Eve, you shall not get access! A cyber-physical blockchain architecture for electronic toll collection security

Ahmed Didouh, Anthony Bahadir Lopez, Yassin El Hillali, Atika Rivenq, Mohammad Abdullah Al Faruque

Eve, You Shall Not Get Access! A Cyber-Physical Blockchain Architecture for Electronic Toll Collection Security

Ahmed Didouh[1], Anthony Bahadir Lopez[2], Yassin El Hillali[1],
Atika Rivenq[1], Mohammad Abdullah Al Faruque[2]

***Abstract*— Cooperative intelligent transportation system (C-ITS) applications are generally susceptible to position spoofing-dependent attacks such as Sybil and DDoS attacks due to a lack of established solutions. This paper presents a novel cyber-physical blockchain cryptographic architecture to help prevent position spoofing attackers from becoming validated nodes in C-ITS applications. The solution also guarantees security requirements including the non-trivial non-repudiation in light of these and other attacks. With a use case of electronic toll collection (ETC), our architecture implements techniques based on Received Signal Strength Indication (RSSI) measurements in conjunction with blockchain authentication methods such as Proof-of-Location and smart contracts to determine the legitimacy of a node. We demonstrate our solution in experiments using ITS-G5 Cohda Wireless technology (a Road Side Unit and two On-Board Units programmed with the ITS Vanetza stack) with functionalities specified by the European Telecommunications Standardization Institute (ETSI). From our experimental results from several driving-based data gathering tests, we discovered that our solution is able to cope with noise and relative velocity challenges because it incorporates both OBUs and RSUs in the Proof of Location computation steps. In light of this, the proposed architecture may also be applicable to govern V2X in general.**

I. Introduction

The IEEE 802.11p amendment to the IEEE 802.11 standard enables vehicular wireless communication (V2X) and serves as the basis for the Dedicated Short-Range Communication (DSRC) in the U.S. and the ITS-G5 technology in Europe. It specifies and requires suitable communication for rapid spatial mobility (up to 130 km / h) and operates in the 5.9 GHz frequency band with a reserved bandwidth of 70 MHz. Governments are leveraging these technologies to develop cooperative Intelligent Transportation Systems (ITS or C-ITS), whose primary objective is to improve road safety and comfort through rapid secure communication between on-board units (OBUs) in the vehicles and roadside units (RSUs) in traffic control system infrastructure. As an example, the DIR Nord (Directection Interdepartementale de Route du Nord: a motorway operator for northern roads in France) in collaboration with the DGITM (Ministere de Transition: Transportation Department of France's Government) are working on implementing ITS in two large-scale projects called InterCor and SCoop@F [3][4] and others to improve road safety.

However, the stakes are high with these developments. A fault within the vehicle's control logic, whether forced or unforced and internal or via a communication port to the outside, implies a real danger for the life of the driver or loss of critical information. For this reason, industry and researchers are constantly coming up with new ways to potentially secure vehicular communication channels.

One such application with high risk is electronic toll collection (ETC). ETC involves transactions between service providers, via toll stations, and drivers. As these transactions involve personal account and money-related data as well as position and speed, ETC regions may be targeted for identity and/or location spoofing-based attacks such as Sybil and DDoS [8]. Such attacks could constitute a danger for the personal information of the users as well as for the traffic flow itself.

In this work, we offer a new security architecture based on consortium blockchain cryptography which is built upon two critical components: a smart contract and a consensus-based Proof of Location (PoL). Both components are critical contributions in our work. The smart contract integrates the legal aspect of verification since all the nodes are obliged to execute the same code (smart contract). On the other hand, the PoL is a cyber-physical aspect designed to strengthen the authenticity of a vehicle attempting to be involved in the ETC system.

This solution will help ensure that vehicles are authenticated upstream of toll stations in a mutual authentication fashion between all the involved entities. As the architecture is blockchain cryptography-based, security requirements including confidentiality, integrity, availability, and non-repudiation of all information exchanged are also ensured. Further, as we comprehend the importance of evaluating security architectures and methods using real state-of-the-art equipment, we conduct preliminary experiments using ITS-G5 technology from NXP (two OBUs and one RSU) connected with real vehicles in an realistic setting.

