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

Mémoire de MASTER

Domain : Mathématiques et Informatique
Filière : Informatique
Option : Réseaux, Systèmes et Applications Réparties

Par :
....MOUSSAOUI YAZID.

THEME

L'authentification des messages de broadcast dans les VANET

Soutenu publiquement devant le jury composé de:

*Mr. **Lahcen Bensaad***	*M.C.(B)*	*Président*
Mr.Zine el abidine nadhir	*M.A.(A)*	*Examinateur*
Mr.Ouladdjedid lakhdar kamel	*M.A.(A)*	*Examinateur*
Mr.CHAIB Noureddine	*M.A.(A)*	*Encadreur*

Année Universitaire 2015/2016

Remerciments

Nous remercions tout d'abord, Allah qui nous a donné la force et le courage afin de parvenir à élaborer ce modeste travail.

Nous tenons à remercier de tout cœur mon encadreur

Monsieur chaib Noureddine et témoigner toute notre reconnaissance pour ses conseils judicieux, de ses remarques objectives et surtout de ses gentillesses permanentes.

Nos vifs remerciements à tous les enseignants qui ont contribués à mon formation, et ainsi tous les gens de prés et de loin qui ont aidé à l'élaboration de ce sujet.et à tous nos professeurs et travailleurs de l'université AMAR TELIDJI– LAGHOUAT-

Et enfin, que nos chers parents et familles, et bien avant tout, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation de Master dans les meilleures conditions.

Dédicaces

Avant tout, je remercie le bon Dieu, qui m'a élaboré ce modeste travail.
J'ai l'immense honneur de dédier travail :

A mes très chers parents qui étaient présents à coté de moi durant toute ma vie.

A mes frères et mes sœurs.

A mes amis.

A tous ceux que j'aime, tous ceux qui m'aiment et tous ceux qui me sont chers.

A tous les professeurs et enseignants qui m'ont participe à ma formation Master.

A tous ceux qui m'ont aidé durant ma vie universitaire
A toute la promotion RESAR 2015.

Table des matières

Table des figures

Liste des tableaux

Résumé

Les réseaux véhiculaires ou les VANETs, sont des réseaux qui capable de communiqué entre deux ou plusieurs véhicules et notamment avec des éléments d'infrastructure sur la route. Récemment, le concept de systèmes de transports intelligent a connu beaucoup d'intérêt. Les STI sont des systèmes utilisant les nouvelles technologies de communication sans fil appliquées au domaine du transport pour améliorer la sécurité routière, la logistique et les services d'information. Des défis majeurs ont besoin cependant d'être abordés pour offrir une communication sur la route sécurisée et fiable dans des environnements anonymes et quelquefois hostiles à la communication. Comme dans tout système de communication, les réseaux véhiculaires doivent opérer en respectant des contraintes en termes de qualité de service. Ces contraintes sont d'autant plus strictes quand il s'agit de fournir des services de sécurité sur la route.

Avec le développement de projet VANET, des techniques de communication ont été créé pour le relayage d'informations de manière fiable et à faible délai entre véhicules voyageant à haute vitesse. Ces techniques devront permettre de respecter des contraintes temporelles sévères afin d'envisager leur utilisation dans des applications de sécurité sur la route.

Mots clé: Authentification, Diffusion ,VANET

Abstract

Vehicular networks or VANETs, are networks that can release two or more vehicles, particularly with infrastructure elements on the road. Recently, the concept of smart transportation systems experienced a lot of interest. ITS are systems using new wireless communication technologies applied to transportation to improve road safety, logistics and information services. However, major challenges need to be addressed to provide a communication on the road in secure and reliable anonymous and sometimes hostile communication environments. As in any communication system, vehicular networks must operate respecting constraints in terms of quality of service. These constraints are particularly strict when it comes to providing security services on the road.

With the development of VANET project, communication techniques were created for the relaying of information reliably and low delay between vehicles traveling at high speed. These techniques will enable compliance with strict time constraints to consider their use in security applications on the road.

Keywords: Authentication, Broadcast, VANET

Introduction générale

Depuis de nombreuses années, les gouvernements, constructeurs automobiles et consortiums d'industriels, ont fixé la réduction des accidents de la route comme une priorité majeure. Afin de réussir ce challenge, une idée novatrice a été de rendre les véhicules et les routes plus intelligents par le biais des communications sans fil. En effet, les véhicules actuels génèrent et analysent déjà une quantité de données importante, mais ne diffusent rien.

Avec des communications sans fil, l'environnement du véhicule et le ≪ champ de vision ≫ du conducteur sont accrus. Ainsi, grâce à des véhicules à l'écoute de leur environnement, plus de 75 applications potentielles ont été identifiées, dont 34 à vocation de sécurité (les 41 restantes étant pour l'optimisation du trafic routier et le confort des usagers).

Avec l'avènement des technologies sans fil telles que la 3G, le Wifi, ou le Bluetooth, les communications sans fil sont devenues omniprésentes et peu onéreuses. C'est pourquoi, afin de déployer ces applications, un type de réseau a émergé : le réseau sans fil véhiculaire. Une des principales composantes d'un tel réseau est la communication inter-véhicules. En effet, elle permet d'assurer la disponibilité des services en cas d'infrastructure inexistante. Le réseau est alors appelé réseau sans fil ad hoc véhiculaire (VANET, *Vehicular Ad hoc NETwork).*

La sécurité est un prérequis pour déployer ces réseaux. En effet, des signatures et des certificats numériques doivent être rattachés aux messages beacons periodiques afin d'assurer l'authentification de données échangées. Ces informations ont un impact négatif sur le réseau, car elles augmentent l'overhead.

Ce mémoire est organisé comme suit : le premier chapitre est consacré aux généralités sur les réseaux ad hoc et particulièrement les réseaux VANET, Le second présente la sécurité dans les réseaux ad hoc de manière générale et montre les mécanismes utilisés et ceux qui peuvent être mis en œuvre pour la sécurité dans les VANETs. En fin troisième chapitre présente notre propre analyse de simulation sur les messages de broadcast avec outils puissant ns-3.

Chapitre 1 : Les Réseaux VANET

Introduction

Le VANET ou Véhicule ad hoc networks est une forme de mise en application du MANET, très inspiré de celle-ci elle permet aux véhicules de communiquer via des messages d'alertes de sécurité envoyés entre eux par un système de communication par nœud. Chaque nœud est capable de gérer et d'organiser un ensemble d'information envoyé par les véhicules se trouvant dans la zone à proximité du danger.

1. Les réseaux MANET

C'est un système autonome composé des nœuds mobiles dynamiques interconnectés par des liens sans fil sans l'utilisation de l'infrastructure fixe. Les nœuds sont libres de se déplacer de façon aléatoire, par conséquence, la structure du réseau changé fréquemment et d'une manière imprévisible.

2. Les réseaux VANET

Un réseau VANET fonts partie de la famille des réseaux mobiles MANET qui peut communiquer entre véhicules intelligents équipés de calculateurs, de cartes réseau et de capteurs. La Fig. 1.1 illustre l'échange des informations sur le trafic par exemple ou avec des RSUs (*ROAD SIDE UNIT*) tout au long des routes pour demander des informations ou accéder à internet...etc. Les réseaux véhiculaires regroupent deux grandes classes d'applications, à savoir les applications qui permettent de bâtir un système de transport intelligent ITS (Intelligent transport System) et celles liées au confort ou avertissement des conducteurs et des éventuels passagers.

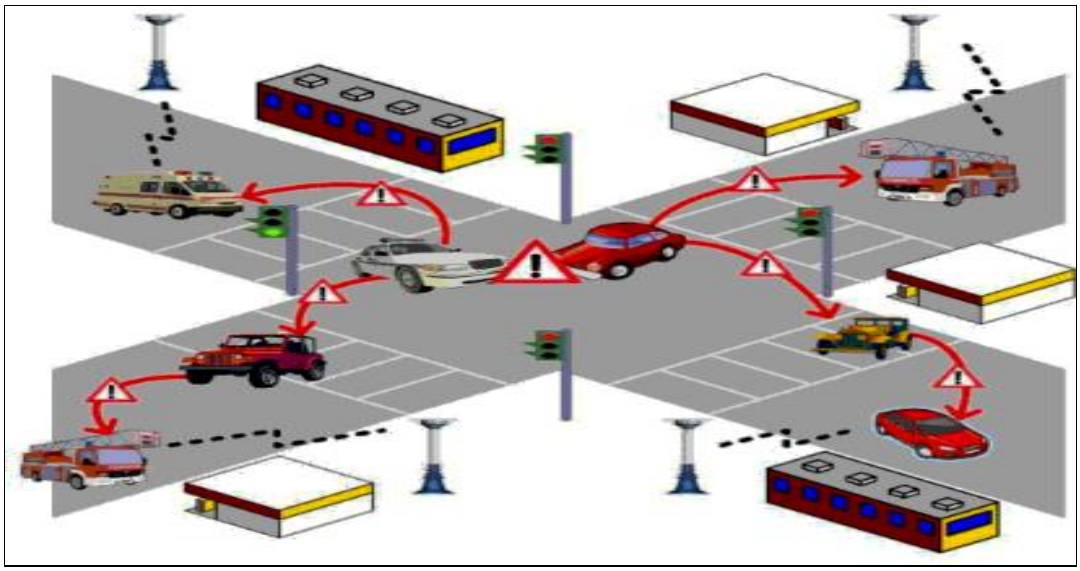

Fig. 1.1 : Exemple d'un réseau VANET [1]

3. *Messagerie et architecture des réseaux VANET*

Un réseau VANET est un ensemble d'entités communicantes organisées selon une architecture de communication. Ces entités embarquées peuvent rencontrer des environnements différents (urbain, peri-urbain, autoroutier), ayant leurs propres contraintes.

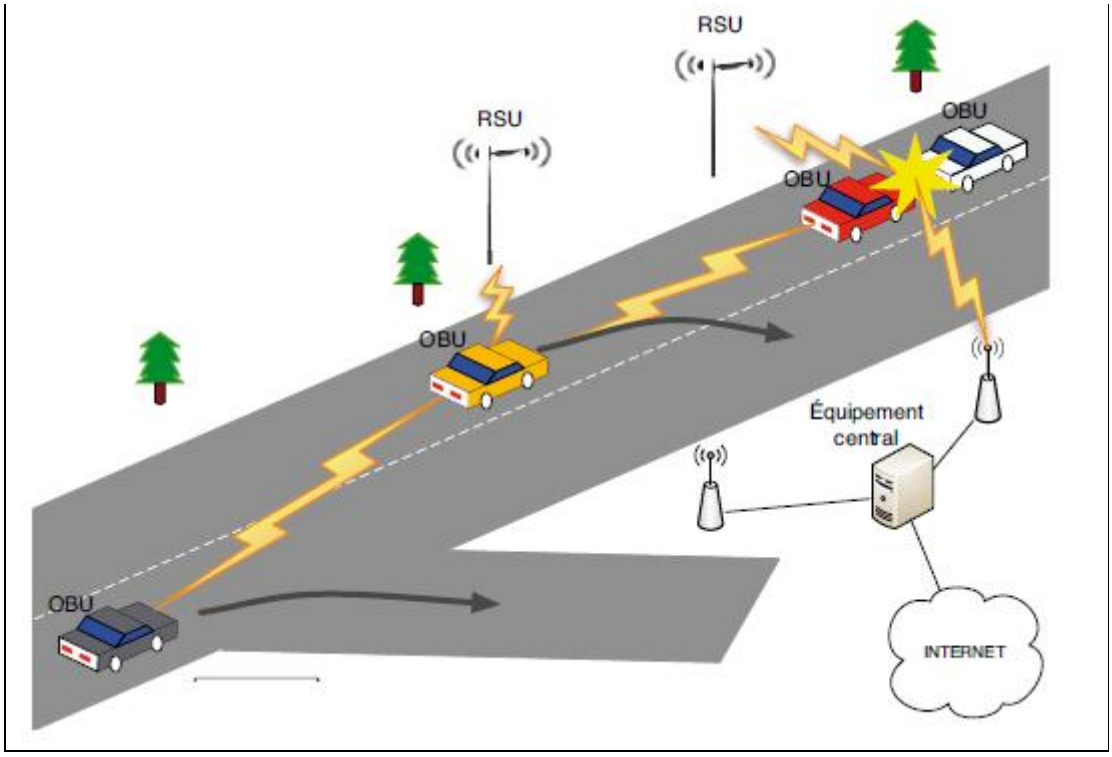

Fig. 1.2 : Exemple d'échange des messages d'un réseau VANET [2]

3.1 Entité de communication

Dans un réseau VANET, il existe quatre entités communicantes : l'équipement personnel, le véhicule, l'équipement de bord de route et l'équipement central. La Fig. 1.2 illustre un exemple de réseau véhiculaire faisant intervenir les différentes entités lors d'un accident de la route.

- **Les équipements personnels :**

Sont les équipements qui peuvent être apportés par l'utilisateur à l'intérieur de son véhicule. Cela peut être un téléphone portable, un ordinateur portable ou encore un GPS autonome. Ces équipements peuvent interagir avec le véhicule. De nos jours, en activant l'interface Bluetooth du téléphone portable, on peut utiliser son téléphone portable par la commande vocale (en utilisant les microphones intègres au véhicule) ou par le biais de l'interface Homme- Machine (IHM) du véhicule.

- **Les véhicules modernes :**

Sont équipés d'un ensemble de processeurs connectés à une plateforme centrale de calcul qui dispose d'interfaces filaires et sans fil. Les véhicules intelligents sont des véhicules équipés d'une unité nommée OBU (*On-Board Unit)*. Cette unité peut enregistrer, calculer, localiser et envoyer des messages sur une interface réseau. La Fig. 1.3 illustre un exemple d'un véhicule intelligent.

- **Les entités de bord de route :**

Sont appelées *Road-Side Unit* (RSU). Ces unités peuvent informer les véhicules à proximité en diffusant les conditions de trafic, météorologiques ou spécifiques à la route (vitesse maximale, autorisation de dépassement, etc.). Les RSUs peuvent aussi jouer le rôle de station de base en relayant l'information envoyée par un véhicule.

