THÈSE

Présentée pour obtenir le titre de :
Docteur de l'Ecole Nationale Supérieur
des Télécommunications de Paris
Spécialité : Informatique et Réseaux

par

Hamid Menouar

Prédiction de Mouvement pour le Routage et le Contrôle d'Accès au Canal dans des Réseaux Sans-Fil Véhiculaires

Soutenue publiquement le 22 Fevrier 2008 devant le jury composé de :

Président :	Philippe	Jacquet	*INRIA Rocquencourt, France*
Rapporteurs :	Mario	Gerla	*UCLA, USA*
	Luigi	Fratta	*Politecnico di Milano, Italy*
Examinateurs :	Philippe	Godlewski	*ENST de Paris, France*
	Javier Manuel	Gozalvez Semper	*UMH de Elche, Spain*
Directeurs de thèse :	Fethi	Filali	*Eurécom, Sophia Antipolis, France*
	Massimiliano	Lenardi	*HITACHI, Sophia Antipolis, France*

15:00 - Eurécom - Sophia Antipolis.

Prédiction de Mouvement pour le Routage et le Contrôle d'Accès au Canal dans des Réseaux Sans-Fil Véhiculaires

Hamid MENOUAR

Movement Prediction for Routing and Medium Access Control in Vehicular Wireless Networks

"Les plaisirs intellectuels consistent dans l'approche de la vérité des choses, plaisirs qui ne procurent de jouissance ni a l'ouïe, ni a la vue, ni a l'odorat, ni au goût, ni au ventre. C'est l'esprit qui en jouit, ..."

***Imir Abd el-Kader**, dans "Lettre aux Français"*
Traduction par René R. Khawam

À mes parents,
à tous ceux que j'aime,
et à tous ceux qui m'aiment ...

Acknowledgments

This doctoral thesis has been done within the framework of a CIFRE contract. The contract funded by the French government, involves a PhD. student in joint collaboration between academia, and industry. In my case, it was ENST ParisTech through the Eurecom institute for the academic part and Hitachi Europe for the industrial part. This collaboration allowed me to have a unique experience of having the chance to touch the two worlds at the same time, namely the academia and industry. The success of this thesis is due to the, direct or indirect, contributions of many people whom I would like to thank at this moment.

First, I would like to thank my supervisors Dr. Fethi Filali (from Eurecom institute) and Dr. Massimiliano Lenardi (from Hitachi Europe) who initiated and oriented this thesis work. During these three years, they have always found the time for me to guide and encourage my research activities whenever it was needed. I very much appreciate their dynamism and their competences that made this thesis work a success.

Then, I would like to thank all members of the jury for taking keen interest on my work. I thank the reviewers, Prof. Mario Gerla and Prof. Luigi Fratta, for the rapidity of their reviews and the quality of their remarks and comments. I also thank them for having honored my defense by their participation, with special thanks for Prof. Mario Gerla who accepted to participate by video-conference from the USA very early in the morning. Many thanks for Prof. Philippe Jacquet for having accepted to chair the jury, and for his constructive comments. I also thank Prof. Philippe Godlewski and Dr. Javier Gozalvez for taking interest in my work and for their fruitful discussions.

Many thanks to Dr. Stephane Amarger, the manager of Hitachi Lab in Sophia Antipolis, to have trusted me from the beginning of my thesis. I also thank him for having fully engaged me in his team right from the first day in Hitachi Sophia Antipolis Laboratory, and especially for having given me the opportunity to continue in contributing to the success of the lab by engaging me after my thesis. I also thank Dr. Maedda-san, the head of HSDL (Hitachi Systems and Development Laboratory) in Japan, Mr. Susumu Matsui, Mr. Hayashi Masato, and all the rest of the HSDL team for their interest in my work.

My most sincere thanks go to all my colleagues in Hitachi Sophia Antipolis lab, particularly to Mrs. Beatrice Dessus, Miss. Lin Lan and Mr. Nestor Mariyasagayam, for the good, friendly and professional, atmosphere they offered every day at the office.

My biggest acknowledgment goes to my parents who eagerly waited for me to succeed in this endeavor Moreover; it is for them that I dedicate this work. I would also like to thank the rest of my family, in particular my dear wife Khadidja, who supported me patiently all this time. Many thanks for Dr. Yacine Khaled, Dr. Yacine Challal and Dr. Imed Romdhani for their support and useful advices. I take this opportunity to mention that they have played a

big role in contributing to the success of this doctoral thesis.

Finally, my acknowledgments go to all my friends, and of course to any person whom I did not quote here and who, directly or indirectly, has contributed to the success of this work.

Hamid Menouar
Sophia-Antipolis
22 February 2008

Contents

List of Figures

List of Tables

Abstract

Vehicular Ad-hoc Networks (VANETs) represent a rapidly emerging, particularly challenging class of Mobile Ad-hoc Networks (MANETs). VANETs are distributed, self-organizing communication networks built up from traveling vehicles, and are thus characterized by very high speed and limited degrees of freedom in nodes movement patterns. This makes the network topology changes very frequently and very rapidly, therefore more unstable when compared to MANETs, and existing protocols initially proposed for MANETs, mainly at the NET and the MAC layers, are not suitable for VANETs as they are. The vehicles' movement information assumes an important parameter which should be considered when designing any protocol for VANETs. In this work, we propose a concept which exploits the movement information of involved vehicles to predict the future status of the network topology. We call this concept MOPR (MOvement PRediction). Based on the prediction of the network topology evolution, the MOPRcross-layer architecture introduces a new metric called Link Stability (LS) metric to each communication link.This metric is then used at the NET layer to help the routing protocol in selecting the most stable routes, and at the MAC layer to help the MAC protocol to guarantee a better control between nodes when accessing the medium. Based on extensive simulations, we show the network performances improvements that MOPR can bring, mainly in case of highly dynamic networks. We present as well a preliminary prototype of MOPR. This prototype, even if still at an early stage, gives already an idea on the problems we may meet in implementing MOPR for realistic environments which will help us to improve our proposals.

Résumé

Les réseaux véhiculaires ad hoc (VANETs) représentent une sous-classe intéressante des réseaux mobiles ad hoc (MANETs). Les VANETs sont des réseaux distribués et auto-configurables, qui sont composés par l'interconnexion de véhicules communicants. À cause de la nature des véhicules, leur vitesse élevée et la limitation de leur mouvement par les routes, la topologie des VANETs change rapidement et fréquemment, et donc, elle est moins stable en comparant aux MANETs. Cela fait que les protocoles existants, au niveau MAC et Réseaux, initialement conçus pour les MANETs, ne peuvent pas faire face à l'environnement dymanique et instable des VANETs. Le mouvement des véhicules est donc un paramètre très important, qu'il faut impérativement considérer lors de la conception de tout protocole pour les VANETs. Dans ce travail, nous proposons un nouveau concept, qui exploite les informations de mouvement des véhicules pour prédire l'évolution de la topologie du réseau dans le future. Nous nommons ce concept MOPR (MOvement PRediction). Grace à cette prédiction, l'architecture MOPR fournie une nouvelle métrique qui mesure la stabilité des liens nommée Link Stability (LS). LS est utilisé au niveau Réseau afin d'aider le protocole de routage à choisir les routes les plus stables, et au niveau MAC afin d'aider le protocole MAC à garantir un accès efficace et équitable au meduim. Par le moyen de simulations extensives, nous démontrons l'amélioration des performances du réseau que MOPR est capable d'apporter, surtout dans le cas de réseaux à forte mobilité. Pour aller au monde réel, nous présentons une implémentation réelle de MOPR. Malgré qu'elle soit encore incomplète, cette implémentation nous donne d'ores et déjà une idée sur les problèmes de déploiement de MOPR dans un environnement réel ce qui nous aidera à raffiner nos propositions.

Chapter 1

Thesis Abstract in French (*Résumé de la thèse en Français*)

1.1 Introduction

Aujourd'hui, là où vous êtes, à la maison, dans votre bureau au travail, à l'aéroport, dehors dans la rue ou dans un lieu publique, vous étés connecté à Internet. De là où vous êtes, vous pouvez utiliser votre téléphone mobile ou votre ordinateur portable pour vous connecter à Internet, afin de lire vos emails ou les actualités, ou même pour discuter avec vos amis et collègues. Cela est devenu possible grâce aux grandes avancées technologiques dans le domaine de la communication sans-fil.

Les technologies de communication sans-fil peuvent êtres classifiées sous deux grandes catégories. La première est celle des réseaux cellulaires, pour lesquels les réseaux GSM, 3G/4G, et prochainement WiMax peuvent êtres donnés comme exemples. La deuxième catégorie regroupe les réseaux mobiles ad hoc, autrement dits les réseaux MANETs (Mobile Ad hoc Networks). Pour ces derniers, nous ne trouvons pas encore d'exemple d'application assez concret dans notre quotidien, à part quelques réseaux sans-fil basés sur la technologie WiFi (Wirless Fidelity).

De nos jours, l'une des applications des réseaux VANETs qui a une bonne réputation, et un bon potentiel, est celle des réseaux mobiles ad hoc véhiculaires, autrement dits les réseaux VANETs (Vehicular Ad hoc Network). Ces derniers, ne sont en fait qu'une sous-classe des réseaux MANETs, avec quelques spécificités qui sont engendrées par le fait que les véhicules remplacent les nœuds dans ces réseaux. Dans cette thèse, notre intérêt sera entièrement concentré autour des réseaux sans-fil ad hoc, et principalement autoure des réseaux VANETs.

Par la spécificité de leurs caractéristiques et leur terrains d'application, qui sont directement liés à la vie humaine (celle des conducteurs et des passagers), les réseaux VANETs ont besoin d'une attention particulière. Leurs exigences en performance technique sont plus importantes que dans les autres types de réseau. Dans cette thèse nous nous intéressons aux performances de réseau au niveau MAC et Routage. Et il faut savoir que les protocoles de routage et MAC

existants, initialement proposés pour les réseaux MANETs, ne sont pas adaptés aux besoins des réseaux VANETs.

Dans ce travail, nous ne proposons pas un nouveau protocole de routage, ni un protocole MAC, mais nous proposons plutôt un nouveau concept, ou algorithme, qui fait en sort que les protocoles existants s'adaptent le mieux aux réseaux VANETs, et cela par la considération des informations de mouvement des véhicules. Nous proposons donc un algorithme que nous appelons MOPR (MOuvement PRediction), qui opère entre la couche réseau et la couche MAC comme un "Cross Layer".

En utilisant les informations de mouvement des véhicules voisins, MOPR permet à chaque nœud d'attribuer une métrique de stabilité LS (Link Stability) à tout lien de communication le connectant à un voisin de ses voisins. Cette métrique LS est utilisée par la couche réseau, pour améliorer les performances de routage des données, mais aussi au niveau MAC pour améliorer les performances de control d'accès au canal.

Le reste de ce résumé en Français est organisé comme suite. D'abord nous commençons par présenter les réseaux MANETs et puis les réseaux VANETs dans Section 2, puis nous introduirons notre algorithme de prédiction de mouvement MOPR dans Section 3. Dans Section 4 et Section 5, nous présentons brièvement comment MOPR améliore les performances de communication au niveau routage et au niveau MAC respectivement. Dans Section 6, nous présentons d'une manière très générale le prototype de MOPR que nous avons développé, pour finalement conclure ce résumé dans Section 7.

1.2. Les Réseaux MANETs et les Réseaux VANETs

Ces dernières années, les réseaux MANETs ont eu un grand intérêt de la part des chercheurs, que ce soit du milieu industriel ou académique. Ces réseaux qui étaient initialement proposés pour l'utilisation dans les domaines militaires, aujourd'hui montrent de plus en plus de potentielle pour les applications civiles. Un réseau MANET est un ensemble de nœuds interconnectés entre eux par le moyen de communication radio. Ces réseaux sont d'une nature totalement distribuée et totalement dynamique, dans lesquels chaque nœud dois être capable de s'auto-configurer sans la nécessité d'aucune gestion centralisée, ni d'aucune infrastructure préalablement déployée. Figure 1.1 montre un exemple d'un réseau MANET très réduit.

Des réseaux semblables aux réseaux MANETs sont nés pour donner un champ d'application plus large et plus important dans notre quotidien. Ces nouveaux réseaux sont les réseaux VANETs.