This paper will introduce and demonstrate the novel security architecture within the context of an ETC application. Section II consists of related work with a brief summary of the state-of-the-art of C-ITS and security solutions dedicated to ETC. In Section III, we present our security architecture and methods for securing ETC regions. In Section IV, we present and discuss the results of our realistic experiments

[1]Ahmed Didouh and Yassin El Hillali and Atika Rivenq are with the Department of Institute of Microelectronics and Nanotechnology Electronics, at Université polytechnique haut de France {ahmed.didouh,Yassin.ElHillali, Atika.Menhaj}@uphf.fr

[2]Anthony Bahadir Lopez and Mohammad Abdullah Al Faruque are with the Department of Electrical Engineering and Computer Science at the University of California Irvine, United States {anthl10,alfaruqu}@uci.edu

of our solution. Finally, conclusions and future work are in Section VI.

II. State of the Art

A. ITS-G5

ITS-G5 technology enables and permits vehicles to operate as an ad-hoc network without the need for RSU intervention. In Europe, C-ITS authorities have defined three application classes: road safety, traffic management, and comfort applications. In the European ITS-G5 standard, the following types of messages have been defined:

- Cooperative Awareness Message (CAM): [11] Intended for cooperative awareness (i.e., locating surrounding vehicles in real time). This message type is sent automatically by the vehicle every 10 ms.
- Decentralized environmental notification message (DENM): [9] Alert messages that are intended to be broadcast over a geographic area. They are issued only during an unexpected event. Triggering the sending of this message can be automated involving the various sensors present on the vehicle or can result from a manual signal from the driver.
- In-Vehicle Information Message (IVIM): Supports dissemination of mandatory and advisory road sign information. These messages are sent only by the infrastructure (e.g., RSUs).

TABLE I
ITS G5 frequency standard

	Frequency band	Specification
ITS-G5A	5875 - 5905	ITS road safety related applications
ITS-G5B	5855 - 5875	ITS non-safety applications
ITS-G5D	5905 - 5925	Future ITS applications

B. Electronic Toll Collection based on IEEE 802.11p

At the edge of the toll systems, the highway operators use various means to collect as much data possible to better identify the toll service user. However, this also implies that this equipment must be installed at each of the toll stations. In order to reduce these costs, researchers have attempted to find optimal tolling locations to install such equipment [17]. Randriamasy et. al. demonstrate a solution that adopts the ITS-G5 standard for secure toll payments.

The European Committee for Standardization (CEN) DSRC technology [5] is used for electronic fee collection (uses a 5.8 GHz band and is incompatible with DSRC in U.S.). Research tends to go through the most implemented standard in order to optimize the means deployed by motorway operators for interoperability with each technology. In [13], authors study the feasibility of using the WSMP standard in tolls.

C. Blockchain and Consensus

Blockchain cryptography was originally introduced to resolve the challenges of implementing multiple access networks through various nodes [16]. To ensure the security of the nodes and to be precise on how consensus is reached for a transaction validation per each network and corresponding blockchain, *smart contracts* were developed and introduced by Ethereum [19]. These smart contracts include rules and requirements as well their enforcement all in the form of software.

As explained by [21], the various types of blockchain may be classified as follows:

- *Public Blockchain*: All nodes have the right to participate in the consensus process, it is considered to be a fully decentralized blockchain.
- *Consortium Blockchain*: Only a subset of nodes have privileged rights to participate in the consensus vote and it is therefore partially decentralized.
- *Private Blockchain*: Only a single organism and the nodes belonging to it have the right to participate in the consensus. It is therefore considered to be a centralized blockchain.

Yang et. al. [20] propose a consortium blockchain for V2X, giving only the right to RSUs to participate in the consensus of creating blocks in order to give the reputation score to each node, while being based on specific feedback from vehicles. In [7], the author proposes a blockchain based on the consensus PoL using a vehicle's sensors. The PoL is used for authentication to permit a vehicle into the blockchain-oriented system.

In Bitcoin [15], distributed consensus is achieved through a Proof of Work (PoW) approach. To produce a valid block and add it to the blockchain (e.g., the data mining process), a peer must perform extremely time-consuming work characterized by low probability of success (the first to meet the condition will get right to add blocks) [6]. More specifically, the miner must randomly mine the block header until a value below a target threshold is obtained (also called the nonce difficulty). To encourage competition among minors, a reward is given to the first worker to finish the job.

