الجمـــهوريـــة الجـــزائريـــة الديـمقـراطيـــــــة الشـعبيـــــة
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعـلـيـم الـعـالـــي و الـبـحـث الـعـلـمي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جـامـعـة عمّـــار ثـلـيـــجـــي بالأغـــواط
UNIVERSITE AMAR TELIDJI LAGHOUAT
كـلـيـــــة الـعـلـــــوم
FACULTE DES SCIENCES
قسم الإعلام الآلي
DEPARTEMENT D'INFORMATIQUE

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Réseaux , systèmes et application répartis

Par : Siga Fayçal/Geullouma Ali.

THEME

Defending On Pseudonym Changing Attacks

Soutenu publiquement le 07/07/2021 devant le jury composé de:

Mr Taher BENDOUMA MC Président
Mr Omar Sami OUBATTI M.C Examinateur
Mr Noureddine CHAIB M.C Encadreur

N_ d' ordre :...../Année universitaire 2020/2021

Dédicace

Avec un énorme plaisir, un Coeur ouvert et une immense joie, je dédie ce modeste travail particulièrement à mes chers parents, qui ont consacré leur existence a bâti la mienne, pour leur soutien, patience et soucis de tendresse et d'affection pour tout ce qu'ils ont fait pour que je puisse arriver à ce stade.

À ma très chère sœur et m'adorable Chahrazed

À mes chères sœurs

À toute ma famille

À tous mes amis de ma promotion

À tous ceux qui m'ont aidé de prés ou de loin.

Siga Fayçal

Je dédie ce modeste travail à mes parents :

grâce a leurs cendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études, aucune dédicace ne pourrait exprimer mon respect, ma considération et mes profonds sentiments envers eux A mes frères

NASRO, Youcef, Abdelkader A ma sœur Fatima Zohra , a tous mes: oncles et tantes , mes cousins particulièrement Ali, Mohammed Je dédie ce mémoire aussi à mes amis et à tous mes collègues de la promotion de 2021, surtout a mon cher binôme Fayçal Siga et sa famille

Guellouma Ali

Remerciements

Toute notre gratitude et remerciements au bon DIEU qui nous a donné la force, le courage et la volonté d'élaborer ce travail.

Nous adressons notre profond remerciement à Monsieur l'encadreur Noureddine Chaib pour avoir dirigé ce travail.

Nous remercions Messieurs les membres du jury de nous faire l'honneur de juger notre modeste travail.

Nous remercions tous nos professeurs du département d'informatique.

Remerciements les plus sincères a toutes les personnes qui nous ont aidés de prés ou de loin à accomplir notre travail.

ملخص

تعتبر شبكات المركبات (VANETs) واتصالات المركبات علامة فارقة في تحسين السلامة والكفاءة والراحة في النقل. تعتمد الشبكات المخصصة للمركبات والعديد من تطبيقات المركبات على البث الدوري لموقع المركبات. على سبيل المثال ، يمكن استخدام موقع المركبات لاكتشاف وتجنب الاصطدامات أو التوجيه الجغرافي للبيانات لنشر رسائل التحذير. في الوقت نفسه ، يمكن استخدام هذه المعلومات لتتبع أماكن تواجد المستخدمين. تعد حماية خصوصية الموقع لمستخدمي VANET أمرًا مهمًا ، لأن الافتقار إلى الخصوصية قد يعيق القبول الواسع لهذه التكنولوجيا.

يتم قبول تغيير الأسماء المستعارة بشكل متكرر كحل لحماية الخصوصية في VANET ، ولكن هذه التقنية لها مشاكلها الخاصة حيث يمكن استغلال عيوب معينة ، من خلال شن هجمات أو تعطيل عمل نظام VANET ، ويمكن للمهاجم تغيير اسمه المستعار في كثير من الأحيان حتى يتمكن من استخدامه في هجمات معينة.

في هذه المذكرة قمنا باستحداث تقنية لمنع المركبات من تغيير اكثر من اسم مستعار في الفترة المخصصة لتغيير الاسماء المستعارة، تظهر نتائج المحاكاة التي تم إجراؤها فعالية حلولنا.

الكلمات المفتاحية : شبكة المركبات ، خصوصية الموقع في شبكات المركبات ، تغيير الأسماء المستعارة في شبكة المركبات ، إخفاء الهوية.

Abstract

Vehicle networks (VANETs) and vehicle communications are an important step in improving the safety, efficiency and convenience of transportation. VANET networks and many vehicle applications rely on periodic transmissions of the location of the vehicle. For example, vehicle location can be used to detect and avoid collisions or geo-routing data to post warning messages. At the same time, this information can be used to track the whereabouts of users. It is important to protect the privacy of users of the site for VANET users, as the lack of feature can hamper the widespread acceptance of this technology.

Changing pseudonyms frequently is accepted as a solution to protect privacy in VANETs, but this technique has its own problems where certain flaws can be exploited, by carrying out attacks or disrupting the functioning of the VANET system, and the attacker can change his pseudonyms frequently so that he can use it in certain attacks.

In this memory, we have developed a technique to prevent the pseudonyms change attack and minimize its impact on the network. The results of simulations carried out show the effectiveness of our solutions.

Keywords: vehicle network, location privacy in vehicle networks, change of aliases in vehicle network, anonymity.

Résumé

Les réseaux de véhicules (VANET) sont une étape importante dans l'amélioration de la sécurité, de l'efficacité et de la commodité des transports. Les réseaux VANET et de nombreuses applications de véhicules reposent sur des transmissions périodiques de l'emplacement du véhicule. Par exemple, la localisation du véhicule peut être utilisée pour détecter et éviter les collisions ou les données de géo-routage pour afficher des messages d'avertissement. Dans le même temps, ces informations peuvent être utilisées pour suivre les allées et venues des utilisateurs. Il est important de protéger la vie privée des utilisateurs du site pour les utilisateurs de VANET, car le manque de fonctionnalité peut entraver l'acceptation généralisée de cette technologie.

Changer fréquemment de pseudonyme est accepté comme une solution pour protéger la vie privée dans les VANET, mais cette technique a ses propres problèmes où certaines failles peuvent être exploitées, en menant des attaques ou en perturbant le fonctionnement du système VANET, et l'attaquant peut changer fréquemment ses pseudonymes afin qu'il peut l'utiliser dans certaines attaques.

Dans ce mémoire, nous avons développé une technique pour empêcher l'attaque de changement de pseudonyme et minimiser son impact sur le réseau. Les résultats des simulations réalisées montrent l'efficacité de nos solutions.

Mots-clés : réseau de véhicules, confidentialité de la localisation dans les réseaux de véhicules, changement de pseudonyme dans le réseau de véhicules, anonymat.

Sommaire

Liste des figures

Liste des tableaux

Introduction générale

Chaque année dans le monde, des millions d'accidents routiers constituent les premières causes de décès et de blessures. Ces accidents ont aussi un impact négatif sur l'économie à cause des pertes de biens correspondants. Ils rendent aussi la situation des routes congestionnées plus grave. Ce qui augmente les heures de conduite et de transport de marchandises.

Avec la prolifération des équipements électroniques et l'émergence de la technologie de communication, il devient possible d'équiper les véhicules d'interfaces de communication, d'appareils GPS, des unités de traitement, de radars, de capteurs,…etc. Donc, les véhicules peuvent détecter les situations dangereuses et diffuser des messages d'alerte pour avertir les véhicules voisins. En conséquence, les conducteurs où les véhicules eux-mêmes peuvent intelligemment décider l'action adéquate à entreprendre. Ces éléments constituent les réseaux véhiculaires VANET (*Vehicular Adhoc NETwork*) qui peut alléger la congestion routière en informant les conducteurs sur l'état des routes et les espaces de parking libres. Ils permettent aussi d'éviter les fluctuations de vitesse ce qui réduit la quantité de carburant consommée. Donc, les VANETs ont un impact positif sur l'environnement et l'économie.

Les réseaux véhiculaires et leurs applications prometteuses sont devenus un centre d'intérêt de plusieurs entités, que ce soit des organisations gouvernementales ou de standardisation, des entreprises (notamment les constructeurs automobiles et les opérateurs de télécommunication) ou des centres de recherche. Ces futurs réseaux véhiculaires seraient parmi les plus grands réseaux dans le monde. A cet effet, ils constitueraient une cible idéale aux attaques des entités malveillantes qui pourraient viser à dégrader leur performance, les exploiter à leur profit ou voire même commettre des actions menaçant la vie des personnes et leurs biens.

L'authentification des nœuds du réseau constituent un élément fondamental pour la sécurisation de ces réseaux et l'identification des nœuds malveillants. Pour cela, les différents organismes de standardisation ont traité ce problème et ont défini les outils cryptographiques nécessaires et le format d'un message sécurisé.

Les systèmes de révocation locale doivent avoir des mécanismes autonomes afin d'empêcher les nœuds malveillants d'exploiter l'aspect distribué dans la révocation de nœuds honnêtes. Ce qui pose plus de contraintes à la sécurisation de ces réseaux.

Avec les travaux de recherches intensifs sur les VANETs et l'émergence de la cryptographie moderne, les chercheurs ont proposé des solutions pour protéger la vie privée des utilisateurs des VANETs. Elles consistent essentiellement à employer les pseudonymes pour assurer l'anonymat de ces réseaux. Ce qui permet d'encourager les décideurs aux déploiements de ces derniers.

Les solutions de l'anonymat protègent la vie privée d'une part, et posent des contraintes sévères à la détection et l'identification de nœuds malveillants.

Ce mémoire est composé de trois chapitres :

Nous présentons dans le premier chapitre l'environnement véhiculaire. Nous détaillons, nous présentons la technologie des réseaux véhiculaires et ses applications prometteuses. Ensuite, nous décrivons les éventuelles attaques contre les VANETs.

Le chapitre II présent les systèmes de pseudonymat dans les VANETs et les différents systèmes de révocation de pseudonymes. Enfin, nous décrivons la solution basée sur les pseudonymes.

Dans le troisième chapitre, nous présentons notre proposition solution. Ensuite, nous présentons les simulations réalisées ainsi que l'analyse des résultats.

Finalement, Nous concluons ce mémoire en présentant les conclusions et quelques perspectives.

Chapitre 1 :

Introduction aux réseaux VANET

1.1 Introduction

Le nombre croissant de véhicules aujourd'hui a conduit à un déséquilibre au trafic routier. En effet, ils entrainent des dégâts environnement aux ainsi qu'une mauvaise qualité de vie. Comme les systèmes de transport actuels fournissent très peu d'informations sur les conditions routières, de nombreux gouvernements, constructeurs automobiles et consortium d'industriels ont fixé la réduction des accidents de la route comme une priorité majeure. Afin d'aboutir à ce but, la première idée consistait à rendre les véhicules et les routes plus intelligents par le biais des communications sans fil, d'où la technique VANET s'est présentée et qui permet aux véhicules de communiquer via des messages envoyés entre eux.Les réseaux véhiculaires sont une projection des systèmes de transports intelligents (STI) (ou ITS pour *Intelligent transportation System*). Le but des STI est de réduire les risques dans le domaine du transport de façon significative en travaillant simultanément sur quatre bases: la prévention des accidents; la réduction des dégâts en cas de collision; la gestion des secours et enfin la protection des utilisateurs[1] [2].

Dans ce chapitre, nous présentons le réseaux VANET et ses applications prometteuses. Ensuite, nous décrivons les éventuelles attaques contre les VANETs, et enfin nous passons en revue les travaux de standardisation et les différents projets et groupes de recherche dans la communauté VANET.

1.2 Pourquoi les réseaux véhiculaires ?

Les réseaux véhiculaires ont été introduits pour résoudre deux problèmes principaux :

1.2.1 Problème de la sécurité routière

Les accidents de la route représentent la 8ème cause de décès dans le monde et la première cause de décès chez les jeunes (âgés de 15 à 29 ans). Les tendances actuelles indiquent que les accidents de la route passeront au cinquième rang des causes des décès à l'horizon 2030 [3].

1.2.2 Problème économique

La congestion de la route engendre des coûts importants sur le plan économique. Les prix des produits et des services sont directement liés à la durée de transport nécessaire et à la quantité des carburants consommés. Une gestion intelligente du trafic routier va certainement permettre la réduction des dépenses annuelles.

La congestion réduit la qualité de vie des individus et engendre des coûts environnementaux importants. Les embouteillages entraînent un gaspillage d'énergie et une production de gaz à effet de serre et d'autres polluants qui sont néfastes pour l'environnement.

1.3 Architecture et caractéristiques des réseaux véhiculaires sans fil

1.3.1 Architecture des réseaux véhiculaires sans fil

Un réseau VANET constitue une nouvelle forme de réseaux MANET « pour Mobile Ad-hoc NETworks ». Il permet aux véhicules de communiquer entre eux (cf. Figure 1.1), ou avec des infrastructures installées aux bords de routes appelées RSU (Road Side Units). Par rapport à un MANET, un réseau VANET est caractérisé par une forte mobilité de nœuds rendant le système difficile à concevoir.

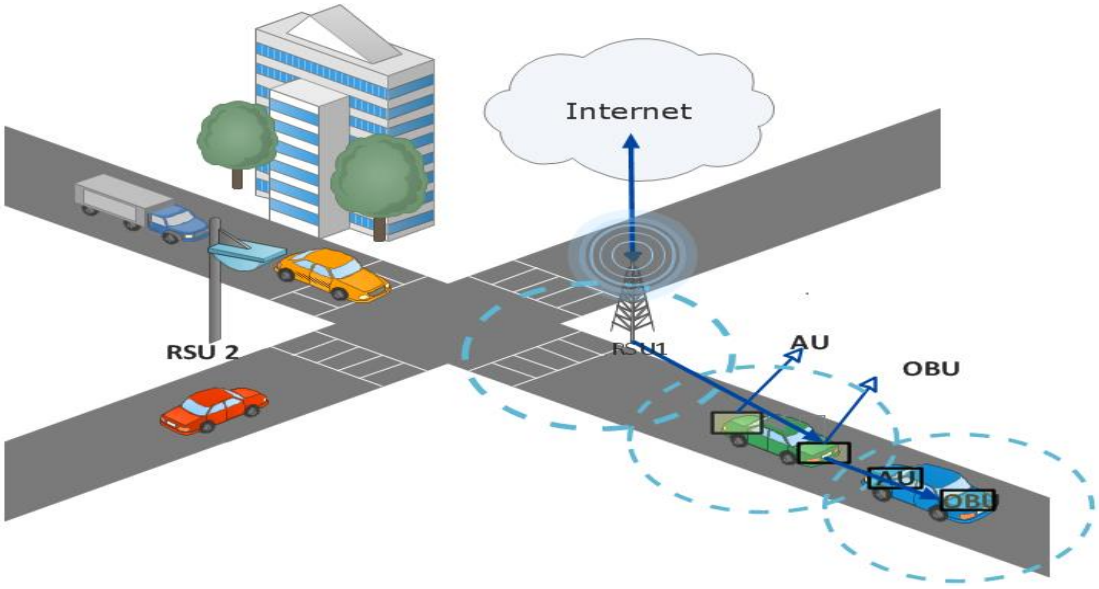

Figure1.1:Exemple d'un réseau VANET.

L'architecture des réseaux véhiculaires sans fil (VANETs) peut être décrite par plusieurs entités. Trois principales entités permettent d'établir la communication dans les réseaux VANET [2] :

a. RSU

Les «RSUs» (Road Side Unit) sont des équipements externes aux véhicules installés au bord des routes. Ils diffusent vers les véhicules des informations liées à l'état du trafic, l'état de la route, ainsi que des informations météorologiques. Ils sont d'ailleurs utilisé comme des routeurs entre les véhicules.

b. OBU

Les «OBUs» (On-Board Unit) sont donc des équipements radio installés dans les véhicules qui permettent à ces derniers de se localiser. ils garantissent l'envoie et la réception des données sur l'interface réseau. Les «OBUs» utilisent les signaux DSRC (Dedicated Short Range Communication) pour communiquer avec les RSU.

c. Autorité centrale

L'autorité centrale ou l'autorité de confiance est un tiers de confiance qui a comme rôle de signer et délivrer les certificats numériques. L'autorité centrale (Central Authority: CA) peut aussi dans certaines circonstances révéler l'identité de l'expéditeur d'un message [4].