- **L'équipement central :**

Se situe du côté serveur. Il est transparent pour l'utilisateur. Cet équipement central pourra être un serveur de stockage, un point d'entrée à un réseau filaire (Internet) ou un serveur de transaction (télépéage par exemple).

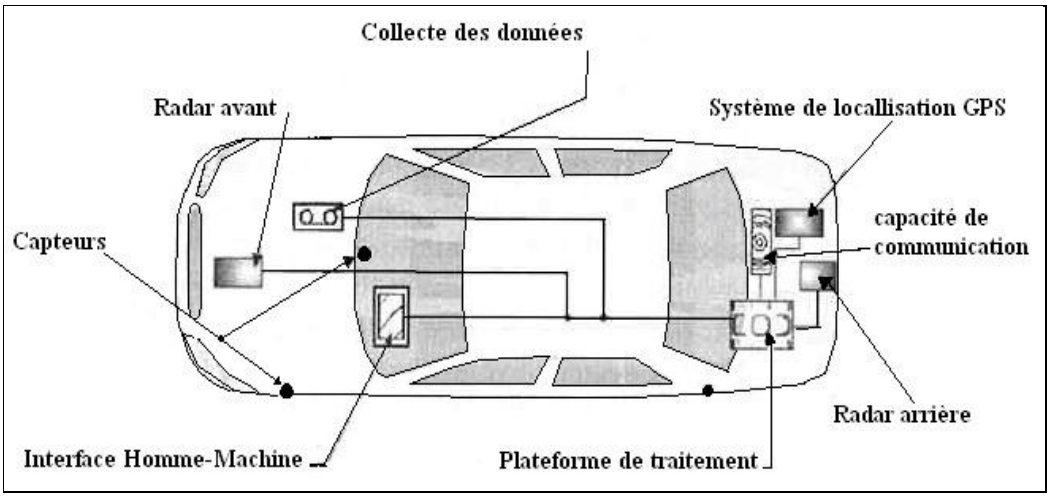

Fig. 1.3 : Exemple de véhicule intelligent [3]

3.2 Type des messages

Les entités formant un réseau VANET peuvent générer et échanger des différents types de messages. En fonction de l'application et du contexte environnemental, un véhicule peut envoyer (ou recevoir) les messages suivants.

3.2.1 Messages beacon

Suivant le standard DSRC, un message beacon est émis périodiquement plusieurs fois par second. Ce message contient la position, la vitesse, la direction et l'itinéraire du véhicule émetteur. Le véhicule peut aussi prédire et anticiper des situations dangereuses. Le message

beacon est l'équivalent du message HELLO des protocoles de routage, qui sont diffusées aux voisins à un saut.

3.2.2 Messages d'alerte

Le message d'alerte est généré lorsqu'un évènement est détecté. Cela peut être la détection d'une situation dangereuse. Les messages d'alerte doivent être retransmis périodiquement à fin d'avertir les nouveaux nœuds voisins, qu'ils soient transmis rapidement. Les messages d'alerte doivent inclure les coordonnées du lieu de l'accident.

3.2.3 Autres messages

Ils comprennent tous les messages qui ne sont pas des messages d'alerte ou des messages beacon. Généralement ces messages ne sont pas retransmis. En effet, il peut s'agir d'un message de transaction financière ou l'envoi de courrier électronique. Tous les messages reçus seront stockes dans un cache des messages récemment reçus.

3.3 Architecture système de communication

Les systèmes de gestion de trafic conventionnels sont basés sur des infrastructures centralisées ou des caméras et des capteurs fixés sur la route collectent des informations sur la densité et l'état du trafic. Ces informations sont transmises à une unité centrale pour traiter et prendre les décisions adéquates. De tels systèmes exhibent un coût de déploiement assez important et se caractérisent par un temps de réaction de l'ordre de la minute pour le traitement et le transfert des informations. Dans un contexte ou le délai de transmission de l'information est vital et revêt une importance majeure dans ce type de systèmes, ce délai est un véritable frein. De plus, les équipements mis en place sur les routes nécessitent une maintenance périodique et chère. Par conséquent, pour déployer un tel système à large échelle, un important investissement dans l'infrastructure de communication et de capteurs est nécessaire. Cependant, avec le développement rapide des technologies de communication sans fil, des systèmes de localisation et de collecte d'information par capteurs, une nouvelle architecture décentralisée (ou semi-centralisée) basée sur des communications véhicule-a-véhicule (V2V, *Vehicle to Vehicle*) suscite ces dernières années un réel intérêt auprès de la communauté scientifique, des constructeurs automobiles et des opérateurs Télécoms. Ce type d'architecture s'appuie sur un système distribué, autonome, et est formé par les véhicules eux-mêmes sans l'aide d'une infrastructure fixe pour le relayage des données et des messages. On parle dans ce cas d'un réseau ad hoc de véhicules (VANET, *Vehicular Ad hoc NETwork*). Le VANET n'est autre qu'une application dédiée et spécifique des réseaux ad hoc mobiles conventionnels (MANET, *Mobile Ad hoc NETwork*). La Fig. 1.4 illustre un exemple d'architecture réseau de DSRC. On remarque aussi la présence de deux types de communications nommées V2V et V2I.

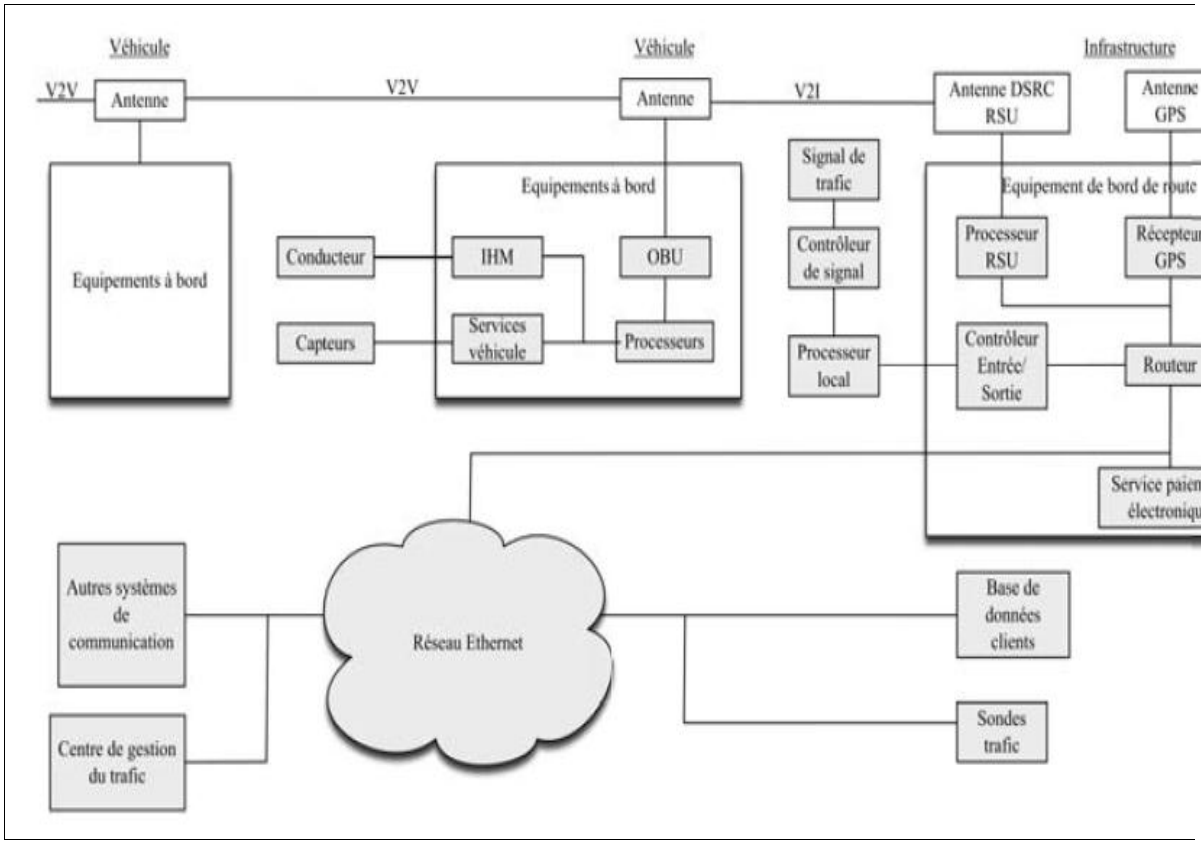

Fig. 1.4 : Architecture réseau de DSRC dans le projet VII [4]

3.3.1 Communication de véhicule à véhicule

Cette architecture peut être utilisée dans le scénario de diffusion d'alertes (freinage d'urgence, collision, ralentissement…) ou pour la conduite coopérative. Aucune infrastructure n'est utilisée, aucune installation n'est nécessaire sur les routes et tous les véhicules sont équipés pour communiquer directement entre eux n'importe où, que ce soit sur les autoroutes, des routes de montagnes ou des routes urbaines, ce qui donne une communication moins coûteuse et plus flexible(5).Cette approche souffre de certains inconvénients dont nous citons :

- Les délais de communication qui sont élevés, étant donné que la communication se fait en utilisant les multi-sauts.
- Les déconnexions fréquentes dues au fait que les véhicules sont mobiles.
- La sécurité du réseau est très limitée

3.3.2 Communication de véhicule à infrastructure

Dans cette architecture, on ne se concentre pas seulement sur des simples systèmes de communications inter-véhicules mais aussi ceux qui utilisent des stations de bases ou des RSUs (Road Side Units). Cette approche repose sur le modèle client/serveur où les véhicules sont les clients et les stations installées le long de la route sont les serveurs. Ces serveurs sont connectés entre eux via une interface filaire ou sans fil. Toute communication doit passer par eux. Ils peuvent aussi offrir aux utilisateurs plusieurs

services concernant le trafic, accès à Internet, échange de données de voiture-à-domicile et même la communication de voiture-à-garage pour le diagnostic distant. L'inconvénient majeur de cette approche est que l'installation des stations le long des routes est une tâche coûteuse et prend beaucoup de temps, sans oublier les coûts relatifs à la maintenance des stations [5].

3.3.3 Communication hybride

La combinaison des communications véhicule à véhicule avec les communications des véhicules à infrastructures, permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures (stations de bases) étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette distance. Dans un but économique et afin d'éviter la multiplication des stations de bases à chaque coin de rue, l'utilisation de véhicules intermédiaires prend tout son importance.

4. Applications

Les principales applications des réseaux VANET peuvent être classées comme suit.

4.1 Applications de sécurité du trafic routier

La sécurité routière est devenue une priorité dans la plupart des pays développés, cette priorité est motivée par le nombre croissant d'accidents sur ses routes associé à un parc de véhicules de plus en plus important. Les VANETs permettent de prévenir les collisions et les travaux sur les routes, de détecter les obstacles (fixes ou mobiles) et de distribuer les informations météorologiques par envoi de messages d'alerte. A titre d'exemple, alerter un conducteur en cas d'accidents permet d'avertir les véhicules qui se dirigent vers le lieu de l'accident que les conditions de circulations se trouvent modifiées et qu'il est nécessaire de redoubler de vigilance. Les messages d'alertes et de sécurité doivent être de taille réduite pour être transmis le plus rapidement possible et doivent être émis à des périodes régulières.

4.2 Applications de gestion du trafic routier

Le trafic automobile peut être grandement amélioré grâce à la collecte et au partage de données collectées par les véhicules, ce qui devient un support technique pour les conducteurs. Une voiture peut, par exemple, être avertie en cas d'un ralentissement anormal (bouchon, embouteillage, éboulement de rochers ou travaux [6].

4.3 Applications de confort

Le trafic automobile peut être grandement amélioré grâce à la collecte et au partage de données collectées par les véhicules, ce qui devient un support technique pour les

conducteurs. Une voiture peut, par exemple, être avertie en cas d'un ralentissement anormal (bouchon, embouteillage, éboulement de rochers ou travaux).

5. Environnement de déploiement

Le réseau routier est diversifié et propose plusieurs milieux de déplacement. Ces milieux se différencient par leur localisation (urbain, périurbain, rural, montagneux) et par leurs moyens (autoroute, route départementale, route nationale, chemins communaux… etc.). En raison de leurs spécificités (vitesse, densité du trafic routier), nous nous intéressons au milieu urbain et au milieu autoroutier.

5.1 Milieu urbain

Nous définissons le milieu urbain comme un réseau routier formé d'intersections et de points d'arrêt (feux tricolores, stop, cédez le passage, …etc.). Il s'agit d'un environnement ou les ondes sont fortement perturbées à cause de la forte présence de bâtiments et d'obstacles. Le milieu urbain se caractérise par un modèle de mobilité complexe, une densité de véhicules importante et une vitesse réduite (inférieure à 60 km/h). De plus, il y'a déjà une infrastructure importante (panneaux, etc.). Il semble donc facile d'ajouter un équipement sur cette infrastructure afin de déployer les réseaux sans fil véhiculaires (V2I).Dans ce milieu, les réseaux V2V sont aussi réalisables et présentent l'avantage d'éviter le déploiement de RSU.

5.2 Milieu autoroutière

Le milieu autoroutier est caractérise par une vitesse des véhicules importante (limitée à 130 km/h en France), une forte densité et une impossibilité (financière et de maintenance) de couvrir toutes les autoroutes avec des RSUs. On y retrouve aussi une forte diversité de véhicule (poids lourd, voitures). En raison de l'absence d'obstacles tels que des immeubles, cet environnement semble moins perturbant pour les ondes radio. Néanmoins, il rencontre des problèmes d'étalement Doppler à cause de la vitesse élevée. De plus, certaines solutions actuelles, comme l'analyse par caméra numérique, sont perturbées par les poids lourds. En effet, ils gênent la vision des caméras, mais sont aussi des obstacles perturbants pour les communications. Sur une autoroute, un simple accident peut vite dégénérer à cause, en partie, de la vitesse. La vitesse élevée peut engendrer des accidents plus graves, et soulève des contraintes de temps réel, de tolérance aux fautes et de fiabilité. Les applications de sécurité du trafic routier y seront donc très utiles.