However, as we mentioned earlier, we propose the use of a consortium blockchain instead. In order to validate a vehicle in the network, RSUs will collect all a vehicle's PoLs provided by other vehicles and then calculate its overall score. For an overview of our proposed architecture and methods, please refer to Figure 2, where vehicle Alpha is having its score be calculated by the RSU.

III. Current Solution

A. Public Key Infrastructure (PKI) Architecture

The traditional PKI security architecture for wireless vehicular communications is a hierarchical architecture where each layer consists of different authorities. The Certificate Authority (CA) is at the top of the pyramid, where a trusted cryptographic certificate is provided to each lower-layer legitimate entity (who may also have the capability to provide

certificates) and may be revoked or blacklisted if an entity is misbehaving. According to the IEEE standard [2], here is an overview of functions that the PKI system offers:

- Securing the private keys corresponding to public keys via the software or the hardware
- Logging actions (in centralized archives)
- The recovery of the private key
- Archiving certificates over time
- Misbehavior detection and certificate revocation

The PKI system is based on credential and identification information management where access control is at the heart of this environment [12]. The PKI system ensures that only those with the appropriate permissions can access the data by using cryptographic key pairs and certificates to verify the identity of users and legitimacy of data. The digital certificate links each ITS station to its public key. In addition to the public key, certificates contain additional information, such as the issuer, their intended use, and any other type of metadata, as shown Figure 1.

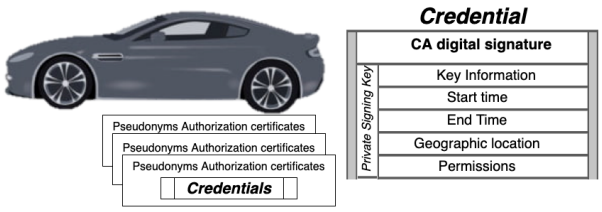

Fig. 1. Credential composition

B. Security Threats

Currently, the potential security vulnerabilities in vehicular communications networks form a handicap on the performance of C-ITS applications and can have severe repercussions on finances or even human life. To address these potential vulnerabilities and specifically the attacks listed by the ETSI standard [10], we have developed a novel security architecture based on blockchain cryptography, smart contracts, and cyber-physical characteristics of the V2X environment. Below we summarize notable attacks on V2X with high potential impact. For other types of attacks on V2X networks, we refer to the survey in reference [14].

- *Wormhole Attack*: Messages are replayed in a different place and at a different time. These attacks can be used to confuse recipients who are unable to resolve the problem.
- *Position Spoofing Attack*: A GNSS satellite simulator can generate stronger radio signals than those received from a real GNSS satellite. Besides tampering with the software and sending fake positions, this method also allows an attacker to provide false location information to ITS stations and thus, potentially, causing traffic accidents. If an ITS station synchronizes its internal clock with GNSS time, the simulator can be used to set an inaccurate current time and this may cause its acceptance of expired messages received during a replay attack.
- *Sybil Attack*: By sending multiple messages from a node with multiple identities, other nodes will receive false information about the density and behavior of neighbors and become confused. The main motivation of these attacks is to attain advantage of the road or to just cause havoc.

IV. Proposed Security Solution

As we have seen, most of the attacks come from falsified GPS positions or the replayed timestamps in messages. This leads us to the notion that cyber-physical aspects related to time and space of the ETC region may be integrated into V2X security to help strengthen integrity and authentication.

Our solution integrates these cyber-physical aspects with a consortium blockchain. For this, we will use smart contracts to guarantee the non-repudiation of messages by proving their location within the blockchain network. Our solution offers real-time control of the certainty of the information that the transmitter is circulating, in particular the GPS positions of vehicles with message time stamps.

A. Network Setup

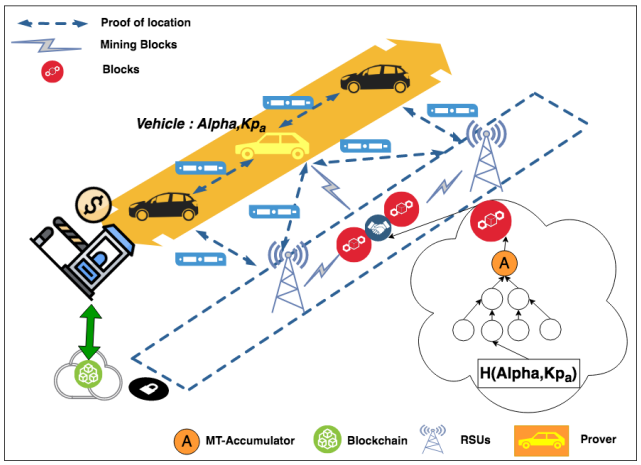

Fig. 2. Witness process

In the network setup for our proposed architecture, the road operator who owns the toll booths will maintain a blockchain where RSUs are the only nodes that have the privilege of mining new blocks and permitting nodes into the blockchain network. For a new node to be admitted into the network, it must prove its location through smart contracts. Hence, the vehicles holding the PoLs send them to the RSUs so that the latter can verify and accept them into the network.

