République Algerienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de Master Professionnel

Thème

Implémentation d'une nouvelle approche pour la révocation des certificats dans les VANET

Présenté par :

DEFLAOUI Hamidouche DJEBBARI Sofiane

Soutenu devant le jury composé de :

Président	Mme MITIDJI
Encadreur	Mlle TASSOULT Nadia
Examinatrice	Mme ZIDANI Faroudja

Promotion 2015 – 2016

Remerciements

Nous tenons en premier lieu à remercier Dieu tout puissant de nous avoir aidés et donnés courage pour arriver au terme de ce travail.

Nous tenons à remercier *Mlle* TASSOULT Nadia pour l'honneur qu'elle nous a fait en acceptant de nous encadrer, pour sa contribution à nous fournir les informations nécessaires pour ce projet.

Nos remerciements les plus sincères vont à nos chères familles qui nous ont soutenus avec tous les moyens pour notre réussite.

Nous tenons également à remercier tous nos enseignants ainsi que nos camarades et amis.

Enfin, nous sommes reconnaissants aux membres du jury de nous avoir fait l'honneur de juger notre travail.

Dédicaces

A nos parents, pour leurs sacrifices déployés à notre égard,

pour leur patience, leur amour et leur confiance. Qu'ils trouvent dans ce modeste travail, le témoignage de notre profonde affection et de notre attachement indéfectible ; nulle dédicace ne puisse exprimer ce qu'on leur doit.

A nos frères et sœurs et tous nos amis pour chaque mot reçu,

chaque geste d'amitié, à chaque main tendue et pour toute attention témoignée.

Table des Matières

Table des figures

Liste des Abréviations

A-STAR Anchor-based Street and Traffic Aware Routing

AC Access Category

AODV Ad Hoc On Demand Distance Vector

BSS Basic Service Set

CA Central Authority

CBDRP Cluster-Based Directional Routing Protocol

CBLR Cluster Based Location Routing

certI Certificat De Véhicule I

CH Cluster Head

DoS Denial of Service

DSR Dynamic Source Routing

DSRC Dedicated Short Range Communication

DTN Delay Tolerant Network

DVCAST Distributed Vehicular Broadcast Protocol

EDCA Enhanced Distributed Channel Access

EIRP Effective Isotropic Radiated Power

ETSI European Telecommunications Standards Institute

FCC Federal Communications Commission

FSR Fisheye State Routing

GF Greedy Forwarding

GG Gabriel Graph

GLS Greedy Location Service

GPCR Greedy Perimeter Coordinator Routing

GPRS General Packet Radio Service

GPSR Greedy Perimeter Stateless Routing

GSR Geographic Source Routing

HCB Hierarchical Cluster Based

HSM Hardware Security Module

IBSS Independent Basic Service Set

IDE Environnement de Développement Intégré

IDS Intrusion Détection System

IHM Interface Homme-Machine

ITS Intelligent Transportation Systèmes

ITSA Intelligent Transportation Society of America

JDK Java Development Kit

MAJ Mise à Jour

MANET Mobil Ad-Hoc Network

MPR Relais Multipoints

MSG Messages

MSS Mobile Support Station

non-DTN non-Delay Tolerant Network

OBU On-Board Unit

OLSR Optimized Link State Routing

PF Perimeter Forwarding

QLS Quorum-based location Service

RM Resource Manager

RNG Relative Neighborhood Graph

RREP Route Reply

RREQ Route Request

RSU Road Side Unit

RSUcert Certificat de RSU

RSUPK Clef Publique de RSU

SB Station De Base

SML Liste Des Membres de Secteur

TGP Task Group P

TORA Temporally-Ordered Routing Algorithm

TPD Tamper-Proof Device

TRL Temporary Revocation List

UM Unités Mobiles

V2I Véhicule à Infrastructure

V2V Véhicule à Véhicule

VANET Vehicular Ad-Hoc NETwork

WAVE Wireless Access in Vehicular Environments

WSM WAVE Short Messages

WSMP WAVE Short Messages Protocol

Introduction Générale

Le développement technologique qu'a vu le monde d'aujourd'hui a touché tous les domaines, particulièrement le secteur de la communication qui connaît une évolution considérable par l'apparition de la technologie sans-fil.

Les chercheurs pensent pouvoir exploiter cette technologie afin de permettre aux véhicules d'établir des liens entre eux, avec ou sans infrastructures installées aux bords des routes, ce qui constitue les nouveaux réseaux appelés VANET (*Vehicular Ad-Hoc NETwork*). Une des applications prometteuse de ces réseaux consiste à permettre aux véhicules équipés de capteurs spécifiques de détecter l'environnement proche et d'avertir les conducteurs des véhicules aux alentours suffisamment tôt en cas de risques d'accident.

Vu l'importance des informations échangées entre les véhicules et l'ouverture de l'environnement VANET, un attaquant peut émettre des messages d'alerte dont le contenu est falsifié ou empêcher l'acheminement d'un message légitime afin de causer des accidents.

L'attaquant peut empêcher l'acheminement de ces messages en visant la disponibilité du réseau aux niveaux des différentes couches de la pile protocolaire. Comme le routage est un service fondamental dans tout système de communication, il peut être une cible idéale pour les attaques [1]. Malheureusement, les contraintes entrainées par la forte mobilité des nœuds dans ces réseaux et leur aspect décentralisé, rend la sécurité des VANETs plus problématique que tout autre type de réseau.

Parmi les solutions proposées pour améliorer la sécurité des réseaux VANETs, il y a l'utilisation d'un SDI (*système de détection d'intrusion*) [2] afin de détecter et éviter de choisir les nœuds malveillants comme relais. Mais, les SDI ne peuvent assurer une détection rapide et efficace qu'au détriment d'une consommation élevée de la bande passante dans les VANETs, donc cette solution ne peut être envisagée pour la sécurité de routage dans les VANETs qui sont fortement contraignants en délai et en bande passante [3]. Ainsi, la solution consistant à intégrer les systèmes de réputation dans les protocoles de routage est difficile à appliquer dans ces réseaux caractérisés par une connectivité sporadique et de courte durée [4] [5].

La solution de révocation distribuée est considérée comme la solution la plus efficace et adéquate aux VANETs. Cependant, les CRL (*liste de révocation des certificats*) sont eux-mêmes vulnérables aux attaques de fausses alertes coordonnées qui visent a révoqué un nombre important de nœuds.

Ce travail est consacré à l'implémentation d'une nouvelle approche pour la révocation des certificats dans les réseaux VANETs. l'idée générale de cette approche est l'utilisation d'une liste temporaire de révocation TRL « *Temporary Revocation List* » gérée localement par le RSU. L'objectif principal de cette approche et de minimiser la taille et le temps de recherche dans la liste des certificats révoqués.

Ce mémoire est composé de quatre chapitres : le premier chapitre est consacré à la description des réseaux VANETs : architecture, applications et Activités de standardisation. Le second présente le routage dans les réseaux VANETs. Dans le troisième chapitre nous mettons l'accent sur la sécurité dans les réseaux VANETs de manière générale et en décrivant les différents mécanismes de base de la sécurité ainsi que les différentes approches de révocation proposées dans la littérature. Le dernier chapitre présente une description de l'approche TRL « *Temporary Revocation List* » : l'algorithme de fonctionnement générale, les différentes étapes de l'implémentation et les outils de développement. En fin, nous terminons par une conclusion et quelques perspectives.

1

Généralités sur les VANETs

Introduction

Les communications impliquant un véhicule joueront un rôle important dans les années à venir, que ce soit afin de communiquer avec un autre véhicule ou encore avec les infrastructures existantes. En effet, les voitures de demain ne se contenteront plus de détecter les dangers grâce à des radars ou des caméras, elles seront capables de recevoir des messages d'alerte envoyés par les autres automobilistes ou par l'infrastructure (panneaux, portiques, etc.. . .) et de transmettre ces informations à d'autres véhicules. Tel est en tout cas l'ambition des réseaux de véhicules que les chercheurs américains, japonais et européens veulent mettre en place.

Ces réseaux véhiculaires sont passés du stade de simple curiosité pour revêtir aujourd'hui un intérêt certain aussi bien du point de vue de l'industrie automobile que des opérateurs de réseaux et services et de la communauté de recherche. Ces réseaux véhiculaires sont en effet une classe émergente de réseaux sans fil permettant des échanges de données entre véhicules ou encore entre véhicules et infrastructure. Ils ont été amplement étudies en Europe, au Japon et en Amérique du Nord dans le but de fournir de nouvelles technologies capables d'améliorer la sécurité et l'efficacité des transports routiers.

Dans ce premier chapitre nous allons présenter une vue d'ensemble des réseaux véhiculaires. Nous y présentons les différents types d'applications et les principales technologies de communication qui peuvent être mises en œuvre dans ces réseaux, les caractéristiques et les challenges des réseaux véhiculaires, et travaux de standardisation réalisés dans le but de répondre à ces challenges.

1.1 Les réseaux sans fil

Un réseau sans fil (*Wireless network*), comme son nom l'indique, est un réseau dans lequel au moins deux terminaux (par exemple, ordinateur portable) peuvent communiquer sans liaison filaire.[6]

Le principe des réseaux sans fil est basé sur une liaison utilisant des ondes radioélectriques (radio et infrarouges) au lieu des câbles habituels. Il existe plusieurs technologies qui se dis-

tinguent par la fréquence d'émission utilisée ainsi que par le débit et la portée des transmissions.

1.2 Classification des réseaux sans fil

Les réseaux mobiles sans fil peuvent être classés en deux grandes catégories [6] : les réseaux avec infrastructure qui utilisent généralement le modèle de la communication cellulaire dans lequel les clients sans fil sont connectés à un point d'accès (p.ex. répéteur ou commutateur en réseau Ethernet) (Figure 1.1) ; et [7] les réseaux sans infrastructure ou les réseaux ad hoc dans lesquels les clients sont connectés les uns aux autres sans aucun point d'accès, afin de constituer un réseau point à point (*peer to peer*) dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès (p.ex. , l'échange de fichiers entre portables dans un train, dans la rue, au café...) (Figure 1.2). Plusieurs systèmes utilisent déjà le modèle cellulaire et connaissent une très forte expansion à l'heure actuelle (p.ex. les réseaux GSM) mais exigent une importante infrastructure logistique et matérielle fixe.

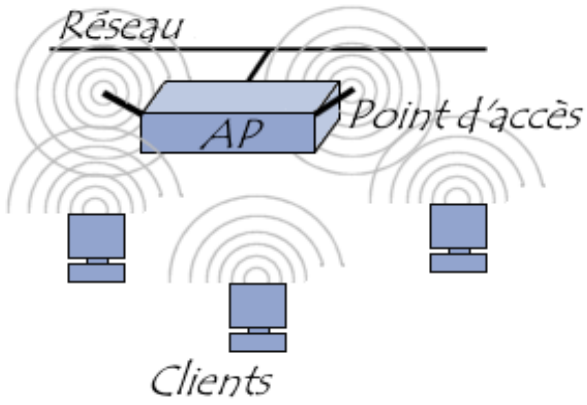


FIGURE 1.1 – Réseau en mode infrastructure

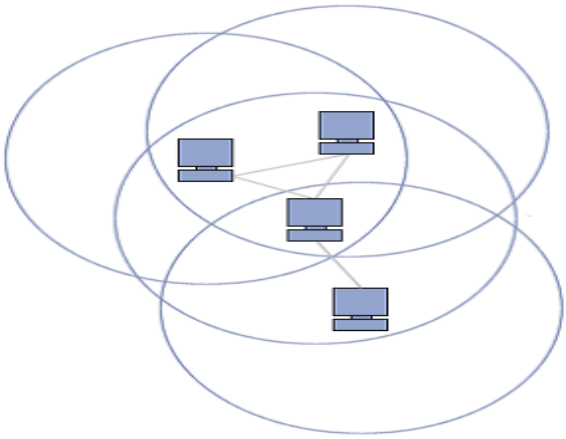


FIGURE 1.2 – Réseau en mode ad-hoc

1.2.1 Les réseaux avec infrastructure (*cellulaires*)

En mode avec infrastructure, également appelé le mode BSS (*Basic Service Set*) certains sites fixes, appelés MSS (*Mobile Support Station*) ou SB (*station de base*), sont munis d'une

interface de communication sans fil pour la communication directe avec des sites ou des UM (*unités mobiles*), localisés dans une zone géographique limitée, appelée cellule voir la (figure 1.3).

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages. Alors que les sites fixes sont inter connectés entre eux à travers un réseau de communication filaire, généralement fiable et d'un débit élevé. Les liaisons sans fil ont une bande passante limitée qui réduit sévèrement le volume des informations échangées. Dans ce modèle, une unité mobile ne peut être, à un instant donné, directement connectée qu'à une seule station de base.

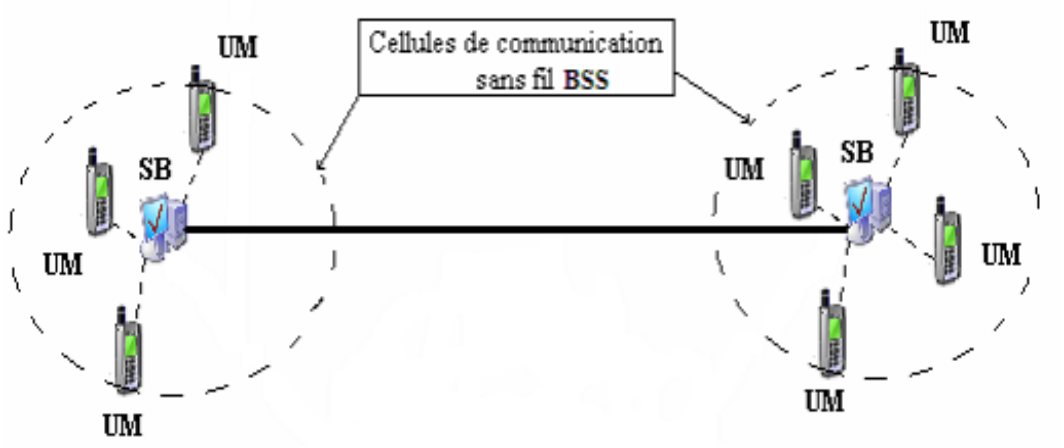


FIGURE 1.3 – Mode infrastructure avec BSS

1.2.2 Les réseaux sans infrastructure (*AD HOC*)

Le réseau mobile sans infrastructure également appelé réseau Ad hoc ou IBSS (*Independent Basic Service Set*) ne comporte pas l'entité « *site fixe* », tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil (Figure 1.2). L'absence de l'infrastructure ou du réseau filaire composé des stations de base, oblige les unités mobiles à se comporter comme des routeurs qui participent à la découverte et la maintenance des chemins pour les autres hôtes du réseau.

1.3 Les réseaux Ad-Hoc véhiculaires

Les réseaux VANETs (Véhicule Ad-Hoc Networks), réalisés par la réunion d'opportunités de plusieurs véhicules mobiles sans infrastructure préexistante pour communiquer, font actuellement l'objet d'une attention accrue de la part des constructeurs et des chercheurs, afin d'améliorer la sécurité sur les routes ou pour aidés les conducteurs. Par exemple, ils peuvent avertir d'autres automobilistes que les routes sont glissantes ou qu'un accident vient de se produire. Les réseaux véhiculaires sont une projection des systèmes de transports intelligents ITS (*Intelligent Transportation Systèmes*)[8]. Les véhicules communiquent les uns avec les autres par l'intermédiaire de la communication de V2V (*véhicule à véhicule*) aussi bien qu'avec les équipements de la route par l'intermédiaire de la communication de V2I (*Véhicule à Infrastructure*). L'objectif est que les réseaux VANETs contribueront à l'élaboration de routes plus sûres et plus efficaces à l'avenir en fournissant des informations opportunes aux conducteurs et aux autorités intéressées. Un exemple d'un réseau VANET urbain est illustré dans la (figure 1.4).

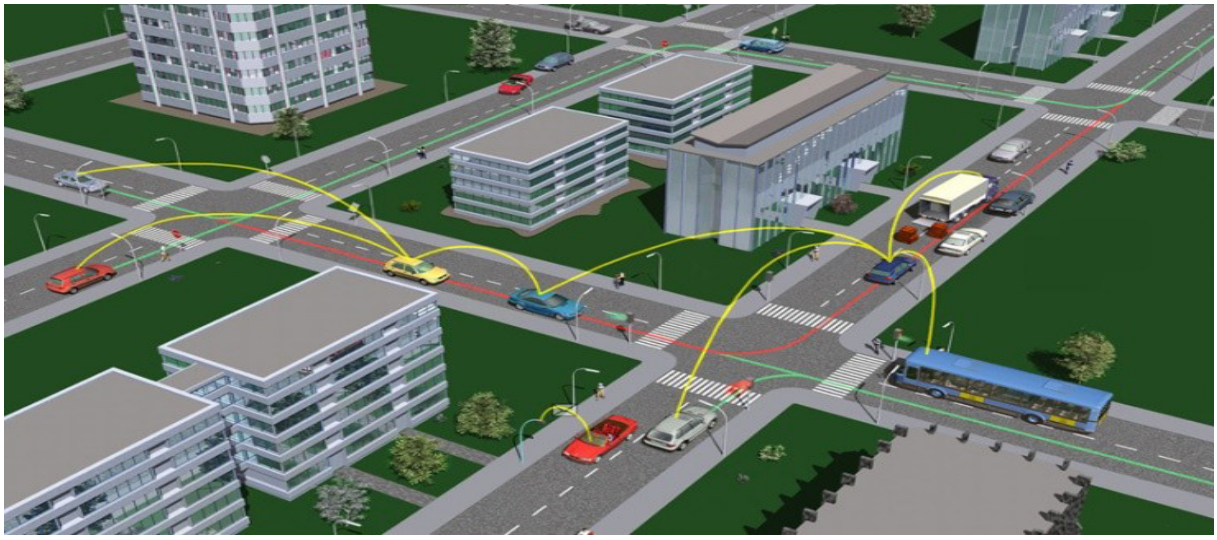


FIGURE 1.4 – Exemple d'un réseau VANET [68]

1.3.1 Caractéristiques des réseaux VANETs

Il est important de signaler que les réseaux VANETs ont quelques spécificités qui les distinguent des réseaux MANET. Les travaux et les études de recherche réalisés dans le contexte

des réseaux MANET ne peuvent pas être directement appliqués dans le domaine des réseaux de véhicules vus ses différences qui rendent l'application des protocoles et les architectures des réseaux ad hoc inadaptée. Dans ce qui suit nous présenterons quelques caractéristiques et contraintes liées à l'environnement des réseaux véhicules [9].

1.3.1.1 Capacité de traitement, d'énergie et de communication

Parmi les contraintes les plus importantes lors d'un traitement dans les réseaux ad hoc mobiles c'est la contrainte d'énergie, par contre dans un réseau VANET, les véhicules ne souffrent pas de cette contrainte vue qu'ils n'ont pas de limite en terme d'énergie et ils disposent d'une grande capacité de traitement (peuvent avoir plusieurs interfaces de communication : Wifi, Bluetooth...)[10]

1.3.1.2 Forte mobilité et topologie du réseau

Le nœud mobile dans un VANET qu'est la voiture est caractérisé par une vitesse élevée, en un temps très court, la voiture peut rapidement rejoindre ou quitter le réseau. Par conséquent, cette forte mobilité des nœuds cause des changements rapides de la topologie du réseau.

