TABLE DES MATIÈRES

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS

AODV: Ad-Hoc on-Demand Distance-Vector Routing Protocol

ASTM: American Society for Testing and Materials

AU: Application Unit

CA: Central Authority

CBDRP: Cluster-Based Directional Routing Protocol

CBLR: Cluster Based Location Routing

CBR: Cluster Based Routing

CDMA: Code Division Multiple Access

CDMA 2000 1x EV: Code division multiple access 2000 1X Evolution

DSDV: Destination-Sequenced-Distance –vector routing protocol

DSR: Dynamic Source Routing

DSRC: Dedicated Short Range Communication

DoS: Déni of Service

DTSG: Dynamic Time-Stable Geocast Routing

EDCA: Enhanced Distributed Channel Access

EDGE: Enhanced Data Rate for GSM Evolution

ETSI ITS-G5: European standard for vehicular communication

ETSI: Institut Européen des normes de télécommunication

FCC: Commission Fédérale des Communications

FSR: Fisheye State Routing

GDVAN: Greedy Detection for VANET

GPS: Global Positioning System

GPRS: General Packet Radio Service

GPSR: Greedy Perimeter Stateless Routing

GSM: Global System for Mobile Communication

GYTAR: Greedy Traffic Aware Routing protocol

HARP: Home Agent Redundancy Protocol

HCB: Hierarchical Cluster Based Routing

HSDPA: *High Speed Downlink Packet Access*

IEEE: Institute of Electrical and Electronics Engineers

I2I: Infrastructure to Infrastructure

IP: Internet Protocol

ITS: Intelligent Transport Systems

LLC: Logical Link Control

LTE: Long Term Evolution

MAC: Medium Access Control

MANET: Mobile Ad hoc NETwork

MIBR: Mobile Infrastructure Based VANET Routing

OBU: On Board Unit

OLSR: Optimized Link State Routing

RAR: Roadside-Aided Routing

RDMAR: Relative Distance Microdiscovery Ad-Hoc Routing

RIN: Real Initial New

ROVER: Robust Vehicular Routing

RSU: Road Side Unit

SADV: Static-Node Assisted Adaptive Routing Protocol

SOS: Save Our Souls

TA: Trusted Authority

TBRPF: Topology Dissemination Based on Reverse-Path Forwarding

TCP: Transmission Control Protocol

TORA: Temporarily Ordered Routing Algorithm

UDP: User Datagram Protocol

UMTS: Universal Mobile Telecommunications System

VANET: Vehicular Ad hoc NETwork

VGPR: *Vertex-Based Predictive Greedy Routing*

V2I: Vehicle to Infrastructure

V2V: Vehicle to Vehicle

WAVE: Wireless Access in Vehicular Environments

WiFi: Wireless Fidelity

WiMAX: Worldwide Interoperability for Microwave Access

WSM: Wave Short Message

WSMP: Wave Short Message Protocol

ZRP: Zone Routing Protocol

2G: Second Generation

3G: Third Generation

4G: Fourth Generation

SYSTEME EFFICACE DE LA PROTECTION DE LA VIE PRIVÉE DANS LES RESEAUX VEHICULAIRES VANETs

Walid Bouksani

SOMMAIRE

Nous proposons dans ce mémoire un protocole de sécurité basé sur un changement dynamique de pseudonymes pour la protection de la vie privée dans le domaine de réseau véhiculaire Ad hoc NETworks (VANET). Notre proposition garantit la vie privée du conducteur et de son véhicule qu'il soit émetteur ou récepteur du message. Avec le traitement de tous les cas possibles de changement de pseudonymes selon le comportement des véhicules pendant la circulation, nous assurons une bonne gestion du trafic routier et sécuritaire. Nous avons développé une architecture pour notre solution basée sur trois principaux dispositifs conçus pour le système VANET. En trois étapes, l'anonymat est garanti par notre nouveau protocole "Real Initial New" (RIN) qui offre une sécurité élevée aux véhicules.

Mots-clés: VANET, sécurité, vie privée, anonymat, pseudonyme.

AN EFFICIENT AND DYNAMIC PSEUDONYMS CHANGE SYSTEM FOR PRIVACY IN VANET

Walid Bouksani

ABSTRACT

We propose in this Master thesis paper, a security protocol based on a dynamic change of pseudonyms for privacy in Vehicular Ad hoc NETworks (VANET). Our proposal ensures privacy for the driver and his vehicle whether he is transmitter or receiver of the message. By handling all possible cases of changes in vehicle behavior during traffic, we ensure a safe and secure traffic management. We built the architecture of our solution on three essential devices designed for VANET. In three steps, the anonymity is guaranteed by our Real Initial New protocol (RIN). This latest provides a high security to vehicles.

Keywords: VANET, security, privacy, anonymity, pseudonym.

CHAPITRE 1

INTRODUCTION GÉNÉRALE

Les accidents de la route tuent, chaque année près de 1,25 million de personnes et laissent environ 20 à 50 millions de blessés ou handicapés. C'est la principale cause de décès parmi les jeunes âgés de 15 à 29 ans [1]. En raison de ces statistiques, il a été constaté que les anciens feux et les panneaux de signalisation étaient incapables ou pas assez efficaces pour maintenir la sécurité routière. Si rien n'est fait, les accidents de la route deviendront la septième cause de décès avant 2030 [1].

Afin de résoudre ce genre de problèmes, les recherches se sont initiées par un système appelé Intelligent Transport Systems (ITS). Le système des technologies intelligentes pour les communications sans fil (WiFi, WiMAX, GSM et 4G) et les technologies de localisation (GPS et Galileo) assurent une bonne gestion de la circulation et minimisent les dommages causés par la route.

Une grande partie des recherches ITS est dédiée aux réseaux véhiculaires (VANET). C'est une sorte de réseau mobile utilisé pour la communication entre les véhicules. Il se compose de trois éléments principaux: le nœud (véhicule), l'unité routière (RSU) et l'autorité centrale (CA).

Le nœud représente le véhicule équipé de l'unité OBU (unité embarquée) et de l'unité d'application (AU). L'OBU est utilisé pour calculer et afficher toutes les informations nécessaires à la localisation et pour partager et échanger des données. Le RSU est composé d'un ensemble de dispositifs installés sur le bord de la route, c'est un intermédiaire entre les véhicules et l'infrastructure. Enfin, la CA représente une autorité de certification pour la communication entre les véhicules et l'infrastructure des réseaux VANET. VANET est un réseau dynamique à densité variable qui opère en milieu urbain et en autoroute.

La norme IEEE 802.11p est un système dédié aux communications à courte portée (DSRC) dans un environnement de véhicules sans fil (WAVE).

Pour assurer une communication dans les réseaux VANET, les Etats-Unis réservent un spectre entre 8,850 GHz et 5,925 GHz avec une bande passante de 75 MHz. Quant à la norme européenne ETSI ITS-G5, elle définit une norme pour les

communications véhiculaires avec 30 MHz. La norme IEEE 802.11p utilise un canal de 10 MHz et une gamme de données d'échange entre 3 et 27 Mbps.

Les trois modes de communication existant dans ce réseau véhiculaire sont:

a) La communication dans le véhicule lui-même;
b) La communication ad hoc par les deux sous-modes: Véhicule à véhicule V2V et Véhicule à Infrastructure V2I;
c) La communication dans le réseau mondial (Infrastructure to Infrastructure, I2I).

Le réseau VANET gère trois types de messages: Beacon, alerte et service. Le message Beacon est utilisé pour l'identification, la découverte et le contrôle des voisins. Les messages d'alerte sont utilisés pour la gestion du trafic routier et les messages de service qui sont destinés aux sites de localisation et de découverte.

Les applications dans VANET sont classées sous trois types:

i. Applications de la sécurité routière basées sur:
   • Eviter les collisions entre les intersections,
   • Sécurité publique (service S.O., urgence ...),
   • Extension de signal (vitesse de courbe, avertissement, avertissement de zone de travail)
   • Diagnostic et entretien des véhicules,
   • Informations provenant d'autres véhicules (mise en garde sur les conditions routières, avertissement de collision ...);
ii. Applications du confort: Divers services et informations sont proposés aux conducteurs pour améliorer la qualité des déplacements, tels que l'emplacement des stations-service, l'accès au réseau Internet, le partage des fichiers multimédias et l'échange d'informations avec d'autres conducteurs;
iii. Applications commerciales pour l'achat en ligne par des véhicules intelligents équipés de technologies de pointe.

Pour déployer des réseaux VANET afin d'offrir les applications mentionnées ci-dessus, nous devons garantir les exigences de sécurité suivantes: l'authentification, l'intégrité, la confidentialité, la disponibilité, la non-répudiation, le temps réel et la

vie privée. Cette dernière se concentre sur la protection de la vie privée de l'information personnelle et la sensibilité des véhicules contre les attaques.

Notre objectif est de proposer une solution efficace et dynamique afin de résoudre le problème de la protection de la vie privée dans le domaine de réseau véhiculaire VANET. Dans ce travail, Nous proposons un protocole qui assure l'anonymat et qui utilise un changement de pseudonymes pour protéger les informations personnelles. Cette solution garantit la confidentialité de tous les véhicules et de leurs voisins, qu'il s'agisse d'un émetteur ou d'un récepteur d'informations et quel que soit le comportement du véhicule.

Le reste de ce mémoire est organisé comme suit: Nous présenterons dans le chapitre II le réseau véhiculaire VANET et les exigences de sécurité. Dans le chapitre III, nous discuterons de l'état de l'art sur la vie privée dans les réseaux VANET. Nous présenterons par la suite dans le chapitre IV notre solution de protection de la vie privée sous forme d'un article scientifique, en montrant l'efficacité de cette solution par des simulations et analyse de sécurité dans le chapitre V. Nous terminerons par une conclusion qui représentera le chapitre VI.

CHAPITRE 2

GÉNÉRALITÉS SUR LES RÉSEAUX VÉHICULAIRES AD HOC VANET

2.1 Introduction

Les recherches dans le domaine des systèmes de transport intelligents ITS sont en plein essor. Le réseau véhiculaire VANET fait partie du système ITS et est conçu essentiellement pour réduire le nombre d'accidents mortels de la route. Le système VANET améliore les services et offre donc une solution de sécurité pour les utilisateurs routiers.

Nous consacrerons, à ce sujet, un premier chapitre se rapportant à la définition des réseaux véhiculaires VANET, à l'architecture ainsi qu'aux technologies d'accès aux réseaux véhiculaires. Nous décrirons également les modes de communication, les normes et les standards utilisés. La classification des applications, la description des caractéristiques du réseau VANET ainsi que la sécurité dans les réseaux véhiculaires seront également abordées.

2.2 Définition

Le réseau véhiculaire VANET (Vehicular Ad hoc NETwork) est l'un des types de réseaux mobiles MANET (Mobile Ad hoc NETwork), conçu spécialement pour assurer la communication entre les véhicules.

La recherche dans les réseaux véhiculaires VANET fait partie du grand domaine de recherche dans les systèmes de transport intelligents ITS **(Intelligent Transportation Systems).**

La **figure 1** montre un système de transport intelligent (ITS):

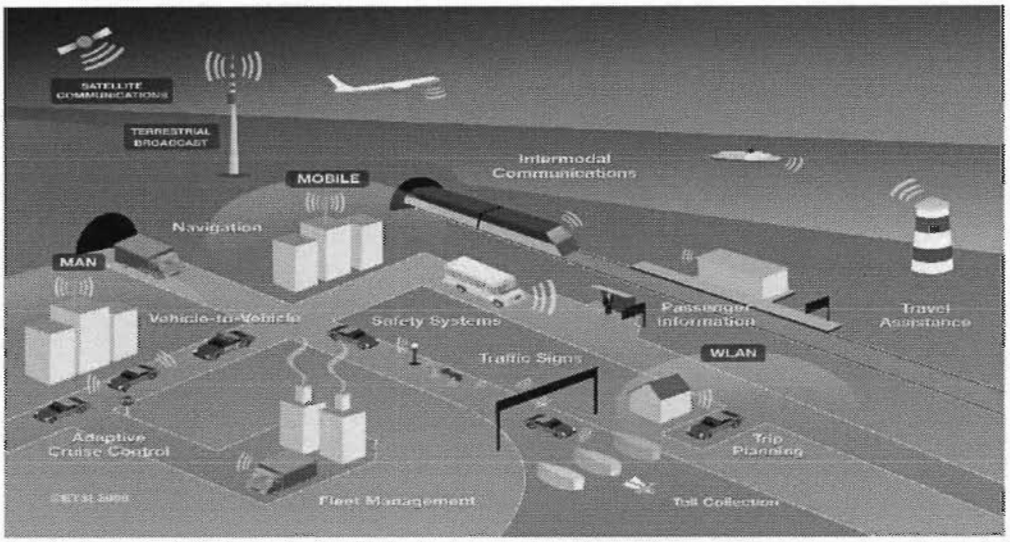

Figure 1: Système de transport intelligent ITS [2]

Tout comme les autres applications du domaine du transport intelligent ITS, la recherche sur les réseaux VANET s'intéresse au développement de nouvelles solutions afin d'améliorer la sécurité routière.

En plus de l'organisation du trafic routier, VANET propose des technologies de communication facilitant l'accès aux services routiers.

La **figure 2** montre un exemple d'un réseau véhiculaire ad hoc VANET:

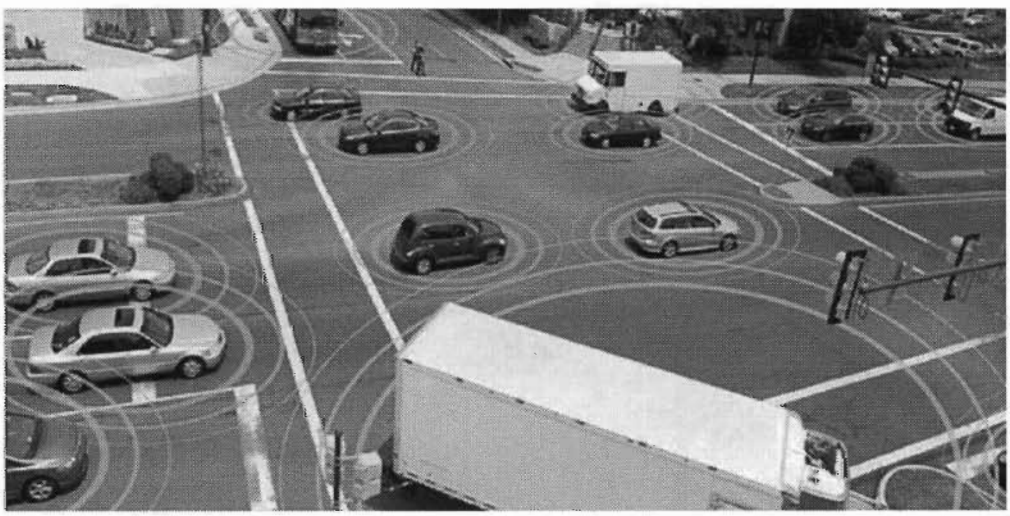

Figure 2: Exemple d'un réseau VANET [3]

2.3 Architecture VANET

Dans le domaine des réseaux ad hoc, les nœuds communiquent entre eux à l'aide des composants électroniques. Dans ce paragraphe, nous décrivons l'architecture complète d'un réseau VANET.

2.3.1 Véhicule intelligent

Le véhicule intelligent est un véhicule avec des appareils électroniques installés **(figure 3)**, permettant des communications avec les autres véhicules ou avec l'infrastructure. Il est équipé de plusieurs capteurs, de radars, d'un système de localisation, d'un équipement de communication, d'une plateforme de traitement, d'une collecte de données et d'une interface homme-machine. Ce véhicule permet d'enregistrer des paramètres et des événements importants durant la circulation, tels que la vitesse, le comportement de la conduite et autres.

