UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES

COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES ET INFORMATIQUE
APPLIQUÉES

PAR
KAHINA MOGHRAOUI

GESTION DE L'ANONYMAT DES COMMUNICATIONS DANS LES RÉSEAUX VÉHICULAIRES AD HOC SANS FIL (VANETs)

JUILLET 2015

Université du Québec à Trois-Rivières

Service de la bibliothèque

Avertissement

L'auteur de ce mémoire ou de cette thèse a autorisé l'Université du Québec à Trois-Rivières à diffuser, à des fins non lucratives, une copie de son mémoire ou de sa thèse.

Cette diffusion n'entraîne pas une renonciation de la part de l'auteur à ses droits de propriété intellectuelle, incluant le droit d'auteur, sur ce mémoire ou cette thèse. Notamment, la reproduction ou la publication de la totalité ou d'une partie importante de ce mémoire ou de cette thèse requiert son autorisation.

CE MÉMOIRE A ÉTÉ ÉVALUÉ PAR

UN JURY COMPOSE DE

- **Boucif Amar Bensaber,** directeur de recherche.

Professeur au département de Mathématiques et Informatique
Université du Québec à Trois-Rivières.

- **Mhamed Mesfioui,** évaluateur.

Professeur au département de Mathématiques et Informatique
Université du Québec à Trois-Rivières.

- **Adel Omar Dahmane,** évaluateur ;

Professeur au département de génie électrique et génie informatique
Université du Québec à Trois-Rivières.

À
Ma précieuse Thanina,
Mon cher mari,
Mes parents,
Mon frère,
Ma sœur.
Tous ceux qui me sont chers.

REMERCIEMENTS

Je tiens à remercier mon directeur de recherche, Professeur Boucif Amar Bensaber, pour son aide et ses conseils, sans lui ce travail n'aurait pas vu le jour, il m'a donné l'opportunité de faire mon premier pas dans le domaine de la recherche scientifique.

J'adresse particulièrement, mes sincères remerciements au professeur Mhamed Mesfioui, pour ses qualités humaines et intellectuelles. Il est sans doute l'un des grands piliers du département de Mathématique et Informatique.

Je remercie le professeur Adel Omar Dahmane d'avoir accepté d'évaluer mon travail.

Je remercie tous mes professeurs à l'UQTR qui m'ont permis d'acquérir plus de connaissances durant mes études.

Je remercie tous mes collègues du Laboratoire de Mathématiques et Informatique appliquées (LAMIA).

Je remercie mon collègue Joseph pour ses conseils, sans lui je n'aurais pas eu l'occasion de découvrir le domaine des VANETs.

Je remercie également tous ceux qui de près ou de loin m'ont soutenu et encouragé pour réussir mes études, particulièrement Cherifa en Algérie.

TABLE DES MATIÈRES

Page

REMERCIEMENTS..... iii

TABLE DES MATIÈRES..... iv

LISTE DES ABRÉVIATIONS vii

SOMMAIRE..... ix

ABSTRACT..... x

CHAPITRE 1 INTRODUCTION GENERALE..... 1

CHAPITRE 2 LES RÉSEAUX VÉHICULAIRES, NOTIONS ET DESCRIPTION...3

2.1 Définition 3

2.2 Le système des réseaux VANETs 4

2.2.1 Architecture et composants.....4

2.2.2 Les modes de communication dans VANETs..... 5

2.2.3 Caractéristiques..... 7

2.2.4 Les types de messages..... 9

2.2.4.1 Message lié à la sécurité..... 9

2.2.4.2 Message à valeur ajoutée..... 9

2. 3 La sécurité dans les réseaux VANETs..... 10

2.3.1 Introduction..... 10

2.3.2 Caractéristiques de la sécurité..... 10

2.3.3 Menaces sur la sécurité..... 11

2.3.4 Exigences de sécurité 13

2.3.5 Mécanismes de base de la sécurité 15

2.4 Conclusion..... 17

CHAPITRE 3 REVUE DE LA LITTÉRATURE..... 18

3.1 Introduction..... 18

3.2 La vie privée et l'anonymat dans les réseaux VANETs..... 18

3.3 Conclusion..... 23

CHAPITRE 4 ARTICLE SCIENTIFIQUE 25

An Efficient Pseudonym Change Protocol Based on Trusted Neighbors for Privacy and Anonymity in VANETs.....26

CHAPITRE 5 DISCUSSIONS GÉNÉRALES DES RÉSULTATS.....32

5.1 Analyse de la confidentialité 32

5.2 Discussion des résultats.....32

5.3 Comparaison des performances 33

CHAPITRE 6 CONCLUSION GÉNÉRALE.....35

BIBLIOGRAPHIE.....37

Figure 1 : Modèle des réseaux MANETs et son mode de communications.....3

Figure 2 : Modèle des réseaux VANETs et son mode de communications.....6

LISTE DES ABRÉVIATIONS

CA: Central Authority.

DOS: Denial Of service

DSRC: Dedicated Short Range Communication.

GPS: Global Positioning System

IEEE: Institute of Electrical and Electronics Engineers.

MAC: Medium Access Control.

MANET: Mobile Ad hoc Network.

OBU: On Board Unit.

RSU: Road Side Unit.

ITS: Intelligent Transport System.

TA: Trusted Authority.

TPD: Tamper Proof Device.

VANETs: Vehicular Ad hoc Network.

V2V: Vehicular-to-Vehicular.

V2I: Vehicular-to-Infrastructure.

GESTION DE L'ANONYMAT DES COMMUNICATIONS DANS LES RÉSEAUX VÉHICULAIRES AD HOC SANS FIL (VANETs)

Kahina MOGHRAOUI

SOMMAIRE

Dans les réseaux véhiculaires Ad hoc (VANETs), les changements réguliers des pseudonymes de communication privés sont importants pour éviter tout suivi illégal des véhicules et pour assurer leur anonymat. Dans ce contexte, nous proposons deux protocoles de changement de pseudonymes privés.

Le premier protocole est basé sur la détection des voisins de confiance. En l'absence de ces derniers, nous avons opté pour l'attribution d'une durée de vie aux pseudonymes privés. Ce protocole est basé sur un comportement de déclenchement coopératif et assure le déclenchement de changement des pseudonymes privés dans plusieurs véhicules en même temps, une solution qui permet d'améliorer l'anonymat des véhicules.

Le deuxième protocole est une approche basée sur le déclenchement à comportement individuel. Chaque véhicule, à la fin de la durée de vie de son pseudonyme, trie aléatoirement un temps, dans un petit intervalle de temps, puis change son pseudonyme. Cela garantit le changement des pseudonymes périodiquement, mais pas toujours en même temps. Ainsi les véhicules malveillants ne peuvent pas prédéfinir à l'avance le temps de changement des pseudonymes privés pour chacun des véhicules.

Dans ce travail, nous évaluons les performances de nos deux approches avec simulation, qui définissent des scénarios dans toutes les conditions et dans les deux milieux urbains et sur autoroute.

GESTION DE L'ANONYMAT DES COMMUNICATIONS DANS LES RÉSEAUX VÉHICULAIRES AD HOC SANS FIL (VANETs)

Kahina MOGHRAOUI

ABSTRACT

In vehicular ad hoc networks (VANET), regular changes of private communication pseudonyms are important to prevent any illegal tracking of vehicles and ensuring their anonymity. In this context, we propose two protocols of changing private pseudonyms.

The first protocol is based on the detection of trusted neighbors. In the absence of these, we opted for the allocation of a lifetime to private pseudonyms. This protocol is based on a cooperative behavior, it insures the triggering change private pseudonyms in several vehicles at the same time, a solution that improves the anonymity of the vehicles.

The second protocol is an approach based on individual behavior triggering. Each vehicle at the end of the lifetime of his pseudonym, changes it at random time, at a small time interval. This ensures pseudonym changes periodically but not at a constant time. Malicious vehicles cannot predefine the time change.

In this work, we evaluate the performance of our two approaches with simulations in all conditions and in both urban and highway environments.

CHAPITRE 1

INTRODUCTION GÉNÉRALE

Dans les réseaux véhiculaires (VANETs), les véhicules sont équipés de dispositifs de communication sans fil, appelés unités embarquées (OBU), pour permettre les différents types de communications. Véhicule à véhicule (V2V) et véhicule à infrastructure (V2I). Au cours de ces communications, les véhicules diffusent une gamme d'informations très sensibles, tels que la position, la vitesse et la direction.

Ainsi, un adversaire malveillant peut retracer un véhicule et le suivre. Ceci rend la protection de la vie privée des véhicules, par authentification anonyme, une question fondamentale selon Florian Dötzer [1], Hubaux JP et autres [2], Youngho Park et autres [3], mais particulièrement difficile, en raison de la grande mobilité du réseau.

Pour résoudre ce problème, les changements réguliers des pseudonymes de communication sont importants pour éviter tout suivi illégal des véhicules et pour assurer l'anonymat dans les réseaux VANETs, selon Freudiger J et autres [4].

De nombreux mécanismes de changement de pseudonyme ont été proposés. Ces solutions sont basées principalement sur le déclenchement de changement des pseudonymes, avec un comportement individuel ou coopératif, Yuanyuan Pan et Jianqing Li [5].

Dans ce mémoire, nous proposons deux approches différentes. La première approche est un protocole de changement de pseudonymes privés à comportement de déclenchement coopératif, basé sur la détection de vrais nouveaux voisins que nous appelons des voisins de confiance. Les nouveaux voisins directs sont déterminés et selon les paramètres de la zone de circulation, nous vérifions la présence de ces voisins de confiance. En l'absence de ces voisins, le déclencheur sera la fin de la durée de vie des pseudonymes. Dans les deux cas, notre système change les pseudonymes dans plusieurs véhicules en même temps, en préservant leur anonymat.

La seconde approche est une solution pour le déclenchement de changement des pseudonymes privés avec un comportement individuel. Chaque véhicule, à la fin de la durée de vie de son pseudonyme, le change en un temps aléatoire, dans un petit intervalle de temps. Ceci garantit le changement des pseudonymes périodiquement, mais pas en temps constant. Ce qui empêche les véhicules malveillants de prédéfinir à l'avance le temps de changement des pseudonymes privés de chaque véhicule.

Notre objectif est d'évaluer les deux approches proposées dans toutes les circonstances. En les analysant et en comparant les résultats des simulations, dans les deux environnements de circulation, urbaine et autoroute.

Le reste de ce mémoire est organisé comme suit : dans le chapitre 2, on va présenter les réseaux VANETs, leurs différentes caractéristiques et composantes, pour mieux définir leurs besoins en termes de sécurité. Dans le chapitre 3, nous présentons quelques travaux de littérature portants sur la vie privée dans les réseaux véhiculaires. Puis dans le chapitre 4, nous présentons notre contribution et les solutions proposées, pour la préservation de la vie privée des véhicules et l'anonymat dans les réseaux VANETs, sous forme d'article scientifique. Nous discutons nos résultats dans le chapitre 5. Enfin, nous concluons dans le chapitre 6.

