N° Ordre : .....

UNIVERSITÉ MOHAMED BOUDIAF - M'SILA
FACULTÉ DES MATHEMATIQUES ET DE L'INFOMATIQUE
Département d'informatique

THÈSE

Présentée en vue de l'obtention du grade de

DOCTEUR EN SCIENCES

Filière : Informatique
Spécialité : Informatique

Par :
MOUSSAOUI BOUBAKEUR

Thème

Sécurité et protection de la vie privée dans les réseaux véhiculaires

Soutenue le : .. / .. / ....

Devant le jury composé de :

M. Allaoua Hemmak	MCA	Univ. de M'sila	**Président**
M. Noureddine Chikouche	Professeur	Univ. de M'sila	**Rapporteur**
M. Salim Bitam	Professeur	Univ. de Biskra	**Examinateur**
M. Lamri Sayad	MCA	Univ. de M'sila	**Examinateur**
M. Chaker Abdelaziz Kerrache	MCA	Univ. de Laghouat	**Examinateur**
M. Hacène Fouchal	Professeur	Univ. Reims Champagne-Ardenne, France	**Examinateur**

Année universitaire : 2022-2023

Remerciements

En tout premier lieu, je remercie Dieu le Miséricordieux pour m'avoir donné la force et le courage de réaliser ce travail.

Mes reconnaissances s'adressent à Mr Chikouche Noureddine, professeur à l'université de M'sila, d'avoir accepté de m'encadrer pour un sujet d'actualité que j'ai trouvé très intéressant et pour tout l'intérêt et la disponibilité qu'il a montrés.

Je tiens à exprimer mes sincères remerciements aux membres du jury :

" M. Allaoua Hemmak, M. Salim Bitam, M. Lamri Sayad, M. Chaker Abdelaziz Kerrache, M. Hacène Fouchal " d'avoir accepté de juger ce travail.

Mes remerciements s'adressent particulièrement à Messieurs : Soufiene Djahel, Mohamed Smati, Wassim Benabbas, Salah Guesmia, Khaled Rouabeh, Farid Boutout et Salih Aidel.

Je remercie, enfin, toute personne ayant aidé de près ou de loin dans la réalisation de ce travail.

إهداء

اهدي ثمرة هذا المجهود الى الوالدين الكريمين، الى من قال الله تعالى فيهما : ﴿وَقَضَىٰ رَبُّكَ أَلَّا تَعْبُدُوٓاْ إِلَّآ إِيَّاهُ وَبِالْوَٰلِدَيْنِ إِحْسَٰنًا ۚ إِمَّا يَبْلُغَنَّ عِندَكَ ٱلْكِبَرَ أَحَدُهُمَآ أَوْ كِلَاهُمَا فَلَا تَقُل لَّهُمَآ أُفٍّ وَلَا تَنْهَرْهُمَا وَقُل لَّهُمَا قَوْلًا كَرِيمًا﴾

كما اهديها الى الزوجة الكريمة و ابنتاي هاجر و سارة

الى اخوتي و اخواتي وكل عائلة موساوي

الى كل الاصدقاء

الى كل الزملاء بجامعة برج بوعريريج وجامعة المسيلة

Résumé

Dans les systèmes de transport intelligents coopératifs (STI-C), les véhicules et les unités routières échangent divers messages sur la sécurité, le contrôle du trafic et les conditions météorologiques. Ces messages sont diffusés à tous les voisins. Chaque message doit être authentifié et doit protéger la vie privée des utilisateurs, principalement en masquant leur emplacement.

L'authentification est réalisée en signant des messages à l'aide d'une clé privée liée au certificat du pseudonyme (CP), fourni par une autorité de confiance. Le certificat est attaché aux messages envoyés afin que les récepteurs puissent les authentifier. La confidentialité est assurée en changeant plusieurs fois le pseudonyme au cours d'un trajet, de sorte que les suiveurs ne peuvent pas obtenir les traces des conducteurs. Ce travail propose une nouvelle approche pour gérer les périodes de commutation des CP par les véhicules. La méthode proposée repose sur l'utilisation d'un pseudonyme commun à tous les véhicules pendant une courte période avant de passer à un nouveau pseudonyme. Durant cette période, les véhicules signent leurs messages par le pseudonyme commun. Des expériences de simulations ont été menées dans un environnement OMNET++, montrant une amélioration significative de la protection de la vie privée par rapport aux schémas de confidentialité bien connus.

Mots Clés : STI-C, vie privée, authentification, anonymat, sécurité.

Abstract

In Cooperative Intelligent Transport Systems (C-ITS), vehicles and Road Side Units (RSU) exchange various messages about safety, traffic control, and weather conditions. These messages are broadcast to all neighbors. Each message should be authenticated and should protect users' privacy, mainly by hiding their locations. The authentication is achieved by signing messages using a private key related to the Pseudonym Certificate (PC), provided by a Trusted Authority (TA). The PC is delivered together with messages so that receivers can authenticate the messages. Privacy is ensured by changing PCs many times during a journey, so that trackers cannot get drivers' traces. This work proposes a novel approach to manage PC switching periods between vehicles. The proposed method uses a Common PC (CPC) during a short period before switching to a new PC. Vehicles use the same shared PC during this period to sign their messages. Simulations have been conducted in an OMNET++ environment, showing significant improvement in privacy protection compared to well-known privacy schemes.

Key Words : C-ITS, privacy, authentication, anonymity, security.

ملخص

في أنظمة النقل الذكية التعاونية ، تتبادل المركبات والوحدات المثبتة على حافة الطرقات رسائل مختلفة حول السلامة والتحكم في حركة المرور والظروف الجوية. يتم دوريا ارسال هذه الرسائل لجميع المركبات المجاورة. من الضروري مصادقة كل رسالة كما يجب حماية خصوصية المستخدمين ، عن طريق إخفاء مواقعهم بشكل أساسي. يتم تحقيق المصادقة من خلال توقيع الرسائل باستخدام مفتاح خاص مرتبط بشهادة الاسم المستعار، والتي يتم توفيرها من قِبل جهة موثوقة . يتم ارسال شهادة الاسم المستعار مع كل الرسائل حتى يتمكن المستلمون من مصادقة الرسائل. يتم ضمان الخصوصية من خلال تغييرالاسم المستعار عدة مرات أثناء الرحلة ، بحيث لا يتمكن المتتبعون من الحصول على آثار السائقين. يقترح هذا العمل نهجًا جديدًا لإدارة فترات تبديل الاسم المستعار بين المركبات. تستخدم الطريقة المقترحة إسما مستعارا مشتركا خلال فترة قصيرة قبل التبديل إلى اسم مستعار جديد. تستخدم المركبات نفس الاسم المستعار المشترك خلال هذه الفترة لتوقيع رسائلهم. بعد إجراء عدة عمليات للمحاكاة ، أظهرت النتائج الخاصة باستراتيجيتنا تحسنًا كبيرًا في حماية الخصوصية مقارنة بأنظمة الخصوصية المعروفة.

كلمات مفتاحية :
الخصوصية، المصادقة، إخفاء الهوية، الأمن، أنظمة النقل الذكية التعاونية.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AC	Autorité de Confiance
C-ITS	Cooperative Intelligent Transport Systems
CP	Certificat du Pseudonyme
CPC	CP commun
CR	Cloaking Region
DSRC	Dedicated Short Range Communication
ECC	Elliptic Curve Cryptography
EDR	Event Data Recorder
ETSI	European Telecommunications Standards Institute
GPS	Global Positioning System
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
IoV	Internet of Vehicles
IP	Internet Protocol
IVC	Inter-Vehicle communication
LBS	Location Based Services
LLC	logical link control
MAC	Medium Access Control
MANET	Mobile Ad-hoc Networks
MLME	MAC Layer Management Entity
NNPDA	Nearest-Neighbor Probabilistic Data Association
OBU	On-Board Units
OMNET++	Objective Modular Network Testbed in C++
PKI	Public Key Infrastructure
PLME	Physical Layer Management Entity
PREXT	Privacy Extension for Veins VANET
RGS	Route Guidance Systems
RSU	Road Side Units
STI-C	Systèmes de Transport Intelligents coopératifs
SPFX	Same Pseudonym beFore eXchange
SUMO	Simulation of Urban MObility

TA	Trusted Authority
TCP	Transmission Control Protocol
TPD	Tamper-Proof Device
UDP	User Datagram Protocol
VANET	Vehicular Ad-Hoc Network
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VEINS	VEhicles In Network Simulation
WAVE	Wireless Access in Vehicular Environments
WME	WAVE Management Entity
WSMP	WAVE Short-Message Protocol

Introduction générale

Les réseaux véhiculaires (VANETs) sont une solution prometteuse pour les Systèmes de Transport Intelligents Coopératifs (STI-C). Ils permettent de réduire les accidents de la route, d'optimiser la consommation de carburant et de réduire la durée des trajets. Les nœuds communicants sont soit des véhicules intelligents équipés d'unités embarquées appelées On Board Unit (OBU), soit des unités fixes situées le long des routes appelées Road Side Units (RSU). Un véhicule communique avec un autre véhicule ou l'RSU proche via la communication de véhicule à véhicule (V2V) et de véhicule à infrastructure (V2I), respectivement. L'évolution des solutions STI-C et de l'Internet des objets attire un grand nombre de chercheurs et d'industries à investir dans le domaine de l'Internet des véhicules (IoV). L'IoV consiste à connecter les véhicules à Internet pour couvrir les besoins des clients. Certains estiment que les expéditions de véhicules connectés pourraient atteindre 76 millions d'unités, ce qui rendrait le système de transport plus intelligent.

La protection de la vie privée du véhicule et du conducteur est cruciale et est considérée comme une exigence importante pour les STI-C, car les applications STI-C impliquent la transmission d'informations sensibles telles que l'emplacement, la vitesse, la direction et l'identité du véhicule. En effet, chaque véhicule diffuse périodiquement ses données dans un message de sécurité appelé "Beacon" à ses voisins. Comme les réseaux sans fil sont ouverts, les véhicules malveillants peuvent écouter les messages et les utiliser pour suivre et prédire la trajectoire d'un véhicule cible bien déterminé (comme on peut avoir plusieurs véhicules cibles). Étant donné que les conducteurs sont liés à leurs véhicules, leur vie privée est intrinsèquement affectée. On s'intéresse ici à la confidentialité d'emplacement, une fois l'emplacement ou le trajet du véhicule n'est pas parfaitement protégé, le conducteur est menacé à plusieurs types d'attaques (le chantage, l'atteinte de la vie privée sur l'endroit où il se rend, une menace politique ou des abus physiques et/ou moraux...).

L'architecture C-ITS utilise des communications authentifiées, en faisant intervenir un tiers de confiance, l'Autorité de Confiance (AC). L'AC enregistre les véhicules du STI-C et leur génère des certificats via des canaux sécurisés. Les certificats sont utilisés à la place de l'identité réelle du véhicule. Il est cependant possible de détecter une relation entre le certificat et l'identité du conducteur. Pour cette raison, chaque véhicule sera doté d'un ensemble de certificats des pseudonymes (CP),

chaque pseudonyme avec son certificat, afin qu'il puisse changer de pseudonyme tout en se déplaçant. Habituellement, une stratégie de changement de pseudonyme est proposée pour perturber les adversaires, les amenant dans une situation confuse entraînant des décisions fausses ou incertaines, même après avoir collecté une grande quantité de données[11, 19, 66, 67, 51].

La majorité des stratégies de changement des pseudonymes existantes s'appuient sur l'ajout d'une période de silence ou le changement des données d'emplacement ou de vitesse [19, 66, 56, 3]. La période de silence désigne que le véhicule éteint sa radio de transmission pendant une période, puis il change son pseudonyme et reprend la dissémination des messages. Le changement des données d'emplacement ou de la vitesse, désigne que le véhicule ne divulgue pas sa position ou sa vitesse exacte. Ces techniques donnent de bons résultats, mais elles ne conviennent pas aux systèmes de transport intelligents. Ces derniers exigent la transmission périodique des messages de sécurité, pour assurer la disponibilité de l'information exacte en temps réel, surtout lorsque cette information concerne une urgence ou une alerte d'accident.

Dans cette thèse, nous proposons un nouveau schéma de confidentialité d'emplacement pour les véhicules. Notre mécanisme se base sur un nouvel algorithme de changement de pseudonyme, et sur l'utilisation d'un pseudonyme commun entre tous les véhicules du réseau. Plus précisément, une fois qu'un véhicule est enregistré dans une AC, il reçoit un pool de CPs ainsi qu'un CP commun (CPC) utilisé par tous les véhicules. Au cours d'un trajet, un véhicule changera de CP lorsqu'il rencontre un ou plusieurs véhicules dans sa région. Tous les véhicules voisins utilisent le CPC pendant une courte période avant d'utiliser leurs nouveaux CPs. Nous supposons ici que tous les véhicules impliqués se comportent correctement (honnêtes). Notre approche a été mise en œuvre à l'aide du simulateur Privacy Extension for Veins VANET (PREXT). PREXT offre différents schémas de confidentialité. Une comparaison à été faite entre les résultats de simulation de notre mécanisme et ceux des autres schémas disponibles, la comparaison est basée sur des métriques spéciales pour mesurer la confidentialité de l'emplacement dans les VANETs [38].

Les principaux apports de cette étude sont décrits comme suit :

— Une nouvelle stratégie de changement de CP.

— Implémentation de la stratégie proposée dans l'environnement OMNET++.

— Comparaison de la proposition avec des schémas bien connus de la littérature.

— Analyse de la robustesse de l'algorithme face à un adversaire global sur le simulateur PREXT.

Cette thèse est structurée comme suit : Dans le premier chapitre, on présente le concept des réseaux véhiculaires, leurs exigences et les applications sur les STIC-Cs. La sécurité des réseaux véhiculaires et particulièrement la vie privée de l'emplacement ainsi que les techniques d'attaques et de protections existantes sont présentés dans le chapitre 2. Le troisième chapitre discute les stratégies de changements des pseudonymes comme une technique de protection de la vie privée dans les VANETs. Le quatrième et le cinquième chapitre sont dédiés à notre schéma de confidentialité. On commence par détailler le principe de base de notre mécanisme puis on présente la simulation et la discussion des résultats obtenus. On termine par une conclusion générale et quelques perspectives.

Chapitre 1

Les réseaux véhiculaires

1.1 Introduction

Les véhicules de nos jours sont devenus une arme à double tranchant, du fait qu'ils offrent des services de déplacement d'un côté et une cause de dégâts humains d'un autre côté. D'après des statistiques établies par les services de la protection civile en mois de Janvier 2022, en Algérie, le bilan était plus lourd que celui établi dans les années passées. Pas moins de 1683 personnes ont trouvé la mort dans 57982 accidents de la circulation et 71 744 autres ont été blessées. Le nombre d'accidents et de victimes des accidents de la route tire la sonnette d'alarme pour penser à rendre nos routes plus sécurisées. Les réseaux véhiculaires sont une solution prometteuse pour la sécurité routière et rendent les systèmes de transport plus fiables. De ce fait, la technologie VANET est devenue de plus en plus un sujet très attractif que ce soit pour les chercheurs ou les industriels.

1.2 Définition

Un réseau véhiculaire (VANET) est un réseau de communication adhoc sans fil, considéré comme une sous classe des réseaux mobiles adhoc (MANET). Les véhicules connectés et les éléments fixes de l'infrastructure, sont équipés de dispositifs et de technologies de communication avancés. L'idée de base consiste à interconnecter les véhicules intelligents entre eux ou avec les équipements fixes placés au bord de la route. Les véhicules du réseau peuvent échanger des informations sur leur position, leur vitesse, leur direction et d'autres informations utiles, ce qui permet de créer des réseaux de communication dynamiques en temps réel.

Un VANET promet, dans le cadre de la construction des systèmes de transport intelligents (STI), de fournir divers services aux conducteurs et aux passagers et d'aider les autorités de la circulation routière à mieux contrôler et atténuer les embouteillages, réduisant ainsi la pollution de l'air et le nombre d'accidents sur les routes. Les réseaux véhiculaires sont une composante clé de la technologie de conduite autonome, car ils permettent aux véhicules de communiquer entre eux

pour éviter les collisions et pour optimiser le flux de trafic.

1.3 Eléments de bases

Plusieurs éléments peuvent participer au déploiement d'un réseau de véhicules à savoir les OBU, les RSU, les piétons, les autorités de confiance...etc, on s'intéresse ici à deux éléments de base qui sont l'OBU et l'RSU.

1.3.1 On Board Unit

C'est l'élément essentiel installé sur les véhicules, ces véhicules sont dits intelligents. Les véhicules intelligents permettent d'améliorer la sécurité, la commodité et l'efficacité de la conduite. Les principales caractéristiques que l'on peut trouver dans un OBU sont :

1. Un émetteur-récepteur sans fil pour communiquer avec les autres OBUs et les RSUs. Les normes de communication utilisées sont généralement basées sur la technologie Wi-Fi ou DSRC (Dedicated Short Range Communication). Le véhicule peut aussi être connecté à Internet.
2. Un système de positionnement global (GPS) pour fournir la position actuelle du véhicule. Ce système de navigation avancé utilise des données en temps réel pour calculer les itinéraires optimaux, éviter les embouteillages et fournir des instructions de conduite précises.
3. Un système de stockage pour stocker les messages et les informations de sécurité échangées avec d'autres véhicules et les RSU.
4. Un processeur pour traiter les données, prendre des décisions et émettre des alertes.
5. Des capteurs tels que des caméras, des radars, des lidars et des capteurs ultrasoniques pour surveiller l'environnement autour du véhicule et collecter les données.
6. Des fonctionnalités d'assistance à la conduite telles que la détection de collision, le freinage d'urgence automatique, l'aide au stationnement et la surveillance de la fatigue du conducteur.
7. Une interface de communication Homme-Machine.

La Figure 1.1 illustre ces composants du véhicule intelligent.

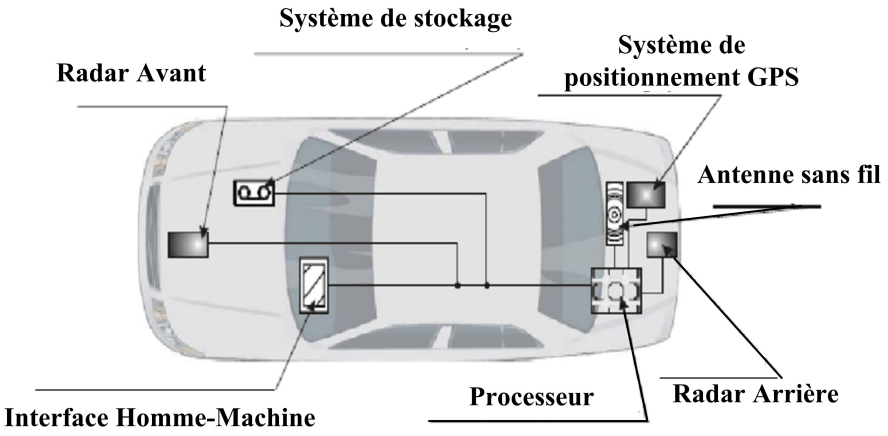

FIGURE 1.1 – Véhicule intelligent [29]

1.3.2 Road Side Unit

Un autre élément qui caractérise les VANETs sont les équipements installés aux bords des routes, sur des plaques de signalisation ou les feux de signalisation, afin de faciliter la communication au sein du réseau. Ces unités sont appelées RSU. Les RSUs rendent la communication plus performante, particulièrement dans les endroits moins denses. Les principales caractéristiques que l'on peut trouver dans l'RSU sont :

1. Un émetteur-récepteur sans fil pour communiquer avec les OBU des véhicules à proximité.
2. Une connexion guidée, filaire ou fibre optique, avec les autres RSUs.
3. Un système de stockage pour stocker les informations de sécurité et les données de trafic collectées auprès des OBU des véhicules à proximité.
4. Un processeur pour traiter les données, prendre des décisions et émettre des alertes.
5. Des capteurs tels que des caméras et des capteurs de mouvement pour surveiller l'environnement autour de l'RSU et collecter des données sur le trafic et les conditions de la route.
6. Une source d'alimentation, généralement un panneau solaire ou un réseau électrique, pour fournir de l'énergie à l'RSU.

1.4 Architecture WAVE

Dans cette section, on présente l'architecture WAVE (Wireless Access in Vehicular Environments), qui est adoptée spécialement pour les applications V2V et V2I des réseaux véhiculaires. Cette architecture est basée sur la technologie de communication sans fil appelée DSRC.

1.4.1 Normes et standards

L'évolution des VANETs est due grâce aux systèmes de communications et aux réseaux. L'IEEE (Institute of Electrical and Electronics Engineers) a développé une architecture de système connue sous le nom de WAVE pour fournir un accès sans fil dans des environnements véhiculaires. En Octobre 1999, la Commission Fédérale des Communications aux États-Unis a alloué 75 MHz (5.85 - 5.925 GHz) dans la bande 5,9 GHz en tant que nouveau spectre DSRC pour les communications véhiculaires. En Europe, l'Institut européen des normes de télécommunications (ETSI) a également attribué un spectre radioélectrique de 30 MHz (5,875 - 5,905 GHz) à 5,9 GHz. Des groupes similaires existent au Japon [34, 64]. En 2004, le groupe de travail TGP, de l'IEEE 802.11, a commencé à développer un amendement de la norme 802.11 pour inclure les environnements véhiculaires. Le document est connu sous le nom IEEE 802.11p [43]. Le groupe 802.11 de l'IEEE s'est concentré sur la norme de couche physique (DSRC PHY) et la sous-couche MAC (Medium Access Control) pour l'accès sans fil dans l'environnement véhiculaire. Une autre équipe IEEE (groupe de travail 1609) a entrepris la tâche de développer des spécifications pour couvrir des couches supplémentaires dans la suite de protocoles. L'ensemble de normes IEEE 1609 se composait de quatre documents : IEEE 1609.1 [16], IEEE 1609.2 [1], IEEE 1609.3 [17] et IEEE 1609.4 [18]. L'ensemble des normes IEEE 802.11p et IEEE 1609.x sont appelées WAVE. L'objectif principal de ces protocoles consiste à présenter l'architecture de communication, le partage de fréquences, la gestion des applications, les algorithmes de sécurité et la messagerie. La figure 1.2 présente la pile protocolaire de communication utilisant ces normes, par rapport aux sept couches du modèle OSI.

