République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mohamed El Bachir El Ibrahimi de Bordj Bou Arreridj
Faculté des Mathématiques et d'Informatique

Mémoire de fin d'études
Présenté en vue de l'obtention du diplôme de
Master en Informatique
Spécialité : Réseaux et multimédias

Thème :

La vie privée dans les VANET : Amélioration du schéma SLOW

Présenté par :

Guennouh hassiba

Kirouani yousra

Encadreur : Moussaoui Boubakeur

2023-2024

Remerciment

Tout d'abord nous remercions dieu le tout puissant de nous avoir donné la volonté et la patience nécessaires pour accomplir ce travail.

Nous souhaitons avant tout remercier nos encadreurs de mémoire, M. Moussaoui Boubakeur. Nous les remercions de nous avoir encadrés, orientés, aidés et conseillés tout au long du processus de rédaction.

Nous adressons nos sincères remerciements à tous les professeurs et aux personnes dans le même domaine qui ont répondu à nos questions durant nos recherches.

Table des matières

Liste des figures

Liste des abréviations

BSM	Basic Safety Message
CA	Central Authority
DSRC	Dedicated Short Range Communication
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transport Systems
MANET	Mobile Ad-hoc Networks
NNPDA	Nearest Neighbor Probabilistic Data Association
OBU	On-Board Units
OMNET++	Objective Modular Network Testbed in C++
PKI	Public Key Infrastructure
PREXT	Privacy Extension for Veins VANET
RSU	Road Side Units
SUMO	Simulation of Urban Mobility
VANET	Vehicular Ad hoc NETwork
VEINS	VEhicles in Network Simulation
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WAVE	Wireless Access in Vehicular Environments

ملخص

تعتبر شبكات المركبات المخصصة تقنية حيوية لضمان السلامة على الطرق وحماية معلومات السائقين تساهم استراتيجيات تغيير الاسم المستعار بشكل دوري في الحفاظ على الهوية الحقيقية للمركبة وكذلك حمايتها من التعقب. وفي هذا السياق نقترح استراتيجية تعمل على تغيير الاسم المستعار إذا كانت السرعة أقل من حد معين 30كلم/ساعة وكذلك وجود جار واحد على الأقل. وهو حل يعمل على تعزيز سرية المركبة وفي هذا العمل قمنا بتقييم هذه الاستراتيجية باستخدام محاكاةOMNET++.

الكلمات المفتاحية : VANETs ، hybride SLOW CPN ، الخصوصية ، تغيير الاسم المستعار ، الامان.

Summary

In vehicular ad hoc networks (VANETs), ensuring road safety and protecting drivers' information are essential. Regular pseudonym change strategies contribute to maintaining the vehicle's anonymity and protecting it against tracking. In this context, we have proposed an approach that changes the pseudonym when the vehicle's speed drops below threshold in the presence of at least one neighboring vehicle. Our solution enhances vehicle privacy. We evaluated this approach using OMNET++ simulations.

Keywords: VANET, Enhanced SLOW CPN, privacy, change of pseudonym, security.

Résumé

Les réseaux ad hoc véhiculaires (VANET), sont essentiels pour assurer la sécurité routière. Il est aussi important de protéger les informations personnelles des conducteurs (Position, Vitesse, Identité réelle…). Les stratégies de changement des pseudonymes contribuent de manière régulière à maintenir l'identité réelle du véhicule et le protègent contre les traqueurs. Dans ce contexte, nous avons proposé une approche qui permet le changement des pseudonymes lorsque la vitesse du véhicule est inférieure à un seuil, en plus on exige la présence d'au moins un voisin qui change son pseudonyme simultanément. Cette solution renforce la confidentialité du véhicule. Nous avons évalué notre approche en utilisant la simulation OMNET++.

Mots-clés : VANET, hybride SLOW CPN , vie privée, changement de pseudonyme, sécurité.

Introduction générale

Avec le développement des Systèmes de Transport Intelligents (ITS), les Réseaux Ad hoc Véhiculaires (VANETs) sont devenus un sujet de recherche très important ces dernières années. Les VANETs sont des réseaux auto-organisés qui peuvent être configurés en reliant les véhicules entre eux et avec des unités installées aux bords des routes appelées Road Side Unit (RSU). Les RSUs sont connectés par des réseaux à haut débit. Il existe deux types de communications dans les VANETs : Véhicule à Véhicule (V2V) et Véhicule à Infrastructure (V2I). L'objectif de ces réseaux est d'augmenter la sécurité routière, de gérer le trafic, et même le confort de la route.

Le véhicule diffuse périodiquement des messages de contrôle liés au trafic comprenant des informations sur son état actuel à savoir : son identifiant, sa localisation, sa direction et sa vitesse, et autres… La transmission en claire de ces informations sensibles devient un moyen de suivi par un attaquant. La complexité de la vie privée induite peut donc constituer un véritable défi pour les réseaux véhiculaires. Pour garantir la confidentialité, il est essentiel d'assurer l'anonymat du véhicule et au même temps l'authentification.

Dans ce travail, nous envisageons à améliorer le schéma SLOW qui fournit une traçabilité minimale par rapport aux autres schémas de confidentialités disponible sur le module de simulation PREXT. La simulation peut être faite sur le simulateur OMNET++.

Le mémoire est structuré comme suit :

- ✓ Le premier chapitre présente les notions de base sur les réseaux véhiculaires.
- ✓ Le deuxième chapitre traite de la vie privée dans les VANETs et des mécanismes de changement des pseudonymes.
- ✓ Le troisième chapitre présente notre contribution, et les tests de simulation et les résultats.
- ✓ On conclut avec une conclusion générale

Chapitre 1 : Notions de base sur les VANETs

1.1 Introduction

Les réseaux véhiculaires (VANETs) sont un cas particulier des réseaux Ad-hoc utilisés dans les systèmes de transport intelligents (ITS). Les VANETs sont devenus l'un des sous-ensembles les plus encourageants et prometteurs à la croissance la plus rapide des réseaux ad hoc mobiles (MANETs). La communication dans le système VANET entraîne l'envoi et la réception des informations pour améliorer le trafic routier, de savoir les conditions routières récentes, de réduire les collisions que possible, de détecter les situations d'urgences et globalement d'augmenter l'efficacité du réseau routier [5].

1.2 Définition

Le réseau véhiculaire VANET est l'acronyme de **" Vehicular Ad hoc NETwork "** Il s'agit d'un type spécifique du réseau de communication ad-hoc sans fil (MANET). Un VANET permet la communication entre les véhicules et les infrastructures routières installées aux bords des routes appelées Road Side Units (RSU). Les véhicules du réseau échangent fréquemment des informations sensibles : position, vitesse, direction et d'autres informations pertinentes. Cette fonctionnalité permet de créer des réseaux de communication dynamiques en temps réel. Les VANETs possèdent le potentiel d'améliorer la sécurité routière en permettant aux véhicules de détecter les dangers potentiels et de réagir en conséquence [1].

La figure 1.1 illustre un réseau véhiculaire composé des véhicules intelligents et des RSU qui communiquent entre eux.

Figure 1.1 : Exemple d'un réseau VANET

1.3 Architecture

Dans cette section, on présente d'une manière assez détaillée l'architecture d'un VANET, en présentons les composants essentiels de ces réseaux et les communications existantes entre ses composants.

La figure **1.3** montre l'architecture d'un VANET, d'après cette figure les réseaux véhiculaires sont composés de trois types de dispositifs On-Board-Unit (OBU), Road-Side-Unit (RSU) et d'une autorité de confiance (TA) [2] :

➢ OBU (On-Board Unit)

L'OBU est l'élément essentiel installé dans les véhicules pour cela ces véhicules sont dits intelligents. Les véhicules intelligents regroupent un ensemble de composants matériels et logiciels selon la technologie actuelle (GPS, radar, caméras, différents capteurs). Chacun d'eux a un rôle particulier tel que : le calcul, la réception, la connaissance de la localisation, le stockage et l'envoi des données sur le réseau.

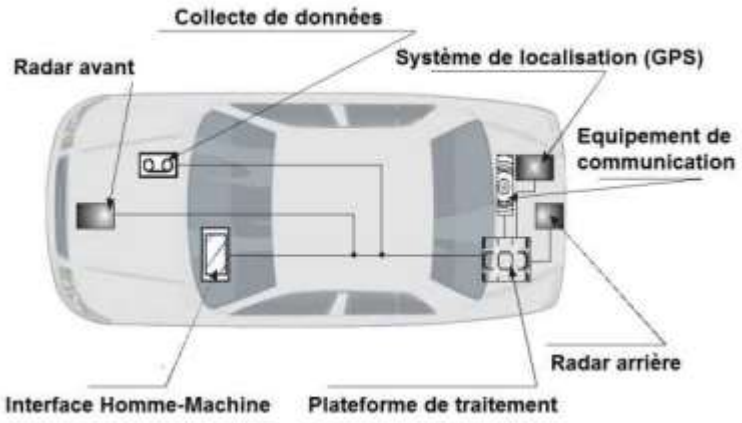

Figure 1.2 : Les composants d'un Véhicule intelligent

➢ RSU (Road Side Unit)

Les RSUs sont des équipements installés au bord des routes sur des feux de signalisation, sur des lampadaires, sur des panneaux d'arrêt etc. elles rendent la communication plus flexible et plus performante, particulièrement dans les endroits moins denses. Les RSUs peuvent êtres considérer aussi comme des points de liaison entre l'autorité de confiance et les véhicules.

➢ TA (Trusted Authority)

L'autorité de confiance est l'entité chargée d'assurer l'enregistrement pour plus tard authentifier et sécuriser les transactions des communications réseau. Elle joue un rôle important dans la gestion des certificats des pseudonymes de communication et d'autres éléments de sécurité.

La figure 1.3 résume les éléments tous les composants d'un réseau VANET traités au-dessus.

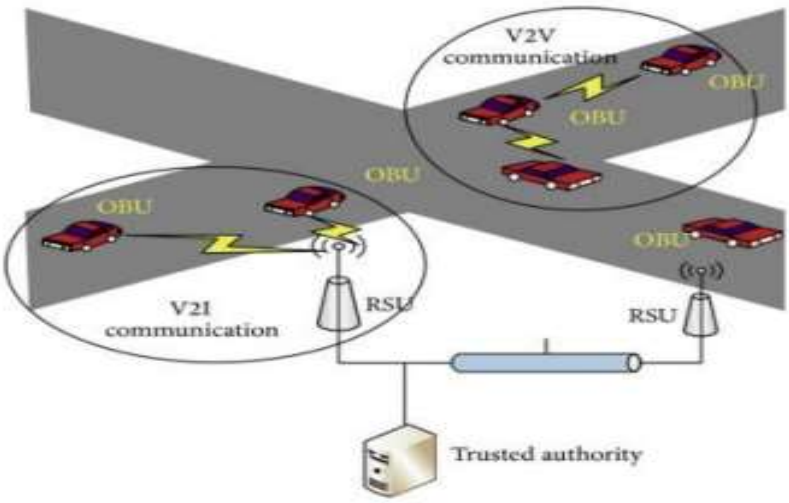

Figure 1.3 : Architecture de base d'un VANT

1.4 Types de communication

Dans les réseaux véhiculaires, il existe deux modes de communication principaux ; utilisés pour faciliter l'échange d'informations entre les véhicules et les infrastructures **:**

➢ V2V (Vehicule To Vehicule)

Dans ce mode, les véhicules communiquent directement entre eux. Ce type de communication fonctionne à l'aide des dispositifs installés sur les véhicules (OBU). Les

communications V2V (vehicle to vehicle) représentent le type de communication essentiel et primordial puisqu'elles permettent aux véhicules de partager des données pertinentes au fonctionnement du réseau, telles que la vitesse, la position, l'état de la route et d'autres informations. Cela permet d'améliorer la sécurité routière en permettant aux véhicules de se coordonner et de prendre des décisions en fonction des informations reçues des autres véhicules.

- **V2I (Vehicle To Infrastructure)**

Dans ce type de communication les véhicules communiquent avec les infrastructures (RSU), Les véhicules peuvent recevoir des informations sur l'état du trafic, les conditions de la route, les travaux en routiers. Ils peuvent également envoyer des informations aux infrastructures pour signaler des incidents ou demander une assistance.

1.5 Les types de message

- **Le message beacon**

Le message Beacon ou messages de sécurité contient des informations du véhicule (Position, vitesse, direction), il diffusé périodiquement leur information et Permet d'identifier et de découvrir les entités environnantes.

- **Le message d'alerte (d'urgence)**

Ce type de message est utilisé pour communiquer rapidement des informations importantes (d'un accident ou d'un embouteillage dans les routes, information météorologique) aux conducteurs et aux véhicules environnants. Ces messages d'alerte aident à améliorer la circulation et la sécurité routière.

- **Le message Service**

Ce type de message concerne la localisation et la découverte des emplacements de services (Stations de services, restaurants, hôtels). Ce type facilite la communication entre services.

1.6 Caractéristiques des réseaux VANETs

Les principes caractéristiques des VANETs sont :

➢ Environnement de déploiement

Il y a deux types environnements de déploiement des réseaux véhiculaires :

❖ Urbain

Ce type se caractérise par un nombre des véhicules dont la vitesse se situe dans une certaine limite. L'environnement urbain permet une bonne communication entre les véhicules grâce à la proximité, mais avec Perturbation importante des ondes radio.

❖ Autoroute

Ce type comporte un très grand nombre des véhicules lourds et légers et une circulation à une vitesse élevée. L'environnement de déploiement routier nécessite une infrastructure plus développée pour assurer les communications. Dans ce type d'environnement, l'utilisation des unités de bord de route RSUs est nécessaire pour surmonter les défis de communication Ad hoc.

➢ Modèle de mobilité

Dans les réseaux véhicule (VANET), la mobilité des véhicules est un aspect essentiel à prendre en compte. Le modèle de mobilité dans VANET est utilisé pour fonction des routes concernées, des feux tricolores, des limitations de vitesse, des conditions du trafic et des comportements des conducteurs dans un environnement réaliste.

➢ Technologies de communications

Les réseaux véhiculaires utilisent généralement des technologies de communication sans fil exactement le IEEE 802.11 pour permettre la transmission des données.il est considéré comme la technologie principale pour les VANETs en raison de sa capacité à fournir des communications à faible latence et à longue portée [3].

➢ Scalabilité

La scalabilité dans ce réseau (VANET) connectés fait référence à la capacité du réseau à fonctionner efficacement et à gérer une augmentation du nombre de véhicule connecté.

1.7 Les systèmes de transport intelligents coopératifs

1.7.1 Définition

Les Systèmes de Transports Intelligents Coopératifs (STI-C) classé en grande importance au sein du secteur des transports. Leur utilisation dans des nouvelles technologies de l'information et de la communication dans le domaine des transports. L'objectif principal de STI-C est améliorer la sécurité des usagers de la route et des agents en activité sur le réseau routier, à faciliter la gestion du trafic, en délivrant des informations en temps réel aux conducteurs. Ils sont basés sur des interactions numériques entre véhicules, véhicules et infrastructure, infrastructure et véhicules. L'action pour répondre aux situations signalées est gérée par le conducteur [4].