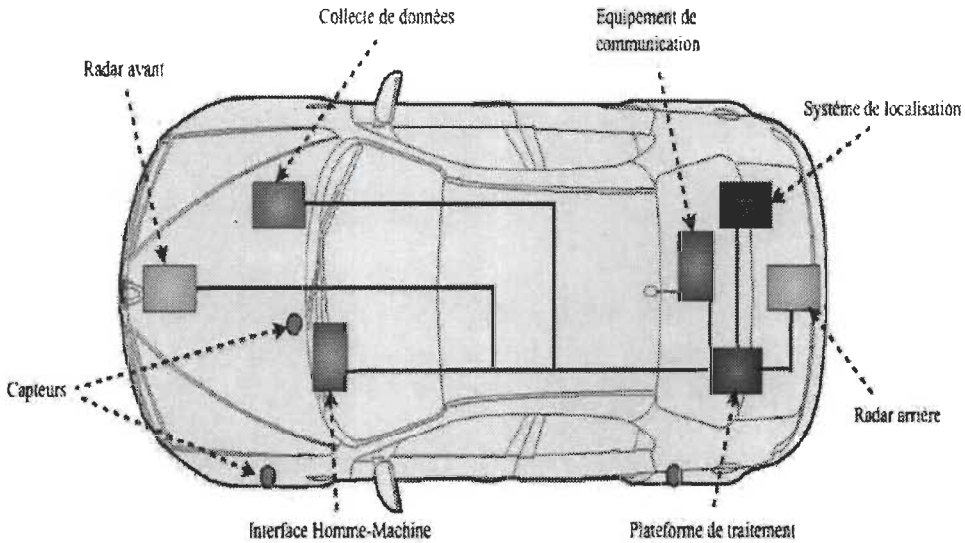

Figure 3: Les composants d'un véhicule intelligent [4]

2.3.2 Composants d'un réseau VANET

Les principaux composants nécessaires pour établir des communications dans un réseau véhiculaire VANET sont les suivants :

2.3.2.1 Nœud

Les nœuds sont les entités principales de ce type de réseau. Ce sont des véhicules intelligents avec des technologies très avancées telles que le GPS, les caméras et autres équipements. Dans la présente étude, les principaux appareils du nœud sont l'AU (Application Unit) et l'OBU (On Board Unit).

- ✓ L'AU est un dispositif électronique installé dans les véhicules pour assurer les communications avec l'autorité de confiance (CA), connecté a l'OBU afin d'exécuter des applications.
- ✓ l'OBU **(figure 4)** est un dispositif installé dans les véhicules intelligents avec un ensemble de composants logiciels pour calculer et afficher toutes les informations nécessaires de localisation, partager et échanger des données.

Figure 4 : Le dispositif OBU (On Board Unit) [5]

2.3.2.2 RSU

Les *RSUs* (Road Side Unit) **(figure 5)** sont des dispositifs installés au bord de la route jouant le role d'un point d'accès afin d'assurer les communications avec

l'infrastructure et échanger les informations relatives à l'état du trafic routier avec les utilisateurs de la route.

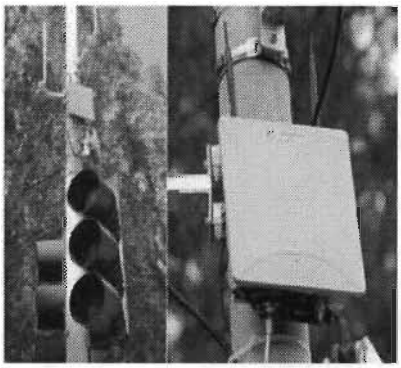

Figure 5 : Le dispositif RSU (Road Side Unit) [5]

2.3.2.3 CA

La CA (Central Authority) représente l'autorité de confiance dans le réseau véhiculaire VANET. La CA joue le rôle d'un serveur qui assure la sécurité des différents services tels que la délivrance des certificats, des clés de communication et le stockage de certaines données.

2. 3.3 Technologies d'accès sans fil VANET

Le domaine du réseau véhiculaire VANET est un réseau hybride qui utilise de nombreuses technologies d'accès sans fil. Ces diverses technologies ont pour but d'assurer la liaison entre les différentes entités de l'infrastructure.
Ci- dessous, nous citons quelques technologies d'accès sans fil :

- **Wi-Fi :** Technologie contenant un ensemble de protocoles de communication décrits par la norme IEEE 802.11, assurant la communication entre un véhicule et un autre ou par l'intermédiaire de l'infrastructure RSU. Il existe plusieurs sous-normes de la norme IEEE 802.11 liées au développement des

technologies, de l'amélioration du niveau de la fréquence d'onde radio, du taux de transfert de données et de la portée de communication. Parmi les sous-normes nous citons: IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac et 802.11ah.

- **Système cellulaire :** Technologie de communication basée sur la fréquence des systèmes cellulaires. Plusieurs normes liées aux techniques de transmission d'ondes radioélectriques dans une bande de fréquence UHF comprise entre 800 et 2600Mhz sont décrites.

  Parmi les générations de normes, nous présentons les suivantes:

  - ✓ 2G: GSM (Global System for Mobile Communication) et CDMA (Code Division Multiple Access)
  - ✓ 2.5G: GPRS (General Packet Radio Service).
  - ✓ 2.75G: EDGE (Enhanced Data Rate for GSM Evolution).
  - ✓ 3G: CDMA 2000 1x EV (Code Division Multiple Access 2000 1X Evolution) et UMTS (Universal Mobile Telecommunications System)
  - ✓ 4G: LTE (Long Term Evolution) et WiMAX (Worldwide Interoperability for Microwave Access)

- **WiMAX:** Le Worldwide Interoperability for Microwave Access ou la norme IEEE 802.16 est une technologie à multiples usages en mode de transmission haut débit dans une zone géographique étendue. Le WiMAX est utilisé dans la gestion de réseaux des systèmes de transport intelligents (ITS). Parmi les standards de réseau WiMAX nous citons: IEEE std 802.16-2001, std 802.16c-2002, std 802.16-2004, 802.16e, 802.16f et 802.16m.

- **DSRC/WAVE:** Dedicated Short Range Communications est une norme d'accès sans fil de la communication de réseau VANET dans un environnement véhiculaire. C'est un ensemble de protocoles assurant les

communications à courtes portées. Cette technologie d'accès sera détaillée dans la section **2.5** (Normes et standards).

- **Technologies d'accès sans fil combinées** : Ce type de technologie permet plusieurs services tels que les services de messages, de données et de localisation. Nous citons comme exemple de cette technologie : GSM/2G et UMTS/3G.

2.4 Modes de communication

Les véhicules peuvent communiquer les uns avec les autres directement sans intermédiaire, ou par l'intermédiaire d'un dispositif installé au bord de la route (RSU). Le transfert des informations et des données entre les véhicules s'effectue à l'aide de différents modes de communication, dont le but est d'assurer une continuité de connexion en courte durée avec le réseau ad hoc VANET sans connaître le type ou la technologie d'accès sans fil.
Dans le domaine de réseau véhiculaire VANET, les communications sont classées selon trois modes :

2.4.1 En véhicule: C'est une communication dans le véhicule lui-même sans intermédiaire. Elle s'exerce exactement entre les deux composants électroniques du véhicule l'OBU et l'AU. L'OBU communique avec l'AU pour exécuter les différentes applications et faire le traitement de données afin de fournir et d'échanger des informations nécessaires aux autres véhicules.

2.4.2 Ad hoc: Ce mode de communication s'effectue directement entre les entités voisines de réseau sans infrastructure; l'échange de données passe d'une entité à l'autre de façon directe sans intermédiaire. Il existe deux types de communication dans ce mode :

2.4.2.1 V2V (Vehicle To Vehicle): Un mode de communication s'exerçant directement entre les nœuds voisins sans infrastructure. Le véhicule équipé d'une unité électronique appelée OBU communique directement avec un autre véhicule voisin dans sa portée.

2.4.2.2 V2I (Vehicle To Infrastructure): Communication entre les nœuds à l'aide d'une unité électronique intermédiaire appelée RSU. Le nœud communique en mode ad hoc avec le RSU dans sa portée. Le RSU lui-même communique en mode ad hoc avec un autre nœud dans sa portée afin d'effectuer un échange de données.

2.4.3 Infrastructure: Communication dans le réseau véhiculaire global ou avec Internet. Ce mode de communication gère une grande bande passante d'une manière efficace et sécuritaire avec le minimum d'énergie consommée. Parmi les technologies utilisées dans ce mode de communication, nous citons les suivantes : GSM, GPRS, UMTS, HSDPA, WIMAX et 4G.

La **figure 6** présente les différents modes de communication dans le réseau véhiculaire VANET.

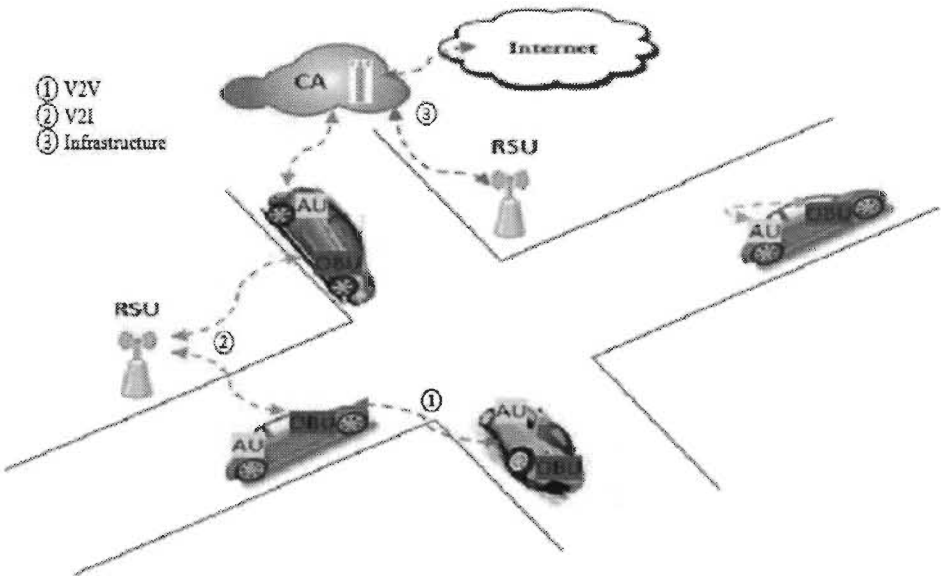

Figure 6: Modes de communication dans le réseau véhiculaire VANET

2.5 Normes et standards

On note une forte concurrence entre les Etats-Unis, l'Europe et le Japon en termes de normalisation et de création des standards dans le domaine de réseaux véhiculaires VANET. La normalisation de protocoles est un acte primordial dans l'industrie des prochaines générations de véhicules.

En effet, la grande vitesse de déplacement des véhicules, ainsi que le changement dynamique du type de communication, obligent de créer un nouveau modèle dans le système de réseau VANET pour mieux répondre aux exigences de ce domaine.

Le modèle DSRC/WAVE (Dedicated Short Range Communication/ Wireless Access in Vehicular Environments) **(figure 7)** permet un accès à la technologie sans fil dans un environnement véhiculaire.

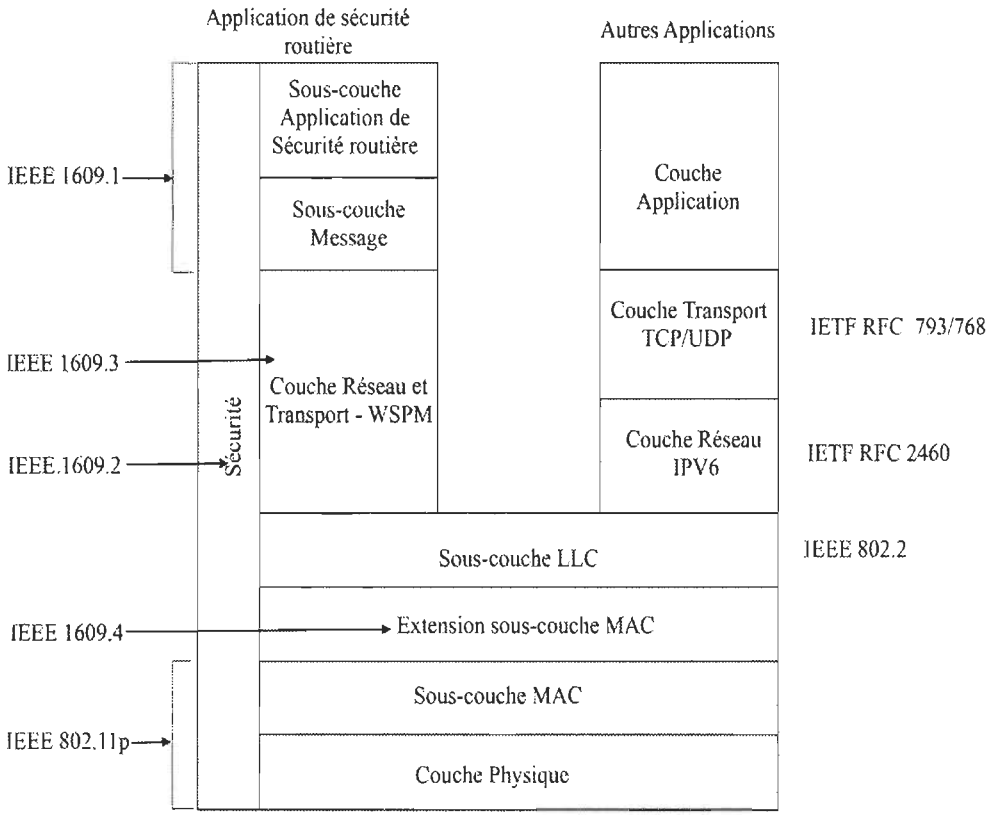

Figure 7 : Le modèle WAVE/DSRC [6]

- **La norme DSRC (Dedicated Short Range Communications):** représente un ensemble de protocoles et de normes définissant la communication à courte portée. Cette norme a été créée en 2002 par l'ASTM (American Society for Testing and Materials) spécialement pour les systèmes de transport intelligents ITS ; précisons qu'elle présente des différences notables entre les Etats-Unis, l'Europe et le Japon.

  En 1999, la Commission Fédérale des Communications (FCC) aux USA avait réservé 75 MHz du spectre électromagnétique divisé en 7 canaux dans la bande des 5.9 GHz (**figure 8**). Tandis que l'Institut Européen des normes de télécommunication (ETSI) en Europe avait réservé en 2008, 30 MHz du spectre divisé en 5 canaux dans la bande 8.9 GHz, utilisant les mêmes technologies radio avec quelques adaptations fonctionnelles (**figure 9**).

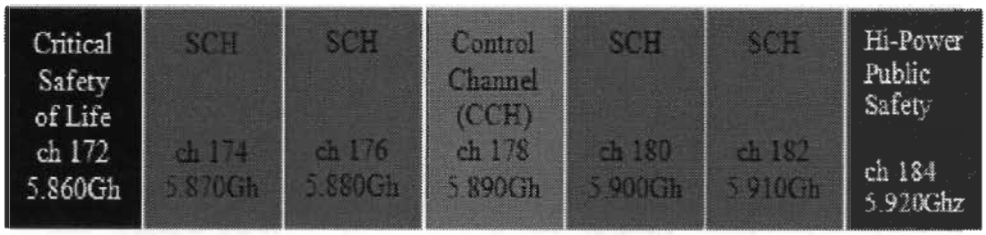

Figure 8 : DSRC aux USA (7 canaux de 10 MHz)

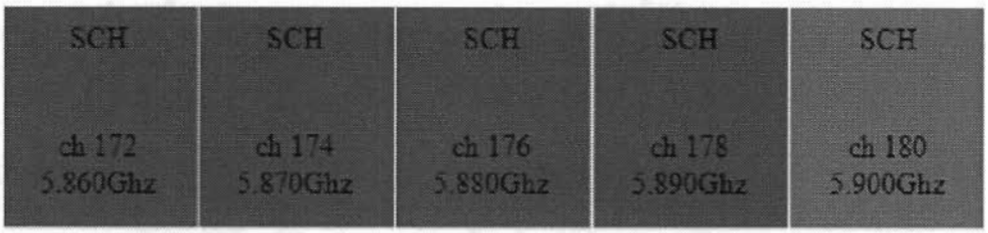

Figure 9 : DSRC en Europe (5 canaux de 10 MHz)

- **La norme WAVE (Wireless Access in Vehicular Environments):** représente un groupe de normes et de protocoles d'accès sans fil dans un environnement véhiculaire. Il s'agit d'une architecture avec un ensemble de standards, de services et d'interfaces permettant de sécuriser les différents types de communications dans le système de réseau VANET.
  L'IEEE *(*Institute of Electrical and Electronics Engineers) *définit également* le standard WAVE sous le nom **IEEE 1609**.

  a. **IEEE 1609.1:** Norme fournissant un gestionnaire de ressources précédant la communication entre les applications et les véhicules dans les réseaux VANETs. Définissant également le format de message et le mode de stockage des données.

  b. **IEEE 1609.2**: Norme définissant les services de sécurité des applications, les circonstances d'échange des messages, leur gestion et leurs formats. Le

standard IEEE 1609.2 répond aux exigences de sécurité dans le système de réseau VANET en termes de confidentialité, d'intégrité et d'authenticité.

c. **IEEE 1609.3:** Norme s'intéressant aux couches des services de transport et de réseaux, telles que l'adressage et le routage. Définissant également le WSM (Wave Short Message) et le protocole d'échange WSMP (Wave Short Message Protocol).

d. **IEEE 1609.4:** Norme définissant les opérations multi-canaux par l'exécution du mécanisme EDCA (Enhanced Distributed Channel Access) de la sous-couche MAC (Medium Access Control), en se basant sur le mécanisme CSMA/CA utilisé dans les réseaux informatiques.

e. **IEEE 802.11p :** Norme du réseau sans fil faisant partie de la famille IEEE 802.11x commercialisée sous forme Wi-Fi. Le standard IEEE 802.11p définit des caractéristiques spécifiques pour le domaine du réseau VANET ; une bande passante de 5.9 GHz assurant l'échange de données avec un débit compris entre 6 et 27 Mb/s et sur une distance de 1000m.