1.4.2 Protocoles de communication

La figure 1.2 illustre l'architecture WAVE. Cette architecture prend en charge deux piles de protocoles. Par rapport à la terminologie du modèle OSI, les éléments suivants sont présents dans le WAVE :

— **IEEE 802.11p** : L'architecture WAVE est basée sur la norme IEEE 802.11, qui spécifie la couche physique et une partie de la couche liaison de données de la pile de protocoles. Une modification de la norme 802.11 a était faite, connue sous le nom d'IEEE 802.11p. Cette nouvelle norme tient compte de l'environnement véhiculaire du fait qu'elle spécifie non seulement la partie transmission de données des protocoles mais également les fonctions de gestion associées à la couche correspondante. Une entité de gestion de la couche physique, PLME : Physical Layer Management Entity, et une entité de gestion de la couche MAC, MLME : MAC Layer Management Entity.

— **IEEE 1609.4** : Une nouvelle sous-couche est ajoutée au niveau de la couche deux. Elle sert au contrôle du fonctionnement multicanal. Les unités WAVE deviennent capables de partager leur temps entre le contrôle du canal et les services du canal.

— **IEEE 802.2** : Le contrôle de liaison logique (LLC) suit cette ancienne norme.

— **IEEE 1609.3** : Au niveau des couches transport et réseau, WAVE prend en charge la pile de la version 6 du protocole Internet traditionnel (IPv6) et une nouvelle pile spécifique au contexte véhiculaire. La nouvelle pile contient un protocole WAVE des messages courts, connu sous le nom de "WAVE Short-Message Protocol" (WSMP). TCP/UDP prend en charge les échanges traditionnels et moins exigeants, tandis que les communications prioritaires et sensibles au facteur temps sont prises en charge par le protocole WSMP. Un ensemble de fonctions de gestion, appelées WAVE Management Entity (WME), qui fournit des services de mise en réseau, fait aussi partie de cette norme IEEE 1609.3.

  Si on prend, par exemple, une application de diffusion des message d'alertes, c'est une application qui nécessite un temps réel pour son exécution et ses messages sont considérés urgents ; WSMP permet à cette application d'envoyer des messages courts et de contrôler directement certains paramètres de la ressource radio pour s'assurer que tous les destinataires reçoivent le message à temps. Cependant, les applications Internet typiques sont essentielles pour attirer les investisseurs dans une telle technologie ; WSMP n'est pas suffisant pour les applications Internet typiques, d'où l'inclusion d'IPv6.

— **IEEE 1609.1** : Ne s'intègre pas au modèle OSI, c'est le gestionnaire des ressources WAVE. Il décrit l'application qui permet l'interaction d'un véhicule avec des ressources informatiques limitées et des processus complexes s'exécutant à l'extérieur du véhicule.

— **IEEE 1609.2** : Ne s'intègre pas au modèle OSI, il fournit les services de

sécurité WAVE. Cette norme couvre le format des messages sécurisés et les traitements possibles comme les fonctions de chiffrement et d'authentification.

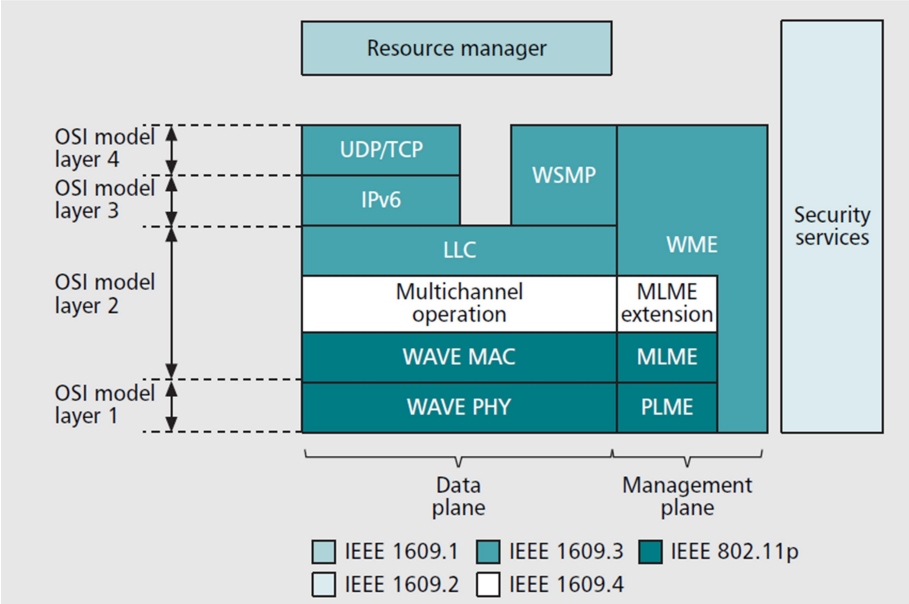

FIGURE 1.2 – Pile de protocoles WAVE [64]

1.5 Modes de communication

Un VANET comprend principalement des véhicules et des éléments fixes appelés RSUs, il peut également connecter des piétons avec leurs smartphones. Selon les entités communicantes, on distingue plusieurs modes de communications à savoir la communication inter-véhicules (V2V), la communication entre les véhicules et l'infrastructure V2I, la communication entre des éléments différents de l'infrastructure I2I.

1.5.1 Véhicule à véhicule

C'est le mode de communication principal des VANETs, appelé V2V (Vehicle to Vehicle) ou communication entre les véhicules. C'est une communication purement sans fil en utilisant des ondes radio, elle permet d'échanger des informations entre les véhicules, telles que la position, la vitesse, la direction. Toutes ces informations permettent la connaissance de la topologie du réseau et le voisinage d'un véhicule. Les véhicules peuvent ensuite échanger des messages utiles sur l'état de la route et les alertes de sécurité.

1.5.2 Véhicule à infrastructure

Appelé V2I (Vehicle to Infrastructure) ou communication entre les véhicules et l'infrastructure routière. C'est le mode qui permet la communication entre les véhicules et l'infrastructure (RSU). La communication est réalisée à travers des réseaux sans fil. Les messages échangés permettent aux véhicules de recevoir des informations sur les conditions de la route, les feux de signalisation, les panneaux de signalisation, les travaux routiers, etc.

1.5.3 Infrastructure à infrastructure

Ce mode est appelé I2I (Infrastructure to Infrastructure) ; comme son nom l'indique, il permet la communication entre les infrastructures routières (RSU). Une infrastructure peut être les feux de signalisation, les panneaux de signalisation, les caméras de surveillance, les stations de mesure, etc. La communication entre ces éléments fixes utilise une connexion filaire ou de la fibre optique, ce qui permet d'optimiser la circulation routière, prévenir les accidents, etc.

1.6 Architecture

Un réseau véhiculaire est un réseau ad-hoc sans fil qui s'organise de manière autonome et spontanée. La Figure 1.3 montre l'architecture d'un réseau véhiculaire. D'après cette architecture, les réseaux véhiculaires sont composés de deux types de dispositifs : les unités à bord (OBU) qui sont installées dans les véhicules et les unités de station de route (RSU) qui sont installées le long des routes. Les OBUs et les RSUs sont capables de communiquer à travers la communication véhicule à infrastructure ou infrastructure à véhicule (V2I). Une communication hybride est possible lors d'une transmission distante ou multi-sauts, à ce moment, différents nœuds (OBU ou RSU) peuvent participer au routage des messages.

1.7 Caractéristiques

Les réseaux véhiculaires se distinguent des autres réseaux et principalement des réseaux ad hoc mobile par :

— **Topologie hautement dynamique**

Les véhicules se déplacent à grandes vitesses en comparaison avec celles des piétons dans le cas des MANETs. Cette forte mobilité rend la topologie du

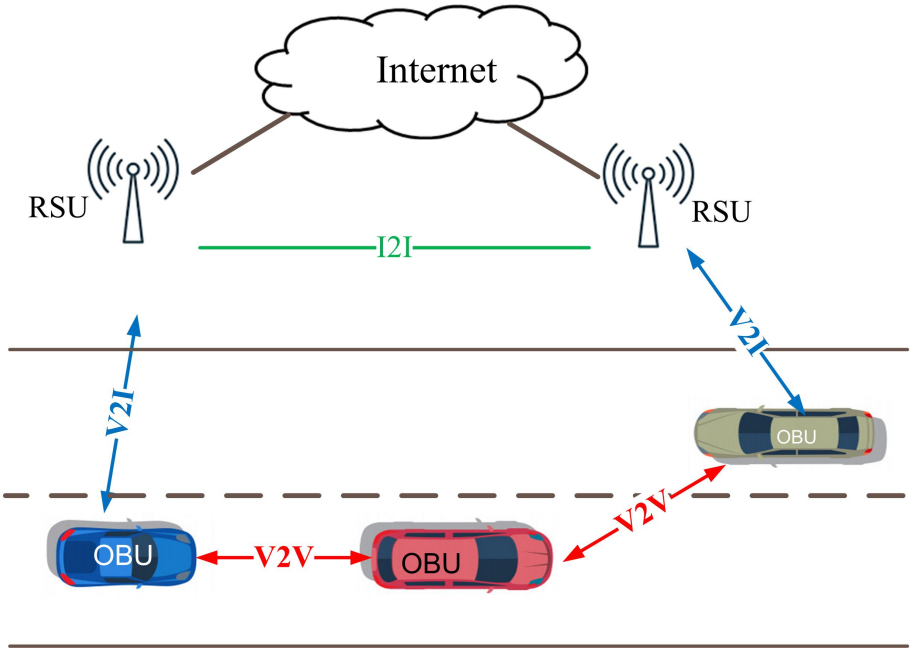

FIGURE 1.3 – Architecture de base d'un VANET

réseau très dynamique, ce qui provoque un sérieux problème lors du routage des paquets.

— **Modèle de mobilité**

Les réseaux MANETs utilisent un modèle de mobilité appelé point de cheminement aléatoire (connu sous le nom Random Waypoint RWP). Par contre, dans un réseau véhiculaire, les véhicules suivent un modèle de mobilité qui est fonction des routes concernées, des feux tricolores, de la vitesse limitée, des conditions du trafic et des comportements des conducteurs. L'évaluation des protocoles de routage n'a de sens que si elle est faite avec des traces de mouvement obtenues à partir du modèle réel.

— **Connectivité intermittente**

La forte mobilité des véhicules, et en particulier dans les autoroutes, rend la topologie du réseau très dynamique, de ce fait la connectivité devient intermittente. Cette caractéristique est très contraignante lors de la conception des applications qui exigent un délai d'attente très court comme c'est le cas des applications multimédia[39].

— **Capacité de traitement et énergie**

Contrairement aux réseaux MANET et aux réseaux de capteurs sans fils, la contrainte d'énergie et de capacité de stockage n'est pas posée dans les VANETs.

— **Service de localisation**

Les véhicules intelligents sont dotés d'équipements de positionnement GPS, ce qui facilite l'échange d'informations de localisation du véhicule à savoir sa position et sa vitesse. Cette caractéristique améliore les performances d'applications liées à la sécurité routière et de la gestion du trafic en prenant une bonne décision du routage. Comme il existe des applications qui nécessitent la dissémination du message dans une zone géographique particulière ou basées sur des critères de mouvement ou de direction du véhicule destinataire[40, 41, 42].

— **Scalabilité**

Le réseau peut s'étendre à une grande échelle, il peut couvrir toute une ville dans les applications urbaines. Les nœuds peuvent fréquemment se connecter ou se déconnecter du réseau.

1.8 Types de messages

Les véhicules du réseau peuvent envoyer ou recevoir trois types de messages ; les messages périodiques, les messages d'alertes ou les messages d'usage général.

1. **Les messages périodiques**

   Ces messages sont appelés Beacons ou messages de sécurité ; chaque véhicule envoie périodiquement à ses voisins ces messages qui contiennent des informations sur son état actuel telles que sa position, sa vitesse, sa direction et d'autres. Ces informations sont nécessaires au fonctionnement du réseau. L'échange de ces messages permet l'identification des nœuds, la découverte des voisins et le contrôle. Ce type de message rentre dans la plupart des protocoles de communications comme il peut être exploité négativement par des utilisateurs malveillants pour violer la sécurité du réseau et des véhicules.

2. **Les messages d'alertes**

   Les applications de sûreté génèrent ce type de messages. Lors d'un accident ou d'un embouteillage dans les routes, les nœuds diffusent ces messages d'une manière très rapide afin de minimiser les dégâts ou de gérer le flux du trafic.

3. **Les messages d'usage général**

   Les véhicules peuvent envoyer ou recevoir des messages de services ou d'usage général. Ces messages facilitent la communication entre les usagers du réseau.

1.9 Les systèmes de transport intelligents coopératifs

1.9.1 Définition

Les systèmes de transport intelligents coopératifs (STI-C) visent à appliquer les nouvelles technologies de l'information et de la communication, notamment des VANETs, aux systèmes de transport. Les véhicules intelligents, connectés et automatisés, rendent le système de transport dans nos routes plus sûr, plus efficace et plus durable. L'objectif principal de ces écosystèmes, STI-C, est de réduire les accidents de la route. Le système communique, à l'aide d'applications embarquées dans les OBU ou RSU, aux conducteurs des informations sur l'état de la route. Les notifications propagées peuvent être : une alerte d'un danger sur la route, une information pour dévier le flux routier d'une route barrée, ou d'un embouteillage. On peut même avoir des alertes envoyées aux autorités concernées, services d'urgence et de sécurité, en cas d'accident ou de danger sur la route. L'adoption généralisée des STI-C nécessite une coordination entre les gouvernements, les industriels et les utilisateurs finaux, ainsi que des investissements dans l'infrastructure des systèmes de transport.

1.9.2 Applications

Les systèmes de transport intelligents coopératifs offrent une gamme de fonctionnalités pour améliorer la sécurité, l'efficacité et la durabilité du transport. Les applications et les fonctionnalités offertes par la communication V2X (Vehicle-to-Everything) sont [9, 26] :

1.9.2.1 Sécurité routière

La sécurité routière est une préoccupation majeure dans les STI-Cs. Cette fonctionnalité vise à améliorer l'efficacité, la sécurité et la durabilité des système de transports.

1. **Contrôle des intersections**

   Le contrôle et la gestion des intersections et le respect des priorités est une nécessité majeure, du fait que la majorité des accidents urbains ont eu lieu aux intersections. Les communications entre les véhicules et l'infrastructure permettent d'informer le contrôleur d'intersection de l'emplacement et de la vitesse des véhicules connectés. La conception d'algorithmes de gestion adaptatif

des intersections a fait l'objet de plusieurs travaux de recherche [50, 10, 25]. Les techniques proposées supposent généralement des communications parfaites.

2. **Évitement d'accidents**

   Le besoin en sécurité routière et d'évitement d'accident est l'un des objectifs principaux des STI-Cs. Des méthodes ont été proposées pour assurer le contrôle automatique des véhicules, ce contrôle permet d'éviter les accidents avant qu'ils ne surviennent. Des messages d'alertes vont être envoyés aux conducteurs en cas de situations anormales ou dangereuses. Plusieurs systèmes ont été proposés pour l'évitement des accidents dans nos routes [7, 46, 33].

3. **Gestion des incidents**

   Une fois qu'un accident se produit, on a besoin de systèmes capables de gérer la situation et de diminuer les dégâts autant que possible. Ces applications offrent des services en relation avec la sûreté, comme : l'avertissement d'accident, l'avertissement de véhicule d'urgence, les services SOS, l'avertissement de conditions dangereuses de la route et les préventions d'obstacles.

   Le principe de fonctionnement de ces systèmes est basé sur l'envoie des messages d'avertissement par les véhicules impliqués. Les messages d'alertes seront diffusés d'une manière urgente aux autres véhicules ou RSU du réseau. Plusieurs applications ont été proposées [8, 27, 62, 60]. Le défi majeur de ces applications est de ne pas submerger le réseau par des messages inutiles, pour ne pas rendre ce service comme une attaque de dénie de service (ou replay) dans le réseau, il faut aussi arrêter la diffusion hors la zone d'intérêt.

1.9.2.2 Gestion du trafic

La gestion du trafic permettra aux véhicules connectés d'éviter les embouteillages dans les routes encombrées. Cette fonctionnalité est assurée par le contrôle intelligent du flux de trafic et la surveillance des routes par le suivi des véhicules. On distingue trois familles [9] :

1. **Systèmes de guidage d'itinéraire**

   ce sont des systèmes proposés pour guider les conducteurs vers leurs destinations en évitant les congestions. TravTek est un système embarqué de guidage routier (RGS), il est conçu pour déterminer les meilleurs itinéraires à travers la région du Grand Orlando [48]. En 2014, un autre système de transport intelligent a été proposé pour le guidage d'itinéraires, ce système aide à capturer les positions futures des véhicules et détermine les itinéraires fiables de manière préventive [61].

2. **Systèmes de stationnement**

   Ces systèmes aident les conducteurs pour trouver un emplacement de stationnement, IPARK est un système proposé dans [70], les auteurs ont affirmé qu'environ 30% de la congestion du trafic est causée par des véhicules circulant autour de leur destination et cherchant une place pour se garer.

3. **Systèmes pour les villes intelligentes**

   Les STI-Cs sont considérés comme l'objectif principal des villes intelligentes. Plusieurs travaux ont été proposés pour construire des systèmes, basés sur les STI-Cs, dédiés aux villes intelligentes comme [31, 59, 2, 49].

1.9.2.3 Applications de confort

Ces applications sont définies comme étant des services n'ayant pas de lien avec la sécurité des véhicules, elles visent à offrir plus de confort aux conducteurs et aux passagers comme entre autres : l'Internet mobile, mettre à jour les prévisions météorologiques et la connaissance des prestations de services autour de sa région.

1.10 Conclusion

Tout au long de ce chapitre, on a donné un aperçu général sur les réseaux véhiculaires. Puis, on est passé à la présentation de l'architecture et les éléments essentiels qui les composent. Ensuite, on a discuté sur les applications, qui rendent cette technologie très intéressante, et terminé par la définition des caractéristiques de ces réseaux. Tous ces points sont abordés dans le but de donner une vision plus claire sur notre travail dans cette thèse, qui consiste à concevoir un mécanisme de sécurité d'emplacement des véhicules.

Chapitre 2

Sécurité et vie privée

2.1 Introduction

La sécurité est une exigence dans la spécification, la conception et la réalisation de tous les systèmes informatiques. Une exigence majeure doit être portée à la sécurité de ces systèmes quand le danger concerne les personnes et non seulement les données. Dans la base, les VANETs connectent des véhicules ; le conducteur ou le propriétaire est lié à son véhicule. De ce fait, le suivi du véhicule désigne le suivi de la personne qui le conduit ou qui le possède. On examine dans ce chapitre la sécurité et la vie privée des véhicules dans les VANETs.

2.2 La sécurité dans les réseaux véhiculaires

La nature et les caractéristiques des VANETs exigent la mise en place des mécanismes de sécurité appropriés pour la construction de ces réseaux. Ces mécanismes doivent assurer que seuls les utilisateurs autorisés ont accès aux informations et que les services sont fiables [12, 34].

2.2.1 Besoin de sécurité

Le grand défi est d'assurer une qualité de service dans un réseau dont la topologie change rapidement, la connectivité est intermittente et ses nœuds échangent des informations sensibles. La sécurité dans ces réseaux ne se limite pas seulement à la protection des informations qui circulent et les services assurés mais elle peut s'étendre à la sécurité des êtres humains. Un message d'alerte falsifié ou éliminé par un utilisateur malveillant peut causer des dégâts de route, l'exploitation des informations de localisation des véhicules par des suiveurs peut toucher aussi à la vie privée des conducteurs et peut les mettre en danger.

2.2.2 Exigences de sécurité

Les exigences de sécurité sont extraites à partir des principaux objectifs de la sécurité telles que la confidentialité, l'intégrité et la disponibilité. Les exigences générales de la sécurité d'un réseau VANET sont : l'authentification, l'intégrité et la cohérence, la confidentialité, la disponibilité et le contrôle d'accès[34, 55, 26].

1. **Authentification**

   L'authentification est une exigence majeure dans les VANETs pour se protéger contre les adversaires potentiels, elle désigne que le récepteur doit être capable d'identifier correctement la source du message. Dans le cas des VANETs, l'authentification concerne l'identificateur (ID) du véhicule et exige que l'entité elle-même soit légitime. L'authentification du ID assure que le message est envoyé par une source de confiance en identifiant correctement son identité. L'ID doit être unique, il peut être par exemple la plaque d'immatriculation ou le numéro de châssis du véhicule. L'authentification de l'entité garantit quant à elle que le message est légitime et envoyé par une entité légitime. Cette authentification d'entité garantit la fraîcheur des messages qui circulent au sein du réseau.

2. **Intégrité et Cohérence**

   L'intégrité désigne qu'on doit protéger l'information durant sa transmission, cette protection concerne toute modification ou suppression du message par une entité non autorisée avant qu'il atteigne correctement sa destination. Une entité honnête et légitime peut émettre des données erronées à cause d'une défaillance possible au niveau de son capteur ou de son émetteur, le même comportement peut être fait par une entité légitime mais malveillante. Cependant, une comparaison avec des messages similaires générés dans des moments ou des espaces proches est obligatoire pour s'assurer que le message est cohérent.

3. **Confidentialité**

   La confidentialité exige que les messages soient protégés contre l'écoute ou l'accès non autorisé à leurs contenus. Seuls l'émetteur et le récepteur doivent avoir l'autorisation d'accès au contenu du message. Cette exigence concerne les messages instantanés entre les véhicules et non les messages d'alerte ou de sécurité.

4. **Disponibilité**

   Cette exigence se réfère à la fiabilité du système et la disponibilité du réseau. Dans les applications de sûreté, les messages d'alertes et d'avertissements né-

cessitent de se propager rapidement dans une région particulière, si le canal n'est pas disponible ou qu'il y a une attaque sur le déni de service, l'alerte n'atteint pas les véhicules à temps et l'application devient inutile.

5. **Contrôle d'accès**

   Les nœuds du réseau doivent être légitimes et honnêtes pour avoir l'accès aux services du réseau, un véhicule qui se comporte mal peut être révoqué du réseau et perd sa légitimité. Cependant son certificat sera ajouté à la liste des certificats rejetés. Une autre forme de l'exigence du contrôle d'accès concerne les applications qui fournissent différents niveaux d'accès, à ce moment là un nœud ne peut pas accéder à un service malgré qu'il soit légitime et honnête s'il n'a pas le privilège d'accès.