6. Caractéristiques des réseaux VANET

Les VANETs ont la particularité d'avoir une très grande mobilité (les nœuds mobiles circulent à très grande vitesse). La topologie dynamique provoque de nombreuses

reconfigurations (mise à jour des tables de routage...etc.), et soulève par conséquent des problèmes de performances. Après cet aperçu, nous détaillons, dans cette section, les caractéristiques des VANETs.

6.1 Energie

La contrainte d'énergie représente un facteur limitant important, les entités des réseaux véhiculaires disposent de capacités énergétiques suffisantes qu'elles tirent du système d'alimentation des véhicules. Même en cas d'arrêt du moteur et donc d'arrêt du système d'alimentation, il est possible pour une plateforme embarquée de recourir au dispositif de batteries dont le véhicule, du fait de sa taille, peut disposer. Les plateformes embarquées dans les véhicules étant pleinement alimentées, elles peuvent bénéficier de capacités de calcul plus massives et de multiples interfaces de communication.

6.2 Mobilité

Les réseaux véhiculaires se distinguent également des réseaux sans fil classiques (réseaux sans fil domestiques) par un modèle de mobilité, les plus évidentes est l'importante vitesse des nœuds. Cette contrainte de mobilité réduit considérablement les durées pendant lesquelles les nœuds peuvent communiquer. Ces conditions sont de nature à poser d'importants problèmes de connectivité (par exemple évanouissement multi-trajet, effet de masque, atténuation de parcours…etc.). Ainsi la durée de vie des liens sur autoroute. Néanmoins, les déplacements des véhicules sont délimites et prédéfinis par les infrastructures routières et le comportement des conducteurs. Les informations sur les infrastructures routières sont souvent disponibles par le biais d'équipements de positionnement comme le GPS. A partir de la vitesse courante, de la vitesse moyenne et de la trajectoire de la route, la prochaine position du véhicule peut être prédite. Cette prédiction peut être affinée par la prise en compte de modèles de déplacement des usagers de la route. En effet, les véhicules sont la plupart du temps dans la même zone géographique, c'est-à-dire à 50 km de la maison du propriétaire. On retrouve aussi les modèles de déplacement réguliers comme le trajet maison-travail [7].

6.3 Topologie du réseau et connectivité

Les réseaux VANET sont caractérisés par la forte mobilité des nœuds (véhicules), liée à la vitesse des voitures qui est très importante dans les autoroutes. Par conséquent, un nœud peut rejoindre ou quitter le réseau en un temps très court, ce qui rend les changements de topologie très fréquent. De plus, des problèmes peuvent apparaitre quand le système IVC (*Inter Véhicular Communication*) n'est pas équipé dans la majorité des véhicules.

6.4 Géolocalisation

Un service de positionnement géo-spatial autonome et précis est nécessaire au bon fonctionnement de la plupart des applications déployées sur les réseaux VANETs. Avec un faible coût des récepteurs et une couverture importante, le système de positionnement par satellites (GNSS) est plus attractif que les systèmes de localisation basés sur les radars, capteurs ultrasons, ou cameras. De plus, les satellites GNSS proposent une horloge commune globale et un système de coordonnées terrestres commun pour les applications distribuées sur de nombreux véhicules. Ces avantages font que GNSS est une technologie de positionnement précise et adaptée pour les systèmes DSRC. Un exemple bien connu du système GNSS est le GPS (*Global Positioning System*). La précision actuelle des récepteurs GPS intégrés dans les véhicules est de l'ordre de 10-15 mètres. Cette précision n'est acceptable que pour le guidage. Pour les applications de sécurité routière, cette précision doit être améliorée. C'est un domaine de recherche actif, ou de nombreux travaux sont conjointement développes par le milieu académique et industriel.

6.5 Environnement de communication

Si les environnements de communication des réseaux sans fil traditionnels se résument généralement a des espaces complètement ouverts et sans obstacle, les réseaux véhiculaires imposent la prise en compte d'une plus grande diversité environnementale. Du fait de la mobilité de véhicules, il est possible de passer d'un environnement urbain à un environnement autoroutier présentant des caractéristiques radicalement différentes. Il est également nécessaire de prévoir une volatilité des conditions climatiques et des contraintes topologiques. Cet environnement de communication conduit à des modèles de propagation d'ondes complexes.

7. Technologie d'accès

Afin de déployer les applications, nous faisons un tour d'horizon des technologies de communication sans fil existantes. Ce tour d'horizon permet de présenter les caractéristiques des technologies envisagées pour les VANETs. Il existe deux types de système possible :

- Les systèmes intra-véhiculaires composés de capteurs internes au véhicule et ne visant pas à diffuser de l'information vers l'extérieur du véhicule.
- Les systèmes extra-véhiculaires visant à l'échange d'informations entre une entité et son environnement**.**

7.1 Système de communications intra-véhiculaires

Nous définissons les systèmes intra-véhiculaires comme des systèmes ne visant pas à la diffusion d'information à l'extérieur du véhicule. Les systèmes intra-véhiculaires sont

composés de capteurs, d'une plateforme de calcul et de réseaux filaires (CAN) ou sans fil (Bluetooth, Wifi). Ces systèmes ont été les premiers développés par les industriels. Chaque constructeur pouvait définir son propre système sans devoir assurer l'interopérabilité avec les véhicules des marques concurrentes. Ces systèmes sont connus sous le nom de systèmes avances d'aide à la conduite (ADAS).

7.2 Système de communications extravéhiculaires

7.2.1 Système de télécommunication

Les systèmes de télécommunications sont également connus sous le nom de réseaux cellulaires mobiles. Cette section traite les standards de télécommunications dominants en Europe : GSM et son extension GPRS, et UMTS (3G). L'architecture réseau d'un système de télécommunications contient une station de base qui contrôle l'accès au support et gère le processus d'itinérance (handover).

7.2.2 Système de radio diffusion

Les systèmes de radiodiffusion numérique proposent de diffuser l'information depuis la station de base jusqu'aux utilisateurs. C'est donc un système unidirectionnel. Leur avantage est que les véhicules reçoivent la même information au même moment. Cette section présente trois standards pour la diffusion mobile : RDS/TMC, DAB/DMB, et DVB-T/DVB-H.

8. Standards de communication VANET

L'IEEE a étendu sa famille de protocoles 802.11 en ajoutant le 802.11p [9], s'inspirant pour cela du standard ASTM (*American Society for Testing and Materials*) E2213-03 [10], lui-même basé sur le 802.11a [11]. Ce protocole modifie la couche physique et la couche MAC pour s'adapter aux réseaux de véhicules, en conformité avec la bande DSRC. En complément, l'IEEE a défini la famille de protocoles 1609, dite WAVE, pour l'accès sans fil dans les réseaux de véhicules. Ce standard, structure en quatre composantes (1609.1 à 1609.4), définit l'architecture, le modèle de communication, la structure de gestion, la sûreté et l'accès physique. Comme l'illustre la Fig. 1.5, 802.11p et WAVE spécifient une pile protocolaire complète. Le modèle DSRC/WAVE utilise deux piles. Une pile pour les applications de sécurité routière et une plus classique pour les deux autres catégories d'applications.

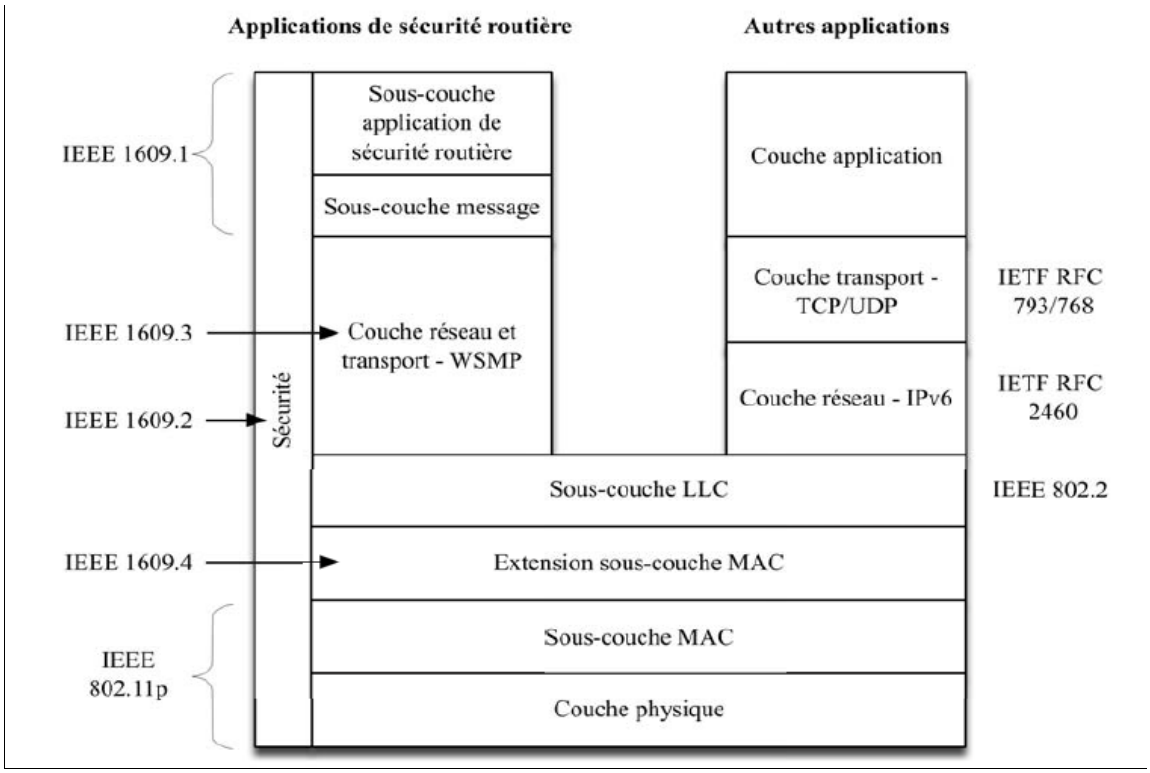

Fig. 1.5 : Le modèle DSRC/WAVE : IEEE 1609 [11]

8.1 IEEE 1609.1

Le standard IEEE 1609.1 se positionne au niveau de la couche application et définit les formats de messages et le mode de stockage des données utilisées par la couche application. Ce standard définit un gestionnaire de ressources qui autorise des applications de l'équipement de bord de route (RSU) à communiquer avec les *On-Board Units* (OBU) des véhicules à proximité.

8.2 IEEE 1609.2

Le but de ce standard est de définir le format des messages sécurisés pour le système DSRC/WAVE. Le standard spécifié les méthodes pour sécuriser les messages de gestion d'applications. Il décrit aussi les procédures que doit accomplir le véhicule afin d'assurer les services de sécurité tels que l'authenticité, la confidentialité, l'intégrité, ou la non-répudiation.

8.3 IEEE 1609.3

Le standard 1609.3 définit le WSM (*WAVE Short Message)* et le protocole d'échange associe WSMP *(WAVE Short Message Protocol*) afin d'assurer les fonctionnalités des couches réseau et transport pour les applications de sécurité routière. Le 1609.3 définit aussi le message WSA (*WAVE Service Advertisement*) qui est utilisé pour annoncer la disponibilité de services DSRC à une localisation donnée. Un WSA peut par exemple être envoyé pour annoncer la présence d'un service d'information trafic offert par un RSU.

8.4 IEEE 1609.4 et IEEE 802.11p

Le standard IEEE 802.11p définit la couche physique du système DSRC. La technologie DSRC est définie dans la bande de fréquence des 5.9 GHz sur une largeur de bande totale de 75 MHz (5.850 GHz – 5.925 GHz). Comme illustrée par la Fig. 1.6, cette largeur de bande est segmentée en 7 canaux de 10 MHz chacun. Ces canaux se répartissant fonctionnellement en 1 canal de contrôle (CCH) et 6 canaux de service (SCH), chacun pouvant offrir des débits allant de 6 à 27 Mbit/optionnellement, des canaux peuvent être configures sur une largeur de bande de 20 MHz, ce qui permet d'obtenir des débits pouvant aller jusqu'à 54 Mbit/s. La portée de transmission d'un système DSRC peut atteindre 1000 mètres.

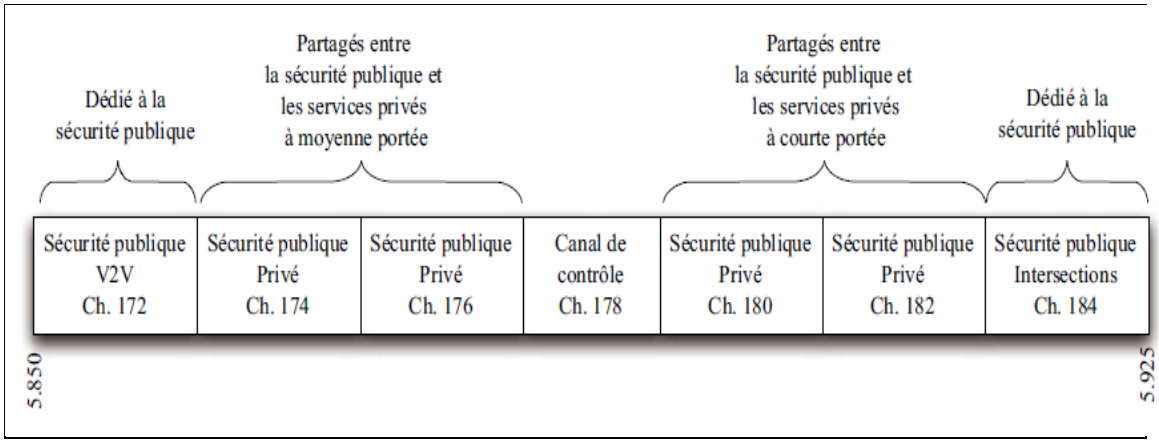

Fig. 1.6 : Canaux du standard IEEE 802.11p [11]

Conclusion

Dans ce chapitre, nous avons montré que les architectures de communications véhiculaires qui permettent d'améliorer d'une part la sécurité routière grâce aux messages échangés entre les véhicules, et de rendre d'autre part les routes plus agréables grâce à la diversité des services offerts.

Dans le chapitre suivant, nous allons illustrer les attaques sur les VANETs, et nous présentons les mécanismes qui ont été mis en œuvre afin d'améliorer la sécurité de ces réseaux.