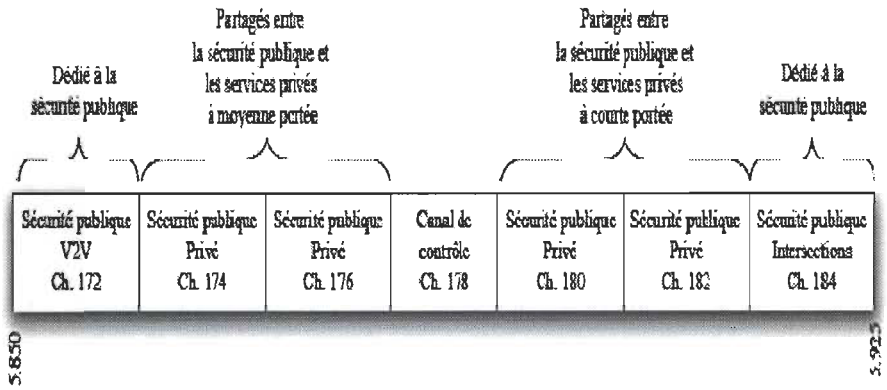

Figure 10 : Canaux du standard IEEE 802.11p [6]

f. **IEEE 802.2 :** Correspondant à la sous-couche LLC (Logical Link Control), ce protocole fournit divers types d'opérations pour les services de qualité.

2.6 Types d'application VANET

De nombreux types d'applications sont pris en charge par les systèmes VANETs. Ces dernières sont classées selon trois grandes catégories quel que soit le type de communication V2V ou V2I :

- Les applications de sécurité routière,
- Les applications de confort,
- Les applications commerciales.

2.6.1 Applications de sécurité routière

Les applications de sécurité routière incluent toutes les informations nécessaires relatives à la route ; elles ont pour objectif d'assurer la bonne gestion du trafic routier.

Nous les classons selon cinq catégories :

2.6.1.1 Évitement des collisions d'intersections

Cette catégorie des applications englobe les sous-catégories suivantes :

a- Avertissement de violer le signal du trafic
b- Avertissement de violer la signalisation d'arrêt
c- Assistant de virage à gauche
d- Assistant de mouvement de la signalisation d'arrêt
e- Avertissement de collision d'intersections
f- Avertissement de détection de fusion aveugle
g- Renseignement sur les passages d'intersection

2.6.1.2 Sécurité publique

Cette catégorie définit les applications de la sécurité publique :

a- Avertissement des véhicules d'urgence

b- Signal préemption des véhicules d'urgence

c- Services SOS

d- Avertissement de collision Poster

2.6.1.3 Extension de la signalisation

Cette catégorie définit les signalisations extensibles de la sécurité routière :

a- Signalisation dans les véhicules

b- Avertissement de vitesse de courbe

c- Structure de stationnement faible et d'alerte de ponts

d- Alerte de ponts

e- Avertissement de mauvaises façons au conducteur

f- Avertissement de zones de travail

g- Alerte AMBER dans les véhicules « Alerte médiatique, but : enfant recherché »

2.6.1.4 Diagnostic et maintenance des véhicules

Cette catégorie renseigne sur l'état du véhicule afin d'assurer la maintenance et les réparations nécessaires :

a- Avis de rappel de sécurité

b- Notification de réparation juste-à-temps

2.6.1.5 Informations provenant d'autres véhicules

Cette catégorie d'applications assure la mise à jour des informations et des états de comportement entre les véhicules :

a- Avertissement de collision

b- Alerte de l'état de la route

c- Feux de freinage d'urgence électronique (EEBL)

d- Avertissement de changement de voie

e- Avertissement sur la tache aveugle

f- Assistant d'entrées/sorties de l'autoroute

g- Activateur de la visibilité
h- Avertissement de la collision
i- Régulateur coopératif de la vitesse adaptative
j- Avertissement sur l'état de la route
k- Détection de la pré-collision
l- Avertissement de la collision autoroute/chemin de fer
m- Notification de la ligne de la route Véhicule à véhicule
n- Système coopératif d'automatisation entre le véhicule et la route

2.6.2 Applications de confort

Cette catégorie définit l'ensemble des types d'applications offrant un meilleur confort au conducteur et assurant les différents services et informations nécessaires pour l'amélioration de la qualité du voyage.

Parmi ces applications, nous citons, à titre d'exemple : les applications de la localisation des stations de service (restaurants, hôtels, stations d'essence…), les applications d'accès au réseau Internet, de partage des fichiers et des données, de streaming multimédia et des échanges d'informations avec d'autres conducteurs.

2.6.3 Applications commerciales

Les véhicules intelligents équipés de technologies avancées créent une véritable concurrence entre les constructeurs de voitures en matière de commerce et de publicité.

En effet, ce type d'applications commerciales permet de fournir aux conducteurs des services de divertissement, tels que l'accès web en vue d'effectuer des achats ou des ventes en ligne, leur donner également la disponibilité de magasiner virtuellement.

Le **tableau I** montre un exemple d'application VANET avec des informations sur le type de communication, le type de message, la fréquence d'émission, la latence et la portée.

Tableau I:

Exemple d'applications du réseau VANET [7]

Application		Information sur l'application				
		Communication	**Type de message**	**Fréquence d'émission (ms)**	**Latence (ms)**	**Autres prérequis**
1	Feux de freinage d'urgence électronique	Ad hoc V2V	Evénementiel, diffusion limitée dans le temps	100	100	Portée : 300 m Priorité haute
2	Alerte de véhicule lent	Ad hoc V2V	Diffusion périodique permanente	500	100	Priorité haute
3	Alerte de collision (intersection)	Ad hoc, infrastructure V2I, V2V	Diffusion périodique permanente	100	100	Positionnement précis Priorité haute
4	Alerte de zone dangereuse	Ad hoc, infrastructure I2V, V2V	Evénementiel, diffusion localisée limitée dans le temps	100	100	Priorité haute
5	Alerte de violation de feux tricolores	Ad hoc, infrastructure I2V	Evénementiel, diffusion limitée dans le temps	100	100	Portée : 250 m Priorité haute
6	Détection pré-accident	Ad hoc V2V	Diffusion périodique, unicast	100	50	Portée : 50 m Priorité haute/moyenne
7	Alerte de changement de voie	Ad hoc V2V	Diffusion périodique	100	100	Précision de positionnement < 2m Portée : 150 m
8	Alerte coopérative de collision	Ad hoc	Périodique,	100	100	Précision de

		V2V	diffusion événementielle, unicast			positionnement < 1m Portée : 150 m
9	Gestion d'intersection	Ad hoc, infrastructure V2I, V2V	Diffusion périodique, unicast	1000	500	Précision de positionnement < 5 m
10	Alerte d'accès limite et de déviation	Infrastructure I2V, autres réseaux de diffusion	Diffusion périodique	100	500	Priorité moyenne/basse
11	Contrôle de la vitesse de croisière	Ad hoc V2V	Diffusion unicast	500	100	Priorité moyenne
12	Télépéage	Ad hoc, infrastructure V2I, cellulaire	Diffusion périodique, unicast	1000	200	DSRC
13	Diagnostic distant	Ad hoc, infrastructure V2I, V2V, cellulaire	Unicast, diffusion, événementiel	N/A	500	Accès Internet Service disponible
14	Téléchargement de média	Infrastructure cellulaire, autres réseaux de diffusion	Unicast, diffusion, a la demande	N/A	500	Accès Internet Gestion des droits numériques
15	Téléchargement de cartes routières	Ad hoc, infrastructure cellulaire, autres réseaux de diffusion, V2I, V2V	Unicast, diffusion, a la demande	1000	500	Accès Internet Gestion des droits numériques Service disponible
16	Assistance de conduite économique	Ad hoc, infrastructure V2I, V2V, cellulaire	Unicast, diffusion, a la demande	1000	500	Accès Internet Service disponible

2.7 Caractéristiques du réseau VANET

Le réseau véhiculaire VANET fait partie du réseau mobile MANET. Il est devenu actuellement un domaine de recherche très actif et très dynamique.

Les principales caractéristiques de ce réseau sont les suivantes :

a. Environnement de déploiement

Avant le dépoilement du réseau VANET, il convient de décrire les deux environnements de communication :

1. **Urbain:** Nous tenons à préciser que dans un environnement urbain, le nombre de véhicules existants est élevé, cependant la vitesse de circulation est limitée. De ce fait, dans ce type, l'environnement de déploiement permet une très bonne connectivité entre les véhicules mais avec une très forte perturbation des ondes radio.

2. **Autoroute :** Étant caractérisé par une très grande variété de véhicules (lourds et légers) et une grande vitesse de circulation, l'environnement de déploiement autoroute nécessite la présence d'une infrastructure plus développée pour la réalisation des communications. Dans ce type d'environnement, nous avons donc besoin des RSUs pour pallier aux difficultés de communication Ad hoc.

- ✓ **Comparaison entre les deux environnements de déploiement:**

Nous présentons une comparaison entre les deux environnements de déploiement urbain et autoroute dans le **tableau II**:

Tableau II

Comparaison entre les deux environnements de déploiement
Urbain & Autoroute

Urbain	Autoroute
-Faible vitesse de circulation des véhicules -Forte perturbation des ondes radio -Faible distance entre les nœuds mobiles -Bonne connectivité entre les véhicules -Importante contrainte de délai d'échange de données -Complexité de la sécurité routière	-Grande vitesse de circulation des véhicules -Grande variété de véhicules (lourds, légers) -Faible perturbation des ondes -Difficulté de communication Ad hoc - Faible connectivité entre les véhicules -Nécessité des RSUs pour établir des communications avec l'infrastructure -Sécurité routière moins complexe.

b. Les systèmes d'accès

Les deux systèmes d'accès aux technologies des réseaux VANET sont :

1. **Système intravéhiculaire :** Permet aux nœuds de communiquer entre eux pour échanger des données en l'absence d'un intermédiaire.
2. **Système extravéhiculaire :** Permet d'échanger des données entre les entités d'une infrastructure de réseau.

c. Types de messages

Trois types de messages VANET peuvent être échangés entre les véhicules ; les messages Beacon, les messages d'alertes ou les messages de services.

1. **Beacon :** représente un message d'identification, de découverte des voisins et de contrôle. Ce type de message fournit des informations nécessaires aux véhicules voisins, telles que la vitesse et le positionnement du véhicule.

2. **Alertes :** représentent des messages de gestion de sécurité du trafic routier, tels que la signalisation de la congestion ou les alertes d'accidents.

3. **Services :** représentent des messages de localisation et de découverte des lieux de services (Stations de services, restaurants...).

d. Modes de communication

Le réseau VANET est un réseau qui change les modes de communication en permanence. Il existe deux modes de communication :

1. **Mode Ad hoc :** établissant des communications directes entre les véhicules (sans intermédiaire). Ce type de communication est désigné par l'appellation V2V (Véhicule To Véhicule).

2. **Mode Infrastructure:** établissant des communications entre les entités du réseau VANET. Ce type comporte deux modes de communication : V2I (Véhicule To Infrastructure) ou I2I (Infrastructure To Infrastructure).

e. Réseau très vaste

A la différence des autres réseaux, VANET n'est pas un réseau centralisé ou défini sur une zone géographique bien déterminée. Ce réseau change d'échelle en fonction des communications présentes entre les véhicules circulant sur les routes, grandissant ou diminuant en permanence selon la disponibilité des véhicules.

f. Topologie très dynamique

Le changement permanent des modes de communication (AD hoc, infrastructure) dans le réseau VANET, fait que ce système soit caractérisé par un très grand dynamisme.

La topologie varie en fonction du nombre de véhicules existant, de la distance entre les nœuds ainsi que de la vitesse de chacun. Le comportement de chaque véhicule dépend du comportement des véhicules voisins circulant dans la même direction ou dans le sens opposé.

g. Densité variable du réseau

La variabilité du nombre des nœuds, rend le système VANET un réseau flexible, ayant la propriété d'être fonctionnel et efficace dans tout environnement, quelle que soit la densité de véhicules.

h. Haute capacité de calcul

L'échange des données entre les nœuds nécessite un calcul efficace et plus rapide pour une meilleure détermination des cas possibles de circulation sur la route. L'ensemble des entités du réseau VANET dispose de grandes capacités énergétiques dans le but de satisfaire les différentes opérations de communications.

i. Temps réel

Les calculs et les informations échangés entre les nœuds doivent être réalisés en temps réel afin d'éviter les collisions et les accidents. Le réseau VANET assure des traitements en temps réel pour mieux gérer le comportement des véhicules vis à vis des véhicules voisins.

j. Diffusion variable

Les modèles de diffusion varient en fonction du type de communication. En effet, la diffusion peut se faire selon trois modes :

- **Diffusion Broadcast :** le véhicule assure une diffusion vers tous les véhicules voisins entrant dans sa portée.

- **Diffusion Unicast :** diffusion entre deux nœuds uniquement.

- **Diffusion Multicast** : le véhicule assure des diffusions vers un groupe de véhicules voisins dans sa portée.

k. Connectivité de courte durée

La connectivité entre les véhicules ou avec l'infrastructure est en actualisation permanente. De ce fait, le réseau VANET nécessite une connectivité de courte durée (telle que le DSRC).

l. Géolocalisation

Le réseau VANET utilise un système de positionnement par satellites pour la localisation des nœuds et des différentes stations de services sur les routes (Exemple : GPS (Global Positioning System)).

Le système de géolocalisation fournit les renseignements nécessaires pour la gestion de la circulation routière.

m. Routage

La contrainte de la mobilité dans le réseau VANET exige l'utilisation de plusieurs types de protocoles de routage. Ces derniers sont classés selon cinq catégories :

1. **Protocoles basés sur la topologie et classés en 3 types** :

   1.1 Protocoles proactifs: tels que FSR (Fisheye State Routing), OLSR (Optimized Link State Routing), DSDV (Destination-Sequenced-Distance –vector routing protocol) et TBRPF (Topology Dissemination Based on Reverse-Path Forwarding). Ces protocoles gardent les routes pendant une période déterminée.

   1.2 Protocoles réactifs: tels que AODV (Ad-Hoc on-Demand Distance-Vector Routing Protocol), DSR (Dynamic Source Routing) et RDMAR (Relative Distance Microdiscovery Ad-Hoc Routing). Ces protocoles créent les routes et les maintient tant que la source lorsqu'un nœud source demande une route.

   1.3 Protocoles hybrides : tels que ZRP (Zone Routing Protocol), TORA (Temporarily Ordered Routing Algorithm) et HARP (Home Agent Redundancy Protocol). Ces solutions utilisent des

protocoles de routage proactifs et réactifs lors de l'envoi d'informations sur le réseau.

2. **Protocoles basés sur la position**: tels que GPSR (Greedy Perimeter Stateless Routing), GYTAR (Greedy Traffic Aware Routing protocol), MIBR (Mobile Infrastructure Based VANET Routing) et VGPR (Vertex-Based Predictive Greedy Routing). Ces protocoles basent sur l'idée que la source envoie un message à l'emplacement géographique de la destination au lieu d'utiliser l'adresse réseau.

3. **Protocoles basés sur clusterings**: tels que HCB (Hierarchical Cluster Based Routing), CBLR (Cluster Based Location Routing), CBR (Cluster Based Routing) et CBDRP (Cluster-Based Directional Routing Protocol). Ces protocoles gèrent le réseau dans une hiérarchie de groupes selon des techniques spécifiées.

4. **Protocoles basés sur l'infrastructure** : tels que SADV (Static-Node Assisted Adaptive Routing Protocol) et RAR (Roadside-Aided Routing). Ces protocoles exploitent les caractéristiques techniques des réseaux véhiculaires. Les protocoles SADV et RAR associent un véhicule à plusieurs unités routières en fonction des contraintes routiers.

5. **Protocoles Geocast** : tels que ROVER (Robust Vehicular Routing) et DTSG (Dynamic Time-Stable Geocast Routing) qui utilisent des informations sur la position des nœuds.

