





UNIVERSITÉ DE LILLE

ÉCOLE DOCTORALE MADIS 631

UNITÉ DE RECHERCHE INRIA LILLE - NORD EUROPE

IMT NORD EUROPE

Thèse préparée par **Marwa Slimene**
et soutenue publiquement le **11 Mai 2026**
en vue de l'obtention du grade de **Docteur en Informatique**
Discipline **Informatique et applications**

Sécurité et audit basés sur la blockchain pour les communications V2X

Devant le jury composé de :

Bruno Quoitin Professeur, Université de Mons	**Rapporteur**
Abdelwahab Boualouache Maître de conférences HDR, Institut de Science et Technologie de Luxembourg	**Rapporteur**
Maryline Laurent Professeur, Telecom SudParis	**Examinatrice**
Sidi-Mohammed Senouci Professeur, Université de Bourgogne	**Président du jury**
Ahmed Meddahi Professeur, IMT Nord Europe	**Examinateur**
Nathalie Mitton Directrice de recherche, Inria	**Directrice de thèse**
Patrick Sondi Professeur, IMT Nord Europe	**Co-directeur de thèse**

Résumé

Les communications Véhicule-à-Tout (V2X) rendent possible la conduite coopérative et automatisée grâce à l'échange de données critiques pour la sécurité entre les véhicules et leur environnement. Toutefois, assurer simultanément l'authentification, la traçabilité auditable et la protection de la vie privée constitue un défi majeur dans les scénarios sans infrastructure, où l'absence de tiers de confiance centralisé limite l'efficacité des approches traditionnelles. Concrètement, un véhicule peut être amené à freiner, dévier de sa trajectoire ou déclencher une manœuvre automatique uniquement sur la base d'un message reçu d'un autre véhicule. Si ce message est corrompu ou malveillant, il peut provoquer un accident qui ne peut pas être analysé uniquement à partir d'observations sur le terrain, mais nécessite des investigations supplémentaires afin de retracer précisément la route depuis la source jusqu'au destinataire des messages échangés, d'établir les responsabilités et d'analyser les causes de l'incident. Dans ce contexte, la blockchain apparaît comme une solution pertinente en raison de ses propriétés d'immutabilité, de distribution et de vérification sans autorité centrale. Néanmoins, les blockchains conventionnelles reposent sur des nœuds stables et continuellement connectés, une hypothèse incompatible avec la forte mobilité des réseaux véhiculaires, caractérisés par des groupes dynamiques et éphémères. Il est donc nécessaire de concevoir une nouvelle approche blockchain capable de créer, maintenir, préserver et fusionner de manière cohérente des blockchains locales. Cette thèse s'inscrit dans cette perspective en proposant une architecture d'audit décentralisée et adaptative, spécifiquement conçue pour les environnements V2X sans infrastructure, et servant de fondation à un protocole d'authentification fiable en mode déconnecté.

Tout d'abord, nous menons une analyse comparative établissant une taxonomie des stratégies d'authentification et évaluant leur capacité à concilier anonymat, intégrité et responsabilité, afin d'identifier les protocoles adaptés à des mécanismes d'audit robustes. Cette analyse met en évidence les limites et atouts des solutions existantes en matière de scalabilité, de protection de la vie privée et de dépendance à l'infrastructure, et montre que l'association de la PKI et de la blockchain permet des communications sécurisées et transparentes.

Ensuite, de nombreux travaux existants abordent l'authentification des communications V2X et Véhicule-à-Véhicule (V2V) en présence d'une infrastructure, notamment en mode Véhicule-à-Infrastructure (V2I). Dans notre travail, nous nous focalisons sur des scénarios V2V. Nous développons une méthode de mise à jour opportuniste en V2V permettant aux véhicules de synchroniser les données d'authentification lors de leurs rencontres, indépendamment de la disponibilité de l'infrastructure. Un modèle analytique basé sur la loi de Poisson est proposé afin d'évaluer la fiabilité de l'authentification en environnements déconnectés, en fonction de la durée de vie des certificats, du taux de révocation et de la

fraîcheur des bases de données. La probabilité de succès de l'authentification est analysée dans des scénarios avec des bases de données à jour et obsolètes. Les résultats démontrent la faisabilité d'une authentification V2V fiable hors couverture réseau et mettent en évidence les améliorations nécessaires pour des communications V2V sécurisées et auditables.

Afin d'assurer la traçabilité des communications, nous introduisons une architecture d'audit basée sur la blockchain, dans laquelle les véhicules maintiennent et partagent des blockchains locales en mode déconnecté, puis les fusionnent et mettre à jour la blockchain globale lors de la reconnexion. Nous évaluons d'abord les performances de la blockchain en mesurant le temps nécessaire à l'enregistrement et à la confirmation d'un message. Les résultats montrent qu'une stratégie de minage fondée sur une périodicité fixe est moins efficace qu'une stratégie basée sur la taille des blocs. À volume de trafic équivalent, cette dernière réduit significativement la durée de stockage des transactions dans les blocs, passant de plusieurs dizaines de secondes à quelques secondes, tout en augmentant le nombre de messages effectivement enregistrés dans la blockchain.

Enfin, nous intégrons les paramètres de la blockchain, notamment le temps requis pour stocker un message, dans une simulation complète de réseau véhiculaire sous VEINS/OMNeT++ pour différents scénarios, permettant une évaluation globale des performances de communication et de la blockchain.

Mots-clés : Communications véhiculaires, V2V, Identification, Authentification, Anonymisation, Audit, Blockchain, Environnement sans infrastructure.

Abstract

Vehicle-to-Everything (V2X) communications enable cooperative and automated driving through the exchange of safety-critical data between vehicles and their environment. However, simultaneously ensuring authentication, auditable traceability, and privacy protection remains a major challenge in infrastructure-less scenarios, where the absence of a centralized trusted third party limits the effectiveness of traditional approaches. Concretely, a vehicle may be required to brake, deviate from its trajectory, or trigger an automatic maneuver solely on the basis of a message received from another vehicle. If this message is corrupted or malicious, it may cause an accident that cannot be analyzed solely from field observations, but requires further investigations in order to precisely trace the path from the source to the destination of the exchanged messages, establish responsibilities, and analyze the causes of the incident. In this context, blockchain emerges as a relevant solution due to its properties of immutability, distribution, and verification without a central authority. Nevertheless, conventional blockchains rely on stable and continuously connected nodes, an assumption incompatible with the high mobility of vehicular networks, characterized by dynamic and ephemeral groups. It is therefore necessary to design a new blockchain approach capable of creating, maintaining, preserving, and coherently merging local blockchains. This thesis is part of this perspective by proposing a decentralized and adaptive audit architecture, specifically designed for infrastructure-less V2X environments, and serving as a foundation for a reliable authentication protocol in disconnected mode.

First, we conduct a comparative analysis establishing a taxonomy of authentication strategies and evaluating their ability to reconcile anonymity, integrity, and accountability, in order to identify protocols suited to robust audit mechanisms. This analysis highlights the limitations and strengths of existing solutions in terms of scalability, privacy protection, and infrastructure dependence, and shows that combining PKI and blockchain enables secure and transparent communications.

Next, many existing works address the authentication of V2X and Vehicle-to-Vehicle (V2V) communications in the presence of an infrastructure, notably in Vehicle-to-Infrastructure (V2I) mode. In our work, we focus on V2V scenarios. We develop an opportunistic V2V update method allowing vehicles to synchronize authentication data during their encounters, independently of infrastructure availability. An analytical model based on the Poisson law is proposed in order to evaluate the reliability of authentication in disconnected environments, as a function of certificate lifetime, revocation rate, and database freshness. The probability of successful authentication is analyzed in scenarios with up-to-date and obsolete databases. The results demonstrate the feasibility of reliable V2V authentication outside network coverage and highlight the improvements required for secure and auditable V2V communications.

In order to ensure communication traceability, we introduce a blockchain-based audit

architecture, in which vehicles maintain and share local blockchains in disconnected mode, then merge them and update the global blockchain upon reconnection. We first evaluate blockchain performance by measuring the time required to record and confirm a message. The results show that a mining strategy based on fixed periodicity is less efficient than a strategy based on block size. For an equivalent traffic volume, the latter significantly reduces the time transactions remain stored in blocks, decreasing from several tens of seconds to a few seconds, while increasing the number of messages actually recorded in the blockchain.

Finally, we integrate blockchain parameters, notably the time required to store a message, into a complete vehicular network simulation under VEINS/OMNeT++ for different scenarios, enabling an overall evaluation of communication and blockchain performance.

Keywords : Vehicular communications, V2V, Identification, Authentication, Anonymization, Audit, Blockchain, Infrastructure-less environment.

Table des matières

Table des matières **vi**

1 Introduction générale **1**
1.1 Contexte et motivation 1
1.2 Problématiques et objectifs 5
1.3 Organisation de la thèse 6
1.4 Liste des publications 8

2 État de l'art **9**
2.1 Concepts et processus liés à l'audit dans les réseaux véhiculaires 9
2.1.1 Systèmes d'identification 10
2.1.2 Systèmes de préservation de la vie privée 12
2.1.3 Systèmes d'authentification 14
2.1.4 Système d'audit 15
2.2 Travaux existants sur les protocoles d'authentification 17
2.2.1 Protocoles à cryptographie symétrique 18
2.2.2 Protocoles d'authentification basés sur l'identité 19
2.2.3 Protocoles à signature de groupe 20
2.2.4 Protocoles basés sur la PKI 21
2.3 Intégration de la blockchain pour la traçabilité des communications V2X 24
2.3.1 Prèsentation du paradigme blockchain 24
2.3.2 Applications de la blockchain à l'audit dans les réseaux véhiculaires 27
2.4 Cadre normatif européen : le standard ETSI TS 102 941 28
2.4.1 Architecture PKI européenne et séparation des rôles 29
2.4.2 Préservation de la vie privée et anonymat conditionnel 29
2.4.3 Gestion des comportements malveillants et auditabilité 30
2.4.4 Positionnement de nos travaux par rapport au standard ETSI . . 30

3 Fiabilité de l'authentification dans les environnements sans infrastructure **33**
3.1 Atteintes à la sécurité et à la vie privée dans les environnements V2X . . 33
3.2 Comparaison qualitative des protocoles d'authentification pour l'audit . 36
3.2.1 Critères qualitatifs d'évaluation des protocoles 36
3.2.2 Comparaison des solutions d'authentification 40
3.2.3 Discussion 42
3.3 Comparaison quantitative des protocoles d'authentification 42
3.3.1 Critères mesurables 43
3.3.2 Analyse des performances des protocoles en contexte de couverture limitée 44
3.3.3 Discussion 48

3.4 Fiabilité de l'authentification dans les environnements sans infrastructure 48
3.4.1 Modèle analytique . . . 49
3.4.2 Résultats et discussion . . . 51
3.5 Synchronisation pair-à-pair des données d'authentification hors infrastructure . . . 53
3.5.1 Protocole proposé . . . 53
3.5.2 Évaluation du protocole proposé . . . 55

4 Un système d'audit basé sur la blockchain pour des communications V2X sécurisées et traçables 59
4.1 Audit des communications V2X : objectifs, exigences et contraintes . . . 59
4.1.1 Objectifs de l'audit dans les communications V2X . . . 59
4.1.2 Exigences fonctionnelles et de sécurité d'un système d'audit . . . 60
4.1.3 Solutions d'audit traditionnelles . . . 61
4.2 Une blockchain pour l'audit des communications V2X . . . 63
4.2.1 Application de la blockchain à l'audit . . . 63
4.2.2 Vue d'ensemble des scénarios véhiculaires . . . 64
4.2.3 Opérations d'audit basées sur la blockchain . . . 65
4.3 Évaluation des performances . . . 66
4.3.1 Contexte de simulation . . . 67
4.3.2 Résultats de simulation . . . 68

5 Évaluation de la blockchain dans un réseau véhiculaire simulé 73
5.1 Mise en place du scénario autoroutier . . . 73
5.1.1 Configuration de la mobilité (SUMO) . . . 75
5.1.2 Paramètres de communication V2V (OMNeT++) . . . 76
5.2 Injection de la latence blockchain dans VEINS/OMNeT++ . . . 80
5.2.1 Extraction de la latence à partir des expérimentations blockchain 81
5.2.2 Intégration de la latence blockchain dans les communications V2X simulées . . . 81
5.3 Métriques d'évaluation . . . 82
5.3.1 Évaluation de la formation des groupes et de la traçabilité . . . 82
5.3.2 Durée de vie des blockchains locales . . . 85
5.3.3 Délai de bout en bout d'enregistrement d'un message . . . 85

6 Conclusion et perspectives générales 87
6.1 Conclusion générale . . . 87
6.2 Perspectives et travaux futurs . . . 88

Bibliographie 91

Table des figures

1.1 Architecture globale d'un réseau véhiculaire 1
1.2 Diffusion d'une alerte d'accident. 3
1.3 Avertissement d'un véhicule d'urgence en approche. 4
1.4 Réseau basé sur une infrastructure 5
1.5 Réseau ad hoc 5
1.6 Processus d'audit 6
2.1 Architecture globale des composants et processus liés à l'audit 10
2.2 Audit de l'intégrité des données pour des communications véhiculaires sécurisées. 17
2.3 Stratégies d'authentification 18
2.4 Système d'infrastructure à clés publiques pour l'authentification. 21
2.5 Vue d'ensemble des principaux concepts liés à la blockchain 24
3.1 Critères qualitatifs pour l'évaluation des protocoles d'authentification. . . . 37
3.2 Scénario d'authentification V2V lors de la transition d'une zone couverte par l'infrastructure vers une zone rurale non couverte. 49
3.3 Évolution de la probabilité d'authentification en fonction du temps selon la durée de vie des certificats. 53
3.4 Comportement d'un véhicule de confiance dans un environnement dépourvu d'infrastructure. 54
3.5 Opportunités stratégiques de mise à jour en fonction de la position et du sens de circulation des véhicules. 55
3.6 Amélioration de P_{auth} sur un segment autoroutier de longueur $L = 600$ km. . 56
3.7 Amélioration de P_{auth} sur un segment autoroutier de longueur $L = 100$ km. . 57
4.1 Processus d'audit de la blockchain pour la traçabilité des messages malveillants. 63
4.2 Vue globale d'un système d'audit basé sur la blockchain pour les communications V2X sans infrastructure. 65
4.3 Latence moyenne en fonction des différents taux de charge des messages . . 69
4.4 Évolution du débit de la blockchain en fonction de la densité véhiculaire . . 70
4.5 Impact du nombre de transactions par bloc sur la latence moyenne, le pourcentage de messages confirmés et le nombre de blocs minés pour 100 véhicules 71
5.1 Topologie autoroutière simulée illustrant les communications V2I et V2V dans l'environnement SUMO. 75
5.2 Processus de formation de groupe V2V et états des véhicules. 78
5.3 Extrait d'une blockchain locale partagée entre les véhicules membres d'un groupe V2V. 80
5.4 Fenêtre de mesure 82
5.5 Durée de vie moyenne des blockchains locales en fonction de la densité véhiculaire 85
5.6 Latence de la blockchain et délai de transmission radio en fonction de la densité véhiculaire 86

Liste des tableaux

3.1 Résistance des schémas d'authentification face aux défis de sécurité et de confidentialité en V2X 35
3.2 Comparaison qualitative des solutions d'authentification 41
3.3 Comparaison entre BCPPA et ACB-MAC à partir des évaluations proposées par leurs auteurs respectifs 44
3.4 Récapitulatif des principales valeurs de paramètres pour les communications V2X 52
4.1 Exemple des approches traditionnelles d'audit dans les systèmes V2X 62
4.2 Comparaison des performances pour des intervalles de minage temporels de 1 s et 2 s 68
4.3 Comparaison des stratégies de minage : approche basée sur le débit et approche basée sur le nombre total de messages générés par seconde 70
5.1 Paramètres de simulation pour les différents niveaux de densité véhiculaire . 76
5.2 Paramètres radio et du canal de communication 77
5.3 Extraction de la latence moyenne d'enregistrement d'un message V2X dans la blockchain 81
5.4 Évaluation de la traçabilité des messages V2X pour une densité de 25 v/km 83
5.5 Évaluation de la traçabilité des messages V2X pour une densité de 102 v/km 84
5.6 Évaluation de la traçabilité des messages V2X pour une densité de 198 v/km 84

Introduction générale 1

1.1 Contexte et motivation . . 1
1.2 Problématiques et objectifs 5
1.3 Organisation de la thèse . 6
1.4 Liste des publications . . . 8

1.1 Contexte et motivation

La communication véhiculaire se positionne à l'avant-garde de l'innovation technologique dans le secteur des transports, incarnant un écosystème dynamique au sein duquel l'information circule en continu grâce aux technologies sans fil. Au cœur de cet écosystème, présenté dans la figure 1.1 se trouvent des véhicules équipés d'unités embarquées (OBU) qui collectent et partagent activement des données avec leur environnement routier, évaluant de manière dynamique le flux de trafic afin d'offrir une expérience de conduite intelligente et confortable [1].

[1]: Sandro Chiocchio, Arianna Persia, Francesco Valentini, Elena Cinque, Marco Pratesi et Fortunato Santucci. « Integrated Simulation Environments for Vehicular Communications in Cooperative Road Transportation Systems ». In : *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*. 2018

Chaque véhicule peut établir différents types de communications avec les diverses entités du domaine véhiculaire. Ces communications comprennent notamment, le Vehicle-to-Vehicle (V2V), qui permet le partage d'informations telles que la position, la vitesse et l'état de la chaussée dans le but de promouvoir la sécurité, de réduire la congestion et d'optimiser la consommation de carburant, le Vehicle-to-Infrastructure (V2I), permettant l'interaction avec les éléments de l'infrastructure routière tels que les feux de signalisation et les stations de péage, ainsi que le Vehicle-to-Cloud (V2C), offrant un accès à divers services cloud pour des informations cruciales telles que les conditions météorologiques et les mises à jour cartographiques. Le Vehicle-to-Pedestrian (V2P), par lequel les piétons interagissent avec les véhicules via leurs appareils personnels, garantit une coordination sécurisée et renforce la sécurité des piétons. Collectivement désignées sous le terme Vehicle-to-Everything (V2X), ces communications contribuent à la création d'un environnement de transport intelligent et connecté, favorisant non seulement l'essor des véhicules autonomes, mais jetant également les bases d'une mobilité plus sûre et plus efficiente [2].

[2]: Xinyu Zhang, Junxian Li, Jingyi Zhou, Shiyan Zhang, Jingyuan Wang, Yi Yuan, Jiale Liu et Jun Li. « Vehicle-to-Everything Communication in Intelligent Connected Vehicles : A Survey and Taxonomy ». In : *Automotive Innovation* 8.1 (2025)

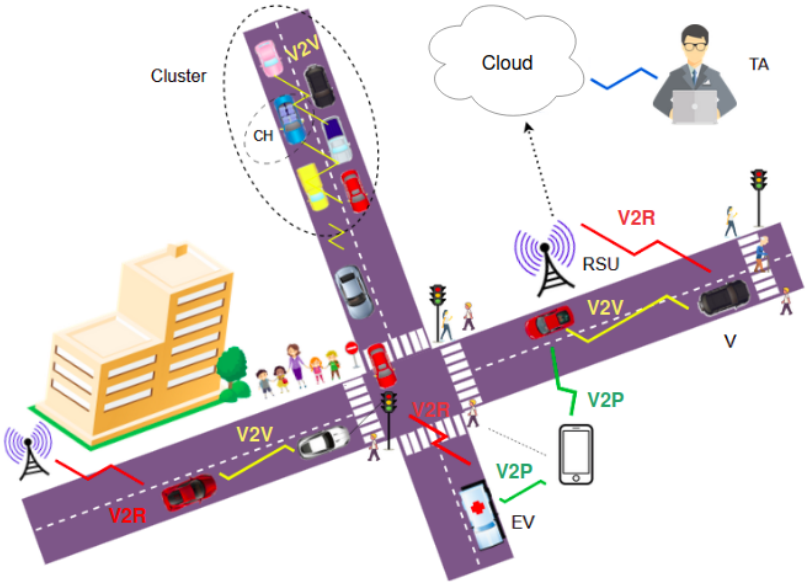

Figure 1.1 – Architecture globale d'un réseau véhiculaire

Plusieurs entités et composants coopèrent afin d'établir une communication efficace, d'assurer la gestion des données et de garantir la sécurité des échanges, comme illustré dans la figure 1.1.

Véhicules : Les véhicules agissent comme des nœuds au sein du réseau de transport connecté. Ils sont équipés d'une OBU ainsi que de divers capteurs leur permettant de collecter et d'échanger des informations avec leur environnement. L'OBU supporte différentes interfaces de communication, notamment les Communications Dédiées à Courte Portée (DSRC), basées sur le standard IEEE 802.11p, ainsi que le Cellular-V2X (C-V2X) reposant sur les réseaux cellulaires 4G/5G, permettant la communication avec les autres véhicules et les infrastructures routières[3]. Ces unités permettent aux véhicules d'envoyer, de recevoir, de traiter, de stocker des données et d'assurer leur propre localisation au sein du réseau. Chaque véhicule diffuse en temps réel des informations essentielles sur les conditions de circulation, à destination des véhicules voisins et des infrastructures environnantes.

[3]: Falk Dettinger, Matthias Weiß, Daniel Dittler, Johannes Stümpfle, Maurice Artelt et Michael Weyrich. *A Survey on Performance, Current and Future Usage of Vehicle-To-Everything Communication Standards*. 2024. arXiv : 2410 . 10264 [cs.ET]

Véhicules d'urgence (EV) : Les véhicules d'urgence, comme les ambulances, les camions de pompiers et les voitures de police, jouent un rôle essentiel dans la gestion des incidents de sécurité publique [4]. Leur efficacité opérationnelle dépend d'une navigation rapide et fiable ainsi que de capacités de communication avancées. L'octroi de privilèges spécifiques à ces véhicules dans les systèmes de communication véhiculaire est crucial pour garantir des interventions rapides et une coordination efficace lors des situations d'urgence.

[4]: Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn et Roy Goudy. « A Security Credential Management System for V2X Communications ». In : *IEEE Transactions on Intelligent Transportation Systems* 19.12 (2018)

Autorité de confiance (TA) : Le TA est une entité tierce considérée comme digne de confiance [5]. Elle joue un rôle central dans le maintien de la confiance au sein du système de communication véhiculaire. Elle veille à ce que tous les participants et dispositifs respectent les règles et protocoles établis et intervient en cas de comportement anormal ou malveillant. Dotée de capacités de calcul et de stockage suffisantes, la TA est généralement responsable de l'initialisation des paramètres du système, de l'enregistrement des identités réelles des véhicules, de la délivrance et de la révocation des certificats, ainsi que de la garantie de la traçabilité au sein du système. En cas d'incident, comme la diffusion d'informations falsifiées par un véhicule malveillant, la TA peut identifier l'auteur grâce aux informations d'authentification enregistrées.

[5]: R. Lu, X. Lin, H. Zhu, P.-H. Ho et X. Shen. « ECPP : Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications ». In : *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*. 2008

Les Unités routières (RSU) : Les RSUs sont des composants d'infrastructure déployés le long des routes pour faciliter la communication entre les véhicules et le réseau. Chaque RSU couvre une zone géographique spécifique et agit comme point d'accès pour les véhicules environnants, en utilisant différentes technologies de communication sans fil, notamment le DSRC et C-V2X. Elles collectent les données transmises par les véhicules, relaient les informations de l'infrastructure et servent de passerelles vers les plateformes cloud pour le traitement et le stockage des données.

Les serveurs cloud : Les serveurs cloud jouent un rôle central dans l'extension des capacités de calcul et de stockage des véhicules et des RSUs. En effet, dans les systèmes de transport intelligents (ITS), les véhicules sont souvent équipés de dispositifs aux ressources limitées, tant en termes de puissance de calcul que de capacité mémoire. Le paradigme cloud offre ainsi une alternative efficace pour la collecte, l'agrégation et l'échange d'informations à grande échelle [6]. Il permet également d'héberger des entités de confiance du réseau, telles que le TA.

[6]: Teodora Mecheva et Nikolay Kakanakov. « Cloud based Intelligent Transportation System architecture ». In : *2021 International Conference Automatics and Informatics (ICAI)*. 2021

Dans les réseaux véhiculaires ad hoc (VANET), les véhicules doivent s'organiser dynamiquement afin de maintenir la communication et de continuer à échanger des informations. Dans ce contexte, on distingue notamment :

Cluster : Un groupe de véhicules coopérant entre eux dans certains contextes de circulation. Par exemple, dans les scénarios de platooning, les véhicules circulent à courte distance les uns des autres, à vitesse et direction similaires. En formant un cluster, les véhicules peuvent échanger des informations de manière efficace et coordonner leurs actions afin d'améliorer la sécurité et l'efficacité du trafic.

Chef de cluster (CH) : Un véhicule désigné pour gérer et coordonner le cluster. Le CH supervise la participation des véhicules membres, contrôle leur entrée et leur sortie du cluster, et agit souvent comme interface de communication entre les membres du cluster et les entités externes telles que les RSUs ou les services d'infrastructure. Ces véhicules disposent généralement de capacités de communication avancées, incluant plusieurs interfaces réseau.

Ces différentes entités collaborent au sein d'un écosystème véhiculaire dont les communications servent des objectifs concrets en matière de sécurité routière, d'efficacité du trafic et de confort de conduite

Réduire les accidents de la route :

La prévention des accidents constitue la motivation première des communications V2X. Grâce aux échanges V2V, un conducteur peut être alerté en temps réel d'un danger situé hors de son champ de vision, tel qu'un freinage brusque d'un véhicule précédent, un obstacle sur la chaussée ou des conditions météorologiques dégradées, et adapter son comportement avant même de percevoir visuellement le danger [7] [8]. Un exemple concret est la diffusion d'une alerte d'accident illustré à la figure 1.2, lorsqu'un véhicule équipé d'une OBU est impliqué dans une collision, il génère immédiatement un message d'alerte contenant les coordonnées spatio-temporelles de l'incident (t, x, y, z). Ce message est propagé par relayage multi-sauts entre les véhicules équipés d'OBU, permettant d'avertir les véhicules distants au-delà de la portée radio directe.

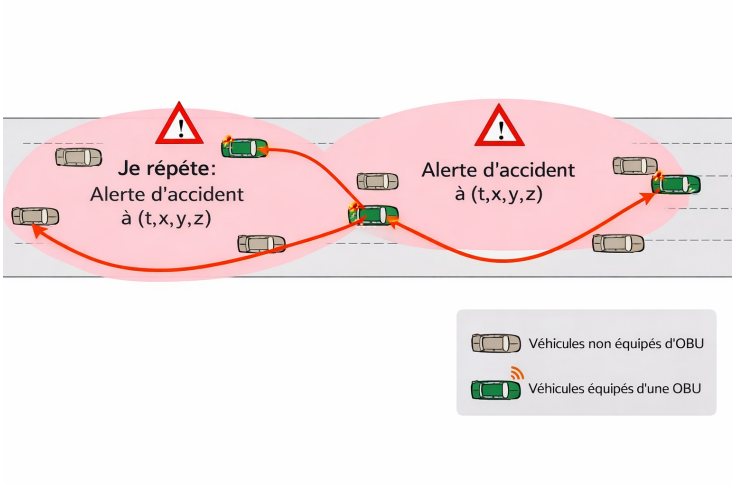

Figure 1.2 – Diffusion d'une alerte d'accident.

[7]: Tianqi Wang, Sukmin Kim, Wenxuan Ji, Enze Xie, Chongjian Ge, Junsong Chen, Zhenguo Li et Ping Luo. *DeepAccident : A Motion and Accident Prediction Benchmark for V2X Autonomous Driving*. 2023. arXiv : 2304.01168 [cs.CV]

[8]: Bruno Ribeiro, Maria Nicolau et Alexandre Santos. « Machine Learning for VRUs accidents prediction using V2X data ». In : juin 2023

Améliorer la gestion du trafic :

À l'échelle du réseau routier, l'agrégation des données V2X par les RSUs et les serveurs cloud permet aux gestionnaires du trafic de disposer d'une vision globale et en temps réel de l'état du réseau, facilitant l'ajustement dynamique des plans de feux de signalisation et la mise en place de déviations préventives. Un cas d'usage particulièrement critique est celui des véhicules d'urgence comme illustré à la figure 1.3, grâce aux communications V2X, une ambulance ou un véhicule de pompiers diffuse en continu sa position et sa trajectoire aux véhicules environnants. À la réception de ce message, les systèmes embarqués déclenchent une alerte pour couper la radio, et diffuse une annonce d'un véhicule d'urgence en approche, invitant les conducteurs à libérer le passage [9]. Cette coordination réduit significativement le temps d'intervention des secours.

[9]: Hossam M. Zohir, Islam M. Ismael, Eman M. El-Gendy et Mahmoud M. Saafan. « Advancements in Accident-Aware Traffic Management : A Comprehensive Review of V2X-Based Route Optimization ». In : *Scientific Reports* 15.1 (2025)

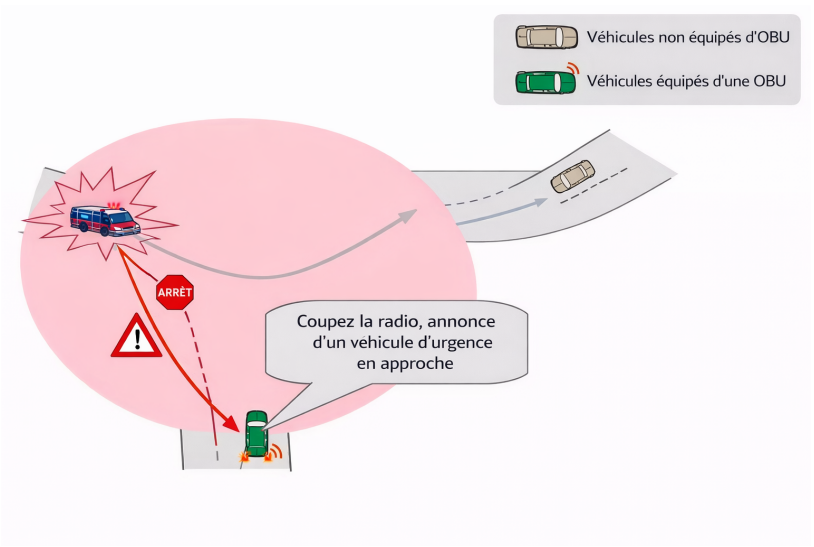

Figure 1.3 – Avertissement d'un véhicule d'urgence en approche.

Réduire le temps de trajet :

Les communications V2X permettent aux véhicules de partager en temps réel des informations sur les conditions de circulation, telles que la densité du trafic, les incidents et les travaux, offrant aux systèmes de navigation embarqués les données nécessaires pour optimiser dynamiquement les itinéraires. Contrairement aux systèmes de navigation classiques reposant sur des données centralisées potentiellement obsolètes, les communications V2X produisent une information locale, fraîche et distribuée, reflétant fidèlement l'état réel du réseau routier. Par exemple, lorsqu'un véhicule détecte un ralentissement important sur son itinéraire, il diffuse immédiatement cette information aux véhicules environnants et aux RSUs. Ces dernières relaient l'alerte aux véhicules encore distants, leur permettant d'emprunter un itinéraire alternatif avant même d'atteindre la zone de congestion, réduisant ainsi le temps de trajet de l'ensemble des usagers concernés.

Améliorer le confort de conduite :

Les applications V2X contribuent à rendre l'expérience de conduite plus sereine en réduisant la charge cognitive imposée au conducteur. La gestion

coopérative des intersections, le maintien automatique des distances de sécurité en convoi ou encore la coordination aux passages piétons sont autant d'exemples d'applications qui préparent progressivement le terrain au déploiement des systèmes de conduite autonome [10].

Cependant, l'efficacité de toutes ces applications repose entièrement sur la confiance accordée aux messages reçus, ce qui soulève des questions fondamentales de sécurité et de confiance que nous allons examiner dans la section suivante.

[10]: Seo-Wook Park, Raynier Suresh et Anusha Ailuri. « Collision Avoidance System at Urban Intersections Using V2X Communication ». In : *WCX SAE World Congress Experience*. SAE International, avr. 2025

1.2 Problématiques et objectifs

Dans les systèmes de transport intelligents, les communications V2X jouent un rôle central dans la coordination des véhicules et la diffusion d'informations critiques liées à la sécurité routière. Les véhicules échangent en permanence des messages concernant leur position, leur vitesse, l'état du trafic ou la présence d'événements dangereux sur la route. Ces informations sont exploitées par les systèmes embarqués afin d'assister le conducteur ou de déclencher automatiquement certaines actions, telles que le freinage d'urgence ou l'évitement d'obstacles. Dans ce contexte, la fiabilité et l'authenticité des messages échangés constituent des conditions essentielles au bon fonctionnement du système.

Au-delà des situations accidentelles, les réseaux véhiculaires peuvent être exposés à des comportements malveillants. Un véhicule compromis pourrait diffuser de fausses alertes d'accident ou de congestion afin de perturber la circulation ou de manipuler le trafic à son avantage [11]. Dans un tel scénario, l'absence d'un mécanisme fiable de traçabilité rend difficile l'identification de l'origine du message frauduleux et l'analyse de sa propagation au sein du réseau.

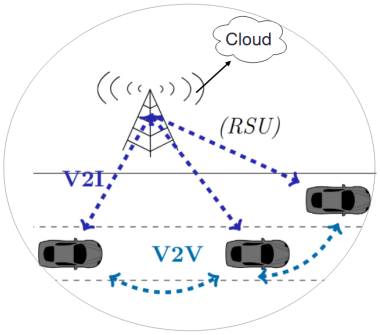

Figure 1.4 – Réseau basé sur une infrastructure

[11]: Muhammad Sameer Sheikh, Jun Liang et Wensong Wang. « A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs) ». In : *Sensors* 19.16 (août 2019)

Ces situations illustrent l'importance de disposer d'un mécanisme capable d'enregistrer et de préserver les traces des communications échangées entre les entités du réseau véhiculaire. Dans les architectures actuelles, cette fonction est assurée par des entités centralisées telles que les autorités de confiance ou les infrastructures cloud (figure1.4). Bien que ces entités jouent un rôle important, cette centralisation introduit un point unique de défaillance susceptible d'être compromis ou manipulé, et suppose un niveau élevé de confiance dans l'entité chargée de gérer et de conserver les données.

Cette limitation devient d'autant plus critique dans les scénarios où les véhicules évoluent dans des environnements dépourvus d'infrastructure fixe, formant un réseau ad hoc dans lequel les échanges s'effectuent directement entre nœuds mobiles sans connexion continue vers un serveur central (figure3.5). La nature hautement dynamique de ces réseaux, dans lesquels les véhicules entrent et sortent continuellement, les connexions sont temporaires et les messages se propagent rapidement, rend particulièrement difficile la conservation d'un historique cohérent et vérifiable des communications.

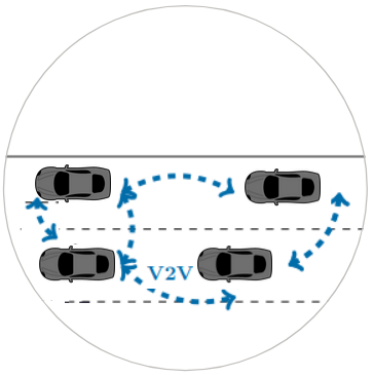

Figure 1.5 – Réseau ad hoc

Face à ces limitations, il devient indispensable de concevoir un système d'audit distribué, capable d'enregistrer et de préserver de manière infalsifiable les traces des échanges entre les entités du réseau véhiculaire, tout en prenant en compte la mobilité des nœuds, les déconnexions fréquentes et l'absence éventuelle d'infrastructure fixe propres aux réseaux VANET.

Dans ce contexte, l'objectif de cette thèse est d'explorer le potentiel de la blockchain afin de concevoir une solution d'audit infalsifiable et de vérification unilatérale des traces d'échanges dans les communications véhiculaires. L'approche proposée repose sur le maintien d'un registre décentralisé et immuable des échanges V2X, dont l'intégrité est garantie par des mécanismes de consensus et de chaînage cryptographique, rendant toute tentative d'altération ou de falsification détectable, y compris par un nœud administrateur [12]. Contrairement aux architectures traditionnelles qui délèguent la confiance à des autorités centrales, cette solution vise à distribuer la fonction d'audit entre les participants du réseau, éliminant ainsi les points de défaillance uniques et réduisant la dépendance aux tiers de confiance. Ce faisant, elle renforce simultanément la **traçabilité** des communications, la **non-répudiation** des échanges et la **transparence** du processus d'audit, tout en restant opérationnelle dans des environnements V2V dépourvus d'infrastructure fixe.

[12]: Souad BelMannoubi, Haifa Touati, Mohamed Hadded, Khalifa Toumi, Oyunchimeg Shagdar et Farouk Kamoun. « A comprehensive survey on blockchain-based C-ITS applications : Classification, challenges, and open issues ». In : *Vehicular Communications* 43 (2023)

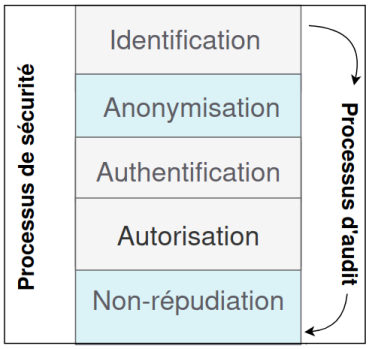

Figure 1.6 – Processus d'audit

Dans cette perspective, les travaux présentés dans cette thèse visent à répondre aux objectifs suivants :

- Analyser de manière approfondie les mécanismes d'identification, d'anonymisation et d'authentification proposés dans la littérature pour les communications V2X, et évaluer leur adéquation au regard des exigences d'audit (figure4.1).
- Analyser et comparer qualitativement et quantitativement les protocoles d'authentification existants afin d'identifier les approches les plus pertinentes pouvant servir de base à la conception d'un mécanisme d'audit fiable dans les réseaux véhiculaires.
- Développer une solution d'authentification adaptée aux communications V2V dans des environnements dépourvus d'infrastructure, capable de fonctionner dans des réseaux ad hoc caractérisés par une mobilité élevée et une connectivité intermittente.
- Concevoir une solution d'audit infalsifiable basée sur la blockchain afin d'assurer la traçabilité des échanges V2V, même en l'absence d'infrastructure centralisée.

Ces objectifs soulèvent les questions de recherche suivantes auxquelles cette thèse apporte des réponses :

- **QR1 :** Quels protocoles d'authentification existants sont les mieux adaptés pour supporter les exigences d'un système d'audit dans les communications V2X, en termes d'identification et de protection de la vie privée ?
- **QR2 :** Comment garantir la fiabilité de l'authentification V2V et comment les véhicules peuvent-ils accéder aux données d'authentification dans des environnements dépourvus d'infrastructure ?
- **QR3 :** Comment concevoir une architecture d'audit décentralisée basée sur la blockchain, capable de maintenir la traçabilité des communications V2X hors de l'accès à l'infrastructure ?
- **QR4 :** Comment évaluer les performances d'un mécanisme d'audit basé sur la blockchain dans un environnement véhiculaire ?

1.3 Organisation de la thèse

Afin de mettre en évidence les contributions issues de l'ensemble de mes travaux au regard des problématiques susmentionnées, la présentation de ce mémoire sera déclinée sous la forme de plusieurs chapitres.

Le chapitre 1 constitue le présent chapitre d'introduction. Il présente le contexte général des communications véhiculaires V2X, décrit les entités et les modes de communication qui composent cet écosystème, illustre la nécessité d'un système d'audit à travers des cas réels, puis formule la problématique, les objectifs et les questions de recherche qui guident l'ensemble de ce travail.

Le chapitre 2 est consacré à l'état de l'art. Il dresse un panorama structuré des travaux existants relatifs aux mécanismes d'identification, de préservation de la vie privée et d'authentification dans les réseaux véhiculaires. Il présente ensuite une taxonomie des principales familles de protocoles d'authentification et analyse leur capacité à répondre aux exigences d'un système d'audit, avant d'examiner l'intégration de la blockchain pour la traçabilité des communications V2X et de positionner nos contributions par rapport au standard européen ETSI TS 102 941.

Le chapitre 3 traite de la fiabilité de l'authentification dans les environnements sans infrastructure. Après une analyse des menaces et des contraintes spécifiques aux scénarios V2V, il propose une comparaison qualitative et quantitative des protocoles d'authentification dans un contexte de couverture réseau limitée. Il développe ensuite un modèle analytique permettant d'évaluer la probabilité de succès de l'authentification en fonction des paramètres du réseau, puis présente un protocole de synchronisation opportuniste des données d'authentification entre véhicules lors de leurs rencontres, dont il évalue les performances par une analyse analytique.

Le chapitre 4 présente la solution d'audit basée sur la blockchain proposée pour les communications V2X sans infrastructure. Il définit les objectifs et les exigences fonctionnelles d'un tel système, analyse les limites des approches traditionnelles, puis décrit en détail l'architecture proposée. Il évalue ensuite, à l'aide d'une simulation, les performances de la blockchain en mesurant le temps nécessaire à l'enregistrement et à la confirmation d'un message, et identifie la stratégie de minage la mieux adaptée aux contraintes des réseaux véhiculaires.

Le chapitre 5 présente l'intégration des paramètres de la blockchain mesurés dans le chapitre précédent, notamment le temps requis pour stocker et confirmer un message, dans une simulation véhiculaire complète sous VEINS/OMNeT++. Il analyse ensuite les résultats obtenus pour différents scénarios de densité véhiculaire, permettant une évaluation globale et réaliste des performances de communication et de la blockchain dans des conditions représentatives d'un réseau véhiculaire réel.

1.4 Liste des publications

Les travaux réalisés dans le cadre de cette thèse ont donné lieu aux publications suivantes :

Revue internationale

Slimene, Marwa, Amira Chriki, Nathalie Mitton, Patrick Sondi, and Ahmed Meddahi. "A Comparative Survey of Authentication Schemes Suitable for the Audit of V2X Communications." IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 11, pp. 18304-18324, Nov. 2025.

Conférences internationales avec actes et comité de lecture

Slimene, Marwa, Nathalie Mitton, Patrick Sondi, and Ahmed Meddahi. "An enhanced authentication solution for infrastructureless vehicle environments." In 2025 21th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1-6. IEEE, 2025.

Slimene, Marwa, Nathalie Mitton, Patrick Sondi, and Ahmed Meddahi. "A Blockchain based Audit System for Secure and Traceable Vehicle-to-Everything Communications," accepted as regular paper to IEEE Vehicular Technology Conference, spring 2026, Nice, France.

État de l'art 2

Introduction

Les communications Véhicule-à-Tout (V2X) constituent un pilier fondamental des systèmes de transport intelligents, en permettant l'échange d'informations critiques pour la sécurité et l'efficacité du trafic. Toutefois, la nature ouverte, dynamique et hautement mobile des réseaux véhiculaires soulève des défis majeurs en matière de sécurité, de protection de la vie privée et de responsabilité. En particulier, l'authentification des entités communicantes doit non seulement garantir l'intégrité et l'authenticité des messages échangés, mais également permettre une traçabilité exploitable à des fins d'audit, tout en préservant la vie privée des usagers légitimes.

Dans ce contexte, de nombreux schémas d'authentification ont été proposés dans la littérature, reposant sur des paradigmes cryptographiques variés et des hypothèses différentes quant à la disponibilité de l'infrastructure et des autorités de confiance. Cependant, tous ne sont pas adaptés aux exigences spécifiques d'un système d'audit fiable, en particulier dans des environnements V2X dépourvus d'infrastructure continue.