CHAPITRE 2

LES RÉSEAUX VÉHICULAIRES, NOTION ET DESCRIPTION

2.1 Définition

VANETs (Vehicular Ad Hoc Networks) est une nouvelle technologie émergente des réseaux Ad hoc mobiles (MANETs) comme illustrés dans la figure 1, où les nœuds mobiles sont les véhicules intelligents, équipés de matériels à très hautes technologies (Calculateurs, radars, systèmes de géolocalisation (GPS), différents types de capteurs et périphériques réseau).

Les réseaux VANETs permettent des communications inter-véhiculaires (V2V) et véhicules à infrastructure (V2I). Les différents nœuds peuvent échanger toutes alertes ou informations utiles pour améliorer la sécurité de la circulation routière. Mais aussi des données (musique, vidéo, publicités…) pour rendre le temps passé sur la route plus agréable et moins ennuyeux.

Les réseaux VANETs se basent sur deux types d'applications. Les applications qui constituent le noyau d'un système de transport intelligent ITS (Intelligent Transport System), pour assurer l'amélioration de la sécurité routière, mais aussi des applications déployées pour le confort des passagers.

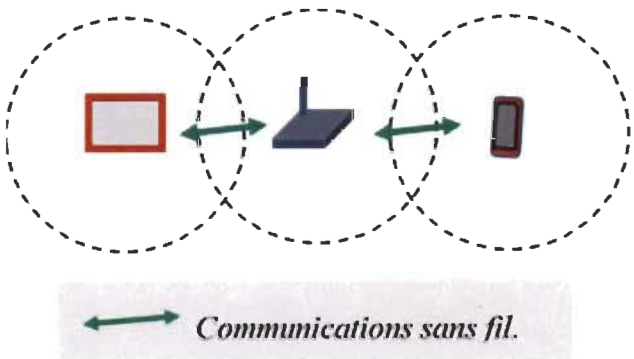

Figure 1 : Mode de communications dans les réseaux Ad hoc mobiles (MANETs).

2.2 Le système des réseaux VANETs

2.2.1 Architecture et composants

Un réseau VANETs est constitué principalement de trois entités [6] :

- **TA (Trusted Authority)**

Dites CA en français (autorité de confiance). C'est une source d'authenticité de l'information. Elle assure la gestion et l'enregistrement de toutes les entités sur le réseau (RSU et OBU). La TA est sensée connaitre toutes les vraies identités des véhicules et au besoin les divulguer pour les forces de l'ordre. Aussi, la TA dans certains travaux se charge de la délivrance et l'attribution des certificats et des pseudonymes de communications [7].

- **RSUs (Road Side Unit)**

Ces entités sont les subordonnés des TA. Elles sont installées au bord des routes. Elles peuvent être principalement, des feux de signalisation, des lampadaires ou autres. Leur principale responsabilité est de soutenir la TA dans la gestion du trafic et des véhicules. Elles représentent des points d'accès au réseau et aux différentes informations sur la circulation.

- **OBU (On-Board Unit)**

Ce sont des unités embarquées dans les véhicules intelligents, elles regroupent un ensemble de composants matériels et logiciels de hautes technologies (GPS, radar, caméras, différents capteurs et autres). Leurs rôles sont d'assurer la localisation, la réception, le calcul, le stockage et l'envoi des données sur le réseau. Ce sont des émetteurs-récepteurs qui assurent la connexion du véhicule au réseau.

2.2.2 Les modes de communication dans VANETs

Dans les réseaux VANETs, on trouve principalement, les entités fixes qui constituent l'infrastructure (RSU et TA) et les entités mobiles (les véhicules). Pour pouvoir échanger les différentes informations et données liées à la sécurité et au confort des usagers de la route, ces différentes entités doivent établir des communications entre elles. Pour cette raison, on distingue deux types de communications véhicule à véhicule (V2V) et véhicule à infrastructure [8] [9]. Comme illustré dans la figure 2.

- **Communication véhicule-à-véhicule (V2V)**

Ce type de communication fonctionne à l'aide des dispositifs installés dans les véhicules appelés OBU (On-Board Unit), suivant une architecture décentralisée. Il est semblable au type de communications entre les nœuds mobiles des réseaux MANETs. La communication entre deux véhicules se fait directement, en mode Ad hoc inter-véhiculaire. Ils n'ont pas besoin de faire appel aux infrastructures pour pouvoir communiquer entre eux. À condition que chaque véhicule soit à la portée de l'autre (zone radio). Sinon, ils font appel à d'autres véhicules, qui vont jouer le rôle d'un pont (intermédiaire) pour eux. Ce type de transmission est appelée communication à multi-sauts.

- **Communication véhicules à infrastructure**

La communication véhicule à infrastructure (V2I) est aussi appelée une communication en mode infrastructure. Ce mode de communication est assuré grâce aux différentes entités du réseau VANETs. En effet, les OBUs (On-Board Unit) des véhicules, les RSUs (Road Side Unit) placés aux bords des routes et même les TA (Trusted Authority) contribuent tous entre eux pour assurer les communications dans le réseau véhiculaire. Ce mode de communication assure une connectivité relativement forte par apport à la communication en mode V2V (véhicule à véhicule). Comme il assure une meilleure utilisation des ressources du réseau.

Ainsi, elle permet aux véhicules de bénéficier de plus de fonctionnalités et services comme l'accès à l'Internet et les informations météorologiques.

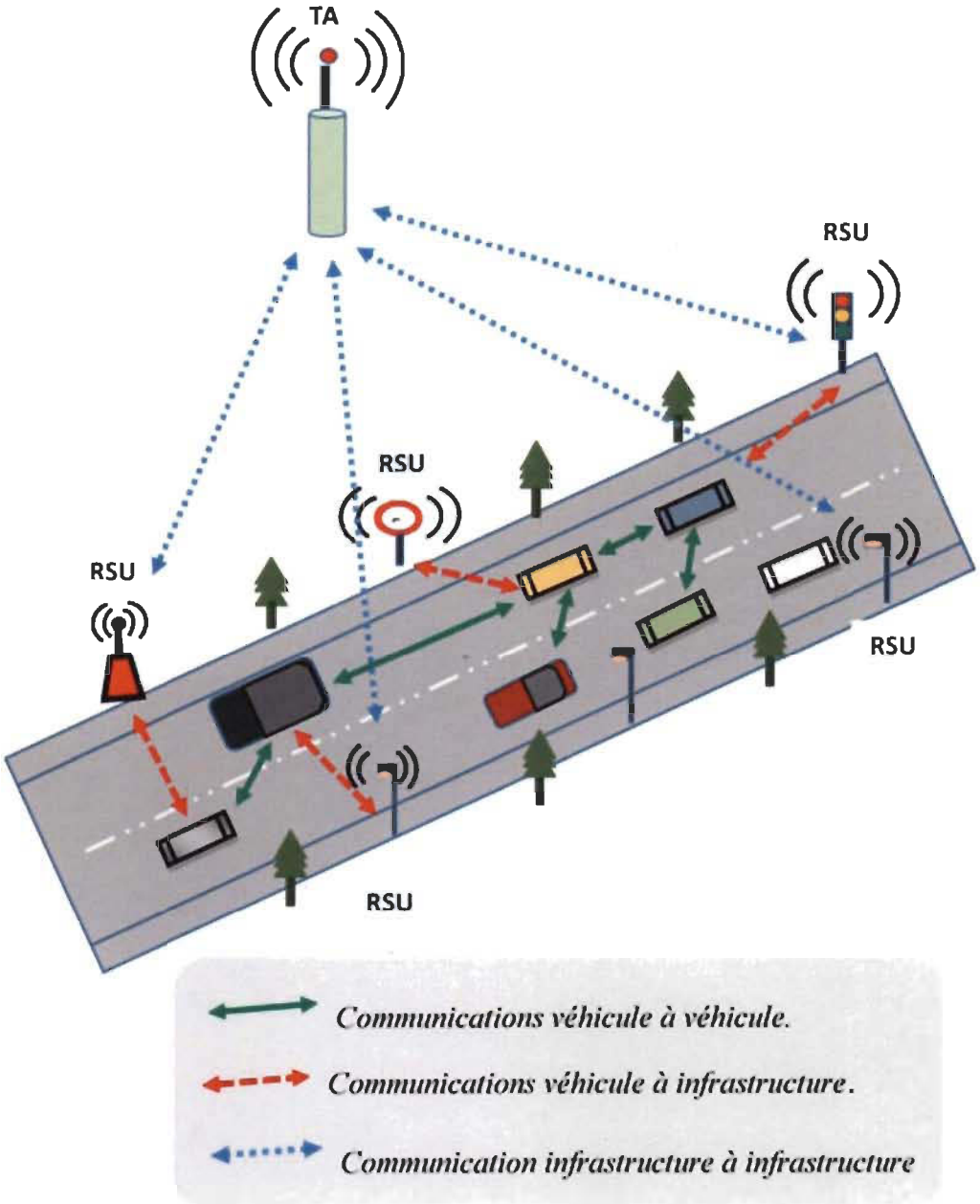

Figure 2 : Modèle des réseaux VANETs et son mode de communications.

2.2.3 Caractéristiques

Bien que les réseaux VANETs dérivent des réseaux Ad hoc mobiles, ils se distinguent avec certaines caractéristiques, qui retiennent une grande attention, à savoir :

- **Capacité et autonomie d'énergie**

Parmi les spécificités des réseaux VANETs, la grande capacité d'énergie caractérisant les véhicules qui les détiennent de leurs systèmes d'alimentation. Ce qui n'est pas le cas des autres types d'appareils des réseaux sans fil, qui incitent une grande préoccupation par apport à la limite de leurs batteries [10].

- **Communication, traitement et stockage**

Les véhicules sont caractérisés par la diversification de leurs modes de communications, car ils sont équipés de différentes interfaces (WIFI, Bluetooth, Radio et autres). Ceci implique une grande capacité de traitement et de stockage des données, qui est assurée grâce aux nouvelles technologies et les nombreuses puces électroniques très puissantes qui sont installées dans les véhicules.

- **Environnement de communication :**

Contrairement aux environnements des réseaux Ad-hoc mobiles qui sont souvent stables et limités en espace (bâtiment, aéroport ou aérogare et centre commercial). Les réseaux VANETs sont caractérisés par la grande diversité de leurs environnements qui sont déployés dans la nature à grande échelle. Passant du milieu urbain qui présente différents obstacles (immeubles) qui peuvent réduire la qualité de transmission radio, à un environnement autoroutier affecté principalement par les très grandes vitesses des véhicules.

- **Modèle de mobilité**

Le modèle de mobilité des réseaux VANETs est lié à la diversité environnementale et les infrastructures routières [11]. Mais dans une certaine mesure, il est possible de prévoir l'évolution des déplacements des véhicules grâce à leurs vitesses, leurs

directions et surtout la connaissance des cartes routières. Car les déplacements des véhicules sont structurés par les routes et les rues [12].

Le mode de mobilité des réseaux VANETs est affecté par la vitesse des véhicules et leurs déplacements aléatoires, qui peuvent réduire considérablement les durées de communications et leurs comportements face à des obstacles.

- **Modèle de communication**

Les réseaux VANETs ont été déployés principalement pour des raisons de sécurité routière (message d'alerte). Ils doivent relier une source d'alerte vers une multitude de destinations (véhicules ou infrastructures), par exemple, ce type de communication nécessite principalement un modèle de transmission en Broadcast. Néanmoins, les entités ont parfois besoin de communiquer en mode Unicast [13].

