# Blockchain and revocation process : towards more secure vehicular communications

Ahmed Didouh

# PhD Thesis

Submitted for the degree of Doctor of **Telecommunication** from

UNIVERSITE POLYTECHNIQUE HAUTS-DE-FRANCE
and INSA HAUTS-DE-FRANCE

Presented and defended by AHMED DIDOUH
On 09/12/2021, Valenciennes

*Doctoral school* : *Hauts-de-France Polytechnic Doctoral School (ED PHF)*
*Laboratory* : *IEMN-DOAE UMR CNRS 8201.*

---

BLOCKCHAIN AND REVOCATION PROCESS : TOWARDS MORE SECURE VEHICULAR COMMUNICATIONS

---

## JURY

| | | | |
|---|---|---|---|
| **Chairman of the Jury** | : | MR. Pierre Boulet | Professor at University of Lille, Cristal Lab Lille. France |
| **Reviewers** | : | MR. Nael B. Abu-Ghazaleh | Professor at University of California Riverside, UCR. USA |
| | | MR. Hacène Fouchal | Professor at University of Reims Champagne-Ardenne, Reims. France |
| **Examiners** | : | MR. Mohammad Abdullah Al Faruque | Professor at University of California Irvine, UCI. USA . |
| | | MR. Jean-Marie Bonnin | Professor at IMT Atlantique, Rennes. France |
| **Thesis director** | : | MRS. Atika RIVENQ | Professor at INSA Hauts de France, UPHF. France |
| **Thesis co-director** | : | MRS. Houda Labiod | Professor at IMT, Télécom Paris, Palaiseau. France |
| **Co-supervisor** | : | MR.Yassin ELHILLALI | Professor at University of Polytechnique Hauts-de-France, UPHF. France. |

**Thèse de doctorat**

Pour obtenir le grade de Docteur de

l'UNIVERSITÉ POLYTECHNIQUE HAUTS-DE-FRANCE
et l'INSA HAUTS-DE-FRANCE

Discipline : **Télécommunication**

Présentée et soutenue par : AHMED DIDOUH.
Le 09/12/2021, à Valenciennes.

*École doctorale* : *École Doctorale Polytechnique Hauts-de-France (ED PHF)*
*Laboratoire* : *IEMN-DOAE UMR CNRS 8201.*

---

# BLOCKCHAIN ET PROCESSUS DE RÉVOCATION : VERS DES COMMUNICATIONS VÉHICULAIRES PLUS SÉCURISÉES

---

## JURY

| | | | |
|---|---|---|---|
| **Président du jury** | : | M. Pierre Boulet | Professeur à l'Université de Lille, Laboratoire Cristal Lille. France |
| **Rapporteurs** | : | M. Nael B. Abu-Ghazaleh | Professeur à l'Université de Californie Riverside, UCR. USA |
| | | M. Hacène Fouchal | Professeur à Université de Reims Champagne-Ardenne, Reims. France |
| **Examinateurs** | : | M. Mohammad Abdullah Al Faruque | Professeur à l'Université de Californie Irvine, UCI. USA . |
| | | M. Jean-Marie Bonnin | Professeur à l'IMT Atlantique, Rennes. France |
| **Directrice de thèse** | : | MME. Atika RIVENQ | Professeure à INSA Hauts de France, UPHF. France |
| **Co-Directrice de thèse** | : | MME. Houda Labiod | Professeure à l'IMT, Télécom Paris, Palaiseau. France |
| **Co-encadrant de thèse** | : | M.Yassin ELHILLALI | Professeur à l'Université Polytechnique Hauts-de-France, UPHF. France. |

## ABSTRACT

Vehicle communication networks are considered as a relevant solution for ensuring the safety of road users and making road traffic more fluid. Indeed, these vehicular networks make possible the deployment of Cooperative Intelligent Transport Systems (C-ITS). Thanks to C-ITS applications, vehicles could exchange information about road traffic and related events.

However, as a side effect, these communications also make vehicles more vulnerable to cyber-attacks. Data exchanges depend on a centralized security architecture, which weakens with the increase in vehicles. A better solution would be to use a decentralized safety architecture to rectify this effect, where each vehicle could be involved in safety management. Thus, growing a fleet of vehicles can lead to more robust security. However, such a solution is not trivial because, in general, solutions of decentralized architectures are generally confronted with significant difficulties in terms of scalability.

Also, in this thesis, an efficient and secure solution for integrating a decentralized architecture dedicated to the vehicular communication system has been defined. To do this, we started by developing a blockchain-based architecture dedicated to highway toll systems. Subsequently, we defined a solution based on operational research for the geographic distribution of blockchain networks. This solution guarantees effective management of the security of vehicle networks depending on road traffic. In addition, thanks to the proposed improvements, the proper functioning of all C-ITS applications could be guaranteed. Finally, a new solution for real-time certificate revocation has been introduced. The proposed approach, thus using Blockchain technology, aims to ensure a high level of security and significant scaling up.



**Keywords:** *Cooperative-Intelligent Transport Systems*, *Cyber-Physical Systems*, *V2X Communications*, *VANETs*, *Blockchain*, *Cybersecurity*.

**Résumé**

Les réseaux de communication véhicule sont considérés comme une solution pertinente pour assurer la sécurité des usagers de la route et fluidifier le trafic routier. En effet, ces réseaux véhiculaires permettent le déploiement de Systèmes de Transport Intelligent Coopératifs (C-ITS). Grâce aux applications C-ITS, les véhicules pourraient échanger des informations sur le trafic routier et les événements qui y sont associés.

Cependant, comme effet secondaire, ces communications rendent également les véhicules plus vulnérables aux cyberattaques. Les échanges de données dépendent d'une architecture de sécurité centralisée, qui s'affaiblit avec l'augmentation du nombre de véhicules. Une meilleure solution serait d'utiliser une architecture de sécurité décentralisée pour rectifier cet effet, où chaque véhicule pourrait être impliqué dans la gestion de la sécurité. Ainsi, la croissance d'une flotte de véhicules peut conduire à une sécurité plus robuste. Cependant, une telle solution n'est pas anodine car, en général, les solutions d'architectures décentralisées sont généralement confrontées à des difficultés importantes en termes d'évolutivité.

Aussi, dans cette thèse, nous nous sommes intéressés à la définition d'une solution efficace et sécurisée pour intégrer une architecture décentralisée dédiée au système de communication véhiculaire. Nous avons donc commencé par proposer une architecture basée sur la blockchain dédiée aux systèmes de péage autoroutier. Par la suite, nous avons défini une solution basée sur la recherche opérationnelle pour la répartition géographique des réseaux blockchain. Cette solution garantit une gestion efficace de la sécurité des réseaux de véhicules en fonction du trafic routier. De plus, grâce aux améliorations proposées, le bon fonctionnement de toutes les applications C-ITS a pu être garanti. Enfin, nous avons introduit une nouvelle solution pour la révocation de certificats en temps réel. L'approche proposée, utilisant ainsi la technologie Blockchain, vise à assurer un haut niveau de sécurité et une mise à l'échelle significative.

**Mots-clés:** *Systèmes de Transport Intelligents coopératifs*, *Système Cyber-Physique*, *Communications V2X*, *VANETs*, *Blockchain*, *Cybersecurité*.

**Remerciement**

Je tiens à remercier toutes les personnes qui ont contribué à ce travail.

Tout d'abord, j'adresse mes remerciements à ma directrice de thèse Mme ***Atika RIVENQ***, grâce à elle ce travail a pu aboutir. Je la remercie chaleureusement pour sa présence, son soutien inconditionnel, ses qualités humaines et sa confiance qui m'ont accompagnée durant ces années.

Je tiens à remercier vivement ma co-directrice de thèse Mme *Houda Labiod* pour sa disponibilité, sa gentillesse et le partage de ses précieux conseils.

Je tiens à remercier mon encadrant Mr *Yassin EL HILLALI* , pour son aide, le temps passé ensemble, son écoute et ses conseils.

Je tiens à remercier vivement Mr *Mohammad Abdullah AL FARUQUE* pour son bon accueil au sein de son laboratoire de recherche durant mon stage à Irvine USA, pour sa disponibilité et le partage de son expérience.

Je présente également mes remerciements à tous les membres du jury : Mr. *Hacène Fouchal*, Mr. *Nael B. Abu-Ghazaleh*, Mr *Mohammad Abdullah Al Faruque*, Mr *Jean-Marie Bonnin*, M *Pierre Boulet* qui ont accepté d'examiner mon travail et pour l'intérêt qu'ils ont porté à ce dernier.

J'adresse mes vifs remerciements à mes parents et mes deux soeurs pour leurs accompagnements et encouragements permanents et leur soutien perpétuel et inconditionnel

Je tiens à remercier tous les membres des laboratoires IEMN à Valenciennes, ceux du CECS à Irvive et sans oublier ceux des projets C-ITS: collègues et amis, qui ont su m'aider, apporter leur soutien et faire de cette période de thèse une profonde réussite professionnelle et personnelle.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

CHAPTER 1

# Introduction

## 1.1 Context and Motivation

Every year, tens of millions of people are killed or injured in traffic accidents. Faced with this observation, the design of tools to ensure the safety of road users appeared essential. With the advent of wireless communication networks and mobile terminals, vehicular communication networks have emerged as a potential solution. Indeed, by establishing communications between vehicles, it becomes possible to guarantee the efficient transmission of information concerning the state of the road, the presence of an obstacle, or sudden braking. Also, based on these vehicular networks, a new paradigm has emerged: the Cooperative Intelligent Transport Systems (C-ITS, Cooperative Intelligent Transportation Systems). These, thanks to vehicular communications, should make it possible to improve road safety, traffic flow, and the comfort of road users.

A fully decentralized architecture based on direct communications between vehicles was first considered for the deployment of vehicular communication networks. This decentralized ad hoc network (VANet, Vehicular Ad Hoc Network) guaranteed rapid transmission of information between neighboring vehicles without requiring the deployment of expensive road infrastructure. Also, vehicular networks have evolved towards a centralized or hybrid architecture: the Internet of Vehicles (IoV, Internet of Vehicles). This architecture combines the advantages of an ad hoc approach (low latency) and a centralized approach (efficient data processing, interoperability). The IoV is based on three main ideas. First of all, different communication technologies are integrated: ITS-G5 (IEEE 802.11p), LTE-V2X, 5G NR, etc. Then, vehicular networks are included in the Internet of Things, allowing communications between vehicles and surrounding objects.

Therefore, it is mandatory to secure these wireless communications to ensure that all technologies meet security requirements. Furthermore, safety should be particularly considered in connected autonomous vehicles, where a vulnerable system component can be exploited to cause dangerous consequences, such as injury or even loss of life. For these reasons, several types of security architectures linked to V2X have been proposed. The current V2X security architecture is based on a centralized architecture where all vehicles are identified, authenticated, authorized, and connected through central cloud servers that use a public key infrastructure (PKI). However, this centralized architecture had different limitations:

- High overload on the Authorities servers;
- It is very difficult or even impossible for the authorities to follow the behavior of each vehicle in order to comment on its "misbehavior/good behavior."
- Vehicles that could detect other vehicles misbehavior could have a hard time denouncing them so that they can be revoked.

Finally, creating a decentralized and collaborative blockchain-based security system becomes possible thanks to the permanent Internet connectivity offered by the IoV. With these developments, the Blockchain opens up vehicle networks to a significant challenge for their adoption.

## 1.2 Problem Formulation

Various works have focused on the use of the Public Key Infrastructure system in the IoV environment. Nevertheless, essential problems remain [64]:

- A PKI security architecture unsuited to the needs of C-ITS applications: the implementation of the security system for exchanges between vehicles, connected objects, and road infrastructures is based on the underlying IoV communication architecture. Also, this architecture must guarantee the proper functioning of C-ITS applications. However, the current reference architecture is faced with various issues related to resource management, network reconfiguration, or even support for heterogeneous platforms. Also, to guarantee optimal operation of C-ITS applications, the definition of a new communication architecture is necessary;
- Insufficient communications security: securing communications is an essential issue for vehicular networks. Indeed, the exchange of information must make it possible to ensure the safety of road users. Securing these exchanges (authentication, access control) is therefore essential. However, the solutions proposed so far have various limitations, including lack of scalability, high deployment cost, an insufficient level of security. This is why the development of new authentication and access control mechanisms for vehicle networks is necessary. The establishment of an efficient STI has opened up several avenues and research challenges;
- The size of Revoked Certificates List: currently, all revoked certificates must be declared to the other vehicles. The authorities must send lists containing all the revoked vehicles, where the size impacts the quantity of data sent to each vehicle and the processing time taken by each vehicle to consider it. This is why several studies have been proposed to simplify this list.

## 1.3 Contribution

In order to allow a geographical distribution of data via an efficient cellular infrastructure, the work carried out within the framework of this thesis aimed to offer a solution to the problems identified above. Thus, we have contributed to:

- The definition of a new IoV communication architecture: as we have noted, the reference IoV communication architecture has various limits, both in management, control and security. To overcome these limitations, different technological solutions could be considered: software networks, virtualization, artificial intelligence, etc. Also, based on an analysis of the benefits of these technological solutions, we have proposed various evolutions of the benchmark IoV architecture to meet current limits;
- The definition and implementation of a framework approach for geographic distribution of data: as we have noted, the protocol used for the geographic distribution of data via the cellular infrastructure is expensive in resources and inflexible. To overcome these limitations, a framework approach seems relevant. Indeed, it could guarantee a high level of dynamicity and programmability as well as centralized decision-making. Also, starting from the current limits, we have proposed a

powerful software approach for the geographic distribution of data. Through various experiments, the benefits of our solution have been demonstrated, both in terms of resource-use flexibility and latency;

- The definition and implementation of a Blockchain-based approach for securing exchanges: as we have noted, securing communications are essential for vehicular networks. For this security, Blockchain technology could be used. Indeed, it could help ensure a high level of security, better scaling up, and low costs. Also, by placing ourselves within the framework of software-defined networks, we proposed a solution based on this technology for authentication and access control of IoV elements. The experiments have demonstrated the benefits of the proposed approach, particularly in scaling up and security (access control).

## 1.4 Manuscript Architecture

Chapter 2 "**Cooperative Intelligent Transport Systems and Internet of Vehicles**": This chapter presents the current state of vehicular networks. To do this, we first introduce the main characteristics of vehicular communications and existing projects and their communications architectures;

Chapter 3 "**Towards a decentralized security system for V2X communications**": This chapter put forward the prerequisites in terms of cybersecurity to introduce the current security system. Following this, we highlight the techniques behind the maintenance of vehicles privacy. Finally, we justify the revolution of ad hoc vehicular networks towards the IoVs and explain the evolution of ad hoc vehicular networks towards decentralized networks based on Blockchain;

Chapter 4 "**TileChain: A new Geographic Blockchain Architecture for V2X Communications**": In this chapter, we introduce our first two contributions: An application case on securing the exchange of confidential data for tolls process using V2X communications, as well that the evolution of the C-ITS blockchain-based reference architecture to enable a system that integrates vehicles with a direct contribution to the security of the vehicular network. To do this, we first identify the current limits of the reference architecture. Then, we present the leading existing technological solutions. Then, we highlight the improvements of the reference architecture already proposed in the literature and identify their limits. Finally, we propose a new TileChain architecture, which is based on an optimization problem and the Blockchain technology;

Chapter 5 "**New Blockchain-Based Cooperative Certificate Revocation Framework**": in this chapter, we introduce our third contribution: an approach for dynamic network clustering by creating a community of vehicles capable of revoking malicious vehicles in real-time. To do this, we begin by identifying the limitations of the protocol currently integrated into the reference architecture. We also highlight the benefits of an approach for this local distribution for certificate revocation. In addition, we target the points that must be considered to offer a powerful software approach in a mobile environment. We then present the existing works and identify their limits. Then, to answer it, we propose a new solution for the creation of cooperative communities. This is based, in particular, on the dynamic selection of the neighborhood suitable for the proper functioning of the revocation process and the use of state machines. Finally, we demonstrate the applicability of our solution for real use;

Chapter 6 "**Novel Centralized Pseudonym Changing Scheme for Location Privacy in V2X communication**": In this chapter, we present three main contributions that aim to enhance privacy in VANET. Firstly, we propose a context-adaptive and Authority-centric privacy scheme, which ensures the protection of sensitive information while facilitating efficient communication within the VANET context. Secondly, we introduce a Knapsack problem-based algorithm designed for trajectory combinations and users' traceability, enabling effective route planning while preserving user anonymity. Lastly, we evaluate

real-life user privacy by analyzing data from On-Board Units (OBUs) developed by different countries, offering valuable insights into privacy measures and identifying potential vulnerabilities for further improvement;

Chapter 7 "**Performance Evaluation**": in this chapter, we introduce our experiments made in-kind graduation: To be able to carry out real experiments, it was necessary to also work on the lower layers of the ITS stack. For that, we introduce the material used as well as Software Defined Radio. Next, we define the techniques on which our algorithm is based. Finally, we demonstrate the feasibility of our approach by focusing on the issue of its deployment;

Chapter 8 "**Conclusion and perspectives"**: in this chapter, we present a general conclusion of the work described in this manuscript. In addition, we also offer some perspectives for future research work in line with this thesis.

CHAPTER 2

# Cooperative Intelligent Transport Systems and Internet of Vehicles

## 2.1 Introduction

To properly prelude autonomous vehicles' arrival, automotive manufacturers rely more and more on individual techniques with partial delegated driving on the highways and shared vehicles with total delegated driving in urban and peri-urban areas shuttles or autonomous taxis. These new vehicles will have to increase their vision beyond the perception bubble of their onboard sensors (camera, lidar, and radar), extending to several hundreds of meters. The only way to do so is to use vehicular communications (V2X). The main objectives are to design road safety improvement devices on board the vehicle on the one hand and deployed in roadside units on the other hand . This should be based on rapid and secure communication between vehicles, infrastructure, and vulnerable users. Hence, the main applications targeted concern, particularly road safety (Active Road Safety) and the technical obstacles to be removed concerning the definition of the communicating equipment carried by vehicles and vulnerable users in passive or active devices based on mobile wireless networks onboard ITS equipment.

## 2.2 Vehicular communications

### 2.2.1 V2X communication types

The transport sector is generally affected by several issues, such as traffic congestion and accidents. Despite this, it is also evolving concerning cooperation between vehicles. Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to Anything (V2X) technologies strive to provide communication models that can be used by vehicles in different application contexts.

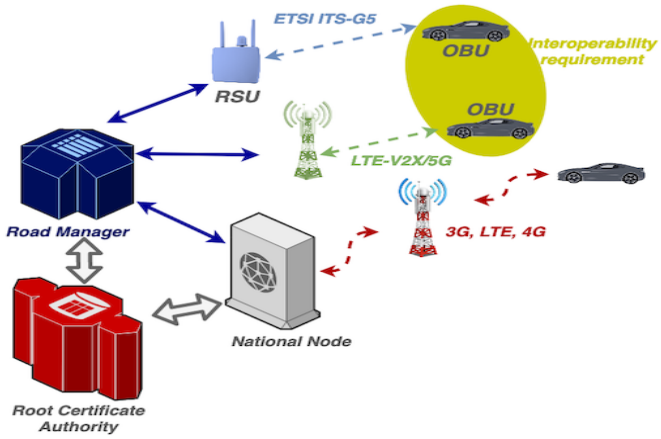



**Fig. 2.1** Global architecture and some of the used technologies in the C-ITS ecosystem

#### *2.2.1.1Vehicle To Vehicle (V2V)*

V2V technology is the wireless transmission of data between vehicles. This communication's primary purpose is to prevent possible accidents, allowing vehicles in transit to transfer data on their position and speed in an ad hoc mesh network. They use a decentralized connection system to provide either a fully connected mesh topology or a partially connected mesh topology. In the first case, each node is directly connected to the others in the network. In the second case, some nodes may be connected to all the others, while the others are attached only to those they frequently exchange most of the data. By exploiting this network topology, the nodes of a mesh network can exchange messages and information with neighboring nodes to which they are directly connected (a single hop, in the case of a fully connected network), or they can choose one of the different paths available to reach the destination (multi-hop, in the case of a partially connected network). This topology also increases the robustness of the network structure.

#### *2.2.1.2Vehicle To Infrastructure (V2I)*

Unlike the V2V communication model, which only allows the exchange of information between vehicles, the V2I allows vehicles in transit to interact with the road network. These items include RFID readers, traffic lights, cameras, lane markers, street lights, signs, and parking meters. In general, V2I communications are wireless, two-way, and similar to V2V, using dedicated short-range communication frequencies (DSRC) to transfer data. Information could be transmitted from the infrastructure elements to the vehicle, or vice versa, by an ad hoc network. In ITS, V2I sensors can acquire infrastructure data and provide travelers with real-time advice, sending information on road conditions, traffic jams, road accidents, the presence of construction sites, and parking spaces' availability.

#### *2.2.1.3Vehicle To All (V2X)*

The V2V and V2I communication models mentioned above are supplemented in V2X, which is a generalization. It transfers data from a vehicle to any entity that can influence it, vice versa, and integrates other more specific communication types, including Vehicle to Pedestrian (V2P) and vehicle to Road (V2R), Vehicle to Device (V2D), Vehicle to Network (V2N), and Vehicle to Grid (V2G).

### 2.2.2 Used Technologies for Vehicular Communications

#### *2.2.2.1ETSI ITS G5*

IEEE 802.11p (ITS-G5) is a WIFI-based (IEEE 802.11) telecommunications standard that is suitable for intelligent transport system (ITS) applications. ETSI (European Telecommunications Standards Institute) has standardized the IEEE 802.11p ITS-G5 standard, typically using 10 MHz bandwidth channels in the 5.9 GHz band (5.850-5.925GHz). ITS-G5 is a suitable standard for C-ITS for the following reasons:

- Low latency communications comparing to 4G cellular links
- No infrastructure requirement
- Reliable communications
- Communications range 200-1000m (View heard for the vehicle compared to RADAR, LIDAR)

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

**Table 2.1** ITS G5 frequency standard

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

#### *2.2.2.2Cellular-V2X technology (C-V2X):*

Cellular technology in V2X communication has started to be improved. The 3GPP organization started to address the evolution beyond mobile internet to IoT from 2020. Its main evolution compared to old networks (2G, 3G, 4G, 4G +, ...) is that in addition to improving its data transmission speed, new IoT and communications use cases will require new types of improved performance. Low latency plays a critical role in the evolution of 5G. This feature enables real-time interactivity of services using the cloud, and it is also a feature that ensures the development of self-driving cars. Also, the low power consumption will allow connected objects to operate for a particular time more significantly than the average (months or years) without human assistance. Currently, IoT services are a compromise in terms of performance in order to take full advantage of current wireless technologies such as those seen in progress (3G, 4G, Wi-Fi, Bluetooth, Zigbee, ...), while 5G networks will be designed to provide the level of performance necessary for a massive IoT. This technology will make it possible to offer an entirely connected world.

### 2.2.3 Type of messages

In the European ITS-G5 standard, the following types of messages have been defined:

#### *2.2.3.1Cooperative Awareness Message (CAM)*

Intended for cooperative awareness [68] (i.e., locating surrounding vehicles in real-time). This message type is sent automatically by the vehicle every 10 ms. They are intended to activate collective awareness, i.e., real-time locating vehicles or cooperative infrastructure, signaling vehicles' position and condition. Vehicles send CAM messages regularly, and all the ITS devices within range can receive and process them. The CAM message architecture is made of mandatory data and conditional data specified depending on the message's sender.

#### *2.2.3.2Decentralized environmental notification message (DENM)*

Alert messages [61] that are intended to be broadcast over a geographic area. They are issued only during an unexpected event. Triggering the sending of this message can be automated involving the various sensors present on the vehicle or result from a manual signal from the driver. DENM messages are defined by a header then a set of containers comprising different unit fields to be completed. The various fields defined in the standards are not all compulsory to fill in: it was, therefore, necessary to choose among the containers and the non-compulsory fields to construct the messages.

#### *2.2.3.3In-Vehicle Information Message (IVIM)*

Correspond to the information exchanged between the infrastructure and the vehicles [88]. This information mainly contains compulsory and advisory road signs, contextual speeds, and warnings concerning road works. In addition, IVIM provides physical road signs such as static or variable road signs, virtual signs, or road works. These messages are sent only by the infrastructure (e.g., RSUs) to support the dissemination of mandatory and advisory road sign information.

#### *2.2.3.4SPAT (Signal Phase and Timing)*

Messages are sent periodically by the ITS Road Unit (RSU) of the traffic light controller managed by the TLM [71] (Traffic Light Maneuverserver). These messages include safety-related information to help traffic participants (vehicles, pedestrians, ...) perform safe maneuvers in an intersection area. The objective is to enter and exit a "conflict zone" intersection in a controlled manner.

#### *2.2.3.5MAP*

Messages contain the topology of traffic infrastructure [71] (e.g., traffic gap, intersection, etc.). In an intersection scenario, the MAP is also sent in combination with a SPAT message. The MAP contains additional information, and a vehicle needs to relate signal phase and traffic light timing information to lane topology. It includes the topology of the tracks for, e.g., Vehicles, bicycles, parking, public transport, and paths for pedestrian crossings and maneuvers allowed in an intersection area or road section.

### 2.2.4 Use cases

This section presents some examples of use cases allowed by C-ITS technologies and currently used in Scoop project [14]:

#### *2.2.4.1Probe vehicle data*

The service is the automatic collection of road traffic data (ITS messages) from the vehicle to the road manager, and it can be used for data mining for specific purposes to create valuable indicators for the road manager.

#### *2.2.4.2Road works warning*

It is all the messages intended for the neutralization of lanes or the activation of emergency access. Neutralization can be due to a static road construction site but also to an accident. This use case can be in alternative mode or permanent road closure. The driver receives information about a road neutralization of part of a lane or a lane closure (but without road closure) due to a planned static or mobile worksite. The messages can also contain information about active operating agents.

#### *2.2.4.3In-vehicle signage*

The service consists of displaying "free text" type information to the user. The information can display what a physical VMS displays or display a new message (virtual VMS). Many other use cases use this service.

#### 2.2.4.4Toll Station Approaching

When a vehicle approaches a toll station, the traffic manager sends a specific message, helping the driver to have any information concerning the toll.

#### 2.2.4.5Hazardous location notifications

This use case is used to share information between the road operator and the vehicles. It is based on the sharing of information captured by sensors or observed.

#### 2.2.4.6Longitudinal Collision Risk Warning

Based on C-ITS received messages, the system detects or is informed of a longitudinal collision risk and send such notification to the driver and the other C-ITS stations involved in this collision risk to take immediate actions (including possibly ADAS actions). Longitudinal collision refers to the vehicles' collision (or a vehicle and an obstacle) at any part on the front or rear side.

#### 2.2.4.7Traffic Information and Smart Routing

Road operators provide Real-time local information on the environmental impact on road accessibility for display in road users' cars. The driver receives information on an intelligent recommended road based on a collective optimum. The service provides dynamic and up-to-date information on various topics on vehicle HMI (by broadcast). The end-user can access additional information in unicast mode. Additionally, a URL link can be displayed for more information. This use case can be customized for a specific type of vehicle (e.g., heavy goods vehicles).

#### 2.2.4.8Traffic Management

This service informs drivers of a permanent ban on driving specific vehicles on a specific road/section/area. A dynamic ban on all vehicles depending on a particular event can also be implemented. The service can also be used to notify vehicles if they can use it, depending on the characteristic of the vehicle chosen by the road manager.

#### 2.2.4.9Vulnerable Users

Based on infrastructure analysis, the service intends to prevent collision between a pedestrian and a vehicle by warning the drivers concerned with vehicles' approach when a risk of collision is identified to send a message to the vehicle approaching pedestrians.

#### 2.2.4.10Multimodal Cargo Transport Optimization

It aims to Optimize freight transport to logistics hubs by improving the predictability of truck travel times. And dynamic verification of status locations or slot reservations. This service is also used to inform freight carriers in real-time.

### 2.2.5 Components

The primary idea of vehicular networks is to ensure road safety by rapidly transmitting information to surrounding vehicles. Also, two components have been specially designed to allow these communications :

#### *2.2.5.1Onboard unit (OBU)*

onboard inside vehicles, this component allows vehicles to establish communication with surrounding terminal equipment and network equipment. The OBU is also used to process the information sent by vehicle sensors. The OBU is composed of different elements, in particular, sensors (GPS, CAMERA, LIDAR, RADAR), a network interface (antenna), and a central control module as shown in Fig. 2.2.

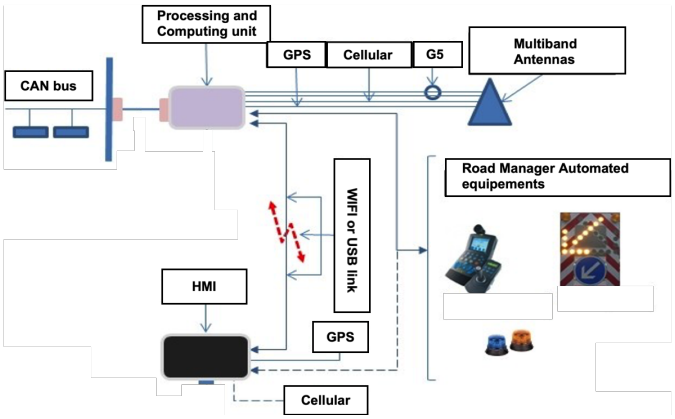



**Fig. 2.2** Onboard Unit components

#### *2.2.5.2RoadSide unit (RSU)*

is a fixed wireless access point positioned along roads (intersection, parking) and specifically designed for vehicular communications. The RSU has two essential roles. The first is distributing the information locally (to vehicles directly connected to it and neighboring RSUs). This RSU is also a gateway to the Internet network for vehicles and communication;

#### *2.2.5.3Traffic manager*

Traffic managers implement a targeted traffic management policy. To do this, they rely on the Center for Engineering and Traffic Management, an operational structure responsible for developing and implementing the dynamic operation strategy of the Road. The definition of traffic management strategies and the corresponding studies are carried out by the Traffic Management and Intelligent Mobility units of the Policy and Technical Department. With the emergence of innovative, intelligent transport systems, the traffic manager has acquired a dynamic management tool capable of real-time knowledge of traffic conditions and being proactive in launching the necessary operating measures. The functions performed by the supervision system are:

- Informing users upstream of disruptions (accidents, recommended routes, traffic jams, intervention on the road surfaces, particular weather conditions, re-routing in a crisis).
- Dynamic access and speed regulations
- The display of travel time data.

- "Non-operational" information (road prevention, pollution peaks).

#### *2.2.5.4The National Node*

The national node is the connection node for cellular communications with vehicles and national servers, and foreign countries through Internet links. The main advantage of hybrid architecture is the vast geographical communication coverage.

## 2.3 V2X European Projects

The hereafter introduced some C-ITS projected in Europe

#### *2.3.0.1InterCor*

InterCor [10] (Interoperable Corridors) is a European project that brings together France, Belgium, Netherlands, and United Kingdom and aims to launch C-ITS deployment in highways. InterCor also aims to make the information systems of European road managers interoperable to optimize the logistics chain. The overall objective is to achieve safer, more efficient, and more convenient mobility of people and goods. It is subsidized of 30 million euros over three years as part of the Connecting Europe Facility (CEF) program. This project brings together seventeen partner organizations in Europe:

- *France:* Ministry of Ecology, Sustainable Development, and Energy; Université Polytechnique Haut-de-France; NeoGLS; French Institute of Sciences and Technologies of Transport, Planning, and Networks; I-TRANS; Marseille Gyptis International; OpentrustKeynectis; SANEF; Telecom Paristech; University of Reims Champagne-Ardenne.
- *Belgium:* ERTICO-ITS, Flemish Ministry of transport,
- *United Kingdom:* The Department of Mobility  Public Works, Department for Transport,
- *Netherlands:* Rijkwaterstraat (ministry of transport); Provincie Noord Brabant; Provincie Utrecht.


**Fig. 2.3** The road network covered by V2X communications as part of the InterCor project

The role of each partner in this vast program is to provide expertise in terms of the interoperability of private systems applied to multimodal logistics. Furthermore, InterCor goes beyond the national perimeter and extends the merchandise traceability zone to the four partner countries. Finally, if the experiments prove conclusive, InterCor propose a technological standard that can be deployed in other European countries.

### 2.3.1 Fenix

FENIX [7] is developing the first European federated architecture for data sharing serving the European logistics community of shippers, logistics service providers, mobility infrastructure providers, cities, and authorities in order to offer interoperability between any individual existing and future platforms.

### 2.3.2 InDid

InDiD [9] is one of the C-ITS projects led by France. Its objective is to develop intelligent transport systems. The European Commission selected it as part of the CEF call for projects. The project is 50% co-financed by the European Union for five years (from 2019 until 2023). It follows on from previous C-ITS projects: SCOOP, C-ROADS, and InterCor. In addition to guaranteeing better road safety and good traffic management, the InDiD project develops new use cases intended for the urban environment and increased perception of the autonomous vehicle. In addition, it discusses high-definition digital infrastructure mapping. It also targets 5G-based vehicle communications tests for autonomous vehicles. This project is based on a solid consortium, bringing together 24 partners spread across France: interdepartmental road directorates, industrial players, motorway companies, and academic partners (universities and research centers ). InDiD aims to continue the deployment of C-ITS on new road test sites to extend the coverage of the services offered by the infrastructure. The pilot sites are located in 4 large French geographic basins, on the Mediterranean side, southwest, center, and north of France.

### 2.3.3 Scoop

SCOOP [14] is a french pilot project for cooperative intelligent transport systems deployment. Launched in 2014, it associates many public and private partners around the ecology ministry, sustainable development, and energy, which acts as a coordinator: local authorities, road operators, PSA and Renault car manufacturers, universities, and research institutes. SCOOP aims to deploy 3000 vehicles on 2000 km of roads on five sites: Ile-de-France, Paris-Strasbourg motorway, Isère, the Bordeaux ring road, Brittany.

### 2.3.4 C-Roads

C-Roads [3] is a platform that brings together the road authorities and operators of the Member States: France, Austria, Belgium, Czech Republic, Denmark, Finland, Germany, Hungary, Ireland, Italy, Portugal, Slovenia, Spain, Sweden, Netherlands, United Kingdom, Norway, Switzerland, and Australia. The objective of the C-Roads platform is to ensure road safety at the European level by aligning the specifications of Cooperative Intelligent Transport Systems (C-ITS) to guarantee the 'interoperability between European ITS. Rapid and EU-wide deployment of harmonized C-ITS services is key to this goal.

### 2.3.5 Interoperabilities tests

Called TESTFEST are interoperability tests, which brought together more than 15 international partners, including many companies in the automotive industry. The tests aim to test the interoperability of C-ITS between European partners. To do this, they have been divided into four parts:

- ITS-G5 tests: Aims to test essential functions of ITS-G5 and signal influence on the information circulation between vehicles and its influence on services.
- Tests for Hybridization: Aims to test hybrid operation, which combines the use of both ITS-G5 and cellular technologies. It allows full connectivity between vehicles and infrastructure.

**Fig. 2.4** Vehicles participating to Testfest in Reims (France)

- Test on the PKI aims to test the compatibility of development with security requirements. in particular, the revocation of certificates
- Test on services: Aims to test all the services developed as part of C-ITS projects and ensure their proper functioning
- Cross-Borders Test: Aims to put the vehicles in a position to cross the borders of two European countries and ensure that the vehicles keep the same operation.

## 2.4 Cyber-Security requirements

### 2.4.1 Required Proprieties of Security

The hereafter described protocol tries to reach the following security objectives

#### *2.4.1.1Authentication/authorization control*

Authentication consists to be sure of the identity which sends data. Authorization control is the verification of an access policy, based on a trusted authentication. Authenticate all entities participating in the protocol is required to prevent illegitimate persons to enter in the system, or to access some unauthorized resources or services.

#### *2.4.1.2Trust*

Is supported by the provision to ITS stations of certificates allowing them to affirm their permission to use the ITS system and to use specific ITS services and applications.

#### *2.4.1.3Access Control*

Is ensured by giving ITS stations cryptographically signed certificates of authorization, which allow them to use specific services or send specific information.

#### *2.4.1.4Integrity*

The integrity of all transmitted data is important to ensure that the contents of the received data are not altered.

#### *2.4.1.5Confidentiality*

Confidentiality of information transmitted in a unicast communication is protected by encryption of messages within an established security association.

#### *2.4.1.6Non-repudiation/Traceability*

Non-repudiation is necessary to prevent ITS Station or others entities from denying the transmission or the content of their messages. Traceability, which is the warranty that an entity can't refute the emission or reception of information, is also extremely important.

#### *2.4.1.7Anonymity*

Ability of a user to use a resource or service without disclosing the user's identity.

#### *2.4.1.8Unlinkability*

Ability of a user to make multiple uses of resources or services without others being able to link these uses together.

### 2.4.2 C-ITS Important Vulnerabilities

This section introduce three of most popular attacks in V2X communications

#### *2.4.2.1Wormhole Attack*

Messages are replayed in a different place and at another time. These attacks can be used to confuse recipients who are unable to resolve the problem.

#### *2.4.2.2Position Spoofing Attack*

A GNSS satellite simulator can generate stronger radio signals than those received from an actual GNSS satellite. Besides tampering with the software and sending fake positions, this method also allows an attacker to provide false location information to ITS-S and potentially cause traffic accidents.

#### *2.4.2.3Sybil Attack*

Other nodes will receive false information about neighbors' density by sending multiple messages from a node with different identities. The primary motivation of these attacks is to control road management by causing havoc. Attacks will be more detailed in section 5.2.

## 2.5 Communication and security architectures

The mapping of OSI modeling layers to the ITS architectural layers is for each layer of the ITS station architecture. For example, the Management and Security services are associated. Therefore, the expected functionality of the ITS station architecture layers can be mapped to the OSI model as shown in Fig. 2.5.

Facilities layer is mapped to the Application layer, Presentation layer and Session layer of the OSI model, Networking and Transport layer is mapped to the Transport layer and Network layer of the OSI model, and finally, the Access layer is mapped to the Data Link layer and Physical layer of the OSI model. Having mapped the OSI protocol layers to the ITS station architecture can be extended into an ITS communications architecture in which the protocol layers communicate on a peer-to-peer basis.

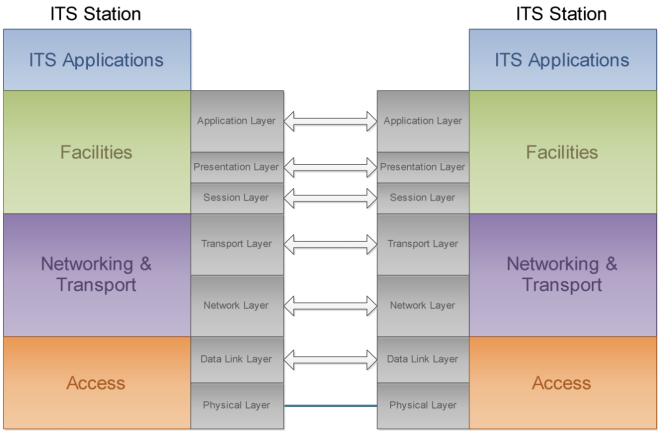



**Fig. 2.5** ITS communications architecture [70]

### 2.5.1 IEEE 1609.2 v2 security architecture

The IEEE 1609.2 standard [16] specifies a set of security services for supporting vehicular communications. It defines secure message formats and processing for Wireless Access in Vehicular Environments (WAVE- equivalent to ITS-G5 in Europe) devices, including methods to secure WAVE management messages and secure application messages. It also describes administrative functions necessary to support the core security functions. The standard classifies all the entities that provide or use IEEE 1609.2 security services into two categories:

– Certificate authority entities (CA entities)

– End entities

The CA entities are the only entities responsible for issuing certificates and Certificate Revocation Lists (CRLs). The IEEE 1609.2 defines two types of end entities: Secure Data Exchange Entity (SDEE) and secure provider service entity. In addition, it includes vehicles, roadside units (RSUs), application servers, and applications. The IEEE 1609.2 standard defines three types of CA entities:

#### *2.5.1.1Root CAs:*

Root CAs are trusted to issue certificates to all other CA entities and end entities. End entities trust the public keys of a Root CA. A Root CA issues certificates to other CA entities to authorize them to issue certificates or CRLs to end entities. The Root CA issues certificates to both CA and end entities within a defined region specified by the region field in the Root CA certificate.

#### 2.5.1.2Secure Data Exchange CAs:

SDE-CAs issue certificates to end entities that send application messages secured with IEEE 1609.2. A Secure Data Exchange CA (SDE-CA) is responsible for issuing certificates to SDEE and SDE-CA. The types of certificates that a SDE-CA is authorized to issue are:

- sde-ca,
- sde-enrolment,
- sde-identified-localized,
- sde-identified-not-localized,
- sde-anonymous
- crl-signer.
- WAVE Service

A SDEE can have three certificates types to secure its V2X communications:

- sde-identified-localized certificate,
- sde-identified-not-localized certificate, and
- sde-anonymous certificate.

#### 2.5.1.3Advertisements (WSA) CAs:

WSA-CAs issue certificates to end entities that send WSA. An end entity uses WSAs to broadcast what WSAs it provides. These certificates are named communication certificates. The sde-enrolment certificate is used to request new certificates. Wave Service Announcement CA (WSA-CA) is authorized to issue certificates for a security provider service that broadcasts WSAs advertising a specific set of services. The CRL Signers are CRLs distribution centers, which store and distribute certificates revocation lists (CRLs).

For user privacy protection, the IEEE 1609.2v2 standard defines anonymous certificates issued by Root CA or SDE-CA to an SDEE. The IEEE 1609.2v2 anonymous certificates are communication certificates without identifying information. More details can be found in [16].

### 2.5.2 ETSI architecture

In Europe, ETSI ITS Technical Committee Working Group 5 is responsible for the ITS security architecture, providing security standards and guidance on the use of security standards to protect and secure the ITS applications. In [70] standard specifies a security architecture for ITS communications. In addition, it identifies :

- Functional entities required to support security in an ITS environment.
- Existing relationships between entities and the elements of the ITS reference architecture.
- Roles and locations of security services for the protection of transmitted information and the Management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces, and basic policies and guidelines for trust establishment.

