able to perform the service. This way, attacks like Man-in-the-Middle will not be effective because all entities have to be registered, authenticated with their signature and certificates and can be detected if some suspectuous actions are perfomed.

Furthermore, the RSU are connected to the road operator network and have access to required servers to validate the transactions. On the other hand, the OBU are not necessarily connected to the internet during the use of the service. For this reason, our proposed method requires reasonable resources to the vehicle.

In this paper, we proposed an architecture for the majority of tolling configuration in Europe, here the toll areas with barriers, but it can be deployed also for the free-flow tolling. The RSU can be deployed anywhere else along the highways, so that other equipment is not disturbed. This solution can reduce traffic jams on the toll areas comparing to the time transactions using the other means of payment: cash, credit/debit card, DSRC, etc.

Another motivation for this work is also the improvement of the road safety by the safety of road operating agents. Indeed, to repair damages of the mandated RSU for toll transaction, the road operating agent will not take dangerous risks to replace or to fix the issues because the equipement is installed on the road side.

Finally, note that the proposed method is adaptable to the standardized ETC architecture with the advantage that it is suitable with the use of the ITS-G5 technology. This proposed security procedure will not prevent a breach, but it can significantly limit the impact of any intrusion that possibly take place in this kind of over-the-air transaction within the ITS-G5 technology towards V2I communications.

VI. CONCLUSIONS AND FUTURE WORK

The information security during over-the-air transactions is self-evident. In this context, we offer an innovative toll collection service for connected vehicles through the roadside unit (RSU) of the infrastructure to the connected vehicles using the ITS-G5 technology. In this paper, we proposed a solution for the security of Vehicle-To-Infrastructure Communications requirement to perform the tolling transaction service.

To do so, we just use one RSU to perform the transaction exchanges with all the vehicles in the toll area. The process is applicable to the ETC role model already standardized in [3]. The approach recommands the authentication of all the entities involved in the whole process (subscriber, OBU, RSU, and trusted part of the toll service provider as server). The chosen cryptographic algorithms satisfy the requirements of authentication, integrity, non-repudiation and confidentiality of exchanges that we have identified to perform the tolling transaction. Now, our future work is to challenge the proposed method by performing the Threat, Vulnerability And Risk Assessment (TVRA) [39].

ACKNOWLEDGMENT

The authors would like to thank the French road operator SANEF and the laboratory IRSEEM-ESIGELEC which closely support this work. Also, it is under contract with the National Agency for Research and Technology (ANRT) under the contract number 2015/1248; it has connections with the SCOOP@F project, which is co-funded by the European Commission under the CEF programme.

REFERENCES

[1] M. Randriamasy, A. Cabani, H. Chafouk, and G. Fremont, "Reliable vehicle location in electronic toll collection service with cooperative intelligent transportation systems," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun.(PIMRC)*, Oct. 2017, pp. 1–7.

[2] M. Randriamasy, A. Cabani, H. Chafouk, and G. Fremont, "Evaluation of methods to estimate vehicle location in electronic toll collection service with C-ITS," in *Proc. 29th IEEE Intell. Vehicles Symp.*, Jun. 2018, pp. 748–753.

[3] *Electronics fee Collection—Systems Architecture for Vehicle-Related Tolling*, ISO Standard 9241-210, 2010. [Online]. Available: https://www.iso.org/standard/45963.html

[4] *Intelligent Transport Systems (ITS)—Access layer specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band*, ETSI Standard EN 302 663 v1.2.1, Jul. 2013.

[5] L. Reinold, J. Gieblat, S. Davrou, G. Fremont, and E. Fischer, "Motorway toll system and method for granting access of a user of a user vehicle to a motorway," US Patend 15 916 587 Sep. 13, 2018. [Online]. Available: https://www.lens.org/lens/patent/030-175-400-039-581

[6] G.-H. Hsu, L.-R. Lin, R.-H. Jan, and C. Chen, "Design of ETC violation enforcement system for non-payment vehicle searching," in *Proc. 15th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jan. 2013, pp. 169–178.