- **Topologie et connectivité**

Les réseaux VANETs sont caractérisés par une connectivité irrégulière et relativement faible, liée directement à la vitesse des véhicules, leurs déplacements aléatoires et leurs comportements face à des obstacles, qui peuvent réduire considérablement les durées des communications. En effet un véhicule peut rapidement rejoindre ou quitter un groupe de véhicules, ce qui rend les changements de topologie très fréquents et très dynamiques, constitués de plusieurs groupes séparés [10], ceci entraîne une réorganisation de la topologie du réseau.

- **Technologies de communications**

Pour mettre en place les différentes communications entre les entités du réseau VANET, diverses technologies ont été conçues, pour offrir les différents services et augmenter la portée des communications et des bandes passantes. Ainsi, une norme de communication appelée DSRC (Dedicated short Range Communication) [14] a était adoptée. Sa couche physique est basée sur la norme IEEE 802.11a [15]. Plus tard, l'IEEE s'inspira de cette norme pour créer la norme actuellement utilisée 802.11p [14]. Cette norme définit essentiellement les services de sécurité et le format des messages.

2.2.4 Les types de messages

Les différents messages échangés dans les réseaux VANETs peuvent être facilement classés, selon leurs utilités et leurs contenus, en deux grands types de message : message lié à la sécurité et message à valeur ajoutée.

2.2.4.1 Message lié à la sécurité

L'objectif principal de la naissance des réseaux VANETs était la sécurité des usagers de la route. Ainsi on trouve deux types de messages de sécurités :

- **Le message beacon**

Ce type de message contient souvent des informations relatives à l'identité et à l'état actuel du véhicule (Position, vitesse, direction et autres), il est diffusé périodiquement et est utilisé principalement pour permettre l'identification du voisinage. Ce type de message joue un rôle primordial dans la plupart des protocoles de routage et de sécurité.

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

Ce type de message est envoyé pour prévenir les autres véhicules de différentes urgences et des catastrophes sur la route (accident, congestion de la circulation, information météorologique, passage d'un véhicule de secoure et autres), afin qu'ils aient plus de temps pour agir. Ce type de message aide à améliorer la circulation et la sécurité routière.

2.2.4.2 Message à valeur ajoutée

Ce type de message peut contenir n'importe qu'elle autre information ou donnée. Il peut contenir des informations sur des services. Comme l'endroit des restaurants ou des hôtels. Il peut aussi contenir des données multimédias ou n'importe quelle donnée ou information, qui peut améliorer le confort des usagers de la route.

2. 3 La sécurité dans les réseaux VANETs

2.3.1 Introduction

La sécurité des réseaux sans fil, comme les réseaux filaires, vise à garantir essentiellement la confidentialité, l'intégrité et la disponibilité des services. C'est une tâche difficile, tout particulièrement dans un contexte de connectivité croissante, ce qui est le cas des réseaux Ad hoc mobiles.

Pour améliorer la sécurité des réseaux en général, il faut mettre en place des mécanismes de sécurité spécifiques à chaque réseau. D'une part, pour assurer que seules les personnes autorisées peuvent avoir accès aux données et services du réseau et d'autre part, pour assurer que les services peuvent être assurés correctement.

L'importance et la sensibilité des informations échangées dans les réseaux VANETs exigent plus d'attention et de mécanismes de sécurité. Puisque cela ne touche pas seulement à la sécurité des données échangées lors des communications, mais aussi, il peut toucher directement à la sécurité humaine et rendre la vie des usagers de la route en danger, notamment lorsque les messages d'alertes sont erronés ou falsifiés.

2.3.2 Caractéristiques de la sécurité

Pour mieux concevoir et mettre en place des protocoles et dispositifs de sécurité, dans les réseaux VANETs et les réseaux sans fil ad hoc en générale. Il est judicieux de commencer par l'analyse de la nature des communications dans ces réseaux et leurs caractéristiques [16] à savoir :

- **Un support de transmission partagé**

La communication sans fil et l'utilisation des ondes radio permettent aux entités attaquantes d'intercepter facilement les signaux et avoir accès aux différents messages échangés entre les entités, mais aussi elle leur permet d'agir en injectant des données erronées, ou des informations falsifiées dans le réseau.

- **Les communications multi-sauts**

Dans les réseaux sans fil mobiles en générale et spécialement dans les réseaux VANETs, il faut avoir des communications sans fil sur une très grande portée, afin d'atteindre certaines entités du réseau. Pour cette raison, il est nécessaire d'utiliser des communications à multi-sauts. Mais cela n'est pas sans conséquence. Car certaines entités malveillantes exploitent cette caractéristique pour mettre en péril le réseau, soit en altérant les communications, soit en refusant la retransmission des messages.

- **La diffusion d'information de localisation**

Dans certains protocoles des réseaux ad hoc mobiles en générale, particulièrement les protocoles de routage et de sécurité, les entités mobiles (véhicules dans les VANETs) envoient périodiquement des messages qui indiquent leur localisation. Cette information est très importante, mais relativement très sensible, étant donné qu'elle peut être utilisée par une entité malveillante pour poursuivre facilement les entités qui l'intéressent (vole d'identités).

- **Les opérations autonomes**

Les entités sont autonomes par l'envoi des messages et la transmission des différentes informations et alertes dans les réseaux VANETs particulièrement et les réseaux sans fil ad hoc mobiles en général. Ce qui donne la possibilité aux entités malveillantes d'envoyer à leurs tours, des informations erronées ou falsifiées, pour nuire considérablement aux autres entités du réseau ou causer le dysfonctionnement du système.

2.3.3 Menaces sur la sécurité

Dans les réseaux VANETs, comme dans les autres réseaux sans fil Ad hoc, on peut trouver trois grandes catégories des attaquants qui représentent des menaces et peuvent mettre le réseau en péril [17] : Internes et externes, actifs et passifs, malveillants et rationnels.

Afin de mettre en place les dispositifs appropriés, pour assurer une bonne sécurité dans les réseaux, il est nécessaire d'étudier et de connaitre les différentes formes de menaces et ainsi comprendre leurs fonctionnements.

- **Le déni de service**

L'une des menaces tant dangereuse est la menace d'attaques par déni de service « Denial Of Service », souvent, abrégé DOS. Elle consiste à paralyser temporairement (rendre inactif pendant un temps donné) les services et les ressources dans le réseau, afin qu'ils ne puissent être utilisés et consultés. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données. Il est généralement provoqué en conséquence à d'autres attaques visant les ressources énergétiques ou la bande passante. Ceci peut empêcher l'échange des messages d'alertes et par conséquent, annuler les services de sécurité dans les réseaux.

- **L'écoute des communications « Le sniffing »**

Dans ce type de menaces, l'attaque n'est pas active, car l'entité malveillante ne fait qu'écouter les conversations échangées dans le réseau et copier tous les messages transmis, pour extraire les données qui l'intéressent. Bien que l'écoute des communications est considérée comme une menace passive. Néanmoins dans la plupart des cas, elle n'est pas sans conséquence. Car l'attaquant peut ensuite utiliser les données récoltées à des fins personnelles ou servir d'autres attaquants qui ont besoin de ces informations pour l'aboutissement de leurs plans d'attaques.

- **L'usurpation d'identité et de rôle (spoofing)**

Dans ce cas, l'entité malveillante prend le rôle ou l'identité d'une autre entité. L'usurpation peut aussi porter sur tout autre élément permettant d'identifier une entité sur le réseau, afin de pouvoir se faire passer pour cette entité et agir en son nom, pour atteindre des niveaux de privilèges et des accès non autorisés. Comme le cas d'usurpation d'un véhicule de police, qui est autorisé à contrôler les véhicules du réseau et donc accéder à leurs informations et données personnelles.

- **L'injection des messages erronés**

Dans ce type de menaces, l'attaque peut provoquer des conséquences très graves dans les réseaux VANETs, qui peuvent même mettre en danger la vie humaine. En effet, des entités malveillantes diffusent des messages et des informations erronées afin d'influencer le comportement des conducteurs des véhicules ou de modifier leurs trajectoires. Cette attaque peut causer le dysfonctionnement du réseau et provoquer des accidents routiers.

- **Menaces sur la vie privée**

Ce genre de menace touche à des informations très sensibles dans le réseau. L'entité malveillante collecte des informations liées à la vie privée d'un véhicule, comme son identité et sa localisation (position géographique), pour suivre sa trajectoire. L'objectif d'une telle menace est très divers et dépend de l'intention de l'entité malveillante envers sa cible. Car il peut utiliser les informations recueillies pour une attaque ultérieure, il peut les transmettre à d'autres entités qui l'ont engagé. Comme il peut tout simplement les divulguer aux autres entités du réseau. Pour remédier à ce genre de menaces. L'utilisation des pseudonymes de communication est très utile. Toutefois, ce n'est pas suffisant. Car il faut les changer périodiquement afin d'éviter que le véhicule malveillant puisse lier chaque entité (véhicule) à son pseudonyme privé. Ainsi permettre à chaque véhicule de garder son anonymat dans le réseau.

2.3.4 Exigences de la sécurité

Lorsqu'on aborde le problème de sécurité dans les réseaux VANETs particulièrement, on vise à atteindre certains objectifs principaux [18]. En effet, dans les réseaux VANETs, une application ou un protocole de sécurité, selon ses fonctionnalités, devrait assurer une ou plusieurs exigences suivantes :

- **L'intégrité**

L'intégrité (l'authentification des messages) est le service qui détecte la falsification ou la destruction des informations de la part des entités non autorisées (malveillantes), durant sa création, sa transmission et son stockage. Cet objectif de sécurité vise à s'assurer que les données reçues n'ont subi aucune altération, modification ou duplication, durant leur transmission et transite, que ce soit volontairement ou accidentellement. L'intégrité peut être réalisée principalement par l'utilisation du hachage et de la cryptographie.

- **L'authentification**

L'authenticité permet de lier un message ou une donnée à son émetteur. Elle permet aux différentes entités du réseau d'avoir confiance dans les messages et les données diffusés. L'authenticité est la seule exigence qui permet la coopération au sein du réseau sans risque, en identifiant tous les participants et en contrôlant l'authenticité des messages échangés. En effet, on ne peut assurer une confidentialité et une intégrité dans le réseau si, dès le départ, on n'est pas sûr de communiquer avec la bonne entité. Si l'authentification est mal gérée, un attaquant peut s'attacher au réseau et injecter des messages erronés. Pour cela, plusieurs travaux portent à assurer cette exigence, pour que le principe de sécurité routière soit satisfait et que les messages d'alertes et de sécurité, par exemple, ne soient diffusés que par les entités autorisées et authentifiées par des signatures [19].

- **La non-répudiation**

Cette exigence de sécurité permet d'identifier, avec certitude, chaque entité qui diffuse un message sur le réseau et de s'assurer qu'elle ne peut nier d'être à l'origine de ce message. Cet objectif est indispensable dans certaines communications sensibles. Les autorités de confiances (TA) doivent être en mesure de retracer un expéditeur d'un message et de l'identifier facilement, en cas, d'une enquête sur une attaque ou un message d'alerte suspecté.