2.8 La sécurité dans les réseaux VANET

Des attaques et des activités malveillantes sur le réseau véhiculaire peuvent falsifier les données échangées entre les véhicules eux-mêmes ou avec l'infrastructure. Compte tenu de l'importance de ces informations, des mesures de sécurité doivent être mises en œuvre afin d'assurer une meilleure protection des informations et du trafic routier.

a. Défis et contraintes des réseaux VANET

La sécurité dans le réseau VANET se confronte à un certain nombre de défis et de contraintes :

- ✓ Bande passante limitée à 5.9 GHz
- ✓ Courte portée (de 1000 m de diamètre en théorie et 300 m en pratique)
- ✓ Grande mobilité des nœuds
- ✓ Besoins de sécurité élevés (le cas de l'ensemble des réseaux sans fil)
- ✓ Temps d'échange des données et durée de communication entre les nœuds courts.
- ✓ Dynamisme élevé de l'échelle de réseau
- ✓ Contrainte de connectivité permanente
- ✓ Mécanismes de routage basés sur plusieurs critères
- ✓ Taux de perte de données important
- ✓ Contrainte de consommation d'énergie
- ✓ Interférences entre les ondes.

b. Les exigences de sécurité

Pour un déploiement sécurisé du réseau VANET, des exigences doivent être assurées : l'authentification, l'intégrité, la confidentialité, la disponibilité, la non-répudiation, le temps réel, l'intimité et la cohérence.

- ✓ **L'authentification :** établir la liaison entre l'identificateur de chaque entité et son message diffusé sur le réseau.

- ✓ **L'intégrité :** Assurer la stabilité du message entre l'entité source et l'entité destinataire durant le transfert.

- ✓ **La confidentialité :** assurer la protection des données contre les attaques. L'accès au réseau véhiculaire n'est autorisé que pour les membres authentifiés.

- ✓ **La disponibilité :** Garantir la disponibilité et la continuité des services d'accès au réseau avec l'infrastructure ou l'envoi des messages vers les entités du réseau.

- ✓ **La non-répudiation :** Déterminer et identifier l'émetteur des messages pour garantir l'unicité d'envoi dans toutes les communications.

- ✓ **Temps réel :** Garantir l'envoi et la réception des messages dans un délai très court pour gérer la rapidité de changement de comportement des voisins.

- ✓ **L'intimité :** Protéger les informations personnelles des conducteurs ou des véhicules lors de l'envoi ou de la réception des messages en vue de garder la vie privée durant les communications.

- ✓ **Cohérence :** Le contrôle des entités et des données transférées est d'une grande importance pour l'exploitation des connectivités entre les nœuds.

c. Les attaques

La protection du réseau véhiculaire contre les attaques et les activités malveillantes est une exigence primordiale afin d'assurer la disponibilité des services avant de passer au déploiement. Nous traitons ci-dessous les deux principaux types d'attaques dans le domaine des réseaux véhiculaires.

1. Attaques basiques

Les attaques basiques sont des attaques classiques. Nous prenons comme exemple :

- ✓ **Fausse information :** nommée aussi BOGUS INFO, signifie qu'un attaquant parmi les nœuds diffuse une fausse information pour les véhicules voisins.

- ✓ **Falsification des informations :** c'est une attaque qui détériore la vie privée par vol de l'identité d'un nœud.

- ✓ **Divulgation d'ID :** Ce type d'attaque diffuse une fausse information pour pouvoir accéder aux entités du réseau et voler leurs identités.

- ✓ **DoS (Déni of Service) :** Ce type d'attaque empêche les autres nœuds d'accéder aux ressources du réseau.

- ✓ **Masquage :** Cette attaque supprime un ou plusieurs bits sur les paquets transférés du réseau.

- ✓ **Retard délibéré des paquets :** nommée aussi Forced delay. Ce type d'attaque retarde la réception des données par le destinataire diminuant ainsi la qualité de services.

2. Attaques sophistiquées

Les attaques sophistiquées sont des attaques plus avancées. Nous citons les exemples suivants :

- ✓ **Véhicule caché :** Ce type d'attaque cache l'existence de véhicules, provoquant ainsi une perturbation dans les informations échangées sur le trafic routier.

- ✓ **Tunnel :** Ce type d'attaque fonctionne par la création d'un tunnel entre les nœuds empêchant la connectivité et arrêtant l'échange d'informations.

- ✓ **Trou de ver :** Nommé aussi wormhole, c'est un type d'attaque plus général et plus large que l'attaque par tunnel, où l'attaquant crée plusieurs tunnels entre les nœuds.

- ✓ **Sybil :** Dans ce type d'attaque, l'attaquant vole et exploite les identités de plusieurs nœuds sur le réseau.

- ✓ **Brouillage :** Nommé aussi jamming, c'est une attaque plus générale que l'attaque DoS, fonctionnant par l'interférence des signaux radios.

- ✓ **Trou noir :** nommé aussi blackhole. Dans ce type d'attaque, l'attaquant modifie le routage pour indiquer la meilleure métrique et ne renvoie pas les messages qu'il reçoit.

- ✓ **Hello flood :** Attaque DoS fonctionnant par l'interférence des signaux radios de longue portée.

d. Les attaquants

Dans le domaine du réseau véhiculaire VANET, les attaquants sont classés en fonction de la zone de fonctionnement, du degré de nuisance au réseau et des conséquences de l'attaque. Nous pouvons les classer comme suit :

1. **Interne vs Externe :** Un attaquant interne fonctionne comme un membre de réseau VANET possédant des privilèges et disposant d'une clé publique certifiée par l'autorité de confiance, difficile de le détecter ou de l'isoler.
   A la différence de l'attaquant interne, l'attaquant externe ne possède pas une clé publique certifiée, ce qui fait de lui un membre limité de réseau.

2. **Malveillant vs Rationnel :** Un attaquant malveillant a pour but de nuire aux mécanismes du réseau, provoquant ainsi son dysfonctionnement.
   A la différence de ce dernier, l'attaquant rationnel est à la recherche d'un profil personnel sans porter nuisance au fonctionnement du réseau.

3. **Actif vs Passif :** Un attaquant actif est un attaquant qui génère des paquets, modifie ou falsifie des informations. L'attaquant passif n'interagit pas sur les informations échangées entre les nœuds. Il se contente d'écouter et de copier les paquets.

e. Caractéristiques d'attaques

L'effet des attaques correspond à la quantité et au degré de dommage. Trois conséquences possibles d'attaques sont dénombrées :

1. **Attaque détectée et corrigée** : les nœuds malveillants sont capables de cibler la corruption avec de fausses données, les victimes se rendent compte de l'incertitude des données qu'ils ont reçues et corrigent cette fausse information afin de garantir le bon fonctionnement du réseau.

2. **Attaque détectée et non corrigée** : Les victimes sont en mesure de détecter l'attaque, cependant ils sont incapables de la corriger. L'existence d'un malveillant dans le réseau empêche donc la communication sécuritaire, ce qui aboutit à son dysfonctionnement.

3. **Attaque non détectée et non corrigée** : C'est le cas d'attaque le plus difficile. Il se produit lorsque les victimes sont incapables de détecter l'attaque. Une attaque non détectée et non corrigée crée une situation plus complexe à résoudre.

2.9 Conclusion

Aujourd'hui et compte tenu de l'augmentation et du développement du trafic routier, la création d'un système de transport intelligent devient une nécessité primordiale afin d'assurer une circulation en toute sécurité.

L'application des résultats de recherche du domaine de réseau véhiculaire VANET dans le système de transport intelligent permet de minimiser les accidents, de contrôler le trafic routier et d'améliorer les conditions de conduite. Le nombre élevé

d'informations échangées entre les véhicules expose le réseau à plusieurs types d'attaques. L'adaptation des systèmes de mesure de sécurité permet de pallier à ce problème assurant ainsi une grande efficacité et productivité dans le domaine de la nouvelle génération des véhicules.

Dans le chapitre suivant, nous présentons quelques travaux de littératures liés à la gestion de la protection de la vie privée dans les réseaux véhiculaires VANET.

CHAPITRE 3

REVUE DE LA LITTÉRATURE

3.1 Introduction

Le système de transport intelligent (ITS) comporte plusieurs volets de recherche qui ont pour objectifs de développer et de mieux gérer les moyens de transport.
Au cours de ces dernières années, de nombreux chercheurs se sont intéressés au domaine des réseaux véhiculaires VANET. Parmi les travaux proposés, le sous-domaine de sécurité dans les réseaux VANET occupe une place considérable. En effet, l'authentification, l'intégrité, la confidentialité, la non-répudiation, la disponibilité, le contrôle d'accès, le temps réel et la protection de la vie la privée sont des profils requis. Le but de ce mémoire est l'étude de la gestion de la vie privée dans les réseaux VANET.

La protection de la vie privée repose sur la mise en place des outils techniques dont le but est d'empêcher l'identification des véhicules émetteurs ou récepteurs et de protéger les informations et les données personnelles des conducteurs et des véhicules.

Dans le présent chapitre, nous présenterons un ensemble de travaux de recherche traitant la vie privée dans le réseau véhiculaire VANET, en étudiant les mécanismes proposés. Les solutions seront exploitées en vue de proposer une solution complète et efficace.

3.2. Protection de la vie privée dans les réseaux véhiculaires VANET

En raison du développement du trafic routier, l'amélioration des systèmes de sécurité est de plus en plus nécessaires.
De nombreux travaux ont mis l'accent sur les réseaux véhiculaires VANET afin d'assurer la sécurité et la protection de la vie privée des nœuds.

Dans [8], les auteurs **Giorgio Calandrielloy, Panos Papadimitratosz, Jean-Pierre Hubauxz** et **Antonio Lioy** proposent un changement périodique de pseudonymes. Ces pseudonymes correspondent à des clés publiques certifiées par l'autorité de confiance CA et à des clés privées caractéristiques de chaque nœud. La durée de vie de chaque pseudonyme est définie au niveau de la CA. Quelque soit le nombre de communications du nœud avec les noeuds voisins, ce dernier maintient son identité jusqu'à l'écoulement du temps de changement. Le réseau VANET est un réseau très dynamique où le nombre de communications de courte durée est très élevé. Cependant, ces auteurs ne traitent pas un scénario dynamique où le changement de pseudonyme correspond à l'authentification des nœuds.

Les auteurs **Hesiri Weerasinghe, Huirong Fu** et **Supeng Leng** dans [9] proposent un protocole d'accès aux services anonymes en ligne (AOSA: Anonymous Online Service Access). Le protocole proposé préserve la confidentialité des emplacements dans les communications véhiculaires. Cette proposition amélior ainsi la confidentialité des sites du réseau VANET, cependant elle ne préserve pas toute la vie privée. La mise en disponibilité et l'autorisation des services sans identité rend la solution proposée incontrôlable et plus difficile à sécuriser.

Dans [10], **Dijiang Huang, Satyajayant Misra, Mayank Verma** et **Guoliang Xue** avaient proposé un protocole de protection de la vie privée nommé pseudonyme d'authentification basé sur la confidentialité conditionnelle (PACP: Pseudonymous Authentication-Based Conditional Privacy) en utilisant un système de jeton. La solution définit un système de billetterie pour communiquer avec l'infrastructure (RSU) et l'obtention d'un jeton permet la mise en fonction des communications entre le véhicule et son voisinage.

Bien que ces auteurs se soient basés sur le protocole de cryptage et de décryptage, leurs travaux n'avaient pas traité les possibilités de changement du comportement du véhicule et des véhicules voisins dans le même cycle avant l'obtention d'un nouveau jeton. D'autre part, la solution proposée est limitée par l'existence d'une RSU, ce qui

rend les communications par ce système de billetterie inaccessibles dans un environnement urbain caractérisé par un faible nombre de RSUs.

Les auteurs **Julien Freudiger, Mohammad Hossein Manshaei, Jean-Yves Le Boudec** et **Jean-Pierre Hubaux** dans [11] proposent une stratégie statique pour la protection de la vie privée en utilisant un modèle de changement de pseudonymes à durée de vie déterminée. Cependant, la fixation de la durée pour effectuer un changement de pseudonyme a pour inconvénient de minimiser le degré de protection contre les attaques et de créer de nombreux problèmes tels que l'interception des communications, l'usurpation d'identité et même la perturbation du trafic routier. D'autre part, ces auteurs ignorent le cas où le comportement d'un véhicule change en permanence durant la circulation.

Dans [12], les auteurs **Mostafa Dikmak, Zahraa Sabra, Ayman Kayssi** et **Ali Chehab** présentent un modèle conditionnel de préservation de la confidentialité utilisant un cryptosystème basé sur l'ID, optimisé essentiellement pour les réseaux véhiculaires ad-hoc (VANET). Ces auteurs enrichissent le processus de mise à jour des pseudonymes par des heuristiques afin d'assurer leur passage à différents moments et augmenter le degré de l'anonymat. Cependant, et contrairement aux principes du réseau véhiculaire VANET qui est un domaine d'application, ce travail a l'inconvénient de présenter une solution théorique sans montrer une efficacité pratique.

Dans [13], **Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang** et **Xuemin (Sherman) Shen** proposent une stratégie efficace pour le changement de pseudonymes dans des lieux spécifiés appelés les spots sociaux (PCS: Pseudonym Changing at Social Spots). Ces auteurs visent la confidentialité des emplacements dans un réseau vaste et dynamique. Pour cela, ils ont développé deux modèles analytiques définis en fonction de l'analyse de l'anonymat (ASS).
Dans les réseaux VANETs, le changement de l'état de la route et du comportement d'un véhicule se fait dans un lieu indéfini et à n'importe quel moment durant la circulation ; en outre, les communications sont de courte durée, même avec une

vitesse élevée des véhicules. En conséquence, l'état de la route et de la circulation tendent à changer dès le changement du pseudonyme mis en œuvre.

Dans [14], **Yuanyuan Pan** et **Jianqing Li** proposent un modèle de changement de pseudonymes CPC (Cooperative Pseudonyme Change) entre les voisins pour assurer l'anonymat. Le modèle d'analyse approximative proposé est basé sur certains paramètres tels que le trafic et la densité des nœuds sur la route. Ces paramètres ont une influence sur la performance du système de gestion de l'anonymat.

La solution proposée par ces auteurs étudie un seul cas de distribution des nœuds répartis de façon uniforme sur la route. A la différence des caractéristiques du réseau VANET qui est un réseau dynamique à densité extensible où le comportement des véhicules change en permanence, la distribution des nœuds de façon uniforme dans ce modèle élimine les autres cas possibles, et fait que cette stratégie proposée est plus proche de la théorie que de la pratique.

Les auteurs **Xinyi Wang, Zheng Huang, Qiaoyan Wen** et **Hua Zhang** dans [15] proposent un lot anonyme des clés publiques auto-certifiées distribuées entre le fournisseur de service (SP) et les véhicules. Le système proposé est paramétré par l'autorité de confiance (TA). Dans ce modèle, les auteurs proposent une solution d'offre de services pour une durée de vie bien déterminée de pseudonymes. Les outils de la gestion de la vie privée et les mécanismes de changement de pseudonymes sont opérationnels selon des critères de fonctionnement mis par ces auteurs.

Ce modèle de protection de la vie privée a pour inconvénient d'être limité par des conditions, et de ne pas assurer la sécurité contre certains types d'attaques.

Dans [16], **Yeong-Sheng Chen, Tang-Te Lo, Chiu-Hua Lee** et **Ai-Chun Pang** présentent un système de changement de pseudonymes basé sur trois critères : l'âge de pseudonyme, la direction de déplacement du véhicule et sa vitesse. Ces auteurs proposent quatre mécanismes : AS, AD, SD et ADS en fonction de la combinaison des trois critères précédemment cités. Les notations de ces quatre mécanismes sont:

1) A (âge): la durée de vie de pseudonyme, 2) S (Speed): la vitesse du véhicule, 3) D (direction): la direction de déplacement du véhicule.

La solution proposée par ces auteurs a l'inconvénient d'être applicable en milieu urbain uniquement et ne traite, en aucun cas, la protection de la vie privée dans un environnement autoroute. Ces auteurs étudient donc le comportement des véhicules dans un seul cas.

Sam Mathews M et **Bevish Jinila Y** dans [17] proposent un modèle de changement de pseudonymes PCP (Pseudonym Changing at Proper Location) dans des lieux (places sociales) précis et bien déterminés, caractérisés et conditionnés par la présence du plus grand nombre de nœuds groupés temporairement. Cependant, ces places sociales, comme les intersections ou les stations de services, sont limitées.
En effet, si les nœuds ne passent pas par ce type de lieux, ils ne changent pas de pseudonymes et gardent leurs anciens pseudonymes qui resteront valides jusqu'au croisement d'une place sociale, sinon ils seront directement exclus par ce système. La solution proposée par ces auteurs est une stratégie limitée par l'existence des places sociales.

