Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering

Ahmed Didouh, Houda Labiod, Yassin El Hillali, Atika Rivenq

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 9, 2022, accepted March 8, 2022, date of publication March 16, 2022, date of current version May 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3160171

Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering

AHMED DIDOUH[1], HOUDA LABIOD[2], (Senior Member, IEEE), YASSIN EL HILLALI[1], AND ATIKA RIVENQ[1], (Member, IEEE)

[1]IEMN, Université Polytechnique Hauts-de-France, 59300 Valenciennes, France
[2]Department of Computer Science and Networks, Telecom Paris, LTCI, 91120 Palaiseau, France

Corresponding author: Ahmed Didouh (ahmed.didouh@uphf.fr)

This work was supported in part by the EU Project Infrastructure Digitale de Demain (InDiD), in part by the Connecting Europe Facility, in part by the European Union, in part by the la région Hauts de France, and in part by the Valenciennes Métropole for la Chaire d'Excellence RIVA.

ABSTRACT Despite the decisive contribution of intelligent transport systems in road safety, they also open new vulnerabilities to cyber-attacks, particularly vehicle position-linked attacks. For that reason, centralized systems are becoming increasingly vulnerable to the growth of the connected-vehicle fleets as it becomes more challenging to revoke certificates in real-time. We have proposed a new method that integrates a decentralized, collaborative system to meet these challenges. This method efficiently allows Blockchain integration for vehicular network's cyber security by dynamically creating communities to revoke malicious vehicles in real-time. This article presents analytical models of the system of real-time revoking certificates and examines our solution's impact on two important types of attacks in V2X communications, Sybil and the faking position attacks. Our experiments using real V2X hardware demonstrated the feasibility and benefits of real-time revocation via vehicle communities. The results were obtained from consensus implementation in a vehicular network comprising three communicating vehicles and a single roadside unit. In parallel, simulations showed feasibility in large-scale communications. As a result, the exposure and detection times of our solution meet real-time requirements.

INDEX TERMS Intelligent transport systems, blockchain consensus, certificate revocation, dynamic clustering.

I. INTRODUCTION

In vehicular communications (V2X), there are promising technologies for solving intelligent transport system (ITS) problems such as accident prevention, traffic monitoring, and transport efficiency. V2X communications rely on types of communicating equipment [11]: on-board units (OBUs), installed in the vehicles, and the road side units (RSUs), deployed alongside the road. Safety-related messages are periodically broadcast over the control channel (CCH) by the OBUs with information on the status of the vehicle. ITS communication contains a vulnerability that makes it possible to track drivers' identities even over more extended periods. Thus, it tracks and creates vehicle movement profiles, representing privacy breaches for vehicle users. Complete anonymity of all network participants is not a viable countermeasure, because critical security systems require data authenticity and participant responsibility. Security authorities must ensure the OBUs' confidentiality, registration, and authorization. The responsibility for verifying the validity of their canonical identifiers is entrusted to an enrollment authority (EA), whereas an authorization authority (AA) distributes access to services. These two authorities are part of the necessary Public Key Infrastructure (PKI) and must be operated in different control domains to achieve additional privacy. Vehicle request-response message schemes require at least short-term message binding capability to establish a joint session. For example, authentication is needed to request data from the infrastructure or manage automatic payment on car chargers. A widely chosen approach to restoring user privacy is to use temporary pseudonyms for identification in the network. This poses a major problem with Certificate Revocation (CR). Since temporary certificates are designed for non-traceability, it becomes almost impossible for vehicles to identify malicious pseudonyms or for the certificate authority (CA) to

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

identify malicious behaviors. This vulnerability could cause two major types of cyberattacks linked to vehicles' position: position-spoofing and the Sybil attacks.

In this article, we propose a new scheme of consortium blockchain for cybersecurity purposes. Our system is based on a Smart Contract and consensus that allows vehicles to detect and revoke malicious vehicles in real time. First, our framework is designed to integrate blockchain technology for cybersecurity purposes against fake position-based attacks. Second, it aims to create dynamic blockchain networks for decentralized trust management in-vehicle networks. Furthermore, it cooperatively enables revocation between vehicles, taking pseudonym changes into account.

This article is organized as follows: The II section gives an overview about clustering, certificate change strategies, and their revocation, and finally, we talk about common cyberattacks in V2X communications. Then, in section III, we detail our proposed solution and revocation algorithm. After that, we present our experimental results using real V2X equipment and we validate the effectiveness of our consensus by means of simulations, see section IV. Next, the results are discussed in section V. Finally, section VI concludes our article, presenting valuable information about our work and prospects.

II. REVIEW OF RELATED WORK

A. CLUSTERING

The existing clustering protocols in V2X communications are broadly divided into five sub-categories: position-based protocols [26], [38], route discovery protocols [28], [45], broadcast protocols [44], infrastructure-based protocols [29], and cluster-based protocols [18], [23], [32], [41]. El Houda *et al.* [2] used a Smart Contract to design a blockchain-based solution (Cochain-SC) to guard against the DDoS collaboration attack. In Cochain-SC, blockchain enables low-cost decentralized security and collaboration between multiple SDN domains to mitigate attacks using clustering techniques. In addition, the authors of [20] consider the reliability of links for clustering. However, this scheme takes fixed arrival rates for nodes on the highway, which remains unrealistic. Based on V2X communications, in recent years some authors [7] have proposed using a heterogeneous network, using IEEE 802.11p and cellular communication. Next, Liu *et al*. [25] proposed a reliable and stable communication scheme using clustering and probabilistic diffusion. This scheme was based on vehicles communications. With this method, a vehicle could broadcast data to other vehicles within connection time. In addition, this system could also improve the coverage rate. However, during vehicle-to-vehicle communications, this system could not detect malicious vehicles, leading to data insecurity.

B. CERTIFICATE CHANGE STRATEGIES

Privacy is considered one of the most critical issues in V2X communications. While vehicles exchange their locations and identities, malicious nodes can track their information and threaten their privacy. PKI authorities use pseudonyms as a solution to protect vehicles from tracking-attacks. Standards proposed several pseudonym schemes to keep the vehicles' identities secure [30]. Contributions argue for occasional pseudonym reloads to intermittent connectivity with pseudonym issuing authorities; these are changed periodically to prevent the tracking of pseudonyms. The confidentiality of users in relation to authorities can be protected by dividing responsibilities between the pseudonym CA (PCA) and the long-term CA (LTCA) as suggested by the CAR 2 CAR Communication Consortium [6]. In addition, data transferred in the V2X network can be modified by an attacker to mislead vehicles, which can lead to traffic accidents. Appropriate security schemes can be adopted, but this could cause additional latency [31]. This is of utmost importance in emerging intelligent connectivity networks, leveraging cloud-based capabilities to support critical security services with stringent security, trust, and privacy requirements [16]. Yang *et al.* [48] proposed two lightweight anonymous authentication schemes for the V2X network. One scheme is applicable for V2V communication, while the other is suitable for V2I communication. Both schemes considered limitations of V2X, such as OBU resource constraints and latency. He *et al.* [3] introduced the preservation of confidentiality based on a security scheme for V2V and V2I communications in VANETs. This scheme uses elliptical curve cryptography (ECC) rather than bilinear pair operation during the diffusion procedure. This scheme supports a batch verification process to authenticate all messages related to the V2X environment state. A random oracle model related to a message's authentication provides authentication between the signer and the receiver. Nowadays, certificates changes strategies remain a challenge for the cybersecurity of V2X communications.

1) PSEUDONYMS MANAGEMENT

To ensure vehicles' confidentiality, the standard [46] mentions the objective of pseudonymity and the dissociation of ITS nodes' identities from their messages. This privacy objective is subdivided into two dimensions: authorities must ensure vehicle registration and authorization confidentiality by limiting knowledge of a node's canonical (fixed) identifier to a limited number of authorities. The enrollment certificate (EC) contains an alias ID signed with a certificate chain that refers back to the originating EA. This EC can then be used to obtain authorization tickets (ATs) from an AA. These ATs are also certificates indicating the authorizations of a node. Authorization ticket certificates can be stored in a hardware security module (HSM) to prevent unregulated direct access to cryptographic keys; the security service specification provides such an option. All authority responses are encrypted and verifiably signed for the node. Certificate requests include a start time and an end time, as well as challenge [13], a random string encrypted with the receiver's public key. Both of these measures prevent replay attacks.

TABLE 1. Table of contributions in the various fields related to our work.

		Centralized architecture	Decentralized architecture	V2X Communications	Blockchain			
					All-nodes-centric	OBU-centric	RSU-centric	RCA-centric
Clustring	[2] [23]		X		X			
	[20]		X					
	[18]		X	X		X		
	[7]	X		X				
	[36] [25] [33]		X	X				
Pseudonym changing and Credential Management	[19] [31] [3]	X		X				
	[39]		X					X
	[48]		X	X		X		
Certificat revocation	[22] [21]		X	X				
	[17] [3]	X		X				
	[27]		X	X		X	X	X
Sybil attack detection	[51] [47] [37] [43]		X	X				
	[50]		X	X		X	X	X

Credentials and ATs can also be updated as needed through similar mechanisms. The ETSI survey also gives an overview of strategies used in existing projects standards.