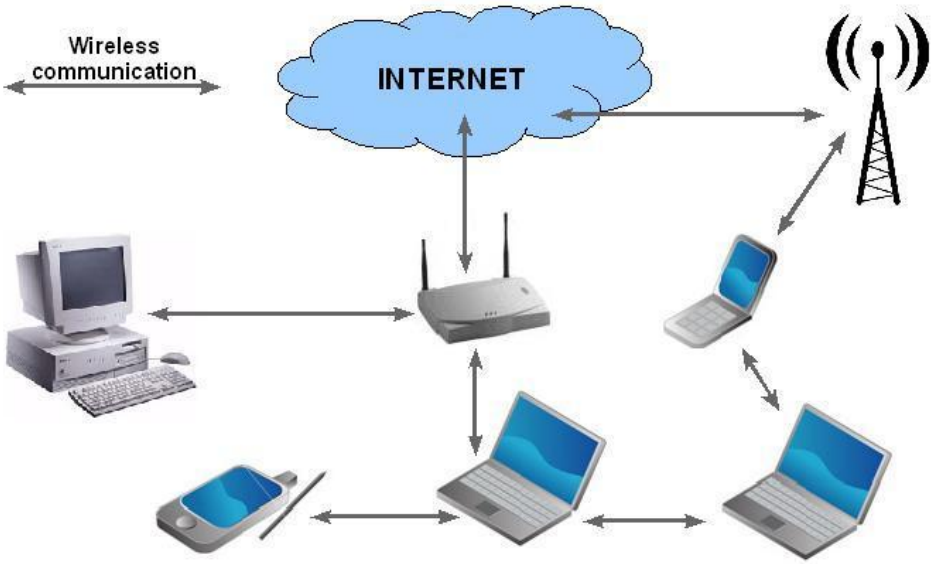

Figure 1.1: Exemple d'un Réseau MANET.

Un exemple d'un petit réseau VANET est donné dans Figure 1.2. Vu de l'extérieur, un réseau VANET n'est en fait qu'une sous classe des MANETs, dans laquelle les nœuds sont des véhicules ou des bornes installées au long des routes. Mais en réalité, les réseaux VANETs sont différents par la nature de leur topologie qui change très fréquemment et très rapidement à cause de la nature de mouvement des véhicules. Le domaine d'application des réseaux VANETs, lui aussi fait que ces derniers sont vus différemment. Leur domaine d'application est en relation direct avec la vue humaine, celle des conducteurs et des passagers.

Les réseaux VANETs ouvrent un grand champ d'application dans notre vie quotidienne. Des applications qui ont le but d'améliorer le confort des conducteurs et des passagers, et aussi pour améliorer la sécurité routière. Ces réseaux, comme précédemment dit, malgré qu'ils se dérivent des réseaux MANETs, ils ont leur propres caractéristiques. Donc, ils ont besoin de leurs propres protocoles de communication afin de bien fonctionner.

1.3 Prédiction de Mouvement (MOPR)

Nous avons vu dans la section précédente que les réseaux VANETs ont besoin de leurs propres protocoles de communication pourle routage et le MAC. Et si nous regardons de plus près les principales caractéristiques de ces réseaux, nous remarquons que la nature de mouvement

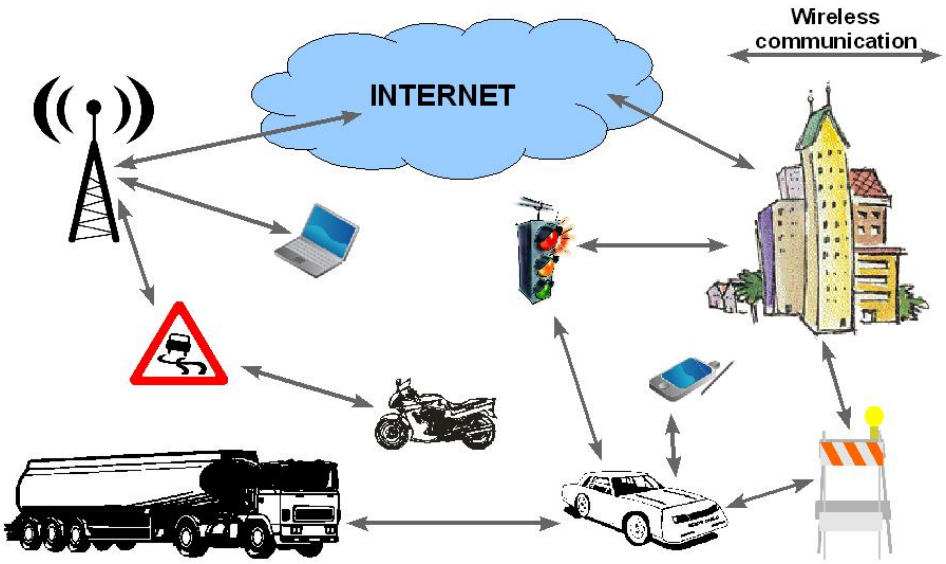

Figure 1.2: Exemple d'un Réseaux VANETs.

des véhicules est la cause principale derrière ces différences. Donc, nous avons pensé qu'il serait avantageux, en terme de performances de communication, si cette nature des véhicules est considérée par les protocoles de routage et/ou MAC durant leurs opérations. Un véhicule est sensé être équipé d'un système de localisation tel que le GPS. Et donc, nous pourrons connaître le mouvement des nœuds (véhicules) à tout moment. Cela est en fait un grand avantage, qui nous permettra de prédire le mouvement des véhicules, chose qui permettra aux protocoles de routage et/ou de MAC de prendre leur précaution par avance, et donc leur permettra d'améliorer leurs performances.

Regarder par exemple le scénario dans Figure 1.3. A t_0 nous avons deux chemins qui permettent de joindre la destination "D" à partir de la source "S". A l'instant t_0 il pourrait nous paraître que ces deux chemins offrent une pareille qualité de service, mais quand nous regardons la situation après quelques instants, à l'instant $t_0 + 1s$, nous voyons bien que cela est faux, et nous voyons bien que le chemin qui passe par le nœud "2" est le plus stable, et donc, offre un meilleur service. En utilisant MOPR, nous choisissons les chemins les plus stables en évitant autant que possible de passer par les liens de communication jugés pas assez stables.

Au niveau MAC, les motivations derrière l'utilisation de la prédiction de mouvement sont claires aussi. Si nous prenons l'exemple d'un véhicule "S" qui a deux véhicules voisins, "A" et "B". Le véhicule "A" roule plus ou moins avec la même vitesse que le véhicule "S", mais le véhicule "B" roule avec une vitesse beaucoup plus élevée. Bien évidement, le véhicule "B" restera moins longtemps dans le voisinage du véhicule "S" que le véhicule "A". Et donc, si

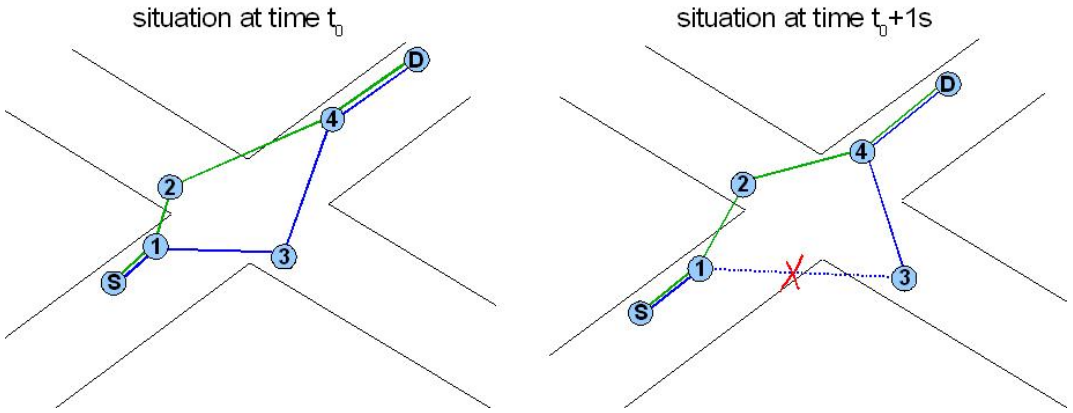

Figure 1.3: Scénario Montrant la Motivation Derrière la Prédiction de Mouvement au Niveau Routage.

le véhicule "S" a une communication en cours avec les deux véhicules, il va forcement avoir moins de temps pour communiquer avec "A" qu'avec "B". Autrement dit, le véhicule qui roule le plus vite (véhicule "A") aura moins de chance dans la communication avec le véhicule "S" que le véhicule qui roule le moins vite (véhicule "B"). Une telle situation pourrait être évitée si notre système était capable de pratiquer une certaine discrimination au niveau MAC. Une discrimination qui donne plus de chance aux voisins quittant le voisinage le plus tôt. C'est ce que MOPR offre, en donnant plus de chance dans l'accès au canal aux voisins correspondants aux liens de communication les moins stable, donc, qui ont les plus faibles LS.

Nous proposons donc une architecture semblable à celle présentée dans Figure 1.4. MOPR qui récupère les informations de mouvement du véhicule par GPS ou par un autre system de geo-localisation, puis les informations de mouvement des autres véhicules dans le voisinage par un système spécifique, tel que MHVB-B, qui est un algorithme développé par HITACHI. Une fois ces informations sont récupérées, MOPR sera apte à fournir une métrique LS pour chaque lien de communication dans le voisinage. Cette métrique est utilisée par la couche réseau au niveau routage et par la couche MAC au niveau du contrôle d'accès au canal. La méthode de calcul des métriques LS est décrite dans ce qui suit.

1.3.1 Calcul de la Métrique LS

Les informations de mouvement d'un véhicule contiennent au moins : sa position, qui est représentée par la latitude et la longitude, sa direction, qui peut être représentée par l'azimut, et enfin sa vitesse. Du point de vue théorique, cela peut être différent. Prenons par exemple

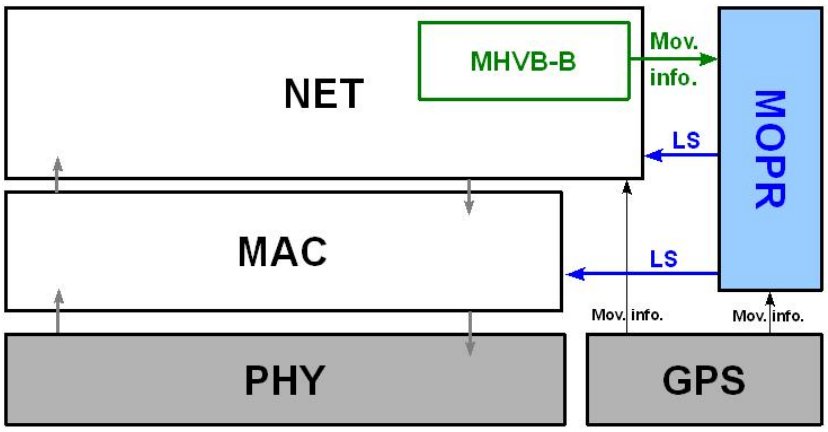

Figure 1.4: Architecture du Réseau Intégrant MOPR.

le simulateur de réseaux NS2 (Network Simulator 2). Dans sont environnement, un nœud se déplacent dans un espace de deux dimensions (2D), représenté par deux axes XX' et YY'. Sur ce plan hertzien, les nœuds ont une position (x, y) et une vitesse de mouvement (dx, dy) qui interprète en même temps la direction de mouvement du nœud en question.

Pour expliquer comment MOPR calcule la métrique LS, nous considérons les deux nœuds "A" et "B" qui se déplacent sur un plan hertzien limité par les axes XX' et YY' (voir Figure 1.5). En fait la métrique LS correspond directement à la durée de vie ($LifeTime$) du lien de communication concerné, que nous normalisons en la divisant par une constante prédéfinie ($MaxLifetime$). Dans notre exemple montré dans Figure 1.5, la $LifeTime$ du lien de communication connectant les deux nœuds "A" et "B" ($LifeTime[A, B]$) correspond à la durée de temps, en secondes, estimée pour que ce lien se brise. Autrement dit, la durée de temps estimée pour que la distance entre ces deux nœuds ($D1$) devient plus importante que le rayon de communication maximal (R).

La constante $MaxLifetime$ doit être choisie intelligemment, en fonction de l'environnement par exemple ou en fonction du type de protocole de routage et/ou MAC utilisé. La manière de choisir et/ou définir cette constante ne sera pas traité dans cette thèse.