1.3.1.3 Connectivité et partitionnement de réseau

La forte mobilité des véhicules et le changement rapide de la topologie de réseau, donne comme conséquence la disparition de certain chemins i.e. le partitionnement du réseau peut fréquemment apparaître.[11]

1.3.1.4 L'environnement de déplacement et modèle de mobilité

Dans un réseau MANET, les nœuds se déplacent aléatoirement, contrairement au réseau VANET où les véhicules suivent un modèle de mobilité spécifique, Les déplacements des véhicules sont liés aux infrastructures routières (limitation de vitesse, ronds-points, carrefours).[9]

1.3.1.5 Diffusion de type d'informations

Généralement les types d'informations communiquées dans un réseau VANET s'orientent sur la diffusion des messages de prévention ou d'alerte d'une source à une ou plusieurs destinations. Néanmoins, la diffusion est faite en fonction de la position géographique et le degré

d'implication de véhicule dans l'évènement déclenché. Dans de telles situations, les communications sont principalement unidirectionnelles.[11]

1.3.2 Défis des réseaux VANET

Des caractéristiques des réseaux véhiculaires découlent plusieurs défis que l'on peut résumer en ces points :

1.3.2.1 Qualité de service

La demande en qualité de service dépend des applications supportées. La principale contrainte des applications de sécurité est la latence. La validité des informations étant limitée dans le temps, les messages doivent parvenir à destination dans des délais courts pour être considérés comme pertinents. Dans le cas des applications de gestion de trafic, il s'agit essentiellement de la définition d'algorithmes d'agrégation des données qui permettent d'inclure autant d'informations de trafic que possible dans les paquets diffusés [12]. Pour les applications de confort tel le transfert de fichiers ou le téléchargement le besoin est une connectivité permanente.

1.3.2.2 Canal radio fiable

Le rôle des mécanismes de gestion du canal radio est d'offrir des transmissions fiables et robustes et un partage équitable du médium de communication. Pour atteindre cet objectif dans le cas des réseaux véhiculaires, il est nécessaire de définir des méthodes qui permettent de faire face aux deux problèmes majeurs des transmissions qui sont, les interférences inter-symboles dues à la propagation des ondes par trajets multiples et l'effet causé par le mouvement des véhicules.

1.3.2.3 Routage

Les protocoles de routage sont utilisés en communications ad hoc. Ils permettent de déterminer la suite de nœuds que les paquets doivent traverser pour un échange d'information entre entités distantes. Les problèmes auxquels doivent répondre les protocoles de routage sont la connectivité intermittente qui rend les routes déjà établies obsolètes et le partitionnement du réseau qui empêche la propagation des paquets.

1.3.2.4 Adressage géographique et geocasting

Le routage geocast [13] est un mécanisme similaire au multicasting dans lequel les destinataires sont identifiés par des contraintes géographiques. Il est utilisé par les applications diffusant des données qui ne sont utiles que pour les véhicules se trouvant dans une zone géographique spécifique. Par exemple, l'information sur un accident n'est pertinente que pour les véhicules qui se dirigent vers le lieu de l'accident. La diffusion des paquets vers tout autre véhicule cause une surcharge inutile du réseau. La complexité dans le geocasting réside dans la détermination de la zone géographique et la définition d'un mécanisme de relayage efficace qui réduit la surcharge du réseau et qui soit adapté à toutes les densités.

1.3.2.5 Sécurité

Les exigences en sécurité doivent être prises en compte aussi bien dans la conception architecturale du réseau que dans la conception des protocoles de communication. Elles diffèrent en fonction des applications et comprennent principalement la confidentialité, l'authentification, la cohérence et l'intégrité des données et la disponibilité. La satisfaction de ces exigences dans des systèmes aussi dynamiques et mobiles que les réseaux véhiculaires est difficile mais particulièrement importante étant donné que des vies humaines sont concernées.

1.3.2.6 Normalisation vis-à-vis de la flexibilité

Il est évidemment nécessaire d'uniformiser les communications afin de permettre aux véhicules conçus par différents fabricants de pouvoir collaborer. Cependant, en raison des enjeux commerciaux, il est probable que les constructeurs voudront créer une certaine différenciation des standards.

1.3.3 Types d'application

Nombreuses sont les applications proposées pour les réseaux véhiculaires [14], [15]. Elles peuvent être classifiées en trois grandes catégories.

1.3.3.1 Les applications de sécurité

C'est le type le plus important qui vise à améliorer la sécurité des passagers sur les routes en avisant les véhicules de toute situation dangereuse. Ces applications se basent en général sur une diffusion, périodique ou non, de messages informatifs permettant aux conducteurs d'avoir une connaissance de l'état de la route et des véhicules voisins. Des exemples répandus de services dans cette catégorie d'applications sont, l'avertissement des collisions, les avertissements sur les conditions de la route, l'assistance dépassement et changement de voie, etc.

1.3.3.2 Les applications de gestion de trafic

Sont axées sur l'amélioration des conditions de circulation dans le but de réduire les embouteillages et les risques d'accidents. Elles consistent à fournir aux conducteurs des informations leur permettant d'adapter leur parcours à la situation du trafic routier. En d'autres termes, ces applications visent à équilibrer la circulation des véhicules sur les routes pour une utilisation efficace de la capacité des routes et des carrefours et à réduire par conséquent les pertes humaines, la durée des voyages et la consommation d'énergie. Parmi ces applications on peut citer, la surveillance du trafic, l'ordonnancement des feux de signalisation, etc.

1.3.3.3 Les applications de confort ou de divertissement

Sans objectif est de rendre les voyages plus agréables en permettant aux passagers de communiquer soit avec d'autres véhicules ou avec des stations fixes comme les hôtes Internet ou le réseau téléphonique public. Des exemples de ces applications sont : la gestion des parkings, les jeux/discussions distribués, les applications pair-à-pair, etc.

1.3.4 Les entités communicantes

Un réseau véhiculaire se compose de quatre entités voir (figure 1.5) : les unités embarquées qui sont les véhicules, des infrastructures fixe appelées RSU (*road Side Unit*) installées le long des routes, l'équipement personnel et l'équipement central.

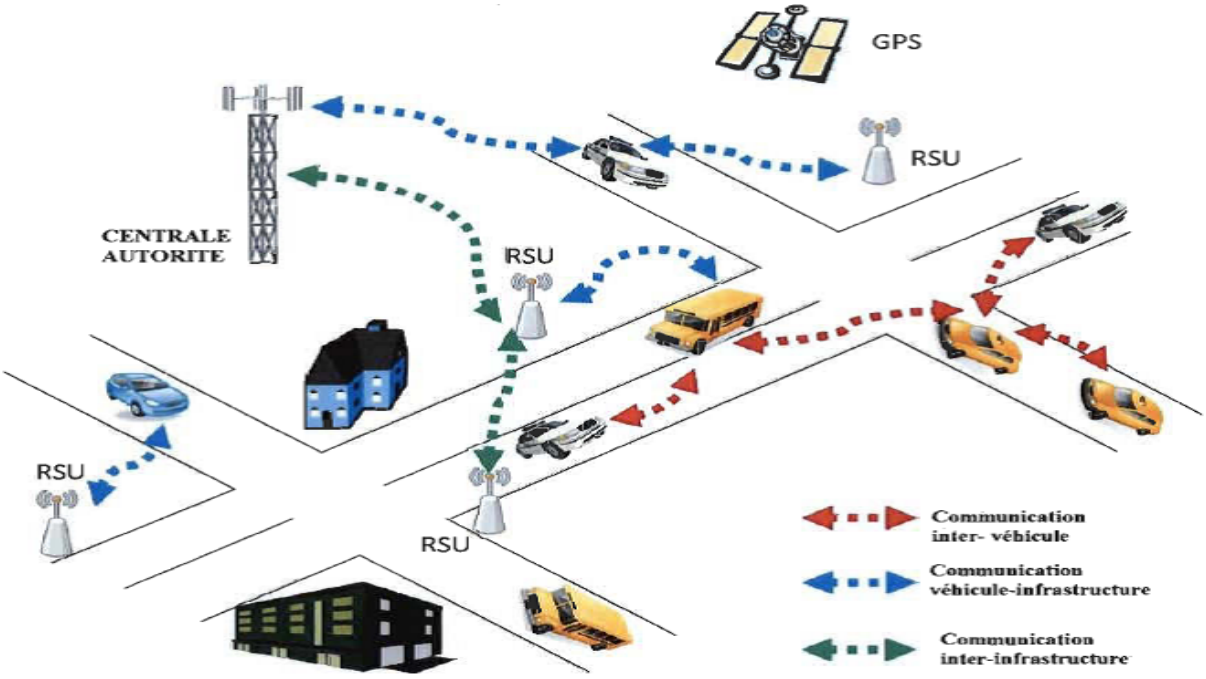


FIGURE 1.5 – Les entités communicantes dans les VANETs [69]

Les différents nœuds du réseau disposent d'équipements leur permettant de communiquer via des technologies sans fil. Les véhicules peuvent communiquer entre eux en mode ad hoc à l'aide de certains standards de communications GPRS (*General Packet Radio Service*) qui sont intégrés dans les OBUs [11] embarques a bord des véhicules et qui de nos jours sont proposés par plusieurs constructeurs automobiles. Ou avec les RSUs en mode cellulaire et peuvent aussi communiquer en hybride avec les autres véhicules et avec les RSUs.

1.3.4.1 Les unités embarquées (*véhicule*)

Les véhicules modernes sont équipés d'un ensemble de processeurs connectés à une plate-forme centrale de calcul qui dispose d'interfaces filaires et sans fil. Les véhicules intelligents comme montrer dans la (figure1.6) 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.

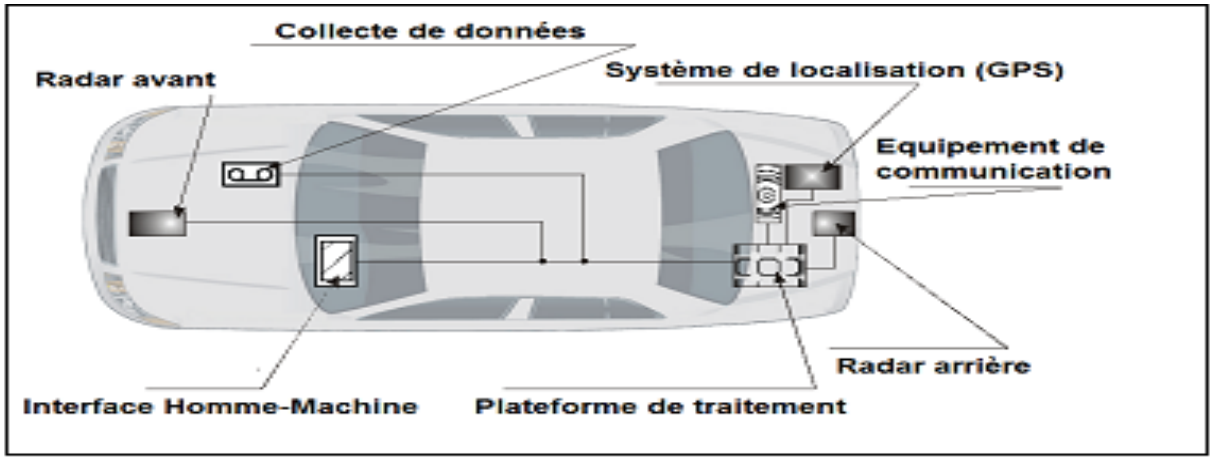


FIGURE 1.6 – Le véhicule intelligent[16]

1.3.4.2 Les infrastructures fixes RSU (*Road Side Unit*)

Les RSUs sont des infrastructures placées sur le long des routes, leur rôle principale est d'informer les véhicules à proximité en diffusant les conditions du trafic, météorologiques ou spécifiques de la route (vitesse maximale, autorisation de dépassement, etc.). Ils peuvent jouer aussi le rôle d'une station de base en relayant l'information envoyée par un véhicule.

1.3.4.3 Equipement personnel

Les équipements personnels sont les équipements qui peuvent être apportés par les utilisateurs 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 commande vocale (en utilisant les microphones intégrés au véhicule) ou par le biais de l'IHM (*interface Homme-Machine*) du véhicule.

1.3.4.4 CA (*Central Authority*)

C'est la Centrale d'autorité. Elle gère le réseau et joue le rôle de serveur de stockage des données. La CA délivre également des certificats et des clés ou pseudonymes de communication aux véhicules [17].

1.3.5 Architecture de communication des réseaux véhiculaires

Les architectures dans un réseau véhiculaire peuvent être déployées suivant trois catégories [18],[19] :

1.3.5.1 Les communications Véhicule à Véhicule (*V2V*)

Celle-ci est une architecture décentralisée basé sur un système distribué autonome, i.e. elle est vue comme un cas particulier d'un réseau MANET où le réseau est formé par des véhicules et même sans appuis sur une infrastructure fixe pour se communiquer voir la (figure 1.7), les véhicules sont équipés de la technologie qui permet aux véhicules de communiquer entre eux n'importe où, que ce soit sur les autoroutes, des routes de montagnes ou des routes urbaines, ce dispositif est connu sous le nom OBU (*On Board Unite*), ce qui donne une communication moins coûteuse et plus flexible.
Cette architecture peut être utilisée dans les scénarios de diffusion d'alerte (freinage d'urgence, collision, ralentissement, ... etc.) ou pour la conduite collaborative.[18],[19]

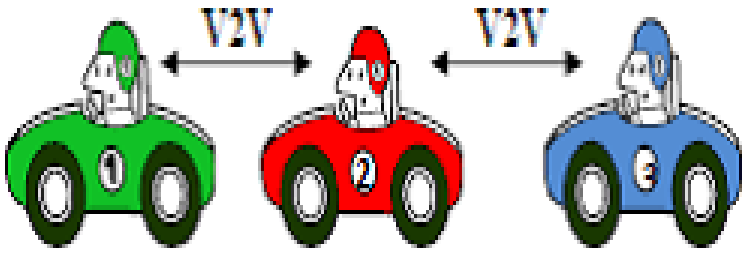


FIGURE 1.7 – Communication véhicule à véhicule

1.3.5.2 Les communications Véhicule à Infrastructure (*V2I*)

Celle-ci est une architecture centralisée basée sur des stations de bases dans leurs communications, les véhicules garantissent des communications avec l'infrastructure en utilisant des points d'infrastructure (voir la figure 1.8). Ces points d'accès sont également connus sous le nom RSU (*Road Side Units*), situés dans certaines sections critiques de la route, tels que les feux de circulation, intersections, ou les stop, afin d'améliorer l'expérience de conduite et la rendre plus sûre. Cette architecture peut être utilisée dans les scénarios comme accès à Internet, état de la circulation, contrôle de vitesse...etc.[18],[19]

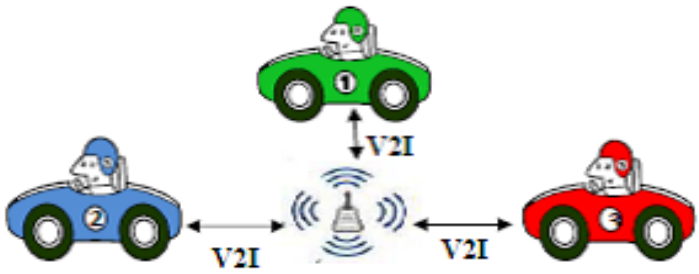


FIGURE 1.8 – Communication Véhicule à Infrastructure

1.3.5.3 Les communications Hybrides (*V2V-V2I-I2I*)

La combinaison de ces deux types de communications permet d'obtenir une communication hybride très intéressante (voir la figure 1.9). En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relais permet d'étendre cette portée. Dans un but économique et afin d'éviter la multiplication des stations de bases, l'utilisation des sauts par véhicules intermédiaires prend tout son importance.[18],[19]

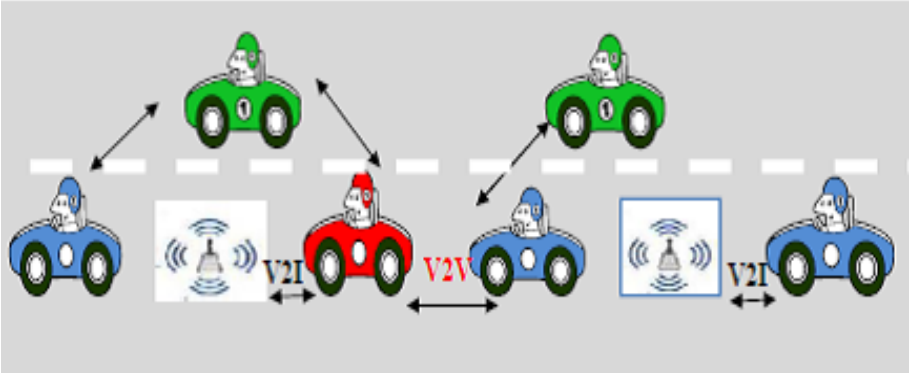


FIGURE 1.9 – Communication Hybrides (*V2V, V2I*)

1.3.6 Types de messages

Les entités formant un réseau sans fil véhiculaire vont générer et s'échanger des messages. En fonction de l'application et du contexte environnemental, un véhicule peut envoyer (ou recevoir) un message de contrôle, d'alerte ou <autre>.

1.3.6.1 Message de contrôle

Le message de contrôle est généré a intervalle régulier. Conventionnellement, chaque véhicule émet un message de contrôle toutes les 100 ms. Ce message, appelé aussi (beacon), contient la position, la vitesse, la direction et l'itinéraire du véhicule émetteur. Grâce aux messages de contrôle, chaque véhicule se crée une vue locale de son voisinage. Le véhicule peut aussi prédire et anticiper des situations accidentogénes ou de congestion. Le message de contrôle est l'équivalent du message HELLO des protocoles de routage. Chaque véhicule se fait donc connaitre de son voisinage direct. Bien entendu, les messages de contrôle ne sont pas transférés et utilisent une diffusion a un saut.

1.3.6.2 Message d'alerte

Le message d'alerte est généré lorsqu'un événement est détecté. Cela peut être la détection d'un accident, d'un obstacle ou la réception d'un autre message d'alerte. Le message d'alerte doit être émis à intervalle régulier afin d'assurer la pérennité de l'alerte. Ainsi le ou les véhicules désignés pour la retransmission des messages émettront des alertes a instants réguliers. Les messages d'alerte doivent donc être de taille réduite pour être transmises le plus rapidement possible. Les messages contiennent en particulier les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission.

1.3.6.3 Autres messages

Ce type de message contient tous les messages qui ne sont pas des messages d'alerte ou de contrôle. Ces messages ne sont généralement pas répétés à intervalle régulier. En effet, cela peut être par exemple un message de transaction financière ou l'envoi de courrier électronique.

Tous les messages reçus seront stockes dans un < cache des messages récemment reçus >. Chaque message se verra associer une durée de vie dans le cache.

1.4 Activités de standardisation

1.4.1 DSRC (*Dedicated Short Range Communications*)[20]

Les premiers standards définis pour les communications sans fil dans les ITS utilisent la bande de fréquence de $915MHz$ essentiellement pour assurer des services tels que, le péage électronique, l'accréditation et la surveillance des opérations des véhicules commerciaux. Cette bande de fréquence étant trop étroite et polluée pour supporter l'évolution envisagée pour les applications dans les réseaux véhiculaires, l'ITSA (*Intelligent Transportation Society of America*) a sollicité la FCC (*Federal Communications Commission*) pour l'allocation d'une bande passante de $75MHz$ dans la gamme de fréquences $5,850-5,925GHz$ pour les communications à courte portée dédiées aux ITS aux USA. Cette demande a été accordée par la FCC en 1999 et a donné naissance à la technologie DSRC. En Europe, l'ETSI (*European Telecommunications Standards Institute*) a créé un comité technique pour les ITS fin 2007 dont la mission est la création de normes et de spécifications pour l'utilisation des technologies de l'information et de la communication dans les futurs systèmes de transport en Europe. Le processus d'attribution des fréquences en Europe est beaucoup plus complexe et plus fastidieux qu'aux USA étant donné que tous les pays européens et leurs autorités nationales sont concernés. Ce n'est qu'en août 2008 que l'ETSI a affecté un spectre de fréquences dans la bande des $5,9GHz$ pour l'accès sans fil dans les réseaux véhiculaires. Du point de vue technique, l'approche européenne pour les communications des véhicules a de nombreux points communs avec le système américain. Les deux se fondent sur la variante 802.11p de la norme IEEE 802.11 [18] avec une bande de fréquences similaires et utilisent principalement des messages périodiques envoyés par chaque véhicule et infrastructure pour les services de sécurité et IPv6 pour les services de données.