1.7.2 Domaines d'application

1.7.2.1 Applications de sécurité

Dans ce type Applications les VANETs peuvent améliorer la sécurité routière en permettant aux véhicules de partager des informations sur les conditions de la route, les accidents, les embouteillages, les travaux routiers. Ces informations peuvent être utilisées pour avertir les conducteurs des dangers potentiels à venir et les aider à rendre des décisions éclairées.

1.7.2.2 Applications commerciales

Ces applications offrent aux conducteurs des services de divertissement, tels que la possibilité d'accéder à Internet pour effectuer des achats ou des ventes en ligne, tout en leur permettant également de faire du magasiner virtuel.

1.7.2.3 Applications de confort

Ce type d'application vise à offrir de confort aux conducteurs, comme disposer d'une connexion Internet mobile et de prévisions météorologiques, ainsi que d'une connaissance de la fourniture de services dans toute leur région.

1.8 La sécurité dans les réseaux VANETs

Les VANETs, en tant que sous-classe de réseaux ad hoc sans fil, partagent les défis de sécurité associés aux VANET. Dans cette section, nous abordons la question de la sécurité du réseau VANET. Nous fournissons plusieurs exemples d'attaques qui pourraient cibler ces réseaux et détaillons les objectifs de sécurité associés.

1.8.1 Exigences de sécurité

La sécurité informatique est essentielle pour garantir que les ressources matérielles ou logicielles d'une organisation sont utilisées uniquement aux fins prévues. L'objectif principal est de maintenir de manière générale cinq services de sécurité de base, à savoir :

- ✓ **L'authentification**

L'authentification est de la plus haute importance dans les VANETs pour se protéger contre les adversaires potentiels. Cela nécessite que le destinataire soit capable d'identifier correctement la source du message. Dans le contexte des VANETs, l'authentification se divise en deux catégories : l'authentification basée sur l'ID et l'authentification basée sur l'entité. L'authentification basée sur l'ID garantit qu'un message provient d'une source fiable en l'identifiant de manière appropriée. L'identifiant doit être unique, par exemple : numéro de plaque d'immatriculation ou numéro de châssis du véhicule. Les réponses des véhicules aux événements doivent être basées sur des messages légitimes, ce qui nécessite une vérification des expéditeurs de ces messages. L'authentification d'entité garantit qu'un message récemment reçu est à jour et en direct, confirmant qu'il a été envoyé et reçu dans un délai approprié.

- ✓ **L'intégrité et la cohérence**

L'intégrité et la cohérence sont des aspects importants à considérer. L'intégrité concerne la nécessité de préserver les informations, telles que les messages pendant leur envoi, pour garantir qu'aucune modification ou suppression n'est apportée au message avant qu'il n'atteigne sa destination prévue, même si l'expéditeur est légitime, car les informations peuvent être incorrectes. Après un éventuel échec. Parfois, des modifications peuvent également être apportées intentionnellement par un expéditeur légitime, mais ces actions sont malveillantes. De plus, il est important de comparer les messages similaires créés à des heures et dans des lieux fermés pour garantir la cohérence. Ceci est nécessaire pour maintenir la fiabilité des informations échangées.

✓ La confidentialité

La confidentialité est un élément essentiel qui nécessite de maintenir les messages transmis sur le réseau contre les attaques d'entités malveillantes. Seuls l'expéditeur et le destinataire sont autorisés à accéder au contenu du message. Cette protection s'applique aux messages instantanés échangés entre véhicules et non aux messages d'alerte ou de sécurité. La confidentialité peut être garantie grâce au cryptage.

✓ La disponibilité

La disponibilité est une exigence de sécurité pour garantir la fiabilité du système et la disponibilité du réseau des véhicules dans les applications de sécurité. Il est essentiel que le réseau soit disponible à tout moment, car les messages d'alerte et d'avertissement doivent être diffusés rapidement dans une zone précise. Si l'alerte n'atteint pas les véhicules à temps, l'application devient inutile, comme c'est le cas de l'alerte post-collision. Par exemple, si une chaîne radio est en panne, l'envoi des messages devient impossible, affectant la disponibilité du réseau.

✓ Le contrôle d'accès

Le contrôle d'accès signifie que seuls les nœuds légitimes et honnêtes peuvent accéder aux services réseau. Un véhicule au comportement suspect est exclu du réseau et perd sa légitimité, et son certificat est alors ajouté à la liste des certificats rejetés. Par ailleurs, le contrôle d'accès concerne également les applications qui proposent différents niveaux d'accès. Ainsi, un nœud légitime et honnête peut se voir refuser l'accès au service s'il ne dispose pas des privilèges appropriés, même s'il est autorisé à utiliser le réseau.

✓ La non-répudiation

La non-répudiation est essentielle pour identifier de manière fiable les incidents criminels, car elle garantit que l'expéditeur des messages peut être identifié avec certitude. Cela garantit une traçabilité individuelle de toutes les communications, afin que l'expéditeur ne puisse nier être l'auteur du message.

- ✓ **La vie prive**

La vie prive est un élément important pour une large acceptation au sein des VANET, où les véhicules transmettent périodiquement des messages contenant des données sensibles telles que la localisation et la vitesse. Ces informations spécifiques au véhicule sont faciles à recueillir, mais les attaquants ne devraient pas être en mesure de déduire la véritable identité du véhicule ou du conducteur. Cela garantit que l'identité des véhicules et des conducteurs est préservée.

1.8.2 Le modèle d'un attaquant

La première étape pour sécuriser un système consiste à identifier les types d'attaquants potentiels. Dans les réseaux VANETs, on peut classer les attaquants comme suit :

- **Interne et externe**

Dans les VANETs, un attaquant interne est un membre normal du réseau qui peut communiquer avec d'autres membres disposant d'une clé publique certifiée par une autorité de confiance. Il est souvent difficile à détecter ou à isoler, et peut provoquer des dommages importants au réseau en raison de son accessibilité. Contrairement à un attaquant externe qui a une capacité limitée à attaquer le réseau.

- **Actifs et passifs**

Attaquants actifs et passifs : Dans les réseaux VANETs, on distingue les attaquants passifs qui écoutent l'information ou l'interceptent pour révéler son contenu sans le modifier, c'est-à-dire qu'ils visent à déterminer le contenu du message ainsi que les deux parties à la communication. D'un autre côté, les attaquants actifs créent de faux messages ou falsifient et modifient des messages interceptés.

Les figures **1.4** et **1.5** résument tous les cas d'attaques actives et passives.

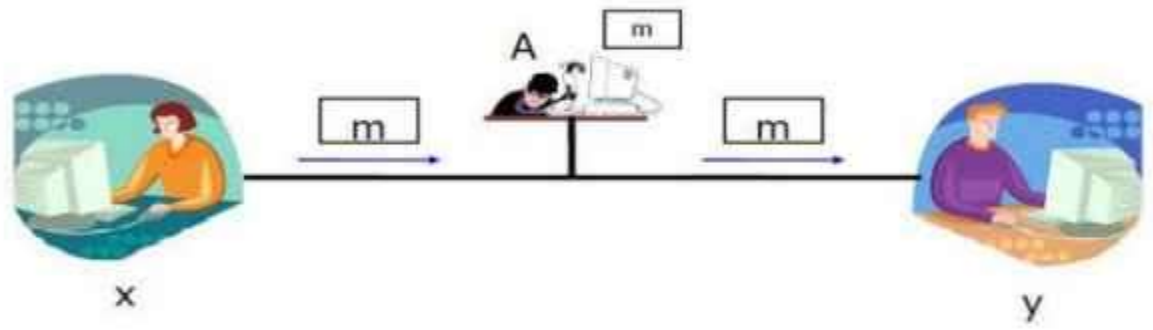

Figure 1.4: Attaque passive

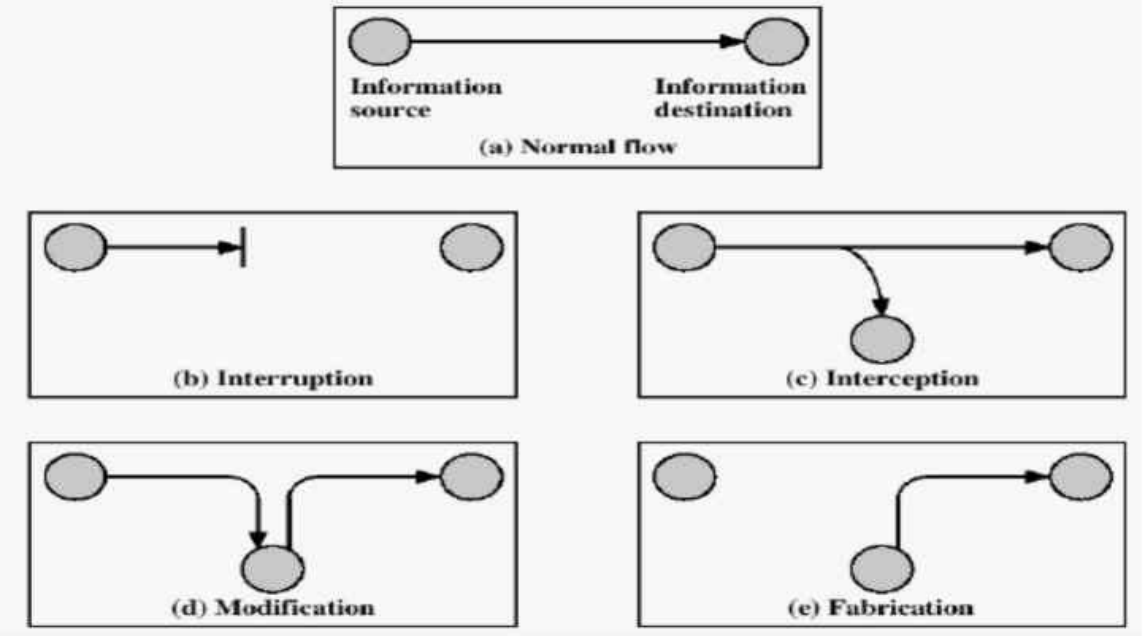

Figure 1.5 : Les déférentes opérations d'un attaquant actif sur les messages échange entre les nœuds

- **Malveillants ou Rationnels :**

L'attaquant malveillant n'a aucun intérêt direct à travers ses attaques et vise principalement à perturber le fonctionnement du réseau. Il peut donc utiliser tous les moyens disponibles, sans se soucier des conséquences qui y sont associées. L'attaquant rationnel vise à obtenir un gain personnel. Il est donc possible de prédire les objectifs de son attaque et les moyens qu'il utilise.

- **Locaux ou globaux**

Locaux ou globaux : Les attaquants locaux utilisent des ressources limitées sur des véhicules spécifiques, ce qui signifie qu'ils ciblent un domaine spécifique tel qu'une entreprise ou une organisation, tandis que les attaquants mondiaux ciblent plusieurs réseaux à travers le monde en exploitant plusieurs ressources, et ces attaquants sont souvent motivés par la réalisation d'un gain financier ou la vente de données volées au marché noir.

- **Attaque contre la vie privée**

Attaque contre la vie privée : la collecte d'informations par un attaquant constitue une menace majeure pour la vie privée d'un conducteur, car elle peut aider à déterminer ses actions et sa position. Cela se fait en échangeant des informations sensibles lors de la communication, notamment dans les messages de sécurité et de contrôle, où le véhicule envoie des messages contenant sa position, sa vitesse et parfois des détails sur son trajet.

- **Nœud caché**

Nœud caché : Cette attaque concerne les applications qui diffusent des messages d'alerte, dont les protocoles de communication dépendent de la position du nœud, et visent à arrêter la diffusion afin que le canal ne soit pas rempli des messages en double. L'attaquant exploite cette situation en convainquant le nœud qu'il est dans la meilleure position, auquel cas ni le nœud honnête ni l'attaquant ne diffusent. On dit que le nœud honnête est devenu un nœud caché.

- **Déni de service (Dos)**

Attaque par déni de service (Dos) : il s'agit de l'une des attaques les plus courantes, même dans les réseaux traditionnels. L'attaquant cherche à submerger le réseau en inondant le canal de messages inutiles, en le surchargeant ou même en empêchant l'envoi de messages d'alerte ou de contrôle.

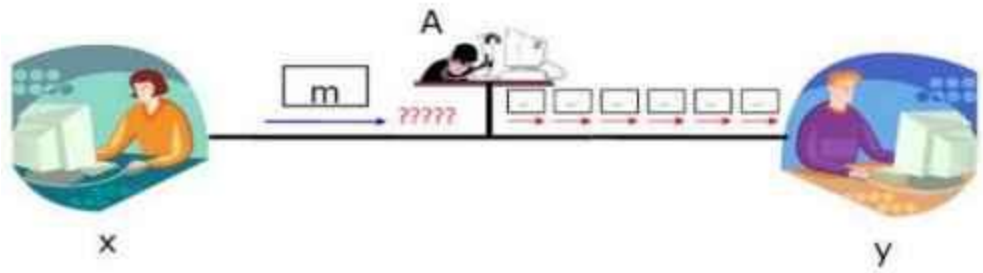

Figure 1.6 : Attaque Déni de service

- **Attaque sur la cohérence**

Attaque de cohérence : un attaquant peut violer la cohérence des messages en les supprimant, en les modifiant ou en insérant des informations incorrectes. En modifiant le contenu des messages, ou en provoquant des problèmes de circulation en détournant tous les véhicules vers une route très fréquentée.

- **Usurpation d'identité et rôle (spoofing)**

Vol d'identité et de rôle (usurpation d'identité) : un attaquant ou une entité malveillante cherche à usurper l'identité d'une autre entité et à agir en son nom, afin d'obtenir tous les privilèges et un accès non autorisé. Si des messages frauduleux sont envoyés ou si le système est désactivé, cela sera difficile à détecter.

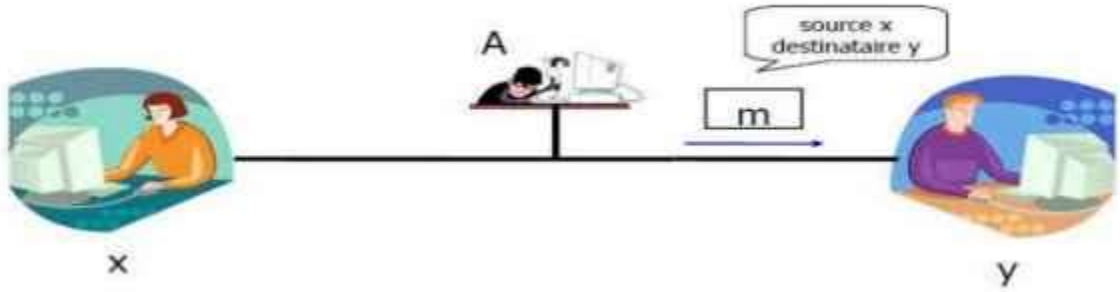

Figure 1.7 : Usurpation d'identité et rôle (spoofing)

- **L'injection des messages erronés**

Injection des messages : Ce type d'attaque peut avoir des conséquences très graves sur les VANETs, mettant potentiellement des vies humaines en danger. L'attaquant diffuse de faux messages et informations dans le but d'influencer le comportement des conducteurs et de modifier leurs itinéraires, ce qui peut entraîner des perturbations du réseau et des accidents de la route.

