
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Mohamed Al Bachir Al Ibrahimi Bordj Bou Arreridj

Faculté des Mathématiques et d'Informatique



Remerciement

En tout premier lieu, nous remercions Dieu le Miséricordieux pour nous avoir donné la force et le courage de réaliser ce travail,

Nos sincères remerciements s'adressent en particulier à notre directeur de mémoire, **Mr Moussaoui Boubakeur**, pour nous avoir donné l'opportunité d'enrichir nos connaissances et nous avoir guidé par ses remarques pertinentes et ses conseils tout au long de la réalisation de ce travail. Nous désirons exprimer notre plus vive et sincère reconnaissance à tous nos professeurs qui nous ont permis d'acquérir plus de connaissances durant notre parcours.

Nous remercions profondément tous nos collègues, et toute l'équipe des deux départements des mathématiques et d'informatique.

Table des matières

Remerciement.....	2
Liste des figures	6
Liste de table	8
List des abréviations	9
Introduction générale.....	13
CHAPITRE 1:	14
1.1 Introduction	15
1.2 Définition	15
1.3 Eléments de bases	16
1.3.1 L'unité de bord (OBU).....	16
1.3.2 Les unités routières (RSU)	17
1.4 Architecture WAVE	18
1.4.1 Normes et standards	18
1.4.2 Protocoles de communication.....	18
1.5 les modes de communication.....	20
1.5.1 Véhicule à Véhicule (V2V) dans les VANETs	20
1.5.2 Véhicule à infrastructure	20
1.5.3 Infrastructure à infrastructure	20
1.6 Architecture.....	21
1.7 Caractéristiques	21
1.8 Types de messages	23
1.8.1 Messages périodiques (Beacons).....	23
1.8.2 Messages d'alerte.....	23
1.8.3 Messages d'usage général	23
1.9 Types d'applications VANET.....	24
1.10 La sécurité dans les VANET	25
1.10.1 Besoin de sécurité.....	25
1.10.2 Exigences de sécurité	25
1.10.3 Nature d'attaquant	27
1.10.4 Types d'attaques.....	29
1.11 Protection de la vie privée dans les VANETs	30
1.11.1 La préservation de la vie privée.....	30
1.11.2 Exigences de la vie privée	31
1.12 Conclusion.....	32
CHAPITRE 2	34
2.1 Introduction	34

2.2 changement de pseudonyme.....	34
2.3 strategies.....	34
2.3.1 pseudonymes	35
2.3.2 la Perturbation	36
2.3.3 Cryptographie.....	37
2.4 Les avantages / inconvénient de chaque méthode.....	38
2.5 Les pseudonymes et les certificats.....	39
2.6 Schémas proposés dans la littérature	40
2.6.1 Schémas statiques.....	40
2.6.2 Schémas dynamiques	41
2.7 conclusion	43
CHAPITRE 03	45
CONTRIBUTION	45
3.1 Introduction	45
3.2 Modèle adversaire et capacité	45
3.3 Schéma choisi.....	47
3.3.1 CAPS.....	47
3.3.2 CPN.....	47
3.4 Critiques et Solutions	47
3.5 Contribution	48
3.6 Notre proposition pour préserver la vie privée dans les réseaux VANET	49
.....	49
3.7 Conclusion.....	50
CHAPITRE 04	52
4.1 Introduction	52
4.2 Adversaire global	52
4.3 Analyse du mécanisme.....	53
4.4 Considération des applications de sûreté.....	53
4.5 Simulation	54
4.5.1 Environnement de la simulation	54
4.5.1.1 OMNET++	54
4.5.1.2 SUMO	55
4.5.1.3 VEINS.....	55
4.5.1.4 PREXT	55
4.5.2 Paramètres	56
1. Traçabilité Normalisée	56
2. Changement moyen des pseudonymes par trace	57

3. Confusion moyenne par trajet	57
4.6 Confusion moyenne par changement de pseudonyme.....	58
4.7 Configuration de Simulation	59
4.8 Discussion des résultats.....	60
4.9- La Conclusion	62
Conclusion générale	63
LES REFERENCE.....	64

Liste des figures

Figure 1 : Exemple d'un réseau VANET	16
Figure 2 : Les composants d'un véhicule intelligent.....	17
Figure 3:Le modèle WAVE/DSRC	19
Figure 4: Modes de communication dans le réseau véhiculaire VANET.....	21
Figure 5: Les attaquants internes et externes.....	28
Figure 6: Attaque passive.....	28
Figure 7: Sujets de recherche	31
Figure 8:Taxonomie des stratégies de changement des pseudonymes	36
Figure 9: Stratégies de changement des pseudonymes	40
Figure 10: Modèle d'adversaire.....	46
Figure 11: Architecture de l'extension de confidentialité proposée.....	53
Figure 12: carte géographique du centre-ville de Munich.....	60

Liste de table

Table 1:Les paramètres de Veins	56
Table 2:Paramètres d'adversaire	57
Table 3:Paramètre des schémas de confidentialité	58

List des abréviations

AU: Application Unit
CCH: Control Channel
CSP: Coordinated-Silent-Period
CA: Central Authority
CNPSR: National Center for Prevention and Road Safety
DSRC: Dedicated Short Range Communication
EDR: Events data recorder
IP: Internet Protocol
IEEE: Institute of Electrical and Electronics Engineers
ITS: Intelligent Transport Systems
GPS: Global Positioning System
GSM: Global System for Mobile Communication
LLC: Logical Link Control
MANET: Mobile Ad hoc NETwork
MAC: Medium Access Control
NNPDA: Nearest Neighbor Probabilistic Data Association
OBU: On Board Unit
PREXT : Privacy Extension for Veins VANET Simulator
RSU: Road Side Unit
RIN: Real Initial New
RCP: Resource Control Processor
RSP: random silent period
SCH: Service Channel
TCP: Transmission Control Protocol
TPD: Tamper-Proof Device
UDP: User Datagram Protocol
VANET: Vehicular Ad hoc NETwork
V2V: Vehicle to Vehicle
V2I: Vehicle to Infrastructure
WIFI: Wireless Fidelity
WAVE: Wireless Access in Vehicular Environments
WIMAX: Worldwide Interoperability for Microwave Access
4G: Fourth Generation

ملخص

في شبكات المركبات الذكية، يتبادل كل مركب معلومات حساسة مثل موقعه وسرعته بانتظام مع المركبات المجاورة. ومع ذلك، يؤثر هذا التبادل للمعلومات مشكلة خصوصية متعلقة بإمكانية تتبع المركبات وبالتالي السائقين. لمعالجة مشكلة التتبع هذه، تم اقتراح استراتيجيات تتضمن تغيير دوري للأسماء المستعارة للمركبات لمنع تتبعها غير المشروع. في هذا السياق، نقترح نهجاً جديداً لتغيير الأسماء المستعارة يعتمد على التعاون بين المركبات المجاورة.

تُمكن استراتيجيتنا من تغيير الأسماء المستعارة بشكل متزامن لعدد كبير من المركبات المجاورة، مما يوفر حماية محسنة ضد التتبع. أظهرت بواسطة) براكست (ان نهجنا يقلل بشكل كبير من قابلية تتبع المركبات، سواء في الشبكات نتائج المحاكاة التي تم إجراؤها الكثيفة أو الشبكات الخفيفة. بالتالي، فإن هذا الحل التعاوني يعزز حماية الخصوصية في شبكات المركبات الذكية.

Abstract

In VANETs, each vehicle periodically exchanges sensitive data such as its position and speed with neighboring vehicles. However, this information exchange raises a privacy issue related to the potential tracking of vehicles and, by extension, drivers. To address this traceability problem, strategies involving regular changing of vehicle pseudonyms have been proposed to prevent their illegal tracking.

In this context, we propose a new approach to pseudonym changing based on cooperation among neighboring vehicles. Our strategy enables simultaneous pseudonym changes for a large number of neighboring vehicles, thereby providing enhanced protection against tracking. Simulation results conducted under PREXT demonstrate that our approach significantly minimizes vehicle traceability, both in dense and sparse networks. This cooperative solution thus improves privacy protection in VANETs.

RESUME

Dans les réseaux VANET, chaque véhicule échange périodiquement des données sensibles comme sa position et sa vitesse avec les véhicules voisins. Cependant, cet échange d'informations soulève un problème de confidentialité lié au suivi potentiel des véhicules et, par extension, des conducteurs. Pour résoudre ce problème de traçabilité, des stratégies de changement régulier des pseudonymes des véhicules ont été proposées afin d'empêcher leur suivi illégal.

Dans ce contexte, nous proposons une nouvelle approche de changement de pseudonymes basée sur la coopération entre véhicules voisins. Notre stratégie permet un changement simultané des pseudonymes pour un grand nombre de véhicules voisins, apportant ainsi une protection renforcée contre le suivi. Les résultats des simulations réalisées sous PREXT démontrent que notre approche minimise considérablement la traçabilité des véhicules, tant dans les réseaux denses que moins denses. Cette solution coopérative améliore donc la protection de la vie privée dans les VANET.

Introduction générale

La sécurité routière est un enjeu majeur à l'échelle mondiale avec environ 1,3 million de décès par an dans des accidents de la route[3]. En Algérie, les statistiques sont également alarmantes avec 3.310 morts et 23.570 blessés sur les routes en 2023, des chiffres en hausse l'année suivante[3].

Pour améliorer cette situation préoccupante, les recherches scientifiques se sont orientées vers les systèmes de transport intelligents (ITS) reposant sur les technologies de communication sans fil et de géolocalisation[3]. Une part importante de ces travaux porte sur les réseaux véhiculaires ad hoc (VANET) où les véhicules communiquent entre eux et avec les infrastructures routières via des équipements embarqués (OBU)[5]. Les objectifs visés sont l'optimisation du trafic, l'amélioration de la sécurité routière grâce à des systèmes d'alerte en cas d'incident, et le confort des usagers avec l'accès à diverses applications[5].

Cependant, ces communications soulèvent des problématiques de sécurité cruciales, notamment les risques d'altération ou de suppression malveillante des messages liés à la sécurité routière, pouvant causer des accidents graves[3]. Parmi les exigences de sécurité à garantir figurent l'authentification, la confidentialité, l'intégrité, la disponibilité et la protection de la vie privée[3].

Le projet se concentre sur la préservation de la confidentialité et de l'anonymat des véhicules au sein du réseau VANET[3]. Bien que l'utilisation de pseudonymes apporte une confidentialité limitée, un changement fréquent de ces pseudonymes s'avère nécessaire pour brouiller les pistes et empêcher les attaquants d'identifier les véhicules[3]. Un mécanisme coopératif pour un changement coordonné des pseudonymes entre véhicules voisins est proposé, visant à minimiser les risques de traçabilité illégale tout en préservant l'anonymat[3].

- Dans le premier chapitre, on va présenter les réseaux VANETs, les caractéristiques et les exigences de sécurité.
- Le deuxième chapitre est dédié pour l'état de l'art sur la vie privée dans les réseaux VANETs,
- Dans le troisième chapitre, on va présenter notre contribution pour la préservation de la vie privée.
- Le quatrième chapitre sera consacré à la simulation et la mesure des performances.
- On conclut avec une conclusion générale.

CHAPITRE 1:

Généralités sur les VANETs

CHAPITRE 1

Généralités sur les VANETs

1.1 Introduction

Les véhicules jouent un rôle ambivalent, offrant des services de déplacement tout en représentant une source de danger pour la sécurité routière. En janvier 2022, les statistiques algériennes faisaient état d'un bilan alarmant, avec 1683 décès et 71 744 blessés dans 57982 accidents de la circulation[6]. Ces chiffres soulignent la nécessité urgente d'améliorer la sécurité sur les routes.

Les réseaux véhiculaires émergent comme une solution prometteuse pour renforcer la sécurité routière et optimiser les systèmes de transport[6]. La technologie VANET suscite donc un intérêt croissant auprès des chercheurs et des industriels, offrant des perspectives innovantes pour réduire les risques d'accidents.

1.2 Définition

Un réseau véhiculaire ad hoc (VANET) est un type particulier des réseaux mobiles ad hoc (MANET) dans lequel les nœuds mobiles sont des véhicules intelligents équipés de technologies de communication avancées. Les VANETs sont spécialement conçus pour permettre les communications entre véhicules. Cette connectivité véhiculaire permet l'échange d'alertes et d'informations pertinentes visant à améliorer la sécurité routière. Elle offre également la possibilité de déployer des applications destinées à accroître le confort des passagers. Ainsi, en établissant des communications dédiées entre les véhicules, les VANETs contribuent à un environnement routier plus sûr et plus intelligent.

La figure (1) présente un exemple d'un réseau VANET, elle montre une capture de communication sans fil entre plusieurs véhicules adjacents. Ces véhicules partagent des messages d'alertes et d'urgences pour assurer la sécurité routière.

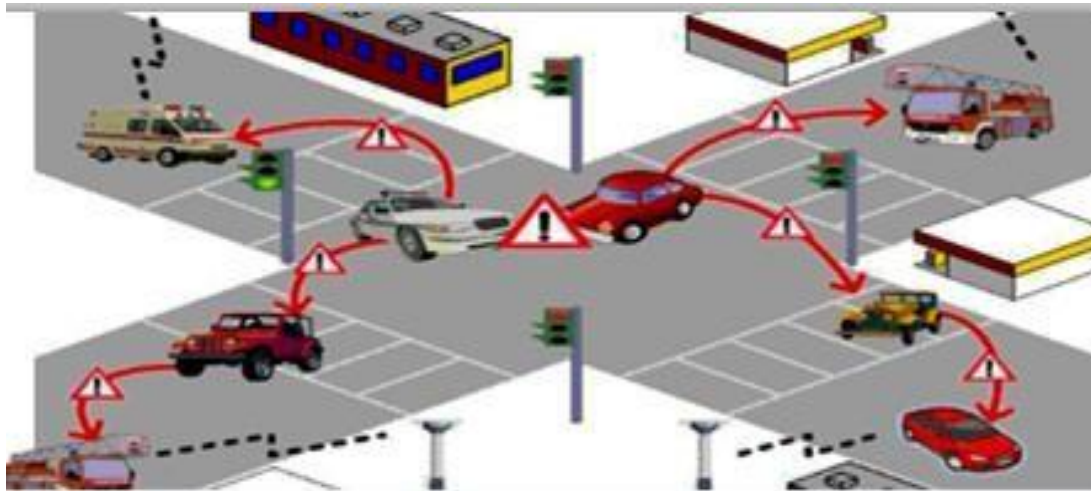


Figure 1 : Exemple d'un réseau VANET

1.3 Eléments de base

Dans le cadre du déploiement d'un réseau de véhicules, différents éléments sont essentiels, tels que les On Board Units (OBU), les Road Side Units (RSU), les piétons, les autorités de confiance, etc. Cependant, nous nous focalisons ici sur deux éléments fondamentaux : l'OBU et l'RSU.