Donc, $LS[A, B]$, qui est la métrique de stabilité correspondante au lien de communication connectant les deux nœuds "A" et "B", est calculée comme suite :

$$LS[A, B] = LifeTime[A, B]/MaxLifeTime$$

Nous avons :

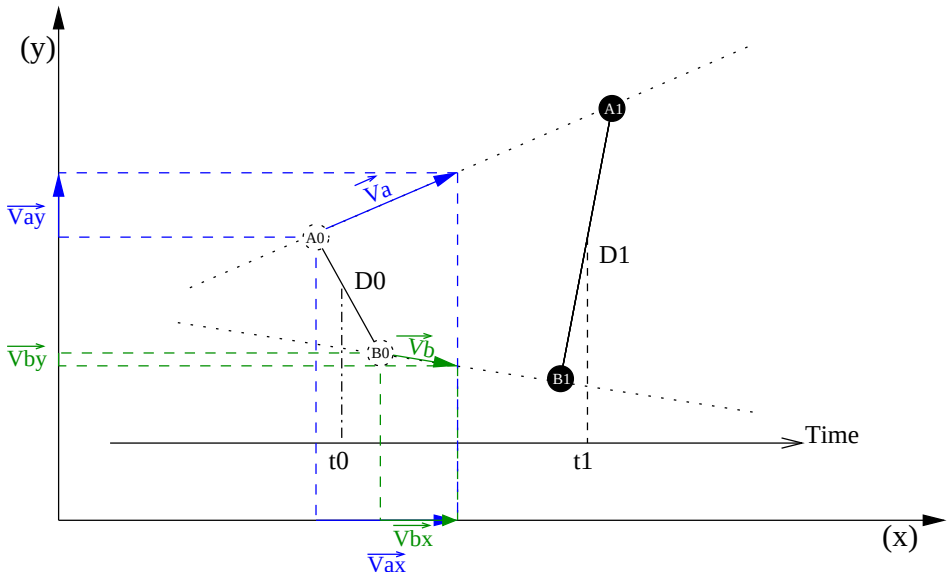

Figure 1.5: Estimation de le Durée de Vie d'un Lien de Communication.

$$LifeTime[A,B] = t_1 \breve{} t_0 = \Delta t \quad quand \ : \ D1 = R \tag{1.1}$$

Et nous avons aussi :
$D_1^2 = \|X_i1 - X_j1\|^2 + \|Y_i1 - Y_j1\|^2$

Et donc,

$$D_1^2 = \|(X_i0 + Vx_i\Delta t) - (X_j0 + Vx_j\Delta t)\|^2 + \|(Y_i0 + Vy_i\Delta t) - (Y_j0 + Vy_j\Delta t)\|^2 \tag{1.2}$$

A partir de (1.2), nous avons :

$$D_1^2 = A\Delta t^2 + B\Delta t + C \tag{1.3}$$

$$Avec \begin{cases} A = (Vx_i - Vx_j)^2 + (Vy_i - Vy_j)^2 \\ B = 2\left[(X_i0 - X_j0)(Vx_i - Vx_j) + (X_i0 - Y_j0)(Vy_i - Vy_j)\right] \\ C = (X_i0 - X_j0)^2 + (Y_i0 - Y_j0)^2 \end{cases}$$

De (1.1), nous avons :

$$LifeTime\,[i,j] = \Delta t \, quand \, D_1^2 = R^2 \tag{1.4}$$

Enfin, à partir de (1.3) et (1.4), nous avons $LifeTime\,[i,j]$ égale à Δt qui résoud la fonction de deuxième degré suivante :
$A\Delta t^2 + B\Delta t + C - R^2 = 0$.

Une fois que MOPR délivre une métrique de stabilité (LS) pour chaque lien de communication dans le réseau, nous pourrons améliorer, en utilisant ces métriques, les performances de nos protocoles de routage et/ou MAC. Dans les deux sous-sections qui suivent, nous présentons comment cela est réalisé, au niveau Routage et au niveau MAC respectivement.

1.4 Routage Assisté par MOPR dans les Réseaux VANETs

Nous avons appliqué MOPR à différents protocoles de routage afin que nous puissions évaluer ses capacités. Ces protocoles de routage peuvent êtres classifiés sous différentes formes, mais comme cela n'est pas le but dans cette thèse, nous nous sommes contenté d'une simple classification comme montré dans Figure 1.6. Cette classification inclue deux grandes catégories. La première regroupe les protocoles de routage basés sur la topologie, dans laquelle nous distinguons deux types de routage : routage réactif et routage proactif, et la deuxième catégorie regroupe les protocoles de routage basés sur la position géographique.

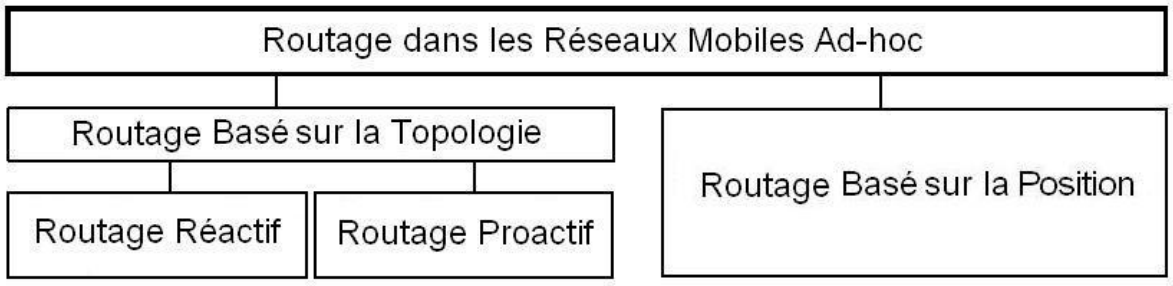

Figure 1.6: Classification des Principaux Protocoles de Routage.

1.4.1 MOPR Appliqué au Routage Basé sur la Topologie

Les protocoles de routage basés sur la topologie ne sont pas nécessairement les plus fiables pour les réseaux VANETs, mais malgré cela nous avons appliqué MOPR à quelques uns de ces protocoles, et cela juste pour voir et mesurer ses capacités et limites avec ce type de routage. Comme candidats pour cette initiative, nous avons choisi AODV (Ad hoc On-Demand Vector) dans la catégorie des protocoles de routage réactifs, et OLSR (Optimized Link State Routing) dans la catégorie des protocoles de routage proactifs.

1.4.1.1 AODV (Routage Réactif)

Avant d'expliquer comment MOPR est appliqué à AODV, nous tenons d'abord à expliquer brièvement le fonctionnement de AODV.

AODV et donc un protocole réactive, ce qui veut dire que quant un nœud source "S", comme dans l'exemple montré dans Figure 1.7, veut trouver un chemin vers une destination "D", il lance une requête de recherche de route dans le réseaux. Cette requête est réalisée par la diffusion d'un message RREQ (Route Requeste) dans le réseau. Une fois que RREQ atteint la destination "D", ou un nœud dans le réseaux qui connaît le chemin vers la destination "D", ce dernier réplique en envoyant un message de réponse RREP (Route Reply) vers la source "S" afin de l'informer sur le chemin recherché. Cette façon de procéder engendre des délais de communication qui peuvent augmenter rapidement, surtout quand la destination est assez loin.

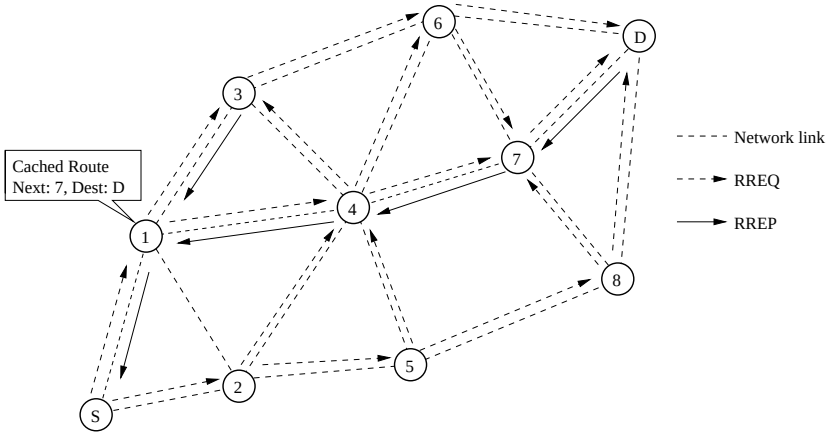

Figure 1.7: Fonctionement de AODV.

MOPR est appliqué à AODV au niveau de la procédure de recherche des chemins. Nous ajoutons un champ PS (Path Stability) dans le message RREQ. Ce champ correspond à la stabilité du chemin qui sera fourni. Le nœud source initialise le PS dans le RREQ à zéro avant de le diffuser dans le réseau. Chaque nœud dans le réseau, quand il reçoit le RREQ, compare le PS dans ce dernier avec le LS correspondant au lien de communication le connectant au voisin d'où le RREQ est arrivé. La valeur la plus petite remplace donc la valeur de PS dans le RREQ avant que ce dernier ne soit retransmis.

En recevant le RREQ, si un nœud est la destination elle même ou connaît le chemin vers la destination, il initialise un RREP en y ajoutant un champ correspondant au PS du chemin concerné, puis il le transmet vers la source. Ce PS, durant l'acheminement de RREP, sera mis à jour de la même manière que le PS l'est dans le RREQ, et cela jusqu'à ce qu'il atteint la source.

Un nœud, quand il reçoit un message RREQ/RREP, met à jour dans sa table de routage le chemin qui mène à la Source/Destination respectivement, si le chemin proposé dans ce message est plus intéressant. Autrement dit, si le PS dans ce message et plus grand que le PS du chemin sauvegardé. Cette procédure garantira une meilleure sélection des chemins.

Regardons l'exemple montré dans Figure 1.8. En utilisant la version basique de AODV, le RREP peut revenir à "S" avec un chemin qui passe par le nœud intermédiaire "1". Mais quand nous appliquons à ce même exemple AODV utilisant MOPR, la situation devient comme montré dans Figure 1.9.

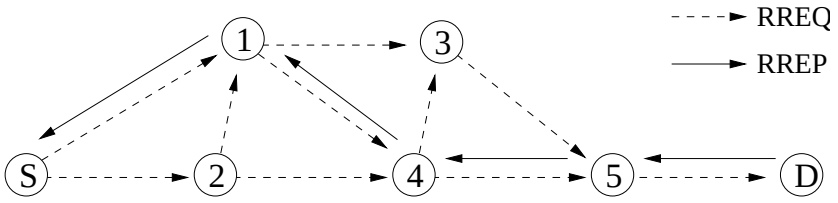

Figure 1.8: Avec AODV basique.

Dans Figure 1.9, nous avons pour chaque lien de communication une métrique LS qui lui correspond. Et nous voyons que le chemin de "S" à "D" qui passe par le nœud "2" et plus stable que le chemin qui passe par le nœud "1". Grass à MOPR, le message RREP proposera à "S" le chemin le plus stable, et donc celui qui passe par le nœud "2".

Afin d'évaluer les performances de MOPR appliqué à AODV, nous avons réalisé plusieurs simulations avec le simulateur de réseaux NS2. Nous avons modifié une implémentation NS2 de AODV, et nous nommons cette version modifiée AODV-MOPR.

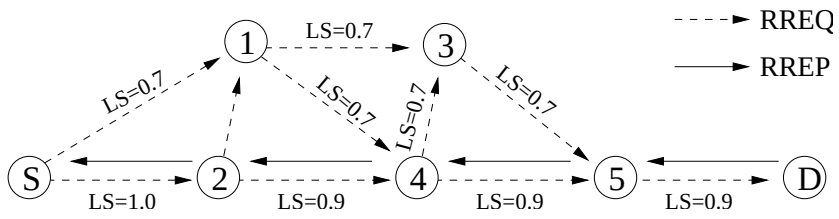

Figure 1.9: Avec AODV base sur MOPR.

Dans ces simulations nous avons utilisé un scénario réaliste (une route avec deux intersections), dans lequel nous lançons quelques liaisons de communication UDP entre différents couples (source, destination). En observant différents paramètres au niveau réseau, nous remarquons que AODV-MOPR améliore AODV en terme de délais, en terme de charge du réseau, et aussi en terme de taux des succès de livraison des paquets à destination.

1.4.1.2 OLSR (Routage Proactif)

Comme pour AODV, avant d'expliquer comment nous avons appliqué MOPR à OLSR, nous tenons d'abord à expliquer brièvement le fonctionnement de OLSR.