Ce chapitre propose un état de l'art des mécanismes d'authentification appliqués aux communications V2X, en mettant l'accent sur leur capacité à supporter des fonctionnalités d'audit telles que la traçabilité et la non-répudiation. Après avoir présenté les concepts fondamentaux liés à l'audit dans les réseaux véhiculaires, nous présentons une taxonomie des principales familles de protocoles d'authentification existants, avant d'analyser leur conformité aux exigences normatives, notamment celles définies par le standard européen ETSI TS 102 941. Cette analyse vise à identifier les limites des approches actuelles et à dégager les éléments clés nécessaires à la conception d'un mécanisme d'authentification adapté à un audit décentralisé et robuste.

2.1 Concepts et processus liés à l'audit dans les réseaux véhiculaires

Pour participer à un système de communication, les utilisateurs doivent pouvoir accorder une confiance totale à la sécurité, à l'intégrité et à la confidentialité de leurs données [13]. En effet, lorsqu'ils interagissent avec les autres véhicules, ils doivent pouvoir distinguer les messages légitimes des tentatives malveillantes telles que la diffusion de fausses informations de trafic. Ils doivent être en mesure de signaler les incidents a posteriori, en ayant l'assurance que chaque interaction est enregistrée de manière fiable par le système. Par conséquent, la garantie de l'auditabilité des communications apparaît comme une exigence fondamentale.

L'audit repose initialement sur l'enregistrement sécurisé, intègre et infalsifiable des flux de données critiques ainsi que des événements significatifs. Il permet également d'identifier les vulnérabilités potentielles du système et de faciliter la mise en œuvre de mesures correctives adaptées afin de renforcer la sécurité globale.

2.1 Concepts et processus liés à l'audit dans les réseaux véhiculaires 9
2.1.1 Systèmes d'identification 10
2.1.2 Systèmes de préservation de la vie privée 12
2.1.3 Systèmes d'authentification 14
2.1.4 Système d'audit 15
2.2 Travaux existants sur les protocoles d'authentification 17
2.2.1 Protocoles à cryptographie symétrique 18
2.2.2 Protocoles d'authentification basés sur l'identité . 19
2.2.3 Protocoles à signature de groupe 20
2.2.4 Protocoles basés sur la PKI 21
2.3 Intégration de la blockchain pour la traçabilité des communications V2X 24
2.3.1 Prèsentation du paradigme blockchain 24
2.3.2 Applications de la blockchain à l'audit dans les réseaux véhiculaires . . . 27
2.4 Cadre normatif européen : le standard ETSI TS 102 941 28
2.4.1 Architecture PKI européenne et séparation des rôles 29
2.4.2 Préservation de la vie privée et anonymat conditionnel 29
2.4.3 Gestion des comportements malveillants et auditabilité 30
2.4.4 Positionnement de nos travaux par rapport au standard ETSI 30

[13]: Panagiotis Papadimitratos, Levente Buttyan, Tamas Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung et Jean-Pierre Hubaux. « Secure vehicular communication systems : design and architecture ». In : *IEEE Communications Magazine* 46.11 (2008)

Afin d'illustrer les caractéristiques clés d'un système d'audit efficace, nous nous référerons à la figure 5.1, inspirée des travaux de [14], qui présente les composants essentiels nécessaires à l'établissement d'un cadre d'audit robuste.

[14]: Chaima Zidi, Patrick Sondi, Nathalie Mitton, Martine Wahl et Ahmed Meddahi. « Review and Perspectives on the Audit of Vehicle-to-Everything Communications ». In : *IEEE Access* 11 (2023)

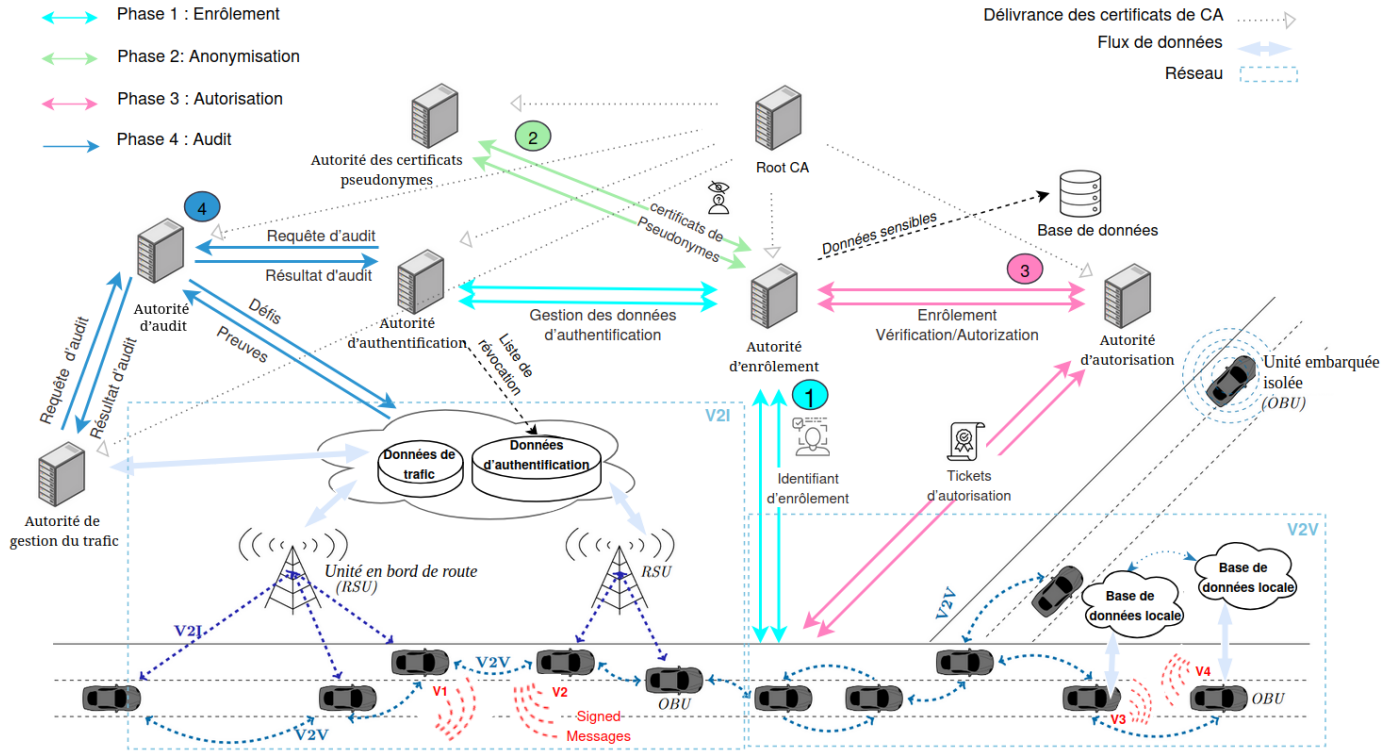

Figure 2.1 – Architecture globale des composants et processus liés à l'audit

Dans cette section, nous détaillerons et décrirons les différents aspects liés à l'audit dans les réseaux véhiculaires, avec un focus sur la définition et l'analyse des mécanismes d'identification, de préservation de la vie privée et d'authentification, lesquels constituent les fondements essentiels d'un audit fiable et sécurisé.

2.1.1 Systèmes d'identification

L'audit repose sur le système d'identification pour assurer la traçabilité des interactions au sein d'un réseau de communication : il permet d'identifier avec précision les entités impliquées dans chaque transaction, de retracer l'origine, la destination et la nature des échanges, et de détecter toute activité suspecte ou non autorisée. Cette traçabilité fine est essentielle au maintien de l'intégrité du système, car elle garantit que les actions sont réalisées par des entités légitimes et que l'ensemble des transactions est enregistré et auditable.

Le concept d'identification dans les communications véhiculaires dépasse les seuls mécanismes techniques et s'inscrit plus largement dans la construction de l'identité au sein des processus de communication, comme l'ont souligné [15] et [16]. Ces travaux mettent en évidence le rôle déterminant de la communication dans la formation et la définition de l'identité des individus ou plus généralement des entités, un principe qui revêt une importance particulière dans le contexte des réseaux véhiculaires. Dans ce cadre, l'identité n'est pas uniquement portée par un identifiant ou un certificat, elle se construit également à travers les interactions, car les autres entités et le système ajustent le niveau de confiance accordé en fonction des attributs déclarés et des comportements observés.

[15]: Edmond-Marc Lipiansky. « L'identité dans la communication ». In : *Communication & Langages* 97.1 (1993)

[16]: Patrick Charaudeau. « La communication et le droit à la parole dans une interaction du même et de l'autre ». In : *Communication & Langages* (1991)

En s'appuyant sur les travaux de [17] relatifs à la construction et à la gestion des identités dans les systèmes de communication dynamiques, il apparaît que le processus d'identification dans les communications véhiculaires s'inscrit dans une dynamique similaire. Il s'agit d'un processus évolutif au cours duquel les identités des entités communicantes, qu'il s'agisse des conducteurs, des véhicules ou des infrastructures, sont continuellement construites et reconstruites. Cette négociation joue un rôle central dans l'établissement de la confiance et dans la garantie de l'authenticité des canaux de communication, deux éléments indispensables au bon fonctionnement des réseaux véhiculaires.

[17]: Marcel Burger. « Vers une analyse de la construction des identités dans les discours de communication publique ». In : *Cahiers du Centre de Linguistique et des Sciences du Langage* 34 (déc. 2013)

Plusieurs méthodes d'identification sont mises en œuvre afin d'assurer la sécurité, la confidentialité et l'efficacité des échanges d'informations. Ces méthodes doivent concilier la nécessité d'identifier de manière fiable Les véhicules participants au réseau véhiculaire avec l'exigence de préservation de leur vie privée. Comme illustré à la Figure 5.1, lorsqu'un véhicule souhaite participer à un système de communication véhiculaire, il doit s'enregistrer auprès d'une autorité d'enregistrement. Celle-ci stocke les données personnelles du véhicule dans une base de données sécurisée et sélectionne une méthode d'identification spécifique au système avant d'attribuer l'identité correspondante. Les principales méthodes d'identification utilisées dans la littérature sont les suivantes :

— **Identité réelle :** L'utilisation de l'identité réelle repose sur l'exploitation d'informations authentiques et vérifiables relatives au véhicule ou au conducteur. Cette approche est généralement réservée aux services nécessitant une identification formelle, tels que les transactions financières ou les interactions avec les autorités. À titre d'exemple, [18] utilisent l'International Mobile Equipment Identity (IMEI) réel dans un système de prédiction du trafic, soulignant ainsi le rôle central de l'identité réelle dans les applications critiques.

[18]: Jin Wang et Peixin Liu. « Traffic prediction with deep learning for vehicular communication network ». In : *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*. Sous la dir. de Miroslava Mikusova. T. 12460. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series. Déc. 2022, 124603E

— **Pseudonymes :** Les pseudonymes correspondent à des identifiants temporaires permettant de masquer l'identité réelle des véhicules ou des conducteurs, tout en conservant un certain niveau de traçabilité. Comme illustré à la Figure 5.1, dans un schéma d'identification pseudonymisée, l'autorité d'enregistrement transmet périodiquement des informations à une autorité de certification des pseudonymes, laquelle délivre un certificat contenant un pseudonyme utilisé par le véhicule lors de ses communications.

— **Plaques d'immatriculation et numéros d'enregistrement :** Les plaques d'immatriculation et les numéros d'enregistrement constituent les principaux moyens d'identification visuelle des véhicules. Associés à des systèmes de reconnaissance automatique des plaques

d'immatriculation (ANPR), ils jouent un rôle essentiel dans la surveillance du trafic et le renforcement de la sécurité publique, offrant un identifiant fiable dans de nombreux contextes véhiculaires.

— **Dispositifs d'identification par radiofréquence :** Les dispositifs d'identification par radiofréquence (RFID) permettent une identification rapide et à distance des véhicules. Dans [19], cette approche repose sur l'utilisation de balises RFID pour améliorer le suivi logistique et la gestion du trafic, sans nécessiter d'observation visuelle directe.Les auteurs proposent un système de gestion de clés intégrant un schéma d'élimination des tags, clés ou nœuds compromis ou suspects, permettant d'exclure du réseau tout véhicule non autorisé, renforçant ainsi la sécurité et facilitant les communications au sein des réseaux véhiculaires ad hoc.

[19]: S Suganya et Shanmuganathan Chandrasekaran. « Key Management of Vehicular Ad-Hoc Network with Eliminating Scheme ». In : (oct. 2019)

En résumé, les systèmes d'audit nécessitent un mécanisme d'identification robuste afin de garantir la traçabilité et la sécurité de l'ensemble des transactions au sein d'un réseau de communication véhiculaire. Toutefois, ces mécanismes doivent également préserver la vie privée des utilisateurs, en conciliant l'exigence d'une identification fiable avec la protection de l'anonymat. Cet équilibre est essentiel pour encourager l'adoption et la participation des véhicules aux applications coopératives. Dans le cadre de cette thèse, nous privilégions l'approche par pseudonymes, qui offre le meilleur compromis entre traçabilité auditée et protection de la vie privée : elle permet d'identifier de manière conditionnelle les entités impliquées dans un incident, tout en préservant l'anonymat lors des communications ordinaires. Cette approche s'inscrit naturellement dans une architecture PKI, où l'autorité de confiance peut lever l'anonymat d'un véhicule en cas de comportement malveillant avéré, garantissant ainsi la non-répudiation sans exposer directement l'identité réelle des participants.

2.1.2 Systèmes de préservation de la vie privée

En intégrant les éléments essentiels issus des travaux antérieurs dans le contexte de la préservation de la vie privée au sein des communications véhiculaires, il apparaît clairement que cet aspect ne constitue pas une fonctionnalité accessoire, mais bien une exigence fondamentale pour l'efficacité globale et l'acceptation des systèmes de communication véhiculaires. Comme le souligne [20], en l'absence de garanties suffisantes en matière d'anonymat et de confidentialité, les entités communicantes pourraient être réticentes à participer aux applications coopératives. La protection de la vie privée apparaît ainsi comme un levier déterminant pour encourager la participation volontaire des véhicules et favoriser l'adoption à grande échelle du système..

[20]: Florian Schaub, Zhendong Ma et Frank Kargl. « Privacy Requirements in Vehicular Communication Systems ». In : *2009 International Conference on Computational Science and Engineering* 3 (2009)

Avec l'évolution des systèmes de communication véhiculaires, la quantité et la granularité des données collectées et transmises ne cessent d'augmenter. Ces données peuvent inclure non seulement la localisation du véhicule, mais également les habitudes de conduite, les itinéraires fréquemment empruntés et les horaires de déplacement. Bien que la collecte et la traçabilité de ces informations, via un système d'audit, soient bénéfiques pour l'optimisation du trafic et l'amélioration de la sécurité routière, elles soulèvent également d'importants risques en matière de vie privée, dans la mesure où chaque transaction peut contenir des informations liées à une identité réelle.

Si ces données ne sont pas protégées de manière adéquate, elles peuvent être exploitées par des acteurs malveillants à des fins préjudiciables, telles que le suivi non autorisé des utilisateurs, le profilage ou encore la publicité ciblée. L'exploitation abusive de ces informations soulève des préoccupations majeures en matière de protection de la vie privée, pouvant conduire à des violations à la fois intrusives et potentiellement dangereuses.

La prise de conscience de ces risques est susceptible d'éroder significativement la confiance des utilisateurs envers ces systèmes, les rendant réticents au partage de leurs données. Une telle réticence pourrait compromettre l'efficacité des systèmes de communication véhiculaires, dont les performances reposent largement sur la qualité et la quantité des informations échangées. Afin de limiter ces risques tout en préservant l'efficacité du système, la mise en œuvre d'un mécanisme d'identification masquant l'identité réelle des utilisateurs s'avère indispensable. Comme illustré à la Figure 5.1, les entités sont identifiées au moyen de pseudonymes, lesquels protègent leur identité réelle tout en leur permettant de participer activement au réseau. Une autorité de certification des pseudonymes délivre ces identifiants aux entités enregistrées, qui les utilisent en lieu et place de leur identité réelle. En cas d'enquête, notamment en consultant le système d'audit, concernant des activités malveillantes associées à un pseudonyme, l'incident est transmis à l'autorité d'enregistrement, seule entité habilitée à lever l'anonymat et à révéler l'identité réelle de l'utilisateur impliqué.

Dans le but de préserver la vie privée dans les communications véhiculaires, une part importante des travaux de recherche s'est concentrée sur deux approches majeures. La première, mise en évidence dans les études [21-26], repose sur l'utilisation de pseudonymes ou de schémas cryptographiques basés sur l'identité afin de dissimuler l'identité réelle des utilisateurs. Dans cette approche, les pseudonymes sont généralement délivrés et enregistrés par une autorité de confiance lors de la phase d'enregistrement. Les utilisateurs participent ensuite au système de communication véhiculaire sous ces identités pseudonymisées, leur permettant d'échanger des informations sans révéler leur identité réelle. L'utilisation de pseudonymes constitue ainsi une stratégie centrale pour garantir un certain niveau d'anonymat, protégeant efficacement l'identité du véhicule et de ses occupants [21-24, 26].

Toutefois, la gestion de ces pseudonymes représente un processus critique. L'autorité de confiance chargée de leur émission doit disposer de la capacité exclusive de relier un pseudonyme à l'identité réelle correspondante. Cette exigence est essentielle pour des raisons légales et sécuritaires, car elle permet d'assurer la responsabilité des entités tout en préservant la confidentialité des utilisateurs. Néanmoins, bien que les pseudonymes offrent un degré significatif d'anonymat, ils introduisent également certaines vulnérabilités, notamment en matière de traçabilité. La possibilité de relier différents pseudonymes peut conduire à l'inférence des routines et des habitudes des utilisateurs [5, 27-29], compromettant ainsi la confidentialité des déplacements et des activités. Par exemple, l'analyse des schémas d'utilisation des pseudonymes peut permettre de déduire des lieux fréquemment visités ou des comportements de mobilité, soulevant des interrogations quant au niveau réel de protection de la vie privée offert par ces mécanismes.

Cette problématique devient particulièrement critique lorsque les pseudonymes sont statiques ou réutilisés sur de longues périodes, comme le soulignent [23, 30], car cela accroît considérablement les risques de

[21]: A. F. M. Suaib Akhter, Mohiuddin Ahmed, A. F. M. Shahen Shah, Adnan Anwar et Ahmet Zengin. « A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET ». In : *Sustainability* 13.1 (2021)

[22]: Lei Xu & Feng Gao Shi Kexin Liehuang Zhu Can Zhang. « Blockchain-based multimedia sharing in vehicular social networks with privacy protection ». In : *Multimedia Tools and Applications* (2020)

[23]: Anusha Vangala, Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar et Youngho Park. « Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems ». In : *IEEE Sensors Journal* 21.14 (2021)

[24]: Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang et Zonghua Zhang. « CreditCoin : A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles ». In : *IEEE Transactions on Intelligent Transportation Systems* 19.7 (2018)

[25]: Udit Bansal, Jayaprakash Kar, Ikram Ali et Kshirasagar Naik. « ID-CEPPA : Identity-based Computationally Efficient Privacy-Preserving Authentication scheme for vehicle-to-vehicle communications ». In : *Journal of Systems Architecture* 123 (2022)

[26]: Sharqa Hameed, Sakeena Javaid, Sheeraz Ahmed et Nadeem Javaid. « Sharing Mechanism of Intelligent Vehicles Trust Points based on Blockchain for Vehicular Networks ». In : *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*. 2020

[27]: Jean-Pierre Raya Maxim ; Hubaux. « Securing vehicular ad hoc networks ». In : *Journal of Computer Security* 15 (2007)

[28]: Chao Lin, Debiao He, Xinyi Huang, Neeraj Kumar et Kim-Kwang Raymond Choo. « BCPPA : A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks ». In : *IEEE Transactions on Intelligent Transportation Systems* 22.12 (2021)

[29]: Jing Zhang, Hong Zhong, Jie Cui, Lu Wei et Lu Liu. « CVAR : Distributed and Extensible Cross-Region Vehicle Authentication With Reputation for VANETs ». In : *IEEE Transactions on Intelligent Transportation Systems* (2023)

corrélation et de traçabilité. Afin de remédier à ces limitations, plusieurs travaux [21, 31, 32] proposent l'utilisation de pseudonymes dynamiques, renouvelés fréquemment, afin de garantir l'absence de liaison entre les communications et de renforcer la protection de la vie privée. L'enjeu réside ainsi dans l'équilibre entre l'anonymat des utilisateurs et la capacité de traçabilité nécessaire à des fins de sécurité et de responsabilité.

La seconde approche visant à renforcer la protection de la vie privée dans les communications véhiculaires repose sur l'utilisation de paires de clés dynamiques, distinctes pour chaque communication, afin d'empêcher toute traçabilité. Cette méthode ajoute une couche supplémentaire d'anonymat et améliore significativement la protection des identités des utilisateurs [5, 27-29]. Une première stratégie, proposée par [27], consiste à stocker un grand nombre de paires de clés dans l'unité embarquée (On-Board Unit, OBU) du véhicule pour une durée limitée. À chaque communication, une nouvelle paire est sélectionnée, garantissant ainsi que chaque échange repose sur des clés uniques et difficilement corrélables. Une seconde stratégie, introduite par [5], s'appuie sur l'utilisation de certificats temporaires délivrés par les unités routières (Road Side Units, RSUs). À chaque passage à proximité d'une RSU, le véhicule reçoit un nouveau certificat, lui fournissant une nouvelle paire de clés pour les communications ultérieures, assurant ainsi un renouvellement fréquent des mécanismes cryptographiques.

Cependant, ces approches présentent également certaines limitations. La première, fondée sur le stockage d'un grand nombre de paires de clés dans l'OBU, est contrainte par les capacités de stockage limitées de ces dispositifs [28]. La seconde, reposant sur un renouvellement fréquent des certificats via les RSUs, peut engendrer une surcharge des communications et une dégradation des performances du réseau [28].

Afin de surmonter ces limitations, des auteurs [28] proposent une solution innovante fondée sur un algorithme de dérivation de clés. Cette approche permet à l'OBU de générer dynamiquement une nouvelle paire de clés pour chaque communication, sans nécessiter le stockage d'un grand nombre de clés ni des échanges fréquents avec les RSUs. L'algorithme de dérivation de clés offre ainsi un compromis efficace entre la protection de la vie privée, les contraintes de stockage et la charge de communication, tout en garantissant un niveau élevé de sécurité.

En conclusion, les mécanismes d'identification et de pseudonymisation permettent d'attribuer des identités anonymisées aux entités, constituant une étape essentielle pour la protection de la vie privée au sein du réseau. Toutefois, la présence d'un système d'authentification demeure indispensable pour garantir que ces identités anonymes correspondent effectivement à des entités autorisées. Grâce à l'authentification, le système d'audit est en mesure de suivre avec précision les actions des entités légitimes et, en cas d'anomalies, de retracer l'origine des comportements suspects. Ainsi, l'intégration conjointe des mécanismes d'identification et d'authentification permet d'assurer simultanément la protection de la vie privée, la légitimité des entités et une traçabilité fiable, éléments indispensables à la mise en œuvre d'un système d'audit efficace.

2.1.3 Systèmes d'authentification

L'authentification constitue un pilier fondamental des systèmes d'audit dans les réseaux véhiculaires, dans la mesure où elle conditionne la

[30]: Righa Tandon, Ajay Verma et Pradeep Gupta. « D-Blac : A Dual Blockchain-Based Decentralized Scheme for Authentication and Communication in Vanet ». In : *SSRN Electronic Journal* (jan. 2022)

[31]: Qianmin Du, Jianhong Zhou et Maode Ma. « EAIA : An Efficient and Anonymous Identity-Authentication Scheme in 5G-V2V ». In : *Sensors* 24.16 (2024)

[32]: Sujash Naskar, Gerhard P. Hancke, Tingting Zhang et Mikael Gidlund. « Pseudo-Random Identification and Efficient Privacy-Preserving V2X Communication for IoV Networks ». In : *IEEE Access* 13 (2025)

fiabilité même des mécanismes de traçabilité et de responsabilité. En effet, un système d'audit ne peut produire des journaux exploitables et juridiquement pertinents que si l'identité des entités à l'origine des actions enregistrées est préalablement vérifiée. Comme le souligne [20], l'authentification joue un rôle central dans la prévention des accès non autorisés aux données et garantit ainsi la sécurité, l'intégrité et la confidentialité des communications.

Dans un système d'audit, l'authentification intervient comme un prérequis indispensable à toute opération de surveillance et d'enregistrement. Elle permet d'établir un lien fiable entre une action observée et une entité légitime, conférant ainsi une valeur probante aux traces collectées par le mécanisme d'audit. L'authentification et l'audit forment dès lors un couple indissociable : tandis que l'authentification assure la validité et l'intégrité des identités, l'audit garantit la traçabilité, la responsabilité et, le cas échéant, la non-répudiation des actions. Cette complémentarité est essentielle pour maintenir un niveau élevé de confiance dans le réseau et pour assurer que seules des entités autorisées puissent interagir et être soumises à un suivi.

Le processus d'authentification est illustré à la figure 5.1. Lors de la phase 1 d'enrôlement, une fois les étapes d'identification et d'anonymisation accomplies, l'autorité d'enregistrement sollicite l'autorité d'authentification afin de fournir à l'entité les données nécessaires à son authentification. Ces données, qui peuvent prendre la forme de certificats, de paramètres cryptographiques ou d'autres éléments d'authentification, sont générées conformément au schéma cryptographique retenu. Par la suite, chaque tentative d'émission ou d'échange d'informations par le véhicule est conditionnée par une authentification préalable, garantissant ainsi que seules les entités reconnues puissent produire des traces d'audit valides.

Par ailleurs, afin de préserver la cohérence et la fiabilité du système d'audit, l'autorité d'authentification doit assurer la mise à jour régulière des listes de révocation et leur diffusion auprès de l'ensemble des participants du réseau. Comme illustré à la figure 5.1, cette exigence prend une importance particulière dans des scénarios où l'accès à l'infrastructure est limité, notamment dans les réseaux V2V. Dans de tels contextes, l'authentification peut s'appuyer sur des informations potentiellement obsolètes, ce qui complique la validation des entités et fragilise la valeur des traces d'audit produites.

L'importance de mécanismes d'authentification robustes et efficaces ne saurait être sous-estimée, dans la mesure où ils constituent le fondement opérationnel de tout système d'audit fiable. Ces mécanismes, qu'ils soient déployés dans des communications V2V ou V2R, et quels que soient les schémas cryptographiques utilisés, jouent un rôle déterminant dans la protection de la vie privée tout en assurant une identification sécurisée des entités. En garantissant simultanément l'authenticité des participants, la confidentialité des échanges et la traçabilité des actions, les systèmes d'authentification confèrent au mécanisme d'audit la capacité de détecter les comportements malveillants, d'en retracer l'origine et de supporter des processus de responsabilisation au sein des réseaux véhiculaires.

2.1.4 Système d'audit

Un système d'audit dans les réseaux véhiculaires désigne un mécanisme d'enregistrement structuré et infalsifiable des événements et des échanges

survenant au sein du réseau, permettant leur analyse a posteriori. Contrairement à une supervision en temps réel, l'audit vise à constituer une base de preuves vérifiables, à partir de laquelle il devient possible de retracer l'origine d'un incident, d'établir les responsabilités des entités impliquées et de garantir la non-répudiation des actions. Son efficacité ne repose pas uniquement sur l'application de normes, mais également sur la capacité à exercer un jugement éclairé et à évaluer les risques de manière appropriée [33].

[33]: Benoît Pigé. *Audit et contrôle interne*. Jan. 2017. isbn : 9782847699937

Afin d'atteindre ces objectifs, les systèmes d'audit doivent s'appuyer sur des protocoles d'authentification robustes permettant de vérifier de manière fiable l'identité des entités qui y accèdent. Par ailleurs, la mise en place d'un anonymat contrôlé par une autorité légale est indispensable pour permettre l'audit en cas de comportement malveillant, tout en préservant la vie privée des utilisateurs dans les situations normales. La relation étroite entre audit, anonymat et authentification est mise en évidence dans [14], comme illustré à la Figure 5.1. Cette approche garantit que seules des entités ou des systèmes autorisés peuvent initier ou examiner les processus d'audit, préservant ainsi l'intégrité des opérations d'audit et limitant les risques de violations de sécurité ou de fuites de données. Grâce à des audits réguliers, les vulnérabilités peuvent être identifiées et corrigées, renforçant ainsi la résilience et la fiabilité globales du réseau véhiculaire.

L'Organisation internationale de normalisation (ISO) fournit des lignes directrices pour la gestion et la conduite des audits, notamment à travers la norme ISO/SAE 21434 [34], qui met en avant les objectifs suivants en matière d'audit dans le contexte de la cybersécurité automobile :

[34]: International Organization for Standardization. *Road vehicles – Cybersecurity engineering*. Published by ISO/SAE International. ISO/SAE, 2021

- Assurer une surveillance et une inspection continues par la mise en œuvre de processus formalisés.
- Protéger la sécurité et la vie privée du réseau grâce à l'introduction d'une méthodologie d'analyse des menaces et d'évaluation des risques (Threat Analysis and Risk Assessment – TARA) appliquée tout au long du cycle de vie du produit.
- Vérifier l'efficacité des mécanismes d'authentification au moyen de tests de cybersécurité obligatoires.
- Garantir la traçabilité et la responsabilité des activités.

Plusieurs travaux de recherche se sont intéressés à l'amélioration de la sécurité routière et de l'expérience de conduite en analysant le rôle des mécanismes d'audit dans les réseaux véhiculaires. Les auteurs de [35] mettent en évidence l'apport majeur de la technologie blockchain pour satisfaire les exigences de sécurité, notamment grâce à la mise en œuvre de mécanismes d'audit public reposant sur l'immutabilité de la blockchain. Chaque bloc ajouté à la chaîne peut être vérifié de manière indépendante par l'ensemble des nœuds du réseau, fournissant ainsi une piste d'audit transparente et infalsifiable. Dans [36], l'audit est identifié comme une exigence de sécurité clé, au même titre que la non-répudiation, en particulier dans les scénarios d'accidents où il est essentiel de déterminer les causes réelles des incidents. Par ailleurs, l'étude présentée dans [14] propose une revue des solutions existantes pour l'enregistrement des événements dans les systèmes véhiculaires et explore l'utilisation de la blockchain comme solution potentielle, tout en mettant en lumière les défis à relever pour permettre un audit efficace dans les communications véhiculaires.

[35]: Tejasvi Alladi, Vinay Chamola, Nishad Sahu, Vishnu Venkatesh, Adit Goyal et Mohsen Guizani. « A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks ». In : *IEEE Communications Surveys & Tutorials* 24.2 (2022)

[36]: Avleen Kaur Malhi, Shalini Batra et Husanbir Singh Pannu. « Security of vehicular ad-hoc networks : A comprehensive survey ». In : *Computers & Security* 89 (2020)

La Figure 2.2 inspiré de [14] illustre les interactions au sein d'un système d'audit dans un réseau de communication véhiculaire. L'autorité de

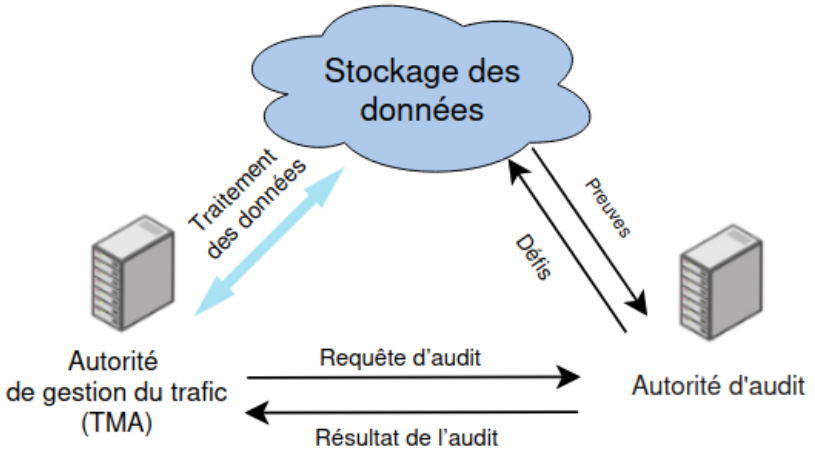

Figure 2.2 – Audit de l'intégrité des données pour des communications véhiculaires sécurisées.

gestion du trafic (TMA) initie le processus d'audit en adressant une requête d'audit à l'autorité d'audit. Cette requête conduit l'autorité d'audit à vérifier l'intégrité et l'authenticité des données stockées dans le système de communication véhiculaire. Ces vérifications peuvent porter sur la validation des identités, l'intégrité des messages échangés entre les véhicules ou encore la sécurisation de l'accès à des informations confidentielles. En retour, la TMA reçoit un rapport d'audit contenant les conclusions ainsi que les preuves de conformité ou les anomalies détectées dans les données. Ce mécanisme permet à la TMA de surveiller en continu la sécurité et l'authenticité des informations, renforçant ainsi la fiabilité du réseau.

L'autorité d'audit émet des défis à destination du système de stockage des données, exigeant des preuves d'intégrité, telles que la vérification de signatures numériques ou de condensats cryptographiques, afin de s'assurer que les données n'ont pas été altérées. Le système de stockage répond par les preuves requises, lesquelles sont ensuite examinées par l'autorité d'audit afin d'en évaluer la validité et la conformité aux exigences de sécurité. Cette architecture permet une supervision robuste du réseau, dans laquelle la TMA valide l'authenticité des données, tandis que l'autorité d'audit garantit la conformité des preuves aux normes de sécurité. Elle assure également la non-répudiation, en empêchant toute entité de nier ses actions au sein du réseau, un aspect fondamental pour maintenir la confiance et la conformité réglementaire.

Dans la section suivante, nous chercherons en grande partie à identifier et présenter une méthode d'authentification adaptée à la mise en œuvre d'un système d'audit efficace dans le contexte des communications V2X. L'objectif est de garantir la sécurité, la traçabilité et la responsabilité au sein du réseau, tout en assurant la non-répudiation et la protection des données, afin de permettre des audits fiables et conformes aux exigences réglementaires.

2.2 Travaux existants sur les protocoles d'authentification

Cette section présente une taxonomie complète des stratégies d'authentification utilisées dans les réseaux véhiculaires. Chaque catégorie est représentée par des travaux pertinents pour mettre en évidence les différentes approches et méthodes qui caractérisent les protocoles

d'authentification actuels et émergents dans ce domaine. La figure 2.3 illustre cette taxonomie. Nous analysons ensuite en détail les principales caractéristiques, avantages et défis de chaque stratégie.

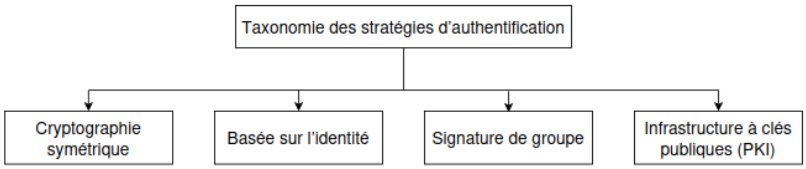

Figure 2.3 – Stratégies d'authentification

2.2.1 Protocoles à cryptographie symétrique

Dans le domaine des communications véhiculaires, et plus particulièrement dans les réseaux VANETs, le recours aux protocoles d'authentification basés sur la cryptographie symétrique suscite un intérêt croissant. Les algorithmes symétriques reposent sur l'utilisation d'une clé secrète partagée, utilisée à la fois par l'émetteur et le récepteur pour le chiffrement et le déchiffrement des messages. L'un des principaux inconvénients de l'application de ces techniques réside toutefois dans la distribution sécurisée des clés secrètes aux nœuds du réseau véhiculaire. Étant donné que toute entité possédant la clé secrète est en mesure de déchiffrer les messages, il est impératif d'empêcher toute compromission ou diffusion non autorisée de ces clés.

Un exemple représentatif de cette approche est le protocole d'authentification proposé par [37]. Dans ce protocole, tous les véhicules partage une même clé système utilisée pour générer des codes d'authentification de message (MAC) sur les messages diffusés. Les destinataires peuvent alors vérifier l'authenticité des messages reçus en recalculant le MAC à l'aide de cette même clé système. Ce mécanisme de vérification ne nécessite qu'un calcul de hachage et une opération MAC, ce qui permet d'atteindre une authentification légère et efficace.

[37]: Fei Wang, Yongjun Xu, Hanwen Zhang, Yujun Zhang et Liehuang Zhu. « 2FLIP : A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET ». In : *IEEE Transactions on Vehicular Technology* 65.2 (2016)

Ces protocoles, centrés sur la cryptographie, permettent une authentification directe entre les unités embarquées (OBUs) dans un environnement V2V, offrant aux véhicules la capacité de vérifier mutuellement leur authenticité sans recourir à des certificats ou à des tiers de confiance. Cette approche se révèle particulièrement avantageuse dans des scénarios où l'accès à l'infrastructure, telle que les unités routières (RSUs), est limité, voire inexistant.

Parmi les techniques cryptographiques notables utilisées dans ces protocoles figure la cryptographie sur les courbes elliptiques (ECC). Les schémas d'authentification basés sur l'ECC constituent une alternative aux mécanismes reposant sur les appariements bilinéaires, en réduisant la complexité computationnelle associée à ces derniers [38]. L'utilisation de paramètres cryptographiques stockés localement dans l'OBU permet ainsi une authentification efficace dans un environnement V2V [25, 30, 39], tout en maintenant un niveau de sécurité élevé.

[38]: SK Hafizul Islam, Mohammad S. Obaidat, Pandi Vijayakumar, Enas Abdulhay, Fagen Li et M Krishna Chaitanya Reddy. « A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs ». In : *Future Generation Computer Systems* 84 (2018)

En résumé, bien que les protocoles centrés sur la cryptographie constituent une solution prometteuse pour l'authentification dans les systèmes de communication véhiculaires, en particulier dans les environnements dépourvus de support infrastructurel, ils présentent également un certain nombre de défis. leur principal défi reste la distribution sécurisée des clés partagées. La compromission d'une seule clé peut en effet affecter l'ensemble du système, ce qui limite leur déploiement dans des réseaux

[39]: Gopal Singh Rawat, Karan Singh, Noreen Izza Arshad, Komeil Hadidi et Ali Ahmadian. « A lightweight authentication scheme with privacy preservation for vehicular networks ». In : *Computers and Electrical Engineering* 100 (2022)

véhiculaires à grande échelle et remet en cause leur adéquation aux exigences de traçabilité et de responsabilisation d'un système d'audit fiable.

2.2.2 Protocoles d'authentification basés sur l'identité

Dans les systèmes de communication véhiculaires, les protocoles d'authentification basés sur l'identité suscitent un intérêt croissant en raison de leur capacité à améliorer l'efficacité et à renforcer la sécurité par rapport aux méthodes d'authentification classiques fondées sur la gestion de clés. Ces protocoles exploitent l'identité unique de chaque entité afin de simplifier la gestion des clés et d'accroître l'efficacité opérationnelle, un aspect essentiel dans des environnements nécessitant des mécanismes d'authentification rapides. L'utilisation de pseudo-identités, générées par des dispositifs inviolables embarqués dans les véhicules, constitue un élément central de ces approches. Grâce à la cryptographie basée sur l'identité, les clés privées sont dérivées directement à partir de ces pseudo-identités, supprimant ainsi le besoin de certificats numériques et réduisant la surcharge liée aux échanges.

Une contribution notable dans ce domaine est présentée dans [40], où les auteurs proposent une méthode efficace permettant à la fois l'authentification des véhicules et la préservation de la confidentialité de leurs identités. Cette approche repose sur l'utilisation de pseudo-identités générées par des dispositifs inviolables installés dans chaque véhicule. À l'aide de la cryptographie basée sur l'identité, le système génère des clés privées associées à ces pseudo-identités, éliminant ainsi le recours aux certificats et réduisant la charge de communication. Les véhicules signent ensuite leurs messages, lesquels sont vérifiés de manière groupée par les unités routières.

[40]: C. Zhang, R. Lu, X. Lin, P.-H. Ho et X. Shen. « An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks ». In : *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*. 2008

Le schéma ID-CEPPA proposé dans [25] illustre une application concrète de cette technologie. En combinant la cryptographie sur les courbes elliptiques avec la cryptographie basée sur l'identité, ce schéma est spécifiquement conçu pour les communications véhicule-à-véhicule dans les réseaux véhiculaires ad hoc. Par ailleurs, l'étude présentée dans [41] propose un cadre de sécurité global pour les réseaux véhiculaires reposant sur la cryptographie basée sur l'identité, visant à assurer l'authentification, la confidentialité, la non-répudiation et l'intégrité des messages, renforçant ainsi significativement la sécurité des réseaux véhiculaires.

[41]: Pandurang Kamat, Arati Baliga et Wade Trappe. « An Identity-based Security Framework For VANETs ». In : *VANET '06 : Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks*. ACM, sept. 2006

Néanmoins, ces protocoles présentent certaines limitations en termes de performances, notamment lorsqu'ils reposent sur des schémas de signature de groupe. Ces derniers souffrent souvent de coûts élevés liés à la vérification des signatures, laquelle peut s'avérer complexe et chronophage. De plus, la forte mobilité et la nature dynamique des réseaux véhiculaires compliquent la gestion des groupes, rendant l'implémentation de tels schémas plus délicate [39]. Malgré ces contraintes, les approches basées sur l'identité permettent de s'affranchir des systèmes de gestion de certificats, simplifiant ainsi certains aspects administratifs et opérationnels [40, 42].

[42]: Qinglei Kong, Le Su et Maode Ma. « Achieving Privacy-Preserving and Verifiable Data Sharing in Vehicular Fog With Blockchain ». In : *IEEE Transactions on Intelligent Transportation Systems* 22.8 (2021)

En résumé, bien que les protocoles d'authentification basés sur l'identité offrent une approche efficace et rationalisée pour la sécurisation des réseaux véhiculaires, leur déploiement doit prendre en compte les contraintes spécifiques de ces environnements, telles que la nécessité d'une authentification rapide, la mobilité élevée des véhicules et la complexité de la gestion des groupes. Malgré ces défis, ces protocoles

constituent une avancée significative pour répondre aux exigences opérationnelles des systèmes de communication véhiculaires modernes.

2.2.3 Protocoles à signature de groupe

L'authentification fondée sur les signatures de groupe est une technique permettant à un ensemble de véhicules d'être authentifiés au moyen d'une signature unique, tout en préservant l'anonymat des membres du groupe et en garantissant l'intégrité des messages échangés. Cette approche est particulièrement adaptée aux réseaux véhiculaires ad hoc, dans lesquels des communications rapides et sécurisées entre véhicules sont indispensables.

L'étude présentée dans [43] propose un schéma novateur et efficace d'authentification de messages basé sur des signatures de groupe à seuil pour les réseaux véhiculaires. Ce schéma s'appuie sur la cryptographie à les courbes elliptiques afin de réduire la complexité des opérations, et adopte des pseudonymes pour assurer la préservation de la vie privée. Il permet également une authentification par lots, démontrant ainsi une réduction significative du délai d'authentification par rapport aux schémas conventionnels. Une autre approche, décrite dans [44], introduit un schéma d'authentification anonyme fondé sur les signatures de groupe. Ce mécanisme permet aux véhicules de s'authentifier mutuellement et de communiquer avec l'infrastructure routière, tout en protégeant la vie privée des conducteurs. Il combine des mécanismes d'alias avec des signatures de groupe afin de proposer une solution distribuée, dans laquelle aucune autorité unique n'est en mesure de révéler directement l'identité réelle des véhicules.