6. **Non répudiation**

   La non répudiation est une exigence cruciale du fait qu'un véhicule ne doit pas être capable de nier la transmission d'un message, surtout lorsque ce message conduit à un dégât d'accident ou une fausse alerte dans le réseau. Pour cela, les nœuds doivent être identifiés d'une manière fiable et la traçabilité des messages doit être disponible pour aider à l'enquête.

7. **la vie privé ou l'intimité**

   La vie privée des usagers est une exigence précieuse pour réussir le déploiement du VANET et pour convaincre les gens de s'investir dans une telle technologie. Dans un réseau ouvert comme les VANETs, les véhicules propagent des messages périodiques incluant des informations sensibles (position, vitesse, l'identifiant, etc.). La collecte des informations spécifiques aux véhicules (automatiquement aux conducteurs) est facile. Un attaquant suiveur ne doit pas être capable de connaître (ou déduire) la traçabilité du véhicule ni l'identité réelle du conducteur. C'est la garantie d'anonymat des véhicules et des conducteurs.

2.2.3 Nature d'attaquant

Les VANET sont plus vulnérables aux attaques et c'est difficile de reconnaître les véhicules suspects. Un réseau VANET peut être compromis par un attaquant en manipulant le système du véhicule ou les protocoles de sécurité. Généralement l'attaquant a l'intention de perturber l'ensemble du réseau pour son propre intérêt ou casser la vie privée d'un véhicule cible. Les attaquants sont classés en quatre catégories [55].

1. **Internes ou Externes**

les attaquants internes sont des utilisateurs légitimes authentifiés, tandis que les attaquants externes ne sont pas des utilisateurs authentifiés. les attaquants externes ont une capacité limitée à attaquer le réseau par rapport aux attaquants internes.

2. **Actifs ou Passifs**

   Les attaquants actifs génèrent de faux messages ou ne retransmettent pas les messages reçus, alors que les attaquants passifs ne font que l'écoute ou la collecte des informations lors de la communication.

3. **Malveillants ou Rationnels**

   L'objectif principal des attaquants malveillants ou malicieux est de détruire le système ou d'attaquer d'autres nœuds sur le réseau sans attendre un gain personnel, tandis que les attaquants rationnels sont plus professionnels, ils attaquent le réseau pour obtenir des avantages personnels.

4. **Locaux ou globaux**

   Les attaquants locaux utilisent des ressources limitées sur des véhicules spécifiques et couvrent une zone géographique restreinte, tandis que les attaquants globaux ou étendus couvrent plusieurs réseaux en exploitant plusieurs ressources, une unité centrale analyse les données collectées du réseau pour atteindre l'objectif de l'attaque.

2.2.4 Types d'attaques

Comme les messages périodiques sont diffusés dans un environnement à accès ouvert, tout le système de la communication sera perturbé lorsqu'un attaquant intercepte, modifie ou génère des messages dans le réseau. Ces défis exposent les VANETs à divers types d'attaques non souhaitées. Les menaces de sécurité les plus significatives sont :

— **Attaque sur la vie privée**

  La collecte des données par un attaquant peut engendrer un risque majeur sur la vie privée des conducteurs, il peut identifier avec précision le nœud d'origine ainsi que les actions et les endroits du conducteur. La vulnérabilité réside dans l'échange des informations sensibles lors de la communication, notamment dans les messages de sécurité et de contrôle où le véhicule est censé envoyer des messages identifiés et contenant des informations sur sa localisation, sa vitesse et même des fois des détails de voyage.

— **Attaque sur la cohérence**

L'attaquant peut violer la cohérence des messages en les modifiant ou par l'injection de fausses informations. Il peut ainsi altérer les connaissances de sa victime pour la rediriger, ou même générer des problèmes dans le trafic en déviant tous les véhicules vers une route déjà encombrée.

— **Usurpation d'identité**

Cette attaque est très dangereuse, l'adversaire utilise un faux identifiant pour se faire passer pour une entité légitime, il peut donc profiter de tous les privilèges. Si l'attaquant envoie des faux messages ou perturbe le système, il sera très difficile de le détecter.

— **Déni de service (Dos)**

C'est l'attaque la plus connue même dans les réseaux traditionnels, l'attaquant vise à submerger le réseau par l'inondation du canal par des messages inutiles pour alourdir ou même empêcher la diffusion des messages d'alertes ou de contrôle.

— **L'Écoute**

Dans ce type d'attaque, l'adversaire possède des capacités d'écoute au canal et d'extraire des informations pertinentes pour son profit. Le grand défi de cette attaque est que l'attaquant peut être passif et donc difficile à détecter. Ce type d'attaque peut aussi initier une attaque sur la vie privée des conducteurs.

— **Noeud caché**

Cette attaque concerne les applications de diffusions des messages d'alertes, où les protocoles de communication sont basés sur la position du nœud. Si un nœud détecte un voisin mieux positionné par rapport à lui pour effectuer la diffusion, il arrête de diffuser pour ne pas submerger le canal par des messages dupliqués. L'attaquant profite de cette stratégie pour convaincre un nœud prêt à diffuser qu'il est mieux positionné pour la diffusion par rapport à lui, à ce moment ni le nœud honnête diffuse, ni l'attaquant. On dit que le nœud honnête est devenu un noeud caché.

2.2.5 Architecture de sécurité pour les VANETs

En plus des recherches qui s'interessent au développement de la couche MAC appropriée aux VANETs (par exemple IEEE 802.11p), d'autres projets de recherches accordent plus d'attention à l'architecture et aux protocoles de sécurité de ces réseaux (Car 2 Car Communication Consortium, le groupe de travail IEEE 1609.2, le projet NoW et le projet SeVeCom). Tous ces industriels utilisent une Autorité

de Certification (AC) et la cryptographie à clé publique pour protéger les messages Véhicule-à-Véhicule (V2V) ou Véhicule-à-Infrastructure (V2I). Il est devenu un consensus d'utiliser la cryptographie à clé publique dans les VANETs. La cryptographie symétrique est loin d'être utilisée dans les VANETs, du fait que les messages sont diffusés et que la communication en point-à-point n'est pas la norme. Les noeuds du réseau sont toujours en mouvement, ce qui rend difficile la mise en oeuvre des procédures d'établissement des clés secrètes. L'authentification, l'intégrité et la non-répudiation des messages, ainsi que la protection de la vie privées des utilisateurs sont identifiées comme des exigences primaires dans tous les protocoles de sécurité [34].

2.2.5.1 L'infrastructure à clé publique PKI

Un véhicule doit être d'abord enregistré pour qu'il soit capable de se connecter au réseau. La principale caractéristique, des véhicules, est le changement de régions lors de déplacement, par conséquent ils peuvent être au-delà de leurs zones d'enregistrement. Un schéma de gestion des clés robuste et flexible est devenu donc une nécessité. L'implication des autorités dans l'enregistrement des véhicules nécessite un certain niveau de centralisation. Dans un VANET, un véhicule doit être identifié d'une manière unique par tous les autres véhicules connectés sans aucun appel à un serveur, comme il doit être également identifié par les stations de bases. L'utilisation de la cryptographie à clé publique, pour la protection des messages, est plus appropriée pour déployer la sécurité des communications véhiculaires.

Il est donc nécessaire d'impliquer une infrastructure à clé publique (PKI). Une autorité de confiance (AC), ou de certification, est chargée d'établir et de révoquer des certificats, les véhicules peuvent établir une connexion sécurisée et peuvent se faire confiance entre eux lorsque les certificats sont valides (voir Figure 2.1). Un véhicule envoi une requête d'enregistrement auprès du cette autorité de confiance. Une fois enregistré, le véhicule obtient un certificat signé avec la clé privée de l'AC. Avant de délivrer le certificat signé, l'AC vérifie si le bon véhicule reçoit la bonne clé et si le véhicule est digne de confiance. Pour que les véhicules puissent vérifier la validité de tout certificat de clé publique émis par l'autorité, la clé publique de l'AC doit être connue par tous les véhicules du réseau.

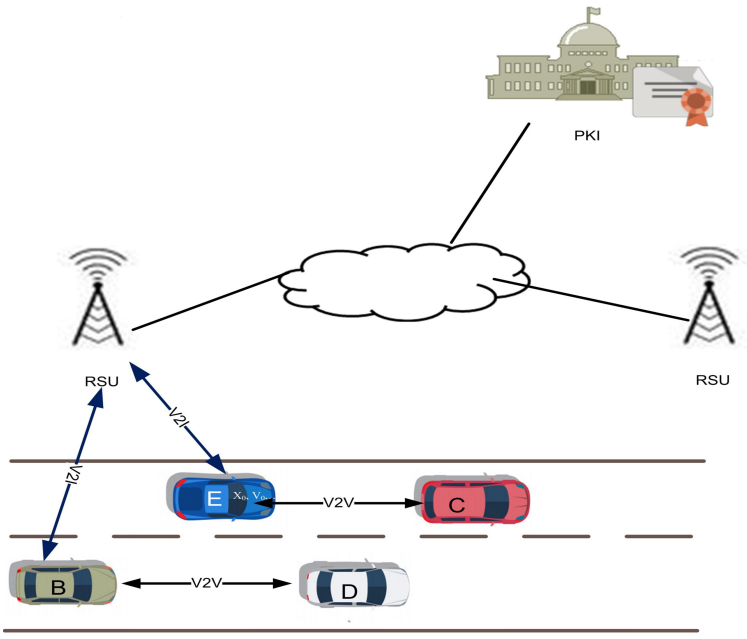

FIGURE 2.1 – Architecture de la sécurité VANET

2.2.5.2 Le standard de sécurité IEEE 1609.2

Comme on a montré dans la section 1.4.2, le standard 1609 est une amélioration du 802.11 pour qu'il soit compatible aux réseaux véhiculaires. On s'intéresse ici plus particulièrement à la norme IEEE 1609.2 qui répond aux problématiques de sécurisation des messages WAVE. La sécurité des messages permet de lutter contre les écoutes non autorisées, le spoofing et toutes autres attaques de sécurité vues dans la section 2.2.4. Les services de sécurité offerts par cette infrastructure, basée sur les normes et standards de l'industrie pour la cryptographie à clé publique, sont possibles grâce à ses composants qui incluent : (a)La prise en charge de la cryptographie à courbe elliptique (ECC), (b)des formats de certificat WAVE, et (c)des méthodes de chiffrement hybrides. Cette norme, IEEE 1609.2, a laissé de nombreux problèmes liés à la sécurité non résolus, à savoir la révocation des certificats, l'identification du véhicule et la protection de la vie privée des conducteurs (propriétaire) du véhicule. Cette thèse propose une solution pour la préservation de la vie privée.

2.2.5.3 Materiel de sécurité

L'architecture de sécurité des VANETs, comprend aussi des éléments matériels de sécurité. Deux modules différents peuvent êtres intégrés ou connectés aux OBUs :

1. **L'enregistreur de données d'événements (EDR : Event Data Recorder)**

   Est un équipement de sécurité qui enregistre les données relatives à un évènnement (tel que accident) de véhicule. L'EDR est parfois appelé "boîte noire" car il fonctionne de manière similaire à la boîte noire des avions, en enregistrant des informations importantes en cas d'incident. Ce dispositif enregistre généralement des données critiques du véhicule telles que la vitesse, la position , et d'autres informations pertinentes. La plupart des véhicules modernes sont équipés d'un EDR, bien que les exigences en matière de fonctionnalités et de capacités varient selon les pays et les réglementations locales. Les données stockées dans l'EDR peuvent être récupérées à l'aide d'un outil de diagnostic spécialisé après un accident, et ces données peuvent être utilisées dans le cadre d'une enquête sur un accident ou pour aider à améliorer la sécurité des véhicules.

2. **Le dispositif HSM (Hardwere Security Module)**

   Un Hardware Security Module, ou Tamper-Proof Device (TPD), est un dispositif de sécurité matériel qui est utilisé pour protéger les données et les clés cryptographiques. Les HSMs sont conçus pour être résistants aux tentatives de fraude ou de piratage en utilisant des techniques de sécurité physiques et logiques. Ces équipements peuvent être utilisés pour une variété de tâches de sécurité, telles que la gestion de clés de chiffrement, la génération des nombres aléatoires sécurisés, la vérification de l'intégrité des données, l'authentification de l'utilisateur et la signature numérique de documents. Ils sont couramment utilisés dans les systèmes de paiement, les réseaux de télécommunications, les systèmes de gestion des identités et des accès, ainsi que dans d'autres applications de sécurité critiques. Ces dispositifs sont construits à l'aide des matériaux et des techniques de fabrication qui les rendent extrêmement difficiles à compromettre. Ils sont conçus pour détecter toute tentative de manipulation ou d'altération, et pour effacer automatiquement les données sensibles en cas de violation de la sécurité. Les HSM sont généralement utilisés en conjonction avec des logiciels de sécurité pour fournir une sécurité totale. Les clés et les données cryptographiques sensibles sont stockées dans l'HSM, tandis que les opérations cryptographiques sont exécutées par le logiciel de sécurité. Cette

combinaison de matériel et de logiciel offre une sécurité supérieure à celle qui serait obtenue avec l'un ou l'autre des deux seul. Notre contribution dans cette thèse rentre dans la partie logicielle, tandis que on fait appel aux HSMs pour le stockage des clés privés et des certificats (voire section 4.2).

2.3 Protection de la vie privée dans les VANETs

2.3.1 Motivation

La nécessité de la protection de la confidentialité de l'emplacement désigne la protection du véhicule contre les tentatives d'attaques de suivi de sa localisation. La vulnérabilité réside dans la corrélation entre l'identité du véhicule et son emplacement. On rappelle que dans les VANETs, chaque véhicule transmet en permanence un message de sécurité contenant des informations vitales, notamment sa vitesse, sa position et son identité qui sont étroitement liées au conducteur (propriétaire). D'autre part, les informations transmises sont nécessaires pour le fonctionnement des applications véhiculaires telles que l'évitement des collisions, l'avertissement d'accidents, les services d'urgence, les systèmes de navigation, etc. Le défi est donc de protéger le véhicule contre toute corrélation entre son identificateur et son comportement, son emplacement et ses caractéristiques spéciales. En quelque sorte, l'identité du véhicule doit être masquée ou dissociée de sa localisation.

2.3.2 La vie privée au sein de la sécurité

Pour qu'un écosystème VANET soit efficace, un grand défi est d'assurer un compromis entre une sécurité renforcée et une protection de la confidentialité (la vie privée des conducteurs). Une fois qu'on échoue d'assurer ce compromis, notre système subit des problèmes de vulnérabilité ou d'inefficacité et sera par conséquent inutilisable.

Une présentation non exhaustive des sujets de recherches a été proposée par [20]. Les quatre principaux domaines de la sécurité dans la communication inter-véhicules sont : la gestion des identifiants et authentification des messages, protection de la vie privée, cohérence des données et sécurité embarquée. La figure 2.2 montre la relation de ces quatre domaines et l'impact de la préservation de la vie privée au sein du projet VANET. Cette thèse propose une stratégie de changement des pseudonymes. La figure 2.2 montre que le changement des pseudonymes est une solution prometteuse pour la préservation de la vie privée, on discute ces stratégies plus tard dans la section 2.3.5.

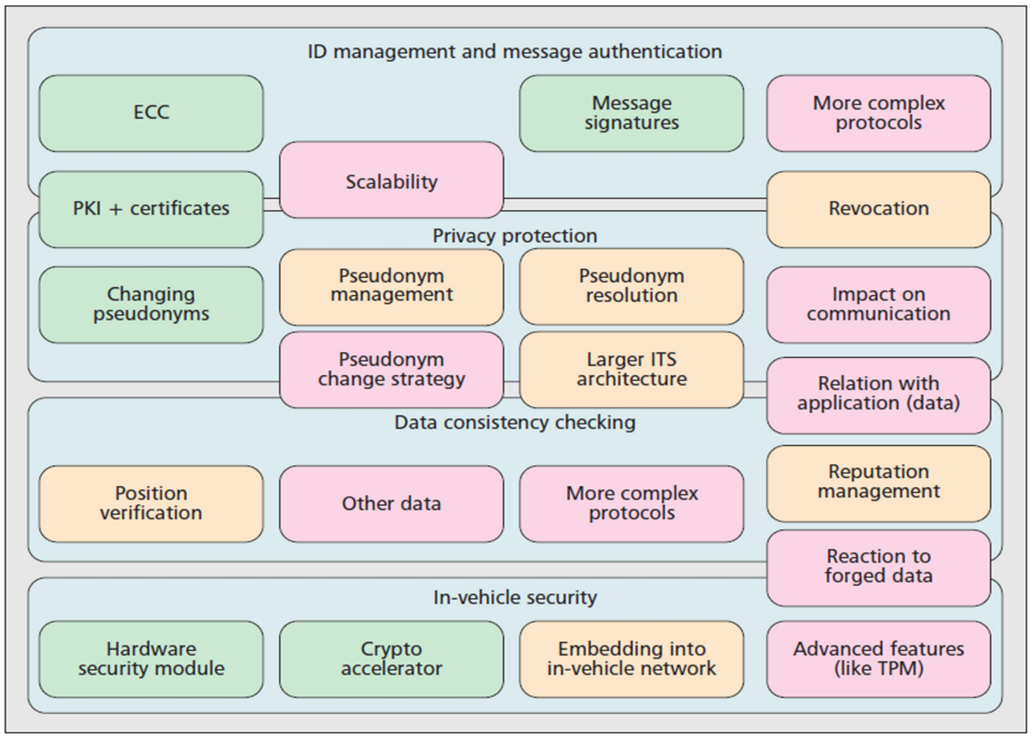

FIGURE 2.2 – Sujets de recherche [20]

2.3.3 Exigences de la vie privée

1. **Divulgation minimale**

   Lors de la construction d'un schéma de confidentialité ou de protection de la vie, on ne divulgue que l'information pertinente et nécessaire au fonctionnement du système. La divulgation minimale des informations dans le système protège l'utilisateur contre toute attaque sur sa vie privée. L'information moins détaillée met le suiveur en conflit.

2. **Anonymat**

   L'anonymat est une exigence très importante pour protéger la vie privée des conducteurs ou propriétaires des véhicules ; elle désigne que l'identité de l'émetteur est cachée ou non compréhensible. Il faut que la distinction de son identité soit impossible par un attaquant. Cette exigence se contredit avec la responsabilité des utilisateurs vis à vis de leurs comportements. Lorsqu'un véhicule se comporte mal, l'autorité doit être capable de le distinguer. La manipulation de l'anonymat doit être soigneusement traitée pour assurer un compromis entre le droit d'un véhicule de cacher son identité au sein du système et celle de sa responsabilité.

3. **Non traçabilité**

On doit interdire toute liaison possible entre deux messages envoyés par un même véhicule. la majorité des attaques s'appuient sur cette vulnérabilité.

4. **Confidentialité persistante**

   La confidentialité persiste ou reste valable même si l'identité du véhicule est résolue. Cependant, il doit être impossible à un adversaire de relier les futurs messages à un utilisateur, même après la résolution de son identité ou la résolution d'une information qui le distingue des autres utilisateurs.

2.3.4 Menaces

Deux catégories principales d'attaques qui violent la vie privée des conducteurs de véhicules et des utilisateurs des réseaux véhiculaires sont : (i) l'attaque de révélation d'identité et (ii) l'attaque de localisation [26].

2.3.4.1 Révélation d'identité

Dans cette attaque, l'identité du propriétaire d'un véhicule est en danger. Les informations personnelles du propriétaire sont compromises, ce qui peut entraîner de graves conséquences à l'avenir.

L'attaque révélatrice d'identité est empêchée grâce à l'utilisation d'un cadre d'authentification avec des mécanismes de préservation de la confidentialité.

2.3.4.2 Suivi de localisation

L'adversaire suit l'emplacement d'un véhicule ainsi que le chemin suivi par ce dernier pendant une certaine période de temps. Dans les approches existantes, l'identité du véhicule est cachée des accès non autorisés grâce à des clés anonymes et temporaires. Par conséquent, la confidentialité de l'emplacement du véhicule est maintenue et la trajectoire du nœud ne peut pas être suivie par des suiveurs malveillants.

2.3.5 Stratégies

Vu l'importance de la protection de la vie privée dans les réseaux et notamment dans les VANETs, plusieurs stratégies ont été proposées dans la littérature : des stratégies basées sur la cryptographie, d'autres sur l'utilisation des pseudo-identités à la place de l'identité réelle, ... La majorité des stratégies renforcent la confidentialité de la vie privée des conducteurs ou passagers au détriment de la qualité de service du réseau. Les approches sont présentées dans cette section selon [35].

2.3.5.1 Cryptographie

Plusieurs approches sont proposées en se basant sur la cryptographie, elles font appel aux techniques de chiffrement. Lorsqu'un véhicule envoie une requête à un fournisseur de service, l'emplacement de sa requête sera chiffré pour qu'il devient non compréhensible, le fournisseur de service obéit à la requête sans pouvoir comprendre l'emplacement de la requête. Cette technique garantit aux véhicules la confidentialité de leurs emplacements et de leurs identités, mais ne convient pas aux applications ou services de sécurité qui nécessitent que l'emplacement de la requête doit être non seulement clair mais précis.

2.3.5.2 La perturbation

Contrairement aux techniques cryptographiques, la requête est envoyée en clair (sans chiffrement), mais les informations subissent des perturbations avant d'être envoyées. La perturbation des informations est réalisée soit par l'ajout d'un bruit contrôlé, soit par l'envoi d'une information plus générale ou en les combinant avec des informations fausses. En raison des caractéristiques intrinsèques des schémas de perturbation, ils sont principalement utilisés pour préserver la confidentialité de la localisation dans quelques services basés sur la localisation mais pas dans les systèmes coopératifs de sécurité. On présente ici trois types de schémas basés sur cette stratégie.

1. **L'anonymisation**

   Cette stratégie repose sur l'hypothèse d'existence d'un tiers appelé l'Anonymiseur (Anonymizer), ce dernier est un serveur de confiance qui offre des services basés sur la localisation (LBS). L'anonymiseur connaît bien la localisation des utilisateurs. Lorsqu'un utilisateur veut accéder à un service, il doit d'abord passer par l'anonymiseur, qui lui créera une région de camouflage (Cloaking Region (CR)) relativement à son emplacement. L'utilisateur utilise cette nouvelle localisation dans ses messages pour circuler d'une manière cachée parmi un groupe d'utilisateurs où il est difficile de le distinguer. Des travaux plus récents dans cette stratégie comme [24] ont été publiés.

