**République Algérienne Démocratique et Populaire**
**Ministére de lEnseignement Supérieur et de la Recherche Scientifique**
**Université A. Mira de Béjaïa**
**Faculté des Sciences Exactes**
**Département dInformatique**


# Mémoire de Fin de cycle

**En vue de lobtention du diplôme de Master Recherche en Informatique**

**Option :**

**Réseaux et Sécurité**

**Thème**

## Maintien de la stabilité du platooning pour la sûreté et l'efficacité du trafic

Réalisé par :

MESSAOUDI Mounir
SAHKI Ghilas

Devant le jury composé de :

| | | | | |
|---|---|---|---|---|
| **Président :** | Dr. BOUADEM | Nassima | M.C.B | U.A.M Béjaïa |
| **Encadrante :** | Dr. ZAMOUCHE | Djamila | M.C.B | U.A.M Béjaïa |
| **Examinatrice :** | Dr. OUYAHIA | Samira | M.C.B | U.A.M Béjaïa |
| **Examinatrice :** | Pr BOUALLOUCHE | Louiza | Professeur | U.A.M Béjaïa |
| **Examinateur :** | Dr. SADI | Mustapha | M.C.B | U.A.M Béjaïa |

Promotion 2024 – 2025

# Remerciements

NOUS rendons grâce à notre Dieu, le Tout-Puissant et Miséricordieux, pour nous avoir donné le courage, la patience et la persévérance nécessaires à l'accomplissement de ce travail.

CEST avec une profonde gratitude que nous remercions notre encadrante, **Madame ZAMOUCHE Djamila**, pour ses précieux conseils, sa patience et son suivi attentif tout au long de la réalisation de ce mémoire. Son accompagnement rigoureux et bienveillant a été déterminant dans toutes les phases de ce travail.

NOTRE reconnaissance sadresse également aux membres du jury pour lhonneur quils nous font en acceptant dévaluer ce mémoire et pour lintérêt quils y ont porté.

TOUTE notre estime va aux enseignants et aux personnels administratifs du **département dInformatique de lUniversité Abderrahmane Mira de Béjaïa**, pour la qualité de leur encadrement, leur disponibilité et leur accompagnement tout au long de notre parcours académique.

UNE pensée particulière va à toutes les personnes, proches ou moins proches, qui nous ont soutenus, encouragés ou aidés, de quelque manière que ce soit, dans la concrétisation de ce travail.

# Dédicace

**On dédie ce travail**

À nos parents, pour leur amour et leurs sacrifices,

à nos frères et surs, pour leur soutien constant,

et à nos amis (les Hmida), pour leur présence et leurs

encouragements.

**Ghilas et Mounir**

# Table des Matières

# Table des figures

# Liste des tableaux

# Liste des Abréviations

| | |
|---|---|
| **ACC** | Adaptive Cruise Control |
| **AD** | Autonomous Driving |
| **AEB** | Autonomous Emergency Braking |
| **AMF** | Access and Mobility Management Function |
| **ARPF** | Authentication Credential Repository and Processing Function |
| **AUSF** | Authentication Server Function |
| **CACC** | Cooperative Adaptive Cruise Control |
| **CAN** | Controller Area Network |
| **$CO_2$** | Dioxyde de carbone |
| **CSK** | Color Shift Keying |
| **DoS** | Denial of Service |
| **ECC** | Elliptic Curve Cryptography |
| **ECU** | Electronic Control Unit |
| **GUTI** | Globally Unique Temporary Identifier |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **ITS** | Intelligent Transportation System |
| **LIN** | Local Interconnect Network |
| **LKA** | Lane Keeping Assist |
| **LWE** | Learning With Errors |
| **OBU** | On Board Unit |
| **RSU** | Road Side Unit |
| **SEAF** | Security Anchor Function |
| **SMF** | Session Management Function |

| | |
|---|---|
| **SUCI** | Subscription Concealed Identifier |
| **SUPI** | Subscription Permanent Identifier |
| **TA** | Temporary Identifier |
| **UDM** | Unified Data Management |
| **V2I** | Vehicle to Infrastructure |
| **V2V** | Vehicle to Vehicle |
| **V2X** | Vehicle to Everything |
| **VANET** | Vehicular Ad-hoc Network |
| **VLC** | Visible Light Communication |

# Introduction Générale

Depuis l'apparition de l'automobile, les véhicules ont toujours été conduits de manière individuelle. Toutefois, face à l'augmentation constante du trafic routier, à la saturation des infrastructures et à la montée des coûts énergétiques, les approches de conduite coopérative suscitent un intérêt croissant. Parmi elles, le vehicular platooning se distingue comme l'une des solutions les plus prometteuses [1].

Le platooning désigne un système de convoi dans lequel plusieurs véhicules se déplacent de manière coordonnée, en s'appuyant sur l'automatisation partielle ou totale des tâches de conduite. Ce mode de déplacement collaboratif contribue à renforcer la sécurité routière, à fluidifier le trafic et, surtout, à réduire significativement la consommation de carburant ainsi que les émissions de $CO_2$, grâce à la diminution de la traînée aérodynamique un avantage particulièrement notable dans le cas des poids lourds [4, 13].

Pour atteindre ces objectifs, le platooning repose sur deux piliers technologiques essentiels : le régulateur de vitesse coopératif adaptatif (Cooperative Adaptive Cruise Control, CACC) et les réseaux véiculaires ad hoc (Vehicular Ad Hoc Networks, VANETs) [13]. Grâce à la communication sans fil, les véhicules échangent des informations critiques, telles que la vitesse, l'accélération, la position ou les intentions de manuvre. Ces échanges s'effectuent via des technologies V2V, V2I ou V2X, en fonction du type d'entité communicante [2, 13].

Chaque peloton est organisé selon une architecture de type leader-suiveur : le Platoon Leader (PL), généralement conduit manuellement, est chargé de la gestion globale du convoi, tandis que les Platoon Members (PM) suivent automatiquement ses instructions transmises via les communications V2V [4]. Ces véhicules s'appuient également sur une variété de capteurs embarqués (RADAR, LIDAR, caméras), dont les données sont traitées par des unités de contrôle électronique (ECU) et transmises au système de commande via des réseaux internes tels que le CAN ou le LIN [4].

Cependant, malgré ses nombreux avantages, le platooning soulève d'importants défis, notamment en matière de cybersécurité. En effet, la plupart des protocoles embarqués actuels n'intègrent ni chiffrement ni authentification des messages, exposant ainsi les ECU à des attaques potentielles. Un attaquant pourrait perturber la coordination du peloton, voire annuler les bénéfices énergétiques attendus [2, 4].

Face à ces enjeux critiques, de nombreux travaux de recherche ont été menés afin d'identifier les vulnérabilités existantes et de proposer des solutions adaptées. Toutefois, aucune approche ne satisfait encore pleinement les exigences élevées en matière de sécurité, de robustesse et de performance requises pour les applications modernes de platooning. C'est dans ce contexte que nous introduisons une nouvelle approche, nommée PDHP (Proof-of-Work and Dilemma-based Hybrid Protocol). Ce protocole hybride combine des mécanismes de preuve d'ancienneté, d'évaluation comportementale et d'authentification cryptographique, afin d'assurer une sélection du leader à la fois fiable, sécurisée et efficace, tout en maintenant les objectifs d'optimisation énergétique du peloton.

Ce mémoire est structuré en quatre chapitres. Le premier chapitre introduit les concepts fondamentaux du vehicular platooning, en détaillant ses composants, son architecture ainsi que les principaux enjeux de sécurité qui y sont liés. Le deuxième chapitre est consacré à une étude approfondie des solutions existantes proposées dans la littérature, visant à améliorer la sécurité, la communication et la stabilité au sein des pelotons. Le troisième chapitre présente notre propre contribution, une solution conçue pour pallier certaines des limites identifiées dans l'état de l'art. Enfin, le quatrième chapitre expose les résultats issus de l'évaluation expérimentale de la solution proposée, en analysant ses performances, ses apports et ses éventuelles limites.

Dans ce contexte, la sécurité du platooning constitue un enjeu majeur, notamment en ce qui concerne la désignation et l'authentification du leader, éléments essentiels pour garantir la confiance et la stabilité du peloton. Ce mémoire propose une nouvelle approche combinant un mécanisme de sélection de leader avec une authentification multi-niveaux, dans le but de renforcer la résilience du système face aux menaces potentielles et d'assurer une communication fiable et sécurisée entre les véhicules.

Enfin, afin de démontrer l'efficacité et la pertinence de la solution proposée, une phase de simulation et d'évaluation des performances a été réalisée. Celle-ci repose sur un ensemble de métriques essentielles telles que le temps de traitement, le coût de communication, le coût de stockage et la consommation énergétique. Les résultats obtenus, comparés à ceux de protocoles récents issus de l'état de l'art, mettent en évidence la supériorité de notre approche et confirment son applicabilité dans un contexte réel de platooning sécurisé.

# 1

# Platooning dans les Systèmes de Transport Intelligents

## 1.1 Introduction

Les progrès réalisés ces dernières décennies dans le domaine des communications sans fil et des capteurs intelligents ont permis la réalisation des systèmes de platooning. Ces systèmes représentent une avancée majeure, notamment dans le cadre de la conduite autonome et coopérative. Le platooning permet à un groupe de véhicules de circuler de manière coordonnée et sécurisée, tout en assurant des échanges d'informations constants entre les membres du peloton.

Dans ce qui suit, nous présenterons en détail le concept de platooning, tout en indiquant les topologies de communication les plus classiques utilisées dans les systèmes de transport intelligents. Par la suite, nous décrirons l'architecture générale d'un système de platooning, en insistant sur les composants essentiels tels que les modules de communication V2V, les capteurs embarqués et les unités de contrôle. Nous examinerons également les principales contraintes et exigences de sécurité inhérentes à ce type de système, en particulier les défis liés à l'authentification des véhicules, à la protection contre les attaques malveillantes et à la fiabilité des communications dans un environnement dynamique.

## 1.2 Definition du platooning

Les convois de véhicules (vehicular platoons) sont des groupes de véhicules connectés par des liaisons numériques, permettant au véhicule de tête de dicter les mouvements et le comportement de tous les membres. Le platooning peut être décrit comme une application des réseaux véhiculaires (VANET), où un véhicule conduit manuellement permet aux autres véhicules de rouler de manière autonome ou semi-autonome [13].

Dans un convoi, le conducteur du véhicule de tête devient responsable de la conduite de l'ensemble du convoi, qui peut alors se comporter comme un seul véhicule. De telles manuvres sont rendues possibles grâce à l'utilisation de communications sans fil pour transmettre les informations de contrôle aux autres membres du convoi [7].

La Figure 1.1 fournit une illustration du platooning de véhicules dans le contexte plus large des environnements de véhicules connectés et autonomes (CAV) et de VANET basés sur les villes intelligentes. Le convoi communique avec l'environnement plus large du VANET, où d'autres CAV peuvent être connectés à des infrastructures telles que les unités en bord de route (RSU), ainsi qu'à d'autres usagers de la route tels que les piétons.

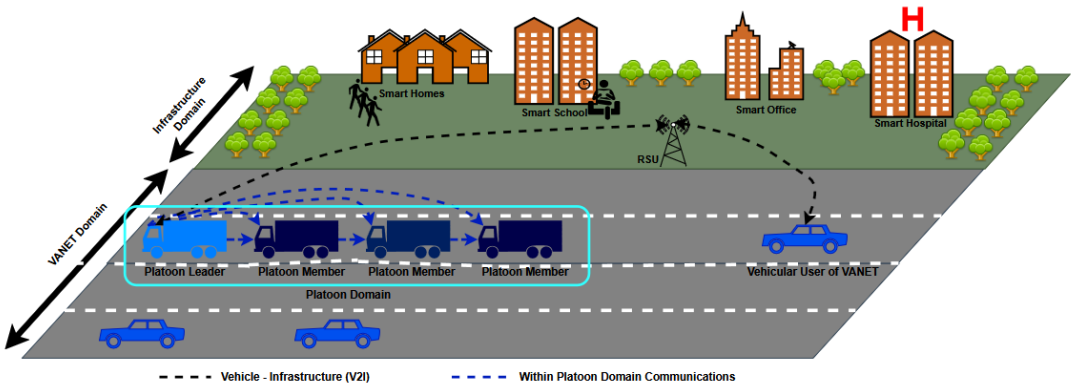



FIGURE 1.1 – Exemple de platooning de véhicules dans une ville intelligente [7].

## 1.3 Composition d'un convoi de véhicules autonomes

Un convoi de véhicules est composé de trois types de véhicules :

— **Véhicule de tête (Lead Vehicle - PL) :** généralement conduit manuellement afin d'observer l'environnement de manière plus précise.

— **Véhicules membres (Member Vehicles - PM) :** conduits de manière autonome ou semi-autonome, les conducteurs se contentant de surveiller les systèmes de leur véhicule .

— **Véhicules en phase d'entrée ou de sortie (Join/Leave Vehicles) :** Ce sont les véhicules qui intègrent ou quittent le convoi. Ils sont conduits manuellement

par le conducteur jusqu'à ce qu'il soit sûr d'intégrer le convoi, puis, lors de leur sortie du convoi, ils restent en mode autonome jusqu'à ce que le système autorise le conducteur à reprendre le contrôle du camion.

## 1.4 Topologie de communication

De nombreuses topologies de communication sans fil peuvent être observées dans la mise en uvre du platooning. L'enjeu central consiste à créer un réseau stable afin d'assurer la fiabilité du convoi, où les informations peuvent être transmises rapidement et de manière fluide à tous les membres.

1. **Topologie Centralisée :** La topologie centralisée correspond à un modèle dans lequel le PL communique avec tous les véhicules du convoi, tandis que les PM ne communiquent pas entre eux. Cela place donc le PL en contrôle exclusif du convoi. Cette approche présente l'avantage de permettre une diffusion rapide des décisions prises par le PL aux PM, mais ces derniers ne disposent d'aucune information sur les autres membres, comme illustré dans la Figure **??**.

   Le grand nombre de paquets transmis au sein du convoi représente un défi pour cette topologie, ce qui peut provoquer un retard important dans la transmission.