- **La confidentialité**

L'exigence de la confidentialité est conditionnelle, en effet, elle garantit que seules les autorités de confiance (TA) ont accès aux identités réelles des véhicules, ainsi elles peuvent les divulguer aux services de l'ordre, lorsque cela est nécessaire. La confidentialité consiste à préserver le secret des véhicules et fournir l'anonymat aux expéditeurs des messages échangés dans le réseau. Ceci empêche les entités malveillantes d'observer, de suivre ou d'écouter les messages concernant un véhicule ciblé dans le réseau. La confidentialité peut être assurée par l'usage de la cryptographie.

- **La disponibilité**

Cette exigence de sécurité vise à garantir que tous les ressources et services prévus sur le réseau sont disponibles en tout moment, aux entités autorisées du réseau. En effet, les véhicules doivent avoir un accès rapide et fiable aux informations importantes, de routage et de sécurité, et toutes autres données du réseau qui leur sont autorisées. Cela nécessite du matériel et des protocoles de sécurités de très grandes performances. Car la disponibilité est principalement menacée par les attaques de type dénis de services (DOS) et trou noir, qui sont des attaques très difficiles à prévoir et à contrôler. Car ces attaques sont souvent, très bien préparées par des professionnels de grandes compétences intellectuelles qui utilisent du matériel de haute performance.

2.3.5 Mécanismes de base de la sécurité

Après avoir étudié les caractéristiques des réseaux VANETs et détaillé ses différentes menaces et exigences de sécurité, il est primordial de voir quelques éléments et mécanismes essentiels qui permettent d'assurer un niveau de sécurité dans le réseau.

- **La cryptographie**

La cryptographie est la technologie utilisée pour la protection des données transmises, qui contiennent les messages des différentes communications. La cryptographie utilise principalement des clés et des codes secrets pour crypter (coder) le contenu d'un

message à l'aide d'un algorithme de chiffrement, pour le rendre illisible et donc inexploitable par les entités malveillantes. Pour rendre un message crypté lisible, les entités destinataires disposent d'une clé (code) et d'algorithmes de déchiffrement appropriés pour décrypter le message et rendre son contenu lisible et utilisable. Il existe deux types de cryptographies : cryptographie symétrique et asymétrique.

- **Les certificats**

Parmi les résultats des algorithmes de la cryptographie, on trouve les certificats, qui permettent d'augmenter le degré de la sécurité dans les réseaux VANETs. Chaque véhicule possède un seul certificat à long terme [20], qui contient l'identité et les caractéristiques du véhicule. Il se charge principalement de renouveler les certificats à court terme. Ainsi, le véhicule possède donc plusieurs certificats à court terme, qui contiennent un identifiant virtuel et des pseudonymes de communication. Les certificats doivent permettre la préservation de la vie privée et l'anonymat du véhicule.

- **Le hachage**

Le hachage consiste à déterminer une information de taille fixe et réduite appelée « l'empreinte ou le condensé » à partir d'une chaine de données fournit en entrée, de différentes tailles plus longues. Les fonctions de hachage à sens unique sont les plus utilisées. La particularité de cette fonction est qu'il est très facile de calculer et d'extraire une empreinte de n'importe quelle chaine donnée, mais très difficile, voire impossible, de retrouver la chaine initiale à partir de l'empreinte [21]. C'est une fonction irréversible.

- **La signature numérique**

La signature numérique est un code (une donnée) numérique, associé à un message afin de permettre aux destinataires de vérifier son authenticité et ainsi prouver son intégrité. Elle est implémentée et obtenue avec des fonctions de hachage en utilisant la clé privée de la source du message (l'expéditeur) appelée aussi signataire du message.

- **La technique MAC**

L'un des mécanismes de base de la sécurité dans les réseaux VANETs est la technique MAC (Message Authentification Code). Elle assure la même fonctionnalité que la signature numérique. C'est un code qui accompagne les données. Il est implémenté en utilisant la clé secrète de la cryptographie avec des fonctions similaires à celle de hachage. Il assure principalement l'authentification des messages dans le réseau.

- **Le dispositif TPD**

Le TPD (Tamper-Proof Device) est un dispositif composé de matériels et logiciels qui contiennent plusieurs capteurs, de hautes performances, qui permettent de détruire automatiquement les informations stockées, après chaque manipulation du matériel [20]. Son mécanisme permet de stocker et garder en secret les données liées à la confidentialité du véhicule, comme les certificats et les pseudonymes privés. Ainsi il se charge de la signature de tous les messages envoyés par le véhicule.

2.4 Conclusion

Dans ce chapitre, on a présenté et décrit les principaux concepts du réseau VANETs, ses caractéristiques, ses types de messages et applications, qui font de ce réseau l'un des plus complexes, nécessitant plus d'attention et de sécurité. Ensuite, on a décortiqué les concepts de la sécurité dans ces réseaux. On a vu l'ensemble de ses caractéristiques, ses principales menaces et les exigences de sécurité. Enfin, on a terminé par une vue d'ensemble sur les mécanismes utilisés pour assurer au mieux la sécurité dans les réseaux VANETs.

Bien que la sécurité dans VANETs suscite déjà beaucoup d'attention et d'études. Elle reste l'une des principales faiblesses du réseau. En effet, face au développement constant des menaces sur la vie privée des véhicules et la préservation de leurs anonymats dans les réseaux, les solutions proposées ne sont pas très performantes et souvent défaillantes. Dans le chapitre suivant, nous allons présenter quelques travaux de littératures liés à la préservation de la vie privée et à l'anonymat des véhicules,

CHAPITRE 3

REVUE DE LA LITTÉRATURE

3.1 Introduction

Au cours de ces dernières années, beaucoup de travaux de recherche ont été axés sur la sécurité des véhicules dans le domaine des réseaux véhiculaires (VANETs). Mais plus particulièrement, une attention considérable a été accordée à l'anonymat et à la préservation de la vie privée des véhicules.

Dans le chapitre présent, nous résumons quelques travaux qui ont été réalisés récemment, dans le cadre de la préservation de la vie privée conditionnelle des véhicules et de leur localisation. Afin d'assurer l'anonymat dans des réseaux Ad Hoc véhiculaires (VANETs).

Nous avons choisi de résumer des travaux qui ont été réalisés sur différents axes et qui ont utilisé différentes stratégies et méthodes, mais qui ont tous le même objectif de sécurité, à savoir, la préservation de la vie privée des véhicules dans les réseaux VANETs.

3.2 La vie privée et l'anonymat dans les réseaux VANETs

Dans [5] Yuanyuan Pan et Jianqing Li considèrent que la coopération sur le changement des pseudonymes peut améliorer l'anonymat des véhicules. Dans ce contexte, ils présentent un système de changement des pseudonymes en mode coopératif, basé sur le nombre de voisins dans VANETs (Cooperative Pseudonym change scheme based on the number of Neighbors (CPN)). Ils font une analyse générale sur l'anonymat fourni par le système PCN et le comparent avec son système correspondant sans la coopération, Non-PCN (NCPN).

La méthode présentée par les auteurs est intéressante, mais incomplète puisqu'elle ne présente pas des solutions pour tous les cas possibles sur les routes, par exemple, le cas où le véhicule durant son parcours n'atteint pas le nombre précisé des voisins pour déclencher le changement de son pseudonyme.

Mathews SM et Bevish Jinila Y proposent dans [22] une stratégie appelée PCP (Pseudonym Changing at Proper Location). Ils proposent des endroits spécifiques pour le changement des pseudonymes privés par les véhicules. Des endroits qui rassemblent plusieurs véhicules, par exemple, quand le feu de circulation passe au rouge dans une intersection ou dans un parking gratuit à proximité d'un centre commercial. Avec cette stratégie, les auteurs estiment que si tous les véhicules changent leurs pseudonymes avant de quitter le lieu social, la confidentialité de la localisation et l'anonymat peuvent être atteints.

Les auteurs ont présenté le modèle PPSD (Practical Pseudonym self-Delegation), qui génère plusieurs pseudonymes sur demande, à une courte durée de vie. Ensuite ils ont utilisé l'ASS (Anonymity Set Size) comme mesure de la vie privée (plus l'ASS est grande, plus l'anonymat est assuré). Pour prouver formellement la faisabilité de la stratégie PCP (Pseudonym Changing at Proper Location), ils ont utilisé les techniques de la théorie des jeux simplifiés. Néanmoins, ce modèle de PCP présenté ici est loin d'être le meilleur pour l'anonymat et la sécurité des véhicules dans la réalité. En effet, un véhicule peut parcourir une très longue distance, sans passer par un lieu social (comme décrit par les auteurs).

Dans [23] Yeong-Sheng Chen et autres proposent un mécanisme de changement des pseudonymes privés pour la protection de la confidentialité de localisation dans les réseaux VANETs. Ils ont développé quatre mécanismes, AS, AD, SD et ADS (A pour l'âge, D pour la direction et S pour la vitesse) en utilisant différents critères fondés sur l'âge de pseudonymes (lorsque l'âge est sur le seuil, le véhicule va essayer de changer son pseudonyme), la direction de déplacement des véhicules (le changement de pseudonyme doit être effectuée lorsque le véhicule change de direction de déplacement) et la vitesse de déplacement des véhicules (lorsqu'un véhicule se déplace

à faible vitesse, ceci implique qu'il est en train de changer sa direction de déplacement ou les routes sont entassées par des véhicules).

Bien que les auteurs ont évoqué des questions importantes dans leur solution, leur contribution reste basique et incomplète, car ils n'ont pas étudié la plupart des cas de comportements des véhicules sur la route, par exemple, dans le cas où les véhicules roulent avec des vitesses supérieures à 54 kilomètres par heure, aussi ils n'expliquent pas comment ils ont choisi le seuil de l'âge des pseudonymes.

Dans [24] Wang Ying et autres proposent, un mécanisme établi avec un système de chiffrement, basé sur l'identité (ID-based cryptosystem). Pour assurer une vie privée conditionnelle et faire avancer l'anonymat. Ils ont utilisé un système CFP (Pseudos Synchrone Change). Mais ils n'ont jamais simulé leur mécanisme.

Bien que théoriquement la méthode adoptée par les auteurs semble efficace, pour la protection de la vie privée et la localisation, dans VANETs, mais sans simulations et analyse, rien ne peut être prouvé. Ajoutant à cela que cette méthode ne présente pas tous les scénarios possibles sur les routes, par exemple, ils ne limitent pas le temps d'attente, il peut avoir une très longue période sans aucun changement de pseudonymes.

Boualouache et autres proposent dans [25] une stratégie pour les pseudonymes, appelée, silence et échange aux intersections signalisées S2SI (Silence and Swap at Signalized Intersection), ce protocole est censé maintenir la responsabilité et réduire le nombre total de pseudonymes. Les auteurs proposent un protocole pour créer des zones de mélange silencieuses, SMS (A Silent Mix Zones) aux intersections signalisées et un protocole d'échange (Swapping Protocol), qui permet l'échange des pseudonymes entre les véhicules. Quand que le feu de signalisation est en rouge, les véhicules tournent leur transmission radio en position « éteint ». Le RSU choisit alors, au hasard, deux véhicules pour l'échange de leurs pseudonymes. Les deux véhicules choisis échangent leurs pseudonymes entre eux, puis ils renvoient un message crypté au RSU, chacun utilisant son ancien pseudonyme, qui contient le pseudonyme de l'autre véhicule choisi.