[43]: Jingru Fang, Xiaoming Jiang, Hao Wu et Xue Du. « A Threshold Group Signature Authentication Scheme for VANETs ». In : *The 2nd International Conference on Computing and Data Science*. CONF-CDS 2021. Stanford, CA, USA : Association for Computing Machinery, 2021. ISBN : 9781450389570

[44]: Yanji Jiang, Shaocheng Ge et Xueli Shen. « AAAS : An Anonymous Authentication Scheme Based on Group Signature in VANETs ». In : *IEEE Access* 8 (2020)

Par ailleurs, l'étude présentée dans [45] propose un nouveau schéma de signature de groupe sans certificat visant à masquer l'identité des véhicules et à garantir des communications sécurisées entre eux, contribuant ainsi à la protection des informations véhiculaires sensibles. Ce schéma intègre un mécanisme d'authentification associé à une évaluation de crédit, combinant la cryptographie asymétrique sans certificat et les signatures de groupe. De son côté, [46] présente un schéma évolutif et sécurisé de gestion des clés pour l'authentification basée sur les signatures de groupe, ainsi que pour la gestion des listes de révocation de certificats dans les réseaux véhiculaires. Les auteurs proposent une topologie hiérarchique du réseau, dans laquelle une unité routière leader gère un domaine composé de plusieurs unités routières. Dans ce cadre, des mécanismes de chiffrement symétrique sont utilisés entre les véhicules et les unités routières afin d'assurer la distribution sécurisée des clés de groupe.

[45]: Yanfei Lu, Suzhen Cao, Qizhi He, Zixuan Fang, Junjian Yan et Yi Guo. « Group Signature Authentication Scheme with Credit Evaluation Mechanism in VANET ». In : *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. 2023

[46]: Kiho Lim, Weihua Liu, Xiwei Wang et Jingon Joung. « SSKM : Scalable and Secure Key Management Scheme for Group Signature Based Authentication and CRL in VANET ». In : *Electronics* 8.11 (2019)

Ces travaux mettent en évidence la diversité des approches et des améliorations apportées aux mécanismes d'authentification basés sur les signatures de groupe dans les réseaux véhiculaires, chacune visant à renforcer la sécurité, l'efficacité et la protection de la vie privée dans les communications inter-véhicules. Ces protocoles se caractérisent par un niveau élevé d'anonymat, dans la mesure où les messages sont authentifiés par un membre du groupe sans révéler son identité individuelle. Toutefois, ils présentent généralement une limitation en matière d'identification, rendant difficile, voire impossible, la détermination précise du véhicule émetteur d'un message. Seule l'appartenance au groupe peut être établie.

Sur la base des mécanismes décrits précédemment, nous examinons dans la section suivante, les schémas d'authentification existants répondent

aux différents défis liés à la sécurité et à la protection de la vie privée dans les environnements de communication véhicule-à-véhicule.

2.2.4 Protocoles basés sur la PKI

Dans l'étude des protocoles fondés sur l'infrastructure à clés publiques dans les systèmes de communication véhiculaires, de nombreux travaux ont contribué à approfondir la compréhension de leurs applications et des défis associés. La Figure 2.4 présente l'architecture d'un système d'infrastructure à clés publiques garantissant que seules les entités autorisées peuvent participer aux échanges de données. Le processus débute par l'Autorité d'Enrôlement, qui reçoit les informations des entités, telles que les véhicules, lors de leur phase d'enregistrement et vérifie leur légitimité. Si les informations fournies sont jugées valides, l'Autorité d'Enrôlement soumet une requête à l'Autorité d'Authentification afin de générer un certificat numérique associé à une clé publique pour l'entité requérante. Ce certificat, servant de preuve d'identité, est ensuite transmis à l'Autorité d'Autorisation, qui en vérifie l'authenticité et la conformité. Ce mécanisme garantit que seuls les véhicules ou entités disposant d'un certificat approuvé peuvent participer à des communications sécurisées. À chaque étape, des vérifications de signatures sont effectuées afin de s'assurer que les messages échangés proviennent d'entités authentiques et qu'ils n'ont pas été altérés.

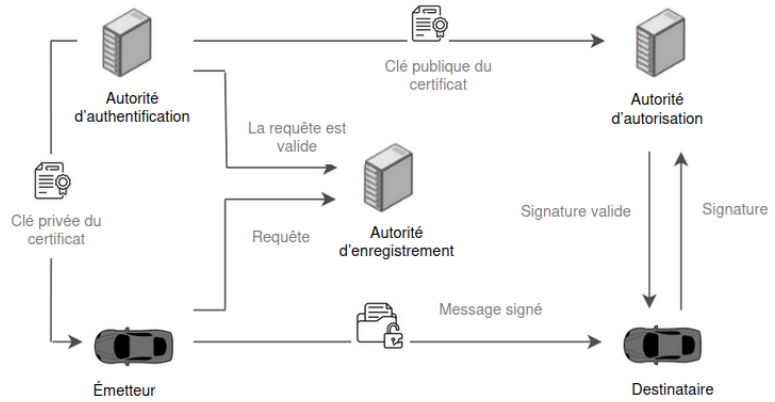

Figure 2.4 – Système d'infrastructure à clés publiques pour l'authentification.

Le schéma d'authentification basé sur les pseudonymes proposé dans [27] se distingue par son approche de l'authentification dans les réseaux véhiculaires ad hoc à l'aide de pseudonymes. Bien qu'il réponde efficacement à la majorité des exigences du réseau, ce schéma impose le préchargement de l'unité embarquée avec un grand nombre de certificats ainsi que leurs paires de clés correspondantes. Cette contrainte, notamment pour les paires de clés à courte durée de validité, pose un problème en raison de la capacité de stockage limitée des unités embarquées. Cette limitation met en évidence un défi plus général des systèmes à infrastructure à clés publiques : la gestion, la distribution et la révocation des certificats sont des processus complexes et coûteux en ressources, nécessitant une administration rigoureuse et des capacités importantes [39]. Par ailleurs, les contraintes de stockage des unités embarquées empêchent la conservation d'un grand nombre de clés, ce qui constitue une limitation notable dans plusieurs travaux [25, 28].

Une autre contribution majeure introduit le protocole de préservation conditionnelle efficace de la vie privée [5]. Ce protocole met l'accent sur la protection conditionnelle de la vie privée dans des communications

véhiculaires sécurisées, en visant à prévenir les accès non autorisés et les fuites de données. Une caractéristique distinctive de ce protocole réside dans l'utilisation de certificats temporaires en collaboration avec les unités routières. Ces certificats temporaires jouent un rôle central dans le processus d'authentification en offrant un mécanisme dynamique et à durée de validité limitée pour les véhicules du réseau. Cette approche permet de répondre à certaines limitations des certificats permanents, telles que la nécessité de mises à jour fréquentes et le risque de compromission à long terme. En réduisant la durée de validité des certificats, la fenêtre de vulnérabilité est limitée, rendant leur exploitation plus difficile pour un attaquant. De plus, ce mécanisme s'adapte naturellement à la forte mobilité des véhicules, les certificats pouvant être mis à jour ou révoqués efficacement lors du passage d'un véhicule d'une zone de couverture à une autre.

Cependant, la dépendance vis-à-vis des unités routières pour l'émission de certificats temporaires met en évidence la forte dépendance des systèmes d'authentification des réseaux véhiculaires à l'égard des autorités de confiance et de l'infrastructure. Cette dépendance peut engendrer des complications et des délais dans la transmission des informations, en particulier lorsque les véhicules se déplacent à grande vitesse. Les requêtes d'authentification fréquentes adressées aux unités routières et aux autorités de confiance augmentent la complexité du système et la charge administrative [39]. Malgré ces contraintes, l'approche proposée par ce protocole, fondée sur l'utilisation de certificats temporaires associés aux unités routières, constitue une avancée innovante dans les systèmes véhiculaires basés sur l'infrastructure à clés publiques. Elle permet de concilier les exigences élevées de sécurité offertes par ce cadre avec l'efficacité opérationnelle requise dans des environnements véhiculaires dynamiques [21, 26].

L'évolution des solutions d'authentification dans les systèmes de communication véhiculaires, et en particulier dans les réseaux véhiculaires ad hoc, s'oriente de plus en plus vers des approches décentralisées. Cette évolution se caractérise par un abandon progressif des modèles centralisés traditionnels, généralement fondés sur une autorité tierce unique, au profit de cadres distribués. Cette transition est essentielle pour dépasser les limites des systèmes centralisés, notamment leur vulnérabilité aux points uniques de défaillance et leurs difficultés de mise à l'échelle.

Dans ce contexte, l'intégration de la technologie blockchain dans les réseaux véhiculaires ad hoc afin de mettre en place des mécanismes de confiance décentralisés constitue une avancée majeure. Les auteurs de [47] soulignent l'importance de cette approche en mettant en évidence le changement de paradigme induit par le stockage distribué et les capacités offertes par la blockchain. La gestion de la confiance ne repose plus sur une autorité centrale unique, mais s'appuie sur un modèle distribué exploitant la nature décentralisée de la blockchain. Le rôle de la blockchain en tant que plateforme de stockage distribué sécurisé est déterminant, grâce à ses propriétés intrinsèques d'immutabilité et de résistance à la falsification [21, 26, 28, 48]. Ces caractéristiques renforcent l'intégrité et la fiabilité des mécanismes d'authentification, les rendant nettement plus résistants aux altérations et aux attaques.

Par ailleurs, l'intégration des contrats intelligents dans les systèmes basés sur la blockchain représente une avancée significative dans la gestion des certificats. Les contrats intelligents automatisent et sécurisent les opérations liées à cette gestion, réduisant ainsi la complexité et les coûts associés [21, 28]. En encodant directement les règles de gestion

[47]: M. A. Afzal et M. A. Shah. « PRIVACY-PRESERVING AUTHENTICATION SCHEME FOR VANETS IN DIGITAL ECONOMY ». In : *Competitive Advantage in the Digital Economy (CADE 2021)*. T. 2021. 2021

[48]: Sanjeev Kumar Dwivedi, Ruhul Amin, Ashok Kumar Das, Mark T. Leung, Kim-Kwang Raymond Choo et Satyanarayana Vollala. « Blockchain-based vehicular ad-hoc networks : A comprehensive survey ». In : *Ad Hoc Networks* 137 (2022)

dans le code, ces mécanismes limitent les risques d'erreurs humaines ou d'interférences malveillantes. Dans [21], les auteurs proposent un cadre fondé sur la blockchain destiné aux réseaux véhiculaires, dans lequel les informations d'authentification des véhicules sont stockées de manière sécurisée. Des centres locaux d'authentification assurent l'enregistrement des véhicules et la génération des clés, lesquelles sont conservées dans une blockchain locale. Lorsqu'un véhicule se déplace entre différents groupes, le nœud responsable peut accéder rapidement à cette blockchain afin de vérifier son authenticité, avec une attention particulière portée aux véhicules prioritaires.

Une autre contribution, présentée dans [26], introduit un mécanisme de partage de points de confiance pour les véhicules intelligents, reposant sur la blockchain afin de faciliter l'établissement de la confiance entre les communications véhicule-à-véhicule, véhicule-à-infrastructure et véhicule-à-réseau. Cette intégration renforce significativement la fiabilité de l'environnement de communication véhiculaire.

Dans une perspective de sécurisation des réseaux véhiculaires ad hoc, [49] propose un schéma d'authentification des messages basé sur la blockchain, visant à concilier anonymat et traitement décentralisé de l'information. Ce schéma combine des paires de clés publiques et privées avec des codes d'authentification de message pour chiffrer les messages diffusés contenant des informations de trafic et d'identification de l'émetteur. L'anonymat de l'émetteur est ainsi préservé, tandis que la blockchain garantit l'authentification sécurisée des messages. L'intégration de mécanismes de consensus renforce également la fiabilité et la sécurité du processus d'authentification.

[49]: Jaewon Noh, Sangil Jeon et Sunghyun Cho. « Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles ». In : *Electronics* 9.1 (2020)

Dans le cadre des systèmes de transport intelligents, le schéma BCAS-VADN proposé dans [23] constitue une solution d'authentification fondée sur la blockchain dédiée à la détection et à la notification des accidents. Lorsqu'un accident est détecté, le véhicule informe le nœud responsable, qui transmet l'information à des serveurs périphériques. Ceux-ci génèrent ensuite des blocs de transactions envoyés à un centre de validation blockchain, assurant ainsi la sécurité, la transparence et la décentralisation du processus.

Enfin, le protocole d'authentification conditionnelle préservant la vie privée fondé sur la blockchain, présenté dans [28], exploite la blockchain Ethereum afin de garantir l'intégrité des données et d'automatiser les opérations grâce à des contrats intelligents. Ce protocole vise à assurer des communications sécurisées dans les réseaux véhiculaires tout en protégeant la confidentialité des véhicules par le biais d'un algorithme de dérivation de clés.

Si la technologie blockchain apporte des bénéfices significatifs en matière de sécurité et de traçabilité dans les réseaux véhiculaires, elle soulève également plusieurs défis. L'un des principaux concerne la forte consommation de ressources des mécanismes de consensus, nécessitant une puissance de calcul et une énergie importantes, ce qui peut limiter leur déploiement sur des dispositifs aux ressources restreintes. De plus, bien que robuste, la sécurité des systèmes blockchain n'est pas exempte de vulnérabilités, notamment au niveau des contrats intelligents, qui peuvent être la cible d'attaques s'ils ne sont pas conçus et vérifiés rigoureusement [48]. Les performances des solutions blockchain dans les réseaux véhiculaires dépendent également fortement de technologies réseau avancées, telles que la 5G, indispensables pour garantir des temps de latence acceptables et un fonctionnement efficace [21, 48]. Enfin, la latence inhérente aux

blockchains traditionnelles pose problème pour des applications nécessitant des communications en temps réel, ce qui a conduit à la proposition d'architectures multi-niveaux et de systèmes à double blockchain afin d'améliorer la scalabilité et de réduire les délais [21].

2.3 Intégration de la blockchain pour la traçabilité des communications V2X

2.3.1 Prèsentation du paradigme blockchain

La blockchain constitue aujourd'hui une innovation technologique majeure, généralement définie comme une technologie distribuée de stockage, de validation et de transmission d'informations. Elle se distingue par l'absence d'un organe central de contrôle. En effet, la confiance ne repose plus sur une autorité unique, mais sur un ensemble d'acteurs connectés en réseau qui appliquent des règles communes et s'appuient sur des mécanismes cryptographiques. Concrètement, cette approche permet de partager et d'historiser des données entre participants sans recourir à un intermédiaire de confiance, tout en renforçant l'intégrité et la traçabilité des enregistrements.

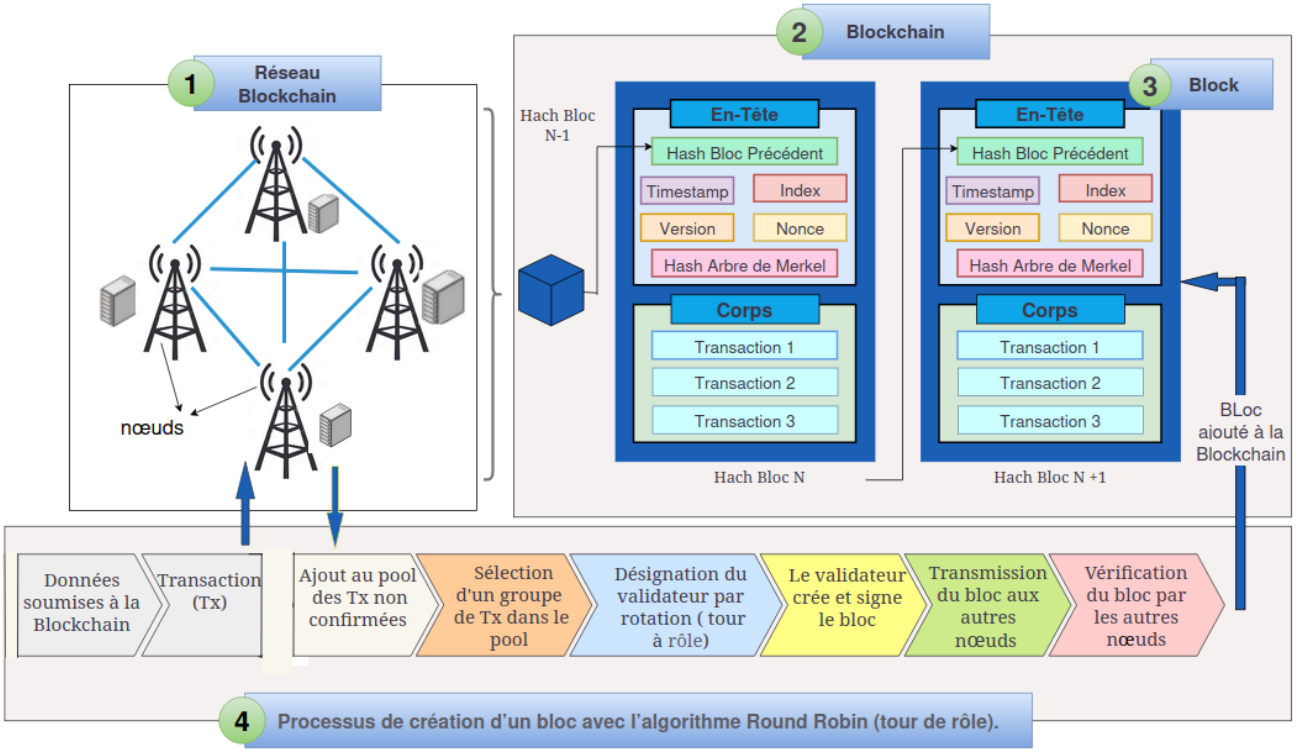

Figure 2.5 – Vue d'ensemble des principaux concepts liés à la blockchain

Le premier modèle opérationnel de blockchain a été introduit en 2008 par Satoshi Nakamoto [50], donnant naissance à Bitcoin, réseau pionnier ayant démontré la faisabilité d'un registre distribué sécurisé à grande échelle. Initialement associée aux cryptomonnaies et aux usages financiers, la blockchain a toutefois rapidement dépassé ce cadre historique pour s'imposer comme un outil de traçabilité et d'audit dans des domaines variés [51].

[50]: Satoshi Nakamoto. « Bitcoin : A peer-to-peer electronic cash system ». In : (2008)

[51]: ISO. *ISO 22739 :2024 Blockchain and distributed ledger technologies — Vocabulary*. International Standard ISO 22739 :2024. International Organization for Standardization, 2024

Vue d'ensemble

Pour garantir une compréhension précise du vocabulaire relatif à la blockchain, la figure 2.5 est présentée comme figure de référence pour les définitions développées ci-après.

La blockchain est un registre numérique distribué, partagé entre un ensemble de nœuds participants, dans lequel les données sont organisées sous forme de transactions regroupées en blocs successifs comme présenté au point **2** de la figure 2.5. Ces blocs sont ordonnés chronologiquement et enchaînés cryptographiquement, de sorte que la modification de l'un des blocs passés entraîne mécaniquement l'invalidation de tous les blocs suivants. C'est ce mécanisme de chaînage qui confère à la blockchain sa propriété fondamentale d'immutabilité, une fois qu'une transaction est confirmée et intégrée à la chaîne, son contenu ne peut plus être altéré sans que cette altération ne soit immédiatement détectable par l'ensemble des participants du réseau.

Le réseau blockchain est un réseau distribué, de type pair-à-pair, illustré au point**1** de la figure 2.5, qui ne repose sur aucune autorité centrale. Il est constitué d'un ensemble de nœuds interconnectés exécutant la blockchain.

Un nœud désigne toute entité participant activement à un réseau blockchain, capable de recevoir, valider et propager des transactions et/ou des blocs. Dans le contexte des communications V2X, ces nœuds peuvent notamment correspondre à des RSUs, comme celles utilisées par [52] en tant que nœuds de la blockchain afin de renforcer l'intégrité des enregistrements et la confiance dans les mécanismes d'authentification.

[52]: Dheerendra Mishra et Purva Rewal. « A blockchain-based quantum-secure protocol for efficient V2I handover authentication in vehicular Ad-Hoc networks ». In : *Peer Peer Netw. Appl.* 18.6 (2025)

Le bloc est défini comme un regroupement de transactions. Il se compose de deux parties distinctes, comme illustré au point **3** de la figure 2.5 : un en-tête et un corps. L'en-tête regroupe l'ensemble des métadonnées structurelles du bloc. Il contient en premier lieu le hash du bloc précédent, qui assure le chaînage entre blocs consécutifs et fonde la propriété d'immutabilité de la chaîne. Il inclut également un horodatage enregistrant le moment exact de création du bloc, un index identifiant sa position dans la chaîne, ainsi que le numéro de version du protocole cryptographique employé. Il contient aussi un nonce, valeur à usage unique que les nœuds ajustent lors du processus de consensus afin de satisfaire les conditions imposées par l'algorithme. Enfin, l'en-tête contient la racine de l'arbre de Merkle [53], qui représente le hash de l'ensemble des transactions incluses dans le bloc. Le corps du bloc contient quant à lui la liste ordonnée des transactions validées qui y sont enregistrées.

[53]: M Andreas et M Antonopoulos. « Mastering Bitcoin : Programming the Open Blockchain ». In : *O'Reilly Media* (2017)

Une transaction est l'unité atomique d'information enregistrée dans la blockchain. Dans le cadre des communications V2X, chaque transaction peut représenter un message V2X généré [43]. Avant d'être intégrée à un bloc, une transaction est diffusée au réseau blockchain et placée dans un pool de transactions non confirmées, en attente de validation par l'algorithme de consensus, comme illustré au début du processus de création d'un bloc dans 4.

L'algorithme de consensus est le mécanisme par lequel les nœuds du réseau s'accordent collectivement sur le contenu du prochain bloc à ajouter à la chaîne, en l'absence de toute autorité centrale d'arbitrage. Le processus de création d'un bloc, illustré au point **3** de la figure 2.5, se déroule selon les étapes suivantes dans le cadre d'un algorithme

Round Robin (tour de rôle) : les données soumises au réseau génèrent des transactions ajoutées au pool des transactions non confirmées ; un groupe de transactions est ensuite sélectionné depuis ce pool pour constituer le prochain bloc ; un nœud validateur est désigné par rotation parmi les participants, chaque nœud jouant le rôle de validateur à tour de rôle, ce validateur crée le bloc, le signe cryptographiquement, puis le transmet aux autres nœuds du réseau, ces derniers vérifient la validité du bloc avant de l'ajouter à leur copie locale de la chaîne. Cet algorithme, inspiré des mécanismes de consensus de type preuve d'autorité (PoA), est adapté aux environnements véhiculaires, où les participants sont identifiés et où une validation rapide est requise [54]. Il est simple et peu gourmand en ressources, car il évite les calculs intensifs et la compétition de minage, contrairement au mécanisme de consensus par preuve de travail (PoW) utilisé dans Bitcoin [55].

[54]: Shu-Ping Lu, Chin-Laung Lei et Meng-Han Tsai. « An efficient Proof-of-Authority consensus scheme against cloning attacks ». In : *Computer Communications* 228 (2024)

[55]: Naseem Sehar, Imran Khan, Faisal Rehman, Muhammad Fayyaz, Ali Ansari et Raheel Nawaz. « Blockchain enabled data security in vehicular networks ». In : *Scientific Reports* 13 (mars 2023)

Un contrat intelligent est un programme informatique autonome, déployé directement sur la blockchain et dont le code constitue lui-même une transaction permanente et immuable de la chaîne. Contrairement à un contrat classique dont l'exécution dépend d'une autorité tierce chargée de faire respecter ses clauses, un contrat intelligent s'exécute de manière automatique et déterministe dès lors que les conditions encodées dans son code sont remplies, sans possibilité d'intervention, de modification ou d'interruption extérieure. Cette propriété lui confère un niveau de confiance intrinsèque, puisque le code est public, vérifiable par tous les nœuds du réseau et immuable une fois déployé, son comportement est prévisible et ne peut être contourné unilatéralement par l'une des parties [56]. Dans le contexte des communications V2X, les contrats intelligents trouvent des applications directes dans l'automatisation d'opérations critiques telles que la révocation de certificats compromis [57].

[56]: Konstantinos Christidis et Michael Devetsikiotis. « Blockchains and Smart Contracts for the Internet of Things ». In : *IEEE Access* 4 (2016)

[57]: Yves Christian Elloh Adja, Badis Hammi, Ahmed Serhrouchni et Sherali Zeadally. « A blockchain-based certificate revocation management and status verification system ». In : *Computers & Security* 104 (2021)

types d'implémentation de la blockchain

En fonction des contraintes de l'application cible, en particulier le contrôle d'accès, les performances requises et le degré de décentralisation souhaité, trois principaux types d'implémentation de la blockchain peuvent être distingués.

Les blockchains publiques sont ouvertes à tout participant sans restriction d'accès ni d'identité. N'importe quel nœud peut rejoindre le réseau, soumettre des transactions et participer au processus de consensus. Bitcoin et Ethereum en constituent les exemples les plus emblématiques. Si cette ouverture totale garantit un niveau maximal de décentralisation et de transparence, elle se traduit en contrepartie par des limitations significatives en termes de performances : les mécanismes de consensus associés, tels que la preuve de travail, engendrent une latence de validation élevée et une consommation énergétique importante, rendant ces blockchains difficilement compatibles avec les contraintes temps réel des communications véhiculaires [58].

[58]: Gengrui Zhang, Yunhao Mao, Shiquan Zhang, Shashank Motepalli, Fei Pan et Hans-Arno Jacobsen. *V-Guard : An Efficient Permissioned Blockchain for Achieving Consensus under Dynamic Memberships in V2X*. 2023. arXiv : 2301.06210 [cs.DC]

Les blockchains privées se situent à l'opposé de ce spectre. L'accès au réseau y est contrôlé par une entité unique qui administre les droits de participation et de validation. Si ce modèle se traduit généralement par de meilleures performances et une gouvernance plus simple, il réintroduit de facto une centralisation de la confiance et du contrôle. Cette concentration crée une vulnérabilité structurelle majeure, l'entité administratrice devient à la fois une cible privilégiée pour les cyberattaques et un point de défaillance unique [59] [60], l'intérêt des blockchains privées pour des

[59]: Yonas Teweldemedhin Gebrezgiher, Sekione Reward Jeremiah, Xianjun Deng et Jong Hyuk Park. « Machine Learning-Based Blockchain Technology for Secure V2X Communication : Open Challenges and Solutions ». In : *Sensors* 25.15 (2025)

[60]: Andrei Vladyko, Vasiliy Elagin, Anastasia Spirkina, Ammar Muthanna et Abdelhamied A. Ateya. « Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications ». In : *Electronics* 11.2 (2022)

applications d'audit dans les environnements V2X demeure limité, dans la mesure où la fiabilité du registre repose entièrement sur l'intégrité de l'autorité gestionnaire

Les blockchains permissionnées, également appelées blockchains de consortium, représentent un compromis intermédiaire particulièrement pertinent pour les environnements véhiculaires [58]. L'accès y est restreint à un ensemble prédéfini de participants identifiés, tels que des autorités de transport, des constructeurs automobiles ou des opérateurs d'infrastructure, qui partagent collectivement la responsabilité de la validation des transactions. Cette architecture permet de concilier décentralisation partielle, contrôle d'accès rigoureux et performances acceptables, grâce notamment à des mécanismes de consensus légers tels que la preuve d'autorité [61].

[61]: James Meijers, Edward Au, Yuxi Cai, Hans-Arno Jacobsen, Shashank Motepalli, Robert Sun, Andreas Veneris, Gengrui Zhang et Shiquan Zhang. « Blockchain for V2X : A Taxonomy of Design Use Cases and System Requirements ». In : *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. 2021

2.3.2 Applications de la blockchain à l'audit dans les réseaux véhiculaires

La décentralisation, la traçabilité et l'immutabilité constituent des propriétés fondamentales pour garantir un audit fiable des communications V2X. Dans ce cadre, la blockchain s'impose comme un mécanisme d'enregistrement particulièrement adapté, dans la mesure où elle permet de consigner les événements sous forme de transactions au sein d'un registre distribué, transparent et résistant aux altérations. Une telle structuration facilite l'analyse a posteriori des échanges, la vérification de leur intégrité, ainsi que l'imputabilité des actions aux entités participantes.

Toutefois, l'intégration de la blockchain dans les réseaux véhiculaires se heurte à des contraintes structurelles liées à la volumétrie, à la temporalité et à la forte dynamique des communications V2V. En effet, les architectures blockchain ont été initialement conçues pour traiter des transactions de taille limitée, principalement dans des contextes financiers [62]. À l'inverse, dans un environnement véhiculaire, la génération d'événements est continue et peut être assimilée à la production périodique de messages, impliquant potentiellement l'inscription d'un nombre massif de transactions. Si l'on considère qu'une transaction doit inclure, a minima, un horodatage, l'identifiant de l'émetteur, celui du ou des destinataires, ainsi que des informations relatives au type de message et au contenu requis pour l'audit, la charge informationnelle devient rapidement prohibitive.

[62]: ETSI. *IPv6 Security, Cybersecurity, Blockchain*. Group Report ETSI GR IP6 031. Version V1.1.1. Accessed : 2026-03-05. Sophia Antipolis, France : European Telecommunications Standards Institute (ETSI), nov. 2020

Cette problématique est amplifiée par les spécificités des communications ITS-G5. Les messages de sensibilisation au contexte périodiquesCAM (CAM), dont la taille se situe typiquement entre 200 et 800 octets, sont diffusés à une fréquence pouvant atteindre 10 émissions par seconde et par véhicule. Dans des scénarios de trafic dense, ce flux soutenu engendre une inflation du nombre de transactions, conduisant à la formation de blocs volumineux, difficiles à propager, à valider et à stocker sur des nœuds embarqués caractérisés par des ressources limitées [63]. En outre, l'accumulation progressive des blocs induit une croissance continue du registre, ce qui amplifie les exigences de stockage et de synchronisation au sein d'une blockchain globale, et pose ainsi un enjeu majeur de passage à l'échelle, notamment lorsque la conservation d'un historique long est requise pour les besoins d'audit [14].

[63]: Yi-Ting Sun, Hsin-Chieh Lee, Yun-Chen Yu, Ting-Feng Wu, Ibrahim Althamary et Chih-Wei Huang. *A Multi-Layer Blockchain Simulator and Performance Evaluation of Social Internet of Vehicles with Multi-Connectivity Management*. 2024. arXiv : 2411.14000 [cs.NI]

Dans des scénarios disposant d'une infrastructure (RSU, connectivité cellulaire), l'externalisation de certaines fonctions vers des ressources

cloud est couramment proposé pour atténuer ces contraintes, en apportant des capacités additionnelles de stockage et de calcul et en facilitant la mise en œuvre des mécanismes de consensus [59]. En revanche, dans un contexte strictement V2V, caractérisé par l'absence d'accès continu au cloud, la création et la gestion de la blockchain doivent être réalisées de manière entièrement distribuée par les véhicules. Ce choix ouvre un ensemble de questions de conception déterminantes pour la viabilité du système, notamment :

- Quel véhicule peut créer une nouvelle blockchain ?
- Comment former le groupe de véhicules participant à une même blockchain ?
- Comment décider de maintenir une blockchain en cours d'exécution ou de l'archiver en fonction des changements des nœuds participants ?
- Comment les différentes blockchains archivées dans ce contexte sans infrastructure doivent-elles être fusionnées par les serveurs d'infrastructure lorsque les véhicules reviennent dans des zones couvertes ?

Ces questions restent à ce jour sans réponse normative établie, ce qui reflète un vide plus large dans la standardisation de l'audit des communications V2X, en particulier dans les scénarios reposant exclusivement sur des échanges V2V. Les initiatives des constructeurs automobiles témoignent néanmoins d'une prise de conscience croissante de cet enjeu : l'équipement des véhicules en boîtes noires, désormais préconisé comme fonctionnalité de sécurité obligatoire par la Commission européenne [64], illustre concrètement la volonté d'intégrer les mécanismes d'audit dès la conception du véhicule. Cette absence de standardisation engendre une confusion persistante entre les notions de responsabilité et d'auditabilité, tant dans la communauté académique qu'industrielle, tout en ouvrant des horizons d'innovation pour la conception de mécanismes d'audit adaptés aux spécificités des réseaux V2X.

[64]: European Commission. *Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles*. Article R.476 : Event Data Recorder (EDR) obligatoire juillet 2024. Nov. 2019

Dans ce contexte de normalisation partielle, les standards existants fournissent néanmoins des orientations précieuses. Parmi eux, le standard européen ETSI TS 102 941 constitue la référence principale pour la gestion de la confiance, de l'authentification et de la protection de la vie privée dans les communications ITS. Son étude s'impose comme une étape indispensable pour identifier les mécanismes sur lesquels un système d'audit pourrait s'appuyer et pour positionner notre contribution par rapport aux exigences normatives en vigueur.

2.4 Cadre normatif européen : le standard ETSI TS 102 941

Le déploiement des systèmes de transport intelligents coopératifs (C-ITS) en Europe repose sur un cadre normatif structuré, défini par l'European Telecommunications Standards Institute (ETSI), visant à garantir la sécurité, l'interopérabilité et l'acceptabilité des communications véhiculaires. Parmi les spécifications publiées par l'ETSI, le standard ETSI TS 102 941 constitue la référence principale pour la gestion de la confiance, de l'authentification et de la protection de la vie privée dans les communications ITS.

Ce standard définit une architecture complète de sécurité couvrant l'ensemble du cycle de vie des entités communicantes, depuis leur

enrôlement initial jusqu'à la gestion des comportements malveillants et la révocation des droits de communication. Il introduit notamment des mécanismes explicites de séparation des rôles, de pseudonymisation et de traçabilité conditionnelle, qui placent l'audit au cœur du fonctionnement des systèmes C-ITS.

2.4.1 Architecture PKI européenne et séparation des rôles

Le standard ETSI TS 102 941 [65] spécifie une architecture de sécurité fondée sur une infrastructure à clés publiques hiérarchique, spécifiquement adaptée aux contraintes des environnements véhiculaires. Contrairement aux architectures PKI classiques, cette infrastructure est conçue pour concilier deux objectifs souvent antagonistes : assurer une authentification forte des entités communicantes et préserver la vie privée des usagers.

[65]: *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*. Version 2.2.1. European Telecommunications Standards Institute (ETSI), sept. 2022

L'architecture repose sur une séparation stricte des rôles entre plusieurs autorités indépendantes, chacune étant responsable d'une fonction bien définie. Cette séparation vise à limiter la concentration de la confiance et à empêcher qu'une entité unique ne puisse à la fois identifier un véhicule et suivre l'ensemble de ses communications opérationnelles.

L'Autorité d'Enrôlement est chargée de l'admission initiale des stations ITS dans le système. Elle vérifie l'identité réelle du véhicule ou de son propriétaire ainsi que la conformité technique de la station, puis délivre un certificat d'enrôlement à long terme. Ce certificat atteste de l'appartenance légitime de la station au système C-ITS, mais n'est jamais utilisé directement dans les communications V2X.

L'Autorité d'Autorisation, quant à elle, est responsable de la délivrance des certificats pseudonymes utilisés lors des communications quotidiennes. Avant de fournir ces certificats, elle vérifie la validité du certificat d'enrôlement présenté par la station, sans avoir accès à son identité réelle. Cette dissociation garantit que l'autorité chargée de l'émission des pseudonymes ne peut pas relier ces derniers à un véhicule identifié.

Cette séparation fonctionnelle constitue l'un des piliers du modèle de protection de la vie privée défini par ETSI TS 102 941 [65]. Elle permet de satisfaire simultanément les exigences d'authentification, de responsabilité et de confidentialité, tout en posant les bases d'un système d'audit impartial et juridiquement exploitable.

2.4.2 Préservation de la vie privée et anonymat conditionnel

La protection de la vie privée est considérée par le standard ETSI TS 102 941 [65] comme une condition essentielle à l'acceptation des systèmes C-ITS par les usagers. À cette fin, le standard adopte une approche fondée sur la pseudonymisation systématique des communications, tout en maintenant la possibilité d'établir des responsabilités en cas d'incident.

Deux types de certificats sont ainsi distingués. Le certificat d'enrôlement possède une durée de validité longue et contient l'identité canonique de la station ITS. Il est exclusivement utilisé pour les échanges sécurisés avec les autorités de confiance et n'est jamais diffusé dans le réseau véhiculaire. À l'inverse, les certificats d'autorisation, ou tickets d'autorisation, sont

des certificats pseudonymes à courte durée de validité, utilisés pour signer les messages diffusés dans le cadre des communications V2X.

Le changement fréquent de pseudonymes constitue un mécanisme clé pour empêcher la corrélation des messages émis par un même véhicule sur une longue période. Le standard recommande plusieurs stratégies de renouvellement, incluant des changements périodiques, contextuels ou synchronisés entre plusieurs véhicules, afin de renforcer l'inaliénabilité des communications.

Toutefois, ETSI TS 102 941 [65] ne vise pas un anonymat absolu. Il introduit explicitement le concept d'anonymat conditionnel, selon lequel l'identité réelle d'un véhicule peut être révélée dans des circonstances exceptionnelles, telles que des comportements malveillants avérés, des accidents graves ou des procédures judiciaires. Cette levée d'anonymat ne peut être réalisée qu'à travers la coopération de plusieurs autorités indépendantes, sous contrôle réglementaire, garantissant ainsi un équilibre entre protection de la vie privée et responsabilité des usagers.

2.4.3 Gestion des comportements malveillants et auditabilité

Un apport majeur du cadre normatif ETSI réside dans la formalisation de mécanismes dédiés à la détection et à la gestion des comportements malveillants dans les réseaux C-ITS. Ces mécanismes, regroupés sous le terme de *misbehavior reporting*, constituent le socle normatif de l'audit des communications V2X.

Lorsqu'une station ITS détecte un comportement anormal ou potentiellement dangereux, par exemple la diffusion de messages incohérents, falsifiés ou contradictoires, elle peut générer un rapport de comportement malveillant. Ce rapport inclut le pseudonyme de la station suspectée, une description du comportement observé, ainsi que des éléments de preuve tels que des messages reçus ou des horodatages.

Ces rapports sont transmis à une autorité dédiée, chargée de leur analyse et de leur corrélation. L'objectif est d'identifier les comportements déviants, d'en évaluer la gravité et de décider des mesures appropriées. Cette autorité peut conclure à un faux positif, à un dysfonctionnement technique ou à un comportement malveillant intentionnel.

En cas de comportement avéré, le standard prévoit des mécanismes de révocation des droits de communication. La révocation peut être passive, en cessant de délivrer de nouveaux certificats pseudonymes à la station concernée, ou active, via la diffusion de listes de révocation lorsque la situation exige une réaction immédiate. Ces mécanismes assurent la traçabilité des actions, la non-répudiation et la capacité de reconstituer les événements a posteriori, répondant ainsi aux exigences fondamentales d'un système d'audit.

2.4.4 Positionnement de nos travaux par rapport au standard ETSI

Le standard ETSI TS 102 941 [65] définit un cadre normatif de référence pour la sécurité des communications C-ITS. Nous nous inscrivons globalement dans les principes qu'il établit, tout en identifiant certaines limites que notre travail cherche à dépasser.

Nous sommes favorables au principe de séparation des rôles, qui constitue un pilier central du modèle de sécurité C-ITS. La distinction entre fonctions d'enrôlement et d'autorisation nous semble indispensable pour garantir qu'aucune entité unique ne dispose simultanément des informations d'identité réelle et des pseudonymes opérationnels, limitant ainsi les risques d'abus de pouvoir et renforçant la protection de la vie privée des usagers.

Nous adhérons également au principe d'anonymat conditionnel tel que défini par ETSI. Il nous semble essentiel que l'anonymat des véhicules soit préservé lors de leur fonctionnement normal, et que sa levée ne soit envisageable que dans des circonstances strictement justifiées, telles que des comportements malveillants avérés, et reste soumise à des conditions strictes de contrôle et d'autorisation.

Par ailleurs, nous partageons l'objectif de traçabilité des communications porté par le standard. Le mécanisme de signalement des comportements malveillants introduit par ETSI nous paraît pertinent, et nous estimons que l'utilisation d'une structure immuable et vérifiable pour l'enregistrement des événements d'authentification et de communication renforce naturellement les propriétés de non-répudiation et d'intégrité des traces visées par ce standard.

Nous sommes également favorables à la prise en compte des mécanismes de pseudonymisation dans l'évaluation de la fiabilité de l'authentification, notamment l'impact de la durée de validité des certificats pseudonymes, du renouvellement des identités et de la fraîcheur des informations de sécurité.

En revanche, le standard ETSI TS 102 941 [65] repose implicitement sur l'hypothèse d'une disponibilité suffisante et continue de l'infrastructure de communication, notamment pour le renouvellement des certificats, la transmission des rapports de comportements malveillants et la diffusion des informations de révocation. Or, cette hypothèse n'est pas toujours vérifiée dans des environnements réels caractérisés par une forte mobilité, des connexions intermittentes ou l'absence prolongée d'infrastructure.

C'est précisément dans ces contextes que se situe l'apport principal de notre travail. Nous proposons une extension du cadre ETSI permettant la continuité des fonctions d'authentification et d'audit en environnement partiellement ou totalement déconnecté. L'audit décentralisé basé sur la blockchain, associé à des mécanismes de synchronisation opportuniste entre véhicules, permet de conserver des traces fiables même en l'absence d'autorités centrales accessibles.

Ainsi, notre contribution ne remet pas en cause les fondements normatifs définis par ETSI TS 102 941 [65], mais les complète en offrant une solution adaptée aux scénarios V2V sans infrastructure permanente. Elle vise à renforcer la résilience du système d'audit tout en respectant les exigences de séparation des rôles, d'anonymat conditionnel et de responsabilité qui constituent le socle du standard européen.

Conclusion

Dans ce chapitre, nous avons analysé de manière détaillée les fondements conceptuels de l'audit dans les réseaux véhiculaires ainsi que les principaux schémas d'authentification proposés dans la littérature. Cette étude comparative met en évidence la diversité des approches existantes,

allant des protocoles à cryptographie symétrique aux solutions basées sur l'identité, les signatures de groupe et les infrastructures à clés publiques, chacune présentant des avantages spécifiques mais également des limitations notables.

Il ressort de cette analyse que si de nombreux protocoles parviennent à assurer l'authentification et, dans une certaine mesure, la préservation de la vie privée, peu d'entre eux répondent pleinement aux exigences d'un audit fiable et exploitable, en particulier dans des environnements V2X sans infrastructure. Les mécanismes fortement dépendants d'autorités centrales ou d'unités routières souffrent de problèmes de disponibilité et de scalabilité, tandis que les solutions offrant un anonymat élevé peinent souvent à garantir une traçabilité suffisante en cas de comportement malveillant.

Par ailleurs, l'étude du cadre normatif européen ETSI TS 102 941 souligne l'importance d'un anonymat conditionnel et d'une séparation stricte des rôles pour concilier protection de la vie privée et responsabilité. Cette norme met en lumière le besoin de mécanismes capables de fonctionner efficacement dans des contextes dynamiques, tout en fournissant des preuves d'authentification exploitables à des fins d'audit.

Ces constats motivent la nécessité de nouvelles approches d'authentification et d'audit, capables de s'affranchir partiellement de l'infrastructure tout en conservant des garanties fortes en matière de sécurité et de traçabilité. Le chapitre suivant s'inscrit dans cette perspective en s'intéressant à la fiabilité de l'authentification dans les environnements V2X sans infrastructure, et en proposant des outils d'analyse permettant d'évaluer les performances et les limites des solutions existantes dans de tels contextes.

Fiabilité de l'authentification dans les environnements sans infrastructure

3

3.1 Atteintes à la sécurité et à la vie privée dans les environnements V2X . . 33
3.2 Comparaison qualitative des protocoles d'authentification pour l'audit 36
3.2.1 Critères qualitatifs d'évaluation des protocoles . . 36
3.2.2 Comparaison des solutions d'authentification . 40
3.2.3 Discussion 42
3.3 Comparaison quantitative des protocoles d'authentification 42
3.3.1 Critères mesurables . . . 43
3.3.2 Analyse des performances des protocoles en contexte de couverture limitée . . 44
3.3.3 Discussion 48
3.4 Fiabilité de l'authentification dans les environnements sans infrastructure 48
3.4.1 Modèle analytique 49
3.4.2 Résultats et discussion . 51
3.5 Synchronisation pair-à-pair des données d'authentification hors infrastructure 53
3.5.1 Protocole proposé 53
3.5.2 Évaluation du protocole proposé 55

Introduction

L'audit des communications véhiculaires repose intrinsèquement sur la capacité du système à établir, de manière fiable, l'identité des entités à l'origine des messages échangés. En effet, un mécanisme d'audit ne peut produire des traces exploitables, cohérentes et juridiquement pertinentes que si les informations qu'il enregistre sont associées à des entités préalablement authentifiées. L'authentification constitue ainsi un prérequis fondamental à toute démarche d'audit, en garantissant que les actions observées et consignées dans le système proviennent de participants légitimes et non d'acteurs malveillants ou usurpateurs.