C. CERTIFICATE REVOCATION

In recent years, few studies have been proposed on certificate revocation list (CRL) distribution methods [22]. The revocation of pseudonym certificates is generally limited to revoking the vehicle ID for scalability reasons. If the long-term identity is revoked, the OBU cannot get new pseudonyms (PC). Additionally, letting OBUs check other vehicles' PCs against Certificate Revocation Lists (CRLs) would be impractical due to the high message frequency and potentially voluminous CRLs, especially in heavy traffic scenarios. In [21], the authors proposed an approach for revoking certificates based on the region of operation.

Only a few trust models have recently been proposed to enhance honest information-sharing in-vehicle networks. In terms of security and confidentiality by establishing trust in VANETs, which are based on security infrastructure, most models often use certificates.

Almulla *et al.* [4] proposed a k-means clustering approach for validating certificate revocation in VANETs in which detailed system security analysis has been provided. The scheme improves certificate validation and thus enhances the security of communications within the scheme.

Malik *et al.* [27] propose a framework for authenticating and revoking transactions. It authenticates vehicles with mitigating reliance on a trusted authority and quickly updates the status of revoked vehicles in the blockchain ledger shared with the PoA mechanism. In [49], the authors present a blockchain-based event validation scheme to verify every event that occurs on the road. However, there is a need for an incentive mechanism to encourage vehicles to participate in the event validation process.

D. POSITION-RELATED ATTACK DETECTION

In V2X communications, vehicles and infrastructure continuously exchange traffic safety and navigation messages. As a result, these messages are exposed to various attacks such as denial-of-service (DoS), Sybil, and false alert attacks, which may disrupt the traffic flow and cause accidents. We cite Bin Xiao *et al.* [47] reserved for the detection and localization of Sybil attack in VANET nodes. Authors in [51] have proposed a Sybil detection method based on received signal strength indicator (RSSI) named Voiceprint. It relies on RSSI time series as vehicular speech.

Ruj *et al.* [37] propose using a data-centric misbehavior detection system in order to detect false location information. It works by classifying data instead of classifying vehicles. Each vehicle can verify the location information independently by using the proposed technique. This leads to fines imposed on attackers instead of isolating them from the network. Yang *et al.* [50] proposed a Sybil detection scheme based on motion similarities among vehicles by using three ML classification models.

In the Table.1 we compare our solution and the other papers cited above.

III. PROPOSED REAL TIME REVOCATION FRAMEWORK

In this paper, our work focuses on proposing a real time cooperative revocation system using a clustering algorithm. We propose a distributed algorithm in which each communication node initiates its own process by executing a Smart Contract. It creates a cooperative communities that contain sets of vehicles that participate in their local blockchain and agree on each vehicle behavior.

A. SYSTEM MODEL

All vehicles are assumed to be equipped with a GPS system that provides the vehicle's basic information and an ITS-G5 system communicating based on the *IEEE*802.11*p* standard. The broadcasted information includes the vehicle's current location, velocity, and direction. Moreover, each vehicle can calculate speed and detect the RSSI rate of received messages using its communicating module. Periodic status information, such as beacons or CAM messages, is broadcasted by each vehicle to its neighbors every 0.1 seconds. The traffic management center (TMC) plays a significant role in disseminating messages, as it can reach every vehicle using cellular

TABLE 2. Abbreviations and symbols.

Abreviation			
TMC	Traffic management center	CRL	Certificate revocation list
CA	Certificate authority	OBU	On-board unit
RSU	Roadside unit	PoL	Proof of location
CAM	Cooperative awareness message [10]	PC	Pseudonym certificate
Symbols			
G_{com}	List of community members	$Clus_{for}$	The cluster formation message
Δ_v	Relative velocity between vehicles	Δ_D	Relative distance between vehicles
ID_{clus}	The community identifier	$List_{com}$	List of vehicles likely to contribute to the community
NS	One-hope neighbor table	P_r	Received power (RSSI)
Pos	Vehicle's position	N	Number of community's vehicles
Sp	Vehicle's speed	Hd	Vehicle's driving Heading
T_{link}	Estimated time of communication link between vehicles	T_{life}	Estimated lifetime for community communication
T_{har}	Time ID identification	T_{link}	Estimated time of communication link between vehicles
T_{Tlife}	Estimated lifetime for community communication	T_{th}	Efficient threshold time for community contributions

technology. Our Blockchain consensus model is based on proving each vehicle's position in the clusters and sharing decisions about vehicles' behavior among all participants. The position-proving process is in peer-to-peer mode. The witness provides proof-of-location (PoL) to the prover.

There are N vehicles in the vehicular network, and we assume N to be fixed in time. For $i = 1, \ldots, N$, the *i-th* node, N_i is associated with a position, represented, as $Pi(t) = (x_i(t), y_i(t))$ at time t. The nodes are users of a PKI. We define a communication range, also called coverage area, for each node, as a circle of radius R having the node as its center. If V is the set of all vehicular network nodes, i.e., $V = N_i : i = 1, \ldots, N$ then we define the neighbor set of a node N_i at time t, as the set of nodes V which are in i's communication range at time t; more formally defined as $NS_i(t) = \{j \in Vi : \|(P_i(t), P_j(t))\| \leq R\}$.

Each communicating vehicle is assumed to have its own credentials, corresponding to the IDs it uses in community communication. The asynchronous accumulator acts as the initial accumulator for the CRL. Each user registers with the credential issuance authority.

The authority checks the validity of the user by consulting the dynamic asynchronous accumulator within the blockchain.

Since vehicles are resource-limited devices, the problems of building a distributed network structure have been examined in [15]. In this work, we propose to use a chain made up of only limited communities. Each vehicle contributes to the community according to the parameters and capabilities used in the vehicle subnet. Below we take a more detailed look at the proposed version of the block structure.

B. COMMUNITY CONSTRUCTION

This part is the first step of our framework process for determining how vehicle clusters, called communities, (local blockchain networks) are constituted. We attempt to construct communities and to enable a cooperative process to transmit periodical CAM messages. When initialized, the vehicle does not yet have any knowledge of its neighborhood. When the vehicle is switched on, its wireless communication module starts to transmit periodical CAM messages. When initialized, the vehicle does not yet have any knowledge of its neighborhood. to detect and revoke malicious vehicles. The community construction process is triggered when the vehicle receives multiple CAM messages, also called beacons, with different pseudonyms.

Vehicles are aware of their surroundings via the CAM messages. Once a vehicle receives the CAM messages, it records the vehicles' *IDs* in a time T_{har}. and sends the list to the TMC. Thus, the TMC, therefore, receives several lists after the time T_{har}. After concatenating the lists, the TMC obtains a graph. Then, based on the graph rules specified in subsections bellow, the TMC issues the community's start list with a cluster ID (ID_{clus}). The vehicles in the community will use their pseudonyms as tokens to sign transactions in order to avoid any risk of tracking.

1) ONE-HOP NEIGHBOR TABLE

At the beginning of the clustering procedure, each node is in an initial state. Then, the system starts a timer, called T_{har}, during which vehicles exchange and collect Beacons to discover their one-hop neighbor table (NS). For example, a CAM message received by a node V_i from a neighbor node V_j triggers a routing table. Then the neighbor sampling process selects a set of stable neighbors, denoted as Graph G where $G \subset NS$.

2) CLUSTER PROCESSING

The *TMC* is responsible for this step. First, the *TMC* must processes the vehicles' conditions in order to identify the best OBU candidates for the community. Then, it selects the cluster head (CH) which maintains the cluster.

The *NS* represents a neighboring vehicle list that presents a similar mobility pattern, moving in the same direction. $Hd_{V_i} = Hd_{V_j}$ these are the driving headings of V_i and V_j. The *TMC* decides then if the vehicle can be a candidate for the community. For that, the link time (T_{link}) must be smaller than the predetermined threshold T_{th}:

$$T_{th} = \frac{(R - (\frac{1}{QT_{max}}))}{VT} \tag{1}$$

where QT_{max} is the maximum value of the density of vehicles (vehicle per Kilometer $-Vh/Km-$) the *TMC* had on its road network for the same period, the 5 or 10 past years, VT is the estimated value of the vehicles' speed (Km/h) in the *TMC* network. All *TMCs* have easy access to these values since they represent important parameters for traffic management.

The community should have a lifetime, T_{life}, to avoid a hacker having a monopoly on it. This is calculated based on the average life of the link, T_{link}, between vehicles.

$$T_{life} = \overline{T_{link}} = \sum_{j=0}^{N_i} \frac{(R - \overline{\Delta D_{ij}})}{\overline{\Delta v_{ij}} * N_i} \leq T_{th} \tag{2}$$

where $\overline{\Delta D_{ij}} = \|(P_i(t), P_j(t))\|$ and $\overline{\Delta v_{ij}} = v_i - v_j$ are respectively the average distance between V_i and V_j and the average of their relative velocities.