Chapitre 2 : Sécurité des réseaux VANET

Introduction

Les applications de sécurité du trafic routier, présentées dans le chapitre 1, utilisent les messages d'alerte pour informer le conducteur de situations potentiellement dangereuses (conditions de route dégradées, freinage d'urgence d'un autre véhicule, obstacle, etc.). Si ces alertes sont envoyées à tort, ou à outrance, alors l'utilisateur n'y prêtera plus d'attention. L'alerte elle-même peut devenir une menace, et provoquer des accidents à cause des

réactions (inutiles, inappropriées, inadaptées) des utilisateurs. Ainsi, un attaquant pouvant injecter des messages falsifiés dans les VANETs, pourra causer la ≪ désensibilisation ≫ de l'utilisateur ou des accidents, contrairement à l'objectif d'amélioration du trafic routier. Ce dysfonctionnement peut aussi venir d'un équipement défectueux qui génèrerait des informations erronées. Par exemple, un capteur peut détecter un obstacle sur la route, alors qu'il s'agit simplement d'une obstruction partielle du capteur. Devant la criticité d'utilisation des VANETs, les mécanismes de sécurité doivent donc adresser deux types de problèmes : le dysfonctionnement ou l'utilisation malveillante.

Dans ce chapitre. Nous déterminons pour pouvoir sécuriser un VANET, il est nécessaire de connaitre les menaces possibles. Ainsi, nous détaillons les modèles d'attaquant et les attaques possibles. Pour s'en prémunir, des services de sécurité sont nécessaires. Nous les présentons avec les mécanismes de sécurité associés.

1. Sécurité des réseaux sans fil ad hoc

Comme les réseaux VANET sont partie des réseaux sans fil ad hoc. Dans cette section, nous nous intéressons à la sécurité des réseaux sans-fil ad hoc de manière générale, nous présentons quelques exemples d'attaques sur ces réseaux, ensuite nous en décrivons les objectifs de sécurité et les mécanismes de sécurité.

1.1 Quelques exemples d'attaques

Les réseaux sans fil ad hoc peuvent subir plusieurs attaques à cause des failles de sécurité au niveau du support de transmission, nous citons quelques exemples d'attaque :

1.2 Attaque man in the middle (l'homme au milieu)

C'est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties. La plupart des attaques de type « *man in the middle* » consistent à écouter le réseau à l'aide d'un outil appelé sniffer.

1.3 Ecoute des communications

Dans ce type d'attaque, entité malveillante écoute le trafic de réseau pour extraire et déduire les informations échangées sur le canal. Ces informations sont très variées et peuvent comprendre par exemple (courriers, fichiers…etc.).

1.4 Accès non autorité

Dans cette attaque, l'entité malveillante accède au service du réseau sans en avoir les droits ou les privilèges.

1.5 Le déni de service (*Denial of Service "DoS")*

Ce type d'attaque regroupe l'ensemble des actions malveillantes au niveau applicatif ou au niveau des couches inférieures de la pile protocolaire visant à empêcher la fourniture régulière des services dans le réseau. Il peut comprendre le brouillage du canal radio pour bloquer les transmissions, l'injection massive de paquets visant à épuiser les ressources des terminaux ou du réseau ou encore l'exploitation des vulnérabilités des protocoles. La multiplicité des formes que peuvent prendre ces attaques fait qu'elles sont parmi les plus difficiles à contrer.

2. Objectifs fondamentales de la sécurité

Nous présentons dans cette section les principaux objectifs de sécurité, nous citons :

- **L'authentification:**

Cet objectif de sécurité permet aux entités du réseau de s'assurer de la bonne identité ou du bon droit des entités avec lesquelles elles communiquent.

- **La non-répudiation:**

Cet objectif de sécurité permet de prouver l'origine des données. Il est donc atteint lorsque tout émetteur de message dans le réseau ne peut nier avoir émis ledit message. Ainsi la non répudiation va permettre d'identifier les entités malveillantes qui seraient tentées de commettre des actes répréhensibles pour ensuite ne pas les reconnaître.

- **La confidentialité:**

Cet objectif de sécurité garantit que seules les parties autorisées peuvent accéder aux données transmises via le réseau, il s'agit de données de la couche applicative ou de données des couches inférieures.

- **L'intégrité:**

Cet objectif de sécurité permet de s'assurer que les communications ne sont pas modifiées ou altérées par des entités non-autorisées. Ainsi, toute manipulation de données est détectée et les paquets correspondants invariablement rejetés.

- **La disponibilité:**

Cet objectif de sécurité garantit que toute entité autorisée puisse accéder aux ressources du réseau avec une qualité de service adéquate.

3. Mécanismes de sécurité

- **Cryptographie**

La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages en employant souvent des secrets ou des clés. Elle consiste à appliquer des

transformations sur le contenu d'un message à l'aide des algorithmes de chiffrement (afin de l'en rendre incompréhensible) et de déchiffrement (afin de reconstruire le message original).

- **La cryptographie symétrique (ou cryptographie à clé secrète)**

Elle consiste à utiliser une seule clé secrète partagée entre l'expéditeur et le destinataire pour chiffrer et déchiffrer les données.

- **La cryptographie asymétrique (ou cryptographie à clé publique)**

Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.

- **Le hachage**

Il consiste à déterminer une information de taille fixe et réduite (appelée l'empreinte ou le condensé) à partir d'une donnée de taille indifférente. Une fonction de hachage est dite à sens unique ou fonction irréversible et fournit l'empreinte à partir d'une chaine donnée en entrée. L'irréversibilité signifie qu'il est aisé de calculer l'empreinte d'une chaine donnée, mais il est difficile de retrouver ou déduire la chaine initiale à partir de l'empreinte.

- **La signature numérique**

C'est un code numérique associé à un message électronique afin que les destinataires puissent en authentifier les origines et en vérifier l'intégrité. Son implémentation fait appel aux fonctions de hachage et l'utilisation de la clé privée du signataire.

- **Le certificat numérique**

C'est une structure de données permettant de prouver l'identité du propriétaire d'une clé publique. Les certificats numériques sont signés et délivrés par un tiers de confiance appelé l'autorité de certification (AC).

- **Infrastructures à clés publiques**

Une infrastructure à clés publiques est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériels), de procédures humaines (vérifications, validation) et de logiciels (système et application) qui permettent de délivrer, révoquer, renouveler, et de façon générale gérer les certificats numériques .

4. La sécurité dans les VANETs

Nous donnons dans cette section, une classification générique des attaques recensées ou à venir dans les réseaux véhiculaires.

4.1 Taxonomie des attaques

La sécurisation des réseaux véhiculaires passe par la détermination d'une typologie des attaques dans ces réseaux. Compte tenu de la diversité des applications que l'on peut y opérer et de celle des environnements d'opération, il est aisé d'imaginer que ces réseaux feront l'objet de nombreuses attaques dont certaines pourront même relever du terrorisme. Nous définissons 4 grandes déclinaisons pour toute attaque dans ces réseaux:

- **Interne ou Externe:**

Une attaque est dite interne si elle est instiguée par une entité identifiée comme légitime par les autres nœuds du réseau. De manière courante, une entité sera déclarée légitime si elle est authentifiée dans le réseau. Les attaques internes font partie des attaques les plus dangereuses puisque l'attaquant est injustement considéré comme étant de confiance et a généralement accès aux services du réseau. Une attaque externe est, quant à elle, menée par une entité a priori considérée et reconnue comme illégitime. L'attaquant dans ce cas n'est généralement pas authentifié dans le réseau et n'a pas accès aux services de ce réseau. Il est donc de ce fait limité dans la diversité des attaques qu'il peut entreprendre.

- **Intentionnelle ou Non intentionnelle:**

Une attaque est dite intentionnelle si elle est instiguée par une entité malveillante visant délibérément à remettre en cause le bon fonctionnement du réseau. Ce type d'attaque est à distinguer d'une attaque non intentionnelle ou involontaire qui peut par exemple être le fait d'une erreur de transmission radio ou d'une erreur protocolaire dans le réseau.

- **Active ou Passive:**

Une attaque est dite active lorsque l'attaquant injecte, modifie ou supprime du trafic dans le réseau. A contraire, dans une attaque passive, l'attaquant ne fait qu'écouter et collecter le trafic pour une éventuelle utilisation malveillante ultérieure.

- **Indépendante ou Coordonnée:**

Une attaque est dite indépendante lorsqu'elle est menée de manière isolée par un seul attaquant. Elle est en revanche dite coordonnée lorsque plusieurs attaquants partageant la même information se concertent pour la mener.

4.2 Attaques de base

L'attaque délibérée ou non d'un VANET repose sur un but précis. Nous dressons une liste des attaques évidentes ou faisables et qui constituent un risque non négligeable en cas de réalisation. En raison de l'impossibilité d'envisager toutes les attaques possibles dans les réseaux véhiculaires, nous nous limitons aux exemples les plus significatifs dans notre contexte.

- **Attaque sur la vie privée :**

Dans cette attaque, l'entité malveillante essaie d'obtenir l'identité ou des informations personnelles d'un utilisateur du réseau. Cela peut également se traduire par tracer l'activité et les déplacements de cet utilisateur. Pour identifier et tracer une victime, l'attaquant peut utiliser toute chaine de caractères identificatrice dont la récurrence est constatée dans les échanges de la victime. Cette chaine de caractères peut être une adresse IP, une adresse MAC, des informations d'identification d'un certificat, etc. Au-delà des chaines de caractères, l'empreinte radio de la victime peut également être utilisée: on parle alors d'attaque de la couche physique. D'après les modèles d'attaquants, l'attaquant peut être Interne ou Externe, Mal intentionné, Passif et Indépendant.

- **Attaque sur la cohérence de l'information :**

Dans cette attaque, l'entité malveillante porte atteinte à la cohérence des informations acheminées dans le réseau en les modifiant ou en injectant des informations erronées. L'intention de l'attaquant est d'altérer la perception qu'ont ses victimes des conditions de circulation (position, vitesse, direction). Ce faisant, l'attaquant peut par exemple provoquer un changement d'itinéraire de ses victimes. La Fig. 2.1 qui illustre ce cas, un attaquant (M) diffuse des informations de trafic erronées amenant les victimes A et B à changer de voie. Dans cette attaque, l'attaque est Interne, Intentionnelle, Active et Indépendante.

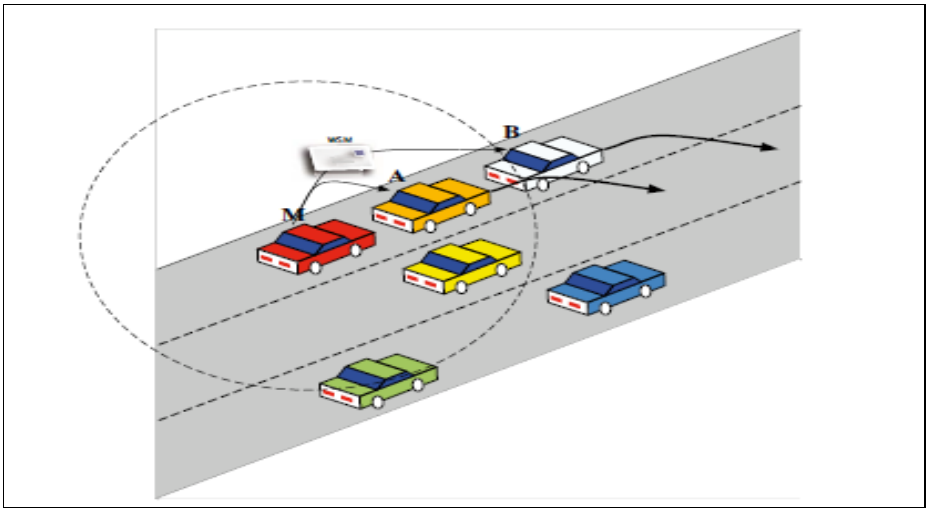

Fig. 2.1 : Attaque sur la cohérence de l'information [12]

- **Usurpation d'identité ou de rôle :**

Dans cette attaque, l'entité malveillante utilise une fausse identité ou de fausses lettres de créance pour se faire passer pour une entité légitime ou pour jouir des privilèges de cette dernière. La Fig. 2.2 illustre un cas ou l'attaquant M usurpe l'identité du véhicule A pour récupérer des données du véhicule B. L'attaquant peut être Interne ou Externe, Malicieux ou Rationnel, Mal intentionné, Actif et Indépendant.

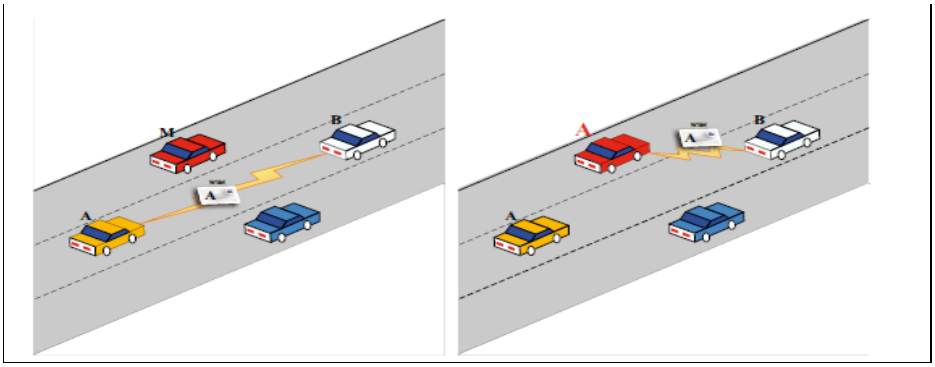

Fig. 2.2 : Usurpation d'identité ou de rôle [12]

- **Déni de service (DoS) :**

Dans ce type d'attaque, l'entité malveillante empêche l'accès normal aux services du réseau. Ce type d'attaque peut être généré en brouillant le canal radio, en surchargeant ou en épuisant les ressources du réseau par des requêtes abondantes, en exploitant la vulnérabilité des protocoles, ou en ayant une attitude non coopérative (refus de relayer des paquets par exemple). La Fig. 2.3 illustre une attaque par déni de service aboutissant à une collision, car l'attaquant M empêche l'échange de messages critiques entre le véhicule accidente B et le véhicule A. L'attaquant peut être Interne ou Externe, Mal intentionné, Actif et Indépendant.