Dans [18], **Adetundji Adigun**, **Boucif Amar Bensaber** et **Ismail Biskri** proposent un changement périodique de pseudonymes selon deux approches : la première se base sur l'infrastructure où le véhicule demande périodiquement son nouveau pseudonyme de l'autorité centrale (CA). La seconde approche repose sur le véhicule lui-même qui change périodiquement son pseudonyme sans l'intermédiaire de l'infrastructure. Bien que le changement de comportement des véhicules soit périodique, ces auteurs conditionnent le système de la gestion de l'anonymat par la vitesse des véhicules, l'existence des voisins et autres limitations dans un domaine dynamique.

Dans [19], **Abdelwahab Boualouache** et **Samira Moussaoui** proposent une stratégie de changement de pseudonymes appelée S2SI (Silence & Swap at Signalized Intersection). Cette stratégie englobe trois règles :

1) Protocole SMs (Mixe Zones) pour la création des zones de silence au niveau des intersections signalées, 2) Protocole permettant l'échange des pseudonymes entre les véhicules par l'intermédiaire des RSUs et enfin 3) Stratégie de protection de l'anonymat contre les attaques. Le modèle proposé est limité par l'existence des RSUs et des intersections signalées; en l'absence de ces deux facteurs, cette stratégie devient alors inapplicable. Bien que le nombre de véhicules dans l'environnement urbain soit élevé, la solution proposée par ces auteurs exige l'existence des RSUs comme condition d'application pour la protection de la vie privée.

Wang Ying et **Yang Shiyong** dans [20] proposent un mécanisme basé sur un système de cryptographie et un régime de changement de pseudonyme (PSC: Pseudonyms Synchronously Change). Le travail réalisé par ces auteurs est un travail théorique n'ayant pas prouvé l'efficacité de la solution proposée par des simulations pratiques.

Le réseau véhiculaire VANET étant un domaine d'application de réseau mobile, la gestion de l'anonymat ne peut en aucun cas être assurée par un régime théorique non prouvé. L'efficacité d'application des résultats de recherche dans le réseau VANET est d'une importance cruciale.

Dans [21], **Chang-Ji Wang, Dong-Yuan Shi** et **Xi-Lei Xu** proposent deux systèmes afin d'assurer la protection de la vie privée des véhicules : 1) un système crypto système à base de pseudonymes avec une autorité de confiance et 2) un système d'accès aux données basé sur la technologie de mise en cache coopérative. La solution proposée permet le partage des données mises en cache entre multiples véhicules et sépare l'identité et les données du même véhicule. La mise en cache augmente les risques contre les attaques. Celles-ci empêchent de ne pas garantir la protection de la vie privée et la gestion de l'anonymat.

Dans [22], **Song Guo, Deze Zeng** et **Yang Xiang** proposent un protocole léger LPP (Lightweight Privacy-Preserving) basé sur deux aspects : la signature caméléon (langage graphique de programmation fonctionnelle) et l'algorithme de signature numérique (mécanisme permettant de garantir l'intégrité). Les simulations montrent

les avantages de ce travail réalisé en plusieurs variantes ECPP (Elliptic Curve), Bi-LPP (bilinear pairing based LPP) et EC-LPP (EC based LPP). Les auteurs proposent une clé publique fixe pour chaque véhicule. En effet, les auteurs ne proposent pas un changement de pseudonymes périodique ou dynamique. Le non-changement de pseudonymes cause une augmentation des attaques et facilite le suivi de véhicules (tracking).

Kahina Moghraoui Aoudjit et **Boucif Amar Bensaber** dans [23] proposent un changement de pseudonymes par deux approches : la première est basée sur l'existence des voisins de confiance tandis que la deuxième est basée sur le changement périodique de pseudonymes. Les auteurs proposent une solution de communication directe entre les voisins de confiance seulement sans l'intermédiaire des entités de l'infrastructure.

Le travail proposé est une solution partielle pour garantir la vie privée. La deuxième approche de ce travail propose une solution statique par un changement périodique de pseudonymes. Cette dernière ne prend pas en considération les différents cas de changement de comportement des voisins. Le domaine du réseau VANET est un domaine dynamique et flexible, la solution proposée par les auteurs reste donc une solution limitée.

Dans [24], les auteurs **Amit Kumar Tyagi** et **N. Sreenath** traitent la notion de protection de la vie privée dans le domaine du réseau véhiculaire VANET par plusieurs techniques. Les auteurs proposent des mécanismes et des outils contre les attaques comme le cloaking (k-anonymat, p-sensibilité, la localisation spatiale cloaking et cloaking spatio-temporelle). Le cloaking est une technique pour optimiser la visibilité dans les moteurs de recherche. Ces auteurs proposent des fonctionnalités pour assurer la protection de la vie privée. Les auteurs proposent aussi d'autres travaux à faire au futur pour réaliser la notion de l'anonymat. En effet, la solution proposée est une solution incomplète.

Dong Wang, Deshu Li, Xiaohong Li et **Zhu Xiao** dans [25] proposent une application de changement de pseudonymes en fonction de la situation des véhicules LBS (Location Based Services). La solution proposée détermine le lieu de changement de pseudonymes et le temps. Les auteurs traitent un seul cas où les véhicules ne circulent pas et l'existence de place sociale pour effectuer le changement de pseudonymes. Cette proposition est une solution conditionnée par deux facteurs : le lieu et le temps. Cependant, le domaine du transport intelligent et exactement le sous-domaine des réseaux véhiculaires VANET, dépend fortement de ces deux facteurs de lieu et de temps. Le réseau VANET est un réseau dynamique. Les véhicules changent leur comportement à n'importe quel moment et à n'importe quel lieu.

3.3 Conclusion

Les nouvelles technologies et le développement des réseaux véhiculaires exigent un nouveau système de transport intelligent. La protection de la vie privée dans les réseaux véhiculaires VANET est une exigence de la sécurité. Le fonctionnement des réseaux VANET en toute sécurité est réalisé par des solutions de recherche afin d'assurer la bonne gestion du trafic routier. Beaucoup de chercheurs traitent le sujet de la vie privée en proposant des solutions basées sur des mécanismes, des outils ou des protocoles. La réalisation du respect de la vie privée par la gestion de l'anonymat est un moyen de ne pas être identifiable dans le réseau. Les travaux réalisés dans ce sujet de recherche sont des solutions incomplètes ou non applicables dans un milieu dynamique et extensible. Les travaux proposés par les chercheurs dans ce présent chapitre sont des solutions statiques, partielles, théoriques, incomplètes ou conditionnelles.

Notre travail est une solution complète et applicable qui traite tous les cas possibles de changement de comportement du véhicule, partout, à tout moment et à n'importe quel environnement d'application. Les informations personnelles des véhicules et des conducteurs sont réservées. Que le véhicule soit émetteur ou récepteur, les communications entre les entités du réseau sont confidentielles.

Le prochain chapitre fera l'objet de notre travail qui sera présenté sous-forme d'un article scientifique. Ce dernier, traite la notion de la vie privée dans le réseau véhiculaire VANET. Nous proposons un protocole appelé RIN (Real Initial New) qui assure la notion de la vie privée en toute sécurité et satisfait les exigences du réseau véhiculaire VANET.

CHAPITRE 4

ARTICLE SCIENTIFIQUE

An Efficient and Dynamic Pseudonyms Change System for Privacy in VANET

Soumis, accepté et presenté à la conférence PEDISWESA 2017, 9th IEEE International Workshop on Performance Evaluation of Communications in Distributed Systems and Web Based Service Architectures.

Date: 03 juillet 2017.
Lieu: Heraklion Crete Greece.
Numéro de papier: 1570352626.

An Efficient and Dynamic Pseudonyms Change System for Privacy in VANET

Walid Bouksani
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivières
Trois-Rivières, QC, Canada
Walid.Bouksani@uqtr.ca

Boucif Amar Bensaber
Department of Mathematics and Computer Science
University of Quebec at Trois-Rivières
Trois-Rivières, QC, Canada
Boucif.Amar.Bensaber@uqtr.ca

Abstract— **We propose in this paper a security protocol based on a dynamic change of pseudonyms for privacy in Vehicular Ad hoc NETworks (VANET). Our proposal ensures privacy for the driver and his vehicle whether he is transmitter or receiver of the message. By handling all possible cases of changes in vehicle behavior during traffic, we ensure a safe and secure traffic management. We built the architecture of our solution on three essential devices designed for VANET. In three steps, the anonymity is guaranteed by our Real Initial New protocol (RIN). This latest provides a high security to vehicles.**

Keywords— VANET, security, privacy, anonymity, pseudonym.

I. INTRODUCTION

Each year, road accidents kill nearly 1.25 million of people and leave 20 to 50 million with injured or disabilities, according to the World Health Organization (WHO) [1]. It is the leading cause of death among young people aged between 15 and 29. Due to these statistics, it was found that old signal lights and traffic signs were unable or not effective enough to maintain the traffic safety. If nothing is done, road accidents will become the seventh leading cause of death by 2030 [1].

In order to solve these kind of problems, researches initiated Intelligent Transport Systems (ITS). A large part of ITS researches is dedicated to Vehicular Ad hoc NETworks (VANET). It's a kind of mobile network used for the communication between vehicles. It is composed of three main components: Node (vehicle), Road Side Unit (RSU) and Central authority (CA). The Node represents the vehicle that is equipped with the OBU (On-Board Unit) device and the AU (Application Unit). The OBU is used to calculate and display all information necessary for localization and to share and exchange data. The RSU is composed of a set of devices installed on the roadside. It is an intermediary between vehicles and the infrastructure. In addition, it is a communication tool in less vehicle environments. Finally, the CA: represents a trusted authority for communication between vehicles and infrastructure in VANET.

IEEE 802.11p is a system for Dedicated Short-Range Communications (DSRC) [2] in a wireless vehicular environment (WAVE).

To deploy VANET networks in order to offer applications mentioned above, we must ensure the following requirements of security: authentication, integrity, confidentiality, availability, non-repudiation, real time and privacy. The last one focuses on protecting the private life, personal and sensitive information of the cars against attacks.

In this work, we propose a protocol that ensures anonymity. It uses a pseudonyms change of the nodes to protect personal information. This solution guaranteed privacy for all vehicles and their neighbors, whether it was a transmitter or a receiver of information regardless the behavior of the vehicle.

The remainder of this paper is organized as follows. In section II, we discuss the state of art on privacy in VANET. In section III, we explain our model. In section IV, we present a security analysis, simulations and discussion and finally we conclude in section V.

II. STATE OF THE ART

The requirements increase with the rise of sophisticated attacks. We discuss in this section some recent works that have been proposed for VANET in order to ensure the security of the drivers' private life.

In [3], the authors proposed a periodical change of pseudonyms, by using public and private keys that have been certified by a trusted authority (TA). However, this scenario is not dynamic because of its dependence to the TA. The authors in [4] proposed a pseudonym change model by a fixed and determined lifetime, without addressing the case or the behavior of a vehicle that changes all the time during circulation. In [5], the authors proposed an effective pseudonym changing at social spots (PCS) strategy for location privacy in VANET. The authors have developed two analytical models according to the anonymity analysis (SSA). Therefore, the problem is that, when a vehicle found a place to change its pseudonym, the network topology has already changed. Another study on the behavior of vehicles was done in a single case in [6]. The strategy is called "Pseudonym Changing at Proper Location (PCP) for pseudonym changing". Social spots precise the number of nodes grouped temporarily. Indeed, if the node does not pass through this place, it cannot change its pseudonym and it is directly deny by the system.

As has been noted, no proposed works, system models or strategies offer an effective solution for the problems of

privacy in vehicular ad hoc networks. They propose only partial solutions.

In this work, we propose a protocol that treats all possible cases (any time, anywhere, any speed, any direction, any environment, any traffic density, any neighbors and any change of vehicle's behavior) and ensures vehicles' privacy.

III. SYSTEM MODEL

In this section, we present our model, which aimed to ensure the privacy of vehicles and their confidentiality. We called this solution **RIN** (Real Initial New).

Our model is based on three main entities: Trusted Authority, Road Side Unit and On Board Unit. Each one is responsible for issuing its own pseudonym.

A. RIN protocol description:

We ensure privacy by the pseudonym change strategy. This is done independently of the device type or the time of communication. To change pseudonym, our protocol is based on three main: 1) Trusted Authority (TA) generates a real pseudonym called "Rpseud"; 2) Road Side Unit (RSU) generates an initial pseudonym called "Ipseud"; and 3) On-Board Unit (OBU) generates a new pseudonym called "Npseud".

The different phases of RIN model are described in figure1.

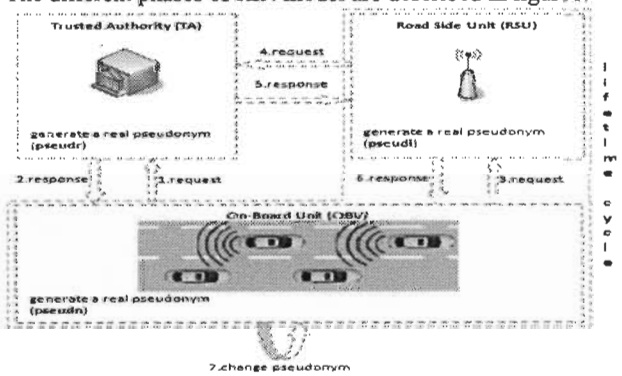

Fig.1. Description of RIN protocol

At the start of the vehicle, the node requests a real pseudonym from a trusted authority. This later sends the real pseudonym to the node. The vehicle does not start the communication before its first communication with Road Side Unit (RSU). In this step, the node asks a Road Side Unit for its initial pseudonym. After verification and validation between the RSU and the trusted authority, the RSU sends the initial pseudonym to the node. In the third step, at each discovery process between nodes, a node checks the confidentiality of its neighbours. After validation, the node changes its new pseudonym. When a node discovers another RSU, the life of its pseudonym is over and the cycle starts again.

B. Main steps:

In the next section, we present the different steps of our solution. Notations used in our model are presented below in table 1:

Table. I: Notations used in the proposed model

Notation	Description
RIN	Real Initial New
Rpseud	Real pseudonym
Ipseud	Initial pseudonym
Npseud	New pseudonym
RpseudCopy	Copy of real pseudonym
TA	Trusted authority
RSU	Road side unit
OBU	On-board unit
λ	Average number of past vehicles in range
k	Number of initial pseudonyms for period time [0,T]
T	Time reset for RSU
P	Probability
t	Time to generate a pseudonym
F	Function of Exponential distribution
Z	New neighbour
μ	Average number of change pseudonyms
NpseudTTL (Δt)	Life time of the new pseudonym
N	Node (vehicle)
D	Difference of speed between two nodes
E	Exponential distribution
R	Range of the vehicle
C	Poisson process
TN	Trust node
NTN	No trust node
trust_Z	Trust new neighbour
Ipseud_Z	Initial pseudonym of the new neighbour
Sign	Digital signature
dir_N	Direction of the node
dir_Z	Direction of the new neighbour
V	Speed of vehicle
N_transm	Transmitter node
N_receiv	Receiver node
Vtransm	Speed of transmitter node
Vreceiv	Speed of receiver node
$\xi(t)$	Time required for communication between two nodes

The three steps of change are classified by type of device and are presented below in this section:

1) Trusted Authority phase:

In this first phase of our strategy, TA generates the real pseudonym <Rpseud> for each vehicle as described below:

1. OBU requests his <Rpseud> from the TA.
2. TA generates <Rpseud> for each node.
3. TA saves <Rpseud> in its database.
4. TA authenticates RSUs neighbours in the range of applicant node.
5. TA sends a copy <RpseudCopy> to RSUs.
6. TA sends <Rpseud> to the node N.

2) Road Side Unit phase:

In this phase, the RSU generates initial pseudonym <Ipseud> for each vehicle. The RSU uses the Poisson process to calculate k, which is the necessary number of initial pseudonyms (formula 1). The RSU takes into account road traffic in its range, by calculating the average number of vehicles passed λ.

$$C(k) = P(X=k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad , k=0,1,2,\ldots \qquad (1)$$

Again, the RSU recalculates the number of Ipseud change k at each period T and regenerates the new Ipseud. RSU checks the trust of the node with TA before sending the Ipseud.

Below, the summary of the process done by the RSU:

1. RSU calculates λ, the average number of vehicles passed.
2. RSU calculates the value k of initial pseudonyms for each period of time [0, T]:

$$C(k)= P(X=k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!} \quad , k=0,1,2,\ldots$$

3. RSU generates <k-Ipseud> randomly.
4. RSU orders the <k-Ipseud> based on time.
5. RSU adds a digital signature for <k-Ipseud>.
6. Repeat steps 1 to 5 at the end of each time T.
7. Node N requests its <Ipseud> (in the range of RSU).
8. RSU requests from node N its <Rpseud>
9. Node N sends its <Rpseud> to RSU
10. RSU compares the Rpseud with RpseudCopy sent by TA
    If Rpseud = RpseudCopy then
      N = TN //// Node is trusted node
      RSU sends <Ipseud> to the node N (digital signature)
      RSU sends the value of λ to the node N
    else N = NTN //// Node is no trusted node
11. Repeat steps 7 to 10.