2. **Obscurcissement**

   Contrairement aux schémas d'anonymisation, ces schémas assurent la confidentialité de l'emplacement sans l'aide de l'anonymiseur, c.à.d qu'on ne cherche pas à cacher un utilisateur parmi d'autres utilisateurs. Cependant, l'idée de base est de réduire l'exactitude des informations de localisation envoyées aux fournisseurs des services et, par conséquent, aux clients. L'emplacement réel

est soit remplacé par un emplacement plus général, comme une zone circulaire ou une région, soit par l'ajout d'un bruit contrôlé.

3. **Régions factices**

   Ces schémas ne déforment pas l'emplacement réel de l'utilisateur, ils protègent la confidentialité de l'emplacement d'un utilisateur indépendamment des autres utilisateurs, mais au détriment de frais généraux de traitement et de communication élevés. L'idée de base est de combiner les emplacements réels avec d'autres faux emplacements générés et les envoyer à un fournisseur de services. L'approche basée sur les régions factices (Dummy-Based) a été introduite par [32], les chercheurs se sont ensuite concentrés principalement sur la génération d'emplacements factices plausibles pour empêcher l'adversaire d'identifier ces emplacements factices.

2.3.5.3 La mise en cache

Pour protéger l'emplacement du véhicule, cette stratégie sert à minimiser l'envoi des demandes aux fournisseurs de services. Le contenu cherché doit être donc mis en cache local du véhicule, de l'RSU ou des voisins. Une demande ne sera envoyée au fournisseur que si elle n'est pas disponible dans le cache. Les schémas basés sur la mise en cache sont adaptés uniquement aux applications non liées à la sécurité, en particulier les applications de confort basées sur la localisation telles que la recherche d'un point d'intérêt (Université, Restaurant, Hypermarché....) . Ces applications n'exigent pas un temps réel de réponse (non critiques en matière de retard) comme c'est le cas des applications de sûreté.

2.3.5.4 Changement des pseudonymes

Le pseudonyme désigne que le véhicule n'envoie pas son identité réelle dans ses messages, il utilise un pseudonyme à sa place. Le pseudonyme perd sa raison d'existence s'il ne sera pas changé. Chaque véhicule possède un pool de pseudonymes pour les utiliser dans son trajet. Après l'utilisation de tous les pseudonymes disponibles, l'utilisateur peut en demander à l'autorité de confiance soit en se déplaçant physiquement pour en avoir, ou bien par le biais des protocoles de sécurité tels que [11].

L'idée principale de cette stratégie est de rompre les liens entre l'identité et les messages du véhicule ; comme elles éliminent les liens entre les messages d'un même véhicule. Cette technique est plus appropriée aux applications de sûreté du fait qu'elle ne déforme pas les données de localisation dans les messages envoyés,

n'utilise pas des messages factices et prend en charge les services d'authentification. Plusieurs schémas sont proposés dans ce sens, on peut les classifier en (i) Périodes de silence (Silent Period), (ii) Mix-Zone, (iii) Mix-Context, (iiii) Mix group. Toutes ces classes seront détaillées dans le chapitre 3.

L'objectif principal de la mise en œuvre d'un écosystème véhiculaire est la sécurité routière, le schéma de la protection de la vie privée doit considérer en priorité les applications de sûreté. Les trois premières stratégies qu'on a vues au début (cryptographie, perturbation et mise en cache), ne sont pas compatibles avec les applications de sûreté. Alors qu'on peut adapter la stratégie de changement des pseudonymes à ce type d'applications. Le défi majeur dans les approches de changement des pseudonymes est d'empêcher les liaisons syntaxiques ou sémantiques des pseudonymes. Pour suivre un utilisateur cible, l'attaquant collecte plusieurs pseudonymes pour les analyser pour pouvoir ensuite déduire une liaison entre ces pseudonymes. Il est important de noter qu'un attaquant local ne possède pas les moyens et les données suffisants pour casser cette protection.

2.4 Conclusion

La nature et les caractéristiques des réseaux véhiculaires, à savoir la vitesse de déplacement des véhicules et la scalabilité du réseau rend la sécurité du réseau une tâche fastidieuse ; beaucoup de recherches ont été investies dans ce domaine. La protection de la vie privée des véhicules et des conducteurs (propriétaires) est une exigence majeure pour rendre ces réseaux possibles dans la pratique, surtout lorsqu'il s'agit de la sécurité routière dans les systèmes de transport intelligents. Les menaces qui peuvent exploiter les vulnérabilités du système sont discutées dans ce chapitre, ainsi que les stratégies de protection proposées dans la littérature. C'est la stratégie de changement des pseudonymes qui nous intéresse beaucoup plus du fait qu'elle peut être adaptée aux applications de sûreté.

Chapitre 3

Stratégies de changement des pseudonymes

3.1 Introduction

Le travail de cette thèse rentre dans la proposition d'un nouveau mécanisme de protection d'emplacement dans les VANETs. Notre contribution suit la technique de changement des pseudonymes, vu les résultats de cette approche dans les travaux de recherches. Ce chapitre est dédié à cette technique, on présente quelques travaux existants dans la littérature afin de mieux comprendre le principe des pseudonymes, des certificats et du choix des moments de changement des pseudonymes.

3.2 Pseudonymes et certificats

L'authentification est un mécanisme nécessaire pour connaître la source de tout message ou comportement dans un réseau véhiculaire, l'identité réelle doit être donc claire et précise à l'autorité pour pouvoir gérer les événements qui se déroulent et protéger le réseau et les utilisateurs contre toute infraction. Pour convaincre les gens à investir dans un tel système, les propriétaires des véhicules et les conducteurs préfèrent ne pas divulguer les informations personnelles ou exactes. Les systèmes de transport intelligents se confrontent donc avec un grand défi, il faut avoir un nombre suffisant de véhicules enregistrés dans le réseau pour qu'il fonctionne correctement, et assurer l'authentification des véhicules enregistrés tout en protégeant leurs informations personnelles.

L'identité réelle ne doit pas être utilisée en clair dans les messages, et l'utilisation d'un pseudonyme unique au lieu de l'identité réelle n'est pas suffisante aussi. Le véhicule démarre dans la matinée d'un point donné pour arriver à un autre point (domicile, lieu de travail...) et revient le soir au même point de son départ, un attaquant peut corréler les traces de localisation de ce véhicule, et facilement connaître que le pseudonyme est alloué à sa cible. L'adversaire est capable de suivre plus tard toutes les traces du véhicule et la vie privée du conducteur est devenue en danger.

Pour chaque véhicule enregistré, l'autorité de confiance lui fournit un ensemble de pseudonymes certifiés, une clé privée pour chaque certificat et une seule identité réelle. Le véhicule choisit un pseudonyme de son pool, signe ses messages avec la clé privée correspondante au lieu d'utiliser son identité personnelle. L'autorité de confiance est la seule entité qui peut lier le pseudonyme utilisé par un véhicule avec son identité réelle.

Le changement de pseudonyme doit être soigneusement réalisé, du fait que l'attaquant peut corréler les certificats, les analyser pour pouvoir lier les pseudonymes utilisés par le même véhicule, pour pouvoir plus tard tracer son trajet. La section suivante présente les schémas proposés dans la littérature pour décider le moment ou le lieu idéal pour le changement des pseudonymes en toute sécurité.

3.3 Schémas proposés dans la littérature

Vu l'importance de soutenir l'anonymat des véhicules, le changement des pseudonymes a attiré plusieurs chercheurs et centres de recherches pour investir à sa résolution d'une manière fiable, efficace et sécurisée. Récemment, [51] a proposé une classification des schémas existants. La figure 3.1 illustre cette classification.

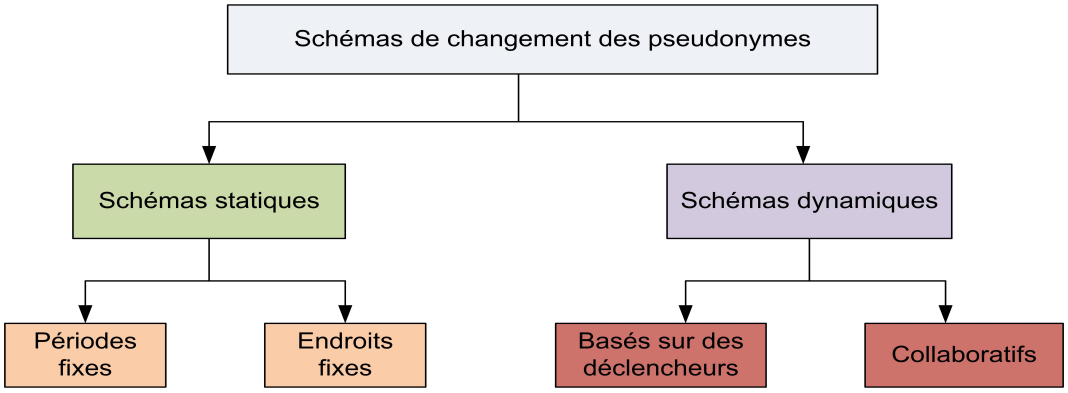

FIGURE 3.1 – Stratégies de changement des pseudonymes

3.3.1 Schémas statiques

Les travaux qui suivent cette stratégie reposent sur la fixation des périodes ou des endroits des changements des pseudonymes. Cela résulte à un changement relativement prévisible des pseudonymes, ce qui peut être considéré comme une information ajoutée qui aide l'attaquant.

Le changement des pseudonymes est précédé par des périodes de silence, une période de silence désigne que le véhicule éteint sa radio de transmission et s'arrête d'émettre les messages de contrôle.

3.3.1.1 Endroits fixes

Les travaux basés sur la fixation des endroits de changement s'appellent "Mix-Zone", ils choisissent des lieux connus comme les intersections, les feux de circulation, ou les lieux sociaux comme les hyper marchés.

X. Deng et al [19] proposent un protocole de changement de pseudonyme appelé (PCP), pour préserver la confidentialité de la localisation. Les auteurs ajoutent l'hypothèse d'existence des stations de bases dans le réseau ; en plus des entités connues comme les véhicules, les RSUs et l'autorité de confiance. Chaque station de base est chargée de l'enregistrement des véhicules qui se déplacent dans sa région en collaboration avec les RSUs. L'Autorité de confiance s'occupe de l'enregistrement des stations de base et des RSUs. Lors de l'enregistrement d'un véhicule auprès d'une station de base, cette dernière lui génère des pseudonymes et une clé du groupe. La clé du groupe est partagée entre tous les véhicules qui circulent dans sa région, et elle sera utilisée pour la signature des messages lors du changement des pseudonymes. Le mécanisme tient compte du nombre de véhicules dans la région et de la différence d'états de conduite entre les véhicules. Le changement se fait dans la région de la station de base seulement. Une fois le véhicule sort de la région de la station de base, tous les pseudonymes et toutes les clés qu'il possède n'ont plus de sens, il doit s'enregistrer de nouveau auprès de la station de base de son nouvel endroit. Cette approche nécessite un calcul énorme et supplémentaire qui influe sur la qualité de service du réseau, et une infrastructure trop chère, et loin des réseaux véhiculaires qui s'appuient beaucoup plus sur les communications inter-véhicules. Même si les véhicules changent de PC indépendamment dans ce protocole, les véhicules au sein du même domaine de station de base ne sont pas nécessairement voisins, de sorte qu'une éventuelle attaque de liaison syntaxique ou sémantique peut se produire.

A. Wahid et al [66] ont développés un schéma de préservation de l'emplacement, appelé «Coupling Privacy with Safety» (CPS). Les véhicules circulant dans la portée d'un RSU envoient des balises moins fréquemment pour assurer l'anonymat et

protéger l'emplacement du conducteur. Lors de l'enregistrement du véhicule, l'autorité lui attribue un identificateur et une clé secrète. L'autorité envoie la liste des identificateurs aux RSUs, les auteurs supposent que le véhicule circule dans sa ville seulement. Une fois que le véhicule rentre dans une région d'une RSU, il envoie un message à l'RSU pour s'authentifier, l'RSU vérifie sur sa liste si l'identificateur du véhicule figure ou non. Le véhicule et l'RSU calculent ensuite le pseudonyme qui sera utilisé le temps de séjour du véhicule dans la région du RSU. Le véhicule utilise le pseudonyme même lorsqu'il quitte la région. Les auteurs dans ce schéma manipulent l'identité comme un simple identificateur sans certificat, alors que réellement l'identité ou le pseudonyme doit être traité comme un certificat. Le véhicule envoi son identité lors de sa première communication avec chaque RSU rencontrée, de ce fait l'attaquant peut facilement suivre le trajet du véhicule et connaître toutes les régions qu'il a visitées puisque les réseaux véhiculaires sont ouverts, l'attaquant peut écouter tous les messages qui circulent y compris les messages entre les véhicules et la RSU. Le pseudonyme dans ce schéma est calculé sur la base de l'identité et la localisation, le suiveur peut donc déduire le nouveau pseudonyme. Le schéma CPS suppose que le véhicule n'est pas obligé d'envoyer les messages beacons périodiquement pour sa sécurité, il cède l'opération de diffusion des alertes aux RSUs, en oubliant que les messages beacons contribuent même au routage et à la connaissance de la topologie du réseau.

La stratégie proposée par [56] est basée sur la combinaison de deux schémas (CAPS) et (CPN) précédemment discutés appelée (CCAPS). Ce schéma profite des avantages de ces deux idées et les combine. le mécanisme de confidentialité d'emplacement proposé dans ce travail propose la fixation de trois régions autour du véhicule, la première région est sa portée du signal (R1), la seconde région (R2) sur laquelle il va appliquer la stratégie CPN, et une troisième région (R3) pour appliquer la stratégie CAPS. Sachant que R1 > R2 > R3, et que ces régions sont fixées par l'autorité de confiance pour unifier le schéma pour tous les véhicules du réseau. Le protocole CCAPS favorise la stratégie CPN qui est basée sur la densité des véhicules. Une fois le véhicule atteint son temps d'utilisation d'un pseudonyme, il cherche dans son voisinage R2 s'il y a des véhicules qui sont prêts au changement ; si c'est le cas il change son pseudonyme d'une manière synchrone avec ces voisins. En revanche, si aucun nœud dans sa région CPN n'est trouvé, il écoute l'état de ses voisins dans R3, s'il y a un véhicule voisin qui devient silencieux, le véhicule arrête la transmission de ses messages pour changer son pseudonyme après la période de silence. Cette stratégie montre de bons résultats, comme elle permet de minimiser l'inconvénient du schéma CAPS sans l'éliminer. Sauf que, elle repose sur les périodes de silences

qui se contredit avec la raison d'existence des systèmes de transport intelligents qui exigent que les messages périodiques ne doivent pas s'arrêter.

3.3.1.2 Périodes fixes

Initialement, la stratégie de changement de pseudonyme périodique (PPC : Periodical Pseudonym Change) a été introduite dans le sens où chaque pseudonyme peut être utilisé pour une période spécifiée. Le véhicule change son pseudonyme dans des intervalles de temps fixes ou aléatoires. Ce changement régulier offre à l'attaquent la possibilité de prévenir le prochain changement. A cet effet, le PPC était sensible aux attaques de liaison entre deux pseudonymes consécutifs utilisés par le même véhicule.

Pour lutter contre les attaques de liaison des pseudonymes, [28] ont proposé un mécanisme appelé RSP (Random Silent Period). Ils ont affirmé que la période de silence doit contenir une période constante et une autre période variable. La période constante permet de confusionner la relation spatiale entre la position initiale du véhicule et celle de sa nouvelle position. Tandis que la période variable mélange la relation temporelle entre les temps de disparition et les temps d'apparition du véhicule.

Les auteurs [52] ont proposé une extension du travail réalisé dans [28] appelé CARAVAN . Le véhicule rentre dans une période de silence aléatoire. Si deux véhicules A et B, entrent en même temps en silence et effectuent un changement de pseudonyme pendant cette période, l'attaquant ne pourrait plus corréler les pseudonymes des deux véhicules.

La stratégie « PCPPA » proposée dans [47] garantit une authentification, d'une manière efficace, des OBUs et des RSUs dans un réseau VANET. L'authentification repose sur la génération interne, dans un véhicule, d'un ensemble de pseudonymes et les partager via un canal sécurisé avec l'RSU proche. Chaque véhicule change son pseudonyme dans des moments bien déterminés, ce changement non coopératif ou qui ne tient pas compte du contexte de changement risque de ne pas assurer une indépendance des pseudonymes utilisés par le même véhicule. Les auteurs de PCPPA confirment qu'il est impossible de déduire une relation entre deux pseudonymes consécutifs, en oubliant qu'il y a des attaques syntaxiques et sémantiques dans les réseaux véhiculaires (voir Section 5.2.2).

3.3.2 Schémas dynamiques

Contrairement aux schémas statiques, les schamas dynamiques prend en considération l'environnement du véhicule pour effectuer un changement. Par l'environnement du véhicule, on sous-entend le nombre de ses voisins, le comportement de ses voisins, etc. Les stratègies de cette classe favorise le changement simultané de plusieurs véhicules.

3.3.2.1 Collaboratifs

Dans cette famille d'approches, le changement du pseudonyme nécessite la coopération entre plusieurs véhicules. Le changement tient compte du contexte des véhicules.

Dans [67], les auteurs proposent un nouveau schéma basé sur l'échange des pseudonymes entre deux véhicules. L'autorité de confiance enregistre les véhicules et les RSUs, un seul pseudonyme sera livré, via un canal sécurisé, à chaque véhicule avec son certificat et sa clé de signature. Le véhicule peut faire un échange de pseudonyme avec un autre véhicule rencontré, la condition d'échange repose sur l'état des deux véhicules. Si les deux véhicules sont proches d'états (exemple : déplacements avec la même vitesse), l'échange n'est pas intéressant. Si la condition est vérifiée, le véhicule qui veut effectuer l'échange de son pseudonyme envoie une requête encryptée à l'RSU, la requête contient les deux pseudonymes. L'RSU vérifie que le véhicule émetteur est authentique, et passe la requête à l'AC pour faire un changement dans sa base et informe les deux véhicules du changement. Ce mécanisme de sécurité repose sur l'échange des pseudonymes entre deux véhicules, ce qui donne une couverture de la vie privée des véhicules. Cette stratégie favorise le changement individuel, l'adversaire peut en déduire facilement, par l'attaque syntaxique des pseudonymes, que le nœud a changé son pseudonyme (Voir Figure 5.1.b). Un autre inconvénient de ce schéma est le contact fréquent de l'autorité et des RSU ; dans un réseau véhiculaire la vitesse de déplacement des véhicules est très élevée, ce qui fait que le nœud peut sortir de la zone d'une RSU et rentrer dans une autre zone rapidement. Les calculs supplémentaires sont aussi une limite de cette solution.

Les auteurs de [23] ont proposé un autre schéma appelé (CAPS), ce schéma supporte le changement de pseudonyme dans un contexte mixte pour interrompre la corrélation spatiale et temporelle des messages. La coopération dans ce schéma vient du fait que chaque véhicule surveille les véhicules de son voisinage, si un ou plusieurs voisins n'ont pas émis de messages beacons pendant une certaine durée de temps, il entre en période de silence. Il reprend l'envoi des messages de contrôle avec un nouveau pseudonyme lorsque son état réel est susceptible d'être confondu à l'état

d'un voisin silencieux. Le changement des pseudonymes est efficace d'un point de vue efficacité dans ce mécanisme, mais les applications de sûreté ne sont pas prises en compte, les véhicules sont en mode silence et arrêtent la diffusion des messages de sécurité, ce qui influe négativement sur le fonctionnement du système, et rend la sécurité routière, qui est considérée comme la raison d'existence de l'écosystème véhiculaire, en risque de ne pas fonctionner correctement. Une autre critique sur ce schéma est du fait qu'il suppose que la non réception des messages de sécurité de ses voisins, le véhicule comprend que ces voisins sont en silence, ce qui n'est pas toujours vrai, puisque le véhicule peut être dans une intersection ou circule dans le sens contraire de ses voisins ; à ce moment les véhicules ont quitté sa zone de couverture et ne deviennent plus des voisins.

Une autre proposition donnée par [44], le mécanisme est appelé (CPN). c'est un schéma coopératif pour le changement des pseudonymes. Il est basé sur le nombre de voisins. Lorsque le nombre de voisins atteint un seuil, les véhicules changent leurs pseudonymes. c'est une bonne stratégie du fait qu'elle favorise le changement simultané des pseudonymes par plusieurs véhicules, pour dévier le suiveur. Quand l'état des véhicules est très proche, c'est très difficile de les distinguer. L'inconvénient majeur est que le schéma effectue de nombreux changements de PC, même lorsque ces changements ne sont pas nécessaires. La taille du pool des pseudonymes est relativement limitée, le véhicule peut être obligé à revenir à un pseudonyme déjà utilisé. Une autre limite peut être liée à la non disponibilité du nombre nécessaire des voisins, lorsque le réseau n'est pas dense, le propriétaire du véhicule se déplace dans des endroits moins denses pour éviter la circulation par exemple, dans ce cas le pseudonyme ne sera jamais changé et le suiveur peut traquer le véhicule et savoir la totalité de son trajet.

Dans [51] , les auteurs ont proposé un nouveau schéma de changement de pseudonyme appelé « Context-Aware and Traffic Adaptive » (CATA), ce dernier profite des informations liées au contexte du véhicule et les modèles de trafic actuels pour choisir la situation optimale de changement des pseudonymes tout en préservant la confidentialité. Dans une région couverte par la même unité RSU, plusieurs véhicules changent leurs pseudonymes simultanément, à l'aide de déclencheurs dynamiques, afin d'assurer la confidentialité en maximisant l'anonymat. Les moments de changements sont décidés par les RSUs, et seront communiqués à tous les véhicules dans leur couvertures. Chaque véhicule génère son pseudonyme d'une manière autonome, à condition qu'il soit enregistré auprès de l'RSU. Un véhicule non enregistré est considéré comme intrus, son pseudonyme sera diffusé à tous les véhicules de la région pour qu'ils ne traitent pas les messages reçus de ce véhicule.