[7] European Commission Directorate-General for Mobility and Transport, "Study on 'state of the art of electronic road tolling," Tech. Rep. MOVE/D3/2014-259, Oct. 2015. [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/modes/road/road_charging/doc/study-electronic-roadtolling. pdf

[8] *Intelligent Transport Systems (ITS)—Vehicular Communications; Basic Set of Applications; Part2: Specification of Cooperative Awareness Basic Service*, ETSI Standard EN 302 637 v1.3.1, Sep. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.01_30/en_30263702v010301v.pdf

[9] *Intelligent Transport Systems (ITS)—Vehicular Communications; Basic Set of Applications; Part2: Specification of Decentralizes Environmental Notification Basic Service*, ETSI Standard EN 302 637 v1.2.1, Sep. 2014. [Online]. Available: http://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.02.01_30/en_30263703v010201v.pdf

[10] *Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communications; Part 3: Communications system for the planning and reservation of EV energy supply using wireless networks*, ETSI Standard TS 101 556 - 3 V1.1.1, Oct. 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/101500_101599/10155603/01.01.01_60/ts_10155603v010101p.pdf

[11] *Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification*, ETSI Standard EN 102 890-1 v1.1.1, May 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102800_102899/10289001/01.01.01_60/ts_10289001v010101p.pdf

[12] *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, ETSI Standard TS 103 097 v1.3.1, Oct. 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

[13] S. Actors, *Delivrable 2.4.4.4—State of the Art of Public Key Infrastructures for Cooperative ITS*, document, 2017.

[14] B. Lonc and P. Cincilla, "Cooperative ITS security framework: Standards and implementations progress in europe," in *Proc. IEEE 17th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2016, pp. 1–6.

[15] I. SystemX. (2017). *Description of ISE Project*. [Online]. Available: https://www.irt-systemx.fr/project/ise/

[16] A. Bose and J.-F. Denis, "World payment report," Capgemini, BNP Paribas, Tech. Rep., Oct. 2017. [Online]. Available: https://www.capgemini.com/fr-fr/wp-content/uploads/sites/2/2017/10/world-payments-report-2017_year-end_ final_web-002.pdf

[17] S. Karnouskos, "Mobile payment: A journey through existing procedures and standardization initiatives," *IEEE Commun. Surveys Tuts.*, vol. 6, no. 4, pp. 44–66, 4th Quart., 2004.

[18] M. Dabrowski and L. Janikowski. (2018). *Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead*. [Online]. Available: http://www.europarl.europa.eu/cmsdata/149900/CASE_FINAL%20publication.pdf

[19] G. K. Niven *et al.* (2017). *The Future of Money*. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-the-future-of-money/$FILE/ey-the-future-of-money.pdfsss

[20] R. Jin *et al.*, "Detecting node failures in mobile wireless networks: A probabilistic approach," *IEEE Trans. Mobile Comput.*, vol. 15, no. 7, pp. 1647–1660, Jul. 2016.

[21] R. Moalla, B. Lonc, H. Labiod, and N. Simoni, "How to secure ITS applications?" in *Proc. 11th Annu. Medit. Ad Hoc Netw. Workshop*, Jun. 2012, pp. 113–118.

[22] P. Cincilla *et al.*, "Security of C-ITS messages: A practical solution the ISE project demonstrator," in *Proc. 7th Int. Conf. New Technol.*, Jul. 2015, pp. 1–2.

[23] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209616301231

[24] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[25] S. Sharma and E. Sharma, "A review: Analysis of various attacks in vanet," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 3, pp. 249–253, 2017. [Online]. Available: https://www.ijarcs.info/index.php/Ijarcs/article/view/2693

[26] EMVCo. (Dec. 2018). *Protocol and Core Functions Specification*. [Online]. Available: https://www.emvco.com/wp-content/plugins/pmpro-customizations/oy-getfile.php?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf

[27] S. Sharma and E. S. Sharma, "A review: Analysis of various attacks in VANET," *Int. J. Adv. Res. Comput. Sci.*, vol. 3, p. 7. May 2016.

[28] R. Moalla, H. Labiod, B. Lonc, and N. Simoni, "Risk analysis study of ITS communication architecture," in *Proc. 3rd Int. Conf. Netw. Future*, Nov. 2012, pp. 1–5.

[29] V. H. LA and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. Ad Hoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, Apr. 2014.

[30] M. S. Al-kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. 6th Int. Conf. Signal Process. Commun. Syst.*, Dec. 2012, pp. 1–9.