Dans ce contexte, la robustesse d'un système d'audit est directement conditionnée par la fiabilité du mécanisme d'authentification sur lequel il s'appuie. Toute défaillance dans le processus d'authentification, qu'elle soit liée à des informations obsolètes, à une gestion inefficace des révocations ou à une dépendance excessive à l'infrastructure, compromet la valeur probante des traces d'audit produites.

L'objectif de ce chapitre est d'analyser la fiabilité de l'authentification dans de tels environnements contraints. Nous proposons tout d'abord une comparaison qualitative et quantitative des principaux protocoles d'authentification identifiés dans l'état de l'art, en évaluant leur capacité à satisfaire les exigences de sécurité, de protection de la vie privée et d'auditabilité en contexte de couverture limitée. Nous introduisons ensuite un modèle analytique permettant de quantifier la probabilité de succès de l'authentification en fonction de paramètres clés tels que la durée de vie des certificats, le taux de révocation et la fraîcheur des bases de données dans les environnements V2X dépourvus d'infrastructure. Enfin, nous étudions un mécanisme de synchronisation pair-à-pair des données d'authentification, visant à améliorer la fiabilité des communications V2V en l'absence d'infrastructure, et à préparer le terrain pour la conception d'une architecture d'audit décentralisée et robuste.

3.1 Atteintes à la sécurité et à la vie privée dans les environnements V2X

Le déploiement des systèmes de communication V2X introduit un ensemble de défis en matière de sécurité et de confidentialité en raison de leur nature décentralisée, notamment en contexte V2V, des contraintes temps réel et de leur exposition à des entités malveillantes. Ci-dessous, nous présentons les menaces et attaques les plus critiques qui doivent être atténuées afin de maintenir des réseaux véhiculaires robustes et fiables :

— **Traçage et atteinte à la vie privée :** Même avec l'utilisation de pseudonymes, l'observation persistante des schémas de communication peut conduire à la désanonymisation et au profilage des véhicules ou de leurs utilisateurs.

— **Manque d'efficacité de la révocation :** Des mécanismes de révocation inefficaces permettent à des entités compromises ou malveillantes de rester actives et de continuer à transmettre des messages.
— **Attaques Sybil :** Une entité malveillante peut présenter simultanément plusieurs identités, créant une fausse densité de trafic ou manipulant des protocoles basés sur le consensus.
— **Falsification de messages et usurpation :** Des attaquants peuvent injecter de faux messages (par exemple, de fausses alertes de danger routier) ou se faire passer pour des véhicules légitimes afin de tromper les autres et de perturber la sécurité du trafic.
— **Attaques par rejeu :** Des messages légitimes peuvent être capturés puis retransmis ultérieurement afin de tromper le système, par exemple en rejouant une ancienne alerte de freinage d'urgence.
— **Déni de service (DoS) :** Des attaquants peuvent submerger le réseau ou les services d'authentification avec de fausses requêtes, empêchant l'accès aux véhicules légitimes.
— **Liabilité et échec de l'inaliénabilité :** Une mauvaise rotation des pseudonymes ou l'utilisation d'identifiants statiques permet aux attaquants de lier plusieurs messages et de suivre les véhicules dans le trafic à travers le temps.

Face à l'ensemble de ces menaces, l'authentification des entités communicantes, qu'il s'agisse des véhicules, des RSUs ou des services d'infrastructure, constitue le mécanisme central autour duquel s'articulent les différentes mesures de protection. Elle permet au système de distinguer les entités légitimes des acteurs malveillants, de garantir l'intégrité et l'origine des messages échangés, de prévenir les usurpations d'identité ainsi que les attaques Sybil, et d'assurer la traçabilité nécessaire aux mécanismes d'audit.

Sans un mécanisme d'authentification robuste, les autres mesures de sécurité ne peuvent être mises en œuvre efficacement. En effet, la révocation ne peut cibler que des entités préalablement identifiées, la non-répudiation ne peut être assurée que si les actions sont associées à des identités vérifiées, et la protection de la vie privée ne peut être garantie que dans le cadre d'un anonymat conditionnel reposant lui-même sur des mécanismes d'authentification fiables. Le choix du protocole d'authentification apparaît ainsi comme un facteur déterminant pour assurer la mise en œuvre d'un mécanisme d'audit fiable dans les environnements V2X.

Afin d'évaluer les propriétés de sécurité et de confidentialité des principales catégories d'authentification en V2X, le Tableau3.1 propose une vue comparative de ces mécanismes face aux menaces clés.

Les schémas basés sur la PKI présentent une forte résistance à la falsification de messages et aux attaques par rejeu grâce à l'utilisation de signatures numériques et de l'authentification par certificats. Toutefois, leur résilience face aux attaques Sybil et au traçage des véhicules dépend fortement de l'efficacité des stratégies de gestion et de rotation des pseudonymes. Des travaux récents de [74] montrent que des mécanismes de renouvellement de pseudonymes inadéquats peuvent conduire à une liabilité à long terme, compromettant ainsi la confidentialité des utilisateurs. De plus, bien que la révocation soit généralement bien prise en charge via les CRL ou le protocole OCSP, ces mécanismes introduisent

[66]: Diana Magalhaes, Vinicius C. Ferreira, Nelson Rodrigues et João M. Fernandes. « A 5G-based Authentication Framework for V2X Communication ». In : *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2023

[67]: Zuobin Ying, Kaichao Wang, Jinbo Xiong et Maode Ma. « A literature review on V2X communications security : Foundation, solutions, status, and future ». In : *IET Communications* 18 (juin 2024)

[68]: Yaling Zhu, Jia Zeng, Fangchen Weng, Dan Han, Yiyu Yang, Xiaoqi Li et Yuqing Zhang. « Sybil Attacks Detection and Traceability Mechanism Based on Beacon Packets in Connected Automobile Vehicles ». In : *Sensors* 24.7 (2024)

[69]: Babajide Asaju. « Addressing Public Key Infrastructure (PKI) Challenges in V2X Networks : Strategies for Scalability, Certificate Management, and Trusted Authorities ». In : 4 (jan. 2024)

[70]: Gianluca Scopelliti, Christoph Baumann, Fritz Alder, Eddy Truyen et Jan Mühlberg. « Efficient and Timely Revocation of V2X Credentials ». In : jan. 2024

[71]: Ahmed Manasrah, Qussai Yaseen, Hussain Al-Aqrabi et Lu Liu. « Identity-Based Authentication in VANETs : A Review ». In : *IEEE Transactions on Intelligent Transportation Systems* 26.4 (2025)

[72]: Jia Liu, Liqun Chen, Mehrdad Dianati, Carsten Maple et Yan Yan. « A Novel Computationally Efficient Group Signature for Anonymous and Secure V2X Communications ». In : *arXiv* 2307.13759 (2023). arXiv :2307.13759 [cs.CR]

[73]: Seema Gaba, Monisha Gupta et Harmanjeet Singh. « A comprehensive survey on VANET security attacks ». In : jan. 2023

[74]: Gianluca Scopelliti, Christoph Baumann, Fritz Alder, Eddy Truyen et Jan Tobias Mühlberg. « Efficient and timely revocation of v2x credentials ». In : *Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS'24)*. Internet Society. 2023

Table 3.1 – Résistance des schémas d'authentification face aux défis de sécurité et de confidentialité en V2X

Type de schéma	Falsification / usurpation de messages	Attaque Sybil	Traçage	Attaque par rejeu	Attaque DoS	Inaliénabilité	Révocation
Basé PKI	✓ Fort [66, 67] (authentique et traçable)	Faible [68] (identités multiples via pseudonymes ou abus de certificats)	Moyen (dépend de la gestion des pseudonymes)	✓ Bon [66] (horodatages, nonces)	Sensible [69] (vérification de signatures coûteuse)	Variable [69] (dépend du renouvellement des pseudonymes)	✓ Bon [70] (CRL ou OCSP)
Basé sur l'identité	✓ Fort [32] (authentification sans certificats)	Faible [25] (pas d'unicité d'identité, clés duplicables)	Faible [25] (support limité des pseudonymes)	✓ Modéré [31] (signatures horodatées)	Sensible (coût computationnel élevé)	Absente [25]	Faible [71] (nécessite un renouvellement complet des clés)
Signature de groupe	✓ Fort [72] (authentique et anonyme)	✓ Fort [72] (signature au niveau du groupe)	✓ Élevé [72] (identité masquée dans le groupe)	✓ Bon (horodatage)	Coût élevé (vérification lente)	✓ Fort [70] (signataires et signatures non liables)	Complexe [70] (nécessite l'ouverture des signatures par le gestionnaire du groupe)
Cryptographie symétrique	✓ Légère [67, 73] (rapide mais risquée en cas de compromission de clé)	Faible [67] (pas de contrôle d'identité)	Nulle [73] (pas d'anonymat)	Nécessite un mécanisme de nonce [73]	✓ Résiliente [67] (faible surcharge)	Non supportée	Non supportée

des latences et une surcharge en bande passante, en particulier dans des réseaux véhiculaires dynamiques.

Les schémas à signature de groupe sont intrinsèquement respectueux de la vie privée, offrant une forte inaliénabilité et un anonymat robuste en permettant aux véhicules de s'authentifier en tant que membres d'un groupe sans révéler leur identité individuelle. Cela les rend particulièrement adaptés aux scénarios V2X sensibles à la confidentialité. Néanmoins, comme le souligne [75], ces schémas souffrent de coûts computationnels élevés et d'une complexité importante de la révocation. La révocation d'un seul membre nécessite généralement l'identification et le renouvellement des clés de l'ensemble du groupe, ce qui engendre une surcharge significative. Bien que des solutions telles que la vérification par lots ou la révocation basée sur des seuils aient été proposées, leur déploiement pratique reste limité.

[75]: Morteza Azmoudeh Afshar, Nesrine Benchoubane, Busra Cayoren, Gunes Karabulut Kurt et Enver Ozdemir. *Privacy-Preserving and Simultaneous Authentication in High-Density V2X Networks*. arXiv preprint arXiv :2501.06087. v2. Mai 2025

Les systèmes cryptographiques basés sur l'identité permettent une authentification forte sans recourir aux certificats classiques, simplifiant ainsi la gestion des clés. Cependant, ils ne garantissent pas intrinsèquement l'unicité des identités, ce qui les expose aux attaques Sybil. De plus, de nombreux protocoles basés sur l'identité offrent un support limité des pseudonymes, affaiblissant la confidentialité des utilisateurs. Selon [76], le processus de renouvellement des clés dans ces schémas est souvent complexe et peu adapté aux réseaux véhiculaires hautement dynamiques et temps réel.

[76]: Ahmed Manasrah, Qussai Yaseen, Hussain Al-Aqrabi et Lu Liu. « Identity-Based Authentication in VANETs : A Review ». In : *IEEE Transactions on Intelligent Transportation Systems* (2025)

Enfin, les approches d'authentification basées sur des clés symétriques offrent une vérification des messages légère et efficace, ce qui les rend résilientes face aux attaques DoS. En revanche, elles offrent des garanties de confidentialité minimales, car les clés partagées ne permettent ni l'inaliénabilité de l'émetteur, ni une différenciation claire des identités.

De plus, en l'absence d'une autorité centrale pour la révocation des clés, la compromission d'une seule clé compromet l'ensemble du domaine. Cette vulnérabilité a été mise en évidence par les auteurs de [77] qui préconisent l'intégration des méthodes symétriques dans des cadres hybrides soutenus par la PKI pour assurer une gestion et une révocation sécurisées des clés.

[77]: S. Al-Khalaf, A. Al-Rasheed et R. Khan. « Lightweight Symmetric-Key Authentication Schemes for V2X Communications : Performance and Limitations ». In : *IEEE Access* 12 (2024)

Ces analyses fonctionnelles du comportement de sécurité de chaque schéma constituent la base d'une analyse plus structurée et comparative, présentée dans la section suivante, en s'appuyant sur une définition de critères d'authentification sécurisée au sein d'un système d'audit.

3.2 Comparaison qualitative des protocoles d'authentification pour l'audit

Afin d'identifier des critères pertinents pour l'évaluation de mécanismes d'authentification sécurisés dans un système d'audit, nous avons analysé plusieurs travaux de référence portant sur la cybersécurité des communications V2X. Les auteurs de [66] examinent des exigences de sécurité essentielles telles que l'autorisation des équipements utilisateurs, la protection de l'intégrité des données et la préservation de la vie privée. L'étude présentée dans [78] propose une taxonomie des solutions de sécurité existantes pour les communications V2X, en analysant les menaces et les critères pertinents pour l'évaluation de la sécurité. Enfin, [79] abordent les exigences de sécurité, les attaques et les solutions associées aux communications V2X, tout en mettant en évidence les défis actuels et les pistes de recherche futures.

[78]: Roshan Sedar, Charalampos Kalalas, Francisco Vázquez-Gallego, Luis Alonso et Jesus Alonso-Zarate. « A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths ». In : *IEEE Open Journal of the Communications Society* 4 (2023)

[79]: Monowar Hasan, Sibin Mohan, Takayuki Shimizu et Hongsheng Lu. « Securing Vehicle-to-Everything (V2X) Communication Platforms ». In : *IEEE Transactions on Intelligent Vehicles* 5.4 (2020)

Dans cette section, nous identifions, analysons et définissons, à travers la figure 3.1, les critères qualitatifs nécessaires à la mise en œuvre d'un mécanisme d'audit. Nous procédons ensuite à une évaluation approfondie de différentes solutions d'authentification, en examinant soigneusement leurs avantages et leurs inconvénients au regard des critères identifiés. L'objectif est de fournir une analyse complète de leur efficacité et de leur adéquation particulière au contexte d'un système d'audit. En étudiant dans quelle mesure ces solutions permettent des audits fiables, transparents et sécurisés, nous cherchons à déterminer quels protocoles d'authentification sont les plus adaptés pour garantir l'intégrité, la traçabilité et la non-répudiation requises dans les réseaux véhiculaires.

3.2.1 Critères qualitatifs d'évaluation des protocoles

En nous appuyant sur les analyses de sécurité et les stratégies d'authentification étudiées dans [80], nous avons identifié et consolidé six critères qualitatifs récurrents dans les solutions proposées par la littérature. Ces critères communs constituent la base de notre analyse comparative des solutions d'authentification pour les communications V2X, comme illustré à la figure 3.1 : la méthode cryptographique, le domaine réseau, le principe de confidentialité, le principe d'identification, la base de données et le principe de révocation.

[80]: Mir Ali Rezazadeh Baee, Leonie Simpson, Xavier Boyen, Ernest Foo et Josef Pieprzyk. « Authentication Strategies in Vehicular Communications : A Taxonomy and Framework ». In : *EURASIP Journal on Wireless Communications and Networking* 2021 (mai 2021)

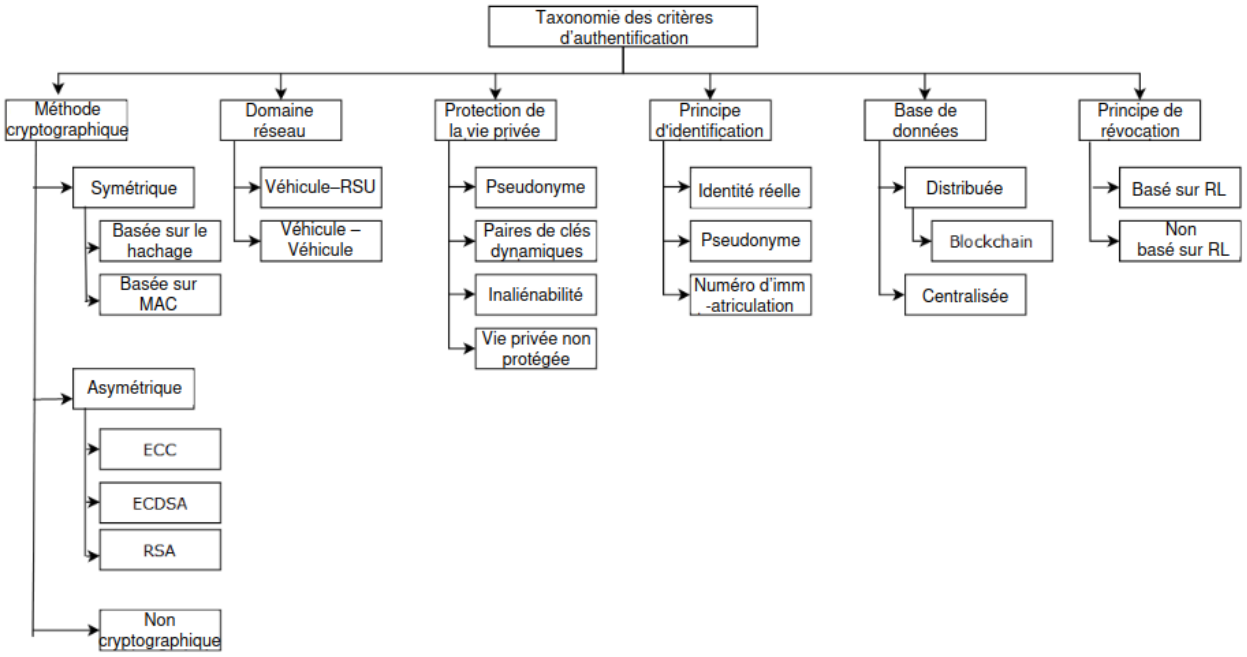

Figure 3.1 – Critères qualitatifs pour l'évaluation des protocoles d'authentification.

Méthode cryptographique

Comme illustré à la figure 3.1, lorsqu'un véhicule V_1 communique avec un véhicule V_2, il est essentiel de garantir l'authenticité et l'intégrité des messages échangés. Les méthodes cryptographiques jouent un rôle fondamental dans ce processus en fournissant un cadre sécurisé pour les systèmes d'authentification véhiculaires. Elles assurent la protection des données transmises contre toute altération, tout en garantissant leur authenticité. Grâce à l'utilisation de techniques cryptographiques avancées telles que le hachage et le chiffrement, les informations sensibles restent protégées durant leur transmission, les rendant infalsifiables par des entités malveillante. Ce niveau de sécurité est indispensable pour renforcer la fiabilité et la confiance globale envers le système de communication, soulignant ainsi l'importance de la cryptographie dans les mécanismes d'authentification véhiculaires [81]. Les principales techniques utilisées sont les suivantes :

[81]: Mahmoud A. Shawky, Syed Tariq Shah, Mohammed Abdrabou, Muhammad Usman, Qammer H. Abbasi, David Flynn, Muhammad Ali Imran, Shuja Ansari et Ahmad Taha. « How secure are our roads ? An in-depth review of authentication in vehicular communications ». In : *Vehicular Communications* 47 (2024)

— Cryptographie symétrique : Cette méthode utilise une clé unique pour le chiffrement et le déchiffrement. Elle est rapide et efficace pour sécuriser les communications, mais la gestion des clés partagées constitue un défi majeur. La cryptographie basée sur le hachage repose sur des fonctions de hachage pour transformer les données d'entrée en une chaîne de longueur fixe, principalement afin de vérifier l'intégrité des données. La cryptographie basée sur les MAC (Message Authentication Code) utilise la cryptographie symétrique et une clé secrète pour générer un code d'authentification de message (MAC), permettant de vérifier à la fois l'authenticité et l'intégrité du message.
— Cryptographie asymétrique : Cette méthode repose sur une paire de clés pour le chiffrement et le déchiffrement des messages et est largement utilisée pour l'authentification et la sécurisation des canaux de communication. Parmi ces méthodes, la cryptographie sur courbes elliptiques (ECC) se distingue par un haut niveau de

sécurité avec des clés plus courtes, la rendant plus efficace que d'autres algorithmes asymétriques. L'un de ses principaux usages est l'algorithme de signature numérique ECDSA, qui garantit l'intégrité et l'authenticité des messages. À l'inverse, l'algorithme RSA, bien qu'étant largement utilisé, nécessite des clés plus longues pour offrir un niveau de sécurité équivalent à celui de l'ECC.
— Solution non cryptographique : Certaines solutions d'authentification ne reposent pas forcément sur des mécanismes cryptographiques et privilégient des approches plus légères ou alternatives. Par exemple, [39] propose un mécanisme d'authentification basé sur des opérations XOR légères et des fonctions de hachage à sens unique.

Domaine réseau

Le domaine réseau définit les types de communications et les mécanismes d'authentification utilisés, influençant directement la portée et la structure des interactions au sein du système. La figure 3.1 illustre deux domaines distincts :

— V2R : Dans ce modèle, l'infrastructure, notamment à travers les unités routières RSU (Road Side Units), joue un rôle central. Les véhicules communiquent avec l'infrastructure afin d'accéder à des données d'authentification mises à jour. Par exemple, le véhicule V_1 peut vérifier les listes de révocation les plus récentes lors de l'authentification de V_2. Ce modèle améliore la sécurité, car les données sont continuellement actualisées via le réseau.
— V2V : En l'absence d'infrastructure, le modèle V2V repose sur des communications directes entre véhicules. Dans ce cas, les véhicules s'appuient sur une base de données locale pour l'authentification, comme illustré par l'authentification entre V_3 et V_4. Toutefois, cette base de données locale peut ne pas être à jour, ce qui pose des problèmes de sécurité et d'intégrité des échanges.

Protection de la vie privée

La protection de la vie privée des utilisateurs est assurée par des mécanismes visant à préserver la confidentialité des données personnelles tout en empêchant le traçage. Ces mécanismes garantissent l'anonymat et la résistance au traçage des messages tout en permettant l'authentification [82]. Par exemple, dans la figure 5.1, une autorité de certification de pseudonymes est utilisée pour attribuer des pseudonymes anonymes aux véhicules. Plusieurs techniques peuvent être mises en œuvre pour renforcer la protection de la vie privée :

[82]: Jiaqi Huang, Dongfeng Fang, Yi Qian et Rose Qingyang Hu. « Recent Advances and Challenges in Security and Privacy for V2X Communications ». In : *IEEE Open Journal of Vehicular Technology* 1 (2020)

— Pseudonyme : Les pseudonymes permettent aux véhicules de communiquer à l'aide d'identifiants temporaires ou anonymes, réduisant la capacité des observateurs externes à relier les messages à un utilisateur ou un véhicule spécifique.
— Paires de clés dynamiques : Cette méthode repose sur le renouvellement périodique des clés afin d'empêcher le traçage et de garantir des communications sécurisées.
— Non-traçage (unlinkability) : Elle garantit que différentes sessions d'un même utilisateur ne peuvent pas être corrélées, préservant ainsi la confidentialité des activités.

— Absence de confidentialité : Absence de confidentialité : certaines solutions ne privilégient pas la protection de la vie privée, ce qui peut être acceptable dans des contextes spécifiques où cette exigence n'est pas prioritaire. Par exemple, certains schémas d'authentification basés sur l'identité utilisent directement l'identité réelle du véhicule lors du processus d'authentification. Dans ce type d'approche, la protection de la vie privée n'est pas garantie, car l'identité du véhicule peut être exposée ou facilement traçable. C'est notamment le cas du protocole proposé dans [40], dans lequel l'authentification repose sur des identités explicites des entités communicantes, sans mécanisme spécifique d'anonymisation.

Principe d'identification

Les entités d'un système peuvent être identifiées selon différentes méthodes, chacune ayant un impact significatif sur la sécurité globale et la protection des données. Le choix du mécanisme d'identification influence directement l'équilibre entre confidentialité et responsabilité [80]. Les méthodes courantes incluent :

— Identité réelle : Les utilisateurs sont identifiés par leur identité réelle, ce qui est nécessaire dans des environnements exigeant une authentification stricte.
— Pseudonyme : L'identification par pseudonyme permet de masquer l'identité réelle tout en assurant l'authentification.
— Numéro d'immatriculation : L'utilisation du numéro d'immatriculation comme identifiant offre une identification claire, souvent utilisée dans les systèmes de gestion de flotte ou de péage.

Base de données

Une base de données est indispensable pour stocker les informations nécessaires à l'authentification. Son type, sa gestion et sa disponibilité sont des éléments clés pour garantir la sécurité et la fiabilité du système. Le choix entre une base de données centralisée ou distribuée influence directement l'architecture et la résilience du système :

— Centralisée : Une base de données centralisée regroupe toutes les informations d'authentification en un point unique. Bien que plus simple à gérer, elle présente un risque de point de défaillance unique. Comme illustré à la figure 3.1, cette base peut être hébergée dans le Cloud ou localement dans le véhicule lorsque l'infrastructure est absente. Dans ce dernier cas, les données peuvent devenir obsolètes, augmentant les risques de sécurité.
— Distribuée : Les bases de données distribuées répartissent les informations sur plusieurs nœuds, améliorant la résilience et la disponibilité du système. La blockchain, en tant que base de données distribuée et immuable, offre un haut niveau de sécurité et de transparence [83]. Toutefois, comme observé dans plusieurs solutions telles que [21] et [26], la blockchain est souvent hébergée dans le Cloud, introduisant une forme de centralisation partielle.

[83]: « Blockchain challenges and opportunities : a survey ». In : *Int. J. Web Grid Serv.* 14.4 (jan. 2018)

Principe de révocation

Les mécanismes de révocation garantissent que seuls les véhicules légitimes peuvent accéder au système. Une solution de révocation efficace permet de retirer de manière sécurisée les privilèges d'authentification des véhicules compromis [27]. Plusieurs méthodes peuvent être utilisées :

— Basée sur des listes de révocation : Cette méthode repose sur des listes contenant les identifiants des entités révoquées. L'autorité d'authentification est chargée de mettre à jour ces listes, qui doivent être régulièrement diffusées pour maintenir la sécurité du système.
— Non basée sur des listes de révocation : Ces méthode utilisent des mécanismes alternatifs, tels que des jetons d'authentification à durée de validité suffisamment courte pour se passer du maintien d'une liste de révocation : un jeton compromis devient invalide avant même qu'une procédure de révocation ne soit nécessaire [70].

3.2.2 Comparaison des solutions d'authentification

La taxonomie des critères d'authentification pour les protocoles de communication véhiculaires constitue un cadre structuré permettant l'évaluation et la comparaison des différentes solutions. La taxonomie présentée dans la section précédente facilite l'identification des critères essentiels pour des solutions d'authentification fiables et permet une comparaison systématique. Comme détaillé dans le tableau 3.2, l'application des critères retenus permet d'évaluer dans quelle mesure chaque protocole répond aux exigences spécifiques de l'audit dans les réseaux de communication véhiculaires.

L'analyse du tableau 3.2 permet de dégager plusieurs constats. Les protocoles basés sur la PKI constituent la famille la plus représentée et la plus adaptée aux exigences d'audit : ils recourent majoritairement à la cryptographie asymétrique sur courbes elliptiques (ECC/ECDSA), offrent une identification par pseudonymes préservant la vie privée, et intègrent la blockchain comme base de données distribuée garantissant l'immutabilité des traces. Cependant, ils restent pour la plupart conçus pour des environnements V2R, où l'infrastructure est disponible en permanence pour la gestion des certificats et la révocation.

Les protocoles basés sur l'identité présentent l'avantage de ne pas nécessiter de certificats numériques classiques, réduisant la charge de gestion des clés. Toutefois, plusieurs d'entre eux ne garantissent pas l'unicité des identités, les exposant aux attaques Sybil, et leur support limité des pseudonymes affaiblit la protection de la vie privée. La révocation y est également plus complexe, nécessitant souvent un renouvellement complet des clés.

Les protocoles à signature de groupe offrent un niveau d'anonymat élevé, les membres s'authentifiant collectivement sans révéler leur identité individuelle. Cependant, ils souffrent de coûts computationnels élevés et d'une gestion de révocation particulièrement complexe, ce qui les rend peu adaptés aux contraintes temps réel des réseaux véhiculaires.

Enfin, les protocoles à cryptographie symétrique sont efficaces et légers, mais ils n'offrent ni pseudonymisation robuste, ni inaliénabilité, et la

[84]: Zhuo Ma, Junwei Zhang, Yongzhen Guo, Yang Liu, Ximeng Liu et Wei He. « An Efficient Decentralized Key Management Mechanism for VANET With Blockchain ». In : *IEEE Transactions on Vehicular Technology* 69.6 (2020)

[85]: Anil Kumar Sutrala, Palak Bagga, Ashok Kumar Das, Neeraj Kumar, Joel J. P. C. Rodrigues et Pascal Lorenz. « On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment ». In : *IEEE Transactions on Vehicular Technology* 69.5 (2020)

[86]: Ikram Ali, Tandoh Lawrence et Fagen Li. « An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs ». In : *Journal of Systems Architecture* 103 (2020)

[87]: Abdelkrim Imghoure, Fouzia Omary et Ahmed El-Yahyaoui. « Hybrid cryptography-based scheme with conditional privacy-preserving authentication and memory-based DOS resilience in V2X ». In : *Vehicular Communications* 49 (2024)

Catégorie	Articles	Méthode cryptographique	Domaine réseau	Confidentialité	Identification	Base de données	Révocation
PKI	[28]	ECDSA modifié	V2R/V2V	Paires de clés dynamiques	Pseudonymes dynamiques	Blockchain Ethereum	Via des smart contracts
	[21]	RSA-1024	V2V	Pseudonymes dynamiques	Pseudonymes	Blockchain Ethereum multi-niveaux	Via des smart contracts
	[26]	ECC	V2V/V2I	Pseudonymes	Pseudonymes	Blockchain	–
	[49]	ECC	V2V/V2I	Identité chiffrée	Identification biologique	Blockchain	Par une autorité de confiance
	[23]	ECC et ECDSA	V2V/V2R	Identité unique	Pseudonymes	Blockchain	Par l'autorité d'enregistrement
	[84]	ECC, ECDSA, ECIES et fonction bivariée	V2R	Identité unique	Pseudonymes	Blockchain	Vote décentralisé via smart contracts
	[30]	ECC et RSA-128	V2V/V2R	Pseudonymes	Pseudonymes	Blockchain	–
	[85]	ECC	V2V/V2R	Pseudonymes	Pseudonymes générés par RSU	Non spécifiée	Par une autorité de confiance
	[5]	ECC	V2V/V2R	Certificat à courte durée de vie	Pseudonymes	Cloud	Liste de révocation mise à jour par RSU
Basé sur l'identité	[25]	Basé sur le hachage et ECC	V2V	Identité anonyme	Identité anonyme	Non spécifiée	Par une autorité de confiance
	[40]	Basé sur le hachage, appariements bilinéaires	V2R	Pseudonymes	Pseudonymes	Non spécifiée	Par une autorité de confiance
	[42]	2-DNF	V2R	Chiffrement basé sur l'identité	Chiffrement basé sur l'identité	Blockchain permission-née	–
	[86]	ECC, fonctions de hachage à sens unique	V2V	Identité anonyme	Identité anonyme	Blockchain permission-née	Par une autorité de confiance
	[32]	Hachage, QR, XOR	V2X	Identités pseudo-aléatoires	Pseudonymes temporaires	BD centralisée	Journalisation des jetons + réattribution
	[31]	ECC, ECDH, hachage, AES	V2V	Pseudonymes temporaires	Identité anonyme	BD centralisée	Par une autorité de confiance
	[87]	Hybride : ECC, ECDH, HMAC	V2V/V2I	Pseudonymes dynamiques	Pseudonymes	Centralisée	Par une autorité de confiance
Signature de groupe	[43]	ECC	V2I	Pseudonymes temporaires (PIDi), clé privée aléatoire	Pseudonymes	Non spécifiée	–
	[45]	Basé sur le hachage	V2V	Pseudonymes, certificats d'adhésion	Pseudonymes	Non spécifiée	–
	[46]	Signature de groupe courte, clé symétrique, Diffie-Hellman	V2V/V2I	Signature de groupe	Pseudonymes	Non spécifiée	Liste de révocation des certificats
	[44]	Diffie-Hellman, AES	V2I	Pseudonymes	Pseudonymes (non-traçabilité)	Non spécifiée	Liste de révocation des identifiants
Symétrique	[39]	PUF, XOR, hachage	V2V	Pseudonymes dynamiques	Identité réelle via TA	Non spécifiée	Gérée par la TA
	[38]	Hachage + mot de passe	V2V/V2I	Identité anonyme	Identité réelle via TA	Non spécifiée	Gérée par la TA
	[29]	ECDSA, ECC	V2V/V2I	Identité anonyme	Identités temporaires	Cloud	Gérée par la TA

Table 3.2 – Comparaison qualitative des solutions d'authentification

compromission d'une seule clé peut compromettre l'ensemble du système. Leur absence de mécanisme de révocation structuré constitue également une limite majeure pour les systèmes d'audit.

3.2.3 Discussion

Pour répondre aux exigences d'un audit rigoureux des communications véhiculaires, un système d'authentification doit garantir une authentification forte, la non-répudiation et une scalabilité adaptée aux réseaux de grande taille. Afin de favoriser la participation des véhicules aux applications coopératives, il doit également préserver l'anonymat des utilisateurs. Par conséquent, la PKI est largement reconnue comme une solution privilégiée pour l'authentification dans les réseaux véhiculaires, notamment dans les VANETs.

En effet, plusieurs standards soutiennent l'utilisation de la PKI dans les environnements véhiculaires. La norme ISO/SAE 21434 [34] traite de la cybersécurité des véhicules et fournit des recommandations détaillées sur la gestion des clés et de l'authentification. ETSI TS 102 941 [65] définit des mécanismes de sécurité basés sur la PKI pour les Systèmes de Transport Intelligents.(ITS), tandis que le NIST SP 800-57 [88] fournit des lignes directrices sur la gestion des clés et la scalabilité des systèmes PKI. La norme IEEE 1609.2 [89] constitue également une référence majeure pour la sécurisation des systèmes de transport intelligents coopératifs.

Ces convergences normatives, combinées aux résultats de la comparaison qualitative du tableau 3.2, motivent le choix ces deux protocoles d'authentification basé sur PKI intégrant la blockchain : ACB-MAC (Authentication for Cluster-Based Medium Access Control)[21] et BCPPA (A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks)[28] pour une comparaison quantitative approfondie dans la section suivante, en contexte de couverture réseau limitée.

[88]: National Institute of Standards and Technology (NIST). *NIST Special Publication 800-57 : Recommendation for Key Management*. Rapp. tech. 800-57. Version Part 1 Revision 5. Gaithersburg, MD, USA : National Institute of Standards et Technology, mai 2020

[89]: « IEEE Approved Draft Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages ». In : *IEEE Std 1609.2-2022 (Revision of IEEE Std 1609.2-2016)* (2023)

3.3 Comparaison quantitative des protocoles d'authentification

Dans cette étude, nous avons choisi de comparer deux solutions majeures d'authentification basées sur la PKI et intégrant la blockchain : ACB-MAC [21] et BCPPA [28]. Ces deux protocoles ont été retenus en raison de leur capacité à proposer des mécanismes avancés de gestion de la confidentialité et d'authentification sécurisée, tout en exploitant la blockchain pour garantir l'intégrité des transactions et faciliter l'audit. ACB-MAC s'appuie sur l'utilisation de pseudonymes dynamiques pour anonymiser les véhicules dans un contexte de communication V2I, ce qui protège la vie privée des usagers tout en maintenant une interaction continue avec l'infrastructure. À l'inverse, BCPPA utilise des paires de clés dynamiques et favorise les communications V2V au sein de clusters, rendant les véhicules plus autonomes et réduisant la dépendance à une infrastructure centralisée. Ces deux approches offrent ainsi des perspectives différentes pour la gestion de la sécurité et de la confidentialité dans les communications V2X. Il convient de noter que les deux solutions utilisent la blockchain afin d'assurer la traçabilité et l'immutabilité des

événements d'authentification, un aspect essentiel pour établir des systèmes d'audit robustes et maintenir un haut niveau de sécurité à l'échelle du réseau.

3.3.1 Critères mesurables

Afin de comparer efficacement les performances de ces protocoles d'authentification, plusieurs critères peuvent être considérés, notamment la latence d'authentification, le débit, l'utilisation des ressources, les taux d'échec, la scalabilité, ainsi que l'efficacité de la gestion des clés [90]. Ces critères mesurables fournissent un cadre d'évaluation complet, couvrant à la fois l'efficacité et la fiabilité des solutions.

[90]: Farooque Azam, Sunil Kumar Yadav, Neeraj Priyadarshi, Sanjeevikumar Padmanaban et R. C. Bansal. « A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network ». In : *IEEE Access* 9 (2021)

Sur la base de l'analyse détaillée des articles examinés et des évaluations réalisées par leurs auteurs, nous avons retenu un ensemble de critères mesurables constituant un cadre robuste pour apprécier, de manière objective, l'efficacité et la fiabilité d'une solution d'authentification. Ces critères, issus d'études empiriques et de résultats expérimentaux validés, permettent de comparer les protocoles d'authentification selon leurs performances et leur niveau de fiabilité :

- **Latence d'authentification** : temps moyen nécessaire pour compléter le processus d'authentification d'un véhicule.
- **Débit d'authentification** : volume de données échangées par seconde lors du processus d'authentification.
- **Taux de perte de paquets (PLR)** : proportion de messages perdus durant les échanges d'authentification, reflétant la fiabilité des transmissions dans le réseau véhiculaire.
- **Coût de déploiement** : coût en ressources computationnelles (gas) associé aux opérations sur blockchain, évaluant la viabilité économique de la solution.
- **Capacité de stockage** : volume de données nécessaire au stockage des informations d'authentification au sein du système.
- **Taux d'échec d'authentification** : proportion de tentatives d'authentification échouées, reflétant la fiabilité du protocole en contexte de couverture réseau limitée.

À partir des simulations décrites par les auteurs des deux solutions, ACB-MAC et BCPPA, nous avons rassemblé les critères effectivement mesurés dans le tableau 3.3, afin d'identifier ceux qui sont les plus pertinents pour comparer les deux protocoles sur des bases homogènes.

Dans la première simulation, le protocole BCPPA fonctionne sur une zone de 1 km^2 divisée en quatre sous-zones de 0.5×0.5 km^2, chacune couverte par une RSU disposant d'une portée de communication de 600 m. Les véhicules, se déplaçant à des vitesses comprises entre 7.5 m/s et 40 m/s, échangent des messages toutes les 100 ms avec une portée de communication de 300 m. La bande passante est limitée à 6 Mbps et la taille des paquets transmis est de 264 octets, pour une durée totale de simulation de 100 secondes. L'objectif principal de ce protocole est d'assurer la confidentialité tout en garantissant une authentification efficace au sein du réseau véhiculaire.

De manière complémentaire, le protocole ACB-MAC adopte une approche basée sur des clusters dans un environnement où les véhicules circulent sur une route à deux voies, chaque voie ayant une largeur de 5 mètres, et une vitesse maintenue à 100 km/h. Les véhicules sont organisés en clusters afin d'optimiser la gestion des communications, chaque cluster

Table 3.3 – Comparaison entre BCPPA et ACB-MAC à partir des évaluations proposées par leurs auteurs respectifs

Métrique	**BCPPA**	**ACB-MAC**
Délai d'authentification (ms)	40 ms lorsque la densité < 70 véhicules, > 60 ms au-delà	Maximum 3.10 ms
Taux de perte de paquets (PLR)	Quasi nul pour une densité < 70 véhicules, augmente au-delà	NSM : faible ; SM : légèrement plus élevé
Coût en gas (USD)	0.1536 USD (déploiement), 0.0093 USD (opération)	–
Stockage (MB)	540 MB (pour un million de véhicules)	606 MB (pour un million de véhicules)
Débit (Mbps)	17.57 Mbps	15 Mbps
Simulateur	VanetMobiSim, NS-2, Ethereum Rinkeby	MATLAB, Ganache, Truffle, MetaMask, VM
Objectif de l'évaluation	Sécurité, authentification rapide, protection de la confidentialité, anonymat et traçabilité	Amélioration du débit et réduction du délai avec coûts réduits

étant dirigé par un leader dit cluster head (CH). Le protocole distingue les messages de sécurité (SM) et les messages non liés à la sécurité (NSM), en appliquant des mécanismes de communication spécifiques visant à réduire la latence et à améliorer le taux de réussite de transmission. Une attention particulière est accordée aux véhicules d'urgence, qui sont priorisés au sein des clusters afin d'assurer une transmission rapide et sécurisée des messages.

Le tableau 3.3 met en évidence les différences fondamentales entre les protocoles BCPPA et ACB-MAC, sur la base des évaluations réalisées par leurs propres auteurs. BCPPA se distingue par son orientation vers la sécurité, la protection de la confidentialité et une authentification rapide, avec des coûts en gas relativement faibles pour les opérations sur Ethereum. Toutefois, son délai d'authentification augmente lorsque la densité de véhicules dépasse 70, et certaines métriques de performance, notamment en environnement fortement chargé, ne sont pas toujours détaillées. À l'inverse, ACB-MAC met l'accent sur l'optimisation du débit (15 Mbps) et propose des délais de transmission très faibles (3.10 ms au maximum), ce qui le rend particulièrement adapté aux applications exigeant une forte réactivité, en particulier pour les messages de sécurité. Malgré des besoins de stockage comparables (606 MB pour un million de véhicules), ACB-MAC présente également un coût computationnel plus faible pour assurer des transmissions efficaces. Ainsi, BCPPA apparaît davantage orienté vers la protection contre les attaques et l'anonymat, tandis que ACB-MAC offre de meilleures performances en termes de débit et de latence ; chaque protocole répond donc à des priorités distinctes : la sécurité pour BCPPA, et l'efficacité pour ACB-MAC.

3.3.2 Analyse des performances des protocoles en contexte de couverture limitée

Dans un environnement autoroutier, l'efficacité de protocoles d'authentification tels que BCPPA et ACB-MAC dépend fortement de la densité de l'infrastructure de communication. Cet environnement est caractérisé par des RSU déployées tout au long d'une autoroute de 5 km, chacune disposant d'une portée de communication de 600 m, ce qui correspond à une couverture de 1,200 m le long de l'autoroute. Les véhicules, quant à eux, possèdent une portée de communication de 300 m et se déplacent

à des vitesses allant de 7,5m/s à 40m/s, avec une vitesse moyenne de 23.75 m/s. Ces paramètres de portée et de vitesse sont identiques à ceux utilisés dans la solution BCPPA. De plus, les véhicules diffusent des messages d'authentification toutes les 100 ms (soit 10 messages par seconde), un intervalle également conservé dans BCPPA, et la durée totale de simulation est de 100 secondes.

Dans ce contexte, nous modélisons un segment d'autoroute compris entre deux RSU afin d'analyser le comportement du protocole BCPPA. L'objectif est d'évaluer la fiabilité du protocole à travers les taux de succès et d'échec des requêtes d'authentification, en tenant compte des limitations de couverture des RSU et des caractéristiques de communication des véhicules. Nous passons ainsi à une analyse détaillée des valeurs calculées, afin de déterminer dans quelle mesure une couverture limitée des RSU peut affecter les performances du protocole dans un scénario autoroutier réaliste.