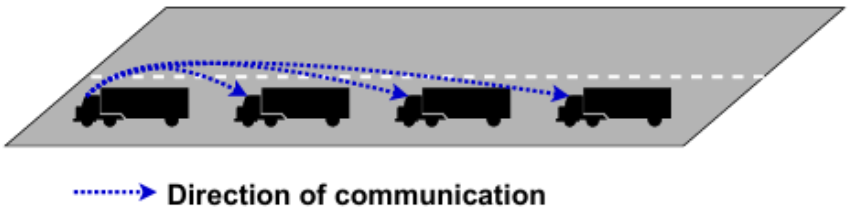



FIGURE 1.2 – Topologie centralisée des communications dans le platooning [13].

2. **Topologie Décentralisée :** Dans une topologie décentralisée, chaque véhicule communique uniquement avec le véhicule qui le suit directement. Avec cette configuration, le PL effectue beaucoup moins de tâches de calcul, comme illustré dans la Figure **??**. L'avantage de cette méthode réside dans le fait que le risque de retard lors de la transmission des paquets est réduit, en raison de leur faible nombre.

   L'entrée ou la sortie du convoi présente un défi majeur pour cette approche, car elle peut entraîner une instabilité dans le convoi. Lorsqu'un véhicule quitte le convoi sans être en dernière position, cela provoque un trou de connectivité. Les PM doivent détecter rapidement cette situation et ajuster leur vitesse pour maintenir la stabilité du convoi.

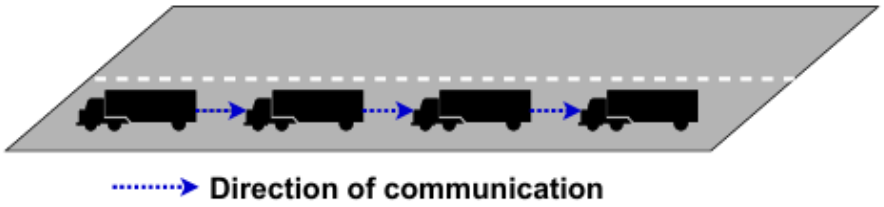



FIGURE 1.3 – Topologie décentralisée des communications dans le platooning [13].

3. **Topologie Hybride :** Pour la topologie hybride, il existe quatre principales façons de combiner les topologies centralisée et décentralisée. Chaque méthode possède ses propres avantages et inconvénients. Ces variantes sont :

   — Suivi du prédécesseur et du leader (Predecessor-leader following).
   — Bidirectionnelle (Bidirectional).
   — Leader bidirectionnel (Bidirectional leader).
   — Suivi des deux prédécesseurs (Two predecessors following).

   La topologie *suivi du prédécesseur et du leader* fonctionne en faisant en sorte que le leader transmette des informations à tous les véhicules, tandis que chaque véhicule communique également avec le véhicule qui le suit directement, comme illustré dans la Figure 1.4.

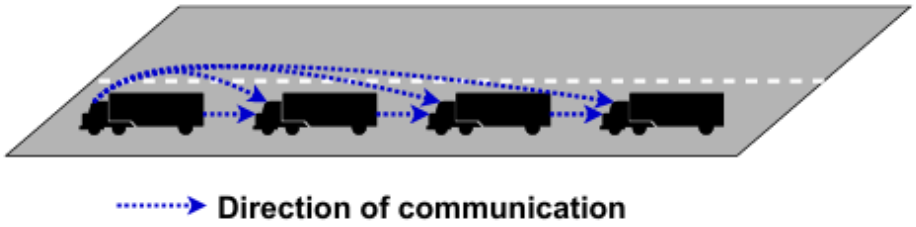



FIGURE 1.4 – Topologie de suivi prédécesseur-leader des communications dans le platooning [13].

La topologie *ń bidirectionnelle ż* permet à chaque véhicule d'envoyer et de recevoir des messages de ses véhicules voisins. L'avantage de cette approche est que les informations peuvent circuler dans les deux sens, comme illustré dans la Figure 1.5.

La topologie *leader bidirectionnelle* combine les approches **bidirectionnelle** et **centralisée** afin de surmonter les faiblesses de chacune. Dans cette configuration, le leader conserve le contrôle de la taille et de la stabilité du convoi, tandis que les membres peuvent communiquer directement entre eux, comme illustré dans la Figure 1.6.

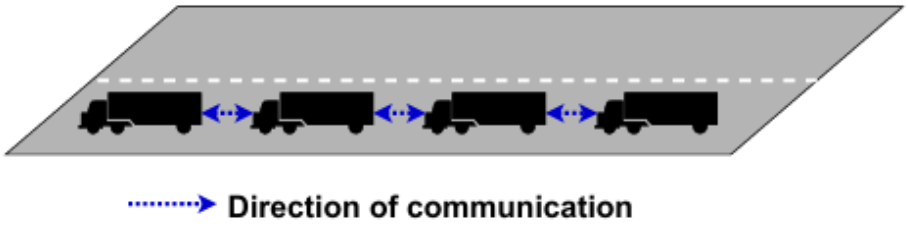



FIGURE 1.5 – Topologie de suivi prédécesseur-leader des communications dans le platooning [13].

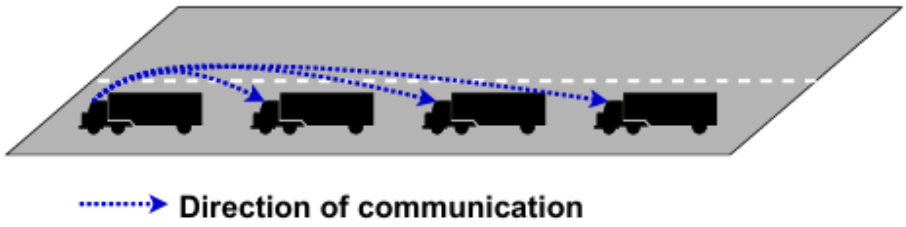



FIGURE 1.6 – Topologie bidirectionnelle avec leader des communications dans le platooning [13].

La topologie *ń suivi des deux prédécesseurs ż* est une amélioration de la topologie *suivi du prédécesseur* et du *leader*, permettant aux véhicules d'avoir une meilleure perception de ce que font les autres véhicules, sans augmenter le nombre de paquets transmis. Elle nécessite en contrepartie une puissance de traitement bien plus élevée pour analyser et réagir rapidement à toutes ces informations supplémentaires, comme illustré dans la Figure **??**.

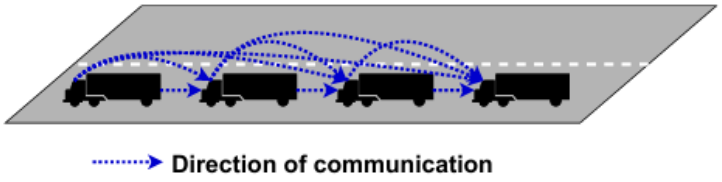



FIGURE 1.7 – Topologie de suivi des deux prédécesseurs dans les communications de platooning [13].

## 1.5 Technologie de conduite automatisée

La technologie de conduite automatisée (Automated Driving  AD) constitue une avancée majeure dans l'évolution des systèmes de transport intelligents, offrant la possibilité de transformer en profondeur la mobilité routière.

L'objectif de cette technologie est de permettre aux véhicules de circuler de manière autonome et en toute sécurité, tout en réduisant les accidents, en évitant les embouteillages et en diminuant la consommation de carburant.

De nombreux systèmes faisant partie de la technologie AD sont déjà disponibles commercialement, tels que [7] :

— **Le régulateur de vitesse adaptatif (Adaptive Cruise Control (ACC)) :** C'est un petit bijou de technologie automobile qui rend les trajets sur la route encore plus confortables et sûrs.

L'ACC utilise des capteurs sophistiqués positionnés sur le véhicule pour détecter les véhicules qui se trouvent aux alentours de votre véhicule. Il mesure la distance qui vous sépare de ces véhicules et ajuste automatiquement votre vitesse pour maintenir une distance de sécurité en effectuant le freinage à votre place [5].

— **L'assistance au maintien dans la voie (Lane Keeping Assist (LKA)) :** Le LKA est un système d'aide à la conduite automobile. Sa fonction consiste à alerter le conducteur lorsqu'il quitte involontairement sa voie de circulation.

Ce système d'assistance à la conduite se différencie de la simple alerte de franchissement involontaire de ligne par sa capacité à intervenir dans certains cas, où il agit directement sur la commande de la direction pour corriger la trajectoire du véhicule [16].

— **Le freinage d'urgence autonome (Autonomous Emergency Braking (AEB)) :** L'AEB est un système d'aide active permettant de réaliser un freinage d'urgence de manière autonome. Ce système est composé de différents lasers et radars, reliés à des dispositifs capables de calculer la vitesse. Les résultats de ces calculs permettent de détecter s'il existe un risque de collision entre le véhicule en marche et un obstacle situé devant lui.

Lorsque le véhicule détecte la présence d'un élément qu'il considère comme étant un obstacle devant lui, il va tout d'abord alerter le conducteur. Si la détection intervient trop tardivement ou si le système ne remarque aucune réaction de la part du conducteur, le véhicule prendra alors la décision d'enclencher automatiquement le système de freinage, afin d'éviter la collision ou d'en réduire l'impact [12].

— **Le stationnement automatisé ou l'aide au stationnement :** permet d'aider le conducteur à effectuer les manuvres de stationnement. Ce dispositif a été conçu pour identifier une place de parking et se garer automatiquement dans celle-ci, grâce à des capteurs à ultrasons installés sur le véhicule [14].

Le platooning s'appuie sur ces technologies en développant le régulateur de vitesse adaptatif coopératif. *(Cooperative Adaptive Cruise Control - CACC).*

La technologie de conduite automatisée repose sur des systèmes robotiques qui ń perçoivent ż l'environnement à l'aide d'une combinaison de capteurs, tels que le lidar (détection et télémétrie par la lumière), le radar et les caméras. Les capteurs peuvent également compenser les faiblesses des uns et des autres et fournir une redondance. En cas de brouillard dense, les caméras deviennent inefficaces, mais le radar et le lidar prennent le relais.

Pour la communication sans fil, une norme Wi-Fi spécifique a été approuvée : IEEE 802.11p. Il s'agit d'une extension de la technologie Wi-Fi (802.11), mais qui ajoute une prise en charge des applications des systèmes de transport intelligents (ITS), comme le platooning de camions. La norme 802.11p permet l'échange de données entre véhicules (V2V), ainsi que la communication entre véhicule et infrastructure (V2I) [7].

## 1.6 Menaces de sécurité dans le pelotonnage véhiculaire

Les menaces de sécurité liées au pelotonnage véhiculaire sont variées et nombreuses en cybersécurité. Les communications des pelotons véhiculaires sont confrontées à plusieurs types d'attaques, chacune visant un objectif spécifique. Ces objectifs peuvent être répartis en quatre catégories distinctes, comme illustré dans le tableau 1.1.

| Objectif de l'attaque | Fonction de l'attaque | Attaques associées |
|---|---|---|
| **Gestion des accès** | L'attaquant se fait passer pour un autre individu afin de manipuler les véhicules au sein d'un peloton. | — Collision<br>— Usurpation (Impersonation) |
| **Empêcher le pelotonnage** | Rendre le fonctionnement du convoi instable ou inutilisable. | — Déni de service (DoS)<br>— Inondation (Flooding)<br>— Brouillage (Jamming) |
| **Collecte de données** | L'attaquant récupère des informations issues des communications sans fil. Ces données peuvent ensuite être revendues ou utilisées à d'autres fins. | — Écoute clandestine (Eavesdropping)<br>— Vol d'informations (Information Theft) |
| **Perturbation du peloton** | es attaques visant principalement à perturber un peloton, à réduire son efficacité voire à le rendre dangereux. | — Fausse manuvre (Fake Maneuver)<br>— Injection de fausses données<br>— Fausses positions |

TABLE 1.1 – Objectifs des attaques et exemples associés.

## 1.7 Exigences de sécurité dans les communications de pelotons

1. **Authentification :** L'authentification est l'un des moyens utilisés par les mécanismes de sécurité pour prouver ou donner de la crédibilité à un message. Lorsqu'un attaquant parvient à contourner ce mécanisme, cela implique souvent l'usage d'identifiants de sécurité volés ou falsifiés.

   (a) **Disponibilité :** La disponibilité, dans un réseau de pelotons, désigne la capacité des membres à former un réseau, ainsi qu'à conserver un accès continu aux données. Toutefois, elle peut parfois être naturellement réduite, par exemple en raison de conditions météorologiques défavorables ou d'obstacles physiques tels que les tunnels.

   (b) **Confidentialité :** La confidentialité, dans un réseau de pelotons, signifie que seuls les membres du réseau ou les membres autorisés peuvent déchiffrer les messages diffusés par le leader ou par les autres membres du peloton.

   (c) **Vérification des données :** La vérification des données consiste à contrôler en permanence les informations en s'appuyant sur plusieurs messages. Cela

permet de s'assurer que les messages circulant dans le domaine du peloton sont corrects.

(d) **Intégrité :** L'intégrité correspond à la garantie de la fiabilité des informations, en s'assurant qu'elles n'ont pas été altérées et que le contenu des messages est exact.

(e) **Vie privée :** La vie privée est essentielle dans les réseaux de pelotons. Dans ces réseaux, les utilisateurs et leurs véhicules ne doivent divulguer que les informations strictement nécessaires au bon fonctionnement du peloton.

(f) **Non-répudiation :** Dans ce contexte, lorsqu'un message est reçu, l'émetteur ne peut pas en nier l'envoi et doit en assumer la responsabilité. Cela peut être assuré par l'utilisation d'une *ń boîte noire ż*.

## 1.8 Chiffrement entierement Homomorphe

Le chiffrement entièrement homomorphe (FHE) est une primitive cryptographique puissante qui permet d'effectuer des calculs sur des données chiffrées, sans avoir accès à la clé secrète et sans devoir les déchiffrer. Le résultat obtenu reste chiffré et seul le propriétaire de la clé peut le déchiffrer. La robustesse du FHE repose sur un problème mathématique connu sous le nom de *Learning With Errors* (LWE), basé sur les réseaux euclidiens, réputés résistants aux attaques quantiques [3].