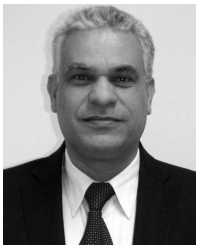
[31] (2013). *ISO/IECInformation Technology—Security Technology Security Management Systems—Requirements*. [Online]. Available: https://www.iso.org/standard/54534.html
[32] I. U. Artificial Intelligence Laboratory (AI-Lab) at DIST, Universit di Genova, F. CASSIS group at INRIA, Nancy, S. Information Security Group at ETHZ, Zárich, and G. Siemens AG, Munich. (2018). *AVISPA: Automated Validation of Internet Security Protocols and Applications*. [Online].Available: http://www.avispa-project.org/
[33] B. Blanchet. (2010). *CryptoVerif: Cryptographic Protocol Verifier in the Computational Model*. [Online]. Available: http://prosecco.gforge.inria.fr/personal/bblanche/cryptoverif/
[34] B. Blan. *ProVerif: Cryptographic Protocol Verifier in the Formal Model*. [Online]. Available: http://prosecco.gforge.inria.fr/personal/bblanche/proverif/
[35] P. Lafourcade, V. Terrade, and S. Vigier, "Comparison of cryptographic verification tools dealing with algebraic properties," in *Formal Aspects Security Trust*, P. Degano and J. D. Guttman, Eds. Berlin, Germany: Springer, 2010, pp. 173–185.
[36] T. A. Team. (2016). *HLPSL Tutorial: A Beginners Guide to Modelling and Analysing Internet Security Protocols*. [Online]. Available: http://www.avispa-project.org/package/tutorial.pdf
[37] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.
[38] T. A. Team. (Jun. 2006). *AVISPA v1.1 User Manual*. [Online]. Available: http://www.avispa-project.org, Jun. 2006.
[39] *Intelligent Transport Systems (ITS)—Security; Hreat, Vulnerability and Risk Analysis (TVRA)*, ETSI Standard EN 102 893 v1.1.1, Mar. 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf

MALALATIANA RANDRIAMASY received the Engineering degree in networks and telecommunications systems from the National School of Applied Sciences, Tangier, Morocco, in 2015.

She is currently pursuing the Ph.D. degree in computer science with Normandy University, UNIROUEN, ESIGELEC, IRSEEM. She is also a Project Assistant with the Department of Technologies and Systems Division with Sanef, France. Her research interest includes the new mobility services through the ITS-G5 technology, for example, new mean of collecting toll fees on highways to the connected vehicles.

ADNANE CABANI received the M.S. degree from INSA Rouen Normandie and the Ph.D. degree in computer science from the Information Processing and Systems Laboratory (LITIS – INSA Rouen Normandie), in 2008.

He was an invited Visiting Research Exchange Scholar with the Department of Computer Science, University of Arkansas at Little Rock, USA. He has been an Associate Professor in computer science with ESIGELEC/IRSEEM, since 2008. He is currently the Academic Coordinator of Master Information Systems and also a member of the Steering Committee of federative structure in logistics SFLog FED 4230. His research interests include multiagent systems, networks, and distributed systems.



HOUCINE CHAFOUK received the M.S. and Ph.D. degrees in automatic control from the University of Nancy, Nancy, France, in 1986 and 1990, respectively. He then joined the Graduate School in Electrical Engineering, ESIGELEC, Rouen, France. From 2000 to 2008, he was the Leader of the Automatics Control and Systems Research Team and the Research Head with ESIGELEC. He is currently with IRSEEM/ ESIGELEC, Normandy University of Rouen, France. From 2000 to 2018, he has been the co-author of 115 research papers in the areas of advanced control systems, fault tolerant control and fault diagnosis applied to renewal energy, and automotive and aerospace fields.

GUY FREMONT received the master's (Dipl.Ing.) degree in electrical engineering from Ecole Supérieure d'Eléctricité (SUPELEC), Paris, in 1982. He has been working during the first ten years in the aerospace and defence industry for the development of navigation and guidance systems. Then, he was with Cofiroute, a motorway company, as Innovation Manager in the study and development of Intelligent Transport Systems.

He joined Sanef, in 2007, where he is currently the Head of the Innovation and Transverse Projects Department, Technology and Systems Division. He is responsible for coordinating the design of future electronic tolling systems, of traffic management and travellers' information systems, and for managing the research and development activities. He is also coordinating the deployment and improvement of technical systems on Sanef motorway networks.