La génération locale du pseudonyme désigne que le pseudonyme est considéré comme un identifiant simple, tandis que réellement le pseudonyme doit être traité comme un certificat pour pouvoir responsabiliser les véhicules contre tout comportement malicieux (envoi d'un faux message, le déni de service...)

Récemment, les auteurs de [3] ont proposé un schéma de confidentialité lié à la sûreté nommé « Safety-Related Privacy Scheme » (SRPS), qui préserve la confidentialité en respectant les exigences des applications de sûreté VANET. L'idée de base de cette approche est de réduire les périodes de silence. Pour qu'un véhicule change son pseudonyme, il rentre dans une période de silence et continue à surveiller ses véhicules voisins ; si un accident est prévu, il sort de la période de silence et commence à partager les messages de sécurité avec ses voisins. SRPS est composé de deux algorithmes basés sur l'état du véhicule, l'un pour l'état silencieux et l'autre pour l'état actif. Les deux algorithmes inclus dans SRPS sont basés sur un algorithme de suivi multi-cibles MTT (Multi-Target Tracking) [22] pour la recherche d'un contexte efficace de changement des pseudonymes tout en évitant tout accident potentiel. MTT permet à un véhicule de deviner son prochain emplacement, ainsi que l'emplacement prochain de ses voisins actifs ou silencieux et enregistre ces prévisions. Une fois que la durée de vie du pseudonyme s'approche de l'expiration, le véhicule rentre dans une période de silence et calcule la distance entre son état actuel et celui prévu dans son historique. Si la distance est minimale, le véhicule ne change pas de pseudonyme, tandis qu'il le change une fois la distance est grande. Dans cette stratégie, la connaissance qu'un nœud voisin est silencieux est basée sur la non réception de deux beacons consécutifs. Cette hypothèse n'est pas toujours valable, puisqu'un nœud peut changer de direction dans une intersection ou tout simplement s'arrêter dans sa destination. Une autre limite qu'on peut tirer de cette stratégie est que les situations d'urgence n'impliquent pas forcément tous les véhicules à proximité, et ce pour ne pas submerger le réseau, c'est-à-dire que le véhicule doit estimer son implication ou son exclusion du processus de diffusion, avant qu'il ne sorte de son silence..

Parmi les travaux publiés récemment dans cette classe d'approches, les auteurs de [36] ont proposé un schéma d'échange de pseudonyme indépendant de l'infrastructure, au lieu du changement, appelé RIPS (RSU-Independent Pseudonym Swap Scheme). Le travail a été amélioré plus tard dans [37]. L'échange des pseudonymes économise le nombre de pseudonymes nécessaires pour un véhicule, du fait que le même pseudonyme sera utilisé par un autre véhicule plus tard. Les stratégies d'échange traitent le pseudonyme comme une simple identité, cette hypothèse se contredit avec les exigences de sécurité, de confidentialité et de respon-

sabilité liées aux réseaux véhiculaires. La majorité des stratégies d'échange utilise l'RSU comme entité d'échange. Dans le schéma RIPS, les véhicules, indépendants des RSU, échangent et changent de manière coopérative les pseudonymes dans des contextes mixtes qui satisfont un niveau élevé de confidentialité de l'emplacement. RIPS signale chaque échange à l'autorité pour assurer la responsabilité et la non-répudiation, sauf que même cette signalisation n'assure pas une liaison étroite entre le véhicule et son pseudonyme.

Pour atteindre l'indépendance de l'infrastructure, l'autorité de confiance fournit à chaque véhicule, après son enregistrement, un ensemble de pseudonymes échangeables et un seul pseudonyme non échangeable.

Dans une situation favorable, basée sur le rapprochement du contexte, les véhicules voisins changent deux à deux leurs pseudonymes échangeables. Une mise à jour sur la liste des pseudonymes échangeables sera faite, en remplaçant le pseudonyme en cours par celui du véhicule partenaire. Ensuite, chaque véhicule choisit au hasard un pseudonyme, d'une manière synchronisée avec ses voisins, de sa liste pour l'utiliser comme prochain pseudonyme. Un rapport sera envoyé à l'autorité pour l'informer de ce changement, le rapport contient entre-autres le pseudonyme non échangeable comme moyen d'authentification.

3.3.2.2 Déclencheurs

L'idée principale de ces schémas est la satisfaction de certaines conditions liées au trafique, soit les véhicules circulent au dessous d'une vitesse, ou se trouvent dans des conditions similaires comme c'est le cas des endroits de congestions.

Une technique ou stratégie qui est devenue par la suite une référence dans la majorité des travaux a été publiée dans [15] appelée SLOW. Cette stratégie n'entraîne pas les infrastructures RSUs, par conséquent, les véhicules doivent pouvoir créer leurs propres zones mixtes. Le principe est simple mais efficace, d'un point de vue vie privée. Chaque fois que la vitesse du véhicule est au-dessous d'un seuil donné, le véhicule désactive sa transmission radio (Rentre en période de silence) pendant une période et change son pseudonyme avant qu'il ne sorte de cette période de silence. Prenons par exemple les endroits appelés « zone-30 », les véhicules dans cette zone ne dépassent pas la vitesse 30km/h, ces endroits connaissent une densité majeure. A ce moment, le véhicule n'envoie aucun message périodique ou un message qui contient sa position ou sa trajectoire, il en profite pour changer son pseudonyme dans cette période, et reprend la transmission des messages périodiques quand il sort de sa période de silence. Le même scénario est valable devant les feux de signalisation ou les endroits de circulations. Les concepteurs de cette idée supposent que

les véhicules dans ces endroits ne roulent pas trop vite et donc on enregistre moins d'accidents ou de dégâts même en cas d'accident. SLOW est très simple à mettre en œuvre, et même efficace en termes de confidentialité mais si tout passe comme prévu. On peut tirer quelques limites de cette solution, (1) Le changement inutile des pseudonymes : chaque fois que la vitesse du véhicule diminue du seuil choisi, il rentre dans une période de silence et change son pseudonyme, le nombre de pseudonymes alloués n'est pas infini, en plus du traitement supplémentaire ajouté, (2) Si le véhicule se trouve seul dans un endroit, il est totalement inutile de changer son pseudonyme, une attaque syntaxique ou sémantique peut facilement lier ses deux pseudonymes consécutifs, (3) La principale raison d'apparition des VANETs et des STICs est la sécurité des routes et l'envoi des alertes d'urgences dans un temps réel, cet objectif se contredit carrément avec les périodes de silences ajoutées.

Un schéma basé sur la prise en compte du trafic est publié dans [13], les auteurs proposent un protocole de détection du trafic basé sur le comportement du véhicule. Lorsque la vitesse du véhicule diminue, il envoie un message de détection du trafique, il attend jusqu'à la réception du même message d'un autre voisin pour valider l'existence de la congestion. Un seul véhicule sera élu parmi ses voisins, par rapport à sa position vis-à-vis de ses voisins, pour qu'il soit un initiateur de la zone de silence. Le véhicule initiateur éteint sa radio de transmission, change son pseudonyme et diffuse périodiquement une notification de congestion. Chaque véhicule qui reçoit cette notification vérifie sa vitesse et sa position pour qu'il éteigne sa radio de transmission quand il vérifie certaines conditions. Un véhicule qui se trouve derrière l'initiateur d'une distance proche à la portée du signal sera élu comme un nouvel initiateur pour que la zone de silence reste toujours valable, et le premier initiateur arrête de diffuser ses notifications. Les notifications de congestion s'arrêtent lorsqu'un véhicule initiateur détecte la fin de la congestion en appliquant un protocole de détection.

A.Boualouache et al [14] ont développé un nouveau cadre pour le changement des pseudonymes. La zone couverte du réseau est divisée en différentes zones sous la forme d'une grille à des cellules. Chaque cellule contient une ou plusieurs zones logiques, ces zones logiques sont considérées comme les zones de confidentialité d'emplacement des véhicules (Vehicular Location Privacy Zones (VLPZs)). Les VLPZs sont déployées par des RSUs sur les infrastructures routières, telles que les stations-service, pour fournir un changement et une gestion sécurisées des pseudonymes. Chaque RSU envoie des messages périodiques dans sa région, pour informer les véhicules qui rentrent dans sa région de la disponibilité du service de changement des pseudonymes. Une fois le véhicule est concerné par le changement, il envoie une

requête à l'RSU, éteint sa radio de transmission, et suit le chemin tracé par un routeur de la zone vers un emplacement choisi d'une manière aléatoire et sécurisé. Le véhicule reste pendant un temps de service à la station puis quitte la station après le changement du pseudonyme ; le temps de service entre les véhicules est variable selon les services demandés. de cette manière la période de silence est non gênante du fait que les applications de sûreté ne sont pas affectées.

Un autre travail qui a été publié par [71] rentre dans le cadre des travaux de cette famille. Les auteurs proposent un schéma basé sur l'estimation du nombre de voisins et leur localisation, appelé « ENeP-AB :Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing », les véhicules réduisent leurs portés du signal et changent leurs pseudonymes ensuite, pour empêcher un attaquant de distinguer entre les véhicules du groupe. Ensuite, ENeP-AB a été amélioré dans un second travail appelé E-ABRP, qui permet aux véhicules d'utiliser des intervalles variables entre les beacons.

3.4 Comparaison

Dans la fin de ce chapitre on aimerait bien synthétiser les résumés cités ci-dessus. Le Tableau 3.1 établit une comparaison entre ces travaux. L'analyse des travaux a été faite selon plusieurs critères à savoir :

1. **La classe**

   Dans la deuxième colonne, on rappelle la classe du schéma par rapport à la classification adoptée.

2. **Changement des pseudonymes**

   Cette métrique représente la fréquence du changement des pseudonymes dans chaque schéma. Le changement fréquent des pseudonymes influence négativement sur la qualité du schéma de confidentialité du fait que le pool des pseudonymes est un ensemble fini qu'on doit consommé avec modération. Il est donc important de considérer cette caractéristique lors de la conception d'un nouveau schéma de confidentialité basé sur la pseudonymisation. Les valeurs de cette métrique dans les schémas PCP [19] et CPS [66] dépendent du scénario, tandis que les autres, le changement peut être fréquent où la stratégie effectue des changements supplémentaires inutiles, moyen pour les schémas qui effectuent quelques changements supplémentaires et faible quand la stratégie effectue des changements nécessaires. Le schéma RIPS [36] repose sur l'idée d'échange, pour cela on ne peut pas mesurer la fréquence du changement des pseudonymes.

3. **Décision du changement**

   La décision du changement peut être prise dans différents niveaux (Véhicule, RSU,....). La majorité des schémas prennent la décision du changement au niveau du véhicule.

4. **Génération du pseudonyme**

   La génération des pseudonymes est une tâche allouée généralement à l'autorité de confiance, comme on peut trouver d'autres cas où la génération des pseudonymes est réalisée par les véhicules, l'RSU ou d'autres éléments comme les stations de base dans le PCP [19].

5. **Période de silence**

   Avant d'effectuer le changement du pseudonyme, les véhicules peuvent admettre ou non des périodes de silence pour confusionner le suiveur.

6. **Considération des applications de sûreté**

   La stratégie de changement des pseudonymes doit assurer un compromis entre la préservation de la confidentialité et le respect des exigences des applications de sûreté. Les valeurs de cette métriques montrent si ces schémas perturbent ou non les applications d'urgences.

7. **Calcul supplémentaire**

   Cette caractéristisue représente le taux de calcul interne des véhicules.

8. **Communication supplémentaire**

   Les communications supplémentaires sont considérées comme une limite pour les solutions VANETs, du fait que ces réseaux ont une bande passante limitée. La stratégie de confidentialité doit minimiser, dans la mesure du possible, les communications entre les composants du réseau (Véhicule, RSU, Station de base,...).

3.5 Conclusion

Ce chapitre a été consacré à la présentation de l'élément essentiel de notre sujet, qui est le pseudonyme et le certificat lié. Ensuite, un état de l'art sur les travaux de recherches publiés a été présenté. Tous ces travaux suivent la stratégie de changement des pseudonymes et visent à la résolution du problème de la confidentialité d'emplacement dans les VANETs.

TABLE 3.1 – Comparaison entre les schémas de confidentialité étudiés

Schéma	**Classe**	**Changement des pseudonymes**	**Décision du changement**	**Générateur du pseudonyme**	**Période de silence**	**Considère les applications de sûreté**	**Calcul supplémentaire**	**Communication supplémentaire**
PCP [19]	Endroits Fixes	Dépend des endroits visités	Véhicule	Station de base	Groupement	Oui	Elevé	Elevée
CPS [66]	Endroits Fixes	Dépend de la couverture des RSU	RSU	RSU	Oui	Oui	Elevé	Elevée
CCAPS [56]	Endroits Fixes	Moyen	Véhicule	Autorité de confiance	Oui	Non	Moyen	Faible
RSP [28]	Périodes fixes	Fréquent	Véhicule	Autorité de confiance	oui	Non	Faible	Faible
CARAVAN [52]	Périodes fixes	Fréquent	Véhicule	Autorité de confiance	Oui	Non	Moyen	Moyen
PCPPA [47]	Périodes fixes	Fréquent	Véhicule	Véhicule	Oui	Non	Elevé	Moyen
Trigger-based [67]	Collaboratif	Moyen	Véhicule	Autorité de confiance	Non	Non	Elevé	Elevée
CAPS [23]	Collaboratif	Fréquent	Véhicule	Autorité de confiance	Oui	Non	Elevé	Elevée
CPN [44]	Collaboratif	Fréquent	Véhicule	Autorité de confiance	Oui	Non	Moyen	Moyen
CATA [51]	Collaboratif	Fréquent	RSU	Véhicule	Non	Non	Elevé	Elevée
SRPS [3]	Collaboratif	Moyen	Véhicule	Autorité de confiance	Oui	Oui	Elevé	Elevée
RIPS [36]	Collaboratif	ECHANGE	Véhicule	Autorité de confiance	Non	Non	Elevé	Elevée
SLOW [15]	Déclencheur	Fréquent	Véhicule	Autorité de confiance	Oui	Non	Faible	Faible
TAPCS [13]	Déclencheur	Moyen	Véhicule	Autorité de confiance	Oui	Non	Elevé	Elevée
VLPZs [14]	Déclencheur	Faible	Véhicule	Autorité de confiance	Oui	Oui	Faible	Faible
ENeP-AB [71]	Déclencheur	Fréquent	Véhicule	Autorité de confiance	Oui	Non	Faible	Faible

Chapitre 4

SPFX : La stratégie du pseudonyme commun

4.1 Introduction

Ce chapitre présente notre mécanisme de confidentialité proposé. L'idée de base se concentre sur l'utilisation d'un pseudonyme commun par plusieurs véhicules voisins. Le pseudonyme commun sera utilisé pendant une courte durée de temps pour permettre aux véhicules de changer leurs pseudonymes après. Dans notre étude, le PC est un certificat fourni par une AC et il est utilisé pour signer tous les messages à envoyer. Par ce nouveau schéma, on peut éviter pas mal de limites des autres solutions vues dans le Chapitre 3.

4.2 Architecture

Dans cette section, on présente les éléments de base participants dans notre système, comme on présente toutes les communications possibles entre ces entités. Rappelons les principaux enjeux de sécurité pour les systèmes de transport intelligents coopératifs (STI-C) déjà vus dans la section 2.2. Un écosystème de transport intelligent coopératif est composé de véhicules, de RSU, d'une Autorité de confiance (AC) et de serveurs d'applications d'opérateurs routiers. Un véhicule bénéficie d'applications de sécurité critiques et contraignantes, et d'autres applications moins contraignantes telles que les systèmes de gestion du trafic. Ces services sont fournis à travers les communications V2V et V2I. Les RSU sont connectées à l'infrastructure par des réseaux filaires. Chaque véhicule envoie ses messages signés, le message contient en plus de sa charge utile (l'information à transférer) le certificat du pseudonyme (Figure 4.1).

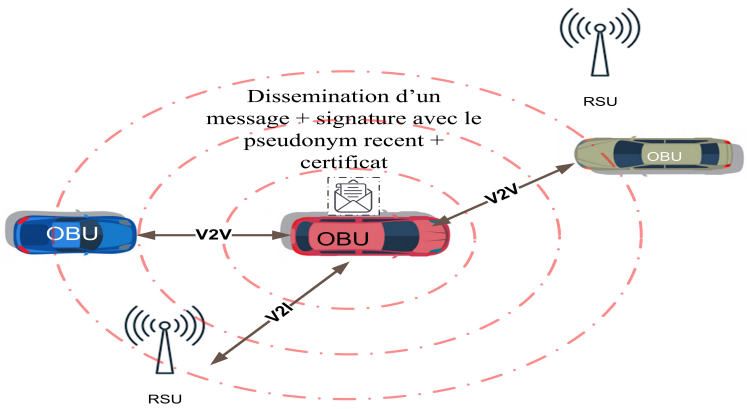

FIGURE 4.1 – Architecture et système de communication

Pour pouvoir communiquer avec l'ensemble du système, les véhicules doivent s'enregistrer auprès de l'autorité de confiance. La confiance entre les véhicules est garantie par l'utilisation de clés et de certificats délivrés par l'AC, comme illustré à la figure 4.2 . Étant donné qu'un véhicule est équipée d'un module de sécurité matériel (HSM : Hardware Security Module), c'est garanti que les clés privées sont protégées en toute sécurité sur le véhicule.

L'enregistrement se réalise en deux étapes, le véhicule envoie une requête à l'AC via un canal sécurisé (peut être même un déplacement physique), l'AC génère à ce véhicule un ensemble de certificats des pseudonymes (CPs) et un certificat pour le pseudonyme commun (CPC). Si deux véhicules 'A' et 'B' demandent l'enregistrement auprès de l'autorité, le seul certificat identique est celui du pseudonyme commun. A ce moment l'autorité connaît bien la liaison entre l'identité réelle du véhicule et celle des pseudonymes livrés. Une fois que le véhicule ou le conducteur transmet un faux message ou fait une infraction, l'autorité peut facilement le distinguer des autres stations, en plus on a garanti que l'identité réelle du véhicule soit cachée.

Chaque véhicule utilise un CP contenant une clé publique signée par l'autorité pour assurer des communications sécurisées et anonymes. Les clés privées correspondantes sont stockées en toute sécurité dans le HSM du véhicule. Ces clés et certificats ne contiennent aucune information réelle sur le véhicule, ni sur le conducteur. De plus, un pool de CP est préchargé [65] ; ces CPs sont changés fréquemment pour assurer la confidentialité de l'emplacement du véhicule. Afin de garantir l'authentification, l'intégrité et la non-répudiation, chaque message envoyé doit contenir sa charge utile ainsi que la signature du message et le PC. Un véhicule utilise la clé pri-

vée de son PC actuel pour la signature, un récepteur vérifie la validité de la signature en utilisant le CP attaché.

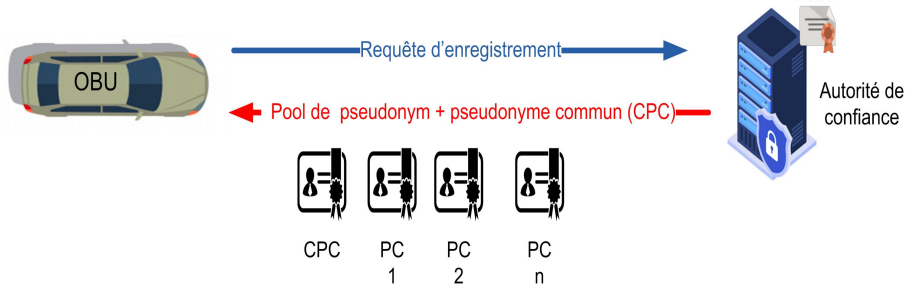

FIGURE 4.2 – L'enregistrement d'un véhicule

4.3 Modèle adversaire et capacité

L'objectif principal d'un adversaire dans notre étude est le suivi d'emplacement des véhicules. Malgré que les véhicules changent leurs pseudonymes fréquemment pendant un trajet, l'adversaire peut briser le mécanisme de confidentialité en écoutant les messages de contrôle, en collectant les données incluses et en traitant ultérieurement ces données. Supposons que l'adversaire connaît l'adresse d'un propriétaire, il commence à le suivre dès son démarrage de son domicile ou lieu de travail, une fois le véhicule change de pseudonyme, il peut facilement connaître le nouveau pseudonyme utilisé malgré qu'il ne contient aucune information détaillée sur le véhicule. A ce moment, la vie privée de la personne victime est en danger.

Plus l'adversaire possède des moyens et des mécanismes sophistiqués, plus il devient difficile de l'éviter ou de le dévier. Pour mesurer les performances de notre schéma de confidentialité, un modèle adversaire très puissant est utilisé. Cet adversaire contient un attaquant global qui couvre l'ensemble du réseau par des unités d'écoutes sans fil, et qui surveille et écoute tous les messages échangés, et envoie ses captures à un serveur central (Figure 4.3). On a utilisé le modèle d'adversaire existant inclus dans le module PREXT [21] pour tester notre système de confidentialité. Ce module facilite l'évaluation et la comparaison entre les schémas de confidentialité existants par rapport à un adversaire puissant dans un environnement véhiculaire. Les moyens du modèle sont les suivants :

1. **Des capteurs d'écoutes**

   Le modèle de menace comporte des récepteurs sans fil simulés par des modules

RSU ; ces récepteurs peuvent écouter le support sans fil. La fonctionnalité d'écoute non autorisée est implémentée dans la couche application de chaque récepteur. Les stations d'écoutes envoient tous les messages de balise capturés au serveur, qui collecte et traite ensuite toutes les informations reçues.

2. **Une couverture complète du réseau routier**

   L'attaquant est un adversaire global, il déploie plusieurs récepteurs (écouteurs clandestins) couvrant la totalité du réseau. Le nombre et l'emplacement des capteurs sont déterminés en fonction de leurs portées de communication attendues et du chevauchement possible entre les capteurs adjacents. La couverture complète du réseau routier, permet à l'entité centrale de collecter, traiter et analyser les messages de sécurité reçus, afin de suivre facilement le véhicule cible durant ses déplacements.

3. **Un serveur central de suivi**

   Pour plus d'efficacité, l'adversaire utilise une entité centrale appelée "Vehicle Tracker". Cette entité collecte les messages de balise reçus par les capteurs installés, pour suivre la cible. L'algorithme NNPDA (Nearest-Neighbor Probabilistic Data Association) est utilisé pour l'association et la liaison des messages.