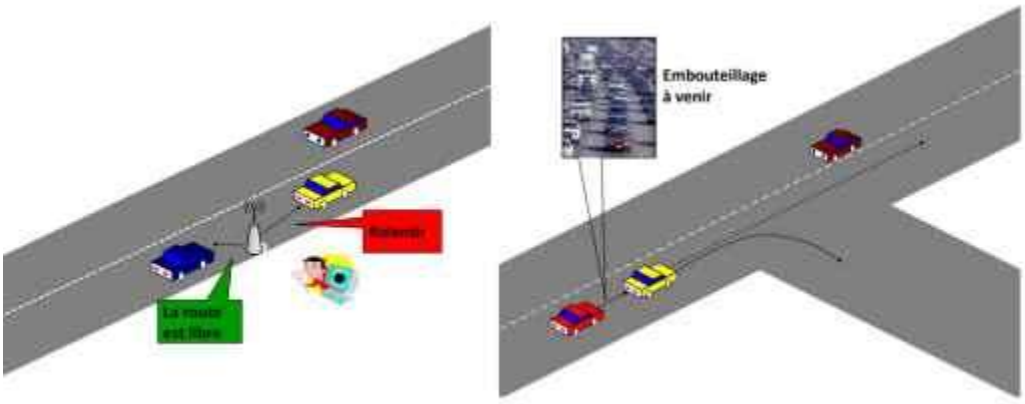

Figure 1.8 : Attaques par l'injection des messages erronés

1.8.3 Mécanismes de base de la sécurité

- **Cryptographie**

Le cryptage est la technologie utilisée pour protéger les données transmises ‹Il protège les messages échangés contre les attaques et assure la confidentialité et l'intégrité des informations grâce à des algorithmes de chiffrement ‹Il utilise principalement des clés et des codes secrets pour le chiffrement. Il existe deux types de chiffrement:

1. Chiffrement symétrique

Utilise la même clé pour chiffrer et déchiffrer le message.

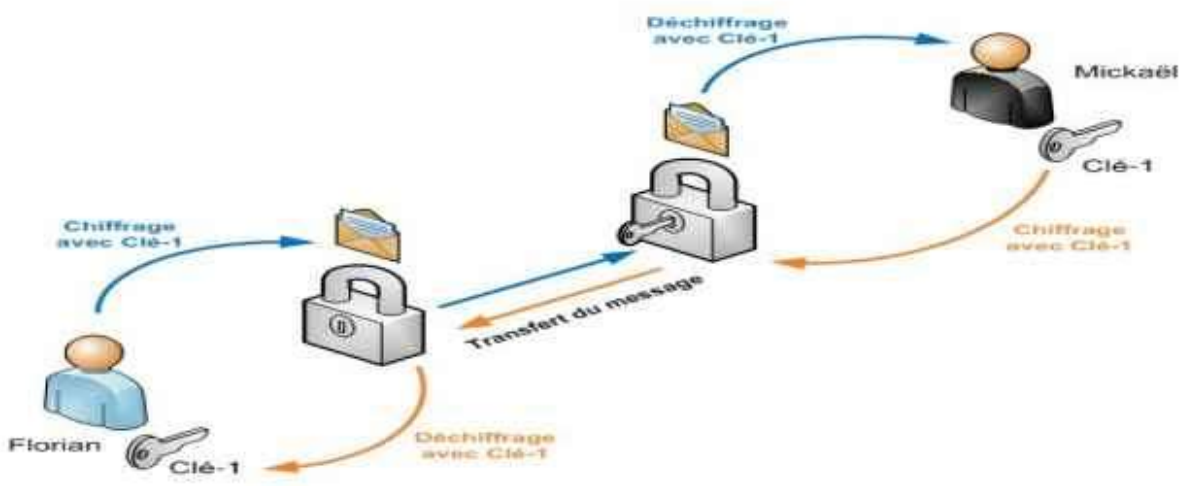

Figure 1.9: Chiffrement symétrique

2. Chiffrement asymétrique

Les clés de chiffrement est de déchiffrement sont différents, dans ce type de chiffrement on utilise une paire de clés : une clé publique pour chiffrer et une clé privée pour déchiffrer connue uniquement par le destinataire.

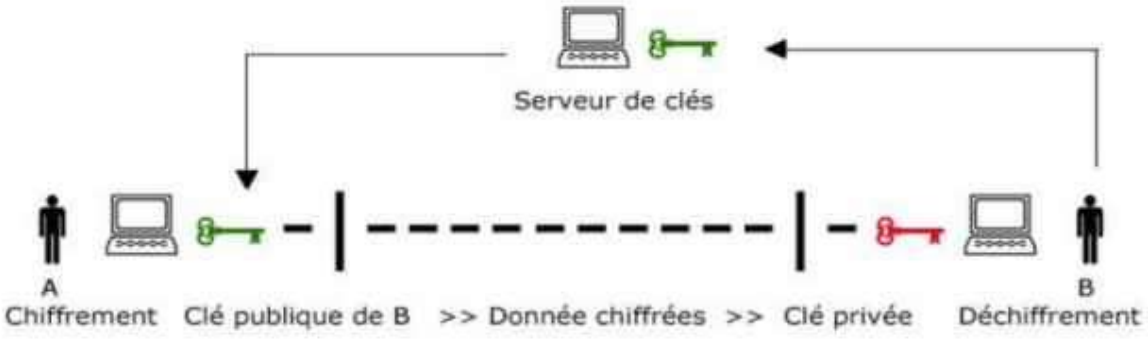

Figure 1.10: Chiffrement asymétrique

- **Le hachage**

Le hachage est le processus consistant à appliquer une fonction mathématique pour créer l'empreinte numérique d'un message en convertissant un message de taille variable en un code de taille fixe, dans le but de vérifier son authenticité ou de le stocker en toute sécurité.

- **Signature numérique**

Une signature numérique est un code numérique associé aux messages, créé par des fonctions de hachage utilisant la clé privée de la source du message, également appelée signataire du message, afin de garantir l'authenticité et l'intégrité des messages.

- **Certificats numériques**

Certificats numériques : Parmi les résultats des algorithmes de cryptage, on trouve dans le réseau VANET des certificats numériques, qui augmentent le degré de sécurité de celui-ci, prouvent l'identité du propriétaire de la clé publique et sont délivrés par l'autorité de certification.

- **MAC (Message Authentication Code)**

MAC (Message Authentication Code) : Il fait partie des mécanismes de sécurité de VANET et nécessite deux éléments d'entrée : les données à protéger et la clé secrète utilisée pour le chiffrement. Il assure essentiellement l'authentification des messages sur le réseau. Vérifiez s'il a fait l'objet de modifications.

- **TPD (tamper-proof device)**

Il s'agit d'un appareil composé de matériel et de logiciel qui contient de nombreux capteurs hautes performances. Ce dispositif permet de détruire automatiquement les informations stockées après chaque traitement du matériel, ainsi que de stocker les données du véhicule et de les garder confidentielles. Il est également responsable de signer tous les messages envoyés depuis le véhicule.

1.8.4 Architecture de sécurité pour les VANETs

En plus des recherches axées sur le développement de la couche MAC appropriée pour les VANETs, de nombreuses autres recherches accordent davantage d'attention à l'architecture de sécurité et aux protocoles de ces réseaux (tels que le consortium Car 2 Car Communication, le groupe de travail IEEE 1602.2, le projet NOW et le projet SEVCOM). Elles travaillent toutes au développement de l'environnement de sécurité VANET, toutes en utilisant l'autorité de certification (CA) et la cryptographie à clé publique. Pour protéger les messages V2V (véhicule à véhicule) et V2I (véhicule à infrastructure), le consensus est que l'utilisation d'une clé publique est la méthode à suivre pour les VANETs, principalement en raison du fait que les messages sont diffusés et que la communication est point à point. Ce n'est pas la norme, et comme les nœuds du réseau sont toujours en mouvement, le cryptage de clés symétriques nécessite des coûts élevés dans les procédures répétées de génération de clés, et c'est également difficile à mettre en œuvre en raison de leur mouvement constant. L'authentification, l'intégrité et la non-répudiation des messages, ainsi que la protection de la vie privée des utilisateurs, sont identifiées comme des exigences fondamentales dans tous les protocoles de sécurité [6].

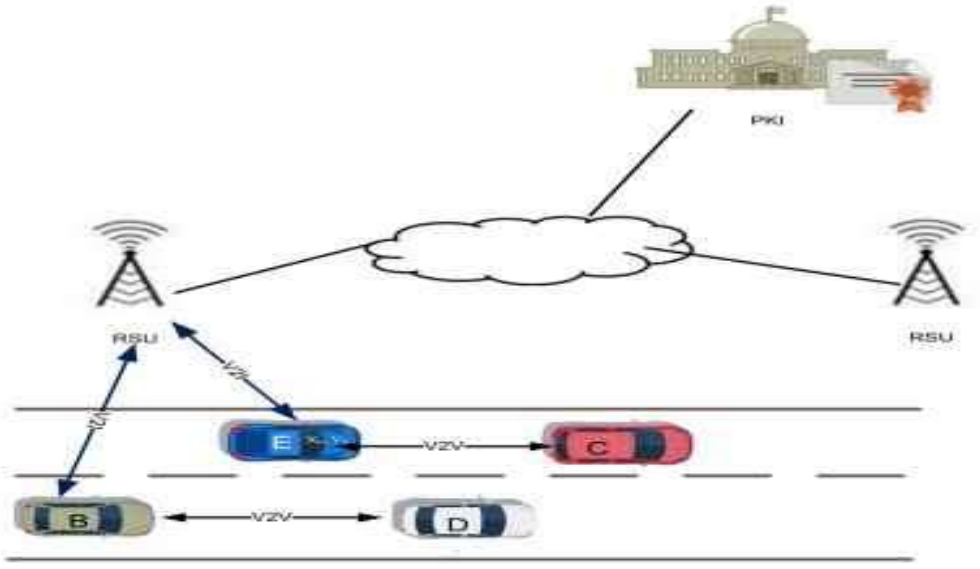

Figure 1.11 : Architecture de la sécurité VANET

1.8.4.1 L'infrastructure à clé publique PKI

Le véhicule doit être immatriculé avant de pouvoir se connecter au réseau, car les véhicules se caractérisent par un changement de région lors de leur déplacement, ce qui signifie qu'ils peuvent se trouver en dehors de leurs régions d'immatriculation, ce qui nécessite un système de gestion des clés solide et flexible. Dans les VANETs, le véhicule doit être identifié de manière unique parmi tous les autres véhicules connectés sans se connecter au serveur. Le cryptage par clé publique est plus approprié pour assurer la sécurité des communications du véhicule. C'est pourquoi il est nécessaire d'utiliser la clé publique (PKI) avec TTP qui émet et révoque les certificats. La solution appropriée est donc l'infrastructure à clé publique (PKI) avec l'autorité de certification (CA) qui est utilisée pour introduire la confiance au sein du réseau, et pour communiquer, le nœud (CA) doit être enregistré dans le centre de confiance, et une fois le processus d'enregistrement terminé, les véhicules peuvent obtenir un certificat signé avec une clé d'autorité de certification (CA), chaque participant au sein du réseau sait la clé publique de l'AC. Deux véhicules peuvent échanger leurs clés publiques et vérifier leur authenticité sans atteindre aucun nœud. Si les certificats sont valides, les véhicules peuvent se faire confiance et établir une connexion sécurisée [7].

1.8.4.2 Le standard IEEE 1609.2

Les normes de communication IEEE 1609, également connues sous le nom des protocoles Dedicated Short Range Communications (DSRC), ont récemment émergé pour améliorer le 802.11 afin de prendre en charge les communications sans fil entre les véhicules et les infrastructures routières. L'un des aspects clés abordés par la norme IEEE 1609.2 concerne les questions de sécurisation des messages WAVE, qui visent à lutter contre les écoutes clandestines, l'usurpation d'identité et autres attaques potentielles sur les messages WAVE (Wireless Access in Vehicular Environments). Le cadre de sécurité IEEE 1609.2 intègre des composants de cryptographie à clé publique basés sur les normes industrielles, avec prise en charge de la cryptographie à courbe elliptique (ECC), des formats de certificat WAVE et des méthodes cryptographiques hybrides. Ces mesures sont cruciales pour garantir des services sécurisés pour les communications WAVE, comme le montre la figure 1.12. En outre, pour faciliter les fonctions de sécurité de base telles que la révocation de certificats, l'infrastructure de sécurité doit également gérer efficacement les nécessités administratives. La révocation de certificat est essentielle pour tout système de sécurité basé sur une infrastructure à clé publique (PKI), mais n'est pas abordée dans la norme IEEE 1609.2

actuelle, notamment en ce qui concerne les caractéristiques et exigences uniques des réseaux de véhicules. De plus, la norme IEEE 1609.2 n'identifie pas le pilote et ne protège pas la confidentialité, ce qui laisse de nombreux problèmes non résolus [6].

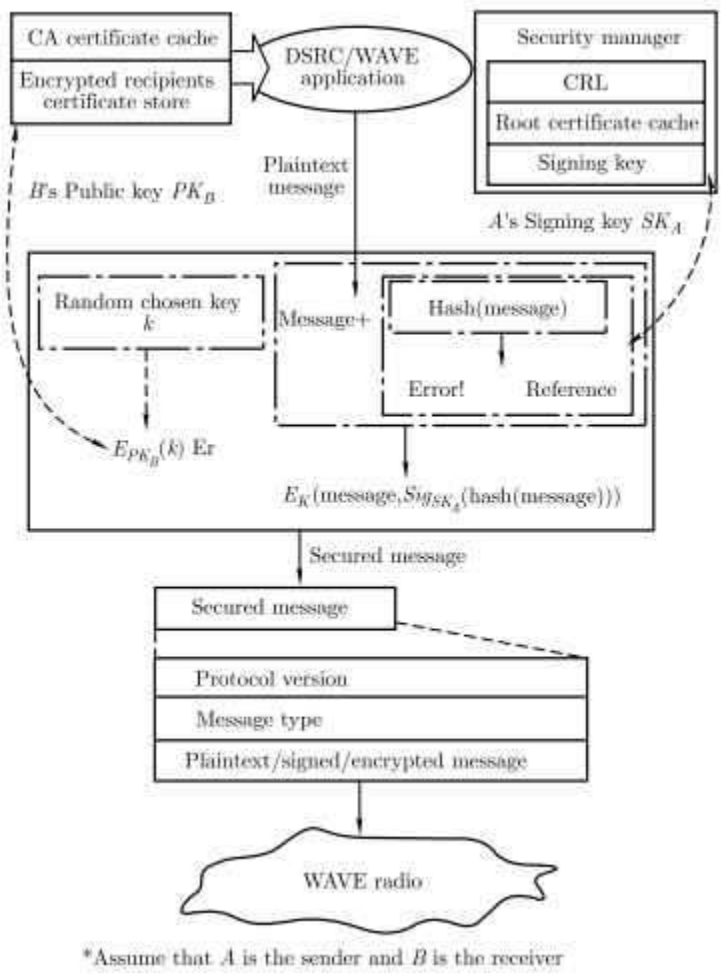

Figure 1.12 : Le cadre des services de sécurité IEE 1609.2 pour la création et l'échange des messages WAVE entre les appareils WAVE

1.8.4.3 Matériel de sécurité

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

❖ L’enregistreur de données d’événements (EDR : Event Data Recorder)

L'équipement de sécurité qui enregistre les données liées à un événement du véhicule est appelé enregistreur des données d'événement (EDR). Parfois appelée « boîte noire », elle fonctionne de la même manière que les boîtes noires des avions, enregistrant des informations importantes en cas d’accident. Cet appareil enregistre généralement des données importantes sur le véhicule telles que la vitesse, l'emplacement et d'autres informations. La plupart des véhicules modernes sont équipés d'un système EDR, bien que les exigences et les capacités varient selon les réglementations nationales et locales. Les données stockées dans un EDR peuvent être récupérées à l'aide d'un outil de diagnostic spécialisé après un accident, et ces données peuvent être utilisées dans le cadre d'une enquête sur un accident ou pour améliorer la sécurité du véhicule.