L'idée essentielle de la construction du FHE consiste à ajouter du bruit, à la fois lors du chiffrement et lors de la génération des clés, afin de garantir la sécurité. Ce système repose sur plusieurs paramètres qui déterminent son niveau de sécurité, ses performances et la précision des calculs :

— Nombre de bits fractionnaires ($f$), correspondant à la précision.
— Modulus du texte clair ($p$).
— Modulus du texte chiffré ($q$).
— Dimension du texte chiffré ($n$).

On distingue deux preuves mathématiques, représentées comme suit 1.1 1.2 :

**Addition homomorphe** $\text{Add}(c_1, c_2)$ : à partir des chiffrés de $m_1$ et $m_2$, retourne le chiffrement de $m_1 + m_2$.

$$\text{Enc}(m_1 + m_2) = \text{Enc}(m_1) + \text{Enc}(m_2) \tag{1.1}$$

**Multiplication homomorphe** $\text{Mult}_{evk}(c_1, c_2)$ : à partir des chiffrés de $m_1$ et $m_2$, retourne le chiffrement de $m_1 \times m_2$,

$$\text{Enc}(m_1 \times m_2) = \text{Enc}(m_1) \times \text{Enc}(m_2) + e_{\text{mult}} \mod q \tag{1.2}$$

où $e_{\text{mult}}$ est une erreur supplémentaire dans $R$.

Le bruit augmente au fur et à mesure que les calculs chiffrés s'enchaînent, en particulier avec la multiplication homomorphe, ce qui peut entraîner des déchiffrements erronés si trop d'opérations sont effectuées

## 1.9 La théorie des jeux et le dilemme du prisonnier

La théorie des jeux est un cadre mathématique permettant de modéliser et d'analyser les interactions stratégiques entre plusieurs acteurs rationnels. Dans le contexte du pelotonnage, elle est exploitée pour évaluer le comportement des véhicules et renforcer la sécurité lors de la sélection et de l'authentification du leader. Un modèle classique de cette approche est le dilemme du prisonnier, qui illustre les choix entre coopération et tricherie.

Chaque véhicule se voit attribuer un score en fonction de ses décisions :
— **Coopération (C)** : le véhicule contribue au maintien de la stabilité et de la sécurité du peloton.
— **Tricherie (D)** : le véhicule adopte un comportement malveillant ou non coopératif.

Le gain (ou la pénalité) associé à chaque stratégie peut être représenté par une matrice de paiements, où $C$ désigne la coopération et $D$ la défection :

| | **C** | **D** |
|---|---|---|
| **C** | $(R, R)$ | $(S, T)$ |
| **D** | $(T, S)$ | $(P, P)$ |

Avec :
— $R$ : Récompense mutuelle lorsque les deux coopèrent,
— $T$ : Tentation de tricher lorsque l'autre coopère,
— $S$ : Déception du joueur qui coopère alors que l'autre triche,
— $P$ : Punition mutuelle lorsque les deux trichent.

| | $C$ | $D$ |
|---|---|---|
| $C$ | $(R, R)$ | $(S, T)$ |
| $D$ | $(T, S)$ | $(P, P)$ |

avec : $R$ : récompense mutuelle pour la coopération. $T$ : tentation de tricher. $S$ : perte pour celui qui coopère alors que l'autre triche. $P$ : pénalité mutuelle en cas de tricherie simultanée.

Ainsi, en intégrant ce mécanisme dans le protocole de sécurité, le système favorise la coopération entre véhicules et pénalise automatiquement les comportements malveillants, garantissant un choix optimal pour la stabilité et la fiabilité du peloton.

## 1.10 Conclusion

Nous avons présenté les concepts fondamentaux sur lesquels repose le *platooning* véhiculaire, en mettant en évidence la composition d'un convoi de véhicules autonomes interconnectés selon différentes topologies, ainsi que les technologies d'aide à la conduite qui le soutiennent. Nous avons également exposé les principales menaces de sécurité auxquelles un convoi peut être confronté, ainsi que les exigences essentielles pour assurer la fiabilité et la sécurité des communications.

Dans la littérature, plusieurs mécanismes de sécurité appliqués au *platooning* ont été proposés par différents chercheurs. Le chapitre suivant sera consacré à une analyse critique de certaines de ces solutions existantes.

# 2

# État de l'art sur les mécanismes de sécurité dans le platooning

## 2.1 Introduction

Assurer la sécurité et la confidentialité des échanges dans le platooning représente un véritable défi, en raison de la nature dynamique des communications V2V (véhicule-à-véhicule) et des exigences strictes en matière de fiabilité. Ce chapitre est donc consacré à l'analyse des principales approches existantes visant à sécuriser ces environnements coopératifs.

Nous commencerons par définir les critères essentiels d'évaluation permettant de juger de l'efficacité des protocoles de sécurité. Chaque solution retenue fera ensuite l'objet d'une présentation détaillée, accompagnée d'un regard critique sur ses avantages, ses limites et son applicabilité. Enfin, nous clôturerons ce chapitre par une synthèse comparative, afin de mettre en lumière les tendances actuelles et d'identifier les approches les plus prometteuses pour améliorer la sécurité des pelotons de véhicules autonomes.

## 2.2 Critères d'analyse essentiels pour la sécurité du platooning

— **Confidentialité :** Protection des données échangées entre véhicules contre les accès non autorisés.
— **Intégrité :** Garantie que les messages reçus n'ont pas été altérés.
— **Authentification :** Vérification de l'identité des véhicules pour éviter les intrusions malveillantes.
— **Résistance aux attaques :** Capacité du système à faire face aux attaques comme la relecture, la falsification ou la collusion.
— **Temps de réaction (latence) :** Rapidité de traitement pour garantir la sécurité dans des contextes critiques.
— **Surcharge en communication et calcul :** Efficacité des mécanismes sans trop alourdir le réseau ou les processeurs embarqués.
— **Robustesse face à la dynamique du peloton :** Capacité à maintenir la sécurité malgré les changements de topologie (entrée/sortie de véhicules, changement de leader).

## 2.3 Classification des travaux étudiés

Après avoir analysé les travaux recueillis, il nous est apparu qu'une classification était nécessaire afin de répertorier les différentes approches suivies. Le tableau **??** présente notre classification des différentes solutions proposées pour le problème de sécurité dans les réseaux corporels sans fil.

## 2.4 Étude critique des travaux

Pour répondre aux défis de sécurité dans les réseaux de véhicules en convoi (platooning), plusieurs mécanismes cryptographiques ont été conçus afin de garantir l'intégrité, l'authenticité et la confidentialité des données échangées. Dans ce qui suit, nous étudions une partie des travaux réalisés dans ce contexte.

### 2.4.1 Le protocole SPMSA

Le protocole proposé par Junaidi et al. [8] a été conçu dans l'intention de remédier à la plupart des limites des solutions cryptographiques actuelles. Ces limites incluent notamment une authentification incomplète des identités et des

messages, ainsi que des coûts de calcul élevés. En ce qui concerne la gestion des pelotons, le protocole proposé fonctionne autour de deux événements principaux :

— **L'entrée dans le peloton :**L'entrée dans le peloton a pour enjeu de vérifier l'identité du véhicule entrant et l'intégrité des messages échangés dans le peloton. Le protocole SPMSA répond à ces enjeux à travers un processus structuré en quatre phases :

(a) **Initialisation :** les véhicules s'enregistrent auprès du réseau 5G via les RSU pour obtenir leurs identifiants, une paire de clés privéepublique, ainsi qu'une clé initiale de peloton, tout en assurant la fraîcheur des messages grâce aux horodatages.

(b) **Authentification d'identité :** le mécanisme de détection repose sur l'échange de clés publiques éphémères et de signatures numériques. En cas d'échec de ces échanges, le message est suspecté comme une tentative d'attaque Sybil. Dans le cas contraire, le leader du peloton (PL) répond de la même manière et les deux véhicules peuvent alors dériver une clé de session secrète, qui sera utilisée pour chiffrer les messages échangés entre eux.

(c) **Authentification des messages :** cette phase a pour objectif principal de transmettre la clé du peloton au véhicule rejoignant (JV) de manière sécurisée. Elle est conçue pour contrer les attaques internes.

(d) **Mise à jour de la clé du peloton :** elle est déclenchée dès qu'un nouveau véhicule est authentifié pour rejoindre le peloton. L'objectif principal est d'envoyer une requête de mise à jour contenant la nouvelle clé partielle du peloton, un horodatage et une signature numérique basée sur l'ancienne clé du peloton pour les membres existants.

— **Événement de communication dans le peloton :** c'est un scénario dans lequel des membres du peloton, déjà authentifiés avec succès, souhaitent transmettre des informations utiles à d'autres membres pendant la conduite en peloton. L'algorithme d'échange de messages utilisé est similaire à celui de la phase d'authentification des messages.

## Discussion et critiques

Le protocole SPMSA apporte une réponse structurée aux défis liés à la formation sécurisée de pelotons de véhicules, notamment en matière d'authentification hybride des identités et des messages. Il combine un échange de clés sécurisé, la signature et le chiffrement des messages. Le protocole assure à la fois la confidentialité et l'intégrité des communications.

Cependant, plusieurs avertissements peuvent être formulés. D'une part, la complexité du protocole, avec ses multiples phases et clés dérivées, peut engendrer une charge non négligeable pour les unités embarquées dans les véhicules. D'autre part, une forte dépendance au réseau 5G lors de l'initialisation et de la vérification des

identifiants pourrait poser problème dans les zones à faible couverture. Enfin, même si la détection des attaques Sybil est bien intégrée, la gestion dynamique des clés de groupe à chaque ajout de membre reste coûteuse en termes de synchronisation et de bande passante.véhicules dans le système est assuré par un réseau Blockchain.

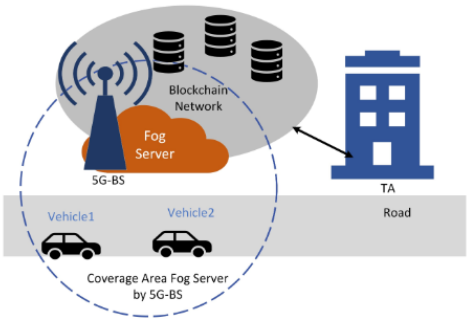



FIGURE 2.1 – Architecture du modèle système pour le protocole HAFC [10].

Le schéma HAFC proposé se compose de deux étapes, décrites ci-dessous :

— **ÉTAPE D'AUTHENTIFICATION INITIALE :**

Au cours de cette phase, un SF va aider un véhicule à authentifier son identité afin que le serveur puisse générer une clé de session à utiliser tant que le véhicule reste dans la zone de couverture du signal du SF.

Un ensemble de clés est créé au cours de cette phase. La toute première clé est la GenKey, une clé secrète Diffie-Hellman utilisée pour démarrer le processus d'authentification. Les véhicules possèdent également une clé privée unique, GenVehPK, utilisée pour signer les messages envoyés. Enfin, GenFogPK est une clé privée propre au SF, destinée au déchiffrement des messages reçus.

— **ÉTAPE D'AUTHENTIFICATION DE TRANSFERT ( HANDOVER) :**

Cette phase se produit lorsqu'un véhicule quitte la couverture de signal d'un SF et entre dans celle d'un autre, comme représenté dans la Figure 2.2. Le SF vérifie d'abord la légitimité du véhicule via la blockchain. Si la fiabilité du véhicule n'a pas changé depuis qu'il a été authentifié par le précédent serveur de fog, alors le SF actuel n'a pas besoin de réauthentifier la fiabilité du véhicule.

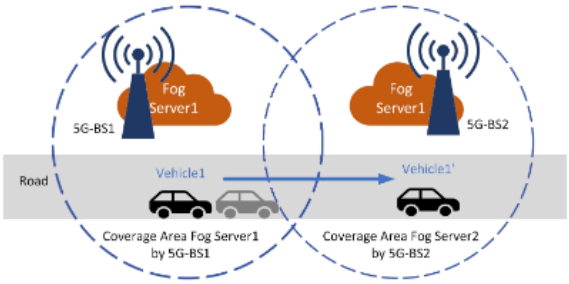



FIGURE 2.2 – Présentation du schéma HAFC [10].

### Discussion et critiques

Le modèle HAFC repose sur une architecture protégée intégrant le Fog computing et la blockchain dans le cadre des réseaux C-V2X. Ses principaux atouts résident dans sa nature distribuée, qui permet une mobilité fluide des véhicules lors du changement de zone de couverture, grâce à l'utilisation de certificats de transfert et de jetons. La blockchain, de son côté, assure la fiabilité des entités et la traçabilité des actions dans le réseau, en s'appuyant sur une authentification initiale robuste.

Cependant, sa mise en uvre pratique soulève plusieurs obstacles. Le premier concerne l'exigence d'une couverture 5G stable afin de maintenir une communication fluide entre les membres du convoi. En effet, même si la réauthentification est allégée grâce à des mécanismes de transition, elle n'est pas totalement supprimée. Cela peut constituer une limite en termes de performance et de passage à l'échelle.

## 2.4.2 H3PC : Enhanced Security and Privacy-Preserving Platoon Construction Based on Fully Homomorphic Encryption

Chah et al. [3] ont proposé la solution H3PC pour sécuriser la formation et la coordination des convois de véhicules autonomes (CAVs), tout en préservant la confidentialité des données sensibles échangées entre les véhicules et le serveur central (PSP). Ce système s'appuie sur l'utilisation du chiffrement homomorphe, afin de permettre le partage d'informations critiques telles que la vitesse, la position ou la trajectoire sans révéler directement ces données.

Le système H3PC repose sur trois composants principaux nécessaires à la constitution d'un convoi, comme illustré dans la Figure 2.3 :

Un serveur centralisé : il gère les instructions nécessaires au peloton, notamment le calcul de l'accélération de chaque CAV. Ce calcul est effectué à partir de données chiffrées transmises par les véhicules, sans que le serveur ait accès aux informations sensibles (position, vitesse, trajectoire). La communication entre le serveur et les véhicules est établie via des canaux sécurisés.