Cette stratégie peut fonctionner dans une zone urbaine, où on peut trouver de grands nombres de véhicules qui s'arrêtent aux intersections signalisées. Mais, elle n'est pas toujours valable dans les zones rurales ou autoroutières, où il n'y a pas nécessairement d'intersections signalisées.

Aussi ce protocole ne donne pas la possibilité de rompre le silence radio, s'il y a un message d'urgence ou une alerte, car dans la vraie vie, on ne peut rien prédire.

Dans [26], Xinyi Wang et autres proposent une solution qui se base sur un lot de véhicules anonyme authentifié et un régime d'agrément de clés à l'aide des clés publiques auto-certifiées, « A novel anonymous batch authenticated and key agreement scheme using self-certified public keys », ces clés publiques sont impliquées dans la distribution de clés secrètes entre les fournisseurs de services (SPs) et les véhicules, pour authentifier simultanément plusieurs requêtes, envoyées par les différents véhicules et de négocier les différentes sessions entre-temps.

Les auteurs, dans leur solution, supposent que les véhicules sont équipés d'un dispositif inviolable TPD (Tamper-Proof Device), qui est fixé contre les tentatives, ensuite ils présentent le système d'amorçage et ils expliquent comment l'autorité de confiance TA (Trusted Authority) configure les paramètres du système. L'enregistrement des fournisseurs de services est basé sur les clés publiques auto-certifiées.

Les Auteurs estiment que leur proposition est une solution pour la préservation de la vie privée conditionnelle, en tirant avantage des pseudo identités et qu'elle répond aux questions de sécurité, mais ils n'ont fait aucune analyse ni simulation pour prouver sa faisabilité.

Dans [27] Huang Lu, Li Jie et Mohsen Guizani proposent un protocole d'identification basée sur l'authentification entre les véhicules et les RSUs (ID-based Signature) et un autre protocole qui gère l'authentification entre les véhicules (IBOSS: ID- based Online / Offline Signature), qui peut fournir une sorte de confidentialité.

Les auteurs de ce travail n'ont pas déterminé l'intervalle de temps pour les changements de clés des véhicules, puisque c'est une question fondamentale pour la sécurité et la vie privée contre les attaques malveillantes.

Song Guo, Deze Zeng et Yang Xiang dans [28] proposent un protocole d'authentification, préservant la vie privée avec traçabilité de l'autorité, en utilisant les courbes elliptiques basées sur le hachage caméléon.

La caractéristique des algorithmes de signature de caméléon est non-interactive. Cela signifie que la signature peut être générée sans interagir avec le récepteur prévu. Cependant, elle nécessite la même clé publique. La version améliorée proposée par les auteurs permet d'éviter l'utilisation des clés publiques fixes. Les auteurs estiment que leur protocole assure l'authentification mutuelle et anonyme, l'intraçabilité du véhicule, la capacité de suivi d'autorité et une grande efficacité de calcul.

Bien que les auteures croient que l'utilisation des courbes elliptiques basées sur le hachage caméléon est efficace, mais pour assurer l'anonymat et la prévention contre la traçabilité illégale, l'établissement d'un bon protocole pour l'utilisation et le changement régulier des pseudonymes de communications est fondamental.

Dans [29] Dijiang Huang et autres proposent, un protocole d'authentification et de confidentialité basé sur les pseudonymes des véhicules pour le système de transport intelligent STI. Le mécanisme de leur proposition est basé sur l'enregistrement de chaque véhicule au sein de l'autorité centrale TA et sa réception d'un billet, qui doit être transmis aux RSUs. Ensuite, les RSUs communiquent aux véhicules les informations nécessaires pour qu'ils puissent générer leurs pseudonymes de communication.

Les auteurs de ce travail n'ont pas bien expliqué tout le mécanisme des pseudonymes de communications, par exemple, le moment quand les véhicules doivent changer leurs pseudonymes de communications et comment ils les communiquent aux autres véhicules, avec lesquels ils doivent communiquer dans le réseau.

Dans [30], Adetundji Adigun et autres proposent un protocole de sécurité basé sur un changement de pseudonyme périodique. Ils proposent deux approches. Dans la première approche, chaque véhicule demande à l'autorité centrale un nouveau pseudonyme de communication, après un temps donné. Dans la seconde approche, chaque véhicule génère lui-même un nouveau pseudonyme de communication, après un temps donné. Ils ont évalué la bande passante utilisée en considérant la vitesse du véhicule dans chaque approche. Le protocole proposé est basé sur la répartition équidistante des unités routières RSUs et l'utilisation de la vitesse moyenne autorisée sur la route, pour évaluer la durée de vie des pseudonymes de communication.

Les vitesses utilisées dans ce travail sont les vitesses autorisées sur les routes, alors qu'en réalité, les véhicules se déplacent à des vitesses variables et peu de véhicules circulent avec les vitesses autorisées.

3.3 Conclusion

Bien que l'utilisation de différents pseudonymes de communication permette d'avoir un bon niveau de sécurité dans les réseaux véhiculaires VANETs, il est crucial de les changer régulièrement pour assurer l'anonymat et de prévenir la traçabilité illégale.

La plupart des études et des travaux proposés dans ce contexte n'ont pas été en mesure d'offrir une solution fiable et fonctionnelle dans toutes les situations, en conséquence aucune solution n'a pu atteindre le niveau de sécurité recommandé avec des résultats garantis.

Notre contribution consiste à fournir un protocole sûr et fiable en toutes circonstances pour changer les pseudonymes de communication privés, sur des périodes définies et en tenant compte des voisins de confiance (vrais nouveaux voisins directs). Nous présentons nos deux méthodes et les résultats de simulations, sous forme d'article scientifique.

Dans le chapitre 4 nous présentons notre article soumis à la conférence MSWIM 2015. 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. Novembre 2-6, 2015 Cancun Mexico.

CHAPITRE 4

An Efficient Pseudonym Change Protocol Based on Trusted Neighbors for Privacy and Anonymity in VANETs

Soumis à la conference MSWIM'15, 18th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. Novembre 2-6, 2015 Cancun Mexico.

Numéro papier: 1570164665.

An Efficient Pseudonym Change Protocol Based on Trusted Neighbours for Privacy and Anonymity in VANETs

Kahina MOGHRAOUI AOUDJIT[1]
Laboratoire de Mathématiques et Informatique Appliquées (LAMIA), Department of Mathematics and Computer Science, University of Quebec at Trois-Rivières
Trois-Rivières, QC, Canada
Kahina.Moghraoui@uqtr.ca

Boucif AMAR BENSABER[2]
Laboratoire de Mathématiques et Informatique Appliquées (LAMIA), Department of Mathematics and Computer Science, University of Quebec at Trois-Rivières
Trois-Rivières, QC, Canada
Boucif.Amar.Bensaber@uqtr.ca

Abstract—**In vehicular ad hoc networks (VANETs), regular changes in private communication pseudonyms are important to avoid illegal tracking of vehicles and to ensure their anonymity. In this paper, we propose a pseudonym change protocol based on the detection of trusted neighbours. In the absence of the latter, we opted for the attribution of a lifetime to pseudonyms. This protocol triggers the pseudonym change in several vehicles at the same time, a solution that improves vehicles anonymity.**

In this paper, we evaluate the performance of our protocol and compare our work to that based on a triggering system that changes pseudonyms with individual behaviour after a limited lifetime.

Categories and Subject Descriptors
C.2.2 [**Network Protocols**]

General Terms
Security

Keywords
VANET pseudonym, privacy, anonymity, neighbours, vehicles, traceability, security.

I. INTRODUCTION

In vehicular ad hoc networks (VANETs), vehicles are equipped with wireless communication devices called onboard units (OBUs) to enable different types of communication between them: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). During these communications, vehicles broadcast a range of highly sensitive information, such as position, speed and direction.

Thus, a malicious adversary can trace a vehicle and follow it. This makes protecting the privacy of vehicles by anonymous authentication a fundamental issue [1], [2], [3] but particularly difficult due to the high mobility of the network.

To address this problem, regular changes in communication pseudonyms are important to avoid illegal tracking of vehicles and to ensure their anonymity [4]. Many pseudonym change mechanisms have been proposed. These solutions are based mainly on triggering individual or cooperative behaviour [5].

In this paper, we propose two different approaches. The first approach is a private pseudonym change protocol based on the detection of true new neighbours that we called trusted neighbours. New direct neighbours are determined and, according to the traffic area parameters, we verified the presence of these trusted neighbours. In the absence of these neighbours, the trigger will be the end of the lifetime of the pseudonyms. In both cases, our system changes the pseudonyms in several vehicles at the same time, preserving their anonymity.

The second approach is a solution with individual behaviour. Each vehicle, at the end of its pseudonym's lifetime, changes the pseudonym in a small random time interval. This ensures pseudonym changes periodically but not at a constant time. Malicious vehicles cannot predefine the time change.

Our objective is to evaluate the two proposed approaches by analyzing them and comparing the results of the simulations.

The remainder of this paper is organized as follows. In Section II, we discuss the state of art on privacy in VANETs. In Section III, we present our model. In Section IV, we describe the simulation parameters and provide an analysis of the results. Finally, we conclude in Section V.

II. STATE OF THE ART

Much work has focussed on vehicle ad hoc networks (VANETs) in recent years in order to improve vehicle safety. In this research, considerable attention has been paid to the location privacy and anonymity of vehicles. In [5], the authors present a cooperative pseudonym change scheme based on the number of neighbours in VANETs (CPN). They generally analyze the anonymity provided by the CPN system and compare it to its corresponding system without cooperation, in other words, non-CPN (NCPN). The method presented by the authors is interesting but does not provide a solution to any possible cases on the road, such as whether the vehicle is travelling on a very long road without reaching the specified number of neighbours to change the pseudonym. The authors in [6] propose a strategy called PCP (Pseudonym Changing at