La longueur couverte par une RSU est calculée comme suit :

$$L_{\text{coverage}} = 2 \times \text{RSU range} = 2 \times 600\,\text{m} = 1{,}200\,\text{m}$$

La fraction de l'autoroute couverte par une seule RSU est donc :

$$f_{\text{coverage}} = \frac{L_{\text{coverage}}}{L_{\text{total}}} = \frac{1{,}200\,\text{m}}{5{,}000\,\text{m}} = 0.24$$

Le nombre de véhicules présents dans la zone couverte est :

$$N_{\text{covered}} = N_{\text{vehicles}} \times f_{\text{coverage}} = 100 \times 0.24 = 24\,\text{véhicules}$$

Par conséquent, le nombre de véhicules hors zone couverte est :

$$N_{\text{outside}} = N_{\text{vehicles}} - N_{\text{covered}} = 76\,\text{véhicules}$$

La longueur de l'autoroute non couverte est :

$$L_{\text{outside}} = L_{\text{total}} - L_{\text{coverage}} = 3{,}800\,\text{m}$$

Le taux d'entrée des véhicules dans la zone couverte vaut :

$$\lambda_{\text{entry}} = \frac{N_{\text{outside}} \times v_{\text{avg}}}{L_{\text{outside}}} = \frac{76 \times 23.75}{3{,}800} \approx 0.475\,\text{véhicules/s}$$

Sur une durée de 100 secondes, le nombre total de véhicules entrant dans la zone couverte est :

$$N_{\text{entering}} = \lambda_{\text{entry}} \times T = 0.475 \times 100 = 47.5\,\text{véhicules}$$

Le temps de traversée de la zone couverte par un véhicule est :

$$t_{\text{covered}} = \frac{L_{\text{coverage}}}{v_{\text{avg}}} = \frac{1{,}200}{23.75} \approx 50.53\,\text{s}$$

Le nombre de messages envoyés par un véhicule dans la zone couverte est :

$M_{\text{vehicle, covered}}$ = fréquence des messages$\times t_{\text{covered}} = 10{\times}50.53 \approx 505\,\text{messages}$

Le nombre total de messages envoyés dans la zone couverte est :

$$M_{\text{total, covered}} = (N_{\text{covered}} + N_{\text{entering}}) \times M_{\text{vehicle, covered}} \approx 36{,}107$$

Pour les véhicules hors zone couverte, le temps de traversée dépasse la durée de simulation ; nous considérons donc 100 secondes. Le nombre de messages envoyés par véhicule hors zone couverte est :

$$M_{\text{vehicle, outside}} = 10 \times 100 = 1{,}000 \,\text{messages}$$

Le nombre total de messages envoyés hors zone couverte est :

$$M_{\text{total, outside}} = N_{\text{outside}} \times M_{\text{vehicle, outside}} = 76 \times 1{,}000 = 76{,}000 \,\text{messages}$$

Le nombre total de requêtes d'authentification correspond à la somme des messages issus des deux zones :

$$D_{\text{total}} = M_{\text{total, covered}} + M_{\text{total, outside}} = 112{,}107 \,\text{requêtes}$$

Le nombre de requêtes d'authentification réussies correspond aux messages émis dans la zone couverte :

$$D_{\text{successful}} = M_{\text{total, covered}} = 36{,}107 \,\text{requêtes}$$

Ainsi, le taux de succès d'authentification est :

$$T_{\text{success}} = \frac{D_{\text{successful}}}{D_{\text{total}}} \times 100\% \approx 32.22\%$$

Par conséquent, le taux d'échec d'authentification est :

$$T_{\text{failure}} = 100\% - T_{\text{success}} \approx 67.78\%$$

Les mêmes métriques sont ensuite évaluées pour ACB-MAC. Les véhicules y sont organisés en clusters afin d'optimiser la gestion des communications. Chaque cluster est dirigé par un CH, lequel joue un rôle central dans l'authentification et la coordination des communications entre les membres du cluster. Dans un contexte d'autoroute avec une couverture RSU limitée, l'efficacité du protocole ACB-MAC dépend fortement de la position du CH par rapport à la zone couverte par la RSU. En effet, l'authentification des véhicules est directement influencée par cette position, dans la mesure où le CH agit comme intermédiaire entre les véhicules du cluster et l'infrastructure réseau.

Le nombre de segments entre véhicules est calculé comme suit. Pour déterminer ce nombre, nous utilisons :

$$n_{\text{segments}} = \frac{L_{\text{cluster}}}{d_{\text{average}}}$$

où L_{cluster} représente la longueur maximale du cluster, égale à la portée de communication des véhicules :

$$L_{\text{cluster}} = R_{\text{com}} = 300 \,\text{m}$$

et $d_{\text{average}} = 50\,\text{m}$ représente la distance moyenne entre véhicules. On obtient donc :

$$n_{\text{segments}} = \frac{300}{50} = 6$$

Le nombre de véhicules par cluster vaut :

$$N_{\text{cluster}} = n_{\text{segments}} + 1 = 7\,\text{véhicules}$$

Le nombre total de clusters est :

$$N_{\text{clusters}} = \frac{N_{\text{vehicles}}}{N_{\text{cluster}}} = \frac{100}{7} \approx 14.29$$

En arrondissant à l'entier supérieur :

$$N_{\text{clusters}} = 15\,\text{clusters}$$

La longueur couverte par une RSU reste identique :

$$L_{\text{coverage}} = 2 \times R_{\text{RSU}} = 1{,}200\,\text{m}$$

et la longueur totale de l'autoroute est :

$$L_{\text{total}} = 5{,}000\,\text{m}$$

D'où la fraction couverte :

$$f_{\text{coverage}} = \frac{1{,}200}{5{,}000} = 0.24$$

Le nombre de *cluster heads* (CH) situés dans la zone couverte est :

$$N_{\text{CH, covered}} = N_{\text{clusters}} \times f_{\text{coverage}} = 15 \times 0.24 = 3.6$$

En arrondissant à l'entier inférieur :

$$N_{\text{CH, covered}} = 3\,\text{CH}$$

Ainsi, le nombre de CH hors zone couverte est :

$$N_{\text{CH, outside}} = N_{\text{clusters}} - N_{\text{CH, covered}} = 12\,\text{CH}$$

Le pourcentage de clusters dont le CH est dans la zone couverte (donc authentifiés) est :

$$P_{\text{clusters, authenticated}} = \frac{N_{\text{CH, covered}}}{N_{\text{clusters}}} \times 100\% = \frac{3}{15} \times 100\% = 20\%$$

Par conséquent, le pourcentage de clusters dont le CH est hors zone couverte est :

$$P_{\text{clusters, non-authenticated}} = 80\%$$

Le nombre de véhicules appartenant à des clusters authentifiés est :

$$N_{\text{vehicles, authenticated}} = N_{\text{CH, covered}} \times N_{\text{cluster}} = 3 \times 7 = 21\,\text{véhicules}$$

Le nombre de véhicules appartenant à des clusters non authentifiés est :

$$N_{\text{vehicles, non-authenticated}} = N_{\text{vehicles}} - N_{\text{vehicles, authenticated}} = 79 \text{ véhicules}$$

Ainsi, le taux de succès d'authentification est :

$$T_{\text{success}} = \frac{N_{\text{vehicles, authenticated}}}{N_{\text{vehicles}}} \times 100\% = 21\%$$

Le taux d'échec d'authentification est donc :

$$T_{\text{failure}} = 100\% - T_{\text{success}} = 79\%$$

3.3.3 Discussion

Nous avons mené une analyse comparative des schémas d'authentification adaptés aux communications V2X, en mettant en évidence les protocoles les plus robustes en matière d'identification et d'anonymisation, deux propriétés essentielles pour un système d'audit. À travers cette étude, nous avons évalué différents mécanismes d'authentification selon des critères qualitatifs et quantitatifs. Cette analyse nous a permis d'identifier les solutions les plus pertinentes pour garantir l'intégrité, l'identification et l'anonymisation au sein des réseaux véhiculaires, tout en maintenant un niveau élevé de confidentialité. Toutefois, aucune de ces solutions ne permet d'assurer une authentification continue et efficace lorsque les véhicules basculent vers un mode de communication purement V2V, notamment en dehors de la zone de couverture de l'infrastructure.

Dans la suite de nos travaux, nous prévoyons de développer un schéma d'authentification hybride capable de fonctionner de manière optimale à la fois dans des environnements avec infrastructure et dans des environnements sans infrastructure. Une telle solution devra minimiser la dépendance vis-à-vis de l'infrastructure, tout en garantissant des mises à jour régulières des données d'authentification. Cela permettrait d'assurer un service continu et de renforcer la robustesse des systèmes d'audit dans des réseaux véhiculaires dynamiques, tout en répondant aux exigences de traçabilité et de non-répudiation propres aux environnements sans infrastructure.

3.4 Fiabilité de l'authentification dans les environnements sans infrastructure

Garantir une authentification sûre et fiable dans les réseaux véhiculaires est un enjeu majeur, en particulier dans des contextes où l'accès aux infrastructures telles que les réseaux 5G, les services Edge/Cloud ou les RSU est intermittent, voire totalement inexistant. Bien que de nombreux travaux se soient intéressés aux mécanismes d'authentification en présence d'une couverture par infrastructure, les problématiques liées aux environnements dépourvus d'infrastructure restent encore insuffisamment explorées.

Afin de combler cette lacune, nous proposons un modèle analytique permettant d'évaluer la probabilité de réussite de l'authentification entre des véhicules évoluant sans accès continu à l'infrastructure réseau.

3.4.1 Modèle analytique

Dans le scénario illustré à la figure 3.2, nous considérons un véhicule circulant initialement sur une autoroute située dans une zone couverte par l'infrastructure. Ce véhicule est connecté à l'infrastructure via des RSU, ce qui lui permet d'accéder à une base de données globale d'authentification contenant des certificats à jour délivrés par les autorités d'authentification, ainsi que les listes de révocation correspondantes.

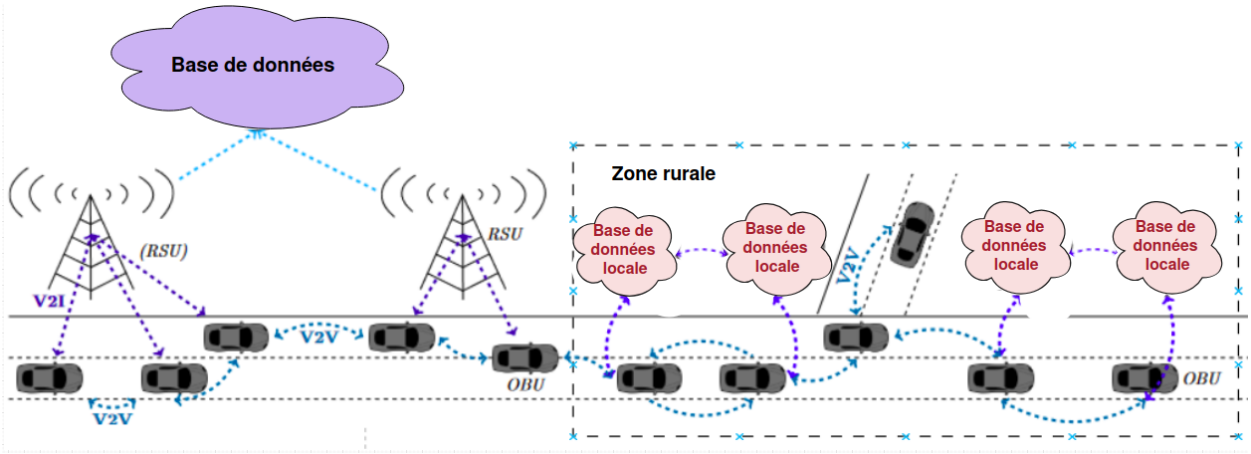

Figure 3.2 – Scénario d'authentification V2V lors de la transition d'une zone couverte par l'infrastructure vers une zone rurale non couverte.

Lorsque le véhicule quitte la zone de couverture et pénètre dans une zone rurale, il perd l'accès à cette infrastructure, y compris toute connectivité basée sur des gNB 5G, des RSU ou des services Edge/Cloud. Au moment de la déconnexion t_0, le véhicule conserve une copie locale complète des bases de données d'authentification disponibles juste avant la sortie de la zone couverte.

À partir de cet instant, le véhicule s'appuie exclusivement sur cette copie locale pour authentifier les autres véhicules rencontrés via des communications V2V. Avec le temps, ces bases de données deviennent de plus en plus obsolètes, ce qui affecte directement la fiabilité du processus d'authentification. L'objectif est donc d'évaluer la fiabilité de l'authentification dans les zones non couvertes.

Nous développons un modèle analytique permettant de calculer la probabilité qu'un véhicule puisse en authentifier un autre, en se basant sur des bases de données locales potentiellement obsolètes, à un instant donné t_i après la sortie de la zone de couverture. Cette probabilité est notée $P_{\text{auth}}(t_i)$. L'étude est menée dans un scénario simplifié d'autoroute, où les véhicules se déplacent le long d'une route rectiligne. Le modèle prend en compte la mobilité des véhicules, la probabilité de rencontre (modélisée par un processus de Poisson), ainsi que des facteurs clés tels que l'expiration des certificats, le taux de révocation et la fraîcheur des bases de données locales. Ces éléments sont représentés à l'aide de lois exponentielles afin de capturer leur comportement dépendant du temps dans un contexte de déconnexion.

La probabilité de réussite de l'authentification à l'instant t_i est donnée par :

$$P_{\text{auth}}(t_i) = P_r \cdot P_{\text{val}}(t_i)$$

avec :

— P_r : probabilité de rencontrer un véhicule,
— $P_{\text{val}}(t_i)$: probabilité qu'un certificat soit valide à l'instant t_i.

La probabilité de rencontre d'un véhicule suit un modèle de Poisson :

$$P_r(t_i) = \int_0^{t_i} \lambda_v v e^{-\lambda_v v t}\, dt = 1 - e^{-\lambda_v v t_i}$$

où :

— λ_v : densité de véhicules (véhicules/km),
— v : vitesse moyenne des véhicules (km/h),
— $\Delta t = t_i - t_0$: durée écoulée depuis la déconnexion.

Un certificat est considéré comme valide si :

1. le véhicule n'est pas révoqué ($1 - P_{\text{rev}}$) et les bases de données locales sont à jour,
2. ou si le véhicule est révoqué mais que cette révocation n'est pas connue ($P_{\text{rev}} \cdot P_{\text{unk}}$),
3. et si le certificat n'a pas expiré ($1 - P_{\text{exp}}$).

Ainsi :

$$P_{\text{val}}(t_i) = [(1 - P_{\text{rev}}) + P_{\text{rev}} \cdot P_{\text{unk}}] \cdot (1 - P_{\text{exp}})$$

La probabilité qu'un véhicule soit révoqué à l'instant t_i dépend du taux de révocation λ_R :

$$P_{\text{rev}}(t_i) = \int_0^{t_i} \lambda_R e^{-\lambda_R t}\, dt = 1 - e^{-\lambda_R t_i}$$

La probabilité qu'un certificat ait expiré dépend du temps écoulé depuis son émission ($t_i - t_{\text{emis}}$) et suit une loi exponentielle :

$$P_{\text{exp}}(t_i) = \int_0^{t_i} \lambda_{\text{exp}} e^{-\lambda_{\text{exp}}(t - t_{\text{emis}})}\, dt = 1 - e^{-\lambda_{\text{exp}} \cdot (t_i - t_{\text{emis}})}$$

La probabilité qu'un certificat soit révoqué sans que l'information ne soit connue est donnée par :

$$P_{\text{unk}}(t_i) = P_{\text{not_meeting}}(t_i) \cdot P_{\text{deconnection}}(t_i)$$

avec :

— $P_{\text{not_meeting}}(t_i)$: probabilité de ne pas rencontrer un véhicule disposant de bases de données à jour,
— $P_{\text{deconnection}}(t_i)$: probabilité que le véhicule soit resté hors ligne pendant une durée $t_i - t_{\text{update}}$.

$$\begin{aligned} P_{\text{not_meeting}}(t_i) &= \int_0^{t_i} \lambda v p_{\text{comm}} f \cdot e^{-\lambda v p_{\text{comm}} f (t - t_{\text{update}})}\, dt \\ &= e^{-\lambda v p_{\text{comm}} f (t_i - t_{\text{update}})} \end{aligned}$$

avec :

— λ : densité de véhicules (véhicules/km),

— v : vitesse moyenne des véhicules (km/h),
— p_{comm} : probabilité de communication réussie entre deux véhicules,
— f : fraction de véhicules disposant d'une base de données à jour,
— T_{obsolete} : temps au-delà duquel les données deviennent obsolètes,
— t_{update} : instant de la dernière mise à jour.

$$P_{\text{unk}}(t_i) = \begin{cases} e^{-\lambda v p_{\text{comm}} f (t_i - t_{\text{update}})}, & \text{si } t_i - t_{\text{update}} > T_{\text{obsolete}}, \\ 0, & \text{sinon.} \end{cases}$$

L'équation finale s'écrit alors :

$$P_{\text{auth}}(t_i) = (1 - e^{-\lambda_v v t_i}) \cdot [(1 - P_{\text{rev}}(t_i)) + P_{\text{rev}}(t_i)\, P_{\text{unk}}(t_i)] \cdot (1 - P_{\text{exp}}(t_i))$$

$$= (1 - e^{-\lambda_v v t_i}) \cdot \left(e^{-\lambda_R t_i} + (1 - e^{-\lambda_R t_i})\, P_{\text{unk}}(t_i)\right) \cdot e^{-\lambda_{\text{exp}}(t_i - t_{\text{emis}})}$$

En remplaçant $P_{\text{unk}}(t_i)$, on obtient :

$$P_{\text{auth}}(t_i) = \begin{cases} (1 - e^{-\lambda_v v t_i}) \cdot \left(e^{-\lambda_R t_i} + (1 - e^{-\lambda_R t_i})\, e^{-\lambda v p_{\text{comm}} f (t_i - t_{\text{update}})}\right) \cdot e^{-\lambda_{\text{exp}}(t_i - t_{\text{emis}})}, & \text{si } t_i - t_{\text{update}} > T_{\text{obsolete}} \\ (1 - e^{-\lambda_v v t_i}) \cdot e^{-\lambda_R t_i} \cdot e^{-\lambda_{\text{exp}}(t_i - t_{\text{emis}})}, & \text{sinon.} \end{cases}$$

Afin d'estimer cette probabilité de manière réaliste, nous nous sommes appuyés sur la littérature scientifique et sur les normes existantes afin d'identifier des valeurs typiques des principaux paramètres. Celles-ci incluent notamment la durée de vie des certificats, le délai au-delà duquel une base de données locale devient obsolète, la vitesse moyenne des véhicules, ainsi que les taux de révocation et de communication. Les valeurs retenues sont récapitulées dans le Tableau 1.

Nous définissons ensuite l'ensemble des paramètres utilisés pour le calcul des probabilités d'authentification. Toutes les valeurs sont issues de l'état de l'art et d'études empiriques récentes :

— Taux de révocation des certificats : $\lambda_R = 0.005$ par heure.
— Seuil d'obsolescence des données : $T_{\text{obsolete}} = 0.5$ heure.
— Densité de véhicules : $\lambda_v = 20$ véhicules/km.
— Vitesse moyenne des véhicules : $v = 100$ km/h.
— Durée de vie moyenne des certificats : $T_{\text{cert}} = \{5\,\text{min}, 24\,\text{h}, 168\,\text{h}\}$.
— Taux d'expiration des certificats : $\lambda_{\text{exp}} = \frac{1}{T_{\text{cert}}}$ par heure.
— Instant initial de mise à jour : $t_{\text{update}} = 0$.
— Hypothèse initiale d'absence de rencontre : $P_{\text{not_meeting}}(t_i) = 1$.

3.4.2 Résultats et discussion

Afin d'évaluer la fiabilité de l'authentification véhicule-à-véhicule dans des environnements dépourvus d'infrastructure, nous simulons le modèle analytique pour trois durées de vie de certificats différentes : 168 heures, 24 heures et 5 minutes. Cette dernière configuration reflète les contraintes imposées par les systèmes respectueux de la vie privée, dans lesquels des pseudonymes de courte durée sont fréquemment renouvelés afin de limiter le traçage des véhicules. De tels mécanismes nécessitent donc un renouvellement très fréquent des certificats.

[91]: Helsinki University Team. « Accountable De-anonymization in V2X Communication ». In : *Vehicular Communication Journal* (2023)

[92]: *C2C-CC (Car2Car Communication Consortium) Security Standards*. Car2Car Communication Consortium, 2019

[93]: A. Haidar. « Validation Platform for Secure V2X Communications ». In : *PhD Thesis, Politecnico di Torino* (2020)

[94]: J. Smith et A. Doe. « Post-quantum Impacts on V2X Certificates ». In : *IEEE Vehicular Communications* (2023)

[95]: *ETSI ITS-G5 - European ITS Communication Standards*. European Telecommunications Standards Institute, 2016

[96]: T. Wang et Y. Lee. « Survey on Certificate Revocation Schemes ». In : *IEEE Access* (2020)

[97]: M. A. Simplicio et C. B. Margi. « Revocation in Vehicular Public Key Infrastructures ». In : *Vehicular Networking Conference* (2021)

[98]: *IEEE 802.11p - Wireless Access in Vehicular Environments*. IEEE Standards Association, 2010

[99]: *ETSI TS 103 097 - Intelligent Transport Systems (ITS) ; Security ; Security header and certificate formats*. European Telecommunications Standards Institute (ETSI), 2016

Table 3.4 – Récapitulatif des principales valeurs de paramètres pour les communications V2X

Paramètres	**Valeurs typiques**	**Sources et justifications**
Durée de vie du certificat de l'AC racine	5–10 ans	[91] [92] [93],[94] Les ETSI10certificats racine sont rarement renouvelés afin de préserver la stabilité de la chaîne de confiance.
Certificats de courte durée	1 jour, 1 mois ou 1 certificat par message	[95] Une validité courte permet de renforcer la protection de la vie privée et de limiter l'impact en cas de compromission de clé.
Taux de révocation des certificats	0,1% à 1% par heure	[70] [4][96] [97] Le taux varie selon le scénario, et reste généralement faible dans des conditions d'exploitation normales.
Fréquence des messages BSM	Toutes les 100 ms	[98] [95] Messages utilisés pour les applications critiques de sécurité.
Messages d'événement ou d'annulation	1 message toutes les 1 à 5 secondes	[95] Émis lors d'événements spécifiques ; la fréquence dépend du contexte et du niveau d'urgence.
Fréquence de mise à jour des CRL	Toutes les 30 minutes à 1 heure	[89][99] Des mises à jour fréquentes permettent de refléter rapidement les changements d'état des certificats.

La Figure 3.3 illustre l'évolution de la probabilité d'authentification $P_{\text{auth}}(t)$ en fonction du temps écoulé depuis la perte de connectivité du véhicule avec l'infrastructure. L'axe des abscisses représente le temps, exprimé en heures, tandis que l'axe des ordonnées correspond à la probabilité de réussite de l'authentification, calculée uniquement à partir de la base de certificats locale, potentiellement obsolète.

Comme attendu, des durées de vie de certificats plus longues entraînent une décroissance plus lente de la fiabilité de l'authentification. Lorsque $T_{\text{cert}} = 168$ heures, la probabilité d'authentification reste supérieure à 0.65 même après 40 heures de déconnexion. En revanche, pour $T_{\text{cert}} = 24$ heures, la dégradation est nettement plus marquée, avec une chute de $P_{\text{auth}}(t)$ en dessous de 0.2 sur la même période, réduisant fortement les chances d'une authentification réussie entre pairs.

Le scénario le plus critique correspond à la durée de certificat la plus courte, $T_{\text{cert}} = 5$ minutes. Dans ce cas, la probabilité d'authentification chute brutalement, passant sous le seuil de 0.3 en moins d'une heure et tendant rapidement vers zéro. Cette décroissance rapide s'explique par le taux d'expiration élevé $\lambda_{\text{exp}} = 1/T_{\text{cert}}$, qui entraîne l'invalidation de la majorité des certificats stockés localement en un laps de temps très court. De telles conditions sont typiques des systèmes orientés anonymat, où les changements de pseudonymes sont fréquents et agressifs.

Ces résultats mettent en évidence un compromis fondamental entre respect de la vie privée et robustesse opérationnelle. Si les certificats de

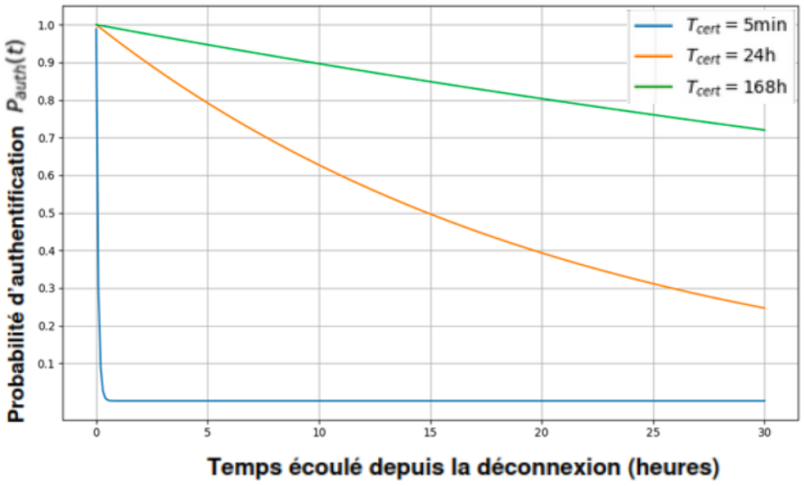

Figure 3.3 – Évolution de la probabilité d'authentification en fonction du temps selon la durée de vie des certificats.

courte durée renforcent l'anonymat et limitent la possibilité de corrélation à long terme, ils réduisent également la fenêtre temporelle durant laquelle une authentification efficace peut être assurée, en particulier dans des contextes déconnectés. Lorsque les mises à jour pair-à-pair sont rares, en raison d'une faible densité de véhicules ou de communications peu fiables, le processus d'authentification se dégrade rapidement. Cela souligne la nécessité de concilier les mécanismes orientés protection de la vie privée, tels que la rotation fréquente des pseudonymes, avec des exigences de résilience opérationnelle. Une solution potentielle, présentée dans la partie suivante, consiste à permettre une synchronisation opportuniste des données d'authentification entre véhicules. Un tel protocole distribué pourrait prolonger significativement la validité pratique des certificats de courte durée en diffusant des informations d'authentification récentes, même en l'absence d'infrastructure.

3.5 Synchronisation pair-à-pair des données d'authentification hors infrastructure

Dans les zones dépourvues d'infrastructure, l'authentification V2V repose uniquement sur des bases de données locales, dont la fraîcheur se dégrade inévitablement avec le temps. Cette obsolescence réduit progressivement la fiabilité des décisions d'authentification et peut compromettre la continuité des services de sécurité. Pour répondre à cette limitation, cette section introduit une approche de synchronisation pair-à-pair permettant la diffusion opportuniste d'informations d'authentification entre véhicules. Nous présentons le protocole proposé, puis nous analysons son impact sur la probabilité de réussite de l'authentification dans différents scénarios autoroutiers. Enfin, une évaluation quantitative met en évidence les gains obtenus et les conditions pratiques de déploiement.

3.5.1 Protocole proposé

Dans les environnements véhiculaires déconnectés, la réussite de l'authentification V2V dépend fortement de la fraîcheur de la base de données locale d'authentification de chaque véhicule. Afin de contrer la dégradation naturelle du niveau de confiance au fil du temps, nous proposons un protocole de mise à jour décentralisé permettant aux véhicules de

rafraîchir opportunément leurs bases de données lors de rencontres avec d'autres véhicules.

Le protocole distingue deux catégories de véhicules :

— **Véhicules de confiance** : cette catégorie inclut les services d'urgence (par exemple la police, les ambulances ou les véhicules de lutte contre l'incendie), les véhicules de flotte provenant de constructeurs certifiés, ainsi que toute entité officiellement reconnue comme fiable.
— **Véhicules standards** : l'ensemble des autres véhicules ne disposant pas d'un statut de confiance formel. Ils peuvent participer à l'échange de données, mais sont soumis à des conditions plus strictes pour la mise à jour de leurs bases d'authentification.

Cette distinction est essentielle afin de hiérarchiser les niveaux de confiance et d'éviter la propagation de données obsolètes ou malveillantes.

Comportement des véhicules de confiance (TV)

Comme illustré à la Figure 3.4, les véhicules de confiance commencent à vérifier la fraîcheur de leur base de données dès qu'ils quittent la zone couverte par l'infrastructure. Ils ne peuvent se mettre à jour qu'à partir de l'infrastructure ou d'un autre véhicule de confiance. Tant que la base de données reste valide, ils fonctionnent normalement et diffusent périodiquement leur présence, permettant ainsi aux véhicules standards situés à proximité de se mettre à jour à partir d'eux. En revanche, si la base de données devient obsolète, ils tentent d'obtenir une mise à jour via un pair de confiance.

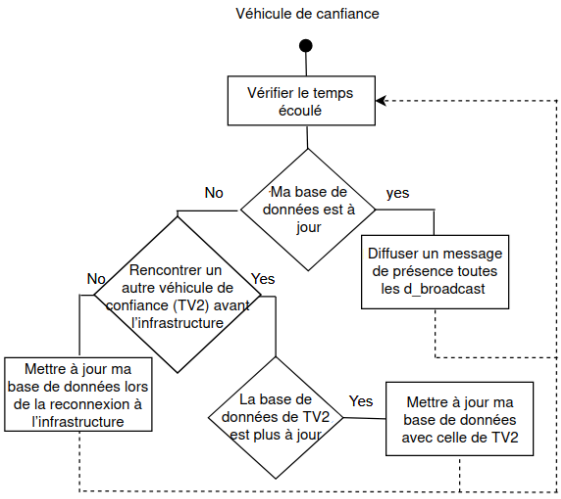

Figure 3.4 – Comportement d'un véhicule de confiance dans un environnement dépourvu d'infrastructure.

Comportement des véhicules standards

Dès qu'un véhicule standard quitte l'infrastructure, il commence à surveiller l'âge de sa base de données locale d'authentification. Lorsque celle-ci devient obsolète, c'est-à-dire qu'elle dépasse le seuil d'obsolescence défini, le véhicule adopte un mode de fonctionnement prudent : il limite les échanges de données sensibles et diffuse des requêtes de mise à jour à destination des véhicules voisins.

Lors des rencontres avec d'autres véhicules, le processus de mise à jour suit les règles suivantes :

- Si un véhicule de confiance répond, la mise à jour est effectuée immédiatement à partir de sa base de données.
- Si le véhicule rencontré est un autre véhicule standard, la mise à jour n'est acceptée que si la base de données du pair est plus récente et qu'elle reste dans la fenêtre d'obsolescence acceptable.
- En présence de plusieurs candidats à la mise à jour :
  - un véhicule de confiance est toujours prioritaire ;
  - à défaut, le véhicule standard sélectionne la version valide la plus récente de la base de données disponible.

Ce mécanisme est itératif et permet au véhicule standard d'améliorer progressivement la fraîcheur de ses données d'authentification au fur et à mesure de ses déplacements hors de la zone de couverture infrastructurelle.

3.5.2 Évaluation du protocole proposé

Afin d'évaluer l'efficacité du protocole proposé, nous avons étudié le cas le plus favorable pour le renouvellement de la fraîcheur des bases de données d'authentification, dans le but d'observer l'amélioration maximale possible de la probabilité d'authentification.

Nous considérons un scénario autoroutier dans lequel un véhicule V_1, après avoir téléchargé une base de données d'authentification récente depuis l'infrastructure, entre dans un segment dépourvu de couverture tout en roulant à une vitesse modérée de 100 km/h. L'objectif est d'identifier la rencontre la plus favorable permettant à V_1 de réinitialiser de manière opportuniste son paramètre de fraîcheur d'authentification (t_{update}).

Ce scénario est illustré à la Figure 3.5, qui montre le véhicule V_1 traversant un segment d'autoroute non couvert et mettant à jour sa base de données d'authentification par interaction avec d'autres véhicules, en fonction de leurs positions respectives.

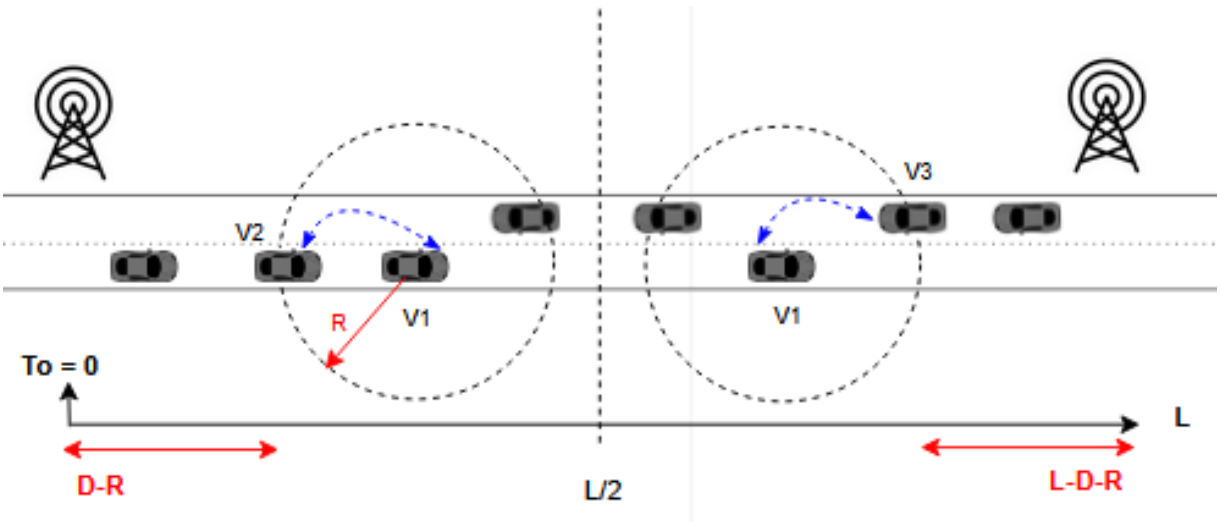

Figure 3.5 – Opportunités stratégiques de mise à jour en fonction de la position et du sens de circulation des véhicules.

Deux cas optimaux sont considérés :

— Si V_1 se situe dans la première moitié du segment non couvert, le cas le plus favorable correspond à la rencontre avec un véhicule plus rapide V_2, circulant dans le même sens à la vitesse maximale autoroutière de 130 km/h, situé à portée de communication de V_1 et aussi proche que possible de l'infrastructure située en amont.
— Si V_1 se trouve dans la seconde moitié du segment, le scénario le plus favorable se produit lorsqu'un véhicule V_3 arrive en sens inverse, également à 130 km/h, et ayant quitté récemment la zone couverte par l'infrastructure.

Dans les deux situations, le véhicule rencontré est supposé disposer d'une base de données plus récente. La valeur de t_{update} est alors ajustée dynamiquement en fonction du temps estimé écoulé depuis le dernier contact du pair avec l'infrastructure, calculé à partir de la position courante D de V_1 sur l'autoroute et de la portée de communication R.

La probabilité d'authentification améliorée s'exprime alors comme suit :

$$P_{\text{auth-improved}}(t_i) = P_{\text{auth}}(t_x)$$
$$\text{avec} \quad t_x = \begin{cases} \frac{D-R}{v_x}, & \text{si } D < \frac{L}{2} \\ \frac{L-D-R}{v_x}, & \text{si } D > \frac{L}{2} \end{cases}$$

Afin de quantifier les bénéfices du protocole proposé, nous évaluons son impact sur la probabilité d'authentification dans deux configurations autoroutières réalistes : $L = 600$ km et $L = 100$ km. Dans les deux scénarios, la route est délimitée à chaque extrémité par des RSU, et chaque véhicule reçoit initialement une base de données d'authentification complète avant de quitter la zone de couverture. Le véhicule observé se déplace à une vitesse constante de $v_{\text{node}} = 100$ km/h, tandis que les véhicules rencontrés circulent à $v_X = 130$ km/h. La portée de communication est fixée à $R = 0.5$ km, et deux durées de vie de certificats sont considérées : $T_{\text{cert}} = 168$ h et $T_{\text{cert}} = 24$ h.

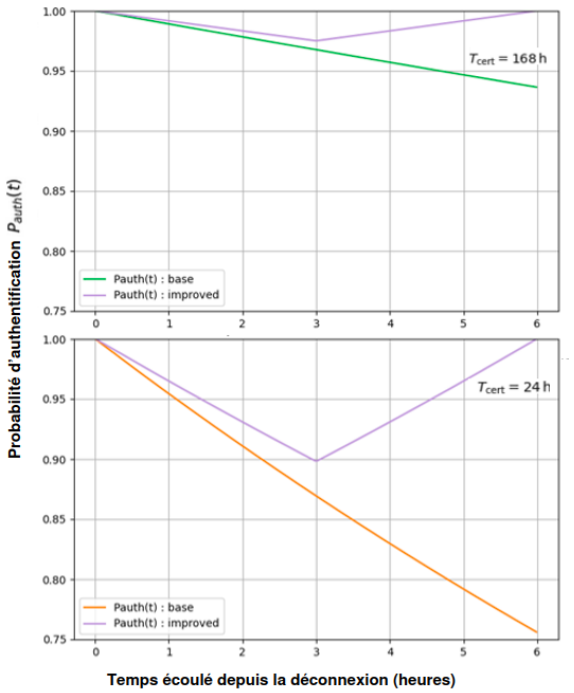

Figure 3.6 – Amélioration de P_{auth} sur un segment autoroutier de longueur $L = 600$ km.

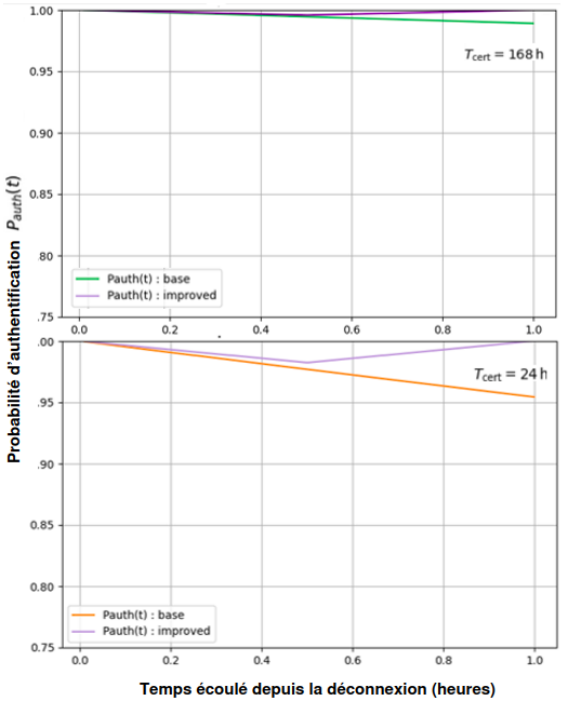

Figure 3.7 – Amélioration de P_{auth} sur un segment autoroutier de longueur L = 100 km.

Dans chaque cas, nous comparons l'évolution de la probabilité d'authentification au cours du temps pour :

- le cas de base, dans lequel la base de données reste statique durant tout le trajet ;
- le cas amélioré, où des mises à jour opportunistes sont permises via des rencontres avec des pairs disposant de bases plus récentes.

Les Figures 3.6 et 3.7 illustrent l'amélioration de la probabilité d'authentification à chaque instant $t_x > 0$ après le départ du véhicule de la zone couverte. Sur l'ensemble du segment de longueur L compris entre deux RSU, la courbe améliorée met en évidence l'effet des mises à jour intermédiaires, qui rafraîchissent la base de données et contribuent à maintenir un taux élevé de réussite de l'authentification.

- Sur un tronçon autoroutier long de 600 km, nous observons une amélioration significative de l'authentification lorsque V_1 est autorisé à mettre à jour sa base de données au cours des rencontres. Cet effet est particulièrement marqué lorsque la durée de vie des certificats est courte, car les mises à jour permettent de compenser la dégradation rapide du niveau de confiance.
- Sur un tronçon plus court de 100 km, les opportunités de mise à jour sont naturellement plus fréquentes en raison d'une densité de véhicules plus élevée à proximité des zones couvertes. L'écart entre P_{auth} et $P_{\text{auth-improved}}$ est alors plus faible, mais reste néanmoins non négligeable, en particulier lorsque la période de validité des certificats est réduite.

Ce modèle d'authentification met en évidence plusieurs implications pratiques pour le déploiement. Il améliore significativement la fiabilité de l'authentification en dehors des zones couvertes par l'infrastructure en permettant des mises à jour opportunistes des bases de données locales. Toutefois, son efficacité dépend de la présence de véhicules à proximité, en particulier de véhicules de confiance, une condition qui peut ne pas être garantie dans des environnements à faible densité de trafic.

Conclusion

L'étude comparative, à la fois qualitative et quantitative, des protocoles d'authentification issus de l'état de l'art a permis d'identifier leurs forces et leurs limites face aux exigences spécifiques des communications V2V en contexte de couverture limitée. Cette analyse a révélé que si certaines solutions offrent des garanties satisfaisantes en matière de confidentialité ou d'efficacité computationnelle, leur dépendance à l'infrastructure ou leur gestion des révocations limite leur aptitude à soutenir un audit fiable en mode déconnecté.

Afin de quantifier ces limitations, nous avons introduit un modèle analytique permettant d'évaluer la probabilité de succès de l'authentification en fonction de paramètres clés tels que la durée de vie des certificats, le taux de révocation et la fraîcheur des bases de données. Les résultats obtenus mettent en évidence une dégradation progressive de la fiabilité de l'authentification lorsque les véhicules s'appuient sur des données obsolètes, soulignant ainsi la nécessité de mécanismes complémentaires capables de pallier l'absence d'infrastructure.

Dans cette perspective, un mécanisme de synchronisation opportuniste pair-à-pair des données d'authentification a été étudié afin d'améliorer la cohérence des informations de sécurité échangées entre véhicules lors de leurs rencontres. Cette approche permet d'augmenter la probabilité d'authentification réussie dans les environnements sans infrastructure et constitue une étape essentielle vers la mise en œuvre de communications V2V sécurisées et auditables en mode déconnecté.

Un système d'audit basé sur la blockchain pour des communications V2X sécurisées et traçables

4

4.1 Audit des communications V2X : objectifs, exigences et contraintes 59
4.1.1 Objectifs de l'audit dans les communications V2X 59
4.1.2 Exigences fonctionnelles et de sécurité d'un système d'audit 60
4.1.3 Solutions d'audit traditionnelles 61
4.2 Une blockchain pour l'audit des communications V2X 63
4.2.1 Application de la blockchain à l'audit 63
4.2.2 Vue d'ensemble des scénarios véhiculaires . . 64
4.2.3 Opérations d'audit basées sur la blockchain 65
4.3 Évaluation des performances 66
4.3.1 Contexte de simulation . 67
4.3.2 Résultats de simulation . 68

Introduction

Dans cette section, nous présentons un système d'audit des communications V2X fondé sur la technologie blockchain, visant à garantir la sécurité, la traçabilité et la vérifiabilité des échanges entre véhicules. Nous décrivons tout d'abord le processus d'audit permettant d'identifier, d'authentifier et de vérifier l'intégrité des messages V2X dans un contexte potentiellement malveillant. Nous introduisons ensuite une architecture décentralisée reposant sur des blockchains locales et globales, adaptée aux environnements véhiculaires dynamiques et aux scénarios sans infrastructure. Enfin, nous évaluons les performances de la solution proposée à travers des simulations contrôlées, en analysant l'impact des stratégies de minage sur la latence, le débit et le taux de confirmation des messages.

4.1 Audit des communications V2X : objectifs, exigences et contraintes

La conception d'un système d'audit pour les communications V2X ne peut se réduire à la simple mise en place d'un mécanisme d'enregistrement des événements. Elle implique une réflexion préalable et structurée sur les finalités poursuivies, les propriétés que le système doit garantir et les contraintes inhérentes aux environnements dans lesquels il sera déployé. Cette section pose ce cadre conceptuel, en définissant les objectifs opérationnels de l'audit dans le contexte V2X, les exigences fonctionnelles et de sécurité auxquelles toute solution doit répondre, et les limitations des approches traditionnelles qui motivent le recours à une architecture décentralisée basée sur la blockchain.