1.3.1 L'unité de bord (OBU)

L'OBU est l'élément essentiel installé à bord des véhicules intelligents, permettant d'améliorer la sécurité, le confort et l'efficacité de la conduite[7][9]. Ses principales fonctionnalités sont :

1. Un émetteur-récepteur sans fil basé sur les normes Wi-Fi ou DSRC (Dedicated Short Range Communication) pour communiquer avec les autres OBU et les RSU (Road Side Unit)[7][8]. Le véhicule peut aussi être connecté à Internet.
2. Un système de positionnement GPS fournissant la position actuelle du véhicule en temps réel, pour calculer les itinéraires optimaux, éviter les embouteillages et donner des instructions de conduite précises.
3. Un système de stockage pour enregistrer les messages et informations de sécurité échangés avec l'environnement.
4. Un processeur pour traiter les données, prendre des décisions et émettre des alertes
5. Des capteurs (caméras, radars, lidars, ultrasons) pour surveiller l'environnement et collecter des données.

6. Des fonctionnalités d'aide à la conduite comme la détection de collision, le freinage d'urgence, l'aide au stationnement ou la surveillance de la fatigue du conducteur.
7. Une interface de communication homme-machine.

La Figure (2) illustre les composants du véhicule intelligent.

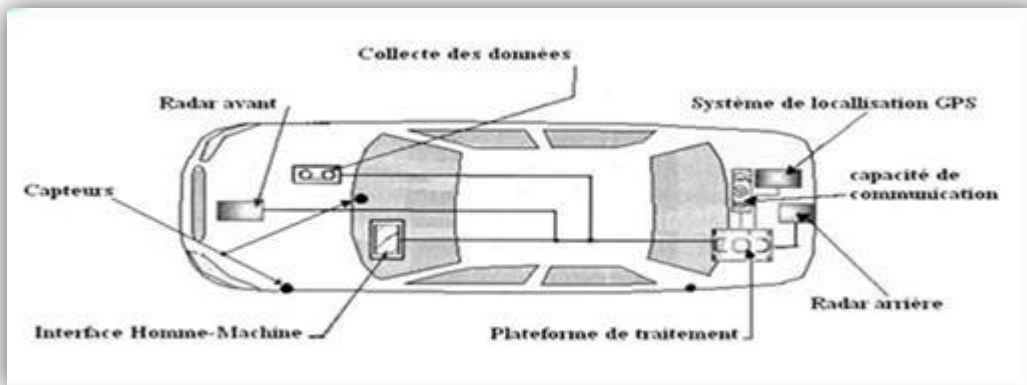


Figure 2 : Les composants d'un véhicule intelligent

1.3.2 Les unités routières (RSU)

Les Road Side Units (RSU) sont des équipements installés le long des routes, sur des panneaux ou des feux de signalisation, pour faciliter la communication au sein des réseaux VANET. Les RSU améliorent l'efficacité de la communication, surtout dans les zones moins denses. Leurs principales caractéristiques incluent :

1. Un émetteur-récepteur sans fil pour communiquer avec les OBU des véhicules à proximité.
2. Une connexion guidée, filaire ou fibre optique, avec d'autres RSUs.
3. Un système de stockage pour enregistrer les informations de sécurité et les données de trafic collectées des OBU des véhicules voisins.
4. Un processeur pour le traitement des données, la prise de décisions et l'émission d'alertes.
5. Des capteurs comme des caméras et des capteurs de mouvement pour surveiller l'environnement autour de l'RSU et recueillir des données sur le trafic et les conditions routières.
6. Une source d'alimentation, souvent un panneau solaire ou un réseau électrique, pour fournir de l'énergie à l'RSU. [10.11.12].

1.4 Architecture WAVE

Dans cette section, nous abordons l'architecture WAVE (Wireless Access in Vehicular Environments), conçue spécifiquement pour les applications V2V et V2I des réseaux véhiculaires. Cette architecture repose sur la technologie de communication sans fil connue sous le nom de DSRC.

1.4.1 Normes et standards

L'évolution des VANETs est attribuable aux avancées dans les systèmes de communication et les réseaux. L'IEEE (Institute of Electrical and Electronics Engineers) a élaboré une architecture de système connue sous le nom de WAVE pour offrir un accès sans fil dans les environnements véhiculaires. En octobre 1999, la Commission Fédérale des Communications aux États-Unis a réservé 75 MHz (5,85 - 5,925 GHz) dans la bande 5,9 GHz comme 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 initiatives similaires existent au Japon. En 2004, le groupe de travail TGP de l'IEEE 802.11 a commencé à élaborer un amendement de la norme 802.11 pour inclure les environnements véhiculaires, connu sous le nom IEEE 802.11p. 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 les environnements véhiculaires. Un autre groupe de travail de l'IEEE (groupe 1609) a travaillé sur le développement de spécifications pour couvrir des couches supplémentaires dans la suite de protocoles. L'ensemble des normes IEEE 1609, composé de quatre documents (IEEE 1609.1, IEEE 1609.2, IEEE 1609.3 et IEEE 1609.4), combiné aux normes IEEE 802.11p, est désigné sous le terme WAVE. Ces protocoles visent à définir l'architecture de communication, le partage de fréquences, la gestion des applications, les algorithmes de sécurité et la messagerie. La pile protocolaire de communication utilisant ces normes est présentée par rapport aux sept couches du modèle OSI. [10.11.12.13]

1.4.2 Protocoles de communication

L'architecture WAVE prend en charge deux piles de protocoles, comme illustré dans la figure 3 Par rapport au modèle OSI, les éléments suivants sont présents :

- IEEE 802.11p : Basée sur la norme IEEE 802.11, cette modification tient compte de l'environnement véhiculaire en spécifiant la transmission de données et les fonctions de gestion des couches physique (PLME) et MAC (MLME)[16].

- IEEE 1609.4 : Ajoute une sous-couche au niveau 2 pour contrôler le fonctionnement multicanal, permettant aux unités WAVE de partager leur temps entre le canal de contrôle et les services.

- IEEE 802.2 : Utilise l'ancien standard pour le contrôle de liaison logique (LLC)[14].

- IEEE 1609.3 : Prend en charge IPv6 et le protocole WAVE des messages courts (WSMP) pour les communications prioritaires et sensibles au temps, ainsi que la gestion réseau (WME)[14][15].

- IEEE 1609.1 : Décrit l'application de gestion des ressources WAVE pour l'interaction véhicule-infrastructure[14].

IEEE 1609.2 : Fournit les services de sécurité WAVE, couvrant le format des messages sécurisés, le chiffrement et l'authentification[14][15]. Le modèle DSRC/WAVE (Dedicated Short Range Communication/Wireless Access in Vehicular Environments), illustré dans la figure 3, permet l'accès à la technologie sans fil dans les environnements véhiculaires.

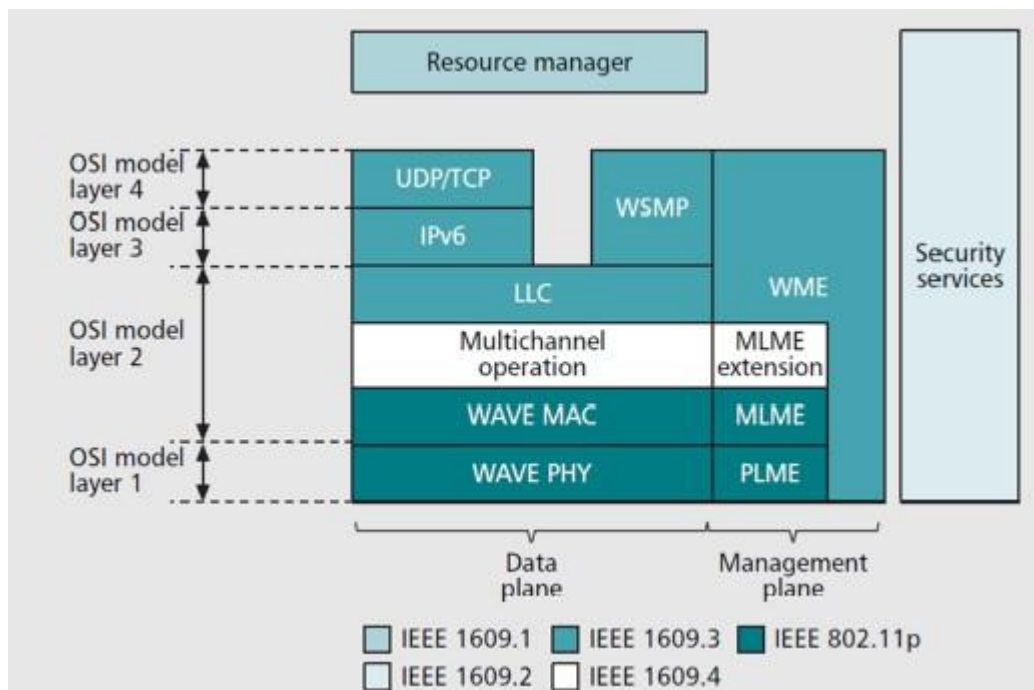


Figure 3. Le modèle WAVE/DSRC

1.5 les modes de communication

Un réseau VANET se compose principalement de véhicules et d'éléments fixes tels que les RSUs, et peut également inclure la connexion des piétons via leurs smartphones. En fonction des entités impliquées, différents modes de communication sont distingués : la communication inter-véhicules (V2V), la communication entre les véhicules et l'infrastructure (V2I), ainsi que la communication entre différents éléments de l'infrastructure (I2I).

1.5.1 Véhicule à Véhicule (V2V) dans les VANETs

Le mode de communication principal des VANETs est le Véhicule à Véhicule (V2V), qui permet aux véhicules d'échanger des informations de manière sans fil en utilisant des ondes radio. Cette communication V2V permet le partage d'informations telles que la position, la vitesse et la direction entre les véhicules, facilitant ainsi la connaissance de la topologie du réseau et des véhicules voisins. Grâce à ces échanges d'informations, les véhicules peuvent transmettre des messages pertinents sur les conditions de la route et les alertes de sécurité.

1.5.2 Véhicule à infrastructure

Le mode de communication appelé V2I (Vehicle to Infrastructure) ou communication entre les véhicules et l'infrastructure routière permet aux véhicules de communiquer avec les éléments fixes le long des routes, tels que les RSU. Cette communication sans fil permet aux véhicules de recevoir des informations sur les conditions de la route, les feux de signalisation, les panneaux de signalisation, les travaux routiers, et bien d'autres éléments essentiels à la sécurité et à la gestion du trafic.

1.5.3 Infrastructure à infrastructure

Le mode de communication appelé I2I (Infrastructure to Infrastructure) permet la communication entre les éléments fixes de l'infrastructure routière, tels que les feux de signalisation, les panneaux de signalisation, les caméras de surveillance et les stations de mesure. Cette communication entre les infrastructures utilise des connexions filaires ou en fibre optique, ce qui permet d'optimiser la circulation routière, de prévenir les accidents et d'améliorer la sécurité routière.

La figure (4) illustre les modes de communication dans le réseau véhiculaire VANET.

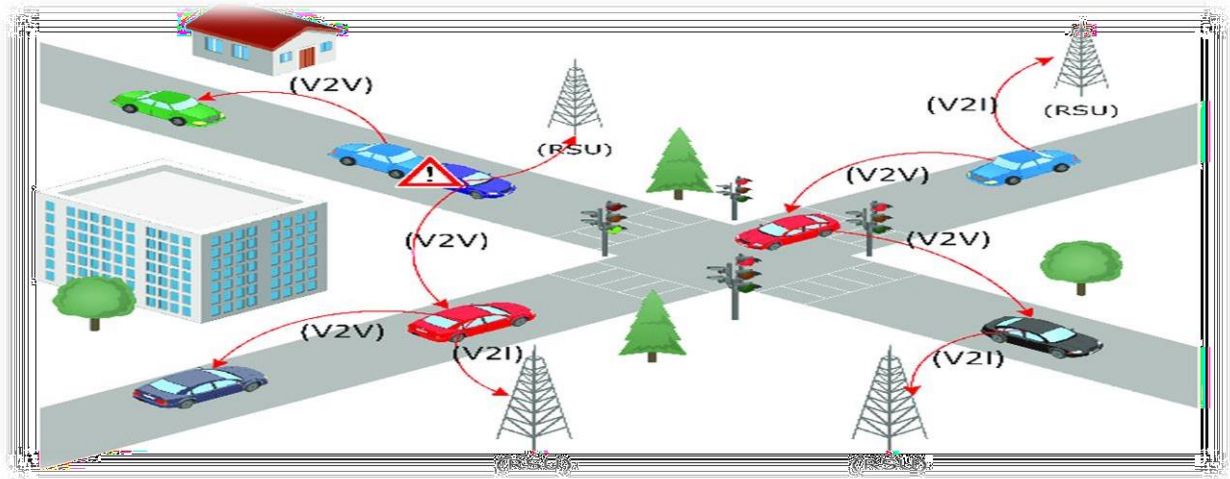


Figure 4: Modes de communication dans le réseau véhiculaire VANET

1.6 Architecture

Un réseau véhiculaire est un réseau ad-hoc sans fil qui se forme de manière autonome et spontanée. La Figure 4 illustre l'architecture d'un réseau véhiculaire. Selon cette architecture, les réseaux véhiculaires se composent de deux types de dispositifs : les unités embarquées (OBU) installées dans les véhicules et les unités de station de route (RSU) placées le long des routes. Les OBUs et les RSUs sont capables de communiquer via la communication véhicule à infrastructure ou infrastructure à véhicule (V2I). Une communication hybride peut également se produire lors d'une transmission distante ou multi-sauts, où différents nœuds (OBU ou RSU) peuvent participer au routage des messages.