OLSR est donc un protocole de routage proactif. Proactif parce que chaque nœud dans le réseau maintient une table de routage qui contient, pour chaque nœud dans le réseau, un chemin. Cette table est périodiquement maintenue à jour, par l'échange de messages de contrôle entre les différents nœuds dans le réseau. Ces messages de contrôle sont principalement regroupés dans deux groupes.

Les messages de contrôle du premier groupe, portants le nom "messages Hello" sont périodiquement envoyés sur une distance d'un saut, pour garantir la détection des voisins mais aussi pour permettre la sélection des nœuds MPR (Multi Point Relay), qui ont le rôle de transmettre les messages de contrôle du deuxième groupe. Figure 1.10 montre comment des nœuds voisins sont sélectionnés pour devenir MPR.

Les messages de contrôle du deuxième groupe sont périodiquement diffusés dans le réseau à travers les nœuds MPR afin de garantir pour chaque nœud une vue globale sur la topologie du réseau. Les nœuds MPR ont le but de réduire le nombre de messages de contrôle dans le réseau.

Dans OLSR, quand un nœud source "S" cherche une route pour acheminer des données vers une destination "D", il n'a pas à chercher le chemin vers cette dernière, puisqu'il doit en avoir déjà une dans sa table de routage. Ce type de routage, contrairement au routage réactif, n'a pas le problème des longs délais de communication puisque les chemins sont preconstruits et prêts à êtres utilisés à tout moment. Par contre, le maintien à jour des tables de routage, coûte beaucoup en terme de charge du réseaux, ce qui peut réduire les performances du réseau,

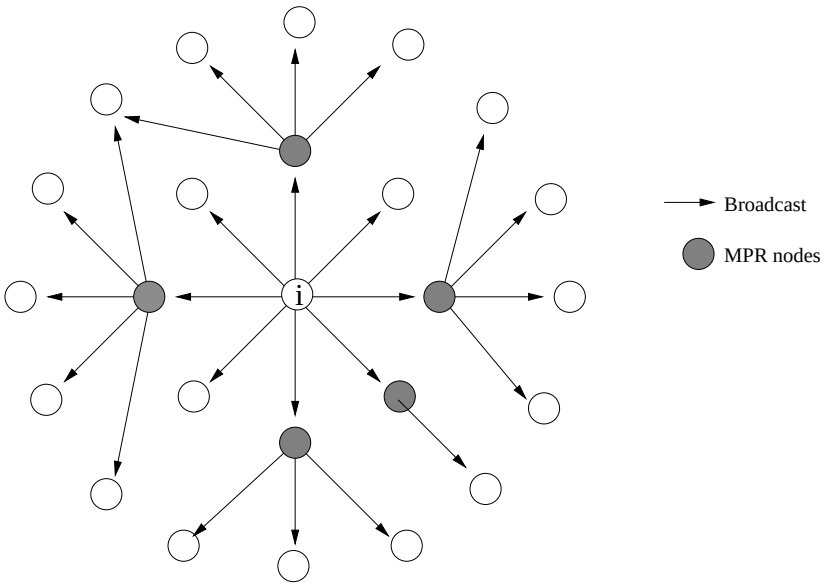

Figure 1.10: Selection des nœuds MPR dans OLSR.

surtout quand ce dernier est assez dense.

MOPR s'applique à OLSR en deux phases. La première en appliquant MOPR à la procédure de sélection des MPRs, et la deuxième en appliquant MOPR à la procédure de construction des tables de routage.

1.4.1.3 Sélection des MPRs Basée sur MOPR

Dans la version basic de OLSR, un voisin qui couvre le plus grand nombre de voisins sur deux sauts sera le premier à être sélectionné comme MPR. En appliquant MOPR, cela devient différent, où un voisin est le premier à être désigné MPR si il garantie une meilleur stabilité dans un rayon de couverture d'un ou deux sauts.

Nous avons appliqué MOPR à OLSR selon deux techniques différentes que nous expliquons dans ce qui suit.

Sélection des MPRs utilisant MOPR sur rayon de un saut : Nous supposons un petit réseau avec i un nœud qui lui appartient. Nous avons donc :

- $NB1hop(i)$: l'ensemble de nœuds voisins de i dans un rayon de un saut.
- $r(i)$: nombre de nœuds dans $NB1hop(i)$.
- $GlobLS(i,j) \in [0,1]$: le poids de stabilité global du lien $[i,j]$. Ce poids est la métrique principale que MOPR considéra dans la sélection des nœuds MPR.

Dans notre algorithme, durant la sélection des nœuds MPR, le nœud i commence par calculer, pour chaque voisin j, le poids de stabilité globale $GlobLS(i,j)$ comme suite :

$$GlobLS(i,j) = LS(i,j)\frac{r(j)}{\sum_k r(k)} \quad Avec\, k \in NB1hop(i) \tag{1.5}$$

Puis il sélection un MPR en première position le voisin j correspondant au plus fort $GlobLS(i,j)$.

Sélection des MPR utilisant MOPR sur un rayon de deux sauts : Dans cette deuxième technique nous considérons les informations de stabilité des liens de communication sur deux sauts. Nous supposons un petit réseau avec i un nœud dans ce dernier. Nous avons donc :

- $NB1hop(i)$: ensemble de nœuds voisins de i dans un rayon de couverture de un saut.
- $NB2hop(i)$: ensemble de nœuds voisins de i dans un rayon de couverture de deux saut.
- $GlobLS(i,j) \in [0,1]$: le poids de stabilité global du lien $[i,j]$. Ce poids est la métrique principale que MOPR considéra dans la sélection des nœuds MPR.

Dans notre algorithme, durant la sélection des nœuds MPR, le nœud i commence par calculer, pour chaque voisin j, le poids de stabilité globale $GlobLS(i,j)$ comme suite :

$$GlobLS\,(i,j) = LS(i,j)\frac{\sum_k LS\,(j,k)}{\sum_{l,m} LS\,(l,m)} \tag{1.6}$$

$$avec \begin{cases} k \in NB1hop(i) \\ l \in NB1hop(i) \\ m \in NB1hop(l) \end{cases}$$

Puis il sélectione un MPR en première position le voisin j correspondant au plus fort $GlobLS(i,j)$.

Dans 1.6, $LS\,(i,j)$ est localement disponible grasse au système de détection des voisins (échange périodique de messages de contrôle) utilisé par OLSR. Mais, $LS\,(j,k)$ qui correspond à un lien de communication dans le deuxième saut, n'est pas localement disponible. Donc, pour pouvoir utiliser cette technique de sélection des MPR il faut que chaque nœud dans le réseau informe ces voisins des informations de stabilité de ses propres voisins. Cela peut être achevé par l'ajout des informations de stabilité des voisins dans le message Hello de OLSR.

1.4.1.4 Construction des Tables de Routage Basée sur MOPR

Nos MPRs sont sélectionnés en se basant sur MOPR, et donc ils sont les plus stables. Cela nous garantie un support plus stable pour l'acheminement des messages de contrôle portants les informations nécessaires pour pouvoir avoir une vue globale sur la topologie de notre réseau, et donc nécessaires pour pouvoir construire un chemin vers chaque nœud dans le réseau. Grâce à MOPR, notre topologie de réseaux est constituée avec une métrique LS correspondante à

chaque lien de communication. Les métriques LS sont considérées dans la construction des tables de routage afin de garantir des chemins avec la plus grande stabilité en terme de durée de vie.

L'objectif de cette partie est de construire, au niveau de chaque nœud, une table de routage qui contient les routes les plus stables dans le réseau.

Grâce à l'échange périodique des messages de contrôle dans le réseau, chaque nœud est capable de construire une table de topologie qui a une vue globale sur le réseau. Pour appliquer MOPR, chaque nœud ajoute dans ses messages de contrôle les informations concernants la stabilité des liens de communication sur un rayon de un saut. Cela rend disponible dans la table de topologie une métrique de stabilité pour chaque lien de communication. Cette table est utilisée dans la construction des tables de routage.

Dans Figure 1.11 nous avons un exemple basique qui montre comment la route la plus stable est sélectionné par l'aide de MOPR. Nous avons dix nœuds (0 a 9), et nous supposons que tous les nœuds voisins du nœud "0" dans un rayon de communication de deux sauts, connaissent le chemin vers "0". Maintenant, prenons comme exemple le nœud "8". Ce dernier, pour atteindre le nœud "0", a le choix parmi trois chemins différents : en passant par le nœud "0", en passant par le nœud "4", ou en passant par le nœud "5". Parmi ces trois chemins, le nœud "8" doit choisir le chemin le plus stable, celui qui a la durée de vie la plus langue. Nous pouvons voir que les nœuds "4", "5" et "6" ont différents chemins pour atteindre le nœud "0", avec les métrique de stabilité $RS\left(4,0\right)=0.9$, $RS\left(5,0\right)=0.7$, et $RS\left(6,0\right)=0.6$ respectivement. Le nœud "8" a différentes métriques de stabilité $GlobLS\left(8,4\right)=1$, $GlobLS\left(8,5\right)=0.9$, and $GlobLS\left(8,6\right)=1$ avec ses trois voisins "4", "5" et "6" respectivement. Cependant, parmi ces trois chemins, le plus stable qui sera choisi grâce à MOPR est celui qui passe par le nœud "4". Ce chemin garantira la meilleur stabilité ($RS\left(8,0\right)=0.9$), sachant que :

$$RS\left(8,0\right)=Min\left(GlobLS\left(8,4\right),RS\left(4,0\right)\right)=Min\left(1.0,0.9\right)=0.9$$

Pour évaluer les performances de MOPR appliqué à AODV, nous avons réalisé plusieurs simulations avec le simulateur de réseaux NS2. Nous avons modifié une implémentation NS2 de OLSR, et nous nommons cette version modifiée OLSR-MOPR.

Dans ces simulations nous avons utilisé un scénario réaliste (une autoroute), dans lequel nous lançons quelques liaisons de communication UDP entre différents couples (source, destination). En observant différents paramètres au niveau réseau, nous remarquons que OLSR-MOPR améliore OLSR en terme de délais de communication, en terme de charge du réseau, et aussi en terme de taux des succès de livraison des paquets à destination.

1.4.2 MOPR Appliqué au Routage Basé sur la Position

Les protocoles de routage basés sur la position sont apparemment les plus adaptés aux réseaux VANETs. Donc, il est indispensable que nous appliquons MOPR à ce type de routage, et c'est ce que nous avons fait. Pour cette initiative nous avons choisi GPSR (Greedy Perimeter

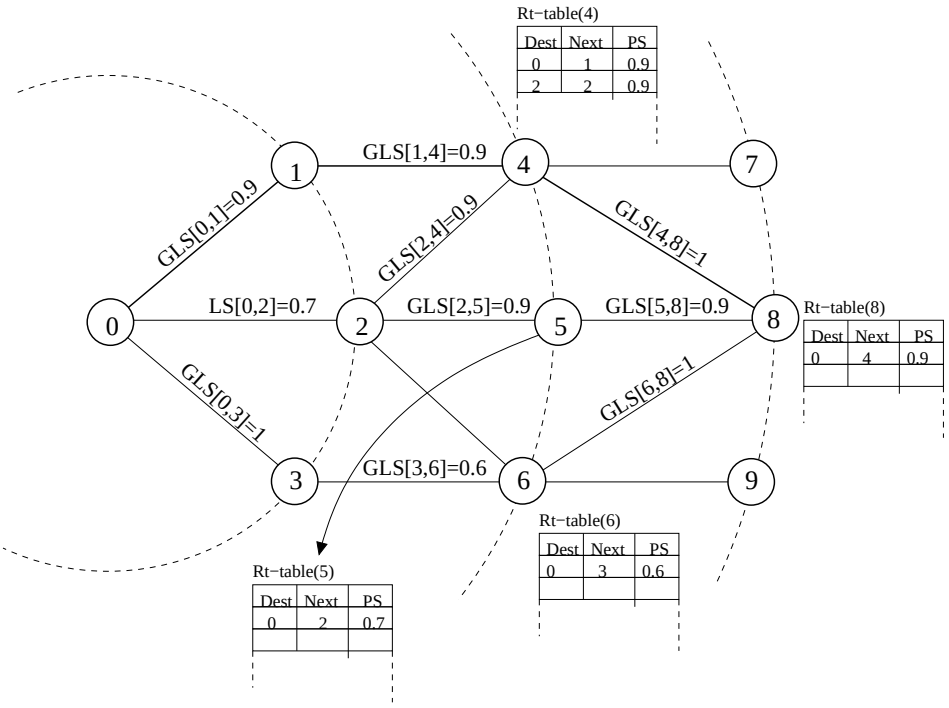

Figure 1.11: MOPR-based routing routes selection example.