1.4.2 La norme IEEE 802.11p

La norme IEEE 802.11p [21] est un amendement du standard IEEE 802.11 Que le groupe de travail IEEE (*TGP, task group p*) a commencé à développer en 2004 pour l'accès sans fil dans les systèmes de transport intelligents. Il définit les spécifications des couches MAC et PHY dans le cadre des réseaux véhiculaires. La couche physique du 802.11p utilise les mêmes mécanismes de traitement de signal et les mêmes spécifications que dans le standard 802.11a avec cependant quelques modifications pour l'adapter aux environnements véhiculaires. Pour

offrir des communications à grandes portées, quatre classes de puissance maximale EIRP (*Effective Isotropic Radiated Power*) sont autorisées. La plus grande valeur, $44,8dBm$ ($30w$), est réservée pour les véhicules d'urgence (*approching emergency vehicules*).La valeur typique des messages de sécurité pertinents est de $33dBm$. Pour augmenter la tolérance à l'effet de propagation des signaux par trajets multiples, une bande passante de $10MHz$ est utilisée au lieu de $20MHz$ comme dans la norme 802.11a. En réduisant la bande passante, tous les paramètres du domaine temporel sont doublés. Ceci permet de réduire d'une part l'effet Doppler grâce à l'utilisation d'une bande passante plus petite et d'autre part, les interférences inter-symboles en doublant la valeur des intervalles de garde. Ces modifications permettent à la norme 802.11p d'offrir des débits allant de 3 à $27Mbit/s$ sur des portées de communications de $300m$ à $1000m$.

La couche MAC de la norme 802.11p est équivalente à la technique EDCA(*Enhanced Distributed Channel Access*) de la norme 802.11e. Dans EDCA, les messages sont classifiés en quatre catégories d'accès (AC, *Access Category*) avec, AC0 la catégorie de messages ayant la plus faible priorité et AC3 la catégorie de ceux ayant la plus grande priorité. A chaque catégorie est associée une file d'attente où sont gardés les paquets en attente d'envoi. La priorité est assurée en affectant différents paramètres d'accès à chaque catégorie.

1.4.3 WAVE (*Wireless Access in Vehicular Environments*)

L'IEEE a développé une architecture connue sous le nom de WAVE (*Wireless Access in Vehicular Environments*), pour fournir l'accès sans fil dans les environnements véhiculaires. Deux modes de communication sont possibles dans l'architecture WAVE [22], véhicule-à-véhicule et véhicule-à-infrastructure. Les véhicules communiquent via un dispositif installé à leur bord dit, OBU (*On Board Unit*) montré sur la (figure 1.10).

Les infrastructures, sont équipées de dispositif dit RSU (*Road Side Unit*) montré sur la (figure 1.11). Les RSU sont des entités fixes qui permettent de connecter les véhicules aux réseaux communs qui par la suite les connectent au cœur central du réseau. Les RSU sont habituellement installés sur des infrastructures existantes tels que les feux de circulation, les panneaux routiers ou encore les lampadaires. En plus des capteurs, les RSU disposent d'un

émetteur-récepteur DSRC et d'un processeur d'applications qui offre des services de sécurité et des services non liés à la sécurité pour les multiples OBU qui sont dans la zone de transmission. Un OBU est un équipement WAVE mobile qui permet des communications OBU à OBU en mode ad hoc, et des communications OBU à RSU en mode infrastructure. Les OBU sont également reliés à une gamme de capteurs et d'actionneurs au sein du véhicule. Ceci facilite la surveillance efficace des véhicules pour rassembler des informations comme la vitesse du véhicule et son accélération.[22]

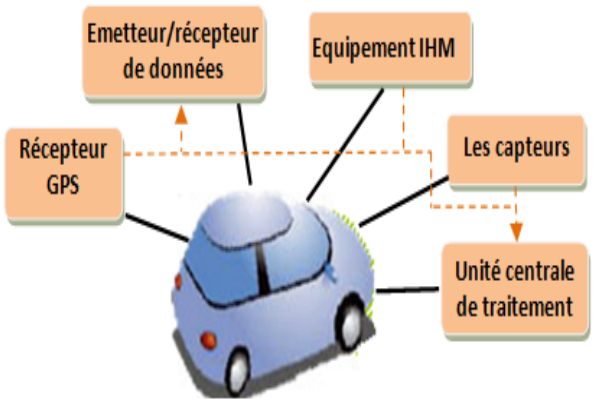


FIGURE 1.10 – WAVE On Board Unit

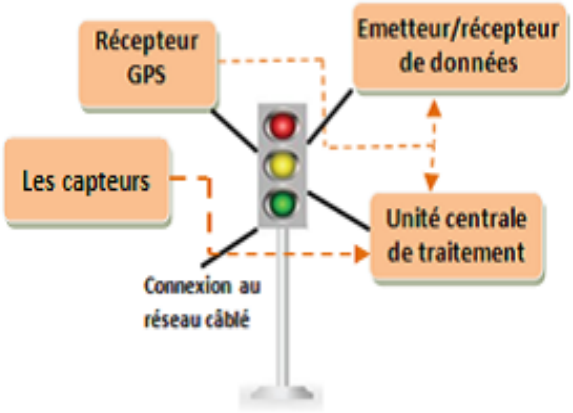


FIGURE 1.11 – WAVE Road Side Unit

La figure 1.12 montre l'architecture WAVE qui est une association de l'amendement IEEE 802.11p et de quatre standards 1609.1, 1609.2, 1609.3, et 1609.4 définis par le groupe de travail IEEE 1609 pour décrire les spécifications des couches hautes pour les communications WAVE :

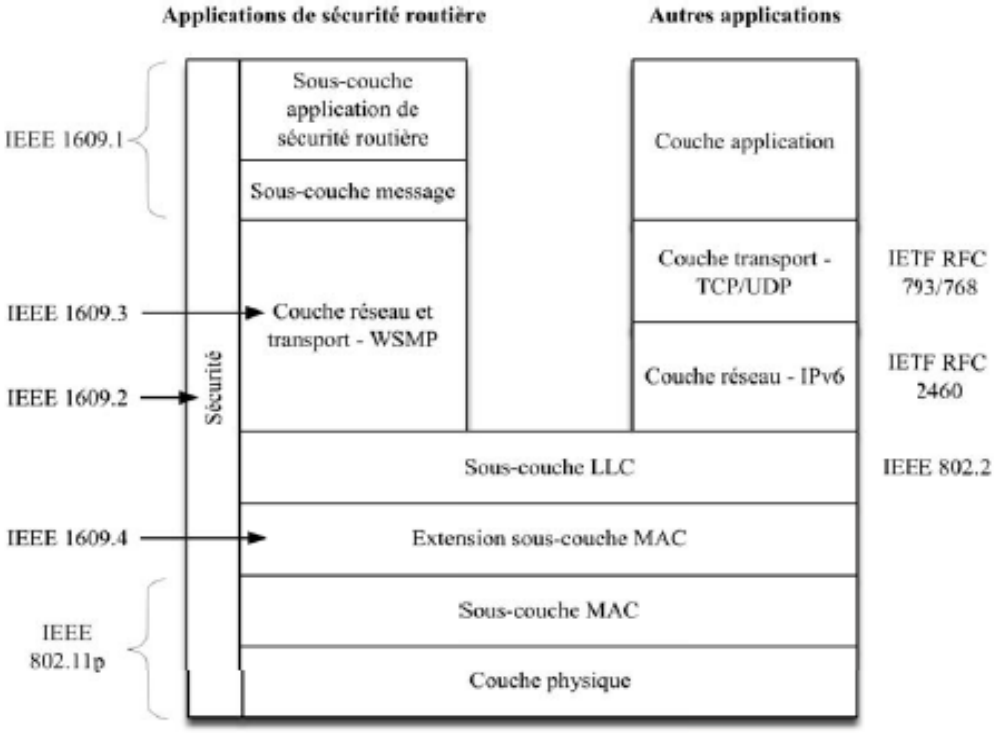


FIGURE 1.12 – Le modèle DSRC/WAVE : IEEE 1609 [23]

- **IEEE 1609.1 (*Gestionnaire des ressources*)[24]**

Ce standard décrit le service de gestion de ressources dit RM (*Resource Manager*) conçu pour permettre aux applications distantes de communiquer avec les OBU via les RSU. Le RM a pour objectif de répondre aux exigences des applications distantes en leur fournissant un accès en temps opportun aux ressources du OBU telles que la mémoire et l'interface utilisateur de manière cohérente et en garantissant l'interopérabilité.

- **IEEE 1609.2 (*Services de sécurité pour les applications et les messages de gestion*)[25]**

Décrit les services de sécurité dans le système WAVE. Les principales applications du système étant des applications de sécurité critiques, il est vital de définir des services de sécurité afin de protéger les messages contre les attaques telles que l'écoute clandestine, l'usurpation d'identité, et aussi de préserver la vie privée des conducteurs. Ce standard définit le format des paquets et les fonctions de sécurité, de chiffrement et d'authentification, pour les trois types

de messages, de sécurité, de données et de gestion.

- **IEEE 1609.3 (*Services de la couche réseau*)[26]**

Ce standard décrit les fonctions des couches réseau et transport pour les communications dans un système WAVE dont l'adressage et le routage. Il définit un nouveau type de messages dits WSM (*WAVE Short Messages*) et un nouveau protocole WSMP (*WAVE Short Messages Protocol*) pour la transmission des WSM. Le WSMP est une alternative à IPv6 qui fournit aux applications un échange de données efficace en leur permettant d'envoyer les WSM directement sur n'importe quel canal de DSRC.

- **IEEE 1609.4 (*Opération multi-canal*)[26]**

Étant basés sur le DSRC, les dispositifs WAVE doivent fournir un accès multi-canal et permettre des communications sur le canal de contrôle et les canaux de service. C'est le rôle du standard 1609.4 qui définit tous les mécanismes nécessaires pour l'accès avec priorité aux canaux, la coordination et le routage des données vers les canaux et la transmission des données.

Conclusion

Le développement des nouvelles technologies de communications et l'avancement des applications des STI ont favorisé un excellent stade pour l'évolution des réseaux véhiculaires. Dans ce chapitre nous avons donné un aperçu sur les réseaux VANETs qui ne sont qu'une particularité des réseaux sans fil MANET. Par la suite, nous avons donné les différentes spécificités, contraintes, architectures et services d'applications pour distinguer les réseaux VANETs par rapport aux réseaux MANET. Dans ce chapitre nous nous sommes basé sur l'aspect communication, i.e. les techniques de communications utilisées dans les VANETs (*Wifi, DSRC*). A la fin, nous avons également présenté la couche protocolaire des standards 802.11p et WAVE.

Un des défis que doivent surmener les réseaux MANETs et surtout les VANETs et le problème d'acheminement et de routage des données entre les nœuds mobile de réseau.

Le chapitre suivant sera consacré à la description de quelques approches et protocoles de routage dédiés aux réseaux VANETs.

2

Le routage dans les réseaux VANETs

Introduction

Les réseaux VANETs se caractérisent par l'absence de l'infrastructure fixe, ce qui conduit ces réseaux d'assurer leur propre organisation d'acheminer les données entre les entités mobiles. Cet acheminement requiert l'utilisation de protocoles de communication ou de routages spécifiques. Ces protocoles visent à sélectionner la meilleure route pour acheminer les paquets depuis la source vers la destination. Router un flux de données dans un environnement sans fil véhiculaire, sans infrastructure (en particulier les communications *V2V*), et à une forte mobilité « *topologie très dynamique* » est une tâche difficile à résoudre. En fait, le routage est considéré comme l'un des problèmes difficiles de réseaux ad hoc véhiculaires.

Dans ce chapitre, nous allons présenter d'abord le routage dans les VANETs, la classification des protocoles (routage basé sur la position, routage basé sur la topologie, et celui basé sur les groupes et sur la diffusion), nous finissons par citer quelques protocoles de routages utilisés dans le routage basé sur la position.

2.1 Classification des protocoles de routage dans les réseaux VANETs

2.1.1 Routage basé sur la position[38] [29]

Est une technique qui permet de délivrer un paquet à un nœud dans un réseau VANET via plusieurs sauts à l'aide de la position géographique. Dans ce routage les décisions ne sont pas basées ni sur les adresses réseau ni sur les tables de routage, au contraire, les messages sont acheminés vers l'emplacement de destination. Avec la connaissance de l'emplacement des voisins, chaque nœud peut sélectionner le voisin qui est plus proche de la destination, et ainsi avancer vers la destination à chaque saut. Le fait que ni les tables de routage, ni les activités de découverte de route ne sont nécessaires rend le routage géographique très attractif pour les réseaux dynamiques, tels que les réseaux véhiculaires.

Pour effectuer un routage géographique dans un réseau ad hoc, il est nécessaire : (i) que tous les nœuds soient muni d'un moyen de localisation comme GPS [30], (ii)qu'un nœud

source doit connaître la position du nœud destinataire. Pour ce faire les nœuds peuvent utiliser un service de localisation tels que GLS (*Greedy Location Service*) [31], QLS (*Quorum-based location service*) [32] ou encore Homezone [33].

Nous verrons ci-après plus en détail certains de ces protocoles.

2.1.2 Routage basé sur les groupes

Dans ce type de protocole de routage, les véhicules ou les mobiles qui sont à proximité des autres forment un groupe ou une grappe (*cluster*) et chaque groupe possède un chef de groupe (*Cluster Head*). La formation de groupes et la sélection du chef de groupe sont des processus déterminants. Chaque chef de groupe jouera le rôle de la passerelle entre son groupe et les autres groupes. D'ailleurs, dans les réseaux VANETs, connus pour leur mobilité très dynamique, la formation des groupes est un processus dominant [34].

Ce type possède un avantage bien important : la diminution des coûts et des retards de livraison des paquets de données lors du transport principalement à cause de sa gestion. En effet, chaque chef de groupe est responsable de la gestion des nœuds au sein d'un même groupe, mais également de la gestion entre les autres groupes. La communication diffère toutefois dans ces deux cas. La communication entre les nœuds d'un même groupe s'effectue par des liens directs entre eux, tandis que la communication entre les groupes s'effectue par le biais des chefs de groupes [35]. À titre d'exemple, nous citons trois des nombreux protocoles de routage basé sur les groupes :

- **HCB (*Hierarchical Cluster Based*)[35]**

Ce protocole est conçu tout particulièrement pour les réseaux ad hoc à forte mobilité et est basé sur une architecture de communication à deux couches. Dans la couche 1, les nœuds peuvent communiquer entre eux via un chemin à multi-sauts à l'aide de leur interface radio unique. Parmi ces nœuds, se trouvent ceux qui possèdent également une autre interface radio de communication à large portée. Ceux-ci sont appelés des « *super nœuds* » et existent à la fois dans la couche 1 et 2. Dans le HCB, le routage pour les chefs de groupes s'effectue

indépendamment pour chaque grappe. Ces chefs de groupes dirigent l'échange périodique des informations entre les nœuds d'un même groupe afin de permettre le routage entre les groupes.

- **CBLR (*Cluster Based Location Routing*) [36]**

Il s'agit d'un protocole de routage réactif, chaque chef de groupe conserve une table de routage contenant les adresses et les localisations géographiques des nœuds de son propre groupe et des nœuds passerelles, en plus de maintenir une table de routage des groupes voisins. Quand une source veut envoyer des données à une destination, le chef de groupe vérifie d'abord si la destination est dans le même groupe ou non. Si celle-ci est dans le même groupe, il envoie le paquet à la plus proche voisine de la destination. Le CBLR est adapté aux réseaux à haute mobilité, puisqu'il met à jour la localisation de la source et de la destination à chaque fois avant de commencer la transmission de données.

- **CBDRP (*Cluster-Based Directional Routing Protocol*) [34], [36]**

Ce protocole divise les véhicules en groupes et les véhicules qui se déplacent dans la même direction sous forme d'un groupe. La source envoie le paquet au chef de son groupe, puis ce dernier transmet le paquet au chef du groupe de destination, qui le transmet à son tour à la destination. La sélection du chef de groupe et l'entretien s'effectuent comme un CBLR, sauf que le CBDRP prend également en considération la vitesse et la direction du véhicule.

2.1.3 Routage basé sur la diffusion

Il se caractérise par sa simplicité, mais il reste incapable de résoudre le problème de la tempête (*Storm*) générée par une divergence des mécanismes de diffusion de proche en proche. La diffusion pour ce type de routage se base sur la structure hiérarchique du réseau routier. La route y est alors divisée en cellules virtuelles qui se déplacent comme des véhicules. On distingue deux niveaux de hiérarchie dans l'organisation des nœuds d'une route : la hiérarchie du premier niveau, qui comprend tous les nœuds dans une cellule, alors que la hiérarchie du second niveau est représentée par des réflecteurs de cellules, qui sont quelques nœuds situés très proches du centre de la cellule. Certains réflecteurs de cellules se comportent temporairement comme des chefs de groupe et gèrent les messages d'urgence provenant des membres mêmes de la cellule ou d'un voisin proche [37]. Ce routage se base sur les inondations pour faire la

diffusion. À titre d'exemple, Le protocole DVCAST (*Distributed Vehicular Broadcast Protocol*) [37], [38].

2.1.4 Routage basé sur la topologie

Il utilise les informations des liens qui existent dans le réseau dans l'acheminement des paquets. Ils peuvent être classifiés en deux familles : protocoles proactifs et réactifs.

2.1.4.1 Les protocoles proactifs

Le principe des protocoles proactifs est de maintenir à tout instant une vue globale et cohérente de la topologie du réseau, et de construire des routes entre les nœuds avant qu'elles ne soient demandées. Ces protocoles exigent que chaque nœud maintienne une table de routage indiquant par quel voisin passer pour atteindre un destinataire. Grâce à ces informations, chaque nœud dispose à tout instant d'un chemin vers n'importe quel autre nœud du réseau.

Pour traiter les changements de topologie, les nœuds diffusent des messages de contrôle à travers le réseau. Actuellement, les protocoles FSR (*Fisheye State Routing*) et OLSR (*Optimized Link State Routing*) ont été proposé pour les réseaux ad hoc véhiculaires [39].