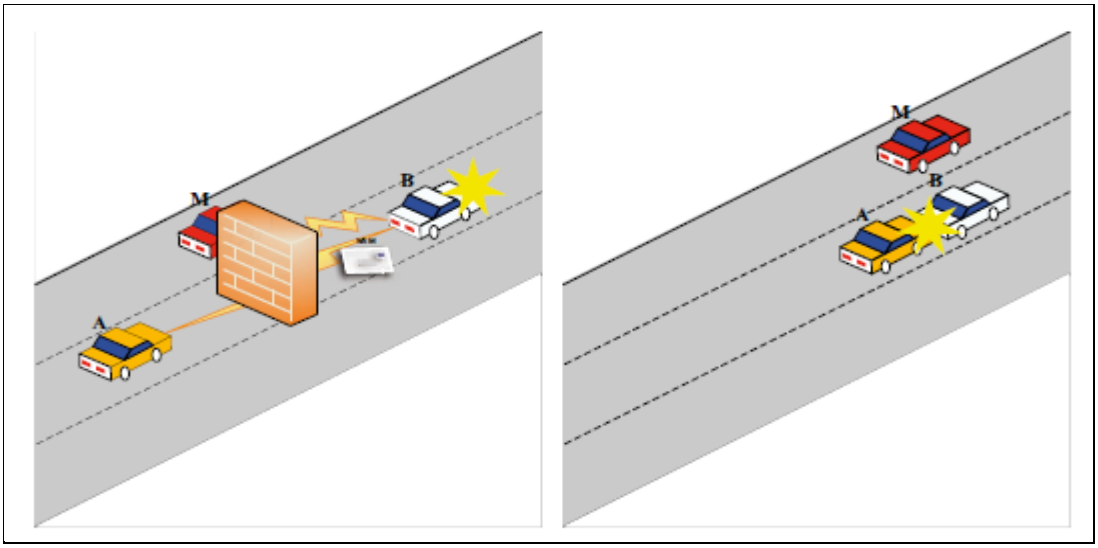

Fig. 2.3 : Déni de service [12]

- **Écoute clandestine du réseau :**

Dans cette attaque, l'entité malveillante collecte les données transmises dans le réseau afin d'en extraire une information dont elle pourrait tirer profit. Un exemple d'attaque est un attaquant qui espionne une transaction commerciale, typiquement un paiement électronique à un péage, en vue d'en extraire les informations bancaires. L'attaquant peut être Interne ou Externe, Mal intentionné, Passif et Indépendant.

4.3 Attaques complexes

Après avoir listé des attaques de base, nous présentons trois attaques complexes. Une attaque complexe est une combinaison d'attaques de base.

- **Véhicule caché :**

C'est un exemple de falsification des informations de positionnement, et une variante du << *Sybil attaque*>>[1]. Dans le protocole de distribution des messages d'alerte, si un véhicule diffusant l'alerte détecte un voisin mieux positionné que lui pour diffuser, alors il arrête d'émettre. Ce protocole permet de réduire la congestion du canal radio. La Fig. 2.4 illustre cette attaque. L'attaquant M fait donc croire qu'il est en meilleure position (M') afin d'être le seul à émettre l'alerte. Mais il ne va pas diffuser l'information d'alerte, rendant le véhicule en danger B cache des autres véhicules (A).

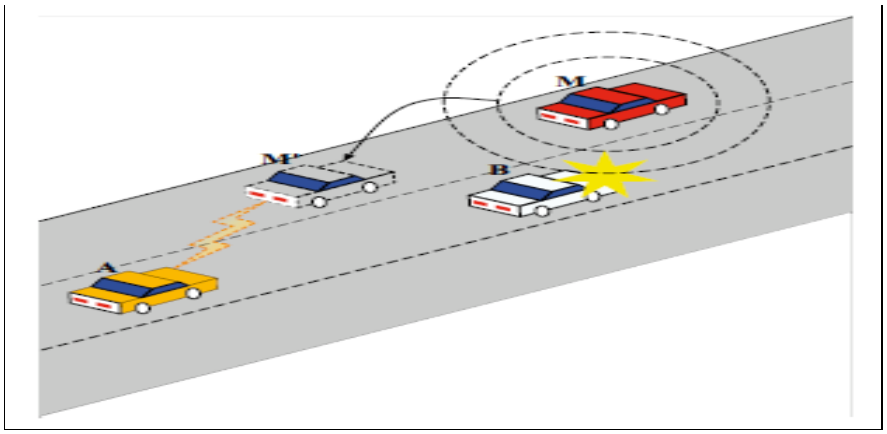

Fig. 2.4 : Attaque du véhicule caché [12]

- **Tunnel :**

Comme le signal GPS connait des pertes (dans un tunnel ou dans certaines zones perturbatrices), un attaquant peut exploiter cette perte de positionnement temporaire. En effet, il peut envoyer de fausses données dès la sortie du tunnel avant que le véhicule victime ne reçoive une mise à jour de position authentique.

- **Wormhole :**

Un attaquant qui contrôle plusieurs entités éloignées, peut établir un tunnel entre ces entités et peut ainsi injecter des données d'un endroit à l'autre. Il diffuse ainsi des informations erronées (mais signées) a divers endroits. C'est un exemple d'attaque étendue.

[1] Sybil attaques ont été considérés comme une menace dangereux à la sécurité des réseaux ad hoc

4.4 Les éléments de base de la sécurité dans les VANETs

4.4.1 Les certificats dans les VANETs

Pour assurer les objectifs de sécurité dans ces réseaux, des outils cryptographiques doivent être mis en œuvre. La cryptographie asymétrique présente des solutions possibles pour les VANETs et parait plus adéquate aux caractéristiques et exigences de ces réseaux. En effet, grâce à la cryptographie asymétrique, il est possible d'utiliser des certificats numériques pour identifier les véhicules de façon unique.

Dans les VANETs il existe deux types de certificats :

- **Le certificat à long terme :**

Chaque véhicule doit avoir un certificat indiquant le véhicule et son propriétaire de manière permanente **;** ce type de certificat contient d'autres informations en plus comme celles concernant les caractéristiques des équipements du véhicule. Il peut être utilisé pour établir une communication sécurisée avec l'AC (Autorité de confiance) et renouveler les certificats à court terme.

- **Le certificat à court terme :**

Comme son nom l'indique, la durée de vie de ce certificat est très courte (d'environ une minute); il ne doit pas contenir les informations indiquant le propriétaire du véhicule; à cet effet il utilise un pseudonyme qui permet d'identifier le véhicule de façon unique. Ce type de certificat est utilisé généralement dans les protocoles de routage.

Il faut souligner que chaque véhicule possède un seul certificat à long terme et plusieurs certificats à court terme. Ainsi, toutes les clés privées correspondantes aux clés publiques sont stockées dans le TPD[2], donc le TPD doit avoir une grande capacité de stockage afin que les véhicules puissent communiquer de manière sécurisée même en absence de connectivité avec l'AC pour des périodes très longues.

4.4.2 La sécurité du système de balisage

Le balisage (en anglais *Beaconing*) consiste en la diffusion périodique aux voisins à un saut d'un paquet spécifique contenant des informations utiles pour les applications ou les protocoles exécutés au niveau des nœuds voisins. Généralement, les informations incluses dans les balises (en anglais *Beacons*) comprennent des informations sur le nœud tels l'identifiant, les coordonnées géographiques et la vitesse de déplacement. La fréquence des balises varie de 1HZ à 10HZ dans la plupart des cas.

Afin de sécuriser l'opération de balisage, chaque nœud V calcule la signature numérique sig(E, m) sur les différents champs du paquet (m dénote les champs qui correspondent aux

[2] C'est un dispositif considéré comme inviolable utilisé pour stocker les informations sensibles comme les clés privées et toutes informations confidentielles, et chargé de signer les messages sortants.

informations énoncées ci-dessus et E l'entête du paquet) à envoyer en utilisant sa propre clé privée CPrV qui correspond à sa clé publique CPuV. La signature numérique sig(E, m) est ensuite ajoutée au message qui sera envoyé conjointement avec son propre certificat numérique CRTV. Les nœuds recevant ce message peuvent authentifier la source du message grâce à la clé publique CPuV incluse dans le certificat numérique CRTV [13]. Format d'un paquet beacon est illustré dans la figure ci-dessous.

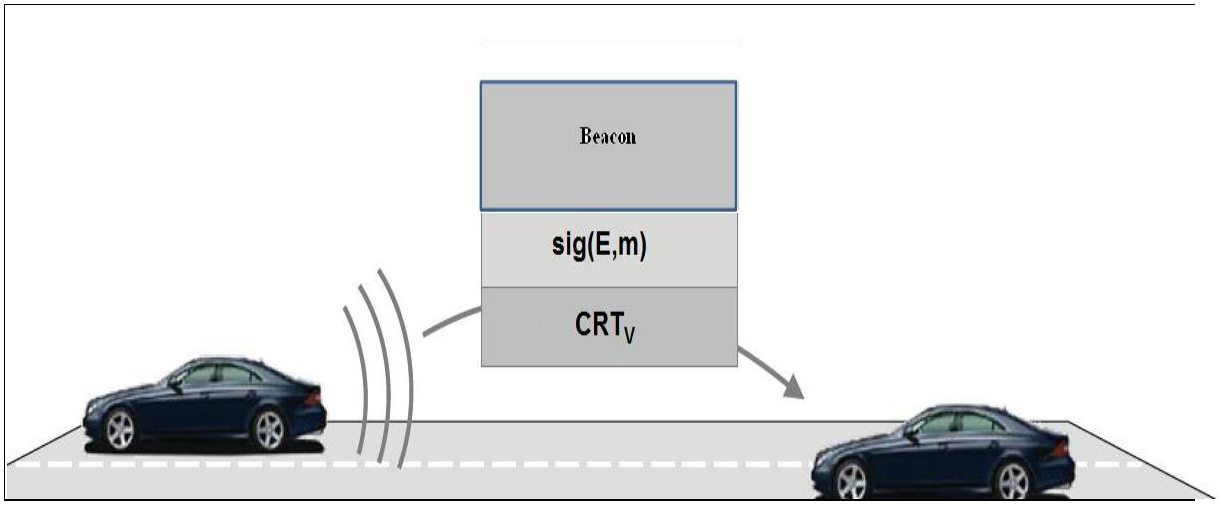

Fig. 2.5 : Format d'un paquet beacon.

4.5 Protocoles de diffusion des messages de sécurité

Les protocoles de diffusion jouent un rôle important dans les réseaux véhiculaires car ils sont conçus pour communiquer des messages importants pour la sécurité routière. L'inondations est généralement utilisée dans les VANETs pour diffuser des messages à tous les véhicules à plusieurs sauts loin de la source. La radiodiffusion dans les VANETs utilisant l'information locale a été largement étudiée dans la littérature. La plupart de ces contributions permettent de réduire la charge de la diffusion et améliorer les performances en terme de taux de livraison de paquets.

4.5.1 Objectifs et contraintes

Les différents objectifs pour résoudre ce problème sont :

- Minimiser le temps de réception des messages de tous les véhicules de la zone de danger.
- Maximiser la portée de transmission de chaque véhicule pour l'envoi des messages.
- Minimiser le nombre de sauts avant la réception des messages.

Pour cela, différents facteurs internes au véhicule entreront en compte pour réaliser ces objectifs :

- La vitesse actuelle du véhicule
- Les coordonnées GPS du véhicule
- Le sens du véhicule

- La portée de transmission du véhicule

D'autres facteurs liés au problème en lui-même seront abordés plus tard comme tout problème, il y a certaines contraintes que l'on prendre en compte pour le résoudre. Tout d'abord la première de ces contraintes est la portée de transmission du message. En effet, plus la portée de transmission du véhicule est grande plus il y a de chances qu'il y ait des interférences avec les ondes radio et que cela ait une incidence sur l'envoi du message (dans le pire des cas il ne l'envoi pas) ou sur la qualité du message reçu (le véhicule qui reçoit le message peut ne pas avoir reçu toutes les informations nécessaires). C'est pour cela qu'il est primordial de ne pas régler la portée de transmission à sa puissance maximale. Ensuite une autre de ces contraintes est le nombre de sauts avant la réception d'un message par un véhicule. En effet, plus le nombre de sauts pour recevoir le message est grand, plus le temps pour le recevoir est grand puisqu'il faut passer par plusieurs véhicules intermédiaires pour recevoir ce message. Il faut donc trouver un compromis entre la portée de transmission du message et le nombre de sauts requis pour recevoir les messages. Une fois que les contraintes ont été respectées, il suffit de trouver toutes les solutions du problème sous forme d'arbres de diffusion et de choisir la plus optimale [14].

4.5.2 Description du problème

- **Modélisation du problème**

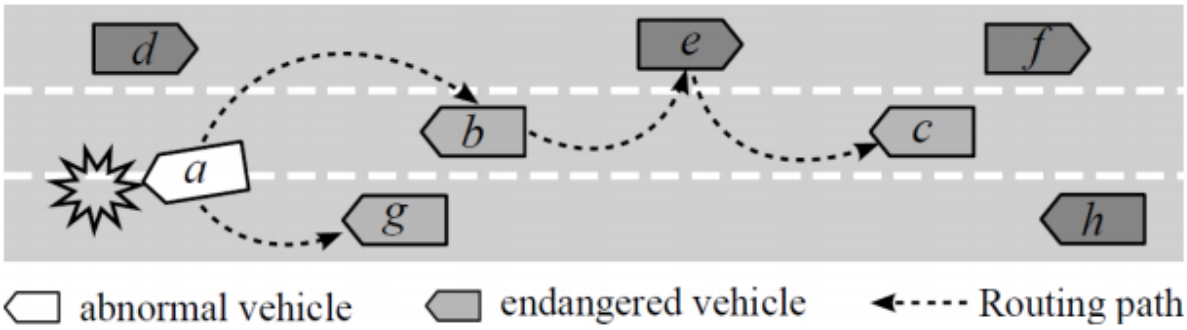

Fig. 2.6 Présentation véhicule en danger [15]

Les interactions entre plusieurs véhicules peuvent être modélisées dans un graphe orienté G = (V, E) où V est l'ensemble des nœuds représentant les véhicules et E l'ensemble des arcs orientés représentant les interactions entre les véhicules. Une interaction est considérée comme un état dans lequel deux véhicules ont une influence entre eux. Le graphe représente les interactions entre plusieurs véhicules dans une région spécifique et à un temps spécifique. Par exemple, soient 2 véhicules v1 et v2, l'interaction entre eux ces 2 véhicules peut être : le véhicule v1 peut mettre en danger le véhicule v2, ou le contraire, ou les 2. Un arc appartenant à l'ensemble E représente l'interaction entre v1 et v2, où v1 influence v2.