3) On-Board Unit phase:

In this phase, the OBU changes the pseudonym each time t to discover new neighbors and to know each changed vehicle behavior.

The OBU device starts its process by the calculation of the time required to the next change of pseudonym. This time is calculated by the Exponential distribution function below:

$$F(x)=P([0,t]) = 1-e^{-\mu x} \quad (2)$$

During the circulation, the OBU tries to find new neighbors. If the OBU identifies new neighbor, it changes its pseudonym again for a period of time t: $t= 1/\mu$ (3)

Where the number μ is the average number of changed pseudonyms during the OBU phase. When the OBU identifies a new neighbor, it checks its confidence. If this new neighbor is not a trusted one, then it ignores it and tries to find another trusted neighbor. Else, it determines the direction of this trusted neighbor. When the vehicle is moving in the same direction as the trusted neighbor, the OBU calculates the difference of speed between him and its trusted neighbor. If its speed is greater than the speed of the trusted neighbor, the OBU generates a Npseud and calculates the time of the next change of pseudonym by the Exponential law below:

$$E(X>t+s|\, X>s)= P(X>t) = e^{-\mu t} \quad (4)$$

If the neighbor is faster than the vehicle, the OBU calculates the time required to effect change of its pseudonym by formula 5 below: $t= (4*R/V_{receiv} - V_{transm})*3600 - \xi(t)$ (5)

In the third case, where the vehicle's speed and its neighbor are equal, the OBU calculates the time required before generating a new pseudonym by formula 6 below: $t= 1/\lambda$ (6)

The vehicle generates and changes its pseudonym each time it identifies a new trusted neighbor. The cycle of pseudonyms change starts always with the detection of a new RSU.

When the vehicle is traveling in the opposite direction of its trusted neighbor, it calculates the time required before making a new change of pseudonym by formula 7 below:

$$t= (2*R/V_{transm} + V_{receiv})*3600 - \xi(t) \quad (7)$$

OBU itself generates a new pseudonym <Npseud> dynamically:

1) At any time t, 2) To any direction, and 3) With any speed of the node.

The different steps are summarized below:

1. OBU calculates the average number of pseudonyms change μ.
2. OBU calculates the time t for the next change of pseudonym: $F(x)=P([0,t]) = 1- e^{-\mu x}$
3. A node N searches and identifies all its neighbors
   If Z = false then //// No new neighbors are detected
     change <Npseud> at time t: $t= 1/\mu$
     go to 7
   else NpseudTTL = x = Δt //// New neighbors are detected
4. A node N requests from the new neighbor its <Ipseud>
   If Ipseud_Z = true then N checks the validity of Sign
     If valid_sign then
       Z = trust_Z ////A new neighbors is trusted neighbors
       If N = N_receiv then ////Node is receiver node
           change pseudonym
       else N = N_transm ////Node is a transmitter node
           go to 5
     else Z = NTN ////A new neighbors is no trusted node
         go to 6
   else Z = NTN ////A new neighbors is not a trusted node
     go to 6
5. N determinates the direction <dir> of its neighbor Z
If dir_N=dir_Z then D=Vtransm-Vreceiv///Same direction
   If D > 0 then //// Transmitter node is faster than receiver
     node N generates a random value for <Npseud>
     node N computes the time t for the next change of <Npseud> using the formula:
$E(X>t+s|\, X>s)= P(X>t) = e^{-\mu x}$
     node N triggers the countdown of the time t
   else
If D < 0 then //// Receiver node is faster than transmitter
     node N calculates the time t:
$$t= (4*R/V_{receiv} - V_{transm})*3600 - \xi(t)$$
     node N triggers the countdown of the time t
     node N generates a random value for <Npseud>
   else ////transmitter and receiver node have the same speed
     node N calculates the time t: $t= 1/\lambda$
     node N triggers the countdown of time t
     node N generates a random value for <Npseud>; end if
else node N calculates the time t: //// opposite direction
$t= (2*R/V_{transm} + V_{receiv})*3600 - \xi(t)$
   node N triggers the countdown of the time t
   node N generates a random value for <Npseud>; end if
6. Until there is no more neighbors Z go to 4
7. Until the next detection of an RSU repeat 3 to 6
8. At each detection of a new RSU repeat 1 to 7

The changing of the Npseud is performed locally when the OBU has detected a new trusted neighbor.

C. Evaluation of the model

We ensure the privacy and the confidentiality of the vehicle by changing pseudonyms according to the behaviour of the vehicle and its neighbours. The TA guarantees the

confidentiality to the vehicle during the traffic by the generation of Rpseud. The RSU guarantees updating of road traffic with an Ipseud. The updating of road traffic state is transferred periodically to the vehicle at each cycle of changing Npseud. This cycle of changing a Npseud periodically is named RSU-OBU.

As has been noted, our solution is compatible with security constraints. Our model is very dynamic and processes all possible cases securely. It meets the criteria topology change at any time on VANET, no matter the density of vehicles on an urban environment or on a highway.

IV. PERFORMANCE AND ANALYSIS

A. Security:

Our model ensures the privacy with more confidentiality by using pseudonyms change techniques and It treats all possible cases. By calculating the probability of time for the next pseudonym change, the anonymity of the vehicle is guaranteed.

In our paper, we applied an algorithm GDVAN [7] for greedy behavior attacks in VANETs. By monitoring network traffic traces, the GDVAN (Greedy Detection for VANETs) has the force to detect the presence of a greedy nodes and to determine responsible nodes. We applied a DoS and Sybil attacks to our protocol. In the DoS attack, the time Δt limits the occupancy of the service by another communicating vehicle. In the Sybil attack, the verification of the pseudonym Rpseud at TA level is mandatory before offering a pseudonym Ipseud to begin communications. The three levels of pseudonym Npseud, Ipseud and Rpseud creates a firewall against attacks.

B. Performance analysis:

We implemented our model on OMNET ++ 5.0 simulator [8] with veins 4.4 [9] and SUMO-0.25.0 simulator [10].

Assessment parameters used are presented in table II:

Table II: Simulation parameters

Item	Value
Map of Montreal	2,5 km * 2,5 km
Simulation time	6000 s
Speed max	30 m/s
Mac protocol	IEEE 802.11p
Packet size	1024 bytes
Bit rate	18 Mbps
Thermal noise	-110 dBm
Number of RSU	4
Communication range of vehicle	800 m
Communication range of RSU	800 m
Time of reset RSU [0,T]	[0,1] h

We evaluated our anonymity management system according to three simulation parameters:

1) Proportion of vehicles that changed their pseudonyms:

As shown in figure 2, over 60% of vehicles are changing their pseudonyms. More than the number of vehicles increases more than the proportion of change of pseudonyms increases until reaching 90%.

These results show that the proportion of vehicles that changed their pseudonyms is strongly correlated with the number of vehicles in circulation (fig.2). Indeed, the fewer vehicles on the road, the less pseudonyms are changed. As a result, this low level of pseudonyms change reflects a lower level of anonymity. Conversely, the more vehicles on the road, the more pseudonyms are changed. As a result, this high level of pseudonyms change reflects more anonymity.

The large number of pseudonyms change is ensured by communications between vehicles. However, the third phase of OBU is a very important phase with regard to the number of changes of the Npseud.

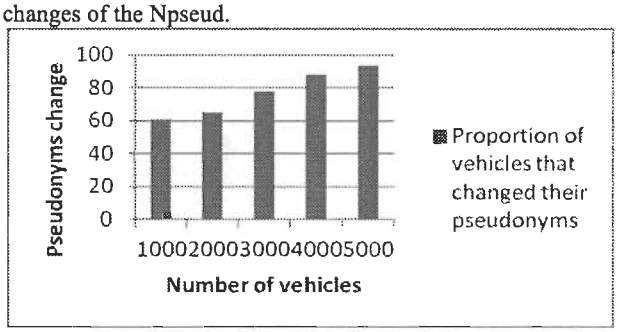

Fig.2. Proportion of vehicles that changed their pseudonyms

The change of Rpseud between vehicles and TA does not greatly increase the proportion of pseudonyms change. The first phase of TA has no great influence on increasing the proportion of pseudonyms change.

Changing Ipseud between vehicle and RSU does not matter much to increase the proportion of pseudonyms change. The primary role of Ipseud change is to update the road condition and to begin inter-vehicles communication.

2) Rate of pseudonyms change by speed of vehicles:

The results presented in figure 3 show that the rate of pseudonyms change depends on the vehicle's speed. At 14 m/s, the rate of pseudonyms change equals 35. The rate of pseudonyms change decreases according to the increase of the vehicle's speed. At 30 m/s, the rate of pseudonyms change equals 7.

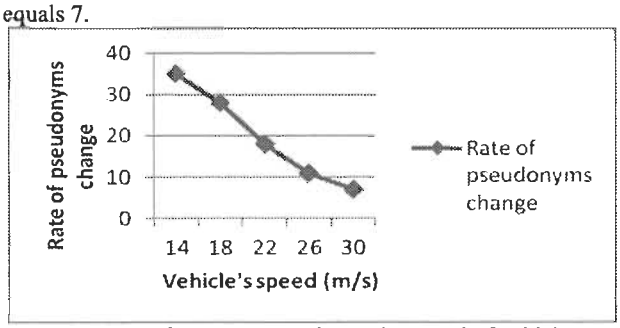

Fig.3.Rate of pseudonyms change by speed of vehicles

The simulation results also show that the rate of pseudonyms change is strongly related to vehicle's speed. An inverted relationship exists between the pseudonym change rate and the vehicle speed. Indeed, the higher the vehicle speed increases the rate of pseudonyms change decreases. As vehicle's speed increases, the probability of crossing neighbors increases and

the possibility of establishing communications increases. Due to the increase in inter-vehicles communication, the third phase of OBU is the most important phase to measure the rate of pseudonyms change according to the vehicle's speed.
The increase in the speed of the vehicle causes the waiting time t to decrease before making the next change of pseudonym. The time value Δt (NpseudTTL) is rounded off to the time value ξ (t) required to establish a communication between two vehicles. Consequently, the calculated time t in order to generate a Npseud is rounded to zero.

3) Packet success proportion by vehicles:
The simulation results in figure 4 shows that the proportion of success packets decreases according to the increase of the number of vehicles in all cases of real, initial or new changing pseudonym. For 1000 vehicles: a proportion of packets success is superior than 90% for a change of Rpseud. For a change of Ipseud, it is equal to 87% and for a change of Npsued it is equal to 62%. For 5000 vehicles: a proportion of success packet is equal to 77% for a change of Rpseud. For a change of Ipseud it is equal to 63% and for a change of Npseud it is equal to 36%.
Simulation results show that the proportion of packets successfully transferred by vehicles is directly related to the number of vehicles in circulation. There is an inverted relationship between the percentage of packets successfully transferred by vehicles and the number of vehicles in circulation. Indeed, as the number of vehicles increases, the percentage of successfully transferred packets decreases.

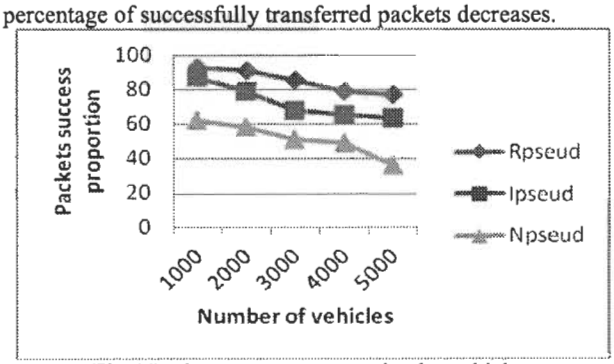

Fig.4.Packets success proportion by vehicles

The percentage of packets transferred successfully by vehicles varies depending on the type of pseudonyms. The percentage of packets transferred successfully by vehicles for a Rpseud is higher than the percentage of packets for a Ipseud and for a Npseud. The percentage of packets transferred successfully by vehicles for a new pseudonym is smaller than that of packets of an initial and real pseudonym.
Simulation results are significant. In our model, the number of calls is strictly increasing respectively in the TA phase, the RSU phase and the OBU phase. The rate of change of Ipseud is average but the rate of Rpseud is low. As long as the number of pseudonyms changes increases, the percentage of packets loss also increases. As a result, the number of successfully transferred packets decreases for any pseudonym type. More the number of neighbors and their speeds increase more the consumption of the bandwidth increases.
The results obtained by the three simulations show the efficiency of our solution and confirm the credibility of our RIN protocol regarding to the privacy assurance in the VANET vehicular network domain.

V. CONCLUSION

In this paper, we have presented a protocol that ensures privacy in Vehicular Ad hoc Networks (VANET). Our pseudonyms change system ensures anonymity in all possible cases. The results show the effectiveness of our solution. Our model satisfies the network security requirements for vehicles in VANET. We have set up an innovative pseudonym management system called RIN protocol. This is an effective protocol, which provides a high level of integrity and confidentiality of transmitted data. The time required to perform a pseudonym change was determined using mathematical formulas. Indeed, the pre-change of pseudonym is an efficient process to guarantee the anonymity of the vehicles and to counter the attacks of malicious ones.
For future work, we will improve the proportion of success packets and we will apply other attacks to our proposed solution.

REFERENCES

[1] http://www.who .int/ (visited 05/10/2016).
[2] ISO 24103:2009 Intelligent transport systems-communication access for land mobiles (CALM), 2009-06-01, TC/SC: ISO/TC 204, ICS: 35.240.60; 03.220.01.
[3] G.Calandrielloy, P. P.dimitratosz, J.P. Hubauxz and A.Lioy, "Efficient and robust pseudonymous authentication in vanet", VANET '07 Proceedings of the fourth ACM international workshop on vehicular ad hoc networks, pages 19-28, ACM NY, USA 2007, ISBN: 978-1-59593-739-1.
[4] J.Freudiger, M.H.Manshaei, J.Y.Le Boudec, and J.P. Hubaux, "On the age of pseudonyms in mobile ad hoc networks", 2010 Proceedings IEEE INFOCOM, March 2010, San Diego,CA/USA, ISBN: 978-1-4244-5838-7.
[5] R.Lu, X.Lin, T.H. Luan, X.Liang and X.(S) Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs", IEEE Transactions on Vehicular Technology (Volume: 61, Issue: 1, Jan. 2012).
[6] S.Mathews M and B.Jinila Y, "An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet", 2014 International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, Feb. 2014, ISBN: 978-1-4799-2320-5.
[7] M.N.Mejri and J.Ben-Othman," GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs", IEEE Transactions on Mobile Computing (Volume: 16, Issue: 3, March 1 2017), pages: 759 - 771, ISSN: 1536-1233.
[8] https://omnetpp .org/ (Visited 06/09/2016).
[9] http://veins.car2x .org/ (Visited 06/09/2016).
[10] https://sourceforge .net/ (Visited 06/09/2016).

CHAPITRE 5

ANALYSE ET INTERPRÉTATION DES RÉSULTATS

5.1 Introduction

Le réseau véhiculaire VANET étant un domaine d'application, nous sommes tenus de prouver toutes nos propositions théoriques par des simulations pratiques.

Le système de changement de pseudonyme est une proposition efficace et fonctionnelle permettant de garantir l'anonymat des véhicules et des conducteurs. Dans le présent chapitre, nous étudierons les résultats des simulations de ce modèle afin d'évaluer notre solution. Nous analyserons ainsi les différents cas possibles en fonction du hangement du comportement du véhicule vis à vis des véhicules voisins.

5.2 Protocole RIN

Notre modèle protège la vie privée des véhicules et des conducteurs et assure une très grande confidentialité. Nous avons appelé cette solution **RIN** (Real New Initial). Ce modèle se base sur les trois principaux entités du réseau véhiculaire VANET : L'Autorité de Confiance (CA), l'infrastructure Road Site Unit (RSU) et l'unité de bord On Board Unit (OBU). Chaque dispositif est responsable de l'émission de son propre pseudonyme. Nous garantissons la confidentialité par la stratégie de changement de pseudonymes décrite dans le protocole RIN, et ceci selon trois étapes principales :

1. Trusted Authority (TA) qui génère un pseudonyme réel;
2. Road Site Unit (RSU) qui génère un pseudonyme initial;
3. On-Board Unit (OBU) qui génère un nouveau pseudonyme.

Les trois niveaux de changement de pseudonyme sont liés aux trois entités du réseau VANET. La **figure 11** montre les trois niveaux.