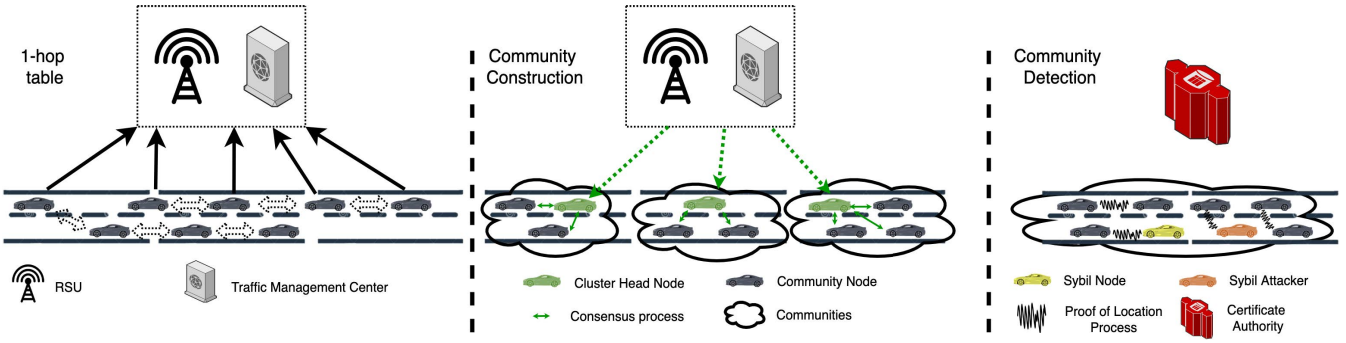


FIGURE 1. The three main steps in community process; 1-Hop table, community construction, community detection.

The selection of the cluster head will be based on the metric T_{life} in Eq(2). The vehicle having the longer link time is the most likely to take the cluster head. In our proposition, the CH receives the list ($List_{com}$) of vehicles that may likely contribute to the community.

3) CLUSTER FORMATION

When a vehicle V_j receives a cluster formation message from TMC Eq(3), it immediately sends a $ReqJoin = Sig_{V_j}(\{Clus_{for})\}$ message to CH_i. After CH_i receives the ReqJoin message, it first checks whether this ID is available in $List_{com}$. If so, CH adds V_j to its cluster member list G_{com} and sends back a *ACKJoin* message; otherwise, it ignores the request to join.

$$Clus_{for} = \{Sig_{TMC}(ID_{CH}, ID_{Clus})\} \tag{3}$$

4) PSEUDONYM CHANGING

The Pseudonym Certificates (PCs) are stored and managed in pseudonym pools, with their corresponding private keys kept in the Hardware Security Modules (HSMs). To keep the privacy of vehicles and avoid tracking or linking their real identities to the used pseudonym certificates, the PCs are changed frequently according to various rules [46]. This ensures that each vehicle has precisely one key pair (own pseudonym and private key) active during each period. Vehicles cannot reuse the pseudonym once it has been changed, even if the certificate has not yet expired.

Due to the highly dynamic nature of VANETs, vehicles keep joining and leaving clusters frequently. Vehicles that apply for the strategies of changing pseudonyms are considered new. Once the vehicles change their PCs, by giving a new identity to the cluster with a new pair of keys, the network assumes them new, in which case they must seek to join the cluster; therefore, they must proceed to re-clustering. The process of re-clustering guarantees that a vehicle could find a proper cluster to follow as long as it foregoes contact with its current G_{com}. However, a long delay in the re-clustering process may lead to severe consequences, primarily when implemented delay-sensitive applications [8]. This is why we propose that the best link-time be calculated in real-time so that the cluster header can be changed. Other solutions are proposed by [33] to solve the problem of re-clustering delay.

In order to maintain the privacy of the vehicles that join the blockchain and also to ensure the stability of the cluster, we propose to use the community changing strategy described by [40], which aims to make all vehicles change their pseudonyms at the same time with a period of silence afterward. Therefore, this makes tracking one of the community vehicles a challenging task for hackers.

5) ISOLATED VEHICLES

In our system of real-time revoking certificates, vehicles could be isolated for two reasons:

- Pseudonym changing,
- Revoked certificates.

Despite the insulation of these vehicles, they remain open to receiving messages. However, these could no longer contribute to the revocation process or the declaration of messages relating to road safety. The change of pseudonyms is always followed by a period of silence as indicated in [14], this could harm the vehicles in critical situations, such as the vehicle will no longer be known to its neighbors. In this case, the vehicle must keep the same PC during the critical period called Time-To-Crash (TTC) [12]. Therefore, the vehicles subscribed in the clusters will fulfill their communication role in critical situations as they must keep the same PC and will not be isolated as long as they "good behave."

C. COMMUNITY DETECTION

1) PROOF-OF-LOCATION CONSENSUS

Misbehavior detection in V2X communication has been well studied (see Section II-D). To evaluate our solution, we have used the detection model developed in our previous work, based on the proof-of-location (PoL) process. It aims to detect any attack from Sybil to position-faking attacks.

In our previous work [9], we proposed a new security architecture based on consortium blockchain cryptography which is built upon consensus-based PoL. In this work, our algorithm aims to give an accurate decision based on fluctuating RSSI values. The communication between the prover and the witness should be estimated based on N number of

Algorithm 1: Algorithm of Community Construction

Input: $Pos_{w/p}$; P_r; $Hd_{w/p}$; $Sp_{w/p}$; N
Output: G_{com}
Function `One-hop neibor Table` ($T_{har}[]$, $Sp_p[]$, $Pos_p[]$) **:**
  while $T_{har} > 0$ **do**
  if V_i *receives Beacon from* V_j **then**
    if $Hd(i) == Hd(j)$ *and* $v_{ij} < v_{th}$ **then**
      if $V_j \in NS_i$ **then**
        V_i Update $NS_i(j)$
      end if
    end if
  end if
  else
    V_i adds the entry $NS_i(j)$ to NS_i
    $n_i = n_i + 1$
  end
return NS_i, n_i
End Function
Function `Cluster Processing` ($NS_i[]$, V_i, n_i, Sp_i, Pos_i, Hd_i) **:**
  $CH \leftarrow V_1$
  $T_{linkCH} \leftarrow T_{link1}$
  if *TMC receives* $NS_i[]$ **then**
    while $T_{har} > 0$ **do**
    TMC calculates T_{linki}
    if $T_{linki} < T_{th}$ **then**
      $T_{link}[]$ add T_{linki}
      $List_{com}[]$ add V_i
      if $T_{linki} > T_{linkCH}$ **then**
        $T_{linkCH} \leftarrow T_{linki}$
        $CH \leftarrow V_i$
      end if
    end if
  end if
  TMC calculates T_{life} from $T_{link}[]$
  return CH, T_{life}, $List_{com}[]$
End Function **Function** `Cluster formation` (CH, $List_{com}[]$) **:**
  if $T_{har} = 0$ **then**
    CH receives $ReqJoin_i$ from V_i
    if $V_i \subset List_{com}$ **then**
      G_{com} add V_i CH sends $ACKJoin_i$ to V_i
    end if
  end if
  return G_{com}
End Function

beacons received from the prover as shown in Fig.2, the N value should be estimated based on their relative velocity. the PoL process is detailed in [9].

The PoL algorithm has an output of three major indicators that permit to identify position-faking attacks, I_1, I_2, I_3

- Indicator 1 (I_1): Indicates average speed and calculates distance traveled by using the prover's traces.

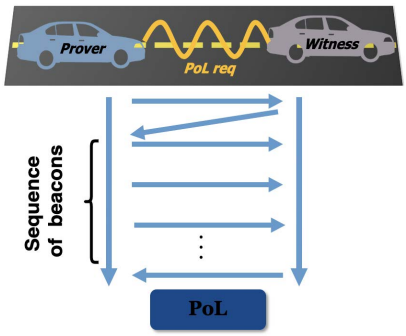


FIGURE 2. The proof-of-location process between the prover and its witness.

- Indicator 2 (I_2): Using RSSI, we estimate the distance between the witness and the prover using the Friis equation and the budget-link formula. Then, based on the prover's declared position, we compare the declared distance between them.
- Indicator 3 (I_3): This indicator represents the communication quality conditions between the witness and the prover. It takes into account the information of the two vehicles to evaluate the accuracy of the witness's detection (i.e., how well it can verify signal strength and distance from the prover). We calculate it based on vehicles' velocities, headings, and yaw rates (and weather can also be considered). Relative velocity greatly impacts the accuracy of RSSI measurements due to the Doppler effect, and heading and yaw rate provide information concerning the line of sight.

$$PoL = (PoL_{Acc}, PoL_{rate}, Pos_p, t_w, Cer_w, S_w[PoLreq, t_w, Kp_p]) \quad (4)$$

where $PoL_{Rate} = \frac{I_1+I_2}{2}$ is the indicator rating the probability of detecting a Sybil attack, and $PoL_{Acc} = I_3$ gives detection accuracy based on the measuring conditions.