- **Source du message**

Le nœud source est défini comme un véhicule qui a besoin d'envoyer des messages d'avertissements. Il existe 2 cas où un véhicule a besoin d'envoyer des messages d'avertissements :

- ✓ Il n'y aucun changement soudain d'état du véhicule ou d'évènements inattendus survenant sur le véhicule. Un changement d'état soudain du véhicule peut être défini comme des changements de mouvement qui excèdent un certain seuil, comme un freinage d'urgence, changé de direction brusquement …, etc. Les évènements inattendus sont d'autres facteurs dangereux qui peuvent causer un accident, comme une panne d'un véhicule, une panne de freins, ou autre disfonctionnements du véhicule.
- ✓ Le système d'avertissement prédit une collision inévitable avec d'autres véhicules basée sur le mouvement actuel des autres véhicules. Il est possible que la collision arrive sans aucune manœuvre soudaine, par exemple dans un véhicule, si le véhicule de tête roule plus lentement que celui de derrière, ils entreront éventuellement en collision. Ce genre d'accident est le plus souvent causé par des conducteurs négligents.

- **Récepteurs du message**

Les nœuds récepteurs sont des véhicules qui seront mis en danger par le véhicule « anormal » (ou le véhicule qui est la source du message).

- **Contrainte de délai pour chaque nœud récepteur**

Un nœud récepteur est un véhicule potentiellement en danger qui peut entrer en collision dans une certaine limite de temps. La collision peut être évitée si les véhicules en danger effectuent une manœuvre d'urgence avant un temps limite. Le temps limite est le temps maximal pour chaque véhicule en danger de recevoir le message d'avertissement pour éviter le danger qui peut être utilisée comme une contrainte de temps.

- **Distance entre deux véhicules et portée de transmission**

Un récepteur peut recevoir un message si celui-ci est dans la zone de couverture de la source.

- **Délai total de transmission**

Le délai total atteint par un message envoyé d'un nœud source à n'importe quel récepteur est la somme des délais de chaque nœud entre la source et le récepteur. Cela dépend du nombre de nœuds intermédiaires entre eux et le délai atteint à chaque nœud intermédiaire.

Conclusion

Dans ce chapitre, nous avons présenté la problématique de la sécurité des réseaux sans fil dans le contexte des réseaux véhiculaires, nous avons montré à travers le prisme de leurs caractéristiques spécifiques - notamment leurs caractéristiques applicatives - et de quelques exemples d'attaques, que les exigences et les défis de sécurité ne s'y posaient pas nécessairement de la même manière selon que l'on traite les services ITS ou les services non- ITS. Ces différents défis et exigences de sécurité ont été passés en revue en mettant chaque fois en lumière quelques pistes susceptibles de concourir à leur mise en œuvre.

Nous avons aussi présenté les attaques et les solutions de base pour sécuriser la diffusion des messages échangés entre les véhicules. Nous avons prouvé sur comment les messages de sécurité sont-ils envoyés du véhicule source jusqu'à tous les véhicules situés à l'intérieur de la zone de danger. Dans le chapitre suivant, nous présenterons notre propre simulation sur différents métriques.

Chapitre 3 : Simulation et analyse

Introduction

Les réseaux informatiques connaissent une expansion importante grâce à plusieurs moyens qui ont pu se développer au cours du temps, donc il est couteux de déployer un banc d'essai complet contenant plusieurs ordinateurs, des routeurs et des liaisons de données pour valider et vérifier un protocole de réseau ou un certain algorithme spécifique. C'est pour cela que les simulateurs de réseaux sont utilisés. Les simulateurs d'un réseau offrent beaucoup d'économie, de temps et d'argent pour l'accomplissement des taches de simulation et sont également utilisés pour que les concepteurs des réseaux puissent, tester les nouveaux protocoles ou modifier les protocoles déjà existants d'une manière contrôlée et productrice. La problématique étudiée dans ce mémoire étant la simulation de réseau VANET, et en particulier les messages beacon avec certificat et signature.

1. Choix de simulateur

Parmi les simulateurs les plus connus nous choisissons le simulateur ns-3 pour réaliser notre travail. Le simulateur ns-3 est un simulateur réseau, utilisant des scripts écrit en C++ ou en Python. Nous avons choisis de travaillé avec ce simulateur pour la simple raison que ce simulateur possède des scripts dont nous pouvons les utilisés n'importe quand contrairement aux autres simulateurs, par exemple le simulateur OPNET est un simulateur qui n'est pas gratuit.

1.1 Présentation du simulateur ns-3

Le simulateur ns-3 vise à remplacer ns-2, écrit en C++, python et OTcl (version orientée objet de Tcl), pour tenter de remédier à ses limites (l'utilisation de multiples interfaces sur un nœud..). Il peut être utilisé sur les plateformes Linux/Unix, Mac et Windows. Son développement a d'abord commencé en juillet 2006, et devait durer quatre ans, il est financé par les instituts comme l'université de Washington, Georgia Institue of Technologie et le Centre de l'ICSI pour la recherche sur Internet, la première version majeure publique et stable a été publié en juin 2008. Les développeurs de ns-3 ont décidé que l'architecture de simulation devait être remaniée complétement en partant du Zéro. Dans cette optique, l'expérience tirée de ns-2 doit être associé avec les progrès des langages de programmation et du génie logiciel. L'idée de la rétrocompatibilité avec ns-2 a été abandonnée dès le départ. Cela libère ns-3 de contraintes héritées de ns-2 et permet la construction d'un simulateur qui est bien conçu depuis de début [16].

1.2 Terminologie et abstraction

Il est important de bien comprendre le sens des termes employés au sein du simulateur, ainsi que les abstractions qui ont été faites. ns-3 utilisent des termes largement employés dans le domaine des réseaux, mais qui peuvent avoir une signification particulière au sein du simulateur. Voici les principaux :

- **Un nœud "Node"**

Il représente l'élément fondamental d'un réseau. La composition d'un nœud peut être gérée (l'ajout de composants, d'applications et de protocoles).

- **Une application "Application"**

Elle représente un code exécuté par un utilisateur. Ce code peut être nécessaire au déroulement d'une simulation. L'échange des paquets durant une simulation nécessite par exemple la description d'une application au sein des nœuds participants. Les applications peuvent être attachées à un nœud.

- **Un canal de communication "Channel"**

Channel est le lien qui relie les Net Devices installés dans les nœuds. Des spécialisations de cette classe sont définies, comme par exemple VANET Channel pour modéliser un réseau VANET.

- **Une interface de communication**

Elle est appelée NetDevice, qui modélise à la fois les équipements et les pilotes de communication. Des spécialisations sont fournies comme par exemple WAVE NetDvice qui peut être reliée à un WAVE Channel. S'il s'agit de connecter un grand nombre de nœuds pour un réseau. [16]

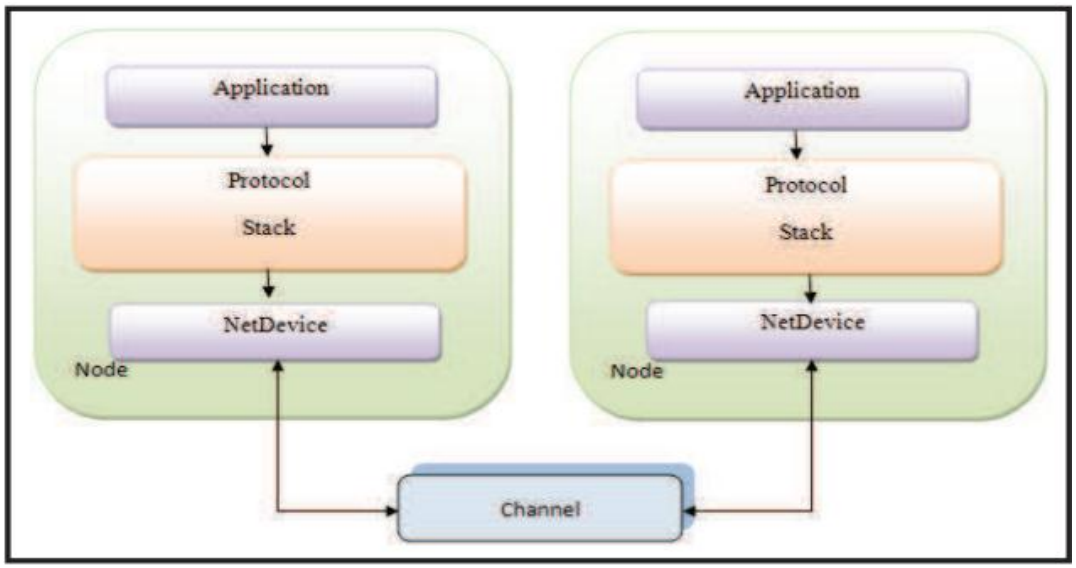

Fig. 3.1 Architecture d'un nœud ns-3 [16]

1.3 Installation du simulateur ns-3

Pour installer ns-3 nous devons avoir un environnement Linux, et cela se fait soit en installant linus directement sur la machine ou bien utiliser une machine virtuelle (VirtualBox ou VMware), alors nous pouvons utiliser directement le système d'exploitation Ubuntu, et nous pouvons suivre les étapes suivantes qui consistent à utiliser des commandes spécifiques pour télécharger et installer les différents packages nécessaires.

Ubuntu/Debian (Linux)

La liste des packages suivants doivent être téléchargée pour la version Ubuntu 12.04.

- Package pour C++, c'est le package minimal pour le besoin de l'installation de ns-3 :

$ sudo apt-get install gcc g++ python

- Package pour Python :

$ sudo apt-get install gcc g++ python python-dev

- Package pour Mercurial :

$ sudo apt-get install mercurial

- Package pour Bazar utilisé pour exécution des scripts Python sur ns-3 :

$ sudo apt-get install bzr

- Debugging :

$ sudo apt-get install gdb valgrind ·

- GNU Scientific Library (GSL) pour éviter les erreurs dans les modèles du réseau WiFI :

$ sudo apt-get install gsl-bin libgsl0-dev libgsl0ldbl

- Simulation réseau (NSC) nécessite l'analyseur lexical flex et générateur d'analyseur syntaxique bison :

$ sudo apt-get install flex bison libfl-dev ·

- Installation des paquets gcc et g++ de la dernière version.

$ sudo apt-get install g++-4.6 gcc-4.6

- Pour lire pcap paquet traces :

$ sudo apt-get install tcp dump

- Structure de support de la base de données

$ sudo apt-get install sqlite sqlite3 libsqlite3-dev

- Version xml-based :

$ sudo apt-get install libxml2 libxml2-dev ·

- configuration système GTK-based

$ sudo apt-get install libgtk2.0-0 libgtk2.0-dev ·

- Pour expérimenter ns-3 avec des machines virtuelles :

$ sudo apt-get install vtun lxc

- Support pour utils/check-style.py code style check program

$ sudo apt-get install uncrustify

- Document sur Doxygen et related inline :

$ sudo apt-get install doxygen graphviz imagemagick

- Support pour open flow module

$ sudo apt-get install libboost-signals-dev libboost-filesystem-dev ·

- Support pour MPI-based :

$ sudo apt-get install open mpi

Après toutes ces étapes nous allons maintenant passer à l'installation de ns-3, en commençant par le téléchargement du dossier ns-3 en utilisant les commandes suivantes :

- cd mkdir tarballs
- cd tarballs
- wget http://www.nsnam.org/release/ns-allinone-3.13.tar.bz2 ·
- tar xjf ns-allinone-3.13.tar.bz2

Pour l'installation de ns-3, nous allons utiliser la commande Build qui se trouve dans le répertoire ns-3.13 · ./build.py .

2. Animation

L'animation est un outil important pour la simulation d'un réseau. Alors que *ns-3* ne contient pas un outil d'animation graphique par défaut, il fournit une interface d'animation pour une utilisation avec des animateurs autonomes. Un tel animateur appelé NetAnim, soutenant actuellement l'animation de flux des paquets pour des liaisons point-à-point, a été développé. Les animateurs et les outils de visualisation autres sont en développement. [16]

- **NetAnim**

NetAnim est un programme autonome qui utilise les fichiers de trace sur commande générés par l'interface d'animation en affichant graphiquement la simulation. NetAnim est basé sur la plate-forme multi- Qt4 toolkit graphique . Il est illustré ci-dessous. Une capture d'écran de l'interface graphique NetAnim.