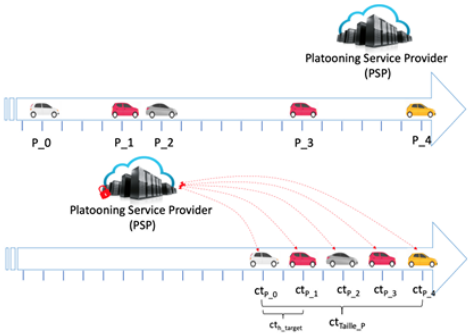



FIGURE 2.3 – Architecture du modèle de système du schéma H3PC [3].

Dans la couche supérieure (au-dessus de TLS 1.3), l'ensemble des véhicules d'un même peloton doit disposer d'une paire de clés commune (clé publique et clé privée). Pour y parvenir, une phase d'initialisation est mise en place : les véhicules exécutent un protocole collaboratif destiné à générer collectivement cette paire de clés.

Une fois la clé publique commune obtenue, elle est transmise au PSP, ce qui permet d'assurer des échanges sécurisés d'informations entre les véhicules du convoi et le serveur central.

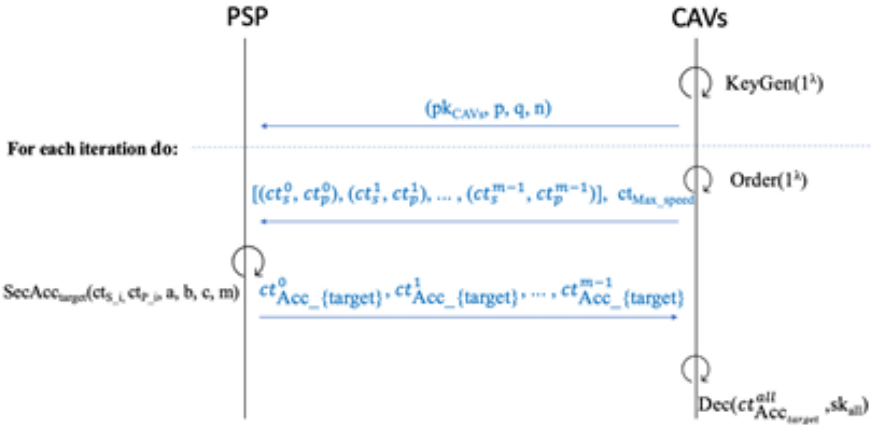



FIGURE 2.4 – Protocole de communication chiffrée H3PC. [3]

### Discussion et critiques

La solution H3PC constitue une avancée notable en matière de confidentialité dans les systèmes de CAVs connectés. Grâce à l'utilisation du chiffrement homomorphe, il devient possible d'effectuer des calculs sur des données chiffrées, assurant ainsi une forte protection contre les intrusions et les fuites d'informations sensibles. Toutefois, ce modèle repose sur une hypothèse de participants semi-honnêtes, ce qui limite sa robustesse face aux attaques actives. De plus, bien que la confidentialité soit préservée, le protocole demeure trop lent pour une utilisation en temps réel, et il présente une complexité accrue lors du remaniement dynamique des pelotons (ajout ou retrait de véhicules).

## 2.4.3 Secure Vehicle Platooning Protocol for 5G C-V2X

Afin de sécuriser la fusion et la coordination des pelotons de CAVs, Liu et al. [9] ont proposé un protocole de communication sécurisé fondé sur les standards 5G-V2X. Ce mécanisme repose sur la génération d'identités pseudonymes et de clés de signcryption, permettant aux véhicules de s'authentifier mutuellement tout en partageant une clé de groupe destinée à chiffrer les échanges internes au peloton.

Le Noyau de Réseau 5G, illustré dans la Figure 2.5, est composé des éléments suivants :

(a) **Un Réseau de Service (SN) :** Le SN , auquel l'utilisateur se connecte lorsqu'il utilise la 5G, inclut un **AMF**, responsable de gérer l'accès et la mobilité des utilisateurs. La connexion de données et les sessions IP sont prises en charge par le **SMF**. Enfin, la première vérification de la sécurité de l'utilisateur est assurée par le **SEAF**.

(b) **Réseau Domestique (HN) :** C'est ce réseau qui possède les données d'authentification et qui valide si l'utilisateur peut accéder au réseau 5G. Il stocke les informations des abonnés dans le **UDM** et gère l'authentification via ce dernier. Les clés de chiffrement sont générées par **ARPF**, qui assure également la sécurité de l'authentification. En revanche, l'authentification mutuelle entre l'utilisateur et le réseau est effectuée par la **AUSF**.

(c) **Canaux de communication utilisés :** Il dispose de deux interfaces de communication : l'interface **PC5**, qui permet une communication directe entre les UEs via le réseau cellulaire (modes *broadcast* et *unicast*), et l'interface **Uu**, qui ne prend en charge que le mode *unicast*.

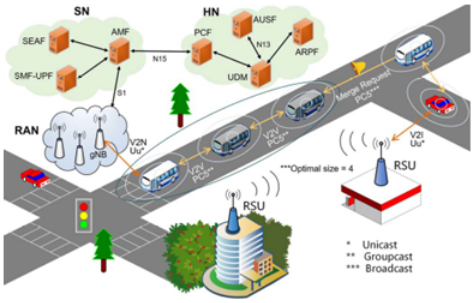



FIGURE 2.5 – Architecture améliorée de la 5G pour prendre en charge le pelotonnage de véhicules. [9]

**GUTI – *Globally Unique Temporary Identifier***

Un identifiant temporaire unique global (**GUTI**) est attribué à un utilisateur mobile après un enregistrement initial réussi. Ce processus implique l'utilisation de l'identifiant d'abonnement dissimulé (**SUCI**), qui constitue une forme de chiffrement asymétrique de l'identifiant permanent d'abonnement (**SUPI**).

Le **GUTI** permet ainsi de protéger la confidentialité de l'utilisateur en remplaçant son identifiant permanent par un identifiant temporaire lors des communications suivantes. [9]

Ce protocole 5G C-V2X fonctionne comme suit :

(a) **L'attribution du GUTI :**Le processus d'authentification débute avec l'identité permanente de l'abonné (SUPI, Subscription Permanent Identifier) et son équivalent chiffré, le SUCI (Subscription Concealed Identifier). Lorsqu'un véhicule (UE  User Equipment) détecte un réseau 5G, il initie une demande d'enregistrement, déclenchant ainsi la procédure d'authentification.

Afin de préserver la confidentialité, le SUPI est chiffré de manière asymétrique grâce à une clé publique appartenant au Home Network (HN), générant ainsi le SUCI. Ce dernier est transmis au réseau, évitant toute exposition du SUPI en clair aux attaquants potentiels.

Seul le HN est capable de déchiffrer le SUCI afin de récupérer le SUPI et de vérifier l'identité de l'utilisateur. Une fois l'authentification réussie, le réseau attribue à l'appareil un GUTI (Globally Unique Temporary Identifier), qui remplace le SUPI lors des communications ultérieures. L'utilisation de ce pseudonyme dynamique renforce la protection contre le traçage et l'usurpation d'identité.

(b) **stockage de la correspondance SUPI-GUTI** : le GUTI est stocké dans AMF du SN. L'AMF conserve un mapping entre le SUPI d'un abonné et son GUTI.

(c) **Ré-authentification optimisée avec le GUTI** : Lorsqu'un utilisateur revient sur le réseau, au lieu d'envoyer son SUPI ou SUCI, il présente simplement son GUTI. L'AMF reconnaît cet identifiant temporaire et associe directement l'utilisateur à son SUPI stocké

### Discussion et critiques

Le protocole 5G C-V2X s'appuie sur les capacités avancées du réseau 5G, adaptées pour assurer une authentification sécurisée tout en préservant l'anonymat des véhicules. Toutefois, son efficacité dépend fortement de la qualité de la connexion au réseau : si un véhicule se trouve dans une zone mal couverte, le protocole risque de ne pas fonctionner correctement.

Par ailleurs, l'utilisation du GUTI, bien qu'efficace pour éviter l'exposition du SUPI, nécessite un stockage fiable des correspondances SUPIGUTI. Cette exigence peut introduire des risques supplémentaires en cas de compromission du réseau d'accès ou du serveur AMF

## 2.4.4 BlockChain for Improved Platoon Security

Hexmoor, Alsamarace et Almaghshi [6] ont proposé une solution innovante utilisant la blockchain pour sécuriser les échanges de données entre véhicules en peloton. Leur système protège la vie privée tout en permettant un partage rapide d'informations, comme la vitesse. Les chercheurs décrivent aussi des protocoles anti-piratage pour contrer les cyberattaques potentielles.

Cette proposition innovante intègre une blockchain managée centralement par un Platoon Cloud (PC) pour sécuriser les échanges de données dans les pelotons routiers. Contrairement aux blockchains décentralisées classiques, l'architecture hybride combine :

Une autorité centrale (PC) : chargée de la gestion des clés cryptographiques et de la validation des transactions.

Une chaîne de blocs légère : optimisée pour répondre aux contraintes temps réel des véhicules.

Pour le partage d'informations, on considère le premier véhicule entrant dans une zone (appelé véhicule frontal, ou FV), qui maintient une vitesse légèrement inférieure à la limite autorisée. Ce véhicule agit comme le leader du peloton (PL), tandis que les véhicules suivants sont appelés véhicules arrière (RV).

**Algorithm 1** Protocole de formation sécurisée d'un peloton de véhicules [6]

**Input :** Véhicule arrière (RV) détecte un véhicule frontal (FV)
**Output :** Intégration sécurisée dans le peloton
**Phase 1 : Établissement de la communication**
RV → FV : Demande de clé publique (PK)
FV → RV : Envoi de sa PK
RV → PC : Transmission de la PK du FV pour vérification
**Phase 2 : Vérification par le Platoon Cloud (PC)**
**if** PK ∈ base de données du PC **then** ▷ Peloton existant
    PC → Base : Ajouter la PK du RV
    PC → RV : Envoi unicast de la CPK
    **Résultat :** RV devient PM du peloton existant
**else** ▷ Nouveau peloton
    PC : Créer un nouveau peloton avec :
        - FV comme Platoon Leader (PL)
        - RV comme Platoon Member (PM)
    PC : Générer une nouvelle CPK unique
    PC → PL, PM : Envoi unicast de la CPK
**end if**
**Phase 3 : Finalisation**
Mise à jour du registre blockchain
Synchronisation des données dans le cloud

Les blocs de la blockchain suivent une architecture stricte pour garantir la sécurité :

(a) Lien avec le bloc précédent : Chaque bloc contient une référence au hachage du bloc précédent pour assurer la continuité.
(b) Données encapsulées : Les informations critiques, telles que la vitesse et l'état du véhicule, sont encapsulées.
(c) Signature unique : Un hachage unique pour chaque bloc garantit son authenticité et facilite la validation des blocs suivants.

Dans cet algorithme de sécurité appliqué au platooning, chaque véhicule conserve localement ses données et les transmet régulièrement au Platoon Cloud (PC). Le leader (PL) envoie des transactions signées contenant ses données de vitesse et sa clé publique. Le PC vérifie l'authenticité de l'émetteur via sa base de données et s'assure de la continuité des transactions à l'aide de hachages.

Si la vérification est correcte, la signature est authentifiée et les données sont comparées à celles enregistrées grâce au système BCSI. Ensuite, un consensus distribué est lancé : les autres véhicules du peloton valident les données, et un seuil de dix confirmations est requis. Une fois ce seuil atteint, les transactions sont regroupées en un bloc, diffusées à l'ensemble du peloton, puis enregistrées sur la blockchain, garantissant ainsi la traçabilité, l'intégrité et l'immutabilité des données, même dans un environnement dynamique.

#### Discussion et critiques

Le système actuel présente plusieurs vulnérabilités potentielles malgré ses mécanismes de sécurité cryptographiques. Un risque majeur concerne l'usurpation prolongée du rôle de leader (PL) par un attaquant, qui pourrait alors détourner le peloton ou perturber son fonctionnement. Un autre scénario implique des membres du peloton (PM) malveillants qui pourraient brouiller les communications ou altérer délibérément leur vitesse pour désorganiser la formation.

Des cas particuliers méritent attention, comme lorsque plusieurs véhicules adjacents tentent simultanément de rejoindre le peloton, ce qui pourrait engendrer des conflits dans l'enregistrement des clés publiques. Ces situations montrent que le système doit encore évoluer pour garantir une sécurité absolue.

### 2.4.5 Attack Mitigation and Security for Vehicle Platoon

Ndambuki et Alhitmi [11] ont proposé une approche originale pour sécuriser les pelotons de véhicules autonomes en combinant la communication par lumière visible (VLC) avec un codage par couleurs (Color-Shift Keying, CSK). L'idée est de détecter les attaques internes sans recourir aux méthodes cryptographiques classiques.

Dans ce système, les véhicules échangent des signaux lumineux codés en rouge, vert et bleu. Le leader encode ses ordres sous forme de couleurs spécifiques à l'aide du CSK, et les autres véhicules les décodent grâce à un convertisseur lumière-fréquence (LTF). Une interruption du signal, un retard ou une chute d'intensité lumineuse (dans le spectre RGB) est interprétée comme une attaque potentielle (de type Sybil, DoS ou retard). En cas d'anomalie, une alerte est déclenchée et le protocole de sécurité est renforcé. Le CSK, couplé à un microcontrôleur, permet de maintenir une transmission sécurisée et directe

des instructions du leader, même dans des conditions de menace.

### Discussion et critiques

Bien que la solution proposée via VLC soit intéressante, cette technologie peut être affectée par les conditions environnementales, ce qui impose une étude approfondie de sa résilience. Par ailleurs, l'adoption de technologies telles que CSK et LTF demeure complexe et coûteuse à déployer à grande échelle. Si les simulations d'attaques fournissent des résultats encourageants, des expérimentations dans des scénarios réels et plus complexes restent indispensables pour valider l'efficacité du système. La gestion des priorités peut également engendrer des interférences lorsque trop de véhicules transmettent simultanément. Enfin, à mesure que le nombre de véhicules dans un peloton augmente, des optimisations supplémentaires seront nécessaires afin de garantir la sécurité et de préserver les performances globales du système.