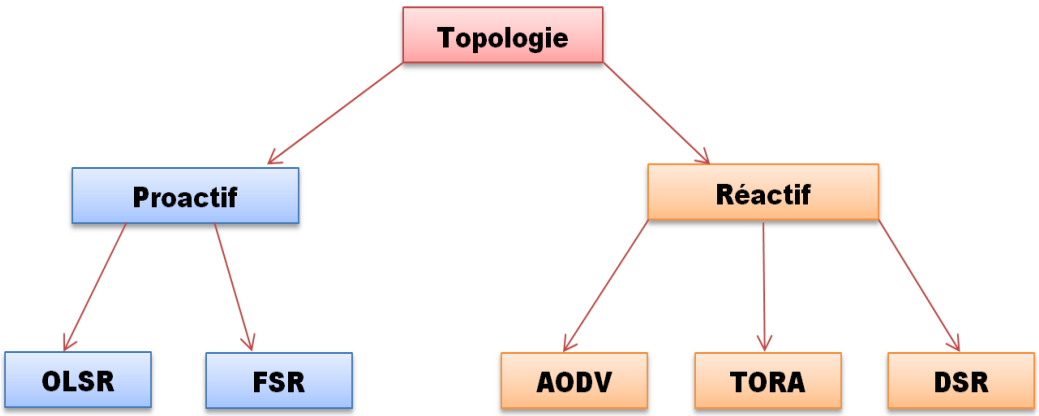


FIGURE 2.1 – Présentation des deux classes de la catégorie de routage basé sur la topologie

- **FSR (*Fisheye State Routing*) [39]**

Le protocole (*Routage à Etat de l'œil du Poisson*) est basé sur l'utilisation de la technique "*œil de poisson*" (*fisheye*), proposée par *Kleinrock et Stevens* [40], qui l'ont utilisé dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques. L'œil d'un poisson capture avec précision, les points proches du point focal. La précision diminue quand la distance, séparant le point vu et le point focal, augmente.

Dans le contexte du routage, ce principe se concrétise par le maintien des données concernant le chemin d'un voisin direct, avec une diminution progressive, de précision, quand la distance augmente. Le protocole FSR est similaire aux protocoles état de lien, dans sa sauvegarde de la topologie au niveau de chaque nœud. La différence principale, réside dans la manière avec laquelle les informations de routage circulent. Dans le FSR, la diffusion par inondation de messages n'existe pas. L'échange se fait uniquement avec les voisins directs.

Dans les protocoles état de lien traditionnel, si on détecte des changements de la topologie, les paquets d'états de liens sont générés et diffusés par inondation dans tout le réseau. Par contre, le FSR maintient la table - la plus récente - d'état des liens reçus à travers les voisins, et l'échange uniquement avec ses voisins locaux, d'une façon périodique. La réduction de volume des données de mise à jour, est obtenue en utilisant des périodes d'échanges différentes pour les différentes entrées de la table. Les entrées qui correspondent aux nœuds les plus proches, sont envoyées aux voisins avec une fréquence élevée (donc avec une période d'échange relativement petite).

Les informations de la topologie sont plus précises dans zone 1 du nœud centrale et devient de moins en moins précises dans les zone 2 et 3 selon le principe expliqué ci-dessus.

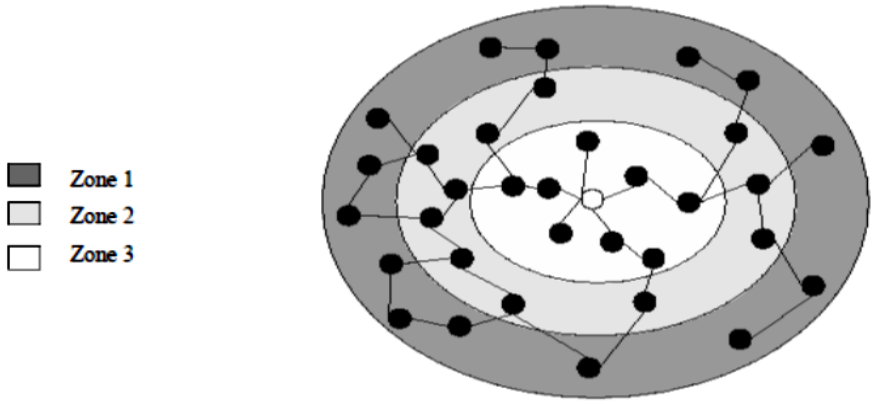


FIGURE 2.2 – Routage Fisheye State Routing [39]

- **OLSR (*Le protocole Optimized Link State Routing protocol*) [41]**

Est un protocole état de liens, qui optimise la manière de diffusion des messages de contrôle afin d'économiser la consommation de la bande passante, grâce à l'utilisation du concept des "*relais multipoints*" (*MPRs*), illustré sur la (figure 2.3). Dans lequel chaque nœud choisit un sous-ensemble de ses voisins pour retransmettre ses paquets en cas de diffusion.

En se basant sur la diffusion en utilisant les (*MPRs*), tous les nœuds du réseau sont atteints avec un nombre réduit de répétitions. Un ensemble de (*MPRs*) d'un nœud N est l'ensemble minimal de ses 1-saut voisins qui couvrent (dans le sens de la portée de communication) ses 2-sauts voisins.

Dans OLSR, chaque nœud diffuse périodiquement des messages *Hello* qui contient l'état de ses liens avec ses 1-saut voisins (*unidirectionnel, bidirectionnel ou MPR pour dire que ce voisin est un MPR*). Grâce aux messages *Hello*, un nœud construit sa table des voisins ainsi que la liste des voisins qui l'ont choisi comme MPR dits "*MPR-sélecteurs*". De plus, un nœud diffuse périodiquement des messages TC (*Topology Control*) qui contient la liste de ses MPR-sélecteurs.

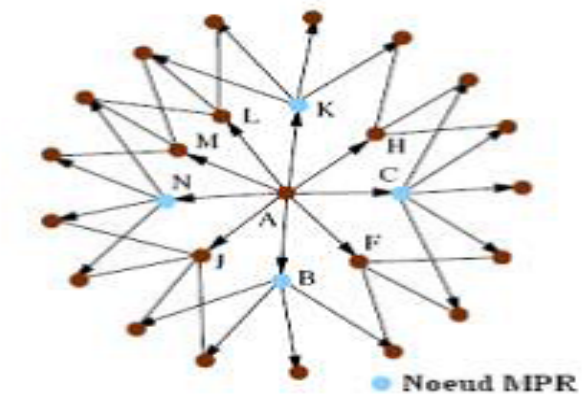


FIGURE 2.3 – Relais multipoints dans OLSR [41]

En exploitant ces messages, chaque nœud remplit les deux champs nommés "*destination*" (correspond aux MPR-sélecteurs dans le message TC) et "*dernier saut*" (prend comme valeur l'identificateur du nœud émetteur du message TC) d'une table dite de topologie. Les tables de topologie et des voisins sont exploitées pour construire la table de routage.

2.1.4.2 Protocoles réactifs

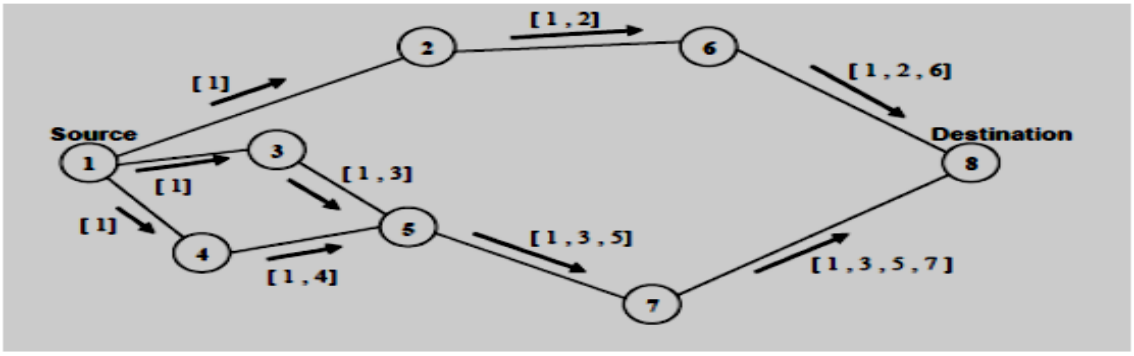
Les protocoles réactifs construisent des chemins uniquement lorsque ces derniers sont requis par un nœud source et ne gardent que les routes en cours d'utilisation par le processus de routage. On dit alors que la topologie du réseau est découverte à la demande.

Ainsi lorsqu'un nœud cherche à communiquer avec une destination pour laquelle il ne connait pas le chemin, il lance un processus de découverte dans le réseau (*généralement par inondation*). Cette phase de découverte se termine lorsque le chemin est trouvé. Ces chemins formés sont susceptibles d'être rompus à cause de la haute mobilité des véhicules. Les ruptures de liens sur les chemins sont alors traitées au moyen d'un mécanisme de maintenance, dont le but est de les identifier, puis si possible de les corriger.

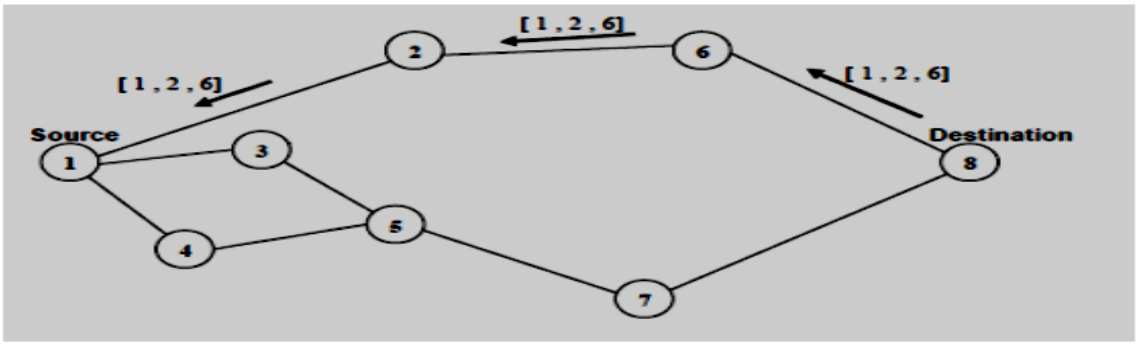
Dans ce qui suit, nous allons présenter les protocoles réactifs les plus connus, proposés par certains travaux de recherche pour effectuer le routage dans les réseaux ad hoc.

- **DSR (*Dynamic Source Routing*) [42]**

Le protocole DSR est basé sur l'utilisation de la technique "*routage source*". Dans cette technique, le trajet parcouru par le paquet est inclus dans l'en-tête du paquet de données à partir de la source. Les deux opérations de base du protocole DSR sont : **la découverte de routes** (*route discovery*) et **la maintenance de routes** (*route maintenance*). Un nœud source qui veut atteindre un nœud cible débute l'opération de découverte par la diffusion d'un paquet **requête de route**.



(a) : Construction de l'enregistrement de la route



(b) : renvoie du chemin dans le DSR

FIGURE 2.4 – Découvert de la route dans DSR

Si cette opération de découverte est réussite, le nœud initiateur reçoit un paquet **réponse de route** qui liste la séquence de nœuds à travers lesquels la destination peut être atteinte. En plus de l'adresse de la source, le paquet requête de route contient un champ **enregistrement de route**, dans lequel est accumulée la séquence des nœuds visités durant la propagation de la requête de route dans le réseau (voir la figure 2.4 (a)). Le paquet requête de route, contient aussi un identificateur unique de la requête. Dans le but de détecter les duplications

de réceptions de la requête de route, chaque nœud du réseau ad hoc maintient une liste de couples (*adresse source, identificateur de requête*), des requêtes récemment reçues. Pour réduire le coût de la découverte de routes, chaque nœud garde les chemins appris à l'aide des paquets de réponses (figure 2.4 (b)). Ces chemins sont utilisés jusqu'à ce qu'ils soient invalides.

Le protocole DSR exécute aussi une procédure de **maintenance de routes** quand un nœud détecte un problème fatal de transmission, à l'aide de sa couche de liaison.

Cette procédure est initiée par l'envoie d'un message erreur de route (*route error*) à l'émetteur original du paquet. Ce message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin. Lors de la réception du paquet erreur de route par l'hôte source, le nœud concerné par l'erreur est supprimé du chemin sauvegardé, et tous les chemins qui contiennent ce nœud sont coupés à ce point là. Par la suite, une nouvelle opération de découverte de routes vers la destination, est initiée par l'émetteur.

- **AODV (*Ad Hoc On Demand Distance Vector*) [43]**

Est un protocole réactif basé sur le principe des protocoles de routage à vecteur de distance. AODV hérite des deux mécanismes qui caractérisent le DSR et qui sont : la découverte et la maintenance des routes et utilise aussi un routage nœud à nœud et le principe des numéros de séquence.

Comme nous avons déjà dit, les réseaux ad hoc véhiculaires sont hautement mobiles, donc les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d'utiliser les routes les plus nouvelles.

Comme le protocole DSR, Lorsqu'un nœud source utilisant AODV désire établir une route vers une destination pour laquelle il ne possède pas encore de route, il diffuse un paquet (*route request*) RREQ à travers le réseau. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque nœud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement :

- l'adresse de la destination

- le nœud suivant
- la distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination)
- le numéro de séquence destination
- le temps d'expiration de l'entrée de la table

Le paquet RREQ envoyé contient l'*IP* de la source, le numéro de séquence courant et un identifiant de diffusion et le numéro de séquence de la destination le plus récent connu par la source. Un nœud recevant un paquet RREQ émettra alors un paquet RREP « *route reply* » s'il est la destination ou s'il possède une route vers la destination avec un numéro de séquence supérieur ou égal à celui repris dans le paquet RREQ. Si tel est le cas, il envoie un paquet RREP vers la source. Sinon, il rediffuse le paquet RREQ. Les nœuds conservent chacun une trace des *IP* sources et des identifiants de diffusion des paquets RREQ. S'ils reçoivent un paquet RREQ qu'ils ont déjà traité, ils le suppriment.

Les nœuds établissent le chemin vers la destination, alors que les paquets RREP reviennent vers la source. Une fois que la source a reçu les paquets RREP, elle peut commencer à émettre des paquets de données vers la destination. Si, ultérieurement, la source reçoit un RREP contenant un numéro de séquence supérieur ou bien le même, mais avec un nombre de sauts plus petits, elle mettra à jour son information de routage vers cette destination et commencera à utiliser la meilleure route.

Afin de maintenir des routes consistantes, une transmission périodique du message "*HELLO*" est effectuée. Si trois messages "*HELLO*" ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant. Dans le cas toutes les entrées des tables de routage participantes dans le chemin actif et qui sont concernées par la défaillance sont supprimées. Cela est accompli par la diffusion d'un message d'erreur entre les nœuds.

- **TORA (*Temporally-Ordered Routing Algorithm*) [44]**

Est un protocole de routage distribué basé sur un algorithme "*d'inversion de lien*". Il est conçu pour découvrir des routes à la demande, fournir des voies multiples vers une destination et de minimiser la surcharge de la communication réseau par la localisation des changements topologiques lorsque cela est possible.

L'optimalité de la route (*chemin le plus court*) est considéré comme d'importance secondaire, et des routes plus longues sont souvent utilisés pour éviter la surcharge de la découverte de nouvelles routes. Il n'est pas nécessaire (ni souhaitable) de maintenir les liaisons entre toutes les paires de sources / destinations à tout moment.

Pour découvrir une nouvelle route, il utilise la propriété appelée "*orientation destination*" des graphes acycliques orientés et utilise également un ensemble de valeurs de taille des nœuds totalement ordonnées à tout moment. Cette taille est utilisée dans l'orientation des liens du réseau. Un lien est toujours orienté du nœud qui a la plus grande taille vers le nœud qui la plus petite taille. Le protocole est basé sur trois fonctionnalités : la création des routes, la maintenance des routes et l'effacement des routes en utilisant trois paquets distincts QRY, UPD et CLR.

Lorsqu'un nœud a besoin d'un itinéraire vers une destination particulière, il diffuse un paquet route query contenant l'adresse de la destination. Ce paquet se propage à travers le réseau jusqu'à ce qu'il atteigne soit la destination ou un nœud intermédiaire ayant un itinéraire vers la destination. Le récepteur du paquet requête diffuse alors un paquet de mise à jour indiquant sa taille par rapport à la destination (*si le récepteur est la destination, cette hauteur est 0*). Comme ce paquet se propage en arrière à travers le réseau, chaque nœud qui reçoit la mise à jour définit sa taille à une valeur supérieure à la taille de la voisine à partir de laquelle la mise à jour a été reçue. Cela a pour effet de créer une série de liens dirigés de l'émetteur de la requête au nœud qui initialement généré la mise à jour. Un exemple de ce processus est illustré dans la (figure 2.5).

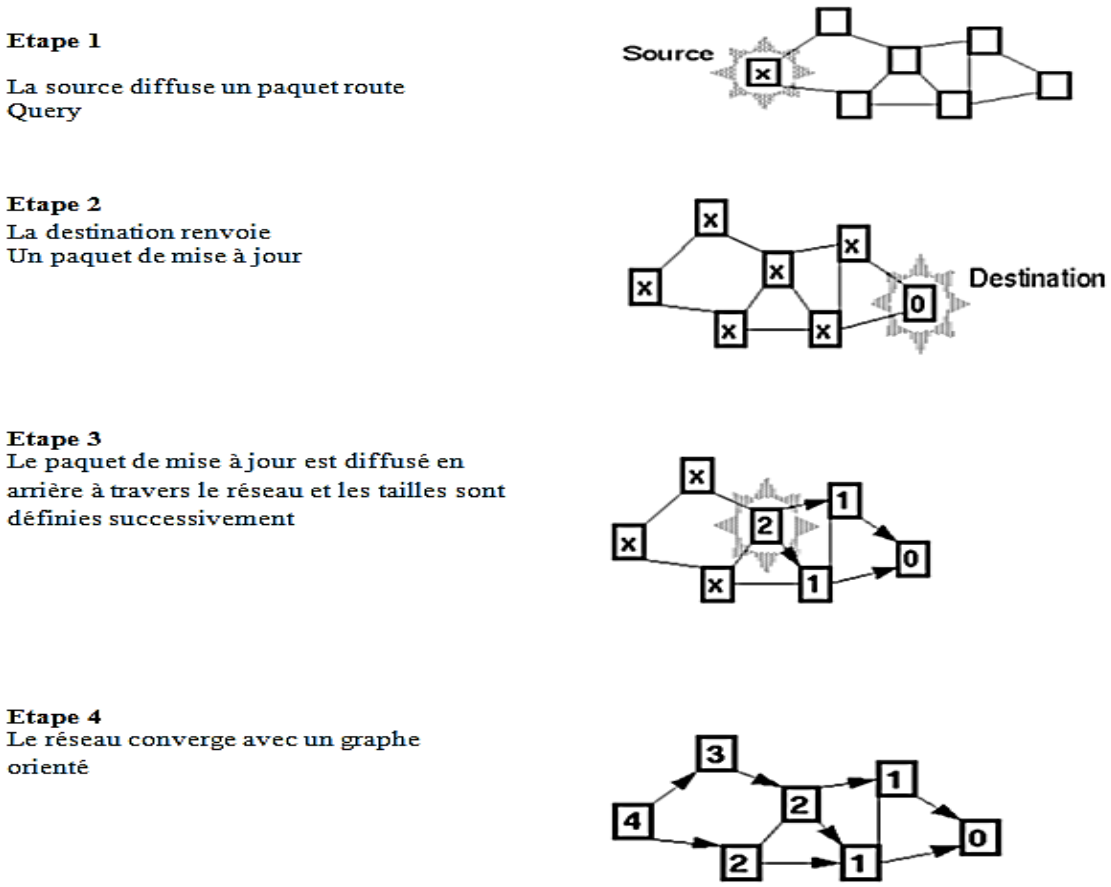


FIGURE 2.5 – Génération d'un graphe ordonné de TORA [44]

Lorsqu'un nœud découvre qu'une route vers une destination n'est plus valide, il ajuste sa taille de sorte qu'il soit un maximum local par rapport à ses voisins et transmet un paquet de mise à jour. Ce processus est illustré à la (figure 2.6).