In order to deal with the RSSI values with high dynamic fluctuations in a mobile environment, we have made an extension on the results obtained in the framework of the tests carried out in [9]. The PoL accuracy is inversely related to the velocity, as shown in Fig. 3 and Fig. 4, the high velocity significantly impacts the distance estimation based on the

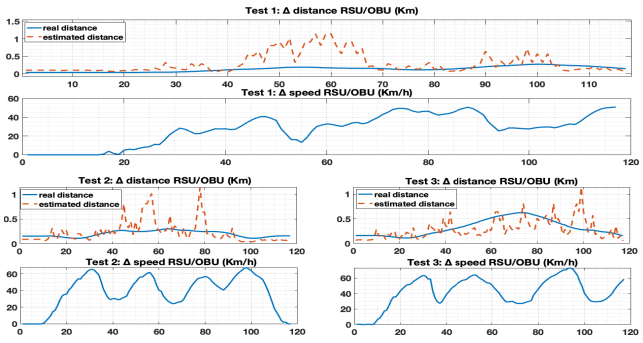


FIGURE 3. The proof-of-location process between the prover and its witness.

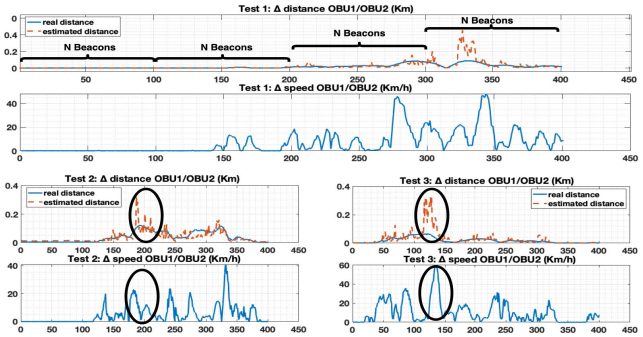


FIGURE 4. The proof-of-location process between the prover and its witness.

TABLE 3. Impact of the velocity of the communicating nodes on detection accuracy.

		Test 1	Test 2	Test 3
I2V mode	Velocity (km/h)	31.60	43.11	46.08
	ACC	41.10%	56.75%	48.07%
V2V mode	Velocity (km/h)	12.27	8.56	15.33
	ACC	72.47%	75.44%	67.12%

RSSI. Therefore, the fluctuation rate of the RSSI-based estimation error depends only on the velocity between the two communicating devices. We have dressed a table to compare the fluctuation between and relative velocity in the V2V communication mode (OBU1 and OBU2) and I2V mode (RSU and OBU). We have demonstrated the importance of integrating vehicles in the detection process. The V2V communication mode can also resist the RSSI fluctuation problem as in the highway, the relative velocity between two vehicles in the PoL is mainly reduced as they drive nearly at the same speed.

Nevertheless, the V2V communication mode could not solve the fluctuation problem entirely. Therefore, our Proof of Location consensus algorithm has proposed an additional mechanism to guard against the Sybil attack and consolidate the vehicles' detection accuracy. Our solution allows an average on the N report of the level of RSSI, which leads to better accuracy, as it is based on the collection of multiple consecutive RSSI reports, of in the worst case, the vehicles with which there will be a high velocity will eventually disappear since it will no longer be within the range of the broadcast.

2) COMMUNITY PROCESSING

Before starting to prove other vehicles' positions, vehicles look for affinities with neighbors in order to establish bilateral communication with the "best" partner.

$$r_t(l) = \int_t^{t+T_{th}} f(T)dt \tag{5}$$

Let $G(V, E, r)$ be a vehicular topology, where V is the number of vehicles, E is the ordered pair of links among vehicles and r represents link reliability. The representation of a given vehicle's graph topology $G(V, E, r)$ is traced by vector A and matrix B of dimension $V \times V$. Once the community is constituted (Section III-B), each vehicle has to calculate the vector of link reliability with all surrounding vehicles using Eq(5). The reliability level of N surrounding vehicles will be included in vector A:

$$A = \begin{pmatrix} r_{ID_1} \\ r_{ID_2} \\ \cdots \\ r_{ID_n} \end{pmatrix} \tag{6}$$

For total detection, the vehicles transmit the *PoL* to one vehicle at a time, in order of preference in terms of the reliability of the link. After sending the vector A, one vehicle proposes a handshake process to another, and it sends its PoL to others down its list. Each pair of vehicles must agree to send each other a *PoL*. The prover must then go down the entire list of *IDs* in its vector *A* before starting peer-to-peer proving with vehicles for the second time.

D. COMMUNITY REVOCATION

In this section, the community must make a joint decision to revoke a given vehicle. The result of the detection is made based on the smart contract. After choosing a prover, the witness must process the smart contract in order to provide detection Matrix B, which contains the information concerning N vehicles of community G based on Eq(4) as given below:

$$B = \begin{bmatrix} Pol_{11} & Pol_{12} & Pol_{13} & \cdots & Pol_{1n} \\ Pol_{21} & Pol_{22} & Pol_{23} & \cdots & Pol_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ Pol_{m1} & Pol_{m2} & Pol_{m3} & \cdots & Pol_{mn} \end{bmatrix}$$

In order to detect malicious vehicles, we use a spectral clustering tool in Laplacian graph matrix. Once the detection matrix B is computed, the Laplacian graph L is computed as $L = D - B$, where D is a diagonal matrix.

Eigen decomposition involves the factoring of a matrix in terms of its eigenvalues and eigenvectors [20]. In the literature [5], in fast-evolving networks with high dimensionality of data, spectral clustering becomes the only option. Eigen decomposition can be used to reduce dimensionality of mobile vehicles. Suppose that J has non-degenerate eigenvalues $\lambda_1, \lambda_2, \lambda_3 \cdots \lambda_n$ and corresponding independent eigenvectors $X_1, X_2, X_3 \cdots X_n$. Then matrix Z, composed of eigenvectors, is:

$$Z = [X_1, X_2, X_3 \ldots X_n] \tag{7}$$

By the end of the detection, matrices are supposed to be given simultaneously in peer-to-peer communications. Each vehicle identifies suspected IDs by means of mean eigenvalue and the smart contract. The community processes each vehicle decision and uses a consensus mechanism to reach agreement.

To feed the real-time CRL of revoked credentials, we use the asynchronous accumulator (explained in more detail in [34]), generating an extra secret for each certificate.

E. BLOCKCHAIN STRUCTURE

After forming the chain, the nodes produce an item-by-item check of the final community. The blockchain must contain all the information of each community steps?. Our proposed blockchain is constructed as follows: In Fig.5, we present the structure of each community structure, where N is the number of the community's vehicles.

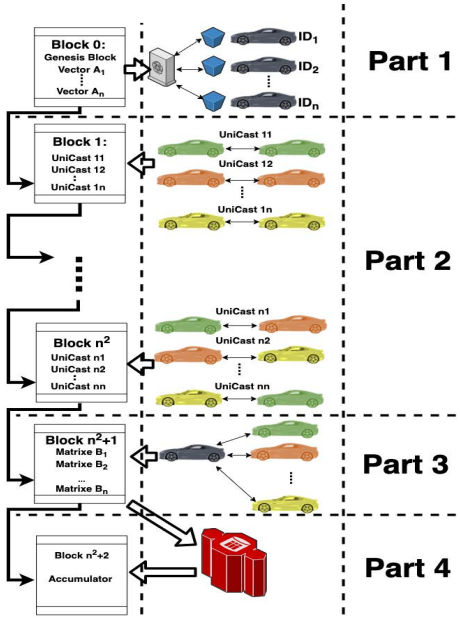


FIGURE 5. Blockchain's global parts.

Part 1: All nodes record the genesis block 0, which must contain the vector A provided by all the community vehicles. The miner in this first step is the *TMC* that supervises the community construction, making sure that only selected vehicles can communicate in the community.

Part 2: Lasts from Block 1 to Block n^2. These blocks are created to register the peer-to-peer combinations of the PoL process between each pair of vehicles in the community. In each round of proving, a block is created to describe the combination of provers. The miner of all these blocks is chosen based on the minimum average of vector A, which indicates that it is the vehicle that is the closest to all other community vehicles.

Part 3: Marked by the block $n^2 + 1$, which must contain all the B matrices generated by the community vehicles.

Part 4: The Block $n^2 + 2$ is characterized by the final decision concerning suspected malicious vehicles that should be aggregated into the asynchronous accumulator.

Each community's node should keep track of all transactions it has learned about waiting pool, partitioned into mutually. The waiting pool can be considered a dynamic memory in which transactions that have not yet been published are waiting to be transcribed into a block. Every transaction should include the blockchain part number and should be broadcast among vehicles for global dissemination. Table.4 shows the composition of transactions.

TABLE 4. Transaction composition.

Transaction Header	
Blockchain part	Indicates the smart contract
Merkel tree root hash	The hash value of transactions
Signature	The issuer's signature
Time stamp (s)	Current universal time

F. SMART CONTRACT

Once the vehicle get into the community it should get the genesis Block that contains the Smart Contract. As shown in Fig.6 our smart contract is considered as a finit state machine, where every part is a vehicle state.