Proper Location). They use specific places for changing pseudonyms by vehicles, for example, the intersection of the road, when the traffic light turns red or in free parking near a shopping center. With this strategy, the authors estimate that if all vehicles change their pseudonyms before leaving the social place, location privacy can be achieved. In order to formally prove the feasibility of the PCP strategy, they used simplified game-theoretic techniques. This PCP model is not a complete solution to ensure vehicle anonymity because a vehicle cannot regain a social spot during its travel. In [7], the authors propose pseudonym changing schemes for location privacy protection in VANETs. Four mechanisms are developed by using different criteria based on the age of the pseudonyms (when the age is over the threshold, the vehicle will try to change its pseudonym), the moving direction of the vehicles (pseudonym change should be performed when the vehicle changes its moving direction) and the moving speed of the vehicles (when a vehicle moves in low speed, it implies that it is changing its moving direction or the roads are crowded with vehicles). This study is incomplete, since the authors have not studied several possible cases of actual vehicle behaviour on the road (such as speed greater than 54 km/h), nor did they explain how they chose the pseudonym age threshold. In [8], the authors propose a mechanism using an ID-based cryptosystem offering conditional privacy. They attempted to advance the anonymity and used the PSC (Pseudonyms Synchronously Change) scheme. However, they never simulate their mechanism. Although theoretically the method adopted by the authors appears to be effective in protecting location privacy in VANETs, without visible simulation results nothing is proven. Also, this method does not present all possible scenarios on roads. For example, they did not limit the waiting time, meaning that there can be a very long period without any change in pseudonyms. In [9], the authors propose a pseudonym strategy called S2SI (Silence and Swap at Signalized Intersection). This protocol is supposed to maintain accountability and reduces the total number of pseudonyms. They proposed a protocol to create Silent Mix Zones (SMs) at signalized intersections and the Swapping Protocol, which allows the exchange of pseudonyms between vehicles. While the traffic light is red, vehicles turn their radio transmission off and the RSU randomly chooses two vehicles to exchange their pseudonyms. It then sends them an encrypted message using its old pseudonym, which contains the pseudonym of another chosen vehicle. This strategy can work in urban areas where a large number of vehicles are stopped at signalized intersections, but it is not valid in rural areas where signalized intersections may not exist. Also, this protocol does not provide the opportunity to break radio silence if there is an emergency message because, in real life, we cannot predict anything. In [10], the authors propose a novel anonymous batch authenticated and key agreement scheme using self-certified public keys, which are involved in distributing secret keys among service providers (SPs) and vehicles. They assume that vehicles are equipped with a tamper-proof device, which is secured against attempts, and explain the initiation system and how TA (Trust Authority) sets up the system parameters. The authors believe that their scheme fulfils conditional privacy by taking advantage of pseudo identities and addresses the safety issues. However, they did not prove their scheme with simulations. In [11], the authors propose an identification protocol based on authentication between vehicles and RSUs (IBS: ID-based Signature) and another that handles authentication between vehicles (IBOSS: ID- based Online / Offline Signature), which can provide a kind of confidentiality. The authors have not determined the time interval to change vehicle keys, as it is a fundamental issue for security and privacy against malicious attackers. In [12], the authors propose a privacy-preserving authentication protocol with authority traceability using elliptic curve-based chameleon hashing. The characteristic of chameleon signature algorithms is non-interactive. It means that the signature can be generated without interacting with the intended receiver. However, it requires the same public key. This improved version avoids using the fixed public keys. The authors believe that their protocol ensures mutual and anonymous authentication, vehicle unlinkability, authority tracking capability and high computational efficiency. Although the use of the elliptic curve-based chameleon hashing looks effective, they did not propose any regular pseudonym changes to ensure anonymity and prevent illegal tracking. In [13], the authors propose an authentication protocol and confidentiality based on vehicle pseudonyms for intelligent transport systems. The mechanism involves registering each vehicle within the central authority and receiving a ticket, which must be transmitted to RSUs. The RSUs then communicate to the vehicles the information necessary to generate the communication pseudonyms. The authors of this work do not adequately explain all the pseudonym communication mechanisms, for example, the time of the change in pseudonyms by vehicles and how it is transmitted to vehicles. In [14], the authors propose a security protocol based on a periodic pseudonym change. They propose two approaches. In the first approach, each vehicle asks the central authority for a new communication pseudonym after time t. In the second approach, each vehicle generates a new communication pseudonym after time t. They evaluated the bandwidth used by considering the vehicle speed in each approach. The proposed protocol is based on the equidistant distribution of the roadside unit and uses the average speed permitted on the road to evaluate the lifetime of the communication's pseudonyms and certificates. The speeds used in this work are the posted road speeds, whereas in reality, vehicles travel at varying speeds and few travel at posted speeds. At least two vehicles change their pseudonym at the same time. This means that the protocol ensures anonymity and prevents illegal tracking. Although, the use of different communication pseudonyms offers a good level of security in VANETs and it is crucial to change them in order to ensure anonymity and prevent illegal tracking.

Most studies and work proposed in this context have not been able to offer a reliable and functional protocol in all situations. Therefore, none had secure and safe results. Our contribution is to provide a safe and reliable protocol for changing the private key (communication pseudonyms) in all

circumstances for defined periods, taking the neighbours into account.

III. SYSTEM MODEL

A. Assumptions and overall idea

Our proposed protocol prevents illegal tracking and preserves anonymity and privacy. It is composed of two different approaches. The first is a system that triggers cooperative change pseudonyms. It depends on the presence of trusted neighbours and changes the pseudonym of several vehicles at the same time. The second is a pseudonym change system with individual behaviour. It ensures the unpredictability of pseudonym changes. In either approach, it is assumed that the vehicles generate their communication pseudonyms themselves.

B. Description of the model

1) Allocation of parameters depending on the traffic area

One objective of our study is to consider a number of criteria, such as traffic area, which was not always considered in most previous works but performs a crucial role in the validation of proposed protocols. Our system works in both urban and highway traffic areas.

2) Assigning a lifetime to pseudonyms

To preserve the confidentiality of data exchanged in VANETs, ensure the anonymity of vehicles and prevent illegal tracking of vehicles, it is crucial to not keep the same communication pseudonyms throughout and to change them periodically [4]. In our work, we opted to limit the lifetime of communication pseudonyms to ensure their periodic changes in the absence of a trigger proposed in our system.

3) Approach 1: Changing pseudonyms in the presence of trusted neighbours

The steps of our first approach are described below.

a) Verification of the presence of trusted neighbours:

At time T0, the vehicle starts with identifying all direct neighbours by sending a data message within its range, including its speed, coordinates and ID. Upon receipt of the responses, it records all of these direct neighbours in a set E_1.

At time $T_1 = (T_0 + T')$, the vehicle follows the same procedure and records all of its direct neighbours in a set E_2.

T' is the minimum time that a neighbour must remain within the range of the vehicle before it is classified as a trusted neighbour. The purpose of this step is to keep only the neighbours with which the vehicle may perform large data exchanges, eliminating false neighbours such as vehicles travelling in the opposite direction at a high speed. This is illustrated in Figure 1.

T' is calculated as follows:

$$T' = 2P \div \left(\frac{Vmax}{2}\right) \times 3600$$

Where P is the range of the vehicle and $Vmax$ is the maximum speed of the traffic area.

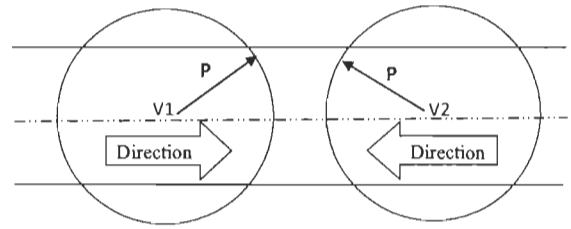

Fig. 1. Search for trusted neighbour

If after T', a neighbour is still present within the vehicle's range, it is considered as trusted neighbour regardless of its direction and speed.

The set of trusted neighbours E_c is obtained as follows:

$E_c = E_1 \cap E_2$

b) Changing the pseudonym in the presence of new trusted neighbours (If $E_c \neq \emptyset$)

The vehicle has at least one new true neighbour. This triggers a change in the communication pseudonym.

c) Changing the pseudonym without new trusted neighbour: (If $E_c = \emptyset$)

The vehicle had no true new neighbour. In this case, it checks if the lifetime (**ΔT**) of its pseudonym has lapsed and then changes it. If not, it keeps looking for new trusted neighbours.

After each pseudonym change, the vehicle resets the **ΔT** to 0.

This approach is summarized below.

ALGORITHM 1

Determine ΔT, T'
Trigger the countdown time ΔT
Step 1: Change the pseudonym based on existence of trusted neighbours:
Calculating the set of direct neighbours E_0 at T_0
Calculating the set of direct neighbours E_1 at $T_1 = (T_0 + T')$
Identifying the set of true direct neighbours
$E = E_0 \Pi E_1$
If $E \neq \emptyset$ then
Change the pseudonym
Else
Step 2: Change the pseudonym at the end of its lifetime:
If $(E = \emptyset)$ and $(\Delta T = 0)$ then
Change the pseudonym.
End if.
End of Algorithm 1.

4) Approach 2: Changing pseudonyms at a random time after a lifetime

This approach involves a trigger-based system for pseudonym changes with individual behaviour after a limited lifetime. At the end of its pseudonym's lifetime, each vehicle changes the pseudonym at a random time within a small time interval. This ensures that pseudonyms change periodically but not at constant times. Malicious nodes cannot predefine the time of private pseudonym changes for each vehicle.

ΔT: the life of the pseudonym

T: time to change the pseudonym

ALGORITHM 2

Determine ΔT
Trigger the countdown time ΔT
If $T = 0$ then
Generate a random number α between 1 and 60
Trigger the timer T
If $T = \alpha$ then
Change the pseudonym
End if.
End if.
End of algorithm 2.

IV. ANALYSIS

A. Confidentiality analysis

Vehicles regularly change their private pseudonyms in the two proposed approaches. This ensures vehicle privacy.

The first approach involves a change in the private pseudonyms of several vehicles at the same time, preventing a malicious vehicles from associating the pseudonyms to each vehicle.

In the second approach, vehicles change their private pseudonyms periodically at random times, which prevents attackers from predicting changes in private pseudonyms for each vehicle.

B. Performance analysis

To demonstrate the efficiency of our two approaches, we considered both urban and highway environments.

We are interested in the proportion of vehicles that changed their private pseudonyms because this parameter is related to the lifetime of private pseudonyms in both approaches, specifically in order to detect trusted neighbours in the first approach. We also turned our attention to the packet loss proportion, as it represents a major constraint in VANETs; we expect that speed plays a very important role. Also, we focused on the proportion of vehicles that changed their private pseudonyms simultaneously. This parameter is directly related to vehicle anonymity. The more vehicles that change their private pseudonyms simultaneously, the more their anonymity is ensured.

C. Assessment parameters

We tested the performance of our two approaches in both urban and highway environments. For simulations, we used OMNET ++ 4.4 [14] with veins-3.0 [15] and SUMO-0.21.0. [16].

TABLE I: SIMULATION PARAMETERS

Item	Value
Map of Manhattan	2.5 km x 2.5 km
Map of highway	15 km
Simulation time	1000 s
Lifetime of private pseudonyms	3 min
Vmax urban	14 m/s
Vmax highway	30 m/s
Packet size	1024 bytes
Number of vehicles in each approach	50;100;150;200
Bit rate	18 Mbps
MAC Protocol	IEEE 802.11p
Communication range of vehicle	800 m

We ran the simulations of each proposed approach five times for each environment (urban and highway) and each proposed number of vehicles (50; 100; 150; 200). We also calculated the average of the simulation results.

D. Results

1) Proportion of vehicles that changed their private pseudonyms in each approach

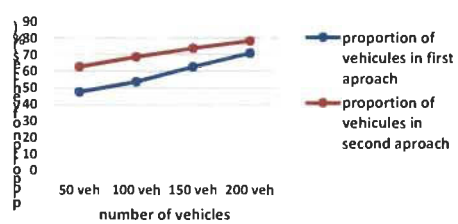

Fig. 2. Proportion of vehicles that changed their private pseudonyms in urban environment

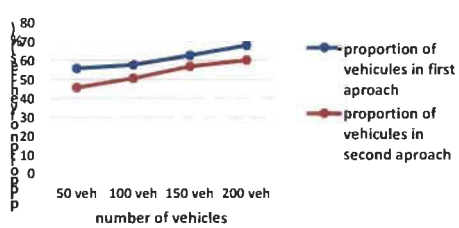

Fig. 3. Proportion of vehicles that changed their private pseudonyms in highway environment

The simulation results in Figure 2 show the rate of vehicles that changed their private pseudonyms in the urban environment. The proportion of the first approach starts at 50% and increases with the increasing number of vehicles; it exceeds 70%. The more vehicles there are on the road, the more trusted neighbours are detected. This explains the large number of private pseudonym changes.