1.3.2 Modes de communication pour les réseaux VANET

Dans les réseaux de véhicules, on peut distinguer deux modes de communication, les communications Véhicule-à-Véhicule (V2V) et les communications Véhicule-à-Infrastructure (V2I) comme les montre la figure 1.2 Les véhicules peuvent choisir un de ces deux modes ou bien les combiner en cas d'échec de communication directe avec les infrastructures. Dans cette partie, nous présentons le principe et l'utilité de chaque mode :

a. Mode de communication Véhicule-à-Véhicule (V2V)

C'est un mode de communication qui ne nécessite pas d'infrastructure pour son fonctionnement. Dans ce mode de communication qui fonctionne en environnement décentralisé, chaque véhicule par l'intermédiaire de son OBU, communique directement avec les véhicules situés à sa portée (exemple 800 m de portée) ou bien peut jouer le rôle de relayeur de message dans le but de transmettre des messages aux autres véhicules. Ce mode de communication est très efficace pour la diffusion rapide des informations liées à la sécurité routière et autres données du trafic routier par contre la connectivité n'est pas permanente entre les véhicules.

b. Mode de communication Véhicule à Infrastructure (V2I)

Ce mode de communication offre une meilleure connectivité et permet l'accès aux divers services (par exemple : accès à Internet, échange de données de voiture à domicile, information météorologique,...etc.) grâce à un échange d'informations entre les véhicules et les entités fixes (RSU et CA) disposées le long de la route.

Le mode V2I est inadéquat pour les applications liées à la sécurité routière puisque il n'est pas performant par rapport aux délais d'acheminement des paquets qui sont plus longs, ce délai est lié au fait que les entités fixes (RSU et CA) prennent plus de temps pour le traitement des paquets avant de les diffuser [4].

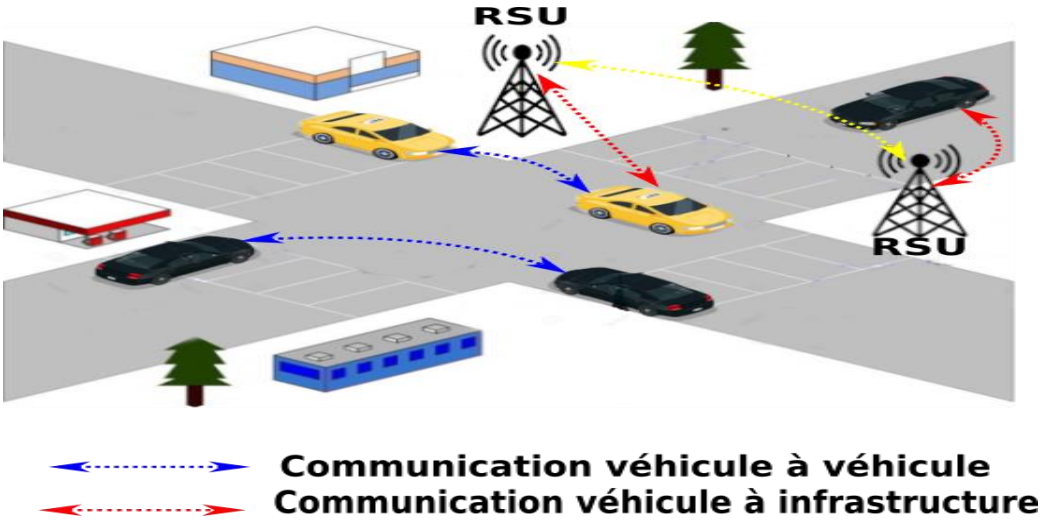

Figure1.2:Modes de Communication dans les réseaux VANET.

C. Mode de communication de Véhicule à piéton (V2P)

Ce mode de communication a été introduit pour permettre l'échange des messages de sécurité entre les véhicules et les piétons qui utilisent des téléphones ou n'importe quel appareil sans fil, intelligent. Ces messages peuvent comporter par exemple des informations sur les piétons qui s'approchent de la route. Les véhicules peuvent aussi émettre des messages d'avertissement vers les appareils intelligents des piétons qui déclenchent des alertes sonores ou via des vibrations. General Motors a réalisé un projet dans ce domaine en 2010 pour réduire le nombre d'accidents avec les piétons et les cyclistes. VOLVO y a aussi investi, et a déjà dévoilé son nouveau concept d'un système des airbags automatiques pour protéger les piétons[13]. La figure suivante montre une démonstration de l'implémentation de HONDA pour les communications V2P.

La figure suivante montre la regard croisé sur le véhicule pour les communications V2P.

Figure1.3:la regard croisé sur le véhicule [12].

1.3.3 Les applications des réseaux VANET

Dans les VANETs, on trouve plusieurs types d'applications ou services qu'on peut classer en 3 catégories [5] :

a. Applications de confort

Comme certains voyages peuvent parfois être longs, dû au trajet ou aux congestions sur la route, les réseaux VANET contribuent également à l'amélioration du confort en permettant d'assurer le confort des véhicules et

leurs occupants durant leurs voyages; ces services comprennent, entre autres l'accès à Internet, la messagerie, le chat inter –véhicule, etc.

L'utilisation de ce genre d'applications, permet aux passagers de s'échanger des musiques, vidéos ou d'accéder à des jeux. Aussi, on pourra procéder à la vérification à distance des permis de conduire, des plaques d'immatriculation par les autorités compétentes, le paiement électronique au niveau des points de péage afin de faire gagner du temps aux utilisateurs.

Figure1.4:Un exemple d'application de confort dans les VANETs[6].

b. Applications d'optimisation et d'amélioration du trafic routier

Outre les services liés aux applications de confort, les réseaux sans fil véhiculaires contribuent également à l'optimisation et à l'amélioration du trafic routier en fournissant des informations sur l'état des routes. En effet, un véhicule peut être informé sur l'état de la circulation de son trajet actuel ou futur à partir des messages échangés par les différentes entités du réseau, ce qui donne la possibilité au conducteur de décider quelle route il peut suivre lorsque le trafic est dense sur un trajet et éviter ainsi la congestion. De plus et grâce à l'échange des informations entre les véhicules, il y aura la possibilité de créer le passage pour les voitures d'urgence, ou de proposer d'autres itinéraires aux véhicules qui sont dans une zone de congestion dans le but d'optimiser le trafic et de le rendre fluide [5] [7].

c. Applications de prévention et de sécurité du trafic routier

Une des applications importantes pour les VANETs est de lutter contre les congestions routières et de fournir aux conducteurs des chemins avec de bonnes conditions. De plus, avec un système de contrôle de variation de vitesses, les véhicules peuvent aussi améliorer la sécurité routière et réduire la consommation de carburants[8].

Il y a aussi une autre possibilité pour diminuer la congestion et améliorer la sécurité routière. En effet, les intersections sont souvent une cause de congestion, et l'amélioration de leur fonctionnement à l'aide des feux de circulation adaptés (cf. Figure 1.5) [9]. Il existe une autre application intéressante qui permet aux voitures d'éviter la recherche d'un espace de parking libre et de payer automatiquement les frais nécessaires[10][11].

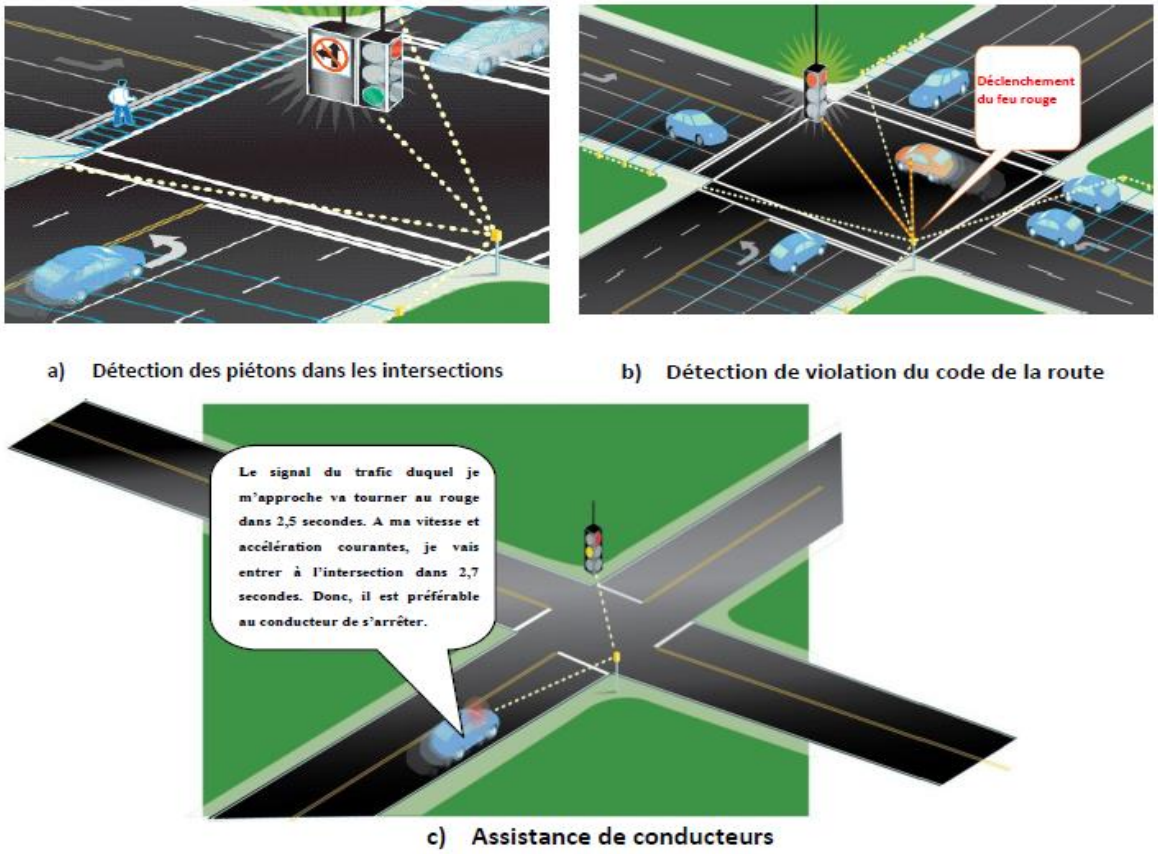

Figure1.5:Gestion des intersections dans les VANETs[14]

1.3.4 Types de messages

a. Les messages « beacon »

Aussi appelé message de contrôle ou d'identification, ils sont envoyés à intervalles réguliers, par convention. Un véhicule peut envoyer un message «beacon» toutes les 100ms. Ils contiennent des informations personnelles sur les véhicules telles que: sa vitesse, sa position GPS (Global Positioning System), sa direction, etc. Grâce à ce type de message, les véhicules se font connaitre à leur entourage [5].

b. Les messages d'alerte

Ce sont des messages générés dans le cas d'un accident, de congestion, d'un obstacle sur la route, etc. Ils permettent d'améliorer la sécurité routière, et de gérer le trafic routier. Lorsqu'un accident survient dans une zone, un message d'alerte est émis, ce message doit être retransmis à intervalle régulier pour assurer que l'alerte est toujours valide. En effet grâce à ces messages, les nœuds mobiles peuvent réduire leurs vitesses ou trouver un autre itinéraire dans le cas d'un secteur à dense trafic routier. Le message de sécurité est généré lorsqu'un évènement qui mérite l'attention du conducteur est détecté. De plus, ces messages doivent être de taille réduite pour pouvoir être retransmis rapidement dans le réseaux.

c. Les autres messages

Outre les messages « beacon » et d'alertes, les entités du réseau véhiculaire sans fil peuvent échanger des messages d'une application, de l'envoi de courriel, etc. Ces messages ne sont émis qu'une seule fois. De plus, les véhicules peuvent échanger des messages multimédias ce qui rend la route moins ennuyeuse et facile.

1.3.5 Environnement de déploiement

Les réseaux véhiculaires sans fil se distinguent principalement par plusieurs milieux de déploiement, on peut définir la circulation des voitures dans le réseau routier sur deux environnements:

a. Environnement urbain

Le milieu urbain est caractérisé par des intersections, des points d'arrêts (les panneaux Stop, le feu tricolore, etc.) et il exige une vitesse réduite jusqu'à un maximum de 50 km/h en ville [15]. C'est un environnement qui présente une forte perturbation des ondes radio causée par la présence des bâtiments, des maisons et autres [5]. De plus, dans ce milieu on peut avoir une bonne connectivité entre les véhicules et une communication ad hoc facile grâce au faible intervalle entre les nœuds. L'installation des infrastructures routières en milieu urbain reste un problème complexe (exemple : insuffisance de place).

b. Environnement autoroutier

Le milieu autoroutier est caractérisé par une vitesse qui varie entre 60 et 100 km/h au Québec [16], de longues routes avec des voies d'accélération et des points de sorties. Comme la vitesse de certains nœuds mobiles est excessive, alors l'écart entre les voitures est important, ce qui entraine une perte de connectivité des nœuds mobiles du réseau voire même une difficulté de la communication en mode ad hoc. L'utilisation les entités fixes (RSU et CA) peut garantir une meilleure connectivité dans cet environnement afin de permettre à toutes les entités mobiles de bénéficier de toutes les fonctionnalités du réseau.

1.3.6 Les caractéristiques des réseaux VANET

Les réseaux véhiculaires ont leurs propres caractéristiques qui les distinguent des réseaux MANET. Ces caractéristiques doivent être considérées lors de la conception des architectures et des protocoles pour les réseaux VANET.

Dans cette section, nous présentons quelques propriétés et contraintes concernant ce type de réseau :

a. **La capacité d'énergie et de stockage:** dans les réseaux VANET, les véhicules disposent suffisamment d'énergie pour alimenter les différents équipements électroniques nécessaires à la constitution d'un réseau VANET. Vue la grande capacité de traitement et de stockage de données, des complexes opérations arithmétiques et cryptographiques peuvent

être mises en œuvre pour assurer la sécurité et le bon fonctionnement de ces réseaux[17].

b. **La topologie et la connectivité:** les réseaux VANET sont caractérisés par une topologie très dynamique et un temps d'interaction entre les véhicules très court. De plus, la topologie est souvent constituée de plusieurs îlots séparés[17], ce qui complique la conception des systèmes efficaces pour les VANETs.

c. **Le modèle de mobilité:** dans les réseaux VANET, la mobilité des nœuds est affectée par plusieurs facteurs : type de route, panneaux de signalisation, ainsi que le comportement des conducteurs et leurs réactions face aux différentes situations rencontrées tels : les embouteillages de la route, les accidents,… etc. [18].

d. **Les contraintes temps réel :** les applications liées à la sécurité routière nécessitent la transmission de données dans des délais très courts. Ce qui limite le choix d'outils et de techniques à utiliser pendant la conception d'un protocole ou une d'architecture pour les VANETs[19].

e. **Une taille illimitée du réseau :** les VANETs peuvent être mis en œuvre au niveau d'une ville, un pays ou voire même plusieurs pays. Ce qui signifie que les VANETs ne sont pas limités géographiquement[19].

f. **Echange des messages fréquents:** dans les réseaux VANET, les véhicules doivent émettre périodiquement des messages beacons, ce qui nécessite un échange fréquent de données entre les différents véhicules[19].

1.4 Normes et standards

Diverses méthodes de communication sont disponibles dans les réseaux véhiculaires, tels que le WiFi , le WiMAX et le DSRC (Dedicated Short Range Communication) [4], dont la couche physique est basée sur la norme IEEE 802.11a.

1.4.1 DSRC

Dedicated Short Range Communication (DSRC) est considéré comme le standard le plus approprié pour les communications sans fil dans les réseaux véhiculaires [21]. Cette technologie a évolué à partir de la norme IEEE 802.11a vers la norme IEEE 802.11p afin de répondre aux caractéristiques des réseaux VANETs. Grâce au standard DSRC, il est possible d'établir une communication véhicule-à-véhicule ainsi qu'une communication véhicule-à-infrastructure. Le standard DSRC est compatible avec les contraintes des réseaux véhiculaires dynamiques. En effet, il offre une fiabilité de communication ainsi qu'une faible latence lors de l'établissement de la communication.

Les caractéristiques du DSRC sont [20] :

- ✓ Il supporte une vitesse des véhicules dépassant 200 km/h.
- ✓ Il offre une portée radio variant entre 300 et 1000 mètres.
- ✓ Il garantit un temps de latence pour l'établissement de la communication ne dépassant pas 50 ms.
- ✓ Il permet un débit théorique (bande passante) atteignant 6 Mbps.

1.4.2 IEEE 802.11 p

En 2003, le groupe de travail IEEE a défini un nouveau standard dédié aux communications inter-véhicules, nommé WAVE (Wireless Ability in Vehicular Environments) et aussi connu sous le nom 21 de IEEE 802.11p [22]. Cette norme utilise le concept de multicanaux afin d'assurer les communications pour les applications de sécurité et les autres services du Transport Intelligent.

IEEE 802.11p est généralement une variante personnalisée de IEEE 802.11a avec une couche physique adaptée pour permettre un fonctionnement à faible charge dans le standard DSRC [22].

La norme IEEE 802.11p est capable d'offrir un débit entre 6 et 27 Mbps (pour des distances jusqu'à 1000 mètres) [22]. De plus, la couche MAC du 802.11p reprend le principe du CSMA/CA (Carrier Sense Multiple Access with Collision

Avoidance) développé dans le protocole MAC de l'IEEE 802.11, pour gérer la qualité de service et le support du protocole de marquage de priorité [22] [17].