1.7 Caractéristiques

Les réseaux véhiculaires ad hoc (VANETs) présentent des caractéristiques uniques qui les distinguent des réseaux ad hoc mobiles classiques (MANETs). Leurs principales spécificités sont :

— Topologie hautement dynamique

Les réseaux véhiculaires se caractérisent par une topologie extrêmement dynamique en raison de la grande vitesse de déplacement des véhicules, comparée à celle des piétons dans les réseaux mobiles ad hoc (MANETs)[1][2]. Cette mobilité intense entraîne des changements fréquents de topologie, ce qui pose un défi majeur pour le routage des paquets. Les véhicules se

déplacent à grande vitesse, ce qui rend la topologie du réseau très changeante, nécessitant ainsi des protocoles de routage adaptés pour gérer ces changements[1][2].

— **Modèle de mobilité**

Le modèle de mobilité dans les réseaux MANETs est souvent décrit comme un point de cheminement aléatoire, tandis que dans les réseaux véhiculaires, la mobilité des véhicules est déterminée par une multitude de facteurs, tels que les itinéraires empruntés, les feux de signalisation, les limitations de vitesse, les conditions de trafic et les comportements des conducteurs. Pour évaluer efficacement les protocoles de routage dans ces environnements, il est crucial d'utiliser des données de mouvement réalistes qui capturent ces dynamiques spécifiques.

— **Connectivité intermittente**

La forte mobilité des véhicules, notamment sur les autoroutes, entraîne une topologie de réseau très dynamique, provoquant une connectivité intermittente. Cette caractéristique constitue un défi majeur pour la conception d'applications nécessitant des délais de réponse courts, comme les applications multimédia. La gestion et l'automatisation des applications en périphérie du réseau sont compliquées par cette connectivité instable, rendant les mises à jour et la synchronisation des données plus difficiles. Les protocoles de routage dans les réseaux véhiculaires (VANETs) doivent résoudre le défi de la connectivité intermittente, qui rend les routes établies rapidement obsolètes. Cette dynamique topologique élevée nécessite des solutions de routage adaptées pour garantir une transmission fiable malgré les déconnexions fréquentes. En somme, la forte mobilité des véhicules crée un défi majeur pour le développement d'applications temps réel et la conception de protocoles de routage efficaces dans les VANETs, exigeant des solutions innovantes pour exploiter pleinement les avantages de ces réseaux. [17.18] .

— **Capacité de traitement et énergie**

Dans les réseaux véhiculaires (VANETs), la contrainte d'énergie et de capacité de stockage n'est pas aussi prégnante que dans les réseaux MANET et les réseaux de capteurs sans fil.

— **Service de localisation**

Les véhicules intelligents sont équipés de systèmes de positionnement GPS qui facilitent l'échange d'informations de localisation des véhicules, telles que leur position et leur

vitesse[19][20][21]. Cette fonctionnalité améliore les performances des applications liées à la sécurité routière et à la gestion du trafic en permettant de prendre de meilleures décisions de routage. Certaines applications nécessitent en effet la diffusion de messages dans une zone géographique spécifique ou en fonction des critères de mouvement ou de direction du véhicule destinataire.

— Scalabilité

La capacité de scalabilité des réseaux VANET permet une extension à grande échelle, couvrant par exemple l'ensemble d'une ville dans des applications urbaines. Les nœuds ont la capacité de se connecter et se déconnecter fréquemment du réseau, offrant ainsi une flexibilité importante dans la gestion des connexions.

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.

1.8.1 Messages périodiques (Beacons)

Chaque véhicule diffuse régulièrement des messages de sécurité (beacons) à ses voisins immédiats. Ces messages contiennent des informations sur l'état actuel du véhicule, comme sa position GPS, sa vitesse, sa direction et d'autres données. L'échange périodique de ces messages permet aux nœuds du réseau de s'identifier mutuellement, de découvrir leurs voisins et de maintenir une connaissance de l'état du trafic. Bien que nécessaires au fonctionnement du réseau, ces messages de routine peuvent aussi être exploités par des utilisateurs malveillants pour compromettre la sécurité des véhicules et du réseau.

1.8.2 Messages d'alerte

Ce type de messages est diffusé pour signaler des événements importants comme des accidents, des conditions routières dangereuses ou des embouteillages. Ils permettent de prévenir rapidement les véhicules à proximité afin d'améliorer la sécurité routière.

1.8.3 Messages d'usage général

En plus des messages de sécurité, les véhicules peuvent aussi échanger des données pour d'autres applications comme la navigation, les services aux conducteurs ou la maintenance

du véhicule. Ces messages non critiques utilisent la connectivité véhiculaire pour offrir des fonctionnalités avancées aux occupants.

1.9 Types d'applications VANET

I. Applications de sécurité

Les applications de sécurité dans les réseaux VANET visent à améliorer la sécurité routière en fournissant des informations en temps réel sur les conditions de circulation. Elles permettent de diffuser des données sur le trafic, les embouteillages et les accidents stockées dans les unités routières (RSU) pour les partager avec les véhicules à proximité. Les véhicules peuvent aussi échanger des messages coopératifs, comme des alertes de freinage d'urgence coordonné pour éviter les collisions. En cas d'accident, un véhicule peut diffuser des notifications post-collision aux autres véhicules à proximité et aux patrouilles routières pour accélérer les secours. Des alertes sur les conditions routières dangereuses, comme les glissements de terrain ou les virages serrés, peuvent aussi être envoyées. Les applications de sécurité comprennent également des systèmes d'alerte de collision qui avertissent deux véhicules sur une trajectoire de collision pour leur permettre de corriger leur trajectoire. Enfin, la surveillance du trafic via des caméras sur les RSU permet de détecter et de signaler les infractions routières[26].

II. Applications commerciales

Les applications commerciales dans les réseaux VANET proposent une variété de services et de divertissements aux conducteurs et passagers. Elles permettent par exemple de télécharger des réglages personnalisés et d'effectuer des diagnostics du véhicule à distance. Les RSU peuvent aussi servir de routeurs pour fournir un accès internet aux véhicules. Avant un trajet, il est possible de télécharger des cartes routières mises à jour. Les passagers peuvent également profiter de services de streaming vidéo en direct sur demande pendant le trajet. Enfin, des publicités ciblées peuvent être envoyées par des commerces à proximité aux véhicules qui passent à portée. Ces applications commerciales visent à rendre le temps passé sur la route plus agréable et productif pour les conducteurs et passagers.

III. Applications de confort

Les applications de confort dans les réseaux VANET visent à fluidifier la circulation et améliorer le confort de conduite des automobilistes. Elles permettent notamment de calculer

des itinéraires alternatifs en cas d'embouteillage pour éviter les ralentissements. Le péage électronique est aussi une fonctionnalité clé, permettant le paiement automatique des péages sans que le véhicule ne s'arrête. Les conducteurs peuvent également recevoir des informations en temps réel sur les places de parking disponibles à proximité, facilitant ainsi leur stationnement. Enfin, les applications de confort peuvent anticiper la topographie de la route à venir pour ajuster automatiquement la vitesse du véhicule et optimiser sa consommation de carburant. La sécurité est essentielle pour protéger ces échanges de données sensibles contre les accès non autorisés et garantir la disponibilité de ces applications en temps réel, cruciales pour le confort et la fluidité du trafic routier.

1.10 La sécurité dans les VANET

La sécurité est un enjeu crucial dans les réseaux véhiculaires (VANETs) en raison de leur nature et de leurs caractéristiques spécifiques. Des mécanismes de sécurité appropriés doivent être mis en place pour garantir que seuls les utilisateurs autorisés ont accès aux informations échangées et que les services fournis sont fiables et sûrs.

Les principaux défis de sécurité dans les VANETs incluent la protection de la vie privée des conducteurs, l'authentification des messages échangés, la détection des attaques et la garantie de la disponibilité du réseau. Des solutions de cryptographie, de signature numérique et de gestion des identités sont nécessaires pour relever ces défis.

1.10.1 Besoin de sécurité

La sécurité est un enjeu crucial dans les réseaux véhiculaires (VANETs) en raison de la nature dynamique de leur topologie, de la connectivité intermittente et de la sensibilité des informations échangées. Les défis de sécurité ne se limitent pas seulement à protéger les données et les services, mais peuvent aussi impacter directement la sécurité des conducteurs et passagers.

Un message d'alerte falsifié ou supprimé par un attaquant peut causer des accidents graves. De plus, l'exploitation des informations de localisation des véhicules par des utilisateurs malveillants compromet la vie privée des conducteurs et peut les mettre en danger.

Les communications sans fil dans les VANETs facilitent l'écoute des messages par des tiers non autorisés. Un attaquant peut ainsi suivre les déplacements d'un véhicule sur une période donnée en analysant les messages échangés.

1.10.2 Exigences de sécurité

Les exigences de sécurité dans les réseaux véhiculaires (VANETs) découlent des principaux objectifs de sécurité que sont la confidentialité, l'intégrité et la disponibilité. Elles peuvent être résumées comme suit:

a) Authentification

Les messages échangés doivent être authentifiés pour s'assurer qu'ils proviennent de sources légitimes et non d'attaquants. Des mécanismes cryptographiques comme les signatures numériques permettent de vérifier l'origine des messages.

b) Intégrité et cohérence

L'intégrité des données transmises doit être préservée, sans altération par des tiers malveillants. Les messages doivent arriver intacts et cohérents à leur destination.

c) Confidentialité

Les informations sensibles comme la localisation des véhicules ne doivent pas être accessibles à des entités non autorisées. Le chiffrement des communications protège la confidentialité des données.

d) Disponibilité

Le réseau et les services doivent rester disponibles en permanence, même face à des attaques visant à les perturber. Une conception robuste et redondante du réseau assure cette disponibilité.

e) Contrôle d'accès

Seuls les utilisateurs et véhicules autorisés doivent pouvoir accéder aux ressources du réseau. Des mécanismes de contrôle d'accès basés sur les rôles permettent de gérer finement les privilèges.

f) Non-répudiation

La non-répudiation est une exigence cruciale dans les VANETs, car un véhicule ne doit pas pouvoir nier avoir transmis un message, surtout si celui-ci a causé un accident ou une fausse alerte[33][34]. Pour garantir la non-répudiation, les nœuds doivent être identifiés de manière fiable et la traçabilité des messages doit être possible pour aider les enquêtes en cas d'incident.

Des mécanismes cryptographiques comme les signatures numériques permettent d'authentifier l'origine des messages et d'empêcher la répudiation[33][35].

g) Vie privée

La vie privée des usagers est une exigence essentielle pour le déploiement réussi des VANETs et pour convaincre les gens d'adopter cette technologie. Dans un réseau ouvert comme les VANETs, les véhicules diffusent régulièrement des messages contenant des informations sensibles comme leur position, vitesse ou identifiant. Un attaquant peut facilement collecter ces données et suivre les déplacements des véhicules. Pour préserver la vie privée, les véhicules doivent pouvoir communiquer de manière anonyme, sans révéler leur identité réelle. L'utilisation de pseudonymes changeants régulièrement empêche tout suivi illégal des véhicules.

1.10.3 Nature d'attaquant

Les VANET sont sensibles aux attaques, rendant difficile la détection des véhicules suspects. Un réseau VANET peut être compromis par un attaquant qui manipule les systèmes des véhicules ou les protocoles de sécurité. En général, l'attaquant cherche à perturber le réseau pour ses propres intérêts ou à violer la vie privée d'un véhicule spécifique. Les attaquants sont généralement classés en quatre catégories..

1. Les attaquants internes et externes

Les attaquants internes dans les réseaux véhiculaires sont des utilisateurs légitimes authentifiés, tandis que les attaquants externes ne possèdent pas d'authentification. En comparaison, les attaquants externes ont une capacité d'attaque limitée par rapport aux attaquants internes. la **figure (5)** donne une illustration sur les attaquants internes et externes .

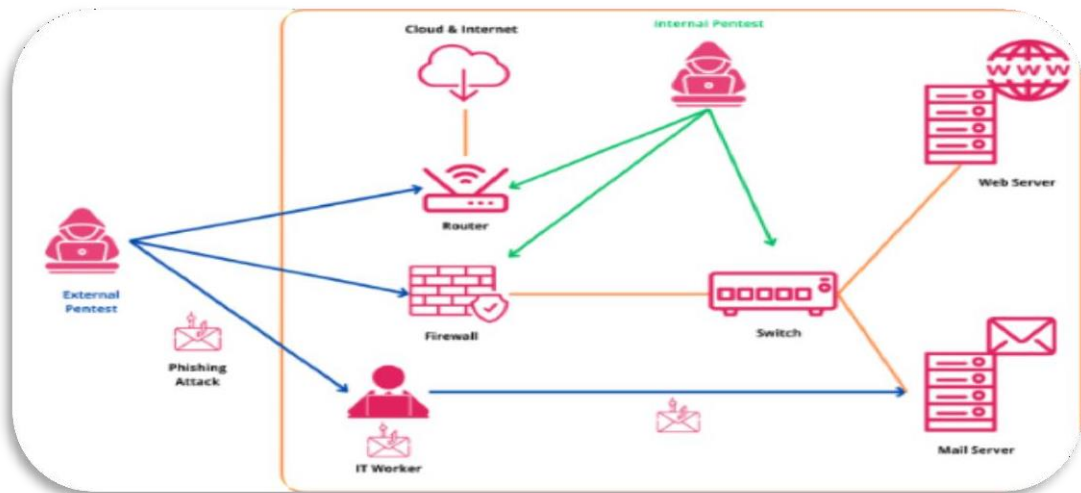


Figure 5: Les attaquants internes et externes

2. Les attaquants malicieux et les attaquants rationnels

cherchent à perturber le fonctionnement du réseau sans intérêt personnel, employant tous les moyens possibles. En revanche, les attaquants rationnels ont des objectifs de gain propres, ce qui permet de mieux prévoir leurs cibles et moyens.

3. Les attaquants passifs et actifs

Ecoutent et interceptent les messages échangés sans les modifier, dans le but de déterminer les parties communicantes et le contenu. Tandis que les attaquants actifs agissent sur les informations transmises en les falsifiant, modifiant ou détruisant.

Dans la **figure (6)**, l'attaquant A écoute seulement les messages échangés entre X et Y.