Firstly, the standard discusses the ITS reference architecture, which is based upon four processing layers identified as follows:

- Access Layer
- Networking Layer  Transport Layer
- Facilities Layer
- Application Layer

Secondly, it presents the communication behavior (addressing, frequency, direction) for each use case of the ITS applications. The ITS station (ITS-S) supports a range of security services. It is presented to provide communications security between ITS Station and other stations. Different categories of security services are defined: Enrollment; authorization; integrity; and plausibility validation service.

Security services are provided on a layer-by-layer basis, in the manner that each of the security services operates within one or several ITS architectural layers or the Security Management layer. Communications security services require more than one element within their functional model. Principal elements are:

- Enrolment Authority: authenticates an ITS Station (ITS-S) and grants its access to ITS communications.
- Authorization Authority: provides an ITS-S with definitive proof that it may use specific ITS services.
- Sending ITS-S: acquires rights to access ITS communications from the Enrolment authority, negotiates rights to invoke ITS services from Authorization Authority, and sends single-hop and relayed broadcast messages.
- Relaying ITS-S: receives broadcast messages from the sending ITS-S and forwards them to the receiving ITS-S if required.
- Receiving ITS-S: receives broadcast messages from the sending or relaying ITS-S.

Thirdly, the standard presents security management supported by ITS stations. For example, an ITS-S must provide secure access to shared resources such as services, information, and protocols. These security requirements can be separated into two parts: external security and internal security. External security represents the security related to the behavior of the ITS-S as a communication end-point, while internal security represents the security related to the ITS-S as a processing platform and application host.

Finally, the standard discusses how the ITS communication system relies on indirect trust relationships built using certification by trusted third parties such as the Enrolment Authority (EA). EA allows an ITS Station to be a part of the ITS communications by providing access control and permissions. Finally, the standard explains how ITS communications should support trust, privacy, access control, and confidentiality regarding ITS stations.

- Trust is supported by provisioning ITS stations with certificates allowing them to assert their permission to use the ITS system and use specific ITS services and applications.
- Privacy is supported by using pseudonyms that can be used in place of a more meaningful and traceable identifier.
- Access Control is assured by giving ITS stations cryptographically signed certificates from the Authorization Authority (AA), which allows it to use specific services or send certain information.

– Confidentiality of transmitted information in unicast communications is protected by encrypting messages within an established security association.

In [72] standard specifies the trust and privacy management for ITS communications. It identifies trust establishment and privacy management required to support security in the ITS environment and the relationships between the entities themselves and the elements of the ITS reference architecture. In addition, the standard presents ITS authority hierarchy, a PKI composed of an Enrolment Authority, Authorization Authority, and a Root CA, and used for distribution and maintenance of trust relationships between ITS stations and authorities or other ITS-S.

- *Enrolment Authority (EA):* The EA issues a proof of identity to authenticate the canonical identifier of the ITS-S by delivering an enrolment certificate. This proof of identity allows to not revealing the canonical identifier to a third party and may be used by the ITS-S to request authorization of services from an Authorization Authority;

- *Authorization Authority (AA):* Having received the enrolment credentials, the ITS-S requests its authorization certificate(s) from the AA. These certificates allow the ITS-S to have specific permissions. Separation of enrolment and authorization is an essential component of privacy management and protects against attacks on a user's privacy.

- *Root CA:* It issues certificates to all other Certificate Authorities. It is the root of trust for all certificates within that hierarchy. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. In order to trust an incoming message, an ITS-S must have access at least to the root certificate at the summit of the hierarchy for the authorization certificate attached to the message. Four key attributes related to privacy (anonymity, pseudonymity, unlinkability, and unobservability) are cited. According to the standard, privacy is provided in two dimensions: privacy of ITS registration and authorization signaling and privacy of communications between ITS stations.

After these definitions, the standard discusses trust and privacy management by presenting the ITS station security lifecycle that begins with the manufacturing phase and passes to the enrollment, authorization, and maintenance phases. Multiple information elements shall be established in the ITS-S at the Manufacture phase using a secure process such as a canonical identifier. Contact information for EA and AA (network address and public key certificate), the set of current known trusted EA and AA that an ITS station might use to initiate the enrolment process, and trust communications from other ITS-S, respectively.

At the end of the document, security associations and key Management between ITS-S during the broadcast, multicast, or unicast communications are discussed. For broadcast communications, messages do not require confidentiality; CAMs and DENMs are signed using authorization certificates. Whereas for multicast and unicast applications, communications shall be encrypted, and key Management is required.

In [67] ETSI defines a Threat, Vulnerability, Risk Analysis (TVRA) approach. TVRA provides security objectives and functional security requirements. It also defines the proof that links security requirements and security objectives by giving the global security architecture.

The standard describes the general ITS G5A security model and presents related security services for each countermeasure. These security services are divided into two levels:

- Security services identified as "The first Level" are those that are invoked directly by applications in the ITS Basic Set of Application (BSA).

- Services identified as "Lower Level" are those that are invoked by other security services.

The standard mapped countermeasures to the CIA paradigm (Confidentiality, Integrity, and Availability) and represents ITS security services into two different groups: security service at transmission (Tx) and security service at reception (Rx).

After that, the document presents the ITS authoritative hierarchy composed of the manufacturer, EA, and AA. It also gives each of these entities the role, the different trust assumptions on which rely on the ITS system's security, ITS security parameters management such as identities and identifiers, and authorization and privacy with authorization tickets.

### 2.5.3 Car 2 Car Communication Consortium architecture

The security working group of the C2C-CC defined the same PKI architecture as ETSI;

#### *2.5.3.1Root CA*

The Root CA issues certificates for LTCA and PCA. It also defines and controls policies among all subordinate certificate issuers. The Root CA is only required once a new LTCA or PCA shall be created or when the lifetime of an LTCA or PCA certificate expires.

#### *2.5.3.2Long Term Certificate Authority (LTCA):*

The LTCA issues for each ITS-Station an LTC that is valid for a long period. This Long Term Certificate is only used to identify and authenticate the ITS-S within the PKI and is never used in V2X communication for privacy reasons. It also enables ITS-S to request pseudonym certificates.

#### *2.5.3.3Pseudonym Certificate Authority (PCA):*

The PCA issues a short lifetime certificate used in V2X communications. The PCA guarantees the privacy of requesting ITS Stations since it is technically and operationally separated from the LTCA, which is the only authority that knows the real identity of the ITS-S.

### 2.5.4 General Security Architecture

On the $15^{th}$ October 2014, The National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT) published a Request for Information (RFI) named as Vehicle-to-Vehicle Security Credential Management System (V2V SCMS). The purpose of this RFI is to seek responses concerning the establishment of an SCMS, security approaches for a V2V environment, and technical and organizational aspects of the SCMS. In the following, we present a brief description of the V2V security system considered by NHTSA. According to the RFI, three primary elements of the V2V system requires security, which are:

– The V2V communication such as the medium, messages, data, certificates, and any other element that supports message exchange,

– V2V devices (cars),

– V2V security system itself through organizational, operational, and physical controls.

For this reason, different security technologies were assumed to be effective in providing trusted message exchange and secure communications. These technologies are symmetric encryption, signature group, and PKI. Since it offered the most effective approach to achieving communications security and trusted messaging for an extensive set of users in the V2V system, asymmetric Public Key Infrastructure (PKI) using the signature method was selected by DOT and NHTSA along with Crash Avoidance Metrics Partnership (CAMP) security experts. The SCMS Manager is responsible for all other entities and functions, including certificate processing for devices, misbehavior detection, and revocation of certificates. The security, privacy operations, and components are used to distribute certificates to protect users' privacy. Entities of the V2V system are grouped into four classes:

– Overall Management,

– Registration and Enrollment,

– Certificate Management,

– Misbehavior Management.

SCMS is an integral part of V2V security design. It encompasses all technical, organizational, and operational aspects of the V2V security system needed to support trusted, safe/secure V2V communications and protect driver privacy appropriately. Fundamental SCMS operating functions categories are:

– Pseudonym functions,

– Bootstrap functions.

– Pseudonym functions/certificates

Since V2V communications rely on sending and receiving CAMs, short-term certificates become necessary to authenticate and validate these messages. A valid short-term certificate indicates that the CAM was transmitted from a good and trusted source. In contrast, a revoked certificate implies that other V2V devices will reject the messages. In order to create, manage, distribute, monitor, and revoke short-term certificates, pseudonym functions were identified in Fig. 2.6 and defined as follow:

#### *2.5.4.1Intermediate Certificate Authority (Intermediate CA)*

It is considered as an extension of the Root CA. Its primary roles are:

- Authorize other CMEs and possibly Enrollment CA, using authority from the Root CA,
- Protect Root CA from direct access to the internet,
- Provide flexibility by removing needs to connect to RCA each time a new SCMS entity is added to the system.

However, Intermediate CA does not hold the same authority as the Root CA; it cannot self-sign a certificate.

Authority (LA)Linkage values help PCA calculating a certificate ID in a way to connect all short-term certificates from a specific device for ease of revocation in the event of misbehavior. Linkage Authority is responsible for:

- Generating linkage values as a response to RA and PCA requests,
- Communicate only with RA to provide these values.

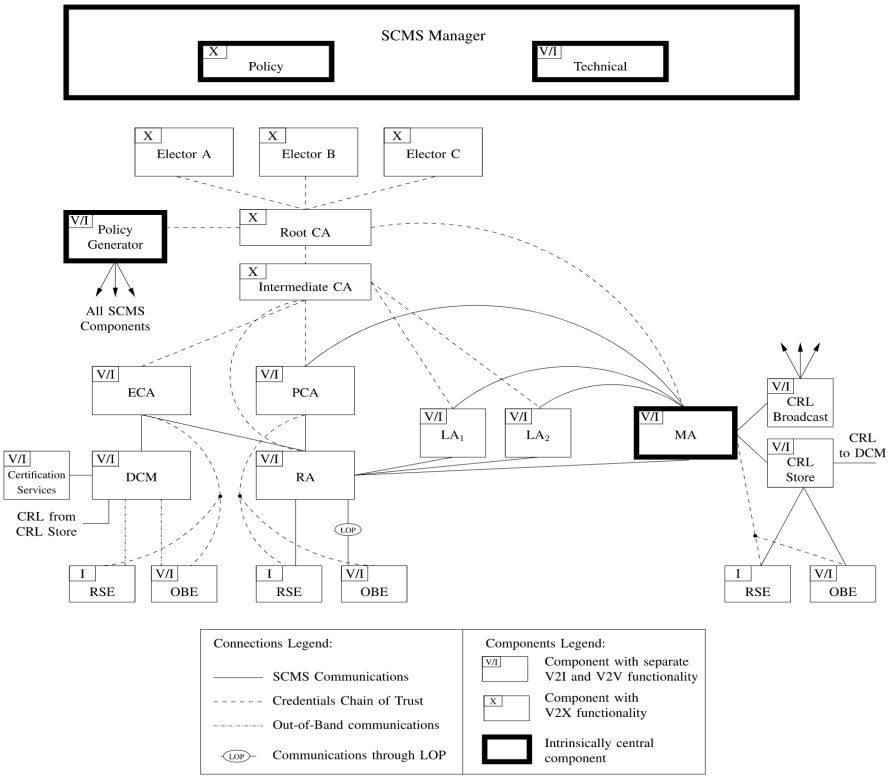



**Fig. 2.6** SCMS architecture overview [39]

#### *2.5.4.2Location Obscurer Proxy (LOP)*

Communications between ITS-Ss and SCMS components must pass through LOP. The leading roles of LOP are:

- Obscure the location of the ITS-S seeking to communicate with the SCMS functions,
- Shuffle misbehavior reports that ITS-Ss send to the MA (for more privacy purposes),
- Increases participant privacy.

#### *2.5.4.3Misbehavior Authority (MA)*

This entity is responsible for detecting misbehavior in the system by performing plausibility checks to messages or detecting potential malfunction or malfeasance within the system. Its main roles:

- Process misbehavior reports
- Produce and publish the certificate revocation list (CRL)
- Works with Pseudonym CA, Registration Authority (RA), and LA to acquire necessary information about a certificate and create entries to the CRL through CRL Generator.

#### *2.5.4.4SCMS Manager*

SCMS Manager is the primary managerial component of the SCMS. It is responsible for managing all other component entities called Certificates Management Entities or CMEs. In addition, it provides

the policy and technical standards for the V2V system, ensures interoperability, security, privacy, and auditing of the system, and manages the activities required for the operation of the SCMS.

In addition to pseudonym functions, the security design also includes the bootstrap process. The Enrollment CA (ECA) is the functional component of this process. It assigns a long-term certificate to V2V devices at the first connection to the SCMS. The bootstrap process includes the following functions:

#### *2.5.4.5Certification Lab*

Provides ECA with policies and rules for issuing enrollment certificates. This is usually done when a new device is released to the market or the SCMS Manager releases new rules and guidelines.

#### *2.5.4.6Device Configuration Manager (DCM)*

This entity is responsible for:

- Giving devices access to new trust information such as updates to authorities certificates, policy decisions, and technical guidelines issued by SCMS Manager,
- Sending software updates to devices,
- Coordinating initial trust distribution with devices by passing on credentials for other SCMS entities,
- Providing devices with information it needs to request short-term certificates from RA,
- Providing a secure channel to the ECA to communicate Enrollment certificates devices. Two types of connections are used between devices and DCM, an in-band communication that passes through LOP, and an out-of-band communication that passes directly from the device to the ECA via DCM.

#### *2.5.4.7Enrollment Certificate Authority (ECA)*

It produces the enrollment certificate and sends it to the OBE, but first, it verifies the validity of the device type with the Certification Lab. The OBE uses the enrollment certificate to be able to request and receive certificates from the SCMS.

#### *2.5.4.8SCMS Organizational model*

The organization of the SCMS should be capable to:

- enable secure and efficient communications,
- protect privacy
- minimize operational costs
- The final organizational model of the SCMS is represented below; it is based on:
  - Organizational connections and separations,
  - Closely related process of characterizing functions as "central" or "non-central" (which is related to the issue of system ownership and operation).
  - Organizational separation of functions is an example of a policy control often used to reduce privacy risks in PKI systems, but such separations come with increased costs and may negatively impact the system's ability to identify and revoke the credentials of misbehaving devices.

## 2.6 Conclusion

In this chapter, we described the vehicular communications environment. To do this, we started by presenting in Section 2.2 the main characteristics, the types of communications, and the components defining vehicular networks.

In a second step, we introduced the various European projects in Europe Section. 2.4.1 and the conditions required to secure the C-ITS system and the major attacks to guard against Section. 2.4.2.

Finally, in the Section. 2.5 we focused on the different security architectures adopted by the standardization organizations. This gives us a macro view of the existing architectures in Europe and the US and their differences.

CHAPTER 3

# Towards a decentralized security systems for V2X communications

## 3.1 Introduction

The traditional PKI security architecture for vehicular communications is a hierarchical architecture where each layer consists of different authorities. The root certification authority (RCA) acts at the top of the hierarchy of certification authorities. It controls all subordinate certification authorities and end entities on its scale. A trusted certificate is provided to every last legitimate entity and can be revoked or blocked if an entity misbehaves. Furthermore, to protect users' privacy, a crucial parameter of pseudonym schemes must be considered. The PKI architecture must respond to how and when pseudonyms are changed.

This chapter points out the similarities between V2X communications and IoTs, shows the limitations of traditional architecture and introduces decentralized solutions. We will also define the most used solution currently in decentralized systems, Blockchain. Finally, we give multiple contributions in different similar fields.

## 3.2 Public Key Infrastructure (PKI)

The PKI system used in intelligent transport systems is based on the architectures introduced in Section 2.5. In this part, we will focus on the different mechanisms used to ensure the security in V2X networks.

### 3.2.1 The Pseudonyms Certificate changes

In this section, we will give a detailed overview of the used mechanisms to ensure users privacy as detailed in [151].

#### *3.2.1.1Identifiers*

There are many different addresses, IDs, or other identifying information scattered around the network layers.

- *GeoNetworking:* Each GN node is identified by [60], containing information about the ITS-S type (passenger car, cyclist, pedestrian, RSU, ...) and 48bit derived from the link-layer address.

  In the case of a pseudonym change, only the latter part is supposed to change. GN packets have a basic, a common, and an optional extended header. The basic header contains information like the packet's maximum lifetime and the remaining hop limit. This information is non-critical for identification.

  The standard header also does not contain identifying information. Only the flag indicating a mobile or stationary ITS-S could slightly reduce the anonymity set. The extended header fields depend

on the actual GN package type and contain information like the sequence number (initialized with 0) and position vectors.

GeoNetworking Location Table entries also contain identifying data: Additionally to the GNADDR, station type, and the link-layer address of the peer node, it contains a timestamped geographical position (including accuracy), its current speed, and its heading. GN packets can be secured by wrapping them into security headers as defined in [65].

The certificates used contain information about the signer subject (name, type, keys), validity restrictions, and the actual certificate signature from the Certificate Authority (CA). The signer information can be given in the form of a digest, certificate or certificate chain. In addition, the security trailer contains a signature for verifying the authenticity and integrity of the message.

- *Facilities Layer:* The Facilities layer introduces a StationID, an integer identifying the ITS system. The standard document [21] already mentions that this ID may be a pseudonym.

- *Basic Transport Port (BTP):* The BTP header is only 4 bytes long and has a simple structure. There are two modes of operation for BTP: interactive packet transport using the BTP-A header, meant for services requiring replies to their messages, and non-interactive packet transport using the BTP-B header.

- *IPv6:* While each IPv6-capable network interface can have multiple addresses, it has at least one link-local address with the interface ID (the lower 64bits) uniquely derived from its data-link layer address. The mapping of the IPv6 link-local address and GNADDR is straightforward, as both addresses are deterministically derived from the same link-layer address. Additionally to the IPv6 address, the IPv6 header can also contain a flow label which could lead to partial linkability of packets even after an address change: Although a flow shall be identified by the triplet of the flow label, source, and destination address, an equal flow label could indicate the resumption of a connection even after an address change.

  There exists a static mapping between IPv6 multicast groups and geographical areas (relative to the station). That means it is possible to contact IPv6-based services within a node's surroundings.

  However, as this mapping is static and relative, it should not help reidentify hosts. Geographical Virtual Links (GVLs) are another important concept for understanding the visibility scope of IPv6 packets to other nodes. These virtual links are defined as non-overlapping, restricted geographical areas wherein all IPv6 multicasts within the same subnet are forwarded via GN to all nodes of that GVL.

  Usually, this zone around a specific RSU serves as an Internet uplink, thus managing the whole subnet and its addresses. Globally routable IPv6 addresses are usually obtained via the stateless autoconfiguration with the help of RAs. So changing the GVL means getting another IPv6 prefix announced via RA and thus implies a change in the node's global IPv6 address.

#### *3.2.1.2Pseudonym Schemes*

As shown in the previous section, ITS communication contains many identifiers potentially allowing linking vehicle communication even over more extended periods and thus tracking and creating movement profiles of vehicles.

This is a clear threat to the vehicle user's privacy, more precisely, the location privacy. Complete anonymity of all network participants is no viable countermeasure, as security-critical systems like these require certain levels of authenticity of data and accountability of the participants.

Furthermore, request-response message schemes require at least short-term linkability of messages to establish a joint session. This is needed, e.g., for requesting data from infrastructure or managing an automatic payment at car chargers.

A widely chosen approach for restoring user privacy is using temporary pseudonyms for identification in the network. This section will look at the usage and kinds of pseudonym schemes in the ETSI standards, explore other approaches outside of the standardized ETSI world and look at when to change pseudonyms to minimize the long-term linkability of nodes.

*Pseudonym Management:* The ETSI standard on trust and privacy management [72] mentions the goal of pseudonymity and unlinkability of ITS nodes and their messages as the way to achieve ITS privacy. This privacy goal is subdivided into two dimensions: The privacy of ITS registration and authorization shall be achieved by limiting the knowledge of a node's canonical (fixed) identifier to a limited number of authorities. Furthermore, the responsibility for verifying the validity of a canonical identifier is given to an Enrolment Authority (EA) and split from the authorization to services by the Authorization Authority (AA). Both these authorities are parts of the needed Public Key Infrastructure (PKI) and need to be operated in different areas of control to achieve a surplus of privacy. During manufacture, the following data is to be stored in an ITS node using a physically secure process:

- a globally unique canonical identifier
- contact addresses + public keys of an EA and AA,
- a set of trusted EA and AA certificates

The EA has to hold the following information about a node: The permanent canonical identifier, enrollment credentials, public key, and a link to further profile information. ITS nodes can now request an enrolment certificate with their enrolment credentials from the EA. The task of the EA is to verify that an ITS node can be trusted to function correctly, as the EA must only know the credentials of certified ITS nodes. The credentials of compromised nodes have to be revoked. With the enrollment request being encrypted and signed by the enrolling node and the response is encrypted, only the EA knows the mapping between the enrollment certificate and the requesting identity. The enrollment certificate contains a pseudonymous identifier signed with a certificate chain leading back to the originating EA. This enrollment certificate can then be used to get Authorization Tickets (ATs) from an AA.

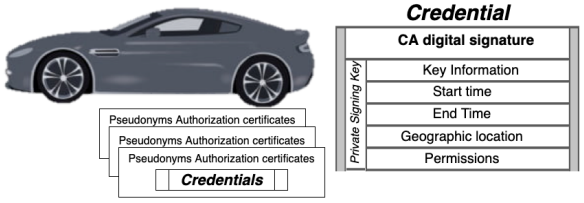



**Fig. 3.1** Credential composition

These ATs are certificates denoting the permissions a node has. Authorization ticket certificates contain some user's information as shown in Fig. 3.1 may be stored in a Hardware Security Module (HSM) to prevent unregulated access to the cryptographic keys. At least the security service Specification offers such an option. All authority responses are encrypted and signed in a way verifiable for the node. Certificate requests include a start and end time, and a challenge [67], a random string encrypted with the receiver's public key. These two measures prevent message replay attacks. Enrolment credentials and ATs can also be updated if needed over similar mechanisms.

The second dimension of privacy covers the communication between ITS-Ss. The obtained authorization tickets serve as pseudonyms for authenticating and signing messages with other ITS services and

nodes. ITS-S must check the validity of the AT certificates included in every message and check the permissions for the message's action (e.g., sending messages to certain broadcast domains) or access to certain services. These pseudonyms are to be regularly changed to preserve the privacy of the node's user by achieving long-term unlinkability of messages by the ITS node. There are different kinds of ATs:

- Those used by official role vehicles (e.g., state authorities) and ITS infrastructure do not always need to preserve the node's privacy and thus can contain a long-lived identifier for the official role they are fulfilling.
- ATs of individual user nodes can contain further personal identifying information if required for service usage but then shall only be sent to already authorized nodes over encrypted channels.
- For broadcasting, first contact, and all other uses, individual user nodes shall only use minimal pseudonymous ATs, which can be sent even over non-encrypted channels.

The ETSI standard [64] mentions retaining an audit log of incoming messages to hold nodes accountable in case of misbehavior. However, this only helps if the EA retains a mapping of enrollment certificates to the canonical identifiers they were given to, and the AA does the same for ATs and enrolment certificates. The legal and organizational framework for making sure that the information from the EA and AA are only combined for legitimate cases is crucial for maintaining user privacy but is left out of the scope of this survey. For Revocation of node access to the ITS network, e.g., in case of misbehavior, there are multiple mechanisms: The EA can be told to revoke the node's enrollment credentials to prevent it from updating its enrollment certificate and thus acquiring further information ATs. Additionally, the EA revokes the validity of the enrollment certificate, and the AA does the same for the authorization tickets. As ITS nodes are expected to check the validity of certificates using Certificate Revocation Lists (CRLs) and Certificate Trust Lists (CTLs), messages of the revoked node are not accepted anymore.

*Pseudonym Change for IPv6 ITS Networking:* Section 11 of the ETSI standard on IPv6 usage over GN covers the support for pseudonyms and their change of that protocol stack. For example, binding a GVL's prefix to a distinct geographical area can threaten users' location privacy as a static interface identifier part of the IPv6 address would allow singling out a node over multiple GVL networks track their location by the GVL prefix and its associated geographical region. The proposed countermeasure is again the adoption and regular change of pseudonyms. In this case, the affected identifier is the interface identifier part of the IPv6 address.

This identifier is derived from the link-layer address, which also implies a change of the link-layer identifier address (MAC address). The same is true for the GNADDR. Thus, it also changes accordingly with the changed link-layer address. All existing IPv6 connections have to be terminated as a clear cut between the old and new pseudonym IP address has to be made to prevent correlation of the old and new pseudonym during migration.

#### *3.2.1.3Pseudonym Change Strategies*

There needs to be some ambiguity regarding which node changed to which pseudonym, there shall be other nodes present within the reception range, coordination and frequency of change matter, and all identifiers need to be changed simultaneously with buffers being flushed or discarded. The position also needs to be updated during pseudonym change to prevent re-identification through stale position coordinates included in GN packets. Finally, control metadata like sequence numbers in GN packets have to be reset as well.

The ETSI, ITS working group, gathers several concepts for pseudonym change strategies in a technical report [66]: The parameters deciding a pseudonym change (e.g., period or length) shall be ran-

domized to prevent linkability by analyzing the periodicity of changes. After changing pseudonyms, random-length silent periods shall be abided in which nodes stop sending any packages. When using a vehicle-centric strategy, pseudonym change time, its frequency, and duration of silent periods are influenced by the vehicle's mobility and trajectory to make linkage of pseudonyms based on broadcasted movement parameters harder. In the density-based approach, pseudonyms are changed only if enough other vehicles are around to avoid unnecessary unambiguous pseudonym changes.

Mix-zones are geographical areas where no messages of location-aware services are exchanged. This concept is supposed to make the linkage of in-going and outgoing vehicles from the zone difficult. These zones are especially effective in high-density and high-fluctuation areas like intersections or parking spots. Vehicles could collaboratively change pseudonyms within these zones by first announcing it via broadcast messages and then changing synchronously. However, as stated in the report, the efficiency of that approach depends heavily on the density of the situation.

A particular variant is cryptographic mix-zones: Within these zones with a size limited to the radio coverage of an RSU, no identifying data is sent in plaintext, but everything is encrypted with the same symmetric key provided by the RSU. Thus, it allows the usage of location-aware collision detection messages while preventing an outsider from eavesdropping without switching off essential safety features. An alternative to just changing from one pseudonym to the next from a node's internal storage is swapping pseudonyms randomly between nearby vehicles. We find this approach to be limited, though, by the inclusion of vehicle-specific data into messages and legal requirements demanding the possibility of an identity resolution for law enforcement.

The ETSI survey [66] also gives an overview of used strategies in existing standards or projects. These include some interesting further approaches: The *SCOOP* project proposes a timeslot-based round-robin pseudonym selection. The exciting thing about this is that using pseudonyms from the local pool is explicitly allowed as the selection mechanism ensures they are not always reused in the same order. This is a practical approach against the problem of pseudonym refill (acquiring new pseudonyms) not always being possible.

The strategy proposed by the Car-2-Car Communication Consortium is dividing each trip into at least three segments: The first one from the start of the trip to a middle segment, the middle segment being familiar to several people and unassociated to specific origins and destinations, and the last segment to the intended destination of the trip. This shall achieve that locations significant to a user can neither be linked together nor the user, thus preventing individual movement profiles. The values for changing pseudonyms have been statistically obtained with the outcome of changing pseudonyms at the beginning of a trip, then randomly after 0.8-1.5 km, and from then on randomly at least every 0.8 km or 2-6 minutes.

Some safety requirements of the ETSI standard affect pseudonym change: In critical situations when a receiving station would need to take immediate action in response to received safety information, pseudonyms have to be locked. The reason behind that is that cooperation collision avoidance depends on all vehicles broadcasting their location and trajectory. Therefore, vehicles in a silent period due to a pseudonym change would not be considered, and vehicles changing pseudonyms without a silent period could appear as duplicate or ghosting vehicles hindering collision evasion. Furthermore, recognizing such critical situations and initiating the pseudonym locking is done by the receiving ITS vehicle, which decreases the risk of an attacker trying to lock pseudonyms without a critical situation being present deliberately.

#### *3.2.1.4Further Pseudonym Scheme Techniques*

Petit et al. made an extensive survey [131] of cryptographic approaches for pseudonym schemes and defined a representative pseudonym life-cycle for comparing the different approaches.

- *Certificate-based Pseudonyms:* The ETSI standardized pseudonym scheme is one instance of the ones categorized as asymmetric cryptography schemes in that survey. The class of these schemes is characterized by asymmetric cryptography based on hierarchical certificates acquired from a PKI. This PKI must be divided into at least two different administrative and legal control domains to ensure pseudonym resolution using the retained pseudonym-to-identity escrow mapping information only happens under specific legal circumstances. Essential parameters of these kinds of pseudonym schemes are the number of available pseudonyms acquired and available at a time, their lifetime, the used way of acquiring new pseudonyms (pseudonym refill), and the number of collaborating different authorities to resolve the split information for pseudonym resolution. Some approaches covered do not require contact to an external PKI for pseudonym refill but allow pseudonym self-issuance: Armknecht et al. [24] propose the self- issuance of pseudonym certificates with the node's master keys. Verifying these pseudonyms utilizes zero-knowledge proofs and bilinear pairings, while Revocation of Certificates works via changing the cryptographic system's parameters. Calandriello et al. [43] combine the classical certificate scheme with group signature schemes (see III-C3) for pseudonym generation with individual private keys and verification with the public standard group key. When it comes to enhancing the privacy of pseudonym resolution, several approaches of further splitting and distributing identity mapping information over several authorities utilizing blind signature schemes or group signature schemes are mentioned. The IFAL protocol [170] introduces a mechanism tackling the issue of pseudonym refill: Pseudonym certificates can be distributed in significant numbers already well in advance, as they are in principle valid in the future, but only if activated with periodically distributed activation codes. Thus, even over bad connections, SMS messages, or broadcasts, the codes are not confidential but require more storage space for the unactivated certificates. We see the clear advantage of this class of schemes in the applicability to existing Vehicle-to-Everything (V2X) standards, as all significant V2X Specifications use some certificates. As mentioned by Petit et al. [131] tough these certificates have to be included in each message, and their storage and verification require considerable resources. Furthermore, the PKI system's maintenance is quite complicated regarding infrastructure requirements and legal and organizational frameworks. **Because of these disadvantaged, we now take a look at other cryptographic pseudonym schemes.**

- Identity-based Cryptographic Pseudonyms: Identity-based cryptography is a form of asymmetric cryptography where a node's identifier (i.e., network interface and proto- col address) serves as a node's public key. A private key has to be derived from that public-key-id. This is usually done by a central Trusted Authority (TA), which has additional secret parameters to prevent any node from doing this derivation. Some of the parameters are published and required for verifying message signatures. This TA can then also retain identity-mapping information but does not distribute these mappings over multiple authorities. Revocation of pseudonyms can work similarly to the classical certificate-based scheme by revoking the canonical registration identifier. The lifetime of pseudonyms can also be limited by adding a timestamp to the identifier string before deriving the private key. In theory, the Revocation of certain pseudonyms could also be done by distributing revocation lists, but this has the same scalability issues with certificates. When it comes to pseudonym change, the same strategies as for certificate-based pseudonyms apply. The network interface identifiers are equivalent to the public key, especially the strategies for changing the network identifiers are relevant. As the public key is directly derivable from the destination address of messages, a Man-in-the-Middle (MITM) relay-interception is prevented. In addition, not including the certificate in each message and the smaller number of pseudonyms reduces ITS nodes' needed storage resources.

- *Group Signature Scheme based Pseudonyms:* The idea behind group signature schemes is that all group nodes use the same shared public key for signing their messages but have individual private keys for creating these signatures. As every group member could have created the signature validated with that shared public key, all group nodes are using the same pseudonym and thus are anonymous within the anonymity set of the group. Therefore, two vehicle's messages are not linkable to each other as they are not distinguishable from two messages of different vehicles that are members of the same group.

  Groups require a setup, during which the group members are determined, and individual private keys are assigned to them by the group leader. The group manager is an entity that determines the system parameters, including the public group key, creates and assigns private keys based on them to members, and may revoke pseudonymity for specific members.

  This role could be assigned to any node of the group, but as it allows specific privileged actions, the process of group manager election needs to be concisely designed. Proposals include using RSUs as regional group managers, which gives infrastructure operators even more powerful potential tracking abilities. Pseudonyms are only changed to manage group dynamics, i.e., change of members of the group. Then the group manager generates new system parameters and issues new keys. When this happens, already mentioned strategies like silent periods may be used. However, individual network interface addresses still need to be unique per node and thus still have to change regularly like other pseudonym schemes. As an advantage of these schemes, nodes do not have to generate, issue, and store many pseudonym certificates. Revocation is more complicated in group signature schemes: As all group nodes are indistinguishable by their exposed pseudonym identifiers, it is not possible to dis- tribute revocation lists. A re-setup of the group by changing system parameters can exclude specific nodes but has a significant overhead as all group members must change their keys. A proposed solution circumvents the problem by remote-controlling the HSM to remove the keys from its memory. The keys from group signature schemes are not directly usable for public-key encryption of messages due to the special relationship of one public and multiple private keys. However, they can be used to authenticate key exchange protocols like Diffie-Hellman, which are unauthenticated by themselves.

- *Pseudonyms using Symmetric Cryptography:* There are also pseudonym schemes utilizing symmetric cryptography authentication using Message Authentication Codes. Symmetric crypto algorithms are often computationally more efficient, which would fit the requirements of near-real-time processing in VANETs. The big issue with these schemes is that the creation and verification of signatures use the same key. Thus, every node with the key for verification can also create valid signatures in the name of another node pseudonym. Thus signature verification can not be done by each node themselves. After a node gets a vehicle-ID from an EA, it creates several pseudonyms by hashing and combining with seed and counter values. These values serve as pseudonym identifiers for connecting to an RSU and jointly creating an asymmetric signature key. The RSU retains a mapping of key and pseudonym identifiers. For verification, a node has to send the message (or a hash of it, depending on the MAC scheme) and the supposed sender pseudonym to the RSU. That station then verifies the signature using the retained mapping and sends the result back to the requesting node. Thus symmetric pseudonym signature schemes heavily rely on infrastructure for signature verification and introduce additional delays due to the needed round trips. Having these issues mentioned in the survey, they are hardly usable in practice. There are some attempts to get rid of these issues. FOR EXAMPLE, the TESLA protocol [129] manages to reduce the infrastructure dependence by revealing previous signature keys using beaconing messages. However, this approach still suffers from high latency times.

### 3.2.2 Certificates Revocation

In asymmetric cryptography, it is challenging to remove certificates once issued. On the one hand, a PKI does not necessarily know all the actors who have a copy of the certificate and, on the other hand, the certificate and the public key it contains may be helpful in the future, for example, to verify a signature previously affixed to an electronic document, or to decrypt the previously encrypted content. Thus the certificates are not deleted but revoked: the information remains but is supplemented by indicating that the certificate should no longer be used to protect data. The revocation function includes the authentication of the entity requesting the Revocation and the publication of information and related material.

#### *3.2.2.1CRL publication*

When a certificate is revoked by a CA, for whatever reason (loss or theft of the private key, leaving a communication network, etc.), the CA must disseminate this revocation information to other users who no longer use it the public key. Thus, the information must, therefore, be publicly accessible at all times. The publication of the Revocation list A Certificate Revocation List (CRL) carries out this dissemination as show in Fig. 6.1.

For Revocation of node access to the ITS network, e.g., in case of misbehavior, there are multiple mechanisms: The EA can be told to revoke the node's enrollment credentials to prevent it from updating its enrollment certificate and thus acquiring further information ATs. Additionally, the EA revokes the validity of the enrollment certificate, and the AA does the same for the authorization tickets. As ITS nodes are expected to check the validity of certificates using Certificate Revocation Lists (CRLs) and Certificate Trust Lists (CTLs), messages of the revoked node are not accepted anymore.

#### *3.2.2.2Types of Certificate Revocation Lists (CRLs)*

There are several types of CRL:

- *CRL:* is the list of identifiers (serial numbers) of the revoked certificates. A list of certificates that are no longer valid and which are no longer worthy of trust. This revocation mechanism is fundamental for PKIs because it allows the certificates to be valid for a relatively long period. Furthermore, it is by Revocation that one guards against unforeseeable attacks on the keys or accidental compromises. Thus, certificates can become invalid for many reasons other than natural expiration, Such as :
  - Loss/compromise of the private key associated with the certificate.
  - Changes of fields included in the certificate holder's name, or even changes in access rights.

  Thus, in the certificate verification-chain, it is always necessary to check the expiration date, but also that the certificate is not on the very last published CRL.

- *Delta-CRL:* A major difficulty with CRLs manages frequent updates of large amounts of data because certificate revocation lists can be very long if many certificates have been revoked, and it can also take a long time to download them. We use delta-CRLs to reduce these downloads. The idea of these delta-CRLs is to reconstruct the most recent CRL from an old CRL and all newer delta-CRLs. Therefore, delta-CRL lists only the certificates whose status has changed since issuing a complete reference CRL ("base CRL"), indicated in the delta-CRL. Thus, the volume of communication necessary for the frequent propagation of CRL information is reduced to only the differences compared to the previous broadcast.

- *Indirect CRL:* In principle, CRLs are issued by issuers of CRLs. Usually, this is the CA itself, as they issue CRLs to provide revocation information on the certificates they give. However, a CA may delegate this responsibility to another trusted authority. Thus, when this CRL sender is distinct from the AC, the CRL is indirect, and the indirect CRL field in the CRL extensions must be valid.

## 3.3 Security Service Management Concerns

We highlight concerns that both certificate owners and issuers have, as explained by [124].

### 3.3.1 Concerns for certificate issuers

Certificate issuers or certification authorities (CAs) are keen to offer services to end entities as efficiently as possible and at a low cost. Here are some of their concerns.

- Delivery of certificates
- Storage of multiple attributes in a certificate and ensures the linkage between enrollment certificates and authorization tickets within a given processing time (as shown in Figure 6.1)
- Certificate revocation.

### 3.3.2 Concerns for certificate owners

A certificate owner is primarily interested in a simple process for obtaining, revoking, and using certificates. The owner (end entities or authorities) wishes to devote as few resources as possible to these operations.

The main concern of certification authorities is the cost of performing each of the operations with a certificate: issue, validation, revocation, and re-issue. These operations remain under the responsibility of the CA. As shown in Fig. 6.1 the reports of OBUs to misbehavior authority of malicious vehicles and the authorities' conducted process to the linkage of Authorization Tickets and their corresponding ECs and attributes to report them into the CRL

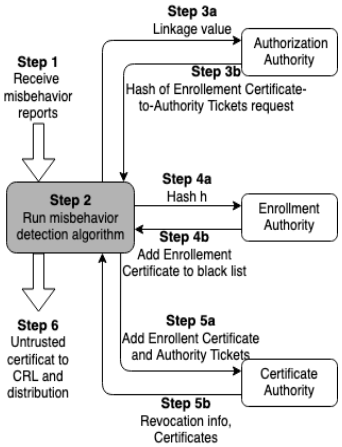



**Fig. 3.2** Reports of OBUs to misbehavior authority

## 3.4 Cyber-Physical Security Revolution

As seen in the previous section, V2X communications use the Geonetworking protocol. Geonetworking's primary specificity is to limit message dissemination in a specific geographic area. Thus, data link to a particular geographic area makes the V2X network special. Moreover, by combining space with time, we come across issues related to Cyber-Physical Systems.

### 3.4.1 V2X and IoTs similarities

For several years now, we have been in a world where the number of connected objects (also called "IoT" for "Internet Of Things") is increasing exponentially. The 5G network will then revolutionize, as we will see below, many areas. We will see the application of this new generation of networks to our connected cars of tomorrow. The communication architecture of V2X networks has certain limits preventing the deployment of all C-ITS applications. This is why a new communication paradigm, inspired by the Internet of Things, has been defined: the Internet of Vehicles (IoV). The Internet of Vehicles is based on three main principles:

- *The integration of different communication technologies:* ITS-G5 communications represent an exciting means of communication for road safety and traffic flow (latency, reliability). However, the ITS-G5 offers limited internet connectivity. Therefore, this technology does not allow the deployment of services linked to entertainment and does not guarantee optimal data processing for road safety and traffic flow applications. This is why the Internet of Vehicles offers to consider different access technologies ITS-G5, LTE-V2X, Li-FI, etc. Thus, continuous Internet access could be guaranteed;

- *The integration of vehicular networks into the Internet of Objects:* the Internet of Objects [26] must allow real-time communications, at all times, between all types of objects. Establishing connections between vehicles and objects (connected road, surveillance camera, connected watch, etc.) could make it possible to broaden the Scope of C-ITS applications. Also, the Internet of Vehicles proposes to integrate vehicular networks with the Internet of Things and Smart Cities [163];

- *Optimal data processing:* the development of ever more efficient C-ITS applications relies on optimal data processing. The guarantee of permanent Internet connectivity makes it possible to escalate information to outsourced Cloud servers and analyze large volumes of data by these servers. This could help ensure traffic flow and maximum road safety. Thus, the Internet of Vehicles offers to integrate high-performance and "intelligent" data processing solutions, such as Artificial Intelligence techniques. By integrating into the Internet of Things, considering different communication technologies, and offering efficient data processing, the Internet of Vehicles seems to represent the future of vehicular networks. Indeed, this approach makes it possible to improve the operation of existing applications (road safety, traffic flow) and develop new services (vehicle maintenance, health, entertainment). In addition, the Internet of Vehicles is opening up to new players (service providers, operators) who will participate in the development of vehicle networks. It should be noted that communications between objects (Internet of Objects) and vehicles could be based on communication technologies and types of communication (V2P, V2I, V2N) already used in vehicular networks. Other communication technologies, specific to the Internet of Things, could also be considered, in particular long-range and low-consumption networks (LPWAN Low-Power Wide-Area Network). In this case, a new type of communication could be considered (cf. Table 2.3),

Vehicle-to-Object communications (V2D, Vehicle-to-Device). Another communication technology based on visible light could be integrated into vehicular networks to offer V2V, V2I, and V2N communications.