1.5 La sécurité dans les réseaux VANET

Il est primordial que les exigences de la sécurité doivent toujours respecter le bon fonctionnement d'un système afin de garantir la sécurité de ce dernier. Lorsqu'un requis n'est pas respecté, celui-ci présente un problème de sécurité. Les requis que doivent respecter les réseaux véhiculaire VANET ont été discuté dans [23] [24] [25] [26],Dans cette section, nous présentons les objectifs de la sécurité dans les VANETs, puis nous donnons les types d'attaquants, ensuite nous décrivons les différentes catégories d'attaques contre les VANETs, enfin nous présentons le matériel utilisé pour protéger les données.. Dans la suite nous détaillons ces différents requis.

1.5.1 Les objectifs de la sécurité dans les réseaux VANET

La sécurisation des communications dans les réseaux VANET nécessite la mise en oeuvre de technique permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent[27] :

1-L'authentification

L'authentification est un requis principal de tout système. Pour les VANETs, il est nécessaire de connaitre les informations liées aux nœuds émetteurs tels que son identifiant, sa position géographique, son adresse et ses propriétés. Cette exigence a pour objectif principal de contrôler les niveaux d'autorisation du véhicule dans le réseau. Dans les VANETs, l'authentification aide à la prévention des attaques telle que l'attaque Sybil en spécifiant un identifiant unique pour chaque véhicule et de cette manière ce dernier ne pourra pas réclamer d'avoir plusieurs identifiants afin de provoquer le mauvais fonctionnement du réseau [23] [28].

Plusieurs types d'authentifications ont été présentés dans [23] [29] :

- ✓ **L'authentification de l'ID :** Un nœud doit être capable d'identifier les transmetteurs d'un message donné de façon unique. A partir de cette authentification, un véhicule émetteur peut accéder au réseau.

- ✓ **L'authentification de la propriété :** Ce type d'authentification peut déterminer si le type d'équipement qui est en communication est un autre véhicule, un « RSU » ou encore d'un autre équipement.

2-La disponibilité : elle permet d'avoir une qualité de service adéquate d'accès aux ressources du réseau véhiculaire.

3-La confidentialité : elle s'agit d'un ensemble de règles à appliquer pour garantir que seules les personnes autorisées peuvent accéder aux ressources. Cet objectif peut être achevé en utilisant le cryptage de données et l'échange de messages spécifiques entre les véhicules et les RSUs.

4-La non-répudiation: elle assure que les émetteurs ne peuvent pas nier d'être à l'origine d'un message qu'ils génèrent.

5-L'intégrité: cet objectif de sécurité permet de s'assurer que les informations échangées ne sont pas soumises à une modification volontaire ou accidentelle.

6-La vie privée et l'anonymat : cet objectif permet de cacher l'identité et la position géographique des nœuds, et d'autres informations qui mettent en péril la vie privée des utilisateurs.

7-La révocabilité : cet objectif permet d'avoir les mécanismes nécessaires pour exclure les nœuds malveillants et de révéler leurs vraies identités.

8-Le contrôle d'accès : il permet de s'assurer que les nœuds accèdent aux ressources suivant des règles et de privilège bien déterminés.

1.5.2 Les types d'attaquants

Les attaquants peuvent être classées suivant les dimensions suivantes [38]:

- ✓ **Interne/Externe :** l'attaquant interne possède les clés cryptographiques qui lui permettent de communiquer avec d'autres nœuds dans le réseau. Les techniques cryptographiques seules ne sont pas suffisantes pour se défendre contre ce type d'attaquant. Ce dernier est capable de dégrader considérablement la performance du réseau. Par contre, l'attaquant externe est perçu par les membres du réseau comme un intrus, il est donc limité dans la diversité des attaques qu'il peut provoquer.

- ✓ **Malveillant/Rationnel:** un attaquant malveillant emploie tous les moyens pour le dysfonctionnement du réseau quels que soient les coûts et les conséquences correspondants. Par contre, un attaquant rationnel cherche un profit personnel, et par conséquent, les cibles d'attaques et les moyens employés peuvent être prévus.
- ✓ **Passif /Actif :** l'attaquant passif écoute simplement les données échangées dans le réseau, tandis que l'attaquant actif peut agir sur les données échangées.

1.5.3 Les attaques contre les VANETs

Les attaques contre les VANETs peuvent être classées comme suit [30]:

1. Attaques contre la disponibilité : les attaques suivantes contre la disponibilité de communication véhiculaire ont été identifiées:

- ✓ **Déni de service:** les attaques DoS (Denial of Service) peuvent être effectuées par des participants malveillants du réseau ou des entités étrangères pour rendre un service indisponible aux utilisateurs de réseau par les inondations inutiles de messages et de brouillage du canal (cf. Figure 1.6)[32]. Cette attaque est dangereuse car elle profite de l'aspect distribué et coopératif du système VANET pour causer son disfonctionnement[31].

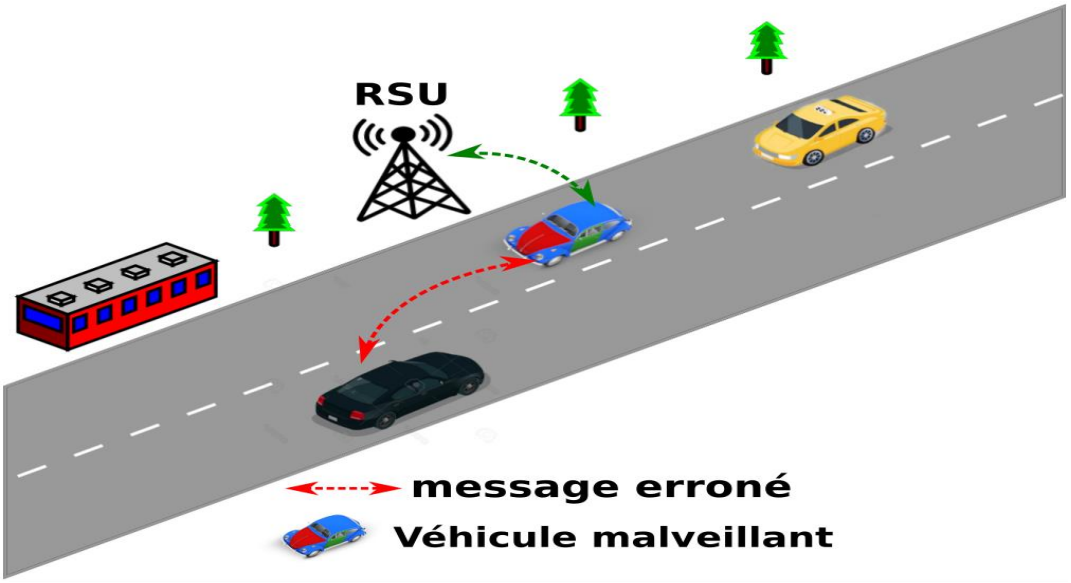

Figure1.6:Attaque DoS.

- ✓ **Falsification de données diffusées:** dans cette attaque, l'adversaire compose un message contenant des informations erronées sur l'état de la route, un message de freinage d'urgence ou un autre sur les conditions du trafic routier par exemple. Ces informations falsifiées affectent la disponibilité de données correctes pour l'assistance du conducteur[33].
- ✓ **Malware:** l'introduction de logiciels malveillants, tels que des virus ou des vers dans les VANETs, peut causer des perturbations au bon fonctionnement des réseaux. Les attaques par des logiciels malveillants sont plus susceptibles d'être effectuées par des attaquants internes plutôt que des externes. Les Malwares peuvent être injectés dans les OBUs1 (On Board Unit), lorsque ces derniers reçoivent les mises à jour logicielles. Dans ces attaques, il se peut que l'entité malveillante vise à dégrader l'efficacité du réseau[34].
- ✓ **L'attaque trou noir (Blackhole):** dans les réseaux VANET, un blackhole est formé lorsque le trafic est redirigé vers un ou plusieurs nœuds qui ne relient pas ces paquets à leurs destinations (cf. Figure 1.7). Cette attaque est très dangereuse car l'attaquant aura un contrôle important sur le réseau[33].

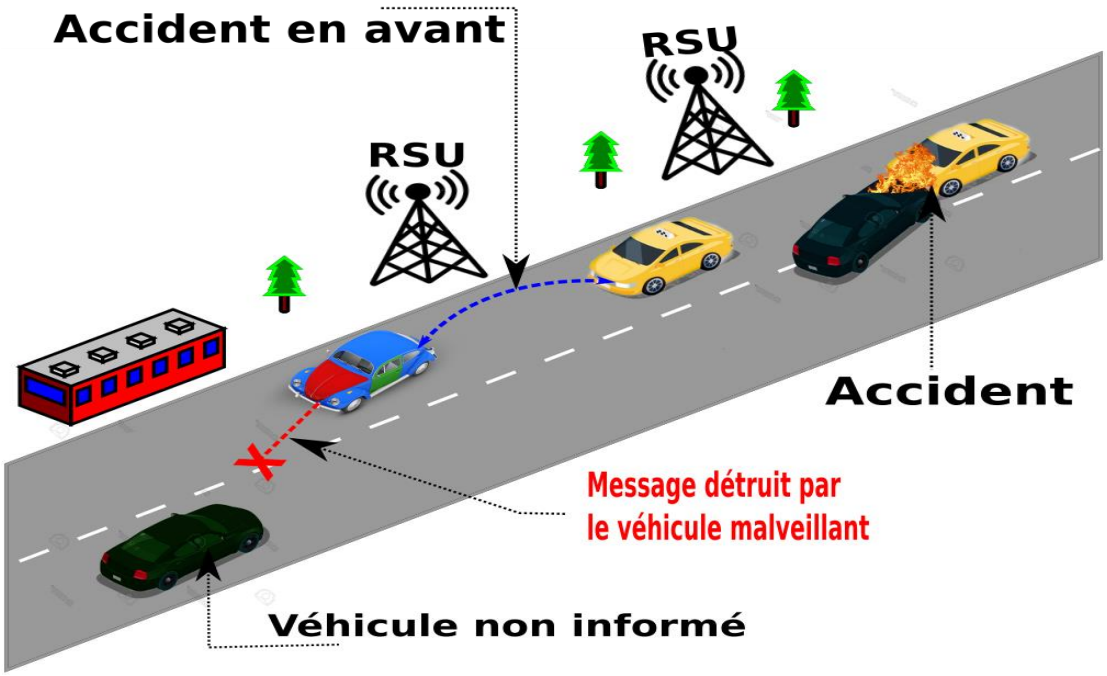

Figure1.7:Attaque Blackhole.

2. Attaques liées à l'authentification : assurer l'authentification dans un réseau véhiculaire consiste à protéger les nœuds légitimes contre les entités étrangères du réseau. L'authentification avec d'autres mécanismes appropriés permet d'éviter la communication avec des nœuds ayant une fausse identité, la réémission illégitime du message et l'injection des informations erronées. Celles-ci comprennent:

- ✓ **Attaque d'usurpation de l'identité d'un nœud (en anglais, Spoofing ou Impersonation) :** dans cette attaque, l'adversaire prend l'identité d'un autre nœud afin d'exercer des activités malveillantes. Par exemple : pour faire vite, l'attaquant prend l'identité d'une ambulance afin que les autres véhicules, automatiquement, lui libèrent la route. L'attaquant peut montrer qu'il a un comportement malveillant sous les identités des autres nœuds afin de dégrader leurs degrés de confiance, et par conséquent, dégrader la performance du réseau[34].
- ✓ **Attaque Replaying:** dans cette attaque, l'attaquant réinjecte des messages déjà émis par d'autres nœuds pour causer, par exemple, l'empoisonnement des tables de routage et de voisins.
- ✓ **Attaque GPS Spoofing:** cette attaque consiste à utiliser un générateur de signaux GPS qui émet des signaux plus forts que ceux émis par les satellites, afin de forcer les nœuds victimes à injecter des données géographiques falsifiées[33]. Un exemple de cette attaque est celle contre le White Rose of Drachs qui est un super-yacht de 80 millions de dollars. Cette attaque a été effectuée par Todd Humphreys, professeur de l'université de Texas, en juin 2013. Les attaquants ont contrôlé ses mouvements à distance(cf. Figure 1.8)[25].

Figure1.8:L'attaque contre le « White Rose of Drachs »[36].

- ✓ **Attaque Tunneling:** un attaquant peut exploiter la perte momentanée par un véhicule de l'information de positionnement géographique lorsque ce dernier entre dans un tunnel pour lui injecter de fausses données géographiques.
- ✓ **Attaque Sybil :** c'est une variante très dangereuse de l'attaque « Spoofing », où l'attaquant est physiquement un seul nœud, mais il utilise l'identité de plusieurs autres nœuds à la fois pour pouvoir contrôler le système et facilement monter d'autres attaques. Dans l'attaque Sybil un nœud peut prétendre être sur plusieurs positions stratégiques à la fois[37].
- ✓ **Attaque sur l'intégrité d'un message :** un nœud intermédiaire dans une communication véhiculaire peut modifier le contenu d'un message légitime pour tromper son récepteur[32].
- ✓ **Attaque de réplication de certificats et de clés cryptographiques :** elle consiste à accéder au contenu d'OBU pour récupérer les données cryptographiques. Cette attaque met le système VANET en péril, car l'entité malveillante peut générer des signatures numériques autant qu'elle veut sans qu'il y ait la possibilité de l'identifier[30].

3. L'attaque contre la confidentialité : cette attaque permet à un nœud, de manière illégitime, d'établir un profil sur les communications effectuées par les autres nœuds. Ce type d'attaque menace la vie privée des utilisateurs des réseaux VANET, du fait que l'adversaire est capable d'analyser les paquets (la

destination, le time stamp, les informations géographiques nécessaires pour le routage,..etc.) pour avoir une idée sur les activités des autres nœuds[30].

1.6 Conclusion

Les réseaux VANET sont des réseaux prometteurs qui ont un large éventail d'applications, que ce soient celles qui visent à améliorer la sécurité routière ou celles qui augmentent le confort des utilisateurs des VANETs durant le voyage. Le nombre de projets de recherche et les efforts énormes déployés par les équipes de standardisation à ce stade montrent l'importance de ces réseaux et leur permet de voir la lumière. Néanmoins, plusieurs défis techniques et économiques font face au déploiement des VANET. La sécurité est le souci principal qui préoccupe les concepteurs vue l'importance des données échangées. Dans le chapitre suivant, nous présenterons l'authentification de données dans les VANETs qui est un mécanisme fondamental pour sécuriser les VANET.

Chapitre 2

Le changement de pseudonymes dans les VANETs

2.1 Introduction

Les VANET devraient pouvoir stocker de nombreuses informations, y compris les données personnelles des propriétaires ou des conducteurs du véhicule, qui doivent être prises en compte. Ces informations privées doivent être protégées en particulier dans les communications des véhicules qui doivent être anonymes, et dans les applications liées à la sécurité qui nécessitent l'authentification des messages et de leurs origines. Changer fréquemment de pseudonyme est communément accepté comme une solution pour protéger la vie privée dans les VANET [39]. L'utilisation de pseudonymes implique que les utilisateurs acquièrent une autre identité au lieu de leur véritable identité. En effet, l'identité des attaquants à l'origine du dysfonctionnement du système doit être identifiée à des fins de révocation et de poursuites judiciaires. Ainsi, il est essentiel d'avoir également la possibilité de corréler l'identité réelle à celle utilisée dans les VANET. Cette exigence est connue sous le nom de « vie privée conditionnelle ». La gestion de l'identité est un problème complexe avec la présence de contraintes sociales, juridiques, économiques et autres liées à la sécurité routière. De nombreuses recherches ont été consacrées à la résolution des problèmes liés à ce sujet. Dans ce chapitre, nous décrivons le fonctionnement actuel de l'identification des véhicules. Ensuite, nous présentons le problème de la vie privée dans les VANET. Enfin, nous décrivons la solution Pseudonymité.

2.2 L'identité dans les VANETs

L'identité d'une entité donnée est un attribut qui l'identifie de manière unique.

Traditionnellement, les numéros de plaques d'immatriculation ont été utilisés comme identifiant principal pour un véhicule donné. Les autorités de transport en ont fait leurs processus administratifs. Par exemple, si un certain conducteur dépasse la limite de vitesse autorisée, il sera poursuivi par les autorités. Pour l'identifier, les autorités utilisent le document de véhicule.

Habituellement, on suppose que le conducteur est le propriétaire du véhicule. Cependant, ce n'est pas toujours le cas. En effet, la plaque d'immatriculation est une plaque fixée sur un véhicule à des fins d'identification, elle permet de

faire la liaison de manière unique entre un véhicule et son propriétaire et non son conducteur.