La Figure 4.3 donne une illustration sur la couverture du réseau par des capteurs, il est clair que le véhicule cible envoi son emplacement pour rendre possibles les applications de sécurité routière et de prévention d'accidents ; le dispositif de sa région capte cette information et l'envoi au serveur central.

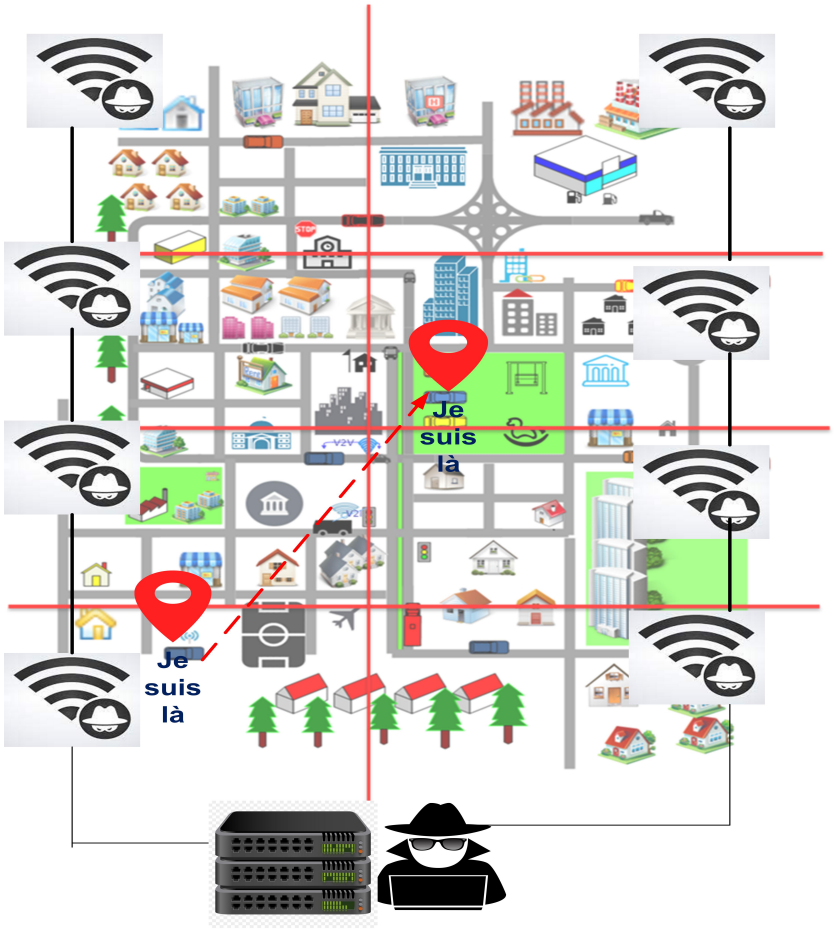

FIGURE 4.3 – Modèle d'adversaire

4.4 Principe

Dans cette section, nous présentons notre politique de confidentialité des véhicules dans un STI-C, appelée SPFX (Same Pseudonym beFore eXchange) [38] .

Nous considérons que chaque véhicule dispose d'un pool valide des pseudonymes. L'autorité délivre, avec tous les CP, un CP supplémentaire noté « CPC », commun à tous les véhicules. Une fois que les nœuds voisins acceptent de changer simultanément de CP, ils utilisent tous le CPC pendant une courte période. Ensuite, chaque véhicule sélectionne de son pool un nouveau CP indépendamment des autres véhicules.

Lorsque les véhicules voisins transitent vers le pseudonyme commun, la période de transition ressemble à la période de silence proposée dans de nombreuses études (par exemple [56]). La période de silence est non convenable aux applications de sûreté, car elle empêche la messagerie même en cas de conditions routières graves.

Une telle rétention d'informations cruciales ne convient pas à l'objectif d'amélioration de la sécurité des STI-C. Dans notre approche on doit s'assurer qu'un nombre considérable de voisins changent simultanément de CP, et de préserver la phase transitoire séparant les pseudonymes consécutifs de chaque véhicule. Pendant la phase de transition, tous les voisins synchronisés pour un changement simultané utilisent le même CP pour dissocier les identités individuelles des véhicules des informations contenues dans les messages de sécurité.

Précisons que chaque véhicule envoie périodiquement des informations d'état (vitesse, localisation, heure, date, etc.) dans un message de sécurité (Beacon) dans sa portée de transmission. Pour nos besoins, nous allons étendre ce message avec trois bits supplémentaires (Ready-Flag, Ready-Emergency-Flag, Node-Emergency-Flag). La Figure 4.4 montre un scénario possible de changement de pseudonymes. La première partie, 4.4.a, montre des véhicules qui se déplacent dans le même endroit utilisant leur pseudonymes (A, B, C, D, E, F, G). Une fois qu'il y a un consensus entre ces véhicules de changer leurs pseudonymes, tous utilisent le CPC comme le montre la figure 4.4.b (rappelons que CPC est le pseudonyme commun). Ensuite, tous les véhicules changent de PC indépendamment des autres, comme illustré à la figure 4.4.c. Si par exemple l'adversaire a ciblé le véhicule 'C' comme victime à suivre, la position du véhicule 'C' vis à vis des véhicules qui l'entourent a été changée pendant la période d'utilisation du CPC, ce qui rend le suiveur incertain pour la connaissance du nouveau pseudonyme choisi par le noeud 'C', qui est 'L' dans la figure. D'ailleurs, on trouve de nouveaux véhicules entrants dans la région d'intérêt (exemple du véhicule N) et d'autres la quittent (par exemple le véhicule A). La caractéristique des réseaux véhiculaires par rapport au changement rapide de topologie, qui est considéré comme une limite pour la majorité des schémas de confidentialité, devient ici un avantage pour mettre le suiveur dans un état de confusion.

4.4.1 Etapes du schéma SPFX

Nous détaillons ici notre approche en considérant les quatre étapes suivantes, suite à l'enregistrement initial du véhicule auprès de l'autorité de confiance (fait une seule fois). Pendant son trajet, le véhicule suit quatre étapes.

— **Etape 0 : L'enregistrement**

Afin de pouvoir communiquer au sein du réseau, un véhicule doit d'abord s'enregistrer auprès de l'autorité de confiance via un canal sécurisé afin de pouvoir s'authentifier ultérieurement. Une fois enregistrée, l'AC lui attribue un pool de CP et un CPC. Le CPC est le même pour tous les véhicules.

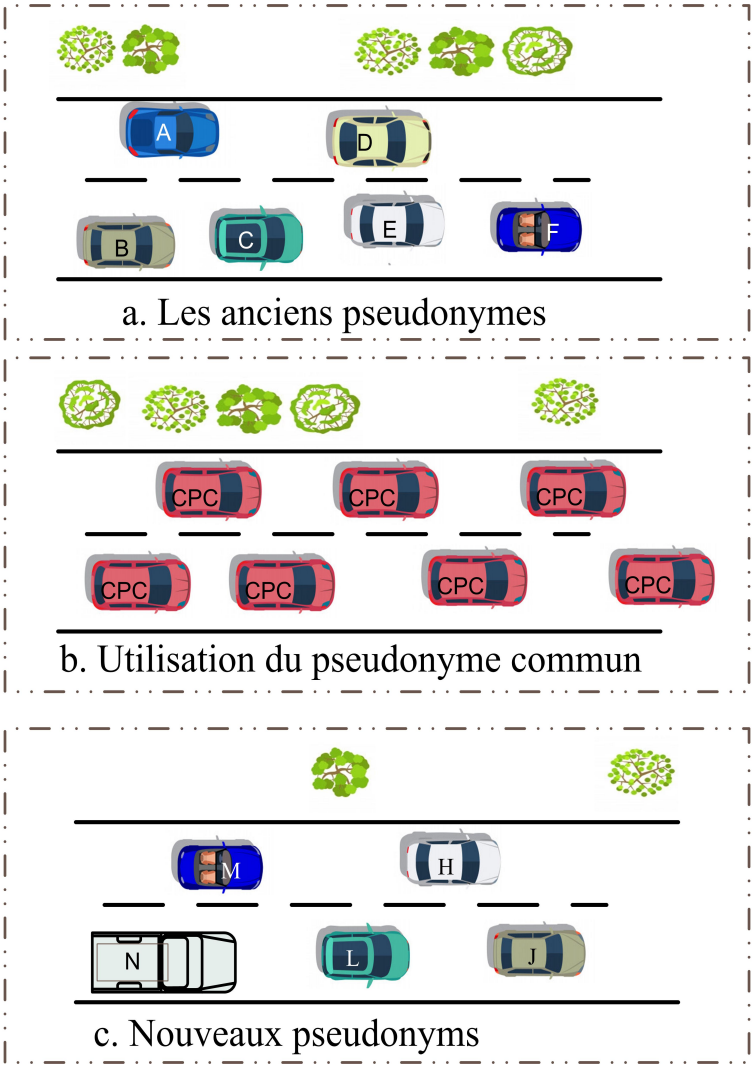

FIGURE 4.4 – Un scénario possible

— **Etape 1 : Sélection d'un CP**

Chaque véhicule dispose d'un ensemble de pseudonymes dans son pool interne à utiliser à la place de son identité réelle. Au début de son trajet, le véhicule doit sélectionner un CP dans son pool. Le CP sera utilisé pendant un temps déterminé T0.

— **Etape 2 : L'expiration de la durée de vie du CP**

De nombreuses recherches affirment que le changement simultané des pseudonymes, par plusieurs voisins, renforce efficacement la confidentialité d'emplacement. Pour cette raison, nous ajoutons un nouveau bit dans la structure de la balise, noté Ready-Flag. Lorsqu'un véhicule a consommé la durée de vie de son CP, il met à jour le bit Ready-Flag à 1 lors de ses prochains messages de sécurités (beacons) pour indiquer qu'il est prêt à changer de CP et que

la durée d'utilisation de son pseudonyme courant est achevée. Les voisins de l'émetteur possèdent un compteur interne pour savoir le nombre de véhicules prêts au changement, chaque récepteur incrémente le nombre des voisins prêts au changement du pseudonyme si le bit Ready-Flag dans le message reçu est mis à 1.

Dans cette étape, le véhicule attend pendant une période donnée, notée $T1$, en anticipant que plusieurs voisins seront prêts à changer de CP. Deux situations possibles peuvent se produire : (a) le nombre de voisins prêts atteint un seuil λ, donc le véhicule envoie un message indiquant à tous les voisins prêts de commuter leurs CP sur CPC à une durée de temps bien déterminée 'Val' ; la durée 'Val' est recommandée pour synchroniser le début de changement. Ensuite, tout les véhicules concernés par la commutation du pseudonyme passeront à l'étape 4. Plusieurs véhicules peuvent envoyer cette notification : dans une telle situation, le nombre de véhicules impliqués dans le processus de commutation peut augmenter. L'autre situation qui peut se produire est que (b) le temps $T1$ expire, dans une telle situation le véhicule entre dans une situation critique où il doit passer à l'étape 3.

— **Etape 3 : Recherche**

Dans cette situation, le CP du véhicule a dépassé sa durée de vie T0, et le véhicule a dépassé le temps d'attente $T1$ pour rencontrer des partenaires possibles qui veulent changer leur pseudonyme. Trois situations peuvent se présenter :

1. Le véhicule n'a pas rencontré suffisamment de voisins prêts lors de l'étape précédente (qui doit dépasser un seuil λ).
2. Aucun voisin prêt au changement n'a été rencontré.
3. Aucun voisin n'a été rencontré.

Le véhicule essaie maintenant d'influencer ses voisins pour qu'ils changent de CP même si leurs conditions pour le faire n'ont pas été déclenchées. Le véhicule passe son bit Ready-Emergency-Flag à '1' pour indiquer que son temps d'attente a expiré, et attend un message d'accusé de réception (Ack-Emergency), pendant une courte période $T2$, d'un ou plusieurs nœuds prêts à changer. Lorsque $T2$ a expiré, si le véhicule a reçu au moins un Ack-Emergency, il passe à l'étape 4. Si aucun Ack-Emergency n'est reçu, le véhicule est dans une situation qui correspond à la deuxième ou la troisième situation citée ci-dessus. Le véhicule essaie d'influencer à ce stade n'importe quel voisin en l'indiquant par le biais de son bit Node-Emergency-Flag. Il attend de recevoir un message

Ack-Emergency pour passer à l'étape 4. Il convient de noter que, si un véhicule reçoit un message Node-Emergency-Flag avant l'expiration de son propre CP, il doit répondre par un message Ack-Emergency, en se portant volontaire pour changer de CP avec le véhicule émetteur. De même, les véhicules recevant un message avec le bit Ready-Emergency-Flag à 1, doivent se porter volontaires pour changer leur pseudonymes en répondant par un Ack-Emergency.

— **Etape 4 : Utilisation du pseudonyme commun**

Nous atteignons cette étape lorsqu'au moins deux voisins acceptent de changer leurs pseudonymes simultanément, donc les actions de cette étape seront exécutées simultanément par au moins deux nœuds. Tous les voisins envoient leurs beacons comme d'habitude, contenant leurs positions et vitesses réelles, mais en utilisant le CPC, signé avec la même clé, pendant une courte période $T3$. Le capteur d'espion sera donc surpris, en voyant que tous les messages capturés semblent appartenir à la même entité émettrice, même si leurs expéditeurs diffèrent. La signature réalisée par tous les participants se fera de manière logicielle puisque le CPC et la clé privée correspondante ne se trouvent pas dans le module de sécurité physique du véhicule. Lorsque $T3$ expire, le processus passe à l'étape 1.

La Figure 4.5 résume le cycle de vie des pseudonymes.

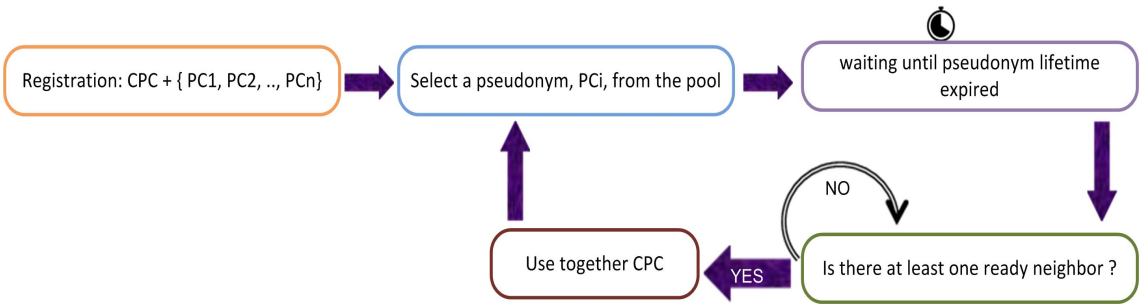

FIGURE 4.5 – Cycle de vie d'un pseudonyme

4.4.2 Temps estimatif de connectivité

Pour mesurer le temps d'utilisation du CPC, qui correspond au temps $T3$ (l'étape 4 vue dans la section précédente), le temps minimal de la connectivité entre les voisins du groupe sera choisi.

Conformément à la méthode faite dans notre travail de recherche [39], chaque véhicule peut estimer le temps restant de la communication avec ses voisins. Il envoie ensuite dans ses prochains beacons le minimum entre les valeurs estimées.

Nous utilisons les informations circulant dans la couche physique pour calculer avec précision la durée prévue pendant laquelle la communication entre deux véhicules voisins existe toujours. De plus, pour que le calcul soit plus réaliste, on utilise les informations disponibles dans un véhicule et la puissance du signal reçu, qui peut être calculée à la réception d'un paquet.

La formule qui établit la relation entre la puissance du signal reçu et la distance actuelle séparant deux véhicules communicants est :

$$Pr = Pt.Gt.Gr.\left(\frac{\lambda}{4\pi R}\right)^2 \tag{4.1}$$

où :

Pt : correspond à la puissance du signal à l'émission mesurée en Watt..

Gt : c'est le gain de l'émetteur (gain de l'antenne) mesuré en décibels..

Gr : c'est le gain du récepteur (gain d'antenne) mesuré en décibel.

R : la distance en mètre.

λ : est la longueur d'onde (m).

De l'équation Eq. (4.1), on peut déduire que la distance qui sépare deux véhicules communicants est la suivante :

$$R = \left(\frac{\lambda}{4\pi}\right)\sqrt{\frac{Pt.Gt.Gr}{Pr}} \tag{4.2}$$

Pour que la communication puisse s'établir entre deux véhicules communicants, la puissance du signal reçu doit être supérieure à une valeur seuil Ps, (qui est généralement très faible car les récepteurs sont très sensibles, on fixe Ps = Pt/2). Par conséquent, on aura :

$$Pr \geq Ps \tag{4.3}$$

Le remplacement de la valeur de Pr de (4.1) dans (4.3), on obtient :

$$Pt.Gt.Gr.\left(\frac{\lambda}{4\pi R}\right)^2 \geq Ps \tag{4.4}$$

Après la simplification de cette formule, on en déduit la distance maximale à

l'intérieur de laquelle deux véhicules peuvent communiquer correctement :

$$R \leq \left(\frac{\lambda}{4\pi}\right)\sqrt{\frac{Pt.Gt.Gr}{Ps}} \tag{4.5}$$

La distance relative entre l'expéditeur et le destinataire devient comme suit.

$$R = Vr.T \tag{4.6}$$

Où Vr représente la vitesse relative entre les deux véhicules et T représente le temps.

Vr peut être calculé comme suit :

$$Vr = || \overrightarrow{Vs} - \overrightarrow{Vr} || \tag{4.7}$$

$\overrightarrow{Vs}$ et $\overrightarrow{Vr}$ représentent la vitesse de l'émetteur et du récepteur respectivement.

Les deux équations Eq.(4.5) et Eq.(4.6), donnent :

$$Vr.t \leq \left(\frac{\lambda}{4\pi}\right)\sqrt{\frac{Pt.Gt.Gr}{Ps}} \tag{4.8}$$

Après simplification, on peut en déduire le temps maximum de communication entre les deux véhicules comme suit :

$$t \leq \left(\frac{\lambda}{4\pi.Vr}\right)\sqrt{\frac{Pt.Gt.Gr}{Ps}} \tag{4.9}$$

4.5 Algorithme proposé

Toutes les étapes de notre approche sont décrites ci-dessous dans un algorithme composé d'un algorithme principal, Algorithme 1, qui commence à s'exécuter lorsqu'un nouveau trajet commence. L'algorithme principal lance un sous-processus, Algorithme 2, qui réagit lorsqu'il reçoit une nouvelle balise. La procédure Waiting() dans l'algorithme 3 fait partie de l'algorithme principal et modélise le deuxième état qui renvoie le nombre de voisins prêts. Cette procédure lance un sous-processus, Algorithme 4, pour réinitialiser le compteur des voisins prêts toutes les 100 ms. Il lance également un sous-processus, l'algorithme 5, qui gère la réception des messages Ack-Emergency.

Algorithm 1 Main program

1: **Begin**
- P : Un pool de pseudonyms $\{P_0, P_1, ..., P_n\}$
- CPC : Certificat du pseudonyme commun
- T0 : Durée de vie d'un pseudonyme
- T1 : Temps d'attente pour effectuer un changement du pseudonyme
- T2 : Le temps d'attente pour recevoir un accusé de réception de voisins prêts.
- T3 : La durée de vie du pseudonyme commun.
- $Ready - Flag$ *: Utilisé par l'émetteur pour indiquer qu'il est prêt à changer de pseudonyme.*
- $Ready - Emergency - Flag$ *: Envoyé aux voisins prêts lorsque T1 est expiré.*
- $Node - Emergency - Flag$ *: Envoyé à tous les véhicules lorsque T2 est expiré.*
- N : Le nombre de voisins prêts à changer leurs pseudonymes.
- λ *: Un seuil de voisins prêts à apporter des changements.*
- $Ack - Emergency$ *: Un message pour indiquer l'acceptation de changer de pseudonyme.*
- $In - State - 4$ *: Une variable booléenne*
- $startCPC(Ti)$ *: Un message pour notifier à tous les voisins prêts (situés à un saut) de commencer à utiliser CPC à l'instant* $T - i$
2: Run-process receive-beacon(X) */*Lancer un processus pour gérer la réception des beacons. */*
3: **repeat**
4: T0 = Rand (min1,max1) ;
5: Ready-Flag = 0 ;
6: Ready-Emergency-Flag = 0 ;
7: Node-Emergency-Flag = 0 ;
8: Select-Pseudonym (P,T0) ; */*sélectionner un pseudonyme de P pendant une période T0 */*
9: In-State-4 = false ;
10: Wait until (T0 expire) or (In-State-4 = true)
11: **if** (In-State-4 = false) **then**
12: T1 = Rand (min,max) ;
13: ReadyFlag = 1 ;
14: N=0 ;
15: Waiting () */* une procédure pour synchroniser la fin du second état */*
16: **if** (State-4 = false) **then**
17: T2 = Rand (min2,max2) ;
18: Ready-Emergency-Flag = 1 ;
19: Wait until T2 expire ;
20: **end if**
21: **end if**
22: **if** (In-State-4 = false) **then**
23: Node-Emergency-Flag = 1 ;
24: Wait until (In-State-4= true)
25: **end if**
26: T3 = Rand (min,max) ;
27: SelectPseudonym (CPC,T3) ;
28: wait until (T3 expire) ;
29: **until** (End of journey)
30: **End.**

Algorithm 2 sub processes receive-beacon(src)

```
1: Begin
2: if ( Src.Node-Emergency-Flag = 1 ) then
3:    Send Ack-Emergency(src) ; In-State-4 = true ;
4: else
5:    if ( this.Ready-Emergency-Flag = 1 ) then
6:       Send Ack-Emergency(src) ; In-State-4 = true ;
7:    else
8:       if (src.Ready-Flag = 1) then
9:          N++ ;
10:      end if
11:   end if
12: end if
13: End.
```

Algorithm 3 Void Waiting ()

```
1: Begin
   /* créer et lancer deux sous-processus indépendamment*/
2: launch sub processes Reset-Neighbors() ;
3: launch sub processes Receive-Emergency-Ack() ;
4: repeat
5:    if (N ≥ λ) then
6:       Val = Rand (Min_T, Max_T) ; /* choisissez une valeur de temps aléatoire
         pour synchroniser le changement de CPC avec les voisins.*/
7:       broadcast startCPC (myclock+ Val) ;
8:       Wait until time expire (Val) ;
9:       In-State-4 = true ;
10:   else
11:      if (receives (startCPC (TTW)) then
12:         Wait until (TTW) ; /* Temps d'attente (TTW) avant de permuter au
            CPC */
13:         In-State-4 = true ;
14:      end if
15:   end if
16: until (T1 expire ) OR (In-State-4 = true)
17: Exit the sub processes Reset-Neighbors() ;
18: return ;
19: End.
```

Algorithm 4 sub processes Reset-Neighbors()

```
1: Begin
2: while (True) do
3:    Timer = 100ms ;
4:    Wait until (Timer expire) ;
5:    N=0
6: end while
7: End.
```

Algorithm 5 sub processes Receive-Emergency-Ack()

```
1: Begin
2: In-State-4 = true ;
3: return ;
4: End.
```

4.6 Conclusion

Il est clair que notre schéma protège la confidentialité d'emplacement des véhicules du réseau. La protection est basée sur le mécanisme du changement des pseudonymes, comme on a évité d'arrêter les messages de contrôle dans le réseau. Par conséquent, cette stratégie n'affecte pas les applications de sûreté qui exigent que l'information soit disponible et en temps réel. Afin de tester l'efficacité de notre mécanisme, on fait appel aux outils de simulations qui facilitent le test de toute solution dans ce cadre. Le chapitre suivant est consacré à la simulation et l'évaluation de performances de notre mécanisme.