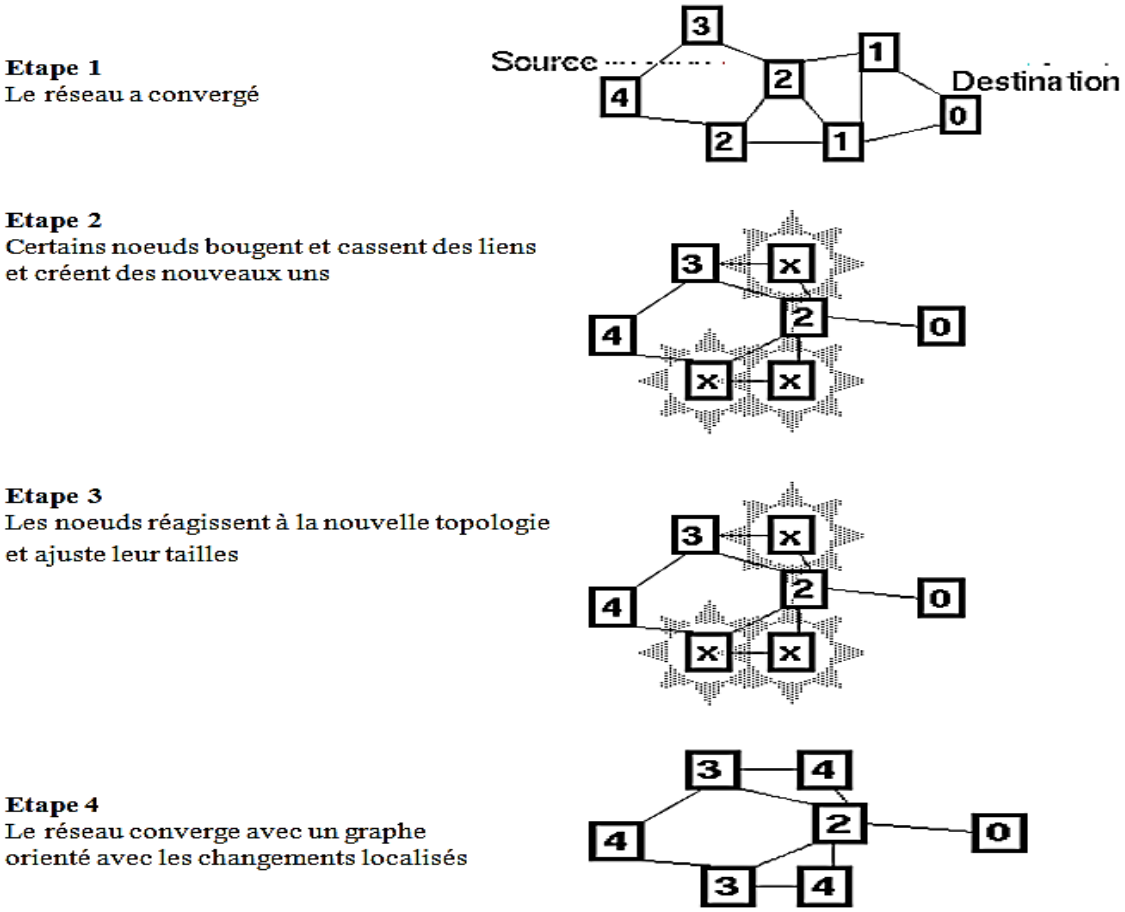


FIGURE 2.6 – La réaction du protocole TORA à la mobilité des nœuds [44]

2.2 Routage basé sur la position

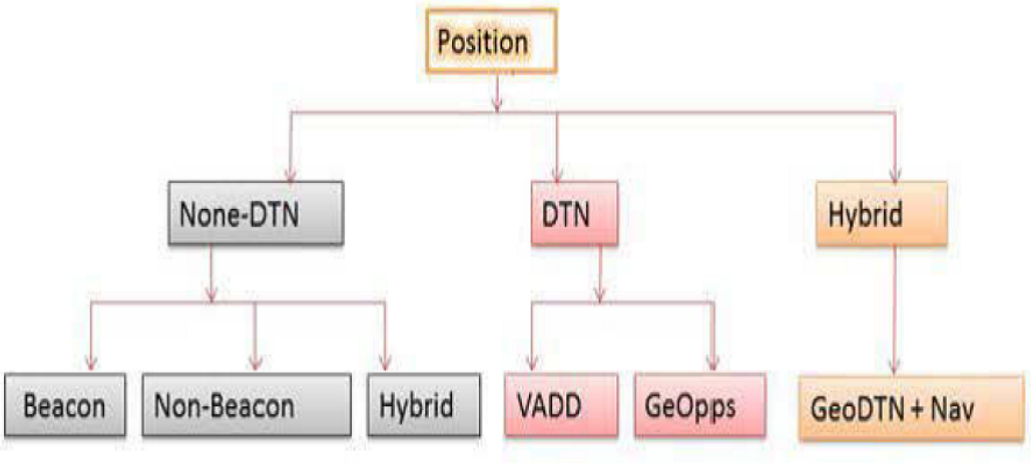


FIGURE 2.7 – Protocole de routage basé sur la position

Dans le routage géographique (*basé sur la position*), la décision de transmission par un nœud est basée essentiellement sur la position des paquets de destination et sur la position du nœud voisin à un saut. Les données de la position de la destination sont stockées dans l'en-tête du paquet par la source. Quant à la position du nœud voisin à un saut, elle est obtenue par les balises envoyées périodiquement avec une gigue aléatoire (*pour éviter une collision*). Les nœuds qui sont à portée radio d'un nœud vont devenir les voisins du nœud.

Le routage ad hoc basé sur la position implique que chaque nœud connaisse sa propre position et que le nœud émetteur connaisse la position du nœud de réception. Un exemple de ce type de routage ad hoc est l'unité du système mondial de localisation (*GPS*), dont la popularité n'est pas à démontrer, qui est à la base de plusieurs systèmes de navigations embarqués et de la recherche récente sur les services de localisation [45].

Les protocoles de routage géographique n'échangent pas d'information sur l'état (*bande passante, délai de transmission, coût d'utilisation, etc.*) des liens disponible au sein d'un mobile et ne maintiennent pas de routes établies comme dans les protocoles de routages conventionnels basés sur la topologie. Ce type de protocole de routage semble selon les dernières études plus promettant en termes de robustesse et de gestion d'une mobilité hautement dynamiques. En

d'autres termes, c'est par la route déterminée en se basant sur la localisation géographique des nœuds voisins que le paquet est transmis. Il n'est pas nécessaire de changer l'état du lien ou de configurer l'installation.

Les protocoles de routage géographique défissent une zone de transfert qui permet de recevoir les paquets par inondation afin de réduire la charge du réseau (*network overhead*) et la congestion du réseau en inondant tout le réseau. Le routage à destination unique (*unicast*) peut quant à lui être utilisé pour expédier les paquets dans la zone de transfert de destination. En effet, les paquets sont envoyés en premier lieu avec un échange (*unicast*) vers la zone de transfert où se trouve le destinataire, puis ils sont diffusés au niveau de toute la zone de transfert par inondation pour atteindre le destinateur des paquets. En d'autres termes, c'est par la route déterminée en se basant sur la localisation géographique des nœuds voisins que le paquet est transmis. Il n'est pas nécessaire de changer l'état du lien ou de configurer l'installation.

Le routage géographique se divise en trois catégories : les réseaux non-tolérants au délai non-DTN (*non-Delay Tolerant Network*), les réseaux tolérants au délai DTN (*Delay Tolerant Network*) et les réseaux hybrides (figure 2.7). Les protocoles de routage géographiques de type non-DTN ne prennent pas en considération la connectivité intermittente et ne sont pratiques que pour les VANET très denses, tandis que ceux de type DTN prennent en considération la dé connectivité. Cependant les non-DTN sont conçus dans l'idée que les réseaux soient déconnectés par défaut. Les protocoles de routage géographiques de type hybride combinent les protocoles de routage non-DTN et DTN pour exploiter la connectivité partielle du réseau.

2.2.1 Quelque exemple de protocole basé sur la position

- **GPSR (*Greedy Perimeter Stateless Routing*) [46] [47]**

GPSR est un protocole de routage réactif et efficace pour les réseaux ad hoc véhiculaire qui exploite la correspondance entre la position géographique et la connectivité dans un réseau sans fil afin de prendre des décisions de transfert de paquets.

Dans un réseau VANET, les nœuds sont susceptibles de se déplacer. Il est donc nécessaire d'utiliser un mécanisme qui permet à chaque nœud de connaître la position de ses voisins,

afin de signaler leur présence et leur localisation, les nœuds inondent le réseau en envoyant un paquet de signalement (*messages« beacon»*) contenant la position et un identifiant (par exemple, son adresse *IP*). L'échange périodique de ces paquets permet aux nœuds de construire leur table de position. La période d'émission des messages « *beacon* » dépend du taux de mobilité dans le réseau ainsi que de la portée radio des nœuds. En effet, lorsqu'un nœud ne reçoit pas de message « *beacon* » d'un voisin après un temps T, il considère que le voisin en question n'est plus dans sa zone de couverture et l'efface de sa table de position. Un des avantages des messages « *beacon* » est qu'un nœud n'a pas besoin que des informations sur ses voisins directs, ce qui nécessite peu de mémoire. Alternativement, le protocole GPSR permet au nœud d'encapsuler sur quelques bits leur position dans les paquets de données qu'il envoie [46]. Dans ce cas, toutes les interfaces des nœuds doivent être en mode promiscuité afin de recevoir les paquets s'ils se trouvent dans la zone de couverture de l'émetteur.

L'acheminement des paquets par GPSR se fait selon deux modes suivant la densité du réseau : le « *Greedy Forwarding* » et le « *Perimeter Forwarding* » (appelés respectivement *GF* et *PF* dans la suite).

Greedy Forwarding

Le GF construit un chemin parcourant les nœuds de la source à la destination où chaque nœud qui reçoit un paquet l'achemine en faisant un saut vers le nœud intermédiaire le plus proche de la destination dans sa zone de couverture. La (figure 2.8) montre un exemple de ce mode d'acheminement.

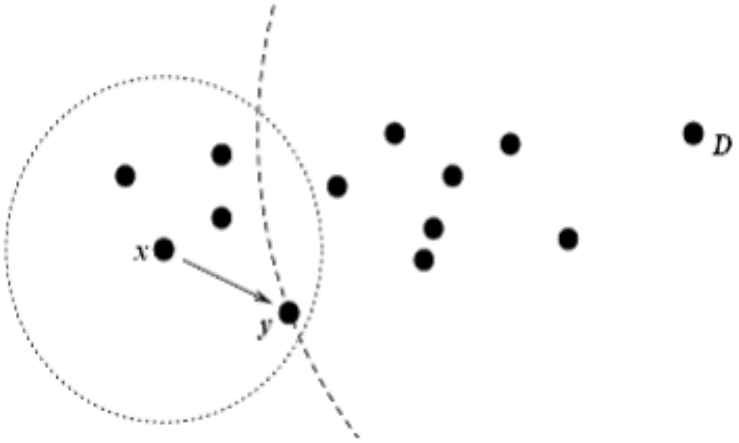


FIGURE 2.8 – y est le voisin de x le plus proche de la destination D

La méthode « *Perimeter Forwarding* », est utilisé lorsqu'un nœud ne trouve aucun voisin plus proche que lui de la destination ou la destination ne se trouve pas à la portée de celui-ci. La (figure 2.9) montre un exemple de ce problème d'acheminement.

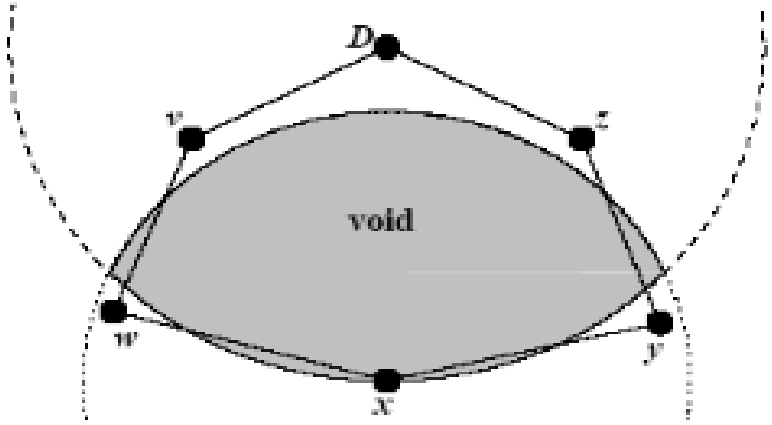


FIGURE 2.9 – X est plus proche de D que ses voisins y, w

Perimeter Forwarding

L a méthode « *perimeter Forwarding* » consiste à transformer la topologie du réseau en un graphe planaire (ne contenant pas des arrêtes qui se croisent). Ce graphe peut être de type RNG (*Relative Neighborhood Graph*) ou GG (*Gabriel Graph*) (figure 2.10).

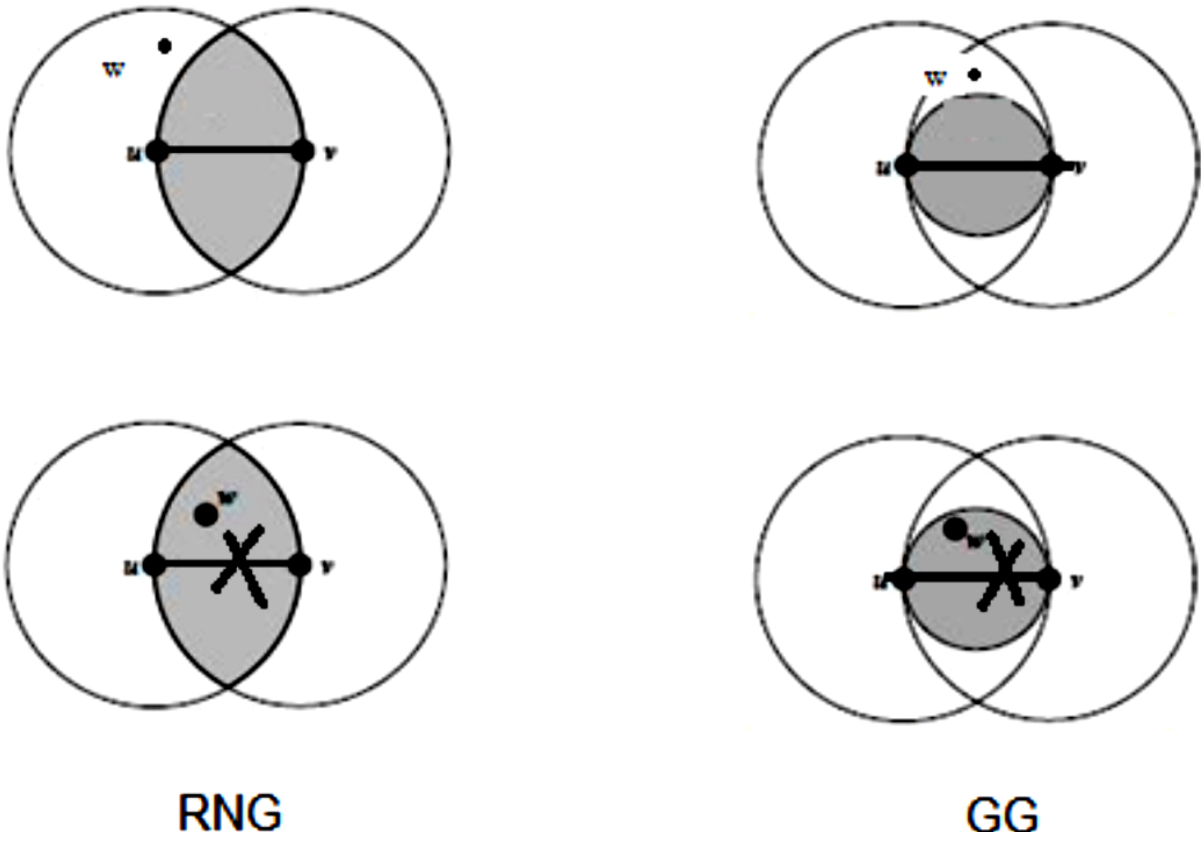


FIGURE 2.10 – Principe des graphes RNG et GG

Les graphes (*Gabriel graph et Relative Neighborhood graph*) sont deux cas des graphes de proximité qui visent à représenter la disposition des points d'un ensemble dans l'espace. Dans un tel graphique, deux points sont reliés par une arrête s'il n'y a pas d'autres points dans une certaine «*zone interdite*»

Ensuite le paquet traverse le graphe jusqu'à la destination en utilisant la règle de la main droite « *Right-Hand Rule* » définit comme suit : Lorsqu'un paquet arrive à un nœud x du nœud y, le chemin à suivre est le prochain qui se trouve dans le sens inverse des aiguilles d'une montre en partant de x et par rapport au segment $[x\ y]$ tout en évitant les « *crossing links* » (route déjà parcourue).

Pour conclure nous allons décrire le protocole GPSR en combinant entre les deux méthodes de routage : Un paquet GPSR contient dans son en-tête un champ pour le mode de routage. Ce champ contient « *Greedy* » lorsque le routage est « *greedy forwarding*» et « *Perimeter* »

lorsque le routage est « *Perimeter forwarding* ». Un nœud x recevant un paquet en mode « *Greedy* » examine sa table de voisins. S'il trouve le voisin le plus proche de la destination alors il lui transmet le paquet. Dans le cas contraire, le nœud va modifier le champ mode de l'en-tête du paquet par « *Perimeter* » et enregistre sa localisation. Ensuite, il construit un graphe planaire à partir de ses voisins et transmet son paquet à travers ce graphe. La (figure 2.11) montre un exemple de ce mode d'acheminement.

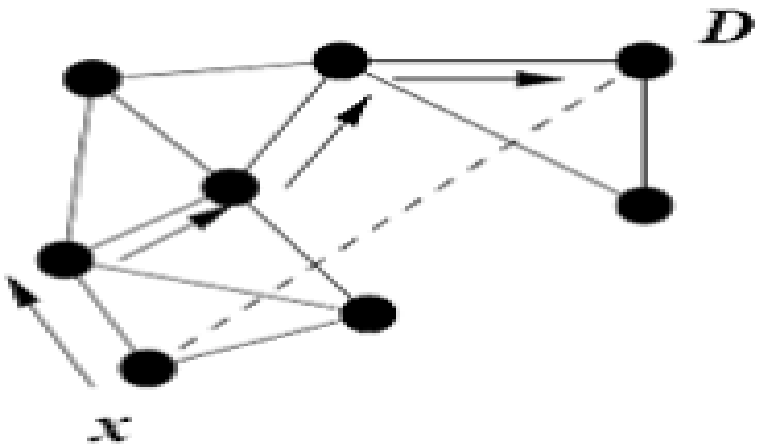


FIGURE 2.11 – Perimeter forwarding. D est la destination ; x est le nœud où le paquet entre en mode Perimeter

- **GSR (*Geographic Source Routing*)**[48]

Le protocole GSR tente de pallier les inconvénients du GPSR dans des scénarios urbains. En utilisant l'emplacement de la destination, le plan de la ville (*cartographie des routes*) et l'emplacement du nœud source, GSR calcule une séquence de jonctions que le paquet doit traverser pour atteindre la destination. Le protocole vise à calculer le plus court chemin entre l'origine et la destination en appliquant l'algorithme Dijkstra sur la carte routière.

Le plus court chemin calculé est composé d'une séquence de jonctions que le paquet d'un véhicule source S doit suivre pour atteindre le véhicule de destination D. Le routage (*Greedy forwarding*) est utilisé pour transmettre des paquets entre deux jonctions impliqués. L'inconvénient de GSR est que le chemin le plus court n'est pas le chemin optimal, car il ne considère pas la circulation des véhicules dans la rue. De plus, il utilise mécanisme de sélection de jonc-

tion fixe où la source S calcule à la fois la séquence de jonctions par lesquelles le paquet doit passer pour atteindre la destination D.