❖ Le dispositif HSM (Hardware Security Module)

Un module matériel de sécurité (HSM), également appelé dispositif inviolable (TPD), est un composant important pour garantir la sécurité des données et des clés de chiffrement. Les HSM sont conçus pour résister aux tentatives de fraude ou de piratage grâce à des mesures de sécurité physiques et logiques. Ils sont polyvalents et peuvent être utilisés pour diverses tâches de sécurité, notamment la gestion des clés de chiffrement, la vérification de l'intégrité des données, l'authentification de l'utilisateur et la signature numérique de documents. Ces appareils sont largement utilisés dans des domaines sensibles tels que les systèmes de paiement, les réseaux de communication, les systèmes de gestion des identités et des accès et d'autres applications critiques pour la sécurité. Les unités HSM sont fabriquées avec des matériaux et des techniques de fabrication qui les rendent extrêmement difficiles à s'en séparer. Il est conçu pour détecter toute tentative de falsification ou d’altération et peut effacer automatiquement les données sensibles en cas de faille de sécurité. Les modules HSM sont utilisés avec un logiciel de sécurité pour fournir une protection complète. Les clés de chiffrement et les données sensibles sont stockées dans le HSM, tandis que les opérations de chiffrement sont effectuées par le logiciel de sécurité. Cette combinaison de matériel et de logiciels offre un niveau de sécurité plus élevé que celui qui peut être obtenu en utilisant l'un ou l'autre seul. Tandis que nous utilisons des HSM pour stocker les clés privées et les certificats. Cela garantit une protection renforcée des informations, améliorant ainsi la sécurité globale du système [6].

1.9 Conclusion

Dans cette section, nous avons présenté le concept de réseau sans fil pour véhicules (VANET), ses caractéristiques distinctives et ses diverses applications. Nous avons également souligné les défis sécuritaires auxquels elle est confrontée. L'objectif principal de VANET est d'améliorer l'expérience de conduite en rendant les déplacements plus sûrs et plus interactifs pour les conducteurs et les passagers. Cependant, VANET présente des vulnérabilités en matière de confidentialité des utilisateurs et peut contribuer aux embouteillages. Il est donc nécessaire de mettre en œuvre des protocoles et des mécanismes de sécurité solides pour contrôler les interactions au sein du réseau, assurer la protection des conducteurs et renforcer la confiance des utilisateurs dans cette technologie.

Chapitre 2 : La vie privée dans les VANETs & Mécanismes de changement des pseudonymes

2.1 Introduction

Dans les dernières années, les chercheurs se sont de plus en plus recherchés dans le domaine de la sécurité des véhicules, car c'est un domaine essentiel qui nécessite une attention particulière dans tous les systèmes VANETs. La confidentialité de l'identité et de la localisation (protection de la vie privée), sont parmi les plus importants défis de sécurité dans les Réseaux Ad hoc Véhiculaires (VANETs). Mais les chercheurs ont proposé plusieurs mécanismes (comme la mise en cache, Changement des pseudonymes**,** etc.) pour éviter ces dangers.

Dans ce chapitre nous expliquons la vie privée dans les réseaux de véhicules et le compromis entre la sécurité et la vie privée, leurs exigences, les problèmes qui y sont liés, les mécanismes associés. Par la suite, nous examinons les attaques de corrélation de pseudonyme, suivies d'une analyse détaillée des schémas proposés dans la littérature.

2.2 La vie privée dans les réseaux des véhicules

La vie privée est un domaine de la protection des données qui concerne la manipulation appropriée des données sensibles [8], exactement les données personnelles et autres données confidentielles. Dans les réseaux de véhicules la vie privée est très importante par exemple, Le réseau de véhicule transmet généralement les messages sans aucune confidentialité ni sécurité, signifiant des messages non chiffrés comprenant l'identifiant du véhicule, la vitesse, la localisation du véhicule. La plupart du temps, l'identité du conducteur est associée à ces informations. De cette manière, la sécurité et la confidentialité des utilisateurs pourraient être mises en danger. L'authentification devrait être obligatoire dans les VANETs afin de préserver la vie privée des utilisateurs. Les destinataires doivent authentifier les messages provenant d'une source fiable pour maintenir l'intégrité du réseau, car les messages transmis contiennent des informations sur les événements liés à la sécurité. Par conséquent, les changements pseudonymes sont les principales sources fiables pour les solutions de

protection de la vie privée en conjonction avec le réseau de véhicule. Chaque véhicule devrait être doté des pseudonymes qui ne doivent en aucun cas être associés à l'utilisateur réel. Le pseudonyme de l'utilisateur devrait varier régulièrement pour se protéger contre tous les attaques de suivi, une garantie doit être fournie pour s'assurer que le lien avec le pseudonyme ne doit pas être établi. En cas d'exploitation sur le réseau, la véritable source doit être identifiée par l'autorité de confiance.

2.3 Le compromis entre la sécurité et la vie privée

Dans cette partie, nous abordons les problèmes entre la sécurité et la vie privée, car maintenir un équilibre entre la sécurité et la vie privée est un domaine d'importance significative. Le compromis entre la sécurité et la vie privée dans les réseaux véhiculaires (VANETs) devrait être discuté de trois manières :

Premièrement, l'authentification utilisée pour protéger les VANETs peut créer des risques pour la protection de la vie privée des utilisateurs. Grâce à l'authentification, le réseau connaît précisément l'emplacement exact d'un utilisateur particulier à un moment donné pour garantir que la TTP (Third Trusted Party) puisse intervenir en cas de problème. Cependant, certains conducteurs pourraient ne pas vouloir être surveillés par la TTP (Third Trusted Party) car cela semble violer la vie privée des conducteurs.

Deuxièmement, des nombreux protocoles de confidentialité augmentent le niveau de vie privée au détriment des coûts de sécurité. Par exemple, des chercheurs dans le domaine ont utilisé l'accès aléatoire hors ligne pour atteindre la non-connectivité. Cependant, la durée pendant laquelle des messages texte traditionnels peuvent être envoyés en centaines de millisecondes ne peut pas être garantie. Augmenter la période de silence aléatoire prolonge la durée des messages de sécurité.

Troisièmement, la Liste de Révocation de Certificat (CRL) est la méthode traditionnelle pour annuler les nœuds malveillants. En raison de la taille des VANETs, il est nécessaire une grande quantité d'espace de stockage. Des chercheurs ont proposé plusieurs autres mécanismes d'annulation qui utilisent des stratégies de stockage ainsi que des techniques de hachage pour accroître l'accès aux services neutres. Cependant, le processus de vérification

de l'état du certificat est plus susceptible de révéler les informations de la vie privée de l'utilisateur que la méthode traditionnelle de la CRL.

2.4 Exigences de La vie privée dans (VANET)

A. La vie privée et anonymat

La communication des véhicules (VC) ne devrait pas révéler des données personnelles, confidentielles et privées de leurs utilisateurs. Les spectateurs ne devraient pas connaître les activités futures des autres véhicules. L'anonymat une exigence importante pour tous les véhicules dans les réseaux de communication entre véhicules.

B. authentification d'entité

Les destinataires ne sont pas seulement assurés que l'expéditeur a créé un message, Mais ils ont aussi une preuve de l'activité de l'expéditeur. Cette exigence est obligatoire pour la protection la vie privée.

C. Confidentialité du message

Les détails des messages pendant la communication sont protégés avec les véhicules qui ne font pas partie de la communication et n'ont pas l'autorité pour-il accédé.

D. Non traçabilité

Il faut interdire toute liaison possible entre deux messages transmis par un même véhicule, Cette vulnérabilité devient facile à exploiter pour les attaquants.

2.5 Les problèmes liés à la protection de la vie privée

2.5.1 Dévoiler une identité

Ce problème est une menace très danger sur la vie privée des conducteurs. Cette attaque vise à obtenir des informations privées ou personnelles, Il a des conséquences futures graves sur la sécurité de la vie privée des conducteurs. Pour prévenir ce type de problème, il est important d'utiliser des mécanismes d'authentification et de préservation de la confidentialité dans les communications VANET.

2.5.2 Suivi de la localisation

Dans ce problème les véhicules communiquent entre eux pour partager des informations sur leur localisation, par exemple dans le cas de la prévention des collisions ou la gestion du trafic. Dans ce cas représenter un risque pour la vie privée si les données de localisation sont mal utilisées ou divulguées. Et donc il faut de prendre des mesures appropriées pour garantir la confidentialité des informations de localisation des véhicules (pseudonymes temporaires, la cryptographie pour la protection et sécuriser les messages de localisation).

2.6 Les mécanismes

Il existe de nombreux mécanismes pour la protection de la vie privée dans les réseaux véhiculaires (VANETs). Dans cette partie, nous les expliquons et à travers cela, nous clarifions le mécanisme approprié dans ce cas. Nous continuons l'explication dans le chapitre suivant.

2.6.1 La mise en cache

La stratégie de la mise en cache ou (caching en anglais) peut jouer un rôle important dans l'amélioration de l'efficacité du réseau et la réduction de la latence de communication dans les réseaux véhiculaires. Ce processus de cette stratégie consiste à stocker localement des contenus (c'est-à-dire le contenu fréquemment demandé par les conducteurs) dans des caches (des espaces mémoires), de publier sur des nœuds physiquement proches de conducteur (stations de base cellulaires comme RSU, véhicules, etc.).

2.6.2 La perturbation

Cette technique vise à perturber les informations en ajoutant du bruit, que ce soit en envoyant informations (type des informations sont générales) ou en les combinant avec des données fausses. Ce type de méthode est principalement utilisé pour maintenir la confidentialité de la localisation, mais il n'est pas spécifiquement conçu pour être utilisé dans les systèmes de sécurité coopératifs.

2.6.3 L’approche de Changement des pseudonymes

Le pseudonyme est l'une des solutions pour résoudre le problème de la vie privée exactement (la confidentialité) dans les réseaux des (VANETs). Le terme de pseudonyme a

été proposé pour la première fois dans [9]. C'est une identifiant unique utilisé pour authentifier les messages de l'émetteur. Il remplace le nom réel lors des échanges entre l'émetteur et le récepteur. Son objectif est de contrer les attaques qui consistent à falsifier la communication entre l'émetteur et le récepteur, ainsi que de surveiller si la communication a lieu entre l'émetteur et le récepteur. Les caractéristiques du changement des pseudonymes consistent la restriction à intervalle de pseudonymes pour chaque véhicule, l'unicité, l'opportunité et la fréquence d'échange de pseudonymes [10].

Le mécanisme fondamental de cette approche consiste à briser les connexions entre l'identité et les messages spécialement du véhicule, tout en éliminant également les liens entre les messages émanant d'un même véhicule. Et aussi il préserve l'intégrité des données de localisation dans les messages transmis, Ces messages reposent sur les services d'authentification (des messages authentifier). Cette technique s'avère particulièrement adaptée aux applications de sécurité.

Nous choisissons cette technique (changement des pseudonymes) dans notre travail car elle représente la meilleure approche pour la protection de la vie privée dans les réseaux véhiculaires (VANETs), et nous expliquerons en détail son schéma dans les parties suivantes.

2.7 Mécanismes de changement des pseudonymes

2.7.1 Attaque de corrélation de pseudonymes

L'idée d'utiliser des pseudonymes au lieu des identités réelles des véhicules a été confrontée à des défis importants, car un adversaire peut facilement retracer l'association des emplacements d'alias à des véhicules spécifiques. Il existe plusieurs types d'attaques, Tels que l'attaque de lien par alias unique, l'attaque de lien syntaxique, l'attaque de lien sémantique, etc.

a) Liaison de pseudonyme unique

L'utilisation d'un seul pseudonyme ne suffit pas à garantir l'anonymat des identités des véhicules face à tout adversaire. Par exemple, les habitudes de déplacement peuvent être liées à un véhicule, commençant et se terminant au même endroit les jours de travail, ou au

domicile d'un individu. Pour mieux illustrer les problèmes associés à l'utilisation d'un alias unique, un scénario est présenté à la figure **2.1** dans lequel le véhicule A utilisé « z1 » comme alias pour ses messages de balise. Au temps t0, la voiture émet une surveillance des angles morts (BSM) avec les données suivantes : {identité : z1, localisation : x1, y1, vitesse : s1, direction : d1}. Après un certain temps t0 + Δt, le même véhicule diffuse un autre message de balise avec les données suivantes : {identité : z1, localisation : x2, y2, vitesse : s2, direction : d1}. Un adversaire peut déduire que ces deux messages proviennent de la même entité en utilisant l'alias z1. Ainsi, un seul pseudonyme ne peut garantir la confidentialité de la localisation d'un utilisateur si celui-ci est surveillé à différents moments. Il est recommandé d'utiliser plusieurs alias tout au long du parcours plutôt qu'un seul. L'idée principale était de changer les alias à intervalles réguliers pour contrecarrer les tentatives de suivi, une proposition qui a également été approuvée par la norme de sécurité actuelle pour les VANET, IEEE 1609.2 [11].

Figure 2.1 : Le problème du pseudonyme unique

b) Liaison syntaxique

La figure **2.2** illustre la liaison syntaxique pour l'état des pseudonymes. Si une seule voiture change son pseudonyme (de B1 à B2) parmi les trois véhicules pendant la période Δt, l'adversaire peut facilement relier les deux pseudonymes B1 et B2. Une protection contre ce type d'attaques peut être mise en place en utilisant un mécanisme de synchronisation des changements de pseudonymes entre les véhicules [12].