### 3.4.2 Cyber-Physical Systems (CPS) revolution

In CPS, components are classified into physical parts, and software parts [156]. Physical components include infrastructures, network sensors, and computation devices. Software components contain programs, software operating systems, and the Internet of Things (IoT) environment.

CPS has various use cases, including ITS, smart grid, smart meters, intelligent medical systems, smart cities, etc. These use cases assist the living, improve safety, and release traffic jams. However, challenges hide in the positive impact of CPS. Significant challenges about CPS have been conducted in enhancing security and privacy, and network efficiency [109] [136]. For instance, a wireless sensor network is a well-known CPS use case. It requires a security scheme to maintain efficient secret key distribution and low energy consumption [123]. A cutting-edge CPS scenario is described in the paper [158]. The paper proposes a solution in vehicular fog-computing services (vehicular CPS). The fog-computing follows the distribution structure and distributes the heavy computation tasks to the infrastructures instead of the central manager. Paper [158] enables intelligent resource management to optimize the communication plus computing energy efficiency in order to achieve the best QoS requirement. A more applicable fog-computing-based CPS system is discussed in [28]. This paper developed a framework to optimize TCP/IP virtualized data centers, the dynamic scheduler, and the dynamic queue system are taken into consideration. The dynamic approach maximizes the average workload admitted by the data center and minimizes the resulting network-plus-computing average energy consumption. **However, both the above schemes only cover the network efficiency issue but do not consider the security and privacy vulnerabilities.**

### 3.4.3 Clustering

Usually, to get into the vehicle's system, attackers need to be within close communication range of the vehicle in order to be able to hack into it. However, nowadays, attackers have access to advanced resources and have developed professional skills to execute the hacking process over long distances. Nonetheless, the development of such technology is already becoming essential for drivers and cities and never will [145]. The V2X communication does not have a fully connected network topology because its high mobility vehicles can change networks several times in a limited time. For communication and security purposes, dynamic clustering techniques have been proposed to make these networks more stable.

The existing protocols are broadly divided into five sub-categories:

- Position-based protocols [149], [116],
- Route discovery protocols [126], [167],
- Broadcast protocols [166] ,
- Infrastructure-based protocols [128],
- Cluster-based protocols [95, 155, 104].

El Houda et al. [19] 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 [97] consider the reliability of links for clustering. However, this scheme takes fixed arrival rates for nodes on the highway, which remains unrealistic. Depending on C-V2X, some have proposed [49] using a heterogeneous network in recent years, using IEEE 802.11p and cellular communication. Next, Liu et al. [113] proposed a reliable and stable communication scheme using clustering and probabilistic diffusion. This scheme was based on multi-vehicle 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.

### 3.4.4 Sybil Attack Detection

In V2X communications, vehicles, and infrastructure continuously exchange traffic safety and navigation messages. 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. The Sybil attack is an attack that applies especially on V2X networks. Moreover, since it combines attacks on the temporal and space aspect, it is a purely cyber-physical problem. This is why it is the most studied attack in the field of vehicular communication: Authors in [186] have proposed a Sybil detection method based on received signal strength indicator (RSSI) named Voiceprint, which relies on RSSI time series as vehicular speech and performs the comparison among all received time series, unlike other RSSI methods which were based on absolute or relative distance according to RSSI values. Furthermore, to improve the observation time and decrease the false-positive rate, Voiceprint is further enhanced by allowing it to conduct detection on service-channel (SCH). Efforts have also been made to identify the malicious nodes performing power control using the change-points detection method. Advantages Voiceprint is evaluated to be effective among other RSSI-based methods in cost, complexity, and performance. Disadvantages– Proposed solution to power control is still a complicated problem when adopted with an RSSI-based detection scheme. Among the works in relation to the security of Vehicular networks, but focused on a specific issue, we quote: [175] of Bin Xiao et al. reserved for the detection and localization of Sybil attack in VANET nodes.

Ruj et al. [146] devise a data-centric misbehavior detection system (MDS) that can be used to detect false location information. The idea of the data-centric MDS concept is to classify data instead of classifying vehicles. Each vehicle can verify the location information independently by using the proposed technique. For example, an attacker sends a beacon message that includes fake location information (L1) and the time stamp it is sent (T1). After receiving a vehicle V located at L2 at time T2, V can verify if L1 is correct or false by utilizing L1, L2, speed of light, and the difference between T1 and T2. In that scenario, the attacker is not able to modify T1 in order to deceive V since it does not know the exact distance between itself and V. If the location is detected as false, V broadcasts a message to other vehicles and the CA through the nearest RSU. This leads to fines imposed on attackers instead of isolating them from the network. The authors compared the proposed scheme with existing MDSs regarding communication overhead; however, it is not supported with simulations.

Sowattana et al. [161] propose a distributed consensus-based algorithm to detect Sybil nodes in VANETs using the neighborhood information. Each neighbor's received information will be used to vote on each of the receiver nodes' neighbors, whether they are Sybil. Yang et al. [184] proposed a Sybil detection scheme based on mobility similarities among vehicles by using three ML classification models, namely, naive Bayes classifier, SVM, and decision tree.

### 3.4.5 Trade-off between Road-safety and cyber security

There is a real challenge in the trade-off between road safety and cybersecurity. Full message encryption does not meet temporary road safety requirements. As shown in figure 6.2, the message linked to crash information must be accepted before the event to avoid a crash. Additional latency on message validation can therefore harm people's lives. In the context of revocation policies to remove misbehaving nodes from the network, this can only be achieved when the pseudonym scheme used supports the resolution of participants' long-term identities from their pseudonyms. In this case, information about the revocation of long-term vehicle identification information is disseminated to other participants through CRLs or other means. However, in addition to being computationally intensive (i.e., using CRL also assumes improved connectivity so that all vehicles can periodically retrieve all updated lists, this is detrimental to the protection of their privacy. Overall, although several PKI proposals address the need for pseudonym revocation, there has been no consensus on which method could effectively address this issue. Indeed, there is a trade-off between vulnerability and cost, particularly related to the size of certificate revocation lists.

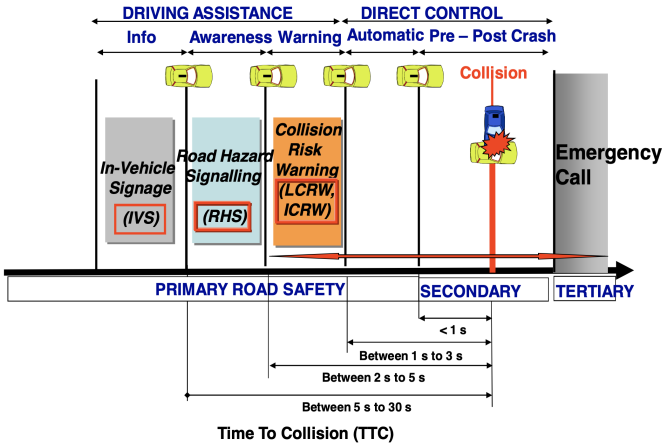



**Fig. 3.3** Applications being served by transmission showing the time to collision [69]

## 3.5 Getting Blockchain Technology more involved

### 3.5.1 Introduction

The current PKI system poses a fundamental problem of certificate revocation, particularly with the distribution of pools of AT certificates. The authority finds it difficult to detect malicious behavior from vehicles and does not have many tools to supervise hundreds/thousands of vehicles. It then becomes essential to involve the vehicles to denounce each other. So even with the individual IDS systems proposed in the literature, the CA cannot revoke a vehicle based on the investigation result of a single-vehicle. However, the revocation process can then take a long time. Add the latency that the canonical data revocation can take at the EA level and make the link with the AA to revoke its AT pool. Therefore, it is essential to integrate decentralized systems to integrate vehicles in the revocation process, it is a collaborative work, but these mechanisms must be governed by a definite codification (consensus). The most popular decentralized technology to use is Blockchain.

### 3.5.2 Toword Decentralized Systems

Blockchain cryptography was originally introduced to resolve the challenges of implementing multiple access networks through various nodes [133]. To ensure the security of the nodes and to be precise on how consensus is reached for a transaction validation per each network and corresponding Blockchain, *smart contracts* were developed and introduced by Ethereum [174]. These smart contracts include rules and requirements as well their enforcement, all in the form of software.

#### *3.5.2.1Blockchain Properties*

A blockchain exhibits several properties that make it a suitable candidate for several application domains. The properties are discussed below.

- *Distributed consensus on the chain state:* One of the crucial properties of any blockchain is its ability to achieve a distributed consensus on the chain's state without being reliant on any trusted third party. This opens up the door of opportunities to build and utilize a system where states and interactions are verifiable by the miners in public blockchain systems or by the authorized entities in private blockchain systems.

- *Immutability and irreversibility of chain state:* Achieving a distributed consensus with the participation of many nodes ensures that the chain state becomes practically immutable and irreversible after a certain period. This also applies to smart- contracts and hence enabling the deployment and execution of immutable computer programs.

- Data (transaction) persistence: Data in a blockchain is stored in a distributed fashion, ensuring data persistence as long as there are participating nodes in the P2P network.

- *Data provenance:* The data storage process in any blockchain is facilitated using a mechanism called the transaction. Every transaction needs to be digitally signed using public-key cryptography, which ensures the authenticity of the data source. Combining this with the Immutability and irreversibility, Blockchain provides a vital non-repudiation instrument for any data in the Blockchain. Distributed data control: A blockchain ensures that data stored in the chain or retrieved from the chain can be carried out in a distributed manner that exhibits no single point of failure.

- *Accountability and transparency:* A blockchain promotes accountability and transparency since an authorized entity can verify the chain's state and every interaction among participating entities.

#### *3.5.2.2Blockchain Layers*

There are several components in a blockchain system whose functionalities range from collecting transactions, propagating blocks, mining, achieving consensus, maintaining the ledger for its underlying cryptocurrencies, etc. These components can be grouped according to their functionalities using layers similar to the well-known TCP/IP layer. There have been a few suggestions to design a blockchain system using a layered approach [**?** ]. The motivation is that a layered design will be much more modular and easier to maintain. For example, if a bug is found in a component of a layer in a blockchain system, it will only affect the functionalities of that corresponding layer while other layers remain unaffected. For example, David et al. [176] suggest four layers: consensus, mining, propagation, and semantic. However, we believe that the proposed layers do not reflect the proper grouping of functionalities. For example, consensus and mining should be part of the same layer, as mining can be considered inherent in achieving

consensus. In addition to this, some blockchain systems might not have any mining algorithms associated with them. Therefore, we will define four layers: network, consensus, application, and meta-application.

- *Meta-Application Layer:* The functionalities of the meta-application layer in a blockchain system is to provide an overlay on top of the application layer to exploit the semantic interpretation of a blockchain system for other purposes in other applications domains. For example, Bitcoin has been experimented to adopt in multiple application domains, such as DNS like decentralized naming system (Namecoin [12]), decentralized immutable timestamped hashed record (Proof of Existence), and decentralized PKI (Public Key Infrastructure).

- *The application layer :* defines the semantic interpretation of a blockchain system. An example of a semantic interpretation would be defining a crypto-currency and then setting up protocols for exchanging such a currency between different entities. Another example is establishing protocols to maintain a state machine embodying programming capabilities within the Blockchain, which can be exploited to create and deploy immutable code (the so-called smart contract). The application also defines the rewarding mechanism, if any, in the blockchain system.

- *The consensus layer:* is responsible for providing the distributed consensus mechanism in the Blockchain that essentially governs the order of the blocks. A critical component of this layer is the proof protocol (e.g., proof of work and proof of stake) used to verify every block, which ultimately is used to achieve the required consensus in the system.

- *Network Layer:* The components in the network layer are responsible for handling network functionalities, including joining in the underlying P2P network, remaining in the network by following the underlying networking protocol, disseminating the current state of the Blockchain to newly joined nodes, propagating and receiving transactions and blocks and so on.

#### *3.5.2.3Types of Blockchain*

Depending on the application domains, different blockchain deployment strategies can be pursued. Based on these strategies, there are predominantly two types of blockchains, namely Public and Private Blockchain [190], as discussed below:

*Public Blockchain*: A public blockchain, also known as the Unpermissioned or permissionless Blockchain, allows anyone to participate in the Blockchain to create and validate blocks and modify the chain state by storing and updating data through transactions among participating entities. This means that the blockchain state and its transactions and the data stored are transparent and accessible to everyone. However, this raises privacy concerns for particular scenarios where the privacy of such data needs to be preserved.

*Consortium Blockchain*: Only a single organism and the nodes belonging to it have the right to participate in the consensus. It is therefore considered to be a Partially decentralized blockchain.

*Private Blockchain*: A private blockchain, also known as the Permissioned Blockchain, has a restrictive notion compared to its public counterpart in that only authorized and trusted entities can participate in the activities within the Blockchain. However, by allowing only authorized entities to participate in activities within the Blockchain, a private blockchain can ensure the privacy of chain data, which might be desirable in some use- cases.

#### 3.5.2.4Consensus and Smart contracts

In the applications of Blockchain, we need to solve two problems- double-spending and Byzantine Generals Problem [108]. A double-spending problem means reusing the currency in two transactions at the same time. The traditional currency is the entity, so we will not face double-spending while using traditional currency. We can also solve the double-spending problem in Internet transactions with centralized trusted institutions. Blockchain solves this problem with the method of verifying the transactions by many distributed nodes together. Byzantine Generals Problem is the problem in the distributed system. The data can be delivered between different nodes through peer-to-peer communications. However, some nodes may be maliciously attacked, which will lead to changes in communication contents. Normal nodes need to distinguish the information that has been tampered with and obtain consistent results with other normal nodes. This also needs the design of the corresponding consensus algorithm. The consensus algorithm has been studied for many years in a distributed system. There are some transplantable consensus algorithms applied in Blockchain. We make a detailed description of the principles of these consensus algorithms in this section.

- *PoW (Proof of Work):*PoW is the consensus algorithm used in bitcoin. Its core idea is to allocate the accounting rights and rewards through the hashing power competition among the nodes. Based on the previous block's information, the different nodes calculate the specific solution of a mathematical problem. It is challenging to solve math problems. The first node that solves this math problem can create the next block and get a particular bitcoin reward. Satoshi Nakamoto used HashCash to design this mathematics problem in bitcoin [29]. The specific calculation steps are as follows:

  - Get the difficulty: After the production of every 2016 block, the bitcoin mining algorithm will dynamically adjust the difficulty value according to the hash rate of the whole network.
  - Collect transactions: Collect all pending transactions on the network after the production of the last block. Then calculate the Merkle Root of these transactions and fill in the block version number, the 256-bit hash value of the previous block, the current target hash value, Nonce random number, and other information.
  - Calculating: Traverse the Nonce from 0 to 232 and calculate the double SHA256 hash value in step 2. The block can be broadcasted if the hash value is less than or equal to the target value. Then, the node completes accounting After the verification of other nodes.
  - Restarting: If the node cannot work out the hash value at a particular time, it repeats step two. However, if any other node completes the calculation, then it restarts from step 1.

  PoW takes the workload as the safeguard. The newly created block is linked to the blocks in front of it. The length of the chain is proportional to the amount of workload. All nodes trust the longest chain. If anyone wants to tamper with the Blockchain, he needs to control more than 50% of the world's hashing power to ensure that he can become the first one to generate the latest block and master the longest chain. The gains from tampering can be much more significant than the cost. So the PoW can effectively guarantee the safety of the Blockchain.

- PoS(Proof of Stake): PoS was mentioned in the first bitcoin project, but it was not used for robustness and other reasons. The earliest application of PoS is PPCoin [100]. In PoS, the digital currency has the concept of Coinage. The Coinage of a coin is its value multiplied by the period after it was created. The more extended one node holds the coins, the more rights it can get in the network. Holders of the coins will also receive a particular reward according to the Coinage. In

the design of PPCoin, mining is also needed to get the accounting rights. The Proofhash is a composed hash value of the weight factor, the unspent output value, and the fuzzy sum of the current time. PoS limits the hashing power of each node. Therefore, the difficulty of mining is inversely proportional to Coinage. PoS encourages the coins holders to increase the holding time. With the concept of Coinage, the Blockchain is no longer entirely relying on proof of work. That effectively solves the resource-wasting problem in PoW. Furthermore, the security of the Blockchain using PoS improves with the increasing value in the Blockchain. The attackers need to accumulate many coins and hold them long enough to attack the Blockchain. This also dramatically increases the difficulty of the attack. Besides the PPCoin, many other coins use PoS, such as the Nxt [13]. However, they consider the rights of the nodes and use a random algorithm to allocate accounting rights.

- *DPoS(Delegated Proof of Stake)*: In the initial design stage of bitcoin, Satoshi Nakamoto hoped that all the participants could use the CPU to mine. So the hashing power can match the nodes, and each node can participate in the decision-making of the Blockchain. With the development of technology and the appreciation of bitcoin, machines specially designed for mining are invented. The hashing power is grouped in the participants that have large numbers of mining machines. The ordinary miners rarely have the opportunity to create a block. BitShares is an example of DPoS [2]. In the Blockchain with DPoS, each node can select the witnesses based on its stake. The top N witnesses who participated in the campaign and got the most votes have the accounting right in the whole network. The number N of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization. The elected witnesses create new blocks one by one as assigned and get some rewards. The witnesses need to ensure adequate online time. If a witness is unable to create its assigned block, the activity of that block will be moved to the next block, and the stakeholders will vote for a new witness to replace it. The Blockchain using DPoS is more efficient and power-saving than PoW and PoS.

- *PBFT(Practical Byzantine Fault Tolerance)* In distributed systems, Byzantine Fault Tolerance can be an excellent method to solve transmission errors. However, the early Byzantine system requires exponential operations. Therefore, until 1999, the PBFT(Practical Byzantine Fault Tolerance) system [46] was proposed, and the algorithm complexity was reduced to a polynomial level, which significantly improved efficiency. The process of PBFT is shown in figure It consists of five states:
  - Request: The client sends a request to the master server node, the master node gives the request timestamp.
  - Pre-prepare: The master server node records the request message and gives it an order number. Then the master node broadcasts a pre-prepared message to the other following server nodes. Thus, the other server nodes initially determine whether to accept the request or not.
  - Prepare: If a server node accepts the request, it broadcasts a prepared message to all the other server nodes and receives the prepared messages from the other nodes. After having collected 2f+1 messages, if most nodes choose to accept the request, it will enter the commit state.
  - Commit: Each node in the commit state sends a commit message to all the other nodes in the server. At the same time, if a server node receives 2f+1 commit messages, it could believe that most nodes reach a consensus to accept the request. Then the node executes the instructions in the request message.
  - Reply: the server nodes reply to the client. If the client does not reply because of the network delay, the request is resent to the server nodes. If the request has been executed, the server nodes only need to send the reply message repeatedly.

- Raft : After the Byzantine Generals Problem was raised, Lamport proposed the Paxos algorithm to solve the consistency problem in certain conditions in 1990. However, because the content of the paper is difficult to understand, it was not accepted. Lamport republished the paper [106] in 1998, and the Paxos was briefly reintroduced in 2001[ 20]. Then Paxos occupies the dominant position in the field of consistency algorithm. Many other algorithms are derived from it. Nevertheless, the Paxos algorithm is too theoretical. The people have great difficulty in understanding it and engineering implementation. In 2013, Standford's Ongaro and others published the paper and proposed the Raft algorithm [107]. Raft achieves the same effect as Paxos and is more convenient in engineering implementation and understanding. The Raft cluster generally contains five server nodes. Up to two nodes are allowed to crash at the same time. The server node has three states: leader, follower, and candidate. There is only one leader in a term, and the leader is responsible for handling all clients' requests.

### 3.5.3 Blockchain-Based PKI

To help resolve PKI security weaknesses, researchers proposed integrating BC into PKI's architecture. Contributions are divided into two major solutions:

– Complementary solution that improves the security of the centralized system.

– Solution that entirely replaces the PKI system.

The Blockchain as a world of research can bring together the computer Science, ITs, and economic aspects. Allows the resolution of some problems prevalent in cyber security. Many solutions turned to find a complementary solution to fill the PKI's lack. In many issues, the decentralized aspect is practical, given its ability to put the power of the whole network to the benefit of general security. The solution came to integrate the Blockchain in the PKI. since then. The Blockchain has been used in several use cases. Two types of solution are distinguished: Blockchain is used whether to help the centralized solution to be better secured, it is used in authentication privacy [27] using the Blockchain to remove the traceability of the identity in the public keys declarations, also in DNS management using Blockchain to avoid internet attacks like DDoS [91]. As for [55], it proposes a decentralized Blockchain framework centrally managed by PKI. The Blockchain can also be an excellent solution to revoke certificates [180]. Also, other research aims to completely replace the centralized architecture as using completely decentralized infrastructure using the key management and Smart Contracts and seeks to replace the PKI system [94] [179]

### 3.5.4 Blockchain for IoTs

Decentralization is introduced in several domains. In [15] it proposes a Decentralized storage service, using a proof of retrievability consensus to encourage proper maintenance of the outsourced files. Storj employs end-to-end encryption and stores cryptographic digests of files on the Blockchain to tie up storage rental connections and enable file integrity check (used a searchable symmetric encryption technic) [40]. It also uses a Smart Contract for space rental for miners. The Blockchain can be optimized every day using specific mechanisms. In [56], the authors propose a new Smart Contract-based method using the Ethereum platform in order to create a Smart Contract between vehicles owners and service providers. It proposes an optimized Blockchain method for IoT called the Lightweight Scalable Blockchain (LSB), and give solutions for the safe use of the cloud concerning privacy and confidentiality.

### 3.5.5 Blockchain for V2X

With the very high mobility and frequent changes within the V2X network, even BC-based security architectures are vulnerable to attacks. However, the V2X network has a unique cyber-physical aspect. The combination of time and space characterizes this network very well and maybe exploited to resolve these challenges.

Blockchain is one of the most popular decentralized technologies used in the domain of IoT. Also, for V2X communications, this work [188], authors introduced the Blockchain-based ecosystem for V2X communications, naming the stack layers changes. In [44], the authors are focused their work to prevent from attacks that may affect the platooning application topology. Therefore, they propose a solution with Blockchain that uses smart contracts to control the validation and the access of other vehicles on the platooning. In [118], the authors propose the Blockchain as a backup to the centralized architecture and to help authorities on their security processes, like the law enforcement authority (LEA). The Blockchain platform is used to record the pairs of public keys and real identity in case of disputes; all the messages are recorded in Blockchain as persistent evidence for LEA to evaluate the reputation score for each vehicle. This Blockchain platform is used mainly for: system initialization, certificate update, and public key revocation. In [183], a Blockchain method is proposed to evaluate the credibility of other vehicles messages and upload it to the infrastructure (RSU), a block is then created using the proof-of-stake and proof-of-work consensus. In [110], there is a solution for heterogeneous networks, where the authors propose a standard Blockchain between security managers to facilitate key management for the car's handover between a security manager and another.

## 3.6 Conclusion

In this chapter, we have described in Section 3.2 the different mechanisms that allow authorities to ensure security within V2X networks. However, the biggest challenge is to be able to apply these mechanisms. We have seen that with a purely centralized architecture, this is not possible.

We, therefore, demonstrated the similarities that exist between V2X networks and IoTs Section. 3.4.1 and the revolution of Cyber-physical systems Section. 3.4, This shows vehicles on the microscopic scale communicating in a decentralized manner which allowed integrating them into overall security. Finally we gave examples of some cybersecurity contributions for cyber-physical systems.

CHAPTER 4

# TileChain : A New Geographic Blockchain Architecture For V2X Communications

## 4.1 Introduction

Nowadays, the automotive industry continues to grow to allow everyone to travel comfortably. Unfortunately, this raises concerns for governments that typically do not have sufficient finances to build new roads and sustain the ever-growing automotive industry. Therefore, governments are looking for new ways to improve road traffic management, such as intelligent mobility and dynamic regulation, to cope with road mobility problems. Besides this, manufacturers are trying to contribute to this process by developing new technologies such as driver assistance and wireless vehicular communications (V2X), which help drivers better control their vehicles and become more aware of their environment. Therefore, it is mandatory to secure these wireless communications to ensure that all technologies meet security requirements. Security should be especially considered in connected autonomous vehicles, where a vulnerable system component can be exploited to cause dangerous consequences, such as injuries or even loss of life. For these reasons, several types of security architectures related to V2X have been proposed. The current V2X security architecture is based on a centralized architecture where all vehicles are identified, authenticated, authorized, and connected via central cloud servers that use a Public Key Infrastructure (PKI).

This chapter aims to propose a new decentralized architecture based on Blockchain technology to guard off from cyberattacks and demonstrate the importance to integrate vehicles in the cybersecurity process.

÷

## 4.2 Motivation

With the development of vehicle fleets, vehicular communications have become essential for functional and road safety purposes. However, as a side effect, these communications make vehicles more vulnerable to cyber-attacks. Moreover, the security of data exchanges depends on a central authority. Therefore, the centralized architecture's significant stake is to maintain efficient security service management for the various security services (e.g., authentication, confidentiality, non-repudiation, real-time misbehavior detection, and security certificate management and revocation), which could be challenging and costly for the authorities and may even weaken the network's overall security. For these reasons, there is a need to find a complementary solution that would use a decentralized security framework to help the authorities better manage their network security by involving each vehicle in the overall security management.

## 4.3 Existing solutions

### 4.3.1 Geographical data processing

The GeoNet protocol requires the redirection of all messages to a control center. Depending on the geographic destination address, this control center is then responsible for individually distributing each message. Therefore, this approach involves a significant consumption of resources (computation, bandwidth) and a latency linked to the delays required to manage each message. The Software Defined Network (SDN) approach appears, by its nature, to provide an answer to this identified limitation for the GeoNet protocol. Indeed, SDN technology allows the control plane to deploy flow rules at the network equipment level dynamically. Therefore, it is possible to deploy flow rules corresponding to each of the geographic distribution areas. Thus, with SDN technology, base stations can autonomously manage the information transmitted by vehicles. Depending on the destination address, they transmit data directly to the destination base stations without intervention from the control center or the SDN controller. Various works, such as [52, 114, 147], have already focused on processing geographic data based on a software approach and not on a control center. In particular, they demonstrated that an approach based on SDN technology could lead to gains of nearly 50% in terms of latency and nearly 60% in terms of bandwidth usage. They also pointed out that eliminating the control center could reduce the additional cost of controlling geographical distribution by almost 80%. Thus, the SDN approach, limiting the intervention of the control center, makes it possible to guarantee better performance in terms of data processing.

### 4.3.2 Data distribution

The main limitation of the GeoNet protocol for data distribution lies in the inflexibility of the approach adopted. The data is systematically transmitted to all base stations located in a given geographical area (broadcast). The presence or absence of recipients connected to these base stations is not taken into account. Likewise, the load level of these base stations is not considered, whereas, for specific C-ITS applications, the distribution area could be a variable dimension. Also, the GeoNet protocol could cause an unnecessary increase in network load and degradation of performance. This is why various works have already studied the possibility of defining a software approach to geographically distributing data [57]. This work has focused more particularly on selecting the destination base stations according to the position of the vehicles (multicast). Thus, using the information fed back by the base stations, the SDN controller determines where the vehicles are currently located and which base stations must be served. It then builds a multicast tree guaranteeing efficient data dissemination. Finally, it deploys the flow rules to ensure these communications at the network equipment level. Depending on the solution's objective, energy efficiency [90], or minimum latency [177], different methods were considered for the construction of the multicast trees. Nevertheless, all of this work has shown that using a software approach could allow a significant performance improvement. More efficient use of bandwidth and reduced latency and packet loss rate could thus be measured. These advantages are notably enabled by the centralized vision of the SDN controller and the dynamic deployment of flow rules.

A first approach [18] consists of pre-calculating flow rules as a function of the mobility prediction of the terminal equipment. Thus, for each terminal equipment, the mobility prediction tool calculates the upcoming positions, and the SDN controller determines the flow rules that will be necessary. Thus, this approach reduces the response time of the SDN controller [30]. Indeed, the flow rules having already been pre-calculated. When an SDN controller receives a packet request, it simply has to deploy these rules at the network equipment level. However, this approach does not reduce the number of packets requests sent to the SDN controller.

This is why a second solution consists of pre-calculating and pre-deploying the flow rules to ensure the continuity of communications [137]. Thus, in this work, for each terminal device, the mobility prediction tool calculates, first of all, the upcoming positions. Then, the SDN controller determines the flow rules that will be necessary and pre-deploys them at the network equipment level (routers, base stations). Thanks to this approach, communication continuity can generally be ensured without the intervention of the SDN controller (see Appendix F.). Indeed, with the flow rules being already deployed, the base station can manage the communications of the terminal equipment without sending packet requests. Thus, this approach makes it possible to limit the use of the control channel.

### 4.3.3 Blockchain-based decentralized data management

Blockchain has been given increasing attention for decentralized data management. For example, [42] presented an encrypted decentralized storage system based on blockchain techniques to handle the fraudulent behaviors of clients. In this system, meaningful information about the stored files, e.g., the digests, tokens, and metadata of integrity checking, is stored in the Blockchain, which provides fair judgments for storage and search services. Moreover, in [41], the authors designed a blockchain-based distributed storage and keyword search platform. In this paper, the blockchain stores the public keys of well-behaved nodes, which are confirmed by most of the network. Therefore, due to decentralization, consistency, and tamper-proofing features, Blockchain can be a promising technique to help cope with vehicular network trust management problems.

### 4.3.4 Security Blockchain-Based solution for CPS

Existing security management systems will not reliably cope with increasing numbers of connected vehicles, especially when revoking misbehaving vehicle certificates and detecting unreliable messages and position spoofing attacks. Besides, cloud servers will remain a bottleneck and a single point of failure that could disrupt the entire network. Therefore, there is a need for a single homogeneous security solution to handle the diverse and heterogeneous V2X environments, which can replace or complement the traditional PKI system. However, due to the large and dynamic V2X environment, it is difficult for Cooperative-ITS (C-ITS) authorities to assess the credibility of messages [178]. Above all, it is most challenging to deal with dynamic and heterogeneous devices (e.g., different types of equipment and security managers [110]).

Indeed, for this reason, it is crucial to make OBUs operate in a decentralized network topology, where each OBU could participate in network security by reporting misbehaviors of other vehicles in real-time [54]. Hence, Blockchain (BC) technology became an attractive potential solution thanks to its decentralized aspect and its ability to harness the entire network's power to benefit general security. BitCoin [125] is BC's most widely known application. BC also guarantees non-repudiation and the integrity of transactions and messages, which is very important for V2X's security. The ITS components from the V2X ecosystem that could be considered as participating nodes in our BC-based architecture are shown in Figure **??**: Root Certificate Authority (RCA), road operators, service providers, On-Board Units (OBUs), Road Side Units (RSUs), and all other ITS-Stations (ITS-S) related to road traffic.

However, the decentralized solutions currently proposed for V2X [118] have to deal with large-scale networks. The computation time of these solutions will enormously increase since every participant has to agree on all the transactions of the other nodes [47]. As we can have many of OBUs communicating in a large-scale network, it is clear that the real challenge of BC-based solutions to V2X networks would be scalability.

### 4.3.5 Proof of Location consensus

Although the Blockchain has been used a lot recently for its efficiency and response to several issues linked to decentralization, it also has weak points that can make it vulnerable to several attacks. Its strong point, which is the consensus, can also be its Achilles heel if we omit vulnerabilities. Therefore, it must be adapted to system constraints. In order to adapt solutions to the constraints of V2X network topology, the Proof of Location (PoL) consensus has been used [36].

Proof of location is a digital certificate that attests to someone's presence at a specific geographic location at a particular time. [37] The decentralized nature of peer-to-peer systems guarantees higher privacy levels, as it removes the central authority from knowing both the geographic location of users and the information they exchange. The Blockchain is used to store proofs of location. Here are some examples of PoL requirements: Every request or response has to be signed by a sender's private key so that the other can check its integrity using the public key; The Proof of location check could be done based on System's Physical layer technics. The distance between the witness location and the received request's location does not exceed the communication range.

## 4.4 Cyber-Physical Blockchain Architecture for Electronic Toll Collection security

### 4.4.1 Introduction

The IEEE 802.11p amendment to the IEEE 802.11 standard enables vehicular wireless communication (V2X) and serves as the basis for the Dedicated Short-Range Communication (DSRC) in the U.S. and the ITS-G5 technology in Europe. It specifies and requires suitable communication for rapid spatial mobility (up to 130 km / h) and operates in the 5.9 GHz frequency band with a reserved bandwidth of 70 MHz. Governments are leveraging these technologies to develop cooperative Intelligent Transportation Systems (ITS or C-ITS), whose primary objective is to improve road safety and comfort through rapid secure communication between on-board units (OBUs) in the vehicles and roadside units (RSUs) in traffic control system infrastructure. As an example, the DIR Nord (Directection Interdepartementale de Route du Nord: a motorway operator for northern roads in France) in collaboration with the DGITM (Ministere de Transition: Transportation Department of France's Government) are working on implementing ITS in two large-scale projects called InterCor and SCoop@F [10][14] and others to improve road safety.

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

One such application with high risk is electronic toll collection (ETC). ETC involves transactions between service providers, via toll stations, and drivers. As these transactions involve personal account and money-related data as well as position and speed, ETC regions may be targeted for identity and/or location spoofing-based attacks such as Sybil and DDoS [59]. Such attacks could constitute a danger for the personal information of the users as well as for the traffic flow itself.

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

attempting to be involved in the ETC system.

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

### 4.4.2 Proof of Location

| Abbreviations | meaning |
|---|---|
| $P_r$ and $P_t$ (dBm) | Powers at the receiving and transmitting antennas, respectively |
| $G_r$ and $G_t$ (dBi) | Gains of the receiving and transmitting antennas, respectively |
| $L_M$, $L_t$, $L_r$ (dB) | constitute all the losses in the Link Budget equation (4.3), are respectively miscellaneous losses, transmitter losses and receiver losses |
| $Hd_r$ and $Hd_t$ (°) | Headings/ directions of receiving and transmitting vehicles, respectively |
| $Pos_w$ and $Pos_p$ | Latitude and longitude coordinates of Witness' and Prover's positions, respectively |
| d (Km) | is distance between the vehicles |
| $t_w$, $t_p$ (s) | Time stamps of the Witness and Prover, respectively |
| $Cer_p$, $Cer_w$ | The Prover's and Witness' certificates, respectively |
| $S_p$, $S_w$ (Km/h) | The Prover's and Witness' signatures, respectively |
| $Kp_p$, $Acc$ | The Prover's public key and the PoL accuracy |

**Table 4.1** Abbreviations

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

For the execution of smart contracts we use the Proof of Location (PoL) process. This is the evidence obtained by other RSUs or OBUs in the neighbors (Witnesses) to prove that a node is actually in the position in which it claims to be. For a PoL, only the radio wave metric is taken into account in our solution, but other algorithms can be used to have more precision in the detection of vehicles, such as those which take into account vehicle sensors [35].

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

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

$$PoLreq = (Cer_p, Pos_p, t_p, S_p[Pos_p]) \tag{4.1}$$

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

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

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

#### *4.4.2.1Radio wave propagation theory*

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

$$\frac{P_r}{P_t} = G_r G_t \left(\frac{\lambda}{4\pi d}\right)^2 \tag{4.2}$$

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

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

$$P_r = P_t + G_t + G_r - L_t - L_r - L_{FS} - L_M \tag{4.3}$$

#### *4.4.2.2Distance estimation*

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

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

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

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

$$N = \frac{3600R}{|Sd_w - Sd_p|} \tag{4.4}$$

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

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

From the list of $N$ beacons, the Witness extracts the following data sequence $Sq$. The subscripts $w/p$

for data variables correspond to the Witness ($w$) and the Prover ($p$):

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

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

- Indicator 1 ($I1$): We calculate the average speed and calculate distance traveled from it to compare with the distance between the coordinates from the first and last collected beacons.
- Indicator 2 ($I2$): We calculate the distance traveled of a message from the sender to the receiving vehicle from the power received using the Friis equation (5.1) and the Budget link formula (4.3). Then, we compare the result with the distance between the Witness and Prover (via their positions).
- Indicator 3 ($I3$): This indicator represents the communication quality conditions between the Witness and the Prover. It takes into account the information of the two communicators to give a value for the judgment accuracy of the Witness (i.e., how well they can verify the signal strength and distance of the Prover). We calculate it based on their velocities, headings, and yaw rates (though weather can also be considered). Relative velocity greatly impacts the accuracy of the RSSI measurements due to the Doppler effect and heading/yaw rate provides insights with respect to line of sight.

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

$$PoL_{Rate} = \frac{I_1 + I_2}{2} \tag{4.5}$$

$$PoL_{Acc} = I_3 \tag{4.6}$$

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

$$\begin{aligned} PoL = (PoL_{Acc}, PoL_{rate}, Pos_p, t_w, Cer_w, \\ S_w[PoLreq, t_w, Kp_p]) \end{aligned} \tag{4.7}$$

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

As mentioned, we use a consortium blockchain where the RSUs accumulate the various PoLs corresponding to a single vehicle (say, Alpha) to permit it into the tolling blockchain network. To do this, the RSU will compute a global averaged $PoL_{Rate}$ for a vehicle using the Equation 4.8:

$$\bar{PoL}_{Rate} = \frac{\sum_{i=1}^{n} PoL_{Acc(i)} PoL_{Rate(i)}}{\sum_{i=1}^{n} PoL_{Acc(i)}} \tag{4.8}$$

Then, the vehicle will be validated if its overall PoL rate exceeds some average threshold that will be continously adapted to the environmental and historical circumstances. After the verification of PoL by all RSUs, a mined block by one of these RSUs will correspond to an addition of a new element to the blockchain. Afterwards, the tolling system can carry out a quick check of the last block (the most up to

**Algorithm 1:** Proof of Location Process

**Input:** $Pos_{w/p}$; $P_r$; $Hd_{w/p}$; $Sp_{w/p}$;$N$
**Output:** $PoL_{Rate}$; $PoL_{Acc}$
**Function** `Indicator1` ($t_p[]$,$Sp_p[]$,$Pos_p[]$,$N$) **:**
  **foreach** $i \in N-1$ **do**
    $dis \longleftarrow distance(Pos_p(i), Pos_p(i+1))$;
    $dis' \longleftarrow Ave(Sp_p(i), Sp_p(i+1)) * \Delta(t_p(i), t_p(i+1)) : I_1 \longleftarrow I_1 + |dis - dis'|$;
  **end**
**return** $\frac{I_1}{N-1}$;
**End Function**
**Function** `Indicator2` ($P_r[]$,$Pos_{(w/p)}[]$) **:**
  $G_t = G_r \longleftarrow 5$
  $P_t \longleftarrow 23$ ▷ normalized transmission power
  **foreach** $i \in N$ **do**
    $D_R = distance(Pos_p, Pos_w)$ ▷ the real distance
    $D_E$ ▷ the Estimated distance using equation 5.1 and 4.3
    $I_2 \longleftarrow I_2 + \frac{|D_R - D_E|}{D_R}$;
  **end**
  **return** $\frac{I_2}{N}$;
**End Function**
**Function** `Indicator3` ($Sp_{w/p}$,$Hd_{w/p}$,$YR_{w/p}$) **:**
  **foreach** $i \in N$ **do**
    $Vel \longleftarrow \frac{|Sp_w - Sp_p|}{Max(Sp)}$
    $\delta Hd \longleftarrow \frac{|Hd_w - Hd_p|}{Max(Hd)}$
    $\delta YR \longleftarrow \frac{\left|YR_w - YR'_p\right|}{Max(Hd)}$
    $I_3 \longleftarrow I_3 + \frac{2.Vel + \delta YR + \delta Hd}{4}$;
  **end**
  **return** $\frac{I_3}{N}$;
**End Function**
$PoL_{Rate}$ ▷ Calculating the PoL rate using 5.4 $PoL_{Acc}$ ▷ Calculating the PoL Accuracy using 4.6

date) to check if the node has been authenticated and admitted into the blockchain system. The payment hash will also be listed in the blockchain.

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

**Table 4.2** Block composition

#### *4.4.2.3Properties*

Our solution may guarantee the following security properties:

- *Confidentiality:* Our solution ensures confidentiality since the payment transactions are listed in the blocks. These are not returned to the vehicles.
- *Availability:* With this solution, DoS attacks can be detected and reassembled
- *Integrity:* This solution adds the spatio-temporal aspect of the physical location which helps to prevent attacks with modified or replayed toll requests messages. This solution also avoids the Sybil attack because it allows us to link each identity with each location and it makes it extremely challenging for a single user to imitate several devices in a distributed network.
- *Non-repudiation:* Because blockchain keeps track of transaction history, no device can deny that a transaction had or had not occurred. Thus blockchain naturally ensures non-repudiation. This is a crucial security requirement for finance-related applications such as tolling, and especially for ETC over the highly distributed V2X environment.

### 4.4.3 Proposed Security Solution

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

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

#### *4.4.3.1Network Setup*

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

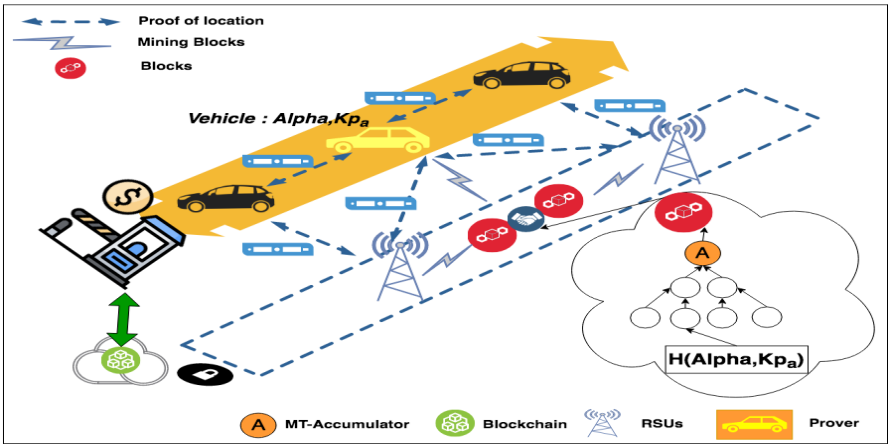



**Fig. 4.1** Witness process

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

The asynchronous Merkle tree accumulator explained in [142] effectively stores a list of all the public key of accepted vehicles in the network. Each individually mined block contains a Merkel tree (an efficient data structure) made up of all the acceptable vehicle's public keys, as described in Table 4.6.1.3. Additionally, in a Merkel tree, every leaf node is labelled with the cryptographic hash of a data block.