Stateless Routing) comme le protocole de routage basé sur la position qui adoptera notre algorithme.

1.4.2.1 GPSR

GPSR est donc un protocole de routage basé sur la position, qui contient deux parties.

La première correspond à une méthode de choix du prochain nœud transmetteur qui aura le rôle de retransmettre les paquets, et cela tout en se basant sur les informations de position des voisins (nœuds candidats) et de la destination des paquets. Cette méthode consiste à choisir le candidat qui est à une distance la plus proche à vol d'oiseau de la destination. Par exemple, dans Figure 1.12 le nœud "S" a des données à envoyer à la destination "D", et donc il doit choisir parmi ces voisins celui qui va retransmettre ces données vers la destination. En calculant la distance qui sépare chaque voisin de la destination, le nœud "S" choisira le voisin "2" comme transmetteur puisque ce dernier est le plus proche de la destination.

La deuxième partie de GPSR est en fait une méthode pour contourner les obstacles et les zones géographiques vides, qui ne présentent aucun candidat transmetteur dans le voisinage. Cette deuxième partie de GPSR ne sera pas traitée dans cette thèse. C'est plutôt la première partie qui retient notre entière attention dans cette thèse.

MOPR est appliqué à GPSR dans la partie de sélection du prochain transmetteur. Au lieu de choisir, comme prochain transmetteur, le candidat le plus proche de la destination, nous proposons de choisir plutôt celui qui correspond au lien de communication le plus stable.

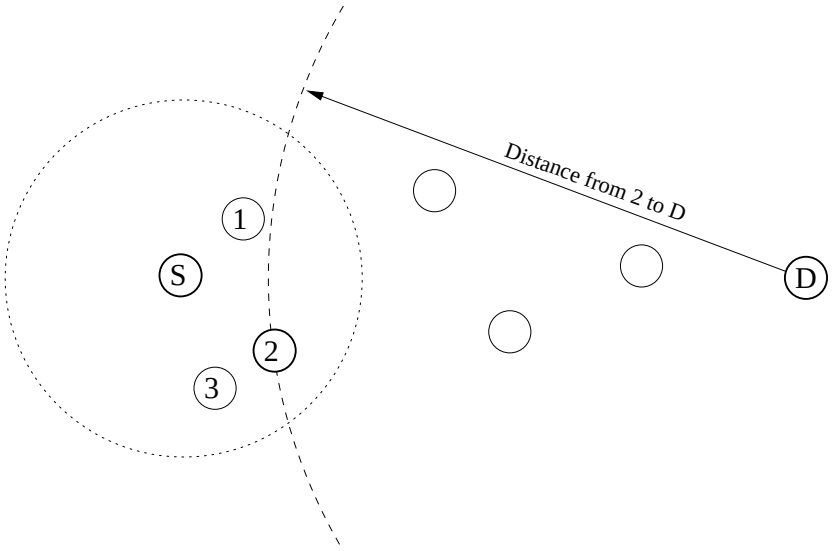

Figure 1.12: Fonctionement de GPSR.

Autrement dit, on choisira celui qui correspond à la métrique LS la plus grande.

Prenons l'exemple dans Figure 6.19, qui montre comment le prochain transmetteur est sélectionné dans GPSR, avec et sans l'utilisation de MOPR.

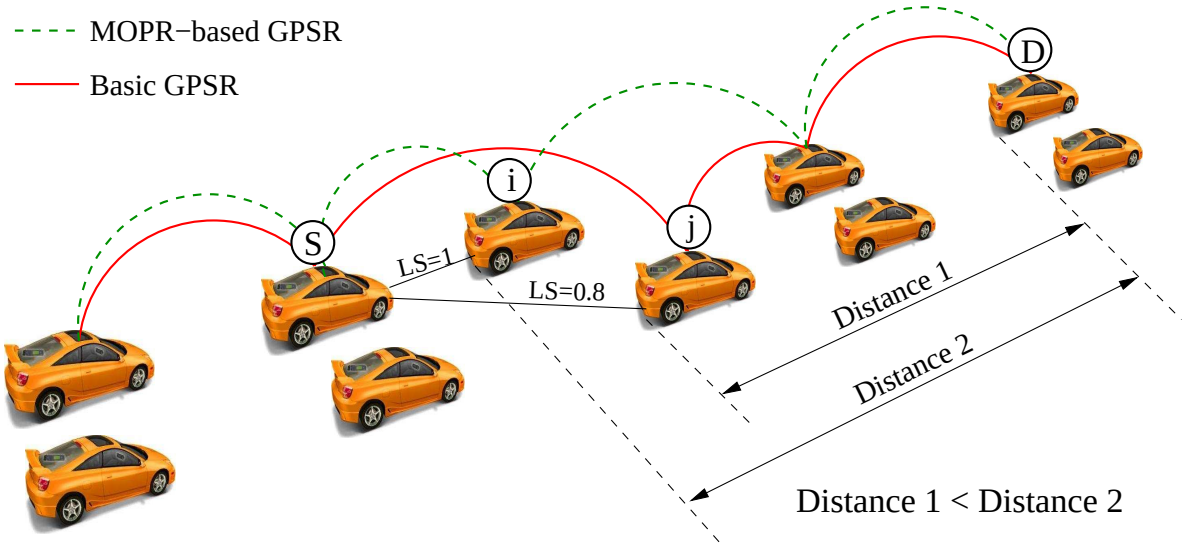

Figure 1.13: Sélection du Prochain Transmetteur dans GPSR Basée sur MOPR.

Le nœud "S" connait la métrique de stabilité LS de chacun de ses voisins (nœud i et nœud j) grâce à MOPR. En se basant sur cette information, le prochain transmetteur est choisi. Dans notre exemple, "S" choisira comme transmetteur le nœud "j', qui n'est pas le plus proche de la destination ($Distance2 > Distance1$), mais le plus stable (le LS correspondant est le plus fort).

Nous avons réalisé plusieurs simulations avec le simulateur de réseaux NS2 afin d'évaluer les performances de MOPR appliqué à GPSR. Nous avons modifié une implémentation NS2 de GPSR, et nous nommons cette version modifiée GPSR-MOPR.

Dans ces simulations nous avons utilisé un scénario réaliste (une autoroute), dans lequel nous lançons quelques liaisons de communication UDP entre différents couples (source, destination). En observant différents paramètres au niveau réseau, nous remarquons que GPSR-MOPR améliore GPSR en terme de délais de communication, en terme de charge du réseau, et aussi en terme de taux des succès de livraisons des paquets à destination.

1.5 MAC assisté par MOPR dans les Réseaux VANETs

Apres avoir montré les capacités de MOPR dans l'amélioration des performances d'un réseau au niveau routage, nous allons montrer ces capacités au niveau MAC.

Ils existent plusieurs protocoles MAC qui peuvent êtres utilisés pour garantir les communications dans les réseaux VANETs, mais aujourd'hui il semble que c'est le standard IEEE 802.11p qui sera adopté pour ce type de communication, nous avons donc choisi le protocole MAC de ce dernier pour étudier l'application de notre algorithme.

1.5.1 Les Standards IEEE 1609 et IEEE 802.11p

Le IEEE 802.11p fait partie de l'architecture IEEE 1609. Ce standard est inspiré, au niveau MAC, des deux standards IEEE 802.11a et IEEE 802.11e, tout en utilisant la technique CSMA/CA et en intégrant le support de la qualité de service (QoS) par l'utilisation de différents niveaux de priorité, où chaque niveau utilise une valeur de CW (Contention Window) spécifique. La CW est expliquée dans ce qui suit.

1.5.2 Fenêtre de Contention (CW : Contention Window) dans le IEEE 802.11

Dans les standards IEEE 802.11, au niveau MAC, la CW est utilisée pour éviter/réduire les collisions entre les transmissions voisines.

La CW est une fenêtre de slots de temps, initialisée entre la CW la plus petite ($CWmin$) et la plus grande ($CWmax$), dans laquelle un nœud choisira d'une manière aléatoire un temps d'attente qui le sépare de la prochaine tentative d'accès au canal. Ce temps d'attente est choisi d'une manière aléatoire afin de réduire les risques de collisions entre les transmissions.

Au départ, la CW est initialisée avec la valeur de $CWmin$, puis elle est augmentée après chaque échec d'accès au canal, jusqu'à ce qu'elle atteigne la valeur de $CWmax$.

La CW est un paramètre très important qui doit être choisi judicieusement. Si elle est très petite, le risque de collision augmente, et si elle est très grande elle engendrera des délais supplémentaires non nécessaires. Idéalement, la valeur de la CW est initialisée en fonction du nombre des nœuds présents dans le voisinage de communication.

1.5.3 Adaptation de la CW en se Basant sur MOPR

La CW est un moyen pour réduire les collisions entre les transmissions, mais aussi un moyen pour offrir différents niveaux de priorités entre les transmissions, et cela par l'utilisation de différentes valeurs de CW. Ce système de priorité est utilisé pour offrir une certaine QoS dans le réseau. La plus petite CW et attribuée aux transmissions correspondantes au messages de plus haute priorité, et les CW les plus larges sont attribuées aux transmissions correspondantes aux messages de plus faible prioritè.

Dans cette thèse nous proposons de combiner MOPR avec ce système de priorité. Quand nous avons différents voisins avec qui nous avons des transmissions en cours, nous proposons de donner plus de priorité aux voisins quittant notre voisinage le plus tôt. Autrement dit, une transmission correspondante à un lien aillant la plus petite valeur de LS, donc correspondante à un voisin qui va partir plus tôt, aura le plus d'avantage. Pour réaliser cela, nous adaptons la valeur de la CW à la celle de LS du lien de communication en question. Plus la valeur de LS est impotante, plus celle de la CW est important aussi, et vice-versa.

Regardons le scénario montré dans Figure 1.14. Nous avons deux nœuds (véhicules) "A" et "B", conduisant à coté d'une station de base "U". Les deux nœuds, qui ont le même rayon de communication, ont en même temps une communication en cours avec "U". Nous supposons que le nœud "A" roule avec une vitesse plus importante que celle de "B". Donc, le nœud "B" restera plus longtemps dans le rayon de communication de "U" que le nœud "A". Autrement dit, le nœud "A" aura moins de temps, et donc moins de chance, pour accéder au canal et communiquer avec "U" que le nœud "B".

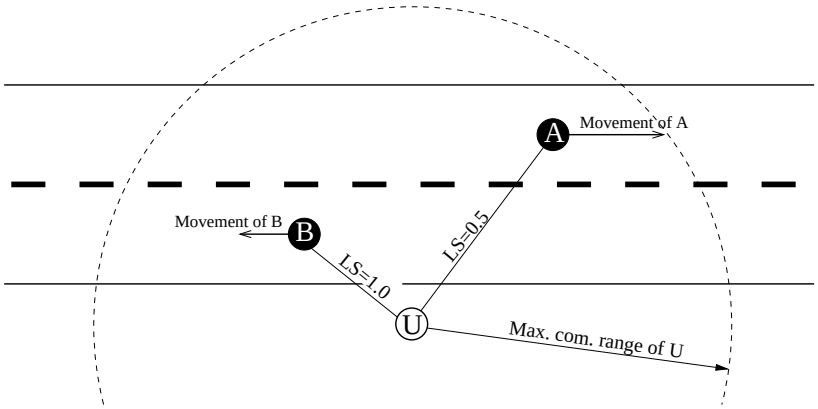

Figure 1.14: Scenario Motivant l'Importance de le Prediction de Mouvement dans l'initialisation de la CW.

Pour pouvoir garantir une même chance dans l'accès au canal, une certaine discrimination entre les nœuds est nécessaire. Cette discrimination donnera plus de chance, et de priorité, aux nœuds quittant le rayon de communication le plus tôt. Dans notre exemple, nous donnons plus de priorité au nœud "A".

Pour cela, le nœud "A" utilisera une CW avec des valeurs plus petites. Dans le même exemple montrè dans Figure 1.14, le lien de communication entre "A" et "U" a un LS plus

petit quand nous le comparons au LS correspondant au lien de communication entre “B” et “U”. Donc, en donnant plus de chance dans l’accès au canal au nœud correspondant au plus petit LS, nous donnerons plus de priorité au nœud “A”.