Once a vehicle is validated, its public key is therefore added into the Merkel tree accumulator. Once a vehicle is about to arrive to the toll station, the monitoring device directly checks its legitimacy by checking the existence of its public key in the accumulator.

The asynchronous Merkle tree accumulator explained in [18] effectively stores a list of all the public key of accepted vehicles in the network. Each individually mined block contains a Merkel tree (an efficient data structure) made up of all the acceptable vehicle's public keys, as described in

Table III. Additionally, in a Merkel tree, every leaf node is labelled with the cryptographic hash of a data block.

Abbreviations	meaning
P_r and P_t (dBm)	Powers at the receiving and transmitting antennas, respectively
G_r and G_t (dBi)	Gains of the receiving and transmitting antennas, respectively
L_M, L_t, L_r (dB)	constitute all the losses in the Link Budget equation (3), are respectively miscellaneous losses, transmitter losses and receiver losses
Hd_r and Hd_t (°)	Headings/ directions of receiving and transmitting vehicles, respectively
Pos_w and Pos_p	Latitude and longitude coordinates of Witness' and Prover's positions, respectively
d (Km)	is distance between the vehicles
t_w, t_p (s)	Time stamps of the Witness and Prover, respectively
Cer_p, Cer_w	The Prover's and Witness' certificates, respectively
S_p, S_w (Km/h)	The Prover's and Witness' signatures, respectively
Kp_p, Acc	The Prover's public key and the PoL accuracy

TABLE II
ABBREVIATIONS

B. Smart Contract

The purpose of incorporating a smart contract is that it is published in a blockchain and accessible by all nodes to prove the veracity of their information by executing the program (smart contract) and giving evidence (beacons) without need for external party. Once evidence is given, a PoL will be provided to the Witness to send to the Prover.

For the execution of smart contracts we use the Proof of Location (PoL) process. This is the evidence obtained by other RSUs or OBUs in the neighbors (Witnesses) to prove that a node is actually in the position in which it claims to be. For a PoL, only the radio wave metric is taken into account in our solution, but other algorithms can be used to have more precision in the detection of vehicles, such as those which take into account vehicle sensors [7].

The vehicle must collect PoLs to allow its proper integration into the blockchain toll payment system. In order to have a PoL, the vehicle goes through the following steps:

Step 1: the Prover will send its PoL request only by ITS-G5 (or WAVE) technology

$$PoLreq = (Cer_p, Pos_p, t_p, S_p[Pos_p]) \tag{1}$$

Step 2: The Witness (RSU or Vehicle) will check and validate the PoL request using the smart contract process explained in the next paragraph. Lastly, the Witness responds with a PoL.

Step 3: The Prover sends its PoL and its beacon together to be verified only by the RSU. Once the PoL is verified, the hash of the OBU's public key can be stored into the blockchain.

We use smart contracts to allow the stakeholders (OBUs and RSUs) to execute the same code in order to be able to agree on the obtained results, and reach the consensus. For this, the ITS stations need to prove via their ITS-G5 radio modules by taking into account certain parameters of RSSI in order to estimate distance.

1) Radio wave propagation theory: As the radio wave propagates through the atmosphere and through several objects, its strength will be lost. A model for the first source of loss is called the free space propagation loss, where loss is related to the distance traveled by the signal. The powers in a free space environment are determined by the Friis equation:

$$\frac{P_r}{P_t} = G_r G_t \left(\frac{\lambda}{4\pi d}\right)^2 \tag{2}$$

The Friis equation expresses the loss of signal strength depending on the distance traveled, d. This loss depends on the signal frequency $f = \frac{\lambda}{c}$. Where λ is the wavelength and $c = 3.10^8 m.s^-1$ is the speed of light.