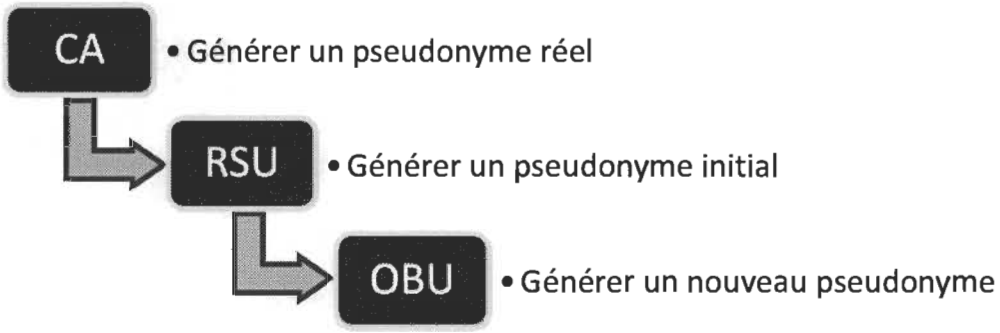

Figure 11: Les différents niveaux de changement de pseudonymes

Dès sa mise en marche, le véhicule demande à l'autorité de confiance (CA) son pseudonyme réel et cette dernière le lui envoie. Le véhicule ne démarre pas la communication avant de communiquer avec l'unité Road Side Unit (RSU). Dans la deuxième étape, le véhicule demande à la première unité RSU qui se trouve dans sa portée son pseudonyme initial. Après la vérification et la validation du pseudonyme réel entre le RSU et la CA, le RSU envoie le pseudonyme initial au véhicule demandeur.

Dans la troisième étape et à chaque découverte de voisins, le véhicule vérifie la confidentialité de ces derniers. Après validation de la communication, le véhicule change son pseudonyme. Le système de changement de pseudonymes étant un mécanisme cyclique, lorsque le nœud découvre une nouvelle unité RSU, la durée de vie de son pseudonyme s'écoule et le cycle recommence de nouveau.

La **figure 12** résume les différentes étapes de changement de pseudonymes selon le protocole RIN.

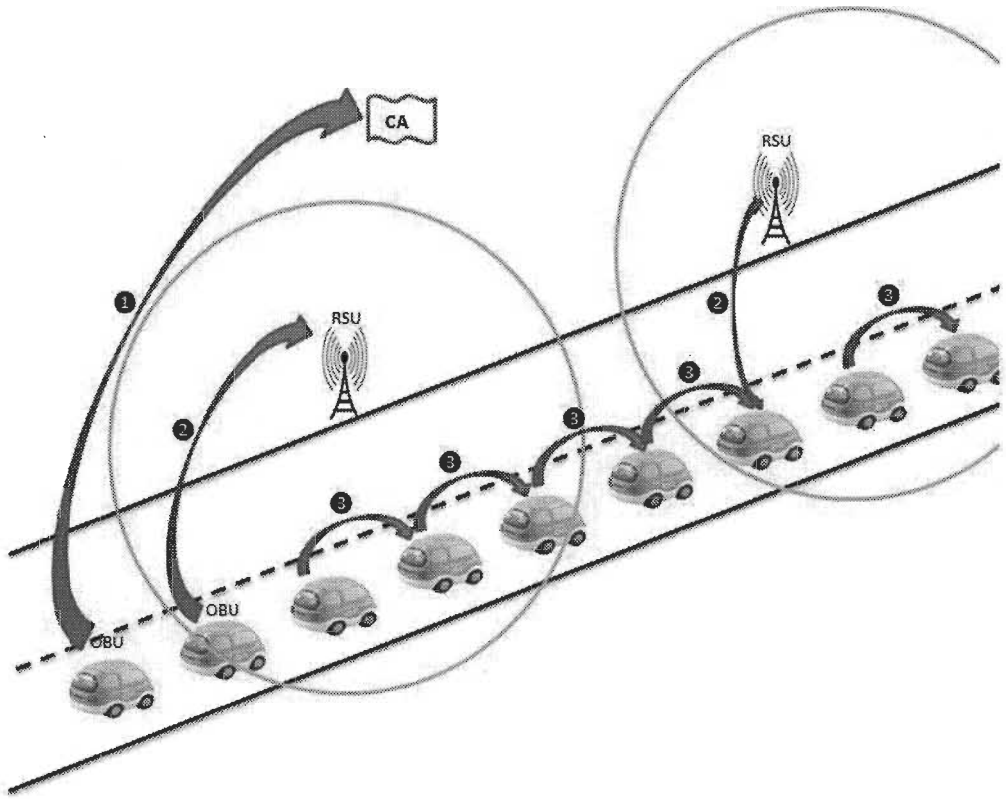

Figure 12 : Les différentes étapes de changement de pseudonymes

Dans la deuxième étape, l'unité RSU envoie le pseudonyme initial signé numériquement pour garantir l'intégrité des données en toute confidentialité.

La **figure 13** montre la signature numérique d'un pseudonyme initial:

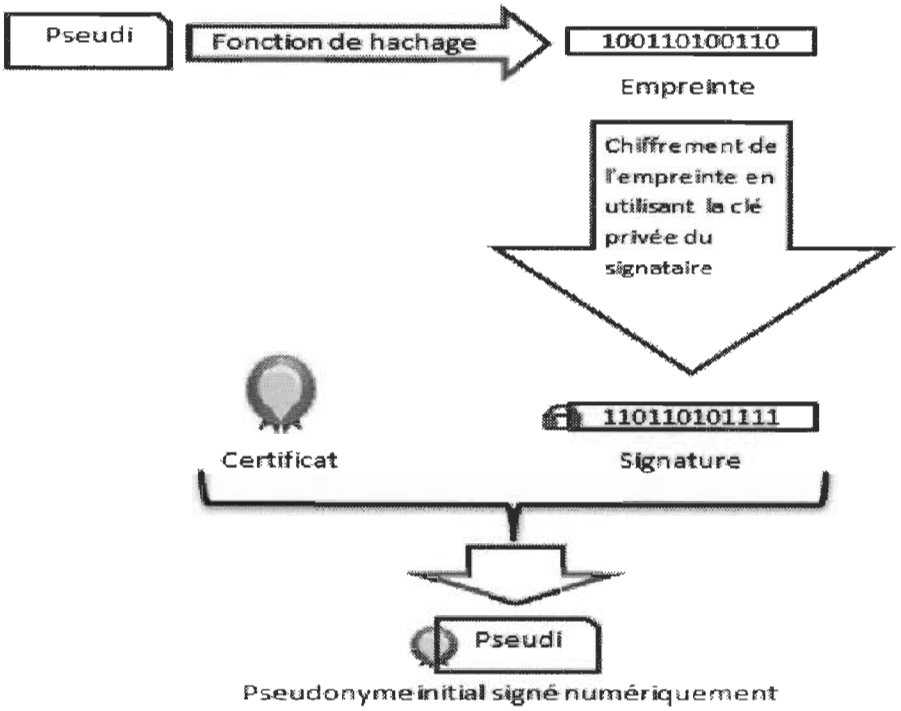

Figure 13: Signature numérique d'un pseudonyme initial

Dans la troisième étape, le véhicule vérifie la validation du pseudonyme initial de chaque véhicule voisin entrant en communication avec lui.

La **figure 14** montre la vérification du pseudonyme initial d'un voisin par la signature numérique.

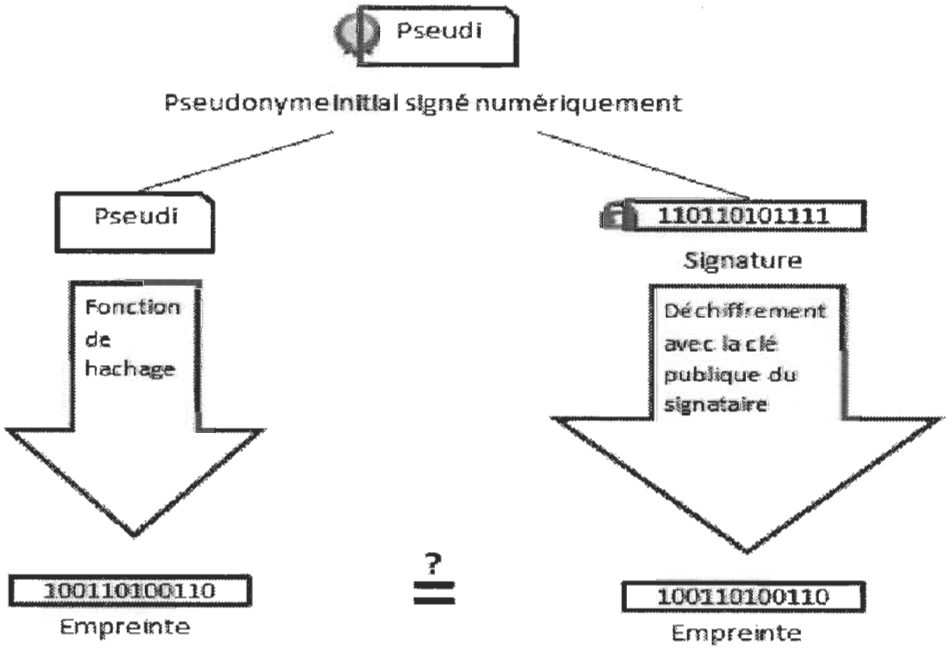

Figure 14: Vérification de la signature numérique d'un pseudonyme initial

5.3 Environnement de simulation

Afin d'évaluer la performance de notre protocole, nous avons implémenté notre modèle sur le simulateur OMNET++5.0 [26] avec VEINS 4.4 [27] et SUMO-0.25.0 [28].

Les paramètres de simulation de notre solution sont mentionnés dans le **tableau III**.

Tableau III

Paramètres de simulation

Item	Value
Map of Montreal	2,5 km * 2,5 km
Simulation time	6000 s
Speed max	30 m/s
Mac protocol	IEEE 802.11p
Packet size	1024 bytes
Bit rate	18 Mbps
Thermal noise	-110 dBm
Number of RSU	4
Communication range of vehicle	800 m
Communication range of RSU	800 m
Time of reset RSU [0,T]	[0,1] h

Nous avons choisi la carte de la ville de Montréal pour bénéficier des deux environnements d'application : urbain et autoroute.

5.4 Résultats des simulations

Nous avons étudié les trois résultats de simulation en vue d'évaluer notre modèle de protection de la vie privée des véhicules.

5.4.1 Proportion des véhicules ayant changé leurs pseudonymes

En vue d'analyser le taux de changement de pseudonyme dans les trois niveaux de notre proposition, nous nous sommes basés sur la proportion des véhicules ayant changé leurs pseudonymes.

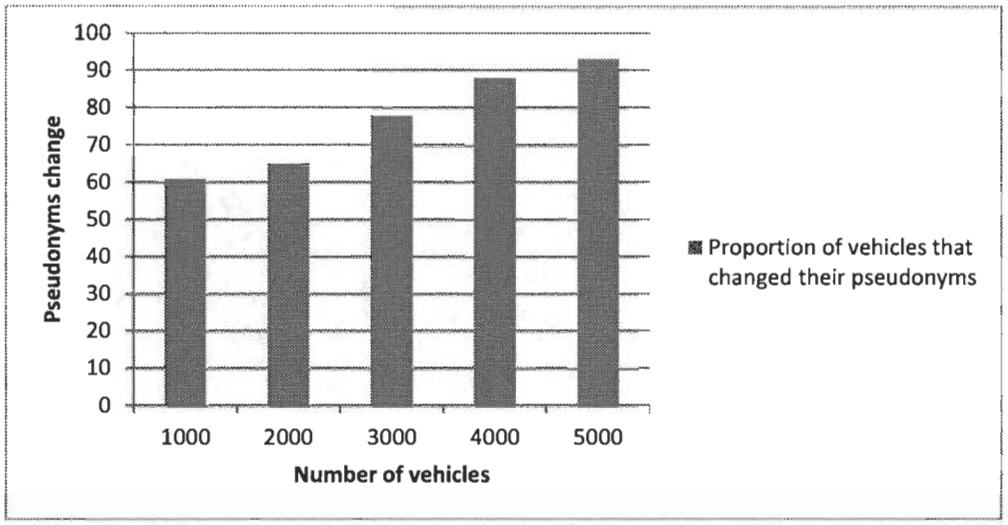

Figure 15: Proportion de véhicules ayant changé leurs pseudonymes

Les résultats montrent que plus de 60% des véhicules changent leurs pseudonymes et que plus le nombre de véhicules augmente, plus la proportion de changement de pseudonyme augmente jusqu'à atteindre environ 90% de changement. En comparant les résultats obtenus dans ces simulations avec ceux des travaux antérieurs (mentionnés précédemment dans l'article scientifique (voir chapitre 3), nous confirmons l'efficacité de notre solution.

Ces résultats montrent que la proportion de véhicules ayant changé de pseudonymes est fortement corrélée au nombre de véhicules en circulation **(figure 15).** En effet, moins il y a de véhicules sur la route, moins de pseudonymes sont changés. Ce bas niveau de changement de pseudonymes reflète un niveau inférieur d'anonymat. A l'inverse, plus il y a de véhicules sur la route, plus il y a une augmentation de changement de pseudonymes. Ce niveau élevé de changement de pseudonymes reflète plus d'anonymat.

Le grand nombre de changements de pseudonymes est assuré par les communications entre les véhicules. Cependant, la troisième phase de l'OBU est une phase très importante en ce qui concerne le nombre de changements du nouveau pseudonyme (Npseud). L'existence d'un nombre élevé de véhicules en circulation offre plus d'anonymat.

Le changement de pseudonyme réel (Rpseud) entre les véhicules et l'autorité de confiance (TA) n'augmente pas grandement la proportion des changements de pseudonymes. La première phase de changement de pseudonyme réel au niveau de la TA n'a donc pas une grande influence sur l'augmentation de la proportion de pseudonymes.

Le changement du pseudonyme initial (Ipseud) entre le véhicule et le RSU n'augmente pas beaucoup la proportion des changements de pseudonymes. Le rôle principal de ce changement de pseudonyme est de mettre à jour l'état de la route et de commencer la communication entre les véhicules.

5.4.2 Taux de changement des pseudonymes selon la vitesse du véhicule

Nous avons étudié les résultats de la simulation concernant le taux de changement de pseudonyme en fonction de la vitesse de circulation des véhicules.

La **figure 16** montre le taux de changement de pseudonymes selon la vitesse du véhicule.

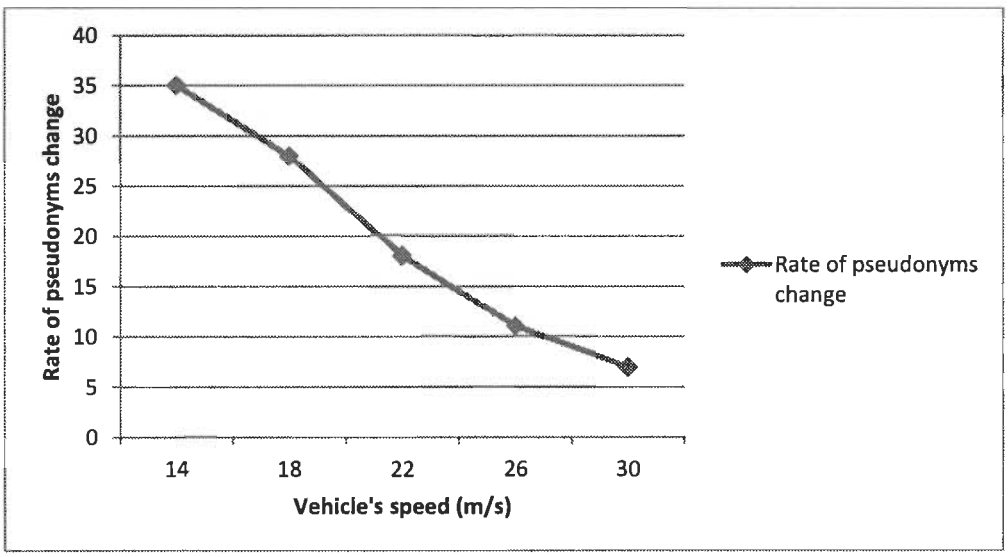

Figure 16: Le taux de changement de pseudonymes en fonction de la vitesse du véhicule

Les résultats montrent que le taux de changement de pseudonyme dépend de la vitesse du véhicule. A une vitesse de circulation de 14 m / s, ce taux est égal à 35 et il diminue avec l'augmentation de celle-ci, tandis qu'à 30 m / s, il est égal à 7.
Les résultats de simulation montrent également que le taux de changement de pseudonymes est fortement lié à la vitesse du véhicule. En effet, il existe une relation inverse entre le taux en question et la vitesse du véhicule : plus cette dernière augmente, plus le taux de changement de pseudonymes diminue **(figure 16).** La diminution du taux de changement de pseudonymes selon la vitesse du véhicule est très significative. À mesure que la vitesse du véhicule augmente, la probabilité de croiser les voisins et la possibilité d'établir des communications augmentent. En raison de l'augmentation de la communication inter-véhicules, la troisième phase de l'OBU est la phase la plus importante pour mesurer le taux de changement de pseudonymes en fonction de la vitesse du véhicule.