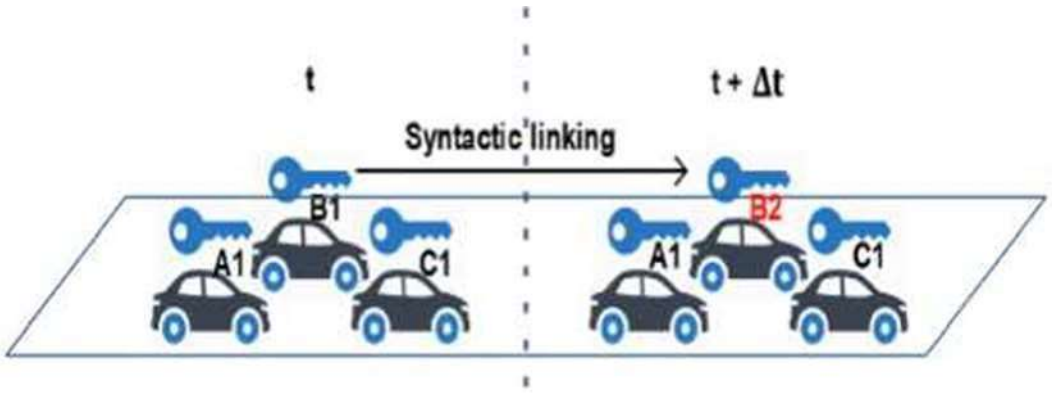

Figure 2.2 : La liaison syntaxique des pseudonymes

c) Liaison sémantique

La simple méthode de changement d'alias de manière synchrone ne suffit pas. Un adversaire peut collecter l'identité et la localisation et les utiliser pour prédire la prochaine localisation d'un véhicule dans une période de temps donnée grâce à des trajectoires fixes. On constate que l'adversaire est toujours capable d'établir une connexion entre le nouvel alias et le précédent en utilisant des informations temporelles et spatiales. Par exemple, si des véhicules portant les alias A et B diffusent des messages de sécurité de base contenant respectivement les emplacements Al0 et Bl0, à l'instant t0, l'adversaire peut prédire qu'après une période de temps t0+, les véhicules A et B se trouveront aux emplacements Al0 + et Bl0+ respectivement comme le montre la figure **2.3**. Ce type d'attaque peut être évité en empêchant l'adversaire d'écouter les messages de sécurité de base (BSM) pendant un certain temps [13].

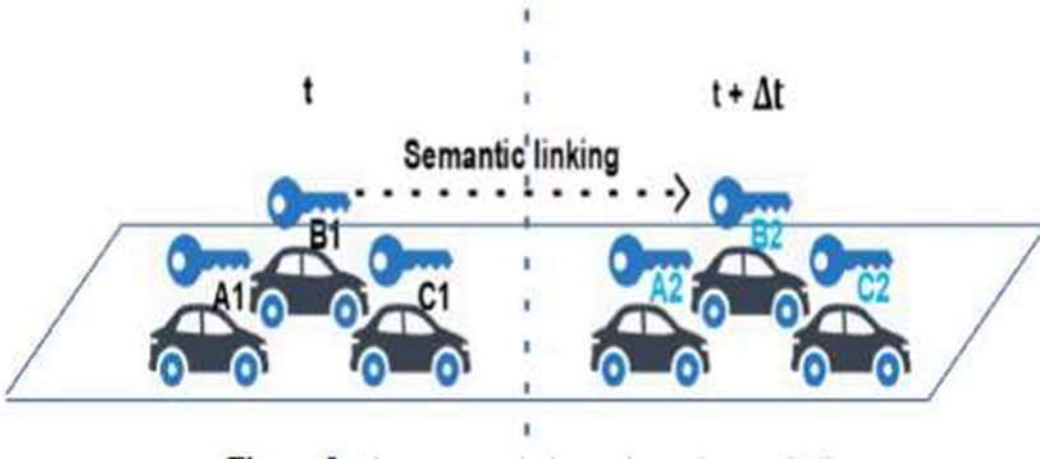

Figure 2.3 : La liaison sémantique des pseudonymes

d) Attaque Sybil

Attaque Sybil au sein d'un réseau des véhicules. Un acteur malveillant exploite les vulnérabilités en envoyant plusieurs messages pour créer l'illusion des plusieurs véhicules signalant le même événement, comme un accident ou un embouteillage. Cette tactique vise à inciter les véhicules voisins à changer de trajectoire afin de réaliser un gain personnel [14].

e) Attaque d'usurpation

Il s'agit d'une attaque par usurpation d'identité, ce qui signifie que l'attaquant tente de voler l'identité d'origine d'une personne et de l'utiliser pour envoyer de faux messages à d'autres véhicules et nœuds distants.

f) Fausse alerte d'attaque

Une attaque par fausse alarme est une tactique utilisée par des attaquants malveillants dans le but d'induire en erreur les autres véhicules. Cette alarme peut être liée à des blocages routiers, des accidents, etc. Si d'autres entités ne parviennent pas à détecter l'attaque, elles prennent des décisions basées sur cet avertissement. Cela peut perturber le système ou causer des dommages ou un manque de confiance.

2.7.2 Pseudonymes et Certificats

L'authentification est un mécanisme important pour déterminer l'origine de tout message ou comportement au sein d'un réseau automobile. Une identification précise des utilisateurs est essentielle pour que l'autorité puisse gérer efficacement les événements et protéger le réseau ainsi que les utilisateurs contre les intrusions. Pour inciter les gens à investir dans un tel système, les propriétaires des véhicules préfèrent souvent ne pas divulguer leurs informations personnelles. Cette préférence pose un défi majeur aux systèmes de transport intelligents : ils doivent disposer d'un nombre suffisant des véhicules immatriculés pour fonctionner correctement tout en assurant l'authentification des véhicules immatriculés et en protégeant les données personnelles de leurs utilisateurs. Il ne suffit pas d'utiliser un seul pseudonyme à la place de la véritable identité, car l'attaquant peut relier les traces de la localisation du véhicule et découvrir l'identité de sa cible. Pour résoudre ce problème, chaque véhicule immatriculé se voit attribuer un ensemble d'alias approuvés par l'autorité de confiance ainsi qu'une clé privée correspondant à chaque certificat, en plus de sa véritable identité. La voiture choisit alors un alias dans sa liste et signe ses messages avec la clé privée correspondante, gardant ainsi secrète son identité personnelle. Seule une autorité de confiance peut relier le pseudonyme utilisé par le véhicule à sa véritable identité. Il est important que le changement d'alias soit effectué avec soin, car un attaquant peut associer les certificats et les alias pour retracer ultérieurement le trajet du véhicule. La littérature propose diverses méthodes pour déterminer le moment et le lieu optimaux pour effectuer ce changement de surnom en toute sécurité.

2.7.3 Schémas proposés dans la littérature

Un certain nombre de schémas de pseudonyme ont été proposés pour améliorer l'anonymat des conducteurs en les protégeant contre les attaques de liage des pseudonymes. Un pseudonyme est une identité fictive utilisée par les véhicules à la place de leur véritable identité. Les systèmes de changement de pseudonyme fonctionnent sur le principe du changement répété des fausses identités. Ces programmes peuvent être classés en formations de groupe, en emplacement fixe, centrés sur le véhicule et coopératifs, comme le montre la figure **2.4**.

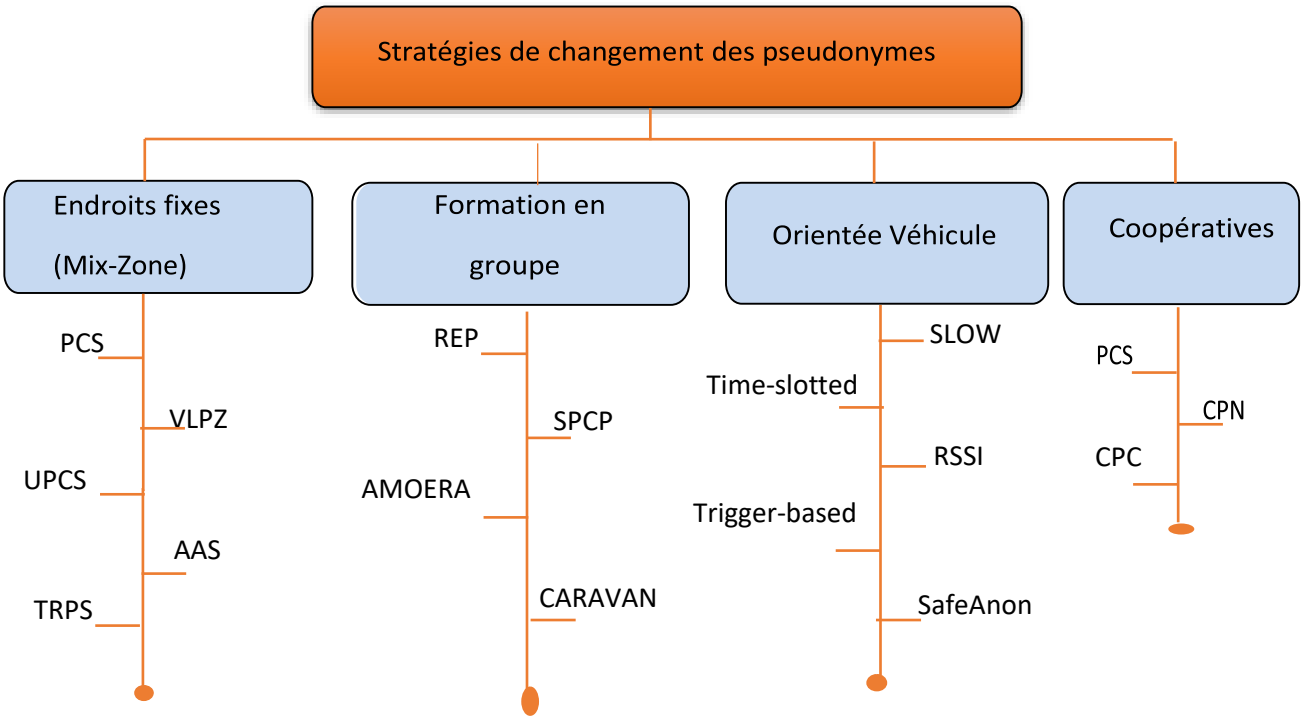

Figure 2.4 : Taxonomie des stratégies de changement des pseudonymes [4]

2.7.3.1 Formation en groupe

Dans la recherche, le schéma REP (Random Encryption Period) propose un nouveau protocole de communication de groupe qui adopte la distribution de probabilité des clés. Chaque OBU change périodiquement son pseudo-ID en déclenchant une requête REP vers les véhicules voisins. REP garantit l'anonymat des utilisateurs et la confidentialité de leur localisation, même si la charge de stockage sur l'OBU entraîne le problème d'une consommation élevée des ressources.

Un autre schéma, AMOEBA, consiste en une combinaison de composés et une période de silence aléatoire. Les composites élisent un chef de groupe (GL) qui communique au nom des membres du groupe. A ce moment, les véhicules restent silencieux pendant une durée aléatoire. Le système garantit la confidentialité de l'emplacement pour les membres du groupe, mais met en danger la vie privée du chef du groupe.

CARAVAN combine également une période de silence aléatoire avec la formation des groupes des véhicules.

Le concept MixGroup est introduit par l'échange des titres entre véhicules de la zone groupe. L'identifiant de groupe (TID) est utilisé pour envoyer des messages lors de la procédure d'échange d'alias. Une fois que la voiture rencontre d'autres membres du groupe aux intersections routières, elle diffuse une demande d'échange d'alias avec l'aide du RSU.

Un protocole appelé « Synchronous Pseudonym Change Protocol (SPCP) » a également été introduit pour éviter le suivi des véhicules sans compromettre leur sécurité. Le protocole suggère de former un groupe de composés avant de changer d'alias. La voiture crée un groupe s'il n'y a pas de groupe à proximité et attribue une nouvelle clé secrète de groupe et une nouvelle clé publique de groupe aux membres du groupe pour la communication. Le chef de groupe conserve une trace du sur nom et de la clé secrète qui lui sont attribués. Dans un groupe, toutes les communications se font via la clé publique du groupe, ce qui protège la source du message.

SPCP protège les membres du groupe contre le suivi. Il prévoit également une confidentialité conditionnée à la coopération entre le CA et le chef du groupe même après la dissolution du groupe. Cependant, le chef de groupe supporte des frais de stockage supplémentaires dus au maintien de la correspondance entre la clé secrète des membres du groupe et leurs pseudonymes [14].

2.7.3.2 Endroits fixes

Le véhicule réside dans la VLPZ (Zone de Protection de Vie Privée Virtuelle) pendant une durée aléatoire et change d'alias avant d'en sortir. Cela facilite l'association sémantique et syntaxique des alias. La confusion des voies est un autre type de zone mixte, dans laquelle deux usagers changent de sur nom lorsqu'ils s'arrêtent à une intersection. En quittant l'intersection, le service de localisation confond les trajectoires des deux véhicules pour tromper les adversaires potentiels, garantissant ainsi la confidentialité de la localisation.

La stratégie silence-et-échange-à-l 'intersection signalée (S2SI) et la stratégie UPCS ont été proposées. Dans un premier temps, les véhicules créent des zones de mixage silencieuses lorsque les feux de circulation passent au rouge, puis échangent des alias à l'aide

de RSU (Unités de Service Routier). Cela réduit le nombre d'alias utilisés et réduit les coûts de stockage. Cependant, le véhicule peut être suivi s'il n'y a pas de point d'intersection.

Les chercheurs ont proposé un système de publicité anonyme (AAS) pour obtenir les conditions de circulation tout en garantissant la confidentialité. Les entités concernées comprennent les émetteurs de systèmes, les bornes de recharge et les véhicules. Les bornes de recharge, en tant qu'entités de confiance, délivrent un jeton à chaque véhicule à son arrivée. Les véhicules utilisent ce jeton pour signer des messages de rapport sur l'état du trafic, la précision des messages étant déterminée sur la base d'un indice de précision prenant en compte les différences de localisation et d'heure entre les bornes de recharge précédemment visitées, les incidents signalés et les messages reçus.

Le vérificateur attend que les messages signalés atteignent un seuil prédéfini, garantissant ainsi l'authenticité et la confidentialité. Cependant, les messages envoyés par un même véhicule entre les bornes de recharge sont connectables, et le critère d'annulation n'est pas prévu dans le schéma AAS.

Dans une autre proposition, un plan efficace pour modifier et gérer les pseudonymes à l'aide de l'infrastructure a été présenté. Les véhicules deviennent silencieux dans les zones de confidentialité et changent de pseudonyme pour induire les attaquants en erreur. Le système de réputation incite les véhicules à remplir les zones de confidentialité afin de maximiser la taille du pool d'anonymat, ce qui améliore les performances du système. Cependant, l'anonymat n'est assuré que dans les zones de confidentialité et l'installation d'autorités de confiance (TA) supplémentaires coûte cher. De plus, une surcharge de calcul est occasionnée lors de l'exécution du système de réputation pour chaque véhicule qui traverse la zone de confidentialité.