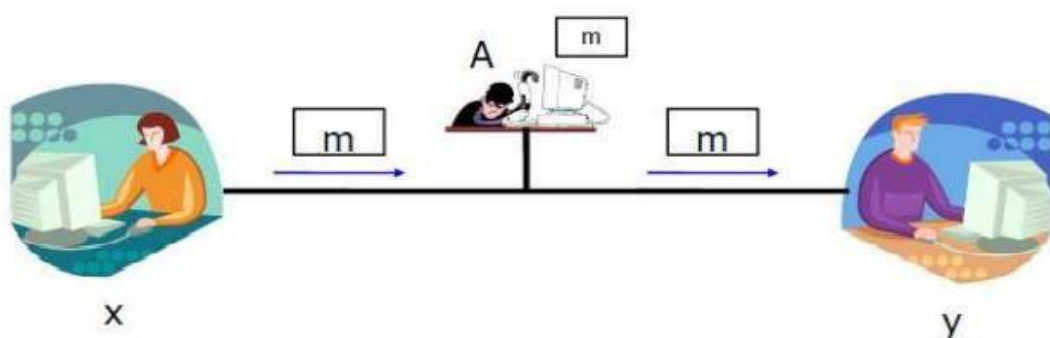


Figure 6: Attaque passive

1.10.4 Types d'attaques

Les transmissions périodiques dans un environnement ouvert posent un risque majeur de perturbation du système de communication lorsqu'un attaquant intervient pour intercepter, altérer ou même générer des messages dans le réseau. Ces défis exposent les VANETs à une gamme variée d'attaques non désirées. Parmi les menaces de sécurité les plus préoccupantes, on peut citer :

— Les attaques sur la vie privée

Les attaques sur la vie privée dans les réseaux véhiculaires représentent un risque majeur. Un attaquant peut collecter des données pour identifier précisément l'origine d'un nœud, ainsi que les actions et déplacements d'un conducteur. Cette vulnérabilité provient de l'échange d'informations sensibles lors de la communication, en particulier dans les messages de sécurité et de contrôle. En effet, un véhicule est censé envoyer des messages identifiés contenant des données sur sa localisation, sa vitesse et parfois même des détails de voyage. Cette collecte de données par un attaquant peut gravement compromettre la vie privée des conducteurs.

— Attaque sur la cohérence

Un attaquant a la capacité de compromettre l'intégrité des messages en les altérant ou en insérant de fausses informations. Cette manipulation peut perturber la perception de la réalité par les destinataires et les orienter dans une direction erronée. De plus, l'attaquant peut créer des perturbations dans le trafic en déviant tous les véhicules vers une route déjà congestionnée, entraînant ainsi des problèmes supplémentaires.

— Usurpation d'identité

L'usurpation d'identité est une attaque extrêmement dangereuse dans les réseaux véhiculaires. L'attaquant utilise de faux identifiants pour se faire passer pour une entité légitime, lui permettant ainsi d'abuser de tous les privilèges associés à cette identité. Lorsque l'attaquant envoie des messages frauduleux ou perturbe le système en se faisant passer pour un véhicule autorisé, il devient très difficile de le détecter et de l'identifier comme une menace. Cette attaque est particulièrement insidieuse car elle exploite la confiance du réseau envers les identités connues pour injecter des informations malveillantes sans éveiller les soupçons. Les conséquences peuvent être désastreuses si un attaquant parvient à usurper l'identité d'un véhicule de sécurité ou d'urgence par exemple. C'est pourquoi la détection et la prévention de

ce type d'attaque sont essentielles pour garantir l'intégrité et la fiabilité des communications dans les VANETs.

— **Déni de service (Dos)**

Le déni de service (DoS) est une attaque largement reconnue, même dans les réseaux traditionnels. L'objectif de l'attaquant est de saturer le réseau en envoyant une quantité excessive de messages inutiles pour surcharger le canal de communication, ce qui peut ralentir ou même bloquer la diffusion des messages d'alerte ou de contrôle.

— **L'Écoute**

est une forme d'attaque où l'adversaire possède des capacités d'écoute sur le canal de communication et peut extraire des informations pertinentes pour son profit. Le grand défi de cette attaque est que l'attaquant peut rester passif, ce qui rend difficile sa détection. Ce type d'attaque peut également initier une atteinte à la vie privée des conducteurs, en collectant des informations sur leurs déplacements et leurs habitudes.

1.11 Protection de la vie privée dans les VANETs

La protection de la confidentialité de l'emplacement dans les VANETs vise à sécuriser les véhicules contre les tentatives d'attaques visant à suivre leur localisation. Cette vulnérabilité découle de la relation entre l'identité du véhicule et son emplacement. Chaque véhicule dans un VANET envoie régulièrement un message de sécurité contenant des données cruciales telles que sa vitesse, sa position et son identité, étroitement liées au conducteur. Ces informations sont essentielles pour le bon fonctionnement des applications véhiculaires, comme la prévention des collisions, les alertes d'accidents, les services d'urgence et la navigation. L'enjeu majeur consiste à préserver la confidentialité en évitant toute corrélation entre l'identifiant du véhicule, son comportement, sa localisation et ses caractéristiques spécifiques. Ainsi, il est impératif de dissocier l'identité du véhicule de sa localisation pour garantir sa protection contre toute forme de surveillance ou de compromission de la vie privée.

1.11.1 La préservation de la vie privée

Pour qu'un écosystème VANET soit efficace, un défi majeur est de trouver un équilibre entre une sécurité renforcée et une protection de la vie privée des conducteurs. Si cet équilibre n'est pas assuré, le système devient vulnérable et inefficace, le rendant inutilisable[35].

Une présentation non exhaustive des domaines de recherche en sécurité des VANETs a été proposée par Raya et Hubaux. Les quatre principaux aspects sont : la gestion des identités et l'authentification des messages, la protection de la vie privée, l'intégrité des données et la sécurité embarquée. **La figure(7)** montre les relations entre ces domaines et l'importance de préserver la vie privée au sein des VANETs.

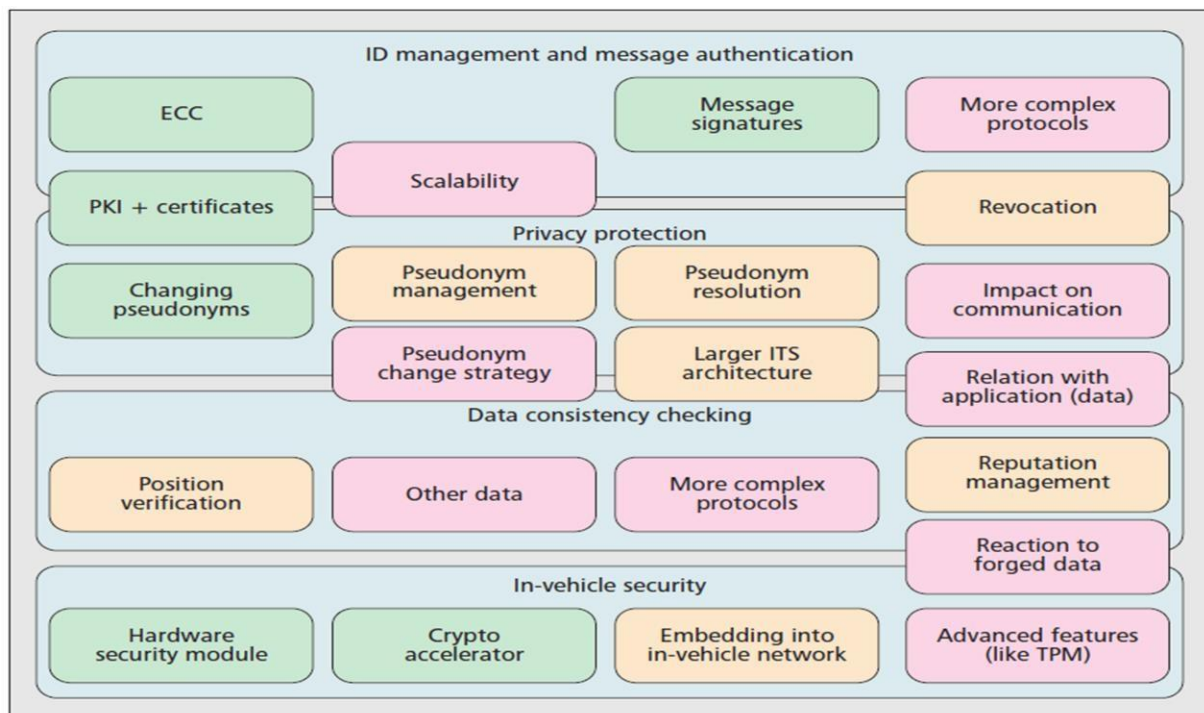


Figure 7: Sujets de recherche

1.11.2 Exigences de la vie privée

1. La divulgation minimale

La divulgation minimale est un principe clé pour protéger la vie privée dans les systèmes de communication véhiculaire. Il consiste à ne divulguer que les informations strictement nécessaires et pertinentes pour le bon fonctionnement du réseau, sans révéler de détails superflus. En limitant la quantité d'informations partagées, on réduit les risques d'atteinte à la vie privée des utilisateurs.

2. L'anonymat

L'anonymat dans les réseaux véhiculaires est crucial pour protéger la vie privée des conducteurs en cachant leur identité aux attaquants. Cependant, cette exigence entre en conflit avec la responsabilité des utilisateurs envers leurs actions sur la route. Trouver un équilibre délicat est essentiel : les véhicules doivent pouvoir préserver leur anonymat pour la confidentialité, tout en permettant son levée lorsque le comportement d'un véhicule le justifie pour assurer sa responsabilité. Cette gestion complexe nécessite des solutions techniques avancées et des cadres juridiques clairs pour garantir à la fois la protection de la vie privée et la sécurité routière dans les réseaux véhiculaires.

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.

1.12 Conclusion

Ce chapitre nous a permis de présenter plus ou moins en détail les réseaux véhiculaires (VANET), en décrivant leur architecture, leurs caractéristiques spécifiques, leurs différents domaines d'application ainsi que les problématiques cruciales liées à leur sécurité.

L'objectif principal des VANET est de faciliter la conduite et d'améliorer le confort et l'expérience des conducteurs et des passagers sur les routes. Cependant, ces réseaux sont vulnérables à diverses attaques menaçant la vie privée des utilisateurs et pouvant entraîner des perturbations du trafic routier.

Il est donc primordial de mettre en œuvre des protocoles et des mécanismes de sécurité robustes afin de contrôler les entités du réseau, de préserver la sécurité des conducteurs et de permettre aux utilisateurs d'adopter cette technologie en toute confiance.

CHAPITRE 2 :

Etat de l'art

CHAPITRE 2

Etat de l'art

2.1 Introduction

La sécurité est cruciale pour assurer un fonctionnement fiable et sûr de tout système. La préservation de la confidentialité de localisation est l'un des principaux défis de sécurité dans les réseaux véhiculaires ad hoc (VANETs). L'objectif est d'empêcher un attaquant potentiel de pouvoir suivre un véhicule spécifique.

Dans ce chapitre, nous allons présenter quelques stratégies proposées pour préserver la vie privée dans les réseaux VANETs. Ensuite, nous exposerons notre proposition de changement de pseudo-identité visant à garantir la confidentialité de localisation dans un réseau véhiculaire.

2.2 Changement de pseudonyme

Dans le domaine de la sécurité des réseaux de véhicules, l'utilisation de pseudo-identités est une pratique courante pour protéger la confidentialité des données et la vie privée des utilisateurs. Les pseudo-identités sont des identités fictives attribuées aux véhicules, qui sont utilisées à la place de leurs identités réelles. Les schémas de changement de pseudo-identité reposent sur le principe de modifier régulièrement ces identités fictives pour renforcer l'anonymat des véhicules.

Comme évoqué précédemment, le suivi des véhicules constitue un problème majeur en matière de sécurité, car il peut compromettre la confidentialité des données et violer la vie privée des utilisateurs du réseau. Dans ce chapitre, nous examinons différentes stratégies qui reposent sur le changement des pseudo-identités, et qui ont été proposées pour garantir un niveau élevé d'anonymat.

Ces stratégies visent à perturber la corrélation entre les mouvements des véhicules et leurs identités réelles en changeant régulièrement les pseudo-identités. En effet, en altérant fréquemment ces identités fictives, il devient plus difficile pour les observateurs malveillants de suivre et de tracer les activités des véhicules jusqu'à leurs propriétaires réels. Cette approche offre ainsi une couche supplémentaire de protection de la vie privée des utilisateurs et limite les risques de surveillance indésirable ou de traçage non autorisé dans les réseaux de véhicules.

2.3 Stratégies

2.3.1 Pseudonymes

La méthode pseudonyme est une stratégie de protection de la vie privée utilisée dans les réseaux VANET (Vehicular Ad Hoc Networks) pour préserver l'anonymat des véhicules tout en permettant une communication efficace. Voici les principes de base de la méthode pseudonyme dans les VANET :

1. Rotation des identifiants

Les véhicules utilisent périodiquement différents identifiants pseudonymes lors de leurs communications. Cela signifie qu'un véhicule n'utilise pas le même identifiant en permanence, ce qui rend plus difficile pour les observateurs de suivre ou de tracer les mouvements d'un véhicule spécifique.

2. Attribution aléatoire d'identifiants

L'attribution des identifiants pseudonymes est effectuée de manière aléatoire, ce qui rend difficile pour les observateurs de prédire quel identifiant un véhicule utilisera ensuite. Cela contribue à augmenter l'anonymat des véhicules dans le réseau.

3. Gestion centralisée ou décentralisée des identifiants

Les identifiants pseudonymes peuvent être gérés de manière centralisée par une autorité de certification ou de manière décentralisée par les propres véhicules. Dans les systèmes décentralisés, les véhicules peuvent générer leurs propres identifiants de manière autonome.

4. Révocation d'identifiants compromis

En cas de compromission d'un identifiant pseudonyme (par exemple, en cas d'attaque ou de violation de la sécurité), des mécanismes peuvent être mis en place pour révoquer cet identifiant et en attribuer un nouveau au véhicule concerné.

5. Compatibilité avec les exigences de sécurité

La méthode pseudonyme doit être conçue de manière à ne pas compromettre la sécurité des communications dans le réseau. Cela implique de garantir que les identifiants pseudonymes ne peuvent pas être utilisés pour mener des attaques ou compromettre l'intégrité des données échangées. La **figure(8)** présente une Taxonomie des stratégies de changement des pseudonymes.