L'augmentation de la vitesse du véhicule amène le temps d'attente t à diminuer avant de faire le prochain changement de pseudonyme. La valeur de temps t (NpseudTTL) est arrondie à la valeur du temps ξ (t) requise pour établir une communication entre deux véhicules. Par conséquent, le temps calculé t pour générer un nouveau pseudonyme est arrondi à zéro dans divers cas que nous avons traités par notre modèle dans la phase OBU.

5.4.3 Proportion de paquets reçus avec succès en fonction du nombre de vehicules

Nous avons analysé la proportion de paquets reçus avec succès en fonction du nombre de véhicules. Les résultats sont indiqués sur la **figure 17**.

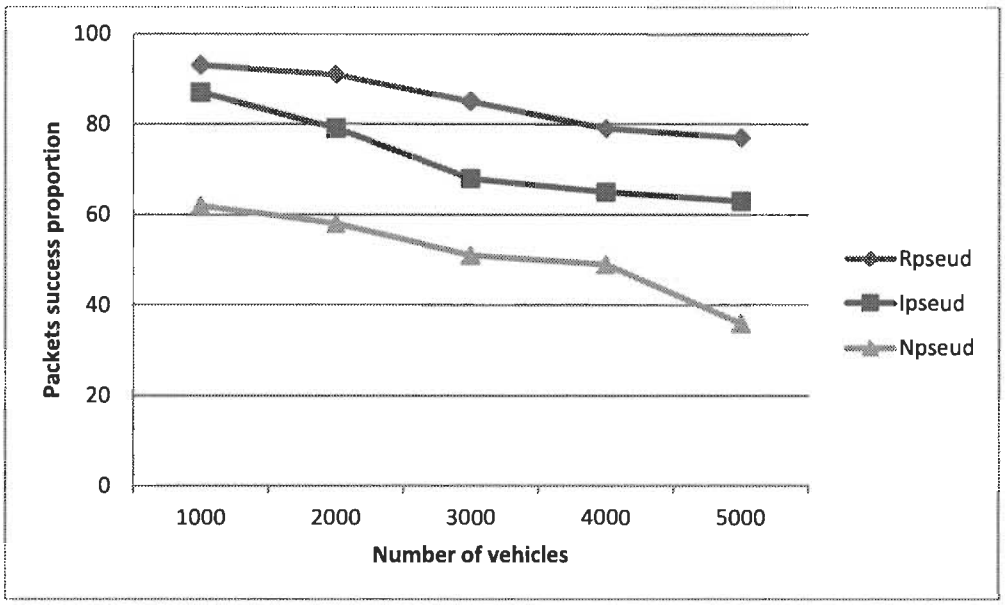

Figure 17: Proportion de paquets reçus avec succès en fonction du nombre de véhicules

Les résultats de la simulation montrent que la proportion de succès des paquets diminue en fonction de l'augmentation du nombre de véhicules dans les trois cas de changement de pseudonymes réels, initiaux ou nouveaux.

Nous avons analysé, respectivement, les deux cas suivants : 1000 et 5000 véhicules en circulation :

a) Pour 1000 véhicules: la proportion de succès de paquets est supérieure à 90% pour les changements de pseudonymes réels Rpseud. Elle est de 87% pour les changements de pseudonymes initiaux Ipseud et de 62% pour les changements de pseudonymes nouveaux Npseud.

b) Pour 5000 véhicules: cette proportion est égale à 77% pour les changements de pseudonymes réels Rpseud, à 63% pour les changements de pseudonymes initiaux Ipseud et à 36% pour les changements de pseudonymes nouveaux Npseud.

La proportion de succès des paquets pour un changement de nouveau pseudonyme est plus faible par rapport aux pseudonymes initiaux et réels parce que le taux de changement de nouveaux pseudonymes est plus élevé.

La proportion de succès de paquets transférés par les véhicules varie selon le type de pseudonyme (**Figure 17**). Elle est plus élevée pour un pseudonyme réel que pour un pseudonyme initial ou pour un nouveau pseudonyme. Les résultats de la simulation sont significatifs. Dans notre modèle, le nombre de communications augmente respectivement dans la phase TA, la phase RSU et la phase OBU. Le taux de changement de pseudonymes nouveaux (Npseud) est très élevé. Le taux de changement de pseudonymes réels (Rpseud) est moyen et celui de pseudonymes initiaux (Ipseud) est faible.

Tant que le nombre de pseudonymes augmente, le pourcentage de perte de paquets augmente également. Le pourcentage de perte de paquets augmente à cause du temps t très court entre deux changements de pseudonymes. En conséquence, le nombre de paquets transférés avec succès diminue pour tout type de pseudonyme. Nous étudions l'idée de la construction d'une base de données afin de maintenir les nœuds de confiance et ainsi diminuer le nombre de paquets perdus.

5.5 Évaluation du modèle

Notre solution est basée sur l'étude de changement de comportement des nœuds. Nous avons appliqué l'algorithme GDVAN [29] pour la détection des attaques de comportement dans les réseaux VANETs. En surveillant les traces du trafic réseau, le GDVAN (Greedy Detection for VANET) a la force de détecter la présence des nœuds gourmands. L'algorithme GDVAN détermine aussi les nœuds responsables des attaques.

Nous avons appliqué deux attaques DoS et Sybil pour évaluer l'efficacité de notre protocole. Dans le type d'attaque DoS, la durée de vie Δt d'un pseudonyme limite l'occupation du service par un autre véhicule communicant. Dans le type d'attaque Sybil, la vérification du pseudonyme Rpseud au niveau TA est obligatoire avant d'offrir un pseudonyme Ipseud. Les trois niveaux de changement (New, Initial and

Real) de pseudonymes Npseud, Ipseud et Rpseud créent un pare-feu contre les attaques.

Le changement de pseudonymes nouveaux au niveau d'OBU commence toujours par un pseudonyme initial émis par le RSU. Le début et la fin du nouveau cycle de changement de pseudonyme nouveau sont déterminés par la détection de nouvelles RSUs. La traçabilité est inaccessible dans les trois étapes de notre système de changement de pseudonyme.

D'autre part, les informations personnelles sont réservées et l'accès est impossible aux autres véhicules.

Nous assurons la protection et la confidentialité du véhicule en changeant le pseudonyme en fonction du comportement du véhicule et de ses voisins. L'autorité de confiance (CA) garantit la confidentialité du véhicule pendant le trafic par la génération d'un pseudonyme réel. Le RSU garantit la mise à jour de la circulation routière avec un pseudonyme initial. Le biais RSU-OBU assure l'application de changement de pseudonymes périodiquement dans un cycle de mise à jour d'informations nécessaires à la circulation.

Nous avons donc proposé un système de protection de l'anonymat qui traite les différents cas possibles dans le réseau véhiculaire VANET. Nous avons étudié ce modèle en deux cas selon la circulation des véhicules:

a) La même direction de circulation pour les deux véhicules communicants : nous avons divisé ce cas en trois sous-catégories possibles en fonction de la différence de la vitesse entre l'émetteur et le récepteur.

b) Les cas d'une direction de circulation opposée : nous avons étudié les différentes sous-catégories possibles de la différence de vitesse entre les deux véhicules communicants.

Nous concluons que notre modèle est très dynamique, traitant les différents cas

possibles en toute confidentialité. En outre, notre solution est compatible avec les contraintes de sécurité et répond aux critères de changement de topologie à tout moment sur le réseau routier quelle que soit la densité des véhicules dans un environnement urbain ou autoroute.

5.6 Conclusion

Les résultats obtenus dans les différentes simulations de notre système visant la protection de la vie privée dans les réseaux véhiculaires VANET montrent l'efficacité de notre proposition. Nous satisfaisons l'ensemble des exigences de sécurité : la confidentialité, l'intégrité, la disponibilité, le temps réel et la vie privée.

CHAPITRE 6

CONCLUSION GÉNÉRALE

Le réseau véhiculaire VANET est un sous-domaine de recherche très dynamique dans le domaine du système de transport intelligent (ITS). Les requis de sécurité dans ce type de recherches informatiques sont : l'authentification, l'intégrité, la confidentialité, la non-répudiation, la disponibilité, le contrôle d'accès, le temps réel et la protection de la vie privée. Les chercheurs proposent des solutions afin de résoudre les problèmes liés au réseau VANET. D'une part, la satisfaction des exigences de sécurité nécessite une étude profonde, d'autre part, les caractéristiques de ce type de réseau augmentent la complexité pour trouver une solution efficace. Le domaine du réseau véhiculaire VANET est un domaine d'application ; toute solution proposée a besoin d'être analysée et validée en pratique avant l'application.

Dans notre travail, nous avons présenté un protocole qui assure la vie privée dans les réseaux véhiculaires ad hoc (VANET). Notre solution se base sur trois composantes principales: l'autorité de confiance (TA), l'unité routière (RSU) et les véhicules (OBU).
Notre système de changement de pseudonyme assure l'anonymat dans tous les cas possibles et répond aux exigences de sécurité liées à ce type de réseaux véhiculaires. Les résultats montrent l'efficacité de notre solution.

Nous avons mis en place un système innovant de gestion des pseudonymes appelé protocole RIN. Il s'agit d'un protocole efficace qui fournit un haut niveau d'intégrité et de confidentialité des données transmises.

Le temps requis pour effectuer un changement de pseudonyme a été déterminé à l'aide de formules mathématiques. En effet, le pré-changement de pseudonymes est un processus haut niveau qui garantit l'anonymat des véhicules et limite les attaques de malveillants contre le réseau VANET.

Le changement de comportement du véhicule est un facteur influant dans le système VANET qui garantit une confidentialité totale. Notre algorithme est basé sur le changement de comportement du véhicule ainsi que celui de ses voisins, en tout temps et en tout lieu ou environnement (urbain ou routier).

Les résultats de nos travaux montrent l'importance d'analyser et d'étudier le changement de comportement des véhicules. La direction du trafic par rapport aux voisins, la nature du véhicule (émetteur ou récepteur) et le changement de vitesse sont trois facteurs importants dans l'analyse du comportement des véhicules.

Nous proposons un protocole qui traite tous les cas possibles (en tout temps, n'importe où, n'importe quelle vitesse, n'importe quelle direction, n'importe quel environnement, n'importe quelle densité de trafic, n'importe quels voisins et n'importe quel changement de comportement de véhicule).

Dans les travaux futurs, nous avons l'intention d'approfondir l'étude de transfert de données entre les véhicules afin d'améliorer la proportion de succès des paquets transférés.

RÉFÉRENCES

[1] http://www.who.int/ vu le 05/10/2016 (Statistic of WHO: World Health Organization)

[2] http://www.etsi.org/ vu le 10/03/2015 (ETSI: European Telecommunications Standards Institute)

[3] Ayoub Benchabana et Ramla Bensaci, "Analyse des protocoles de routage dans les réseaux VANETs", Université Kasdi Merbah-Ouargla Algérie, 06/2014.

[4] Hubaux J.P., "Vehicular Networks: How to Secure Them", MiNeMa Summer School, Klagenfurt, Germany, July 2005.

[5] Chung-Hsien (Stanley) Hsu, "WAVE/DSRC Development and Standardization", Industrial Technology Research Institute, Information & Communications Research Laboratories, Telematics & Control System Division, October 01, 2010.

[6] Jonathan Petit, " Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires", Thèse de doctorat, Juillet 2011, Université de Toulouse 3.

[7] Papadimitratos P., La Fortelle A., Evenssen K., Brignolo R., Cosenza S., "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation", IEEE Communications Magazine, vol. 47, no. 11, pp. 84-95, November 2009.

[8] Giorgio Calandrielloy, Panos Papadimitratosz, Jean-Pierre Hubauxz and Antonio Lioy, "Efficient and robust pseudonymous authentication in vanet", VANET '07 Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pages 19-28, ACM New York, NY, USA 2007, ISBN: 978-1-59593-739-1.

[9] Hesiri Weerasinghe, Huirong Fu and Supeng Leng, "Anonymous service access for vehicular ad hoc networks", Information Assurance and Security (IAS), 2010 Sixth International Conference on, date of conference: 23-25 Aug. 2010, Electronic ISBN: 978-1-4244-7409-7.

[10] Dijiang Huang, Satyajayant Misra, Mayank Verma and Guoliang Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs", IEEE Transactions on Intelligent Transportation Systems, pp. 736–46, (Volume: 12, Issue: 3, Sept. 2011).

[11] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Yves Le Boudec, and Jean-Pierre Hubaux, "On the age of pseudonyms in mobile ad hoc networks", 2010

Proceedings IEEE INFOCOM, date of conference: 14-19 March 2010, San Diego,CA/USA, Electronic ISBN: 978-1-4244-5838-7.

[12] Mostafa Dikmak, Zahraa Sabra, Ayman Kayssi and Ali Chehab, "Optimized conditional privacy preservation in VANETs", 19th International Conference on Telecommunications (ICT 2012), date of conference: 23-25 April 2012, Jounieh, Lebanon, Electronic ISBN: 978-1-4673-0747-5.

[13] Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang and Xuemin (Sherman) Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs", IEEE Transactions on Vehicular Technology (Volume: 61, Issue: 1, Jan. 2012).

[14] Yuanyuan Pan and Jianqing Li, "An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional vanets", proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), date of conference: 23-25 May 2012, Wuhan, China, Electronic ISBN: 978-1-4673-1212-7.

[15] Xinyi Wang, Zheng Huang, Qiaoyan Wen and Hua Zhang, "An efficient anonymous batch authenticated and key agreement scheme using self-certified public keys in vanets", 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013), date of conference: 22-25 Oct. 2013, Xi'an, China, Electronic ISBN: 978-1-4799-2827-9.

[16] Yeong-Sheng Chen, Tang-Te Lo, Chiu-Hua Lee and Ai-Chun Pang, "Efficient pseudonym changing schemes for location privacy protection in vanets", 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, Nevada, USA, date of conference: 2-6 Dec. 2013, Electronic ISBN: 978-1-4799-2491-2.

[17] Sam Mathews M and Bevish Jinila Y, "An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet", 2014 International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, date of conference: 13-14 Feb. 2014, Electronic ISBN: 978-1-4799-2320-5.

[18] 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.

[19] Abdelwahab Boualouache and Samira Moussaoui, "S2SI: a practical pseudonym changing strategy for location privacy in vanets", 2014 International Conference on

Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, date of conference: 17-19 June 2014, Electronic ISBN: 978-1-4799-5178-9

[20] Wang Ying and Yang Shiyong, " Protecting Location Privacy via Synchronously Pseudonym Changing in VANETs", Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, date of conference: 7-9 April 2014, Electronic ISBN: 978-1-4799-3070-8.

[21] Chang-Ji Wang, Dong-Yuan Shi and Xi-Lei Xu, "Pseudonym-based cryptography and its application in vehicular ad hoc networks", 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications, Guangzhou, China, Date of Conference: 8-10 Nov. 2014, Electronic ISBN: 978-1-4799-4173-5.

[22] Song Guo, Deze Zeng, and Yang Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications", IEEE Transactions on Parallel and Distributed Systems (Volume: 25, Issue: 11, Nov. 2014), pages: 2794 - 2803, date of publication: 04 November 2013, Print ISSN: 1045-9219.

[23] Kahina Moghraoui Aoudjit and Boucif Amar Bensaber, "An efficient pseudonym change protocol based on trusted neighbours for privacy and anonymity in vanets", DIVANet '15.5th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications 2015, pages 93-99, Cancun, Mexico , November 02 - 06, 2015, ISBN: 978-1-4503-3760-1.

[24] Amit Kumar Tyagi and N. Sreenath, "Location privacy preserving techniques for location based services over road networks", Communications and Signal Processing (ICCSP), 2015 International Conference on, date of conference: 2-4 April 2015, Electronic ISBN: 978-1-4799-8081-9.

[25] Dong Wang, Deshu Li, Xiaohong Li and Zhu Xiao, "An analysis of anonymity on capacity finite social spots based pseudonym changing for location privacy in vanets", Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on , date of conference: 15-17 Aug. 2015, Electronic ISBN: 978-1-4673-7682-2.

[26] https://omnetpp.org/ vu le 06/09/2016.

[27] http://veins.car2x.org/ vu le 06/09/2016.

[28] https://sourceforge.net/ vu le 06/09/2016.

[29] Mohamed Nidhal Mejri and Jalel Ben-Othman," GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs", IEEE Transactions on Mobile

Computing (Volume: 16, Issue: 3, March 1 2017), pages: 759 - 771, ISSN: 1536-1233.