Les plaques d'immatriculation en Algérie (cf. Figure 2.1) comprennent respectivement les quatre champs suivants : les cinq premiers chiffres correspondent à un numéro spécifique (il permet d'identifier le véhicule de manière unique en considérant les autres champs), le chiffre suivant au type de véhicule, les deux suivants à l'année de mise en circulation, et les deux derniers au code de Wilaya.

La relation entre un véhicule et un conducteur n'est pas une relation un à un. Une personne peut posséder ou conduire plusieurs véhicules, comme un véhicule peut être conduit par plusieurs personnes. L'exemple de cette relation est dans les bus publics qui sont conduits par plusieurs conducteurs dans une journée donnée.

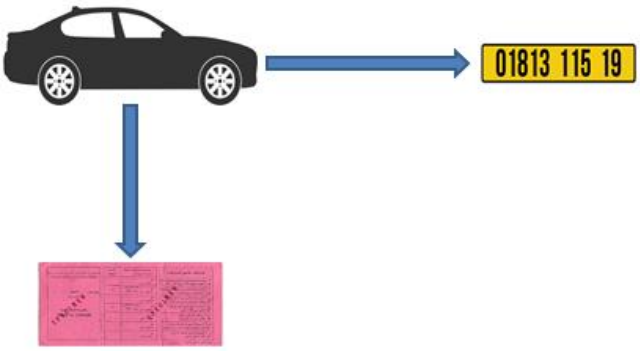

Figure2. 1:La relation entre un matricule, le propriétaire et le conducteur.

Dans les VANETs, tous les identifiants qui sont utilisés dans le système d'identification actuel devraient maintenir son rôle. La plaque d'immatriculation, le permis de conduire et le véhicule lui même sont tous des éléments d'identification dans les VANETs émergents. Les fabricants de véhicules attribuent un numéro d'identification du véhicule unique VIN (Vehicle Identification Number) qui est en relief sur le châssis, et cela peut servir d'identifiant avec des attributs tels que le fabricant, la date de production, le modèle et la couleur.

Dans les VANETs, un identifiant de véhicule (souvent abrégé VID pour «Vehicle IDentifier») peut être considéré comme un certificat signé qui permet d'authentifier sans ambiguïté un véhicule. Le VID est un identificateur de

longue durée supposé être préinstallé dans l'OBU d'un véhicule. Le VID pourrait être délivré avec l'immatriculation du véhicule et de la plaque d'immatriculation par une autorité d'immatriculation du véhicule, tel le service d'immatriculation.

2.3 Les risques de la vie privée dans les VANETs

L'échange périodique des messages beacons est indispensable dans les VANETs, car il jouera un rôle essentiel pour augmenter la prise de conscience contextuelle des véhicules.

Malheureusement, ces messages beacons contiennent des informations concernant l'identité et la position géographique des nœuds, et d'autres informations qui mettent en péril la vie privée des utilisateurs. En effet, des profils des activités personnelles des utilisateurs de VANETs peuvent être établis contenant des informations personnelles telle la trajectoire parcourue. Ce dernier scénario est connu dans la littérature sous le nom de « Big brother scenario »(cf. Figure 2.2)[40].

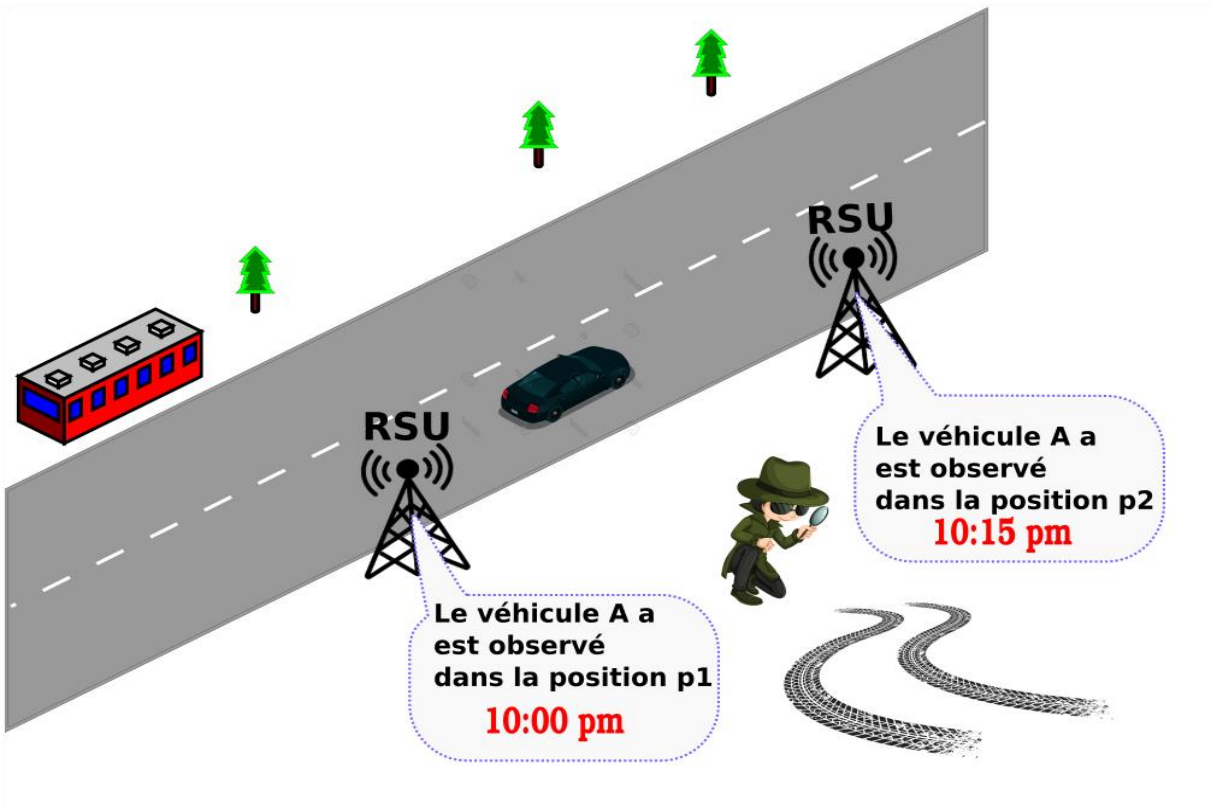

Figure2.2:Le syndrome Big Brother.

2.4 Les pseudonymes pour assurer la vie privée dans les VANETs

Chaum [19] a introduit les pseudonymes numériques, en tant que clé publique utilisée pour vérifier les signatures faites par le détenteur anonyme de la clé privée correspondante, afin de fournir l'anonymat aux transactions électroniques. Pftzmann et Hansen [20], ont défni les pseudonymes numériques comme une chaîne de bits qui est unique comme identifiant (du moins avec une probabilité très élevée). Elle peut être utilisée pour authentifier les messages de son détenteur. Nous pouvons conclure qu'un pseudonyme doit être utilisé pour l'authentification, mais ne doit contenir aucune information personnelle qui pourrait être liée à l'identité réelle du titulaire du pseudonyme. Toutefois, le titulaire peut utiliser un ensemble de pseudonymes pour assurer son anonymat. Une entité dans un réseau peut soit changer les pseudonymes au fil du temps pour éviter de corréler les actions effectuées sur une longue période de temps, soit un pseudonyme différent pourrait être utilisé pour chaque action.

2.5 Classification des systèmes de pseudonymes

En examinant les mécanismes cryptographiques utilisés pour la réalisation des systèmes de pseudonymes, quatre grandes catégories peuvent être distinguées dans les VANETs :

Les systèmes basés sur la cryptographie asymétrique: dans cette catégorie, les pseudonymes sont généralement représentés par des clés publiques[41]. Pour faciliter la vérification des messages reçus par les véhicules, un certificat de pseudonyme doit être envoyé conjointement avec le message.

Les systèmes basés sur la cryptographie basée sur l'identité : ils permettent d'atteindre les mêmes objectifs, mais ils ne nécessitent pas de certificats à clés publiques explicites. Cela permet, d'une part, d'éviter d'échanger des informations cryptographiques de taille importante, mais introduit de nouveaux défis pour la génération de pseudonymes d'autre part[42].

Les systèmes de pseudonymes basés sur les signatures de groupe : ils introduisent une clé privée pour un groupe de véhicules, qui permet à une

entité d'un groupe de générer une signature au nom de celui-ci, c'est à dire, que la signature peut être vérifiée à l'aide d'une clé publique correspondante. Malgré que ces systèmes offrent, généralement, l'anonymat aux signataires au sein du groupe[43] et réduisent la nécessité de changements de pseudonyme, ils posent de nouveaux défis pour la résolution de pseudonyme et la révocation.

Les systèmes basés sur la cryptographie symétrique: ils sont attrayants en raison de leur efficacité de calcul. Dans ces systèmes, un récepteur doit connaître la clé secrète (partagée entre l'émetteur et le récepteur) pour être en mesure d'authentifier l'émetteur.

2.6 Le pseudonymat conditionnel

La partie secrète du pseudonyme (l'information qui permet de déduire l'identité réelle) ne doit être connue que de son titulaire.
Il s'agit de garantir l'anonymat de l'identité réelle d'un véhicule honnête, à moins que des activités malveillantes ou la suspicion de la présence d'un comportement malveillant ne soient détectées par une autorité spéciale que pouvant déterminer les identités correspondantes. Cette dernière opération est appelée résolution de pseudonyme. Cette caractéristique permet de satisfaire l'objectif de non-répudiation.

2.7 Le modèle d'adversaire

Les attaques à la vie privée appartiennent aux catégories suivantes :

1. Attaque de position unique : dans cette attaque, l'entité malveillante essaye de localiser la position ou déterminer l'identité d'un nœud en analysant le contenu d'une requête.

2. Attaque de positions multiples : dans cette attaque, l'entité malveillante essaye de corréler les différents pseudonymes et d'établir le chemin complet parcouru par un nœud (cf. Figure 2.3).

3. Attaque à base de contexte : elle consiste à utiliser des informations personnelles concernant la victime comme des contrats signés avec des entreprises spécifiques, ses préférences et ses intérêts pour faire la corrélation spatiotemporelle et établir un profil d'activité de l'utilisateur. Une autre

attaque qui est classée dans cette catégorie est l'identification de l'empreinte radio d'un nœud[39].

4. Attaque à travers d'un tiers de confiance compromis : si un attaquant parvient à compromettre un tiers de confiance, il peut accéder aux informations qui lui permettent de mettre la vie privée des utilisateurs des VANETs en péril.

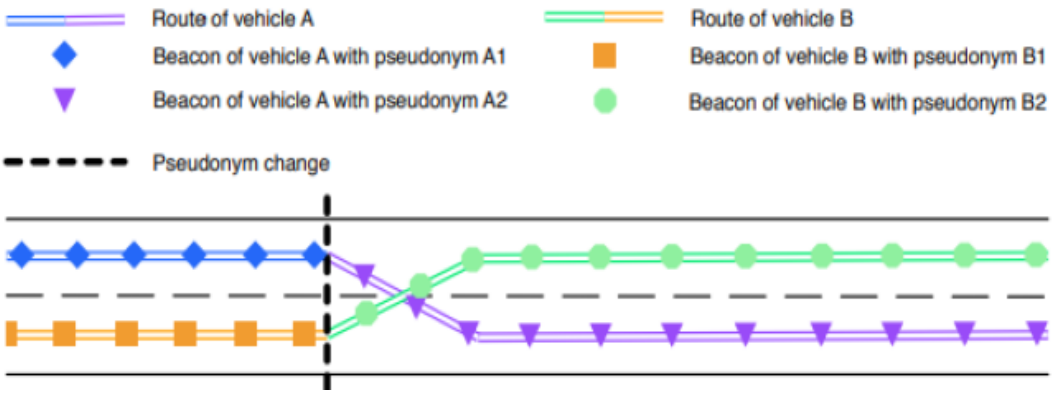

Figure2.3:La traque d'un véhicule [43].

Un réseau véhiculaire est un système distribué complexe où un adversaire peut effectuer différents types d'attaques selon ses capacités. En se basant sur les dimensions de la classification d'attaques dans [45], nous décrivons le modèle d'attaquant comme suit :

- ✓ **Global ou Local :** cette dimension définit le rayon d'action de l'adversaire. Un adversaire local a un nombre limité de stations qui écoutent le trafic du réseau. Par exemple, les stations d'écoute déployées aux intersections de la route peuvent écouter le communications des nœuds entrants et sortants de l'intersection[46]. Un attaquant global peut suivre les chemins de n'importe quel véhicule, en écoutant leurs messages diffusés, dans la région de ses intérêts[47][48]. Il peut exploiter des infrastructures déployées (RSUs par exemple) aux bords des routes. Cet attaquant peut avoir intérêt à avoir une idée sur le modèle de mobilité afin de personnaliser des annonces publicitaires ou réaliser des techniques de datamining[49]. Donc, l'attaquant peut être un gouvernement ou de grandes entreprises comme les opérateurs de télécommunication.

- ✓ **Actif ou Passif :** un adversaire passif n'injecte ni ne modifie des messages, mais il collecte des pseudonymes à des points stratégiques (comme les intersections) où il dispose d'une station d'écoute. Les activités malveillantes d'un adversaire actif dépendent du mécanisme d'utilisation et du changement de pseudonyme. Cet adversaire pourrait bloquer le changement de pseudonyme, forcer son changement, ou perturber sa gestion. Il existe une variante d'attaque active très connue appelée l'attaque d'épuisement de pseudonymes, où un attaquant vise à forcer leurs changements, de manière répétitive, jusqu'à ce que l'ensemble des pseudonymes de véhicule ciblé soit épuisé. Dans cette situation, la victime doit contacter l'autorité pour acquérir de nouveaux pseudonymes.
- ✓ **Interne ou Externe :** un attaquant interne est authentifié dans le réseau et peut avoir, par conséquent, plus de capacité pour écouter et analyser le trafic, alors que l'attaquant externe a plus de difficultés à analyser les messages qui sont éventuellement chiffrés. Donc, l'attaquant interne a plus de chance de corréler les différents pseudonymes utilisés par un seul nœud.

2.8 Les exigences de pseudonymat dans les VANETs

Les attaques éventuelles définissent les exigences qui doivent être pris en compte par un système de pseudonymes. L'exigence de la vie privé principal est de rester intraçable et anonyme. Néanmoins, une balance doit être établie entre les exigences de la sécurité et celles de la vie privée. Dans ce contexte, Schaub et al.[50] ont défini les exigences suivantes :

a-La divulgation minimale : la quantité d'informations à révéler dans une communication doit être minimale. Par exemple : Pas plus que les informations nécessaires pour une communication V2X (V2I, V2V ou V2P).

b-L'anonymat conditionnel : un émetteur d'un message doit être anonyme parmi un ensemble d'émetteurs éventuels. Cet ensemble est appelé l'ensemble d'anonymat du message. Comme l'identité du conducteur doit être résolue en cas de conflit, l'anonymat est conditionnel dans les VANETs.

c-La non-corrélation : elle nécessite que la relation entre deux pseudonymes de la même entité physique dans le réseau ne doit pas être trouvée.

d-L' autorité de résolution distribuée : l'aptitude de résolution d'identité doit être distribuée à plusieurs autorités de telle manière que la coopération entre plusieurs d'entre elles soit nécessaire pour corréler les pseudonymes d'un individu.

e-La résolution parfaite : une opération de résolution de pseudonymes pour une entité x ne doit pas mener à (ou augmenter les chances de) révéler la vraie identité des nœuds qui sont pas en question.

Nous donnons ci-après les caractéristiques qui doivent être satisfaites par un pseudonyme pour protéger la vie privée :

1. La limitation de durée de vie : afin d'empêcher la traque, un pseudonyme doit avoir une durée de vie limitée. Cette caractéristique peut être garantie à l'aide du certificat qui accompagne le pseudonyme.

2. L'unicité : afin d'éviter qu'une identité à court terme soit utilisée par plusieurs véhicules, chaque pseudonyme doit être unique. Cette caractéristique est garantie par le système cryptographique de base qui est utilisé pour générer les pseudonymes.

3. La disponibilité : un nouveau pseudonyme doit être toujours disponible pour un éventuel changement de pseudonyme. Cette caractéristique peut être garantie en stockant un très grand nombre de pseudonymes dans l'OBU.

4. Le verrouillage de changement de pseudonyme : cette caractéristique est nécessaire pour empêcher des attaques comme l'épuisement de pseudonymes.

5. L'abandon des anciens identifiants : une fois, un nouveau pseudonyme est utilisé, n'importe quel ancien identifiant au niveau de la pile protocolaire doit être aussi changé afin d'empêcher la traque. Par exemple : les identifiants utilisés le standard ETSI[51],sont dérivés du pseudonymes.