Il a également proposé un système des pseudonymes résistant aux traces (TRPS) basé sur des signatures dynamiques avec des pseudonymes spécifiques à un domaine. Lorsqu'un véhicule entre dans une zone, le RSU lui attribue une clé publique correspondante et le véhicule calcule un alias unique. Lors de l'envoi d'un message, si l'alias figure sur la liste de révocation, le message sera rejeté, ce qui évite d'avoir à stocker un ensemble d'alias approuvés [14].

2.7.3.3 Orientée Véhicule

Un système appelé SLOW (Low Speed Silence) a été proposé, qui s'active lorsque la vitesse du véhicule descend en dessous d'un certain seuil, changeant ainsi son pseudonyme Bien que cette approche soit simple, elle entraîne une surcharge due aux mises à jour des alias dans les zones très fréquentées. Les composés peuvent échanger des alias avant utilisation, ce qui réduit les coûts de stockage et de calcul et garantit que les alias ne peuvent pas être liés. Cependant, ce système est limité aux messages importants non liés à la sécurité. Dans un autre article, ils ont proposé un système de confidentialité basé sur l'opérateur pour VANET, comprenant des autorités de certification (CA), des unités de route (RSU) et des véhicules. L'AC attribue un alias à chaque véhicule et maintient une base des données mappant les alias avec des identités réelles. Lorsqu'une condition de déclenchement est exécutée (par exemple, deux véhicules se dirigent vers la même zone avec des différences minimes de position et de vitesse), le véhicule demande un échange d'alias via le RSU, qui transmet la demande au AC pour authentification et mise à jour de la base des données. Cela réduit la surcharge de stockage mais augmente la surcharge de communication. Le système SafeAnon bloque périodiquement la localisation et la vitesse, trompant les adversaires, tout en assurant la sécurité en diffusant des messages d'avertissement lorsque les véhicules violent les distances de sécurité. Cependant, l'installation du radar et la charge de calcul requise pour calculer les emplacements d'origine posent des problèmes. Un système basé sur la génération de valeurs pseudo-aléatoires trompe les attaquants en calculant et en diffusant de fausses localisations par rapport aux véhicules à proximité. Bien que ce schéma soit simple et indépendant de l'infrastructure, il impose des charges de calcul élevées et peut compromettre l'intégrité des VANET [14].

2.7.3.4 Coopératives

Les auteurs ont proposé un schéma de changement synchrone de pseudonyme (PSC). Le RSU surveille la densité des véhicules à proximité et la diffuse périodiquement. Lorsque la densité des véhicules est égale ou supérieure à un seuil prédéfini, les véhicules changent d'alias de manière synchrone. Cette approche offre des avantages tels qu'un temps de calcul réduit, l'anonymat et la confidentialité de la localisation. Cependant, cela peut entraîner des

embouteillages lorsque plusieurs véhicules à proximité demandent à changer de pseudonyme en même temps.

Dans le système TAPCS, le véhicule de détection de congestion initie une zone de mixage silencieuse. Les véhicules dans cette zone deviennent silencieux et mettent à jour leurs alias. Si la vitesse du démarreur dépasse un certain seuil, il diffuse un message de fin d'embouteillage aux autres véhicules. Bien que cela améliore la confidentialité de l'emplacement dans les zones très fréquentées, il est toujours possible de suivre les véhicules dans les zones peu fréquentées.

Le schéma de changement de pseudonyme coopératif (CPC) vise à répondre aux limites des schémas de changement d'alias asynchrones. Les véhicules changent de pseudonyme lorsqu'un nombre spécifié de véhicules à proximité est détecté. Ce comportement coopératif améliore l'anonymat dans les scénarios de trafic élevé. Cependant, un trafic dispersé sur des routes unidimensionnelles, telles que les autoroutes, peut conduire à l'incapacité de remplir les conditions d'exécution, réduisant ainsi la possibilité d'anonymat.

Les auteurs abordent le problème du faible anonymat dans les schémas de changement de pseudonyme basés sur des déclencheurs en introduisant un mécanisme de déclenchement coopératif. Les véhicules surveillent en permanence le nombre de véhicules à proximité et activent le drapeau de disponibilité en conséquence. Si ReadyFlag est défini sur 1, les véhicules changent de pseudonyme au cours de la période suivante avec leurs voisins, favorisant ainsi les changements des pseudonymes coopératifs. Bien que ce schéma soit simple et exécutable sans support d'infrastructure, des changements de pseudonyme fréquents en cas de trafic intense peuvent entraîner une surcharge de calcul.

Le système de gestion de la confiance (RaBTM) est basé sur des messages de balise et des RSU. RaBTM utilise des pseudonymes pour diffuser des messages de sécurité de base (BSM) et maintient un modèle de confiance pour chaque véhicule. Il évalue la fiabilité des événements signalés en comparant les emplacements dans les BSM avec les emplacements des événements signalés, avec l'aide du RSU. Bien que ce schéma protège principalement contre les attaques de changement et les faux messages, il lui manque une description détaillée du schéma d'alias.

Un mécanisme qui collecte des pseudonymes synchrones avec des périodes de temps spécifiques a également été proposé pour maintenir la confidentialité et l'intégrité dans les VANET. Chaque véhicule possède un ensemble d'alias obtenus auprès d'une autorité de certification (CA) sur la base d'un identifiant de base. Avec les horloges synchrones, les véhicules changent d'alias de manière synchrone. Pour éviter toute confusion lors de situations critiques, les anciens alias sont utilisés aux côtés des nouveaux, et le mécanisme de révocation garantit une confidentialité conditionnelle. Cependant, le mécanisme de détection des cas critiques n'est pas abordé. Un large éventail de surnoms peut également augmenter les coûts de stockage des voitures électriques.

En résumé, différents systèmes ont été proposés pour répondre aux problèmes de confidentialité dans les VANETs, et chacun présente des avantages et des inconvénients. Les systèmes coopératifs offrent une plus grande confidentialité dans les scénarios de trafic intense, mais peuvent manquer de protection de la vie privée dans les situations de faible densité [14].

2.8 Conclusion

En conclusion, la sécurité des véhicules, notamment dans les réseaux VANETs, demeure une préoccupation centrale pour les chercheurs. Le défi principal réside dans le maintien de la confidentialité des utilisateurs, en garantissant la protection de leur identité et de leurs données personnelles. Pour relever ces défis, les chercheurs ont proposé divers mécanismes, tels que la mise en cache et le pseudonyme, afin de renforcer la protection de la vie privée. Ce chapitre explore en profondeur ces concepts et examine également les attaques visant les liens entre les pseudonymes. En résumé, ce chapitre offre un aperçu approfondi de la sécurité et de la vie privée dans les réseaux VANET, ainsi que des solutions actuelles et des pistes potentielles pour les améliorer.

Chapitre 03 : Contribution

3.1 Introduction

Dans cette section nous clarifions l'idée de base sur CPN et faire leur simulation, La simulation est une technique qui consiste à utiliser différents modèles de validation les plus fréquemment utilisés pour tester des propositions dans le domaine des réseaux. Dans ce chapitre, nous discutons de l'environnement de simulation (les outils de simulation) utilisé pour notre contribution. Ensuite, nous expliquons et analysons les résultats des simulations de notre proposition, puis nous les comparons à d'autres schémas existants proposés par le simulateur.

3.2 L'idée de base

Parmi les schémas mis en œuvre par Prext pour préserver la confidentialité, nous avons les protocoles SLOW et CPN :

❖ Protocole SLOW :

SLOW est un schéma conçu pour changer les pseudonymes pratique pour la confidentialité de l'emplacement dans les réseaux ad hoc véhiculaires (VANETs). Cette approche repose sur le principe selon lequel les véhicules ne transmettent aucun message lorsque leur vitesse passe en dessous d'un seuil défini comme « Vs », et ils changent ensuite tous leurs pseudonymes après ces périodes de silence. Le nom « SLOW » est l'acronyme de « silence at low speeds ».

Le fonctionnement de « SLOW » consiste à définir un seuil de vitesse, par exemple « Vs = 30 km/h », puis à arrêter le véhicule d'émettre tout message contenant des données de localisation ou d'autres informations lorsque sa vitesse est inférieure à « Vs ». Si le véhicule ne transmet aucun message pendant une certaine période, il effectue ensuite un changement de pseudonymes avant sa prochaine transmission.

En résumé SLOW est un schéma efficace visant à améliorer la confidentialité de l'emplacement en utilisant des périodes de silence et des changements de pseudonymes lorsque la vitesse est faible, tout en réduisant les exigences matérielles des (OBU) [18].

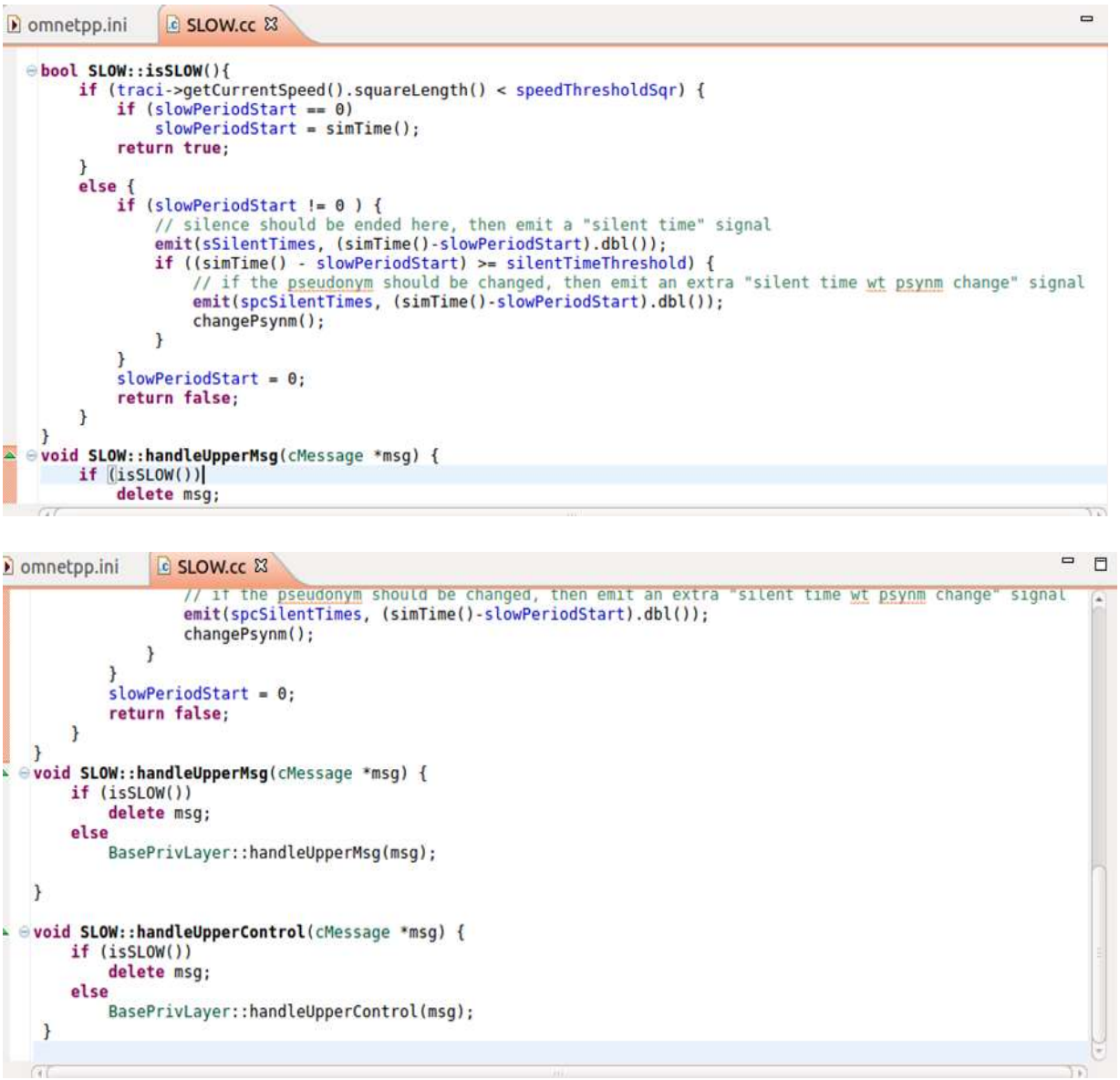

Figure 3.1 : Les parties du code de slow

❖ Protocole CPN

Le schéma CPN (Cooperative Pseudonym Change) fonctionne en changeant l'identité attribuée à chaque véhicule dans le réseau, en se basant sur le nombre de véhicules voisins dans une plage spécifique. Chaque véhicule doit vérifier le nombre de ses voisins, c'est-à-dire les véhicules adjacents, dans une un rayon appelée R. Si le nombre de voisins atteint un seuil spécifique appelé K, le véhicule change l'état ’un paramètre interne appelée "ReadyFlag". Ensuite, le véhicule envoie un message de type "beacon" contenant le "ReadyFlag", puis il fait un changement de pseudonyme dans la diffusion suivante du beacon. Lorsqu'un véhicule reçoit un "beacon" avec un changement de "ReadyFlag", il change immédiatement son identité, même s'il n'a pas atteint le seuil K de véhicules voisins [19].

Ce schéma contribue à changer les pseudonymes de manière coopérative entre les véhicules voisins, renforçant ainsi la confidentialité et réduisant le suivi.