## 2.4.6 Modeling and Analyzing Cyberattack Effects on Connected Automated Vehicular Platoons

Yang et al. [15] ont étudié l'impact des cyberattaques sur les pelotons de véhicules connectés et automatisés (CAVs) en s'appuyant sur le modèle CIDM 2.1. Les auteurs ont simulé trois types d'attaques : l'injection de faux messages, la relecture de données et les attaques coordonnées. Ces perturbations influencent directement la dynamique du peloton, entraînant une désynchronisation, des instabilités et un accroissement du risque de collision.

Le modèle CIDM (Cooperative Intelligent Driver Model) constitue une extension du modèle IDM classique. Il intègre les effets des communications inter-véhicules (V2V) ainsi que l'impact potentiel des cyberattaques, afin de modéliser avec davantage de réalisme la dynamique longitudinale des véhicules au sein d'un peloton.

$$\dot{v}_n(t) = a \left[ 1 - \left( \frac{v_n(t)}{v_0} \right)^{\delta} - \left( \frac{s^* \left( v_n(t), \Delta \tilde{v}_{\text{eff}}(t - \tilde{\tau}) \right)}{\tilde{s}_{\text{eff}}(t - \tilde{\tau})} \right)^2 \right] \tag{2.1}$$

Les perturbations dans un peloton peuvent provenir non seulement d'erreurs techniques ou de défaillances de communication, mais également d'attaques intentionnelles. Ces anomalies entraînent une perte de synchronisation entre les véhicules : certains freinent ou accélèrent au mauvais moment, ce qui peut provoquer des comportements imprévisibles, voire des accidents.

Plusieurs scénarios d'attaques ont été étudiés. Par exemple, lorsqu'un véhicule reçoit une information erronée concernant sa vitesse, il peut réagir de manière inappropriée et perturber la dynamique globale du peloton. D'autres attaques consistent à rejouer d'anciens messages (attaques par relecture) ou à orchestrer une action coordonnée de plusieurs véhicules compromis, dans le but de générer volontairement du désordre et de l'instabilité au sein du groupe.

En définitive, ces travaux soulignent l'importance de surveiller à la fois l'état physique des véhicules et l'intégrité des communications inter-véhicules (V2V), afin de préserver la stabilité et la sécurité de la conduite en peloton.

### Discussion et critiques

L'article présente néanmoins plusieurs limites. Les modèles proposés reposent sur des hypothèses simplificatrices, telles que l'idée que tous les véhicules possèdent des caractéristiques identiques ou que la route est parfaitement rectiligne, ce qui réduit leur applicabilité à des scénarios plus complexes et réalistes. Par ailleurs, l'absence de métriques spécifiques pour évaluer les impacts telles que le temps de collision ou les variations d'espacement constitue une faiblesse notable. Enfin, les simulations se limitent à un peloton de 15 véhicules, ce qui empêche d'examiner les effets à grande échelle, notamment dans le cas de formations plus importantes.

## 2.5 Comparaison des approches étudiées

Le Table 2.1 illustre la comparaison entre les travaux présentés précédemment.

| **Solution** | **Technologie utilisée** | **Menaces prises en compte** | **Niveau de sécurité / confidentialité** | **Type de communication** |
|---|---|---|---|---|
| **HAFC [10]** | Contrôle longitudinal hybride basé sur modèle et consensus | Collision, désynchronisation | Élevé | V2V |
| **H3PC [3]** | Contrôle prédictif hiérarchique, formation 3D | Défaillance de capteur, désalignement | Moyen | V2V + perception |
| **CIDM [15]** | Modèle dynamique coopératif intelligent | Faux messages, relecture, attaques coordonnées | Faible à moyen | V2V |
| **VLC + CSK [11]** | Communication optique (VLC) + modulation colorimétrique (CSK) | Sybil, retard, DoS | Moyen | VLC |
| **Blockchain + Platoon Cloud [6]** | Blockchain, cloud distribué, IA | Non-répudiation, intégrité, Sybil | Élevé | V2C + Cloud |
| **SPMSA [8]** | ECDH, ECDSA, ECIES modifié, réseau 5G | Sybil, interception, relecture, falsification, perte d'intégrité | Très élevé | V2V + 5G + cryptographie |
| **5G C-V2X [9]** | 5G-V2X, 5G-AKA, GUTI, Signcryption | Usurpation d'identité, écoute, traçage, falsification de messages | Élevé | V2V (PC5), V2I (Uu) |

TABLE 2.1 – Tableau comparatif des solutions de sécurité du platooning.

L'étude comparative des solutions de sécurisation appliquées au platooning met en évidence deux grandes orientations. D'une part, les approches centrées sur le contrôle dynamique coopératif telles que HAFC, H3PC ou CIDM cherchent avant tout à renforcer la stabilité et la fluidité du peloton. Toutefois, elles demeurent limitées face à des attaques sophistiquées, comme l'injection de faux messages ou les attaques de type Sybil. D'autre part, les approches axées sur la sécurisation des communications et l'authentification à l'image de SPMSA, de l'intégration de la blockchain avec le Platoon Cloud ou encore du recours au VLC associé au codage CSK privilégient la confidentialité, l'intégrité et l'authenticité des échanges inter-véhiculaires. Bien qu'elles offrent un niveau de sécurité élevé, ces solutions se heurtent à une forte complexité computationnelle et dépendent largement de l'infrastructure réseau.

Cette analyse met ainsi en évidence les atouts spécifiques de chaque approche, mais aussi leurs limites, notamment en termes de scalabilité, de résilience face à des attaques avancées ou encore de surcharge computationnelle dans des environnements contraints. Aucune des solutions existantes ne parvient à satisfaire simultanément l'ensemble de ces critères, ce qui souligne la nécessité de concevoir un modèle plus équilibré.

Dans cette perspective, et dans la continuité des travaux consacrés à la sé-

curisation des communications dans les pelotons de véhicules autonomes, nous proposons une approche hiérarchisée et résiliente. Contrairement aux solutions fortement dépendantes de la 5G, de la blockchain ou de systèmes cryptographiques centralisés, notre protocole articule la désignation du leader et son authentification en deux niveaux complémentaires : d'abord au sein du Contrôleur Fonctionnel de Haute Autorité (HAFC), puis via le système PASS, en collaboration avec les unités en bord de route (RSU). Cette double authentification instaure un climat de confiance durable au sein du convoi, tout en réduisant la dépendance à une architecture purement centralisée.

## 2.6 Conclusion

La sécurité du platooning de véhicules autonomes constitue un enjeu essentiel afin de garantir simultanément la sûreté, la confiance et l'efficacité des déplacements en convoi. Dans ce chapitre, nous avons mené une étude approfondie des solutions existantes, en les évaluant au regard de critères précis : confidentialité, intégrité, authentification, résistance aux attaques, latence, charge computationnelle et robustesse face à la dynamique du peloton.

Le chapitre suivant sera consacré à la présentation de notre propre approche : une solution hybride conçue pour renforcer la sécurité du platooning, tout en restant compatible avec les contraintes pratiques des véhicules autonomes connectés.

# 3

# Secure Autonomous Platooning through Leader Selection and Multi-Layer Authentication

## 3.1 Introduction

Dans le chapitre précédent, nous avons examiné les différentes approches existantes visant à sécuriser les communications au sein d'un peloton de véhicules autonomes. Bien que certaines de ces solutions se révèlent efficaces sur des aspects particuliers, aucune ne parvient à couvrir pleinement l'ensemble des exigences de sécurité, en particulier en ce qui concerne l'authentification, la résistance aux attaques et la robustesse face aux dynamiques du peloton.

Dans ce chapitre, nous présentons notre contribution à travers une approche de gestion de peloton, nommée PDHP (Proof-of-Work and Dilemma-based Hybrid Protocol (HAFC+PASS)) dans un environnement de véhicules connectés. Nous commençons par exposer les motivations qui sous-tendent cette proposition. Ensuite, nous décrivons le modèle réseau de notre système de gestion et d'authentification du leader, en formulant les hypothèses nécessaires à son bon fonctionnement. Par la suite, nous détaillons les différentes phases constituant l'approche proposée. Enfin, nous clôturons le chapitre par une analyse de

sécurité de notre protocole.

## 3.2 Motivation

Dans un peloton de véhicules autonomes, la coordination collective repose sur un échange continu d'informations via les communications véhicule-à-véhicule (V2V). Ces interactions sont indispensables pour assurer la cohésion, la sécurité et l'efficacité du peloton. Toutefois, cette interconnectivité accroît également la surface d'attaque et expose le système à diverses menaces, telles que les attaques Sybil, la falsification de messages ou encore les attaques par rejeu. Ces vulnérabilités peuvent compromettre gravement la stabilité du convoi et conduire à des dysfonctionnements critiques, voire à des collisions.

Afin de contrer ces menaces, nous proposons un mécanisme de sécurité structuré en deux phases principales. La première consiste en une sélection du leader reposant sur des preuves simples de participation passée, garantissant l'authenticité et la légitimité du véhicule candidat au sein du peloton. La seconde correspond à une authentification renforcée du leader, articulée en deux étapes : une authentification rapide sans certificat à l'aide du modèle HAFC (High Authority Functional Controller), suivie d'une vérification complète avec certificat pseudonyme via le système PASS (Platoon Authentication and Secure System), en collaboration avec les unités en bord de route (RSU).

L'objectif de notre approche est d'établir un compromis optimal entre sécurité, performance et robustesse du système de platooning.

## 3.3 Modèle du réseau et hypothèses

Dans le cadre de notre approche, chaque convoi de véhicules autonomes repose sur une architecture semi-centralisée, dans laquelle le véhicule leader agit en tant que gestionnaire de la confiance. Contrairement aux approches classiques où le leader est authentifié dès sa désignation, nous proposons qu'il n'obtienne cette authentification qu'après avoir évalué le comportement de ses suiveurs. Il commence donc par surveiller localement les interactions au sein du peloton, en s'appuyant sur un protocole de coopération sécurisé. Une fois la chaîne de confiance interne validée, le leader peut alors être authentifié de manière fiable vis-à-vis des entités externes telles que le serveur cloud.

L'élément central de notre contribution est l'intégration de fonctions cryptographiques et de la théorie des jeux dans le modèle de peloton. Chaque véhicule

connaît précisément son prédécesseur et son successeur (notés PM1, PM2, etc.), ce qui permet d'assurer une chaîne de confiance distribuée, robuste et traçable dans l'ensemble du convoi (cf. Figure 3.1).

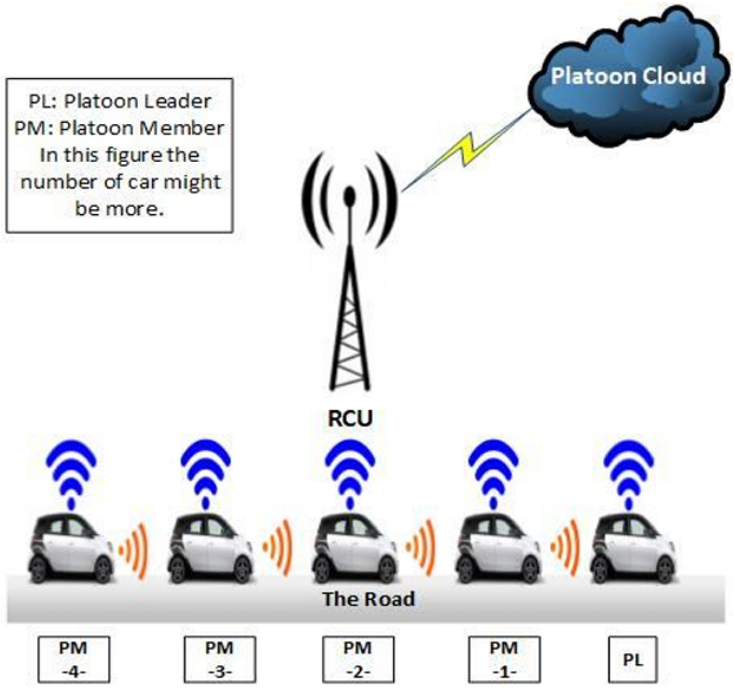



FIGURE 3.1 – Modèle de platoon [6].

## 3.4 Proposition

Dans cette section, nous décrivons en détail notre protocole de sélection et d'authentification sécurisée du leader dans un système de platooning coopératif. L'objectif principal de ce protocole est de garantir un mécanisme fiable de désignation du leader, fondé sur la confiance établie entre les véhicules, ainsi qu'un processus d'authentification sécurisé et anonyme, assurant l'intégrité du rôle de leader au sein du peloton.

Le protocole proposé se compose de deux phases principales :

la désignation du leader via une preuve de travail et une stratégie de coopération (Tit-for-Tat) ;

l'authentification du leader, subdivisée en deux sous-phases : une authentification rapide via HAFC (sans certificat), suivie d'une vérification stricte via le protocole PASS avec la collaboration d'une unité RSU.

Les principaux acteurs et paramètres intervenant dans le protocole, ainsi que les significations de tous les paramètres utilisés, sont récapitulés dans la Table 3.1 et la Table 3.2, respectivement.

| **Acteur** | **Description** |
|---|---|
| Véhicules normaux (PM) | Membres coopératifs du peloton, qui suivent les instructions reçues et contribuent à la sécurité collective. |
| Leader (PL) | Coordinateur légitime chargé de diffuser les consignes de mouvement (vitesse, trajectoire) à l'ensemble du groupe. |
| Véhicule pirate | Entité malveillante tentant d'usurper le rôle de leader pour perturber le peloton. |

TABLE 3.1 – Description des acteurs du peloton.

| **Notation** | **Description** |
|---|---|
| $ID_i$ | Identifiant unique du véhicule $i$ |
| $T_i$ | Estampille temporelle locale du véhicule $i$ |
| $PoW_i$ | Preuve de travail proposée par le véhicule $i$ |
| $X_i$ | Valeur aléatoire utilisée pour générer une preuve de travail |
| $H(\cdot)$ | Fonction de hachage cryptographique sécurisée |
| $Score_i$ | Score de confiance attribué au véhicule $i$ |
| $G$ | Un groupe en mathématiques fini |
| $q$ | L'ordre d'un groupe (le nombre d'éléments qu'il contient) |
| $g, h$ | Générateurs publics du groupe $G$ |
| $C$ | Engagement cryptographique envoyé par le leader |
| $S$ | Un secret à engager |
| $t$ | Un nombre aléatoire |
| $sk_i$ | Clé privée du véhicule $i$ |
| $pk_i$ | Clé publique du véhicule $i$ |
| $R$ | Composant de l'engagement temporaire |
| $s$ | Composant d'une signature prouvant l'authenticité |
| $\sigma$ | Signature complète transmise avec l'engagement |
| $e$ | Challenge dérivé du message signé |
| $\text{Pseudo}_L$ | un pseudonyme |
| $PK_L$ | une clé publique temporaire |
| $Date_{\text{expiration}}$ | une limite de validité |
| $Signature_{TA}(...)$ | une signature faite par une autorité de confiance (TA) |
| $Cert_L$ | Certificat pseudonyme utilisé par le leader |
| $CLU$ | Identifiant temporaire attribué au leader après validation |

TABLE 3.2 – Notations utilisées dans le protocole de sélection et d'authentification du leader.