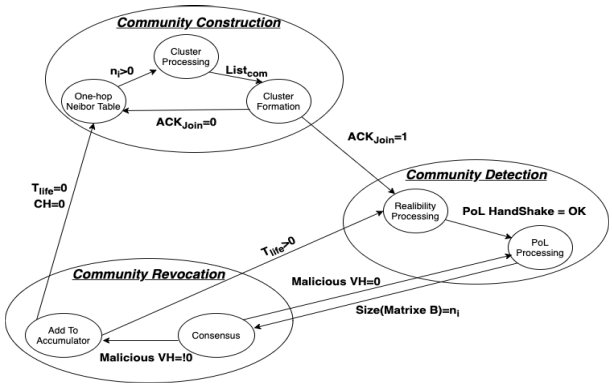


FIGURE 6. Communities steps of an algorithm state machine.

G. CONSENSUS

Once the vehicle get access into the community, the transmitted transactions indicate the state of the blockchain to the vehicle.

Part 1: the *TMC* is responsible for generating the genesis block with the smart contracts.

Part 2: The consensus in this part is based on the results of the genesis block, in that the miner of the blocks is selected based on the minimum of the sum of the vector's A values.

Part 3: This part is the most important for our consensus process, in which the vehicles must reach consensus to produce block $n^2 + 1$, which contains the B matrices for all vehicles. For that, we use the Paxos consensus algorithm [24].

Part 4: The consensus is held on the last block (Block $n^2 + 2$) of the blockchain in order to declare vehicles malicious. The decision is based on the agreement of more than 50% of the vehicles in the community. The trust authority is responsible for aggregating agreement and constructing the block.

IV. PERFORMANCE EVALUATION

To evaluate performance, we have examined metrics using results captured from real-life experiments. These experiments tend to demonstrate the effectiveness of our proposed method using real vehicular communications. Simulations indicate that our solution will perform well in large-scale implementation.

A. EXPERIMENTS

1) EXPERIMENTS SETUP

We used three vehicles equipped with 3 OBUs, 1 RSU, and 2 USRP (Universal Software Radio Peripheral) cards. Fig.7 shows the campus, the road tests, and the material we used to test four different scenarios.

FIGURE 7. Experiment's equipements: In the green circle, the RSU installed in the campus and red circle the computer with the two USRP cards to simulate the attack messages.

To obtain detailed results in terms of communication conditions, we experimented with four different scenarios. Fig.7 shows the campus and the road tests we point to the material used.

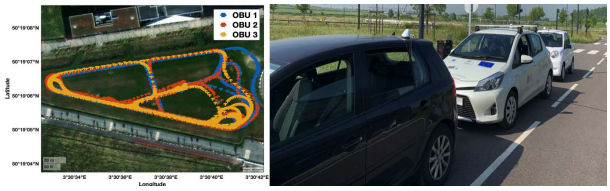


FIGURE 8. Setup for campus scenarios.

We experimented with the community revocation process by creating/simulating a Sybil attack and a position-faking attack. We evaluated to fake the community decision by sending faked messages using USRPs.

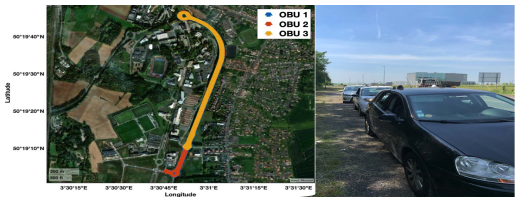


FIGURE 9. Setup for route scenarios.

We evaluated our systems under different conditions for the exclusivity of the data and the situations tested, in four different scenarios. In all scenarios the USRPs have performed as the attacker, whether in static or dynamic way.

- *Scenario 1 (Campus static test):* The first scenario was performed on the campus circuit with the static attacker (USRPs cards).
- *Scenario 2 (Static Road Test):* The second scenario took place on the driving road with the static attacker.
- *Scenario 3 (Dynamic Campus Test):* The third scenario took place on the campus circuit with the dynamic attacker.
- *Scenario 4 (Dynamic Road Test):* The fourth scenario was done on the driving road with the dynamic attacker.

2) METRICS

Three metrics are considered for the accuracy detection rate: the true positive rate (TPR) (8), the true negative rate (TNR) (9), and detection accuracy (ACC) (10), which are defined in [50].

$$TPR = \frac{TP}{TP + FN} \tag{8}$$

$$TNR = \frac{TN}{FP + TN} \tag{9}$$

$$ACC = \frac{TP + TN}{TP + FN + FP + TN} \tag{10}$$

where TN represents true-negative decisions; FN represents false-negative decisions; TP represents true-positive decisions; FP represents false-positive decisions.

To calculate the variation of witness proofs, we have estimated σ, which is the variation of *PoL* reports sent during communication.

3) DETECTING A FALSE POSITION ATTACK

In this part, we compare detection accuracy, based on our *PoL* algorithm applied by each vehicle, to the accuracy of our revocation framework.

In Fig. 10, we show the profile perceived by the witnesses (OBU 1, 2, and 3). We have concatenated the time series of all scenarios tested for each vehicle in each scenario in Appendices.

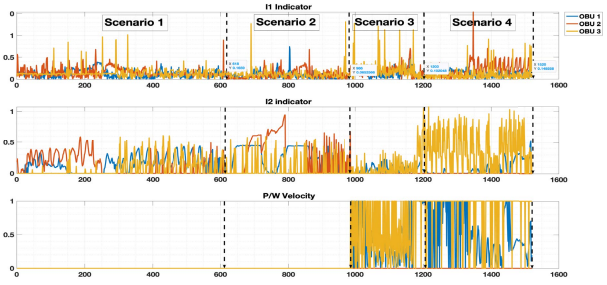
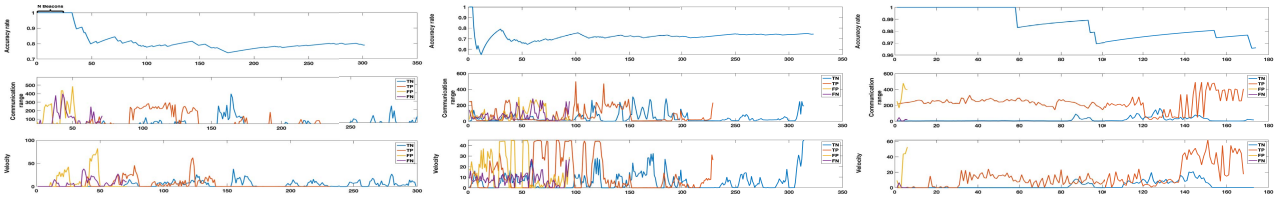


FIGURE 10. All malicious nodes reports.

Fig.10 is based on the reports as well as on information such as velocity and average speed and our two indicators. We have analyzed the reports on each communicating node (OBU). Fig.12, shows each vehicle's profile. We have reported the different indicators from each witness in each scenario.

Based on the mean and the variance of *PoL* indicators, each vehicle decides whether or not to trust another vehicle. Table.5 shows the results obtained from the peer-to-peer PoL process. We did not register a high accuracy rate in scenarios 1 and 2 because of the high relative velocity because the hacker is static. However, scenarios 3 and 4, in which the hacker was mobile, present a better accuracy rate.

We illustrate in Fig 11 the ACC indicator evolution according to the communication range between the witness and the provers, where we detail the evolution of the four indicators (TN, TP, FP, and FN) for each point of the time series. The



(a) OBU 1's reports accuracy (b) OBU 2's reports accuracy (c) OBU 3's reports accuracy

FIGURE 11. Each OBU's accuracy rate.

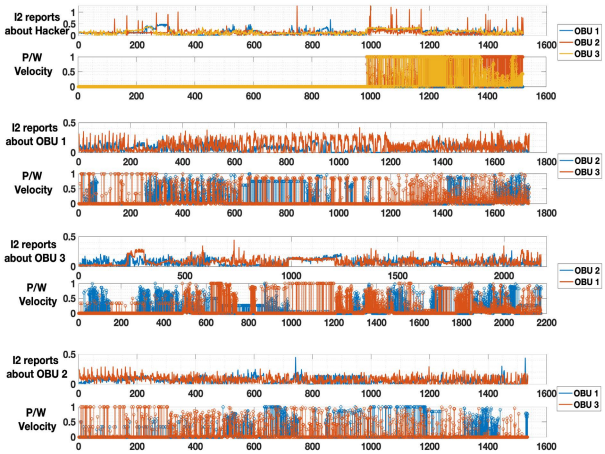


FIGURE 12. All trusted vehicles reports.

TABLE 5. Indicators results for peer-to-peer communication for each scenario, Where δ_{vel} is the relative velocity between both nodes, σ and ACC.