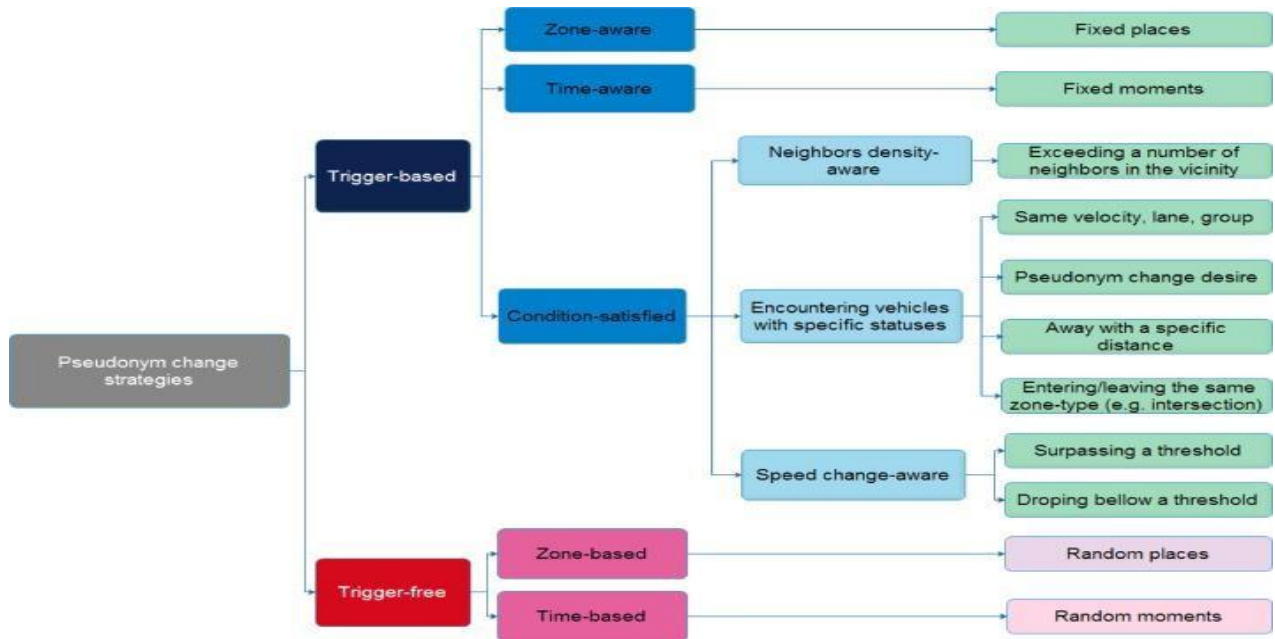


Figure 8: Taxonomie des stratégies de changement des pseudonymes

2.3.2 la Perturbation

La méthode de perturbation dans les réseaux VANET est une approche utilisée pour améliorer la sécurité et la confidentialité des communications entre les véhicules et les infrastructures routières. Voici les principes fondamentaux de la méthode de perturbation dans les VANET :

1. Intentionnalité de la perturbation

La perturbation des communications est réalisée de manière intentionnelle pour rendre plus difficile l'interception ou la manipulation des messages échangés entre les véhicules. Cette perturbation peut prendre différentes formes, telles que l'ajout de bruit aux transmissions ou l'altération des données.

2. Contrôle de la perturbation

La méthode de perturbation implique un contrôle précis sur la manière dont les communications sont perturbées. Cela peut inclure la modulation de la puissance du signal, l'introduction de retards aléatoires dans les transmissions ou la manipulation des caractéristiques du signal pour rendre la détection et l'interception plus difficiles.

3. Minimisation des effets sur la communication

Bien que la perturbation soit utilisée pour renforcer la sécurité et la confidentialité, il est essentiel de minimiser ses effets sur la qualité et la fiabilité des communications dans le réseau.

Cela nécessite une conception soignée des mécanismes de perturbation pour garantir que les performances du réseau ne sont pas compromises de manière significative.

4. Adaptabilité aux conditions du réseau

La méthode de perturbation doit être adaptable aux conditions changeantes du réseau, telles que la densité du trafic, la mobilité des véhicules et les variations de la qualité du lien. Cela peut nécessiter des algorithmes dynamiques qui ajustent les paramètres de perturbation en fonction de l'environnement du réseau.

5. Équilibre entre sécurité et performance

L'objectif principal de la méthode de perturbation est d'améliorer la sécurité des communications dans les VANET, mais il est également important de maintenir des performances globales acceptables du réseau. Cela nécessite un équilibre entre les mesures de sécurité mises en œuvre et l'impact sur la performance du système.

2.3.3 Cryptographie

La méthode de cryptographie dans les réseaux VANET (Vehicular Ad Hoc Networks) vise à sécuriser les communications entre les véhicules et les infrastructures routières en utilisant des techniques de chiffrement et d'authentification. Voici les principes fondamentaux de la méthode de cryptographie dans les VANET :

1. Chiffrement des données

Les données échangées entre les véhicules et les infrastructures routières sont chiffrées pour garantir leur confidentialité. Le chiffrement rend les données illisibles pour toute personne non autorisée qui intercepterait les transmissions.

2. Utilisation de clés de chiffrement

Un système de clés est utilisé pour chiffrer et déchiffrer les données. Les véhicules et les infrastructures routières disposent de clés de chiffrement partagées ou publiques pour sécuriser leurs communications.

3. Authentification des entités

La cryptographie est utilisée pour garantir l'authenticité des entités participant aux communications. Cela implique souvent l'utilisation de certificats numériques et de signatures numériques pour vérifier l'identité des véhicules et des infrastructures routières.

4. Protection contre les attaques

La cryptographie est utilisée pour protéger les communications contre diverses attaques, telles que l'usurpation d'identité, la falsification de messages et les attaques par rejeu. Des mécanismes de vérification d'intégrité et d'authenticité sont utilisés pour détecter et prévenir ces types d'attaques.

5. Gestion sécurisée des clés

La gestion des clés de chiffrement est essentielle pour garantir la sécurité des communications. Des protocoles sécurisés sont utilisés pour distribuer et gérer les clés de manière efficace, en minimisant les risques d'exposition ou de compromission des clés.

6. Compatibilité avec les performances du réseau

Les algorithmes de chiffrement et d'authentification doivent être conçus pour fonctionner de manière efficace dans un environnement VANET, en tenant compte des contraintes de ressources telles que la bande passante, la puissance de calcul et la latence.

2.4 Les avantages / inconvénient de chaque méthode

1. Les pseudonymes

- Avantages

- Protège la vie privée des utilisateurs en rendant difficile le suivi des véhicules.
- Permet aux utilisateurs de communiquer de manière anonyme sans révéler leur identité réelle.

- Inconvénients

- Peut compliquer la gestion de la sécurité, en particulier lorsqu'il est nécessaire d'identifier les véhicules impliqués dans des incidents ou des violations.
- La rotation fréquente des identifiants peut entraîner une surcharge du réseau et des problèmes de cohérence des données.

2. La perturbation

- Avantages

- Améliore la sécurité en rendant plus difficile l'interception et la manipulation des données.
- Peut dissuader les attaquants en compliquant l'analyse des communications.

- Inconvénients

- Peut affecter négativement la qualité des communications en introduisant du bruit ou des retards.
- La perturbation excessive peut entraîner une dégradation des performances du réseau.

3. Cryptographie

- Avantages

- Assure la confidentialité des données en les chiffrant, garantissant que seuls les destinataires légitimes peuvent les déchiffrer.
- Fournit un mécanisme d'authentification robuste pour vérifier l'identité des entités dans le réseau.

- Inconvénients

- Peut ajouter une surcharge de traitement et de bande passante au réseau en raison des opérations de chiffrement et de déchiffrement.
- La gestion des clés peut être complexe et sujette aux attaques si elle n'est pas correctement sécurisée.

2.5 Les pseudonymes et les certificats

jouent un rôle crucial dans l'authentification des véhicules dans les réseaux véhiculaires, tout en préservant la confidentialité des utilisateurs. Cependant, l'utilisation d'un pseudonyme unique pour chaque véhicule peut ne pas suffire à garantir la confidentialité, car les attaquants peuvent corréler les traces de localisation et identifier les véhicules.

Pour résoudre ce problème, différentes stratégies de changement de pseudonymes ont été proposées dans la littérature. Chaque véhicule enregistré reçoit un ensemble de pseudonymes certifiés par une autorité de confiance, ainsi qu'une clé privée correspondant à chaque certificat. Le véhicule choisit un pseudonyme de son ensemble pour signer ses messages, au lieu d'utiliser son identité réelle. Seule l'autorité de confiance peut faire le lien entre le pseudonyme utilisé par un véhicule et son identité réelle.

Il est essentiel de changer de pseudonyme de manière stratégique pour éviter toute corrélation par un attaquant. Les schémas proposés dans la littérature visent à déterminer le moment et le lieu idéaux pour effectuer ce changement en toute sécurité. Ces schémas prennent en compte divers facteurs, tels que la densité du trafic, la couverture des infrastructures routières et les schémas de déplacement des véhicules, pour garantir que le changement de pseudonyme ne compromette pas la confidentialité des utilisateurs.

2.6 Schémas proposés dans la littérature

D'après les sources fournies, les schémas proposés dans la littérature pour le changement des pseudonymes des véhicules ont suscité un intérêt considérable parmi les chercheurs. Une récente étude a présenté une classification des schémas existants, mettant en lumière différentes approches pour garantir un changement de pseudonymes fiable, efficace et sécurisé. Cette classification explore des schémas basés sur la confiance, impliquant une autorité centrale pour gérer les pseudonymes, ainsi que des schémas distribués où les véhicules changent de pseudonymes de manière autonome. Ces derniers incluent des approches basées sur la proximité géographique, le temps, et des schémas hybrides combinant ces aspects pour assurer un anonymat adéquat. **La figure (9)** illustre cette classification.

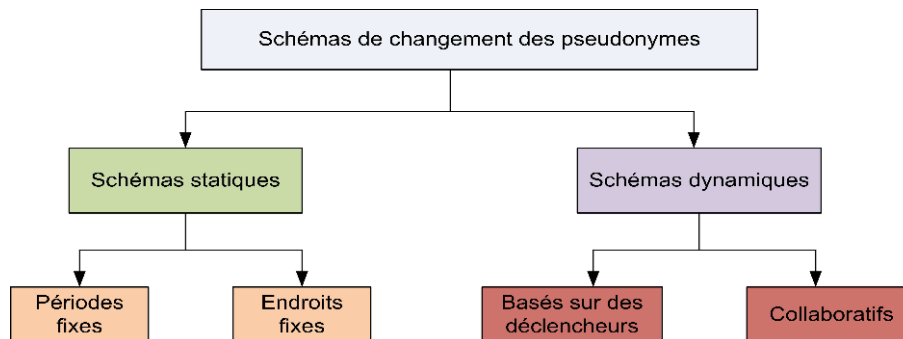


Figure 9: Stratégies de changement des pseudonymes

2.6.1 Schémas statiques

Les schémas statiques pour le changement de pseudonymes des véhicules reposent sur la prédétermination des moments ou des lieux de changement de pseudonymes. Cette approche structurée peut cependant entraîner une certaine prévisibilité dans les changements de pseudonymes, ce qui peut être considéré comme une information supplémentaire potentiellement exploitable par un attaquant.

a) Endroits fixes

Les travaux de recherche sur les schémas de changement de pseudonymes dans des endroits fixes, appelés "Mix-Zones", ont exploré diverses approches. X. Deng et al. ont proposé le protocole PCP, où les véhicules changent de pseudonyme uniquement dans la région d'une station de base, nécessitant une infrastructure coûteuse. A. Wahid et al. ont développé le schéma CPS, où les véhicules envoient moins fréquemment des balises pour garantir l'anonymat, mais ce schéma suppose des conditions peu réalistes. La stratégie CCAPS combine les schémas CAPS et CPN, définissant trois régions autour du véhicule pour le changement de pseudonyme, mais elle repose sur des périodes de silence pouvant poser des problèmes pour les systèmes de transport intelligents.

b) Périodes fixes

Les schémas de changement de pseudonymes à périodes fixes, comme le PPC (Periodical Pseudonym Change), consistent à utiliser chaque pseudonyme pendant une période spécifiée, en changeant à intervalles de temps fixes ou aléatoires. Cependant, ce changement régulier permet à un attaquant de prévoir le prochain changement, rendant ces schémas vulnérables aux attaques de liaison entre pseudonymes consécutifs d'un même véhicule.

Pour contrer ces attaques, des mécanismes comme le RSP (Random Silent Period) ont été proposés. Ils introduisent une période de silence composée d'une partie constante, pour brouiller la relation spatiale entre les positions avant et après le changement, et d'une partie variable, pour mélanger la relation temporelle entre les temps de disparition et réapparition du véhicule.

Une extension du RSP, appelée CARAVAN, Le véhicule entre dans une période de silence aléatoire, et si deux véhicules A et B entrent en silence en même temps et changent de pseudonyme pendant cette période, un attaquant ne peut plus corréler leurs pseudonymes.

2.6.2 Schémas dynamiques

Les schémas dynamiques pour le changement de pseudonymes des véhicules se distinguent des schémas statiques en tenant compte de l'environnement du véhicule pour effectuer ce changement. Cet environnement inclut des facteurs tels que le nombre de voisins du véhicule, le comportement de ces voisins, et d'autres paramètres contextuels. Cette approche dynamique vise à ajuster le changement de pseudonymes en fonction des conditions en temps réel, offrant ainsi une meilleure adaptation aux variations de l'environnement du véhicule.

En intégrant des éléments dynamiques tels que les interactions avec les voisins et les conditions environnementales changeantes, les schémas dynamiques visent à renforcer la sécurité et la confidentialité des communications dans les réseaux véhiculaires. Cette approche permet une adaptation plus fine et réactive aux situations en constante évolution, offrant ainsi une protection plus robuste contre les attaques potentielles.

A. Collaboratifs

L'objectif est de préserver l'anonymat des véhicules en coordonnant les changements de pseudonymes entre véhicules voisins selon leur contexte.

