Blockchain-Based Collaborative Certificate Revocation Systems Using Clustering

AHMED DIDOUH1, HOUDA LABIOD 2(SENIOR MEMBER, IEEE), YASSIN EL HILLALI1, ATIKA RIVENQ1.
1IEMN-DOAE, Université Polytechnique Hauts-de-France, 59300 Valenciennes, France(e-mail: Ahmed.Didouh,Yassin.EHillali,Atika.Menhaj@uphf.fr)
2Dept. of Computing and Networks ENST-Telecom Paris 91120 Palaiseau- France(e-mail: houda.labiod@telecom-paris.fr)
Corresponding author: Ahmed Didouh (e-mail: Ahmed.Didouh@uphf.fr).

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 [14]: 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 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 [39], [27], route discovery protocols [29], [46], broadcast protocols [45], infrastructure-based protocols [30], and cluster-based protocols [19], [24], [33], [42]. 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 [21] 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. [26] 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 [31]. 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 (LTC) 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 [32]. 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 [17]. 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 change strategies remain a challenge for the cybersecurity of V2X communications.

1) Pseudonyms Management
To ensure vehicles’ confidentiality, the standard [10] 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 [11], a random string encrypted with the receiver’s public key. Both of these measures prevent replay attacks. Credentials and ATs can also be updated as needed through similar mechanisms. The ETSI survey [9] also gives an overview of strategies used in existing projects standards.
TABLE I. Table of contributions in the various fields related to our work

| Clustering | Centralized architecture | Decentralized architecture | V2X Communications | Blockchain |
|------------|--------------------------|---------------------------|-------------------|------------|
|            |                          | X                         |                   | All-nodes-centric | OBU-centric | RSU-centric | RCA-centric |
|            | [2] [24]                 | X                         |                   |              |            |            |            |
|            | [21]                     | X                         |                   |              |            |            |            |
|            | [19]                     | X                         |                   |              |            |            |            |
|            | [7]                      | X                         |                   |              |            |            |            |
|            | [17] [26] [34]           | X                         |                   |              |            |            |            |
| Pseudonym changing and Credential Management | [20] [32] [3]           | X                         |                   |              |            |            |            |
|            |                          |                           |                   |              |            |            |            |
|            | [40]                     | X                         |                   |              |            |            |            |
| Certificate revocation | [23] [22]          | X                         |                   |              |            |            |            |
|            | [18] [13]                | X                         |                   |              |            |            |            |
|            | [28]                     | X                         |                   |              |            |            |            |
| Sybil attack detection | [51] [17] [38] [44]   | X                         |                   |              |            |            |            |
|            | [50]                     | X                         |                   |              |            |            |            |

C. CERTIFICATE REVOCATION

In recent years, few studies have been proposed on certificate revocation list (CRL) distribution methods [23]. 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 [22], 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. [28] 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. [38] 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 I 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 IEEE802.11p 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 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3160171, IEEE Access

Ahmed Didouh et al.: Blockchain-Based Collaborative Certificate Revocation System Using Clustering
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 \( i - \text{th} \) node, \( N_i \), is associated with a position, represented, as \( P_i(t) = (x_i(t), y_i(t)) \) at time \( t \). The nodes are users of a PKI. We define a communication area, 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 \( N_S_i(t) = \{ j \in V : \| (P_i(t), P_j(t)) \| \leq R \} \).

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 [16]. 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.

### TABLE II. Abbreviations and symbols

| Abbreviation | Description |
|--------------|-------------|
| TMC          | Traffic management center |
| CA           | Certificate authority |
| RBU          | Remote board unit |
| CAM          | Certificate issuance authority |

Symbols:

- \( N \): List of community members
- \( DT_{n-1} \): The cluster formation message
- \( D_i \): Relative distance between vehicles
- \( CL_i \): Cluster identification
- \( N_S_i \): List of vehicles likely to contribute to the community
- \( N \text{V} \): One-hop neighbor table
- \( v \): Vehicle's speed
- \( H_d \): Vehicle's driving heading
- \(\text{QT}_{\text{max}}\): Estimated time of communication link between vehicles
- \(\text{DT}_{\text{har}}\): Estimated lifetime for communication link between vehicles

#### 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 \( T_{\text{har}} \), and sends the list to the TMC. Thus, the TMC, therefore, receives several lists after the time \( T_{\text{har}} \). After concatenating the lists, the TMC obtains a graph. Then, based on the graph rules specified in subsections below, the TMC issues the community’s start list with a cluster ID (\( ID_{\text{clus}} \)). 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 \( T_{\text{har}} \), 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 \( G \in N_S \).