4.1.1 Objectifs de l'audit dans les communications V2X

L'audit des communications V2X poursuit un ensemble d'objectifs complémentaires, structurés autour de quatre axes fondamentaux.

Le premier objectif est **la traçabilité des communications**. Tout message échangé au sein du réseau véhiculaire doit pouvoir être retrouvé, daté et associé à son émetteur de manière fiable, y compris a posteriori. Cette traçabilité est indispensable pour reconstituer la séquence exacte des événements ayant précédé un incident, qu'il s'agisse d'un accident de la route, d'une attaque par injection de faux messages ou d'un comportement anormal détecté a posteriori. Comme illustré dans le scénario d'investigation, la capacité à remonter un message suspect jusqu'à son émetteur, en passant par la vérification de son intégrité et de son horodatage, constitue le socle opérationnel de tout processus d'audit exploitable.

Le deuxième objectif est **la responsabilisation des entités communicantes**. Un système d'audit efficace doit être en mesure d'établir, de

manière certaine et juridiquement recevable, que telle entité a bien émis tel message à tel instant et à tel endroit. Cette exigence implique non seulement l'enregistrement des messages, mais également la conservation des preuves cryptographiques permettant de lier chaque message à un émetteur identifiable au moins par les autorités compétentes sans compromettre l'anonymat des usagers légitimes dans les conditions normales d'utilisation. L'équilibre entre responsabilisation et préservation de la vie privée constitue à cet égard l'une des tensions fondamentales de la conception d'un système d'audit V2X.

Le troisième objectif est la **non-répudiation**. Aucune entité ayant émis un message ne doit pouvoir nier après coup en être l'auteur, dès lors que ce message a été enregistré dans le système d'audit. Cette propriété est essentielle dans les contextes d'investigation judiciaire ou de résolution de litiges, où la valeur probante des traces collectées dépend directement de l'impossibilité pour l'émetteur de contester leur authenticité.

Le quatrième objectif est **le support à la détection et à l'investigation des comportements malveillants**. L'audit doit permettre non seulement de détecter des anomalies en cours de fonctionnement, mais également d'analyser a posteriori les causes et la chronologie d'un incident. Cela suppose que les traces enregistrées soient suffisamment riches en contexte identifiants, horodatages, contenus et localisations pour permettre une reconstruction fidèle des événements, et suffisamment protégées pour ne pas avoir pu être altérées entre le moment de leur production et celui de leur consultation. À cet égard, la présence d'une même trace de message dans les enregistrements de plusieurs véhicules s'étant trouvés simultanément au même endroit constitue un élément concordant de premier ordre : chaque véhicule agit en quelque sorte comme témoin indépendant, renforçant la confiance dans l'authenticité des traces collectées et réduisant considérablement la possibilité de les contester ou de les falsifier.

4.1.2 Exigences fonctionnelles et de sécurité d'un système d'audit

Pour répondre à ces objectifs, un système d'audit des communications V2X doit satisfaire un ensemble d'exigences à la fois fonctionnelles et sécuritaires, dont la rigueur conditionne directement la valeur opérationnelle et juridique des traces produites.

Sur le plan fonctionnel

Le système doit être capable d'**enregistrer** de manière sélective les événements pertinents pour l'audit comme les messages d'authentification, les signalements d'incidents et les communications critiques de sécurité, sans chercher à consigner l'intégralité du trafic, dont le volume serait prohibitif comme établi en section 2.3.2. Il doit garantir **la disponibilité** des traces enregistrées, c'est-à-dire leur accessibilité en cas de besoin d'investigation, y compris dans des environnements où la connectivité est intermittente. Il doit enfin assurer **la vérifiabilité** des traces, en permettant à toute partie autorisée de contrôler l'authenticité et l'intégrité d'un enregistrement sans dépendre d'une autorité centrale de certification disponible en temps réel.

Sur le plan de la sécurité

Quatre propriétés sont indispensables.

1. **Intégrité des traces :** garantit qu'aucun enregistrement ne peut être modifié ou supprimé après sa création, que ce soit par un attaquant externe ou par un participant malveillant du réseau.
2. **Confidentialité conditionnelle :** assure que l'identité réelle des entités communicantes est protégée dans des conditions normales d'utilisation, mais peut être révélée par les autorités compétentes dans des circonstances justifiées, conformément au principe d'anonymat conditionnel défini par le standard ETSI TS 102 941.
3. **Résistance aux attaques Sybil :** empêche qu'une entité malveillante crée de multiples identités afin de polluer le registre d'audit avec de faux enregistrements.
4. **Résilience du système :** garantit le fonctionnement continu du système en l'absence d'infrastructure fixe, condition nécessaire pour les scénarios V2V sans connectivité permanente.

À ces exigences générales s'ajoutent des contraintes spécifiques aux environnements véhiculaires. **La faible latence** d'enregistrement est indispensable pour que les messages soient consignés dans des délais compatibles avec la dynamique des communications V2X. **La scalabilité du système** doit lui permettre d'absorber les variations importantes de densité vehiculaire sans dégradation des performances. Enfin, l'indépendance vis-à-vis de l'infrastructure constitue l'exigence la plus structurante de notre contexte : le système doit fonctionner de manière autonome même lorsque les véhicules ne disposent d'aucune connectivité réseau.

4.1.3 Solutions d'audit traditionnelles

Les approches traditionnelles d'audit dans les réseaux V2X reposent sur trois grands mécanismes :

Audit PKI centralisé : Dans les systèmes V2X conformes aux standards ETSI ITS et IEEE 1609.2, les Autorités de Certification (CA), notamment, l'Enrolment Authority (EA) et l'Authorization Authority (AA), émettent des certificats pseudonymes à court terme signés par ECDSA. L'audit s'effectue à deux niveaux : une validation a priori lors de chaque réception de message (BSM/CAM), et une traçabilité a posteriori permettant, sous conditions légales, de lever l'anonymat afin de relier un pseudonyme à l'identité réelle d'un véhicule [4].

La journalisation des événements de sécurité : Les déploiements V2X s'appuient sur des journaux centralisés collectés au niveau des infrastructures V2I (RSU, TMC) et des serveurs cloud pour enregistrer les événements de sécurité : messages rejetés, tentatives d'authentification échouées, alertes d'anomalies et mises à jour des Liste de révocation des certificats (CRL). Ces journaux constituent la principale source d'information pour l'analyse post-incident des communications véhiculaires.

La vérification forensique post-incident : Cette approche désigne l'analyse des données capturées par les RSU ou remontées vers le cloud afin de reconstituer la séquence des événements ayant précédé un accident ou une anomalie. Elle s'appuie principalement sur les messages BSM [100] et CAM [101], qui encapsulent la position, la vitesse et l'état cinématique du véhicule émetteur.

[100]: SAE International. *V2X Communications Message Set Dictionary (DSRC Message Set Dictionary)*. SAE International, 2020

[101]: ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2 : Specification of Cooperative Awareness Basic Service (CAM)*. European Telecommunications Standards Institute, 2019

Table 4.1 – Exemple des approches traditionnelles d'audit dans les systèmes V2X

	Référence	Année	Contribution	Avantages	Limites
Audit PKI centralisé	[4]	2018	Architecture PKI hiérarchique (EA, AA, MA) pour l'émission et la révocation des certificats pseudonymes ECDSA en V2X via CRL.	Traçabilité a posteriori des messages V2X ; levée d'anonymat légale possible via la MA ; mécanismes normalisés (ETSI, SCMS) d'émission et de révocation des certificats pseudonymes ; interopérabilité entre constructeurs et opérateurs d'infrastructure.	Point de défaillance unique autour de la Misbehavior Authority (MA) ; délai de propagation des CRL aux véhicules laissant une fenêtre d'exploitation non auditée ; surcharge opérationnelle liée à la gestion massive de certificats pseudonymes à courte durée de vie ; révocation partielle difficile en l'absence de linkage authority (contexte ETSI).
	[97]	2021	Protocole de liaison et de révocation de pseudonymes VANET préservant la vie privée tout en permettant la traçabilité légale.		
	[65]	2022	Standard C-ITS européen définissant Root CA, EA et AA pour la gestion des certificats pseudonymes et les procédures de révocation.		
	[102]	2017	Compression probabiliste des listes de révocation (C2RL) afin d'optimiser leur distribution dans des environnements V2X à forte densité.		
	[103]	2024	Mécanisme de listes de révocation temporaires (PRL) permettant la révocation rapide des certificats V2X via auto-révocation.		
Journaux de sécurité	[104]	2020	Vérification de cohérence des messages BSM/CAM par les RSU avec journalisation locale des anomalies consolidée dans un cloud central.	Traçabilité structurée des événements de sécurité (messages rejetés, alertes d'anomalies) ; support aux enquêtes post-incident ; détection locale par RSU réduisant la dépendance au réseau central.	Stockage centralisé vulnérable à la compromission ; absence d'immuabilité native des entrées de log ; couverture incomplète hors zones équipées en RSU ; exploitation uniquement réactive, sans détection en temps réel.
	[105]	2017	Chaîne de journaux auditable assurant la traçabilité des opérations de désanonymisation entre autorités légales, autorité de résolution et véhicules.		
Vérification forensique	[106]	2023	Système IoV multi-sources combinant BSM (OBU/RSU) et apprentissage automatique pour reconstruire les trajectoires pré-collision à partir des communications V2X archivées.	Reconstruction précise des trajectoires et événements pré-collision à partir des messages BSM/CAM ; exploitation de sources multiples (OBU, RSU, cloud) ; contribution à l'analyse accidentologique et aux enquêtes légales.	Approche strictement réactive (post-incident uniquement) ; dépendance à la complétude des captures BSM/CAM ; authenticité des données archivées non garantie sans mécanisme cryptographique ; hétérogénéité des formats BSM vs CAM limitant l'interopérabilité forensique.
	[107]	2024	Intégration des messages CAM/BSM dans l'analyse accidentologique afin d'évaluer l'impact des avertissements V2X sur le temps de réaction pour la reconstruction forensique.		

Le tableau 4.1 met en évidence un ensemble de limitations structurelles communes aux trois catégories d'approches traditionnelles.

Sur le plan architectural, ces solutions reposent systématiquement sur des entités centralisées (CA, MA, serveurs de logs, cloud) qui constituent autant de points de défaillance uniques, incompatibles avec les exigences de résilience des réseaux véhiculaires. Sur le plan temporel, elles opèrent exclusivement en mode réactif, sans capacité de détection ou de prévention en temps réel. Enfin, aucune de ces approches ne garantit nativement l'immuabilité des traces d'audit produites, ce qui fragilise leur valeur probatoire dans un contexte légal ou forensique.

Ces limitations convergent vers un même constat : les architectures centralisées ne peuvent constituer le fondement d'un système d'audit fiable pour les communications V2X, en particulier dans les environnements sans infrastructure permanente. C'est précisément pour répondre à ces insuffisances que nous proposons, dans la section suivante, une architecture d'audit décentralisée et adaptative basée sur la blockchain,

spécifiquement conçue pour les contraintes des réseaux véhiculaires V2V.

4.2 Une blockchain pour l'audit des communications V2X

Ce travail explore le potentiel de la technologie blockchain pour l'enregistrement infalsifiable et la vérification unilatérale des traces de messages dans le contexte des communications V2X. En considérant chaque message V2X comme une transaction, la technologie blockchain présente ainsi les propriétés nécessaires à la mise en œuvre d'un système d'audit fiable pour les communications V2X, dans lequel le véhicule connecté, son propriétaire (opérateur de services ou éditeur d'applications), l'opérateur de télécommunications et des tiers (assureurs, autorités judiciaires) peuvent mener des investigations a posteriori à la suite d'un incident.

4.2.1 Application de la blockchain à l'audit

La figure 4.1 illustre un scénario d'attaque dans un réseau véhiculaire. Considérons un véhicule malveillant $V1$ diffusant des messages frauduleux dans son voisinage. Ces messages peuvent contenir des informations erronées sur les conditions de circulation [108], telles qu'un accident inexistant ou un danger fictif. Le véhicule $V2$ reçoit l'un de ces messages et prend une décision sur la base de cette information incorrecte. Supposons alors que la réaction de $V2$ à ce message provoque un accident avec un autre véhicule $V3$. La victime de cet accident, $V3$, dépose une plainte auprès des autorités judiciaires, lesquelles doivent alors mener un audit afin de déterminer et attribuer les responsabilités. Au cours de l'enquête, les questions suivantes doivent être traitées :

— Le message exploité par $V2$ a-t-il effectivement été émis par un véhicule, et ce dernier (en l'occurrence $V1$) peut-il être identifié ?
— Le véhicule identifié comme émetteur (ici $V1$) peut-il nier l'émission de ce message sans possibilité d'ambiguïté ?
— Le message a-t-il pu être modifié, de quelque manière que ce soit, par une entité autre que l'émetteur identifié (ici $V1$) ?

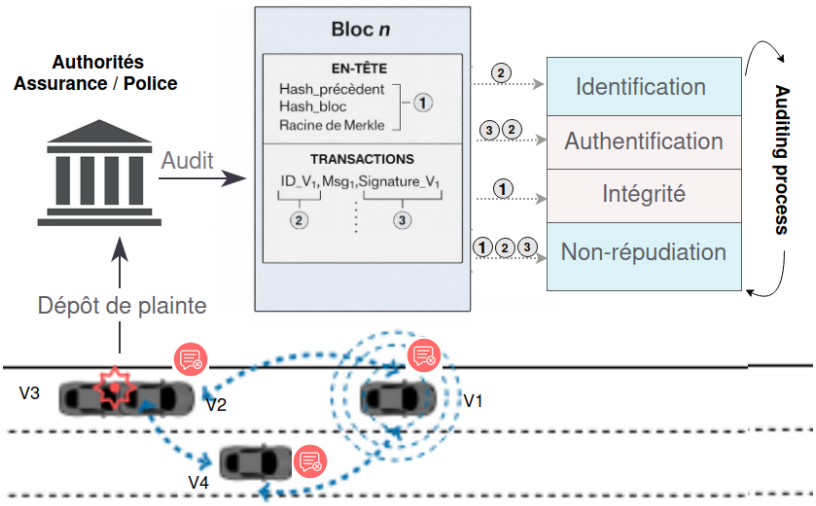

Figure 4.1 – Processus d'audit de la blockchain pour la traçabilité des messages malveillants.

[102]: Giovanni Rigazzi, Andrea Tassi, Robert J. Piechocki, Theo Tryfonas et Andrew Nix. « Optimized Certificate Revocation List Distribution for Secure V2X Communications ». In : *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017

[103]: Gianluca Scopelliti, Christoph Baumann, Fritz Alder, Eddy Truyen et Jan Tobias Mühlberg. « Efficient and timely revocation of v2x credentials ». In : *Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS'24)*. Internet Society. 2024

[104]: Joseph Kamel, Ines Ben Jemaa, Arnaud Kaiser, Loic Cantat et Pascal Urien. « Misbehavior Detection in C-ITS : A comparative approach of local detection mechanisms ». In : *2019 IEEE Vehicular Networking Conference (VNC)*. 2019

[105]: Masoud Naderpour, Tommi Meskanen, Andrew Paverd et Valtteri Niemi. « Auditable De-Anonymization in V2X Communication ». In : *Journal of ICT Standardization* 5.1 (2017)

[106]: Abin Oommen Philip et RA.K. Saravanaguru. « Multisource traffic incident reporting and evidence management in Internet of Vehicles using machine learning and blockchain ». In : *Engineering Applications of Artificial Intelligence* 117 (2023)

[107]: Maximilian Bauder, Daniel Paula, Claus Pfeilschifter, Franziska Petermeier, Tibor Kubjatko, Andreas Riener et Hans-Georg Schweiger. « Influences of Vehicle Communication on Human Driving Reactions : A Simulator Study on Reaction Times and Behavior for Forensic Accident Analysis ». In : *Sensors* 24.14 (2024)

[108]: Abdelwahab Boualouache et Thomas Engel. « A Survey on Machine learning-based misbehavior detection systems for 5G and beyond vehicular networks ». In : *IEEE Communications Surveys and Tutorials* 25.2 (2023)

Les enquêteurs peuvent alors engager un processus d'audit structuré selon les étapes suivantes :

1. **Identification du message suspect et évaluation de sa crédibilité :** les enquêteurs interrogent la copie locale de la blockchain détenue par $V2$ afin de retrouver le bloc contenant le message incriminé sous forme de transaction. À partir des données locales de la blockchain, ainsi que des horodatages et des informations de localisation associées à la transaction, ils peuvent également retrouver cette même transaction dans les copies locales de la blockchain d'autres véhicules présents au moment de l'accident (notamment $V1$ et $V4$). Cette redondance renforce la crédibilité du fait que le message incriminé a effectivement été émis par un véhicule, répondant ainsi à la première partie de la première question.
2. **Identification de l'émetteur du message :** les enquêteurs extraient ensuite l'identifiant du véhicule émetteur (ID_Vi) associé au message suspect. Cette étape permet de répondre à la seconde partie de la première question, dans la mesure où tous les participants à la blockchain sont identifiés (ici $V1$).
3. **Authentification de l'émetteur du message :** la signature numérique ($Signature_Vi$) du message suspect, stockée dans la transaction, est vérifiée à l'aide de la clé publique de $V1$. La validité de cette signature garantit que le message a bien été créé et signé par $V1$, et non par un attaquant usurpant son identité. Cette vérification assure à la fois l'authentification de l'émetteur du message et la non-répudiation de son émission, répondant ainsi à la deuxième question.
4. **Vérification de l'intégrité du message :** les enquêteurs comparent le condensat cryptographique du message avec celui de la transaction correspondante stockée dans le $Merkle_root$ du bloc [109]. Ils vérifient également le hachage du bloc ($Hash_block$) ainsi que celui du bloc précédent ($Hash_previous$) afin de s'assurer que ni le message ni le bloc n'ont été altérés. Cette étape garantit l'intégrité de l'ensemble des données, répondant ainsi à la troisième question.
5. **Établissement des responsabilités :** en combinant les enregistrements des transactions de la blockchain (preuve de l'existence du message), l'identifiant ID_Vi (identification de l'émetteur), la signature $Signature_Vi$ (authentification de l'émetteur et non-répudiation), ainsi que les valeurs de hachage vérifiées (intégrité du message), les enquêteurs disposent de preuves irréfutables et vérifiables. Les conséquences juridiques qui en découlent dépassent toutefois le cadre de ce travail.

[109]: Marcos A. Simplicio, Eduardo Lopes Cominetti, Harsh Kupwade Patil, Jefferson E. Ricardini, Leonardo T. D. Ferraz et Marcos Vinicius M. Silva. « Privacy-Preserving Certificate Linkage/-Revocation in VANETs Without Linkage Authorities ». In : *IEEE Transactions on Intelligent Transportation Systems* 22.6 (2021)

Cette description des étapes logiques du processus d'audit consécutif à la diffusion d'un message V2X malveillant facilite désormais la présentation de leur mise en œuvre dans un environnement véhiculaire dynamique, à travers notre proposition d'une architecture blockchain décentralisée dédiée à l'audit des communications V2X.

4.2.2 Vue d'ensemble des scénarios véhiculaires

L'architecture proposée, présentée à la figure 4.2, constitue le cadre opérationnel permettant la mise en œuvre effective du processus d'audit illustré à la figure 4.1. À cette fin, nous introduisons les deux définitions suivantes :

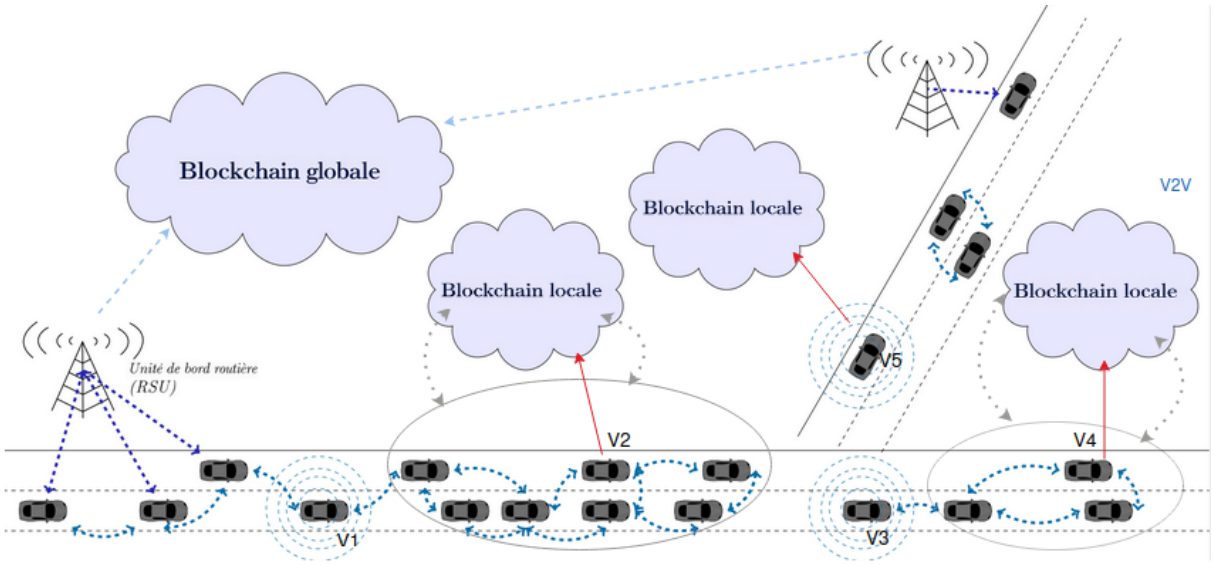

Figure 4.2 – Vue globale d'un système d'audit basé sur la blockchain pour les communications V2X sans infrastructure.

— **Blockchain locale** : une blockchain de courte durée, créée et maintenue de manière collaborative par un groupe de véhicules connectés via des communications V2V. Cette chaîne est chargée d'enregistrer, sous forme de transactions, l'ensemble des messages V2X échangés entre les membres du groupe, ainsi que de miner les blocs correspondants. Elle est archivée dès lors que les véhicules participants ne peuvent plus être considérés comme appartenant au même groupe.
— **Blockchain globale** : une blockchain permanente, généralement gérée par une autorité de confiance (Trusted Authority, TA), qui construit des blocs à partir de l'ensemble des messages V2X échangés au sein de la zone couverte par l'infrastructure, sous forme de transactions, et qui fusionne toutes les blockchains locales archivées reçues des véhicules lors de leur reconnexion à l'infrastructure. Cette approche garantit l'auditabilité à long terme tout en assurant la scalabilité du système et en réduisant la charge de stockage.

Cette approche permet à des groupes de véhicules de former dynamiquement des blockchains locales afin de gérer des événements auditables se produisant dans leur domaine spatio-temporel local. Ces blockchains locales agissent comme des journaux distribués stockant les informations d'identité, de signature et d'intégrité associées aux messages échangés ainsi qu'à leurs émetteurs, même en l'absence totale d'infrastructure. Lorsque les véhicules retrouvent une couverture d'infrastructure, ces enregistrements sont ancrés dans une blockchain globale, permettant ainsi une auditabilité centralisée complète par les autorités de confiance. Le mécanisme de fusion des blockchains locales dans la blockchain globale dépasse le cadre de ce travail.

4.2.3 Opérations d'audit basées sur la blockchain

Nous supposons qu'un système d'authentification est déjà déployé et accessible dans les zones couvertes par l'infrastructure, et que les informations d'authentification obtenues permettent aux véhicules de s'authentifier mutuellement dans les zones dépourvues d'infrastricture

et de garantir une participation sécurisée à la blockchain locale pour une durée déterminée, comme proposé dans [110]. Le protocole s'articule autour de quatre phases principales, chacune étant conçue pour assurer la continuité des procédures d'audit face à la dynamique des réseaux véhiculaires :

[110]: Marwa Slimene, Nathalie Mitton, Patrick Sondi et Ahmed Meddahi. « An enhanced authentication solution for infrastructureless vehicle environments ». In : *2025 21th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. Marrakech, Morocco, 2025

1. **Initialisation de la blockchain locale :** lorsqu'un véhicule quitte la zone de couverture de l'infrastructure, il commence par écouter les messages diffusés par les pairs à proximité afin de détecter l'existence d'une blockchain locale active. Si aucune blockchain locale n'est détectée dans sa portée V2V, le véhicule initie unilatéralement une nouvelle blockchain locale. Il génère alors un bloc de genèse contenant son identifiant pseudonymisé, l'horodatage courant et sa signature numérique. Le véhicule diffuse ensuite un message d'initialisation de blockchain locale à destination de ses voisins afin d'annoncer la création de cette nouvelle chaîne. Les véhicules à proximité qui reçoivent ce message entrent dans un état de synchronisation et peuvent choisir de rejoindre la blockchain locale nouvellement formée. Comme illustré à la figure 4.2, les véhicules $V2$ et $V4$ peuvent agir comme initiateurs et attirer dynamiquement des participants proches. À l'inverse, le véhicule $V5$ peut initier une blockchain locale sans parvenir immédiatement à recruter des participants.
2. **Adhésion d'un véhicule à un groupe :** lorsqu'un véhicule n'appartenant à aucun groupe détecte une blockchain locale active dans sa portée de communication V2V, généralement via un message de signalisation, il rejoint cette dernière. Ce processus implique le téléchargement d'une copie de la blockchain locale depuis l'un des véhicules participants. Une fois synchronisé, le véhicule commence à participer activement à la validation des transactions et au minage des blocs, contribuant ainsi à la gestion décentralisée de la blockchain. À la figure 4.2, le véhicule $V1$ s'approche du groupe géré par le véhicule $V2$. Lorsque $V1$ entre dans la portée V2V de $V2$, il détecte et rejoint la blockchain locale existante.
3. **Départ d'un véhicule d'un groupe :** la mobilité des véhicules induit des changements fréquents de topologie, nécessitant des mécanismes robustes pour gérer les départs et les transitions entre groupes. Lorsqu'un véhicule perd la connectivité avec les autres pairs de sa blockchain locale, il archive cette dernière jusqu'au dernier bloc miné et commence à rechercher un nouveau groupe à rejoindre. Comme illustré à la figure 4.2, le véhicule $V3$ perd la connectivité avec son groupe initial, puis rejoint ultérieurement une seconde blockchain locale initiée par le véhicule $V4$.
4. **Fusion des blockchains locales dans la blockchain globale :** la phase finale vise à garantir une auditabilité permanente en ancrant les blockchains locales archivées dans une blockchain globale lorsque les véhicules rétablissent leur connectivité avec l'infrastructure. Cette phase dépasse le cadre de cet article et fera l'objet de travaux futurs.

4.3 Évaluation des performances

Les évaluations proposées dans cette section visent à analyser les performances d'une blockchain locale en fonction du nombre de véhicules participants, tout en s'affranchissant des dégradations liées aux communications. Nous étudions l'impact conjoint de la densité véhiculaire,

du volume de trafic soumis à la blockchain et de la stratégie de minage sur plusieurs métriques, notamment le débit de validation des transactions (nombre de transactions soumises à la blockchain et validées par seconde), la latence de la blockchain locale lors du stockage des blocs soumis, ainsi que le pourcentage de données effectivement conservées lorsque la blockchain est archivée à la fin du scénario d'évaluation.

4.3.1 Contexte de simulation

Afin de garantir des résultats fiables et reproductibles, nous nous appuyons sur un ensemble d'outils stables, étroitement alignés avec les déploiements Ethereum. L'environnement de simulation repose sur une architecture à deux couches séparant le niveau applicatif (génération des messages V2X) du niveau blockchain (traitement transactionnel), ce qui permet d'observer indépendamment la génération des messages et leur enregistrement *on-chain* sous différentes charges. Nous utilisons Ganache CLI v7.x pour exécuter une blockchain Ethereum locale avec une production de blocs déterministe, configurée pour fournir jusqu'à 150 comptes afin d'émuler jusqu'à 150 véhicules concurrents. L'interaction avec la blockchain est assurée via Web3.js sur une connexion WebSocket, tandis que le contrat intelligent est développé et testé à l'aide de Remix IDE. La latence est définie comme le temps écoulé entre la soumission d'une transaction et l'émission de l'événement du contrat intelligent confirmant son enregistrement réussi dans la blockchain. L'ensemble des expériences a été réalisé sur une station de travail équipée d'un processeur Intel Core i7-13800H et de 31 Go de mémoire vive, sous Linux, et chaque exécution de simulation a une durée de 60 secondes.

Au niveau applicatif, implémenté en JavaScript à l'aide de Node.js, les véhicules simulés génèrent périodiquement trois types de messages conformément au standard ETSI ITS-G5 [111]. Afin de maintenir une charge blockchain maîtrisée tout en préservant la pertinence de l'audit, une politique de journalisation sélective est appliquée avant la soumission des messages à la blockchain.

[111]: ETSI. *TS 102 894-2 V1.2.1*. Rapp. tech. European Telecommunications Standards Institute, 2014

Messages DENM : Ces messages correspondent à des alertes critiques liées à la sécurité, déclenchées par des événements tels que des dangers ou des situations d'urgence. Dans notre simulation, chaque véhicule génère des DENM via une fonction événementielle : un événement est actif pendant une durée aléatoire tirée uniformément entre 3 s et 10 s, puis inactif pendant 20 s avant le déclenchement du suivant. Pendant la durée d'activité, un DENM est émis toutes les 200 ms. Ces messages constituent des éléments de preuve essentiels pour l'investigation d'incidents , ils sont donc intégralement conservés.

Messages CAM : Chaque véhicule émet un message CAM toutes les 100 ms, soit 10 messages par seconde. En raison de leur forte redondance sur de courtes fenêtres temporelles, seuls **10%** des messages CAM sont journalisés, afin de réduire la charge tout en conservant une traçabilité des messages susceptibles d'être liés à un incident.

Messages CPM : Chaque véhicule émet environ 10 CPM toutes les 3 s, soit approximativement 3,3 messages par seconde. Ces messages fournissent des informations contextuelles riches sur les objets perçus et les situations de quasi-collision, les rendant plus pertinents pour l'analyse forensique. Un taux de journalisation de **50%** est appliqué, représentant un compromis entre utilité pour l'audit et taille de la blockchain.

Après filtrage, chaque message V2X retenu génère une transaction Ethereum de taille fixe de 132 octets. Chaque transaction soumise invoque la fonction `logMessage` du contrat intelligent, laquelle enregistre le message, l'adresse de l'émetteur, un horodatage et le type de message.

4.3.2 Résultats de simulation

Afin d'analyser le comportement de la blockchain dans un contexte V2X et de déterminer la stratégie de minage la plus appropriée pour la journalisation des audits V2X, nous comparons deux approches distinctes : le minage déclenché selon un intervalle temporel fixe et le minage basé sur un nombre fixe de transactions (messages) par bloc. L'objectif est de maximiser le taux de confirmation des transactions tout en maintenant une latence minimale.

Minage à intervalle de temps fixe

L'approche à intervalle de temps fixe déclenche le minage des blocs à des instants réguliers, indépendamment du nombre de transactions en attente. Le tableau 4.2 compare les performances obtenues pour des intervalles de minage de 1 s et de 2 s, selon différentes densités de véhicules.

Table 4.2 – Comparaison des performances pour des intervalles de minage temporels de 1 s et 2 s

Intervalle de minage (s)	Nombre de véhicules	Nombre total de messages	Latence moyenne (s)	Débit moyen (tx/s)	Pourcentage de messages confirmés (%)
1	50	5090	68.9	78.27	92.26%
	100	6025	95.7	95.93	95.54%
	150	6587	122.8	106.78	97.27%
2	50	5015	70.3	76.83	91.92%
	100	6555	138.6	106.17	97.18%
	150	7350	190.3	119.88	97.86%

Avec un intervalle de minage de 1 s, le système prend en charge entre 50 et 150 véhicules, mais les taux de confirmation restent inférieurs à 100 %, variant de 92,26 % à 97,27 %. La latence moyenne augmente fortement avec la densité véhiculaire, atteignant 122,8 s pour 150 véhicules. L'augmentation de l'intervalle de minage à 2 s dégrade davantage les performances : la latence s'élève alors à 190,3 s pour 150 véhicules, tandis que les taux de confirmation ne progressent que marginalement. Globalement, ces résultats montrent que le minage basé sur des intervalles temporels peine à garantir une journalisation complète des messages sous forte densité véhiculaire, l'intervalle de 1 s offrant néanmoins une latence plus faible que celui de 2 s.

Ainsi, si les premiers messages arrivant au début d'un cycle peuvent être confirmés dès le bloc suivant, soit après 1 s ou 2 s selon l'intervalle de minage, les messages arrivant en cours de cycle ont tendance à s'accumuler dans le pool de transactions lorsque le taux d'arrivée dépasse la capacité de traitement par bloc. Dans ce cas, un message arrivant tardivement doit attendre que les blocs successifs absorbent l'ensemble des transactions qui le précèdent dans la file d'attente. Plus le pool est chargé, plus ce délai de confirmation s'allonge, pouvant atteindre plusieurs centaines de secondes pour les transactions situées en fin de file. La latence moyenne observée résulte ainsi d'une distribution hétérogène,

combinant des messages confirmés rapidement lors des premiers cycles et d'autres confirmés tardivement après une attente prolongée dans le pool de transactions. Ces derniers contribuent de manière significative à l'augmentation de la latence moyenne. Ce phénomène est d'autant plus marqué lorsque la densité véhiculaire augmente, l'afflux de messages croissant plus rapidement que la capacité d'absorption du système. Il en résulte un effet de saturation structurelle du pool de transactions, difficilement compatible avec les exigences de traçabilité et de réactivité quasi temps réel requises par les systèmes d'audit V2X.

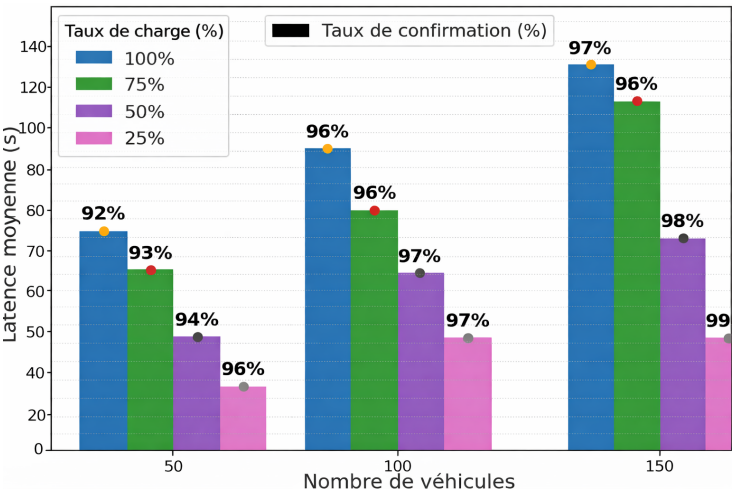

Figure 4.3 – Latence moyenne en fonction des différents taux de charge des messages

En se concentrant désormais uniquement sur les scénarios à intervalle de minage de 1 s, on observe que la latence augmente avec le nombre de véhicules et avec la charge transactionnelle injectée (Tableau 4.2). Un moyen de maintenir une latence cible consiste à réduire le volume de messages enregistrés dans la blockchain. Comme illustré à la figure 4.3, la diminution du nombre de messages soumis à la blockchain réduit significativement la latence et améliore les taux de confirmation. Toutefois, ces derniers n'atteignent pas 100 %, même pour les charges les plus faibles, ce qui met en évidence l'incapacité du minage à intervalle fixe à s'adapter efficacement aux pics de trafic, entraînant encore des pertes de messages.

Ces résultats offrent une perspective importante pour le concepteur d'un protocole d'audit basé sur la blockchain. La figure 4.3 met en évidence une corrélation positive entre le nombre de messages soumis à la blockchain et la latence moyenne observée. Plutôt que de chercher à enregistrer systématiquement l'intégralité des messages échangés, un concepteur pourrait adopter une stratégie de traçage adaptatif en réduisant sélectivement le taux de messages soumis à la blockchain en fonction de la densité instantanée du réseau afin de maintenir la latence en dessous d'un seuil cible acceptable pour les besoins d'audit. Par exemple, dans un scénario à forte densité où la charge transactionnelle est élevée, ne soumettre qu'une fraction des messages les plus critiques pour la sécurité permettrait de préserver les performances de la blockchain tout en garantissant une traçabilité suffisante. Cette approche implique néanmoins de définir au préalable des critères de sélection des messages à auditer en fonction de leur type, de leur priorité ou du contexte de circulation.

Table 4.3 – Comparaison des stratégies de minage : approche basée sur le débit et approche basée sur le nombre total de messages générés par seconde

Stratégie de minage	Nombre de véhicules	Transactions cibles par bloc	Latence moyenne (s)	Pourcentage de messages confirmés (%)	Nombre de blocs minés	Transactions observées par bloc
Basée sur le débit moyen (1 s)	50	78	1.1	100%	62	84.32
	100	96	1.2	100%	55	114.71
	150	107	1.6	100%	51	137.31
Messages générés par seconde (1 s)	50	150	1.6	99.86%	33	151.12
	100	300	3.5	78.44%	21	237.14
	150	450	7.1	52.54%	17	234.35

Minage avec un nombre fixe de messages par bloc

Afin de surmonter les limitations du minage basé sur le temps, nous mettons en œuvre deux stratégies, présentées dans le tableau 4.3. La première déclenche le minage d'un bloc lorsque le nombre de transactions en attente atteint le débit observé avec un minage à intervalle fixe de 1 s (voir Fig. 4.4).

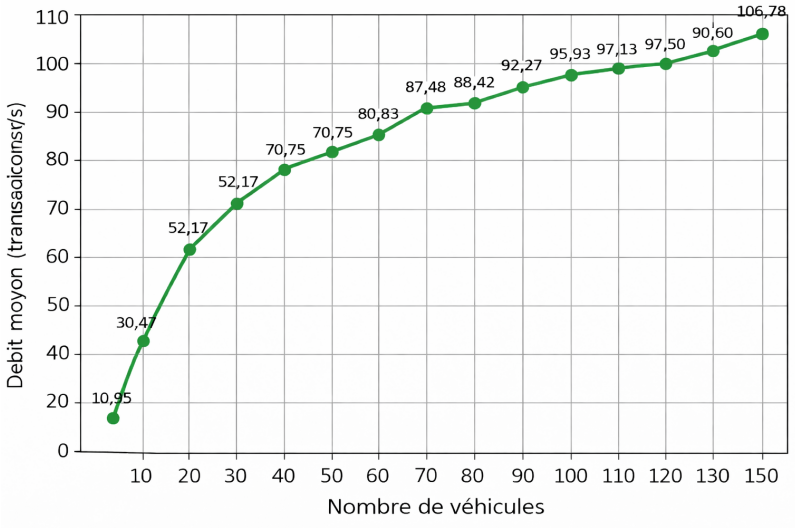

Figure 4.4 – Évolution du débit de la blockchain en fonction de la densité véhiculaire

La seconde stratégie déclenche le minage lorsque le nombre de transactions en attente atteint le nombre total de messages générés par l'ensemble des véhicules en une seconde. Étant donné que chaque véhicule génère en moyenne trois messages par seconde, la taille cible d'un bloc pour N véhicules est d'environ $3N$ transactions par seconde.

Le tableau 4.3 présente une analyse comparative de ces deux méthodes. L'approche basée sur le débit permet d'atteindre un taux de confirmation de 100 % pour toutes les densités de véhicules, avec une latence réduite d'environ 98 % par rapport au minage temporel à intervalle fixe de 1 s. Afin de mieux comprendre l'augmentation de la latence et la diminution du taux de messages confirmés observées lorsque le nombre de transactions par bloc augmente dans la seconde approche, nous avons fixé le nombre de véhicules à 100 et fait varier, pour chaque expérience, le nombre imposé de transactions par bloc, comme illustré à la figure 4.5. Pour des tailles de blocs comprises entre 10 et 200 transactions, la courbe (b) montre un taux de confirmation de 100 %. La valeur de 96 transactions par bloc, correspondant au seuil basé sur le débit et mise en évidence en (a), marque le point à partir duquel la latence commence à augmenter.

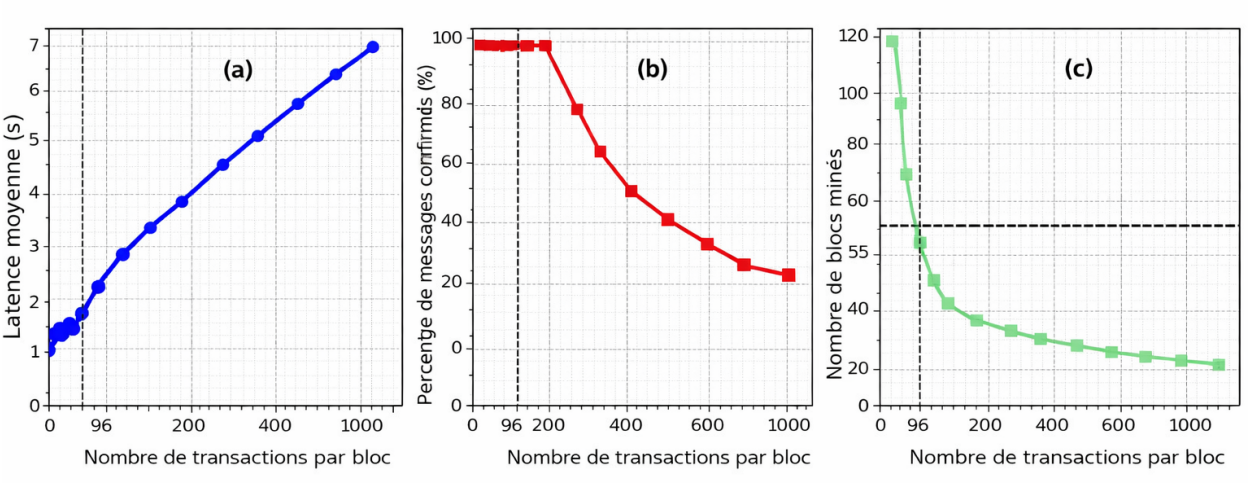

Figure 4.5 – Impact du nombre de transactions par bloc sur la latence moyenne, le pourcentage de messages confirmés et le nombre de blocs minés pour 100 véhicules

Ainsi, lorsque le nombre de transactions par bloc se situe dans l'intervalle [1, *throughput*], la latence demeure faible tout en garantissant 100 % de messages confirmés. En revanche, lorsque le nombre fixe de transactions par bloc est inférieur au débit, la courbe (c) indique qu'un nombre excessif de blocs est miné, ce qui surcharge le réseau, chaque bloc devant être miné, propagé et traité avant son intégration dans la blockchain globale. Ces résultats démontrent qu'une stratégie de minage basée sur le débit est la plus adaptée à une solution d'audit V2X fondée sur la blockchain.

Conclusion

Dans ce chapitre, nous avons proposé et évalué un système d'audit basé sur la blockchain visant à assurer un enregistrement sécurisé, immuable et vérifiable des traces de communications V2X. En permettant aux véhicules de participer en tant que nœuds au sein de blockchains locales formées par des véhicules évoluant conjointement, cette approche réduit la dépendance vis-à-vis des infrastructures fixes et demeure opérationnelle même dans des contextes V2V sans infrastructure. À travers des simulations contrôlées, ce travail montre que le minage basé sur le temps, avec un intervalle fixe, ne permet pas de garantir un enregistrement complet sous forte charge, tandis qu'une stratégie de minage basée sur le débit de transactions supporté par la blockchain permet d'atteindre un taux de confirmation des messages de 100% tout en réduisant significativement la latence. Le chapitre suivant a pour objectif d'évaluer l'approche proposée à l'aide d'un simulateur V2X réaliste intégrant la mobilité des véhicules et les communications, et d'analyser différents paramètres de performance de la blockchain conjointement aux métriques de la couche communication.