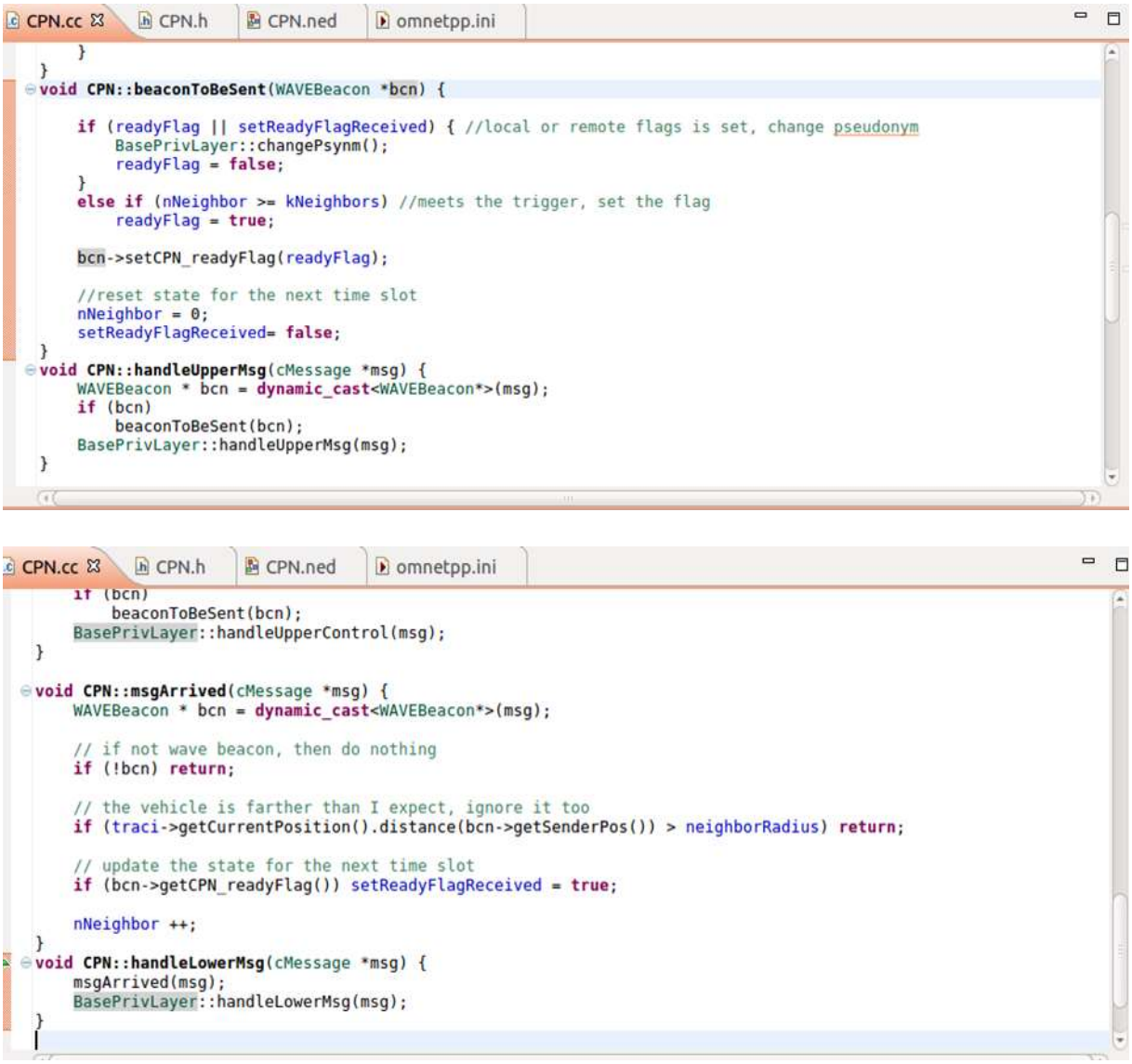

Figure 3.2 : Les parties du code de CPN

3.3 Hybridation de deux schémas

3.3.1 Notre organigramme

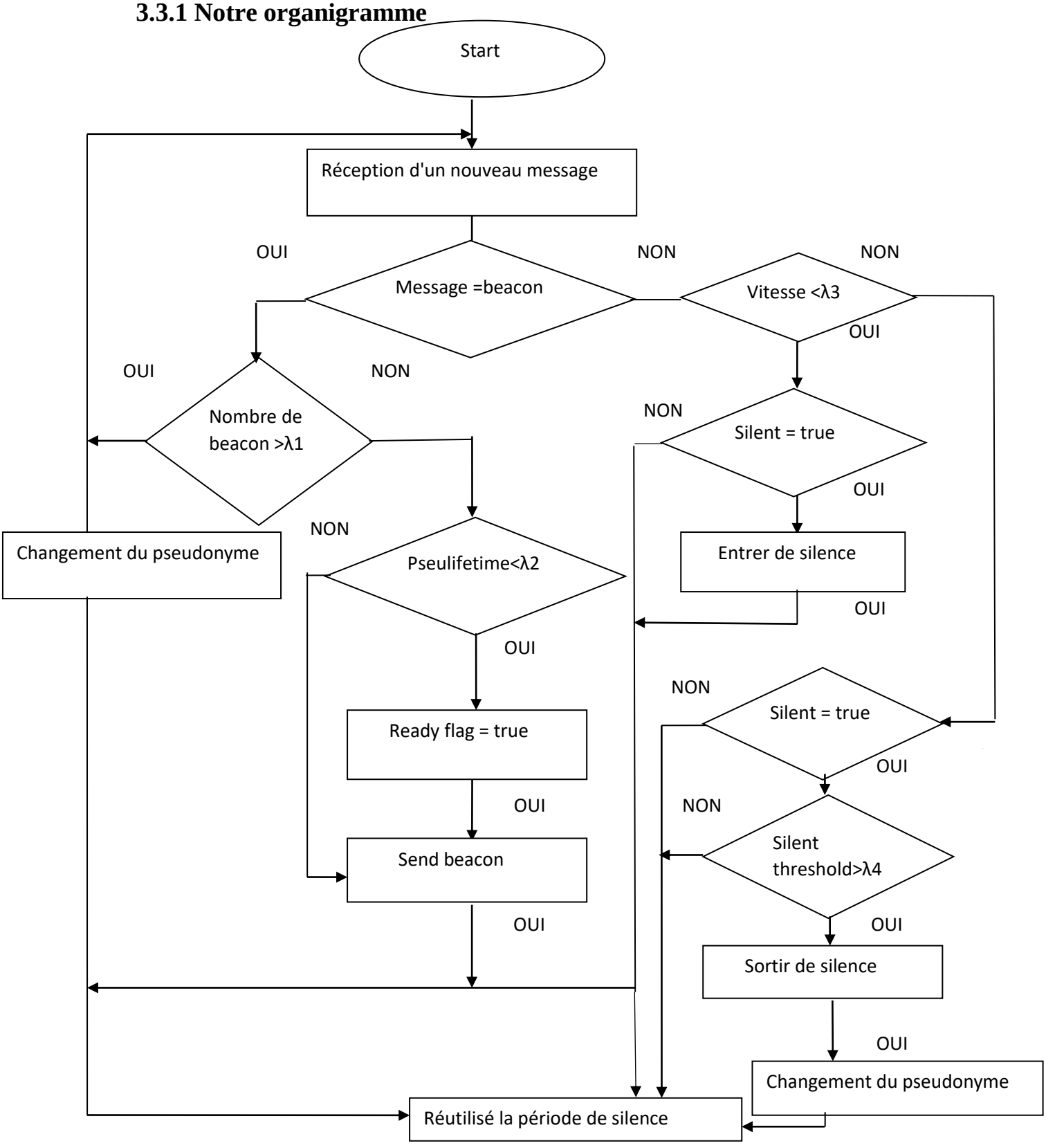

Figure : Organigramme d'E_SLOW

Au début, chaque véhicule s'enregistre auprès de l'autorité de confiance. L'autorité de confiance lui fournit un lot de pseudonymes pour l'utiliser plus tard lors de la signature des messages.

Après avoir enregistré, lorsqu'un véhicule reçoit un message de contrôle (Beacon), il procède à différentes vérifications. Dans le premier cas, il vérifie si le nombre de voisins dépasse le seuil. Si c'est le cas, il procède au changement de pseudonyme, sinon il vérifie si sa condition de temps de vie du pseudonyme (pseulifetime) est achevée. Dans le cas où cette durée de vie est achevée il prépare un nouveau beacon avec un flag appelé Read flag à true dans tous ses prochaines beacons jusqu'à ce qu'il change pseudonyme.

Dans le Deuxième cas, lorsqu'il s'agit de messages qui ne sont pas des beacon. Dans ce cas le véhicule vérifie sa vitesse. Si celle-ci est inférieure à un seuil en dès que le véhicule en un état slow cette situation identique appelé de schéma slow d'origine. Dans ce cas la si silence à true il entre en mode de silence, sinon il ne fait rien. Notre cas si la vitesse supérieure à seuil il vérifie s'il est en mode de silence si oui il vérifie si la période de silence autorisé est achevée donc il sort de mode de silence si non reste dans leur mode silence et change son pseudonyme une fois la période de silence est achevé.

Cette organigramme assurer une gestion dynamique des communications et des périodes de silence pour optimiser les transmissions et la sécurité du réseau.

3.4 Environments de travail

3.4.1 OMNET++

OMNET++signifie "Objective Modular Network Testbed in C++" est une bibliothèque de simulation C++ qui est extensible, modulaire et basée sur des composants, utilisé pour la modélisation et la simulation de réseaux de communication, de protocoles, des applications de sécurité dans les réseaux sans fil. Dans ce projet nous utilisons la version OMNET++ 5.0.

3.4.2 SUMO « Simulation of Urban MObility »

Dans notre projet, nous utilisons la version 0.25.0 de SUMO, est une simulation de trafic open source, Elle permet de simuler comment une demande de trafic donnée, composée de véhicules individuels, se déplace à travers un réseau routier donné. La simulation permet d'aborder un large éventail de sujets liés à la gestion du trafic. Chaque véhicule est modélisé de manière explicite, possède son propre itinéraire et se déplace individuellement à travers le réseau.

Figure 3.3 : Catre géographique du centre-ville de Munich

Nous avons utilisé une carte géographique du centre-ville de Munich, d'une taille de 2,67 km sur 2,8 km, comme illustré dans la Figure. Cette carte a été obtenue à partir d'OpenStreetMap puis convertie en un réseau SUMO à l'aide des outils netconvert et polyconvert inclus dans SUMO 0.25.0 [15].

3.3.3 Veins "Vehicles in Network Simulation"

Veins est un Framework open source pour exécuter des simulations de réseaux véhiculaires [16]. Il s'appuie sur deux simulateurs : OMNET++, un simulateur de réseau basé sur des événements, et SUMO, un simulateur de trafic routier. Il étend ces simulateurs pour offrir une

suite complète de modèles pour la simulation de la communication inter-véhiculaire (IVC). Dans notre projet, nous utilisons la version veins-4.4.

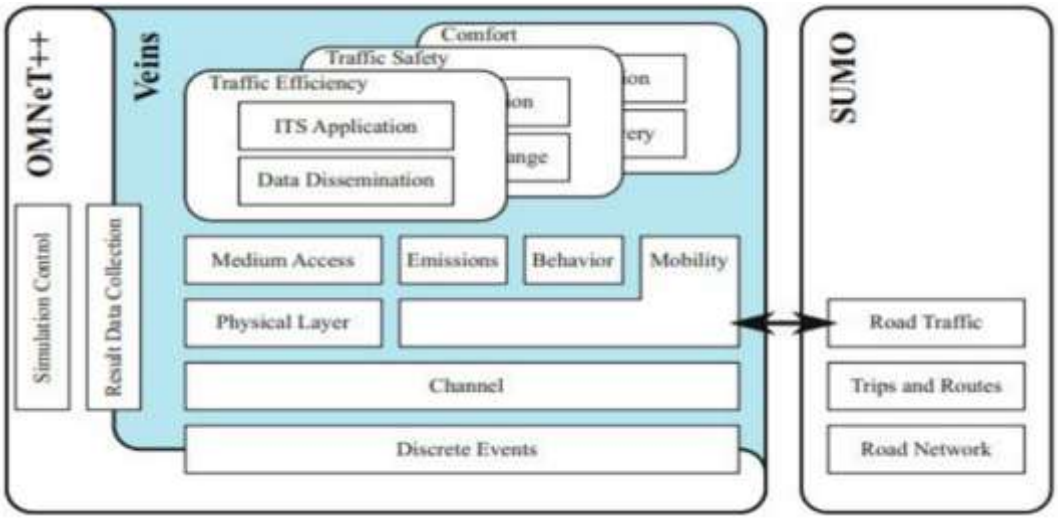

Figure 3.4 : Architecture de Veins [16]

3.3.4 PREXT « Privacy Extension for Veins VANET Simulator»

PREXT, un cadre unifié et extensible, simule les schémas de changement de pseudonyme (autrement dit, les schémas de confidentialité) dans les VANET. La principale hypothèse de PREXT est de diffuser des messages beacons à des intervalles courts (par exemple, entre 0,1 et 1 seconde), incluant leur position, leur vitesse, leur date, ainsi qu'un pseudonyme changeant (c'est-à-dire, une identité temporaire de nœud). PREXT présente de nombreux avantages très importants :

Les avantages de PREXT

Les avantages de l'extension proposée incluent [15] :

- Un design modulaire d'une couche de confidentialité qui facilite la mise en œuvre de nouveaux schémas de confidentialité.

- Prext supporté sept schémas (caps, slow, RSP, CPN, Mix-zone, CSP, PeriodicalPC) de confidentialité basés sur différentes approches (les périodes de silence, les contextes et les mix-zones). Ces schémas intégrés permettent aux spécialistes de la confidentialité d'intégrer ces aspects de confidentialité dans leurs simulations.

- Prext prend en charge de nombreuses mesures de confidentialité :

- La traçabilité
- L'entropie
- La taille de l'ensemble d'anonymat
- Les statistiques sur les pseudonymes.

Il inclut un module d'adversaire basé sur l'algorithme d'association de données probabilistique du plus proche voisin Nearest Neighbor Probabilistic Data Association (NNPDA). En mesure de suivre les véhicules efficacement. La puissance de cet adversaire est entièrement contrôlée en déterminant sa couverture du réseau routier.

3.5 Métriques

Les mesures des indicateurs de performance :

3.5.1 Traçabilité

Cette mesure évalue à quel point un adversaire peut constamment suivre un véhicule sur plus de 90 % de son trajet [15].

3.5.2 Traçabilité Normalisée

La traçabilité normalisée est une métrique similaire à la traçabilité, mais en ignorant les traces qui n'ont jamais changé de pseudonyme. De plus, un bon suivi fournit des informations précises sur l'efficacité du schéma et protège même la vie privée du conducteur contre les attaques [17].

3.5.3 Changement moyen des pseudonymes par trace

Dans un trajet, un véhicule peut modifier son pseudonyme à plusieurs reprises. Ce changement fréquent évalue en moyenne le nombre de modifications de pseudonyme des véhicules. Il est déconseillé de changer fréquemment de pseudonyme ; il est essentiel de trouver un équilibre entre l'efficacité de la confidentialité et les coûts de gestion. Par conséquent, nous devons parvenir à un équilibre dans le nombre de changements de pseudonymes des véhicules [17].

3.5.4 Confusion moyenne par trace

Dans ce cas de mesure les stratégies de confidentialité sont conçues pour dissimuler l'identité des véhicules afin d'éviter toute traçabilité de leurs emplacements Pour ce faire, des

méthodes doivent être mises en place pour perturber le suivi lorsque quelqu'un tente de suivre la trajectoire d'un véhicule. Cette mesure reflète l'efficacité de la stratégie de confidentialité [17].

3.5.5 Confusion moyenne par changement de pseudonyme

Cette mesure se caractérise comme le rapport entre le nombre moyen de confusions par trajet et le nombre moyen de changements de pseudonyme par trajet. Plus ce ratio est élevé, plus la solution est efficace. Comme précisé dans la définition de la métrique moyenne de changement de pseudonyme par trajet [17].