Un premier schéma propose un échange de pseudonymes entre deux véhicules via une unité sur route (RSU) qui fait la liaison avec l'autorité de certification. Cependant, cela implique une dépendance fréquente aux RSU à cause de la mobilité des véhicules.

Le schéma CAPS fait entrer les véhicules en mode silence et changer de pseudonyme lorsque leur état est confondu avec un voisin silencieux. Mais ces périodes de silence posent un risque pour la sécurité routière.

Dans le schéma CPN , les véhicules changent simultanément de pseudonymes lorsqu'un nombre seuil de voisins est atteint. Cela rend la traçabilité plus difficile mais peut gaspiller des pseudonymes inutilement.

Le schéma CATA déclenche des changements synchronisés dans une région donnée selon le contexte de trafic décidé par les RSU.

L'approche SRPS réduit les périodes de silence en les interrompant en cas d'urgence détectée par un algorithme de suivi multi-cibles (MTT).

Enfin, RIPS permet un échange direct de pseudonymes entre véhicules voisins sans passer par les RSU. Chaque véhicule dispose d'un ensemble de pseudonymes échangeables et d'un pseudonyme fixe pour l'authentification.

B. Déclencheurs

SLOW : Les véhicules entrent en mode silence et changent de pseudonyme lorsque leur vitesse passe en dessous d'un certain seuil (ex : zones 30 km/h, feux rouges, embouteillages). Limites : changements inutiles si seul, conflits avec les messages de sécurité pendant les silences.

Schéma de détection du trafic : Un véhicule "initiateur" détecte le ralentissement du trafic et déclenche une zone de silence où les véhicules à proximité changeront de pseudonyme. L'initiateur change ensuite.

VLPZs (Vehicular Location Privacy Zones) : Le réseau routier est divisé en zones gérées par des RSUs. Lorsqu'un véhicule entre dans une zone, il peut changer de pseudonyme de manière sécurisée, sans perturber les messages de sécurité.

ENeP-AB : Les véhicules réduisent la portée de leur signal et changent de pseudonyme selon l'estimation du nombre et de la position des véhicules voisins, pour brouiller les pistes.

2.7 Conclusion

L'utilisation de pseudonymes dans les réseaux véhiculaires ad hoc (VANET) est cruciale pour assurer la confidentialité et la protection de la vie privée des utilisateurs. Dans un environnement où les véhicules communiquent constamment des informations sensibles telles que leur position, leur vitesse et leur identité, l'emploi de pseudonymes permet de préserver l'anonymat des conducteurs et des passagers.

En utilisant des identités temporaires et régulièrement modifiées, les pseudonymes empêchent la création de profils détaillés des trajectoires et des habitudes de conduite des utilisateurs. Cela réduit considérablement les risques d'atteintes à la vie privée et de suivis non autorisés par des tiers malveillants.

De plus, les pseudonymes renforcent la sécurité globale du réseau VANET en prévenant les attaques d'usurpation d'identité et en rendant plus difficile le traçage et le pistage des véhicules. Cette protection est essentielle pour garantir la confiance des utilisateurs dans le système et favoriser une adoption généralisée des technologies VANET.

Cependant, l'équilibre entre la confidentialité offerte par les pseudonymes et la nécessité de traçabilité en cas d'incidents ou d'urgences reste un défi à relever. Des mécanismes de gestion des pseudonymes, tels que l'utilisation d'autorités de confiance, sont nécessaires pour permettre une révocation contrôlée des identités tout en préservant la vie privée des utilisateurs légitimes.

CHAPITRE 03 : CONTRIBUTION

CHAPITRE 03

CONTRIBUTION

3.1 Introduction

Dans les réseaux véhiculaires ad hoc (VANET), deux concepts cruciaux sont le CAPS (Context-Aware Privacy Scheme) et le CPN (Cooperative Pseudonym change scheme based on the number of Neighbors). Le CAPS utilise les échanges de messages entre les véhicules et les infrastructures routières pour estimer leur position, offrant ainsi une alternative résiliente et moins dépendante des signaux GPS. De son côté, le CPN repose sur une approche de contention où les véhicules compétitionnent pour l'accès au canal de communication en fonction de leur positionnement relatif, ce qui garantit une localisation précise même dans des environnements dynamiques. Ces deux approches complémentaires jouent un rôle essentiel dans le développement de systèmes de transport intelligents et sécurisés, permettant une communication efficace et une localisation fiable des véhicules dans les réseaux VANET.

3.2 Modèle adversaire et capacité

Le suivi d'emplacement des véhicules est l'objectif principale d'un adversaire, Bien que les véhicules changent leur pseudonymes pendant un trajet mais l'adversaire peut contourner ce mécanisme de confidentialité en écoutant les messages de contrôle, collectant les données incluses.

Supposons que l'adversaire connaît l'adresse d'un propriétaire, il commence à le suivre dès son départ de domicile ou de travail. Même si le véhicule change de pseudonyme, l'adversaire peut facilement identifier le nouveau pseudonyme utilisé. Cela met en danger la vie privée de la personne ciblée.

Pour mesurer les performances du schéma de confidentialité, un modèle d'adversaire très puissant est utilisé, incluant un attaquant global qui couvre l'ensemble du réseau avec des unités d'écoute sans fil. 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. Le modèle de menace se compose de :

A. Capteurs d'écoute

Des récepteurs sans fil, simulés par des modules RSU, écoutent le support sans fil et envoient les messages capturés à un serveur central pour traitement.

B. Couverture complète du réseau routier

L'attaquant déploie plusieurs récepteurs couvrant la totalité du réseau routier. La couverture complète permet de collecter, traiter et analyser les messages de sécurité reçus pour suivre le véhicule cible durant ses déplacements.

C. Serveur central de suivi

Une entité centrale appelée "Vehicle Tracker" collecte les messages de balise reçus par les capteurs pour suivre la cible en utilisant l'algorithme NNPD (Nearest-Neighbor Probabilistic Data Association) pour l'association et la liaison des messages. **La Figure(10)** donne une illustration sur le modèle d'adversaire.

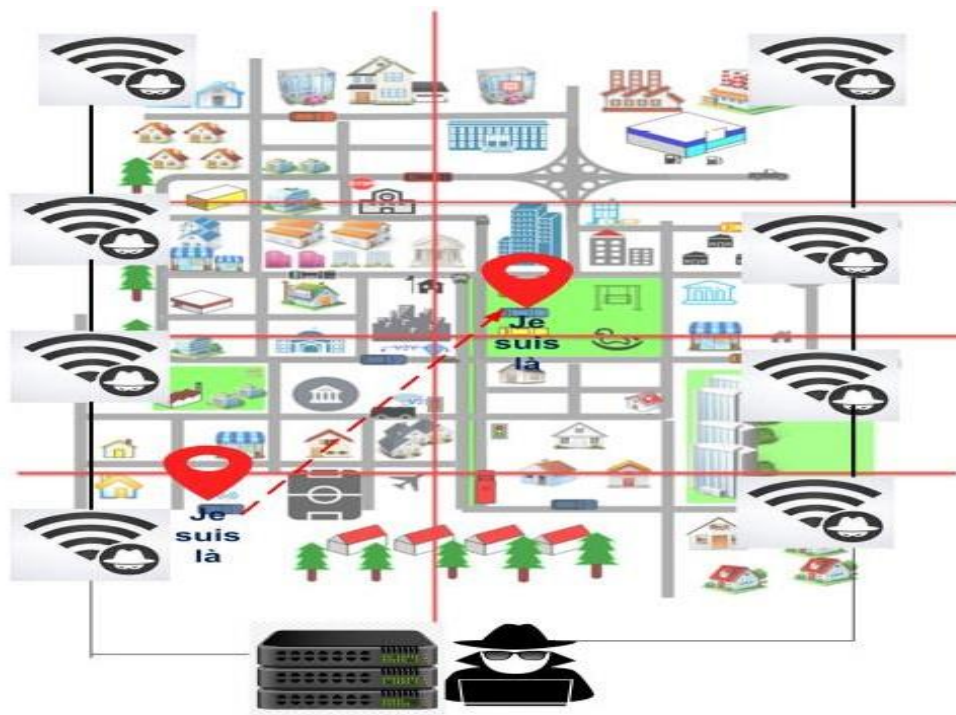


Figure 10: Modèle d'adversaire

3.3 Schéma choisi

3.3.1 CAPS

Le CAPS permet aux véhicules de déterminer leur position en tenant compte des conditions de communication environnantes telles que la qualité du signal, la disponibilité des canaux et la charge du réseau.

En adaptant leur positionnement selon ces paramètres, les véhicules optimisent la transmission et la réception d'informations critiques, contribuant ainsi à une conduite plus sûre et plus fluide.

3.3.2 CPN

Le CPN repose sur un mécanisme de partage de ressources où les véhicules utilisent des protocoles de contention pour estimer leur position.

Plutôt que de dépendre uniquement du GPS ou des infrastructures, le CPN permet aux véhicules de coopérer entre eux pour déterminer leur position relative en utilisant des techniques comme la synchronisation temporelle et la triangulation avec les véhicules voisins.

La combinaison du CAPS et du CPN confère aux VANET une localisation robuste et précise ainsi qu'une communication efficace même dans des environnements dynamiques sujets aux interférences. Ces technologies jouent un rôle essentiel dans le développement de systèmes de transport intelligents et connectés, offrant des solutions innovantes pour améliorer la sécurité, la gestion du trafic et l'expérience de conduite.

3.4 Critiques et Solutions

Les réseaux VANET présentent plusieurs défis et critiques, mais des solutions sont envisagées pour y remédier :

- **Sécurité et Confidentialité**

La communication sans fil est vulnérable aux attaques et au piratage , ainsi que la transmission d'informations sensibles comme la position, la vitesse.... soulève des préoccupations en matière de confidentialité.

- **Fiabilité de la Connectivité :**

Le caractère hautement dynamique des VANET peut entraîner une connectivité intermittente et des pertes de paquets, et la densité variable des véhicules affecte la qualité de la communication .

- **Passage à l'Échelle**

La gestion d'un grand nombre de nœuds mobiles (véhicules) dans un réseau VANET pose des défis en termes de passage à l'échelle.

- **Consommation d'Énergie**

Les communications sans fil et le traitement des données peuvent entraîner une consommation d'énergie importante pour les véhicules

3.5 Contribution

Pour éviter les problèmes rencontrés dans les réseaux VANET, une solution prometteuse consiste à combiner les concepts de CAPS et de CPN. Cette approche hybride, appelée CAP-CPN, vise à tirer parti des avantages de chaque technique tout en compensant leurs limites respectives. Voici comment elle pourrait fonctionner :

- **Optimisation de la Communication**

Les véhicules adaptent leur positionnement en fonction des conditions de communication pour optimiser la transmission et la réception d'informations critiques, améliorant ainsi la fiabilité de la connectivité .

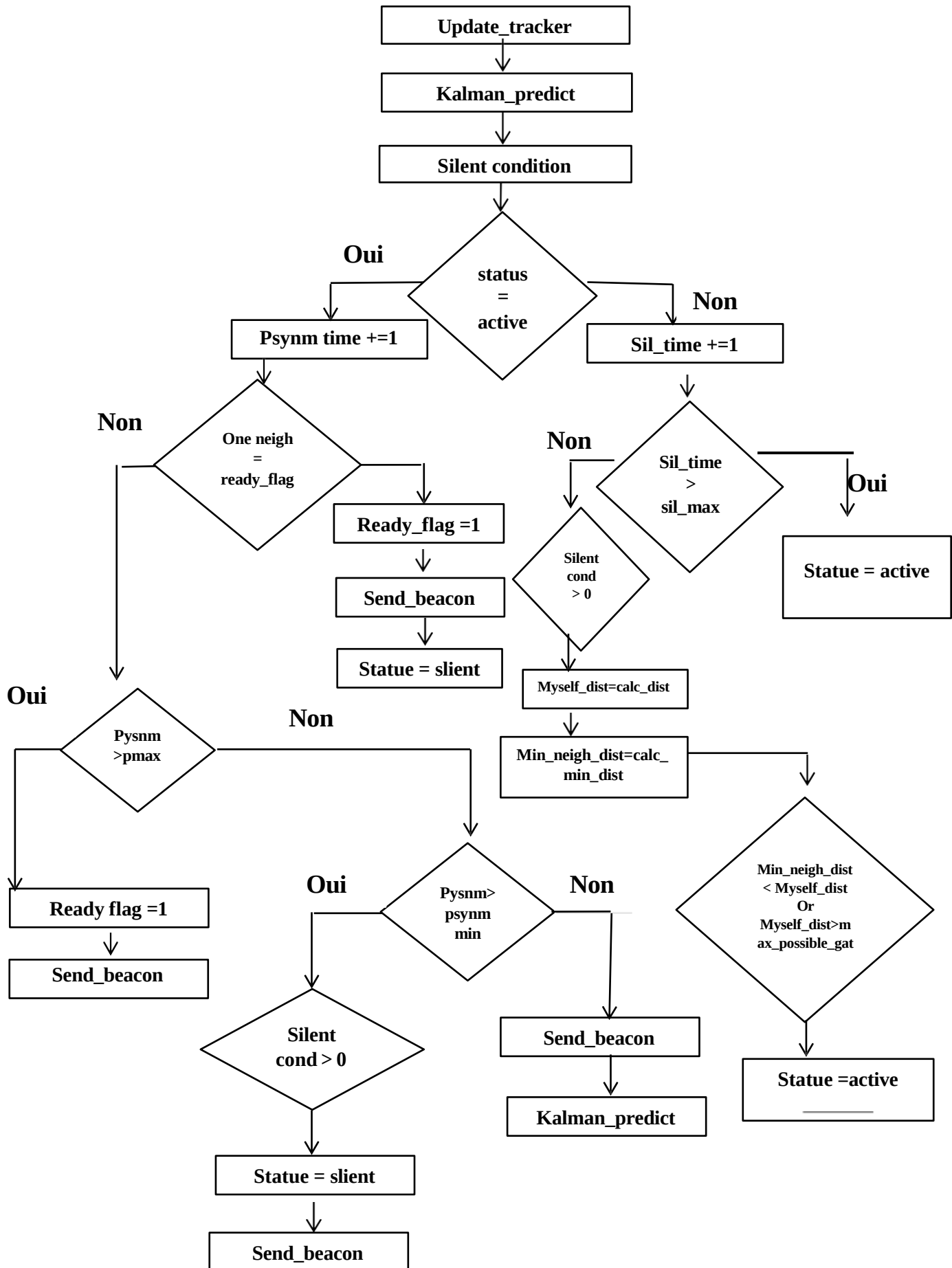
- **Combinaison des Avantages**

Le positionnement optimisé de CAPS facilite la communication pour les échanges de données nécessaires au CPN qui fournit une localisation précise utilisée par CAPS pour ajuster le positionnement des véhicules.