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 \( N \text{S} \) represents a neighboring vehicle list that presents a similar mobility pattern, moving in the same direction. \( H_d V_i = H_d V_j \) 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 \( (T_{\text{link}}) \) must be smaller than the predetermined threshold \( T_{\text{th}} \):

\[
T_{\text{th}} = \frac{R - \left(\frac{1}{\text{QT}_{\text{max}}}\right)}{VT}
\]  

Where \( \text{QT}_{\text{max}} \) 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, \( T_{\text{life}} \), to avoid a hacker having a monopoly on it. This is calculated based on the average life of the link, \( T_{\text{link}} \), between vehicles.

\[
T_{\text{life}} = T_{\text{link}} = \sum_{j=0}^{N_i} \left( \frac{R - \Delta D_{ij}}{\Delta v_{ij} \times N_i} \right) \leq T_{\text{th}}
\]  

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

The selection of the cluster head will be based on the metric \( T_{\text{life}} \) 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 \( \text{List}_\text{com} \) of vehicles that may likely contribute to the community.

3) Cluster formation
When a vehicle \( V_j \) receives a cluster formation message from \( TMC \), it immediately sends a \( \text{ReqJoin} = \text{Sig}_{V_j}\left(\text{Clus}_{for}\right) \) message to \( \text{CH}_i \). After \( \text{CH}_i \) receives the \( \text{ReqJoin} \) message, it first checks whether this ID is available in \( \text{List}_\text{com} \). If so, \( \text{CH} \) adds \( V_j \) to its cluster member list \( G_{\text{com}} \) and sends back a \( \text{ACKJoin} \) message; otherwise, it ignores the request to join.

\[
\text{Clus}_{for} = \{ \text{Sig}_{TMC}(\text{ID}_{\text{CH}}, \text{ID}_{\text{Clus}}) \}
\]

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 [10]. 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 \( G_{\text{com}} \). However, a long delay in the re-clustering process may lead to severe consequences, primarily when implemented delay-sensitive applications. 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 [34] 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 [41], 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 [15], 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) [13]. 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 [8], 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 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 [8].

The PoL algorithm has an output of three major indicators that permit to identify position-faking attacks, \( I_1, I_2, I_3 \)
Algorithm 1: Algorithm of Community construction

**Input:** Pos<sub>p</sub>; P<sub>r</sub>; Hd<sub>w</sub>; Sp<sub>w</sub>; N

**Output:** G<sub>com</sub>

**Function One-hop neighbor**

| Table (T<sub>har</sub>[i], Sp<sub>p</sub>[i], Pos<sub>p</sub>[i]) |
|---------------------------------------------------------------|
| while T<sub>har</sub> > 0 do                                     |
|     if V<sub>i</sub> receives Beacon from V<sub>j</sub> then   |
|         if H<sub>i</sub> == H<sub>j</sub> and v<sub>ij</sub> < v<sub>th</sub> then |
|             if V<sub>j</sub> ∈ NS<sub>i</sub> then             |
|                 V<sub>i</sub> Update NS<sub>i</sub>(j)         |
|         end if                                               |
|     end if                                                  |
|     end if                                                  |
|     V<sub>i</sub> adds the entry NS<sub>i</sub>(j) to NS<sub>i</sub> |
|     n<sub>i</sub> = n<sub>i</sub> + 1                       |
| else                                                       |
|     V<sub>i</sub> receives ACKJoin<sub>i</sub> from V<sub>i</sub> |
| end if                                                     |

**Function Cluster Processing** (NS<sub>i</sub>[i], V<sub>i</sub>, n<sub>i</sub>, Sp<sub>i</sub>, Pos<sub>i</sub>, Hd<sub>i</sub>):

- CH ← V<sub>i</sub>
- T<sub>link</sub>CH ← T<sub>link1</sub>
- if TMC receives NS<sub>i</sub>[j] then
  - while T<sub>har</sub> > 0 do
  - TMC calculates T<sub>linki</sub>
  - if T<sub>linki</sub> < T<sub>th</sub> then
    - T<sub>linki</sub> add T<sub>linki</sub>
    - List<sub>com</sub> add V<sub>i</sub>
    - if T<sub>linki</sub> > T<sub>link</sub>CH then
      - T<sub>link</sub>CH ← T<sub>linki</sub>
      - CH ← V<sub>i</sub>
    end if
  end if
- TMC calculates T<sub>life</sub> from T<sub>linki</sub>
- return CH, T<sub>life</sub>, List<sub>com</sub>[i]