The following link budget equation includes all the gains and losses of power as a communication signal.

$$P_r = P_t + G_t + G_r - L_t - L_r - L_{FS} - L_M \tag{3}$$

2) Distance estimation: On receipt of a PoL_{req} from a nearby vehicle (Prover) the two vehicles (Witness and Prover) establish a uni-cast communication. The execution of our smart contract will go through the following steps:

Step 1: The smart contract chooses the number of beacons (sent by the Prover to the Witeness) to be taken into account to provide the PoL. The choice of the said number depends on the following conditions:

- The number of beacons must be maximized to validate the information
- The two vehicles must keep a communication without interruption, thus we consider the vehicles' speeds with respect to the range of the ITS G5 signal
- The Prover must not be static (its speed must be greater than zero).

We calculate the chosen number of beacons N using the following equation:

$$N = \frac{3600R}{|Sd_w - Sd_p|} \tag{4}$$

Where: Sd_w and Sd_p, respectively, are the the speeds of the Witness and Prover, and R is the distance of the ITS G5 range (estimated to be 700 meters).

Step 2: In this part of the smart contract, the beacon belonging to the Prover is extracted and processed. Each time the Witness receives a beacon from the Prover, it stores it in a local beacon list, until reaching the N beacons. These contain useful information to better estimate distance.

From the list of N beacons, the Witness extracts the following data sequence Sq. The subscripts w/p for data variables correspond to the Witness (w) and the Prover (p):

$$Sq = \begin{bmatrix} P_r(1), Pos_{w/p}, Sp_{w/p}, Hd_{w/p}, YR_{w/p}, t_p \\ \cdot \\ \cdot \\ P_r(N), Pos_{w/p}, Sp_{w/p}, Hd_{w/p}, YR_{w/p}, t_p \end{bmatrix}$$

Step 3: We obtain three cyber-physical indicators to verify the claimed locations of a Prover.

- Indicator 1 ($I1$): We calculate the average speed and calculate distance traveled from it to compare with the distance between the coordinates from the first and last collected beacons.
- Indicator 2 ($I2$): We calculate the distance traveled of a message from the sender to the receiving vehicle from the power received using the Friis equation (2) and the Budget link formula (3). Then, we compare the result with the distance between the Witness and Prover (via their positions).
- Indicator 3 ($I3$): This indicator represents the communication quality conditions between the Witness and the Prover. It takes into account the information of the two communicators to give a value for the judgment accuracy of the Witness (i.e., how well they can verify the signal strength and distance of the Prover). We calculate it based on their velocities, headings, and yaw rates (though weather can also be considered). Relative velocity greatly impacts the accuracy of the RSSI measurements due to the Doppler effect [**?**] and heading/yaw rate provides insights with respect to line of sight.

We have two indicators (I_1, I_2) for the truthiness of the claimed location and one indicator (I_3) on the accuracy of the measurements. From these, we may calculate two components of the PoL: PoL_{Rate} and PoL_{Acc}. They are defined as follows:

$$PoL_{Rate} = \frac{I_1 + I_2}{2} \tag{5}$$

$$PoL_{Acc} = I_3 \tag{6}$$

After having executed these 3 functions of the smart contract, the Witness converts them along with other variables into the finalized PoL.

$$PoL = (PoL_{Acc}, PoL_{rate}, Pos_p, t_w, Cer_w, S_w[PoLreq, t_w, Kp_p]) \tag{7}$$

The above-mentioned steps and indications are presented in detail in Algorithm 1 to conduct and validate a Proof of Location.

As mentioned, we use a consortium blockchain where the RSUs accumulate the various PoLs corresponding to a single vehicle (say, Alpha) to permit it into the tolling blockchain network. To do this, the RSU will compute a global averaged PoL_{Rate} for a vehicle using the Equation 8:

$$\bar{PoL_{Rate}} = \frac{\sum_{i=1}^{n} PoL_{Acc(i)} PoL_{Rate(i)}}{\sum_{i=1}^{n} PoL_{Acc(i)}} \tag{8}$$

Then, the vehicle will be validated if its overall PoL rate exceeds some average threshold that will be continously adapted to the environmental and historical circumstances. After the verification of PoL by all RSUs, a mined block by one of these RSUs will correspond to an addition of a new element to the blockchain. Afterwards, the tolling system can carry out a quick check of the last block (the most up to date) to check if the node has been authenticated and admitted into the blockchain system. The payment hash will also be listed in the blockchain.