2.9 Le cycle de vie abstrait d'un pseudonyme

Vu les nombreuses exigences de la vie privée dans les VANETs, un nombre important de systèmes de changement de pseudonyme ont été proposés. Ces systèmes paraissent divergents à première vue. Néanmoins, comme ces systèmes sont tous soumis aux caractéristiques de l'environnement véhiculaire, cela nous mène à avoir un cycle de vie abstrait (cf. Figure 2.4) similaire à la plupart des approches des pseudonymes dans les réseaux véhiculaires. L'objectif principal d'un pseudonyme est d'authentifier l'émetteur s'il est valide. Cela peut être achevé en certifiant l'émetteur en tant que véhicule, ou implicitement en assurant que les seuls véhicules valides peuvent faire certaines actions comme la signature de groupe.

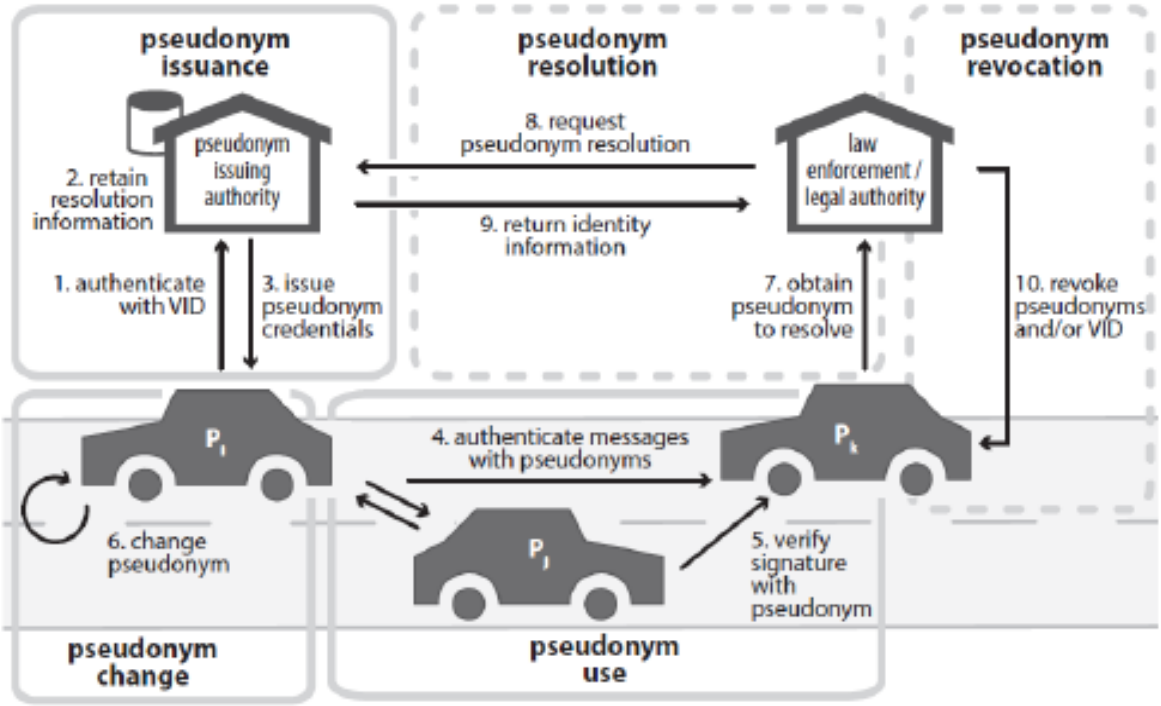

Figure2.4:Le cycle de vie abstrait d'un pseudonyme[52].

Dans les réseaux véhiculaires, les pseudonymes passent par un cycle de vie abstrait commun résultant des exigences précédentes. Avec certains systèmes d'authentification de pseudonymes spécifiques, une partie des phases du cycle de vie peuvent s'écarter de notre modèle de cycle de vie abstrait. Cependant, les phases décrites ci-après peuvent être trouvées dans presque tous les systèmes d'authentification de pseudonymes.

Un cycle de vie abstrait d'un pseudonyme comporte les phases suivantes: la génération et l'émission, l'utilisation, le changement, la résolution et la révocation. La phase de génération et d'émission de pseudonyme doit prendre en compte, à l'avance, celle de la résolution de pseudonyme. Les autres phases aussi dépendent intrinsèquement des mesures prises dans le processus de génération et d'émission de pseudonyme pour qu'elles soient efficaces. L'utilisation de pseudonyme et son changement s'influencent mutuellement et dépendent aussi de la manière de génération ou d'obtention des pseudonymes par les véhicules. Certaines phases sont également en option : par exemple, les systèmes ne considèrent pas tous la résolution de pseudonyme ou la révocation. Dans ce qui suit, nous définissons et discutons chaque phase et soulignons leurs défis spécifiques.

1-Génération et émission de Pseudonyme

Presque tous les systèmes d'authentification de pseudonymes pour les communications véhiculaires supposent qu'un véhicule possède un identifiant numérique unique. Bien que le VID est nécessaire pour l'émission de pseudonymes par la plupart des systèmes proposés, la génération de VID lui-même n'est généralement pas considérée comme faisant partie du système de pseudonymes ou du cycle de vie de pseudonymes, parce qu'ils sont des processus séparables. Dans le processus d'émission de pseudonymes, le VID est utilisé pour authentifier l'OBU du véhicule pour s'assurer que seuls les véhicules valides peuvent obtenir des pseudonymes et peuvent donc participer aux communications véhiculaires. Pour la génération de pseudonymes, deux approches principales peuvent être distinguées: la génération par un tiers de confiance et l'auto-génération.

- ✓ Émission par des tiers : cette approche est adoptée par la plupart des systèmes, les pseudonymes étant générés par une autorité émettrice de pseudonymes. Selon le système, cette entité peut être composée de plusieurs sous-entités : Autorité de certification (CA), Pseudonyme Fournisseur (PP), l'architecture de sécurité de l'ETSI les appelle les autorités d'enregistrement et d'autorisation.
  Le rôle de l'autorité émettrice de pseudonymes est généralement attribué aux infrastructures gérées par les AC et les PP, ou par les

RSU. Dans les deux cas cas, il authentifie le véhicule avec son VID, et vérifie l'admissibilité du véhicule à obtenir des pseudonymes (c.VID est valide et n'a pas été révoqué).

- ✓ Auto-émission : l'OBU d'un véhicule est plus autonome et peut générer les pseudonymes dont il aura besoin. Il est donc possible de minimiser la capacité de stockage requise pour le pseudonyme du pool (l'ensemble des pseudonymes disponibles dans un OBU). Cependant, sibylle attaque sont généralement plus difficiles à éviter dans ces systèmes en raison de le niveau d'autonomie.

2- L'utilisation de pseudonyme

Une fois qu'un véhicule a obtenu des pseudonymes, il peut communiquer avec d'autres véhicules ou infrastructures. L'utilisation d'un pseudonyme comporte deux étapes : l'authentification des messages sortants et la vérification des messages reçus.

En général, les systèmes d'authentification pseudonyme utilisent soit des signatures asymétriques, soit des codes d'authentification de message. L'authentification d'un message nécessite la vérification de la validité d'un pseudonyme. Un pseudonyme valide doit être généré soit par une autorité vérifiable de confiance avec un certificat d'accompagnement, soit indépendamment et peut être authentifié avec des paramètres secrets.

3-Le changement de pseudonyme

Les actions effectuées sous un pseudonyme peuvent être liées les unes aux autres, en raison des caractéristiques mentionnées des pseudonymes.

La modification d'un pseudonyme affecte presque toute la pile de protocoles.

Les identifiants de réseau tels que les adresses IP et MAC doivent tous être modifiés simultanément pour éviter les liens triviaux entre l'ancien et le nouveau pseudonyme.

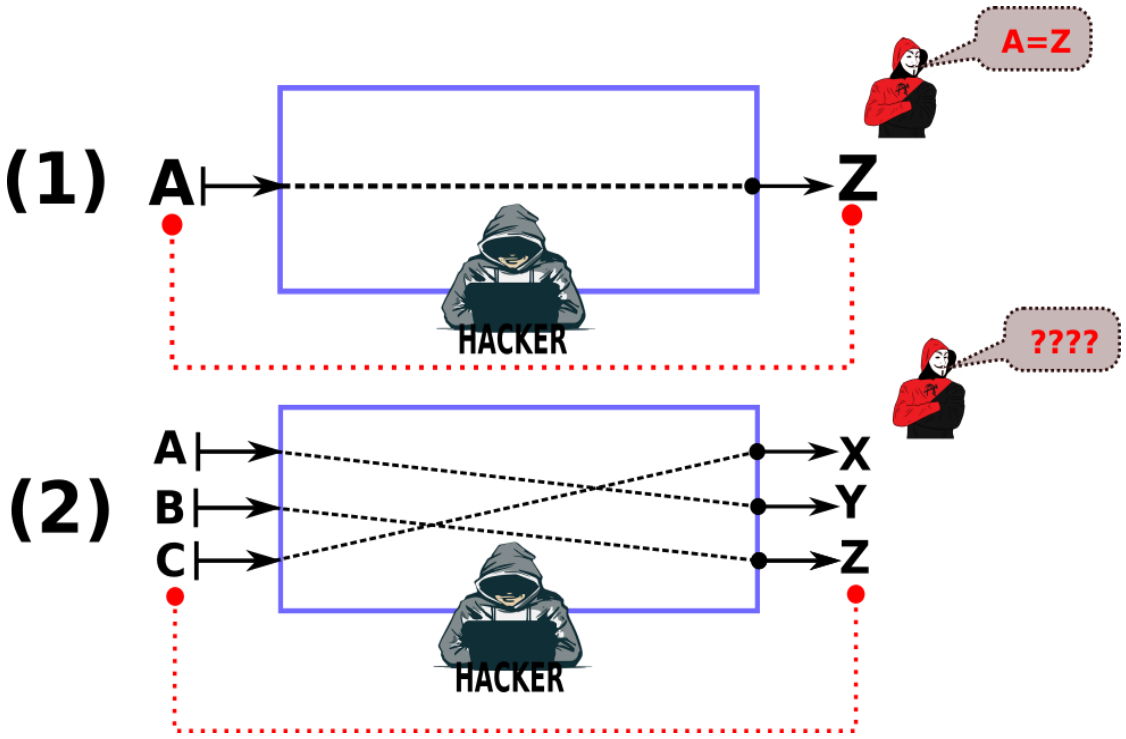

Figure2.5:Le contexte de changement de pseudonyme.

Un autre aspect important est la nécessité d'avoir des véhicules voisins lors du changement de pseudonyme. Comme le montre la figure 2.5, changer le pseudonyme seul n'est pas suffisant pour embrouiller un observateur, en surveillant les emplacements avant et après le changement de pseudonyme, il sera facile pour l'observateur de faire le lien entre deux pseudonymes consécutifs utilisés par un nœud. Alors que dans le second cas où plusieurs nœuds changent de pseudonyme simultanément, un éventuel observateur peut éprouver de la confusion.

La figure 2.6 illustre un algorithme général pour changer le pseudonyme dans les VANET. Dans cet algorithme, les nœuds prennent en compte leurs contextes (comme le nombre de voisins, leurs directions et leurs vitesses) et peuvent collaborer afin de décider du meilleur moment pour changer leurs pseudonymes [39].

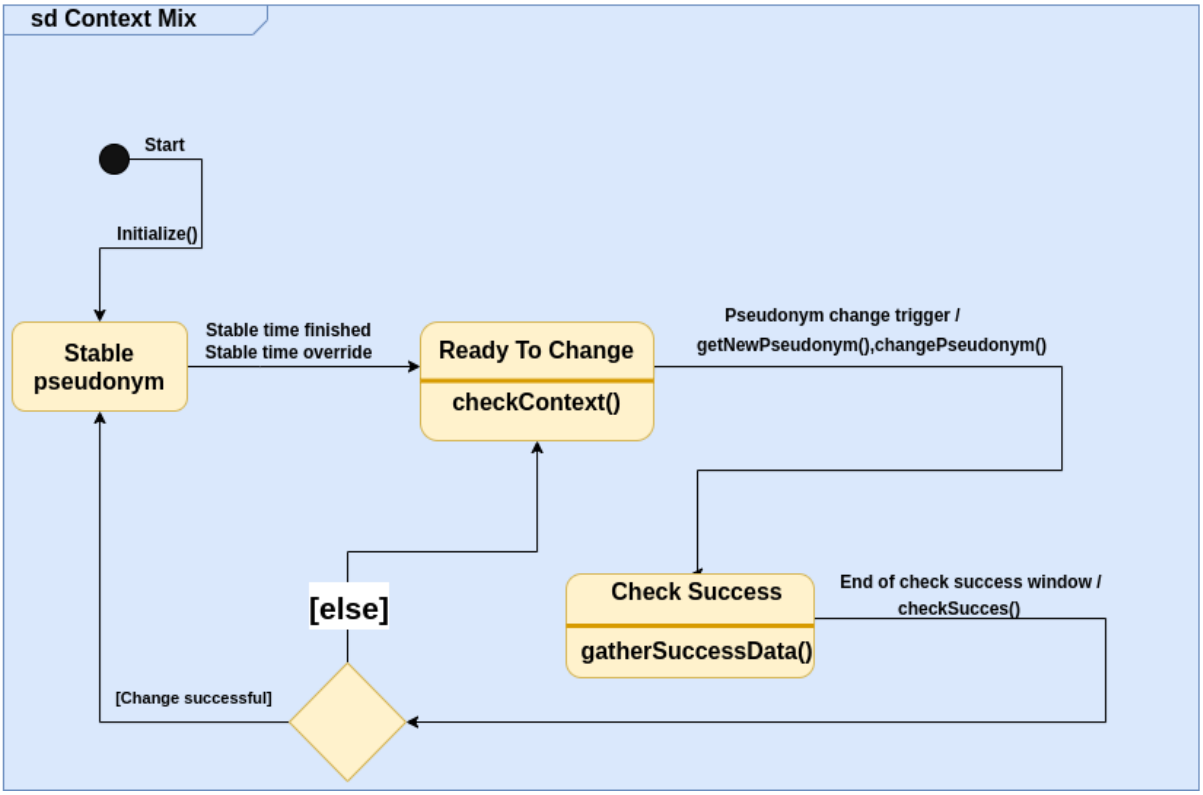

Figure2.6: Un algorithme général pour le changement de pseudonyme .

Selon cet algorithme, le processus de gestion d'un pseudonyme comprend trois phases :

- ✓ La phase de pseudonyme stable : C'est une période pendant laquelle le véhicule ne change pas de pseudonyme et reste dans cette phase jusqu'à avoir un déclencheur pour passer à la phase de prédisposition.

- ✓ La phase de prédisposition : Le véhicule vérifie son contexte pour choisir le bon moment pour changer de pseudonyme, certaines techniques peuvent être utilisées pour créer de la confusion et renforcer la confidentialité dans cette phase.

- ✓ la phase de vérification réussite du changement de pseudonyme : Un véhicule vérifie si le changement de pseudonyme s'effectue dans de bonnes conditions.

4- Résolution des pseudonymes

Elle n'est pertinente que pour la responsabilisation des nœuds malveillants. En cas de détection d'un comportement inapproprié, les représentants des forces de l'ordre déposent une demande de résolution de pseudonyme auprès du fournisseur de pseudonyme pour obtenir le VID du détenteur du pseudonyme. Il s'agit d'améliorer la confidentialité des utilisateurs de VANET.

5- Révocation de pseudonyme

Les nœuds malveillants doivent être révoqués du réseau du véhicule pour assurer son bon fonctionnement. Il s'agit de la révocation des informations d'authentification du nœud (pseudonymes, VID ou les deux). Si seuls des pseudonymes spécifiques ont été révoqués, il y aura une possibilité que le véhicule correspondant puisse avoir d'autres pseudonymes qui peuvent être utilisés pour de futures communications. Si tous les pseudonymes d'un nœud doivent être révoqués, les informations nécessaires pour identifier tous ses pseudonymes doivent être mises en œuvre. Cette possibilité affaiblira considérablement la confidentialité offerte par les pseudonymes.

2.10 Les techniques de changement de pseudonyme

Un paramètre important pour les changements de pseudonyme est le taux de changement. Il influence la communication, la capacité de mémoire de stockage nécessaire et le niveau de confidentialité. De plus, un simple changement de pseudonyme ne suffit pas pour éviter le tracking.

À cette fin, plusieurs stratégies de changement de pseudonyme ont été proposées, notamment :

1- Changement périodique : Dans cette stratégie, un véhicule change de pseudonyme à chaque intervalle de temps prédéfini (voir Figure 2.7), Eckhoff et al.[53] introduit des changements de pseudonyme temporels, afin d'avoir la possibilité de changer le pseudonyme même en l'absence de fournisseurs de pseudonymes.