### 3.4.1 La désignation du leader

#### 3.4.1.1 Vérification d'ancienté

Le leader du peloton est remplacé à intervalles réguliers, soit après une certaine distance parcourue, soit après une période donnée. Cette rotation vise à optimiser les paramètres physiques (notamment l'énergie électrique consommée par les capteurs) ainsi que les mesures de sécurité, en assurant un contrôle fréquent de l'intégrité du leader. Pour cela, la communication relative à l'ordre de changement de leader est centralisée : le leader actuel informe l'ensemble des membres du peloton qu'il est temps d'effectuer la rotation du leadership.

Une fois l'ordre de changement de leader reçu par les membres du peloton (PM), ceux-ci entrent dans la première partie de cette phase, où les véhicules candidats doivent prouver leur ancienneté dans le peloton grâce à une preuve de travail légère (voir la Figure 3.2).

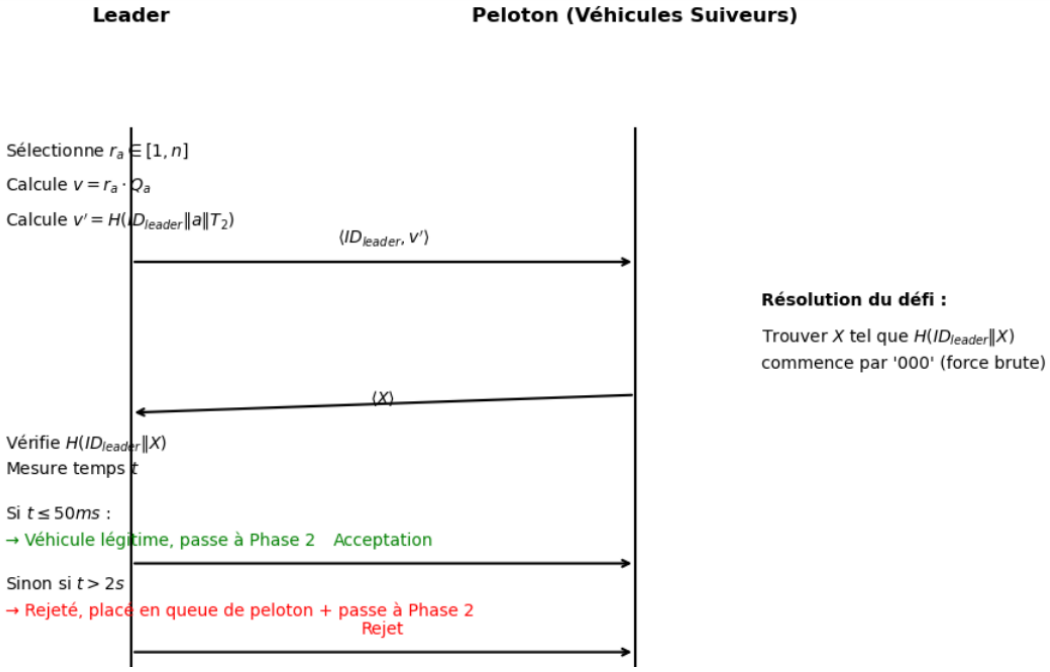



FIGURE 3.2 – Preuve de travail.

Le leader commence par choisir un nombre aléatoire $r_a \in [1, n]$. À partir de ce nombre, il calcule un point elliptique $v = r_a \cdot Q_a$, où $Q_a$ est sa clé publique.

Ensuite, il génère un engagement $v'$ en appliquant une fonction de hachage sécurisée sur l'identifiant du leader, une valeur aléatoire $a$, et une estampille

temporelle $T_2$ (pour prouver que le message est récent et authentique), soit :

$$v' = H(ID_{leader} \,\|\, a \,\|\, T_2)$$

Les membres du peloton doivent ensuite résoudre un défi cryptographique : il s'agit de trouver une valeur $X$ telle que le hachage de la concaténation $ID_{leader} \,\|\, X$ commence par les trois zéros "000".

Cette étape permet au leader de signaler au système qu'un nouveau véhicule est entré dans le peloton sans répondre correctement au test. En conséquence, le système ordonne de maintenir ce véhicule en queue du peloton, afin d'empêcher qu'il ne devienne leader avant d'avoir prouvé sa légitimité. Donc le véhicule pourra accéder à la seconde phase de validation.

#### 3.4.1.2 Èlimination des tricheures

Après la première étape, le leader prend une décision et attribue à chaque véhicule un score de confiance ($0 < \text{score} > 1$). Ce score dépend notamment des paramètres physiques et temps nécessaire pour résoudre la preuve de travail : plus ce temps est court, plus le score est élevé (voire Figure 3.3).

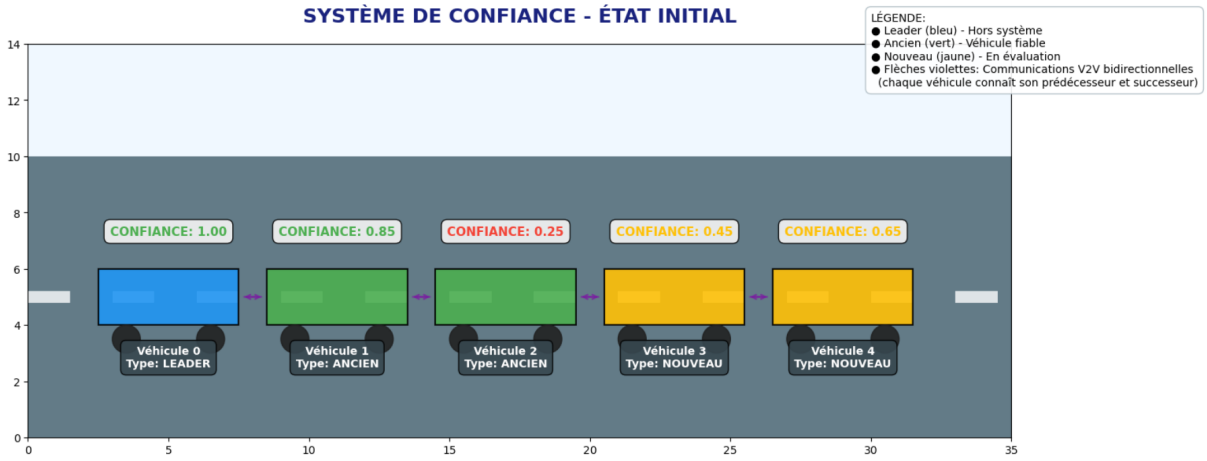
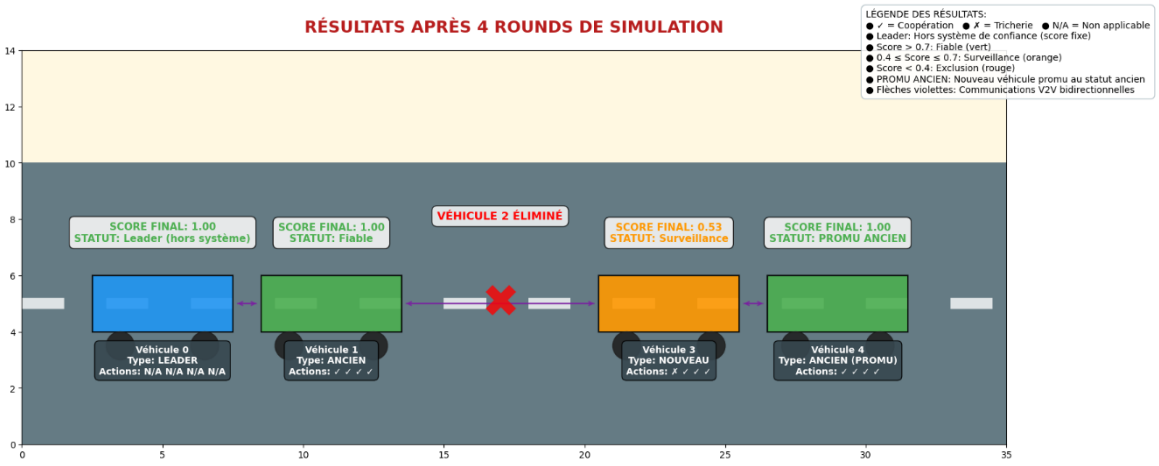



FIGURE 3.3 – Initialisation.

Dans un peloton de véhicules autonomes, chaque véhicule est surveillé en fonction de son comportement : il peut soit coopérer (en communiquant correctement), soit tricher (en perturbant les échanges). À chaque interaction, un score de confiance est ajusté à l'aide de l'algorithme du Dilemme du Prisonnier.

Cet algorithme repose sur une stratégie simple et réciproque. Chaque véhicule commence par coopérer lors de la première interaction. Par la suite, à chaque round, il réplique exactement l'action effectuée par l'autre véhicule au tour précédent. Ainsi, si l'autre a coopéré, il coopère également ; et si l'autre a triché, il triche en retour.

À chaque tour, le véhicule envoie son action, reçoit celle de l'autre, puis l'enregistre dans un historique afin de l'utiliser lors du round suivant. Cette stratégie favorise la coopération mutuelle tout en sanctionnant immédiatement tout comportement déloyal, comme illustré dans la Figure 3.4.




RÉCAPITULATIF DES SCORES ET ACTIONS - TROIS SCÉNARIOS

| Véhicule | Type initial | Actions | Score final | Statut final |
|---|---|---|---|---|
| Véh 0 | leader | N/A N/A N/A N/A | 1.00 | Leader (hors système) |
| Véh 1 | ancien | ✓ ✓ ✓ ✓ | 1.00 | Fiable |
| Véh 2 | ancien | ✗ ✗ ✗ ✗ | 0.00 | Exclu |
| Véh 3 | nouveau | ✗ ✓ ✓ ✓ | 0.53 | Surveillance |
| Véh 4 | nouveau | ✓ ✓ ✓ ✓ | 1.00 | Promu ANCIEN |

FIGURE 3.4 – Dilemme du Prisonnier.

Ce mécanisme intelligent utilise des règles adaptées pour chaque type de véhicule. Les nouveaux venus bénéficient d'un système plus indulgent : ils gagnent plus de points quand ils coopèrent et perdent moins de points en cas d'erreur, ce qui leur permet de s'intégrer plus rapidement. À l'inverse, les anciens membres reçoivent des récompenses modestes pour leur coopération, mais subissent des pénalités sévères s'ils trichent, car leur position centrale dans le peloton est cruciale.

L'innovation clé réside dans la sélection des leaders : le véhicule qui excelle à la fois dans la phase initiale d'authentification (preuve de travail) et dans ce jeu de confiance devient automatiquement éligible au rôle de leader. Cette combinaison garantit que seuls les membres les plus fiables et compétents accèdent au leadership (le véhicule 2 est élu comme prochain leader et intègre la phase

2).

### 3.4.2 L'authentification

Une fois le leader élu, le processus d'authentification est mis en uvre pour garantir l'authenticité de manière sécurisée et anonyme, à l'aide des modèles HAFC et PASS.

#### 3.4.2.1 Authentification rapide avec HAFC

Cette première étape vise à authentifier le leader du convoi de manière anonyme auprès du véhicule suiveur. Elle ne repose pas sur un certificat classique, mais utilise des signatures, des engagements, ainsi que le protocole Challenge-Response.

(a) **Le leader génère une preuve cryptographie :** le leader du convoi doit généré une preuve cryptographie, ce protocole consiste a :

i. **Engagement homomorphe :** Ces engagements sont comme des coffres-forts numériques dans lesquels tu caches une valeur sans la dévoiler. Le leader s'engage sur certaines informations sensibles en utilisant ce schéma. Cela nous permet de protège la vie privée et nous permet de vérifier rapidement plusieurs informations sans les exposer.

Dans notre travail, nous utilisons la version Pedersen Commitment, car il est difficile de s'engager sur deux valeurs différentes pour le même engagement, et elle est additivement homomorphique, ce qui veut dire :

$$\mathrm{Com}(m_1, r_1) \cdot \mathrm{Com}(m_2, r_2) = \mathrm{Com}(m_1 + m_2, r_1 + r_2)$$

Cela indique que si tu multiplies deux engagements, cela est équivalent à créer un engagement combiné des messages $m_1 + m_2$ et $r_1 + r_2$.

$\mathrm{Com}(m_1, r_1)$ représente un engagement du message $m_1$ avec un sel $r_1$.

$\mathrm{Com}(m_2, r_2)$ représente un engagement du message $m_2$ avec un sel $r_2$.

**Calculer l'engagement :**

Pour calculer l'engagement à envoyer par le leader aux suiveurs du convoi, nous utilisons la formule suivante :

$$C = C_{g,h}(S, t) = g^S \cdot h^t$$

— $g^S$ **:** encode le secret $S$
— $h^t$ **:** ajoute un masque aléatoire à l'aide de $t$.

L'engagement $C$ est comme une boite ferme qui contient le message $S$ cache , avec un verrou aleatoire $t$.

ii. **Une signature sans certificat :** La signature ajoutée au leader sert à vérifier l'authenticité de l'engagement qui doit être envoyé aux suiveurs, afin d'empêcher les attaquants de générer un engagement à la place du leader, et de prouver que cet engagement a bien été généré par le leader légitime.