Chapitre 5

Simulation et évaluation de performances

5.1 Introduction

La simulation est l'une des méthodes de validation les plus courantes de toute proposition dans le domaine des réseaux. Notre proposition a été comparée à divers schémas connus, tous ces schémas ont été utilisés comme références de comparaison dans de nombreuses études récentes. La simulation a été réalisée à travers la plateforme de simulation OMNET++, c'est un simulateur largement utilisé pour les réseaux sans fil.

5.2 Analyse du mécanisme

Dans cette section on va analyser notre mécanisme de protection de l'emplacement pour montrer qu'il est rigoureux, et qu'il est mieux adapté aux systèmes de transport intelligents par rapport aux schémas existants. On montre aussi la résistance aux attaques malveillantes possibles sur les techniques de changement de pseudonymes.

5.2.1 Considération des applications de sûreté

Les applications de sécurité nécessitent une dissémination très rapide des messages au sein de l'écosystème véhiculaire. Les stratégies basées sur le principe 'période de silence', où quelques véhicules éteignent leurs antennes et arrêtent de retransmettre les messages, ralentissent cette propagation ou l'annulent. Imaginons qu'un accident grave s'est produit. Les avertissements doivent être diffusés le plus rapidement possible pour minimiser ou éviter les dégâts. La transmission rapide du message d'alerte permet de créer un couloir d'urgence, d'éviter les embouteillages et de faciliter l'arrivée en temps nécessaire des services d'urgence et des autorités concernées. Notre modèle n'empêche pas la transmission de tels messages de contrôle ; cependant, il peut le faire en utilisant temporairement une pseudo-identité commune. Les véhicules dans la phase de transition entre l'ancien et le nouveau pseudonyme, signent leurs messages avec le pseudonyme commun, ce qui permet de transmettre les messages de contrôle d'une manière habituelle, et de retransmettre les messages d'urgence ou d'alerte reçus.

Dans la phase transitoire, les véhicules voisins utilisent un pseudonyme commun et donc signent leurs messages avec la même clé privée. A ce moment, on doit s'assurer que chaque véhicule soit honnête, puisque c'est difficile de distinguer les

véhicules dans cette période. Des mécanismes de révocation rapide des certificats sont utilisés. Si le véhicule se comporte mal ou commence à transmettre des faux messages dans le réseau, l'autorité de confiance lui retire le certificat et l'ajoute dans une liste noir pour ne jamais pouvoir contribuer dans le système. Plusieurs travaux de recherches ont été réalisés dans cet objectif [53, 63].

5.2.2 Résistance aux attaques

Lorsqu'un véhicule utilise en permanence un pseudonyme unique, le pseudonyme perd sa raison d'existence. Dans ce cas, tous les messages beacons ou autres sont diffusés sous la même pseudo-identité. Cela permet au traqueur, après l'écoute de plusieurs messages transmis par le même véhicule, d'en déduire facilement son trajet. L'objectif principal de la technique de changement de pseudonyme est d'éviter une telle liaison entre l'identité réelle et la pseudo-identité utilisée. Or, les stratégies proposées montrent encore une vulnérabilité vis-à-vis des attaquants susceptibles de corréler et d'en déduire une relation entre les différents pseudonymes pris par un même véhicule. Nous distinguons deux attaques de liaison possibles : la liaison sémantique et la liaison syntaxique de pseudonymes.

1. **Liaison basée sur la sémantique**
   Dans les stratégies non coopératives, le véhicule change régulièrement son pseudonyme d'une manière synchrone sans coopérer avec ses voisins, le traqueur peut facilement deviner quel véhicule a changé de pseudo-identité. Dans le scénario illustré sur la partie gauche de la Figure 5.1 (5.1.a) , le véhicule A change de CP après une durée Δt, alors que les autres véhicules voisins ne changent pas leur pseudonymes. Par conséquent, le traqueur détecte que le seul véhicule qui a changé de pseudonyme est le véhicule 'A'. L'attaquant en déduit alors facilement que le nouveau CP dans cette région est associé au véhicule 'A'. Notre approche assure le changement simultané des pseudonymes par plusieurs véhicules voisins, en exigeant des attentes avant le changement, pour éviter ce genre de situation. Si la période d'attente expire et aucun véhicule voisin n'est trouvé, un temps d'attente supplémentaire est ajouté pour donner une autre chance afin d'assurer un changement coopératif.
2. **Liaison basée sur la syntaxe**
   Les applications et la nature des réseaux véhiculaires exigent que tous les véhicules envoient, périodiquement, leurs vitesses et leurs positions actuelles dans des messages de sécurité d'une manière authentique. Les traqueurs utilisent ces informations, après un simple calcul, pour prédire la position future de ces véhicules. Compte tenu de cette information, même les mécanismes basés sur le changement simultané des pseudonymes restent incapables d'empêcher le traqueur de déterminer et d'en déduire le nouveau pseudonyme de sa victime. Comme le montre la Figure 5.1.b, le véhicule qui utilise le pseudonyme "A" se trouve à la position x0 et se déplace avec une vitesse v0. Après une durée Δt, la nouvelle position du véhicule A est simplement x0 + v0 Δt. En conséquence, le nouveau pseudonyme « E » sera associé au véhicule « A ». La conservation de l'emplacement dans notre mécanisme est très puissante vis à vis de cette

attaque, l'utilisation du pseudonyme commun permet au véhicule cible de se déplacer, pendant cette période, d'une manière cachée entre ses voisins.

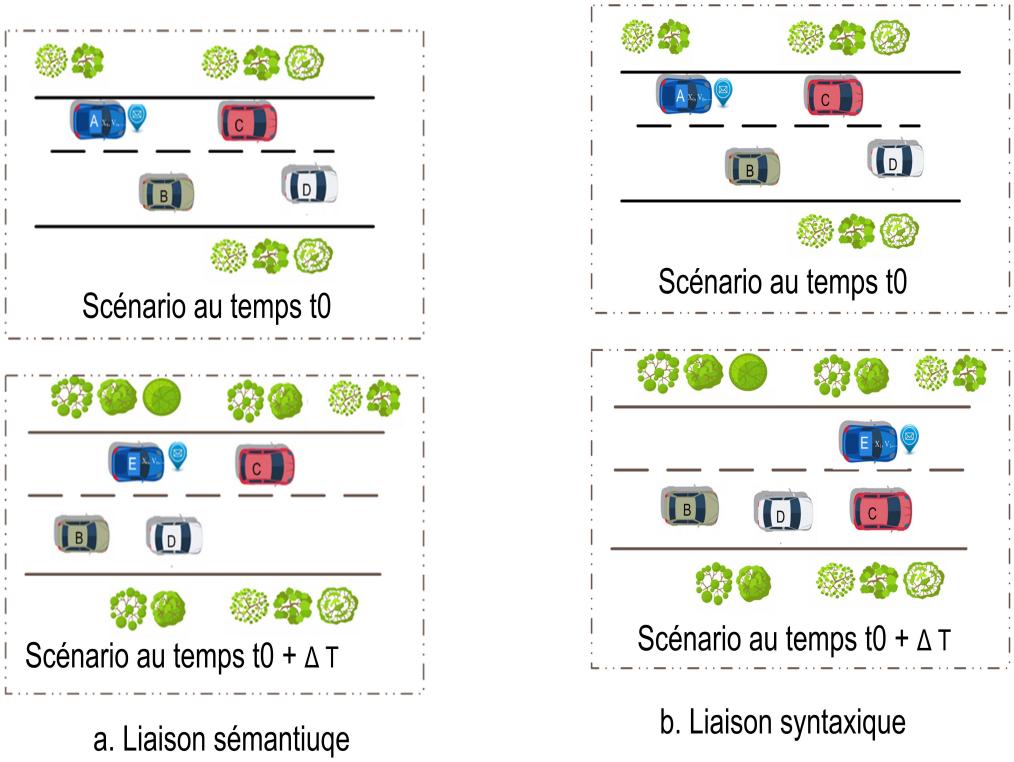

FIGURE 5.1 – Attaques sur la liaison

5.3 Simulation

L'évaluation des performances de notre mécanisme est une phase primordiale pour savoir sa résistance aux attaques possibles, cette section est consacrée à la présentation de l'environnement de simulation utilisé et à la discussion des résultats obtenus.

5.3.1 Environnement de la simulation

5.3.1.1 OMNET++

Nous avons effectué des simulations sous le simulateur événementiel des réseaux OMNET++ (Objective Modular Network Testbed in C++) dans sa version 5.0.

OMNET++ est livré avec une bibliothèque et un framework de simulation C++ extensible, modulaire et basé sur des composants, principalement pour simuler un réseau. Ce simulateur, dans son cadre, ne possède aucun module pour les protocoles de communication. Dans notre cas, on doit faire appel à des frameworks externes qui fournissent des protocoles de communications des VANETs, et d'autres framework pour la simulation du trafic routier.

5.3.1.2 SUMO

SUMO (Simulation of Urban MObility) est un simulateur du trafic routier. Ce simulateur est livré comme un package qui comporte plusieurs outils, permettant la création des scénarios d'un trafic routier qui respecte toutes les contraintes mises par un réseau véhiculaire. Les véhicules suivent la structure fixée par des routes, l'existence des buildings, et même des panneaux de signalisation et des feux de circulation, il inclut même les piétons.

5.3.1.3 VEINS

Le projet Open Source VEINS (VEhicles In Network Simulation), est un cadre de simulation dédié aux réseaux véhiculaires. VEINS contient une suite de modèles de simulation pour les VANETs, les modèles livrés s'exécutent sur l'interface graphique et l'IDE d'OMNET++, et interagit avec le simulateur du trafic routier SUMO. D'autres composants de VEINS s'occupent de la configuration, de l'exécution et de la surveillance de la simulation. L'interaction entre ces modèles offre une suite complète de modèles pour la simulation des communications inter-véhiculaires (IVC).

5.3.1.4 PREXT

PREXT est un cadre unifié et extensible conçu spécialement pour les réseaux véhiculaires, il simule des schémas de confidentialité basés sur le changement de pseudonymes dans les VANETs. PREXT repose sur une hypothèse principale des réseaux véhiculaire, qui est la diffusion des messages de sécurité (beacons) à des intervalles courts, le message contient des informations spatio-temporelle comme la position, la vitesse, l'heure et la date et la pseudo identité du noeud. Cet outil intègre sept schémas de confidentialité, de différentes approches telles que : Les schémas basés sur les périodes de silence (Silent Period,), basés sur le principe des zones mixtes (MIX-ZONE) ou sur le context (MIX-CONTEXT). PREXT intègre un adversaire passif global, qui a la possibilité d'écouter tous les messages de sécurité de tous les véhicules, l'adversaire tente de suivre la trace des véhicules pour casser le schéma de confidentialité. L'algorithme puissant (NNPDA) est utilisé pour le suivi des véhicules, il est capable de suivre les véhicules de manière efficace et efficiente.

La conception modulaire de la couche de confidentialité nous facilite la mise en œuvre de notre nouveau schéma de confidentialité. Plusieurs paramètres pour mesurer la performance de la confidentialité sont pris en charge. Pour cette raison, la plupart des études récentes valident leurs propositions en utilisant le cadre PREXT [57, 71, 56, 4, 58]

5.3.2 Paramètres

Nous mesurons plusieurs indicateurs de performance. Les valeurs correspondent aux paramètres généraux cités dans le Tableau 5.1, tandis que les paramètres d'adversaire sont établis dans le Tableau 5.2. Le Tableau 5.3 résume les valeurs choisies pour configurer chacun des schémas de confidentialité existants.

1. **Traçabilité Normalisée**

TABLE 5.1 – Les paramétres de Veins

Paramètre	**Valeur**
Data rate	18 Mbps
Transmission power	20 mW
Beacon rate	1 Hz
Data length	100 bytes
Header length	256 bits
Simulation time limit	300 s
Network size	2.7 km × 2.9 km
Number of vehicles	(150,300)

La traçabilité mesure l'efficacité avec laquelle un adversaire peut suivre un véhicule en continu sur plus de 90 % de sa trace [21]. Ce suivi est nécessaire afin de briser la confidentialité en terme de vie privée du conducteur ; car la découverte des traces nécessite des trajectoires entières. Une autre métrique proche de la traçabilité, c'est la traçabilité normalisée. Elle est calculée de la même manière, mais en négligeant les traces qui n'ont jamais changé de pseudonyme. De ce fait, la trace normalisée donne une information précise sur l'efficacité du schéma, de la protection de la vie privée du véhicule, contre les attaques de suiveur.

2. **Changement moyen des pseudonymes par trace**
   Un véhicule peut changer son pseudonyme plusieurs fois dans un trajet, cette métrique mesure le nombre moyen des changements de pseudonyme des véhicules. Le changement fréquent des pseudonymes n'est pas recommandé, il faut trouver un compromis entre l'efficacité du mécanisme de confidentialité et son coût de gestion. Pour ces raisons, nous devons équilibrer le nombre de changements de CP.
3. **Confusion moyenne par trace**
   Les schémas de confidentialité visent à cacher l'identité des véhicules pour éviter tout suivi de leurs emplacements. Pour ce faire, on doit mettre des moyens pour mettre le suiveur dans une situation de confusion lorsqu'il essaie de suivre la trace d'un véhicule. Cette métrique reflète la réussite du schéma de confidentialité. La confusion n'est possible que lorsque le véhicule change son pseudonyme. Cette métrique mesure donc l'efficacité de la stratégie de changement

TABLE 5.2 – Paramètres d'adversaire

Paramètre	**Valeur**
Eavesdropper range	300 m
Eavesdropper overlap	30 m
Track interval	1 s
Wait before delete	2 s
Type	eavesdropping and tracking

TABLE 5.3 – Paramétre des schémas de confidentialité

Schéma	**Paramètre**	**Valeur**
Periodical Pseudonym Change [45]	Pseudonym lifetime	60 s
RSP [28]	Pseudonym lifetime	60 s
	Silent period	(3, 9) s
SLOW [15]	Speed threshold	8 m/s
	Silent threshold	5 s
CPN [44]	Radius	100 m
	Neighbors threshold	2
CAPS [56]	Min pseudonym lifetime	60s
	Max pseudonym lifetime	180s
	Silence range	(3, 13) s
	Missed beacons silence threshold	2 beacons
	Neighborhood radius	50 m
SPFX	Pseudonym lifetime T_0	(120, 180)s
	Waiting time T_1	(30, 60)s
	Waiting time T_2	(1, 2) s
	Common pseudonym lifetime T_3	(1, 11) s
	λ	2

des pseudonymes, choisie lors de la conception du schéma de confidentialité.

4. **Confusion moyenne par changement de pseudonyme**
   Cette métrique garantit que le schéma proposé évite les traitements inutiles. Elle est définie comme le rapport entre le nombre moyen de confusions par trace et le nombre moyen de changements de pseudonyme par trace. Plus la métrique est grande, plus la solution est efficace. Comme mentionné dans la définition de la métrique moyenne de changement de CP par trace, nous cherchons à minimiser le nombre de changements de pseudonymes et à maximiser la confusion.

5.4 Discussion des résultats

Dans cette section, nous discuterons les résultats obtenus après simulation. Chaque résultat rapporté représente une moyenne de nombreuses expériences menées séparément. Pour que la comparaison soit significative, le même environnement est offert à tous les schémas. La mesure des performances est basée sur toutes les métriques qu'on a discutées ci-dessus.

5.4.1 Traçabilité normalisée

La figure 5.2 présente le taux de traçabilité moyen après différents tests. Notre mécanisme SPFX minimise considérablement le taux de traçabilité par rapport aux autres schémas.

Ces résultats montrent l'efficacité de l'utilisation du pseudonyme commun entre deux pseudonymes consécutif par chaque véhicule, l'attaquant est devenu incapable de continuer à suivre sa cible tout au long de son trajet.

Le changement simultané de plusieurs véhicules voisins renforce cette ambiguïté, ce qui interprète l'effet des temps d'attentes qu'on a exigé avant le passage à l'utilisation du pseudonyme commun.

Dans le réseau dense, nous avons minimisé la traçabilité par rapport à tous les schémas à l'exception du schéma SLOW, ce dernier minimise la traçabilité mais change fréquemment les pseudonymes (voir Figure **??**), ce qui nécessite un temps de traitement supplémentaire qui influence négativement sur l'écosystème véhiculaire.

Le suiveur doit assurer une traçabilité supérieure à 80 % pour révéler l'identité exacte du véhicule, ce que notre système évite avec succès. C'est bien de garantir un taux de traçabilité acceptable, la prise en compte des autres métriques est aussi nécessaire. Notre approche donne de meilleurs résultats par rapport au schéma SLOW dans les autres métriques.

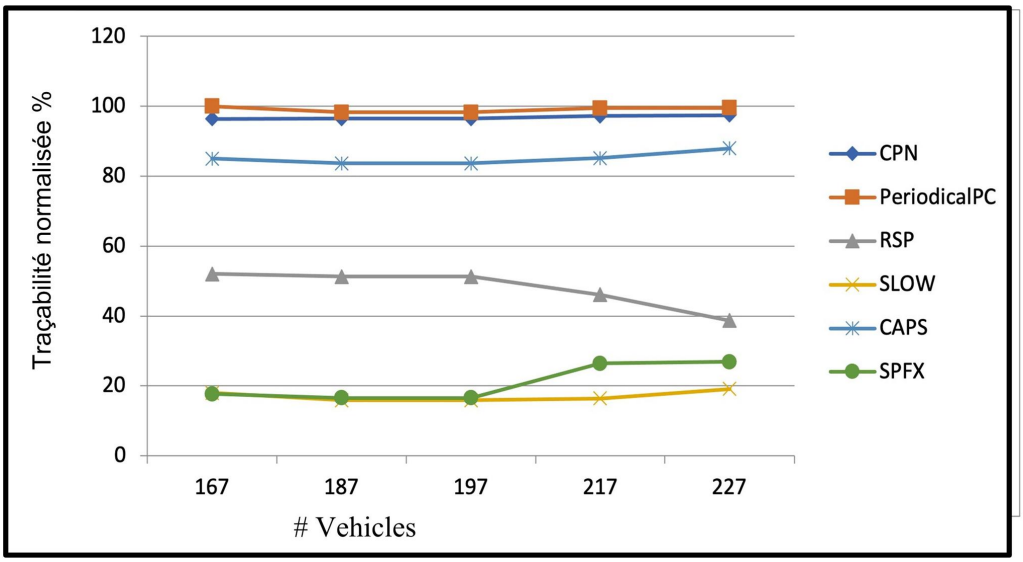

FIGURE 5.2 – Traçabilité

5.4.2 Changement moyen des pseudonymes par trace

Le changement des pseudonymes est nécessaire pour protéger le véhicule contre les attaques de liaison, le changement doit se faire avec modération pour éviter les calculs supplémentaires et garantir que le pool des pseudonymes soit suffisant pour une longue durée de temps. La figure **??** montre les résultats de la simulation en termes de changement moyen des CPs par trace dans différentes densités. Le changement moyen de CP par trace du schéma SLOW dépasse considérablement

celui de notre modèle. Cela est dû aux changements fréquents du modèle SLOW qui sont basés sur le seuil de vitesse et peuvent se produire à une fréquence inutilement élevée sans aucune nécessité. Dans cette figure (**??**), nous n'avons pas présenté la courbe liée au régime CPN ; les résultats obtenus par rapport à ce schéma sont hors de portée par rapport à tous les autres schémas.

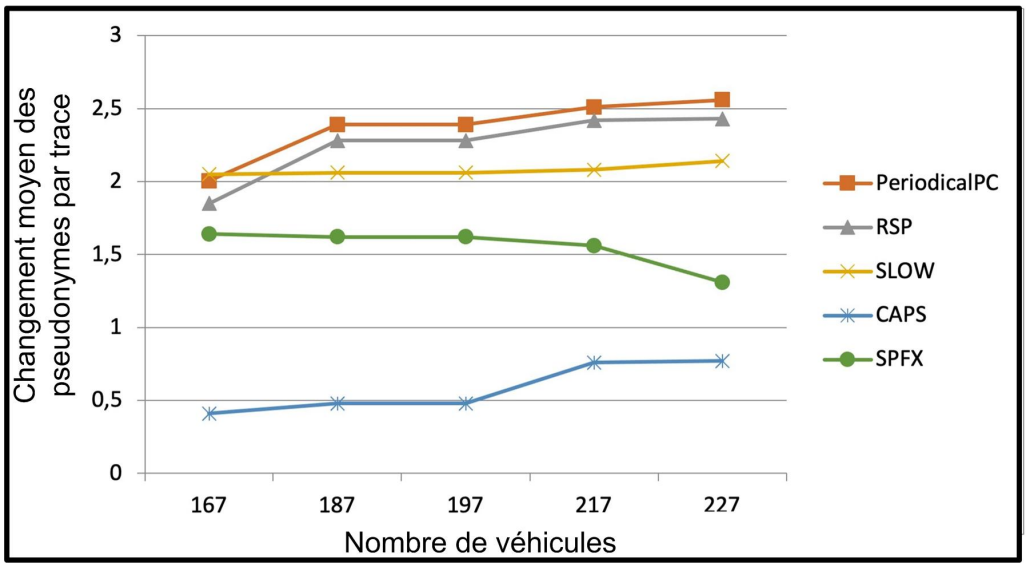

FIGURE 5.3 – Changement moyen des pseudonymes par trace

5.4.3 Confusion moyenne par trace

Cette métrique est aussi améliorée par notre mécanisme. Lorsque la confusion pendant une trace s'élève, le suiveur perd la boussole lors de son attaque, et le mécanisme de sécurité devient plus efficace. Les résultats de simulation par rapport à cette métrique sont illustrés dans la figure 5.4. Il est évident que notre schéma assure plus de confusion que les autres en raison de la phase transitoire ajoutée avant la mise à jour des pseudonymes. Tous les véhicules utilisent le même CP, laissant le traqueur de côté dans une décision incertaine quant aux prochains pseudonymes pris.