		OBU 1			OBU 2			OBU 3		
		Hacker	OBU 2	OBU 3	Hacker	OBU 1	OBU 3	Hacker	OBU 1	OBU 2
Scenario 1	δ_{vel} (Km/h)	6.32	3.16	2.91	14.59	7.46	4.98	7.60	3.60	3.54
	σ	0.0876	0.0563	0.0276	0.1362	0.0633	0.0659	0.1557	0.0083	0.0038
	ACC		65.80%			44.26%			98.41%	
Scenario 2	δ_{vel} (Km/h)	24.60	7.02	6.66	16.99	3.53	6.88	8.58	5.46	4.32
	σ	0.1476	0.1246	0.0467	0.1331	0.0746	0.3228	0.4119	0.0239	0.0408
	ACC		50.32%			31.87%			77.77%	
Scenario 3	δ_{vel} (Km/h)	0	2.35	3.12	2.85	2.85	2.61	5.51	4.12	2.90
	σ	0.0116	0.0183	0.0094	1.6055	0.0359	0.0149	5.1247	0.0024	0.0093
	ACC		87.30%			77.77%			100%	
Scenario 4	δ_{vel} (Km/h)	0	3.44	4.21	7.94	6.26	5.92	38.19	5.97	3.45
	σ	0.020	0.0962	0.0229	0.15	0.0618	0.0708	0.5708	0.0030	0.0631
	ACC		63.01%			70.90%			85.29%	

witness must collect N Beacons to give a PoL as shown in Fig. 11a. We have applied our algorithm to each of the OBUs as shown in figures 11a, 11b and 11c the accuracy rate of the peer-to-peer PoL process of each OBU.

In the first subplot of each figure, we show the evolution of the accuracy of the OBU over time. The communication range and velocity are shown in the second and third subplots. False/True Negative decisions represent witness reports against "Trusted" OBUs. In contrast, False/True Positive decisions are evidence against the Hacker. We notice that the two indicators, communication range, and velocity, significantly impact the witness's accuracy.

These indicators impact is reflected in the following examples:

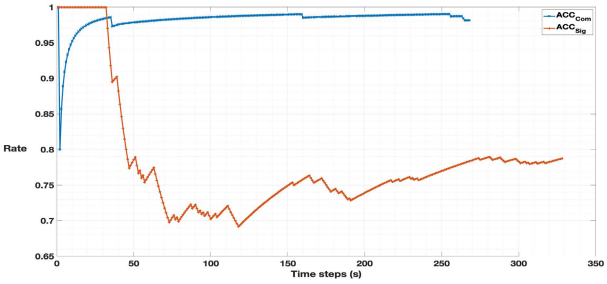


FIGURE 13. The comparison between the community's and the single's strategy detection in terms of accuracy rate.

Case 1: A receiver/transmitter (witness/Prover) with a long communication range (200 to 500 meters) static. According to the figures, these scenarios are often endowed with reasonable accuracy.

Case 2: A receiver/transmitter at a short communication range (0 to 100 meters) but a high relative velocity. According to the figure, these cases are often with poor precision.

Therefore, we distinguish from the two cases that False or True decisions depend considerably on the velocity since the communication range can be an additional indicator but does not significantly impact.

Whereas Fig.16 compares the average of all OBU accuracy rates (ACC_{Sig}) and the rate of community accuracy (ACC_{Com}).

Even with three vehicles in a single community, the accuracy rate in detecting position-faking attacks can be considerably enhanced. Furthermore, comparing individual decision making with the community decision in Fig.16 shows clearly that community decision is more efficient than individual ones.

4) SYBIL ATTACK

For the Sybil attack, only messages received simultaneously were considered in order to compare messages received in the same conditions. This resulted in a reduced number of messages considered.

Fig.14 shows the accuracy rate of each evaluated ID in all faked messages received. We plotted the number of messages received by each OBU from faked ID to establish the relationship between messages treated and accuracy. Using our algorithm, we observed that OBUs could individually detect Sybil attacks.

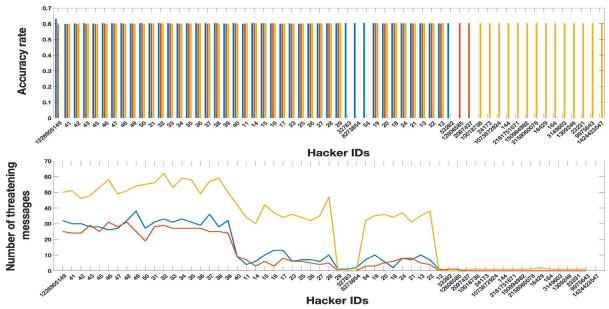


FIGURE 14. Accuracy rate on Sybil attack.

TABLE 6. Simulation parameters.

Communication simulator	OMNET ++
Number of node	***1683***
Application	Veins- VANET [42]
	Aretry Framework [35]
	Broadcast-message based
	100ms update time - CAM
	Communication range - Omnidirectional 500m
	Sensing range 800m
Number of broadcasted CAM	***22301***
Mobility simulator	SUMO
Lanes numbers	4 lanes - bi-directional
Topology	Highway only
Maximum lane speed	130 Km/h
Speed velocities	130km/h; 110 km/h; 90km/h

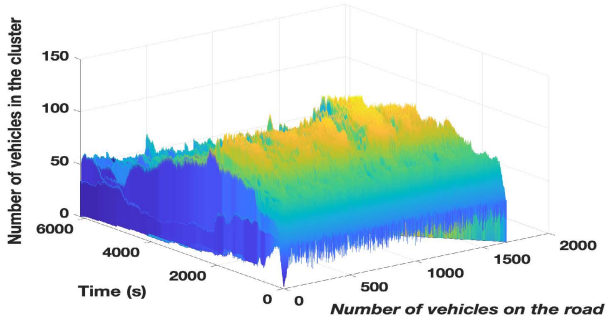


FIGURE 15. Number of vehicles in each cluster vs time and traffic.

B. SIMULATIONS

1) SIMULATION SETUP

For our simulations, we used SUMO for vehicular traffic and OMNE++ for vehicular communications. Using real CAM messages with the Artery with the parameters in Table.6 Framework, we used our revocation framework to evaluate its performances.

2) SIMULATION RESULTS

The purpose of these simulations was to evaluate the applicability of our solution to large-scale networks. In addition, we analyze the solution's performance in terms of cybersecurity using many communication vehicles.

Fig.15 shows the route reliability of our simulation configuration, reporting the number of vehicles in each stable, reliable community in our simulations.

In order to better illustrate the accuracy rate of all vehicles used in our simulation, we have plotted all their accuracy

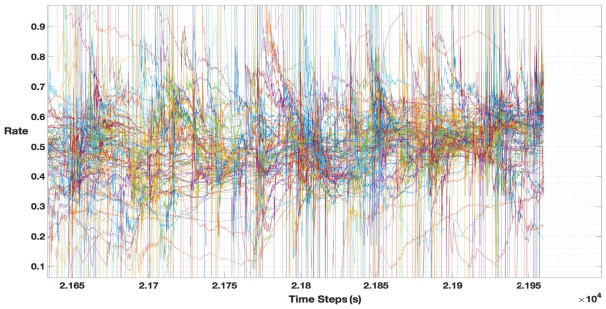


FIGURE 16. All vehicles accuracy rates evolution.

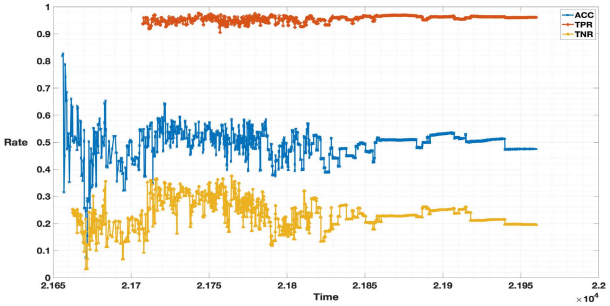


FIGURE 17. The mean of single accuracy rate with true positives and negatives rates.

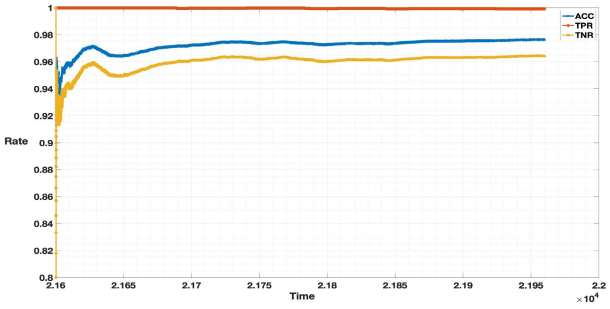


FIGURE 18. The community accuracy with the true positives and negatives rates.

rates. The Fig.16 shows all vehicles' report rates. The accuracy rate of each vehicle varies so much that it is difficult to assess the accuracy of a node.