Malheureusement, leur solution est inefficace une fois que l'attaquant a connu la période utilisée pour les pseudonymes.

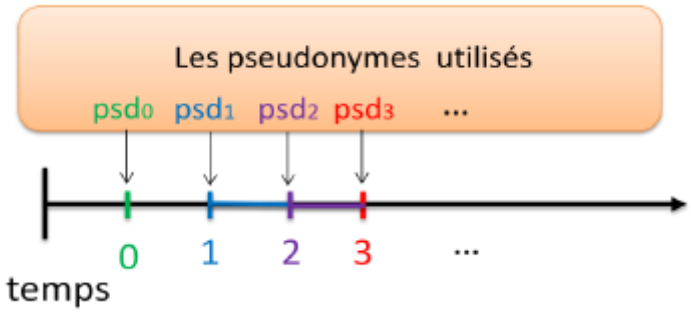

Figure2.7:Le changement périodique.

2- Le changement aléatoire: afin de résoudre le problème de la période de changement fixe, les véhicules peuvent changer la leur selon une période aléatoire (voir Figure 2.8) [55]. Par conséquent, un attaquant ne peut pas prédire le prochain changement de pseudonyme. Cependant, le suivi est toujours possible, si peu de véhicules changent de pseudonyme à un moment précis. De plus, une analyse à long terme permet d'identifier les véhicules qui réutilisent leurs pseudonymes.

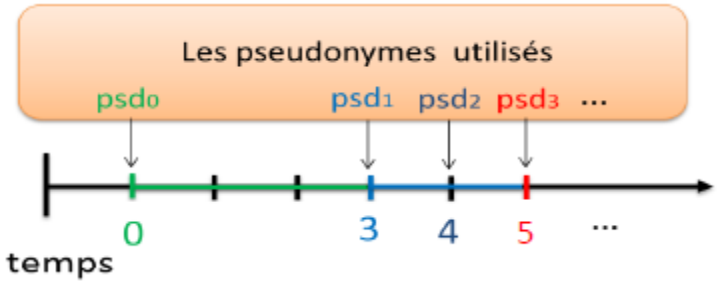

Figure2.8:Le changement aléatoire.

3- La période de silence entre les changements de pseudonyme :

Dans le système de changement CARAVAN [55], un véhicule n'accède pas au canal pendant un certain temps (la période de silence) avant de changer de pseudonyme. La période de silence rend les atteintes à la vie privée difficiles. Si un véhicule utilise la stratégie de période de silence dans une intersection, il sera difficile d'empêcher son déplacement. Cette stratégie consiste à faire un compromis entre intimité et sécurité routière.

4- Changement autonome : Dans cette stratégie, les véhicules déterminent indépendamment où et quand changer leurs pseudonymes. Les deux protocoles Swing et Swap proposés par Li et al [56] adoptent cette stratégie. Dans Swing, les véhicules changent de pseudonyme lorsqu'ils changent de vitesse et de direction. Ainsi, un attaquant ne peut pas prédire le mouvement des nœuds pour établir une corrélation entre leurs emplacements avant et après le changement de pseudonyme. Dans Swap, chaque paire de véhicules échange ses pseudonymes, lors du changement de pseudonyme avec une probabilité de 0,5, puis entre dans une période de silence aléatoire. Ils sont donc indiscernables des autres véhicules. Dans un autre protocole appelé SLOW [57], si la vitesse d'un véhicule descend en dessous de 30 km/h, il entre dans une période de silence et change de pseudonyme.

5- Changement basé sur la densité (La stratégie CROWD) : Dans cette stratégie, le changement de pseudonyme dépend du nombre de voisins actuels. Par conséquent, un véhicule peut éviter le changement de pseudonyme inefficace (lorsqu'il est isolé par exemple). D'après Chaurasia et al.[58][59]. le changement de pseudonyme doit être effectué si la taille de l'ensemble des véhicules voisins est supérieure à un seuil déterminé.

6- Changement collaboratif (synchrone) : Lorsqu'un véhicule change seul de pseudonyme, il est facilement victime d'attaques de pistage. Une meilleure stratégie consiste à changer le pseudonyme simultanément avec ses voisins. Pour cela, le véhicule diffuse un message à ses voisins pour les informer qu'il est dans l'état prédisposé [60]. Cette stratégie crée une Mix-zone où les véhicules, dans la même zone, changent simultanément leurs pseudonymes qui sont soigneusement sélectionnés et sont généralement des intersections routières [61]. Lu et al.[62] suggèrent de placer des Mix-zones dans les Social Spots (par exemple feu de circulation, parking, etc.) pour augmenter le nombre de véhicules changeant de pseudonyme simultanément. L'inconvénient de cette approche est la faible protection de la vie privée dans les scénarios de faible densité de véhicules.

Bien qu'il existe de nombreuses stratégies proposées pour changer les pseudonymes, nous ne pouvons pas savoir laquelle est la plus efficace dans la pratique. Mais, en fonction des objectifs d'anonymat définis ou de métriques

telles que la vitesse de traitement, la taille des messages échangés, la capacité de stockage requise, le degré d'anonymat souhaité, la complexité de résolution des pseudonymes, on peut déterminer lequel est mieux adapté.

2.11 Systèmes de révocation de pseudonyme

Vu de la nature décentralisée des réseaux de véhicules et de leur taille, la diffusion des dernières informations de révocation constitue un enjeu majeur pour un changement efficace de pseudonyme et de révocation [63]. La classification du système de révocation des pseudonymes dans les VANET est la suivante :

a-La révocation passive :

Dans cette catégorie, la révocation de pseudonyme est limitée à la révocation de VID pour des raisons d'évolutivité. Si l'identité à long terme est révoquée, aucun nouveau pseudonyme ne peut être obtenu. selon [64][65] la distribution des CRL (Certificate Revocation List) aux OBU n'est pas pratique, en raison de la fréquence élevée des messages et de la taille des CRL qui peut éventuellement être importante. D'autre part, en révoquant uniquement le VID, le véhicule correspondant peut continuer à participer au réseau jusqu'à ce que tous ses pseudonymes aient expiré, cette approche de révocation globale est connue sous le nom de révocation passive [66]. Une solution à ce problème est de réduire la durée de vie des pseudonymes à un temps très court [67].

Cette approche soulève des défis tels que le changement de pseudonyme, son rechargement et la protection de la vie privée.

b-Auto-révocation :

Cette catégorie de protocoles de révocation [68], consiste à envoyer des notifications d'un comportement malveillant détecté par des véhicules voisins du nœud malveillant à l'autorité de révocation (voir Figure 2.9). Ensuite, l'autorité envoie un message OSR (Order of Self-Revocation) au TPD1 (Tamper Proof Device) du véhicule malveillant détecté (le véhicule malveillant est noir dans la configuration ci-dessous) en mode géocast [69] toutes les Trepeat secondes jusqu'à ce que le le TPD du nœud malveillant confirme la suppression de tous les pseudonymes stockés. Notez que le rayon de la région de

géodiffusion est incrémenté à chaque itération pour augmenter les chances que le TPD du véhicule malveillant reçoive le message OSR.

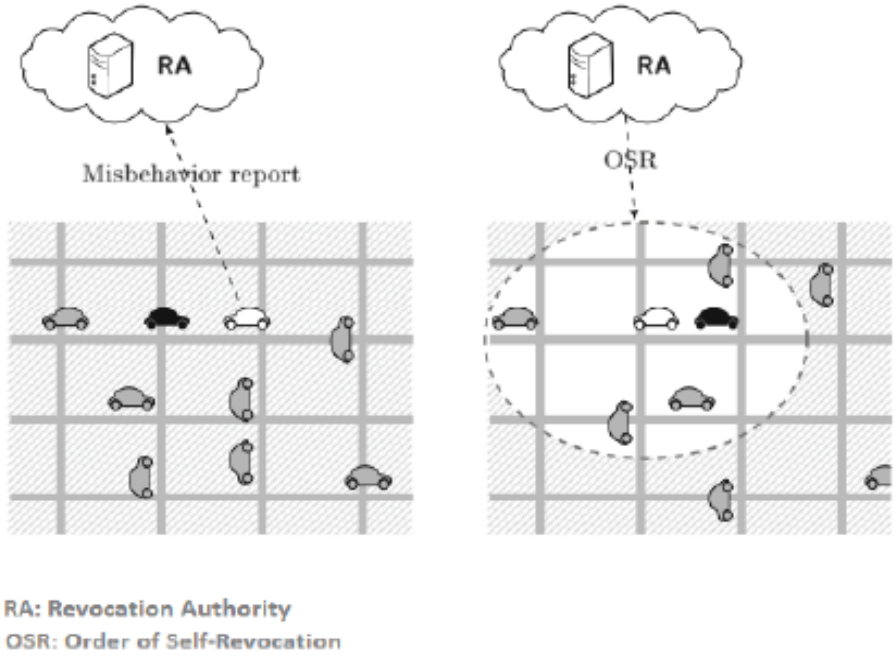

Figure2.9:Le protocole de révocation REWIRE[71].

3- Révocation de pseudonyme basée sur un seuil :

Les techniques de révocation de cette catégorie reposent généralement sur des systèmes de vote qui consistent à compter le taux de nœuds accusant un nœud malveillant et à le révoquer si le taux dépasse un seuil prédéfini. Ils sont nécessaires pour avoir l'aspect distribué du mécanisme de révocation.

Ces techniques peuvent être plus rapides, mais elles présentent des problèmes liés à l'utilisation du concept d'anonymat. En effet, les chercheurs qui ont développé ces techniques n'ont pas pris en compte le cycle de vie des pseudonymes qui a un grand impact sur leurs techniques. Une nouvelle étude est donc nécessaire sur l'impact de l'anonymat sur cette catégorie.

4-L'approche de preuve de non-révocation

Cette approche a été proposée par Ganan et al.[70] en présentant la technique EPA (Efficient and Privacy-Aware revocation mécanisme for vehicular Ad-hoc network) pour minimiser le taux de faux positifs.

L'idée principale de l'EPA, elle permet à chaque véhicule de prouver la validité de son pseudonyme et qu'il n'a pas été révoqué récemment au lieu d'obliger les véhicules à télécharger de grandes listes de révocation. Ces preuves peuvent être obtenues par le CA (Certification Authority) en construisant un MHT (Merkle Hash Tree) qui peut être obtenu à partir de la liste des nœuds révoqués. Ainsi, les traces des informations de révocation et l'ensemble des pseudonymes révoqués peuvent être représentés dans un seul champ (la racine de MHT). A chaque fois, un nœud souhaitant obtenir des informations lui permettant de prouver son existence dans le réseau, il doit communiquer de manière sécurisée avec un RSU. Le RSU doit utiliser le MHT afin de vérifier la validité (non-révocation) de ce nœud avant de transmettre les données de certification requises (voir Figure 2.10). L'inconvénient de cette approche est que les nœuds doivent, de temps en temps, trouver un moyen de communiquer avec les RSU. Il est donc difficile de définir le délai d'expiration de la preuve de non-révocation.

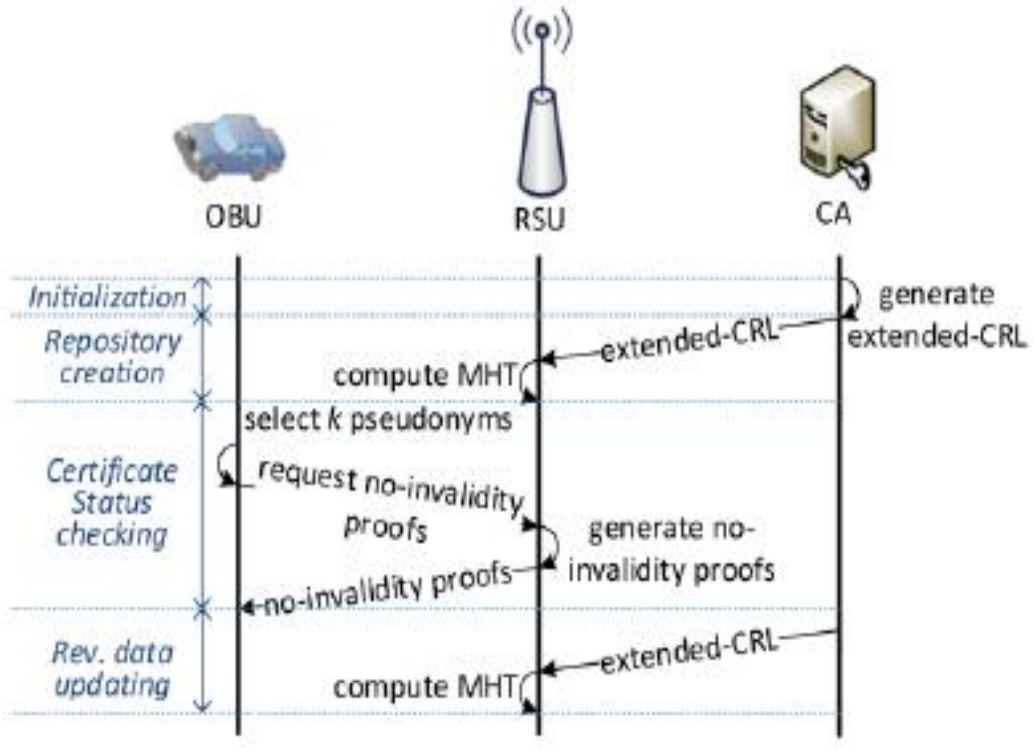

Figure2.10:Les étapes de la technique de révocation de l'EPA [72].

2.12 Conclusion

L'anonymat des futurs utilisateurs des réseaux de véhicules doit être étudié et analysé de manière intensive afin que les systèmes développés sur ces réseaux ne violent pas et ne satisfassent pas aux exigences de sécurité et de confidentialité des VANET. Le pseudonyme est l'approche la plus acceptée dans la communauté des chercheurs pour ce problème. Cependant, il reste encore des défis auxquels les concepteurs sont confrontés.

Chapitre 3

Notre technique de défense contre le changement fréquent de pseudonyme.

3.1 Introduction

Dans les réseaux véhiculaires, le problème majeur est l'établissement de la confiance. Pour éviter tout suivie illégale des véhicules et garantir la confidentialité dans les réseaux VANET.

Le mécanisme de changement de pseudonyme est une solution efficace pour assurer l'anonymat des véhicules dans les réseaux VANET, mais cette technique a ses propres problèmes tels que l'attaque Sybil ou le changement fréquent de pseudonyme pour attaquer le système ou essayer de retrouver la liaison entre deux pseudonymes.

Dans ce chapitre, nous commençons d'abord par une description de notre solution pour détecter et empêcher toute tentative malveillante de changement de pseudonyme en détectant tout comportement malveillant à l'aide de l'estimation de position, ensuite nous essayons de prouver que cette tentative de changement de pseudonyme est malveillante en fonction du voisin de ce nœud, enfin nous analysons la performance de notre protocole avec les différentes simulations.

3.2 Problématique

Le problème le plus important dans le mécanisme de changement de pseudonyme est les utiliser pour attaquer ou paralyser le système de pseudonymes, l'attaque Sybil et le changement fréquent des pseudonymes sont des attaques peut considérons parmi les plus dangereuses attaques sur les réseaux VANNET.

1. L'attaque Sybil : le nœud malveillant généré deux pseudonymes différents PSD1 et PSD2 (cf. la figure 3.1) simultanément avec deux positions différentes,

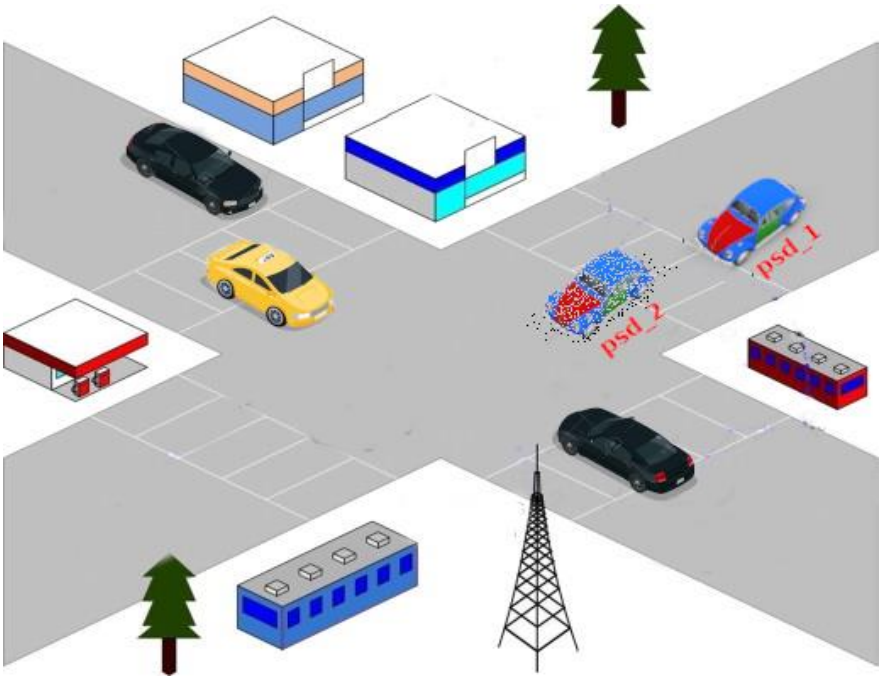

Figure3.1: Attaque sybil.

le pseudonymes Psd 2 (Sybil node) peut prendre le rôle d'une passerelle de PSD1 (Sybil Lancer), cette attaque peut envoyer des fausses informations au nœud victime.