In the second approach, the rate of vehicles that changed their private pseudonyms begins at around 60% and increases slowly to almost 70%. This is due to changes in private pseudonyms made by vehicles individually and is not dependent on any other external factors.

In Figure 3, the results show the proportion of vehicles that changed their private pseudonyms in the highway environment. In the first approach, the proportion begins at close to 60% and increases slightly to close to 70%. The increase in the second approach is also very slight; it starts between 40% and 50% and reaches 60%.

The proportion of change in private pseudonyms in the two approaches for the highway environment is lower than the rate for the urban environment. This is related directly to the packet loss rates, which are more significant for the highway environment because of high vehicle speeds. The results are shown in figures 4 and 5.

In the two approaches of our system and in both urban and highway environments (figures 2 and 3), the proportion of vehicles that changed their private pseudonyms is high because the private vehicle pseudonyms have a lifetime limited to 3 minutes regardless of the scenario on the road.

2) Packet loss proportion by vehicles in each approach

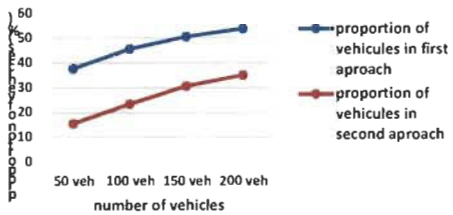

Fig. 4. Packet loss proportion by vehicles in urban environment

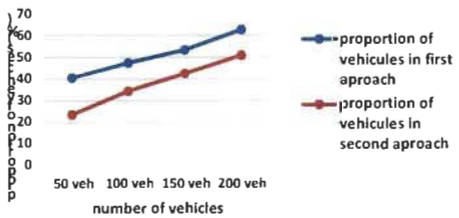

Fig. 5. Packet loss proportion by vehicles in highway environment

Simulation results in Figure 4 show that the packet loss proportion (PLR) for the first approach in the urban environment is nearly 40% with a simulation of 50 vehicles. It increases depending on the increased number of vehicles and exceeded 50% for 200 vehicles. In the second approach, the PLR starts at over 10% and increases slightly to 40%.

Figure 5 shows that the PLR for vehicles in the highway environment exceeds 40% for the first approach and increases to over 60%, while in the second approach, it is almost 20% for the 50 simulated vehicles and reaches 50% for 200 vehicles.

The PLR is higher in the first approach because the number of changes in private pseudonyms is higher.

For both approaches, the PLR is related to the number of vehicles and the traffic environment. Rates increase in the highway environment due to high vehicle speeds.

3) Proportion of vehicles that changed their private pseudonyms simultaneously in each approach

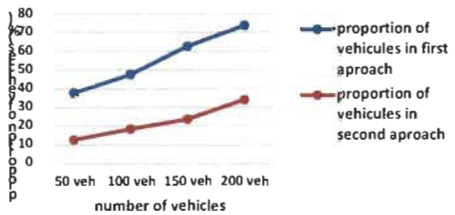

Fig. 6. Proportion of vehicles that changed their private pseudonyms simultaneously in urban environment

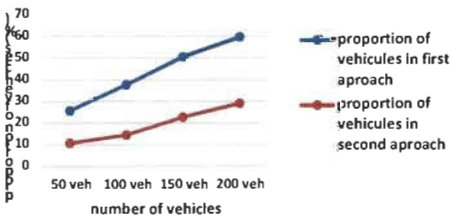

Fig. 7. Proportion of vehicles that changed their private pseudonyms simultaneously in highway environment

The simulation results in Figure 6 show that the proportion of vehicles that changed their private pseudonyms simultaneously in the urban area is about 40%, with a simulation of 50 vehicles in the first approach. It increases to 70% when the number of vehicles is 200. The second approach starts at a little over 10% and increases slightly to 30%.

Figure 7 shows that the proportion of vehicles that changed their private pseudonyms simultaneously in the highway environment for the first approach is above 20%, while the second approach has a result of around 10% for 50 simulated vehicles. In both approaches, the proportion increases with the increase in the number of vehicles to 60% for approach 1 and almost 30% for approach 2 for 200 vehicles.

These results show that our proposed approach based on the presence of trusted neighbours is effective in both areas (urban and highway) and that anonymity is related to the number of vehicles on the road and to the environment (urban and highway). This means that the more vehicles there are on the road, the more anonymity is ensured.

The authors in [5] propose a cooperative pseudonym change scheme based on the number of neighbours in VANETs. They claim that the cooperative pseudonym change scheme solutions are better than the solution to individual behaviour.

The simulation results for our second approach involving changes in pseudonyms with an individual behaviour trigger prove its effectiveness in preserving anonymity. At the end of its pseudonym's lifetime, each vehicle changes the pseudonym at a random time within a small time interval. This ensures that pseudonyms change periodically and not at constant times. Malicious nodes cannot predefine the time of private pseudonym changes for each vehicle. This results in vehicle anonymity.

Also, the method presented by the authors in [5] does not present solutions to any possible cases on the road, such as when a vehicle is travelling on a very long road without reaching the specified number of neighbours in order to change the pseudonym.

Thus, our first approach based on changing pseudonyms according to trusted neighbours considers all possible cases. Private pseudonyms have a limited lifetime, which ensures their change periodically even in the absence of trusted neighbours. This approach also ensures that the private pseudonyms of several vehicles are changed at the same time. After each pseudonym change, all vehicles in the neighbourhood reset the lifetimes of their pseudonyms simultaneously. This ensures vehicle anonymity VANETs.

V. CONCLUSION

In this paper, we propose two different approaches. The first approach is a private pseudonym change protocol based on the detection of trusted neighbours. This solution ensures that pseudonyms are changed in several vehicles at the same time, preserving their anonymity. The second approach is a solution based on individual behaviour. It ensures that private pseudonym changes cannot be predicted. We compared the two approaches and evaluated the proportion of vehicles that changed their private pseudonyms, the packet loss proportion by vehicle and the proportion of vehicles that changed their private pseudonyms simultaneously.

The results show that vehicle anonymity in VANETs is due mainly to two key factors: the number of vehicles on the road and the speed at which vehicles are travelling. This means that the fewer vehicles there are on the road and the higher the speeds at which they travel, the less anonymity is ensured. It follows then that the more vehicles there are on the road and the slower the speeds at which they travel, the more anonymity is ensured.

The results confirm the credibility of our two approaches in ensuring vehicle anonymity and privacy in VANETs in all circumstances and environments (urban and highway).

In future work, we intend to further study the lifetimes of private pseudonyms and develop other approaches with other triggers for pseudonym changes, such as distance travelled.

REFERENCES

[1] Florian Dötzer. Privacy Issues in Vehicular Ad Hoc Networks. In: Proceedings of the fifth international conference on privacy enhancing technologies (PET'05). Cavtat, Croatia; 2006. pp. 197–209.

[2] Hubaux JP, Capkun S, Luo J. The security and privacy of smart vehicles. IEEE Security and Privacy 2004; 2(3):49–55.

[3] Youngho Park, Kyung-Hyune Rhee, Chul Sur. A Secure and Location Assurance Protocol for Location-Aware Services in VANETs. 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 456–61, 2011.

[4] Freudiger J, Manshaei MH, Le Boudec J-Y, Hubaux J-P. On the Age of Pseudonyms in Mobile Ad Hoc Networks. INFOCOM, 2010 Proceedings IEEE, pp. 1–9, Mar. 2010.

[5] Yuanyuan Pan, Jianqing Li. Cooperative pseudonym change scheme based on the number of neighbors in VANETs. *Journal of Network and Computer Applications* 36 (2013):1599–1609.

[6] Mathews SM, Bevish Jinila Y. An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet. Electronics and Communication Systems (ICECS), 2014 International Conference on.

[7] Yeong-Sheng Chen, Tang-Te Lo, Chiu-Hua Lee, Ai-Chun Pang. Efficient pseudonym changing schemes for location privacy protection in VANETs. Connected Vehicles and Expo (ICCVE), 2013 International Conference on.

[8] Wang Ying, Jiujiang, China, Yang Shiyong. Protecting Location Privacy via Synchronously Pseudonym Changing in VANETs. Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on.

[9] Boualouache, Abdelwahab, Moussaoui Samira. S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs. Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on.

[10] Xinyi Wang, Zheng Huang, Qiaoyan Wen, Hua Zhang. An efficient anonymous batch authenticated and key agreement scheme using self-certified public keys in VANETs. TENCON 2013 - 2013 IEEE Region 10 Conference (31194), 22–5, Oct. 2013.

[11] Huang Lu, Jie Li, Mohsen Guizani. A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs. Computing, Communication and Applications Conference (ComComAp), pp. 345–50, 2012.

[12] Song Guo, Deze Zeng, Yang Xiang. Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications. Parallel and Distributed Systems, IEEE Transactions on, Issue Date: Nov. 2014.

[13] Dijiang Huang, Satyajayant Misra, Mayank Verma, Guoliang Xue, PACP. An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. Intelligent Transportation Systems, IEEE Transaction on Volume 12, pp. 736–46, 2011.

[14] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri. Protocol of Change Pseudonyms for VANETs. 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference on. pp. 162–7, ISBN: 978-1-4799-0539-3, 21–24 October 2013, Sydney, NSW.

[15] http://www.omnetpp.org/ visited 25/05/2015

[16] http://veins.car2x.org/ visited 25/05/2015

[17] http://sumo.sourceforge.net/ visited 25/05/2015

CHAPITRE 5

DISCUTIONS GÉNÉRALE DES RÉSULTATS

5.1 Analyse de la confidentialité :

Les véhicules changent régulièrement leurs pseudonymes privés dans les deux approches proposées. Cela garantit la vie privée des véhicules.

La première approche implique un changement des pseudonymes privés de plusieurs véhicules en même temps, empêchant un véhicule malveillant d'associer les pseudonymes à chaque véhicule.

Dans la seconde approche, les véhicules changent leurs pseudonymes privés périodiquement à des moments aléatoires, ce qui empêche les attaquants de prévoir les changements des pseudonymes privés par chaque véhicule.

5.2 Discussion des résultats :

Pour démontrer l'efficacité de nos deux approches, nous les avons simulées dans les deux environnements urbain et autoroutier.
Nous avons étudié et calculé le pourcentage des véhicules qui ont changé leurs pseudonymes (voire fig 2 et fig 3 dans l'article). Ce paramètre est lié à la durée de vie des pseudonymes privés dans les deux approches. En effet, les résultats montrent que les proportions des véhicules qui ont changé leurs pseudonymes privés sont élevées, pour les deux approches et dans les environnements urbain et autoroutier. Car les pseudonymes des véhicules ont une durée de vie limitée à trois minutes, quel que soit le scénario sur les routes.

Nous avons aussi évalué les pourcentages de perte de paquets (voire fig 4 et fig 5 dans l'article). Car elle représente une contrainte majeure pour les réseaux VANETs. Les

résultats montrent que le pourcentage de perte de paquets est plus élevé dans la première approche à cause du nombre élevé des changements de pseudonymes.
Pour les deux approches, le pourcentage de pertes de paquets est lié au nombre de véhicules et à l'environnement de la circulation. Les proportions augmentent dans l'environnement autoroutier en raison des grandes vitesses des véhicules.