## 4.5 Tiling

The Tiling algorithm aims to divide the vehicles' tracks (roads, highways, etc.) into smaller sections (as shown in Figure 4.2), named Tiles. Each Tile will have its own unique cyber-physical Blockchain history and be given its appropriate dimensions. Our algorithm requires the road traffic data as input to provide the optimal configuration for geographical tiling.

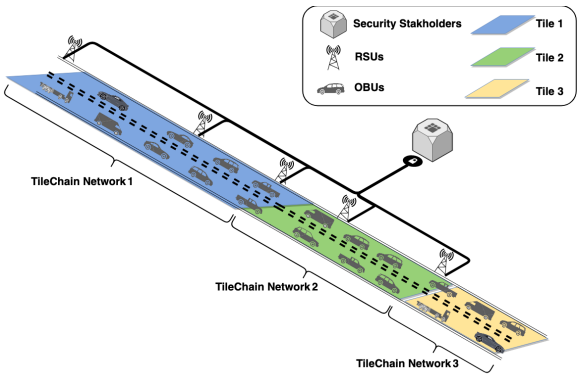



**Fig. 4.2** Security Stakeholders are responsible for running the Tiling algorithm and giving BC parameters to each TileChain Network

The utility of this decentralized system controlled by the security stakeholders (RCA and National Node) is to engage OBUs in the security process. Each Tile can have the same security level and allow the RCA to maintain each Tile's security.

### 4.5.1 Algorithm's Main Inputs

#### *4.5.1.1Traffic Flow*

The traffic data development module is the core of the traffic management system. In connection with the data acquisition module, it collects all the measurements and traffic data from the various road sensors. In the following, we consider highway road segments. One of the main indicators of congestion monitoring that we will be interested in is the density of vehicles $QT$ (vehicle per Kilometer $-Vh/Km-$) in time $i$.

$$QT\left(i\right) = TT\left(i\right) \times VT\left(i\right) \tag{4.9}$$

*VT(i) is the vehicles' speed Km/h at time i*
*is the vehicles' occupancy rate on the Highway at time i*




**Fig. 4.3** Weekly estimation of traffic flow based on temporal aggregation of the same period on past 3 years (2016, 2017, and 2018)

This brings us to calculate the traffic flow $TF$ (Vehicle per Hour $-Vh/h-$), it can also be measured over a time interval. Road managers typically do measurements over 6 minutes periods as shown in Figure 4.3.

$$TF\left(i\right) = QT\left(i\right) \times VT\left(i\right) \tag{4.10}$$

#### *4.5.1.2RSU Coverage*

One crucial input for our study is the RSU coverage on the highway, which ensures infrastructure service availability in the network. It also refers to the mining power (privilege to commit a new transaction) in our proposed TileChain framework: the more RSUs covering the highway, the better stakeholders' devices control the TileChain Networks security. We consider RSUs antennas' electromagnetic radiation to measure coverage ratio. A highway section is "covered" if the RSU radius transmission covers it. The transmission power could reach 33dBm. Therefore, the range of RSU's coverage is $\alpha \times R$, where R is the ITS transmission range, which is standardized to up to 500 meters [62], and $\beta$ the number of traffic direction that the RSU covers, e.g., in highway mostly $\beta = 2$.

$$C_v(\Delta) = \frac{\sum_{i=1}^{n} C_v(i)\beta(i)}{n} \tag{4.11}$$

Where $C_v$ is a boolean operator, $C_v$ is 1 if the highway segment $i$ is covered by an RSU and 0 if not. For a given highway, $\Delta$ that we decide to cutoff into $n$ highway segments, the value $C(\Delta)_v$ (4.11) is $\Delta$ Tile's RSU coverage ratio.

#### *4.5.1.3C-ITS messages dissemination*

Another important indicator for our study is the estimation of the number of disseminated C-ITS messages. C-ITS messages dissemination in each highway segment depends on the C-ITS transmission range ($R$) and, therefore, nodes' inter-distances. We use the truncated exponential distribution to estimate the number of vehicles with inter-distances $0 < X_R < R$ in a given segment:

$$E[X_R] = E[x|x < R] = \frac{\int_0^R \mu x e^{-\mu x} dx}{1 - e^{-\mu R}} = \frac{1 - e^{-\mu R}(\mu R + 1)}{\mu(1 - e^{-\mu x})} \tag{4.12}$$

$\mu :\ Inter - distance\ distribution\ parameter.$

Accordingly, the expected number of C-ITS messages in a total length of the road segment $T$ is given by:

$$E[\Delta] = E[X_R] \times TT(i) \times \alpha \tag{4.13}$$

$\alpha : disseminated\ messages'\ rate\ .$

### 4.5.2 Optimization

Because of the sizeable V2X network scale, we cannot consider all highways as a single geographic Tile. Thus, our algorithm computes several informative characteristics of the road. Based on the following parameters our algorithm gives the best configuration of TileChain Networks:

- The highway's coordinates,
- Highway road traffic information,
- Coordinates of the RSUs existing on the highway.
- The maximum process time that we want the OBUs to handle,
- The targeted security service optimization.

We divide the problem (the original highway input) into sub-problems (small pieces of the highway) to use these inputs. Each highway piece has different attributes: the coverage of RSU, recommended speed limit, traffic data. The optimization target will depend on the security management service and the authority's objectives.

As shown in Figure 6.4, we choose to solve our problem in two steps.

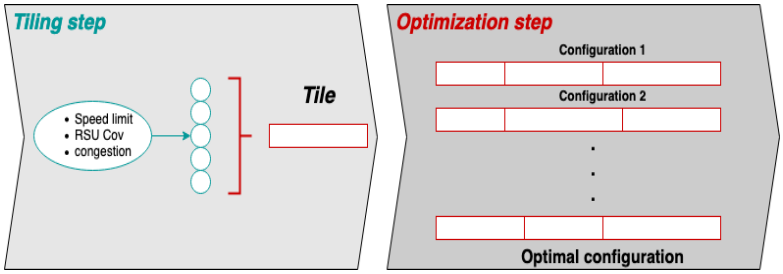



**Fig. 4.4** Tiling algorithm steps

#### *4.5.2.1Tiling Step*

This step aims to determine the best road combination for each Tile, so we consider it as a sub-problem. We first divide the highways into multiple segments (by 1-kilometer section). The optimization problem in this first step is to maximize Tiles' length yet not exceed a specific TileChain Network limit. To formulate our problem, we used the widely-studied knapsack problem [93]. and in particular, the Multiple Multidimensional Knapsack Problem (MMKP) [87] [157].

The weights correspond to each piece of highway's costs in terms of the number of disseminated messages $E[\Delta]$, and the profits correspond to the RSU coverage $C_v$. We want to combine the highway pieces in one or multiple Tiles to maximize connectivity, given a limited TileChain Network storage size.

$$\begin{cases} Maximize \sum_{i=1}^{m}\sum_{j=1}^{n} p_{ij}^{k} x_{ij}^{k}, for\ k = 1,...,s \\ Subject\ to \sum_{j=1}^{n} w_{ij}^{k} x_{ij}^{k} \leq c_k, for\ i = 1,..,m, and\ j = 1,..,n \\ \prod_{p}^{q} x_{ij} = 1, for\ i = 1,2,...,m \\ x_{ij} = 0\ if\ \sum_{i=1}^{m} w_{ij} \geq c \end{cases} \tag{4.14}$$

$x_{ij}$ : Set of highway segments
$w_{ij}$ : The weight of the $i^{th}$ highway segment in the $j^{th}$ Tile
in terms of disseminated messages
$p_{ij}$ : The profit of the $i^{th}$ highway segment in the $j^{th}$ Tile in
terms of RSUs coverage
$c_j$ : The capacity constraint of every $j^{th}$ Tile in
terms of OBUs' processing time
(synonymous with the capacity in the knapsack problem).

In each feasible assignment of items to a given Tile, the Tile $\Delta_j$ corresponding to knapsack $L_k$ satisfies the following properties:

$$x_{ij} = \begin{cases} 1 & if\ p(j) \leq i \leq q(j) \\ 0 & otherwise \end{cases}$$

Where $p, q$ are the coordinates limits of each Tile. The values in positions $[p+1, ..., q]$ contain 1 and 0 otherwise. $X = (x_{ij})$ is said to be the solution of MMKP($L_k$).

The two successive functions have to be disjoint, and every item (a piece of the highway) has to be used at most once.

$$MMKP\,(L_1) = \begin{pmatrix} \Delta_{11} \\ \Delta_{12} \\ \Delta_{13} \end{pmatrix} \begin{pmatrix} 1111\ 0000\ 000 \\ 0000\ 1111\ 000 \\ 0000\ 0000\ 111 \\ \text{X} \end{pmatrix} \tag{4.15}$$

#### *4.5.2.2Service Optimization Step*

In this part of the algorithm, we treat the calculated Tiles (from the tiling step) to have the best configuration of consecutive Tiles. We have the problem formulation using the 0/1 bounded Knapsack problem to maximize the RCA's security management and and not exceed OBU's specific processing power usage in terms of security contribution.

$$\begin{cases} Max \sum_{j=1}^{n} P_j X_j \\ Sub \sum_{j=1}^{n} W_j X_j \leq C \\ \sum_{j=1}^{n} X_i = 1 \\ X_j = \sum_{i=1}^{m} x_{ij}\ i = 1,...,m \end{cases} \tag{4.16}$$

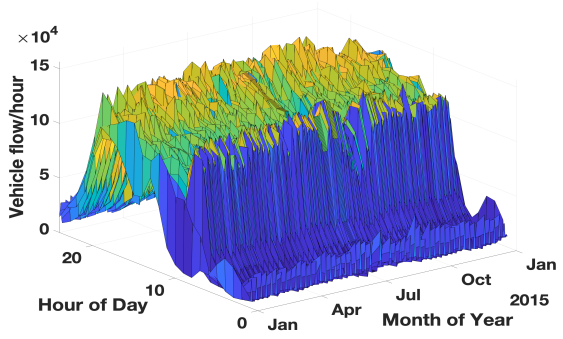
$P_i$ is the profit of each Tile in terms of RCA service management, $W_i$ number of processed messages by OBUs. We note that $C$ is the OBUs' capacity, the chosen best configuration for a given traffic network state.

#### 4.5.2.3Dynamic Traffic Network Topology

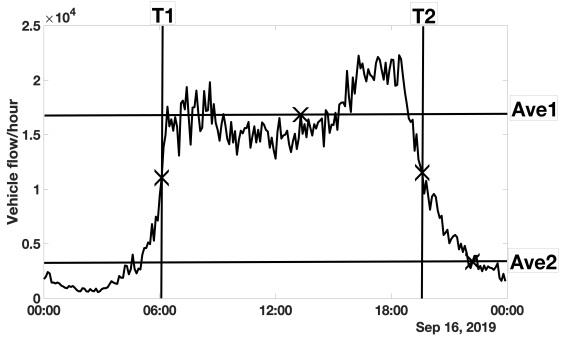
According to our data collection of traffic carried out on DIR Nord's (the French national road network operator) traffic network, we noted that depending on the day, the traffic flow will behave in almost the same manner every day of a year on the A25 motorway between Lille and Dunkerque -French cities- (see Figure 4.5a). Hence, the topology of our TileChain Networks should also change according to the time of day. From Figure 4.5b, we notice that we may distinguish two periods during the day:

- *Period 1*: Corresponds to the period of time from $T1$, until $T2$ $[T_1 \quad T_2]$. We use the average number ($Avg1$) of traffic flow over this period for our tiling method.
- *Period 2*: Corresponds to the period from T2 until T1 of the next day.$[T_2 \quad T_{1nextday}]$. Similarly, we can run the method based on $Avg2$, the average traffic flow of Period 2.

To develop resilient TileChain Networks, we apply dynamic tiling adaptations according to these road traffic topology changes during the day.




**(a)** 2015 year simulation




**(b)** One day simulation

**Fig. 4.5** Daily traffic flow between Lille and Dunkerque, and illustration of the Averages of each tiling day's period

## 4.6 TileChain

For the aforementioned challenges and reasons, we propose a geographic tiling framework called TileChain, which aims to ward off cyber-physical attacks and optimally decompose the extensive V2X network into smaller networks to improve security management. It permits OBUs to participate in the network's overall security in a decentralized manner and the geographic distribution of Blockchain networks will ensure scalability and strengthen security. As part of our optimization approach, the TileChain framework considers traffic densities, road networks, and cyber-physical network topologies in a given geographic area

to determine how to best decompose the BC network based on the security management service and the objectives of the C-ITS authority.

### 4.6.1 Network Setup

#### *4.6.1.1Key Management*

OBUs are assumed to be authenticated by the RCA and have a valid Authorisation Tickets pool to subscribe to the TileChain Network. To contain the hashes of all the trusted Authorisation Tickets in a given Tile, we use the Asynchronous Accumulator (AsAc) (explained in more detail in [142]) in our Blockchain framework. All sent blocks in TileChain Networks will be up to date by getting the latest AsAc in the last block. The witnesses who have approved new OBUs in the blockchain can later prove the node's membership. To add a new block, the AsAc managers are in charge of adding the hash of new member's Authorization Ticket in the AsAc. The AsAc manager broadcasts the new block to all witnesses immediately after the AsAc has been updated.

#### *4.6.1.2Approval Policy*

The Approval Policy contains the Smart Contract and the approval conditions of OBUs inside TileChain Network. Smart contracts and Tile limits are the main dynamic parameters of the Approval Policy.

#### *4.6.1.3Genesis Block*

The Genesis Block is the first Block generated into each TileChain Network and contains the Blockchain and the Approval Policy details. This Block has to be issued by the RCA in order to give all the TileChain Network parameters.

| **Block Header** | |
|---|---|
| *Block Version* | Indicates the Approval Policies |
| *Merkel Tree Root Hash* | The hash value of transaction |
| *Time Stamp (s)* | Current universal time |
| *Parent Block Hash* | Hash value that points to the previous block |
| *Merkel Tree of AsAc* | The hash values of all subscribed Authorisation Tickets in BC and their Witnesses |

**Table 4.3** Block composition

#### *4.6.1.4Blockchain Trust Channels*

A Trust Channel (TC) is a network with similar security privileges and roles. We use two different TCs, each with unique Smart Contracts for our solution. The objective of implementing two different TCs is to adapt blockchain to the V2X network: we dedicate TC 2 to the static part of the V2X network, the RSUs, where there is no need to change the Smart Contract. TC 1 serves to manage the dynamic network of OBUs. We also dynamically regulated its Smart Contract according to time of the day and traffic data. For resilient TileChain Networks, we apply dynamic tiling change according to road traffic topology changes during the day.

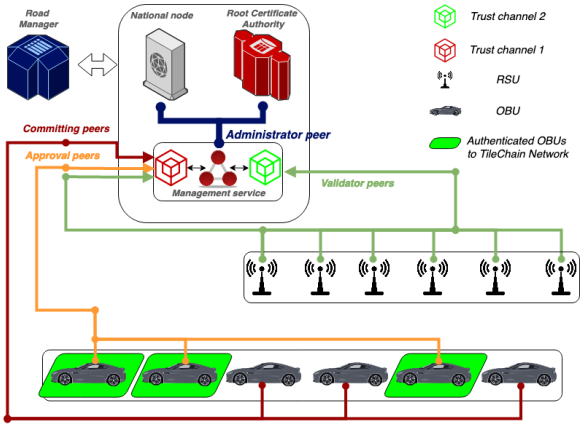



**Fig. 4.6** TileChain framework components. Administrator peers are the security stakeholders that control the Management service and could update Smart Contracts in Trust Channel 1 and 2

#### *4.6.1.5Committer Peers*

The OBUs that have recently joined a given Tile are considered Committer peers and should operate as "Provers" to be authenticated to the TileChain network. Based on the implemented Smart Contract algorithm in TC 1, the Committer Peers collect relevant data to produce transactions and maintain the Blockchain and commits transactions but do not have approval privilege.

#### *4.6.1.6Approval Peers*

A Approval Peer or Prover submits transactions to nearby peers. Only Approval peers could execute this transaction and give output, according to their consensus agreement. They must add their signature to the Smart Contract execution output as part of their endorsement and broadcast it to the Prover and nearby RSUs. The Prover then collects endorsements from multiple Approval Peers in the network to determine that this transaction is valid and that all the outcomes are the same. Peers must install a Smart Contract once they become an Approval Peer.

#### *4.6.1.7Validator Peers*

These peers check if the transactions meet the Approval Policy requirements. They are responsible for naming Committer Peers into Approval Peers. A Validator Peer (RSUs) approves the blocks into the Blockchain.

#### *4.6.1.8Administrator Peer*

These peers are managed by the security stakeholders, They modify the Approval Policy dynamically. To create a new TileChain Network, the must create a new Genesis block with new parameters.

### 4.6.2 Management Service

The management service is the main component determining the order of committed transactions in the network and each TileChain member's role and contribution to the TileChain Network. To guarantee consistency, it ensures that every node in the system must commit transactions in the same order. This service involves the RCA as an administrative entity that manages all the RSU nodes. In our configuration, the National Node can reach any OBU via cellular communication or via IEEE 802.11p technology

using RSUs. The RCA uses the management service to update the Approval Policy and dynamically change tiling parameters in the Genesis Block.

To disseminate transactions into an entire Tile, we assume that the OBUs communicate over both technologies (compatible with both IEEE802.11p / ITS-G5 and cellular communication), using Vehicle To Vehicle Communication (V2V), Vehicle To Infrastructure (V2I), and Vehicle To Infrastructure To Vehicle Communication (V2I2V). To geographically limit the sending of the messages, packets will be encapsulated in Geonetworking protocol [103]. The Geonetworking protocol helps recognize all the nodes present and subscribed to a geographical area (TileChain Network) via their IP addresses.

#### *4.6.2.1Security Stakeholders*

As shown in the Figure 4.6 the third party security stakeholders involved in the Blockchain are the National Node and the RCA.

*RCA:* To optimize the security management of one or more of its services, the RCA must dynamically update the Approval Policy.

*National Node:* This node is responsible for disseminating new Blocks and transactions through the OBUs via V2I2V communication among each TileChain Network. It manages TC 1 transactions and only considers the signed ones by the Approval Peers. The National Node refers to the AsAc that is continuously updated by TC 2.

#### *4.6.2.2Transactions Waiting Pool*

The National Node stores the new transactions validated by TC 1 to make them available to RSUs within TC 2.

#### *4.6.2.3Blockchain Constitution And Storage*

The two TCs contribute to blocks' constitution process. OBUs contribute (in TC 1) with signed Transactions. Once TC 2 reached the consensus, RSUs constitute and publish Blocks with updated AsAc (Table 4.6.1.3). The National Node is responsible for all TileChain Networks' Blockchains storage.

| ***Symbols*** | ***Descriptions*** |
|---|---|
| BC | Blockchain |
| AsAc | Asynchronous Accumulator |
| TC | Trust Channel |
| $N_{Bea}$ | Number of beacons |
| $N_{Sig}$ | Number of AP signatures |
| $VP, AP, CP$ | Respectively Validator and Approval and Committer peers |
| $w, p$ | Respectively witness and prover |
| $Sd, Sd_{ref}$ | Respectively speed and the reference speed |
| $Pos$ | Latitude and longitude coordinates |
| $t$ (s) | Time stamps |
| $Cer, S, H$ | Respectively Certificate, Signature and Hash |
| $Acc$ | the $PoL$ accuracy |
| $Tra$ | Received beacons' traces |
| $C_s$,$C_e$ | Coordinates of Tile's boundaries |

**Table 4.4** Symbols

### 4.6.3 Smart Contract

This section details the implemented security management service that we took as an example for our study case. We have optimized the certificate revocation constraints, as it is one of the main RCA's and OBUs' concerns (see Section 3.3).

To deal with different cyberattacks, we have used two authentication levels. The first authentication level is about promoting OBUs that have valid Proofs to be Approval Peers. Based on the number of collected approved Proofs, the second level involves the revocation lists managed by the RCA. By the borders of two Tiles $T_i$ and $T_{i+1}$, an OBUs that have not been able to collect $N_{Sig}$, the value of $PoL$ will be used to identify malicious vehicles for $T_{i+1}$. The RCA will then add the certificates of these OBUs to the CRL.

As shown in Fig. 4.7 The proposed TileChain framework architecture, it shows how the RCA could be leading multiple geographic TileChain Networks; In Tile 1 we show the consensus process in order to give PoL and Tile 2 we show the consensus process in order to get OBUs approved into TileChain

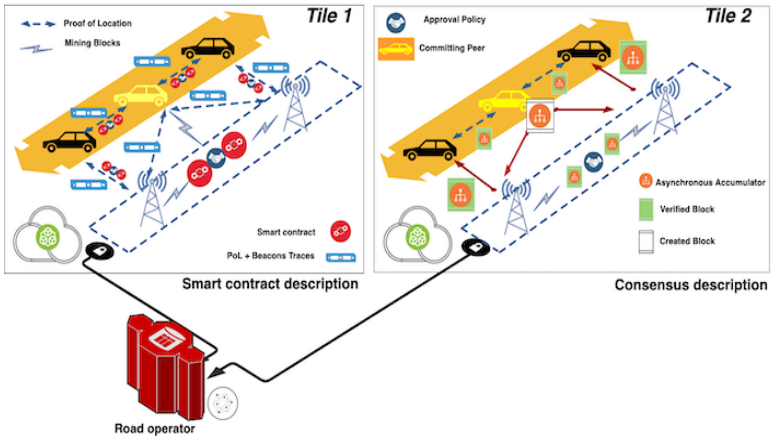



**Fig. 4.7** TileChain framework architecture

The purpose of the Proof-of-Location **(PoL)** consensus is to authenticate OBUs to TileChain Networks by executing the program (Smart Contracts) and proving their information veracity. OBUs must give evidence (beacons) to witnesses without the need for an external party. Each Witness must provide a PoL by executing the Smart Contract to the Prover. A Prover should track its evidence in the BC in order to claim the Approval Peer privilege. We consider only messages from IEEE 802.11p technology for this solution, but other sensors can be used [35].

To illustrate certificate revocation service, we target detection and prevention of position-related cyberattacks in V2X networks (e,g, Sybil attack and position spoofing attack).

This section will detail the adaptation of the chosen security management service (using PoL consensus) to our TileChain framework.

#### *4.6.3.1Approval Policy*

The PoL consensus Approval Policy contains the Smart Contract and the Approval conditions of the PoL transaction among the Approval Peers. For this application, the main parameters used in the Approval Policy are:

- *Tile's borders*: Must contain the geographic coordinates $C_s$ and $C_e$ of the Tile's boundaries.
- $N_{Bea}$: The number of beacons that every witness must collect before providing a PoL.

– $N_{Sig}$: The number of proofs that a node must collect to get authenticated by TC 2.

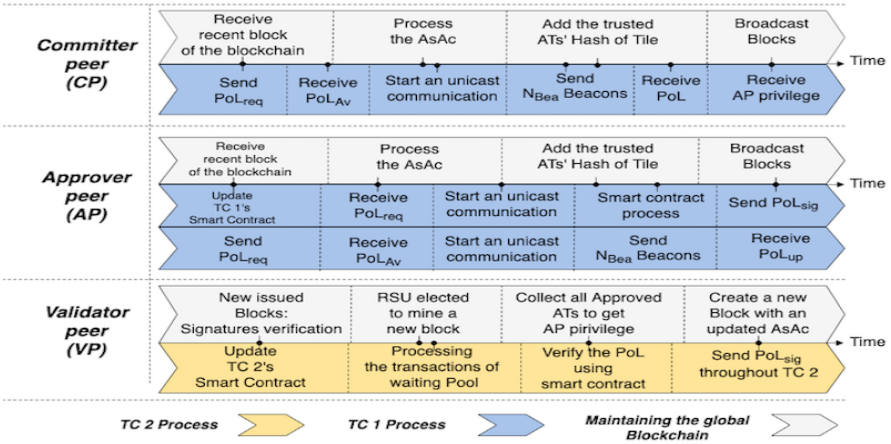



**Fig. 4.8** Timeline of events for each node profile within Trust Channels 1 and 2, Each node should maintain the Blockchain and process its corresponding Smart Contract.

| N | Message | its Composition |
|---|---|---|
| 1 | $PoL_{req}$ | $(Cer_p, t_p, S_p[Pos_p, Sp_p])$ |
| 2 | $PoL_{Sig}$ | $(Cer_{CP}, t_w, Cer_w, S_w[PoL_{Acc}, PoL_{rate}, Pos_{CP}])$ |
| 3 | $PoL_{UnSig}$ | $(Cer_{CP}, t_w, Cer_w, PoL_{Acc}, PoL_{rate}, Pos_{CP})$ |
| 4 | $PoL_{UnCom}$ | $(Cer_w, t_w, Tra_p, S_w[Cer_p, H_{Tra_p}])$ |
| 5 | $PoL_{up}$ | $(Cer_w, t_w, S_w[PoL_{Acc}, PoL_{rate}, Pos_{AP}]])$ |

**Table 4.5** PoL Headers compositions

#### *4.6.3.2Trust Channel 1*

The primary objective of TC 1 is to manage dynamic networks. The PoL consensus is based on the Smart Contract process. The purpose of PoLs is to attest to the integrity of claimed positions by OBUs (see Figure 4.8). When an OBU crosses the Tile, it will be considered as a Committing Peer. The OBU should prove its position to gain AP privilege. The Committing Peer will start the Proof-of-Location consensus process by sending a PoL request $PoL_{req}$ (see Table 4.5.1) to neighboring Witnesses.

In the PoL process, Approval Peers and Committer Peers act like witnesses by executing the Smart Contract and providing proofs. Meanwhile, OBUs with only Committer Peer privilege, may only provide unsigned PoL messages ($PoL_{UnSig}$) by executing Smart Contracts (see Table 4.5.3). These unsigned messages are sent to the National Node for random dissemination to Validator Peers (RSUs) so that it may be verified and signed. Only the Approval Peers could provide a signed PoL, $PoL_{Sig}$ message at will (see Table 4.5.2).

The Witness needs to check the feasibility of providing a PoL to a Prover and entering unicast communication with them. They do this by first calculating the maximum possible Beacons $N$ (see Equation 4.17) with the Prover and then collecting $N_{Bea}$ Beacons.

$$N_{min} = \frac{3600 \times R}{Sd_{ref}} \leq N_{Bea} \leq N_{max} = \frac{3600 \times R}{|Sd_w - Sd_p|} \tag{4.17}$$

To get $N_{Bea}$, the witness must collect the CAM messages under a frequency of one signed message per second [63]. If the Committer Peer does not manage to deliver the $N_{min}$, the unicast communication will crash, the witnesses must report the communication crash via $PoL_{UnCom}$ message (see Table 4.5.4).

Approval Peers should also continuously authenticate by requesting PoLs and get $PoL_{up}$ message (see Table 4.5.5)

#### *4.6.3.3Trust Channel 2*

Nodes in this security category supervise the process of authenticating Approval Peers. These nodes aim to reach a consensus about transactions from TC 1 and set each node's communication privileges. RSUs consider $N_{Sig}$ different parameters in their Approval Policy to authenticate OBUs as trusted nodes. Each new Block contains an up-to-date Certificate Revocation List based on which nodes failed to authenticate or had been detected as misbehaving.

#### *4.6.3.4Certificate Revocation*

The RCA may regulate parameters, $N_{Bea}$ and $N_{Sig}$, to allow RSUs to make the correct revocation decision. Each Trust Channel has a role in the global revocation process. TC 1 is used to provide proofs between OBUs and declare $PoL_{UnCom}$. TC 2 is used to determine the vehicle trust level and revoke the certificates of malicious vehicles.

To give an ideal Approval Policy to address security vulnerabilities, security stakeholders must dynamically set the optimal $N_{Bea}$ and $N_{Sig}$ based on traffic data and data analysis from the previous tiling topology.

In this case study, we consider a cluster as a small ad-hoc network of nodes communicating with ITS-G5 communication. Each OBU goes through multiple clusters during its travel within a tile and uses one or more Authorisation Tickets.

$$N_{Clus}(\Delta) = \frac{E[\Delta]}{E[X_R] \times TD_{\Delta}} \tag{4.18}$$

As shown in Figure 4.9, $N_{Clus}$ quantifies the total number of clusters an OBU has been through during its journey in each Tile, that we calculate from Equations 6.3 and 4.13, where $TD_{\Delta}$ is the OBU's traveled distance in Tile $\Delta$.

The optimal $N_{Sig}$ depends on $N_{Clus}$ as it is expressed in Equation 4.19.

$$\frac{N_{Clus}(\Delta)}{N_{Bea} \times N_{ClusID}(\Delta)} \leq N_{Sig} \leq \frac{N_{Clus}(\Delta)}{N_{Bea}} \tag{4.19}$$

Where $N_{ClusID}$ is the number of used Authorization Tickets and IDs in Tile $\Delta$. This adaptation of TileChain for certificate revocation allows us to guard against two well known cyber-attacks in V2X networks.

*Against Position Spoofing Attack:* Using the $PoL$, the OBU can identify the falsification of the positions according to the parameter $N_{Bea}$. The Approval Peers will not provide a PoL if it does not receive a sufficient proof of the actual physical existence of the OBU.

*Against Sybil Attack:* Supposing that the attacker succeeds in getting a valid PoL, it is difficult to get the minimum mandatory $N_{Sig}$ rate for all claimed IDs. Therefore, entities performing Sybil Attack will not be authenticated and their certificates will be revoked.

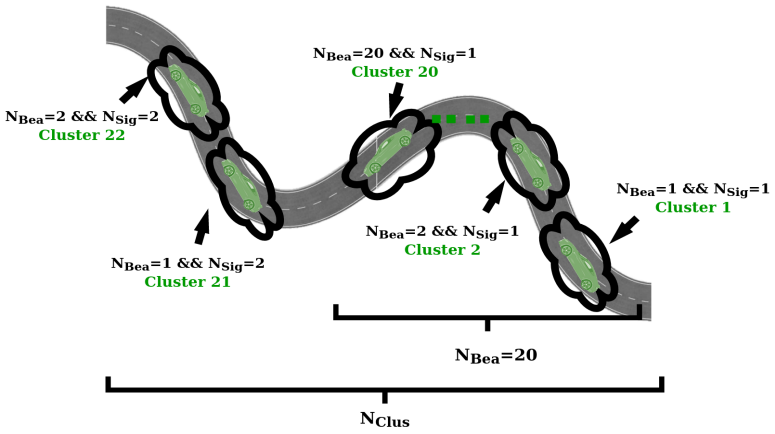



**Fig. 4.9** Representation of Approval Policy features, where the number of clusters an OBU has gone through, $N_{Clus}(\Delta)$, is based on overall beacons and traveled distance within a tile

## 4.7 Performances Analysis

We tested the performance of our solution via experiments with real ITS stations and via state of art simulator.

| **Experimental work** | Experiments in realistic conditions |
|---|---|
| Used equipment | 2 OBUs, 1 RSU |
| Speed velocities | |
| Radio equipment | NXP ITS-G5 chip [6] |
| Communication | with/without line-of-sight |
| Max Velocities (Km/h) | ***Test 1***: 24.62-72.57; ***Test 2***: 24.84-65.59; ***Test 3***: 0.64-59.83 |
| **Communication simulator** | OMNET ++ |
| Number of node | ***Test 1***: 2288; ***Test 2***: 1683 ***Test 3***: 1738; ***Test 4***: 3201 |
| Application | Veins- VANET [159] |
| | Aretry Framework [143] |
| | Broadcast-message based |
| | 100ms update time - CAM |
| | Communication range - Omnidirectional 500m |
| | Sensing range 800m |
| Number of broadcasted CAM | ***Test 1***: 36921; ***Test 2***: 22301; ***Test 3***: 23982; ***Test 4***: 44793 |
| **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 4.6** Experimental Setting And Simulation Parameters

We used the real traffic data provided by the DIR Nord road operator (see Table 5.5 for detailed settings). Collecting 250 GB of simulation raw ITS G5 exchange data was a challenging task, yet proved valuable in demonstrating our proposed solution's practicality.

### 4.7.1 Proof Of Location Accuracy

#### *4.7.1.1Experimental work*

We have conducted tests in natural conditions on a university's campus, using an equipped car track [1]. We have used two on-board units (ITS-G5 equipment) with two real vehicles, and one RSU already

installed on the track. The radio equipment used in each of the three devices is a state-of-the-art NXP ITS-G5 chip [6].

In this experiment, we have compared two location estimation methods in order to use the performances of the most accurate one to prove locations in our simulations. Tests have been repeated three times and averaged to obtain statistically valid results.

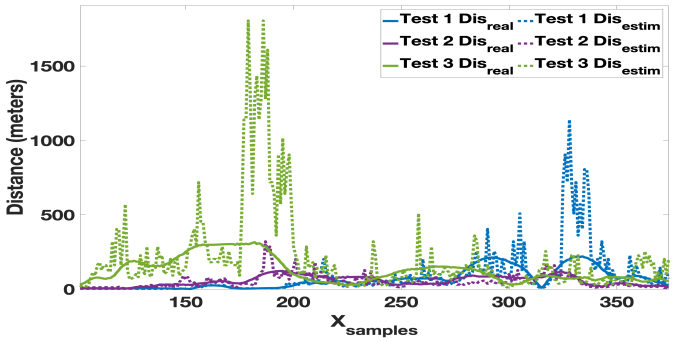



**Fig. 4.10** Distance estimation using Friis equation based on RSSI

- **RSSI method:** We calculate distance according to received RSSI using 1) the Friis equation and 2) the link budget equation [154] (see Figure 5.1).

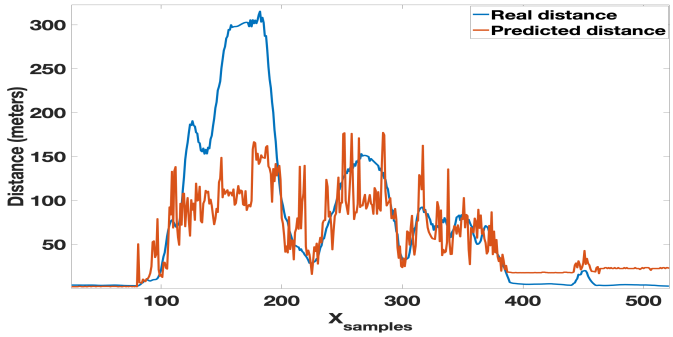



**Fig. 4.11** Predicted distance by trained model based on estimated RSSIs via the two different methods (Riis and link budget)

- **Relative Driving Parameters Method:** Using learning regression on the results of the two different methods, we estimate the distance based on RSSI and three vehicle state measurements: 1) relative velocity, 2) yaw rate, and 3) heading) (see Figure 4.11).

**Table 4.7** PoL Accuracy Using The Methods

| | RSSI Method | | | Parameters Method |
|---|---|---|---|---|
| Test | Test 1 | Test 2 | Test 3 | Prediction |
| $PoL_{Acc}$ | 72.92% | **77.66%** | 66.49% | **81.35%** |

In Table 4.7, we notice a better detection using the difference of driving parameters compared to the estimation of the distance from RSSI.

To demonstrate the Prover's authentication accuracy, we averaged the three tests' median error rates. In Figure 4.12, we show the detection accuracy cumulative distribution functions based on $N_{Bea}$ (number of beacon samples from neighbors). According to the distribution functions, it is clear that increasing the number of $N_{Bea}$ will lead to better misbehavior detection accuracy.

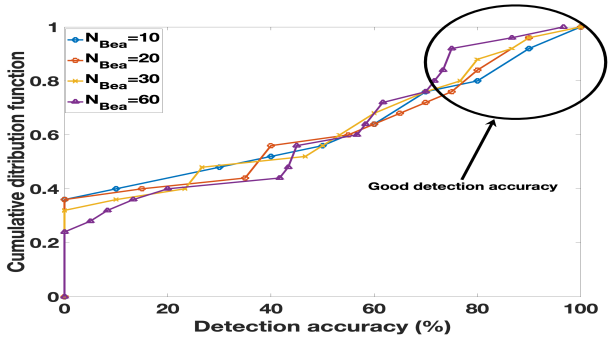



**Fig. 4.12** Distribution function of distance detection accuracy based on used $N_{Bea}$

#### *4.7.1.2Simulation work*

In this section, we present the outcomes of the simulation studies concerning our Blockchain-based solution's scalability.

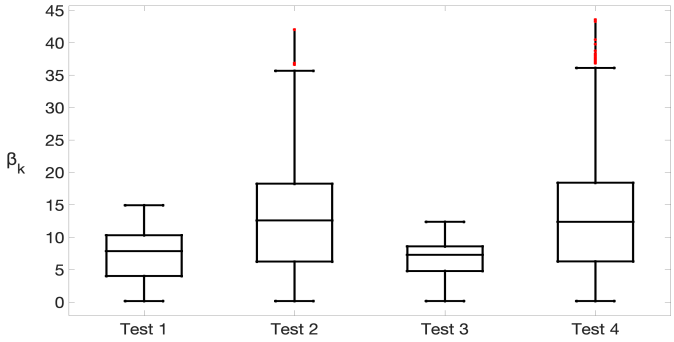



**Fig. 4.13** Simulaion of diffrent traffic densities

Figure 6.7 illustrates the variety of simulations using different traffic densities.

$N_{Bea}$ must be given based on road traffic parameters and should be dynamically adjusted by the RCA through TC 1.

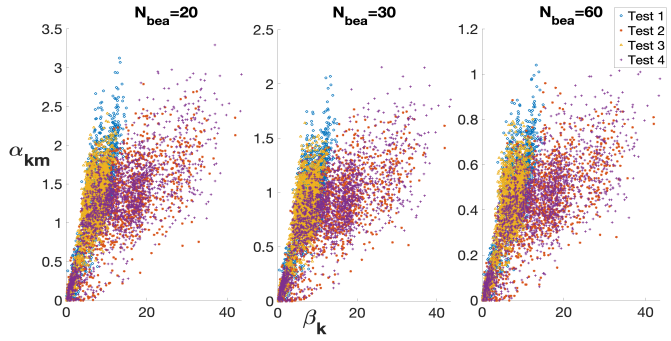



**Fig. 4.14** The evolution of the Tile length over time and based on $N_{Bea}$

First, we show in Figure 4.14, the $PoL$ reception rate in each kilometer depending on the traffic density and $N_{Bea}$.

To prevent the position spoofing attack, $N_{Bea}$ must be calculated based on the relative velocity between vehicles (see Equation 4.17). Considering the average speed on highway is $90 < Sp_a v < 130$, we obtain $20 < N_{Bea} < 30$.

From Figure 4.15, we note that we have a peak of $PoL$s emission because of the handshake phase between vehicles. The authentication delay depends on relative velocity and density of vehicles $(QT)$ in

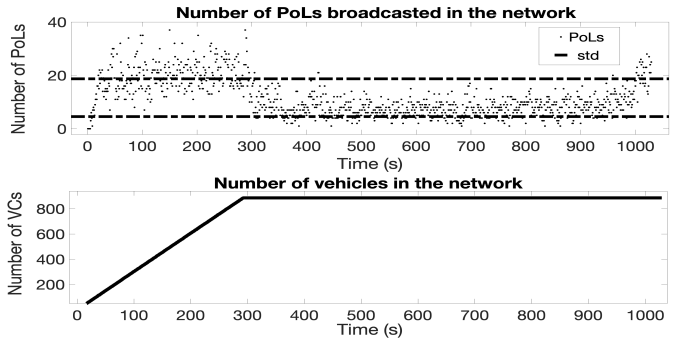



**Fig. 4.15** Total number of the sent PoLs in the network as a function of the number of OBUs

each communication cluster.

**Table 4.8** Correlation between received $PoL$ and traffic parameters

| | Speed average | Spent time | Traveled distance |
|---|---|---|---|
| $PoL$ received | 63.25% | 67.64% | **70.67%** |
| ($PoL$ received)/s | **-71.18%** | -9.83% | 0.42% |

Table 4.8 shows the correlations of the input parameters concerning the global received $PoLs$ in a Tile and the rate of received $PoL$ per second in a specific highway. The input parameters are: average speed, time, and distance traveled within the Tile. As one may observe, the global number of received $PoLs$ is considerably linked to traveled distance and spent time in a Tile. The spent time and traveled distance are not so correlated to $PoL/s$, but average speed is highly correlated to $PoL/s$. Thus, in order for our simulations to emulate various realistic situations, we opted for testing with different vehicle traffic density values, as shown in Figure 6.7 (functions of average speed and number of vehicles in a given area). We deduce that the correlation rates from Table 4.8 are reasonable and may be used with interpolation for real traffic data and scenarios.

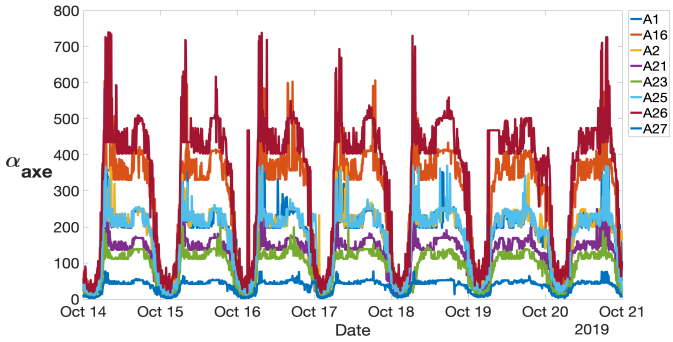



**Fig. 4.16** The $PoL$ emission per second in each highway for $N_{Bea} = 20$

### 4.7.2 Dynamic Tiling

In order to predict the $PoL$ emission curve of real traffic data for $N_{Bea} = 20$, we used the Gaussian Process regression learning model with $R^2 = 0.69$ to reconstitute the number of messages sent, taking into account the traffic data. This is consistent with the results obtained in Table 4.8. We divide our Highway network into different axes. In Figure 4.16, we plot the $PoL$ emission of each highway every second during a week, using the traffic data on $2019/14/10$ to $2019/21/10$.