**Function Cluster formation** (CH, List<sub>com</sub>[]):

- if T<sub>har</sub> = 0 then
  - CH receives ReqJoin<sub>i</sub> from V<sub>i</sub>
  - if V<sub>i</sub> ⊂ List<sub>com</sub> then
    - G<sub>com</sub> add V<sub>i</sub> CH sends ACKJoin<sub>i</sub> to V<sub>i</sub>
  end if
- end if
- return G<sub>com</sub>

**End Function**

**Indicator 1 (I<sub>1</sub>):** Indicates average speed and calculates distance traveled by using the prover’s traces.

**Indicator 2 (I<sub>2</sub>):** 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<sub>3</sub>):** 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.

\[
PoL = (PoL_{Acc}, PoL_{Rate}, Pos_p, t_w, Cer_w, S_w[PoL_{req}, t_w, K_p])
\]

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

**FIGURE 3.** The Proof-of-Location process between the prover and its witness

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 [8]. The PoL accuracy is inversely related to...
TABLE III

| Mode      | Velocity (km/h) | ACC  |
|-----------|----------------|------|
| I2V mode  | 31.60          | 41.10% |
| ACC       | 41.10%         | 56.75% |
| V2V mode  | 12.27          | 72.47% |
| ACC       | 72.47%         | 67.12% |

TABLE III

the velocity, as shown in Fig. 3 and Fig. 4, the high velocity significantly impacts the distance estimation based on the 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 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 $A$:

$$ A = \begin{bmatrix} r_{ID_1} \\ r_{ID_2} \\ \cdots \\ r_{ID_n} \end{bmatrix} $$

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 matrix $L$ 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 [21]. 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:

$$ Z = [X_1, X_2, X_3 \ldots X_n] $$

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 [35]), 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.

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.

![FIGURE 5. Blockchain’s global parts](image)

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.IV shows the composition of transactions.

| Transaction Header | Value |
|---------------------|-------|
| Blockchain part     | Indicates the smart contract |
| Merkle 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](image)

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 [25]

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 equipments: 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.

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 \(\sigma\), 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.

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 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:

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 ($\textit{ACC}_{\text{Sig}}$) and the rate of community accuracy ($\textit{ACC}_{\text{Comm}}$).

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.

Based on the mean and the variance of $\textit{PoL}$ indicators, each vehicle decides whether or not to trust another vehicle. Table V shows the results obtained from the peer-to-peer $\textit{PoL}$ 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.

**TABLE V.** Indicators results for peer-to-peer communication for each scenario, $\delta_{rel}$ is the relative velocity between both nodes, $\sigma$ and ACC

| Scenario | $\delta_{rel}$ (Kmh) | $\sigma$ | $\text{ACC}_{\text{Sig}}$ | $\text{ACC}_{\text{Comm}}$ |
|----------|----------------------|----------|--------------------------|--------------------------|
| Scenario 1 | 6.52 | 0.0896 | 60.5% | 89.1% |
| Scenario 2 | 24.90 | 0.353 | 68,88 | 6.432 |
| Scenario 3 | 0 | 0.0156 | 0.0093 | 0.0003 |
| Scenario 4 | 3.44 | 0.0393 | 0.0984 | 0.0004 |

**FIGURE 12.** All trusted vehicles reports
Ahmed Didouh et al.: Blockchain-Based Collaborative Certificate Revocation System Using Clustering

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

FIGURE 14. Accuracy rate on Sybil attack

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.

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 VI Framework, we used our revocation framework to evaluate its performances.

| Communication simulator | OMNET++ |
|-------------------------|---------|
| Number of node          | 1683    |
| Application             | Veins- VANET [43]| Artery Framework [36]|
|                         | Broadcast-message based |
|                         | 100ms update time - CAM |
|                         | Communication range - Omnidirectional 500m |
|                         | Sensing range 800m |

| 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 |

TABLE VI. Simulation Parameters

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.

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

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

FIGURE 16. All vehicles accuracy rates evolution

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 [8] 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
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.