Algorithm 1: Algorithm for Excluding the Negation

Input: $Pos_{w/p}$; P_r; $Hd_{w/p}$; $Sp_{w/p}$;N
Output: PoL_{Rate}; PoL_{Acc}
Function `Indicator1` ($t_p[]$,$Sp_p[]$,$Pos_p[]$,N) **:**
  foreach $i \in N-1$ **do**
    $dis \longleftarrow distance(Pos_p(i), Pos_p(i+1))$;
    $dis' \longleftarrow Ave(Sp_p(i), Sp_p(i+1)) * \Delta(t_p(i), t_p(i+1))$:
    $I_1 \longleftarrow I_1 + |dis - dis'|$;
  end
return $\frac{I_1}{N-1}$;
End Function
Function `Indicator2` ($P_r[]$,$Pos_{(w/p)}[]$) **:**
  $G_t = G_r \longleftarrow 5$
  $P_t \longleftarrow 23$ ▷ normalized transmission power
  foreach $i \in N$ **do**
    $D_R = distance(Pos_p, Pos_w)$ ▷ the real distance
    D_E ▷ the Estimated distance using equation 2 and 3
    $I_2 \longleftarrow I_2 + \frac{|D_R - D_E|}{D_R}$;
  end
  return $\frac{I_2}{N}$;
End Function
Function `Indicator3` ($Sp_{w/p}$,$Hd_{w/p}$,$YR_{w/p}$) **:**
  foreach $i \in N$ **do**
    $Vel \longleftarrow \frac{|Sp_w - Sp_p|}{Max(Sp)}$
    $\delta Hd \longleftarrow \frac{|Hd_w - Hd_p|}{Max(Hd)}$
    $\delta YR \longleftarrow \frac{|YR_w - YR'_p|}{Max(Hd)}$
    $I_3 \longleftarrow I_3 + \frac{2.Vel + \delta YR + \delta Hd}{4}$;
  end
  return $\frac{I_3}{N}$;
End Function
PoL_{Rate} ▷ Calculating the PoL rate using 5
PoL_{Acc} ▷ Calculating the PoL Accuracy using 6

C. Properties

Our solution may guarantee the following security properties:

- *Confidentiality:* Our solution ensures confidentiality since the payment transactions are listed in the blocks. These are not returned to the vehicles.
- *Availability:* With this solution, DoS attacks can be detected and reassembled
- *Integrity:* This solution adds the spatio-temporal aspect of the physical location which helps to prevent attacks with modified or replayed toll requests messages. This solution also avoids the Sybil attack because it allows us to link each identity with each location and it makes it extremely challenging for a single user to imitate several devices in a distributed network.

TABLE III
BLOCK COMPOSITION

Block Header	
Block Version	Indicates set of block validation rules
Merkel Tree Root Hash	The hash value of all the PoL transactions
Time Stamp (s)	Current universal time
Parent Block Hash	Hash value that points to the previous block
Merkel Tree of Accumulator	The hash values of all subscribed public keys in blockchain and their Witnesses

- *Non-repudiation:* Because blockchain keeps track of transaction history, no device can deny that a transaction had or had not occurred. Thus blockchain naturally ensures non-repudiation. This is a crucial security requirement for finance-related applications such as tolling, and especially for ETC over the highly distributed V2X environment.

V. EXPERIMENTAL RESULTS

We have conducted tests in the Mont Houy campus in Valenciennes, France where we have used two OBUs (with two real vehicles) and one RSU (see Figure 3). The radio equipment used in each of the three devices is the NXP ITS-G5 chip [1].

Fig. 3. Used equipment

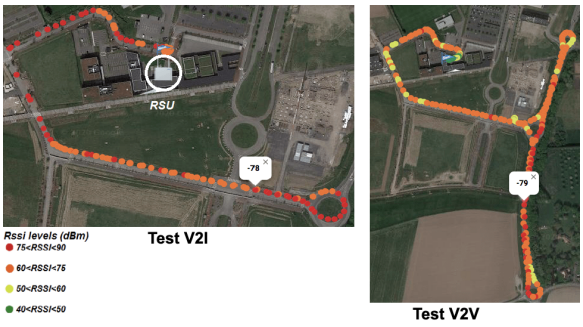

Fig. 4. Path of OBU 1 under V2V communication

The objective of these tests is to demonstrate a proof of concept for our solution. Our solution is based on two types of communication: V2V (vehicle to vehicles) and V2I (Vehicles to infrastructure) communication. Thus, to test the V2V communication, we conducted four tests with different distances between the two vehicles as well as two different environmental conditions (with/without line of sight for communication) (figure 7)