- **GPCR (*Greedy Perimeter Coordinator Routing*) [49]**

Comme GPCR est basé sur le fait que les rues de la ville forment un «*graphe planaire naturel*» et modifie la stratégie de transfert *greedy Forwarding* de telle sorte qu'il n'achemine les messages qu'à travers des intersections rues (figure 2.12), en éliminant l'exigence d'un plan des rues statique externe pour son fonctionnement. L'objectif est de transmettre les paquets vers des nœuds à une intersection, plutôt que de les transmettre à un nœud qui est déjà passé l'intersection. Les nœuds qui sont situés dans la zone d'une intersection sont appelé «*coordonnateurs*». Les nœuds peuvent déterminer s'ils sont coordinateurs en utilisant l'un des deux approches suivantes :

La première approche est l'approche des tables voisines. Dans cette approche, les nœuds transmettent périodiquement des paquets *beacons* qui contiennent les informations de position et les informations de dernière position connue de tous leurs voisins.

En utilisant cette information, un nœud x s'estime être dans une intersection s'il a deux voisins y et z qui sont à portée de transmission, mais aucun d'eux n'indique que l'autre est son voisin. Une telle situation implique que y et z sont séparés par un obstacle et que x nœud peut transmettre les paquets afin de contourner cet obstacle.

La seconde approche (l'approche des coefficients de corrélation) utilise les informations de position d'un nœud et l'information de position de ses voisins immédiats afin calculer le coefficient de corrélation ρ , par rapport à ses voisins. Une forte corrélation linéaire entre les positions des nœuds voisins (ρ *est proche de 1*) indique que le nœud est présent dans une rue. S'il n'y a pas de corrélation linéaire entre les positions des voisins du nœud (ρ *est proche de 0*), ce qui indique que le nœud se trouve à une intersection. Grâce à l'ajustement d'un seuil ε, un nœud peut évaluer le coefficient de corrélation et de supposer que $\rho \geq \varepsilon$ indique le nœud est dans une rue et $\rho < \varepsilon$ indique que le nœud est à une intersection.

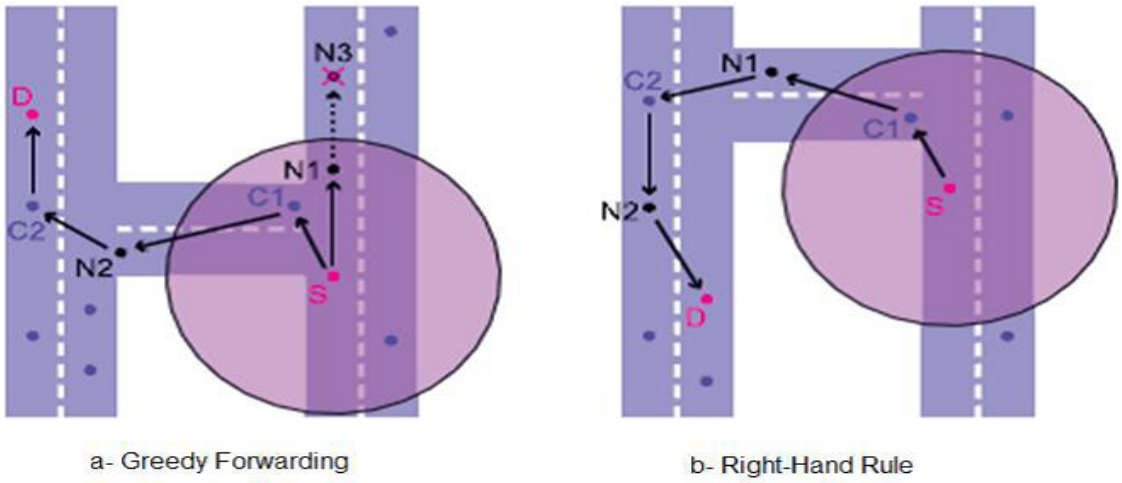


FIGURE 2.12 – L'acheminement des paquets dans GPCR

- **A-STAR (*Anchor-based Street and Traffic Aware Routing*) [50]**

A-STAR est un protocole de routage basé sur la position géographique pour un environnement véhiculaire métropolitain qui utilise les informations sur les itinéraires d'autobus de ville pour identifier un trajet d'intersection (*anchor route*) avec une connectivité élevée pour l'acheminement des paquets.

A-STAR est similaire au protocole GSR dans l'utilisation de la cartographie des routes. Cependant, contrairement à GSR il calcule les "*anchor paths*" en fonction du trafic (trafics de bus, véhicules, etc...). Un poids est assigné à chaque rue en fonction de sa capacité (grande ou petite rue qui est desservie par un nombre de bus différent). Un chemin trajet d'intersection (*Anchor route*) peut donc être calculé en utilisant l'algorithme de Dijkstra (*chemin de plus faible poids*). Les informations des routes fournies par les bus donnent une idée sur la charge de trafic dans chaque rue. Ce qui donne une image de la ville à des moments différents.

Conclusion

Dans ce chapitre nous avons présenté le concept de routage dans les réseaux VANETs, la classification des protocoles selon différentes critères, et nous avons terminé par une présentation de quelques protocoles les plus utilisés dans le routage basé sur la position.

Dans le prochain chapitre nous abordons La sécurité dans les réseaux VANETs.

3

La sécurité dans les réseaux VANETs

Introduction

Les communications véhiculaires constitueront dans le futur le plus grand réseau ad-hoc viable. De plus, la vie de milliers d'êtres humains sera dépendante des informations échangées entre les véhicules eux-mêmes et avec les infrastructures. A cause de l'importance des informations échangées et du nombre énorme d'utilisateurs, l'environnement des réseaux véhiculaires sera plus qu'hostile. En effet, les messages liés à la sécurité peuvent être falsifiés ou éliminés par des entités malveillantes afin de causer des accidents et mettre en péril la vie des personnes. Donc, avant le déploiement de ces réseaux, des mécanismes de sécurité appropriés doivent être mis en œuvre afin d'éviter ces mauvais scénarios et d'identifier les entités responsables de ces activités malveillantes.

Dans ce chapitre, nous présentons un récapitulatif sur les outils et les mécanismes de base de la sécurité en générale, nous passons en revue la sécurité dans les réseaux sans-fil, ensuite nous présentons les problèmes et les mécanismes de base de sécurité dans les VANETs, enfin nous citons quelques techniques et solutions de sécurité existantes qui peuvent être mises en œuvre afin de sécuriser les informations échangées à travers ces réseaux.

3.1 La sécurité dans les réseaux ad-hoc

Comme les réseaux VANETs est une sous classe des réseaux sans-fil ad-hoc, ils en héritent les problèmes de sécurité. Dans cette section, nous nous intéressons à la sécurité des réseaux sans-fil ad-hoc de manière générale, nous en décrivons les objectifs de sécurité, ensuite nous présentons quelques exemples d'attaques sur ces réseaux.

3.1.1 Caractéristiques de la sécurité dans les réseaux ad hoc

Lors de l'analyse de la nature des communications dans les réseaux ad hoc, des propriétés spécifiques liées à la sécurité et la confidentialité doivent être prises en compte pour la conception des protocoles de communications, à savoir [51] :

3.1.1.1 Un support de transmission partagé

Comme avec tout système de communication sans-fil, l'utilisation des ondes radio permet aux attaquants d'intercepter facilement les messages échangés ou bien d'injecter de faux messages dans le réseau.

3.1.1.2 Les communications multi-sauts

Les protocoles de communications multi-sauts sont obligatoires pour avoir des communications sans-fil à longue portée dans les réseaux ad hoc, cela signifie que tous les nœuds doivent coopérer pour assurer le fonctionnement du réseau. Malheureusement, les nœuds malveillants peuvent exploiter ce principe et mettre en péril la sécurité du réseau, donc des mécanismes de sécurité appropriés doivent être mis en œuvre.

3.1.1.3 La diffusion d'information de la position géographique

Avec certains protocoles dans les réseaux ad hoc mobiles, les nœuds sont supposés envoyer périodiquement des messages (*beacon*) indiquant leurs positions courantes ou éventuellement d'autres données nécessaires pour des services spécifiques. Par conséquent, les attaquants peuvent créer un profil sur les trajectoires des nœuds et donc les utilisateurs du réseau.

3.1.1.4 Les opérations autonomes

Les nœuds eux-mêmes déterminent leurs états et décident des informations à envoyer de manière autonome. Par conséquent, il est facile pour les entités malveillantes qui ont le contrôle sur un ou plusieurs nœuds d'envoyer des informations falsifiées. Les systèmes de sécurité, à leur tour, doivent employer des mécanismes qui détectent et empêchent l'utilisation de ces informations.

3.1.2 Les objectifs de la sécurité

La sécurisation des communications dans les réseaux sans-fil comme dans les réseaux filaires nécessite la mise en œuvre de mécanismes permettant d'atteindre un certain nombre d'objectifs généraux de sécurité. Ces objectifs comprennent [52] :

3.1.2.1 L'authentification

Cet objectif de sécurité permet aux membres du réseau de s'assurer de la bonne identité des membres avec lesquels ils communiquent.

3.1.2.2 La non-répudiation

Cet objectif de sécurité permet de s'assurer qu'aucun émetteur ne peut nier d'être à l'origine d'un message. Cet objectif est indispensable dans les transactions électroniques et dans toutes les communications sensibles.

3.1.2.3 La confidentialité

Cet objectif de sécurité garantit que seules les parties autorisées peuvent accéder aux données transmises à travers le réseau. Ces données peuvent concerner la couche applicative ou les couches inférieures.

3.1.2.4 L'intégrité

Cet objectif de sécurité permet de s'assurer que les données échangées ne sont pas soumises à une altération volontaire ou accidentelle. Donc, il permet aux destinataires de détecter les manipulations de données effectuées par les entités non autorisées et rejeter les paquets correspondants.

3.1.2.5 La disponibilité

Cet objectif de sécurité vise à garantir aux entités autorisées d'accéder aux ressources du réseau avec une qualité de service adéquate [52].

3.1.3 Le modèle d'un attaquant

La première étape pour sécuriser un système est l'identification de la nature des éventuels attaquants. Dans les réseaux ad-hoc, nous pouvons classifier un attaquant selon les dimensions suivantes :

3.1.3.1 Interne vs. Externe

L'attaquant interne est perçu comme un membre normal du réseau et peut communiquer avec les autres membres. La présence des attaques internes est très problématique et difficile à détecter, car elle annule le niveau de sécurité assuré par les techniques cryptographiques. L'attaquant externe est considéré par les nœuds membres comme un intrus et est donc limité dans la diversité des attaques qu'il peut provoquer [53].

3.1.3.2 Malveillant vs Rationnel

Un attaquant malveillant n'a pas d'intérêts personnels à travers ses attaques et a pour but le dysfonctionnement du réseau. Par conséquent, il peut employer tous les moyens sans tenir compte des coûts correspondants et des conséquences. Par contre, un attaquant rationnel cherche un profit personnel, et ainsi, on peut prévoir les cibles d'attaques et les moyens employés [55].

3.1.3.3 Passif vs. Actif

L'attaquant passif écoute simplement les informations qui sont échangées entre les nœuds tandis que l'attaquant actif agit sur les informations qui sont échangées. Il peut les falsifier, les modifier, voire même les détruire [53].

3.1.4 Les attaques dans les réseaux sans-fil ad-hoc

Dans les réseaux sans-fil ad-hoc, la nature du support de transmission rend ces réseaux plus vulnérables aux attaques qu'un réseau filaire. Un réseau sans-fil qui n'est pas bien sécurisé est exposé à de plusieurs types d'attaques, nous en citons :

3.1.4.1 L'écoute des communications

Dans ce type d'attaque, l'adversaire ou l'entité malveillante écoute sur le support de transmission afin d'extraire des informations sur le trafic échangé dans son voisinage ; il se peut qu'il veuille espionner sur des informations personnelles, ou bien collecter des informations pour les analyser.

3.1.4.2 L'accès non-autorisé

Dans cette attaque, les entités malveillantes accèdent aux services du réseau sans en avoir les droits ou les privilèges [52].

3.1.4.3 Le déni de service

DoS (*Denial of Service*) consiste à rendre les différentes ressources et les services indisponibles pour les utilisateurs dans le réseau, il est généralement provoqué par d'autres attaques visant la bande passante ou les ressources énergétiques des autres nœuds. La technique la plus naïve pour causer un déni de service dans un réseau sans-fil consiste à causer le brouillage du canal, une autre attaque appelée (*privation de sommeil*) qui consiste à demander un service que le nœud visé offre de manière répétitive afin de lui gaspiller ses ressources systèmes et de l'empêcher de "*se reposer*" [54].

3.1.4.4 L'usurpation de l'identité d'un nœud

Dans ce type d'attaques, l'attaquant essaie de prendre l'identité d'un autre nœud afin de pouvoir recevoir ses messages ou d'avoir des privilèges qui ne lui sont pas accordés.

3.2 Attaques spécifiques sur les VANETs

Dans cette section, nous passons en revue quelques attaques spécifiques sur les VANETs. Ces attaques comprennent :

3.2.1 L'injection des messages erronés

Dans cette attaque l'entité malveillante crée des messages contenant des informations erronées afin de causer un accident ou de rediriger le trafic routier de manière permettant la libération de la route utilisée (figure 3.1) [55].

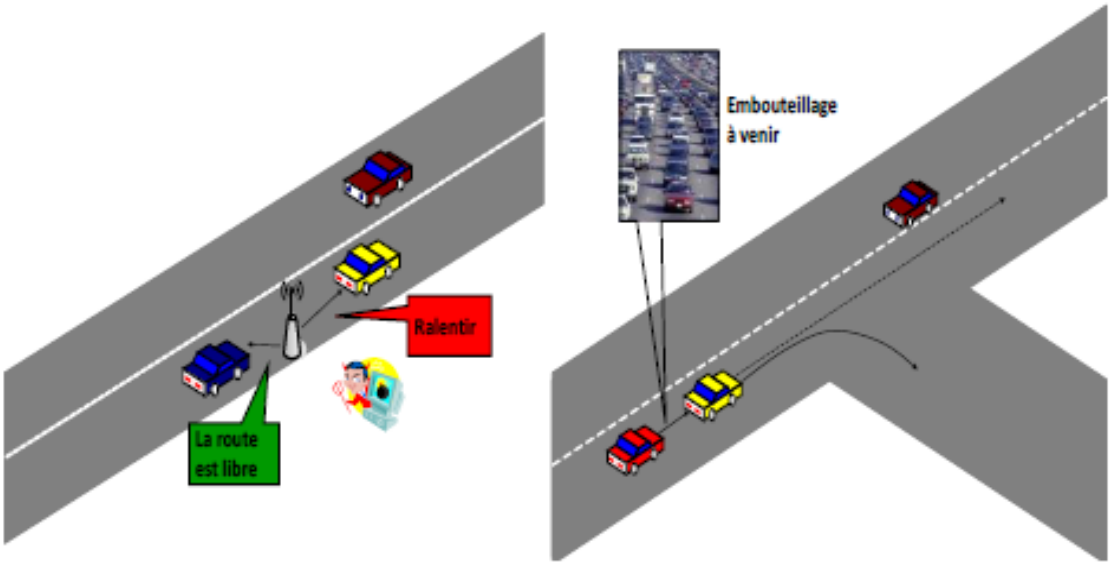


FIGURE 3.1 – Attaques par l'envoi de messages falsifiés [55]

3.2.2 Le déni de service[60]

L'objectif de cette attaque est d'empêcher la réception d'un message lié à la sécurité, donc il vise à annuler les services de sécurité offerts par ces réseaux.

La figure (3.2) montre l'attaque en utilisant le brouillage du canal, l'attaquant empêche *V1* et *V2* à recevoir les messages liés à la sécurité.

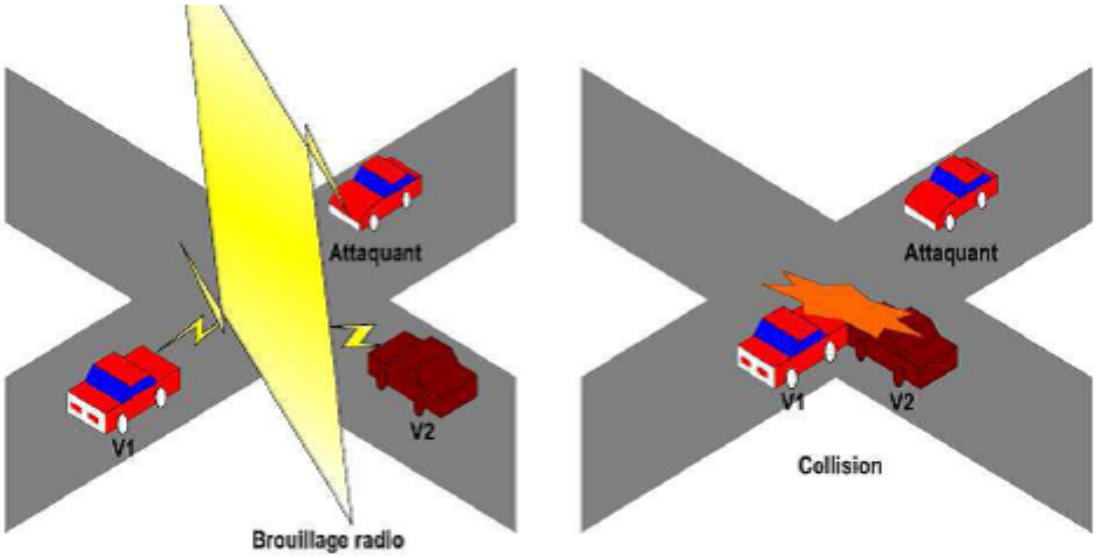


FIGURE 3.2 – Attaque déni de service [56]

3.2.3 La révélation d'identité et de position géographique des autres véhicules

Dans cette attaque, l'entité malveillante collecte des informations sur les transmissions radio effectuées par le véhicule victime afin de surveiller sa trajectoire. L'utilité de cette attaque est diverse et dépend de l'entité collectant ces informations (il peut être par exemple une entreprise de location de voitures qui veut suivre ses propres véhicules de manière illégitime) (figure 3.3).

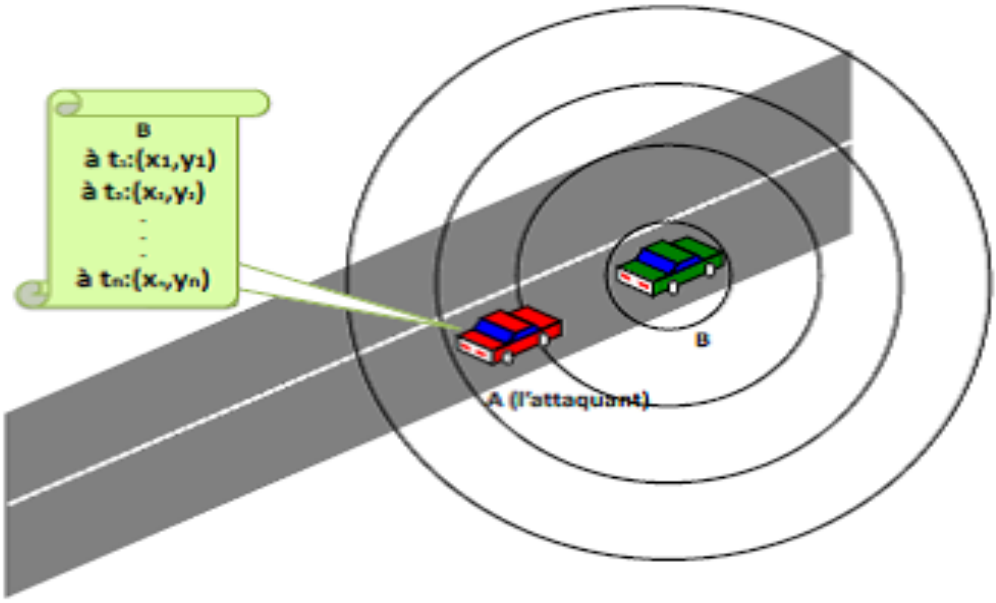


FIGURE 3.3 – Attaque de révélation d'identité et de position géographique d'un véhicule[56]

3.3 Les éléments de base de la sécurité dans les VANETs

3.3.1 Le TPD (*Tamper-Proof Device*)[57]

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.