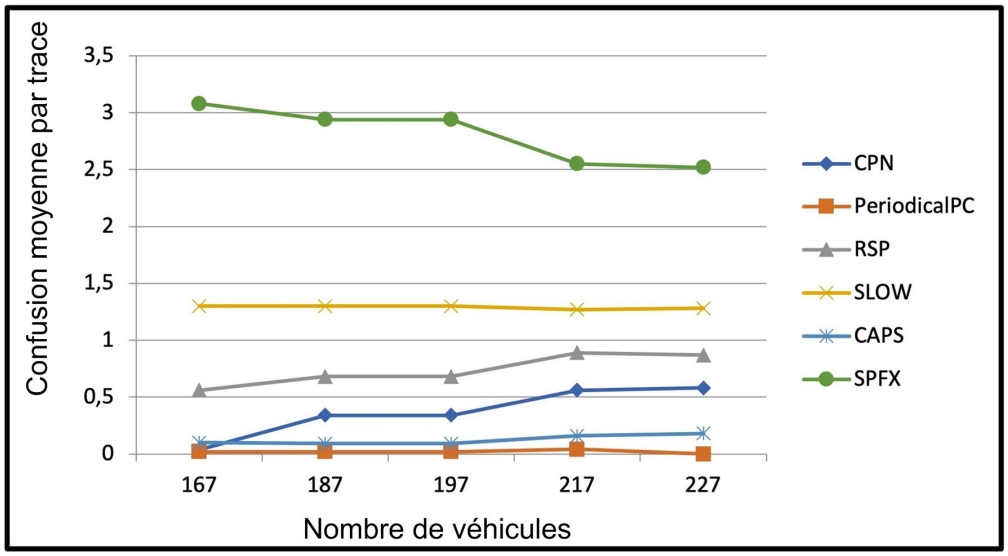

FIGURE 5.4 – Confusion moyenne par trace

5.4.4 Confusion moyenne par changement de CP

La figure 5.5 illustre la confusion moyenne selon la métrique de changement des CPs. Comme cette métrique représente le rapport entre la confusion et le nombre de changements des CPs, plus la métrique est élevée, plus le système est plus efficace. Nous maximisons le conflit au suiveur et minimisons le nombre de changements de pseudonymes pendant une trajectoire. Ainsi, notre approche donne des résultats nettement meilleurs par rapport aux autres.

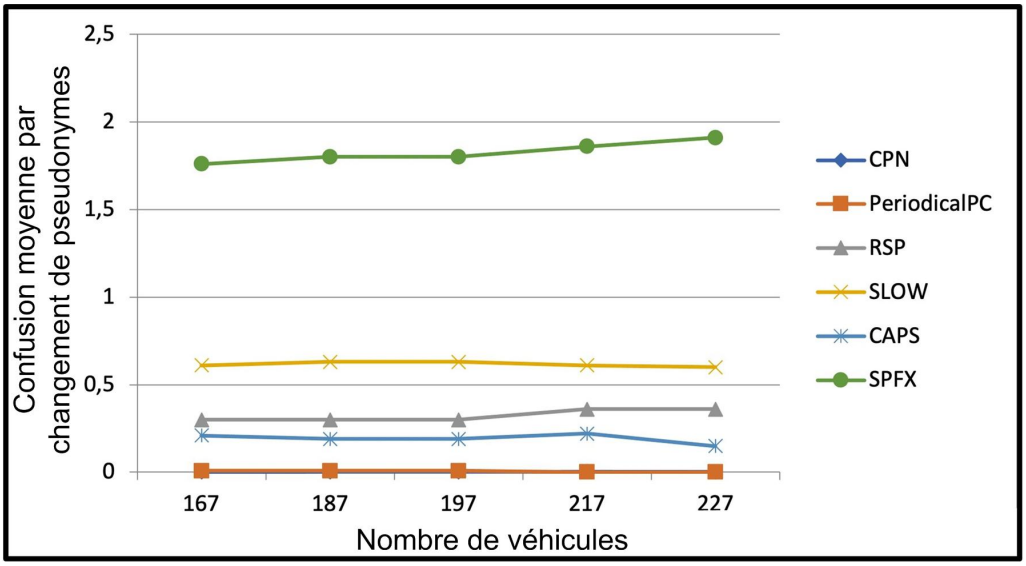

FIGURE 5.5 – Confusion moyenne par changement de pseudonymes

5.5 Conclusion

La simulation est le moyen le plus utilisé dans le domaine des réseaux. On a présenté en détail les acteurs de la simulation réalisée pour tester, évaluer les performances et comparer notre schéma avec quelques schémas existants.

Les résultats de simulation montrent que notre schéma est très efficace par rapport aux schémas qui existent dans le framework PREXT. La traçabilité est réduite considérablement, comme on a réduit le nombre moyen de changement des pseudonymes. Cette dernière métrique donne une impression que notre mécanisme élimine les calculs supplémentaires inutiles et donne la possibilité d'utiliser le pool des pseudonymes pendant une longue durée de temps.

Conclusion et perspectives

La technologie des réseaux véhiculaires est devenue très attractive aux chercheurs vu la promesse qu'elle donne aux usagers de la route. Plusieurs domaines de recherches sont ouverts pour la mise en œuvre de ces systèmes d'une manière efficace, la sécurité de l'écosystème représente la colonne vertébrale pour sa réussite. La sécurité concerne les données (confidentialité, cohérence, disponibilité et intégrité, non répudiation), et concerne aussi la confidentialité de l'emplacement des utilisateurs. Personne n'est autorisé à savoir l'identité du véhicule que l'autorité de confiance. Cacher l'identité du véhicule induit à la protection du propriétaire contre les menaces des suivis qui peuvent être présentes dans le système.

La meilleure façon de protéger l'identité du véhicule est de la remplacer par un pseudonyme. Il reste que l'utilisation d'un pseudonyme unique ne protège pas l'utilisateur contre les suivis d'emplacement, puisque le traqueur peut lier les certificats des véhicules du réseau, pour connaître le trajet de sa cible. Il est donc obligatoire de changer le pseudonyme pendant un trajet. Le défis du changement est le choix des moments où le véhicule change son pseudonyme d'une manière à ce que le suiveur devienne incertain du nouveau pseudonyme utilisé.

L'approche proposée dans cette thèse assure le changement des pseudonymes d'une manière efficace. Par rapport aux schémas existant, notre mécanisme réduit la traçabilité des véhicules avec des résultats nettement supérieurs. En outre des résultats obtenus, notre mécanisme garantit le respect des exigences des applications de sûreté, qui représente l'objectif principale de l'apparition des systèmes de transport intelligents. Ce respect repose sur l'utilisation d'un pseudonyme commun par un ensemble des véhicules voisins avant de basculer aux nouveaux pseudonymes.

Des expériences de simulation ont été conduites sous le simulateur OMNET++, utilisant le framework PREXT qui s'exécute sous VEINS. Cet environnement de simulation donne une signification aux résultats obtenus, du fait qu'il offre un environnement proche de la réalité.

Puisque notre mécanisme ne considère pas les attaques internes au moment d'utilisation du CP commun, on estime qu'il est nécessaire d'ajouter un modèle pour la révocation des certificats, le mécanisme de révocation permet de contrôler le comportement des conducteurs et des véhicules. Quand un véhicule présente un comportement malicieux, son certificat sera retiré par l'AC. Cette dernière informe tous les véhicules du réseau et les RSU pour ne pas considérer ses messages plus tard.

L'Internet des véhicules (IoV), compatible 5G, joue un rôle important dans les STI-Cs. Cependant, les stratégies de préservation de la vie privée proposées ne sont pas adaptées à l'IoV en raison de leur structure complexe et le temps de calcul énorme exigé par ces schémas. Une perspective de cette étude serait d'adapter le schéma de confidentialité proposé pour la préservation de la confidentialité dans le domaine IoV. En plus des véhicules intélligent, les communications dans l'IoV intègre d'autres capteurs et systèmes embarqués, c'est ce qu'on appel la communication V2X (Vehicle to Everything).

Bibliographie

[1] IEEE Std 1609.2 TM-2006, *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)–Security Services for Applications and Management Messages*, 2006.

[2] AA Alhaj et al., « Improving the Smart Cities Traffic Management Systems using VANETs and IoT Features », *in* : (2023).

[3] Ruqayah Al-Ani et al., « Privacy and safety improvement of VANET data via a safety-related privacy scheme », *in* : *International Journal of Information Security* (2023), p. 1-21.

[4] Ruqayah Al-ani et al., « Adjusted Location Privacy Scheme for VANET Safety Applications », *in* : *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2020, p. 1-4.

[5] Muhammad Arif et al., « A survey on security attacks in VANETs : Communication, applications and challenges », *in* : *Vehicular Communications* 19 (2019), p. 100179.

[6] Messaoud Babaghayou et Nabila Labraoui, « Transmission range adjustment influence on location privacy-preserving schemes in VANETs », *in* : *2019 International Conference on Networking and Advanced Systems (ICNAS)*, IEEE, 2019, p. 1-6.

[7] Ganesh Babu Loganathan, « Vanet Based Secured Accident Prevention System », *in* : *International Journal of Mechanical Engineering and Technology* 10.*6* (2019), p. 285-291.

[8] R Balamurugan, MM Hariharan et al., « VANET based accident alerting system », *in* : *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, 2021, p. 661-668.

[9] Sarah Baras et al., « VANETs-based intelligent transportation systems : An overview », *in* : *Advances in Computer Science and Ubiquitous Computing : CSA-CUTE 17* (2018), p. 265-273.

[10] Sarah Hasan Baras, « A citywide Intelligent VANETS-Based protocol for Traffic Control and Management at Intersections », *in* : *Diss. Abu Dhabi University* (2020).

[11] Leila Benarous et al., « Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET », *in* : *International Journal of Communication Systems* 33.*10* (2020), e4087.

[12] Abdelouahab Boualouache, « Sécurité et vie privée dans les réseaux véhiculaires », thèse de doct., université des sciences et de la technologie houari boumediene, 2016.

[13] Abdelwahab Boualouache et Samira Moussaoui, « TAPCS : Traffic-aware pseudonym changing strategy for VANETs », *in* : *Peer-to-Peer networking and Applications* 10 (2017), p. 1008-1020.

[14] Abdelwahab Boualouache, Sidi-Mohammed Senouci et Samira Moussaoui, « PRIVANET : An efficient pseudonym changing and management framework for vehicular ad-hoc networks », *in* : *IEEE Transactions on Intelligent Transportation Systems* 21.*8* (2019), p. 3209-3218.

[15] Levente Buttyán et al., « Slow : A practical pseudonym changing scheme for location privacy in vanets », *in* : *2009 IEEE Vehicular Networking Conference (VNC)*, IEEE, 2009, p. 1-8.

[16] IEEE Intelligent Transportation Systems Committee et al., « Trial-use standard for wireless access in vehicular environments (WAVE)-resource manager », *in* : *IEEE Std* (2006), p. 1609-1.

[17] Intelligent Transportation Systems Committee et al., « IEEE trial-use standard for wireless access in vehicular environments (wave)-networking services », *in* : *IEEE Std* 1609 (2007), p. 1603-2007.

[18] ITS Committee et al., « IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Multi-channel Operation », *in* : *IEEE, Standard* (2011), p. 1609-4.

[19] Xinyang Deng et al., « PCP : A Pseudonym Change Scheme for Location Privacy Preserving in VANETs », *in* : *Entropy* 24.*5* (2022), p. 648.

[20] Falko Dressler et al., « Research challenges in intervehicular communication : lessons of the 2010 Dagstuhl Seminar », *in* : *IEEE Communications Magazine* 49.*5* (2011), p. 158-164.

[21] Karim Emara, « Poster : Prext : Privacy extension for veins vanet simulator », *in* : *2016 IEEE Vehicular Networking Conference (VNC)*, IEEE, 2016, p. 1-2.

[22] Karim Emara, Wolfgang Woerndl et Johann Schlichter, « Beacon-based vehicle tracking in vehicular ad-hoc networks », *in* : (2013).

[23] Karim Emara, Wolfgang Woerndl et Johann Schlichter, « CAPS : Context-aware privacy scheme for VANET safety applications », *in* : *Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks*, 2015, p. 1-12.

[24] Jingyu Feng et al., « Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular networks », *in* : *IEEE Internet of Things Journal* 8.*4* (2020), p. 2087-2101.

[25] Ilya Finkelberg et al., « The Effects of Vehicle-to-Infrastructure Communication Reliability on Performance of Signalized Intersection Traffic Control », *in* : *IEEE Transactions on Intelligent Transportation Systems* 23.*9* (2022), p. 15450-15461.

[26] Amrita Ghosal et Mauro Conti, « Security issues and challenges in V2X : A survey », *in* : *Computer Networks* 169 (2020), p. 107093.

[27] Mustafa Maad Hamdi et al., « VANET-based traffic monitoring and incident detection system : A review. », *in* : *International Journal of Electrical & Computer Engineering (2088-8708)* 11.*4* (2021).

[28] Leping Huang et al., « Enhancing wireless location privacy using silent period », *in* : *IEEE Wireless Communications and Networking Conference, 2005*, t. 2, IEEE, 2005, p. 1187-1192.

[29] Jean-Pierre Hubaux, Srdjan Capkun et Jun Luo, « The security and privacy of smart vehicles », *in* : *IEEE Security & Privacy* 2.*3* (2004), p. 49-55.

[30] Shivkant Kaushik, Ramesh Chandra Poonia et Sunil Kumar Khatri, « Cryptographic key distribution using artificial intelligence for data security and location privacy in VANET », *in* : *Journal of Discrete Mathematical Sciences and Cryptography* 25.*7* (2022), p. 2195-2203.

[31] Ganesh S Khekare et Apeksha V Sakhare, « Intelligent traffic system for VANET : A survey », *in* : *International Journal of Advanced Computer Research* 2.*4* (2012), p. 99.

[32] Hidetoshi Kido, Yutaka Yanagisawa et Tetsuji Satoh, « Protection of location privacy using dummies for location-based services », *in* : *21st International conference on data engineering workshops (ICDEW'05)*, IEEE, 2005, p. 1248-1248.

[33] Nikhil Kshirsagar et US Sutar, « An intelligent traffic management and accident prevention system based on VANET », *in* : *ratio* 14 (2013), p. 2319-7064.

[34] Zihong Zhang Lei Chen Jiahuang Ji, *Wireless Network Security*, Springer Heidelberg New York Dordrecht London : Springer, 2013.

[35] Abdueli Paulo Mdee et al., « Impacts of location-privacy preserving schemes on vehicular applications », *in* : *Vehicular Communications* (2022), p. 100499.

[36] Abdueli Paulo Mdee et al., « Infrastructure-Independent Pseudonym Swap Protocol for Vehicular Networks », *in* : *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, IEEE, 2022, p. 351-356.

[37] Abdueli Paulo Mdee et al., « Security Compliant and Cooperative Pseudonyms Swapping for Location Privacy Preservation in VANETs », *in* : *IEEE Transactions on Vehicular Technology* (2023).

[38] Boubakeur Moussaoui, Noureddine Chikouche et Hacène Fouchal, « An efficient privacy scheme for C-ITS stations », *in* : *Computers and Electrical Engineering* 107 (2023), p. 108613.

[39] Boubakeur Moussaoui et al., « A cross layer approach for efficient multimedia data dissemination in VANETs », *in* : *Vehicular Communications* 9 (2017), p. 127-134.

[40] Boubakeur Moussaoui et al., « Routing over VANET in Urban Environments », *in* : *International Conference on Innovations for Community Services*, Springer, 2016, p. 143-152.

[41] Boubakeur Moussaoui et al., « Towards enhanced reactive routing in urban Vehicular Ad hoc Networks », *in* : *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, IEEE, 2015, p. 1-6.

[42] Boubakeur Moussaoui et al., « Unicast routing on VANETs », *in* : *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, IEEE, 2016, p. 1089-1092.

[43] Task Group p, *IEEE P802. 11p : Wireless Access in Vehicular Environments (WAVE)*, 2006.

[44] Yuanyuan Pan et Jianqing Li, « Cooperative pseudonym change scheme based on the number of neighbors in VANETs », *in* : *Journal of Network and Computer Applications* 36.*6* (2013), p. 1599-1609.

[45] Yuanyuan Pan et al., « An analytical model for random pseudonym change scheme in VANETs », *in* : *Cluster Computing* 17.*2* (2014), p. 413-421.

[46] N Premalatha et al., *VANET based communication on vehicles for accident prevention.*

[47] Jiayu Qi et al., « A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs », *in* : *Vehicular Communications* 38 (2022), p. 100535.

[48] Laurence R Rilett et al., « Simulating the TravTek route guidance logic using the INTEGRATION traffic model », *in* : *Vehicle Navigation and Information Systems Conference, 1991*, t. 2, IEEE, 1991, p. 775-787.

[49] Muhammad Saad et al., « Blockchain-Enabled VANET for Smart Solid Waste Management », *in* : *IEEE Access* (2023).

[50] Iman Saeed et Mourad Elhadef, « A Distributed inVANETs-Based Intersection Traffic Control Algorithm », *in* : *Advanced Multimedia and Ubiquitous Engineering : MUE/FutureTech 2018 12*, Springer, 2019, p. 343-351.

[51] Ikjot Saini, Sherif Saad et Arunita Jaekel, « A comprehensive pseudonym changing scheme for improving location privacy in vehicular networks », *in* : *Internet of Things* 19 (2022), p. 100559.

[52] Krishna Sampigethaya et al., *CARAVAN : Providing location privacy for VANET*, rapp. tech., Washington Univ Seattle Dept of Electrical Engineering, 2005.

[53] Hichem Sedjelmaci, Sidi Mohammed Senouci et Tarek Bouali, « Predict and prevent from misbehaving intruders in heterogeneous vehicular networks », *in* : *Vehicular Communications* 10 (2017), p. 74-83.

[54] Izdihar Sh Shaleesh et al., « Vehicle Location Privacy Protection Mechanism Based on Location and Velocity », *in* : *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, IEEE, 2022, p. 800-803.

[55] Muhammad Sameer Sheikh, Jun Liang et Wensong Wang, « A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets) », *in* : *Sensors* 19.*16* (2019), p. 3589.

[56] Pranav Kumar Singh et al., « CCAPS : Cooperative Context Aware Privacy Scheme for VANETs », *in* : *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, IEEE, 2019, p. 1-5.

[57] Pranav Kumar Singh et al., « CPESP : Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs », *in* : *Vehicular Communications* 20 (2019), p. 100183.

[58] Pranav Kumar Singh et al., « MPFSLP : Masqueraded Probabilistic Flooding for Source-Location Privacy in VANETs », *in* : *IEEE Transactions on Vehicular Technology* 69.*10* (2020), p. 11383-11393.

[59] Mujdat Soyturk et al., « From vehicular networks to vehicular clouds in smart cities », *in* : *Smart Cities and Homes*, Elsevier, 2016, p. 149-171.

[60] Jacob Speiran et Elhadi M Shakshuki, « A Smartphone VANET Based Forward Collision Detection System », *in* : *Procedia Computer Science* 198 (2022), p. 33-42.

[61] T Sujitha et S Punitha Devi, « Intelligent transportation system for vehicular ad-hoc networks », *in* : *International Journal of Emerging Technology and Advanced Engineering* 3.*6* (2014), p. 56-60.

[62] Shafin Talukder et al., « Vehicle Collision Detection & Prevention Using VANET Based IoT With V2V », *in* : *arXiv preprint arXiv :2205.07815* (2022).

[63] Andrea Tesei et al., « A transparent distributed ledger-based certificate revocation scheme for VANETs », *in* : *Journal of Network and Computer Applications* (2023), p. 103569.

[64] Roberto A. Uzcategui, Antonio Jose De Sucre et Guillermo Acosta-Marum, « Wave : A tutorial », *in* : *IEEE Communications Magazine* 47.*5* (2009), p. 126-133, doi : 10.1109/MCOM.2009.4939288.

[65] Eric Verheul, Christopher Hicks et Flavio D Garcia, « IFAL : Issue first activate later certificates for v2x », *in* : *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2019, p. 279-293.

[66] Abdul Wahid et al., « Holistic approach for coupling privacy with safety in VANETs », *in* : *Computer Networks* 148 (2019), p. 214-230.

[67] Shibin Wang et al., « A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs », *in* : *Peer-to-Peer Networking and applications* 11 (2018), p. 548-560.

[68] Theodore L Willke, Patcharinee Tientrakool et Nicholas F Maxemchuk, « A survey of inter-vehicle communication protocols and their applications », *in* : *IEEE Communications Surveys & Tutorials* 11.*2* (2009), p. 3-20.

[69] Besat Zardosht, Stephen Beauchemin et Michael A Bauer, « An in-vehicle tracking method using vehicular ad-hoc networks with a vision-based system », *in* : *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, 2014, p. 3022-3029.

[70] Hui Zhao et al., « IPARK : Location-aware-based intelligent parking guidance over infrastructureless VANETs », *in* : *International Journal of Distributed Sensor Networks* 8.*12* (2012), p. 280515.

[71] Ferroudja Zidani, Fouzi Semchedine et Marwane Ayaida, « Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs », *in* : *Computers and Electrical Engineering* 71 (2018), p. 359-371.