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

REFERENCES

[1] VeReMi dataset https://veremi-dataset.github.io/.
[2] Zakaria Abou El Houda, Abdellahim Senhaji Hafid, and Lyes Khoukhi. Cochain-sc: An intra-and inter-domain ddos mitigation scheme based on blockchain using snsd and smart contract. IEEE Access, 7:98893–98907, 2019.
[3] Ikram Ali, Tandoh Lawrence, and Fagen Li. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in vansets. Journal of Systems Architecture, 103:101692, 2020.
[4] Mohammed Almulla, Qingwei Zhang, Azzedine Boukerche, and Yonglin Ren. An efficient k-means authentication scheme without bilinear pairing for vehicle-to-vehicle communication in vehicular ad hoc networks. Wireless Communications and Mobile Computing, 14(16):1546–1563, 2014.
[5] Mohammad Abu Alsheikh, Shaowei Lin, Dusit Niyato, and Hwee-Pink Tan. Machine learning in wireless sensor networks: Algorithms, strategies, and applications. IEEE Communications Surveys & Tutorials, 16(4):1996–2018, 2014.
[6] Norbert Bimbeyer, Hagen Stübing, Elnar Schoch, Stefan Götz, Jan Peter Stotz, and Brigitte Lonc. A generic public key infrastructure for securing car-to-x communication. In 18th ITS World Congress, Orlando, USA, volume 14, 2011.
[7] Michael Charitos and Grigorios Kalivas. Mimo hetnet icc 802.11 p–lte deployment in a vehicular urban environment. Vehicular Communications, 9:222–232, 2017.
[8] Ahmed Didouh, Anthony Bahadir Lopez, Yassin El Hillali, Atika Rivenq, and Mohammad Abdullah Al Faruque. Eve, you shall not get access! a cyber-physical blockchain architecture for electronic toll collection security. In 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), pages 1–7, IEEE, 2020.
[9] ETSI TR ETSI. 103 415 v1.1.1: Intelligent transport systems (its). Security; Prestandardization study on pseudonym change management.
[10] I ETSI. Intelligent transport systems (its); security; pre-standardization study on pseudonym change management. Technical report, Technical report, ETSI TR 103 415, European Telecommunications Standards . . ., 2018.
[11] TCITS ETSI. Etsi ts 102 731 v1.1.1-intelligent transport systems (its); security; security services and architecture. Standard, TC ITS, 2010.
[12] TCITS ETSI. Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. Draft ETSI TS, 08(2011):448–51, 2011.
[13] TS ETSI. 101 539 (v1.1.1). Intelligent Transport Systems (ITS).
[14] TS ETSI. 102 792 (v1.2.1). Intelligent Transport Systems (ITS).
[15] TS ETSI. 102 941 v1.1.1—intelligent transport systems (its); security; trust and privacy management. Standard, TC C-ITS, 2012.
[16] Ittay Eyal, Adem Efe Gencer, Emin Gün Sızer, and Robbert Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), pages 45–59, 2016.
[17] Thanassios Giannetsos and Ioannis Krontiris. Securing v2x communications for the future: Can pki systems offer the answer? In Proceedings of the 14th International Conference on Availability, Reliability and Security, pages 1–8, 2019.
[18] Jason J Haas, Yih-Chun Hu, and Kenneth P Laberteaux. Design and analysis of a lightweight certificate revocation mechanism for vanet. In Proceedings of the sixth ACM international workshop on VehicularAr InterNEtWorking, pages 89–98, 2009.
[19] Sanaz Khakpour, Richard W Pazzi, and Khalil El-Khatib. Using clustering for target tracking in vehicular ad hoc networks. Vehicular communications, 9:83–96, 2017.
[20] Salabat Khan, Liehuang Zhu, Xiaoyan Yu, Ziqian Zhang, Musaabdul Rahim, Maqbool Khan, Xiaojiaing Du, and Molens Guizani. Accountable credential management system for vehicular communication. Vehicular Communications, 25:100279, 2020.

[21] Zahid Khan, Pingzhi Fan, Sangsha Fang, and Fahkar Abbas. An unsupervised cluster-based vanet-oriented evolving graph (coveg) model and associated reliable routing scheme. IEEE Transactions on Intelligent Transportation Systems, 20(10):3844–3859, 2019.

[22] Mohammad Khodaei and Panos Papadimitratos. Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in vanets. In Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks, pages 172–183, 2018.

[23] Yogesh Kondareddy, Giovanni Di Crescenzo, and Prathima Agrawal. Analysis of certificate revocation list distribution protocols for vehicular networks. In 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pages 1–5, IEEE, 2010.