Le TPD est conçu de manière à détruire automatiquement toutes les informations stockées lors de la manipulation matérielle. A cet effet, il contient un ensemble de capteurs qui lui permettent de détecter ces manipulations et effacer toutes les informations stockées afin de les empêcher d'être compromises [58]. Ce module est connu aussi sous le nom de HSM (*Hardware Security Module*) [57].

3.3.2 Les certificats dans les VANETs[59]

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 :

3.3.2.1 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 et renouveler les certificats à court terme.

3.3.2.2 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, 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.

3.3.3 La sécurité du système de balisage [57]

Le balisage (*Beaconing*) consiste en la diffusion périodique aux voisins a-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 (*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 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. Le format d'un paquet balise est illustré dans la figure ci-dessous.

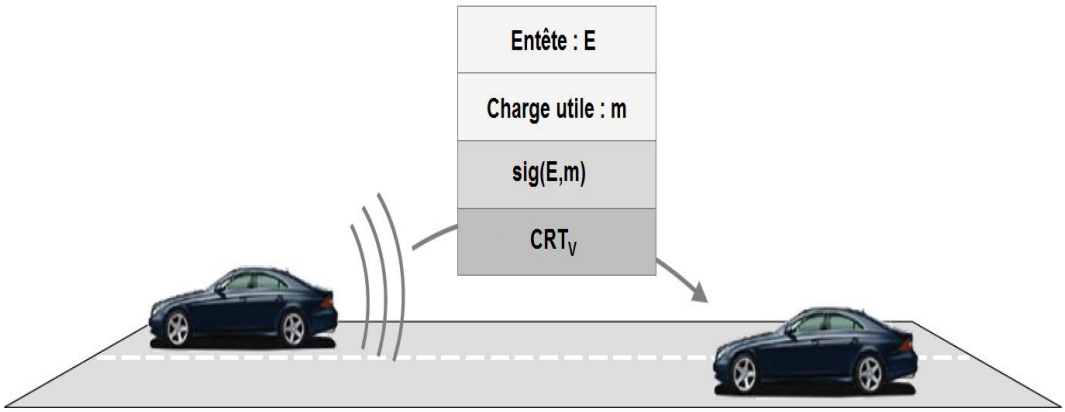


FIGURE 3.4 – Format d'un paquet balise[57]

3.4 Solutions pour la sécurisation des VANETs

Plusieurs solutions ont été proposées pour adresser le problème de la sécurité dans les VANETs. Dans cette section, nous présentons quelques solutions.

3.4.1 Base CRL

L'idée de base de l'approche traditionnelle pour la distribution du CRL [60, 61] est de distribuer la liste complète à un intervalle spécifié. Cette méthode nécessite un temps élevé de recherche dans la CRL, vu que la taille de la liste augmente au fil du temps par rapport au nombre de véhicules dans le réseaux.

3.4.2 Delta CRL

Pour réduire le coût élevé de l'envoi d'une nouvelle liste CRL de base à chaque période de mise à jour, l'émetteur de la CRL peut ne transmettre que les modifications apportées à la liste CRL de base. La distribution de la liste CRL de base à un intervalle régulier est beaucoup plus grande que l'intervalle d'émission Delta CRL. Par exemple, une liste CRL de base pourrait être envoyé le premier jour de chaque mois, avec, quotidiennement ; le Delta CRL contenant uniquement les modifications de la liste CRL de base. La taille du Delta CRL augmente au fil du temps que d'autres changements sont ajoutés à partir de la liste CRL de base.

3.4.3 CRL partitionnée

L'approche du CRL partitionnée est abordée dans [62], c'est une autre méthode pour réduire la taille de la CRL. Elle sert à organiser les certificats en groupes pour établir une hiérarchie des certificats pour accélérer la distribution et la recherche dans la liste. Les groupes sont établis par la CA.

3.4.4 Compressed CRL (*Bloom Filter*)

Cette méthode consiste à utiliser des techniques de compression à savoir le bloom filter. L'idée générale de CRL compressée à été exploitée dans plusieurs travaux de recherche [63, 64, 65]. Dans cette approche, chaque certificat révoqué est haché à un nombre fixe de bits à plusieurs reprises. La valeur de hachage pour chaque certificat révoqué forme un type de signature. Les signatures de plusieurs certificats révoqués peuvent être combinées en une séquence de bits unique. Chaque fois qu'un certificat est reçu, les mêmes hachés sont effectués et la valeur résultante est vérifiée par rapport au filtre de Bloom. Si la signature correspond à un modèle dans le filtre Bloom, cela signifie que le certificat a été révoqué avec une forte probabilité. De cette manière la taille de CRL diminue considérablement. Ainsi, le bloom filter sera distribué au lieu de distribuer 8 à 14 octets pour chaque certificat révoqué. Dans [66], Haas, Hu et Laberteaux explorent cette méthode beaucoup plus en détail.

Conclusion

Plusieurs approches ont été définies pour la sécurisation des VANETs, certaines sont générales et d'autres sont spécifiques. Le challenges demeure cependant de proposer une méthode qui permette de protéger les VANETs dans son ensemble et en considérant toutes les applications.

Dans le chapitre suivant, nous allons présenter une nouvelle approche pour la révocation des certificats TRL « *Temporary Revocation List* », ainsi que les différentes étapes de son implémentation.

4

Implémentation d'une approche pour la révocation des certificats dans les VANETs

Introduction

L'idée de base du CRL traditionnelle est de distribuer la liste complète à un intervalle spécifié. Cette méthode nécessite un coût élevé lors de la distribution d'une nouvelle liste CRL à chaque période de mise à jour. Le temps de recherche dans la CRL est beaucoup plus élevé,vu que la taille de la liste augmente au fil du temps par rapport au nombre de véhicules dans le réseaux. Plusieurs approches ont été proposées dans le but de minimiser la taille et le temps de recherche dans la CRL.

Dans ce chapitre, nous allons décrire une nouvelle approche pour la révocation des certificats par la construction d'une liste temporaire TRL « *Temporary Revocation List* » ; proposée par notre promotrice *Melle TASSOULT Nadia*, ainsi nous détaillons les différentes étapes de l'implémentation de cette approche et les outils de développement adoptés :(*Java*), NetBeans IDE (*Environnement de Développement Intégré*) pour Java, et nous illustrons quelques interfaces de notre application.

4.1 Présentation de l'approche TRL

4.1.1 Model du systeme

CA : attribue les certificats aux véhicules et aux RSUs.

- Gère et MAJ (*mise à jour*) la CRL contenant les certificats des véhicules révoqués dans sa région (en supposant aussi que chaque CA est responsable d'une région).

RSU : assure des communications sécurisées entre les véhicules sous sa couverture (dans son secteur).

- Doté d'un IDS (*intrusion détection system*) capable de détecter correctement des attaques provenant des nœuds malveillant ou d'attaquant, ainsi de les accuser, auprès de CA.
- Désigne le CH (*cluster head*) de secteur périodiquement (*le plus proche de RSU*) pour minimiser le temps de transfert de TRL (*Temporary Revocation List*).

- périodiquement reconstruit la SML (*liste des membres de secteur*)
- Envoi la SML, RSUcert (*certificat de RSU*), RSUpk (*clef publique de RSU*) et TRL Au CH.
- Participe à la révocation des certificats des nœuds malveillant afin de garantir la sécurité de réseau.
- Maintient deux listes :
  CRL : une copie de CRL maintenue par le CA.
  TRL : sous ensemble de CRL contenant les certificats révoqués des véhicules de secteur couvert par RSU.

  VEHICULE : échange et relaye les messages de sécurité avec les membres de secteur et le CH.
- Maintient une liste TRL (*liste temporaire de révocation*), contenant les certificats révoqués des véhicules de secteur couvert par son RSU.
- Participe à la révocation des certificats des nœuds malveillant afin de garantir la sécurité de réseau.
- Les différents membres de secteur peuvent se communiquer en toute sécurité en utilisant le RSUcert (*certificat de RSU*) et sa clef publique RSUpk.

4.1.2 Désignation de CH

Le CH doit être désigné par le RSU après avoir vérifié qu'il s'agit bien d'un véhicule honnête IDS (*intrusion détection system*) de RSU.

4.1.2.1 Critère de choix

- Légitime et le plus proche de RSU, pour assurer une connexion avec le CH et diffusion rapide de TRL.

4.1.2.2 Taches de CH

- Une fois le CH désigné ; envoi un msg de notification aux membres de secteur.
- La diffusion de TRL aux membres de secteur.
- La diffusion de RSUcert, RSUpk aux membres de SML.
- Relayer les requêtes ou les MSG de suspect au RSU.

4.1.2.3 Contraintes

- Les membres de secteurs n'acceptent que les messages signés par la clé publique de RSU responsable.
- Tout message transmet doit contenir le certificat de l'émetteur, celui de RSU.
- Les véhicules envoient leurs beacon contenant seulement vitesse, direction (algorithme de prédiction) et accélération.
- Le RSU peut donc identifier les attaques de la falsification de certificat mais pas des messages parce qu'il n'a pas le message.
- Les véhicules au bord des secteurs peuvent recevoir les messages des véhicules ayant l'intention de joindre un secteur. Ces derniers, envoient leurs beacon au RSU responsable du secteur.

4.2 Procédure de révocation

En fonction des paramètres géographiques (localisation et direction) ainsi que la vitesse de véhicule, le RSU peut à tout moment détecter ou savoir quels sont les véhicules en direction de secteur (l'intention de joindre le secteur). A la détection de ces véhicules ou à la réception d'un MSG de suspect d'un CH ; le RSU récupère leurs certificats et vérifie dans CRL (pour chaque certificat).

4.2.1 Procédure de vérification RSU

certI : certificat de véhicule I

N : Nombre de véhicules dans le secteur

TRL : liste temporaire des certificats révoqués

CRL : liste des certificats révoqués établie par le CA

RSUcert : certificat de RSU

RSUpk : clef publique de RSU

CH : cluster head (véhicules de secteur)

```
DEBUT
Réception d'un msg d'un véhicule non CH ou msg de suspect du CH
    SI attaque détectée ALORS
        SI certI appartenant CRL ALORS
            Insère certI dans TRL ;
            Envoyer TRL au CH ; % ou véhicules de secteur%
            Allez au FIN.
        SINON
            Envoyer une requête 'accusation' au CA
        FINSI
    SINON
        SI Vi n'ayant pas un certificat ALORS
            Envoyer une requête 'attribution certificat' au CA
        SINON
            % il s'agit d'un Vi n'ayant pas RSUcert%
            Envoyer RSUcert RSUpk au Vi ;
            Envoyer notification au CH
            Allez au FIN.
        FINSI ;
    FINSI ;
    VERIFICATION PAR LE CA ;
        SI Requête 'révocation certI' ALORS
```

Relayer 'révocation certI' au Vi

inserer certI dans TRL

MAJ CRL (ajout certI)

Envoyer TRL au CH ; % ou véhicules de secteur%

SINON

Envoyer une requête 'attribution certificat' au Vi

Envoyer RSUcert RSUpk au Vi

FINSI

FIN ;

4.2.2 Procédure de vérification CA

DEBUT

% A la réception d'une requête d'accusation ou attribution ;%

SI accusation ALORS

Vérifier dans CRL ;

SI certI ε CRL ALORS

Envoi de CRL et Requête 'révocation certI ' au RSU ; % parce que en raison de problème de connexion ; certains RSUs peuvent ne pas avoir les MAJ de CRL%

SINON

MAJ CRL (ajout de certI) ;

Diffusion d'une Requête 'révocation certI ' aux RSUs de la region ;

FINSI

SINON

SI 'demande d'attribution de certificat' ALORS

Attribuer certI au VI ;

Envoyer notification au RSU ;

FINSI ;

FINSI ;

FIN ;

4.2.3 Procédure de vérification véhicule

DEBUT
% A la réception d'un MSG de sécurité des autres Vi%
SI msg ne contient pas CertRSU ALORS
Envoyer MSG suspect au CH
CH envoi MSG suspect au RSU
SINON
SI certI ε TRL ALORS
Ignorer le MSG
SINON
Accepter le msg
FINSI
FINSI
FIN

4.3 Outil De développement

4.3.1 Présentation de java (*version 1.6.0-14*)

Java est un langage de programmation orienté objet développé par Sun Micsystems, plus connu pour ses stations de travail UNIX. Conçu sur le modèle de C++, Java est simple, concis et portable sur toutes les plates-formes et tous les systèmes d'exploitation. Cette portabilité existe au niveau des sources et des binaires, ce qui veut dire que les programmes Java (applets et applications) peuvent marcher sur toute machine pourvue d'une machine virtuelle Java [67]. Lors de la création du langage Java, il avait été décidé que ce langage devait répondre à cinq objectifs :

- utiliser une méthode orientée objet.
- permettre à un même programme d'être exécuté sur plusieurs systèmes d'exploitation différents.

- pouvoir utiliser de manière native les réseaux informatiques.
- pouvoir exécuter du code distant de manière sûre.
- être facile à utiliser et posséder les points forts des langages de programmation orientés objet comme le C++.

4.4 Environnement de développement

4.4.1 Présentation de NetBeans IDE (*version 7.2.1*)

NetBeans est un environnement de développement intégrée Open Source et gratuit. Il est écrit en Java mais peut supporter n'importe quel langage de programmation. Il comprend les fonctions suivantes [70] :

- Configuration et gestion de l'interface graphique des utilisateurs.
- Support de différents langages de programmation.
- Traitement du code source (édition, navigation, formatage, inspection, etc.).
- Fonctions d'import/export depuis et vers d'autres IDE, tels que Eclipse ou JBuilder.
- Accès et gestion de bases de données, serveurs Web, ressources partagées.
- Gestion de tâches.
- Documentation intégrée

NetBeans est disponible sous Windows, Linux, Solaris, Mac OS X ou sous une version indépendante des systèmes d'exploitation (*requérant une machine virtuelle Java*). Un environnement JDK (*Java Development Kit*) est requis pour les développements en Java.

4.5 Présentation de quelques interfaces de l'application

4.5.1 L'interface principale

L'interface principale de cette application se compose de :

- une zone qui nous montre une communication ($V2V$)
- une zone qui nous montre la circulation des nœuds dans le RSU1 et RSU2
- une zone qui affiche la TRL du RSU1 et la TRL DU RSU2
- une zone qui affiche la CRL de CA

Cette interface nous permettons aussi de démarrer la simulation et d'ajouter des nœuds et d'afficher le temps de recherche dans les différents cas.

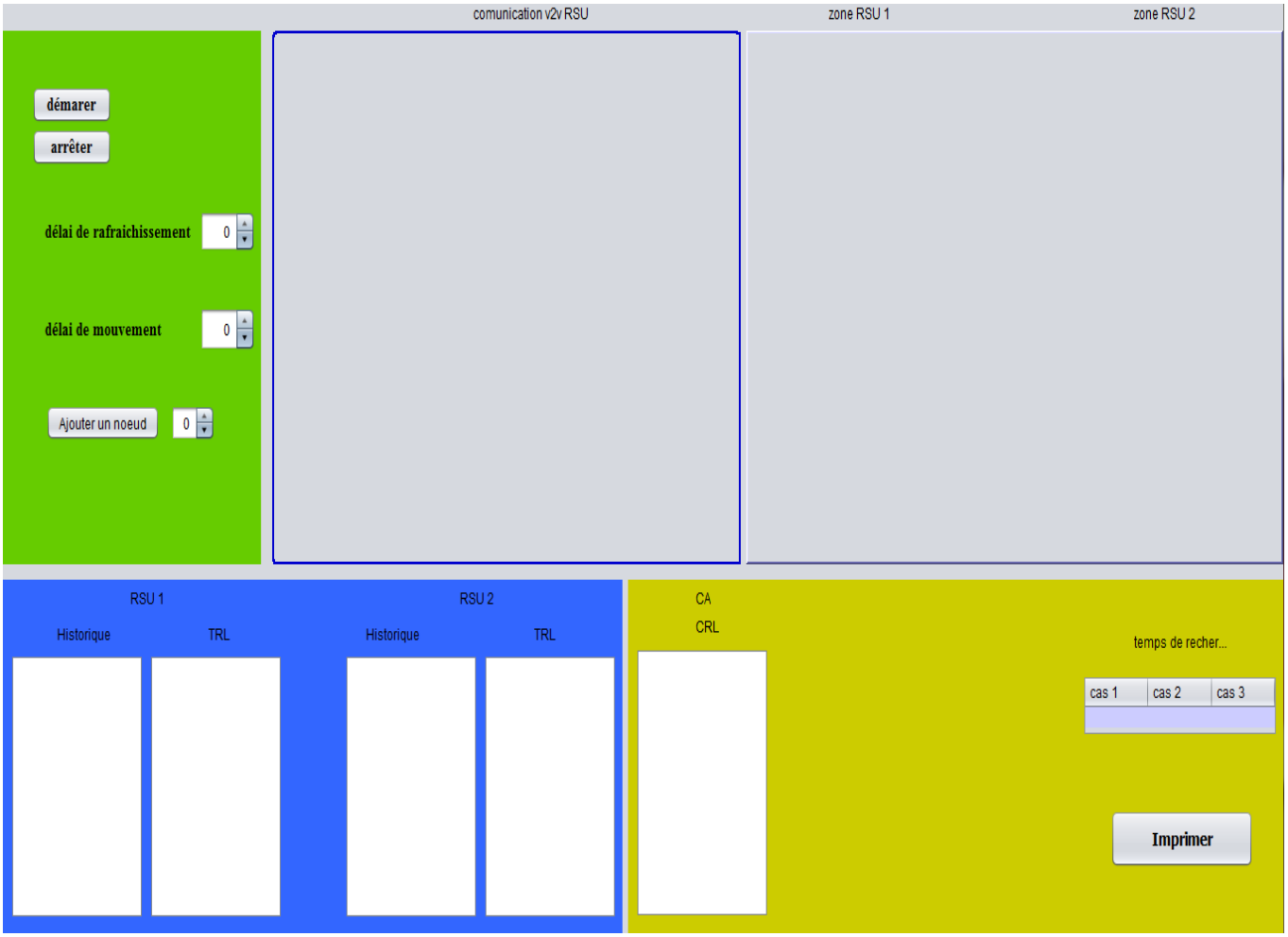


FIGURE 4.1 – l'interface principale de l'application

4.5.2 L'interface de communication v2v

Cette interface illustre la communication inter véhicules.