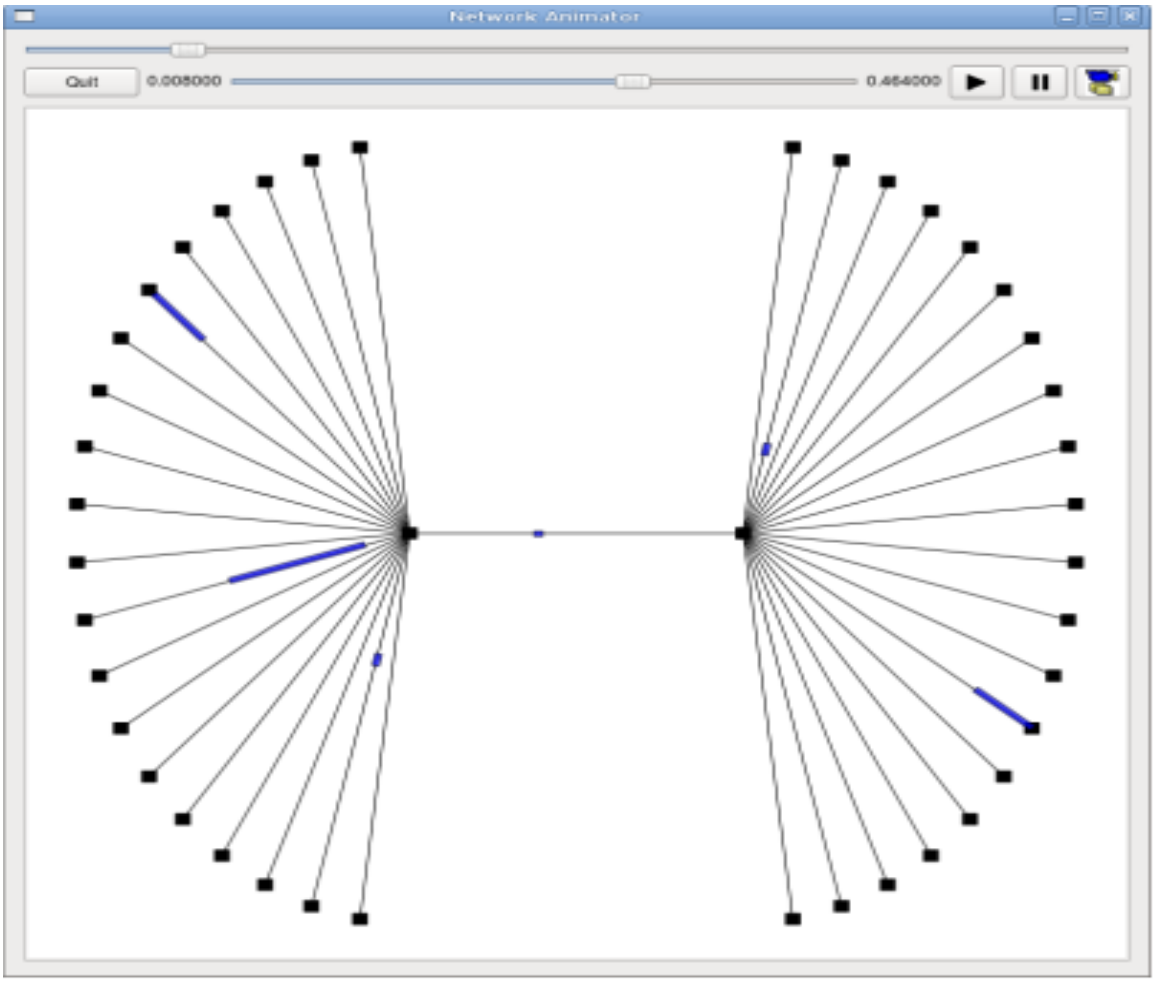

Fig. 3.2 NetAnim avec animation [16]

3. *Déroulement de la simulation*

Voici les démarches de déroulement d'une simulation, telles qu'illustrées à la Fig. 3.3. Premièrement, il faut définir le problème: comprendre et avoir une vue d'ensemble du problème (conception).

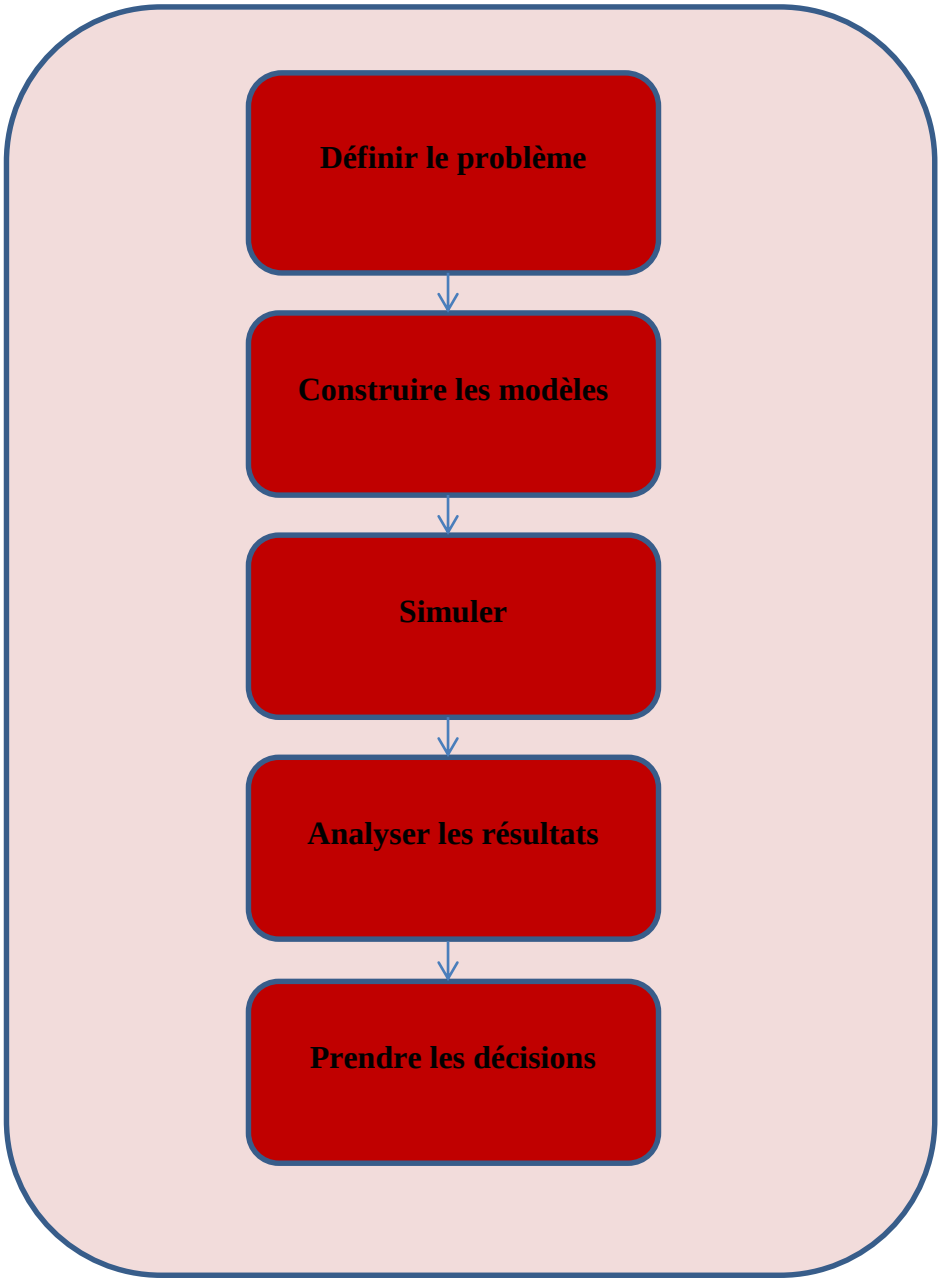

Fig. 3.3 Déroulement de simulation

Nos simulations ont été réalisées sous le simulateur NS-3 (version 3.22), qui possède un module qui permet de simuler le réseau VANET avec une variété de nombre des nœuds, ranges, paquet BSM. Nous avons ainsi utilisé l'Excel pour la représentation graphique de nos résultats.

4. *Modèle de mobilité Random Waypoint*

Ce modèle était d'abord utilisé par Johnson et Maltz dans l'évaluation du protocole de routage DSR et était ensuite raffiné par les mêmes auteurs. Le Random Waypoint est pour modéliser tous les scénarios dans lesquel, les nœuds se déplacent vers une destination, prennent un repos en arrivant, avant de se déplacer vers une autre destination et ainsi de suite. Dans ce modèle chaque nœud choisit aléatoirement, comme destination un point de coordonnées (x, y) dans la surface de simulation, et une vitesse entre *0* et *Vmax*. Le nœud voyage vers la destination choisie avec la vitesse choisie. A l'arrivée, le nœud prend un temps de repos avant de choisir une nouvelle destination et une nouvelle vitesse pour répéter le même processus. Des études ont été faites sur ce modèle puisqu'il est le modèle le plus utilisé dans les simulations dû à la facilité de son implémentation. Certaines études ont traité l'initialisation de ce modèle et le temps de convergence des simulations dans le cas où les nœuds commencent par prendre un temps de repos. On montre que le Random Waypoint, dans sa forme courante, n'atteint pas un état d'équilibre, mais plutôt que la vitesse diminue sans interruption pendant que la simulation progresse, ce qui peut fausser les résultats. Basés sur les analyses faites, les auteurs proposent une solution simple qui est de choisir une valeur strictement positive pour la vitesse minimale. Les auteurs montrent que 1000 s est une durée et elle n'est pas une vitesse du temps et elle n'est pas une vitesse de simulation pour converger, si la vitesse minimale est petite. Les auteurs montrent comment implémenter un générateur de modèle de mobilité équilibré pour le Random Waypoint, vu que, si les valeurs initiales de la position et de la vitesse sont choisies d'une distribution stationnaire, la convergence est immédiate. On remarque que le Random Waypoint est proche du Random Walk à la différence près que la destination choisie est toujours un point intérieur à la surface de simulation, ce qui élimine tout effet de bord. La Fig. 3.4 présente le déplacement d'un nœud utilisant le Random Waypoint [17].

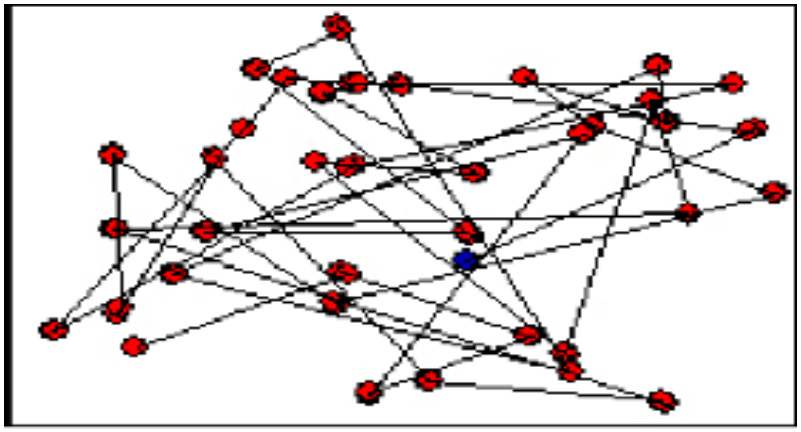

Fig. 3.4 Modèle de mobilité random waypoint [17].

5. Métriques et évaluation

Les scénarios de simulation que nous avons utilisée, nous ont permis de proposer et d'utiliser des métriques importantes pour l'évaluation de performances de notre simulation. Nous avons utilisé quelques métriques tel le PDR (*packets delivery ratio)* qui représente le taux de paquet de sécurité délivré, et il est calculé d'après l'envoie et le recevoir d'un paquet beacon.

❖ Nombre des Beacons reçus en termes nombre des nœuds :

Cette métrique définit le nombre de messages "k" reçus en variant le nombre des nœuds (20, 40, 80, 120,160, 200, 240, 280) et avec 2 cas de messages :

- ✓ Messages avec (signature + certificat).
- ✓ Messages sans (signature + certificat).

Et nous avons définir la taille de la signature et le certificat comme suite :

	Certificat OBU	**Signature OBU**
taille (oct)	**125**	**56**

Tab.1 Taille de certificat et de signature

❖ Le taux de perte :

Le taux des messages perdus permet de mettre en évidence la qualité de la réception. Il est possible d'avoir un délai élevé mais un taux des messages perdus également élevés.

❖ Le taux des messages beacons délivrés :

Le taux des messages délivrés permet d'illustrer les beacons qui sont échangés (envoyés et reçus) dans le réseau.

6. Paramètres de simulation

Nous avons évalué les performances de notre simulation. Le tableau suivant résume la configuration de notre simulation et les paramètres utilisés :

Nombre des nœuds	20, 40, 80, 120, 160, 200, 240,280
Modèle de mobilité	Random waypoint
Modèle de propagation	Two ray ground
Entourage	500*1500 m
Temps de simulation	100 s
Protocole de routage	AODV

Vitesse	20 m/s
Beacons sans certificat et signature Beacon avec certificat et signature	200 bytes 381 bytes
Transmission range	145 m
Power transmission	7,5 dbm

Tab.2 Paramètres de simulation

7. *Résultats et analyse*

Dans cette partie, nous présentons et nous analysons les résultats de simulation que nous avons obtenus à travers les scénarios précédemment définis.