- **Gestion de la Confidentialité et de la Sécurité**

L'utilisation de pseudonymes préserve l'anonymat des utilisateurs, ainsi que les techniques de cryptographie et d'authentification robustes sécurisent les communications du CAP-CPN.

3.6 Notre proposition pour préserver la vie privée dans les réseaux VANET



L'organigramme présente un processus qui alterne entre un état "actif" et un état "silencieux". Les états sont déterminés par des conditions liées au temps d'utilisation du pseudonyme actuel, la présence de voisins "prêts" et des calculs de distances .

Voici les étapes de l'organigramme :

- Mettre à jour un mécanisme de suivi lié aux véhicules voisins dans le réseau avec l'instruction Update_tracker.
- Utiliser un filtre de Kalman pour prédire les positions futures des véhicules voisins avec l'instruction Kalman_predict.
- Vérifier les conditions de silence avec l'instruction Silent condition.
- Si l'état de statut est "Active", incrémenter le temps d'utilisation du pseudonyme actuel.
- Vérifier si un seul voisin est prêt (ready_flag).
- Si oui, passer ready_flag à 1, changer l'état de statut à "Silent", et envoyer un beacon avec l'instruction Send_beacon.
- Si le temps d'utilisation du pseudonyme actuel dépasse une certaine valeur ($Psym > psymmax$),
- Passer ready_flag à 1 et envoyer un beacon avec l'instruction Send_beacon.
- Si le temps d'utilisation du pseudonyme actuel dépasse un certain seuil minimal ($Psym > psymmin$),
- Vérifier la condition $Silent\ cond > 0$, changer l'état de statut à "Silent", et envoyer un beacon avec l'instruction Send_beacon.
- Si aucune des conditions ci-dessus n'est remplie, envoyer un beacon avec l'instruction Send_beacon.
- Si l'état de statut n'est pas "Active",
- Incrémenter le temps passé en mode "silencieux" avec l'instruction $Sil_time += 1$.
- Si le temps passé en mode "silencieux" dépasse un certain seuil maximal ($Sil_time > sil_max$),
- Passer à l'état "Active".
- Sinon, vérifier la condition $Silent\ cond > 0$, calculer la distance pour le véhicule lui-même ($Myself_dist = calc_dist$) et la distance minimale par rapport aux voisins ($Min_neigh_dist = calc_min_dist$).
- Si la distance minimale des voisins est inférieure à la distance du véhicule lui-même, ou si la distance du véhicule dépasse une certaine valeur maximale ($Min_neigh_dist < Myself_dist$ OR $Myself_dist > max_possible_gate$),
- Passer à l'état "Active".

3.7 Conclusion

Ce chapitre a présenté notre contribution qui repose sur l'intégration des concepts CAPS (Communication-Aware Positioning System) et CPN (Contention-based Positioning Network) pour créer une approche hybride appelée CAP-CPN. Cette méthode combine les avantages des deux techniques, améliorant ainsi la localisation précise des véhicules et la communication efficace tout en préservant la confidentialité.

CHAPITRE 04 : ANALYSE ET DISCUSSION DES RESULTAS

CHAPITRE 04

ANALYSE ET DISCUSSION DES RESULTAS

4.1 Introduction

La simulation est une méthode de validation courante dans le domaine des réseaux, et notre proposition a été comparée à divers schémas connus, utilisés comme références de comparaison dans de nombreuses études récentes. La simulation a été réalisée à travers la plateforme de simulation OMNET++, un simulateur largement utilisé pour les réseaux sans fil.

PREXT vise à combler ce manque en facilitant l'évaluation et la comparaison de différents schémas de protection de la vie privée. Il implémente sept schémas basés sur des approches diverses comme les périodes silencieuses, l'adaptation au contexte ou les zones de mixage. PREXT inclut également des modules simulant un adversaire capable d'écouter les communications et de suivre les véhicules. Plusieurs métriques sont proposées pour mesurer le niveau de confidentialité obtenu, comme l'entropie, la traçabilité ou les statistiques d'utilisation des pseudonymes.

4.2 Adversaire global

- Récepteurs (Eavesdropper) installés sur le réseau routier
- Rapportent les messages espionnés au module central VehicleTracker
- VehicleTracker supprime les doublons, exporte les messages et peut exécuter l'algorithme NNPDA pour suivre les véhicules . **La figure (11)** montre que le changement des pseudonymes est une solution prometteuse pour la préservation de la vie privée.

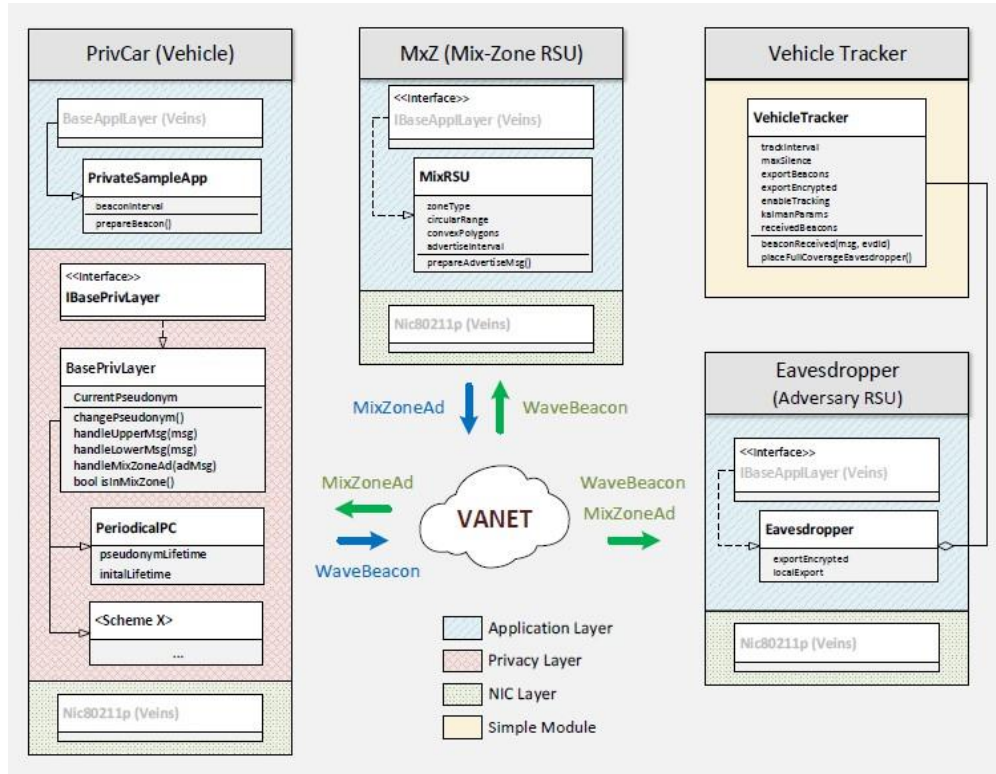


Figure 11: Architecture de l'extension de confidentialité proposée

4.3 Analyse du mécanisme

Dans cette section, nous allons examiner en profondeur notre mécanisme de protection de la confidentialité des localisations. Nous démontrerons sa rigueur et son adaptation supérieure aux systèmes de transport intelligents par rapport aux schémas existants. Nous mettrons également en évidence sa résistance aux éventuelles attaques malveillantes visant les techniques de changement de pseudonymes. L'analyse approfondie soulignera les forces de notre approche et sa supériorité par rapport aux solutions précédentes.

4.4 Considération des applications de sûreté

Les applications de sécurité routière nécessitent une diffusion très rapide des messages d'alerte au sein du réseau véhiculaire. Cependant, les stratégies basées sur le principe de "période de silence", où certains véhicules désactivent leurs émetteurs et cessent de relayer les messages, ralentissent ou empêchent cette propagation.

En cas d'accident grave, il est crucial que les avertissements soient diffusés le plus rapidement possible pour minimiser les dommages. Une transmission rapide des messages d'alerte permet

de créer un couloir d'urgence, d'éviter les embouteillages et de faciliter l'arrivée rapide des services d'urgence.

Notre modèle n'empêche pas la transmission de ces messages critiques, mais utilise temporairement un pseudonyme commun. Pendant la transition entre l'ancien et le nouveau pseudonyme, les véhicules signent leurs messages avec la clé liée au pseudonyme commun, permettant ainsi la transmission normale des messages de contrôle et le relais des messages d'urgence reçus.

Pendant cette phase transitoire où les véhicules voisins utilisent le même pseudonyme, il est essentiel de s'assurer de l'honnêteté de chaque véhicule, car il est difficile de les distinguer. Des mécanismes de révocation rapide des certificats sont donc utilisés. Si un véhicule se comporte de manière malveillante ou transmet de faux messages, l'autorité de confiance lui retire son certificat et l'ajoute à une liste noire, l'empêchant de contribuer davantage au système. Plusieurs travaux de recherche ont été menés sur ce sujet.

4.5 Simulation

L'évaluation des performances de notre mécanisme est cruciale pour déterminer sa résilience face aux attaques potentielles. Cette section est dédiée à la présentation de l'environnement de simulation utilisé et à l'analyse des résultats obtenus.

4.5.1 Environnement de la simulation

4.5.1.1 OMNET++

Nous avons mené des simulations à l'aide du simulateur de réseaux événementiel OMNET++ (Objective Modular Network Testbed in C++) dans sa version 5.0. OMNET++ est fourni avec une bibliothèque et un framework de simulation C++ extensible, modulaire et basé sur des composants, principalement dédié à la simulation de réseaux. Cependant, ce simulateur ne dispose d'aucun module natif pour les protocoles de communication des VANETs. Dans notre cas, nous avons dû faire appel à des frameworks externes fournissant des protocoles de communication pour les VANETs, ainsi qu'à d'autres frameworks pour la simulation du trafic routier.

4.5.1.2 SUMO

SUMO (Simulation of Urban MObility) est un simulateur de trafic routier. Il est fourni sous forme d'un package comprenant plusieurs outils permettant de créer des scénarios de trafic routier respectant toutes les contraintes d'un réseau véhiculaire. Les véhicules suivent la structure définie par les routes, la présence de bâtiments, ainsi que les panneaux de signalisation et les feux de circulation. Le simulateur inclut même la simulation des piétons.

4.5.1.3 VEINS

VEINS (VEhicles In Network Simulation) est un projet open source dédié à la simulation des réseaux véhiculaires. Il contient un ensemble de modèles de simulation pour les VANETs, qui s'exécutent sur l'interface graphique et l'IDE d'OMNET++, et interagissent avec le simulateur de trafic routier SUMO. D'autres composants de VEINS gèrent la configuration, l'exécution et la supervision de la simulation. L'interaction entre ces modèles offre une suite complète pour la simulation des communications inter-véhiculaires (IVC).

4.5.1.4 PREXT

PREXT est un cadre unifié et extensible conçu spécialement pour la simulation des schémas de confidentialité basés sur le changement de pseudonymes dans les VANETs. Il repose sur l'hypothèse principale des réseaux véhiculaires, à savoir la diffusion périodique de messages de sécurité (beacons) contenant des informations spatio-temporelles comme la position, la vitesse, l'heure, la date et le pseudonyme du nœud. Cet outil intègre sept schémas de confidentialité différents, tels que les schémas basés sur les périodes de silence, les zones mixtes ou le contexte. PREXT modélise un adversaire passif global capable d'écouter tous les messages et de tenter de suivre les véhicules pour casser le schéma de confidentialité, en utilisant un puissant algorithme de suivi (NNPDA). Sa conception modulaire de la couche de confidentialité facilite l'implémentation de nouveaux schémas. Plusieurs paramètres permettent de mesurer les performances en matière de confidentialité. Pour ces raisons, de nombreuses études récentes valident leurs propositions en utilisant le cadre PREXT.

4.5.2 Paramètres

Nous mesurons plusieurs indicateurs de performance. Les valeurs correspondent aux paramètres généraux cités dans le Tableau 1, tandis que les paramètres d'adversaire sont établis dans le Tableau 2. Le Tableau 3 résume les valeurs choisies pour configurer chacun des schémas de confidentialité existants.

1. Traçabilité Normalisée

Table 1: Les paramètres 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 de manière continue sur au moins 90% de sa trajectoire. Ce suivi est nécessaire pour briser la confidentialité en termes de vie privée du conducteur, car la découverte des traces requiert des trajectoires complètes. Une métrique proche est la traçabilité normalisée. Calculée de la même manière, elle exclut cependant les traces n'ayant jamais changé de pseudonyme. Ainsi, la trace normalisée fournit une information précise sur l'efficacité du schéma de protection de la vie privée du véhicule contre les attaques de suivi. [22]

2. Changement moyen des pseudonymes par trace

Nombre moyen de changements de pseudonymes par trajet Au cours d'un trajet, un véhicule peut changer de pseudonyme plusieurs fois. Cette métrique mesure le nombre moyen de changements de pseudonymes effectués par les véhicules. Un changement trop fréquent des pseudonymes n'est pas recommandé, il faut trouver un équilibre entre l'efficacité du mécanisme de confidentialité et son coût de gestion. Pour cette raison, nous devons ajuster le nombre de changements de pseudonymes de manière optimale.

3. Confusion moyenne par trajet

Les schémas de confidentialité visent à dissimuler l'identité des véhicules pour empêcher le suivi de leurs déplacements. Pour y parvenir, ils doivent induire une situation de confusion pour l'adversaire tentant de suivre la trace d'un véhicule. Cette métrique reflète l'efficacité du schéma de confidentialité. La confusion n'est possible que lorsqu'un véhicule change de pseudonyme. Cette métrique mesure donc l'efficacité de la stratégie de changement de pseudonymes.