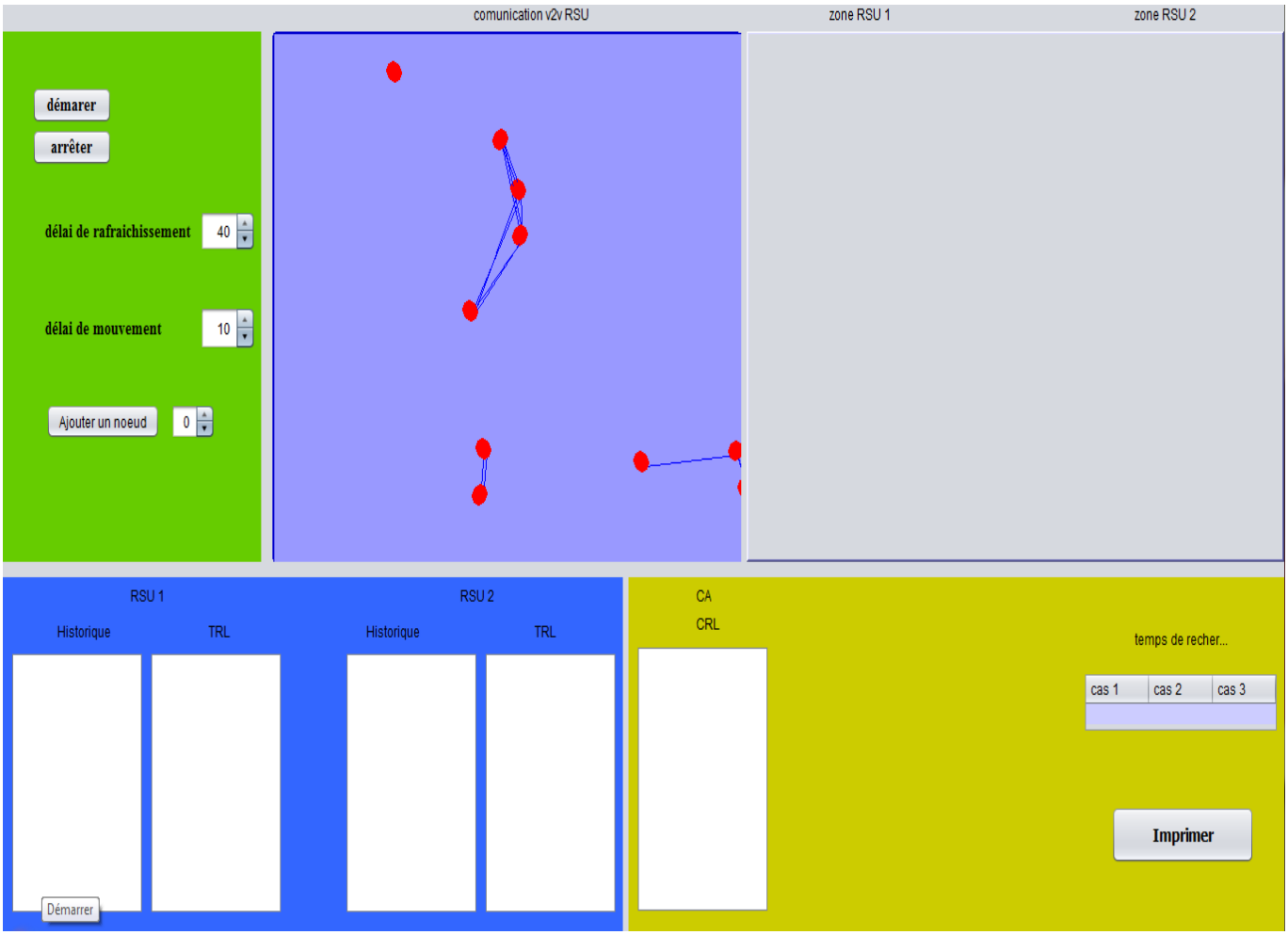


FIGURE 4.2 – l'interface de communication v2v

4.5.3 L'interface de détection de l'intrus par RSU

Cette interface illustre la détection de deux nœuds malveillants par le RSU et l'envoi du message d'alerte ou CA.

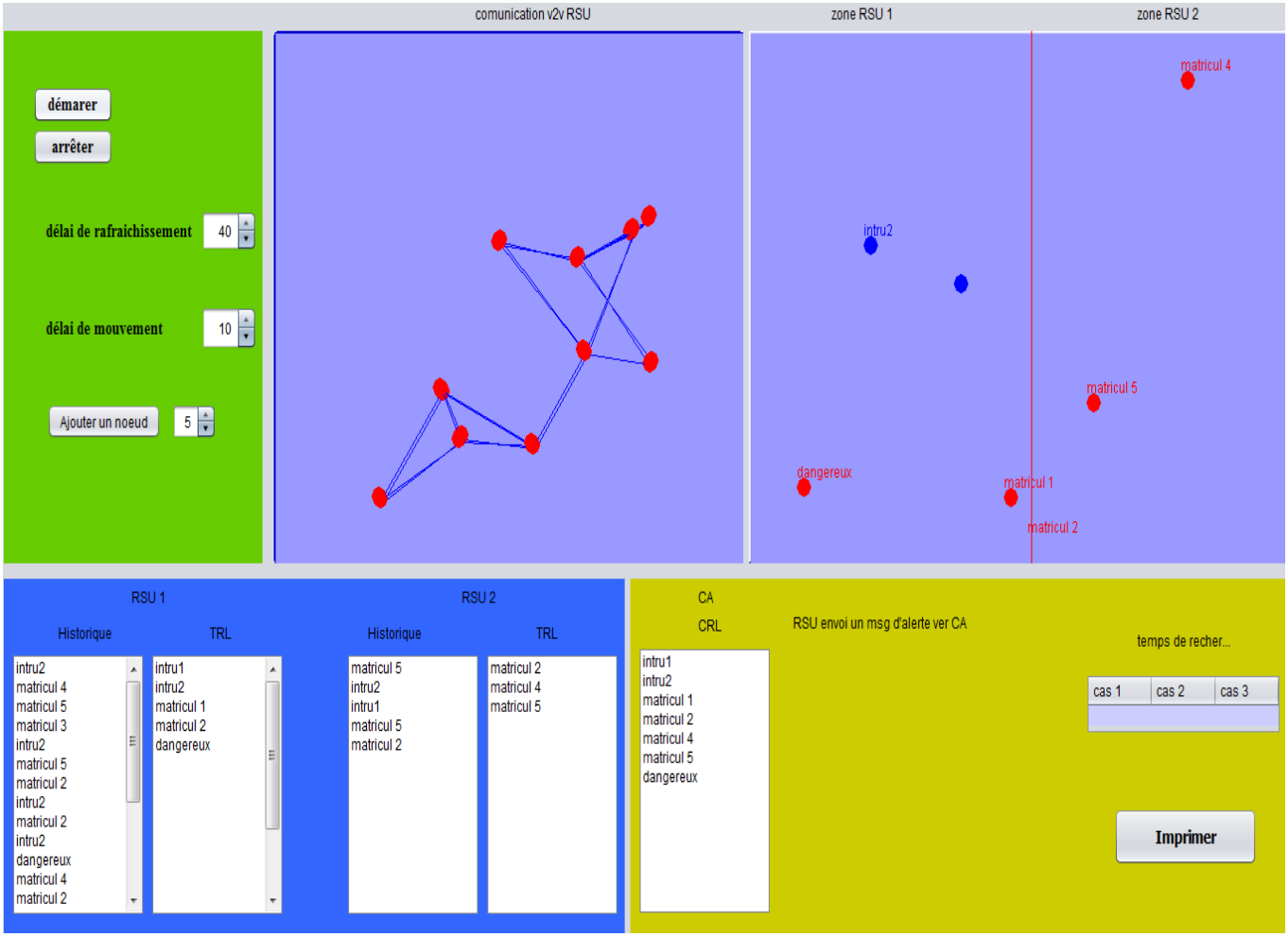


FIGURE 4.3 – l'interface de détection de l'intrus par RSU

4.5.4 L'interface de vérification par CA

Après la vérification par le CA, l'autorité décide d'attribuer un certificat pour l'intrus 1 et l'intrus 2 reste toujours comme un nœud malveillant(*non certifié*).

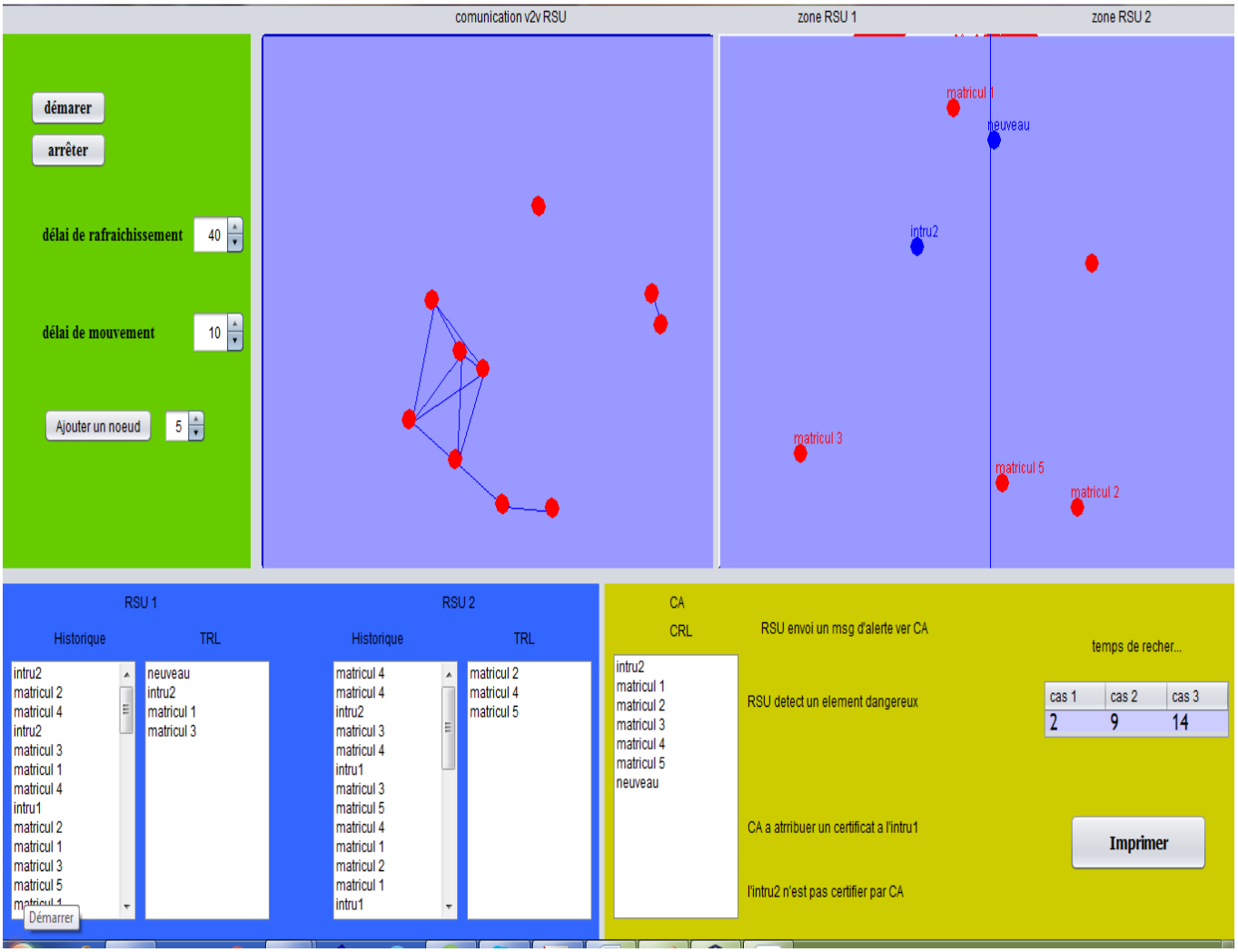


FIGURE 4.4 – l'interface de vérification par CA

4.5.5 L'interface de détection d'un nœud dangereux par le RSU

Le RSU détecte un véhicule qui envoi des fausses alertes, dans ce cas le RSU doit avertir tout les autres véhicules que ce véhicule est dangereux.

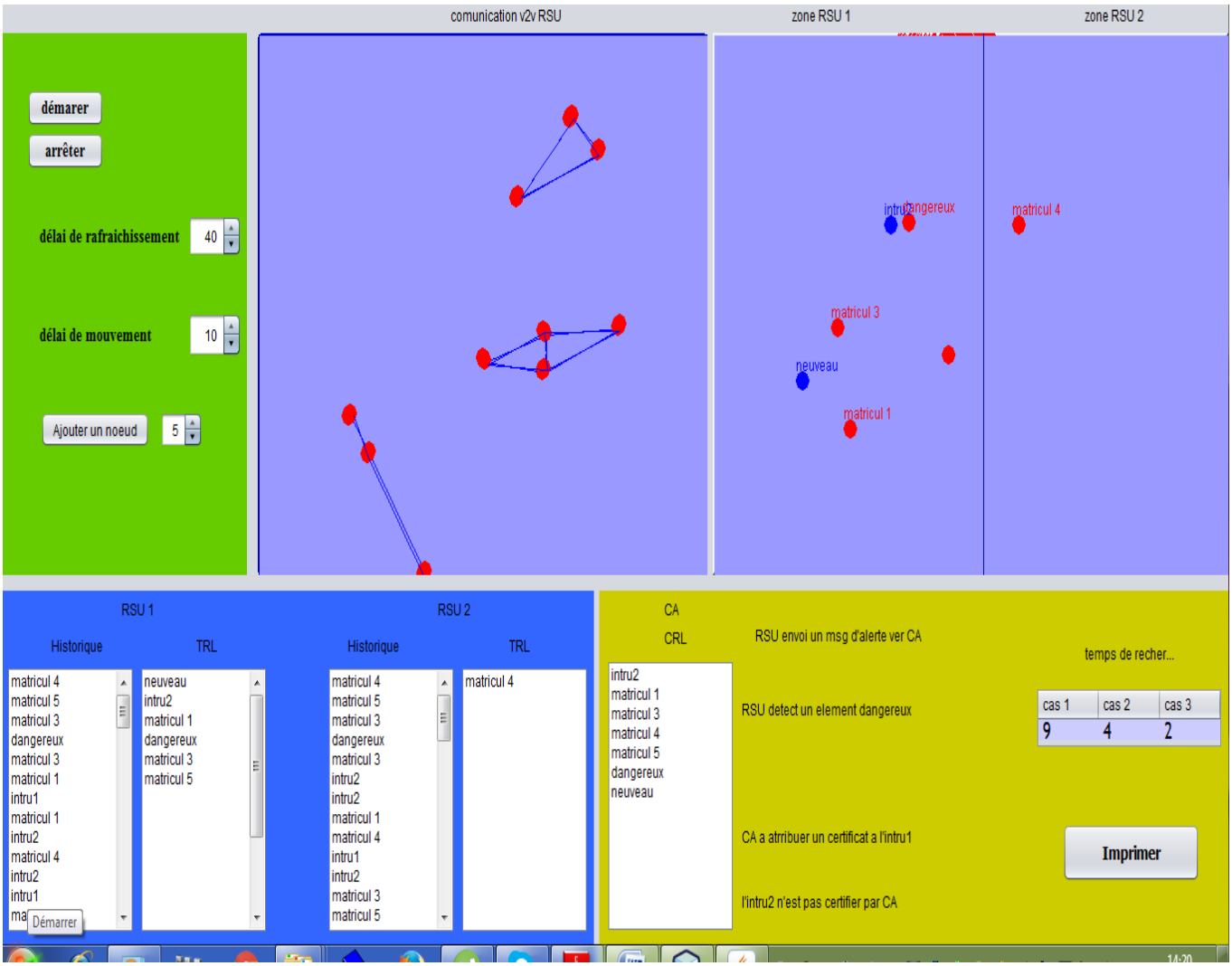


FIGURE 4.5 – l'interface de détection d'un nœud dangereux par le RSU

Conclusion

Dans ce chapitre, nous avons présenté notre nouvelle approche pour la révocation des certificats par la construction d'une liste temporaire (*TRL*) et ces fonctionnalités. Ainsi, nous avons présenté les différents outils du développement de notre application et ses différentes interfaces.

Conclusion Générale et perspective

Les réseaux ad hoc de véhicules constituent un nouveau type de réseaux issu des réseaux ad hoc mobiles (MANET). Leur particularité provient des communications qui peuvent s'instaurer entre véhicules ou bien avec une infrastructure de stations de base. La mobilité est également largement plus contrainte que dans les réseaux ad hoc traditionnels.

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.

Le service du routage est responsable de l'acheminement des messages entre les véhicules. Ces messages sont souvent acheminés avec un protocole de routage multi-sauts, ce qui donne lieu à la possibilité d'avoir plusieurs types d'attaque.

Dans la littérature, les chercheurs souvent proposent l'utilisation des SDI et des systèmes de réputation ; mais, à cause de l'aspect temps réel de certaines applications dans les VANETs, ils ne peuvent pas être utilisés afin de sécuriser le routage.

Les listes de révocation distribuée peuvent détecter les nœuds malveillants même avant l'interaction avec eux.

Dans ce travail, nous avons implémenté une nouvelle approche pour la révocation des certificats par la construction d'une liste temporaire TRL « *Temporary Revocation List* ».Elle vise

à minimiser la taille de CRL à gérer par les différents membres de réseau, ainsi le temps de recherche dans la liste, vue que la TRL ne contenant que les membres de secteur gérés par le RSU.

En guise de perspective, nous espérons implémenter la CRL de base, afin de faire une comparaison et d'évaluer les performances par rapport a notre approche, malheureusement vu la contrainte du temps on a pas pu réaliser notre objectif.

En effet, Il serait également intéressant d'enrichir notre approche afin d'assurer un taux élevé de détection de nœuds malveillants tout en réduisant l'impact de fausses alertes sur la disponibilité du réseau.

Bien que loin d'être le dernier mot, notre travail fournit un point de départ pour approfondir la compréhension et le développement de cette approche.

Résumé

Dans les prochaines années à venir, les réseaux véhiculaires seront capables de réduire significativement le nombre d'accidents via les messages d'alertes échangés entre les véhicules de proximité. La fonction de routage est un élément fondamental pour le système de communication véhiculaire ; par conséquent, il constituera une cible idéale pour les attaques qui pourrait viser à empêcher des messages d'alertes à atteindre leur destinations, et mettre ainsi en danger les vies humaines. Malheureusement, les protocoles de routage basés seulement sur des techniques cryptographiques ne peuvent pas garantir la sécurité contre tous les attaques et particulièrement les attaques provenant de l'interne. Parmi les solutions qui répond à la contrainte temps réel des applications des VANETs, l'utilisation d'une liste de révocation des certificats distribuée afin de détecter et éliminer les nœuds malveillants rapidement.

Dans ce travail, nous implémentons une nouvelle approche proposée pour la révocation des certificats par la construction d'une liste temporaire TRL « *Temporary Revocation List* » dédiée aux réseaux VANETs , visant à minimiser la taille et le temps de recherche dans la liste des certificats révoqués. Elle permet aux nœuds d'un réseau VANET d'éviter d'utiliser les nœuds malveillants.

Mots clés : Révocation distribuée, TRL, SDI, VANET

Abstract

In the next few years, vehicular networks will be able to reduce significantly the number of accidents by way of warning messages exchanged among nearby vehicles. The routing function is a building block for the vehicular communication system, so it will be an ideal target for attacks that could aim to prevent alert messages from reaching their destinations, thus endangering human lives. Unfortunately, routing protocols based only on cryptographic techniques cannot guarantee security against all attacks, especially insider attacks. Among the solutions that meet the real time constraint of VANET applications, the use of a certificate revocation list distributed to detect and eliminate malicious nodes quickly. In this work, we implement a new approach for certificate revocation by building a temporary list TRL "Temporary Revocation List" dedicated to VANETs networks, to minimize the size and search times in the Certificate Revocation List . It enables the nodes of a network VANET to avoid using malicious nodes.

Keywords : distributed Revocation, TRL, SDI, VANET