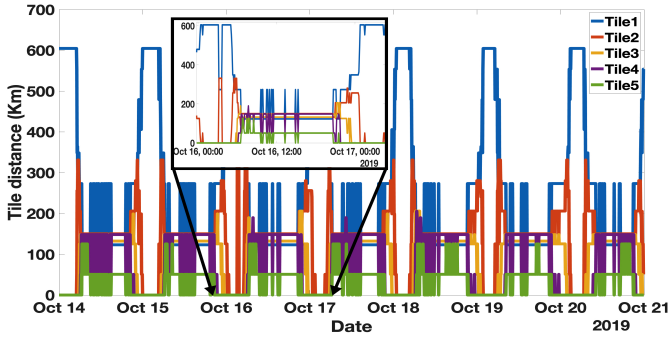
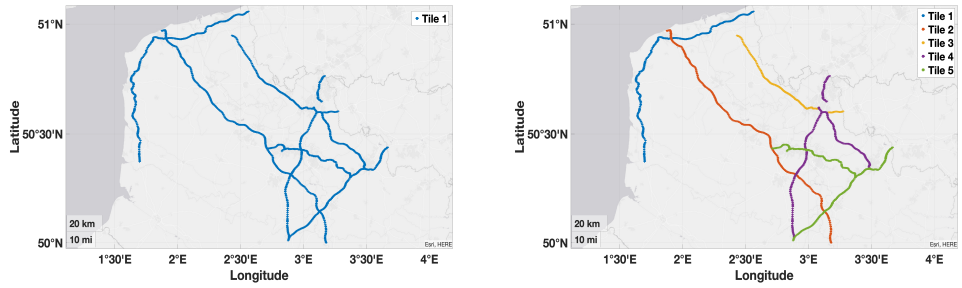



**Fig. 4.17** Evolution of Tile's length in each moment based on traffic data

We applied our optimization algorithm to DIR Nord's traffic data. The RCA has to find the optimal number of extreme traffic situations (high and low vehicle density) to build up scalable TileChain networks. Two parameters may be dynamically changed to get the optimal configuration in terms of security and scalability: $N_{Bea}$ (used by TC 1) and $N_{Sig}$ (used by TC 2).




**(a)** Period 1: In the period [10 pm - 6 am], since traffic density is low, we can have one Tile covering the entire network

**(b)** Period 2: In the period [6 am - 10 pm], the traffic is the densest; thus, we should divide our network into multiple TileChain Networks

**Fig. 4.18** Tiling Network configurations over a day via dynamic Tiling.

In Figure 4.17, we show the evolution of the length of each Tile during a week. We show a periodic evolution of the dimensions of the Tiles correlated with the traffic flow. From that, we can distinguish two periods in the day, as shown in Figure 4.18.

### 4.7.3 TileChain Performance

This section presents an analysis to highlight the benefits of TileChain for RCA's security management optimization. We will concentrate on metrics related to our case study.

In the traditional C-ITS security management, all RCAs must list all revocated Enrollment Certificates under their governance. However, an OBU must process all revocation certificates from the country where it operates. Take the case of an OBU operating in France. To ensure coverage of the entire network, we use our data for the "Haut de France" region, as being 1/13 of the French highway, we will multiply the number of vehicles by 13 to obtain the approximate number of vehicles circulating on the French highways.

In order to estimate the CRL size, here are some assumptions:

[16] recommends $T = 5$ years for the CRL's lifetime. Let parameter $p = 1\% = 0.01$ be the revocation rate, i.e., the fraction of revoked vehicles per year. As per the IEEE 1609.2 Standard, each CRL entry is represented by the higher order $q = 32$ bytes of the revoked certificate's SHA-256 hash value. Hence, the steady-state size of CRLs without TileChain-based certificates is given:

$$TF(k) \times p \times T \times q = TF(k) \times (0.01)(5)(32)bytes \tag{4.20}$$

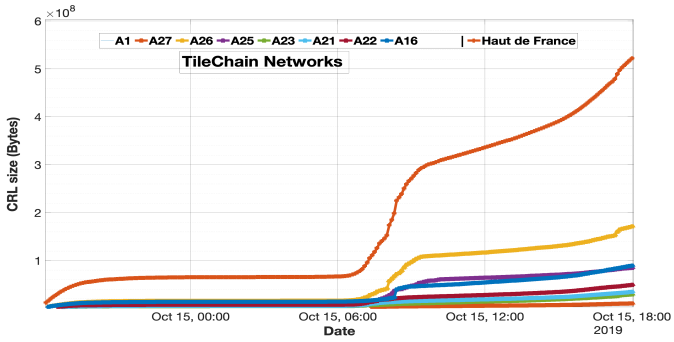



**Fig. 4.19** Comparison of CRL size when using traditional solution versus the sizes of CRLs of each Tile derived from TileChain solution. Haut de France is would be the whole area under the control of the RCA. The traditional solution will consider the entire highway (Haut de France) to manage a CRL, and this potentially large CRL is sent to each OBU. On the other hand, in this TileChain solution example, the highway is cut into multiple Tiles named A1-A16 and each OBU will receive a CRL mapped to the Tile it is in. Therefore there will be a shorter average processing time of the certificate linkage per OBU.

We calculated the size of the CRL over various settings using Equation 4.20. In Figure 4.19 we considered that the RCA controls only DIR Nord's network "Haut de France". We notice that using TileChain, the size of the CRLs remains almost stable and does not add extra processing time to the OBUs in terms of certificate linkage.

Misbehavior reports are done individually in traditional architecture, and it could severely increase the load on the RCA's servers. We are assuming that the PoLs reports are sent individually.

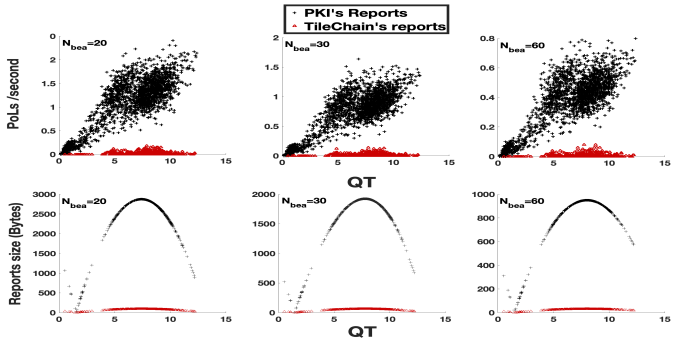



**Fig. 4.20** The optimization of misbehavior reports using our TileChain framework

Figure 4.20 shows that we can reduce the authorities' computational load by a factor of **96.8%** using the TileChain framework. As the information is already confirmed by the Validator and Approval Peers, we can aggregate the sent report to the RCA.

We can see that this adaptation of the TileChain framework using certificate revocation as a case study allows to optimize the RCA's security service management and guard against cyber-attacks. As the results show, the authority can optimize the load on its servers and reduce the OBUs' CRL processing time, making them more available to participate in the overall cybersecurity. The RCA can also dynamically increase the detection accuracy of vehicles concerning cyber-attacks linked to the position. With this solution, the RCA may potentially even protect itself against DoS attacks since the reports and requests are not directly sent back to its servers.

## 4.8 Conclusion

This chapter has demonstrated the importance of involving vehicles in the overall safety process by applying the PoL consensus. This allows us to guard against position-related attacks and create a collaborative framework based on the blockchain.

Our solution aims to bring the decentralized aspect to V2X networks and show the feasibility and scalability of the TileChain framework. The dynamic tiling algorithm makes cyber-physical security manageable and can resolve all runtime vulnerabilities. This framework mainly reinforces the security of the VC network since it does not propose to reject the current solution. We based our case study optimization problem on the certificate revocation framework, but TileChain can be applied using other services, like authentication, which can significantly reduce the load on RCA servers.

CHAPTER 5

# New Blockchain-Based Cooperative Revocation Framework

## 5.1 Introduction

V2X communications have some special requirements: Due to many nodes being constantly on the move at higher speeds, tolerance for quickly changing topologies and low-latency communication are important points. Multi-hop mesh networking is an important ability to keep the network functional in areas without designated infrastructure. As we had introduced in section 3.4, Decentralized systems are emerging today as essential elements of future vehicle communication networks and 5th generation cellular networks. The benefits provided by this technology are numerous. Thus, it could make it possible to guarantee optimal and adaptive management of the resources necessary for the implementation of an optimal security system.

The TileChain approach constitutes a real evolution in the way of thinking and designing vehicular communication networks. Indeed, this technology is based on the idea of decoupling the control and data plane and reducing the load on security authorities by integrating vehicles into collaborative work. Thus, the architecture of the geographic tiles can constitute several independent Blockchains. However, the issue of the compromise between cybersecurity and road safety remains topical. In this chapter, we mainly tackle the revocation of certificates taking into account the constraints of V2X networks.

## 5.2 Problem formulation

### 5.2.1 Motivation

Our aim: ensure real-time certificate revocation, considering V2X constraints. Identify V2X attack vectors, like unauthorized data access or modification, or denial of service. Effective encryption, authentication, and access control can counter these attacks, enabling real-time certificate revocation. Also, emphasize Blockchain's potential for scaling trust and ensuring high security.

### 5.2.2 Cyber Threats

In this section, we will outline various prevalent cyber threats in V2X communications that can significantly impact both communication systems and drivers.

#### *5.2.2.1DoS Attacks*

DoS attacks can happen in different layers of the network where an adversary sends more requests than the system can handle. For instance, an attacker could try to shutdown or to disrupt the network established by RSUs and stop communication between vehicles and/or RSUs [148]. In a distributed DoS

(DDoS) attack [164] malicious nodes launch attacks from different locations, thus making it harder to detect. In the physical layer, an important type of DoS attack is the jamming attack [21], where the attacker disrupts the communication channel (e.g., by electromagnetic interference) and can filter/limit incoming messages. Jamming functions well only in geographically restricted areas, i.e., say within the range of the attacker(s) wireless device. We also note that most jamming/DoS attacks on the PHY level (IEEE 802.11p) or the bands around 5.9 GHz are always restricted by the range of the attacker(s) and do not impact V2X communications everywhere. A jamming attack does not require any particular knowledge of the semantics of the exchanged messages [168]. Although jamming attacks are not specific to V2X systems (i.e., can be a threat for any wireless network), such attacks can increase the latency in the V2X communications and reduce the reliability of the network [134]. In the network layer, routing-based DoS attacks such as the JellyFish attack [17] exploits vulnerabilities in congestion control protocols and the attacker delays. Packet dropping is catastrophic for safety-related applications. Flooding attacks [148] such as data flooding (e.g., where an attacker creates bogus data packets and sends it to their neighbors) can make the network resources (e.g., bandwidth, power, etc.) unavailable to legitimate users. We note that these routing-based attacks can only be performed on multi-hop communication networks.

#### *5.2.2.2Sybil Attacks*

This is a well-known harmful attack in wireless vehicular networks where a vehicle pretends to have more than one identify (e.g., multiple certified key-pairs) either at the same time or in succession [187]. Sybil attackers may also launch DoS attacks, waste network bandwidth, destabilize the overall network and pose threats to safety [25]. For instance, if a malicious vehicle changes its identity, it may use multiple pseudonyms to appear as a different, moving vehicle or make it appear that the road is congested (even though it is not) and send incorrect information about the road conditions to neighboring vehicles/RSUs. A Sybil attacker could also use the pseudo-identities to maliciously boost the reputation/trust score (e.g., that used to measure how much neighbors can rely on information sent by a given vehicle Vi), etc. of specific vehicles or, conversely, reduce the score of legitimate vehicles [168].

#### *5.2.2.3False Data Injection*

A rogue vehicle could generate false traffic/safety messages or incorrect traffic estimation information (that differs from real-world information) and broadcast it to the network with the intention of disrupting road traffic or triggering a collision [75]. Sybil attackers can claim their existence at multiple locations and can thus inject false information into the network. By GPS spoofing, an attacker could inject false position information by using GPS simulators, and the victim vehicles may end up accepting these generated, fake (but stronger than original) signals. Incorrect data such as falsified location information could decrease message delivery efficiency by up to approximately 90% [111]. Researchers have shown that cooperative adaptive cruise control (CACC) is specifically vulnerable to false data injection attacks [23]. Another type of false data injection is replay attack, where an attacker retransmits messages to exploit the conditions at the time when the original message was sent (e.g., the attacker stores the event information and will resend it later, even though it is no longer valid) [82]. For instance, in location-based replay attacks, the attacker records an authenticated message at a location Li, transmits it quickly to a location Lj (and re-broadcasts it at Lj). Similarly, in time-based replay attacks, an adversary records a valid message at time t1 and replays it later (at the same location) at another time t2. For replay protection, there exist mechanisms such as including a timestamp in every message and digitally signing and including sequence numbers [117].

## 5.3 Existing Solution

### 5.3.1 Classification of Detection and Prevention Mechanisms

V2X security approaches can broadly be characterized as proactive and reactive mechanisms [75]. Proactive security refers to any kind of mechanism that enforces a security policy – say, use of a PKI, digital signatures and certificates, tamper-proof hardware, etc. This reduces the chances of bogus information exchange by unauthorized entities due to lack of credentials and can be maintained through a combination of infrastructure and tamper-proof hardware [92]. While these mechanisms reduce attack surfaces by detracting external attackers, insider attackers can generate legitimate false information. Such schemes also face scalability and complex management issues (e.g., key management, revocation, trust establishment in multi-hop communication). Reactive mechanisms can be enforced where the attacks cannot be prevented by proactive security policies. These mechanisms can be grouped into two classes: (a) entity-centric and (b) data-centric.

- *Entity-centric approaches* focus on identifying the misbehaving node based on trust establishment by using a PKI or in a cooperative manner (e.g., using signature verification). Entity-centric detection approaches can be further subdivided into:
  - Behavioral: e.g., observes patterns in the behavior of specific nodes at the protocol level)
  - Trust-based: e.g., evaluation of trust-score, often using a central authority to remove malicious nodes).
- *Data-centric approaches*, in contrast, verify the correctness of the received data (instead of investigating the trustworthiness of the sender). Data-centric mechanisms are similar to intrusion detection in traditional computing systems that correlate the received information with the information already known from previous history/behavior.

These approaches can be either:

– Plausibility-based: a model-based approach that verifies if the information transmitted from a particular sender is consistent with the model.

– Consistency-based: Use the information of packets – generally from multiple participants – to determine the trustworthiness of new data.

We highlight that entity-centric and data-centric detection mechanisms are mostly orthogonal, and often researchers propose to use combinations of both types. Depending on the scope, detection mechanisms can be local and/or cooperative (detection relies on collaboration between vehicles/RSUs). In contrast to RSU-based mechanisms, OBU-based approaches do not need dedicated infrastructure. Researchers also proposed hybrid approaches where both RSU and OBUs are jointly involved in misbehavior detection. Behavioral and plausibility schemes generally operate locally, while consistency and trust-based rely on cooperation among vehicles/RSUs to detect inconsistencies. Some consistency-based mechanisms can also be performed locally for more fine-grained detection with the cost of exposing them to Sybil attacks. We now briefly review the mechanisms to secure V2X communications from different classes of attacks. Table **??** summarizes the exiting solutions.

### 5.3.2 DoS Detection/Mitigation

Since DoS attacks [139] can be implemented at varying layers, researchers proposed different solutions to detect/mitigate the chances of attacks. Jamming-based DoS attacks can be detected by behavioral

mechanisms – for instance, by analyzing the patterns in radio interference [80] as well as by using statistical network traffic analysis and data mining methods [119]. The chances that (external) attackers intrude/disrupt the system can also be reduced by using short-time private-public keys with a hash function [50]. He et al. [83] proposed to use a pre-authentication process before signature verification to prevent DoS attacks against signature-based authentication (where attackers broadcast forged messages with invalid signatures – leading to unnecessary signature verifications). Researchers also proposed alternatives to digital signatures – a new authentication method (called Tesla++) [162] that reduces the memory requirement at the receiver for authentication and can be used to limit the chances of resource (e.g., memory) exhaustion. A downside of these protocols is a high delay between message arrival and message authentication. Given the fact that the routing in V2X is predictable and standardized, network layer DoS attacks such as packet dropping can be detected by watchdog mechanisms [85] where each vehicle uses the idea of neighbor trust level (determined as the ratio of packets sent to the neighbor and the packets are forwarded by the neighbor). Packets may not be forwarded due to a collision and/or an attack. If a vehicle is repeatedly dropping packets (until a tolerance threshold is exceeded), the vehicle is considered malicious – although the evaluation results show that it is difficult to find a global threshold (e.g., for deciding when misbehavior should be detected). Packet dropping/duplication can be prevented by clustering-based monitoring [51] where a set of vehicles in a cluster (called verifiers) monitor the behavior of a (newly joined) vehicle. Vehicles that act maliciously are blocked by a certificate authority (CA) and are informed by other vehicles. There exist mechanisms [160] to detect flooding-based DoS attacks by observing channel access patterns – for instance, by generating an adaptive threshold (that represents the maximum rate of messages any vehicle can send with respect to other vehicles). This approach may not be scalable for generic use- cases since the scheme is designed for vehicles communicating with a single RSU. Similar infrastructure-assisted mechanisms such as those proposed by Verma et al. [171] can prevent DoS attacks by:

– Monitoring V2X messages (that checks the number of outstanding packets with a predetermined threshold within a certain window of time);

– Using a message marking policy where packets are marked by the edge routers (say RSUs), and if the sender IPs are found malicious, an alarm is sent to other vehicles.

This work [32] propose to randomize the RSU packet transmission schedule and a modification of the congestion control schemes to mitigate packet flooding-based DoS/DDoS attacks. Message flooding can also be detected by trust-based mechanisms.

### 5.3.3 Detecting Sybil Attacks

Researchers proposed to detect Sybil attacks in V2X networks that can work either:

- Without any infrastructural support [81]
- With assistance from infrastructure (e.g., RSU, PKI, trusted authority) [48].

#### *5.3.3.1Infrastructure-less Sybil Detection*

Grover et al. [77] suggest that the fake identities of the attacker must always be in the same vicinity (for better control over malicious nodes) and proposed a detection by comparing the tables of several neighboring vehicles over time. This scheme does not protect against Sybil attacks that have a short duration. The communication overhead and detection latency are high, and certain scenarios may increase

false positives or detection latency. Hao et al. [81] proposed a cooperative protocol that utilizes group signature (to preserve privacy) and correlation of mobility traces. The key idea is that vehicles around a possible attacker inform others by broadcasting warning messages with their partial signatures – a complete signature can be derived (and hence the attacker is identified) when the number of vehicles that report anomalies reaches a threshold. The protocol is not verified for the case of multiple Sybil attackers. A model-based approach, based on position verification, is proposed by Golle et al. [78] where each node contains a model of the network and checks the validity of the received data using local sensors (i.e., camera, infrared, and radars). Data collected from the sensors can be used to distinguish between nodes. Inconsistencies can then be detected based on the proposed heuristic mechanism by comparing the received data with the model. For instance, using a camera reading and exchanging data via a light spectrum, a vehicle can verify whether a claimed position is true. Thus one can determine the real existence of the vehicle. However, it is generally hard to obtain a generic model of the V2X network due to its dynamic nature, and the proposed method is designed by considering high-density road conditions only. Researchers also proposed the identification of falsified positions by exploiting channel properties, for instance, by analyzing its signal strength distribution [17] or by observing RSSI (received signal strength indicator) measurements. A Sybil detection approach [78] analyzes physical layer properties under the assumption that antennas, gains, and transmission powers are fixed and known to all the vehicles in the network. The authors use received signal strength to determine the approximate distance to the sender and further verify the transmitted GPS position. A similar idea is also used [146] to verify locations by finding the correlation between location, time, and transmission duration (for both beacons and event messages). A post-event validation approach verifies specific event messages (by analyzing messages from other vehicles), and also pseudonym change mechanism is applied once a claimed event is detected as being malicious. This scheme, however, can be exploited to revoke legitimate vehicles by an attacker with jamming capabilities (since they are based on physical-layer signal properties) [168].

#### *5.3.3.2RSU-assisted Sybil Detection*

There exist mechanisms [74] to use a centralized authority (e.g., RSU) to detect Sybil nodes. In an earlier study, Xiao et al. [175] verify claimed positions using signal strength metrics where vehicles are assigned three roles:

- Claimer (a vehicle claims a position using a beacon),
- Witness, (a node receives a beacon and measures its proximity using the received signal strength that is then transmitted in subsequent beacons)
- Verifier (the vehicle that collects signal strength measurements to estimate and verify the position of a vehicle). RSUs issue signatures of vehicles in their proximity at a specific time along with a driving direction. When a beacon message is received, the verifier waits for a period of time and calculates an estimated position of the claimer.

Researchers also proposed [127] to use message timestamps (e.g., to find each vehicle's recent trajectory and time) for Sybil detection that does not require any PKI. Before sending any messages, a vehicle first obtains a timestamp for the message from a nearby RSU. If a vehicle receives similar timestamp series from the same RSUs for a certain amount of time, then that vehicle is considered as a Sybil node. However, two vehicles coming from opposite directions could be incorrectly marked as Sybil nodes since they will receive similar timestamps for a short time period.

### 5.3.4 Event Validation

Kim et al. [99] propose a message filtering mechanism that combines parameters of messages into a single entity called the 'certainty of event' (CoE) curve. CoE represents the confidence level of a received message and is calculated by combining the data from various sources such as local sensors and RSUs and by using consensus mechanisms. Message validity is defined using a threshold curve, and false positives for events can be reduced when more evidence is obtained over time. At the same time, the mechanism is applied to the emergency electronic brake light application, it is unclear how this scheme behaves for generic V2X applications (say for multiple lanes and urban settings where there may be some uncertainty about the vehicle paths) since it requires specific locations for the events.

Besides, such CoE-based mechanisms could be vulnerable to Sybil attacks depending on how the information from other sources is captured. Researchers also proposed to determine the correctness of event reports through voting [45] the key idea is to develop an efficient way to collect signatures from a sufficient number of witnesses without adding too much (bandwidth) overheads on the wireless channel. If insufficient signatures are received, events may be missed completely. A similar idea is also used by Hsiao et al. [86] where the senders collect a number of witnesses for each possible event. However, this model enforces a specific message format, and there is no deflation protection, i.e., the attacker can reduce the number of signatures attached to the message and/or can hide events. A consensus-based mechanism is proposed [130] where each vehicle collects reports about the same event from neighboring vehicles until a certain threshold of supporting reports is passed. The proposed method allows the system to reach a decision within a bounded waiting time and thus suitable for time/safety-critical applications. Similar to the most consensus-based mechanisms, this approach also suffers from potential Sybil attacks.

The idea of post-event detection [76] can also be used for event validation: for instance, in post-crash notification (PCN) applications, once a PCN message is sent, drivers adapt their behavior to avoid the crash site, and this information can be used to identify whether the event was valid or not. The key idea is to use a technique (called root cause analysis) to detect which part of the event message was false. Such detection approaches suffer if the driver behavior models are fragile – although this may not be a limiting factor for autonomous driving where valid driver behavior will be more well-defined.

### 5.3.5 Behavioral Analysis and Message Integrity Checking

The VEBAS (vehicle behavior analysis and evaluation scheme) protocol [152] allows the detection of unusual vehicle behavior by analyzing all messages received from neighboring vehicles. VEBAS uses a trust-based mechanism. This checking mechanism uses a combination of behavioral mechanisms and physical parameters such as velocity and acceleration to determine the authenticity of a message. However, VEBAS could be vulnerable since there is no mechanism the verify the correctness of the messages received from the neighbors.

The MisDis protocol [181] ensures accountability of vehicle behavior by recording all the (sent/received) messages for each vehicle peer in a secure log. Any vehicle can request the secure log of another vehicle and independently determine deviation from expected behavior. This protocol, however, requires strong identification and authentication mechanisms, and there is no discussion about how vehicle privacy is preserved. Also, the authors do not provide any performance evaluation of the proposed method.

Lo et al. [115] propose a plausibility validation network (PVN) to protect the V2X applications from false data injection attacks (called illusion attacks) where an attacker can indirectly manipulate messages (e.g., through sensor manipulation). The idea is to use a rule database (e.g., a database of rules specifies whether given information should be considered valid or not) and a checking module that checks the plausibility of the received messages. Each message is evaluated with respect to its type (accident report,

generic road condition), and the corresponding predefined rule set is retrieved from the rule database to check the value of the message element fields (e.g., timestamp, velocity). For instance, the plausibility of the timestamp field is checked by determining the minimum and maximum bounds. A limitation of this approach is that since the rule database is shared, a malicious vehicle can generate valid messages to avoid detection.

### 5.3.6 Location and GPS Signal Verification

Researchers used different techniques to predict the position and behavior of vehicles (e.g., whether they follow an expected pattern) in order to identify malicious vehicles. One idea is to verify node positions using two verifiers [172]: acceptors (distributed over the region) and rejecters (placed around acceptors in a circular fashion) – say for a given region, by using multiple RSUs (rejectors) surrounding one (center) RSU (acceptor). If the message is first received by the acceptors, then they will verify that the vehicle is within the region. However, a malicious vehicle can spoof its location when it resides within the region since the protocol does not verify the exact location of the nodes.

There exist mechanisms [89] to verify transmitted CAMs by analyzing the sequence of messages (e.g., to find the trajectory of each vehicle). By tracking a vehicle (say by using a Kalman filter5), the receiver can verify the location contained within each CAM. The idea is extended to applications where the accuracy of the Kalman filter is poor (e.g., for special maneuvers or lane changes scenarios). A signature-based scheme [31] Based on a plausibility checking is proposed where each vehicle is modeled as differently sized (and nested) rectangles – intersecting rectangles that belong to different vehicles indicate false position information. Since the readings from positioning systems (i.e., GPS) could be inaccurate, the probability of intersections is calculated by intrusion certainty (based on the number of observed intersections) and trust values. When Vj intersects with another neighbor and the difference between trust levels of both vehicles is higher than a predefined threshold, then the less trustworthy vehicle is considered to be malicious. While this method can detect false positions despite GPS errors, an attacker with larger transmission ranges (compared to other vehicles) can bypass this mechanism.

Vehicle positions can be verified by physical properties such as Doppler speed measurements of the received signal [165]. The idea is to use the angle of arrival (AoA) and Doppler speed measurements. When this information is combined with the position information included in the message, the estimation error (calculated using an extended Kalman filter-based approach) should not diverge unless the vehicle misbehaves by transmitting false location information. Another approach to verify vehicle position is distance bounding [38] – a technique to estimate distance using physical characteristics such as the speed of light.

An attacker can send delayed responses to each RSU (e.g., by using directed antennas). An alternative trust-based position verification approach is proposed where a vehicle discards packets if the included position information is further than the predefined maximum acceptance range threshold. Since the recipient negatively weighs abnormal observations (e.g., the sender's trust level is more affected by abnormal observations), after sending one bogus information packet, a (malicious) vehicle is required to send correct information packets in order to regain its previous trust level.

There exist mechanisms to detect GPS spoofing by dead reckoning, e.g., where the current position is calculated by using a previously determined position and known (or estimated) speeds over elapsed time. While this method can detect spoofed GPS information, the calculated position is only an approximation. For details of GPS spoofing countermeasures and recent proposals, we refer the readers to further related work [33].

### 5.3.7 Reputation Analysis and Revocation

Researchers have also proposed mechanisms such as statistical analysis and explicit voting to decide the trustworthiness of the vehicles. Zaidi et al. [189] use statistical techniques to predict and explain the trends in traffic flow and determine whether or not a sender is malicious. An approach using Bayesian logic has been proposed to compute the 'probability of maliciousness' of a vehicle for a time t, given some observation Out. This scheme requires prior knowledge of the probability of reception of a particular message, and the authors do not specify how these conditional probabilities can be obtained for generic V2X use-cases. The authors propose to periodically exchange global trust values by adding the addition of new fields to the CAM messages. Besides, DENMs is used to dynamically calculate the trust for specific events (e.g., road hazards).

Raya et al. [138] proposed an entropy-based measurement with k- means clustering to detect which neighbor differentiates from other neighbors (e.g., a misbehaving vehicle). Vehicles exchange 'accusations' about potential attackers, and the malicious vehicle can be evicted temporarily (by revoking its certificate).

Zhuo et al. [191] proposed a cooperative local and global eviction mechanism to remove misbehaving vehicles. The basic idea is that if a vehicle can detect bogus messages, it will broadcast a message accusing the potential attacker vehicle. In contrast to other work, a vehicle can use pseudonyms (i.e., to protect privacy) and can re-join the network after a successful accusation. Limitations of exiting revocation schemes include [112]:

- They assume an honest local majority, and if an attacker manages to create a local majority (that is the case of Sybil attacks) then it is possible to create false accusations (and falsely remove honest vehicles from the network) and
- When pseudonyms are used (i.e., to protect user privacy), an attacker can use multiple pseudonyms in parallel to create a local majority. For voting-based schemes, researchers, therefore, suggest not to use multiple pseudonyms in parallel (i.e., they should be prevented by the underlying pseudonym mechanism).

In the Table.5.1 we classify several proposed solutions according to some criterion that we considered important to compare with this contributions.

| | | Centralised Architecture | Decentralised architecture | V2X Communications | Blockchain | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | All nodes centric | OBU centric | RSU centric | RCA centric |
| Clustring | [19] [104] | | X | | X | | | |
| | [97] | | X | | | | | |
| | [95] | | X | X | | X | | |
| | [49] | X | | X | | | | |
| | [145] [113] [141] | | X | X | | | | |
| Pseudonym changing and Credential Management | [96] [135] [20] | X | | X | | | | |
| | [150] | | X | | | | | X |
| | [182] | | X | X | | X | | |
| Certificat revocation | [101] [98] | | X | X | | | | |
| | [79] [20] | X | | X | | | | |
| | [122] | | X | X | | X | X | X |
| Detection of position-related attacks | [186] [175] [146] [161] | | X | X | | | | |
| | [184] | | X | X | | X | X | X |

**Table 5.1** Table of contributions in the various fields related to our work

## 5.4 Proposed Real Time Revocation Framework

In this section, 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.

| Symbols | | | |
|---|---|---|---|
| $G_{com}$ | List of community members | $Clus_{for}$ | The cluster formation message |
| $\Delta_v$ | Relative velocity between vehicles | $\Delta_D$ | 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 |

**Table 5.2** Abbreviations and symbols

### 5.4.1 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 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 $i = 1, ..., N$, 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., $V = N_i : i = 1, ..., N$ 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.

Data sharing is done based on information shared between entities each node that has received the same message "based on the hash" must appear to give its opinion on the communication maintained with this node

Since vehicles are resource-limited devices, the problems of building a distributed network structure have been examined in [73]. In this work, we propose to use a chain made up of only limited communi-

ties. 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.

### 5.4.2 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.

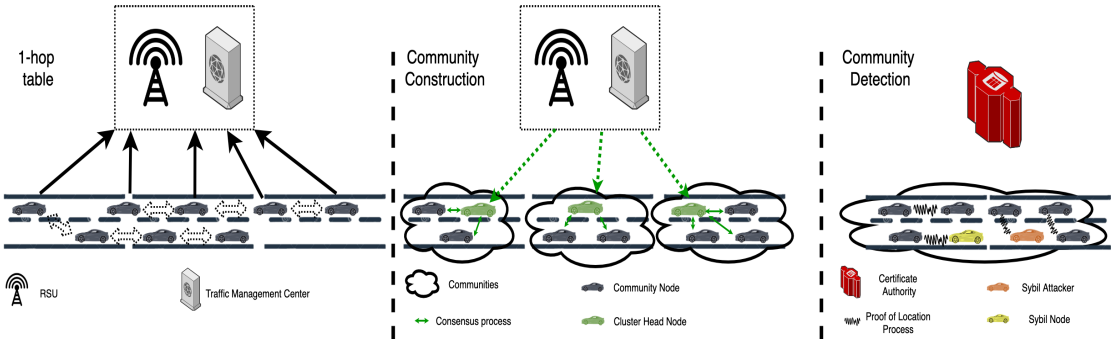



**Fig. 5.1** The three main steps in community process; 1-Hop table, Community Construction, Community Detection

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.

#### *5.4.2.1One-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 $G \subset NS$.

#### *5.4.2.2Cluster 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. $Hd_{Vi} = Hd_{Vj}$ 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 $T_{th}$:

$$T_{th} = \frac{(R - (\frac{1}{QT_{max}}))}{VT} \tag{5.1}$$

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.

$$T_{life} = \overline{T_{link}} = \sum_{j=0}^{N_i} \frac{(R - \overline{\Delta D_{ij}})}{\overline{\Delta v_{ij}} * N_i} \leq T_{th} \tag{5.2}$$

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.

The selection of the cluster head will be based on the metric $T_{life}$ in Eq(5.2). 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.

#### *5.4.2.3Cluster formation*

When a vehicle $V_j$ receives a cluster formation message from $TMC$ Eq(5.3), it immediately sends a $ReqJoin = Sig_{V_j}(\left\{Clus_{for}\right)\}$ 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.

$$Clus_{for} = \left\{Sig_{TMC}(ID_{CH}, ID_{Clus})\right\} \tag{5.3}$$

#### *5.4.2.4Pseudonym 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 [66]. 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 [53]. 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 [141] 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 [151], 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.

#### *5.4.2.5Isolated 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 [72], 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) [69]. 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."

### 5.4.3 Community detection

#### *5.4.3.1Proof-of-Location Consensus*

Misbehavior detection in V2X communication has been well studied (see Section **??**). 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.

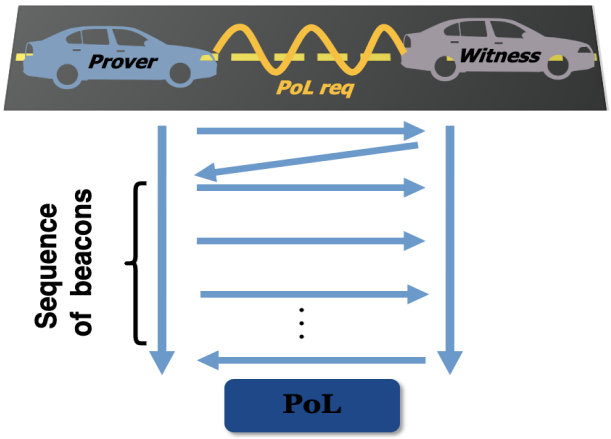



**Fig. 5.2** The Proof-of-Location process between the prover and its witness

In our previous work [54], 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.5.2, the N value should be estimated based on their relative velocity. the PoL process is detailed in [54].

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.

**Algorithm 2:** 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**
    **end**
  **end**
  **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**
    **end**
  **end**
  $TMC$ 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**
  **end**
  **return** $G_{com}$
**End Function**

- 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.

$$PoL = (PoL_{Acc}, PoL_{rate}, Pos_p, t_w, Cer_w, \\ S_w[PoLreq, t_w, Kp_p]) \tag{5.4}$$

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

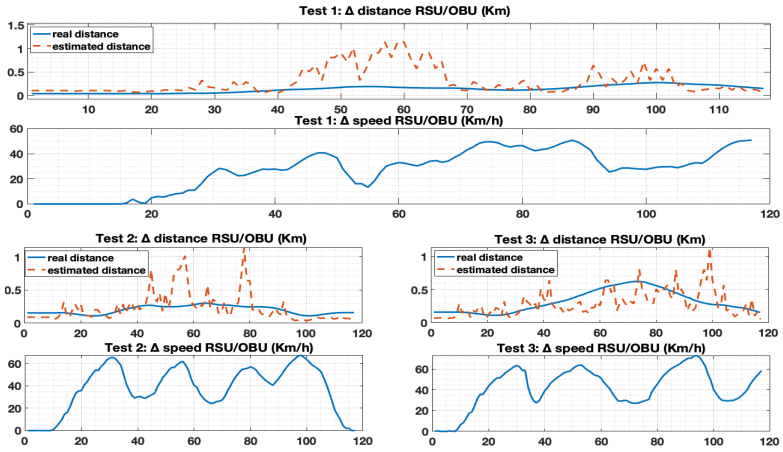



**Fig. 5.3** The Proof-of-Location process between the prover and its witness

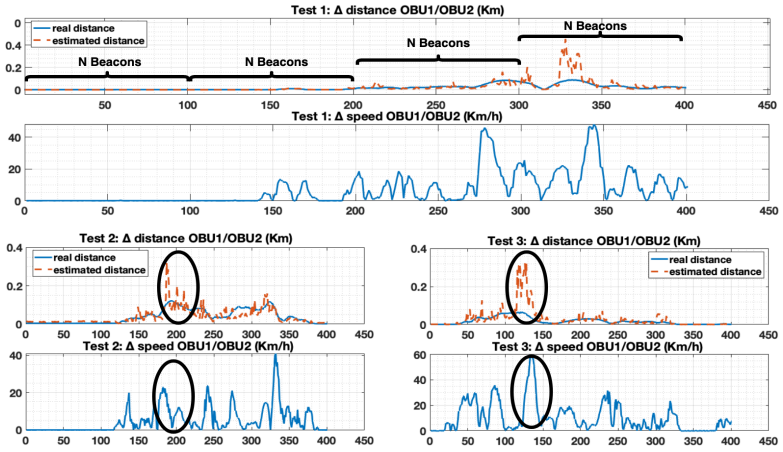



**Fig. 5.4** The Proof-of-Location process between the prover and its witness

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 [54]. The PoL accuracy is inversely related to the velocity, as shown in Fig. 5.3 and Fig. 5.4, 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. There-

| | | Test 1 | Test 2 | Test 3 |
|---|---|---|---|---|
| I2V modeI2V modeI2V modept< -I2V modept> | Velocity (km/h) | 31.60 | 43.11 | 46.08 |
| | $ACC$ | 41.10% | 56.75% | 48.07% |
| V2V modeV2V modeV2V modept< -V2V modept> | Velocity (km/h) | 12.27 | 8.56 | 15.33 |
| | $ACC$ | 72.47% | 75.44% | 67.12% |

**Table 5.3**

fore, 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.

#### *5.4.3.2Community Processing*

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

$$r_t(l) = \int_t^{t+T_{th}} f(T)dt \tag{5.5}$$

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 5.4.2), each vehicle has to calculate the vector of link reliability with all surrounding vehicles using Eq(5.5). The reliability level of $N$ surrounding vehicles will be included in vector A:

$$A = \begin{pmatrix} r_{ID_1} \\ r_{ID_2} \\ \cdots \\ r_{ID_n} \end{pmatrix} \tag{5.6}$$

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.

### 5.4.4 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(5.4) 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 [97]. In the literature [22], 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:

$$Z = [X_1, X_2, X_3 ... X_n] \tag{5.7}$$

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 [142]), generating an extra secret for each certificate.

### 5.4.5 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.5.5, 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.

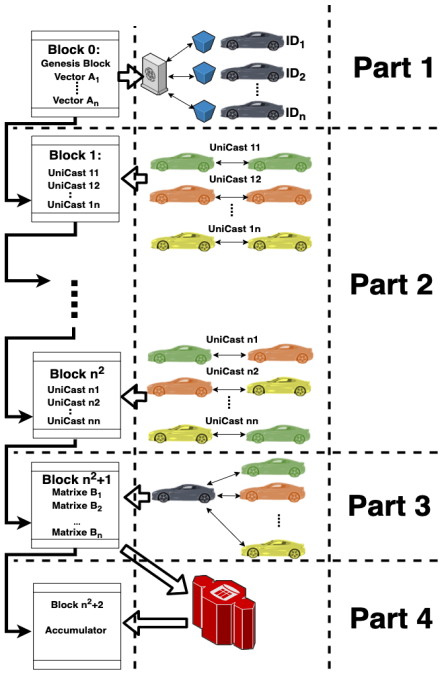



**Fig. 5.5** Blockchain's global parts

*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.5.4 shows the composition of transactions.

**Table 5.4** 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 |

### 5.4.6 Smart Contract

Once the vehicle get into the community it should get the genesis Block that contains the Smart Contract. As shown in Fig.5.6 our smart contract is considered as a finit state machine, where every part is a vehicle state.

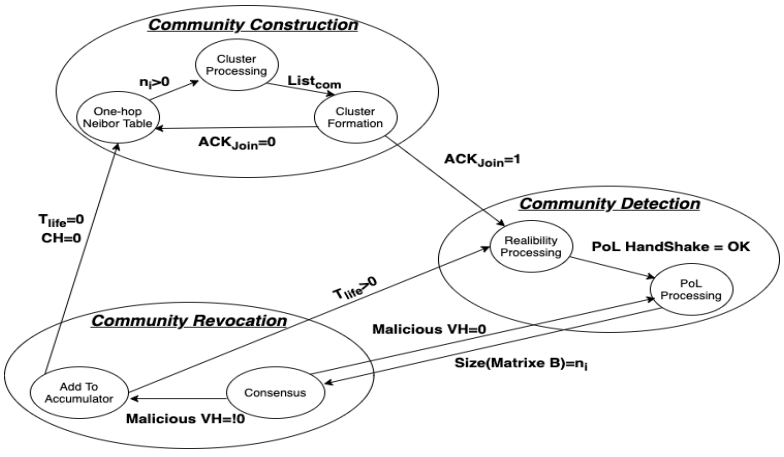



**Fig. 5.6** Communities steps of an algorithm state machine

### 5.4.7 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 [105].

*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.