Table 2: Paramètres d'adversaire

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

Table 3: Paramètres des schémas de confidentialité

Schéma	Paramètre	Valeur
PPC [23]	Pseudonym lifetime	60s
RSP[24]	Pseudonym lifetime	60s
	Silent period	(3,9)s
SLOW [24]	Speed threshold	8m/s
	Silent threshold	5s
CPN [25]	Radius	100 m
	Neighbors threshold	2
CAPS [26]	Min pseudonym lifetime	60s
	Max pseudonym lifetim	180s
	Silence range Missed	(3,13)s
	beacons silence	2
	threshold	50 m
	Neighborhood radius	
CAPS-CPN	Min pseudonym lifetime	60s
	Max pseudonym lifetim	180s
	Silence range Missed	(3,13)s
	beacons silence	2
	threshold	50 m
	Neighborhood radius	100 m
	Radius	2
	Neighbors threshold	

4.6 Confusion moyenne par changement de pseudonyme

Cette métrique vise à s'assurer que le schéma proposé évite les traitements inutiles. Elle est définie comme le rapport entre le nombre moyen de confusions par trajet et le nombre moyen de changements de pseudonymes par trajet. Plus cette métrique est élevée, plus la solution est efficace. Comme mentionné pour la métrique du nombre moyen de changements de pseudonymes par trajet, l'objectif est de minimiser les changements de pseudonymes tout en maximisant la confusion induite.

4.7 Configuration de Simulation

Dans la simulation, nous avons utilisé une carte routière du centre-ville de Munich **figure (12)**

1 - Carte routière du centre-ville de Munich de 2,67 km x 2,8 km obtenue à partir d'OpenStreetMap et convertie en réseau SUMO

2 - Taux d'arrivée des véhicules : 1,43 et 2 véhicules par seconde

- Génération de traces aléatoires avec ces taux d'arrivée (169, 234 et 327 traces au total)

- Véhicules arrivent successivement pendant 5 minutes puis 5 autres minutes pour permettre aux véhicules de sortir

3 - Paramètres des véhicules :

- Vitesse max 50 km/h

- Accélération entre $-4,5 \text{ m/s}^2$ et $2,6 \text{ m/s}^2$

- Durée médiane d'une trace : 290 secondes

- Distance médiane parcourue : $\sim 2 \text{ km}$

4 - Les véhicules émettent des balises (beacons) à toutes les secondes

5 - 6 zones de mélange circulaires de rayon 150m déployées

- Placées aux intersections centrales de la carte (voir Figure 3)

- Permettent aux véhicules de changer de pseudonyme et chiffrer leurs messages dans cette zone

6 - Configuration d'ombrage des obstacles réduite pour éviter les pertes de paquets

- Mais configuration non réaliste, à ajuster pour des scénarios du monde réel



Figure 12: carte géographique du centre-ville de Munich

4.8 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.

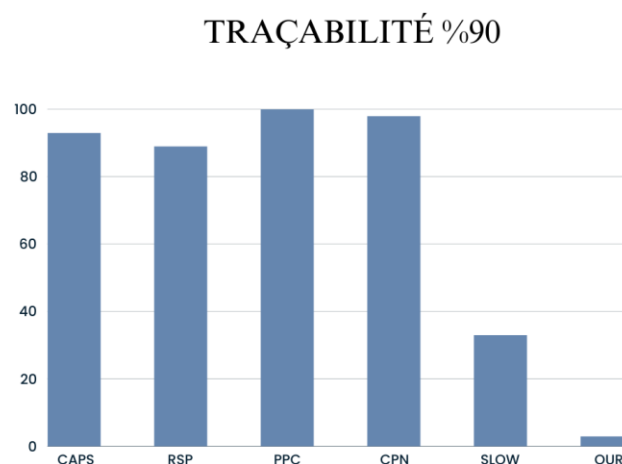


Figure 13: Traçabilité %90

La figure 13 présente le pourcentage de traçabilité, c'est-à-dire l'efficacité avec laquelle un adversaire peut suivre un véhicule en continu sur plus de 90 % de sa trace.

Notre schéma "OUR" obtient le meilleur score avec une traçabilité d'environ 20% par rapport aux autres schémas (CAPS, RSP, PPC, CPN, SLOW) ont des scores extrêmement élevés, proches de 100%.

Cela signifie que ces techniques échouent largement à préserver l'anonymat, puisqu'il est possible dans la plupart des cas de retrouver l'identité réelle derrière les données censées être anonymisées.

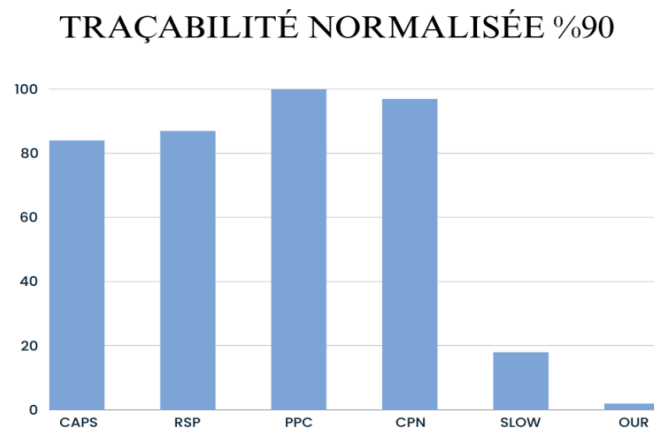


Figure 14: Traçabilité normalisée %90

La figure 14 présente les mêmes données qui sont normalisées sur une échelle de 0 à 100. Cela confirme les bons résultats de notre schéma "OUR" qui a une traçabilité normalisée d'environ 20%, comparée à 80% environ pour les autres schémas.

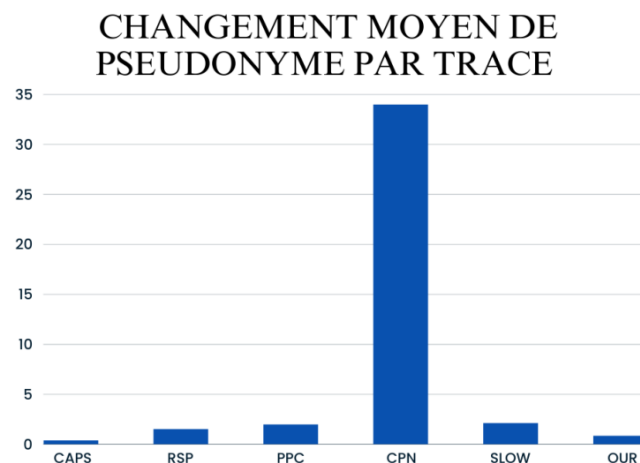


Figure 15 : Changement moyen de pseudonyme par trace

La figure 15 montre le nombre moyen de fois qu'un pseudonyme est changé pour chaque trace d'activité utilisateur dans les données après anonymisation.

Un nombre élevé de changements de pseudonymes par trace est souhaitable, car cela rend plus difficile le suivi et la ré-identification d'un même utilisateur à travers plusieurs points de données.

Notre schéma "OUR" affiche de loin le meilleur résultat avec environ 30 changements de pseudonymes en moyenne par trace utilisateur.

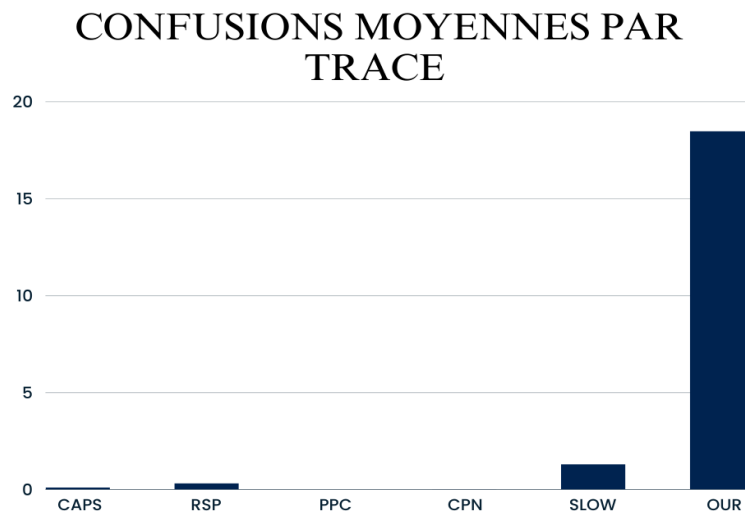


Figure 16: Confusions moyennes par trace

La figure 16 représente le nombre moyen de confusions d'identité par trace d'utilisateur. Un bon score est également élevé pour cette métrique. Encore une fois, "OUR" se démarque avec le plus haut nombre de confusions, autour de 18, contre moins de 5 pour la plupart des autres approches.

4.9- Conclusion

Dans ce chapitre , nous avons proposé et évalué une extension de confidentialité pour le framework Veins. Sa conception flexible permet d'implémenter plusieurs schémas de confidentialité basés sur différentes approches telles que les périodes silencieuses (RSP et CSP), le contexte (CPN, CAPS et SLOW) et les zones de mélange. Elle inclut un adversaire capable de collecter et suivre les messages balises et de reconstruire les traces des véhicules. Elle évalue également la confidentialité préservée en utilisant plusieurs métriques populaires comme la taille de l'ensemble d'anonymat, l'entropie et la traçabilité. Selon les expériences mentionnées, PREXT ajoute un délai significatif au temps de simulation, sauf pour les schémas basés sur les zones de mélange. Cependant, la simulation peut encore tourner en temps réel pour des densités de véhicules faibles et intermédiaires. Dans les futurs travaux, nous utiliserons cette extension pour développer un protocole de confidentialité hybride qui utilisera le schéma de confidentialité approprié selon le contexte du véhicule.

Conclusion générale

La recherche dans le domaine des réseaux véhiculaires (VANETs) a suscité un vif intérêt ces dernières années, en raison des nombreux services qu'ils offrent aux usagers de la route. Leur principal avantage est l'échange d'informations sur l'état du trafic afin de minimiser et éviter les accidents, mais ils permettent également d'améliorer les conditions de déplacement grâce à des services tels que la localisation des stations-service, l'accès à Internet, le partage de fichiers multimédias, l'échange d'informations entre conducteurs, etc.

Pour un déploiement sécurisé des VANETs, certaines exigences doivent être satisfaites, comme l'intégrité, l'authentification, la confidentialité, la disponibilité, la non-répudiation, le temps réel, le respect de la vie privée et la cohérence. Les chercheurs proposent des solutions pour résoudre les problèmes liés aux VANETs, parmi lesquelles le changement de pseudonymes pour préserver la vie privée.

Dans notre travail, nous avons proposé un mécanisme de changement de pseudonyme visant à garantir l'anonymat dans les réseaux véhiculaires. Cette solution assure le changement simultané des pseudonymes de communication privés pour plusieurs véhicules (au moins trois), tout en préservant leur vie privée et leur anonymat dans les VANETs. Ce protocole repose sur un comportement coopératif.

Les résultats des simulations démontrent l'efficacité de notre solution par rapport à d'autres mécanismes de changement de pseudonymes, avec des performances encore améliorées dans les cas de haute densité de trafic.

L'avantage de notre proposition flexible est qu'elle peut être utilisée à tout moment et dans tout environnement (urbain ou routier).

REFERENCES

- [1] <https://www.envoituresimone.com/code-de-la-route/cours/securite-passagersvehicule/prevention-routiere>
- [2] L'article "Sécurité routière : l'application de la technologie pour diminuer les accidents de la route" sur Atlas Magazine
- [3] L'auteur du livre intitulé "Prévention et sécurité routières", cité sur Wikipedia...
- [4] L'auteur du livre "Communication et sécurité routière" référencé dans le site "OpenEdition Journals" est Laurent Carnis. collection "Les Essentiels d'Hermès" du CNRS, datant de 2021 et comptant 236 pages, avec l'ISBN 978-2-271-13940-5.
- [6] L'article "L'essor des marques chinoises dans l'importation de véhicules en Algérie" sur AutoNews-dz.com
- [10] " Étude et caractérisation d'un canal de propagation pour les réseaux VANET" par Hamou Chehri
- [11] "VANET simulators: an updated review" par les auteurs du journal BCS.
- [12] "UNIVERSITÉ DU QUÉBEC MÉMOIRE PRÉSENTÉ À L'UNIVERSITÉ DU ..." par K. Moghraoui.
- [13] "The Wavetable Synthesis Architecture - Meta Function"
<https://www.metafunction.co.uk/post/the-wavetable-synthesis-architecture>
- [14] "Vehicular Ad-Hoc Networks (VANETs): Architectures, Protocols and Applications" par Azzedine Boukerche architecture
- [15] "A Survey on Security and Privacy Issues in Vehicular Ad Hoc Networks" par Manabu Tsukada et al. <https://www.musicradar.com/news/ultimate-guide-wavetable-synthesis>

- [16] "Wireless Access in Vehicular Environments (WAVE): A Survey of Standards and a Glance of Technology" par Yasser L. Morgan
- [17] L'auteur du document "CHEKIMA Faouzi Et AKHDAR Messaoud"
ouargla.dz/jspui/bitstream/123456789/29104/1/
CHEKIMA%20Faouzi%20%D9%8FEt%20AK
HDAR%20Messaoud.pdf
- [18] Le document "Évaluation des performances d'un protocole de dissémination de données dans les Réseaux ad-hoc véhiculaires"
- [19] "Wireless Access in Vehicular Environments (WAVE): A Survey of Standards and a Glance of Technology" par Yasser L. Morgan https://en-us.support.motorola.com/app/answers/detail/a_id/114196/~/utiliser-les-services-de-localisation
- [20] "Vehicular Ad-Hoc Networks (VANETs): Architectures, Protocols and Applications" par Azzedine Boukerche <https://support.apple.com/fr-fr/102647>
- [21] "A Survey on Security and Privacy Issues in Vehicular Ad Hoc Networks" par Manabu Tsukada et al. <https://support.apple.com/fr-ca/10264>
- [22] Karim Emara, « Poster : Prext : Privacy extension for veins vanet simulator », in : 2016 IEEE Vehicular Networking Conference (VNC,) IEEE, 2016, p. 1-2.
- [23] Yuanyuan Pan et al., « An analytical model for random pseudonym change scheme in VANETs », in : *Cluster Computing* 17.2 (2014), p. 413-421.
- [24] 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.
- [25] 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.
- [26] 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.
- [27] 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