Afin d'évaluer les solutions en terme de nombre des nœuds qu'on a pu calculer leurs beacons reçus, nous avons fait varier le nombre des nœuds de 20 à 280, et nous avons obtenu les résultats graphiques ci-dessous :

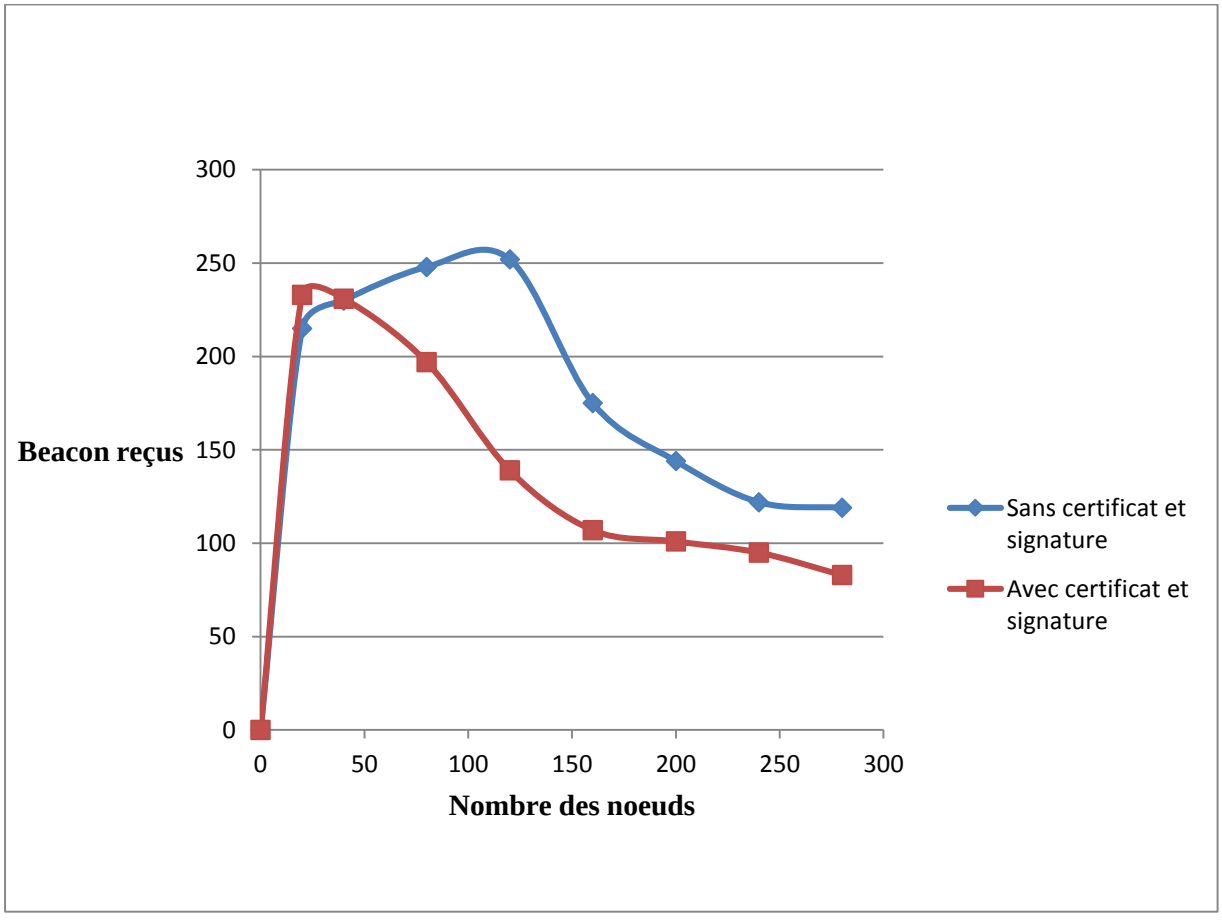

Fig. 3.5 Nombre des messages beacons réçus

Nœuds	beacon reçus sans cert/sig	beacon reçus avec cert/sig
0	0	0
20	215	233
40	230	231
80	248	197
120	252	139
160	175	107
200	144	101
240	122	95
280	119	83

Tab. 3 Résultats de simulation

Ce graphe illustre une comparaison sur le nombre des beacons reçus en fonction de nombres des nœuds avec 2 cas :

- ✓ Beacons avec certificats et signatures
- ✓ Beacons sans certificats et signatures

Nous remarquons lorsqu'on augmente le nombre des nœuds, les messages beacons reçus diminuent pour les deux graphes. Les beacons avec la charge utile importante causent des pertes à cause de la taille des beacons (beacon +certificat + signature).

Le nombre des nœuds dans le réseau et la taille des certificats et de la signature numérique a un impact important sur le nombre de messages beacons reçus.

❖ Le taux des messages perdus avec et sans certificat, signature en fonction de la durée (t) est représenté dans ci-dessous.

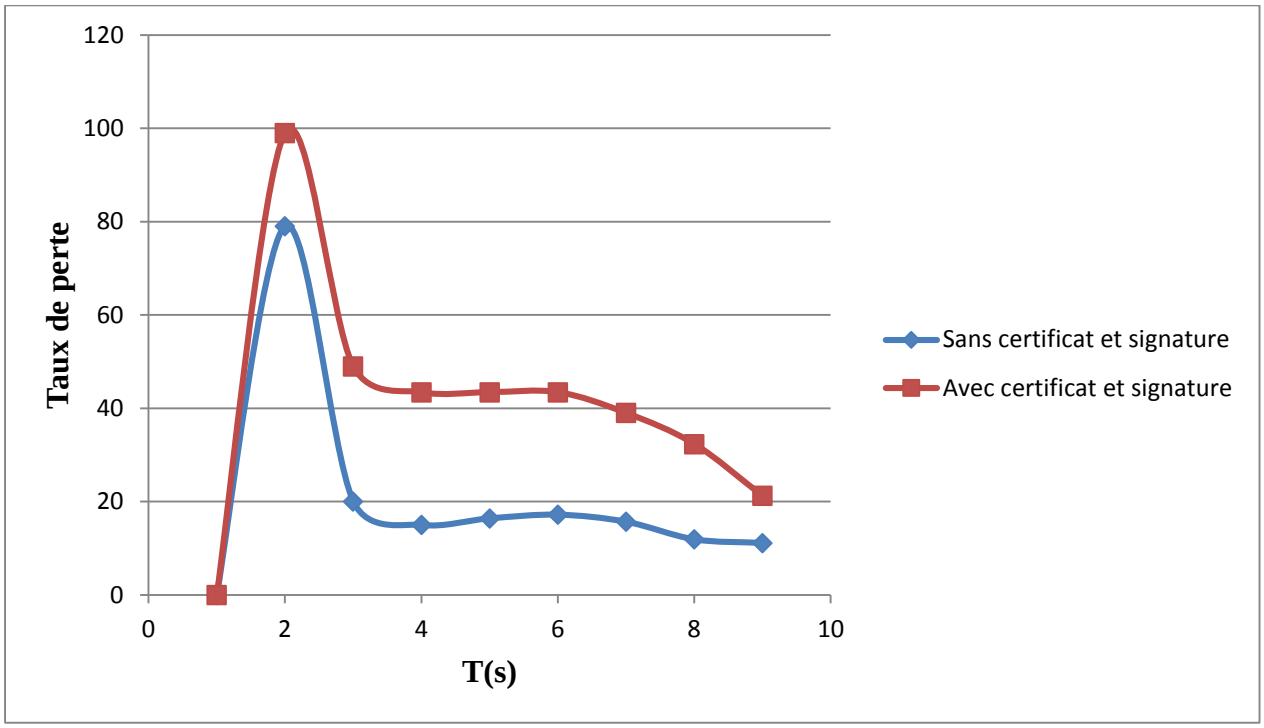

Fig. 3.6 Le taux de perte des messages beacons

Ce graphe montre le taux de perte des messages beacons avec et sans certificat, signature en fonction de temps.

Nous remarquons au début de temps le taux de perte pour les deux graphes plus élevé mais avec le temps diminue graduellement.

Au début de simulation tous les nœuds envoient des messages beacons en même temps c'est pour cela le taux de perte est élevé, tous les nœuds rentre en collision, et d'après la collision et avec le mécanisme de détection de collision tous les nœuds fait un petite time (backoff) pour éviter de rentrer en collision c'est pour cela le taux de perte diminue pour les deux courbes au cours de temps.

❖ Le taux des messages reçus en réseau en termes de nombres des nœuds

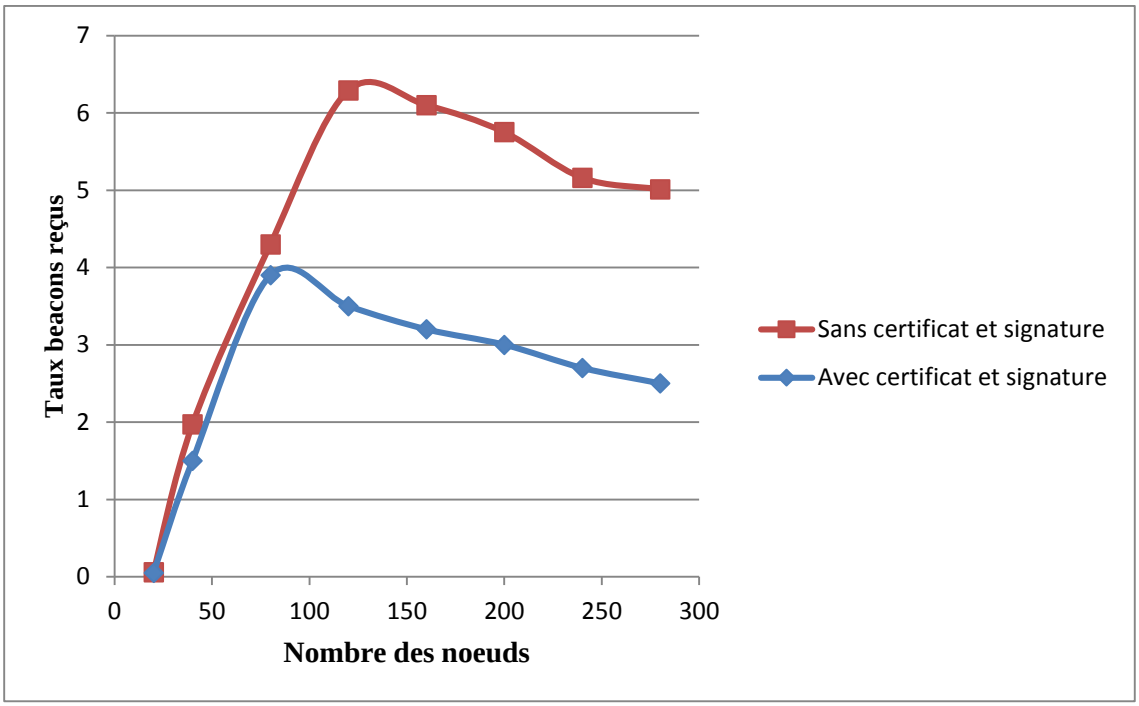

Fig. 3.7 Le taux des messages beacons reçus

Ce graphe illustre une comparaison sur le taux des messages beacons reçus avec et sans certificats, signature. Nous remarquons que la courbe qui représente le taux beacons délivrés sans certificat et signature présente des bons résultats par rapport à celui qui représente les beacons avec certificat et signature. Nous remarquons aussi lorsqu'on augmente le nombre de nœuds, le taux des messages beacons pour les deux courbes diminue.

Lorsqu'on augmente le nombre des nœuds, il y a plus de chance d'avoir des collisions, ce problème influence sur les beacons reçus.

Conclusion

Dans ce chapitre nous avons présenté le simulateur ns-3 et son fonctionnement. Nous avons aussi présenté trois scénarios de simulation avec différents paramètres. D'après les résultats de simulation précédents, nous pouvons dire que les messages beacons de sécurité sont nécessaires dans les VANETs, mais ce dernier peut causer des pertes de messages.

Conclusion générale

Les réseaux véhiculaires sont partie des réseaux mobiles Ad Hoc, permettant des échanges de données entre véhicules ou avec l'infrastructure. Ils suscitent un intérêt certain dans le but d'améliorer la sécurité.

Les réseaux véhiculaires sont vulnérables aux attaques menaçant la vie des usagers et les biens, et donc la sécurité de ces réseaux est un pré-requis pour leurs déploiements. Les techniques cryptographiques peuvent assurer les objectifs de l'authentification, l'intégrité et la confidentialité dans une certaine mesure, mais la disponibilité est difficile à assurer car l'aspect décentralisé des réseaux VANET donne la possibilité d'avoir plusieurs attaques.et avec des protocoles de routage qui devient responsable de l'acheminement des messages entre les véhicules à multi-sauts, ce qui donne lieu à la possibilité d'avoir plusieurs types d'attaque.

Dans ce travail, nous avons fait une présentation des réseaux VANETs nous avons s'intéresser avec la sécurité des messages beacon qui sont échangés entre les véhicules pour assurer la sécurité routière. Nous avons aussi présenté les différents types d'attaque existant pour ce réseau et nous avons choisi quelques métriques pour analyser et simuler l'impact de l'authentification sur la performance du réseau. Nous avons trouvé que l'ajout de la signature et le certificat numériques augmente la probabilité d'avoir plus de collisions, ce qui nécessite plus de recherche pour optimiser la taille de ces champs réservés à l'authentification.

Comme extensions futures à notre travail

- Réduire la charge (du certificat et de la signature numériques) pour n'as pas influe sur la réception des messages beacons
- Simuler notre travail avec d'autre modèle de mobilité

Bibliographie

[1] : International journal of computer application , simulation based analysis of adhoc routing protocol in urban and highway scenario of vanet January 2011.

[2]: linx,luR, Zhang c, ZhuH.,hop.h,shenX., ‘’securité in vehicular adhoc networks”,IEEE communication magazine, vol.46,no.4,pp 88-95 , april 2008.

[3]: Hubaux jp. , “vehicular networks: how to sure then “ ,MINeMa summer school, klagenfunt, Germany , july 2005.

[4]: Zen X , tao C., chen Z, “the application of DSRC technologie in intelegent transporation systeme”,IET international communication conference on wireless mobile & computing (cccwMcg) shangai, china , November 2009.

[5]: Projet VANET les reseaux véhiculaires (VANET)

[6]: Com 2 React , European projet ,www.com 2 react –projet.org application de gestion du traffic routier.

[7] : Mobility blum JJ,eskandarian A.,Hoffman LJ “challenges of inter-vehicular adhoc networks”, IEEE transaction on intelligent transportation systems,vol5 ,no.4,pp-347-351 December 2004.

[8]: Drawil N., “improving the vanet véhicules” localisaation accuracy using GPS receiver in multipath environments”, Master thesis, university of naterloo ,2007.

[9]: IEEE standard 802.11 p, IEEE standard for technologies telecommunication and information exchange between system .. local and metropolitan area networks .. specific requirements port 11: wireless LAN medium access control (MAC) and physical layer (phy) specification amendvent 6: wireless access in vehicular environments” 2010.

[10]: ASTM international, “E2213-03- Standard specification for telecommunication and information exchange between Road side and vehicle systems.5GHZ band dedicated short RANGE communication (DSRC) medium access control (MAC) and physical layer (phy) specification” 2007.

[11]: IEEE standard 802.11.a wireless LAN medium access control (MAC) and physical layer specification; high-speed physical layer in the 5GHZ(phy) band”,1999.

[12]: thèses authentification dans les réseaux véhiculaires université PARIS.

[13] : Mémoire magistère la sécurité des communications dans les réseaux VANET

[14] : Thèses protocole de diffusion des messages dans les réseaux véhiculaires université de MONTREAL.

[15] : Thèses protocole de diffusion des messages dans les réseaux véhiculaires université D'AVIGNON.

[16] : Site officiel de NS3 WWW.NSNAM.ORG/docs/release/models/html/animation consulté le 20/05/2015.

[17] : Site WWW.MEMOIREONLIGNE.COM/.../m-effets-mobilité-protocole consulté le 20/05/2015.