Évaluation de la blockchain dans un réseau véhiculaire simulé

5

5.1 Mise en place du scénario autoroutier 73
5.1.1 Configuration de la mobilité (SUMO) 75
5.1.2 Paramètres de communication V2V (OMNeT++) . . 76
5.2 Injection de la latence blockchain dans VEINS/OMNeT++ 80
5.2.1 Extraction de la latence à partir des expérimentations blockchain 81
5.2.2 Intégration de la latence blockchain dans les communications V2X simulées 81
5.3 Métriques d'évaluation . 82
5.3.1 Évaluation de la formation des groupes et de la traçabilité 82
5.3.2 Durée de vie des blockchains locales 85
5.3.3 Délai de bout en bout d'enregistrement d'un message 85

Introduction

Le chapitre précédent a posé les fondements d'une architecture d'audit basée sur la blockchain pour les communications V2X, et a évalué ses performances en mesurant la latence d'enregistrement des messages dans un contexte contrôlé. Ces mesures ont notamment permis d'identifier cette latence comme un paramètre critique, dont la valeur varie significativement selon la densité vehiculaire et la stratégie de minage adoptée.

Cependant, cette évaluation isolée ne permet pas de capturer les interactions dynamiques entre la blockchain et les communications V2V, où les véhicules sont en mouvement constant, où les groupes se forment et se defont au gré de la mobilité, et où le canal radio est soumis à des conditions de propagation variables. Il devient alors nécessaire d'inscrire ces paramètres dans un environnement de simulation véhiculaire complet et réaliste, afin d'évaluer conjointement les performances de communication et les performances de la blockchain dans des conditions représentatives d'un réseau véhiculaire réel [112].

Ce chapitre présente cette évaluation intégrée. Nous décrivons d'abord le scénario autoroutier mis en place, en détaillant la configuration de la mobilité des véhicules sous SUMO ainsi que les paramètres de communication V2V sous OMNeT++. Nous explicitons ensuite la méthode d'injection de la latence blockchain dans le simulateur VEINS, qui permet de coupler les résultats du chapitre 4 avec le comportement de la couche réseau. Enfin, nous présentons les métriques d'évaluation retenues et analysons les résultats obtenus pour trois scénarios de densité véhiculaire contrastés.

[112]: Christoph Sommer, Reinhard German et Falko Dressler. « Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis ». In : *IEEE Transactions on Mobile Computing* 10.1 (2011)

5.1 Mise en place du scénario autoroutier

L'évaluation d'un mécanisme d'audit distribué pour les communications V2X exige un environnement de simulation capable de reproduire avec fidélité les conditions d'un réseau véhiculaire réel. Dans ce contexte, le choix d'un scénario autoroutier s'impose naturellement, tant pour des raisons scientifiques qu'opérationnelles, en raison de sa pertinence vis-à-vis des objectifs de cette thèse.

L'environnement autoroutier se distingue par une absence fréquente d'infrastructure de communication [113]. Contrairement aux zones urbaines, généralement bien équipées en RSUs, les segments autoroutiers comportent de longues portions dépourvues de couverture fixe, parfois sur plusieurs dizaines de kilomètres. Dans ces conditions, les véhicules doivent s'appuyer exclusivement sur des communications V2V pour maintenir la continuité des échanges et de la traçabilité. Ce contexte met particulièrement en valeur l'intérêt d'un mécanisme décentralisé basé sur la blockchain, où des groupes éphémères de véhicules assurent

[113]: Y. Dai, L. Hu, Y. Liu et A. Yang. « Modeling and analyzing V2V communication limitations impacts on connected and automated vehicle platoons ». In : *PLOS ONE* 20.8 (2025)

collectivement les fonctions de collecte et de conservation du registre d'audit, en l'absence de toute entité de confiance centralisée.

Par ailleurs, les communications V2X en environnement autoroutier présentent des enjeux de sécurité particulièrement critiques [114]. À des vitesses élevées, la diffusion d'un message erroné ou malveillant, tel qu'un faux signal de freinage d'urgence ou une alerte de congestion fictive, peut engendrer des réactions en chaîne aux conséquences potentiellement graves. Dans ce contexte, la capacité à retracer précisément l'origine et la propagation des messages constitue une exigence fondamentale, justifiant la mise en place d'un mécanisme d'audit robuste et distribué.

[114]: Mohamed Nidhal Mejri, Jalel Ben-Othman et Mohamed Hamdi. « Survey on VANET security challenges and possible cryptographic solutions ». In : *Vehicular Communications* 1.2 (2014)

Les caractéristiques de la mobilité autoroutière constituent également un cadre particulièrement exigeant pour les protocoles de formation de groupes. Les véhicules évoluent dans la même direction à des vitesses élevées et relativement homogènes, toutefois, la durée de coexistence radio entre deux nœuds dépend principalement de leur vitesse relative [115]. En conditions réelles, celle-ci demeure non nulle en raison des variations de conduite, des manœuvres de dépassement et des différences individuelles de vitesse.

[115]: Fan Bai, Hariharan Krishnan, Tamer Elbatt et Gavin Holland. « Towards characterising and classifying communication-based automotive applications from a wireless networking perspective ». In : *Int. J. of Vehicle Autonomous Systems* 10 (jan. 2012)

Ainsi, même en présence de vitesses moyennes similaires, la distance entre deux véhicules tend à évoluer rapidement, limitant la durée pendant laquelle ils restent simultanément à portée radio. Par exemple, pour une densité de 25 véhicules par kilomètre et une vitesse moyenne de 36 m/s, deux véhicules initialement séparés de 144 mètres ne disposent que d'une fenêtre de communication de l'ordre de quelques secondes, en fonction de leur vitesse relative. Cette contrainte impose des exigences strictes en termes de réactivité, de synchronisation et de robustesse du protocole de formation de groupe, les opérations de découverte, d'association et d'échange devant être réalisées dans des délais très courts afin d'éviter toute rupture de communication.

Enfin, la mobilité autoroutière présente un caractère structuré et reproductible. Les véhicules suivent des trajectoires rectilignes à sens unique, sans intersections ni interactions complexes, ce qui permet d'isoler plus facilement l'impact des paramètres étudiés, notamment la densité et la vitesse. Ces paramètres influencent directement les performances des communications VANET [116], indépendamment des effets liés à la topologie. Cette régularité est essentielle pour garantir la rigueur des analyses comparatives menées dans le cadre des différents scénarios de simulation.

[116]: Angélica Reyes, Cristina Barrado, Marco López et Cora Excelente. « Vehicle density in VANET applications ». In : *Journal of Ambient Intelligence and Smart Environments* 6.4 (2014). eprint : https://journals.sagepub.com/doi/pdf/10.3233/AIS-140271

Ce choix de scénario s'inscrit également en cohérence avec les standards de communication considérés. Le protocole IEEE 802.11p DSRC [98], défini dans le cadre des communications WAVE (Wireless Access in Vehicular Environments), a été conçu pour des environnements véhiculaires caractérisés par une forte mobilité, des topologies dynamiques et des contraintes strictes de faible latence. Ces caractéristiques correspondent étroitement aux conditions rencontrées en contexte autoroutier. Par ailleurs, les standards ETSI ITS relatifs aux communications V2X, notamment en matière de sécurité ETSI TS 102 940 [117], TS 102 941 [65]et TS 103 097 [99], visent à garantir des échanges fiables et sécurisés dans le cadre des systèmes coopératifs de transport intelligent (C-ITS). Bien que ces spécifications s'appliquent à l'ensemble des environnements routiers, leurs hypothèses de conception en termes de mobilité, de réactivité et de communication opportuniste, sont pleinement compatibles avec le contexte autoroutier. Cette adéquation renforce la pertinence du scénario retenu pour l'évaluation du mécanisme proposé dans cette thèse.

[117]: ETSI. *Intelligent Transport Systems (ITS) ; Security ; ITS communications security architecture and security management*. Rapp. tech. ETSI TS 102 940 V1.3.1. European Telecommunications Standards Institute, 2018

5.1.1 Configuration de la mobilité (SUMO)

La mobilité des véhicules est générée à l'aide du simulateur SUMO (Simulation of Urban MObility), un simulateur de trafic routier microscopique open-source permettant de modéliser le déplacement individuel des véhicules dans un réseau routier. Ce choix se justifie par sa capacité à reproduire fidèlement les dynamiques de mobilité, notamment en termes de vitesse, d'interactions inter-véhiculaires et de changements de voie, tout en offrant une intégration native avec les simulateurs réseau.

SUMO est interfacé avec OMNeT++ via le protocole TraCI, permettant une synchronisation en temps réel entre la mobilité des véhicules et les communications V2X.

La topologie routière est modélisée par un segment autoroutier unidirectionnel de 7 500 mètres, composé de trois voies parallèles (*edge0*), défini dans le fichier *myMap.net.xml*. Les voies sont positionnées respectivement aux coordonnées $y = 22{,}00\,\text{m}$, $y = 25{,}20\,\text{m}$ et $y = 28{,}40\,\text{m}$ dans le plan de simulation.

Un unique type de véhicule est considéré pour l'ensemble des scénarios, caractérisé par une longueur de 4 m, une accélération maximale de $2{,}5\,\text{m/s}^2$, une décélération maximale de $4{,}5\,\text{m/s}^2$ ainsi qu'une dispersion de vitesse $\sigma = 0{,}1$, introduisant une variabilité réaliste du comportement des véhicules tout en conservant la stabilité du scénario.

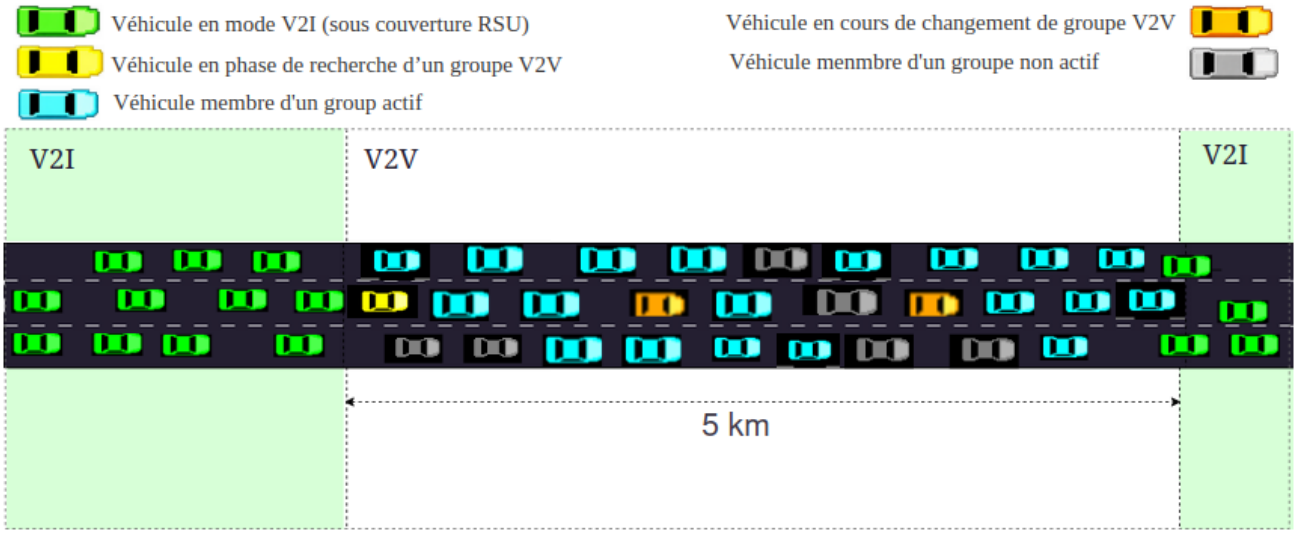

Figure 5.1 – Topologie autoroutière simulée illustrant les communications V2I et V2V dans l'environnement SUMO.

Afin d'évaluer l'impact de la densité véhiculaire sur les performances du mécanisme d'audit basé sur la blockchain, trois scénarios couvrant des régimes de circulation contrastés, représentatifs des conditions autoroutières réelles, ont été définis.

Densité faible 25 v/km (véhicules par kilomètre) qui correspond à un trafic fluide à haute vitesse 130 km/h, caractérisé par un espacement inter-véhiculaire important d'environ 120 m et une fenêtre de coexistence

radio limitée entre deux véhicules. Dans ces conditions, la formation de groupes blockchain est contrainte par la faible probabilité de contact prolongé entre véhicules voisins.

Densité moyenne 102 v/km qui représente un trafic intermédiaire à vitesse modérée 82,5 km/h, favorisant des durées de contact plus longues et une dynamique de groupe plus stable.

Densité élevée 198 v/km, qui permer de simuler un trafic dense à faible vitesse 31,1 km/h, dans lequel les véhicules restent durablement à portée de communication les uns des autres. Cette configuration maximise les opportunités de formation et de maintien des groupes blockchain, tout en augmentant la charge de messages V2X à traiter.

Chaque scénario repose sur une procédure d'initialisation en deux phases :

1. **Phase de pré-remplissage** : les véhicules sont injectés de manière échelonnée sur l'ensemble du segment autoroutier, répartis sur les trois voies, à la vitesse moyenne du scénario. Cette étape permet d'obtenir une densité immédiatement représentative dès le début de la simulation.
2. **Phase de flux de remplacement($t = t_{\text{begin}}$)** : un flux continu de véhicules est injecté sur chaque voie à partir d'un instant t_{begin}, correspondant à la sortie des premiers véhicules du segment. Ce flux est maintenu jusqu'à la fin de la simulation, garantissant une densité stable tout au long de l'expérience.

Les paramètres de configuration de chaque scénario, extraits directement des fichiers de simulation, sont présentés dans le tableau 5.1.

Table 5.1 – Paramètres de simulation pour les différents niveaux de densité véhiculaire

Densité ciblée	**25 v/km**	**102 v/km**	**198 v/km**
Densité effective simulée	24,93	100,40	192,40
Nombre de véhicules	187	753	1 443
Vitesse moyenne	130 km/h	82.5 km/h	31.1 km/h
Entrée en zone V2V	55,4 s	87,3 s	231,2 s
Sortie de la zone V2V	193,8 s	305,5 s	809,2 s
Traversée complète (7,5km)	207,7 s	327,3 s	866,9 s
Marge après renouvellement	392,3 s	372,7 s	333,1 s
Durée de simulation	600 s	700 s	1 200 s

5.1.2 Paramètres de communication V2V (OMNeT++)

Les communications véhiculaires sont simulées à l'aide du framework Veins couplé à OMNeT++, implémentant le standard IEEE 802.11p[98] DSRC, adapté aux réseaux véhiculaires à faible latence.

Paramètres radio et canal

La portée de communication est fixée à 250 m pour les véhicules et les RSUs. La puissance d'émission est définie à 20 mW, avec un débit de transmission des données de 6 Mbit/s. Le modèle de propagation adopté est un modèle en espace libre, supposant l'absence d'obstacles dans la propagation, avec activation du délai de propagation. Le canal

de contrôle (CCH) 5.9 GHz est utilisé conformément au standard ETSI EN 302 663 [118], qui le désigne comme canal exclusif pour les messages de sécurité V2X (CAM, DENM, CPM). Le canal de service (SCH) étant désactivé.

[118]: ETSI. *EN 302 663 V1.3.1 : ITS-G5 Access layer specification*. Rapp. tech. European Telecommunications Standards Institute, 2020

L'ensemble de ces paramètres est récapitulé dans le tableau 5.2.

Table 5.2 – Paramètres radio et du canal de communication

Paramètre	**Valeur**
Portée de communication	250 m
Puissance d'émission	20 mW
Débit de transmission	6 Mbit/s
Modèle de propagation	Espace libre
Délai de propagation	Activé
Canal de communication	canal de contrôle (CCH)

Infrastructure routière

La configuration de l'infrastructure autoroutière est illustrée à la Figure 5.1. Cinq unités RSU sont déployées le long du segment autoroutier. Quatre RSUs couvrent la zone d'entrée s'étendant de 0 à 2 km, tandis qu'un RSU est positionné en sortie et couvre une zone de 0,5 km. La zone centrale, d'une longueur de 5 km, constitue une zone V2V pure, dépourvue d'infrastructure. Cette zone représente le cœur de l'étude, dans laquelle le mécanisme d'audit basé sur la blockchain est activé et évalué, permettant d'analyser son comportement dans des conditions de communication entièrement décentralisées.

Messages V2X

Afin d'assurer la cohérence avec l'évaluation des performances blockchain réalisée au chapitre précédent, les fréquences d'émission des messages V2X sont identiques à celles utilisées lors des expérimentations du Chapitre 4. Ce choix garantit que la charge de trafic soumise au mécanisme de traçabilité est comparable aux conditions dans lesquelles les latences de la blockchain ont été mesurées.

Trois types de messages V2X sont générés par chaque véhicule :

— CAM : émis périodiquement toutes les 1,0 s
— DENM : émis avec une période aléatoire uniforme entre 0,5 s et 1,0 s
— CPM : émis avec une période aléatoire uniforme entre 1,0 s et 2,0 s

Un décalage initial aléatoire est introduit afin de désynchroniser les émissions des véhicules et de limiter les collisions sur le canal de communication.

Modélisation de la formation de groupe V2V : états des véhicules et processus de formation

Le mécanisme de formation de groupe constitue un élément central du système d'audit proposé. Il est implémenté au niveau applicatif dans OMNeT++, en s'appuyant sur les communications V2X définies précédemment. Dans ce contexte, les véhicules évoluent dans une topologie autoroutière structurée, illustrée à la Figure 5.1, où une zone centrale

V2V dépourvue d'infrastructure favorise la formation de groupes dynamiques.

Chaque véhicule évolue selon une machine à états représentant son interaction avec le protocole de formation de groupe. Ces états sont illustrés à la Figure 5.2.

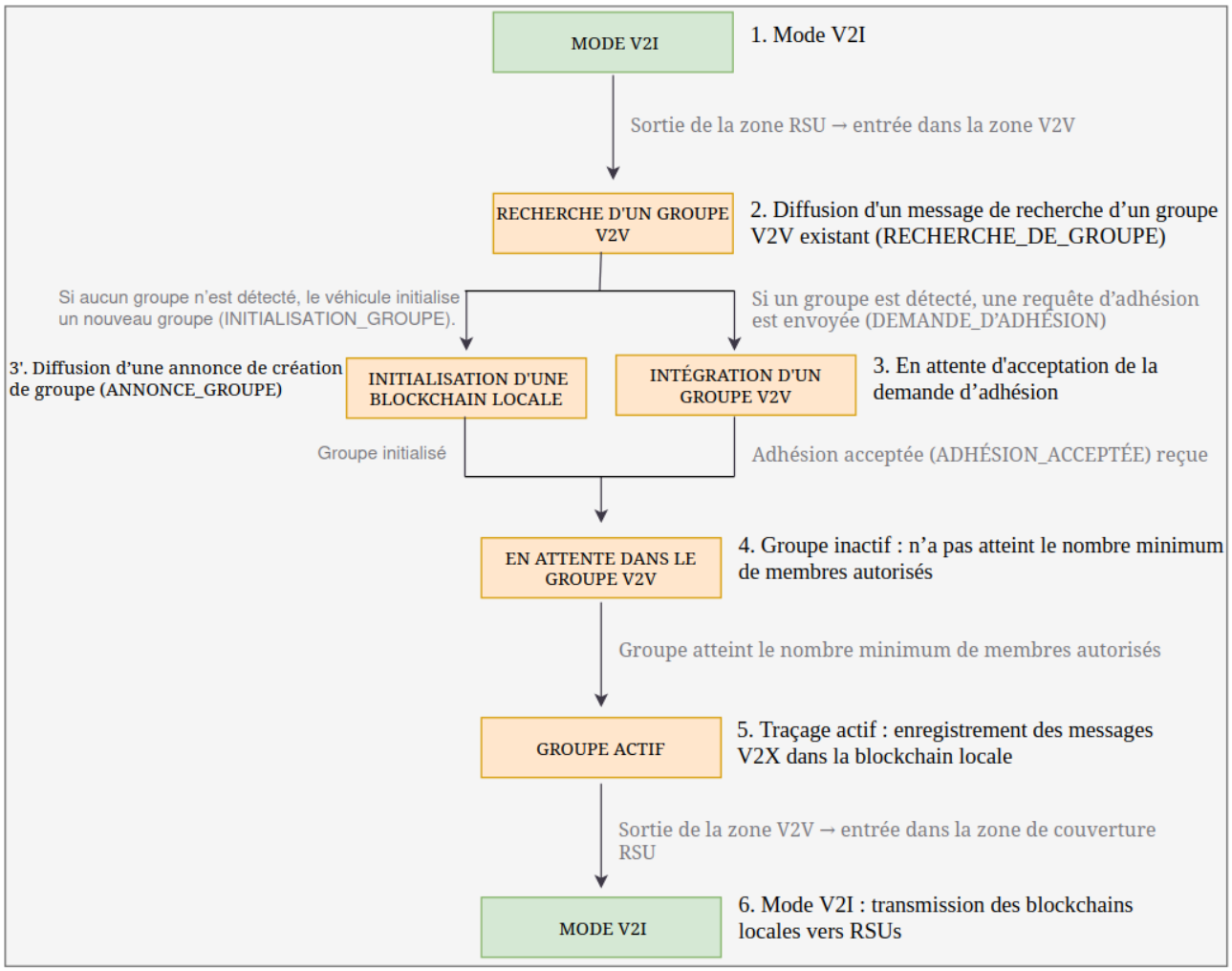

Figure 5.2 – Processus de formation de groupe V2V et états des véhicules.

États des véhicules

Les états considérés sont les suivants :

- **Mode V2I** : le véhicule est sous couverture d'une RSU et communique avec l'infrastructure.
- **Recherche de groupe** : le véhicule entre dans la zone V2V illustrée dans la figure 5.1 et diffuse des messages de découverte.
- **Intégration au groupe** : Si le véhicule trouve un groupé, il envoie une requête d'adhésion et attend une réponse.
- **Initialisation d'une blockchin locale** : si aucun groupe n'est détecté, le véhicule crée un nouveau groupe V2V, initialise une blockchain locale et recherche des membres.

— **En attente dans le groupe** : le groupe est formé mais reste inactif (taille insuffisante).
— **Groupe actif** : le seuil minimal est atteint et le mécanisme d'audit blockchain est activé.
— **Envoi vers RSU** : les blockchains locales sont transmises à l'infrastructure.

Processus de formation de groupe

Le fonctionnement global du protocole de formation de groupe ainsi que les transitions entre les différents états des véhicules sont détaillés à la Figure 5.2.

Lorsqu'un véhicule quitte la zone V2I et entre dans la zone V2V, il passe à l'état de recherche de groupe et diffuse des messages de type *RECHERCHE_DE_GROUPE*. Lorsqu'un groupe est détecté, une procédure d'adhésion est engagée via l'envoi d'un message *REQUÊTE_D'ADHÉSION*.

Si la requête est acceptée (*ADHÉSION_ACCEPTÉE*), le véhicule rejoint le groupe. Tant que le nombre de membres reste inférieur au seuil minimal, le groupe demeure inactif. Dès que ce seuil est atteint, le groupe devient actif, déclenchant le mécanisme de traçage. Dans les résultats présentés, deux valeurs de ce seuil sont évaluées : une taille minimale de 3 véhicules (configuration de référence) et une taille minimale de 2 véhicules (configuration allégée), dont l'impact sur la traçabilité est analysé dans les tableaux 5.4.

Durant cette phase, les messages V2X échangés entre les véhicules membres du groupe sont enregistrés dans une blockchain locale. Dans le cadre de cette simulation, celle-ci est modélisée sous la forme d'un fichier texte partagé. La Figure 5.3 illustre un extrait d'une blockchain locale, générée par le véhicule leader du groupe, et contenant l'ensemble des messages échangés entre les participants. Les messages sont ajoutés sous forme de transactions signées avec la clé privée du véhicule, incluant l'identifiant de l'émetteur, le contenu du message, son type ainsi qu'un horodatage. Étant donné que les communications V2X sont diffusées par broadcast au sein du groupe, tout véhicule ayant reçu un message peut également le soumettre à la blockchain. Ainsi, même si un véhicule malveillant refuse délibérément de soumettre ses propres messages, les autres membres du groupe ayant reçu ces mêmes messages peuvent les enregistrer indépendamment. Cette redondance garantit qu'un émetteur ne peut pas empêcher la traçabilité de ses communications en refusant de participer au mécanisme d'audit.

Comme le montre la figure 5.3, chaque entrée correspond à un message V2X caractérisé par un horodatage, un identifiant de véhicule, un type de message ainsi que les données associées. Ces messages sont ajoutés de manière séquentielle dans le fichier, lequel contient également des métadonnées, telles que l'identifiant du véhicule ayant créé la blockchain locale, celui ayant clôturé le bloc, ainsi que les horodatages associés aux différentes étapes.

Ce fichier constitue ainsi un registre simplifié, partagé entre les membres du groupe, garantissant la traçabilité des échanges V2X. Toutefois, cette modélisation reste une approximation et ne reflète pas les délais inhérents aux mécanismes réels de validation blockchain, tels que le temps de minage ou de propagation des blocs. Afin d'évaluer de manière réaliste l'impact du mécanisme blockchain sur les performances du système, il est nécessaire d'intégrer explicitement la latence d'enregistrement des

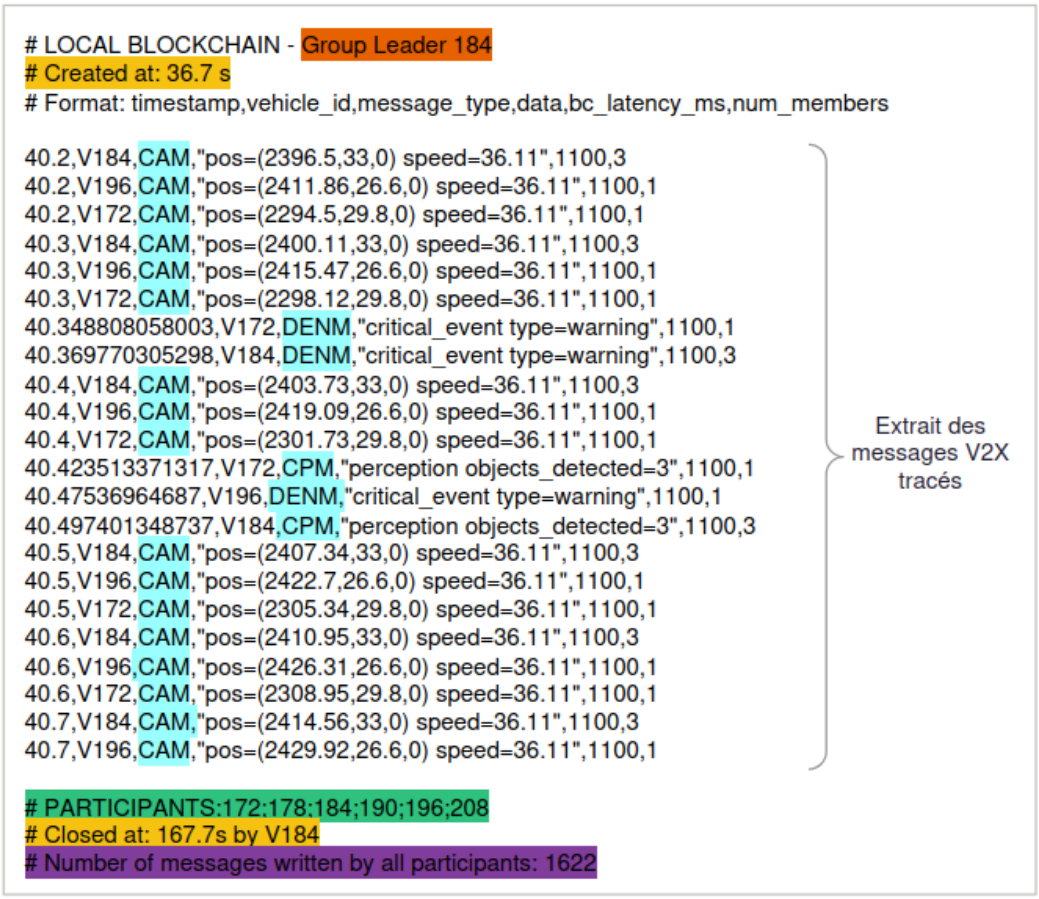

Figure 5.3 – Extrait d'une blockchain locale partagée entre les véhicules membres d'un groupe V2V.

messages dans la blockchain. Comme établi au chapitre précédent, ce paramètre est critique et dépend de la densité véhiculaire ainsi que des caractéristiques de formation des groupes. La section suivante présente donc la méthode retenue pour injecter cette latence dans l'environnement VEINS/OMNeT++, afin d'analyser son influence sur la disponibilité des messages et la performance globale du système.

5.2 Injection de la latence blockchain dans VEINS/OMNeT++

La prise en compte de la latence induite par les mécanismes blockchain constitue un élément essentiel pour une évaluation réaliste des communications V2X. En effet, contrairement aux modèles de communication classiques, dans lesquels les messages sont supposés immédiatement disponibles après transmission, l'introduction d'un processus d'audit basé sur la blockchain impose un délai supplémentaire lié à l'enregistrement et à la validation des données.

Dans cette section, nous proposons d'intégrer explicitement cette latence dans l'environnement de simulation VEINS/OMNeT++, afin de refléter le comportement réel d'un système de communication véhiculaire basé sur la blockchain. Cette intégration repose sur une approche en deux étapes : d'une part, l'extraction des valeurs de latence issues des expérimentations

Table 5.3 – Extraction de la latence moyenne d'enregistrement d'un message V2X dans la blockchain

Paramètres de formation des groupes [119]			
Scénarios	1	2	3
Densité	-	+	++
Nombre de véhicules (v/km)	25 v/km	102 v/km	198 v/km
Nombre des voisins par direction	4	15	20
Durée moyenne du groupe (s)	64.4 s	71.9 s	70.0 s
Paramètres blockchain			
Durée de simulation	64 s	72 s	70 s
Nombre de transactions par bloc	13	51	70
Latence moyenne d'enregistrement (s)	1.05 s	1.07 s	1.10 s

blockchain réalisées au chapitre précédent, et d'autre part, leur injection dans les messages V2X simulés au niveau applicatif.

5.2.1 Extraction de la latence à partir des expérimentations blockchain

Le Tableau 5.3 présente les paramètres utilisés pour l'extraction de la latence blockchain en fonction de la densité véhiculaire. Pour chaque scénario, les caractéristiques de formation de groupe, notamment la taille moyenne des voisins et la durée de vie des groupes, servent de base à la simulation du mécanisme blockchain. Ces paramètres sont issus du travail de référence [119], qui modélise le comportement des véhicules sur un segment autoroutier de 5 km composé de trois voies.

[119]: Lucas Rivoirard. « Modèle d'auto-organisation pour les protocoles de routage dans les réseaux ad hoc de véhicules : application à la perception élargie et à la localisation coopératives ». Theses. Université de Lille, sept. 2018

À titre d'exemple, dans le scénario de faible densité 25 v/km, la taille moyenne des groupes est de 4 véhicules, ce qui correspond au nombre moyen de voisins présents simultanément dans la portée de communication. La simulation est alors réalisée en considérant un groupe de 4 participants évoluant pendant une durée moyenne de 64,4 secondes.

Dans une première phase, le débit de génération des messages V2X est estimé à partir d'un mécanisme de minage à intervalle temporel fixe 1 s , permettant d'obtenir un débit moyen d'enregistrement de treize transactions par seconde (13 tx/s).

Dans une seconde phase, ce mécanisme est remplacé par une stratégie de minage basée sur un seuil fixe de 13 tx/bloc.

Cette approche permet d'adapter la latence d'enregistrement à chaque niveau de densité véhiculaire, en fonction du volume réel de messages générés.

5.2.2 Intégration de la latence blockchain dans les communications V2X simulées

L'intégration de la latence blockchain est réalisée au niveau applicatif en associant à chaque message V2X un délai représentant son enregistrement dans la blockchain.

Lorsqu'un véhicule génère un message V2X, celui-ci est transmis aux véhicules voisins via le réseau V2V. Le message est ensuite pris en charge par le mécanisme d'audit et soumis à un délai correspondant à la latence blockchain extraite pour le scénario de densité considéré.

Le temps total d'enregistrement d'un message est ainsi modélisé comme la somme du délai de transmission et de la latence blockchain :

$$T_{\text{enregistrement}} = T_{\text{transmission}} + T_{\text{latence_blockchain}}$$

Une fois ce délai écoulé, le message est considéré comme validé et enregistré dans la blockchain locale.

Cette modélisation permet d'introduire un décalage temporel réaliste dans la disponibilité des messages V2X, lié aux conditions de trafic.

5.3 Métriques d'évaluation

Après l'intégration de la latence blockchain dans la simulation, une évaluation des performances du système, permettant d'analyser la traçabilité des messages V2X, la dynamique de formation des groupes ainsi que l'influence de la blockchain sur le délai de disponibilité des messages tracés, est nécessaire.

Afin d'assurer la fiabilité des métriques évaluées, une fenêtre de mesure est définie afin d'exclure les effets transitoires liés au démarrage de la simulation. En effet, au début de la simulation, les véhicules sont progressivement injectés dans le réseau, ce qui entraîne la formation de groupes instables et non représentatifs du comportement réel du système. Il est donc nécessaire de considérer uniquement la phase de régime permanent, dans laquelle la densité véhiculaire est stabilisée et les interactions entre véhicules sont pleinement établies.

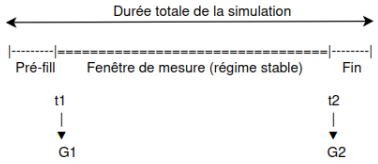

Figure 5.4 – Fenêtre de mesure

La fenêtre de mesure est ainsi délimitée par deux instants clés : l'arrivée du premier groupe éligible G_1 et celle du dernier groupe éligible G_2 au niveau de la RSU de sortie. Le groupe G_1 correspond au premier groupe formé dans la zone V2V ayant parcouru l'intégralité de cette zone sans infrastructure, tandis que G_2 représente le dernier groupe satisfaisant ce critère avant la fin de la simulation. L'intervalle $[t_1, t_2]$, défini par ces deux événements, constitue la période durant laquelle les métriques sont collectées.

5.3.1 Évaluation de la formation des groupes et de la traçabilité

1. **Densitè faible 25v/km :**

   Le tableau 5.4 présente les résultats de l'évaluation de la traçabilité des messages V2X pour une densité de 25 v/km, en faisant varier deux paramètres clés : la fréquence de recherche de groupe, la fréquence d'annonce d'un groupe créé , ainsi que la taille minimale requise pour qu'un groupe soit considéré comme actif.

   Impact des fréquences de recherche et d'annonce d'un groupe sur la traçabilité :

   Dans un premier temps, la taille minimale d'un groupe actif est fixée à 3 véhicules. Pour une fréquence de recherche de 1.5 s et une fréquence d'annonce de 1 s, les résultats obtenus indiquent un taux

Table 5.4 – Évaluation de la traçabilité des messages V2X pour une densité de 25 v/km

Fréquence de recherche d'un groupe (s)	Fréquence d'annonce d'un groupe (s)	Durée de la fenêtre de mesure (s)	Nombre de groupes	Nombre de véhicules par groupe	Nombre de copies par blockchain reçues	Durée pour rejoindre un groupe (s)	Durée d'un groupe avec blockchain inactive (s)	Nombre de messages échangés	Nombre de messages non tracés	Pourcentage de traçabilité
Taille minimale de groupe actif = 3										
1.5	**1**	453	48	**7**	5	65	9.2	613 397	98 143	84%
0.75	**0.5**	437	54	**7.7**	5	46	2.9	570 834	62 791	89%
Taille minimale de groupe actif = 2										
1.5	**1**	453	58	6.6	4.5	39	0.99	613 388	55 204	92 %
0.75	**0.5**	460	56	4.8	4.5	22	1.61	673 612	33 680	95%

de traçabilité de **84 %**, un temps moyen de jonction élevé de 65 s ainsi qu'une durée d'inactivité moyenne de 9.2 s par groupe.
Afin d'améliorer ces performances, les intervalles de recherche et d'annonce ont été réduits à 0.75 s et 0.5 s respectivement, augmentant ainsi la fréquence des échanges de contrôle. Comme le montre le tableau 5.4, cette adaptation permet de réduire le temps de jonction de 65 s à 46 s et de diminuer la durée d'inactivité de 9.2 s à 2.9 s. Le taux de traçabilité s'améliore ainsi de **84%** à **89%**. Toutefois, cette augmentation de la fréquence des échanges de contrôle engendre une surcharge supplémentaire sur le canal de communication. Ce compromis entre traçabilité et charge réseau doit être pris en compte, en particulier dans les environnements à forte densité où le risque de collision sur le canal est plus élevé [120].
Néanmoins, afin de réduire davantage la durée d'inactivité, qui limite structurellement les performances dans un environnement de faible densité, la taille minimale d'un groupe actif a été abaissée à 2 véhicules. Cette adaptation permet d'éviter que les groupes restent trop longtemps dans un état inactif en attente d'un troisième membre, et contribue ainsi à améliorer la traçabilité des messages.

[120]: Pierpaolo Salvo, Francesca Cuomo, Andrea Baiocchi et Izhak Rubin. « Investigating VANET dissemination protocols performance under high throughput conditions ». In : *Vehicular Communications* 2.4 (2015)

Réduction de la taille minimale à deux véhicules :

Pour pallier cette limitation, la taille minimale d'un groupe actif est réduite à 2 véhicules. Pour les mêmes fréquences de recherche 1.5 s et d'annonce 1 s, les résultats obtenus indiquent que le temps de jonction diminue significativement de 65 s à 39 s. La durée d'inactivité devient inférieure à 1 s, avec une valeur de 0.99 s, ce qui indique que les groupes atteignent presque systématiquement leur seuil d'activation. Le taux de traçabilité atteint alors **92%**.
En combinant cette réduction avec une augmentation de la fréquence des échanges, avec une fréquence de recherche de 0.75 s et une fréquence d'annonce de 0.75s, le temps de jonction est encore réduit à 22s, traduisant une meilleure stabilité des groupes formés. Le taux de traçabilité atteint ainsi **95%**, soit un gain de **11%** par rapport à la configuration initiale.

2. **Densité moyenne 102 v/km :**

À partir du Tableau 5.5, relatif à une densité de 102 v/km, on observe que pour des fréquences identiques de recherche et d'annonce d'un groupe 1.5 s et 1 s respectivement, le taux de traçabilité atteint **91 %**. En comparaison avec le cas de faible densité 25 v/km, les résultats montrent une amélioration des performances. En effet, le délai de jonction est significativement réduit à 16s, et la durée d'inactivité des groupes diminue également pour atteindre 3.5s.

Table 5.5 – Évaluation de la traçabilité des messages V2X pour une densité de 102 v/km

Fréquence de recherche d'un groupe (s	Fréquence d'annonce d'un groupe (s)	Durée de la fenêtre de mesure (s)	Nombre de groupes	Nombre de véhicules par groupe	Nombre de copies par blockchain reçues	Durée pour rejoindre un groupe (s)	Durée d'un groupe avec blockchain inactive (s)	Nombre de messages échangés	Nombre de messages non tracés	Pourcentage de traçabilité
Taille minimale de groupe actif = 3										
1.5	**1**	430	44	15	8	16	3.5	553 218	49 789	91%
0.75	**0.5**	460	48	19	8.5	25,4	2.9	720 838	93 709	87%

Cette amélioration s'explique principalement par l'augmentation de la densité véhiculaire, qui permet à un véhicule de trouver plus rapidement un groupe, favorisant ainsi une transition plus rapide vers l'état actif des groupes.
Mais dans le cas d'une densité de 102 v/km, l'augmentation de la fréquence de recherche et d'annonce, respectivement à 0.75 s et 0.5 s, entraîne une surcharge du canal de communication. En effet, lorsque de nombreux véhicules émettent simultanément des messages de recherche et d'annonce à des intervalles réduits, le nombre de collisions au niveau du canal augmente, ce qui peut engendrer une dégradation des performances du réseau [120]. Ces collisions provoquent des pertes de messages, empêchant ainsi certains véhicules de recevoir correctement les annonces de groupe.

3. **Densité élevée 198 v/km :**

Dans le cas d'une densité élevée de 198 v/km presentée dans le tableau 5.6, la forte concentration de véhicules améliore significativement la connectivité entre les véhicules, ce qui permet d'atteindre un taux de traçabilité de **93 %**, ce qui était attendu.

Table 5.6 – Évaluation de la traçabilité des messages V2X pour une densité de 198 v/km

Fréquence de recherche d'un groupe (s)	Fréquence d'annonce d'un groupe (s)	Durée de la fenêtre de mesure (s)	Nombre de groupes	Nombre de véhicules par groupe	Nombre de copies par blockchain reçues	Durée pour rejoindre un groupe (s)	Durée d'un groupe avec blockchain inactive (s)	Nombre de messages échangés	Nombre de messages non tracés	Pourcentage de traçabilité
Taille minimale de groupe actif = 3										
1.5	**1**	553	40	26	14	35.5	3.2	1 806 651	126 461	93%
0.5	**0.75**	490	44	26.7	14	50	4	1 600 830	176 098	89%

Cependant, cette amélioration est rapidement limitée par la saturation du canal de communication. Lorsque les fréquences de recherche et d'annonce sont élevées, respectivement à 0.75 s et 0.5 s, le nombre de transmissions simultanées devient très important, ce qui entraîne une augmentation des collisions [120]. Même pour des fréquences plus faibles, telles que 1.5 s et 1 s, le délai de jonction reste relativement élevé, en raison des pertes de messages causées par ces collisions.

L'analyse avec une taille minimale de groupe actif de 2 véhicules a été limitée au scénario de faible densité 25 v/km, où les groupes peinent à atteindre 3 membres, engendrant des phases d'inactivité prolongées pouvant atteindre 9.2 s, ce qui pénalise la traçabilité. Pour les densités moyennes et élevées 102 v/km et 198 v/km, une telle analyse n'a pas été retenue car les groupes atteignent déjà de manière quasi systématique le seuil de 3 véhicules, avec des durées d'inactivité faibles, de l'ordre de 3.5 s et 3.2 s respectivement. Dans ces conditions, abaisser le seuil à 2 véhicules n'apporterait pas de gain significatif en termes de traçabilité. Au contraire, cela pourrait fragiliser la robustesse du système d'audit en réduisant

la redondance des enregistrements et la diversité des validateurs au sein des groupes. Le seuil de 3 véhicules constitue ainsi un compromis pertinent entre disponibilité et robustesse pour les scénarios de densité moyenne et élevée.

5.3.2 Durée de vie des blockchains locales

La durée de vie moyenne des blockchains locales, illustrée dans la Figure 5.5, augmente significativement avec la densité véhiculaire, passant de 130.9 ms pour une densité de 25 v/km à 424.7 ms pour une densité de 198 v/km. Cette évolution s'explique principalement par la diminution de la vitesse des véhicules lorsque la densité augmente, ce qui prolonge leur temps de présence dans la zone V2V et renforce la stabilité des groupes formés. Par conséquent, les véhicules restent plus longtemps à portée de communication les uns des autres.