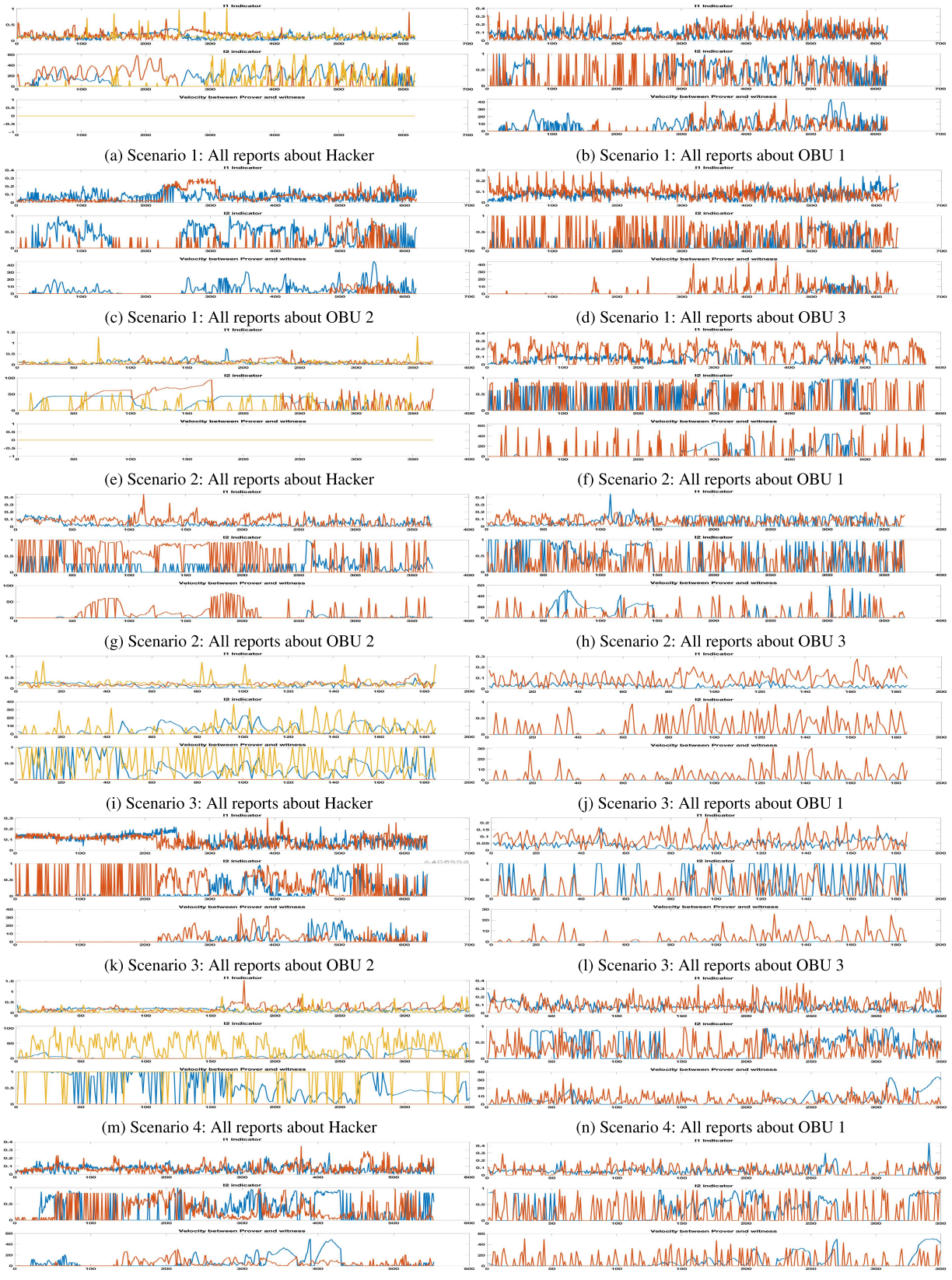
Fig.17, in presenting the average of all accuracy reports of individual vehicles, shows that accuracy is neither constant nor stable.

The Fig.18 shows the accuracy of our algorithm.

V. DISCUSSION

The range of communication is linked to detection accuracy. The Indicator 3 -I3- of our algorithm in section III-C could be based on several parameters: Velocity, distance, direction, yaw-rate, and weather conditions. It turned out from our previous work [9] that the most impacting parameter is velocity. Indeed, this parameter impacts the other parameters in a big way.

We have evaluated one of the most widely used datasets in V2X communication simulations, VeRiMi [1]. Although the date set shows slight variation, all the fake messages are



(a) Scenario 1: All reports about Hacker
(b) Scenario 1: All reports about OBU 1
(c) Scenario 1: All reports about OBU 2
(d) Scenario 1: All reports about OBU 3
(e) Scenario 2: All reports about Hacker
(f) Scenario 2: All reports about OBU 1
(g) Scenario 2: All reports about OBU 2
(h) Scenario 2: All reports about OBU 3
(i) Scenario 3: All reports about Hacker
(j) Scenario 3: All reports about OBU 1
(k) Scenario 3: All reports about OBU 2
(l) Scenario 3: All reports about OBU 3
(m) Scenario 4: All reports about Hacker
(n) Scenario 4: All reports about OBU 1
(o) Scenario 4: All reports about OBU 2
(p) Scenario 4: All reports about OBU 3

FIGURE 19. Appendices: Each vehicle data from each scenario.

far away from their real position. Therefore, it is far from the real-world conditions where a Sybil node could have stated a nearby antennas source.

Consequently, because hackers are always at a distance from receivers, a machine-learning model could easily make the right decision. Our dataset is more realistic and closer to reality as distance varies and RSSI levels fluctuate.

Whereas reports from individual vehicles may be unstable and vary considerably, reports using the community algorithm improve the accuracy rate.

VI. CONCLUSION AND PERSPECTIVES

This contribution corresponds to the definition of an algorithm capable of building autonomous blockchain communities to evaluate their "goodness" and thus revoking malicious vehicles in real-time. The proposed solution allows a collaborative system between individual vehicles and the structure since we cannot rely on only one in the revocation process. Although evaluated in real experimentation, the defined approach could meet the real-time requirements. We can conclude that our algorithm is more accurate than other frameworks simulated through VeriMi dataset as we have used V2X equipment in real-world conditions. Thus, our community algorithm permits using blockchain technology in vehicular communication and adds value to cyber-physical security.

Our perspective is to make a proof-of-concept by turning our algorithm into a real traffic management server and hosting a real-time blockchain to use it in our circuit. Moreover, to enhance the VeRiMi data set with more realistic data.

ACKNOWLEDGMENT

The authors gratefully acknowledge the support of la région Hauts de France and Valenciennes Métropole for la Chaire d'Excellence RIVA.

REFERENCES

[1] *VeReMi Dataset*. [Online]. Available: https://veremi-dataset.github.io/

[2] Z. A. El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An intra- and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7, pp. 98893–98907, 2019.

[3] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692.

[4] M. Almulla, Q. Zhang, A. Boukerche, and Y. Ren, "An efficientk-means authentication scheme for digital certificates revocation validation in vehicular ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 14, no. 16, pp. 1546–1563, Nov. 2014.

[5] M. A. Alsheikh, S. Lin, D. Niyato, and H. P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.

[6] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, "A generic public key infrastructure for securing car-to-X communication," in *Proc. 18th ITS World Congr.*, Orlando, FL, USA, vol. 14, 2011, pp. 1–12.

[7] M. Charitos and G. Kalivas, "MIMO HetNet IEEE 802.11p–LTE deployment in a vehicular urban environment," *Veh. Commun.*, vol. 9, pp. 222–232, Jul. 2017.

[8] A. Didouh, Y. El Hillali, A. Rivenq, and H. Labiod, "Novel centralized pseudonym changing scheme for location privacy in V2X communication," *Energies*, vol. 15, no. 3, p. 692, Jan. 2022.

[9] A. Didouh, A. B. Lopez, Y. E. Hillali, A. Rivenq, and M. A. A. Faruque, "Eve, you shall not get access! A cyber-physical blockchain architecture for electronic toll collection security," in *Proc. IEEE 23rd Int. Conf. Intell. Transp. Syst. (ITSC)*, Sep. 2020, pp. 1–7.

[10] *Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, document 302 637-2 V1.3.2, EN ETSI, Intelligent Transport Systems (ITS), 2014.

[11] T. ETSI, "*Mitigation Techniques to Avoid Interference Between European CEN Dedicated Short Range Communication (CEN DSRC)*, document 102 792 V1.2.1, TS ETSI, Intelligent Transport Systems (ITS).

[12] *V2X Applications; Part 1: Road Hazard Signalling (RHS) Application Requirements Specification*, document 101 539-1 V1.1.1, TS ETSI, Intelligent Transport Systems (ITS).

[13] *Security; Security Services and Architecture*, document 102 731 V1.1.1, TS ETSI, Intelligent Transport Systems (ITS), 2010.

[14] *Security; Trust and Privacy Management*, document 102 941 V1.1.1, TS ETSI, Intelligent Transport Systems (ITS), 2012.

[15] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *Proc. 13th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2016, pp. 45–59.

[16] T. Giannetsos and I. Krontiris, "Securing V2X communications for the future: Can PKI systems offer the answer?" in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, 2019, pp. 1–8.

[17] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Design and analysis of a lightweight certificate revocation mechanism for VANET," in *Proc. 6th ACM Int. workshop Veh. InterNETworking (VANET)*, 2009, pp. 89–98.

[18] S. Khakpour, R. W. Pazzi, and K. El-Khatib, "Using clustering for target tracking in vehicular ad hoc networks," *Veh. Commun.*, vol. 9, pp. 83–96, Jul. 2017.