Cependant, ce que nous proposons ici est une sorte de QoS au niveau MAC pour le standard IEEE 802.11, en donnant plus de priorité aux nœuds correspondants aux plus petits LS. Cette printanisation peut être réalisée en utilisant de plus petites CW par les nœuds correspondants aux liens avec des LS de plus petites valeurs.

Nous proposons donc d’utiliser une nouvelle CW, que nous nommons $CWnew$. Cette $CWnew$ est égale à la valeur originale de CW si la communication concernée doit passer par un lien qui a un LS égale à 100%. La valeur de CWnew est calculée en fonction de la valeur CW originale et la valeur LS du lien correspondant. Plusieurs formules peuvent être utilisées pour le calcule de cette $CWnew$, mais dans ce travail nous considérons que celle-ci :

$$CWnew = CW * LS$$

Figure 1.15 montre comment la CWnew est initialisée pour les nœuds “A” et “B” dans l’exemple présenté dans Figure 1.14. La CWnew est égale à 11 slot de temps pour le lien avec le nœud “A” et à 15 slots de temps pour le lien avec le nœud “B”.

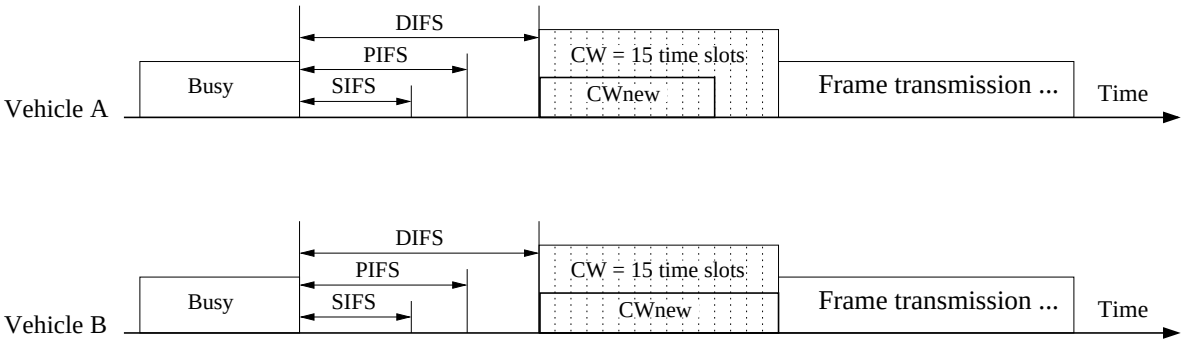

Figure 1.15: Exemple d’initialisation de la CW en utilisant MOPR.

Dans ce qui suit nous montrons quelques simulations, et leur résultats, que nous avons réalisées afin de valider notre proposition d’adaptation de la CW en fonction de la valeur de LS.

1.5.3.1 Simulations et Résultats

Pour valider notre proposition d’adaptation de la CW en fonction de la métrique LS, nous avons réalisé quelques simulations en utilisant le simulateur de réseaux NS2. Pour cela nous avons choisi l’implémentation NS2 du protocole MAC du standard IEEE 802.11, sur laquelle

nous avons apporté quelques modifications afin qu'elle supporte notre algorithme MOPR. Nous nommons l'implémentation initiale "IEEE 802.11" et celle modifiée "IEEE 802.11-MOPR". Parmi les différentes simulations que nous avons réalisé, nous allons citer deux groupes ici. Les premières simulations sont très simples. Elles consistent juste à avoir une première vue sur les performances que notre algorithme peut apporter. Nous fixons donc un nœud "A" quelque part sur une route, et nous l'entourons d'un ensemble de nœuds localisés sur la même route. Nous prenons un nœud "B" et nous l'installons sur la même route, et puis nous faisons en sorte qu'il fasse des va-et-vient entre les deux points P1 et P2 comme montré dans Figure 1.16.

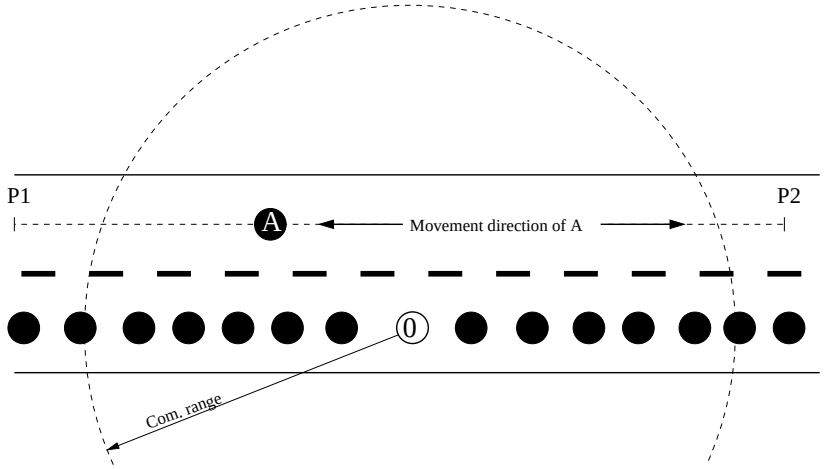

Figure 1.16: Scénario de Simulation Basique.

Nous lançons une transmission continue entre les deux nœuds "A" et "B", et nous observons les différents paramètres au niveau MAC. Nous remarquons que "IEEE 802.11-MOPR" améliore "IEEE 802.11" en terme de collision entre les transmissions, en terme de taux des succès de délivrance des paquets à destination, et en terme de délais moyen des transmissions.

Dans la deuxième série de simulations, nous utilisons un scénario d'autoroute, donc plus réaliste. Dans ces simulations nous lançons quelques communications UDP entre différents couples (source, destination) dans le réseau, et nous observons différents paramètres au niveau MAC et au niveau réseau, sachant que nous utilisons GPSR comme protocole de routage.

D'après nos observations, MOPR améliore les performances du réseau au niveau routage, en terme du taux moyen de succès de délivrance des paquets à destination, et en terme du délais moyen des transmissions.

1.6 Le Prototype de MOPR

Etant donné que cette thèse s'était déroulée dans un cadre industriel, l'exportation de ses résultats dans un environnement réaliste était une réel nécessité. Pour cela, nous avons développé un prototype de MOPR sous Linux, et nous l'avons testé sur la route avec de vraies voitures.

1.6.1 Paramètres et Configurations

Notre prototype comporte deux ordinateurs portables avec les configurations suivantes :

- CPU : Pentium 4
- OS : Linux Fedora Core 2, avec kernel 2.6 et GCC 3.0
- Antenne GPS : Adaptateur USB NAVILook 1Hz
- Interface Radio : IEEE 802.11b
- MaxLifeTime : 30 seconds

Pour les tests nous avons embarqué chacun des deux ordinateurs dans une voiture. Une photo d'une des deux voitures avec notre système embarqué est montrée dans Figure 1.17.

1.6.2 Testes de Validation est Analyse des Résultats

Parmi les tests que nous avons réalisés sur la route autour de notre laboratoire à Sophia-Antipolis, nous en avons choisi que deux à présenter ici.

1.6.2.1 Première série de Tests

Les premiers tests consistent à garder les deux voitures stationnaires sur une route à une distance de 70 mètres l'une à l'autre. Puis, nous lançons notre système et nous observons la variation dans la valeur de LS qui est fournie par MOPR, tout en la comparant à sa valeur théorique qu'on devrait avoir. Cette valeur théorique est bien évidement égale à 100 (100%) sachant que notre rayon de communication ici dépasse largement les 70 mètres. De nos observations nous avons constaté que dans la plupart des cas MOPR donne une valeur de LS égale à 100%, et donc égale à la valeur théorique.

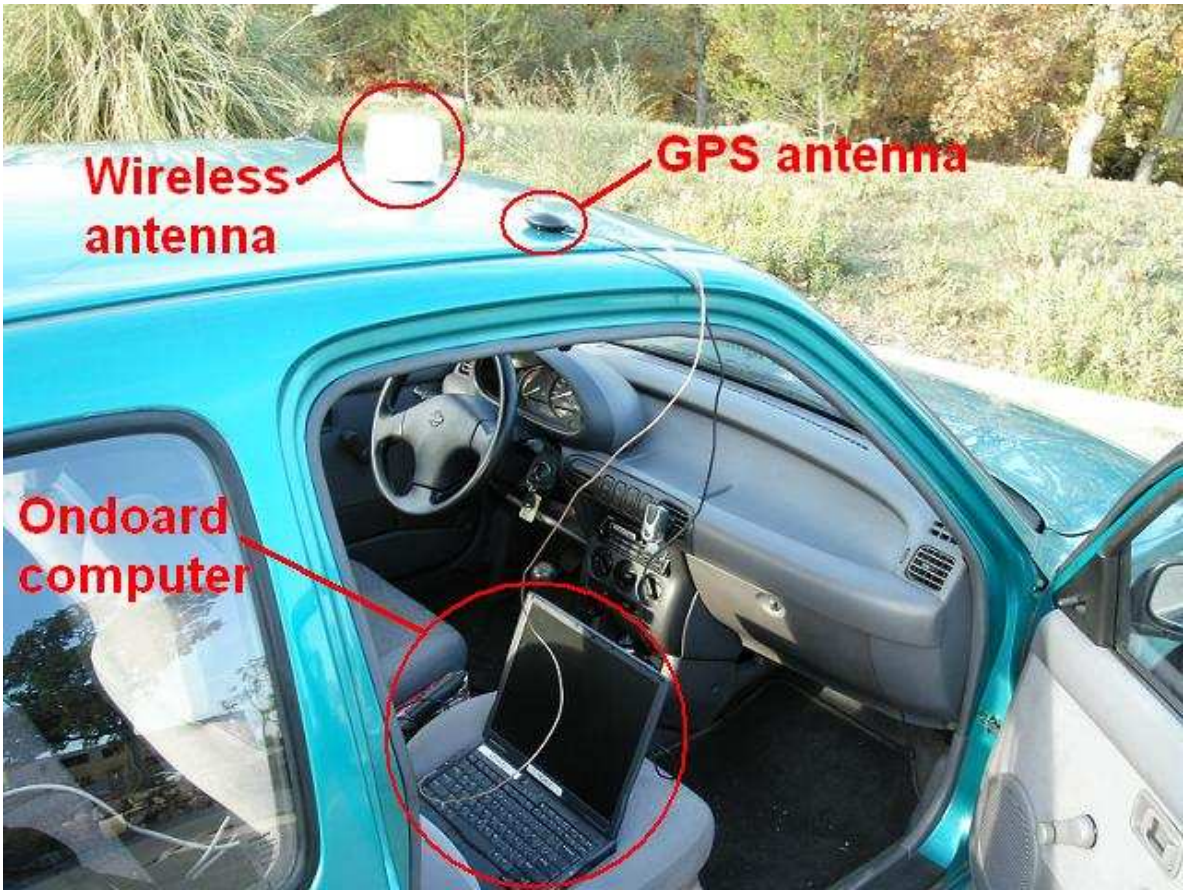

Figure 1.17: Voiture de Test avec le Prototype de MOPR Embarqué.

1.6.2.2 Deuxième Série de Tests

Dans ces tests nous gardons une voiture stationnaire sur la route, et laisser la deuxième rouler avec une vitesse fixe d'environ 15 Km/h d'un point A à un point B sur la même route. Le point A et localisé devant la première voiture à une distance de 7 mètres, et le point B à une distance de 80 mètres. Durant ces tests nous observons la variation de la valeur de LS, tout en la comparant à sa valeur théorique. Nous observons aussi la variation de la distance obtenue à partir des positions fournies par le GPS, tout en la comparant à la distance réel entre les deux voitures. La Figure 1.18 montre une photo que nous avons prise de l'intérieur de la première voiture de façon qu'on puisse voir la deuxième voiture, dehors devant nous.