Dans notre travaille , nous allons prendre en considération la signature *Schnorr modifié* qui est présenter comme suit :

— **Calcule d'un engagement temporaire :**

$$R = g^k \bmod p$$

— **Hachage de l'engagement :** Le leader concatène le message $C$ et $R$, puis calcule un hachage de la concaténation pour obtenir le challenge $e$ :

$$e = H(C \parallel R)$$

Le hachage garantit que la signature est dépendante du message et de l'engagement, ce qui rend la signature difficile à falsifier.

— **Calcul de la réponse** $s$ **:** Une fois que le leader a obtenu le challenge $e$, il calcule la réponse $s$, qui est la signature proprement dite :

$$s = k + sk \cdot e \bmod q$$

Après avoir généré une preuve cryptographique en combinant l'engagement homomorphe et la signature sans certificat, ce couple est transmis aux suiveurs pour leur proposer un challenge visant à vérifier la légitimité du leader.

Le leader envoie alors le message signé sous la forme :

$$(C, \sigma) = (C, (R, s))$$

(b) **Les véhicule suiveurs vérifier cette preuve**

Tous les véhicules suiveurs du leader vérifient que :

$$g^s \stackrel{?}{=} R \cdot pk^e$$

⇒ Si cette équation est vraie, alors :
— Le leader connaît bien $sk$ (sa clé privée),
— Il est bien l'auteur de l'engagement $C$,
— Donc il est authentifié avec succès.

#### 3.4.2.2 Vérification strict via le protocole PASS

(a) **Le leader envoie des données à la RSU :** Le leader envoie trois éléments importants :

i. **Certificat pseudonyme $\text{Cert}_L$**
C'est comme une carte d'identité anonyme. Il contient : $\text{Pseudo}_L$ , $PK_L$ , $\text{Date}_{\text{expiration}}$ , $\text{Signature}_{TA}(...)$

ii. **Signature de Schnorr $\sigma = (R, s)$**
Elle prouve que le leader possède bien la clé privée liée à $PK_L$, c'est-à-dire qu'il est l'auteur légitime du certificat.

iii. **Engagement $C$ (optionnel)**
Parfois, le leader ajoute un engagement cryptographique, comme un engagement de Pedersen :

$$C = g^s \cdot h^t$$

(b) **Vérification par la RSU :** La RSU reçoit $\text{Cert}_L$, $(R, s)$, et doit faire deux types de vérifications :

i. **Vérification du certificat pseudonyme**

La RSU vérifie la signature du certificat, signée par l'autorité de confiance (TA), en utilisant la clé publique de cette dernière afin de s'assurer que $\text{Cert}_L$ est valide et authentique. Si la signature est correcte, la cle $(PK_L)$ est acceptée ; sinon, le certificat est rejeté.

ii. **Vérification de la signature de Schnorr $\sigma = (R, s)$**
Maintenant que la RSU accepte la clé publique $PK_L$, elle veut vérifier que le leader connaît bien la clé privée associée.

— **Recalcul du challenge :**

$$e = H(C \parallel R)$$

— **Calcul de la valeur théorique :**

$$V = g^s \cdot (PK_L)^{-e} \mod p$$

— **Vérification finale :**

$$V \stackrel{?}{=} R$$

— Si l'égalité est vérifiée : la signature est valide, donc le leader est légitime.
— Sinon : on rejette le message.

iii. **Calcul du CLU (Credential Linking Unit)**

Une fois que la RSU a vérifié que le leader est légitime, elle peut calculer un identifiant temporaire, appelé CLU :

$$CLU = H(PK_L \parallel \text{Timestamp} \parallel RSU\_ID)$$

Cela permet à la RSU de suivre temporairement le comportement du leader (par exemple, pour éviter les attaques répétées) sans compromettre son anonymat. En effet, le CLU est une valeur de hachage, il est donc impossible de retrouver l'identité réelle à partir de cette valeur.

## 3.5 Analyse de sécurité

Dans cette section, nous analysons les propriétés de sécurité de la solution proposée pour montrer qu'elle résiste aux attaques suivantes.

### 3.5.1 Attaque d'usurpation d'identité

L'attaque d'usurpation d'identité, également appelée attaque par spoofing, est une attaque dans laquelle un adversaire assume avec succès l'identité de l'une des parties légitimes dans un système ou dans un protocole de communication.

Contrairement aux approches classiques basées uniquement sur des certificats, notre protocole combine une authentification rapide sans certificat

(HAFC) et une vérification réseau via certificats pseudonymes (PASS), renforçant ainsi la résistance contre l'usurpation d'identité.

Dans la phase HAFC, le leader du convoi prouve anonymement sa légitimité aux véhicules suiveurs à l'aide d'un engagement cryptographique et d'une signature Schnorr liée à sa clé privée, empêchant tout attaquant de falsifier son identité sans connaître cette clé.

Dans la phase PASS, le leader prouve son identité au réseau en présentant un certificat pseudonyme signé, vérifié par une RSU, ce qui empêche toute tentative de se faire passer pour un véhicule autorisé.

Grâce à ce double mécanisme, notre système garantit que seule une entité réellement autorisée peut agir en tant que leader, rendant l'usurpation d'identité cryptographiquement infaisable.

### 3.5.2 Attaque de l'homme du milieu et rejeu

Dans une attaque de l'homme du milieu (man-in-the-middle attack), un intrus malveillant s'interpose entre deux entités communicantes, se faisant passer pour chacune d'elles à leur insu, et accède ainsi aux informations échangées.

Dans le cadre de notre approche HAFC+PASS, cette solution protège efficacement contre ce type d'attaque en combinant des engagements homomorphes, des signatures anonymes sans certificat et un mécanisme d'authentification par challenge-réponse.

Lorsqu'un attaquant tente d'intercepter ou de modifier les messages entre un leader et ses suiveurs, il lui est impossible de forger une signature Schnorr valide ou de falsifier l'engagement cryptographique sans connaître la clé privée du leader. De plus, le protocole PASS renforce cette sécurité en validant l'identité du leader à l'aide d'un certificat pseudonyme, empêchant toute substitution ou injection frauduleuse.

Ainsi, toute tentative d'attaque est automatiquement détectée lors de la phase de vérification.

### 3.5.3 Attaque Sybil

Il s'agit d'une version avancée de l'attaque d'usurpation d'identité, dans laquelle un nud malveillant peut prétendre être plusieurs nuds légitimes ou

inexistants dans le réseau. En d'autres termes, l'attaquant peut revendiquer différentes identités dans le but de prendre l'avantage sur les nuds légitimes.

Grâce à l'association de l'authentification rapide anonyme (HAFC) et du mécanisme d'identification pseudonyme (PASS), notre protocole permet de limiter efficacement les attaques de type Sybil. En effet, chaque véhicule possède un certificat pseudonyme délivré par une autorité de confiance, et chaque preuve cryptographique générée est liée à une seule identité pseudonyme unique.

Ainsi, un attaquant ne peut prétendre à plusieurs identités sans posséder autant de certificats valides, ce qui complique considérablement la réalisation d'une attaque Sybil. Par conséquent, le système détecte et rejette les entités suspectes tentant d'introduire de multiples identités dans le réseau.

### 3.5.4 L'attaque par rejeu

L'attaque par rejeu est une attaque où un adversaire intercepte un message valide échangé entre deux entités et le retransmet ultérieurement dans le but de tromper le destinataire, en le faisant passer pour un message légitime et récent.

En intégrant des engagements aléatoires et des signatures éphémères dans HAFC, couplés aux certificats pseudonymes de PASS, notre protocole empêche efficacement les attaques par rejeu. À chaque session, le leader génère un engagement unique basé sur un nonce aléatoire, ce qui rend chaque preuve cryptographique strictement liée à un moment précis.

Ainsi, même si un attaquant intercepte un message signé, il ne pourra pas le rejouer avec succès, car la signature deviendra invalide dans un nouveau contexte temporel ou topologique. Cette propriété garantit que seules les communications fraîches et authentiques sont acceptées par les véhicules suiveurs et les unités RSU.

## 3.6 Conclusion

Ce chapitre a présenté notre modèle d'authentification pour le platooning, structuré en deux phases clés. Grâce à une vérification coordonnée entre HAFC, PASS et les RSU, notre solution permet une sécurisation efficace des échanges inter-véhiculaires, tout en tenant compte des contraintes de mobilité.

Le chapitre suivant présentera les résultats d'évaluation de cette solution dans divers scénarios de simulation.

# 4

# SIMULATION ET ÉVALUATION DE PERFORMANCES

## 4.1 Introduction

Ce chapitre est consacré à l'évaluation des performances de notre protocole d'authentification. Nous présenterons, en premier lieu, l'environnement et les paramètres de simulation considérés pour l'évaluation des performances de notre solution. Nous décrirons, par la suite, les critères et métriques de simulation utilisés. Les résultats obtenus à l'issue de ces simulations seront finalement interprétés et comparés avec deux protocoles étudiés dans le chapitre de l'état de l'art.

## 4.2 Métriques considérées

Afin d'évaluer les performances de notre protocole, nous considérons les métriques de performances suivantes :

— **Coût de communication** : Le nombre total d'octets envoyés par un vé-

hicule dans le système à chaque exécution du protocole.
— **Temps de traitement** : Le temps nécessaire à un véhicule pour exécuter toutes les opérations du protocole.
— **Coût de stockage** : L'espace mémoire requis pour stocker les paramètres cryptographiques et les clés.
— **Énergie consommée** : L'énergie totale dépensée par l'ensemble des véhicules du réseau.

## 4.3 Paramètres de simulation

Pour tester notre protocole de sécurité dans un contexte de platooning, nous avons développé une simulation en Java, dans laquelle plusieurs véhicules coopèrent pour élire un leader, échanger des messages sécurisés et valider les identités. Afin de représenter un scénario réaliste, nous avons utilisé les trois paramètres principaux illustrés dans le tableau 4.1.

| **Paramètre** | **Description** |
|---|---|
| Énergie consommée par le leader | Estimée entre 0,25 et 1,08 joules selon le nombre de véhicules et la durée du protocole. |
| Portée des communications V2V | Fixée à 30 mètres pour simuler la distance moyenne entre véhicules dans le peloton. |
| Paramètres cryptographiques | p , q , g, h. |

Table 4.1 – Paramètres de simulation.

L'énergie consommée par le leader correspond à l'ensemble des calculs qu'il effectue : preuve de travail, génération de signature, envoi de messages, etc. Elle est estimée à l'aide d'une formule simple prenant en compte le *temps total d'exécution* (en millisecondes) et le *nombre de véhicules* :

$$\text{Énergie (J)} = 0{,}0012 \times \text{temps\_total (ms)} \times \text{nombre\_de\_véhicules} \quad (4.1)$$

Cette approche permet de représenter la charge de calcul du leader dans un système embarqué, sans avoir besoin de modéliser l'énergie physique réelle utilisée par un véhicule.

## 4.4 Évaluation des performances

Pour vérifier si notre protocole PDHP est efficace dans un environnement de *platooning*, nous avons mené plusieurs simulations en faisant varier le nombre de véhicules dans le peloton (3, 5, 7, 9 et 12). L'objectif est de comparer notre approche à deux solutions récentes de l'état de l'art : (1) H3PC [3], proposée par Chah et al., qui combine *fog computing* et *blockchain* pour sécuriser les communications entre véhicules, et (2) une approche blockchain renforcée, proposée par Hexmoor, Alsamarace et Almaghshi [6], fondée sur une architecture distribuée.

Pour chaque scénario, 10 tests ont été réalisés et la moyenne de 25 itérations a été utilisée pour assurer des résultats fiables. Les métriques suivantes ont été mesurées :
— le **coût de communication**
— le **temps de traitement**,
— le **coût de stockage**
— et la **consommation d'énergie**.

### 4.4.1 Coût de communication

La Figure 4.1 montre l'évolution du volume de données échangées en fonction du nombre de véhicules. Notre protocole PDHP présente un coût de communication inférieur aux autres solutions, particulièrement pour les grands pelotons. Cette efficacité s'explique par l'utilisation d'une preuve de travail simplifiée pour l'élection du leader, l'absence de certificats numériques réduisant la taille des messages, et l'échange minimal d'informations essentielles entre véhicules. En comparaison, H3PC génère un trafic supplémentaire dû aux échanges avec les serveurs *fog*, tandis que la blockchain renforcée nécessite des synchronisations fréquentes, ce qui alourdit les communications, surtout avec un grand nombre de véhicules..

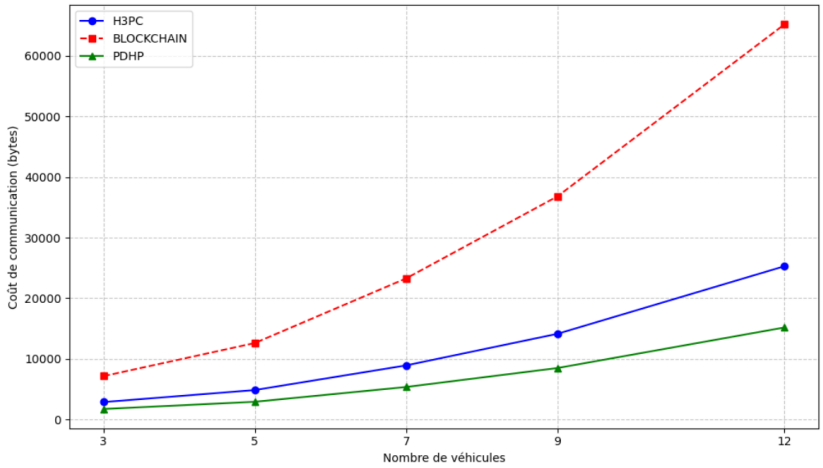



FIGURE 4.1 – Coût de communication global en fonction de nombre de véhicules.