## 5.5 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.

### 5.5.1 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.5.5 Framework, we used our revocation framework to evaluate its performances.

| **Communication simulator** | OMNET ++ |
|---|---|
| Number of node | ***1683*** |
| Application | Veins- VANET [159] |
| | Aretry Framework [143] |
| | 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 |

**Table 5.5** Simulation Parameters

### 5.5.2 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.5.7 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 rates. The Fig.7.15 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.5.9, in presenting the average of all accuracy reports of individual vehicles, shows that accuracy is neither constant nor stable.

The Fig.5.10 shows the accuracy of our algorithm.

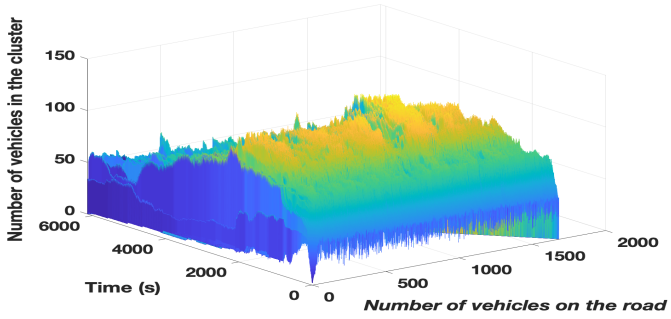



**Fig. 5.7** Number of vehicles in each cluster vs time and traffic

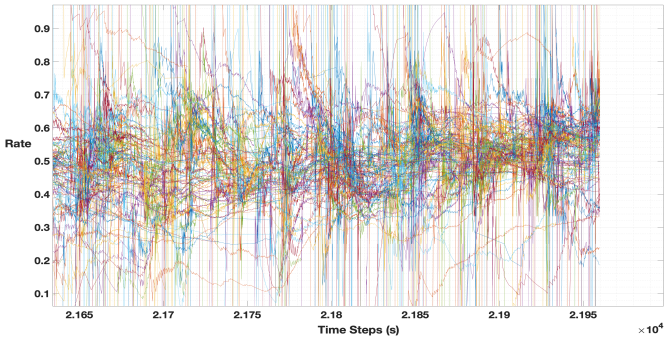



**Fig. 5.8** All vehicles accuracy rates evolution

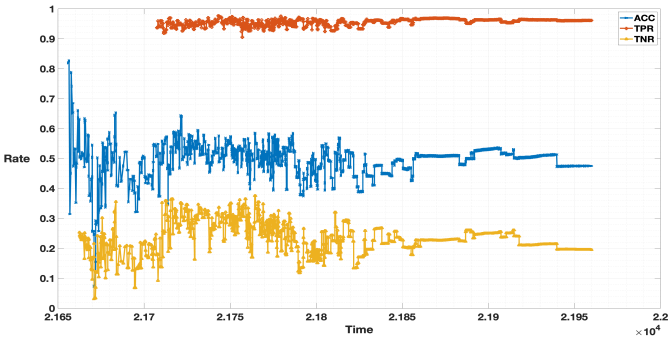



**Fig. 5.9** The mean of single accuracy rate with true positives and negatives rates

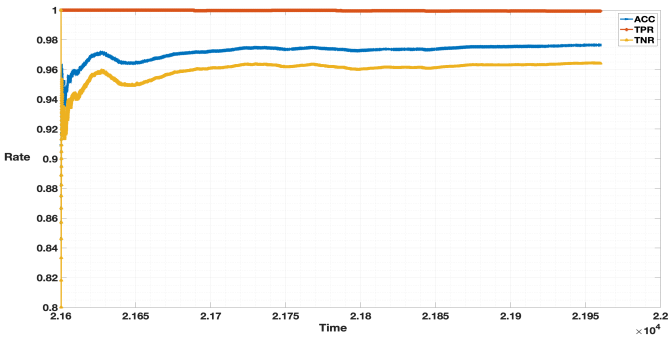



**Fig. 5.10** The community accuracy with the True Positives and Negatives rates

## 5.6 Discussion

The range of communication is linked to detection accuracy. The Indicator 3 -I3- of our algorithm in section 5.4.3 could be based on several parameters: Velocity, distance, direction, yaw-rate, and weather conditions. It turned out from our previous work [54] 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 [**?** ]. Although the date set shows slight variation, all the fake messages are 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.

## 5.7 Conclusion

This chapter 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 the context of 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 helps implement blockchain technology in vehicular communication and adds value to cyber-physical security.

CHAPTER 6

# Novel Centralized Pseudonym Changing Scheme for Location Privacy in V2X communication

## 6.1 Introduction

The vehicular transport sector is frequently affected by issues, such as traffic congestion and accidents. It was thus essential to evolve a cooperative system between vehicles to minimize accidents and permit vehicles and road managers to share information freely. This new ecosystem uses different communication ways as Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to Anything (V2X).

Recently technologies have provided communication models that can be used by vehicles in different application contexts. For example, the ETSI (European Telecommunications Standards Institute) has standardized the ITS-G5 standard, using the IEEE 802.11p standard. It is based on 10 MHz bandwidth channels in the 5.9 GHz band (5.850-5.925GHz)[62]. ITS-G5 is a suitable standard for Cooperative-Intelligent Transport Systems (C-ITS) applications for the following reasons: Low latency communications; No infrastructure requirement; Reliable communications and Communications range 200-1000m [103].

The main components in the V2X ecosystem are On-Board Units (OBUs), which operate in vehicles, and the Road Side Units (RSUs), which act as the infrastructure by broadcasting information in I2V mode. ITS-G5 technology enables vehicles to operate as an ad-hoc network on a V2V mode without the need for RSU intervention [70].

Therefore, it is mandatory to secure these wireless communications to ensure that all technologies meet security requirements [16]. Furthermore, safety should be particularly considered in connected autonomous vehicles, where a vulnerable system component can be exploited to cause dangerous consequences, such as injury or even loss of life.

For these reasons, several types of security architectures linked to V2X have been proposed. The current V2X security architecture is based on a centralized architecture where all vehicles are identified, authenticated, authorized, and connected through central cloud servers that use a Public Key Infrastructure (PKI) [70]. It should ensure the following security requirements: *Trust* of the provision to ITS stations of certificates allows them to affirm their permission to use the ITS system and use specific ITS services and applications. *Access Control* should be ensured by giving ITS stations cryptographically signed certificates of authorization, which allow them to use specific services or send specific information; *Confidentiality* of information transmitted in a unicast communication is protected by encryption of messages within an established security association; ***Privacy*** is based on the use of pseudonyms that can replace meaningful and traceable identifiers.

There is a compromise between the waste of certificates and the Sybil attack as explored by [173] since, on the side of the authority, we can not differentiate between the "honest" vehicles that only use the certificates excessively and the others that use the pool. Pseudonyms to run Sybil Attacks. This contribution focuses on improving the privacy of V2X communications by proposing a dynamically

adaptive system that allows certificate authorities to monitor the pseudonym-changing process. Our contribution allows the authorization authorities to anticipate users' needs in terms of confidentiality and to adapt the pool of pseudonyms to avoid both ends of the problem.

## 6.2 Problem Formulation

The changing pseudonyms scheme presents a significant trade-off. To ensure privacy, certificates must be periodically changed. However, utilizing numerous certificates, each valid for a short duration leads to certificate wastage and potential exploitation for Sybil attacks. Furthermore, including all valid device certificates on the Certificate Revocation List (CRL) results in a large and cumbersome list.

In light of these challenges, this paper seeks to address these issues by dynamically adapting the number of Pseudonym Certificates (PCs) assigned to each vehicle, based on authorization from the Authorities. This adaptive approach aims to regulate the problems associated with the Pool of PCs provided by the Authorization Authorities. By dynamically adjusting the number of PCs allocated to vehicles, we aim to mitigate certificate waste, prevent Sybil attacks, and reduce the size of the CRL, all while maintaining the necessary level of security and privacy in the changing pseudonyms scheme.

Our motivation is to achieve the following objectives in the realm of VANET privacy:

- Propose a context-adaptive and Authority-centric privacy scheme: We aim to develop a privacy scheme that adapts to the specific context of VANET, ensuring the protection of sensitive information while maintaining efficient communication. By employing an Authority-centric approach, we can establish a robust framework for privacy preservation.
- Design a Knapsack problem-based algorithm for trajectory combinations and users' traceability: We will devise an algorithm that leverages the Knapsack problem to efficiently combine trajectories while maintaining the traceability of users. This algorithm will enable effective route planning while considering privacy concerns, striking a balance between optimal navigation and preserving user anonymity.
- Evaluate real-life user privacy using OBUs from different countries: We will assess the privacy levels of actual users by analyzing data shared from On-Board Units (OBUs) developed by various countries, namely France, Germany, Holland, Norway, and Austria. This evaluation will provide insights into the effectiveness of privacy measures implemented in different regions and enable us to identify potential vulnerabilities or areas for improvement.

By accomplishing these objectives, we strive to enhance privacy protection in VANET, ensuring secure and confidential communication for drivers and minimizing the risks associated with information disclosure in vehicular networks.

## 6.3 Existing Solutions

### 6.3.1 Conventional security architecture

The security architecture for V2X is a Public Key Infrastructure (PKI) adapted to the context of C-ITS. It is a hierarchical architecture composed of different authorities. The Root Certificate Authority (RCA) acts at the top of the hierarchy of Certificate Authorities. It controls all the subordinate certification authorities and the final entities in its scale. A trusted certificate is provided to each last legitimate entity and may be revoked or blocked.

The C-ITS system is based on the provision of certificates and access control management [72]. The RCA manages the Certificate of Revocation List (CRL), and Certificate Trusted List (CTL). The RCA also manages two authorities: Enrollment Authority and the Authorization Authority.

*Enrollment Authority:* This authority provides Enrollment Certificates to ITS-S such as RSUs and OBUs. Each node has a unique long-term identifier, an agreement between the car manufacturers and the authorities where each identity is associated with a pair of cryptographic keys and a set of Node attributes. The attributes reflect the node's equipment's technical characteristics and its role in the system.

*Authorization Authority:* This authority provides short-term certificates, also known as Authorization Tickets, to all ITS stations (OBUs, RSUs, ...). The tickets are obtained based on key pairs generated by the OBU's HSM using its EC to authenticate with the AA. The AA signs each of the public keys and generates a set of Pseudonym Certificates (PC) for the station. Each PC contains information about the issuer CA as well as information specific to the OBU station.

According to the IEEE standard and European standard, ETSI [16][8][70], here is an overview of some functions that the C-ITS system offers:

- Secures the private keys corresponding to public keys via the hardware and software security modules implemented in OBUs;
- Logging actions (in centralized archives);
- Archiving certificates over time;
- Misbehavior detection and certificate revocation.

The global architecture is operated under the Security Credential Management System (SCMS) proposition explained by [39]. In addition to the certificates authorities, two more entities ensure the unlinkability of vehicles' identities and ensure their privacy:

*Linkage Authority (LA):* Generates pre-linkage values, forming linkage values in the certificates and supporting efficient revocation. There are two LAs in the SCMS, referred to as LA1 and LA2. The splitting prevents the operator of an LA from linking certificates belonging to a particular device. In Fig.6.1, the linkage process to get the misbehavior identity.

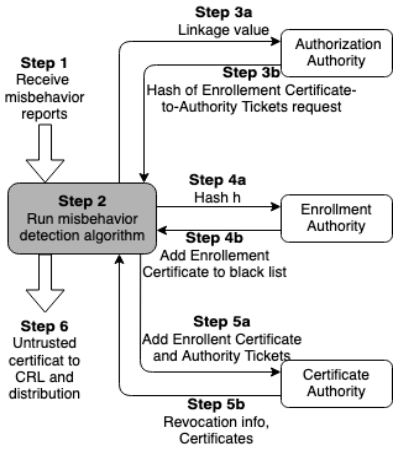



**Fig. 6.1** Reports of OBUs to misbehavior authority of malicious vehicles and the authorities' conducted process to the linkage of Authorization Tickets and their corresponding ECs and attributes to report them into the CRL

*Location Obscurer Proxy (LOP):* Hides the location of the requesting device by changing source addresses, thus preventing linking network addresses to locations.

### 6.3.2 Identifiers

There are many different addresses, IDs, or other identifying information scattered around the network layers.

- *GeoNetworking:* Each GN node is identified by [60], containing information about the ITS-S type (passenger car, cyclist, pedestrian, RSU, ...) and 48bit derived from the link-layer address. In the case of a pseudonym change, only the latter part is supposed to change. GN packets have a basic, a common, and an optional extended header. The basic header contains information like the packet's maximum lifetime and the remaining hop limit. This information is non-critical for identification.
- *Facilities Layer:* The Facilities layer introduces a StationID, an integer identifying the ITS system. The standard document already mentions that this ID may be a pseudonym.
- *IPv6:* While each IPv6-capable network interface can have multiple addresses, it has at least one link-local address with the interface ID (the lower 64bits) uniquely derived from its data-link layer address. The mapping of the IPv6 link-local address and GNADDR is straightforward, as both addresses are deterministically derived from the same link-layer address. Additionally to the IPv6 address, the IPv6 header can also contain a flow label which could lead to partial linkability of packets even after an address change: Although a flow shall be identified by the triplet of the flow label, source, and destination address, an equal flow label could indicate the resumption of a connection even after an address change.

### 6.3.3 Pseudonyms changes strategies

Pseudonym Certificates are stored and managed in pseudonym pools, with their corresponding private keys kept in the HSMs. To keep the privacy of vehicles and avoid tracking or linking their real identities to the used pseudonym certificates (PCs), the Authorisation Tickets are changed frequently according to various rules [66]. This ensures that each VC has precisely one key pair (own pseudonym and private key) active during each period. VCs cannot reuse the pseudonym once it has been changed, even if the PKI certificate has not yet expired.

The ETSI standard on trust and privacy management [72] mentions the goal of pseudonymity and unlinkability of ITS nodes and their messages as the way to achieve ITS privacy. This privacy goal is subdivided into two dimensions: The privacy of ITS registration and authorization shall be achieved by limiting the knowledge of a node's canonical (fixed) identifier to a limited number of authorities. Furthermore, the responsibility for verifying the validity of a canonical identifier is given to an Enrolment Authority (EA) and split from the authorization to services by the Authorization Authority (AA). These authorities are parts of the needed Public Key Infrastructure (PKI) and need to be operated in different control areas to achieve a surplus of privacy. During manufacture, the following data is to be stored in an ITS node using a physically secure process:

– a globally unique canonical identifier

– contact addresses + public keys of an EA and AA,

– a set of trusted EA and AA certificates

There needs to be some ambiguity regarding which node changed to which pseudonym, there shall be other nodes present within the reception range, coordination and frequency of change matter, and all identifiers need to be changed simultaneously with buffers being flushed or discarded. Finally, control metadata like sequence numbers in GN packets have to be reset as well.

The ETSI, ITS working group, gathers several concepts for pseudonym change strategies (PCS) in a technical report [66]: The parameters deciding a PCS (e.g., period or length) shall be randomized to prevent linkability by analyzing the periodicity of changes. After changing pseudonyms, random-length silent periods shall be abided in which nodes stop sending any packages. When using a vehicle-centric strategy, pseudonym change time, frequency, and duration of silent periods are influenced by the vehicle's mobility and trajectory to make linking pseudonyms based on broadcasted movement parameters harder. In the density-based approach, pseudonyms are changed only if enough other vehicles are around to avoid unnecessary unambiguous pseudonym changes. Mix-zones are geographical areas where no messages of location-aware services are exchanged. This concept is supposed to make the linkage of in-going and outgoing vehicles from the zone difficult. These zones are especially effective in high-density and high-fluctuation areas like intersections or parking spots. Vehicles could collaboratively change pseudonyms within these zones by announcing them via broadcast messages and then changing synchronously.

However, as stated in the report, the efficiency of that approach depends heavily on the density of the situation. A particular variant is cryptographic mix-zones: Within these zones with a size limited to the radio coverage of an RSU, no identifying data is sent in plaintext, but everything is encrypted with the same symmetric key provided by the RSU. Thus, it allows the usage of location-aware collision detection messages while preventing an outsider from eavesdropping without switching off essential safety features. An alternative to just changing from one pseudonym to the next from a node's internal storage is swapping pseudonyms randomly between nearby vehicles. We find this approach to be limited, though, by the inclusion of vehicle-specific data into messages and legal requirements demanding the possibility of an identity resolution for law enforcement.

The ETSI survey [66] also gives an overview of used strategies in existing standards or projects. These include some interesting further approaches: The SCOOP project proposes a timeslot-based round-robin pseudonym selection. The exciting thing about this is that using pseudonyms from the local Pool is explicitly allowed as the selection mechanism ensures they are not always reused in the same order. This is a practical approach against the problem of pseudonym refill (acquiring new pseudonyms) not always being possible.

The strategy proposed by the Car-2-Car Communication Consortium is dividing each trip into at least three segments: The first one from the start of the trip to a middle segment, the middle segment being familiar to several people and unassociated to specific origins and destinations, and the last segment to the intended destination of the trip. This shall achieve that locations significant to a user can neither be linked together nor the user, thus preventing individual movement profiles. Some safety requirements of the ETSI standard affect pseudonym change: In critical situations when a receiving station would need to take immediate action in response to received safety information, pseudonyms have to be locked. The reason behind that is that cooperation collision avoidance depends on all vehicles broadcasting their location and trajectory.

### 6.3.4 Tracking Attacks

We set the "unlinkability" as the concept that the greater the distance in time and space between two transmissions from the same device, the harder it is to determine that those two transmissions did come from the same device. Accordingly, vehicles in a silent period due to a pseudonym change would not be considered, and vehicles changing pseudonyms without a silent period could appear as duplicate or ghosting vehicles hindering collision evasion. Furthermore, recognizing such critical situations and initiating the pseudonym locking is done by the receiving ITS vehicle, which decreases the risk of an attacker trying to lock pseudonyms without a critical situation being present deliberately, as shown in figure 6.2.

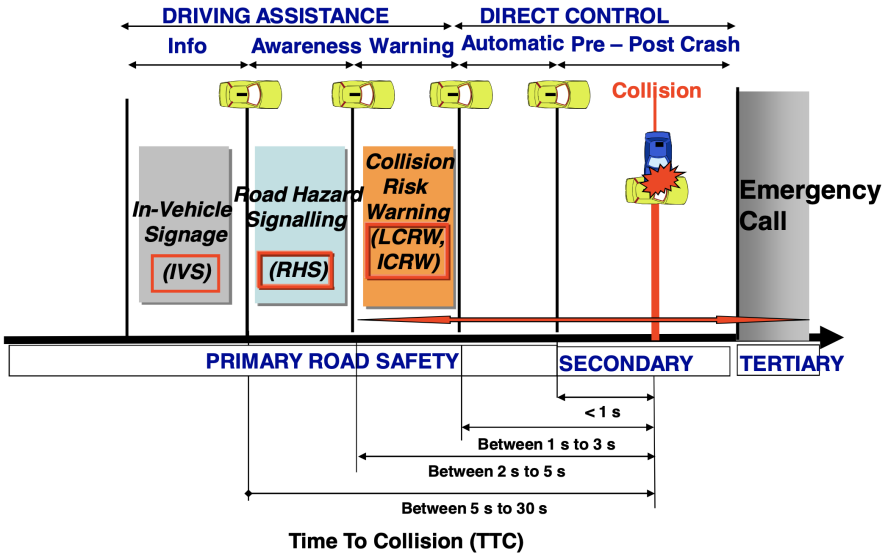



**Fig. 6.2** Applications being served by transmission showing the time to collision [69]

Therefore there is a real challenge in the trade-off between road safety and cybersecurity. Full message encryption does not meet temporary road safety requirements. The message linked to crash information must be accepted before the event to avoid a crash.

In the Likability process, the crucial metric is the period of silence after each pseudonym change as shown in the Fig.6.2 depending on the disseminated messages, as vehicles could not be silent in a period of TTC.

### 6.3.5 Pseudonym privacy

Security architecture is a security design. It addresses the necessities. Moreover, potential risks are involved in a specific environment and when and where to apply security controls. Standard provides detailed requirements on how a policy must be implemented. In VANET, many groups [39, 173] have presented the credential security architecture. The privacy and linkability of pseudonyms are essential issues in V2X communications. Researchers have contributed to resolving several issues for linkability. For example, Rebollo-Monedero et al. [140] suggested a trusted third-party system where privacy depends on collaboration among multiple untrusted users. This solution is related to a situation where the service provider is not trusted. In this way, the untrusted service provider will be unable to access the privacy information of any user. Yao et al. [185] proposed a novel lightweight, secure, and privacy-preserving pseudonym-changing scheme and proposed scheme an asynchronous key agreement.

## 6.4 The Proposed ML-Based Framework

### 6.4.1 Threat model

The confidentiality level of an individual's location is always relative to the control of an attacker trying to follow a person in the network.

In this article, we assume a passive attacker can listen to all messages sent over the network. Thus, what the attacker can gain from observing transmissions in the network is to trace the identity of the drivers.

The assumption of the attack model used is based on the attacker's strong ability to link an identity to a vehicle MAC address at the beginning of the node's lifetime. The individual remains anonymous when the departure has not been linked to an origin/destination pair.

The modeling of an attacker is linked to the tracking algorithm. Therefore, the learning of the attacker is highly dependent on the mobility used and the pseudonym-changing strategies used by the driver. If, for example, nodes do not change pseudonyms or drives in a very predictable way, the tracking algorithms will work much better.

Therefore for our calculations, we choose to use a probabilistic attacker model: Attacker strength is defined as the probability with which an attacker can follow a nickname exchange between two nodes. The entropy H for an attacker who cannot follow a pseudonym exchange for each individual in the network would then be zero.

The force attacker also affects the increased privacy level when a new location in the nickname pool becomes active, i.e., when all nodes start using new nicknames. If we assume that two nodes very close to each other could confuse an attacker by exchanging their nicknames (the extent being dependent on its strength), that attacker will also be confused when these two nodes simultaneously change nicknames. From this, it follows that the level of confusion is based on the number of candidates directly neighboring the node.

### 6.4.2 System model

Our system model is based on the network architecture proposed by the European committee [4], as illustrated in Fig.6.3. Privacy holds paramount importance in trust models, particularly in the context of this architecture. The unique aspect of this architecture lies in the connection between ITS-S nodes. Moreover, this configuration enables certificate authorities to receive and process messages disseminated across the network. By integrating privacy considerations into the trust models within this architecture, we can ensure the secure transmission and handling of messages while safeguarding sensitive information from unauthorized access or exposure.

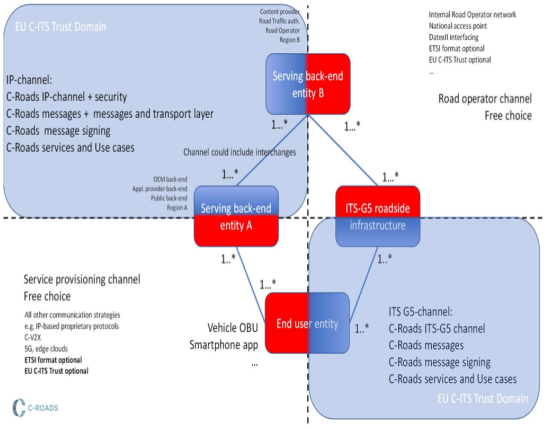



**Fig. 6.3** Overview of C-ITS communication [5]

Our solution aims to set up a scheme of pseudonym changing dynamically. Our system's first actors are the Authorization Authority, as it is the responsible entity for providing pseudonyms to the vehicles. This framework should optimize the size of PC Pools provided to VCs. In our proposition, we assume full connectivity between vehicles and the authorities. This proposed framework could be used as a backup to the conventional solutions to optimize resources and also helps to avoid some attacks such as the Sybil attack.

In order to give an adapted proposition of changing scheme, our solution is put in the shoes of the attacker by trying to track vehicles. It calculates their entropy (privacy metric explained in section 6.4.4) and gives a global PCs changes scheme.

### 6.4.3 Tracking Algorithm

The attacker is assumed to have access to all transiting messages in the network. Thus, our algorithm computes several informative characteristics of each communicating node to relate each MAC address to an Origin/Destination pair.

Our algorithm permits us to solve our problem in the way of the knapsack problem. It has all vehicles messages of a specific region as input and also a couple of O/D pairs.

The optimization target is to attribute each MAC address $m$ to an O/D pair. As shown in Figure 6.4, the output of our algorithm is the probabilities of $m$ MAC address to do the corresponding O/D trajectory.

We determine the best candidate for each O/D pair in real-time, as vehicles keep changing their pseudonyms and MAC addresses. Moreover, this algorithm permits to solve just a first step of the tracking problem, as it is based on the MAC address as an identity.

We formulate our Knapsack problem using the well-studied: Multiple Multidimensional Knapsack Problem (MMKP) [87, 157].

The weights $w_{ij}^k$ correspond to the distance of each vehicle's trajectory to go to each destination pair, and the profits $p_{ij}^k$ correspond to the probability of the set of trajectories corresponding to different MAC addresses to do the $O/D$ pair $k$. In this problem, we want to maximize the combination of the probabilities of several paths corresponding to different mac addresses. respecting the capacity of each $O/D$ pair

$$\begin{cases} Maximize \sum_{i=1}^{m} \sum_{j=1}^{n} p_{ij}^k x_{ij}^k, for\ k = 1,...,s \\ Subject\ to \sum_{j=1}^{n} w_{ij}^k x_{ij}^k \leq c_k, for\ i = 1,..,m, and\ j = 1,..,n \\ \prod_{p}^{q} x_{ij} = 1, for\ i = 1,2,...,m \end{cases} \tag{6.1}$$

$x_{ij}$ : Set of trajectories
$w_{ij}$ : The weight of the $j^{th}$ trajectory correspond to $k^{th}$ O/D pair
$p_{ij}$ : The profit of the $i^{th}$ trajectory in the $j^{th}$ MAC address
in terms of probability
$c_j$ : The capacity constraint of every $k^{th}$ combination
to correspond to the right O/D pair

We first calculate the matched combination to the O/D pair and then calculate each combination probability using the algorithm 3. As shown in Fig.6.4 The algorithm aims to minimize the gap between every identity Origin/destination ($P_s(i)$/$P_e(i)$) and the $O/D$ pair.

The output of this algorithm is the Matrix E given as the following :

$$E = \begin{pmatrix} Tr_1 \\ Tr_2 \\ \vdots \\ Tr_n \end{pmatrix} \begin{pmatrix} ID_{MAC}(3) & ID_{MAC}(1) & 0 & 0 & \cdots \\ ID_{MAC}(4) & ID_{MAC}(5) & ID_{MAC}(7) & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ ID_{MAC}(12) & ID_{MAC}(2) & ID_{MAC}(9) & 0 & \cdots \end{pmatrix} \tag{6.2}$$

We calculate then the gap between IDs ($ID_{MAC}$) in each $Tr$. these gaps could be considered the period of silence used by vehicles to transit from a pseudonym to another. The silence period could be estimated by estimating the number of disseminated security messages, as seen in section 6.3.4 and

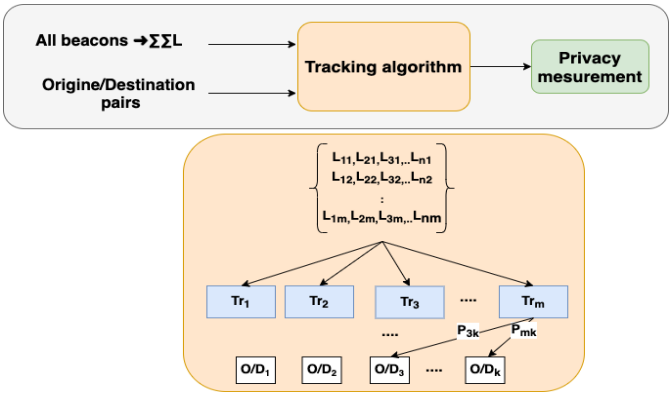



**Fig. 6.4** Tracking algorithm steps

Fig.6.2 the silence period is linked to the TTC period as the OBU could not change the pseudonym or make a silence period in TTC. The dissemination of C-ITS security messages in each geographical zone depends on the C-ITS transmission range ($R$) and, therefore, nodes' inter-distances. We use the truncated exponential distribution to estimate the number of vehicles with inter-distances $0 < X_R < R$ in a given segment:

$$E[X_R] = E[x|x < R] = \frac{\int_0^R \mu x e^{-\mu x} dx}{1 - e^{-\mu R}} \times \frac{1}{\phi} = \frac{1 - e^{-\mu R}(\mu R + 1)}{\mu(1 - e^{-\mu x})} \times \frac{1}{\phi} \tag{6.3}$$

Where $\mu$ is the inter-distance distribution parameter, and $\phi$ is the ratio of security messages upon all disseminated messages.

The probability of silent period is given by:

$$\delta_s = argminPr(E[X_R]) \tag{6.4}$$

### 6.4.4 The measurement model

The metric that is used to quantify location privacy in V2X systems. The level of privacy is quantified based on the uncertainty about that user. In [121] and [58] introduced the method calculation of the privacy metric based on the entropy of exchanged information. In this second part of our framework, we use the results of our Knapsack Algorithm as input to calculate the privacy of each vehicle.

We calculate the confidentiality of the geographical position of each person. In order to prove the traceability of a vehicle, it is necessary to ensure that the person corresponds to the vehicle which served the $O/D$ pair (Origin/Destination).

We give the mathematical model inspired from [58], we can model the vehicular communications as a weighted directed graph $G = (V, E, p)$.

G has several unique properties. G contains all information relative to its trajectory, and vertices in G are connected with directed edges. The probability distributions on the edges model depend on the adversary's knowledge of the users and their movements in the system from the previous algorithm. Moreover, the sum of the probabilities on outgoing edges from a vertex is defined $o \in O$ or $d \in D$ to be 1, $\sum_{k=1}^{m} p(i_j, o_k) = 1$,$\sum_{k=1}^{m} p(o_j, d_k) = 1$,$\sum_{k=1}^{n} p(d_j, i_k) = 1$.

In order to determine the probability distributions and quantify the privacy in the measurement model, we use the information entropy developed by Shannon [153]. We extract the entropy based on the probability distribution, which represents the quantitative measure of information content and uncertainty. Entropy has been accepted as an applicable measure in the privacy research community [58, 120, 132].

**Algorithm 3:** Algorithm of Community construction

**Input:** $ID_{MAC}[]; O/Dpair$
**Output:** $H$
**Function** `KnapSack linking(`$ID_{MAC}[]$`; O/D pair)`**:**
s← $size(ID_{MAC})$;
**while** $i > S$ **do**
VAR← $ID_{MAC}(i)$;
ID$_{MAC}$ ← $\forall ID_{MAC} \setminus \{ID_{MAC}(i)\}$;
i← $i - 1$;
P$_s$ ← $Pos_{start}(VAR)$; $P_e$ ← $Pos_{end}(VAR)$;
D$_{start/O}$ ← $distance(P_s, O)$;
D$_{end/D}$ ← $distance(P_e, D)$;
**if** $D_{start/O} > 0.1km$ **then**
**for** *j<S* **do**
$dis$← $distance(P_s, Pos_{end}(ID_{MAC}(j)))$
**if** $dis < D_{start/O}$ **then**
$ID_{MAC} \leftarrow \forall ID_{MAC} \setminus \{ID_{MAC}(j)\}$;
$ID_{MAC} \leftarrow add(ID_{MAC} + VAR)$;
**end**
**end**
**end**
**if** $D_{end/D} > 0.1km$ **then**
**for** *j<S* **do**
$dis$← $distance(P_e, Pos_{start}(ID_{MAC}(j)))$
**if** *dis* < $D_{end/D}$ **then**
$ID_{MAC} \leftarrow \forall ID_{MAC} \setminus \{ID_{MAC}(j)\}$;
$ID_{MAC} \leftarrow add(VAR + ID_{MAC})$;
**end**
**end**
**end**
**if** $D_{start/O} > 0.1km$ *and* $D_{end/D} > 0.1km$ **then**
$E$← $add(VAR)$
**end**

***return*** $NS_i, n_i$
***End Function***

However, the main challenge here is to rely on the entropy calculation to give an optimal pattern of change of pseudonyms. By definition, for a probability distribution with values $p_1, \cdots, p_n$, the entropy is

$$H = -\sum p_i log(p_i)$$

where $p_i$ is the $i^{th}$ element of the probability distribution. $H$ is the balance of information measure and uncertainty related to the probability distribution. High entropy means an increase in uncertainty and, therefore, a higher level of privacy. The entropy is maximal if the probability values are equal. In order to calculate entropy, we are interested in the source of the information that the adversary captures. For example, we are interested in information linking individuals to their geographical movements to determine who moves from where to where.

For non-zero probabilities, the computation of entropy for $p_i = 0$ means that there is no uncertainty and that the sum of the probability distribution must be equal to 1. Therefore, we compute the entropy for a specific individual as :

$$H(i_s) = -\sum_{j=1}^{m}\sum_{k=1}^{m}\hat{p}_{jk}log(\hat{p}_{jk}) \tag{6.5}$$

where $\hat{p}_{jk}$ is the probability of traveling from $o_j$ to $d_k$
The values of $p\hat{}jk$ is given as

$$\hat{p}_{jk} = \frac{p(i_s, o_j)p(o_j, d_k)p(d_k, i_s)}{\sum_{j=1}^{m}\sum_{k=1}^{m}p(i_s, o_j)p(o_j, d_k)p(d_k, i_s)} \tag{6.6}$$

The maximum entropy for an identity depends on the number of possible trajectories.

### 6.4.5 Dynamic Pseudonym Change

After identifying the level of privacy of each vehicle, the Authorization Authority proceeds to the clustering model (K-Means or others) based on vehicles information and the results obtained by the previous algorithm. The AA classifies vehicles into three categories as shown in Fig. 6.5, these categories represent vehicles in a definite range of privacy levels. Therefore, the AA will adapt the Pseudonym-Changing scheme proposal and the number of PCs in the Pools. The latter could be personalized for each vehicle, depending on the route it usually takes.

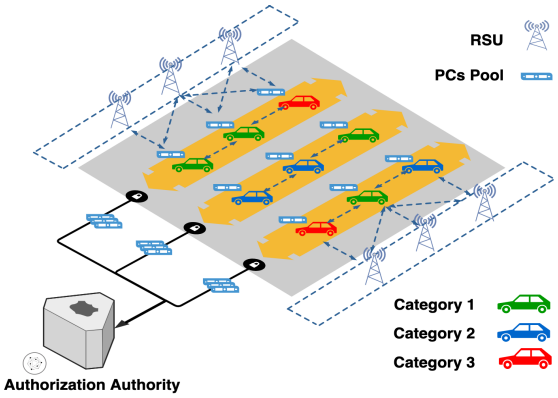



**Fig. 6.5** The authorization authority adapts the pseudonym pools send to each privacy category

## 6.5 Performance Evaluation

We tested the performance of our solution via data collected from real-life tests in the European project InterCor [11]. We have analyzed the raw data using Wireshark. We have implemented and tested our algorithm using Matlab tool.

### 6.5.1 Mobility Model

This scenario is based on the actual data obtained during the TestFest in Holland. Using a sniffer, we captured the messages sent by all the surrounding vehicles in addition to PCAP files received from the other participants. Using this, we have reverse engineering on the identity of each vehicle. Finally, we applied our solution to identify each vehicle and calculate its privacy level. These tests aim to test interoperability between the European partners. For all the test cases, vehicles have the same trajectory using one origin/destination pair. The test site corresponds to the start and arrival points.

### 6.5.2 Data Analysis

In Fig.6.6 we illustrate all the sniffed MAC addresses in their locations. All figures show the positions of each captured MAC address, each of the five figures represents half a day of tests. We notice *Test 2* have represented the peak of the participation of tester vehicles, as we received a more significant number of MAC address.

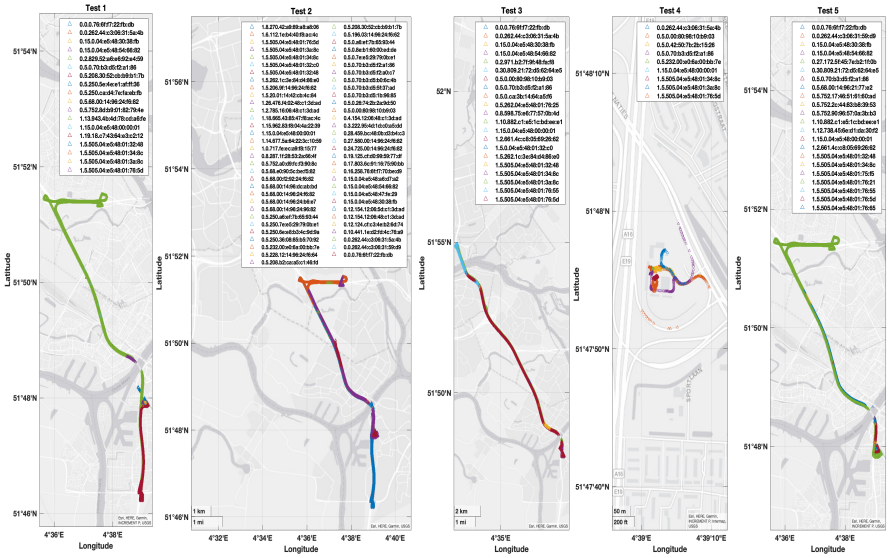



**Fig. 6.6** Applications being served by transmission showing the time to collision

In Table 6.1 we detail one of the first captions tests. The table gives information about the first day of tests. All the information given in this table is based on the received messages. We have calculated the distance traveled and the distance between Origin (travel start point) and destination (Travel endpoint). We also give the different Station IDs used during the travel and the type of messages sent. The IVI message is sent only by RSUs.

| *Test 1* | | | | | | |
|---|---|---|---|---|---|---|
| **Adresse Mac** | **Distance Orig/dist** | **Global distance** | **Nbr** | **StationID** | **Nbr messages** | **Messages** |
| 0.0.0.76:6f:f7:22:fb:db | 94.5262534395616 | 5184.53670513403 | 2 | 9819 | 56 | CAM |
| | | | | 1018 | 2 | DENM |
| 0.0.262.44:c3:06:31:5a:4b | 41.1098151351352 | 4716.54672185718 | 1 | 103897675 | 102 | CAM |
| 0.15.0.04:e5:48:30:38:fb | 0 | 19600.6637273890 | | 1003 | 952 | IVI,DENM |
| 0.15.0.04:e5:48:54:66:82 | 0 | 0 | 2 | 1003,1004 | 402 | IVI,DENM |
| 0.2.829.52:a6:e6:92:e4:59 | 51.2106199650485 | 57523.9932600751 | 1 | 3693631938 | 2109 | CAM |
| 0.5.0.70:b3:d5:f2:a1:86 | 124.131253528893 | 32463.0307367782 | 1 | 168084 | 1025 | CAM |
| 0.5.208.30:52:cb:b9:b1:7b | 61.9013067269062 | 2068.51465404507 | 1 | 1 | 180 | CAM |
| 0.5.250.5e:4e:e1:af:ff:36 | 152.129850286947 | 14238.6524742869 | 1 | 10127 | 6793 | CAM |
| 0.5.250.ca:d4:7e:fa:eb:fb | 159.748513111642 | 2519.89664488219 | 1 | 10127 | 2355 | CAM |
| 0.5.68.00:14:96:24:f6:82 | 75.5658688994478 | 23408.7608841248 | 1 | 2519004802 | 424 | CAM |
| 0.5.752.8d:b9:01:82:79:4e | 77.1344729073641 | 2825.36540019835 | 2 | 8666661. 8666662 | 92 | CAM |
| 1.13.943.4b:4d:78:cd:a6:fe | 50.9554171504651 | 402364.188337610 | 1 | 81449815 | 6406 | CAM |
| 1.15.0.04:e5:48:00:00:01 | 0 | 22262.5490878897 | 3 | 1018. 1015. 1014 | 3150 | IVI,DENM |
| 1.19.18.c7:43:64:e3:c2:12 | 129.128767728228 | 149748.174577024 | 1 | 3843896860 | 2240 | CAM |
| 1.5.505.04:e5:48:01:32:48 | 34.7012165577393 | 14558.6035522886 | 1 | 302050072 | 276 | CAM |
| 1.5.505.04:e5:48:01:34:8c | 96.2617231170404 | 2627.46156317316 | 1 | 302052140 | 107 | CAM |
| 1.5.505.04:e5:48:01:3a:8c | 79.2993996092281 | 2508.76506186629 | 1 | 302058140 | 26 | CAM |
| 1.5.505.04:e5:48:01:76:5d | 45.9832661472935 | 12985.5518446199 | 1 | 302118093 | 283 | CAM |

**Table 6.1** Test 1's details of the analyzed data from Wireshark tool

In Fig. 6.7 each box represents the variation of steps distance between all received messages from each Mac address in the first session of tests. This metric is very useful for our tracking algorithm.

In order to apply our algorithm, we have taken the second set of data (Test 2) as a case study. Our algorithm analyzed all cases based on the different metrics and information in Table 6.1. We have calculated their probabilities and their privacy entropy in order to estimate the identities as seen in section **??**.

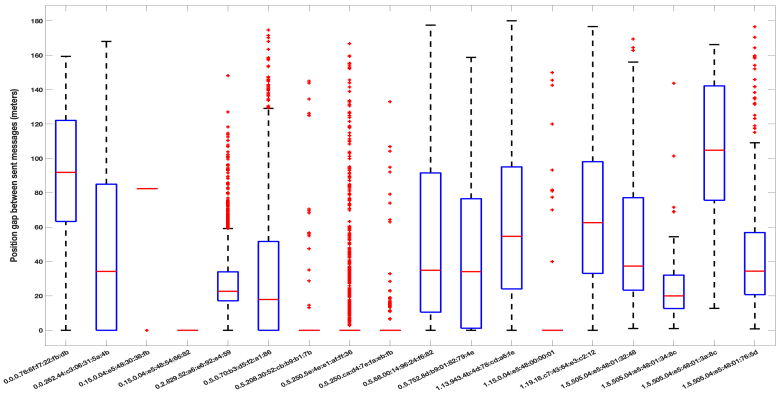



**Fig. 6.7** Representation of all steps distance between the received messages in the first tests

This analysis gave place to the three clusters. All the explanations are based on the assumptions of the attacker model in Section 6.4.1.