Les résultats que nous avons obtenus à partir de ces tests sont représentés dans les graphes montrés dans la Figure 1.19. Les graphes correspondants aux variations des les distances montrent que la distance calculée en se basant sur les informations fournies par le GPS convergent

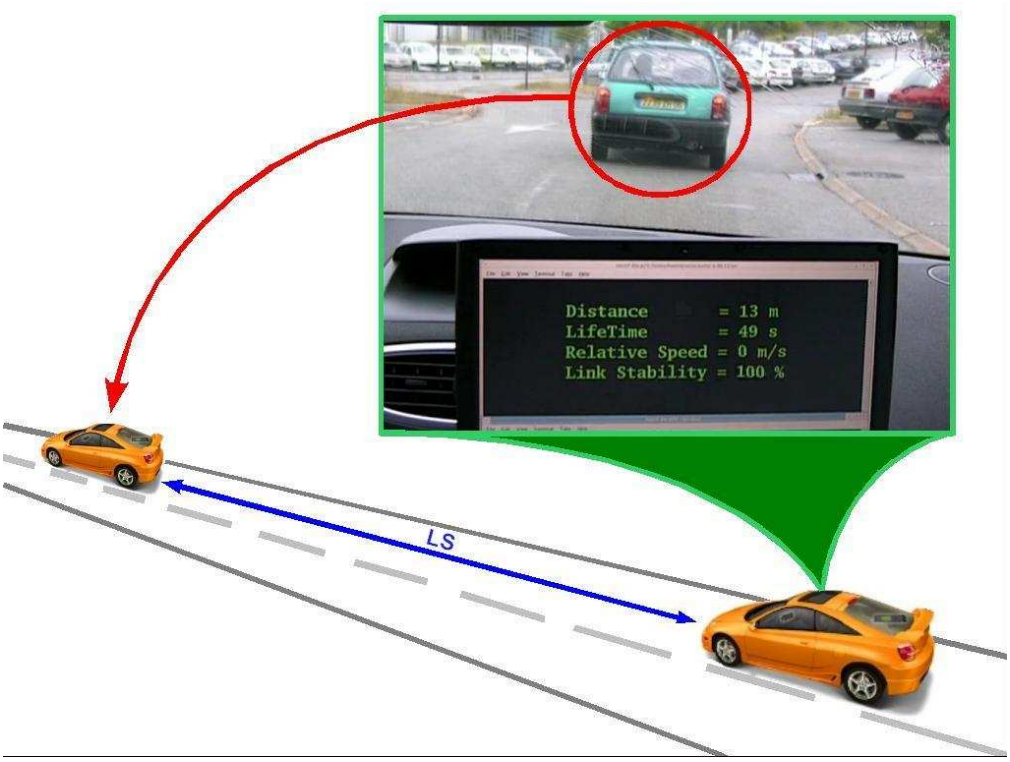

Figure 1.18: Tests sur la Route avec Deux Voitures.

clairement vers les distances réels. Par contre, quand nous observons les variations dans les valeurs de LS, nous remarquons que contrairement aux valeurs théoriques, parfois LS monte brusquement à 100%. Ces piques dans les valeurs de LS sont en fait dues aux erreurs dans le calcul de la vitesse basé sur le GPS. Donc, nous pourrons dire que la précision des données GPS ont un impact direct sur la précision des valeurs LS fournies par MOPR.

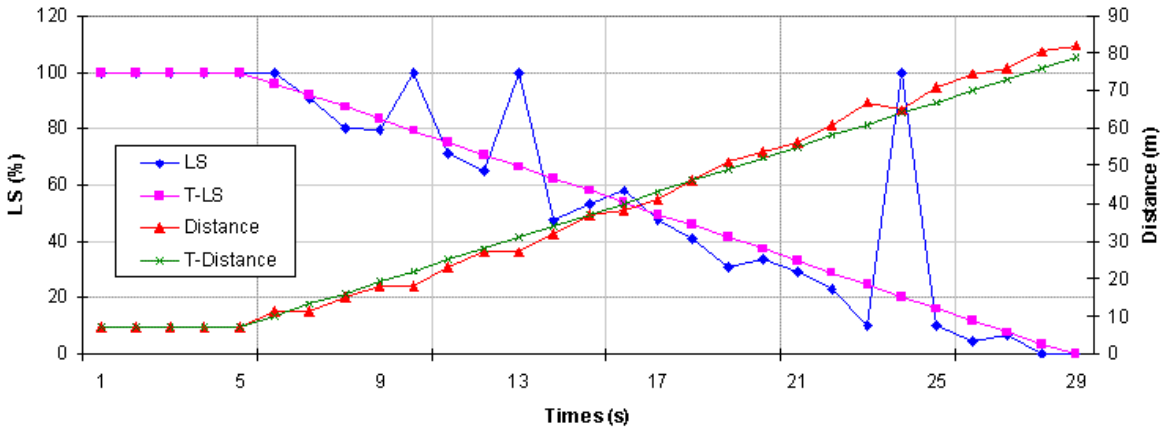

Figure 1.19: Comparaison de Variations dans les valeurs Théoriques et Réels de LS et de la Distance.

1.7 Conclusions et Perspectives

Dans ce résume en Français, nous avons donné un vue générale sur les points les plus importants dans cette thèse. Nous avons d'abord brièvement présenté les réseaux MANET et puis les réseaux VANETs, tout en donnant une idée sur les principales différences entre ces deux types de réseau. Apres cela, nous avons présenté notre algorithme de prédiction de mouvement MOPR. Puis, nous avons présenté comment la métrique LS, fournie par MOPR, pourrait être utilisée au niveau routage et/ou au niveau MAC pour améliorer les performances du réseau. Dans ce résumé nous ne sommes pas rentré dans les détails des résultats de simulation que nous avons obtenu dans cette thèse. Avant de conclure ce résumé, nous avons brièvement présenté le prototype de MOPR que nous avons développé durant cette thèse, et que nous avons validé par des tests sur la route avec de vraies voitures.

On dit que le résultat de la recherche est le besoin de faire plus de recherche. Avec les systèmes hétérogènes et distribués, qui sont tellement compliqués et complexes, nous avons toujours besoin de plus d'effort et plus de recherche. Notre travail présenté ici n'y échappe pas, et donc nous allons essayer de lister quelques directions intéressantes pour le future :

- Pour valider notre algorithme, nous avons utilisé le simulateur de réseaux NS2 seulement, et un prototype que nous avons validé avec quelques tests sur la route à petit échelle. Donc, il serait intéressant de confirmer ces validations par des études et des analyses mathématiques.

- La métrique LS est obtenue par la normalisation de la LifeTime en la divisant par la constante MaxLifeTime. Nous n'avons étudié ni la méthode pour choisir cette constate ni sa valeur optimale, chose qui peut faire l'objet de futures travaux de recherche.

- Au niveau MAC, nous avons investigué l'idée de l'adaptation de la valeur CW à la métrique LS seulement. Plusieurs autres idées peuvent faire l'objet de futurs travaux de recherche, comme l'adaptation de la valeur CWmax à la place de celle de CW.
- Le prototype que nous avons développé, malgré qu'il comporte déjà une bonne partie de MOPR, il n'est pas encore terminé. Il doit faire l'objet d'une intégration avec un protocole de routage afin qu'il forme un system plus complet. Un système qui sera testé sur la route avec de vrais véhicules, chose qui reste toujours très difficile à gérer.

Ce résumé n'est qu'un survol sur le contenu de cette thèse, nous vous invitons donc à consulter le reste de ce manuscrit (partie en Anglais) pour pouvoir mieux comprendre notre travail.

Chapter 2

Introduction

These days, anywhere you are, at home, in your office at work, in the airport when waiting your flight, in the restaurant when taking your lunch or your dinner, or even in the street when you are walking, you may connect to the Internet using your laptop or your mobile phone to see news, to reed your emails, to chat with your friends and colleagues, and etc. What you need is just that your laptop or your mobile phone be equipped with some specific communication technology such as WiFi, GPSR, UMTS, etc.

The world seems like going to have everything connected to everything. Today your television is connected to your computer which is connected to Internet, and through Internet your office computer can communicate with your home computer, or through a direct radio communication it can communicate with any nearby communicating device such as your PDA, etc. What about tomorrow? do you thing everything will be connected to everything? do you think your own car, for example, will be able to communicate with your neighbor's car or even with other vehicles in the road? Do you think it will be possible to connect your car to your home or office computers? or to your PDA? I know, it looks like far future, but if you look to the reality, this seems really feasible in a near future. Let us take the example of making your car communicating. There are many car-makers, if not all of them, believing on such technology, and most of them are already involved in different projects and consortium that have the aim to design and to standardize such technologies. In the Car-to-Car Communication Consortium (C2C-CC) [1] for example, partners aim to standardize the Car-to-Car (C2C) and Car-to-Infrastructure (C2I) communications in Europe, and that for Safety and then for comfort related use.

Necessity is the mother of invention, and human before the age of transport were already looking how to communicate over distance. First solutions used were by using carrier pigeons, smoke signals, morse code flags, etc. Nowadays, the situation has largely progressed, thanks to industrial revolution. The Internet is the best example, where people communicate easily and efficiently over all the world. The Internet and all computer networks resulted from the electronic networks that began with the telephone, or telegraph system as it was known in the beginning. The first telephonic line was built in 1844 from Washington to Baltimore, and by 1858 a transatlantic cable was in place. By 1861, all the USA became interconnected over telegraph connections. The Internet today becomes almost indispensable in our life.

Communications can be set without any wired connection as well, thanks again to technology revolution. By using radio transmission two devices can communicate and exchange data between them. Your cell phone is a good example as a result of this revolution. When

you make a phone call with your mobile phone, it establishes a connection through a wireless communication with a nearby base station, which forwards the call to destination. This networks are called cellular networks because of the coverage being assured by cells, each one managed by a base station which re-uses the frequency used in other further cells.

Within cellular networks, base stations, access points, and the backbone are deployed before the network can be used. In contrast, Mobile Ad hoc Networks (MANETs) [2] are dynamically formed among a group of wireless users and require no existing infrastructure or pre-configuration. Vehicular Ad hoc Network (VANETs) are a special example of MANETs when the mobile devices are integrated in the vehicle. VANETs have the special characteristic of the network topology which changes very fast and very frequently because of the high mobility of the vehicles. Thus, technical solutions proposed for MANETs are not necessary suitable for VANETs. In this work we propose a new cross layer, which, based on the prediction of the movement of involved vehicles, helps both the network and the medium access mechanisms to deal as much as possible with the high mobility of the vehicles in VANETs.

In Section 2.1 we briefly present the mobile ad hoc networks, and then in Section 2.2 we present the vehicular ad hoc networks. Finally, in Section 2.3 we introduce our main contributions in this work, and then we give the remainder of this dissertation.

2.1 MANET: Mobile Ad hoc Network

In the past decade, there has been a growing interest in MANETs proposed in the beginning for military usage, and having a big potential for commercial usage today. A mobile ad hoc network is a set of nodes capable to communicate to each other through a wireless radio network. A MANET is able to exist without any pre-existing infrastructure and any pre-configuration. In such networks, nodes have mainly the same role, and all of them should cooperate to each other for managing the network. MANETs are totally dynamic and auto-configurable. Figure 2.1 shows an example of a small MANET.

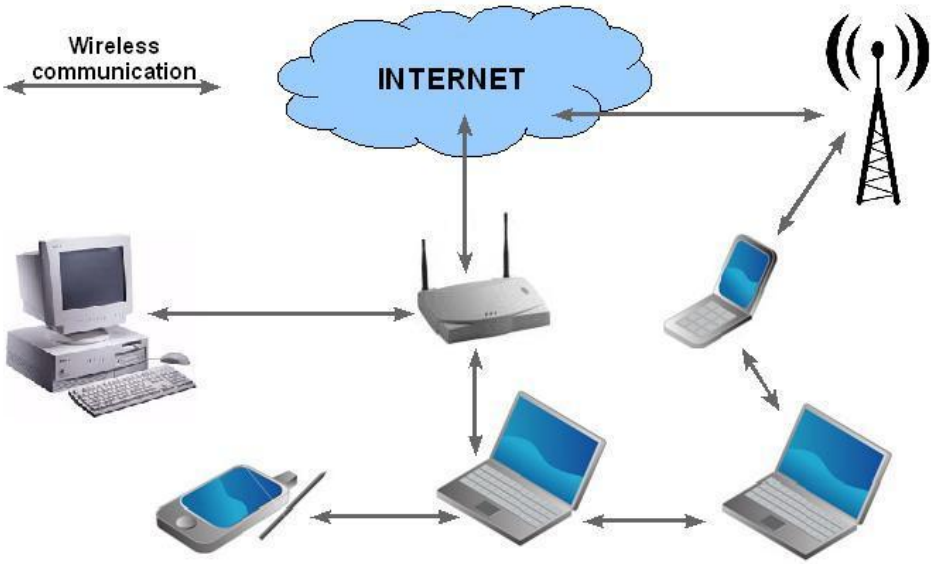

Figure 2.1: An Example of a Mobile Ad hoc Network.