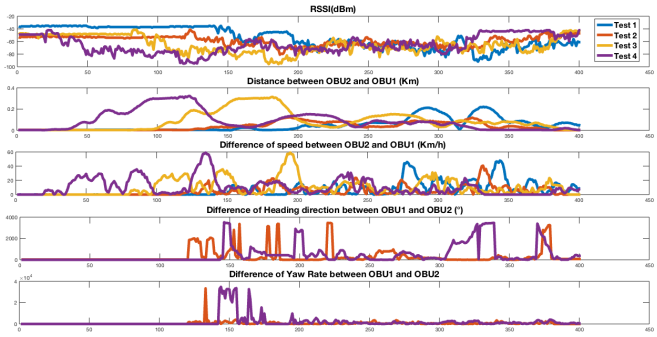

Fig. 5. Measurements

we have considered to abstract the sum of all the other losses ($L_M + L_t + L_r$) is 14 dB for the four tests taking into account meteorological conditions. The distance estimates from RSSI are shown in figure 5.

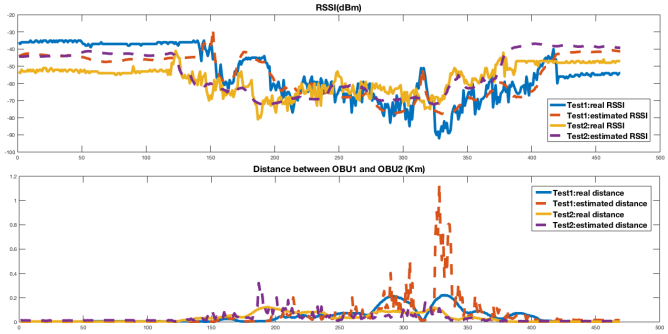

Fig. 6. Test 1/2 V2V estimation

Using Equations 2 and 3, we estimated the values of the expected power from the positions sent and we also estimated the values of the expected distance from the received signal power (see figure V).

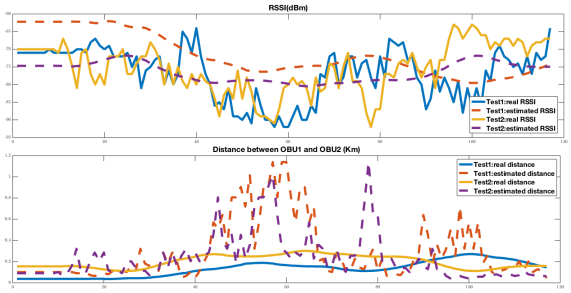

Fig. 7. Test 1 and 2 with RSU's estimation on V2I communication

From our experiments, we noticed that the differences in speeds/velocities of the vehicles greatly impacts the measurements. This is why we integrated it into the measurement accuracy for the verification step.

Referring to Table IV, we notice the RSU's distance and RSSI estimations via V2I communications have 30 percent less accuracy compared to that of the OBU's. This is because of the impacts from relative velocity and we may deduce that the RSU alone cannot make a decision on vehicle verification. Thus, this is why considering all the OBUs and

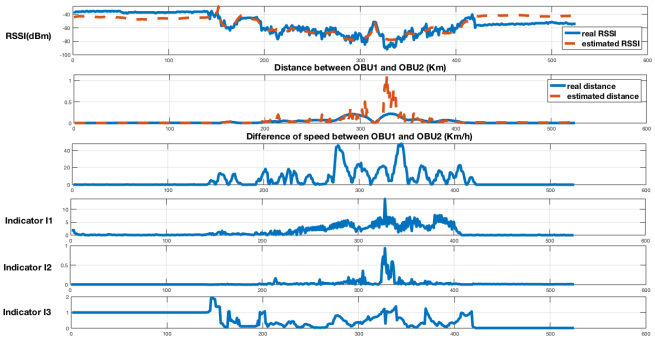

Fig. 8. Test 1 Indicators

RSUs in a surrounding area of a vehicle makes our system more accurate and effective. Since the number of PoLs from all vehicles will allow the RSUs to have more visibility on the truth of the Prover's position.