2. L'attaque utilisant un changement fréquent de pseudonymes :dans ce cas le nœud malveillant fréquemment change son pseudonyme en demandant périodiquement un nouveau pseudonyme.

Cette attaque permet de déterminer le lien entre les pseudonymes ainsi de l'utiliser pour d'autres attaques.(cf. figure 3.2).

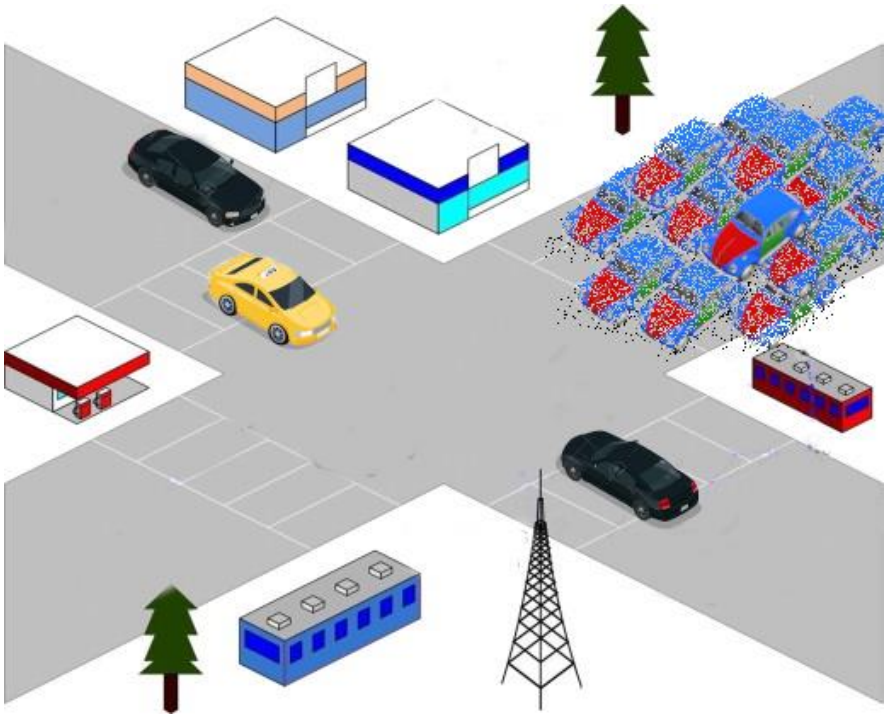

Figure3.2:Attaque changement fréquent des pseudonymes.

3.3 Solution proposée

Afin de résoudre ce problème, nous proposons une technique DCCFP(Défense Contre Changement Fréquent de pseudonyme) visant à empêcher tout nœud suspect d'utiliser plus d'un pseudonyme avant la fin de la durée de vie de pseudonyme.

Comme le montre la figure 3.3, cette technique vise à faire en sorte que le nœud recevant du «message hello» vérifie si l'expéditeur suspect utilise un pseudonyme valide ou l'a modifié à ce moment-là en utilisant ses voisins.

Lorsque le nœud reçoit «hello message», ce dernier vérifie si le nœud suspect est en «quarantaine» ou non.

Si le nœud suspect n'existe pas dans la «quarantaine», le nœud récepteur utilisé trois de ses voisins pour savoir si le nœud suspect a été voisin de ces trois auparavant ou non, si ce nœud suspect est nouvellement présent il est ajouté dans la liste de «quarantaine» pour une certaine période de temps et à partir de là la liste de «quarantaine» est déterminé.

Dans le cas où le nœud suspect était auparavant et était voisin des trois nœuds précédemment sélectionnés, il est accepté.

Mais si le nœud suspect est présent dans la «quarantaine», on vérifie si la durée est supérieure ou égale au seuil (Durée>=Seuil), c'est-à-dire qu'il a expiré dans la «quarantaine», on l'accepte dans ce cas.

Dans le cas contraire, le message envoyé est ignoré.

-Observation :

Nous considérons chaque nœud proche d'un voisin des voisins du nœud récepteur en matière de localisation comme suspect, où nous estimons la localisation en utilisant rapidement et les coordonnées des voisins selon l'équation suivante :

$$Xe=Xni+Vxi(Tc-Ti).$$

$$Ye=Yni+Vyi(Tc-Ti).$$

Xni : coordonnées x pour le voisin i.

Yni : coordonnées y pour le voisin i.

Xe : estimation de X.

Ye : estimation de Y.

Tc: le moment courant.

Ti: le moment où le voisin i est envoyé le message.

Si la distance entre Xe et Ye est inférieur à 2 mètres, alors on considère le nœud comme suspect.

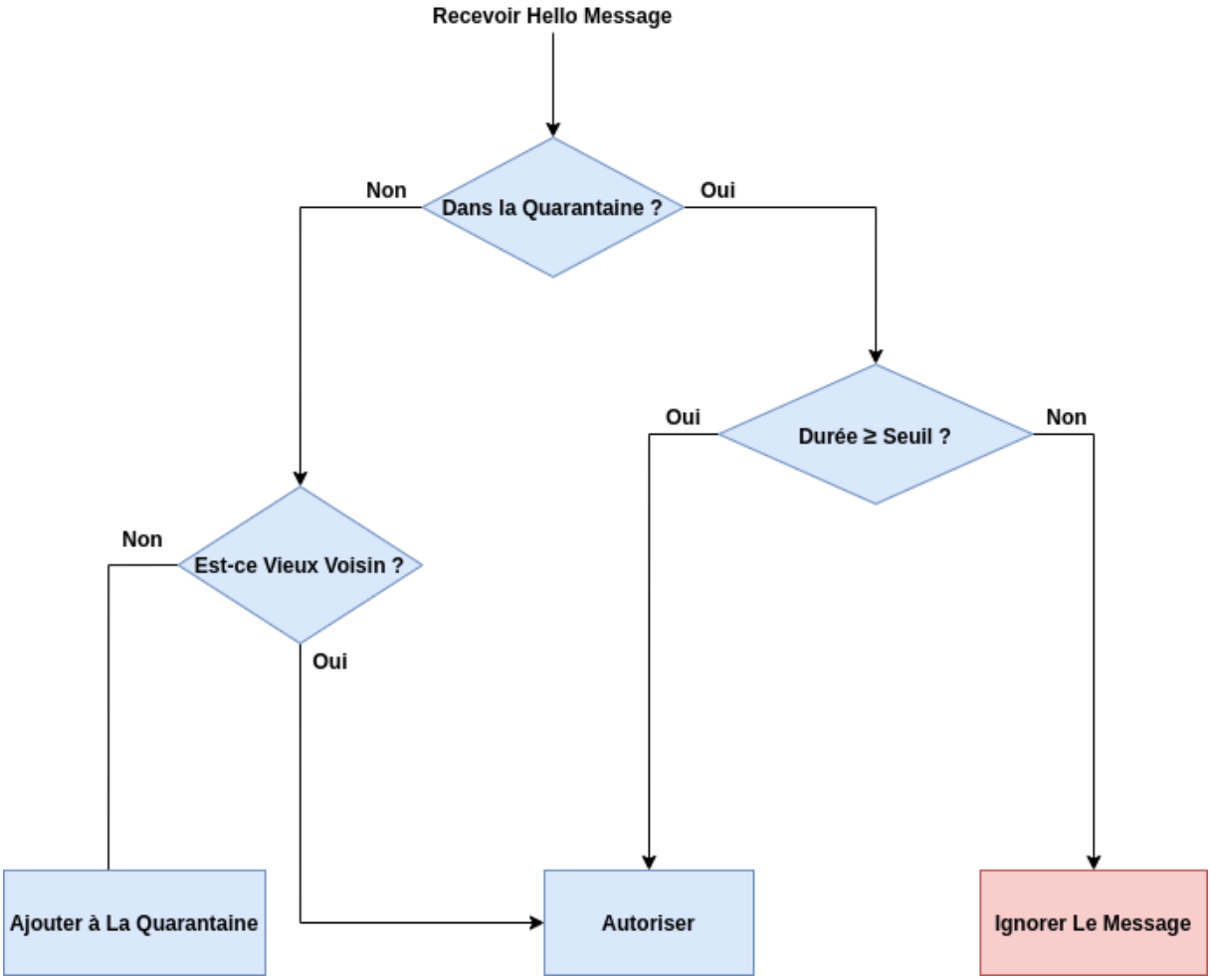

Figure3. 3:Organigramme de la solution proposé.

3.4 Environnement de simulation

Dans cette partie, nous utiliserons le simulateur NS2, afin de simuler notre scénario, nous utilisons un mécanisme de changement de pseudonyme coopératif afin qu'un nœud honnête change de pseudonyme s'il y a "k" voisins qui veulent changer de pseudonyme de l'autre côté un nœud malveillant changera fréquemment son pseudonyme le nœud honnête changera son pseudonyme avec k=3 ce qui veut dire que le nœud honnête changera de pseudonyme s'il y a 3 voisins veulent changer un nœud honnête décidera à changer son pseudonyme toutes les 60s et le nœud malicieux utilisera cette action pour lancer fréquemment une attaque de pseudonyme.

La simulation a effectué en considérant les paramètres suivants :

Paramètre	Valeurs
Portée d'antenne	300m
Couche MAC	802.11P
Région de simulation	2000mx1500m
Protocoles de routage	GPSR
Nombre de nœuds	50
Durée de simulation	600s

Tableau 3.1:Les paramètres de simulation.

3.5 Résultats de simulation et l'analyse

Dans cette section, nous donnons et analysons les résultats de simulations obtenus.

La figure 3.4 ci-dessous montre le taux de détection en termes de nœuds malveillants. Nous pouvons voir qu'au fur et à mesure que le nombre de nœuds malveillants augmente, le nombre de détections augmente également, ce qui signifie que notre solution proposée fonctionne bien, et l'augmentation du taux de détection se produit car à mesure que le nombre de nœuds malveillants augmente, le nombre de détections augmente. Les attaques augmenteront également et cela signifie également que notre solution proposée fonctionnera correctement si un grand nombre d'attaques se produisent.

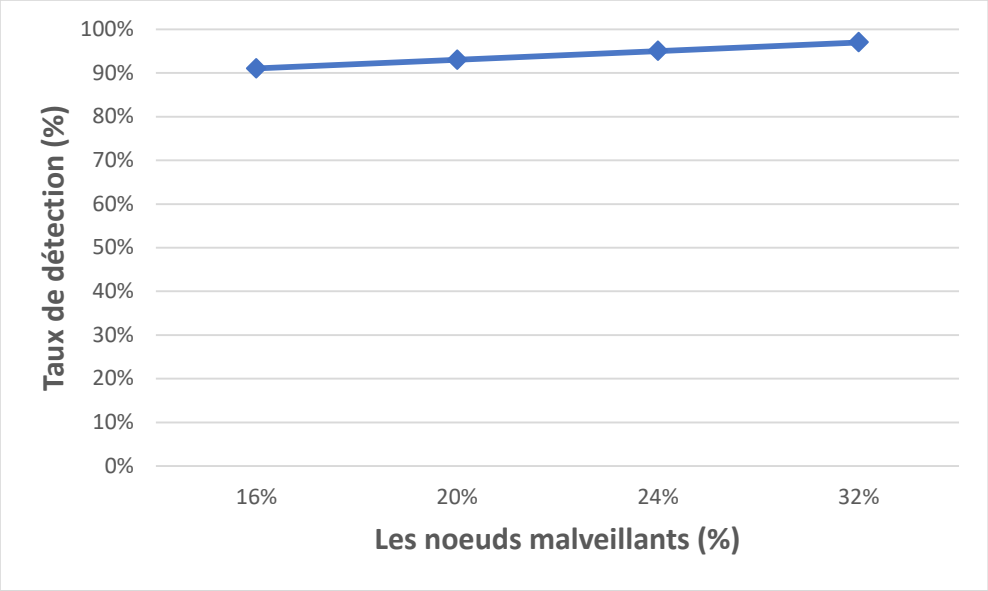

Figure3.4:Détection des nœuds malveillant.

La figure ci-dessous 3.5 montre le taux de faux positifs d'un nœud malveillant, un faux positif signifie un nœud qui ne fait rien mais est détecté et empêché d'obtenir un nouvel pseudonyme, nous avons remarqué que le faux positif diminue lorsque le nœud malveillant s'incrémente, ce qui signifie que notre système fonctionnera s'il y avait moins ou pas d'attaque, cela signifie que notre système retardera et perturbera la distribution des pseudonyme.

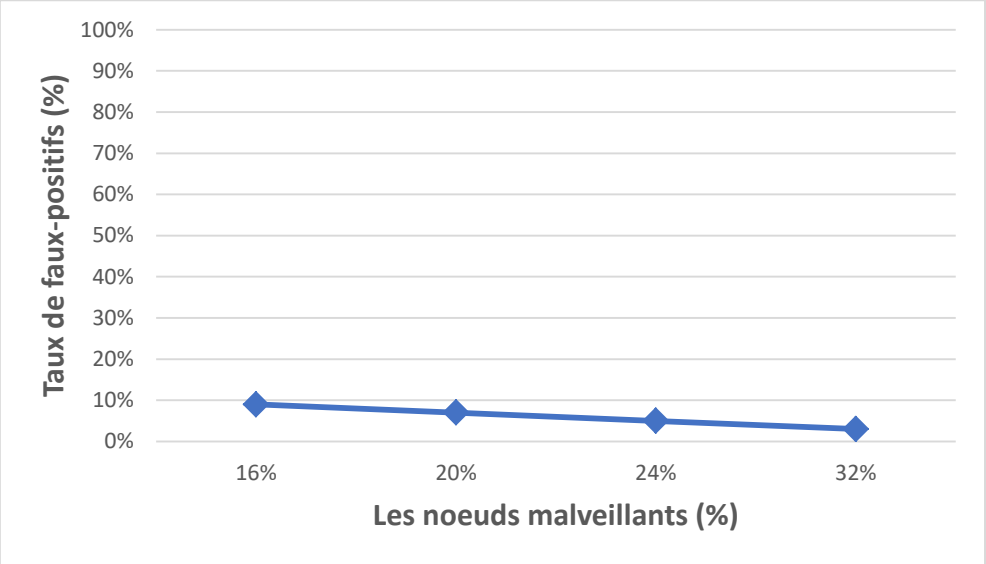

Figure3.5:Taux de faux positif.

3.6 Conclusion

Dans ce travail. nous avons étudié et analysé notre mécanisme dans un environnement sous des pseudonymes fréquemment changeants et notre mécanisme fonctionne parfaitement mais nous avons remarqué que notre technique a un impact sur le changement de système de pseudonymes parce que le faux positif était élevé quand il y avait quelques attaquants, à cet égard, nous avons perdu un peu de performance et de temps, mais nous avons évité des problèmes encore plus grands, et notre objectif futur sera d'améliorer le taux de faux positifs.

Conclusion générale

Les réseaux VANET sont des réseaux ayant des applications prometteuses pour sauver la vie des personnes et assurer le confort des occupants de véhicules. Ces réseaux ne peuvent pas être déployés qu'après l'investigation et l'assurance de leur sécurité. Malheureusement, ces réseaux sont vulnérables aux attaques des entités malveillantes qui peuvent injecter des messages à des fins malveillantes.

L'authentification de l'origine de ces messages est un élément fondamental pour se défendre contre les attaquants. En effet, les nœuds incluent dans les messages échangés des signatures numériques qui permettent aux nœuds récepteurs de les authentifier.
La vérification de signatures numériques nécessite que le nœud vérificateur doit avoir une copie du certificat numérique du nœud signataire. Les différents travaux de recherche proposent le rattachement des certificats aux messages beacon. De cette manière, n'importe quel nœud possède les certificats de tous ses voisins à n'importe quel moment s'ils les rattachent à chaque message beacon diffusé. Le problème de cette approche est qu'elle nécessite des équipements spécifiques qui supportent cette complexité de traitement. Une autre approche est possible et consiste à omettre l'inclusion de certificats dans certains messages beacon qui permet aux nœuds de réduire le traitement et la bande passante consommée d'une part, et d'augmenter les chances des pertes cryptographiques, d'autre part. Ces dernières sont acceptables si elles ne causent pas une dégradation grave de la performance.