*Cluster 1:* It is a trivial case for an attacker because even with changing the pseudonym certificate and the StationID, the attacker could quickly identify users using the same MAC address for all their journeys. Fig. 6.8 shows two cases from this cluster.

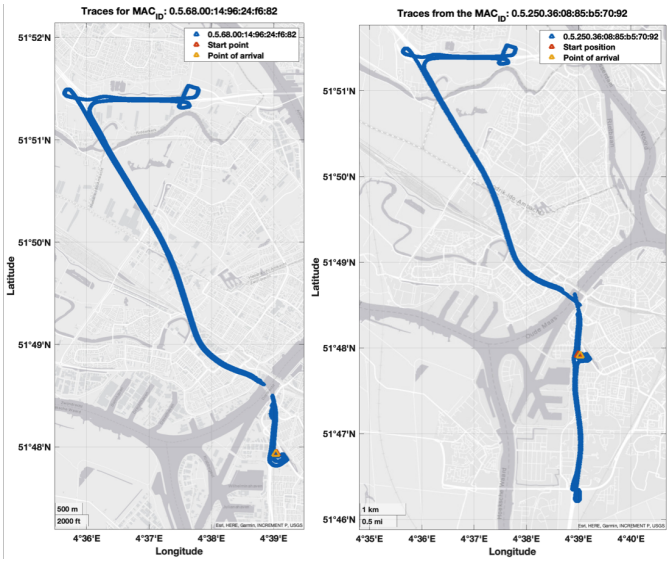



**Fig. 6.8** The first case

*Cluster 2*: In this case, our algorithm could successfully link two different MAC addresses to a single identity that could have done the O/D trajectory. As there is a period of silence in the changing pseudonym strategies, it decreases the truth's probability. In the Fig 6.9 we give indications of different assumed steps that the OBU could have done: (1): is the starting point of the driver's ($i_x$) journey. (2): The point that $i_x$ decided to change its pseudonym; (3): represents the silent period; (4): the starting point with the new $ID_{MAC}$ which ended in the Point of Arrival (Destination-D).

*Cluster 3*: This case is considered as the more secure case that could not be identified or linked. In Fig. 6.10 our algorithm could not link the MAC addresses, which means that the users have different Pseudonym-changing strategies.

Fig.6.11 shows the results of clustering of all the MAC addresses captured for the five tests according to several criteria taken into consideration by our algorithm to classify the privacy. In Fig.6.12, we illustrate the ROC diagram of our algorithm performance in terms of precision.

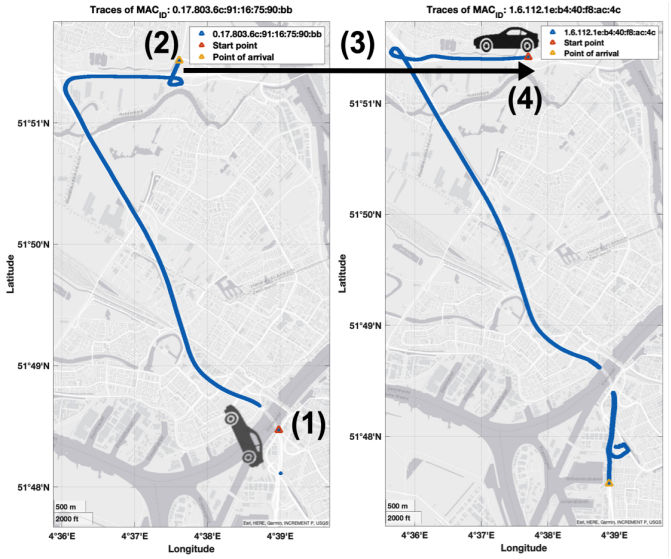



**Fig. 6.9** The first case

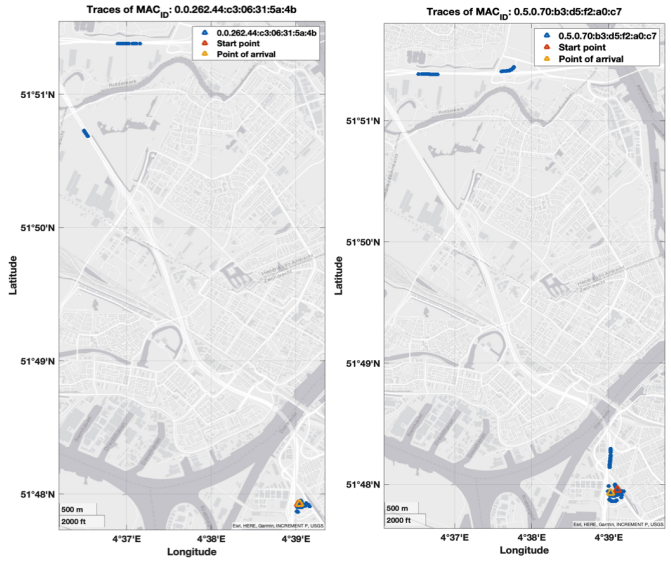



**Fig. 6.10** The first case

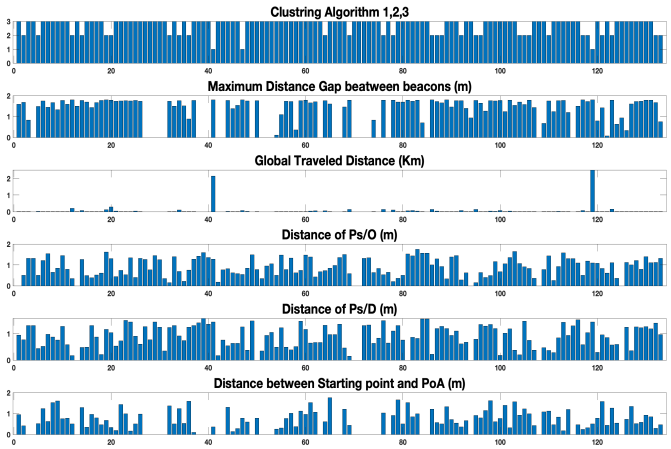



**Fig. 6.11** The first case

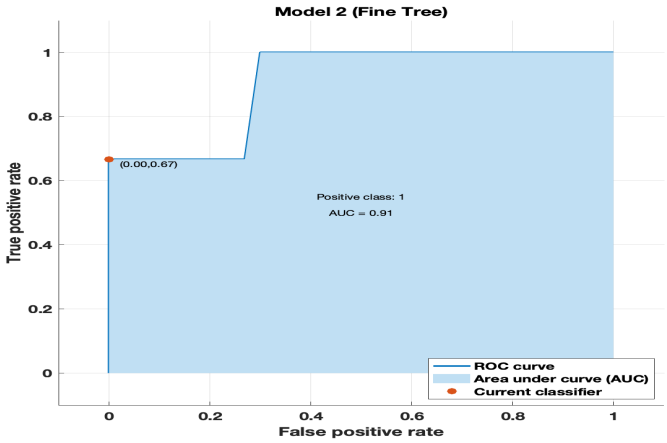



**Fig. 6.12** The first case

## 6.6 Discussion

The authorization authority needs different information on the identity of the vehicles and the common routes for a fleet of vehicles to be able to compare the O/D pairs with the identities. We notice that in our case of tests, c 'is trivial given that the only O/D pair that was possible is the departure from the test site and the arrival on this same site. The AA will have direct access to messages circulating in the network via its link with the national node.

The clustering process shows precisely the privacy level of all users. The three categories represent well the existing configurations. Nevertheless, this framework is flexible and could be used with more categories to classify better. After the classification, the AA should propose an alternative PCS; Nevertheless, this process should be non-deterministic. Therefore, an unsupervised Machine Learning model should fit perfectly into the framework. This framework could perfectly guard against tracking attacks as the attacker does the same process we underwent during these experiments. They stand in the listening mode to receive all the messages through the network and try to detect the identity of each MAC address that passes or at least tracker a particular identity.

## 6.7 Conclusions

This paper applies an algorithm to users' privacy verification. We summarize three different categories of users' privacy. Thus, a formal verification framework for privacy is established. Based on this framework, AA could propose an adapted PCS. This contribution could help to resolve three major issues of the PKI system: Allows to hollow out the wasting certificate problem; The waste of certificates can lead to their use in Sybil attacks; Reducing the CRLs size.

This work shows solid results and is the first algorithm applied to real-life data to estimate their privacy level. Furthermore, these results represent the most common cases in real-life as the tests were done with all the European participants. Thus, we can interpolate the results in all cases. This demonstrates that our framework is real-world applicable.

In the future, we will complete the framework with an unsupervised ML model to propose a PCS. We will improve the verification model with more real-life data. Our goal is to adapt the framework to all types of PCS. In addition, we plan to develop a decentralized manner to collaborate with the certificates authority. It will be a meaningful exploration and attempt in the field of V2X communication privacy.

CHAPTER 7

# Performance Evaluation

## 7.1 Objectives

For the detection of attacks, Decentralized Systems (Blockchain) have been widely proposed in the literature (Section  ref section detection-basedondata). The solutions can be classified into three categories. Detection that relies entirely on infrastructure Detection based on vehicles only Collaborative detection between two.

Our goal is to offer an interoperable solution with the existing environment. We decided to focus our comparison on approaches offering collaborative detection. These existing solutions, securing the various interfaces thanks to the Blockchain, are based on similar models. They all have a contribution to the detection of different types of attacks. Indeed, the main differences are the type of implemented algorithms and the database used to test performances. For our evaluation, we carried out tests in a realistic testing environment with real ITS-Ss. The objective of our tests was to test our algorithms implementation efficiency in real-time. In these experiments, we achieve three phases:

– Electromagnetic range tests for the optimization of the deployment of RSUs (Section 7.3);

– Tests on the efficiency of the Proof of Location consensus process (Section 7.4);

– The impact of real-time certificate revocation in terms of detection performance on a real environment (Section 7.5).

## 7.2 testing environment

### 7.2.1 Software

This experiment required different tools:

- *Veins:* We used the framework Veins [159] for the execution of vehicle network simulations. this Framework includes two parts:
  - Part implemented on OMNeT ++ [169], which is a network simulator
  - Part implemented on the SUMO software [102], which is a road traffic simulator.

  Above all, the Veins Framework integrates well the propagation models for the physical layer of IEEE 802.11p and permits realistic simulations.

- *Artery:* We have used the Artery [144] framework, which is an added application to the previous Framework. It allowed simulating the sending and receiving of real well-constructed ITS messages. We were able to develop our algorithms scenarios using C++ and Python languages for the

implementation of our Proof of Location messages as well as the hand-shake work of our proposed Blockchain Architecture (Section 5.4).

- *Matlab:* We have developed the metrics on Matlab software [84] and analyzed the collected data.

### 7.2.2 Software Defined Radio (SDR)

SDR is a radio communication system that uses software for the modulation and demodulation of radio signals. We used the implementation of the IEEE802.11p radio chain proposed by Bastille [34] on a USRP B210 card. We have fully uploaded the ITS-G5 radio chain via USB 3.0 on the B210 FPGA ship. GNU RADIO was used for software configurations. USRP B210 cards could also work through the USB 2.0 port, but the speed (480 Mbps equivalent to 8 MHz maximum FMCW signal bandwidth) is lower than the USB 3.0 port.

We have also implemented the Framework GeonetWorking on JAVA which implements the entire stack of CAM and DENM messages. This allowed us to configure new messages and send them over the ITS-G5 channel via the USRP card. Still, the objective was to simulate real cyberattacks.

### 7.2.3 Test Road tracks

The experiments were held on two different types of roads

- *University's Campus:* We carried out tests in the track located at the heart of our university campus, [1]. This allowed us to debug our code in real-time and make adjustments.
- *Highway:* In collaboration with the french Road manager, DirNord, we also carried out tests on the highway for research and operational purposes.

## 7.3 Project experiments

### 7.3.1 Link budget

- *Fresnel zone:* The Fresnel zone is a series of elongated concentric ellipsoidal regions between and around a transmitting antenna and a receiving antenna system. The concept calculates the strength of radio waves (or other) propagating between a transmitter and a receiver.
- *The link budget:* is a step-by-step calculation to determine the quality of a link between two antennas. The goal is to obtain a ratio between the signal and the final noise sufficient for the application.

Taking the following parameters:

- Frequency: 5.9 GHz
- Distance: 1 km
- Transmitter power: 20 dBm
- Transmitter antenna gain: 12 dBi
- Transmitter losses: 3 dB
- Total emission loss: 9 dB

**(a)** Road manager operators installing material

**(b)** Installed RSU on the Highway

**(c)** IMTD: University's Campus Track

**(d)** All used material

**Fig. 7.1** Experiments testing environments

– Receiver antenna gain: 12 dBi

– Receiver losses: 3 dB

Using the Friis equation [154], we get the result of the received power: Pr = -78.87 dBm

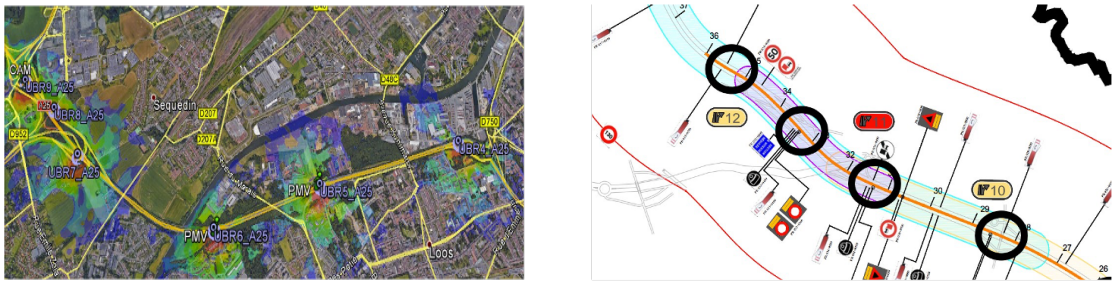
Our ITS-G5 antennas have a receiving sensitivity down to -95 dBm. Therefore, we assumed that we could reach 1 Km of transmission range.

### 7.3.2 coverage test

Experiments were carried out within the framework of studies for installing RSUs on the edge of highways. These tests are the subject of an operational research problem. In order to give the optimal location of the RSUs, we have used three primary criteria:

- The data linked to each section of highway Fig.7.2a which includes several indicators: signals, accident rate, weather conditions, traffic data, etc.
- The conditions of radio transmission in each position: As shown in figure Fig.7.2b, we have used the radio planning software, Atoll, which gives the radiation fields of the antennas based on the transmission indicators. It considers the obstacles that are all around (trees, buildings, etc).
- Without forgetting the economic aspect, which restricts us from equipping the highway with a limited number of units, obliging us to prioritize locations over others.

After having made the preliminary studies of the optimal location of the RSUs, we carried out full-scale tests to test the wear of the RSUs, taking into account the configuration of the antennas.




**(a)** Radio planning using Atoll software **(b)** highway data illustration

**Fig. 7.2** Data criteria for our study

## 7.4 Proof of Location experiments

### 7.4.1 Experimental Setup

We have conducted tests in the Mont Houy campus in Valenciennes, France where we have used two OBUs (with two real vehicles) and one RSU (see Figure 7.3). The radio equipment used in each of the three devices is the NXP ITS-G5 chipz [6].


**Fig. 7.3** Used equipment

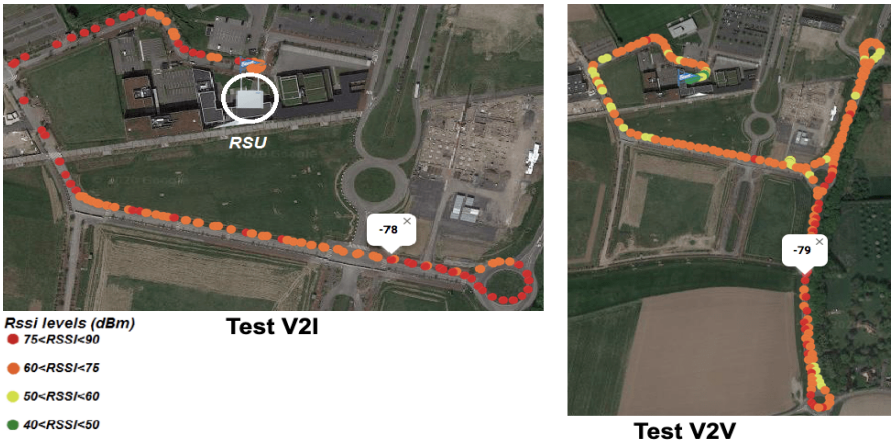



**Fig. 7.4** Path of OBU 1 under V2V communication

### 7.4.2 Results

The objective of these tests is to demonstrate a proof of concept for our solution. Our solution is based on two types of communication: V2V (vehicle to vehicles) and V2I (Vehicles to infrastructure) communication. Thus, to test the V2V communication, we conducted four tests with different distances between the two vehicles as well as two different environmental conditions (with/without line of sight for communication) (figure 7.6)

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

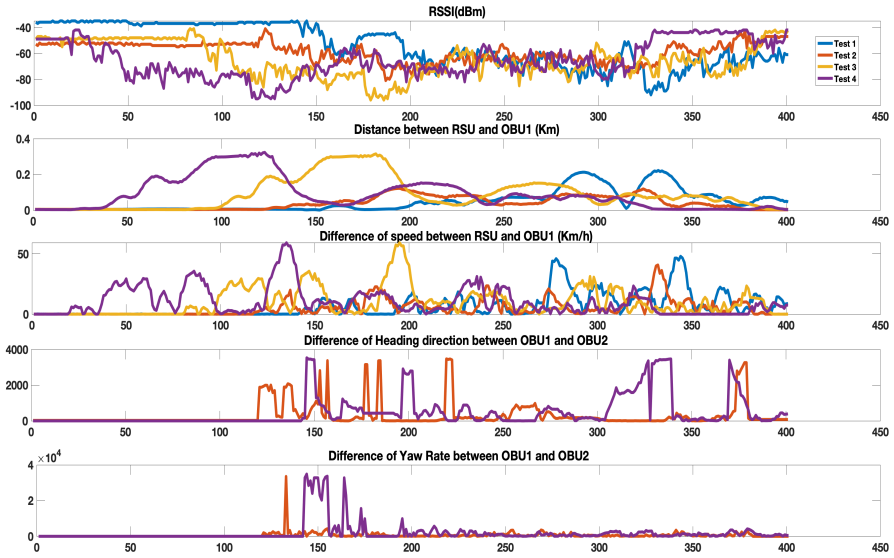



**Fig. 7.5** RSU's RSSI estimation on V2I communication with according to OBUs' information

The Fig. 7.5 shows the measurements reported by the RSU based on information received from vehicles in V2I communication mode.


**Fig. 7.6** Test 1 and 2 with RSU's RSSI estimation on V2I communication

Using Equations 5.1 and 4.3, we estimated the values of the expected power from the positions sent and we also estimated the values of the expected distance from the received signal power in Fig. 7.6 we we have reported the RSU estimation of RSSIs based onf the vehicles information. In the same way OBUs estimate other vehicles' RSSIs as shown in Fig. 7.7

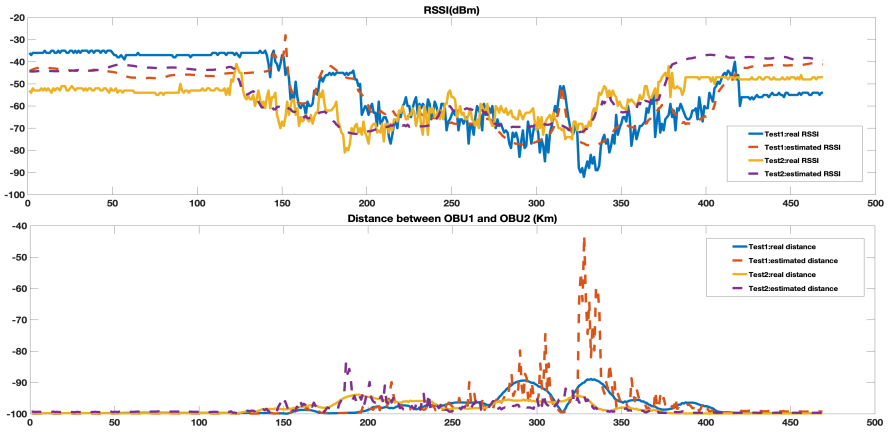



**Fig. 7.7** V2V estimation of RSSI based on test 1 and 2

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

Referring to Table 7.1, we notice the RSU's distance and RSSI estimations via V2I communications have 30 percent less accuracy compared to that of the OBU's. This is because of the impacts from relative velocity and we may deduce that the RSU alone cannot make a decision on vehicle verification. Thus, this is why considering all the OBUs and RSUs in a surrounding area of a vehicle makes our system more accurate and effective. Since the number of PoLs from all vehicles will allow the RSUs to have more visibility on the truth of the Prover's position.

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

**Table 7.1** Cross-correlations of real and estimated RSSI/distance values between OBU1/RSU and OBU2

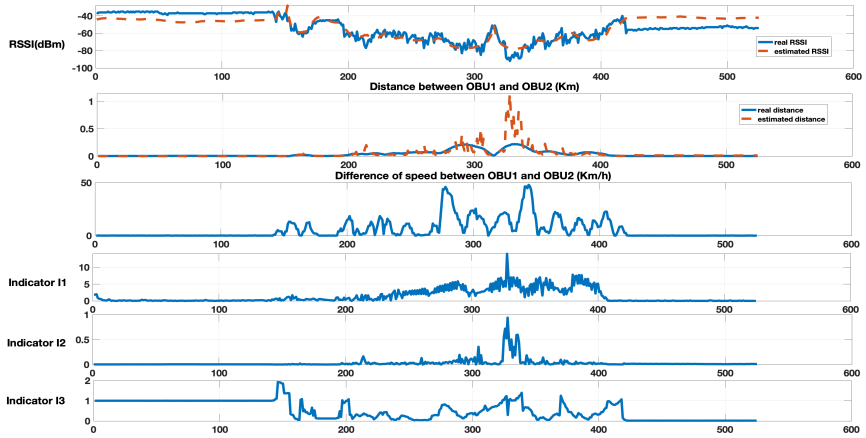



**Fig. 7.8** OBU1's RSSI estimation the resulting indicators

Fig. shows the measurements of the OBU 1 and its resulting indicators of the OBU 2 presence based on the relative information in V2V communication.

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

## 7.5 Revocation framework experiments

### 7.5.1 Experiments

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.

#### *7.5.1.1Experiments Setup*

We used three vehicles equipped with 3 OBUs, 1 RSU, and 2 USRP (Universal Software Radio Peripheral) cards. Fig.7.9 shows the campus, the road tests, and the material we used to test four different scenarios.

**Fig. 7.9** 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.7.9 shows the campus and the road tests we point to the material used.

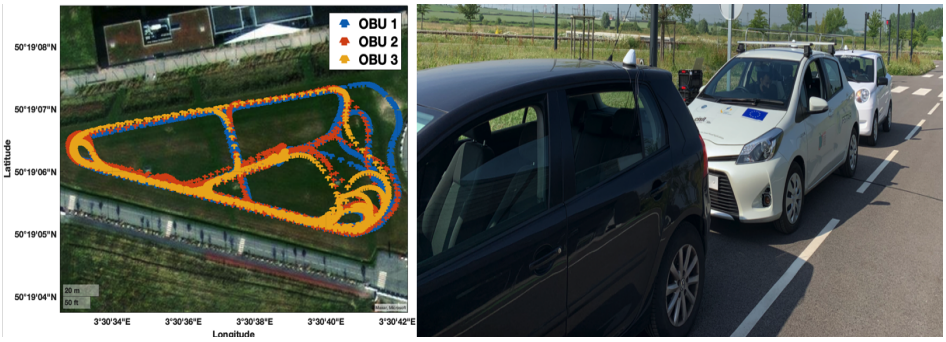



**Fig. 7.10** Setup for campus scenarios

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.

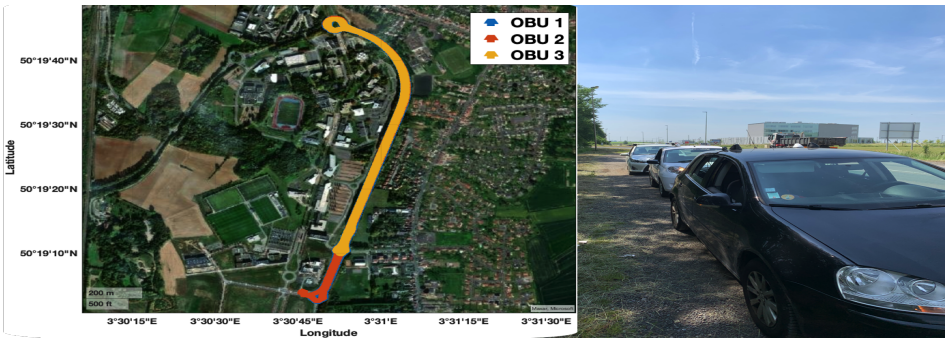



**Fig. 7.11** Setup for route scenarios

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.

#### *7.5.1.2Metrics*

Three metrics are considered for the accuracy detection rate: the true positive rate (TPR) (7.1), the true negative rate (TNR) (7.2), and detection accuracy (ACC) (7.3), which are defined in [184].

$$TPR = \frac{TP}{TP + FN} \tag{7.1}$$

$$TNR = \frac{TN}{FP + TN} \tag{7.2}$$

$$ACC = \frac{TP + TN}{TP + FN + FP + TN} \tag{7.3}$$

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.

#### *7.5.1.3Detecting 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. 7.12, 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 B.

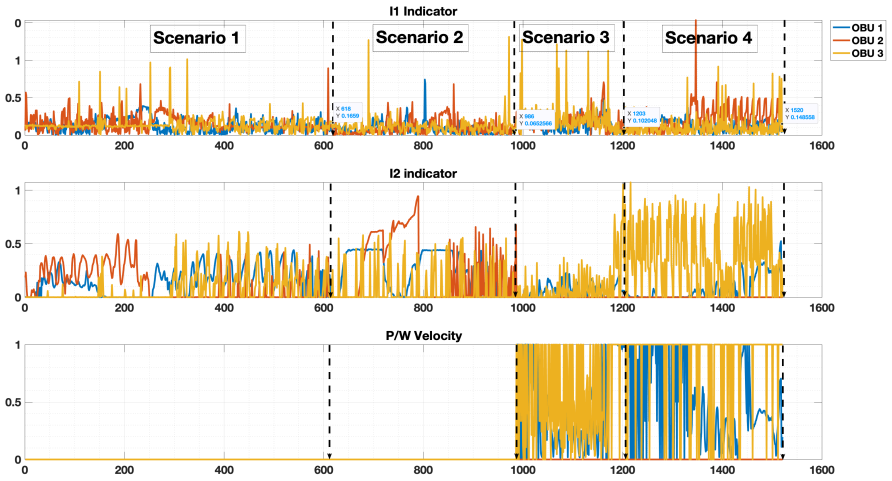



**Fig. 7.12** All reports about Hackers Node

Fig.7.12 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.7.13, shows each vehicle's profile. We have reported the different indicators from each witness in each scenario.

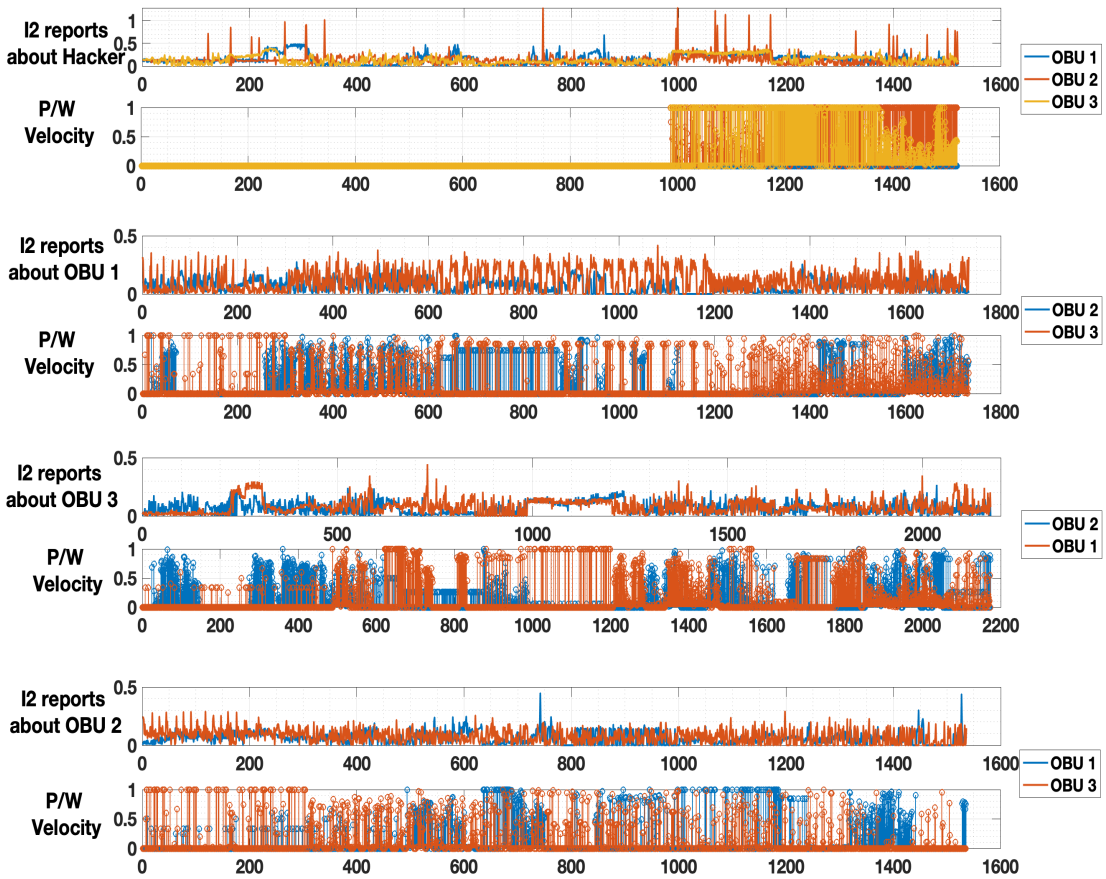



**Fig. 7.13** All trusted vehicles reports

Based on the mean and the variance of $PoL$ indicators, each vehicle decides whether or not to trust another vehicle. Table.7.2 shows the results obtained from the peer-to-peer PoL process. We did not

| | | OBU 1 | | | OBU 2 | | | OBU 3 | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Hacker | OBU 2 | OBU 3 | Hacker | OBU 1 | OBU 3 | Hacker | OBU 1 | OBU 2 |
| Scenario 1 | $\delta_{vel}$ (Km/h) | 6.32 | 3.16 | 2.91 | 14.59 | 7.46 | 4.98 | 7.60 | 3.60 | 3.54 |
| | $\sigma$ | 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 | $\delta_{vel}$ (Km/h) | 24.60 | 7.02 | 6.66 | 16.99 | 3.53 | 6.88 | 8.58 | 5.46 | 4.32 |
| | $\sigma$ | 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 | $\delta_{vel}$ (Km/h) | 0 | 2.35 | 3.12 | 2.85 | 2.85 | 2.61 | 5.51 | 4.12 | 2.90 |
| | $\sigma$ | 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 | $\delta_{vel}$ (Km/h) | 0 | 3.44 | 4.21 | 7.94 | 6.26 | 5.92 | 38.19 | 5.97 | 3.45 |
| | $\sigma$ | 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% | |

**Table 7.2** Indicators results for peer-to-peer communication for each scenario , Where $\delta_{vel}$ is the relative velocity between both nodes, $\sigma$ and ACC

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 applied the detection algorithm to each vehicle separately. Fig. 7.14 shows the accuracy rate of the peer-to-peer PoL process of each OBU, whereas Fig.7.15 compares the average of all OBU accuracy rates ($ACC_{Sig}$) and the rate of community accuracy ($ACC_{Com}$).

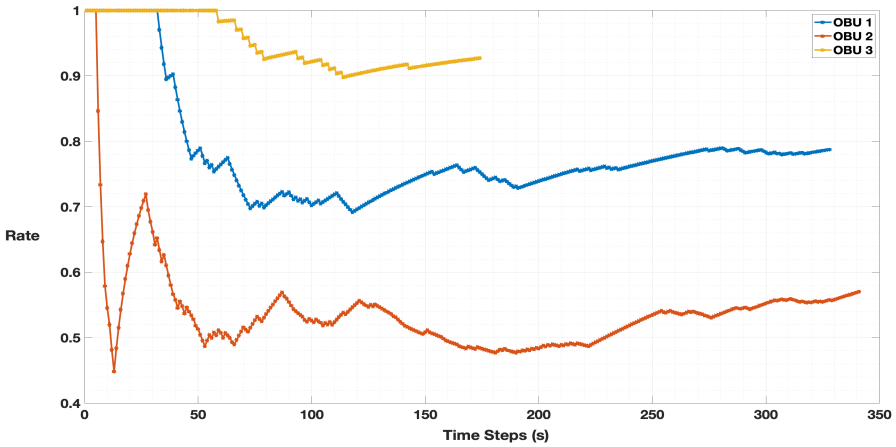



**Fig. 7.14** Each OBU's accuracy rate

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.7.15 shows clearly that community decision is more efficient than individual ones.

#### *7.5.1.4Sybil 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.7.16 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

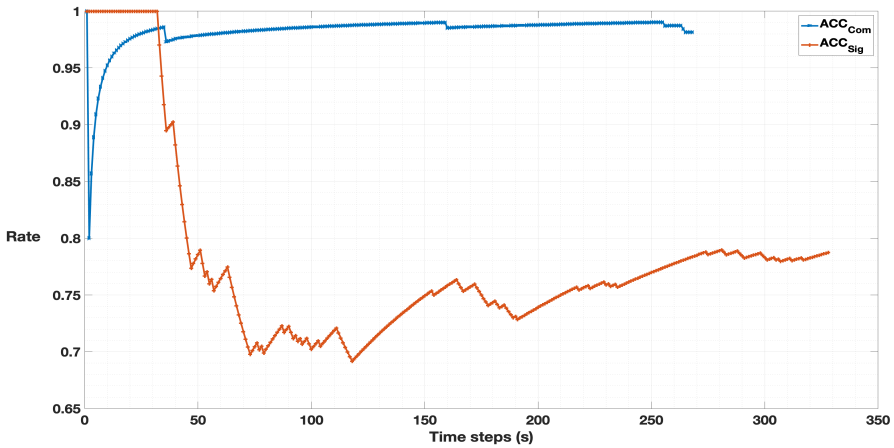



**Fig. 7.15** The comparison between the community's and the single's strategy detection in terms of accuracy rate

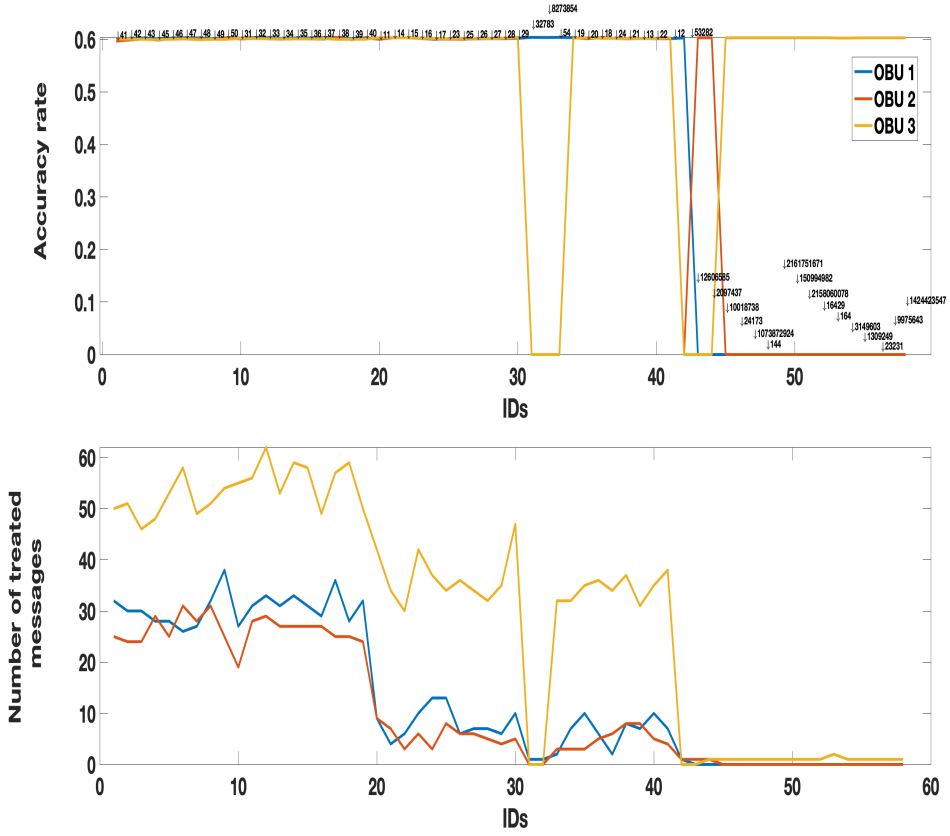



**Fig. 7.16** Accuracy rate on Sybil attack

Sybil attacks.

## 7.6 Conclusion

Toll transactions must be secure, but what is even more important is to have the ability to cope with the essential deployment of ITS G5 technologies in the world of autonomous vehicles. In particular, it is essential to cope with attacks that may occur with these technologies and with their large-scale deployment. It is even of more importance since several car manufacturers plan to have all upcoming vehicles equipped with V2X equipment and because motorway managers have already equipped most of their networks with this equipment.

We have proposed a way to ensure integration and non-repudiation in toll transactions (two non-trivial security requirements). The performance of the proposed identification and verification methods were evaluated using one RSU and two OBUs, each of industrial equipment.

By adding our evaluation indicators and smart contracts, we obtained satisfactory results on the effectiveness of this method. As a result, the performances will be even more effective in communicating and avoid DoS and Sybil attacks. Note, however, that this architecture and its methods can be applied for all vehicular communications.

Therefore, we used the consensus to propose a new architecture based on communities for the revocation of certificates in real time. The performance showed the effectiveness of our method in avoiding Sybil attacks as well as all position-based attacks.

CHAPTER 8

# General conclusion and perspectives

In this thesis, we focused on the implementation of the blockchain in securing V2X networks, particularly the geographical distribution of blockchain communities. In this chapter, we summarize the main contributions to this field which have been detailed in this thesis (Section 1.3). We also introduce some exciting perspectives that could be explored in future work (Section 8.2).

## 8.1 Contributions

As part of securing V2X communications, our goal was to provide high-performance and secure Blockchain-based solutions. The main contributions are:

- **The Definition of a consensus algorithm adapted to the requirements of V2X communications:** this first contribution corresponds to the Definition of a consensus algorithm capable of evolving under the conditions of vehicular communications since the successful implementation in place of the blockchain is based on the choice of consensus. The designed solution is based on techniques related to the physical layer and others within the application layer. Therefore, it perfectly matches the CPS requirements. This allowed us to create a basis for integrating blockchain into V2X communications.

- **Definition of a new architecture, TileChain:** This architecture was based on the needs of the certification authorities responsible for the security of V2X communications. The crossing of the limits of the referenced architecture (PKI) and the possible technological solutions have enabled us to develop a new architecture adapted to the V2X environment. This architecture is based on operational research work that proposes the dynamic cutting of tiles for constructing autonomous blockchain networks. It aims to offer a complete architecture for the implementation of the blockchain since it can ensure a high level of security and respect for privacy;

- **Set up a framework and evaluate a framework for the revocation of certificates in real-time:** This contribution corresponds to the Definition of an algorithm capable of building autonomous blockchain communities to evaluate each of their "goodness" and thus revoke malicious vehicles in real-time. The proposed solution allows a collaborative system between the vehicle and the structure since it has been shown that we cannot rely on just one of them. Although evaluated as part of a real experiment, the defined approach could allow security under real-time requirements.

- **towards enhancing privacy in VANET:** The proposed context-adaptive and Authority-centric privacy scheme provides a robust framework for protecting sensitive information while ensuring efficient communication within the VANET context. The Knapsack problem-based algorithm offers an effective solution for combining trajectories and maintaining users' traceability, striking a balance between optimal navigation and preserving user anonymity. Additionally, the evaluation

of real-life user privacy using OBUs from different countries sheds light on the effectiveness of implemented privacy measures and identifies areas for further improvement. These contributions collectively advance the understanding and implementation of privacy-enhancing mechanisms in VANET, paving the way for more secure and confidential vehicular communication systems.

## 8.2 Perspectives

The work introduced in this thesis contributes to improving the security system and the revocation process in V2X communications. However, this work does not respond to all of the issues raised by cybersecurity issues. Several perspectives can thus be identified:

- **The implementation and evaluation of a pseudonym change technique adapted to our solution:** in Chapter 3.2, we have mentioned the different pseudonym change techniques as well as the different identifiers that can be used to harm the privacy of drivers. We then proposed an architecture allowing the integration of the blockchain and a framework allowing its use for the revocation of certificates. However, the choice of pseudonym change techniques can harm the blockchain hand-shake process. Therefore, it is crucial to define it and carry out a study of the countermeasures that can be considered against any tracking attempt.

- **The development of solutions based on artificial intelligence for the dynamic cutting of tiles:** as we demonstrated in Chapter 4, for the implementation of the blockchain and not to be controlled by the blockchain networks by malicious vehicles that can bypass the voting system by attacking the network at certain low traffic periods. It is essential to build tiles dynamically based on road traffic data. An AI-based solution will allow CA to control better blockchain networks and the number of vehicles participating in each tile.

- **The deployment of the V2X blockchain ecosystem:** The use of an automobile track equipped with a V2X infrastructure and communicating vehicles can help make a Proof of Concept of our Blockchain solution. However, this implies the link with an authority of certifications that contributes to the security of the current V2X networks.