[19] S. Khan, L. Zhu, X. Yu, Z. Zhang, M. A. Rahim, M. Khan, X. Du, and M. Guizani, "Accountable credential management system for vehicular communication," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100279.

[20] Z. Khan, P. Fan, S. Fang, and F. Abbas, "An unsupervised cluster-based VANET-oriented evolving graph (CVoEG) model and associated reliable routing scheme," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 10, pp. 3844–3859, Oct. 2019.

[21] M. Khodaei and P. Papadimitratos, "Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in VANETs," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2018, pp. 172–183.

[22] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal, "Analysis of certificate revocation list distribution protocols for vehicular networks," in *Proc. IEEE Global Telecommun. Conf. GLOBECOM*, Dec. 2010, pp. 1–5.

[23] S. Kushch and F. Prieto-Castrillo, "Blockchain for dynamic nodes in a smart city," in *Proc. IEEE 5th World Forum on Internet of Things (WF-IoT)*, Apr. 2019, pp. 29–34.

[24] L. Lamport, "Fast Paxos," *Distrib. Comput.*, vol. 19, no. 2, pp. 79–103, 2006.

[25] L. Liu, C. Chen, T. Qiu, M. Zhang, S. Li, and B. Zhou, "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs," *Veh. Commun.*, vol. 13, pp. 78–88, Jul. 2018.

[26] C. Lochert, M. Mauve, H. Füßler, and H. Hartenstein, "Geographic routing in city scenarios," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 9, no. 1, pp. 69–72, Jan. 2005.

[27] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 674–679.

[28] V. Naumov and T. R. Gross, "Connectivity-aware routing (CAR) in vehicular ad-hoc networks," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 1919–1927.

[29] Y. Peng, Z. Abichar, and J. Chang, "Roadside-aided routing (RAR) in vehicular networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2006, pp. 3602–3607.

[30] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, Mar. 2015.

[31] H. Qiu, M. Qiu, and R. Lu, "Secure V2X communication network based on intelligent PKI and edge computing," *IEEE Netw.*, vol. 34, no. 2, pp. 172–178, Mar. 2020.

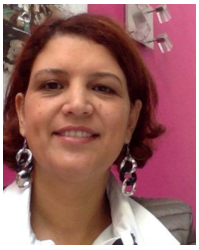
[32] W. Quan, Y. Liu, H. Zhang, and S. Yu, "Enhancing crowd collaborations for software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 80–86, Aug. 2017.

[33] M. Ren, J. Zhang, L. Khoukhi, H. Labiod, and V. Vèque, "A unified framework of clustering approach in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 5, pp. 1401–1414, May 2018.
[34] L. Reyzin and S. Yakoubov, "Efficient asynchronous accumulators for distributed PKI," in *Security and Cryptography for Networks*, V. Zikas and R. De Prisco, vol. 9841. Springer, pp. 292–309.
[35] R. Riebl, H.-J. Gunther, C. Facchi, and L. Wolf, "Artery: Extending veins for VANET applications," in *Proc. Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*, Jun. 2015, pp. 450–456.
[36] L. Rivoirard, M. Wahl, P. Sondi, M. Berbineau, and D. Gruyer, "Chain-branch-leaf: A clustering scheme for vehicular networks using only V2V communications," *Ad Hoc Netw.*, vol. 68, pp. 70–84, Jan. 2018.
[37] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in *Proc. IEEE Veh. Technol. Conf. (VTC Fall)*, Sep. 2011, pp. 1–5.
[38] P. Samar, M. R. Pearlman, and Z. J. Haas, "Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 4, pp. 595–608, Aug. 2004.
[39] A. Sarker, S. Byun, W. Fan, and S.-Y. Chang, "Blockchain-based root of trust management in security credential management system for vehicular communications," in *Proc. 36th Annu. ACM Symp. Appl. Comput.*, Mar. 2021, pp. 223–231.
[40] O. Schmidt, "An ETSI look at the state of the art of pseudonym schemes in vehicle-to-everything (V2X) communication," Tech. Rep.
[41] C. Shea, B. Hassanabadi, and S. Valaee, "Mobility-based clustering in VANETs using affinity propagation," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 2009, pp. 1–6.
[42] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," in *Recent Advances in Network Simulation*. Springer, 2019, pp. 215–252.
[43] C. Sowattana, W. Viriyasitavat, and A. Khurat, "Distributed consensus-based sybil nodes detection in VANETs," in *Proc. 14th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, Jul. 2017, pp. 1–6.
[44] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar, "Broadcasting in VANET," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 7–12.
[45] O. K. Tonguz, N. Wisitpongphan, and F. Bai, "DV-CAST: A distributed vehicular broadcast protocol for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 17, no. 2, pp. 47–57, Apr. 2010.
[46] E. TR, "Security;pre-standardization study on pseudonym change management," *103 415 V1.1.1: Intelligent Transport Systems (ITS)*.
[47] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proc. workshop Dependability issues wireless ad hoc Netw. sensor Netw. - DIWANS*, 2006, pp. 1–8.
[48] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K.-K. R. Choo, and H. Cai, "V2X security: A case study of anonymous authentication," *Pervas. Mobile Comput.*, vol. 41, pp. 259–269, Oct. 2017.
[49] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.
[50] Z. Yang, K. Zhang, L. Lei, and K. Zheng, "A novel classifier exploiting mobility behaviors for sybil detection in connected vehicle systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2626–2636, Apr. 2019.
[51] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou, "Multi-channel based sybil attack detection in vehicular ad hoc networks using rssi," *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 362–375, Feb. 2018.

AHMED DIDOUH received the bachelor's degree equivalent in electrical engineering and industrial computing and the master's degree in embedded systems and telecommunication engineering from the Polytechnic University of Haut de France (UPHF), Valenciennes, where he is currently pursuing the Ph.D. degree with the Institute of Electronics, Microelectronics and Nanotechnology (IEMN) Laboratory. He worked one year as an Embedded Systems Engineer with the European Project InterCor about deploying a smart infrastructure in collaboration with RO DIR Nord in North of France. His research interest includes the use of BC methods in cyber-physical transportation systems.

HOUDA LABIOD (Senior Member, IEEE) received the Habilitation a Diriger les Recherches (HDR), in 2005. She was the Head of the Research Group CCN "Cybersecurity for Communication and Networking," from 2015 to 2018. Prior to this, she held a research position at Eurecom Institute, Sophia-Antipolis, France. She is currently a Full Professor at the Department INFRES (Computer Science and Network Department), Instiute Polytechnique of Paris (IP Paris), Telecom Paris (previously named ENST), Paris, France. She is a Founder of the IFIP NTMS Conference, on New Technologies, Mobility and Security (NTMS 2007). She is a Co-Leader of the Chaire C3S on Cybersecurity for connected and autonomous vehicles with French partners Renault, Valeo, Thales, Nokia, and Wavestone. She is currently involved in major national and European projects focusing on security for connected and autonomous vehicles (SCOOP@F, InterCor, and C-roads). She published six books, ten patents, one IETF RFC, four IETF drafts, and more than 250 research articles in these areas. Her current research interests include security in cooperative ITS, cooperation in wireless and autonomous networks (WLANs/MANETs/WSN/Mesh/vehicular/cellular), QoS, performance evaluation, and link adaptation mechanisms. She served as an associate editor and a member on the editorial board for several journals.

YASSIN EL HILLALI was born in Chemaia, Morocco, in 1979. He received the M.S. and Ph.D. degrees from the University of Valenciennes, France, in 2002 and 2005, respectively. He is currently an Assistant Professor at the Electronics Department, Polytechnic University of the Hauts-de-France (UPHF). He is responsible for ITSCOM platforms (ITS Communications) in the IEMN-DOAE Laboratory. His research interest includes signal processing and wireless communication systems (WAVE, ITSG5 5G) applied to intelligent transportation, and machine learning dedicated to target detection and recognition using heterogeneous sensors (UWB RADAR, cameras, and Lidar). He is also working on cyber-security for ITS and industrial systems.



ATIKA RIVENQ (Member, IEEE) was born in Marrakech, Morroco, in 1970. She graduated in engineering from the ENSIMEV Engineering School, in 1993. She received the M.S. and Ph.D. degrees in electronic engineering from the University of Valenciennes, France, in 1993 and 1996, respectively. She is currently a Full Professor at the IEMN Laboratory, Department of Electronic Engineering, Polytechnic University of the Hauts-de-France (UPHF), France. She is also the Head of the ComNum Group and she is responsible for the SYFRA platform (Systems for smart road applications) with the IEMN-DOAE Laboratory. She participates in many national and European projects dedicated to C-ITS and inter-vehicle communications especially using ITS-G5 and cellular systems. She has more than 100 publications in international journals, conferences, and workshops in the area of digital communications. Her main activities are in digital communications applied to intelligent transports systems: V2X communications (4G/5G, UWB, ITS-G5, and full duplex), cybersecurity and advanced perception (radar, UWB, detection of vulnerable persons, and deep learning). She has participated as a general chair, a member of the technical committee, a session chair, or a program committee member of numerous conferences.