	RSSI		Distance	
	OBU1	RSU	OBU1	RSU
Test 1	81,64%	42,87%	72,92%	40,24%
Test 2	88,53%	70,56%	77,66%	56,57%

TABLE IV
CROSS-CORRELATIONS OF REAL AND ESTIMATED RSSI/DISTANCE VALUES BETWEEN OBU1/RSU AND OBU2

If we consider the traditional PKI system using our Proof of location system. it will use only the infrastructure equipment (RSUs). However, it is clear that the single use of RSUs is not sufficient to approve the accuracy of the claimed positions of neighboring vehicles. It is clearly concluded that this solution cannot be used with the traditional system. we are in real need of integrating a decentralized system accompanying this protocol

VI. Conclusion

It goes without saying that toll transactions must be secure, but what is even more important is to have the ability to cope with the essential deployment of ITS G5 technologies in the world of autonomous vehicles. In particular, it is important to be able to cope with attacks that may occur with these technologies and with its large-scale deployment. It is even of more importance since several car manufacturers plan to have all upcoming vehicles equipped with V2X equipment and also because motorway managers have already equipped most of their networks with this equipment.

In this article, we have proposed a way to ensure integration and non-repudiation in toll transactions (two non-trivial security requirements). The performance of the proposed identification and verification methods was evaluated using one RSU and two OBUs, each of which are state-of-the-art industrial equipment.

By adding our evaluation indicators and with smart contracts, we obtained satisfactory results on the effectiveness of this method. The performances will be even more effective communicating and avoid DoS and Sybil attacks. Note, however, that this architecture and its methods can be applied for all vehicular communications. In future work, we will use this Proof of Location consensus with a real Solidity platform, used for handling smart contracts and for its blockchain test database. This will help us to develop a scalable blockchain-based architecture to govern vehicular communications in general.

ACKNOWLEDGMENTS

This work is further supported by DIR Nord (Road operator of north of France) under contract with the Polytechnique University of Haut de France (UPHF); it has connections with the project InterCor, which is co-funded by the European Commission under the CEF programme.

References

[1] DSRC safety modem | NXP.
[2] IEEE standard for message sets for vehicle/roadside communications. pages 1–134.
[3] InterCor project: Interoperable corridors deploying cooperative intelligent transport systems.
[4] Projet SCOOP : véhicules et routes connectés.
[5] 14:00-17:00. ISO 17573-1:2019.
[6] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.
[7] Felipe Boeira, Mikael Asplund, and Marinho Barcellos. Decentralized proof of location in vehicular ad hoc networks. 147:98–110.
[8] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. VANET security surveys. 44:1–13.
[9] EN ETSI. 302 637-3 v1. 2.2: Intelligent transport systems (its). *Vehicular Communications*.
[10] I ETSI. Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra). Technical report, Technical report, ETSI TR 102 893, European Telecommunications Standards ..., 2010.
[11] TCITS ETSI. Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *Draft ETSI TS*, 20:448–451, 2011.
[12] TS ETSI. 102 941 v1. 1.1—intelligent transport systems (its); security; trust and privacy management. *Standard, TC C-ITS*, 2012.
[13] Mei-Wen Li, Tsung-Hsun Wu, Wei-Yen Lin, Kun-Chan Lan, Chien-Ming Chou, and Chung-Hsien Hsu. On the feasibility of using 802.11p for communication of electronic toll collection systems. 2011:723814.
[14] A. Lopez, A. V. Malawade, M. A. Al Faruque, S. Boddupalli, and S. Ray. Security of emergent automotive systems: A tutorial introduction and perspectives on practice. *IEEE Design Test*, 36(6):10–38, Dec 2019.
[15] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.
[16] Marc Pilkington. Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.
[17] Malalatiana Randriamasy, Adnane Cabani, Houcine Chafouk, and Guy Fremont. Formally validated of novel tolling service with the ITS-g5. 7:41133–41144.
[18] Leonid Reyzin and Sophia Yakoubov. Efficient asynchronous accumulators for distributed PKI. In Vassilis Zikas and Roberto De Prisco, editors, *Security and Cryptography for Networks*, volume 9841, pages 292–309. Springer International Publishing.
[19] Dr Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. page 32.
[20] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor C. M. Leung. Blockchain-based decentralized trust management in vehicular networks. 6(2):1495–1505.
[21] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564. ISSN: null.