[24] Sergio Kuschel and Francisco Prieto-Castrillo. Blockchain for dynamic nodes in a smart city. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pages 29–34, IEEE, 2019.

[25] Leslie Lamport. Fast paxos. Distributed Computing, 19(2):79–103, 2006.

[26] Mohammad Khodaei and Panos Papadimitratos. Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in vanets. In Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks, pages 172–183, 2018.

[27] A data dissemination scheme based on clustering and probabilistic broadcasting in vanets. Vehicular Communications, 13:78–88, 2018.

[28] Christian Lochert, Martin Mauve, Holger Füller, and Hannes Hartenstein. Geographic routing in city scenarios. ACM SIGMOBILE mobile computing and communications review, 9(1):69–72, 2005.

[29] Nisha Malik, Priyadarsi Nanda, Arushi Arora, Xiangjian He, and Deepak Puthal. Blockchain based secured identity authentication and expedited revocation framework for vehicular networks. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), pages 674–679, IEEE, 2018.

[30] Valery Naumov and Thomas R Gross. Connectivity-aware routing (car) in vehicular ad-hoc networks. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, pages 1919–1927. IEEE, 2007.

[31] Yanlin Peng, Zakha Abichar, and J Morris Chang. Roadside-aided routing (rar) in vehicular networks. In 2006 IEEE international conference on communications, volume 8, pages 3602–3607. IEEE, 2006.

[32] Jonathan Petri, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. IEEE communications surveys & tutorials, 17(1):228–255, 2014.

[33] Han Qiu, Meikang Qiu, and Ruqian Lu. Secure v2x communication network based on intelligent pki and edge computing. IEEE Network, 34(2):172–178, 2019.

[34] Wei Quan, Yana Liu, Hongke Zhang, and Shui Yu. Enhancing crowd collaborations for software defined vehicular networks. IEEE Communications Magazine, 55(8):80–86, 2017.

[35] Mengying Ren, Jun Zhang, Siyu Li, and Bin Zhou. A data dissemination scheme based on clustering and probabilistic broadcasting in vanets. In IEEE Global Telecommunications Conference GLOBECOM 2010, pages 1–5, IEEE, 2010.

[36] Zhe Yang, Kuan Zhang, Lei Lei, and Kan Zheng. A novel classifier for distributed vehicular networks using only v2x communication. IEEE Transactions On Intelligent Transportation Systems (MT-ITS), pages 450–456. IEEE, 2015.

[37] Lucas Rivoriard, Martine Wald, Patrick Sondi, Marion Berbineau, and Dominique Gruyer. Chain-branch-leaf: A clustering scheme for vehicular networks using only v2x communications. Ad Hoc Networks, 68:70–84, 2018.

[38] Sushmita Rui, Marcos A Cavenagh, Zhen Huang, Amitya Nayak, and Ivan Stoimenovic. On data-centric misbehavior detection in vanets. In 2011 IEEE Vehicular Technology Conference (VTC Fall), pages 1–5, IEEE, 2011.

[39] Levente Samar, Marc R Pearlman, and Zigmunt J Haas. Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks. IEEE/ACM Transactions On Networking, 12(4):595–608, 2004.

[40] Arijit Sarker, SangHyun Byun, Wenjun Fan, and Sang-Yoon Chang. Blockchain-based trust management in security credential management system for vehicular communications. In Proceedings of the 36th Annual ACM Symposium on Applied Computing, pages 223–231, 2021.

[41] Oliver Schmidt. An etsi look at the state of the art of pseudonym schemes in vehicle-to-everything (v2x) communication.

[42] Christine Shea, Behnam Hassanabadi, and Shahrokh Valaee. Mobility-based clustering in vanets using affinity propagation. In GLOBECOM 2009-2009 IEEE Global Telecommunications Conference, pages 1–6. IEEE, 2009.

[43] Christoph Sommer, David Eckhoff, Alexander Brummer, Dominik S Buse, Florian Hagelauer, Stefan Joerger, and Michele Segata. V2x: The open source vehicle network simulation framework. In Recent Advances in Network Simulation, pages 215–252. Springer, 2019.

[44] Chea Sowattana, Wanatee Viriyasavat, and Assadarat Khurat. Distributed consensus-based sybil node detection in vanets. In 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSEE), pages 1–6. IEEE, 2017.