### 4.4.2 Temps de traitement

La Figure 4.2 illustre le temps d'exécution des opérations cryptographiques. PDHP maintient des temps de traitement réduits, même pour les grands pelotons, grâce à l'utilisation d'opérations légères comme SHA-256, à l'absence de gestion de certificats complexes, et à une méthode de sélection de leader optimisée. À l'inverse, H3PC introduit des délais supplémentaires dus aux vérifications côté *fog*, et la blockchain renforcée nécessite des validations plus longues pour la création des blocs, ce qui devient particulièrement critique avec l'augmentation du nombre de véhicules.

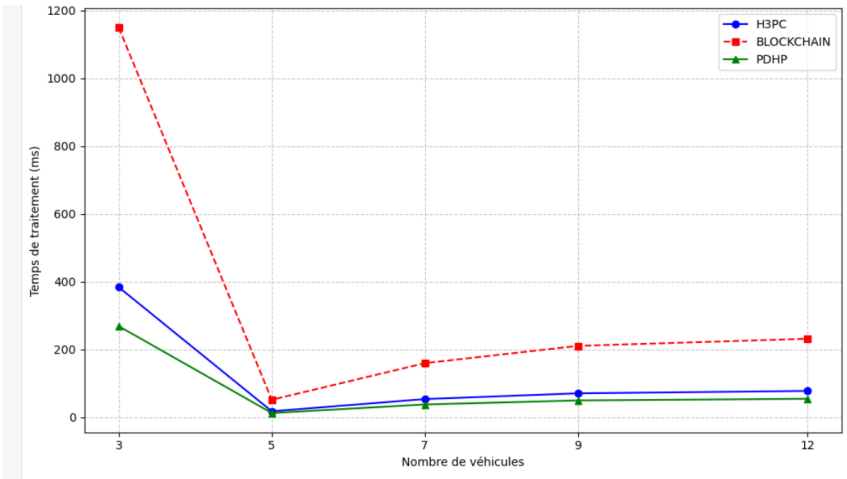



FIGURE 4.2 – Temps de traitement global en fonction de nombre de véhicules.

### 4.4.3 Coût de stockage

Comme le montre la Figure 4.3, PDHP minimise l'espace mémoire requis pour le stockage des paramètres sécuritaires, et ce, même lorsque le nombre de véhicules augmente. Cette efficacité provient de la conservation exclusive des éléments essentiels à la vérification, de l'absence de certificats et d'archives complexes, ainsi que d'un modèle de stockage distribué optimisé. Les approches comparées nécessitent un stockage plus important : H3PC pour les journaux de session et les informations *fog*, et la blockchain renforcée pour le stockage des blocs et des résumés, ce qui devient particulièrement lourd pour les grands pelotons.

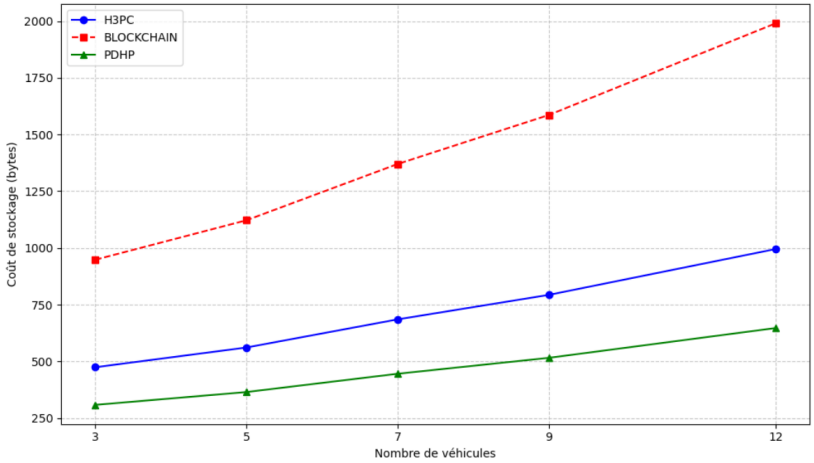



FIGURE 4.3 – Coût de stockage dans chaque objet en fonction de nombre de véhicules.

### 4.4.4 Énergie consommée

La Figure 4.4 démontre l'efficacité énergétique de PDHP, particulièrement notable pour les grands pelotons. Cette performance s'explique par la réduction du nombre de messages échangés, l'utilisation d'opérations cryptographiques légères et l'élimination des redondances ainsi que des vérifications superflues. En comparaison, H3PC consomme plus d'énergie à cause des échanges avec les serveurs *fog*, et la blockchain renforcée nécessite une énergie importante pour la propagation et la validation des blocs, une consommation qui augmente significativement avec le nombre de véhicules.

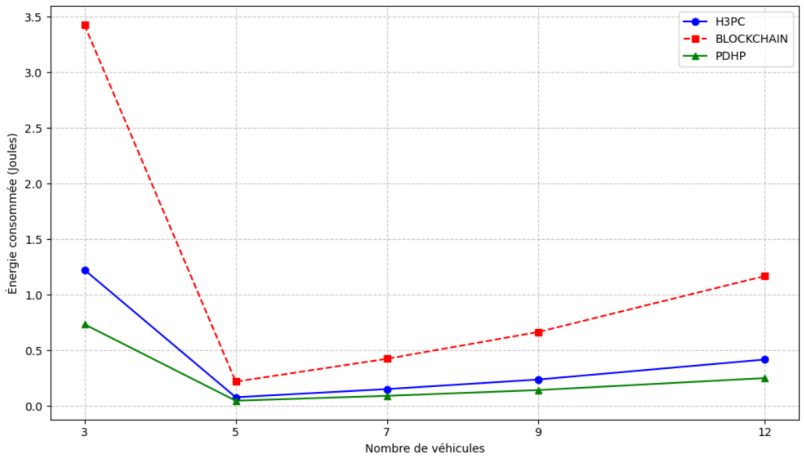



FIGURE 4.4 – Énergie consommée en fonction de nombre de véhicules.

## 4.5 Conclusion

Ce chapitre a présenté une analyse comparative des performances de notre protocole par rapport à d'autres protocoles existants dans la littérature, à l'aide d'un simulateur développé en langage Java. Pour ce faire, nous avons fait varier le nombre de véhicules au sein du peloton afin d'évaluer l'impact de cette variable sur plusieurs métriques de performance, à savoir : le temps d'exécution, la consommation d'énergie, le coût de communication et le coût de stockage. Les résultats obtenus sont prometteurs et démontrent que notre protocole offre des performances supérieures selon les métriques évaluées, ce qui confirme son efficacité et sa pertinence dans un contexte de platooning sécurisé et optimisé.

# Conclusion Générale et Perspectives

Ce mémoire se penche sur un thème novateur : la sûreté dans les systèmes de platooning pour véhicules autonomes. Cette technologie, conçue pour optimiser le flux de circulation  notamment en facilitant l'accès et la sortie des véhicules dans le convoi, ainsi qu'en allégeant la charge cognitive du conducteur  offre plusieurs avantages, tant en matière de sécurité routière que d'économie d'énergie. Toutefois, le bon fonctionnement de ce modèle repose sur la capacité à assurer des communications sûres et fiables entre les véhicules.

Dans un premier temps, nous avons présenté les fondements conceptuels du platooning, en détaillant sa structure, ses processus de communication et les technologies de conduite automatisée qui le rendent opérationnel. Nous avons ensuite mis en lumière les principales vulnérabilités de sécurité auxquelles ces systèmes sont exposés, soulignant ainsi la nécessité de mécanismes robustes garantissant l'authentification, l'intégrité et la confidentialité des données échangées.

L'analyse critique des solutions existantes dans la littérature, menée selon des critères bien définis tels que la résistance aux attaques, la latence, la charge computationnelle et l'adaptabilité aux environnements dynamiques, nous a permis d'identifier leurs points forts ainsi que leurs limites. Cette étude a ouvert la voie à des pistes d'amélioration, concrétisées dans notre proposition en deux phases :  La première concerne la désignation du leader, fondée sur une preuve de travail utilisant des fonctions de hachage, combinée à la théorie des jeux pour établir des liens de confiance entre le leader et les suiveurs.  La seconde phase vise l'authentification, en s'appuyant sur le mécanisme HAFC sans certificat pour les membres du peloton, et sur l'intervention d'unités en bord de route (RSU) via le protocole PASS basé sur des certificats pseudonymes.

Les résultats de simulation, obtenus grâce à une implémentation en langage Java avec un nombre variable de véhicules, sont encourageants. Ils démontrent que notre protocole assure efficacement la sécurité des échanges tout en maintenant de bonnes performances en termes de temps d'exécution, de consommation

énergétique, ainsi que de coûts de communication et de stockage.

En conclusion, notre approche contribue à renforcer la sécurité du platooning sans compromettre les performances du système. Pour les travaux futurs, nous envisageons son intégration dans des environnements réels, ainsi que son évaluation avec de nouvelles normes de communication émergentes, telles que la 6G ou les technologies V2X basées sur l'intelligence artificielle.

# Bibliographie


[1] Axelsson, J. Safety in vehicle platooning : A systematic literature review. IEEE Transactions on Intelligent Transportation Systems 18, 5 (2016), 1033–1045.

[2] Bergenhem, C., Hedin, E., and Skarin, D. Vehicle-to-vehicle communication for a platooning system. Procedia-Social and Behavioral Sciences 48 (2012), 1222–1233.

[3] Chah, B., Lombard, A., Bkakria, A., Abbas-Turki, A., and Yaich, R. H3pc : enhanced security and privacy-preserving platoon construction based on fully homomorphic encryption. In 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC) (2023), IEEE, pp. 4086–4093.

[4] Ghosal, A., Sagong, S. U., Halder, S., Sahabandu, K., Conti, M., Poovendran, R., and Bushnell, L. Truck platoon security : State-of-the-art and road ahead. Computer Networks 185 (2021), 107658.

[5] Grim Occasion. Qu'est-ce quun régulateur de vitesse adaptatif (acc) ?, 2023. Consulté en juin 2025.

[6] Hassija, V., Chamola, V., Zeadally, S., et al. Blockchain for improved platoon security. In Proceedings of the International Conference on Computing, Networking and Communications (ICNC) (2020), IEEE, pp. 232–238.

[7] Janssen, R., Zwijnenberg, H., Blankers, I., and de Kruijff, J. Truck platooning : Driving the future of transportation, February 2015. White Paper.

[8] Junaidi, D. R., Ma, M., and Su, R. Secure vehicular platoon management against sybil attacks. Sensors 22, 22 (2022), 9000.

[9] Liu, F., Liu, D., Sun, Y., Li, D., Cui, J., Guan, Z., and Liu, J. Secure vehicle platooning protocol for 5g c-v2x. In 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) (2021), IEEE, pp. 868–875.

[10] Mohammed, B. A., Al-Shareeda, M. A., Al-Mekhlafi, Z. G., Alshudukhi, J. S., and Al-Dhlan, K. A. Hafc : Handover authenti-

cation scheme based on fog computing for 5g-assisted vehicular blockchain networks. IEEE Access 12 (2024), 6251–6261.

[11] Ndambuki, D. K., and Alhitmi, H. K. Attack mitigation and security for vehicle platoon.

[12] Ornikar. Le freinage automatique d'urgence (afu / aeb), 2025. Consulté le 10 avril 2025.

[13] Taylor, S. J., Ahmad, F., Nguyen, H. N., and Shaikh, S. A. Vehicular platoon communication : Architecture, security threats and open challenges. Sensors 23, 1 (2022), 134.

[14] Valeo. Park4uő automated parking assistance system, 2025. Consulté le 18 avril 2025.

[15] Wang, P., Wu, X., and He, X. Modeling and analyzing cyberattack effects on connected automated vehicular platoons. Transportation Research Part C : Emerging Technologies 129 (2021), 103–142. Manuscript soumis pour publication.

[16] Wikipédia. Aide au maintien dans la file de circulation. `https://fr.wikipedia.org/wiki/Aide_au_maintien_dans_la_file_de_circulation`, 2025. Page consultée le 6 avril 2025.

# Résumé

L'essor des véhicules autonomes a favorisé le développement du platooning, une technologie permettant à plusieurs véhicules de circuler en convoi de manière coordonnée. Ce système vise à améliorer la fluidité du trafic, à réduire la consommation d'énergie et à renforcer la sécurité routière. Toutefois, son efficacité dépend étroitement de la fiabilité et de la sécurité des communications entre les véhicules et les infrastructures routières.
Dans ce contexte, nous proposons une architecture de sécurité hybride articulée en deux phases. La première repose sur un mécanisme de désignation de leader, combinant des fonctions de hachage à la théorie des jeux afin d'établir des relations de confiance dynamiques entre les membres du convoi. La seconde phase concerne une authentification multi-niveaux, réalisée sans certificats classiques grâce au protocole HAFC, et renforcée par l'intervention des unités en bord de route (RSU) via le protocole PASS, fondé sur des certificats pseudonymes.
Une évaluation expérimentale, menée en langage Java à travers divers scénarios de simulation de convoi, a permis de démontrer que la solution proposée garantit un haut niveau de sécurité, tout en préservant d'excellentes performances en termes de latence, de consommation d'énergie, ainsi que de coûts de communication et de stockage.



Mots clés : Platooning, Authentification, Sélection du leader, HAFC, PASS, RSU, Sécurité, Théorie des jeux, Fonction de hachage, Systèmes de transport intelligents, V2X.



# Abstract

The rise of autonomous vehicles has led to the development of platooning, a technology that enables multiple vehicles to travel in a coordinated convoy. This system aims to improve traffic flow, reduce energy consumption, and enhance road safety. However, its effectiveness relies heavily on the reliability and security of information exchanges between vehicles and roadside infrastructures. In this context, wa have proposed a two-phase hybrid security architecture. The first phase is based on a leader selection mechanism, combining hash functions and game theory to establish dynamic trust relationships among convoy members. The second phase addresses multi-layer authentication, carried out without traditional certificates using the HAFC protocol, and reinforced by the involvement of roadside units (RSUs) through the PASS protocol, which relies on pseudonymous certificates. An experimental evaluation, implemented in JAVA across different convoy scenarios, demonstrated that the proposed solution provides a high level of security while maintaining strong performance in terms of latency, energy consumption, communication and storage costs.



Keywords : Platooning, Authentication, Leader Selection, HAFC, PASS, RSU, Security, Game Theory, Hash Function, Intelligent Transportation Systems, V2X.