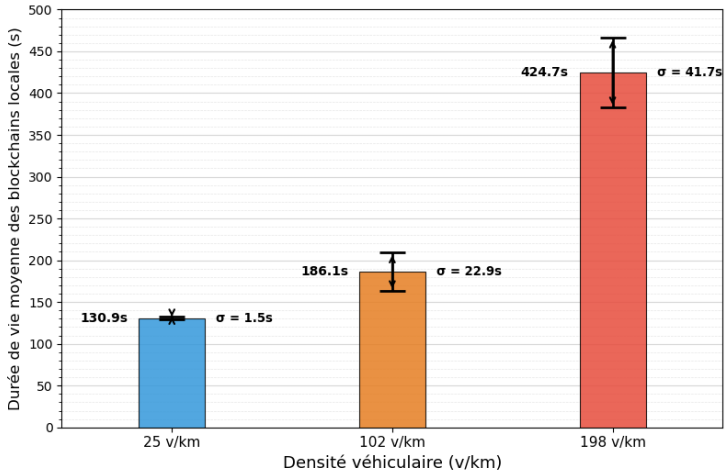

Figure 5.5 – Durée de vie moyenne des blockchains locales en fonction de la densité véhiculaire

5.3.3 Délai de bout en bout d'enregistrement d'un message

Le délai de bout en bout nécessaire pour qu'un message V2X soit enregistré et rendu disponible dans la blockchain correspond à la somme du délai de transmission, intégrant la propagation physique du signal ainsi que l'accès au médium IEEE 802.11p, et de la latence induite par le mécanisme d'enregistrement blockchain. Comme illustré à la Figure 5.6, le délai de transmission reste très faible et quasi constant, de l'ordre de 0.24 à 0.26 ms selon la densité véhiculaire, traduisant une légère augmentation de la contention au niveau du canal MAC à mesure que le nombre de véhicules augmente.

En revanche, la latence blockchain est significativement plus élevée, variant entre 1050 ms et 1100 ms, en raison des opérations de traitement, notamment le hachage, la signature et le minage des blocs, inhérentes au processus d'écriture. Par conséquent, le délai global d'enregistrement est largement dominé par la latence blockchain, qui représente plus de 99,97 % du délai total.

Cette différence d'échelle met en évidence que, dans le système proposé, le facteur limitant n'est pas la communication, mais le processus de traitement et d'enregistrement dans la blockchain. Toutefois, dans le cadre d'un système d'audit forensique, ce délai ne constitue pas une

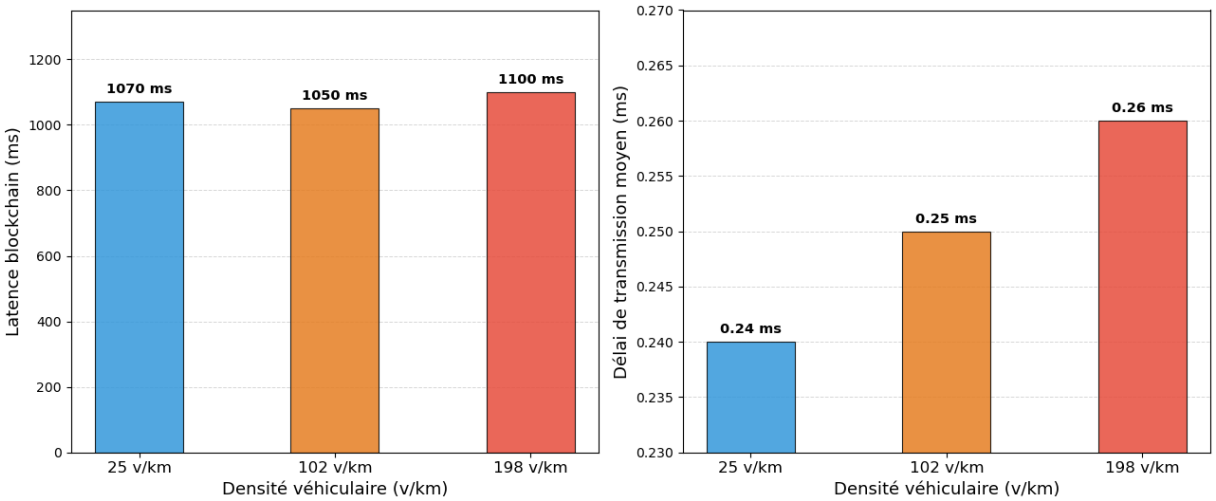

Figure 5.6 – Latence de la blockchain et délai de transmission radio en fonction de la densité véhiculaire

contrainte opérationnelle critique. En effet, l'objectif n'est pas la disponibilité instantanée des messages, comme dans les systèmes de sécurité active, mais leur traçabilité fiable a posteriori. Le délai introduit par la blockchain permet ainsi de garantir l'intégrité, l'immutabilité et la persistance des données, fournissant une trace fiable et exploitable lors d'analyses ou d'investigations ultérieures.

Conclusion

L'évaluation des différentes métriques met en évidence l'impact des paramètres de formation des groupes et de la latence blockchain sur les performances du système d'audit proposé. Les résultats montrent que la traçabilité des messages V2X dépend de la dynamique de formation des groupes, en particulier de la fréquence des échanges de contrôle et de la taille minimale des groupes actifs. Ces résultats montrent que l'approche est bien adaptée aux environnements sans infrastructure dynamiques, où la topologie du réseau évolue continuellement en fonction de la mobilité des véhicules.

Dans les environnements à faible densité, la principale limitation réside dans la difficulté à former des groupes actifs, ce qui engendre des phases d'inactivité et une perte de traçabilité. À l'inverse, dans les environnements à forte densité, la formation des groupes est facilitée, mais les performances peuvent être dégradées par la saturation du canal de communication, due à l'augmentation des collisions.

Par ailleurs, l'analyse du délai de bout en bout montre que la latence blockchain domine largement le délai global d'enregistrement des messages, tandis que le délai de transmission reste négligeable en comparaison. Toutefois, dans le cadre d'un système d'audit, ce délai constitue un compromis acceptable, car il permet de garantir l'intégrité, l'immutabilité et la persistance des données.

Conclusion et perspectives générales

6

6.1 Conclusion générale 87
6.2 Perspectives et travaux futurs 88

6.1 Conclusion générale

Les communications V2X constituent un élément central dans l'évolution des systèmes de transport intelligents. Elles permettent l'échange continu d'informations critiques entre les véhicules, les éléments d'infrastructure et les différents usagers de la route afin d'améliorer la sécurité routière, d'optimiser la gestion du trafic et de soutenir le développement de la conduite coopérative et autonome. Toutefois, l'efficacité de ces systèmes dépend fortement de la confiance accordée aux messages échangés. Assurer simultanément l'authentification des entités, la protection de la vie privée et la traçabilité des communications demeure un défi majeur, en particulier dans les environnements sans infrastructure où les véhicules évoluent dans des réseaux ad hoc dynamiques et intermittents.

Dans ce contexte, cette thèse s'est attachée à concevoir une architecture d'audit décentralisée permettant d'assurer la traçabilité et la fiabilité des communications V2X dans les environnements dépourvus d'infrastructure fixe. L'approche proposée s'appuie sur l'intégration de mécanismes d'authentification robustes et sur l'utilisation de la technologie blockchain afin de garantir l'enregistrement infalsifiable des communications échangées entre les véhicules.

Dans un premier temps, une analyse approfondie de l'état de l'art des mécanismes d'identification, d'authentification et de préservation de la vie privée dans les communications V2X a été menée. Cette étude a permis d'établir une taxonomie structurée des différentes familles de protocoles d'authentification et d'évaluer leur capacité à répondre aux exigences d'un système d'audit. L'analyse qualitative et quantitative des protocoles existants a montré que les approches basées sur une infrastructure à clés publiques utilisant des pseudonymes constituent le compromis le plus pertinent entre sécurité, anonymat conditionnel et responsabilité des entités communicantes.

Dans un second temps, nous nous sommes intéressés à la problématique de la fiabilité de l'authentification dans les environnements V2V sans infrastructure. Pour cela, un modèle analytique basé sur la loi de Poisson a été développé afin d'évaluer la probabilité de succès de l'authentification en fonction de plusieurs paramètres critiques, notamment la durée de vie des certificats, le taux de révocation et la fraîcheur des bases de données d'authentification. Les résultats obtenus ont montré que la dégradation de la probabilité d'authentification dépend fortement de la disponibilité et de la mise à jour des données d'authentification. Elle chute en dessous de 75% après 30 heures de déconnexion avec des certificats de longue durée, tandis que le mécanisme de synchronisation opportuniste pair-à-pair proposé permet de la maintenir au-dessus de 90% dans les scénarios autoroutiers, même avec des certificats de courte durée. Les évaluations menées sur différents scénarios de mobilité ont montré que ce mécanisme permet d'améliorer significativement la probabilité d'authentification, en particulier dans les segments routiers de grande longueur où l'accès à l'infrastructure est limité.

La contribution principale de cette thèse réside dans la conception d'une architecture d'audit décentralisée basée sur la blockchain pour les communications V2X, y compris dans un contexte sans infrastructure. Dans cette architecture, chaque véhicule maintient une blockchain locale dans laquelle sont enregistrés les messages échangés lors des communications V2V. Lors du rétablissement de la connectivité avec l'infrastructure, ces blockchains locales peuvent être fusionnées et synchronisées avec une blockchain globale afin de garantir la cohérence et la complétude du registre d'audit.

L'évaluation des performances de cette architecture a permis d'analyser l'impact de différentes stratégies de minage sur les performances du système. Les résultats ont montré que la stratégie basée sur la taille des blocs permet d'améliorer significativement les performances par rapport à une stratégie basée sur une périodicité fixe. À volume de trafic équivalent, cette approche permet de réduire la latence d'enregistrement des transactions, passant de plusieurs dizaines de secondes à seulement quelques secondes, tout en augmentant le nombre de messages effectivement confirmés dans la blockchain. Les analyses ont également montré que le nombre de transactions par bloc influence directement la latence moyenne du système, le débit de la blockchain et le taux de confirmation des messages.

Afin d'évaluer le comportement du système dans des conditions plus réalistes, les paramètres de la blockchain, notamment le temps nécessaire à l'enregistrement et à la confirmation des messages, ont été intégrés dans une simulation complète de réseau véhiculaire sous VEINS/OMNeT++.

Afin d'évaluer le comportement du système dans des conditions plus réalistes, les paramètres de la blockchain, notamment le temps nécessaire à l'enregistrement et à la confirmation des messages, ont été intégrés dans une simulation complète de réseau véhiculaire sous VEINS/OMNeT++. Les résultats obtenus pour trois scénarios de densité véhiculaire montrent que pour une densité faible de 25 v/km, le taux de traçabilité atteint 89% avec un seuil minimal de 3 membres par blockchain active et 95% avec un seuil minimal de 2 membres, confirmant l'intérêt de réduire ce seuil en environnement peu dense. Pour les densités moyenne et élevée, les taux de traçabilité atteignent respectivement 91% à 102 v/km et 93% à 198 v/km.

Dans l'ensemble, les résultats obtenus dans cette thèse démontrent la faisabilité d'un système d'audit distribué basé sur la blockchain capable d'assurer la traçabilité, l'intégrité et la non-répudiation des communications V2X, même dans des environnements caractérisés par l'absence d'infrastructure et par une forte mobilité des nœuds. Les contributions proposées constituent ainsi une étape importante vers la conception de systèmes de transport intelligents plus sécurisés, transparents et résilients.

6.2 Perspectives et travaux futurs

Bien que les résultats obtenus dans cette thèse démontrent la pertinence et la faisabilité de l'architecture d'audit proposée pour les communications V2X sans infrastructure, plusieurs pistes de recherche peuvent être envisagées afin d'enrichir et d'étendre ces travaux.

Une première piste d'amélioration consisterait à enregistrer les messages V2X durant les phases d'inactivité des groupes, afin de réduire la perte de messages dans les scénarios de faible densité. Toutefois, cette approche reste limitée par l'absence de validation collective, ce qui peut remettre en cause la fiabilité des données enregistrées.

Dans cette continuité, une autre direction de recherche concerne la gestion de la fusion des blockchains locales maintenues par les véhicules en mode sans infrastructure. Dans les environnements véhiculaires caractérisés par une forte mobilité et une connectivité intermittente, plusieurs chaînes locales peuvent être générées simultanément par différents groupes de véhicules. Lors de la reconnexion à l'infrastructure, ces copies de blockchains locales doivent être transmises à une autorité de confiance afin d'être fusionnées de manière cohérente dans la blockchain globale. Ce processus doit garantir l'intégrité, la continuité et la cohérence du registre d'audit.

Dans ce contexte, il devient nécessaire de concevoir des mécanismes de fusion capables de gérer les divergences entre chaînes concurrentes, d'identifier les transactions valides et d'assurer une synchronisation fiable entre les blockchains locales et la blockchain globale. Ces mécanismes devront notamment prendre en compte les situations de conflits entre blocs, les duplications éventuelles de transactions ainsi que les incohérences pouvant apparaître lors de la fusion des registres distribués.

Une seconde perspective concerne l'étude approfondie de la résilience du système face aux attaques de sécurité susceptibles de compromettre l'intégrité ou la fiabilité des communications V2X. Parmi les menaces les plus critiques figurent notamment les attaques Sybil, dans lesquelles un véhicule malveillant emprunte plusieurs identités afin d'influencer le réseau, les attaques par rejeu consistant à retransmettre d'anciens messages afin de perturber le trafic, ou encore les attaques de partition du réseau visant à isoler certains groupes de véhicules.

Dans cette optique, l'intégration de mécanismes avancés de détection et de mitigation de ces attaques constitue ainsi une étape essentielle pour renforcer la robustesse du système d'audit proposé. Des solutions combinant des techniques cryptographiques, des mécanismes de réputation ou des approches basées sur l'analyse du comportement des nœuds pourraient être étudiées afin d'identifier et de neutraliser les entités malveillantes au sein du réseau véhiculaire.

En complément, une autre perspective prometteuse consiste à intégrer des techniques d'intelligence artificielle et d'apprentissage automatique afin d'améliorer la capacité du système à détecter des comportements anormaux dans les communications V2X. L'analyse des traces enregistrées dans la blockchain pourrait permettre d'identifier des schémas de communication suspects révélateurs d'activités malveillantes ou de dysfonctionnements du système.

Par exemple, des modèles d'apprentissage supervisé ou non supervisé pourraient être entraînés à partir des historiques de communication afin de détecter automatiquement des anomalies telles que des messages incohérents, des fréquences d'émission anormales ou des comportements de diffusion atypiques. L'intégration de ces mécanismes d'analyse intelligente permettrait ainsi de renforcer les capacités d'audit et de surveillance du réseau.

Enfin, dans cette même perspective, une approche basée sur l'apprentissage automatique pourrait également être utilisée pour mettre en place un mécanisme intelligent de filtrage des messages V2X. Dans les

réseaux véhiculaires, les véhicules génèrent un volume très important de messages, dont une grande partie peut être répétitive ou redondante. Un système de classification basé sur le machine learning pourrait permettre d'identifier les messages critiques, tels que les alertes d'accident, les freinages brusques ou les événements dangereux, qui doivent être enregistrés dans la blockchain, tandis que les messages moins pertinents pourraient être agrégés, filtrés ou stockés de manière alternative. Une telle approche permettrait d'optimiser l'utilisation des ressources de stockage et d'améliorer la scalabilité du système d'audit.

Bibliographie

[1] Sandro Chiocchio et al. « Integrated Simulation Environments for Vehicular Communications in Cooperative Road Transportation Systems ». In : *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*. 2018, p. 1-4. doi : 10.23919/URSI-AT-RASC.2018.8471321 (cf. p. 1).

[2] Xinyu Zhang et al. « Vehicle-to-Everything Communication in Intelligent Connected Vehicles : A Survey and Taxonomy ». In : *Automotive Innovation* 8.1 (2025), p. 13-45. doi : 10.1007/s42154-024-00310-2 (cf. p. 1).

[3] Falk Dettinger et al. *A Survey on Performance, Current and Future Usage of Vehicle-To-Everything Communication Standards*. 2024. url : https://arxiv.org/abs/2410.10264 (cf. p. 2).

[4] Benedikt Brecht et al. « A Security Credential Management System for V2X Communications ». In : *IEEE Transactions on Intelligent Transportation Systems* 19.12 (2018), p. 3850-3871. doi : 10.1109/TITS.2018.2797529 (cf. p. 2, 51, 52, 61-63).

[5] R. Lu et al. « ECPP : Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications ». In : *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*. 2008, p. 1229-1237. doi : 10.1109/INFOCOM.2008.179 (cf. p. 2, 13, 14, 21, 40, 41).

[6] Teodora Mecheva et Nikolay Kakanakov. « Cloud based Intelligent Transportation System architecture ». In : *2021 International Conference Automatics and Informatics (ICAI)*. 2021, p. 385-388. doi : 10.1109/ICAI52893.2021.9639678 (cf. p. 2).

[7] Tianqi Wang et al. *DeepAccident : A Motion and Accident Prediction Benchmark for V2X Autonomous Driving*. 2023. url : https://arxiv.org/abs/2304.01168 (cf. p. 3).

[8] Bruno Ribeiro, Maria Nicolau et Alexandre Santos. « Machine Learning for VRUs accidents prediction using V2X data ». In : juin 2023, p. 1789-1791. doi : 10.1145/3555776.3578263 (cf. p. 3).

[9] Hossam M. Zohir et al. « Advancements in Accident-Aware Traffic Management : A Comprehensive Review of V2X-Based Route Optimization ». In : *Scientific Reports* 15.1 (2025), p. 35041. doi : 10.1038/s41598-025-20878-x (cf. p. 4).

[10] Seo-Wook Park, Raynier Suresh et Anusha Ailuri. « Collision Avoidance System at Urban Intersections Using V2X Communication ». In : *WCX SAE World Congress Experience*. SAE International, avr. 2025. doi : https://doi.org/10.4271/2025-01-8030 (cf. p. 5).

[11] Muhammad Sameer Sheikh, Jun Liang et Wensong Wang. « A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs) ». In : *Sensors* 19.16 (août 2019), p. 3589. doi : 10.3390/s19163589 (cf. p. 5).

[12] Souad BelMannoubi et al. « A comprehensive survey on blockchain-based C-ITS applications : Classification, challenges, and open issues ». In : *Vehicular Communications* 43 (2023), p. 100607. doi : https://doi.org/10.1016/j.vehcom.2023.100607 (cf. p. 6).

[13] Panagiotis Papadimitratos et al. « Secure vehicular communication systems : design and architecture ». In : *IEEE Communications Magazine* 46.11 (2008), p. 100-109. doi : 10.1109/MCOM.2008.4689252 (cf. p. 9).

[14] Chaima Zidi et al. « Review and Perspectives on the Audit of Vehicle-to-Everything Communications ». In : *IEEE Access* 11 (2023), p. 81623-81645. doi : 10.1109/ACCESS.2023.3301182 (cf. p. 10, 16, 27).

[15] Edmond-Marc Lipiansky. « L'identité dans la communication ». In : *Communication & Langages* 97.1 (1993), p. 31-37. doi : 10.3406/colan.1993.2452 (cf. p. 11).

[16] Patrick Charaudeau. « La communication et le droit à la parole dans une interaction du même et de l'autre ». In : *Communication & Langages* (1991), p. 27-47. doi : 10.4000/praxematique.3123 (cf. p. 11).

[17] Marcel Burger. « Vers une analyse de la construction des identités dans les discours de communication publique ». In : *Cahiers du Centre de Linguistique et des Sciences du Langage* 34 (déc. 2013), p. 101-122. doi : 10.26034/la.cdclsl.2014.785 (cf. p. 11).

[18] Jin Wang et Peixin Liu. « Traffic prediction with deep learning for vehicular communication network ». In : *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*. Sous la dir. de Miroslava Mikusova. T. 12460. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series. Déc. 2022, 124603E, 124603E. doi : 10.1117/12.2658695 (cf. p. 11).

[19] S Suganya et Shanmuganathan Chandrasekaran. « Key Management of Vehicular Ad-Hoc Network with Eliminating Scheme ». In : (oct. 2019) (cf. p. 12).

[20] Florian Schaub, Zhendong Ma et Frank Kargl. « Privacy Requirements in Vehicular Communication Systems ». In : *2009 International Conference on Computational Science and Engineering* 3 (2009), p. 139-145 (cf. p. 12, 15).

[21] A. F. M. Suaib Akhter et al. « A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET ». In : *Sustainability* 13.1 (2021). doi : 10.3390/su13010400 (cf. p. 13, 14, 22-24, 39-42).

[22] Lei Xu & Feng Gao Shi Kexin Liehuang Zhu Can Zhang. « Blockchain-based multimedia sharing in vehicular social networks with privacy protection ». In : *Multimedia Tools and Applications* (2020), p. 1573-7721. doi : 10.1007/s11042-019-08284-8 (cf. p. 13).

[23] Anusha Vangala et al. « Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems ». In : *IEEE Sensors Journal* 21.14 (2021), p. 15824-15838. doi : 10.1109/JSEN.2020.3009382 (cf. p. 13, 14, 23, 40, 41).

[24] Lun Li et al. « CreditCoin : A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles ». In : *IEEE Transactions on Intelligent Transportation Systems* 19.7 (2018), p. 2204-2220. doi : 10.1109/TITS.2017.2777990 (cf. p. 13).

[25] Udit Bansal et al. « ID-CEPPA : Identity-based Computationally Efficient Privacy-Preserving Authentication scheme for vehicle-to-vehicle communications ». In : *Journal of Systems Architecture* 123 (2022), p. 102387. doi : https://doi.org/10.1016/j.sysarc.2021.102387 (cf. p. 13, 18, 19, 21, 34, 35, 40, 41).

[26] Sharqa Hameed et al. « Sharing Mechanism of Intelligent Vehicles Trust Points based on Blockchain for Vehicular Networks ». In : *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*. 2020, p. 1-6. doi : 10.1109/AECT47998.2020.9194208 (cf. p. 13, 22, 23, 39-41).

[27] Jean-Pierre Raya Maxim ; Hubaux. « Securing vehicular ad hoc networks ». In : *Journal of Computer Security* 15 (2007), p. 39-68. doi : 10.1109/TITS.2020.2983466 (cf. p. 13, 14, 21, 40).

[28] Chao Lin et al. « BCPPA : A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks ». In : *IEEE Transactions on Intelligent Transportation Systems* 22.12 (2021), p. 7408-7420. doi : 10.1109/TITS.2020.3002096 (cf. p. 13, 14, 21-23, 40-42).

[29] Jing Zhang et al. « CVAR : Distributed and Extensible Cross-Region Vehicle Authentication With Reputation for VANETs ». In : *IEEE Transactions on Intelligent Transportation Systems* (2023), p. 1-16. doi : 10.1109/TITS.2023.3306547 (cf. p. 13, 14, 40, 41).

[30] Righa Tandon, Ajay Verma et Pradeep Gupta. « D-Blac : A Dual Blockchain-Based Decentralized Scheme for Authentication and Communication in Vanet ». In : *SSRN Electronic Journal* (jan. 2022). doi : 10.2139/ssrn.4240501 (cf. p. 13, 14, 18, 40, 41).

[31] Qianmin Du, Jianhong Zhou et Maode Ma. « EAIA : An Efficient and Anonymous Identity-Authentication Scheme in 5G-V2V ». In : *Sensors* 24.16 (2024), p. 5376. doi : 10.3390/s24165376 (cf. p. 14, 34, 35, 40, 41).

[32] Sujash Naskar et al. « Pseudo-Random Identification and Efficient Privacy-Preserving V2X Communication for IoV Networks ». In : *IEEE Access* 13 (2025), p. 1147-1163. doi : 10.1109/ACCESS.2024.3523358 (cf. p. 14, 34, 35, 40, 41).

[33] Benoît Pigé. *Audit et contrôle interne*. Jan. 2017 (cf. p. 16).

[34] International Organization for Standardization. *Road vehicles – Cybersecurity engineering*. Published by ISO/SAE International. ISO/SAE, 2021 (cf. p. 16, 42).

[35] Tejasvi Alladi et al. « A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks ». In : *IEEE Communications Surveys & Tutorials* 24.2 (2022), p. 1212-1239. doi : 10.1109/COMST.2022.3160925 (cf. p. 16).

[36] Avleen Kaur Malhi, Shalini Batra et Husanbir Singh Pannu. « Security of vehicular ad-hoc networks : A comprehensive survey ». In : *Computers & Security* 89 (2020), p. 101664. doi : https://doi.org/10.1016/j.cose.2019.101664 (cf. p. 16).

[37] Fei Wang et al. « 2FLIP : A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET ». In : *IEEE Transactions on Vehicular Technology* 65.2 (2016), p. 896-911. doi : 10.1109/TVT.2015.2402166 (cf. p. 18).

[38] SK Hafizul Islam et al. « A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs ». In : *Future Generation Computer Systems* 84 (2018), p. 216-227. DOI : https://doi.org/10.1016/j.future.2017.07.002 (cf. p. 18, 40, 41).

[39] Gopal Singh Rawat et al. « A lightweight authentication scheme with privacy preservation for vehicular networks ». In : *Computers and Electrical Engineering* 100 (2022), p. 108016. DOI : https://doi.org/10.1016/j.compeleceng.2022.108016 (cf. p. 18, 19, 21, 22, 38, 40, 41).

[40] C. Zhang et al. « An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks ». In : *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*. 2008, p. 246-250. DOI : 10.1109/INFOCOM.2008.58 (cf. p. 19, 39-41).

[41] Pandurang Kamat, Arati Baliga et Wade Trappe. « An Identity-based Security Framework For VANETs ». In : *VANET '06 : Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks*. ACM, sept. 2006, p. 94-95. DOI : 10.1145/1161064.1161083 (cf. p. 19).

[42] Qinglei Kong, Le Su et Maode Ma. « Achieving Privacy-Preserving and Verifiable Data Sharing in Vehicular Fog With Blockchain ». In : *IEEE Transactions on Intelligent Transportation Systems* 22.8 (2021), p. 4889-4898. DOI : 10.1109/TITS.2020.2983466 (cf. p. 19, 40, 41).

[43] Jingru Fang et al. « A Threshold Group Signature Authentication Scheme for VANETs ». In : *The 2nd International Conference on Computing and Data Science*. CONF-CDS 2021. Stanford, CA, USA : Association for Computing Machinery, 2021. DOI : 10.1145/3448734.3450830 (cf. p. 20, 25, 40, 41).

[44] Yanji Jiang, Shaocheng Ge et Xueli Shen. « AAAS : An Anonymous Authentication Scheme Based on Group Signature in VANETs ». In : *IEEE Access* 8 (2020), p. 98986-98998. DOI : 10.1109/ACCESS.2020.2997840 (cf. p. 20, 40, 41).

[45] Yanfei Lu et al. « Group Signature Authentication Scheme with Credit Evaluation Mechanism in VANET ». In : *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. 2023, p. 1703-1709. DOI : 10.1109/CSCWD57460.2023.10152641 (cf. p. 20, 40, 41).

[46] Kiho Lim et al. « SSKM : Scalable and Secure Key Management Scheme for Group Signature Based Authentication and CRL in VANET ». In : *Electronics* 8.11 (2019). DOI : 10.3390/electronics8111330 (cf. p. 20, 40, 41).

[47] M. A. Afzal et M. A. Shah. « PRIVACY-PRESERVING AUTHENTICATION SCHEME FOR VANETS IN DIGITAL ECONOMY ». In : *Competitive Advantage in the Digital Economy (CADE 2021)*. T. 2021. 2021, p. 85-90. DOI : 10.1049/icp.2021.2418 (cf. p. 22).

[48] Sanjeev Kumar Dwivedi et al. « Blockchain-based vehicular ad-hoc networks : A comprehensive survey ». In : *Ad Hoc Networks* 137 (2022), p. 102980. DOI : https://doi.org/10.1016/j.adhoc.2022.102980 (cf. p. 22, 23).

[49] Jaewon Noh, Sangil Jeon et Sunghyun Cho. « Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles ». In : *Electronics* 9.1 (2020). DOI : 10.3390/electronics9010074 (cf. p. 23, 40, 41).

[50] Satoshi Nakamoto. « Bitcoin : A peer-to-peer electronic cash system ». In : (2008) (cf. p. 24).

[51] ISO. *ISO 22739 :2024 Blockchain and distributed ledger technologies — Vocabulary*. International Standard ISO 22739 :2024. International Organization for Standardization, 2024 (cf. p. 24).

[52] Dheerendra Mishra et Purva Rewal. « A blockchain-based quantum-secure protocol for efficient V2I handover authentication in vehicular Ad-Hoc networks ». In : *Peer Peer Netw. Appl.* 18.6 (2025), p. 304. DOI : 10.1007/S12083-025-02142-1 (cf. p. 25).

[53] M Andreas et M Antonopoulos. « Mastering Bitcoin : Programming the Open Blockchain ». In : *O'Reilly Media* (2017) (cf. p. 25).

[54] Shu-Ping Lu, Chin-Laung Lei et Meng-Han Tsai. « An efficient Proof-of-Authority consensus scheme against cloning attacks ». In : *Computer Communications* 228 (2024), p. 107975. DOI : https://doi.org/10.1016/j.comcom.2024.107975 (cf. p. 26).

[55] Naseem Sehar et al. « Blockchain enabled data security in vehicular networks ». In : *Scientific Reports* 13 (mars 2023). DOI : 10.1038/s41598-023-31442-w (cf. p. 26).

[56] Konstantinos Christidis et Michael Devetsikiotis. « Blockchains and Smart Contracts for the Internet of Things ». In : *IEEE Access* 4 (2016), p. 2292-2303. DOI : 10.1109/ACCESS.2016.2566339 (cf. p. 26).

[57] Yves Christian Elloh Adja et al. « A blockchain-based certificate revocation management and status verification system ». In : *Computers & Security* 104 (2021), p. 102209. doi : https://doi.org/10.1016/j.cose.2021.102209 (cf. p. 26).

[58] Gengrui Zhang et al. *V-Guard : An Efficient Permissioned Blockchain for Achieving Consensus under Dynamic Memberships in V2X*. 2023. url : https://arxiv.org/abs/2301.06210 (cf. p. 26, 27).

[59] Yonas Teweldemedhin Gebrezgiher et al. « Machine Learning-Based Blockchain Technology for Secure V2X Communication : Open Challenges and Solutions ». In : *Sensors* 25.15 (2025). doi : 10.3390/s25154793 (cf. p. 26, 28).

[60] Andrei Vladyko et al. « Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications ». In : *Electronics* 11.2 (2022). doi : 10.3390/electronics11020173 (cf. p. 26).

[61] James Meijers et al. « Blockchain for V2X : A Taxonomy of Design Use Cases and System Requirements ». In : *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. 2021, p. 113-120. doi : 10.1109/BRAINS52497.2021.9569796 (cf. p. 27).

[62] ETSI. *IPv6 Security, Cybersecurity, Blockchain*. Group Report ETSI GR IP6 031. Version V1.1.1. Accessed : 2026-03-05. Sophia Antipolis, France : European Telecommunications Standards Institute (ETSI), nov. 2020 (cf. p. 27).

[63] Yi-Ting Sun et al. *A Multi-Layer Blockchain Simulator and Performance Evaluation of Social Internet of Vehicles with Multi-Connectivity Management*. 2024. url : https://arxiv.org/abs/2411.14000 (cf. p. 27).

[64] European Commission. *Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles*. Article R.476 : Event Data Recorder (EDR) obligatoire juillet 2024. Nov. 2019. doi : 10.2862/758668. url : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32019R2144 (cf. p. 28).

[65] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*. Version 2.2.1. European Telecommunications Standards Institute (ETSI), sept. 2022 (cf. p. 29-31, 42, 62, 63, 74).

[66] Diana Magalhaes et al. « A 5G-based Authentication Framework for V2X Communication ». In : *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2023, p. 385-385 (cf. p. 34-36).

[67] Zuobin Ying et al. « A literature review on V2X communications security : Foundation, solutions, status, and future ». In : *IET Communications* 18 (juin 2024), p. 1683-1715. doi : 10.1049/cmu2.12778 (cf. p. 34, 35).

[68] Yaling Zhu et al. « Sybil Attacks Detection and Traceability Mechanism Based on Beacon Packets in Connected Automobile Vehicles ». In : *Sensors* 24.7 (2024). doi : 10.3390/s24072153 (cf. p. 34, 35).

[69] Babajide Asaju. « Addressing Public Key Infrastructure (PKI) Challenges in V2X Networks : Strategies for Scalability, Certificate Management, and Trusted Authorities ». In : 4 (jan. 2024), pp. 33-52. doi : 10.55662/JST.2024.5103 (cf. p. 34, 35).

[70] Gianluca Scopelliti et al. « Efficient and Timely Revocation of V2X Credentials ». In : jan. 2024. doi : 10.14722/ndss.2024.24017 (cf. p. 34, 35, 40, 51, 52).

[71] Ahmed Manasrah et al. « Identity-Based Authentication in VANETs : A Review ». In : *IEEE Transactions on Intelligent Transportation Systems* 26.4 (2025), p. 4260-4282. doi : 10.1109/TITS.2025.3528932 (cf. p. 34, 35).

[72] Jia Liu et al. « A Novel Computationally Efficient Group Signature for Anonymous and Secure V2X Communications ». In : *arXiv* 2307.13759 (2023). arXiv :2307.13759 [cs.CR] (cf. p. 34, 35).

[73] Seema Gaba, Monisha Gupta et Harmanjeet Singh. « A comprehensive survey on VANET security attacks ». In : jan. 2023, p. 020029. doi : 10.1063/5.0145236 (cf. p. 34, 35).

[74] Gianluca Scopelliti et al. « Efficient and timely revocation of v2x credentials ». In : *Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS'24)*. Internet Society. 2023 (cf. p. 34).

[75] Morteza Azmoudeh Afshar et al. *Privacy-Preserving and Simultaneous Authentication in High-Density V2X Networks*. arXiv preprint arXiv :2501.06087. v2. Mai 2025. url : https://doi.org/10.48550/arXiv.2501.06087 (cf. p. 35).

[76] Ahmed Manasrah et al. « Identity-Based Authentication in VANETs : A Review ». In : *IEEE Transactions on Intelligent Transportation Systems* (2025). doi : 10.1109/TITS.2025.3528932 (cf. p. 35).

[77] S. Al-Khalaf, A. Al-Rasheed et R. Khan. « Lightweight Symmetric-Key Authentication Schemes for V2X Communications : Performance and Limitations ». In : *IEEE Access* 12 (2024), p. 12345-12358. DOI : 10.1109/ACCESS.2024.1234567 (cf. p. 36).

[78] Roshan Sedar et al. « A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths ». In : *IEEE Open Journal of the Communications Society* 4 (2023), p. 325-391. DOI : 10.1109/OJCOMS.2023.3239115 (cf. p. 36).

[79] Monowar Hasan et al. « Securing Vehicle-to-Everything (V2X) Communication Platforms ». In : *IEEE Transactions on Intelligent Vehicles* 5.4 (2020), p. 693-713. DOI : 10.1109/TIV.2020.2987430 (cf. p. 36).

[80] Mir Ali Rezazadeh Baee et al. « Authentication Strategies in Vehicular Communications : A Taxonomy and Framework ». In : *EURASIP Journal on Wireless Communications and Networking* 2021 (mai 2021). DOI : 10.1186/s13638-021-01968-6 (cf. p. 36, 39).

[81] Mahmoud A. Shawky et al. « How secure are our roads ? An in-depth review of authentication in vehicular communications ». In : *Vehicular Communications* 47 (2024), p. 100784. DOI : https://doi.org/10.1016/j.vehcom.2024.100784 (cf. p. 37).

[82] Jiaqi Huang et al. « Recent Advances and Challenges in Security and Privacy for V2X Communications ». In : *IEEE Open Journal of Vehicular Technology* 1 (2020), p. 244-266. DOI : 10.1109/OJVT.2020.2999885 (cf. p. 38).

[83] « Blockchain challenges and opportunities : a survey ». In : *Int. J. Web Grid Serv.* 14.4 (jan. 2018), p. 352-375 (cf. p. 39).

[84] Zhuo Ma et al. « An Efficient Decentralized Key Management Mechanism for VANET With Blockchain ». In : *IEEE Transactions on Vehicular Technology* 69.6 (2020), p. 5836-5849. DOI : 10.1109/TVT.2020.2972923 (cf. p. 40, 41).

[85] Anil Kumar Sutrala et al. « On the Design of Conditional Privacy Preserving Batch Verification-Based Authentication Scheme for Internet of Vehicles Deployment ». In : *IEEE Transactions on Vehicular Technology* 69.5 (2020), p. 5535-5548. DOI : 10.1109/TVT.2020.2981934 (cf. p. 40, 41).

[86] Ikram Ali, Tandoh Lawrence et Fagen Li. « An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs ». In : *Journal of Systems Architecture* 103 (2020), p. 101692. DOI : https://doi.org/10.1016/j.sysarc.2019.101692 (cf. p. 40, 41).

[87] Abdelkrim Imghoure, Fouzia Omary et Ahmed El-Yahyaoui. « Hybrid cryptography-based scheme with conditional privacy-preserving authentication and memory-based DOS resilience in V2X ». In : *Vehicular Communications* 49 (2024), p. 100810. DOI : https://doi.org/10.1016/j.vehcom.2024.100810 (cf. p. 40, 41).

[88] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-57 : Recommendation for Key Management*. Rapp. tech. 800-57. Version Part 1 Revision 5. Gaithersburg, MD, USA : National Institute of Standards et Technology, mai 2020 (cf. p. 42).

[89] « IEEE Approved Draft Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages ». In : *IEEE Std 1609.2-2022 (Revision of IEEE Std 1609.2-2016)* (2023), p. 1-349. DOI : 10.1109/IEEESTD.2023.10075082 (cf. p. 42, 51, 52).

[90] Farooque Azam et al. « A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network ». In : *IEEE Access* 9 (2021), p. 31309-31321. DOI : 10.1109/ACCESS.2021.3060046 (cf. p. 43).

[91] Helsinki University Team. « Accountable De-anonymization in V2X Communication ». In : *Vehicular Communication Journal* (2023) (cf. p. 51, 52).

[92] *C2C-CC (Car2Car Communication Consortium) Security Standards*. Car2Car Communication Consortium, 2019 (cf. p. 51, 52).

[93] A. Haidar. « Validation Platform for Secure V2X Communications ». In : *PhD Thesis, Politecnico di Torino* (2020) (cf. p. 51, 52).

[94] J. Smith et A. Doe. « Post-quantum Impacts on V2X Certificates ». In : *IEEE Vehicular Communications* (2023) (cf. p. 51, 52).

[95] *ETSI ITS-G5 - European ITS Communication Standards*. European Telecommunications Standards Institute, 2016 (cf. p. 51, 52).

[96] T. Wang et Y. Lee. « Survey on Certificate Revocation Schemes ». In : *IEEE Access* (2020) (cf. p. 51, 52).

[97] M. A. Simplicio et C. B. Margi. « Revocation in Vehicular Public Key Infrastructures ». In : *Vehicular Networking Conference* (2021) (cf. p. 51, 52, 62, 63).

[98] *IEEE 802.11p - Wireless Access in Vehicular Environments*. IEEE Standards Association, 2010 (cf. p. 51, 52, 74, 76).

[99] *ETSI TS 103 097 - Intelligent Transport Systems (ITS) ; Security ; Security header and certificate formats*. European Telecommunications Standards Institute (ETSI), 2016 (cf. p. 51, 52, 74).

[100] SAE International. *V2X Communications Message Set Dictionary (DSRC Message Set Dictionary)*. SAE International, 2020 (cf. p. 61).

[101] ETSI. *Intelligent Transport Systems (ITS) ; Vehicular Communications ; Basic Set of Applications ; Part 2 : Specification of Cooperative Awareness Basic Service (CAM)*. European Telecommunications Standards Institute, 2019 (cf. p. 61).

[102] Giovanni Rigazzi et al. « Optimized Certificate Revocation List Distribution for Secure V2X Communications ». In : *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. 2017, p. 1-7. doi : 10.1109/VTCFall.2017.8288287 (cf. p. 62, 63).

[103] Gianluca Scopelliti et al. « Efficient and timely revocation of v2x credentials ». In : *Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS'24)*. Internet Society. 2024 (cf. p. 62, 63).

[104] Joseph Kamel et al. « Misbehavior Detection in C-ITS : A comparative approach of local detection mechanisms ». In : *2019 IEEE Vehicular Networking Conference (VNC)*. 2019, p. 1-8. doi : 10.1109/VNC48660.2019.9062831 (cf. p. 62, 63).

[105] Masoud Naderpour et al. « Auditable De-Anonymization in V2X Communication ». In : *Journal of ICT Standardization* 5.1 (2017), p. 91-106. doi : 10.13052/jicts2245-800X.515 (cf. p. 62, 63).

[106] Abin Oommen Philip et RA.K. Saravanaguru. « Multisource traffic incident reporting and evidence management in Internet of Vehicles using machine learning and blockchain ». In : *Engineering Applications of Artificial Intelligence* 117 (2023), p. 105630. doi : https://doi.org/10.1016/j.engappai.2022.105630 (cf. p. 62, 63).

[107] Maximilian Bauder et al. « Influences of Vehicle Communication on Human Driving Reactions : A Simulator Study on Reaction Times and Behavior for Forensic Accident Analysis ». In : *Sensors* 24.14 (2024). doi : 10.3390/s24144481 (cf. p. 62, 63).

[108] Abdelwahab Boualouache et Thomas Engel. « A Survey on Machine learning-based misbehavior detection systems for 5G and beyond vehicular networks ». In : *IEEE Communications Surveys and Tutorials* 25.2 (2023). doi : 10.1109/COMST.2023.3236448 (cf. p. 63).

[109] Marcos A. Simplicio et al. « Privacy-Preserving Certificate Linkage/Revocation in VANETs Without Linkage Authorities ». In : *IEEE Transactions on Intelligent Transportation Systems* 22.6 (2021), p. 3326-3336. doi : 10.1109/TITS.2020.2981907 (cf. p. 64).

[110] Marwa Slimene et al. « An enhanced authentication solution for infrastructureless vehicle environments ». In : *2025 21th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. Marrakech, Morocco, 2025 (cf. p. 66).

[111] ETSI. *TS 102 894-2 V1.2.1*. Rapp. tech. European Telecommunications Standards Institute, 2014 (cf. p. 67).

[112] Christoph Sommer, Reinhard German et Falko Dressler. « Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis ». In : *IEEE Transactions on Mobile Computing* 10.1 (2011), p. 3-15. doi : 10.1109/TMC.2010.133 (cf. p. 73).

[113] Y. Dai et al. « Modeling and analyzing V2V communication limitations impacts on connected and automated vehicle platoons ». In : *PLOS ONE* 20.8 (2025), e0328555. doi : 10.1371/journal.pone.0328555 (cf. p. 73).

[114] Mohamed Nidhal Mejri, Jalel Ben-Othman et Mohamed Hamdi. « Survey on VANET security challenges and possible cryptographic solutions ». In : *Vehicular Communications* 1.2 (2014), p. 53-66. doi : https://doi.org/10.1016/j.vehcom.2014.05.001 (cf. p. 74).

[115] Fan Bai et al. « Towards characterising and classifying communication-based automotive applications from a wireless networking perspective ». In : *Int. J. of Vehicle Autonomous Systems* 10 (jan. 2012), p. 165-197. doi : 10.1504/IJVAS.2012.051267 (cf. p. 74).

[116] Angélica Reyes et al. « Vehicle density in VANET applications ». In : *Journal of Ambient Intelligence and Smart Environments* 6.4 (2014), p. 469-481. doi : 10.3233/AIS-140271 (cf. p. 74).

[117] ETSI. *Intelligent Transport Systems (ITS) ; Security ; ITS communications security architecture and security management*. Rapp. tech. ETSI TS 102 940 V1.3.1. European Telecommunications Standards Institute, 2018 (cf. p. 74).

[118] ETSI. *EN 302 663 V1.3.1 : ITS-G5 Access layer specification*. Rapp. tech. European Telecommunications Standards Institute, 2020 (cf. p. 77).

[119] Lucas Rivoirard. « Modèle d'auto-organisation pour les protocoles de routage dans les réseaux ad hoc de véhicules : application à la perception élargie et à la localisation coopératives ». Theses. Université de Lille, sept. 2018 (cf. p. 81).

[120] Pierpaolo Salvo et al. « Investigating VANET dissemination protocols performance under high throughput conditions ». In : *Vehicular Communications* 2.4 (2015), p. 185-194. doi : https://doi.org/10.1016/j.vehcom.2015.07.003 (cf. p. 83, 84).