3.6 Discussion de résultats

Dans cette partie nous discuterons et analysons les résultats obtenus après plusieurs simulations réalisées sous PREXT :

A - Confusion moyenne par changement de pseudonyme

La figure 3.5 compare entre les différents schémas par rapport à la confusion moyenne par changement de pseudonyme. Il est évident que lorsque la confusion est élevée, il devient difficile pour un attaquant de suivre le véhicule. Plus la confusion est élevée, plus le système est efficace. Notre schéma E_SLOW présente le nombre moyen de confusions le plus élevé par rapport aux autres schémas, ce qui signifie que les pseudonymes des véhicules changent fréquemment. Cette fréquence élevée de changement crée une confusion significative pour tout attaquant essayant de suivre les utilisateurs, garantissant ainsi que les utilisateurs restent anonymes et difficilement traçables. Cela assure une meilleure protection de la vie privée, car les attaquants perdent régulièrement la trace des véhicules. La métrique de confusion élevée démontre que **E_SLOW** est particulièrement efficace pour préserver la confidentialité, surpassant ainsi les autres schémas en termes de protection de la vie privée.

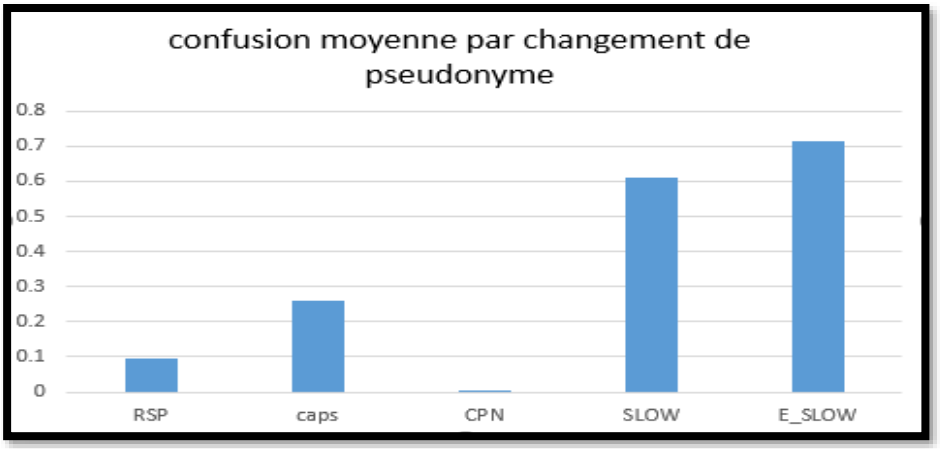

Figure 3.5 : Confusion moyenne par changement de pseudonyme

B - Confusion moyenne par trace

La figure 3.6 illustre que les traces associées à notre schéma sont les plus sujettes aux confusions, tandis que les autres schémas génèrent beaucoup moins de confusions en comparaison. Selon cette métrique, la confusion est prise en compte lorsque le véhicule change de pseudonyme. En cas de confusion, il devient difficile pour l'attaquant de suivre le véhicule et il perd sa trace. Ainsi, cette mesure préserve la confidentialité, ce qui est l'objectif majeur de notre travail.

E_SLOW affiche le taux de confusion par trace le plus élevé, ce qui signifie que les pseudonymes des véhicules changent fréquemment. Cela rend **E_SLOW** particulièrement efficace pour préserver la confidentialité, car il garantit que les utilisateurs restent anonymes et difficilement traçables. En revanche, les schémas RSP, caps et CPN présentent des taux de confusion beaucoup plus faibles, ce qui se traduit par une traçabilité plus élevée et, par

conséquent, une protection de la vie privée moindre. Et ce confirme que E_SLOW est une solution particulièrement efficace pour préserver la confidentialité.

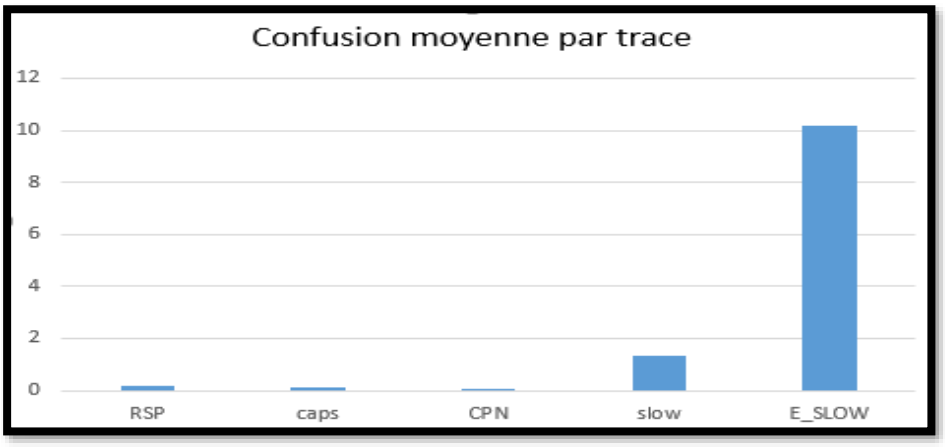

Figure 3.6 : Confusion moyenne par trace

C - Changement moyen des pseudonymes par trace

La figure 3.7 montre le changement moyen des pseudonymes par trace. Nous observons que le taux de changement des pseudonymes dans notre schéma est élevé. Ce taux élevé influe négativement sur la consommation modérer du pool des pseudonymes disponibles, mais en contrepartie on a assuré moins de traçabilité.

Le graphique montre que le protocole E_SLOW atteint un taux de changement de pseudonymes moyen à élever, réduisant ainsi la traçabilité des utilisateurs et augmentant le niveau de confidentialité. Bien que le taux de changement dans E_SLOW ne soit pas aussi élevé que celui de CPN, il est suffisamment élevé pour assurer une grande confidentialité tout en maintenant une consommation modérée des pseudonymes, évitant ainsi l'épuisement rapide des ressources.

La solution E_SLOW offre un excellent équilibre entre l'amélioration de la confidentialité en réduisant la traçabilité et le maintien d'une consommation modérée des ressources. Elle surpasse clairement des nombreuses autres solutions, la rendant ainsi une option efficace et sécurisée.

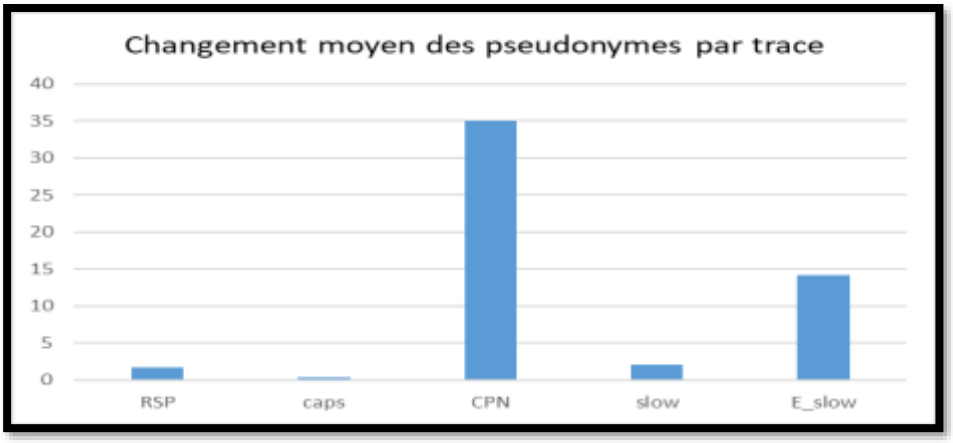

Figure 3.7 : Changement moyen des pseudonymes par trace

D - Traçabilité Normalisée

La figure ci-dessous illustre la traçabilité normalisée effectuée dans les différents schémas. Les stratégies RSP, CAPS et CPN présentent une traçabilité très élevée, ce qui signifie que les véhicules dans ces schémas peuvent être facilement suivis. En revanche, notre schéma, bénéficie de la plus faible traçabilité parmi tous les schémas, rendant le suivi des utilisateurs extrêmement difficile. Cela garantit une meilleure protection de la vie privée.

Ce résultat montre qu'E_SLOW est une solution très efficace pour protéger la vie privée, surpassant largement les autres schémas tels que RSP, CAPS et CPN. Cette métrique indique une bonne conservation de la confidentialité du schéma : plus la traçabilité est faible, plus la confidentialité est élevée. Par conséquent, notre schéma offre une meilleure protection de la confidentialité par rapport aux autres schémas.

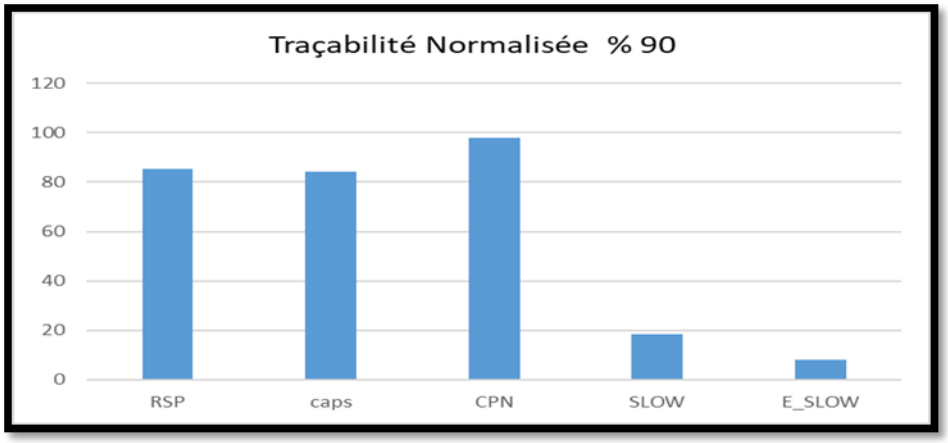

Figure 3.8 : Traçabilité Normalisée

3.7 Conclusion

Dans ce chapitre, nous discutons sur notre contribution et présentons l'environnement de travail de notre approche ainsi que les résultats de la simulation. Cette approche montre de bons résultats et s'avère très efficace par rapport aux autre schémas existants dans PREXT, en termes de traçabilité normalisée, changement moyen des pseudonymes par trace, confusion moyenne par trace et confusion moyenne par changement de pseudonyme.

Conclusion générale

Les réseaux véhiculaires sont d'une grande importance pour les chercheurs en raison de leurs services promis pour les utilisateurs de la route. Pour maintenir la sécurité, plusieurs critères doivent être respectés, notamment la cohérence, l'intégrité, la non-répudiation et la confidentialité des informations utilisateur, qui ne peuvent être divulguées que pour l'autorité de confiance. Cela contribue à protéger l'utilisateur contre les attaques de suivies.

Plusieurs techniques qui garanties la sécurité de la vie privée dans les réseaux véhiculaires existent. La technique de changement des pseudonymes consiste à changer les pseudonymes au fur et à mesure dans le trajet, le changement des pseudonymes est une solution efficace mais qui doit être traitée soigneusement afin de réduire la possibilité qu'un traqueur puissant détecte et relies les différents pseudonymes du même véhicule.

Dans ce projet, nous avons proposé, implémenter et simuler une amélioration de l'approche SLOW. Cette amélioration repose sur le changement des pseudonymes en vérifiant deux conditions : (1) La vitesse est inférieure à un seuil donné et (2) qu'il y a au moins un autre véhicule à proximité. Notre schéma a donné des résultats meilleurs par rapport aux autres schémas de confidentialité. La simulation a été faite sous l'environnement fameux OMNET++, Un projet supplément qui doit être ajouté au simulateur et qui tient compte de l'environnement VANET est appelé VEINS. L'outil PREXT, qui offre des schémas de confidentialité déjà implémenté et un traqueur puissant pour tester l'efficacité de tout schéma, à té aussi utilisé.

Les recherches se poursuivent pour trouver une solution parfaite, sans défauts, assurant la sécurité des véhicules contre le traqueur tout en préservant les applications de sécurité.

Bibliographie

[1] Arif, M., Wang, G., Bhuiyan, M. Z. A., Wang, T., & Chen, J. (2019). A survey on security attacks in VANETs: Communication, applications and challenges. Vehicular Communications, 19, 100179.

[2] Luckshetty, A., Dontal, S., Tangade, S., & Manvi, S. S. (2016, April). A survey: comparative study of applications, attacks, security and privacy in VANETs. In 2016 International Conference on Communication and Signal Processing (ICCSP) (pp. 1594-1598) IEEE.

[3] Ghosal, A., & Conti, M. (2020). Security issues and challenges in V2X: A survey. Computer Networks, 169, 107093.

[4] Guilbot, M. (2020). Les systèmes de transport intelligents coopératifs. Quelles responsabilités pour les acteurs publics?. TEC Mobilité Intelligente, (246), pp42-43.

[5] Tomar, R., Prateek, M., & Sastry, G. H. (2016). Vehicular adhoc network (vanet)-an introduction. International Journal of Control Theory and Applications, 9(18), 8883-8888.

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

[7] http://fr.wikipedia.org/wiki/Infrastructure_à_clés_publiques. Consulté le : 22/02/2010.

[8] AYAD, K., & GASMI, B. (2022). Security and Privacy in VANETs Implementation of TRA protocol on OMNET++ (Doctoral dissertation, UNIVERSITY BBA).

[9] LeventeButtyan, Tamas Holster, Andre Weimerskirch, William Whyte, “SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs” in Proc. IEEEVehicular Networking Conference (VNC), pp.1-8, October 2009.

[10] Kumar, P. S., Parthiban, L., & Jegatheeswari, V. (2019, April). Context Aware Privacy and Security Using P-Gene Based on Pseudonym in VANETs. In 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS) (pp. 1-5). IEEE.

[11] IEEE Standard for Wireless Access in Vehicular Environments—Security Ser-Vices for Applications and Management Messages, IEEE Standards 1609.2-2016(Mar. 2016), 2016.

[12] S.-M. S. S. M. Abdelwahab Boualouachea, VLPZ : The Vehicular Location Privacy Zone, Procedia Computer Science 83 (2016) 369 – 376, 2016.

[13] M. Babaghayou and N. Labraoui, “Transmission Range Adjustment Influence on Location PrivacyPreserving Schemes in VANETs,”, doi: 10.1109/ICNAS.2019.8807823. , 2019.

[14] Wahid, A., Yasmeen, H., Shah, M. A., Alam, M., & Shah, S. C. (2019). Holistic approach for coupling privacy with safety in VANETs. Computer networks, 148, 214-230.

[15] “GitHub - karim-emara/PREXT: PREXT is a unified and extensible framework that simulate pseudonym change schemes (i.e., privacy schemes) in VANET." https://github.com/karimemara/PREXT (accessed Jun. 14, 2022).

[16] AL-SHAREEDA, Mahmood A. et MANICKAM, Selvakumar. A systematic literature review on security of vehicular ad-hoc network (vanet) based on veins framework. IEEE Access, 2023.

[17] MOUSSAOUI BOUBAKEUR Sécurité et protection de la vie privée dans les réseaux véhiculaires, http://dspace.univ-msila.dz:8080//xmlui/handle/123456789/40086.

[18] Buttyán, L., Holczer, T., Weimerskirch, A., & Whyte, W. (2009, October). Slow: A practical pseudonym changing scheme for location privacy in vanets. In 2009 IEEE vehicular networking conference (VNC) (pp. 1-8). IEEE.

[19] Pan, Y., & Li, J. (2013). Cooperative pseudonym change scheme based on the number of neighbors in VANETs. Journal of Network and Computer Applications, 36(6), 1599-1609.