[45] Ozan Tonguz, Nwopom Wisiopongfang, Fan Bai, Priyamani Madugalike, and Varsha Sadekar. Broadcast in vanet. In 2007 mobile networking for vehicular environments, pages 7–12. IEEE, 2007.

[46] Ozan K Tonguz, Nwopom Wisiopongfang, and Fan Bai. Dv-cast: A distributed vehicular broadcast protocol for vehicular ad hoc networks. IEEE Wireless Communications, 17(2):47–57, 2010.

[47] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and localization of sybil nodes in vanets. In Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, pages 1–8, 2006.

[48] Yanjiang Yang, Zhuo Wei, Youcheng Zhang, Haibing Lu, Kim-Kwang Raymond Choo, and Haibin Cai. V2x security: A case study of anonymous authentication. Pervasive and Mobile Computing, 41:259–269, 2017.

[49] Yao-Tsong Yang, Li-Der Chou, Chia-Wei Tseng, Fan-Hsun Tseng, and Chien-Chang Liu. Blockchain-based traffic event validation and trust verification for vanets. IEEE Access, 7:30868–30877, 2019.

[50] Zhe Yang, Kuan Zhang, Lei Lei, and Kan Zheng. A novel classifier exploiting mobility behaviors for sybil detection in connected vehicle systems. IEEE Internet of Things Journal, 6(2):2626–2636, 2018.

[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 Transactions on Mobile Computing, 18(2):362–375, 2018.
HOUDA LABIOD is a full Professor at Department INFRES (Computer Science and Network department) at Telecom Paris (previously named ENST) in Paris (France) of Institute Polytechnique of Paris (IP Paris). She was the head of the research group CCN “Cybersecurity for Communication and Networking” from 2015 to 2018. In 2005, she obtained her HDR (Habilitation a diriger les recherches). Prior to this, she held a research position at Eurecom Institute, Sophia-antipolis, France. Her current research interests include security in cooperative ITS, cooperation in wireless and autonomous networks (WLANs/MANets/WSNs/Mesh/Vehicular/cellular), QoS, performance evaluation and link adaptation mechanisms. She published six books, 10 patents, 1 IETF RFC, 4 IETF drafts and more than 250 research papers in these areas. She is a Founder of IFIP NTMS Conference, on New Technologies, Mobility and Security (NTMS2007). She served as an Associate Editor and a member on the Editorial Board for several journals. She is currently involved in major national and European projects focusing on security for connected and autonomous vehicles (SCOCOP@F, InterCor and C-roads). 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.

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

ATIKA RIVENQ was born in Marrakech (Morocco) in 1970. She was graduated Engineer from the ENSIMEV engineering school in 1993, received an M.S. degree in electronic engineering in 1993, and then a Ph.D. degree in 1996 from the University of Valenciennes (France). She is a Full Professor at the Department of Electronic Engineering, IEMN Lab, Polytechnic University of the Hauts-de-France (UPHF), France. She is the head of ComNum Group and she is responsible for the SYFRA platform (Systems for smart road applications) with the IEMN-DOAE Lab. Her main activities are in digital communications applied to intelligent transports systems: V2X communications (4G/5G, UWB, ITS-G5, Full Duplex), Cybersecurity and Advanced Perception (Radar, UWB, Detection of vulnerable persons, Deep learning). She Participates in many national and European projects dedicated to C-ITS and inter-vehicle communications especially using ITS-G5 and Cellular systems. Pr. Rivenq has more than 100 publications in international journals, conferences, and workshops in the area of digital communications. She has participated as a General Chair, Member of the Technical Committee, Session Chair, or Program Committee Member of numerous conferences.

YASMIN EL HILLALI was born in Chemaia, Morocco, in 1979. He received an M.S degree in 2002, and then a Ph.D. degree in 2005, from the University of Valenciennes, France. Currently, he is an Assistant Professor at the electronics department of the Polytechnic University of the Hauts-de-France (UPHF). He is responsible for ITSCOM platforms (ITS Communications) in the IEMN-DOAE Lab. His research interest includes: signal processing and wireless communication systems (WAVE, ITSG5 5G) applied to intelligent transportation, machine learning dedicated to target detection and recognition using heterogeneous sensors (UWB RADAR, cameras and Lidar) and currently his working on cybersecurity for ITS and industrial systems.
Ahmed Didouh et al.: Blockchain-Based Collaborative Certificate Revocation System Using Clustering

FIGURE 19. Appendices: Each vehicle data from each scenario

(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