Enfin, nous nous sommes intéressés aux pourcentages des véhicules qui ont changé leurs pseudonymes privés simultanément (voire fig 6 et fig 7 dans l'article). Ce paramètre est directement lié à l'anonymat des véhicules. Plus il y a beaucoup de véhicules qui changent leurs pseudonymes privés simultanément, plus leur anonymat est assuré. Nos résultats montrent que notre première approche basée sur la présence des voisins de confiance est efficace dans les deux zones (urbaines et autoroutes) et que l'anonymat est lié au nombre des véhicules sur la route et à la zone de circulation.

5.3 Comparaison des performances :

Pour appuyer les résultats de nos simulations et prouver l'efficacité de nos deux approches proposées, on a comparé les performances de nos solutions à celles de la solution proposée par Yuanyuan Pan et Jianqing Li dans [5], qui propose un système de changement de pseudonyme coopératif, basé sur le nombre des voisins dans les réseaux VANETs.

En effet, la méthode proposée par les auteurs dans [5] ne présente pas de solutions à tous les cas possibles sur la route, comme lorsqu'un véhicule circule durant une longue période sur une route, sans atteindre le nombre spécifié des voisins pour lui permettre de changer son pseudonyme de communication.

Ainsi, notre première approche basée sur le changement des pseudonymes privés en fonction de la présence des voisins de confiance prend en considération tous les cas possibles. Puisque les pseudonymes privés ont une durée de vie limitée, ce qui assure leur changement périodique même en absence de nouveaux voisins de confiance.

Cette approche garantit également le changement des pseudonymes privés par plusieurs véhicules en même temps. Car après chaque changement de pseudonymes,

tous les véhicules du voisinage réinitialisent les durées de vie de leurs pseudonymes en même temps. Ceci assure l'anonymat des véhicules dans les réseaux VANETs, quel que soit le scénario sur la route.

Les auteurs dans [5] affirment que pour assurer l'anonymat dans les réseaux VANETs, les solutions de changement de pseudonymes en mode coopératif sont meilleures que les solutions aux comportements individuels. Ce qui n'est pas souvent vrai. En effet, les résultats de simulations de notre deuxième approche qui présente un système de changement de pseudonymes à comportement individuel prouvent son efficacité pour assurer l'anonymat. Car chaque véhicule change son pseudonyme après la fin de sa durée de vie, en un temps aléatoire dans un petit intervalle de temps. Ce qui garantit le changement périodique des pseudonymes, mais pas à des temps constants. Les véhicules malveillants ne peuvent pas prédéfinir ces temps de changement. Ceci garantit l'anonymat des véhicules.

CHAPITRE 6

CONCLUSION GÉNÉRALE

Les réseaux VANETs se démarquent des autres réseaux sans fil par leurs composants et leurs caractéristiques, qui les rendent très complexes, notamment à cause de la grande mobilité des véhicules. Ainsi la sécurité dans les VANETs devient aussi complexe que le réseau, ce qui nécessite plus d'attention et de contribution pour atteindre un niveau de sécurité bien adapté, particulièrement, contre les menaces à la vie privée du véhicule et son anonymat dans le réseau.

Dans notre travail, nous avons présenté deux approches différentes. La première approche est un protocole pour le changement des pseudonymes de communication privés, basé sur la détection des vrais nouveaux voisins directs qu'on a appelés voisins de confiance. Cette solution assure le changement des pseudonymes de communication privés dans plusieurs véhicules en même temps, en préservant leurs vies privées et leurs anonymats dans les réseaux VANETs. Ce protocole est une solution à comportement coopératif.

La seconde approche est une solution basée sur le comportement individuel des véhicules. Elle assure la non-prédiction des changements des pseudonymes de communication privés par d'autres véhicules malveillants

Nous avons comparé les deux approches par simulations dans les deux milieux urbains et autoroutiers. Nous avons évalué la proportion des véhicules qui ont changé leurs pseudonymes privés, la proportion de perte de paquets par les véhicules et la proportion des véhicules qui ont changé leurs pseudonymes privés simultanément.

Les résultats obtenus montrent que l'anonymat des véhicules dans les réseaux VANETs est principalement lié à deux facteurs principaux : le nombre de véhicules sur la route et leurs vitesses de circulation. En effet, moins il y a des véhicules sur la route et qui circulent à grandes vitesses, moins l'anonymat est assuré. Ainsi, plus il y

a des véhicules sur la route et qui circulent à petites vitesses, plus l'anonymat est assuré.

Les résultats confirment la crédibilité de nos deux approches en garantissant la préservation de la vie privée des véhicules et l'anonymat dans les réseaux VANETs, en toutes circonstances et dans les deux environnements (urbains et routiers).

Dans les travaux futurs, nous avons l'intention d'approfondir dans l'étude des durées de vies des pseudonymes privées de communication et de développer de nouvelles approches, en prenant en considération d'autres facteurs de déclenchement pour les changements des pseudonymes privés, notamment le facteur de distance parcourue par le véhicule, qui est très déterminant, mais pas souvent pris en considération dans les travaux antérieurs. Ainsi, on va contribuer à la mise en œuvre d'un protocole pour le changement des pseudonymes privés de communications en fonction de la distance parcourue par le véhicule.

BIBLIOGRAPHIE

[1] Florian Dötzer. Privacy Issues in Vehicular Ad Hoc Networks. In: Proceedings of the fifth international conference on privacy enhancing technologies (PET'05). Cavtat, Croatia; 2006. pp. 197–209. Print ISBN 978-3-540-34745-3

[2] Hubaux JP, Capkun S, Luo J. The security and privacy of smart vehicles. IEEE Security and Privacy 2004; PP 49–55. ISSN : 1540-7993

[3] Youngho Park, Kyung-Hyune Rhee, Chul Sur. A Secure and Location Assurance Protocol for Location-Aware Services in VANETs. 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 456–61, 2011. E-ISBN : 978-0-7695-4372-7 Conference Location: Seoul.

[4] Freudiger J, Manshaei MH, Le Boudec J-Y, Hubaux J-P. On the Age of Pseudonyms in Mobile Ad Hoc Networks. INFOCOM, 2010 Proceedings IEEE, pp. 1–9, Mar. 2010. Conference Location : San Diego, CA ISSN : 0743-166X

[5] Yuanyuan Pan, Jianqing Li. Cooperative pseudonym change scheme based on the number of neighbors in VANETs. Journal of Network and Computer Applications 36 (2013):1599–1609.

[6] Youngho Park and Kyung-Hyune Rhee, Chul Sur, "A Secure and Location Assurance Protocol for Location-Aware Services in VANETs", 50th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp.456-461, June 30 - July 2, 2011- Seoul, Korea.

[7] 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. Print ISBN: 978-1-61284-668-2

[8] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs," in IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WIMOB), Avignon, 2008. E-ISBN: 978-0-7695-3393-3.

[9] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks," in Proceedings of the 9th International Conference on Smart Spaces and Next Generation Wired/Wireless Networking and Second Conference on Smart Spaces, St. Petersburg, Russia, 2009, pp. 291-300. Print ISBN 978-3-642-04188-4.

[10] M. JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections," UNIVERSITE D'EVRY VAL D'ESSONNE thèse de doctorat, 2008.

[11] M. Fiore, J. Harri, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation for VANETs," in Proceedings of the 40th Annual Simulation Symposium, Norfolk, VA , 2007, pp. 301-309. Print ISBN: 0-7695-2814-7

[12] http://hdl.handle.net/10603/33426 vue le 30/06/2015.

[13] 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.

[14] Moez JERBI, "Protocoles pour les communications dans les réseaux de véhicules en environnement urbain: Routage et GeoCast basés sur les intersections", Thèse de Doctorat, Université d'Evry val d'Essonne, 06 novembre 2008.

[15] Arijit Khan, Shatrugna Sadhu, and Muralikrishna Yeleswarapu, "A comparative analysis of DSRC and 802.11 over Vehicular Ad hoc Networks". Dept. of Computer Science, University of California (2008).

[16] F. Kargl, "Inter-Vehicular Communication," Ulm University Habilitation Thesis, 2008.

[17] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, p. 39–68, 2007.

[18] C. TCHEPNDA, "Authentification dans les Réseaux Véhiculaires Opérés," Ecole Nationale Supérieure des Télécommunications Thèse de doctorat, 2008.

[19] Noureddine CHAm, "La sécurité des communications dans les réseaux V ANET", Mémoire, Université Elhadj Lakhder-Batna, faculté des sciences de l'ingénieur Département d'informatique, 05 Septembre 2011.

[20] 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. Print ISBN: 978-1-61284-668-2

[21] A. Yger and J.-A. Weil, Mathématiques appliquées L3, P. Education, Ed. 2009.

[22] Mathews SM, Bevish Jinila Y. "An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet". Electronics and Communication Systems (ICECS), Coimbatore 2014 International Conference on. Print ISBN: 978-1-4799-2321-2.

[23] Yeong-Sheng Chen, Tang-Te Lo, Chiu-Hua Lee, Ai-Chun Pang. Efficient pseudonym changing schemes for location privacy protection in VANETs. Connected Vehicles and Expo (ICCVE), Las Vegas, NV 2013 International Conference on. P 937 – 938. INSPEC Accession Number: 14254684.

[24] Wang Ying, Jiujiang, China, Yang Shiyong. Protecting Location Privacy via Synchronously Pseudonym Changing in VANETs. Communication Systems and Network Technologies (CSNT), Bhopal 2014 Fourth International Conference on. Print ISBN: 978-1-4799-3069-2. P 644 - 648

[25] Boualouache Abdelwahab, Moussaoui Samira. S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs. Advanced Networking Distributed Systems and Applications (INDS), Bedjaia 2014 International Conference on. P 70 – 75.INSPEC Accession Number: 14805496

[26] Xinyi Wang, Zheng Huang, Qiaoyan Wen, Hua Zhang. An efficient anonymous batch authenticated and key agreement scheme using self-certified public keys in VANETs. TENCON 2013 - 2013 IEEE Region 10 Conference (31194) Xi'an, 22–5, Oct. 2013. Print ISBN: 978-1-4799-2825-5

[27] Huang Lu, Jie Li, Mohsen Guizani. A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs. Computing, Communication and Applications Conference (ComComAp), pp. 345–350, Hong Kong 2012. Print ISBN: 978-1-4577-1717-8

[28] Song Guo, Deze Zeng, Yang Xiang. Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications. Parallel and Distributed Systems, IEEE Transactions on, Issue Date: Nov. 2014. ISSN: 1045-9219. PP: 2794 - 2803

[29] Dijiang Huang, Satyajayant Misra, Mayank Verma, Guoliang Xue, PACP. An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. Intelligent Transportation Systems, IEEE Transaction on Volume 12, pp. 736–746, 2011. ISSN: 1524-9050

[30] Adetundji Adigun, Boucif Amar Bensaber, Ismail Biskri. Protocol of Change Pseudonyms for VANETs. 9th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks, Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference on. pp. 162–7, ISBN: 978-1-4799-0539-3, 21–24 October 2013, Sydney, NSW.