Pour se défendre contre les nœuds malveillants, l'annulation de validité de leurs certificats numériques, au plus tôt, est indispensable pour éviter leurs attaques. A cet effet, les RSUs peuvent être utilisés pour distribuer la dernière liste de révocation de certificats. Cette opération n'empêche pas instantanément les attaques vue la nature centralisée de cette opération. Donc, le mécanisme de révocation locale est nécessaire pour exclure rapidement les nœuds malveillants.

La révocation locale est vulnérable aux attaques de falsification de messages d'accusation. En effet, les nœuds malveillants peuvent employer des accusations afin de provoquer la révocation de nœuds honnêtes, en dégradant ainsi la performance du réseau.

La protection de la vie privée des occupants de véhicules est obligatoire afin que les futurs réseaux véhiculaires prennent place chez les utilisateurs. L'approche la plus fiable pour assurer l'anonymat de véhicules est d'employer les pseudonymes. Ces derniers ont un cycle de vie spécifique comprenant les phases suivantes: la génération, l'émission, l'utilisation, la révocation et la résolution de pseudonymes. Ces phases peuvent coexister simultanément, ce qui pose des défis sans précèdent pour la révocation de ces pseudonymes. En effet, les véhicules malveillants possèdent suffisamment de pseudonymes à un moment donné et peuvent les changer sans suivre les démarches appropriées nécessaires à l'opération, et par conséquent ils peuvent causer une attaque de succession d'accusations qui leurs permet d'amplifier leur impact négatif sur la performance du système.

Pour améliorer les systèmes des réseaux VANET contre le changement fréquent de pseudonyme. Comme extensions futures à notre travail nous proposons:

- ✓ La simulation de notre système de révocation avec d'autres techniques de changement de pseudonyme.
- ✓ L'utilisation d'autres simulateurs pour évaluer la performance de notre système.

Références

[1] Véhicules connectés et systèmes de transport intelligents ,Rapport interne, Michelin Challenge Bibendum,2011, Berlin.

[2] Noureddine CHAIB, "La sécurité des communications dans les réseaux VANET", Mémoire, Université ELHADJ LAKHDER-BATNA, faculté des sciences de l'ingénieur département d'informatique, 05 Septembre 2011

[3] Department of Violence and Injury Prevention and Disability, “Injuries and violence: the facts,” Geneva,Switzerland, 2010.

[4] Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri, "Short-lived Key Management for Secure Communications in VANETs", 11th International Conference on ITS Telecommunications (ITST), pp. 613-618, August 23-25, 2011- St. Petersburg, Russia. ISBN: 978-1-61284-668-2.

[5] Jonathan Petit, "Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires", Thèse de Doctorat, Université de Toulouse, 13 Juillet 2011.

[6] A. M. Vegni, M. Biagi, and R. Cusani, Smart Vehicles , Technologies and Main Applications in Vehicular Ad hoc Networks. Rome, Italy: INTECH, 2013.

[7] GRICH Sofien, "Contribution à la Qualité de Service dans les réseaux VANET", Mémoire, Université d’Oran, département d’informatique, 04 Novembre 2015.

[8] M. K. Nasir, R. Md Noor, M. A. Kalam, and B. M. Masum, “Reduction of Fuel Consumption and Exhaust Pollutant Using Intelligent Transport Systems,” Sci. World J., vol. 2014, pp. 1–13, 2014.

[9] European Conference of Ministers of Transport, Gérer la congestion urbaine. PARIS, FRANCE: OECD, 2010.

[10] G. Tasseron and K. Martens, “Urban parking space reservation through bottom-up information provision: An agent-based analysis,” Comput. Environ. Urban Syst., vol. 64, no. July, pp. 30–41, Jul. 2017.

[11] A. Rasheed, S. Gillani, S. Ajmal, and A. Qayyum, “Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications,” vol. 548, no. March, 2017, pp. 39–51.

[12]https://www.ifsttar.fr/fileadmin/redaction/dossiersthematiques/Mobilites/vehicule_autonome/10169_MOB_VA_FR_interactif.pdf

[13] E. Bergenheim, T. von Eichwald, G. Hallneus, and M. Erlingfors, “Pedestrian protection airbag,” US 20130200603 A1, 2013.

[14] U. S. D. of Transportation, “ITS Research Initiatives.” *Online+. Available: https://ntl.bts.gov/lib/jpodocs/repts_te/14429_files/ch3.html. [Accessed: 02-Mar-2021].

[15] https://securite-routiere.qc.ca/doc/aide-determination-limite.pdf (accédé le 10/04/2021).

[16] http://fr.wikipedia.org/wiki/Autoroutes_du_Québec(accédé le 10/04/2021).

[17] M. JERBI, “Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections,” 2008.

[18] M. Fiore, J. Härri, F. Filali, and C. Bonnet, “Vehicular mobility simulation for VANETs,” in Proceedings - Simulation Symposium, 2007.

[19] R. S. Raw, M. Kumar, and N. Singh, “Security Challenges, Issues and Their Solutions for VANET,” Int. J. Netw. Secur. Its Appl., vol. 5, no. 5, pp. 95–105, 2013.

[20] Fan Li and Wang, “Routing in Vehicular Ad Hoc Networks: A Survey”, IEEE Vehicular Technology Magazine Volume 2, pp. 12-22, June 2007. Print ISSN: 1556-6072.

[21] Abdel Mehsen AHMAD, “Techniques de Transmission et d’Accès sans fil dans les Réseaux Ad Hoc Véhiculaires (VANETs) ”, Telecom Sudparis et l’Université Pierre et Marie Curie en co-tutelle avec l’Université Libanaise, Spécialité : Informatique et Télécommunications, 09 Octobre 2012.

[22] Ahizoune Ahmed, “ Un protocole de diffusion des messages dans les réseaux véhiculaires”, Mémoire, Université de Montréal, Département d’informatique et de recherche opérationnelle, Faculté des arts et sciences, Avril 2011.

[23] Richard Engoulou, "Sécurisation des VANETS par la Méthode de Réputation des Nœuds", Mémoire, Université de Montréal, École Polytechnique de Montréal, Département de Génie Informatique et Génie Logiciel, Avril 2013.

[24] Wafaa A.H. Al-Salihy, R. Sures, Ghassan Samara, "Security Analysis of Vehicular Ad Hoc Networks (VANET) ", Network Applications, Protocols and Services, International Conference, pp.55-60, September 2010, Alor Setar, Kedah Malaysia. ISBN: 978-0-7695-4177-8.

[25] Praveen G Salagar, Shrikant S Tangade, "A Survey On Security In VANET", International Journal for Technological Research in Engineering, Volume 2, Issue 7, pp. 1397-1402, March-2015, Bangalore, India. ISSN: 2347 - 4718.

[26] Swapnil G. Deshpande, "Classification of Security attack in Vehicular Adhoc network: A survey ", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 2, pp. 371-377, March – April 2013, Amravati, Maharashtra, India. ISSN 2278-6856.

[27] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” Veh. Commun., vol. 7, pp. 7–20, 2017.

[28] B. Parno and A. Perrig, "Challenges in securing vehicular networks", in Workshop on Hot Topics in Networks (HotNets-IV), pp. 11-21, November 2005, College Park, Maryland, USA.

[29] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for VANETs", 4th Workshop on Embedded Security in Cars. (escar 2006), pp. 15-22, November 2006, Berlin, Germany.

[30] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” Telecommun. Syst., vol. 50, no. 4, pp. 217–241, 2010.

[31] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” Ad Hoc Networks, vol. 61, pp. 33–50, Jun. 2017.

[32] G. Samara, W. A. H. Al-Salihy, and R. Sures, “Security Analysis of Vehicular Ad Hoc Nerworks (VANET),” in 2010 Second International Conference on Network Applications, Protocols and Services, 2010, pp. 55–60.

[33] M. S. Al-kahtani, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs),” in 2012 6th International Conference on Signal Processing and Communication Systems, 2012, pp. 1–9.

[34] M. Azees, P. Vijayakumar, and L. J. Deboarh, “EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks,” IEEE Trans. Intell. Transp. Syst., vol. 99, no. PP, pp. 1–10, 2017.

[35] M. L. Psiaki and T. E. Humphreys, “GPS Lies,” IEEE Spectr., vol. 53, no. 8, pp. 26–53, 2016.

[36] “University of Texas students send yacht off-course with GPS exploit.” *Online+. Available: https://www.engadget.com/2013/07/30/university-of-texas-yacht-hack-experiment/. [Accessed: 02-Mar-2021].

[37] M. Franeková, P. Hole, E. Bubeníková, and A. Kanáliková, “Transport scenarios analysis within C2C communications focusing on security aspects,” in IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI), 2017, pp. 461–466.

[38] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in Proceedings of the 3rd {ACM} workshop on Security of ad hoc and sensor networks, 2005, pp. 11–21.

[39] M. Gerlach et F. Guttler. "Confidentialité dans les VANETs utilisant des pseudonymes changeants - Idéal et réel" . IEEE Veh. Technol. Conf., 2007.

[40] S. Zeng, Y. Chen, S. Tan, and M. He, “Concurrently deniable ring authentication and its application to LBS in VANETs,” *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 844–856, 2017.

[41] L. M. S. Jaimes, K. Ullah, and E. dos Santos Moreira, “ARS: Anonymous reputation system for vehicular ad hoc networks,” in *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*, 2016, pp. 1–6.

[42] C. Wang, D. Shi, X. Xu, and J. Fang, “An anonymous data access scheme for VANET using pseudonym-based cryptography,” *J. Ambient Intell. Humaniz. Comput.*, vol. 7, no. 1, pp. 63–71, 2016.

[43] Y. Wang, H. Zhong, Y. Xu, J. Cui, and F. Guo, “Efficient extensible conditional privacy-preserving authentication scheme supporting batch verification for VANETs,” *Secur. Commun. Networks*, vol. 9, no. 18, pp. 5460–5471, 2016.

[44] F. Scheuer, K.-P. Fuchs, and H. Federrath, “A Safety-Preserving Mix Zone for VANETs,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6863 LNCS, 2011, pp. 37–48.

[45] M. Raya, M. Raya, J. Hubaux, and J. Hubaux, “Securing vehicular ad hoc networks,” *J. Comput. Secur.*, vol. 15, pp. 39–68, 2007.

[46] M. Humbert, M. H. Manshaei, J. Freudiger, and J. P. Hubaux, “Tracking games in mobile networks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6442 LNCS, pp. 38–57, 2010.

[47] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: Why simple pseudonym change is not enough,” *WONS 2010 - 7th Int. Conf. Wirel. On-demand Netw. Syst. Serv.*, pp. 176–183, 2010.

[48] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust location privacy scheme for VANET,” *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, 2007.

[49] Y. A. Al-Khassawneh and N. Salim, “On the Use of Data Mining Techniques in Vehicular Ad Hoc Network,” in *Advanced Machine Learning Technologies and Applications*, Springer, 2012, pp. 449–462.

[50] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” Proc. - 12th IEEE Int. Conf. Comput. Sci. Eng. CSE 2009, vol. 3, no. March, pp. 139–145, 2009.

[51] ETSI, “Intelligent Transport Systems (ITS): Security Services and Architecture,” sophia antipolis, 2010.

[52] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym Schemes in Vehicular Networks: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, pp. 228–255, Jan. 2015.

[53]D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler."Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping". IEEE Veh. Netw. Conf. VNC 2010, 2010.

[54] Y. Pan, J. Li, L. Feng et B. Xu. « Un modèle analytique pour le schéma de pseudonymes changeant au hasard dans les VANETs ». Réseaux, outils logiciels et applications, 2011.

[55] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki. "CARAVANE : Fournir la confidentialité de l'emplacement pour VANET". 2005.

[56] M. Li, K. Sampigethaya, L. Huang et R. Poovendran. "Swing & Swap : Approches centrées sur l'utilisateur pour maximiser la confidentialité de l'emplacement". WPES, 2006.

[57] L. Buttyan, T. Holczer, A. Weimerskirch et W. Whyte. "RALENTIR: Un schéma pratique de changement de pseudonyme pour la confidentialité de l'emplacement dans les VANETs". IEEE Vehicular Networking Conference (VNC), 2009.

[58] B.K. Chaurasia et S. Verma. "Optimisation de la mise à jour des pseudonymes pour l'anonymat dans VANETS". Conférence IEEE Asie-Pacifique sur l'informatique des services, 2008.

[59] B.K. Chaurasia, S. Verma, G.S. Tomar et S.M. Bhaskar.« Mécanisme basé sur des pseudonymes pour maintenir la confidentialité dans les VANETs ». 1er Int. Conf. Calcul. Informer. Commun. Syst. Réseaux, CICSYN, 2009.

[60] D. Eckhoff, C. Sommer, T. Gansen, R. German et F. Dressler.« Confidentialité d'emplacement solide et abordable dans les VANET : diffusion d'identité à l'aide de créneaux horaires et d'échanges ». IEEE Veh. Réseau Conf. CNV, 2010.

[61] D. Eckhoff, C. Sommer, T. Gansen, R. German et F. Dressler. « Protection de la vie privée avec plusieurs zones de mélange dynamiques basées sur des pseudonymes sur les réseaux routiers ». China Commun, 2017.

[62] R. Lu, X. Lin, T. H. Luan, X. Liang et X. Shen. "Le changement de pseudonyme aux points sociaux : une stratégie efficace pour la confidentialité de l'emplacement dans les VANETs". IEEE Trans. Véh. Technol, 2012. vol. 61, non. 1, p. 86-96.

[63] M. Raya, P. Papadimitratos, I. Aad, D. Jungels et J. Hubaux. « L'éviction de mauvais comportement et de nœuds défectueux dans les réseaux véhiculaires ». IEEE J. Sel. Domaines Commun, 2007. vol. 25, non. 8, pages 1557-1568.

[64] M. E. Nowatkowski et H. L. Owen. « Distribution évolutive de la liste de révocation de certificats dans les réseaux ad hoc de véhicules ». IEEE Globecom Travail. GC'10, 2010. p. 54 -58.

[65] Y. Kondareddy, G. Di Crescenzo et P. Agrawal. "Analyse des protocoles de distribution de liste de révocation de certificats pour les réseaux véhiculaires". IEEE J. Sel. Domaines Commun GLOBECOM - IEEE Glob. Télécommun.Conf, 2010.

[66] F. Schaub. « Pseudonymat conditionnel dans les réseaux ad hoc véhiculaires ». Université d'Ulm, 2008.

[67] Z. Ma, F. Kargl et M. Weber. « Pseudonyme à la demande : une nouvelle stratégie de recharge de pseudonymes pour les communications véhiculaires ». IEEE Veh. Technol. Conf, 2005. pp.1-5.

[68] D. Forster, H. Lohr, J. Zibuschka et F. Kargl. "REWIRE-Révocation sans résolution : un mécanisme de révocation respectueux de la vie privée pour les réseaux véhiculaires ad hoc". dans Trust and Trustworthy Computing, vol. 9229, 2015. p. 193{208.

[69] J. Timpner et L. Wolf. « Geocast de requête-réponse pour la détection de foule de véhicules ». Réseaux ad hoc, 2016. vol. 36, non. 2, p. 435{449.

[70] C. Ganan, J. L. Muñnoz, O. Esparza, J. Mata-Diaz et J. Alins. « EPA : un mécanisme de révocation efficace et respectueux de la vie privée pour les réseaux ad hoc véhiculaires ». Foule envahissante. Calcul, 2015. vol. 21, p. 75-91.

[71] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, “REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks,” in Trust and Trustworthy Computing, vol. 9229, Springer International Publishing, 2015, pp. 193–208.

[72] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, “EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks,” Pervasive Mob. Comput., vol. 21, pp. 75–91, Aug. 2015.

Glossaire

CA	Certificate Authority.
CRL	Certificate Revocation List.
DOS	Denial Of Service.
ITS	Intelligent Transport System.
MANET	Mobile Ad-hoc NETworks.
NHTSA	National Highway Trafic Safety Administration.
OBU	On Board Units.
OSR	Order of Self-Revocation.
PP	Pseudonym Provider.
RSU	Road Side Units.
TPD	Tamper Proof Device.
TTP	Trusted Third Party.
V2I	Vehicle to Infrastructure Communication.
V2P	Vehicle to Passenger communication.
V2V	Vehicle to Vehicle Communication.
VANET	Vehicular Ad-hoc NETwork.
VID	Vehicle IDentifier.
OBU	On Board Unit.
DoS	Denial of Service.