- **Enhancing privacy in VANET.** Looking ahead, there are several promising perspectives to enhance privacy in VANET. Firstly, further refinement and optimization of the proposed context-adaptive and Authority-centric privacy scheme can be pursued to address evolving threats and adapt to changing communication requirements. Additionally, future research can focus on exploring alternative algorithms and approaches to trajectory combinations and users' traceability, aiming for even greater efficiency and privacy preservation. Furthermore, extending the evaluation of user privacy to include a wider range of countries and diverse vehicular environments would provide a more comprehensive understanding of the effectiveness of privacy measures globally. Overall, these perspectives hold the potential to advance the field of VANET privacy, ensuring secure and confidential communication for drivers in increasingly complex vehicular networks.

# REFERENCES


[1] Batiment IMTD : Institut des mobilités et des transports durables, https://imtd.fr/.

[2] BitShares technology – open-source blockchain-based software solutions, https://bitshares.org/.

[3] C-Roads project: C-roads - the platform of harmonised c-its deployment in europe, https://www.c-roads.eu/platform.html.

[4] Car2Car car 2 car communication consortium, https://www.car-2-car.org/about-c-its/c176.

[5] CRoads project: harmonised c-its specifications https://www.c-roads.eu/platform/about/news/news/entry/show/release-20-of-c-roads-harmonised-c-its-specifications.html.

[6] DSRC safety modem | NXP.

[7] Fenix project fenix network, https://fenix-network.eu.

[8] IEEE standard for message sets for vehicle/roadside communications, IEEE std 1455-1999. pages 1–134.

[9] InDiD c-its project, https://www.c-roads.eu/pilots/core-members/france/partner/project/show/indid.html.

[10] InterCor project: Interoperable corridors deploying cooperative intelligent transport systems, https://intercor-project.eu/.

[11] InterCor project: Interoperable corridors deploying cooperative intelligent transport systems, https://intercor-project.eu/.

[12] Namecoin, https://www.namecoin.org/.

[13] Nxt whitepaper - introduction: Nxt whitepaper.

[14] Projet SCOOP : véhicules et routes connectés, http://www.scoop.developpement-durable.gouv.fr/.

[15] Storj - decentralized cloud storage, https://www.storj.io/.

[16] Ieee standard for wireless access in vehicular environments security services for applications and management messages. *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pages 1–240, 2016.

[17] Imad Aad, Jean-Pierre Hubaux, and Edward W Knightly. Denial of service resilience in ad hoc networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 202–215, 2004.

[18] Muhammad Tahir Abbas, Afaq Muhammad, and Wang-Cheol Song. Sd-iov: Sdn enabled routing for internet of vehicles in road-aware approach. *Journal of Ambient Intelligence and Humanized Computing*, 11(3):1265–1280, 2020.

[19] Zakaria Abou El Houda, Abdelhakim Senhaji Hafid, and Lyes Khoukhi. Cochain-sc: An intra-and inter-domain ddos mitigation scheme based on blockchain using sdn and smart contract. *IEEE Access*, 7:98893–98907, 2019.

[20] Ikram Ali, Tandoh Lawrence, and Fagen Li. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in vanets. *Journal of Systems Architecture*, 103:101692, 2020.

[21] Amir Alipour-Fanid, Monireh Dabaghchian, Hengrun Zhang, and Kai Zeng. String stability analysis of cooperative adaptive cruise control under jamming attacks. In *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, pages 157–162. IEEE, 2017.

[22] Mohammad Abu Alsheikh, Shaowei Lin, Dusit Niyato, and Hwee-Pink Tan. Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communications Surveys and Tutorials*, 16(4):1996–2018, 2014.

[23] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6):126–132, 2015.

[24] Frederik Armknecht, Andreas Festag, Dirk Westhoff, and Ke Zeng. Cross-layer privacy enhancement and non-repudiation in vehicular communication. In *Communication in Distributed Systems-15. ITG/GI Symposium*, pages 1–12. VDE, 2007.

[25] Muhammad Arshad, Zahid Ullah, Naveed Ahmad, Muhammad Khalid, Haithiam Criuckshank, and Yue Cao. A survey of local/cooperative-based malicious information detection techniques in vanets. *EURASIP Journal on Wireless Communications and Networking*, 2018(1):1–17, 2018.

[26] Kevin Ashton et al. That 'internet of things' thing. *RFID journal*, 22(7):97–114, 2009.

[27] Louise Axon. Privacy-awareness in blockchain-based PKI.

[28] Enzo Baccarelli, Paola G Vinueza Naranjo, Mohammad Shojafar, and Michele Scarpiniti. Q*: Energy and delay-efficient dynamic queue management in tcp/ip virtualized data centers. *Computer Communications*, 102:89–106, 2017.

[29] Adam Back et al. Hashcash-a denial of service counter-measure. 2002.

[30] Samaresh Bera, Sudip Misra, and Mohammad S Obaidat. Mobility-aware flow-table implementation in software-defined iot. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[31] Norbert Bißmeyer, Christian Stresing, and Kpatcha M Bayarou. Intrusion detection in vanets through verification of vehicle movement data. In *2010 IEEE Vehicular Networking Conference*, pages 166–173. IEEE, 2010.

[32] Subir Biswas, Jelena Mišić, and Vojislav Mišić. Ddos attack on wave-enabled vanet through synchronization. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 1079–1084. IEEE, 2012.

[33] Sebastian Bittl, Arturo A Gonzalez, Matthias Myrtus, Hanno Beckmann, Stefan Sailer, and Bernd Eissfeller. Emerging attacks on vanet security based on gps time spoofing. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 344–352. IEEE, 2015.

[34] Bastian Bloessl, Michele Segata, Christoph Sommer, and Falko Dressler. Performance assessment of ieee 802.11 p with an open source sdr-based prototype. *IEEE transactions on mobile computing*, 17(5):1162–1175, 2017.

[35] Felipe Boeira, Mikael Asplund, and Marinho Barcellos. Decentralized proof of location in vehicular ad hoc networks. 147:98–110.

[36] Felipe Boeira, Mikael Asplund, and Marinho Barcellos. Decentralized proof of location in vehicular ad hoc networks. *Computer Communications*, 147:98–110, 2019.

[37] Giacomo Brambilla, Michele Amoretti, and Francesco Zanichelli. Using block chain for peer-to-peer proof-of-location. *arXiv preprint arXiv:1607.00174*, 20, 2016.

[38] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[39] Benedikt Brecht and Thorsten Hehn. A security credential management system for v2x communications. In *Connected Vehicles*, pages 83–115. Springer, 2019.

[40] C. Cai, X. Yuan, and C. Wang. Towards trustworthy and private keyword search in encrypted decentralized storage. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–7.

[41] Chengjun Cai, Xingliang Yuan, and Cong Wang. Hardening distributed and encrypted keyword search via blockchain. In *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*, pages 119–128. IEEE, 2017.

[42] Chengjun Cai, Xingliang Yuan, and Cong Wang. Towards trustworthy and private keyword search in encrypted decentralized storage. In *2017 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2017.

[43] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in vanet. In *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, pages 19–28, 2007.

[44] J. A. Leon Calvo and R. Mathar. Secure blockchain-based communication scheme for connected vehicles. In *2018 European Conference on Networks and Communications (EuCNC)*, pages 347–351.

[45] Zhen Cao, Jiejun Kong, Uichin Lee, Mario Gerla, and Zhong Chen. Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks. In *IEEE INFOCOM Workshops 2008*, pages 1–6. IEEE, 2008.

[46] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OSDI*, volume 99, pages 173–186, 1999.

[47] Samarjit Chakraborty, Mohammad Abdullah Al Faruque, Wanli Chang, Dip Goswami, Marilyn Wolf, and Qi Zhu. Automotive cyber–physical systems: A tutorial introduction. *IEEE Design and Test*, 33(4):92–108, 2016.

[48] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin Shen. Footprint: detecting sybil attacks in urban vehicular networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(6):1103–1114, 2011.

[49] Michael Charitos and Grigorios Kalivas. Mimo hetnet ieee 802.11 p–lte deployment in a vehicular urban environment. *Vehicular Communications*, 9:222–232, 2017.

[50] Ming-Chin Chuang and Jeng-Farn Lee. Team: Trust-extended authentication mechanism for vehicular ad hoc networks. *IEEE systems journal*, 8(3):749–758, 2013.

[51] Ameneh Daeinabi and Akbar Ghaffarpour Rahbar. Detection of malicious vehicles (dmv) through monitoring in vehicular ad-hoc networks. *Multimedia tools and applications*, 66(2):325–338, 2013.

[52] Roniel S de Sousa, Felipe S da Costa, Andre CB Soares, Luiz FM Vieira, and Antonio AF Loureiro. Geo-sdvn: A geocast protocol for software defined vehicular networks. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2018.

[53] Ahmed Didouh, Yassin El Hillali, Atika Rivenq, and Houda Labiod. Novel centralized pseudonym changing scheme for location privacy in v2x communication. *Energies*, 15(3):692, 2022.

[54] 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.

[55] Yuhao Dong, Woojung Kim, and Raouf Boutaba. Conifer: Centrally-managed PKI with blockchain-rooted trust. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1092–1099.

[56] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak. BlockChain: A distributed solution to automotive security and privacy. 55(12):119–125.

[57] Joao M Duarte, Eirini Kalogeiton, Ridha Soua, Gaetano Manzo, Maria Rita Palattella, Antonio Di Maio, Torsten Braun, Thomas Engel, Leandro A Villas, and Gianluca A Rizzo. A multi-pronged approach to adaptive and context aware content dissemination in vanets. *Mobile Networks and Applications*, 23(5):1247–1259, 2018.

[58] David Eckhoff, Reinhard German, Christoph Sommer, Falko Dressler, and Tobias Gansen. Slotswap: Strong and affordable location privacy in intelligent transportation systems. *IEEE Communications Magazine*, 49(11):126–133, 2011.

[59] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, and Alejandro Quintero. VANET security surveys. 44:1–13.

[60] EN ETSI. 302 636-4-1. *Intelligent Transport Systems (ITS)*.

[61] EN ETSI. 302 637-3 v1. 2.2: Intelligent transport systems (its). *Vehicular Communications*.

[62] EN ETSI. 302 663 (v1. 2.1):" intelligent transport systems (its). *Access layer specification for Intelligent Transport Systems operating in the*, 5.

[63] EN ETSI. 302 637-2 v1. 3.1-intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *ETSI, Sept*, 2014.

[64] I ETSI. Intelligent transport systems (its); security; threat, vulnerability and risk analysis (tvra). Technical report, Technical report, ETSI TR 102 893, European Telecommunications Standards . . . , 2010.

[65] I ETSI. Intelligent transport systems (its); security; header and certificate formats. Technical report, Technical report, ETSI TR 103 097, European Telecommunications Standards . . . , 2017.

[66] 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.

[67] TCITS ETSI. Etsi ts 102 731 v1. 1.1-intelligent transport systems (its); security; security services and architecture. *Standard, TC ITS*, 2010.

[68] TCITS ETSI. Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *Draft ETSI TS*, 20:448–451, 2011.

[69] TS ETSI. 101 539 (v1. 1.1). *Intelligent Transport Systems (ITS)*.

[70] TS ETSI. 102 940,". *Intelligent Transport Systems (ITS)*.

[71] TS ETSI. 103 191 (v3. 1.1): Intelligent transport systems (its). *Signal Phase And Timing (SPAT) and Map (MAP)*, 5.

[72] TS ETSI. 102 941 v1. 1.1—intelligent transport systems (its); security; trust and privacy management. *Standard, TC C-ITS*, 2012.

[73] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, 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.

[74] Xia Feng, Chun-yan Li, De-xin Chen, and Jin Tang. A method for defensing against multi-source sybil attacks in vanet. *Peer-to-Peer Networking and Applications*, 10(2):305–314, 2017.

[75] Fuad A Ghaleb, Anazida Zainal, and Murad A Rassam. Data verification and misbehavior detection in vehicular ad-hoc networks. *Jurnal Teknologi*, 73(2), 2015.

[76] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad A Kherani, and Skanda N Muthaiah. Detecting misbehaviors in vanet with integrated root-cause analysis. *Ad Hoc Networks*, 8(7):778–790, 2010.

[77] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, and Nitesh Kumar Prajapati. A sybil attack detection approach using neighboring vehicles in vanet. In *Proceedings of the 4th international conference on Security of information and networks*, pages 151–158, 2011.

[78] Gilles Guette and Bertrand Ducourthial. On the sybil attack detection in vanet. In *2007 IEEE international conference on Mobile Adhoc and sensor systems*, pages 1–6. IEEE, 2007.

[79] 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 VehiculAr InterNETworking*, pages 89–98, 2009.

[80] Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. Detection of radio interference attacks in vanet. In *GLOBECOM 2009-2009 IEEE Global Telecommunications Conference*, pages 1–5. IEEE, 2009.

[81] Yong Hao, Jin Tang, and Yu Cheng. Cooperative sybil attack detection for position based applications in privacy preserved vanets. In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pages 1–5. IEEE, 2011.

[82] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. *Vehicular Communications*, 7:7–20, 2017.

[83] Li He and Wen Tao Zhu. Mitigating dos attacks against signature-based authentication in vanets. In *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, volume 3, pages 261–265. IEEE, 2012.

[84] Desmond J Higham and Nicholas J Higham. *MATLAB guide*. SIAM, 2016.

[85] Jorge Hortelano, Juan Carlos Ruiz, and Pietro Manzoni. Evaluating the usefulness of watchdogs for intrusion detection in vanets. In *2010 IEEE International Conference on Communications Workshops*, pages 1–5. IEEE, 2010.

[86] Hsu-Chun Hsiao, Ahren Studer, Rituik Dubey, Elaine Shi, and Adrian Perrig. Efficient and secure threshold-based event validation for vanets. In *Proceedings of the fourth ACM conference on Wireless network security*, pages 163–174, 2011.

[87] Binchao Huang, Jianping Li, Ko-Wei Lih, and Haiyan Wang. Approximation algorithms for the generalized multiple knapsack problems with k restricted elements. In *2015 7th International Conference on Intelligent Human-Machine Systems and Cybernetics*, pages 470–474. IEEE.

[88] Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures, volume = 2020, address = Geneva, CH, institution = International Organization for Standardization. Standard, 2020.

[89] Attila Jaeger, Norbert Bißmeyer, Hagen Stübing, and Sorin A Huss. A novel framework for efficient mobility data verification in vehicular ad-hoc networks. *International Journal of Intelligent Transportation Systems Research*, 10(1):11–21, 2012.

[90] Ahmed Jawad Kadhim and Seyed Amin Hosseini Seno. Energy-efficient multicast routing protocol based on sdn and fog computing for vehicular networks. *Ad Hoc Networks*, 84:68–81, 2019.

[91] Enis Karaarslan and Eylul Adiguzel. Blockchain based DNS and PKI solutions. 2(3):52–57.

[92] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys and tutorials*, 13(4):584–616, 2011.

[93] Hans Kellerer, Ulrich Pferschy, and David Pisinger. Multidimensional knapsack problems. In *Knapsack Problems*, pages 235–283. Springer Berlin Heidelberg.

[94] Elie Kfoury and David Khoury. Distributed public key infrastructure and PSK exchange based on blockchain technology. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1116–1120.

[95] 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.

[96] Salabat Khan, Liehuang Zhu, Xiaoyan Yu, Zijian Zhang, Mussadiq Abdul Rahim, Maqbool Khan, Xiaojiang Du, and Mohsen Guizani. Accountable credential management system for vehicular communication. *Vehicular Communications*, 25:100279, 2020.

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

[98] 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 and privacy in wireless and mobile networks*, pages 172–183, 2018.

[99] Tiffany Hyun-Jin Kim, Ahren Studer, Rituik Dubey, Xin Zhang, Adrian Perrig, Fan Bai, Bhargav Bellur, and Aravind Iyer. Vanet alert endorsement using multi-source filters. In *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, pages 51–60, 2010.

[100] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 19(1), 2012.

[101] 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.

[102] Daniel Krajzewicz, Georg Hertkorn, Christian Rössel, and Peter Wagner. Sumo (simulation of urban mobility)-an open-source traffic simulation. In *Proceedings of the 4th middle East Symposium on Simulation and Modelling (MESM20002)*, pages 183–187, 2002.

[103] S. Kuhlmorgen, I. Llatser, A. Festag, and G. Fettweis. Performance evaluation of ETSI GeoNetworking for vehicular ad hoc networks. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–6.

[104] Sergii Kushch 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.

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

[106] Leslie Lamport. The part-time parliament. In *Concurrency: the Works of Leslie Lamport*, pages 277–317. 2019.

[107] Leslie Lamport et al. Paxos made simple. *ACM Sigact News*, 32(4):18–25, 2001.

[108] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency: the Works of Leslie Lamport*, pages 203–226. 2019.

[109] Edward A Lee. Cyber physical systems: Design challenges. In *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*, pages 363–369. IEEE, 2008.

[110] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. 4(6):1832–1843.

[111] Tim Leinmüller and Elmar Schoch. Greedy routing in highway scenarios: The impact of position faking nodes. In *Proceedings of Workshop On Intelligent Transportation (WIT 2006)(Mar. 2006)*, 2006.

[112] Bisheng Liu, Jerry T Chiang, and Yih-Chun Hu. Limits on revocation in vanets. In *8th international conference on applied cryptography and network security*, pages 38–52, 2010.

[113] Lei Liu, Chen Chen, Tie Qiu, Mengyuan Zhang, Siyu Li, and Bin Zhou. A data dissemination scheme based on clustering and probabilistic broadcasting in vanets. *Vehicular Communications*, 13:78–88, 2018.

[114] Yu-Chun Liu, Chien Chen, and Suchandra Chakraborty. A software defined network architecture for geobroadcast in vanets. In *2015 IEEE International Conference on Communications (ICC)*, pages 6559–6564. IEEE, 2015.

[115] Nai-Wei Lo and Hsiao-Chien Tsai. Illusion attack on vanet applications-a message plausibility problem. In *2007 IEEE globecom workshops*, pages 1–8. IEEE, 2007.

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

[117] Brigitte Lonc and Pierpaolo Cincilla. Cooperative its security framework: Standards and implementations progress in europe. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–6. IEEE, 2016.

[118] Z. Lu, Q. Wang, G. Qu, and Z. Liu. BARS: A blockchain-based anonymous reputation system for trust management in VANETs. 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 98–103.

[119] Nikita Lyamin, Denis Kleyko, Quentin Delooz, and Alexey Vinel. Ai-based malicious network traffic detection in vanets. *IEEE Network*, 32(6):15–21, 2018.

[120] Zhendong Ma, Frank Kargl, and Michael Weber. A location privacy metric for v2x communication systems. In *2009 IEEE Sarnoff Symposium*, pages 1–6. IEEE, 2009.

[121] Zhendong Ma, Frank Kargl, and Michael Weber. Measuring location privacy in v2x communication systems with accumulated information. In *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, pages 322–331. IEEE, 2009.

[122] Nisha Malik, Priyadarsi Nanda, Arushi Arora, Xiangjian He, and Deepak Puthal. Blockchain based secured identity authentication and expeditious 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.

[123] Amjad Mehmood, Muhammad Muneer Umar, and Houbing Song. Icmds: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks. *Ad Hoc Networks*, 55:97–106, 2017.

[124] Ravi Mukkamala. Qpki: A qos-based architecture for public-key infrastructure (pki). In *International Conference on Cryptology in India*, pages 108–121. Springer, 2002.

[125] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[126] 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.

[127] Soyoung Park, Baber Aslam, Damla Turgut, and Cliff C Zou. Defense against sybil attack in vehicular ad hoc network based on roadside unit support. In *MILCOM 2009-2009 IEEE Military Communications Conference*, pages 1–7. IEEE, 2009.

[128] Yanlin Peng, Zakhia 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.

[129] Adrian Perrig, Ran Canetti, J Doug Tygar, and Dawn Song. The tesla broadcast authentication protocol. *Rsa Cryptobytes*, 5(2):2–13, 2002.

[130] Jonathan Petit, Michael Feiri, and Frank Kargl. Spoofed data detection in vanets using dynamic thresholds. In *2011 IEEE Vehicular Networking Conference (VNC)*, pages 25–32. IEEE, 2011.

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

[132] Andreas Pfitzmann and Marit Hansen. Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology. 2005.

[133] Marc Pilkington. Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[134] Oscar Punal, Carlos Pereira, Ana Aguiar, and James Gross. Experimental characterization and modeling of rf jamming attacks on vanets. *IEEE transactions on vehicular technology*, 64(2):524–540, 2014.

[135] 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.

[136] Ragunathan Rajkumar, Insup Lee, Lui Sha, and John Stankovic. Cyber-physical systems: the next computing revolution. In *Design automation conference*, pages 731–736. IEEE, 2010.

[137] Seyed Hamed Rastegar, Aliazam Abbasfar, and Vahid Shah-Mansouri. On fair rule caching in software defined radio access networks. *IEEE Wireless Communications Letters*, 7(3):460–463, 2017.

[138] Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and Jean-Pierre Hubaux. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE Journal on Selected Areas in Communications*, 25(8):1557–1568, 2007.

[139] Mohammad Abdur Razzaque, Ahmad Salehi, and Seyed M Cheraghi. Security and privacy in vehicular ad-hoc networks: survey and the road ahead. In *Wireless Networks and Security*, pages 107–132. Springer, 2013.

[140] David Rebollo-Monedero, Jordi Forné, Agusti Solanas, and Antoni Martínez-Ballesté. Private location-based information retrieval through user collaboration. *Computer Communications*, 33(6):762–774, 2010.

[141] Mengying Ren, Jun Zhang, Lyes Khoukhi, Houda Labiod, and Véronique Vèque. A unified framework of clustering approach in vehicular ad hoc networks. *IEEE Transactions on intelligent transportation systems*, 19(5):1401–1414, 2017.

[142] Leonid Reyzin and Sophia Yakoubov. Efficient asynchronous accumulators for distributed PKI. In Vassilis Zikas and Roberto De Prisco, editors, *Security and Cryptography for Networks*, volume 9841, pages 292–309. Springer International Publishing.

[143] Raphael Riebl, Hendrik-Jörn Günther, Christian Facchi, and Lars Wolf. Artery: Extending veins for vanet applications. In *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, pages 450–456. IEEE, 2015.

[144] Raphael Riebl, Christina Obermaier, and Hendrik-Jörn Günther. Artery: Large scale simulation environment for its applications. In *Recent Advances in Network Simulation*, pages 365–406. Springer, 2019.

[145] Lucas Rivoirard, Martine Wahl, Patrick Sondi, Marion Berbineau, and Dominique Gruyer. Chain-branch-leaf: A clustering scheme for vehicular networks using only v2v communications. *Ad Hoc Networks*, 68:70–84, 2018.

[146] Sushmita Ruj, Marcos A Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. On data-centric misbehavior detection in vanets. In *2011 IEEE Vehicular Technology Conference (VTC Fall)*, pages 1–5. Ieee, 2011.

[147] Ousmane Sadio, Ibrahima Ngom, and Claude Lishou. Sdn architecture for intelligent vehicular sensors networks. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*, pages 139–144. IEEE, 2018.

[148] Fatih Sakiz and Sevil Sen. A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov. *Ad Hoc Networks*, 61:33–50, 2017.

[149] Prince Samar, Marc R Pearlman, and Zygmunt 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.

[150] Arijet Sarker, SangHyun Byun, Wenjun Fan, and Sang-Yoon Chang. Blockchain-based root of 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.

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

[152] Robert K Schmidt, Tim Leinmüller, Elmar Schoch, Albert Held, and Günter Schäfer. Vehicle behavior analysis to enhance security in vanets. In *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*. Citeseer, 2008.

[153] Claude Elwood Shannon. A mathematical theory of communication. *The Bell system technical journal*, 27(3):379–423, 1948.

[154] Joseph A Shaw. Radiometry and the friis transmission equation. *American journal of physics*, 81(1):33–37, 2013.

[155] 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.

[156] Jianhua Shi, Jiafu Wan, Hehua Yan, and Hui Suo. A survey of cyber-physical systems. In *2011 international conference on wireless communications and signal processing (WCSP)*, pages 1–6. IEEE, 2011.

[157] David B. Shmoys and Éva Tardos. An approximation algorithm for the generalized assignment problem. 62(1):461–474.

[158] Mohammad Shojafar, Nicola Cordeschi, and Enzo Baccarelli. Energy-efficient adaptive resource management for real-time vehicular cloud services. *IEEE Transactions on Cloud computing*, 7(1):196–209, 2016.

[159] Christoph Sommer, David Eckhoff, Alexander Brummer, Dominik S Buse, Florian Hagenauer, Stefan Joerer, and Michele Segata. Veins: The open source vehicular network simulation framework. In *Recent Advances in Network Simulation*, pages 215–252. Springer, 2019.

[160] Joseph Soryal and Tarek Saadawi. Dos attack detection in internet-connected vehicles. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 7–13. IEEE, 2013.

[161] Chea Sowattana, Wantanee Viriyasitavat, and Assadarat Khurat. Distributed consensus-based sybil nodes detection in vanets. In *2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, pages 1–6. IEEE, 2017.

[162] Ahren Studer, Fan Bai, Bhargav Bellur, and Adrian Perrig. Flexible, extensible, and efficient vanet authentication. *Journal of Communications and Networks*, 11(6):574–588, 2009.

[163] Kehua Su, Jie Li, and Hongbo Fu. Smart city and the applications. In *2011 international conference on electronics, communications and control (ICECC)*, pages 1028–1031. IEEE, 2011.

[164] Irshad Ahmed Sumra, Halabi Bin Hasbullah, et al. Effects of attackers and attacks on availability requirement in vehicular network: a survey. In *2014 International Conference on Computer and Information Sciences (ICCOINS)*, pages 1–6. IEEE, 2014.

[165] Mingshun Sun, Ming Li, and Ryan Gerdes. A data trust framework for vanets enabling false data detection and secure vehicle tracking. In *2017 IEEE Conference on Communications and Network Security (CNS)*, pages 1–9. IEEE, 2017.

[166] Ozan Tonguz, Nawapom Wisitpongphan, Fan Bai, Priyantha Mudalige, and Varsha Sadekar. Broadcasting in vanet. In *2007 mobile networking for vehicular environments*, pages 7–12. IEEE, 2007.

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

[168] Rens Wouter van der Heijden, Stefan Dietzel, Tim Leinmüller, and Frank Kargl. Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Communications Surveys and Tutorials*, 21(1):779–811, 2018.

[169] András Varga. Omnet++ http://www. omnetpp. org. *IEEE Network Interactive*, 16(4), 2002.

[170] Eric R Verheul. Issue first activate later certificates for v2x. *Presentation InterCor project*, 2017.

[171] Karan Verma and Halabi Hasbullah. Bloom-filter based ip-chock detection scheme for denial of service attacks in vanet. *Security and Communication Networks*, 8(5):864–878, 2015.

[172] Adnan Vora and Mikhail Nesterenko. Secure location verification using radio broadcast. *IEEE Transactions on Dependable and Secure Computing*, 3(4):377–385, 2006.

[173] William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn. A security credential management system for v2v communications. In *2013 IEEE Vehicular Networking Conference*, pages 1–8. IEEE, 2013.

[174] Dr Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER. page 32.

[175] 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.

[176] David Xiao. The four layers of the blockchain.

[177] Shunyi Xu, Chuan Wu, and Zongpeng Li. Software defined mobile multicast. In *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*, pages 208–216. IEEE, 2015.

[178] Zhiqian Xu and Hai Jiang. A framework of decentralized PKI key management based on dynamic trust. page 8.

[179] Sophia Conner Fromknecht Yakoubov, Dragos Velicanu. A decentralized public key infrastructure with identity retention.

[180] Alexander Yakubov, Wazen M. Shbair, Anders Wallbom, David Sanda, and Radu State. A blockchain-based PKI management framework. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6. ISSN: 2374-9709.

[181] Tao Yang, Wei Xin, Liangwen Yu, Yong Yang, Jianbin Hu, and Zhong Chen. Misdis: An efficent misbehavior discovering method based on accountability and state machine in vanet. In *Asia-Pacific Web Conference*, pages 583–594. Springer, 2013.

[182] 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.

[183] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung. Blockchain-based decentralized trust management in vehicular networks. 6(2):1495–1505.

[184] 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.

[185] Yingying Yao, Xiaolin Chang, Jianhua Wang, Jelena Mišić, Vojislav B Mišić, and Hong Wang. Lpc: A lightweight pseudonym changing scheme with robust forward and backward secrecy for v2x. *Ad Hoc Networks*, 123:102695, 2021.

[186] 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.

[187] Bo Yu, Cheng-Zhong Xu, and Bin Xiao. Detecting sybil attacks in vanets. *Journal of Parallel and Distributed Computing*, 73(6):746–756, 2013.

[188] Yong Yuan and Fei-Yue Wang. Towards blockchain-based intelligent transportation systems. In *2016 IEEE 19th international conference on intelligent transportation systems (ITSC)*, pages 2663–2668. IEEE, 2016.

[189] Kamran Zaidi, Milos B Milojevic, Veselin Rakocevic, Arumugam Nallanathan, and Muttukrishnan Rajarajan. Host-based intrusion detection for vanets: a statistical approach to rogue node detection. *IEEE transactions on vehicular technology*, 65(8):6703–6714, 2015.

[190] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564. ISSN: null.

[191] Xuejun Zhuo, Jianguo Hao, Duo Liu, and Yiqi Dai. Removal of misbehaving insiders in anonymous vanets. In *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, pages 106–115, 2009.

# Appendices

## Appendix A

# RSSI

This appendix illustrates the results of the RSSI measurements' experiment between two OBUs compared to measurements done between our RSU and OBU. These results are valuable to show the ability of vehicles to verify the other vehicles' presence compared to RSU.

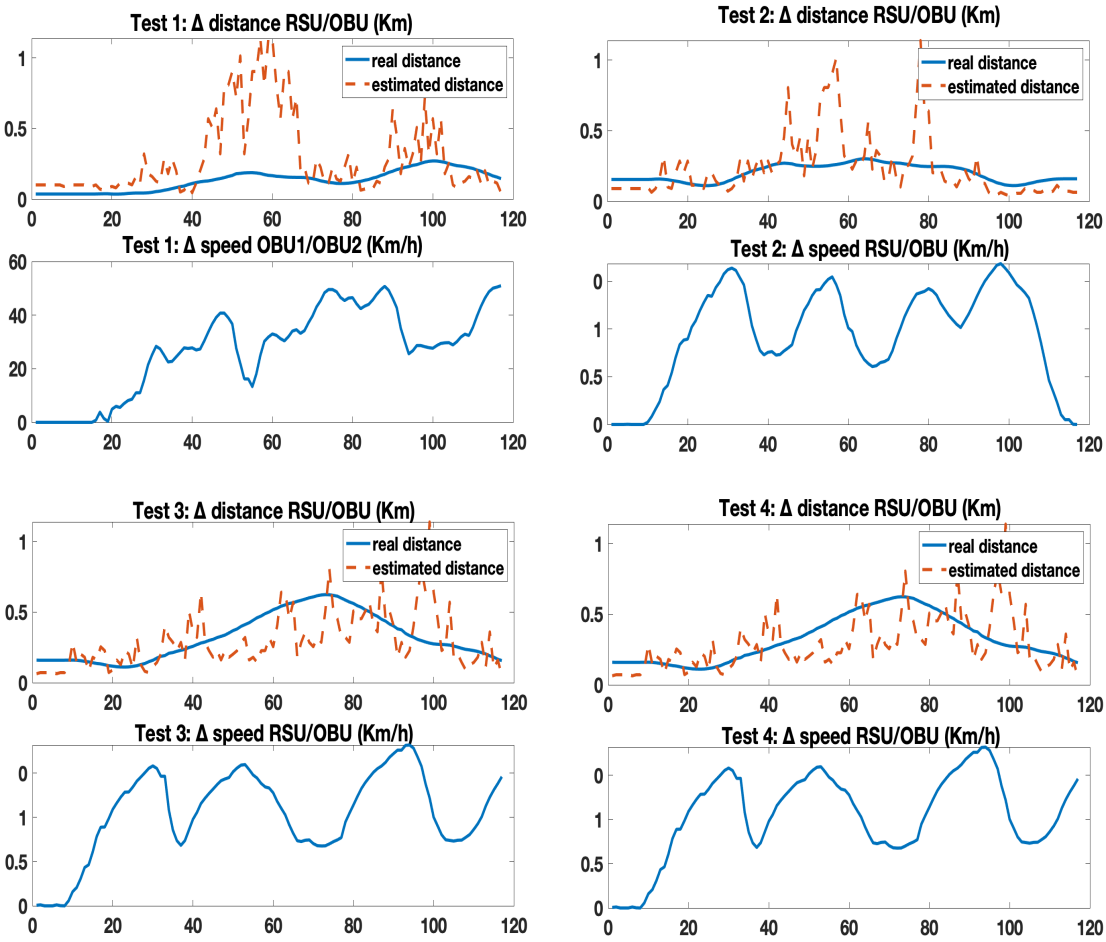



**Fig. A.1** RSSI estimation based on RSU beacons

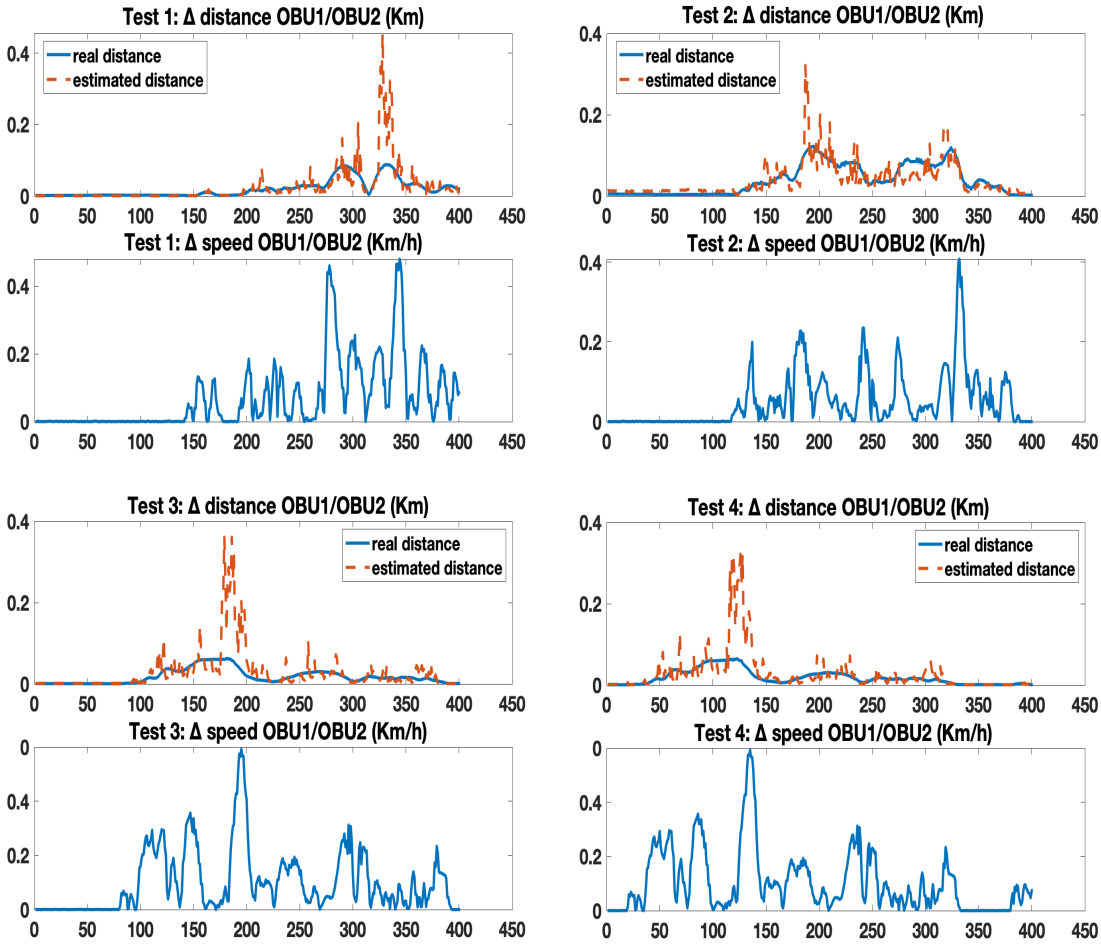
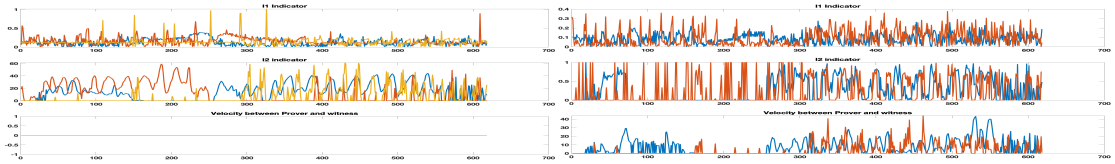



**Fig. A.2** Setup for route scenarios

**Appendix B**

# Indicators measurements based on vehicles information

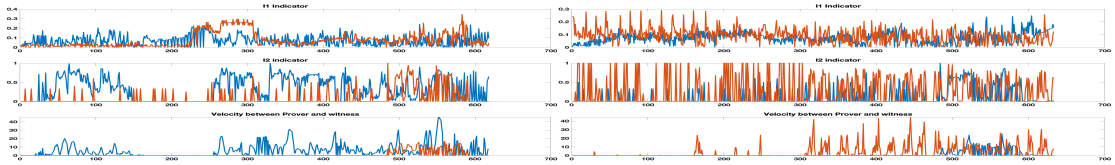
To ensure the community revocation process as indicated in the chapter 5.4, it is necessary to take awareness of the reports of each vehicle concerning each communicating node. The figures illustrate the decision variation for each node depending on its velocity with the prover. This will improve the detection performance that each has enough data and therefore to be able to give the best joint decision.



**(a)** Scenario 1: All reports about Hacker



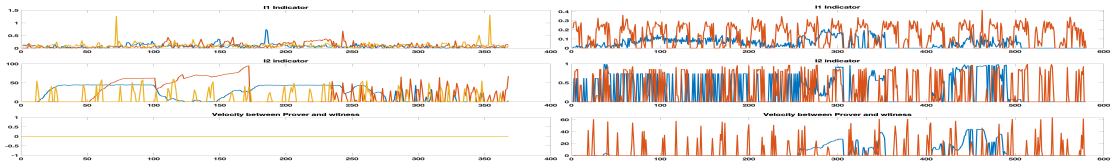
**(b)** Scenario 1: All reports about OBU 1



**(c)** Scenario 1: All reports about OBU 2



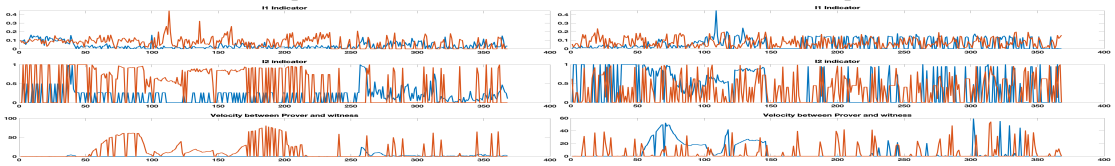
**(d)** Scenario 1: All reports about OBU 3



**(e)** Scenario 2: All reports about Hacker



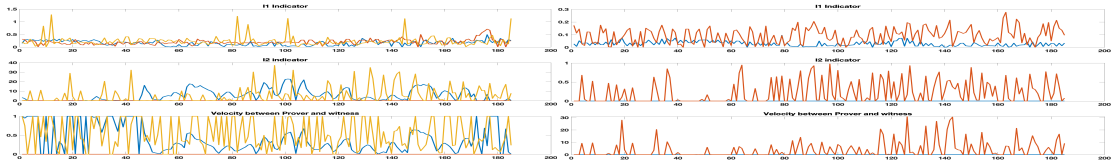
**(f)** Scenario 2: All reports about OBU 1



**(g)** Scenario 2: All reports about OBU 2



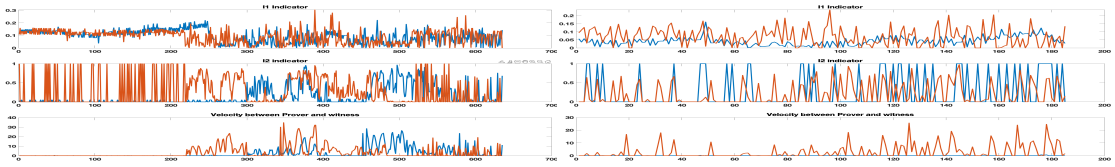
**(h)** Scenario 2: All reports about OBU 3



**(i)** Scenario 3: All reports about Hacker



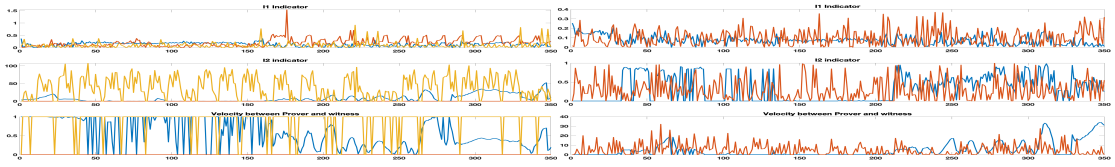
**(j)** Scenario 3: All reports about OBU 1



**(k)** Scenario 3: All reports about OBU 2



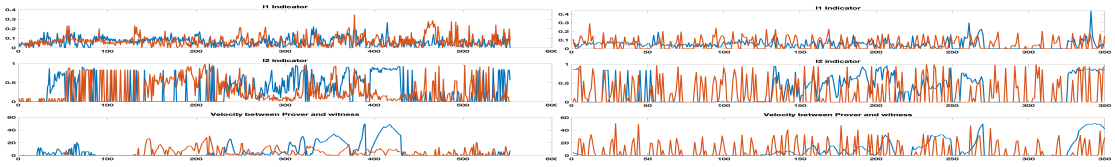
**(l)** Scenario 3: All reports about OBU 3



**(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

**Fig. B.1** Appendices: Each vehicle data from each scenario