From a communication perspective, the main characteristics of generic MANETs include:

- Distributed networks: network configuration and management must be done in an automatic, dynamic, and distributed manner.
- Node mobility: since the nodes are mobile, the topology of the network can change rapidly and frequently.
- Resources limitation: nodes are often small devices to facilitate their mobility, thus they have resources limited, e.g. laptops, PDAs and mobile phones have power and CPU processing constraints.
- Potentially large networks, e.g. a network of sensors may comprise thousands or even tens of thousands of mobile nodes.

The main advantage of such kind of networks is that they can be quickly deployed, anywhere and at anytime, since they do not require any pre-existing and any centralized infrastructure. Some example applications of such networks include:

- Node to node data exchange: you are somewhere faraway from your office, in a conference room for example, and you want to share some documents with other people from your laptops. With connecting your laptops to each other you form a small MANET which allows you to exchange information.
- Military and emergency use: MANET can be formed among armed forces soldier or emergency service agents to create a tactical network in unfamiliar territory for communications and distribution of situational awareness information.
- Sensor networks: some times we need to deploy a network which covers some areas where deploying infrastructure is very expensive and difficult, or even impossible (e.g., in a dense forest where a network of sensors is needed to gather environmental conditions information). Here, a MANET formed with sensor modes is a good alternative.
- Vehicular MANETs: without deploying infrastructure on all roads, and without using a cellular network (which is potentially expensive), a Vehicular MANET (VANET) [3, 12] allows each vehicle to communicate with nearby or farther vehicles on the same road, or even on different roads. In a VANET, vehicles on the road can communicate to each other for safety use (e.g., to inform vehicles about dangers on the road) or for comfort use (e.g., to exchange information among connected vehicles such as video and music).

2.2 VANET: Vehicular Ad hoc Network

Vehicular Ad-hoc Networks (VANETs) [3, 12] represent a rapidly emerging, particularly challenging class of MANETs. VANETs are distributed, self-organizing communication networks built up from traveling vehicles, and are thus characterized by very high speed and limited degrees of freedom in nodes movement patterns. Figure 2.2 shows an example of a small VANET. Of course some nodes of a VANET can be static, like an intersection cross-light.

In contrast to classical nodes in MANETs, vehicles in VANETs have not the problem of storage and power resources limitation. Thus, in VANETs, wider transmission ranges and

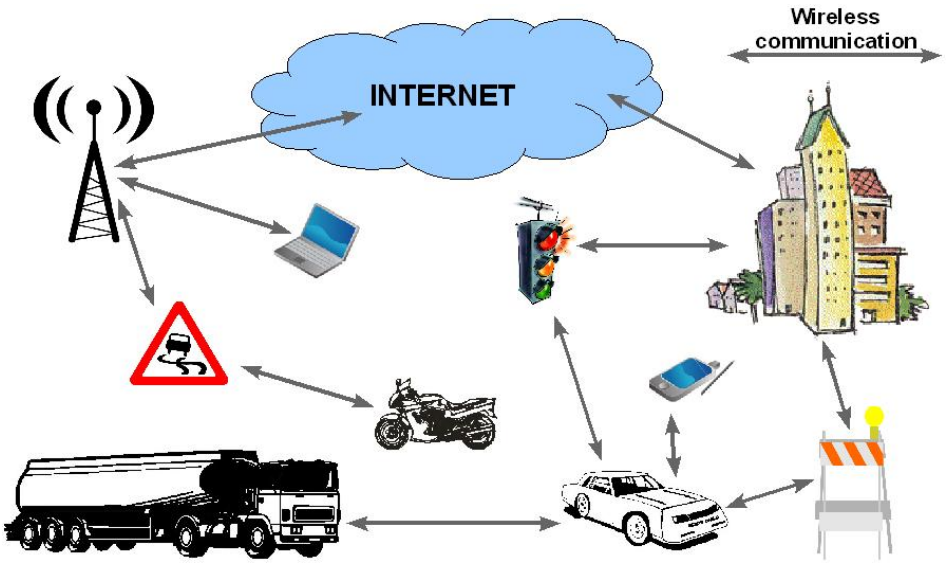

Figure 2.2: An Example of a Vehicular Ad hoc Network.

longer communication lifetimes are possible [3, 12]. In VANETs, vehicles are supposed to be equipped with some satellite based geo-positioning system, like the Global Positioning System (GPS) [5, 6, 7] or the future European positioning satellite system GALILEO [8], which allows each vehicle to get its own physical position. This position information are useful for the application layer, but also for the MAC and the routing layers. These geo-localization systems provide another useful information, which is a common clock that can be used for time synchronization in the network. Another advantage in VANETs is the non-random mobility of the nodes; roads are mapped and digitally available, and driving rules can be electronically represented as well.

The main disadvantage in VANETs when compared to MANETs, is that nodes speed could be relatively high. Which makes the network topology changes frequently and very fast, and it decreases the stability of the transmission wireless channel.

VANETs' applications can be roughly divided into two main categories: the ones related to active safety on the roads[1], and the applications dedicated to improve the comfort of drivers and/or passengers (imagine for example a road-side unit wanting to contact a vehicle for downloading a previously requested set of data). Both of these categories are important, but the first one is very sensitive since human lives will depend on it. C2C communications are suitable for active safety applications because of their nature to be available anywhere, to satisfy strict latencies and to cover localized communications. Taking intersection collision avoidance as an example, listed in the document issued by US DOT (Department of Transportation) [9], the allowable latency to obtain the necessary information should be less then 0.1 second, and the application requires a communication coverage to be up to 300 meters. An article of Tony et al. [10] says that the allowable latency for various V2V applications is typically estimated to be between 100 - 500 ms, while the communication coverage is between 50 - 300 meters, and some requires up to 1000 meters.

[1] active because trying to inform the drivers and/or to act on the vehicle in order to avoid accidents instead of alleviating their consequences like airbags.

For any application in a wireless network, the communicating nodes needs to access to the radio channel in order to transmit or to receive data. The radio channel is considered as a common resource to which several terminals in the same neighborhood can attempt to access at the same time. And since only one terminal should transmit in the same medium at the same time, the access to this channel must be efficiently managed. This is the task of Medium Access Control (MAC) protocols.

Again because of the radio channel characteristics, a node's transmission can be heard only by nearby nodes (a nearby node refers here to a node located not farther than the maximum communication range). Thus, in case the desired node is farther than the communication range, the communication has to go through multi-hop transmission, i.e. the data packet will be forwarded from the source to the destination through intermediate nodes located in between. This process is called "data forwarding" and it is the task of routing protocols.

The inherent characteristics of VANETs often make networking solutions proposed for MANETs inefficient or unusable for VANETs, and this, combined with the huge impact that the deployment of VANET technologies could have on the automotive market, explains the growing effort in the development of communication protocols which are specific to vehicular networks.

VANETs are a very promising use-case of MANETs, that is why we consider VANETS as our main interest in this thesis. We concentrate only on data routing and medium access. The existing and well working MANETs' MAC and routing protocols are not suitable (as they are) for vehicular communications [11, 12]. Our goal in this thesis is to investigate the routing and the MAC protocols in VANETs. And, since the main characteristic of VANETs highly belongs as previously said in the movement pattern of vehicles which results in a network topology dynamic when comparing to MANETs. We believe that considering this parameter (i.e., vehicles' movement information) is important when improving or adapting data routing and MAC mechanisms for VANETs' usage. For example, by predicting the movement of surrounding vehicles we get a future view on the network topology which helps in improving network performances.

2.3 Contributions and manuscript organization

A VANET is a set of interconnected vehicles, and a vehicle is supposed to know its physical position (e.g., by using a GPS), its speed, and its movement direction as well. So, a vehicle knows its movement information. A vehicle may be aware about the movement information of vehicles located in its vicinity, based on an information exchanging mechanism. All these information may be exploited to improve the performances of the network in terms of data routing and MAC process.

We know that one of the main properties of VANETs when compared to MANETs is the vehicles' movement pattern. Thus, we believe that, if we want to adapt existing MANET solutions to VANETs characteristics, first thing we should consider is the vehicles' movement pattern. A node can have an advanced view on the network topology by predicting the movement of vehicles. Thus, a node is able to know in advance which neighbor is going to leave sooner its vicinity or not. Based on this feature (movement prediction), we propose a MOvement PRediction (MOPR) concept. MOPR is a sort of a cross layer running between the MAC and the network (NET) layers. It has as input the neighbors' movement information (which comes from the NET layer), and as an output the Link Stability (LS) metric which is

attributed to each neighboring communication link. This LS is then used by both the NET layer (by the routing mechanism), and the MAC layer (by the medium access mechanism).

At the NET layer, by knowing in advance the network topology status, thanks to the movement prediction-based link stability metric, most stable routes may be selected when needed, i.e. if different routes are available from a source to a destination, the route which is the most stable is chosen. Knowing that a stable route is the one composed by the most stable intermediate links (communication links corresponding to the highest LS). We name this contribution as MOPR-assisted routing.

At the MAC layer, because of the high dynamic network topology, some nodes get less chance then others to get access to the medium. When several nodes cross an area covered by the communication range of a common neighbor, the node which moves faster will spend less time in this area. Thus, it will get less chance to communicate with it when comparing to the other nodes which drive with a lower speed. To avoid such discrimination, the prediction of the movement of the neighbors can play a big role. We can predict the duration time each neighbor is going to stay in the communication range, and then we be able to give more advantage to nodes leaving the communication range sooner, when trying to access the medium . The main idea behind this contribution, which we call MOPR-assisted MAC, is to give more chance when attempting to access the medium to a nodes that correspond to lower Link Stability (LS) metrics.

The rest of this manuscript is organized as follows.

We provide a general overview on both routing and MAC protocols in Chapter 3 with focus on those adapted or proposed for VANETs. This review identifies three main families: unicast topology-based routing in reactive and proactive modes, unicast position-based routing, and hybrid routing. We focus on position-based family which seems the most suitable for vehicular ad hoc networks. In Chapter 4 we briefly review the Medium Access Control (MAC) protocols proposed for MANETs, and then we investigate their suitability, adaptation proposal for VANETs.

From our reviews and investigations in both Chapter 3 and Chapter 4, we conclude that technical solutions at both MAC and network layer that have been proposed for MANETs or VANETs, can hardly deal with VANETs' characteristics, such as the network topology that changes fast and often because of the high mobility of vehicles. Therefore, in Chapter 5 we propose the MOPR (MOvement PRediction) cross layer architecture, which has the aim to help the routing and the MAC process in very dynamic networks such as VANETs.

In Chapter 6 we explain in detail how MOPR can be applied to topology-based and to position based routing protocols. In case of topology-based routing, we present two implementations of MOPR, the first one to a reactive routing protocol, and the second one to a proactive routing protocol. Since topology-based routing protocols are not the most suitable for VANETs, this two implementations are presented in this chapter just to show how MOPR improves that routing mode. Position-based routing protocols are most suitable for VANETs, thus we present an implementation of MOPR in GPSR, which is one of the well known position-based routing protocols.

In Chapter 7 we present how MOPR can improve the performances of MAC mechanisms in high mobile networks, such as in VANETs. MOPR attributes to each communication link a LS, and this LS information helps the MAC mechanism to avoid the bad discrimination between nodes in getting access to the medium. MOPR may improve different MAC mechanisms, but in this thesis we have limited our implementation to IEEE 802.11 MAC since it has a big

potential to be the MAC mechanism used in vehicular networks. MOPR may enhance the IEEE 802.11 MAC mechanism in several ways, but only one has been presented in this work, which consists on adapting the contention window to the LS information.

Finally, Chapter 8 summarizes this dissertation and discusses future perspectives.

Chapter 3

Data Routing in Vehicular Ad hoc Networks

3.1 Introduction

A mobile ad hoc network consists on a set of mobile nodes able to communicate between them through wireless transmission. A wireless transmission has limitations in terms of distance coverage. Because of this limitation, a node is able to physically communicate only with nodes located in its communication range. To communicate with other nodes, located farther than the maximum communication range, a multi-hop communication is needed. This communication manner is done by making a set of intermediate nodes forwarding data from the source node until the destination node. The set of nodes involved in this data forwarding from the source to the destination form a route, or a path. This route is found and maintained in a specific way by some dedicated protocols which we name routing protocols. Thus, a routing protocol is responsible of discovering end eventually maintain in the network a routing route from a source to a destination.

In this chapter we start by giving an overview on only few routing protocols that are of our interest in the rest of this thesis. Then, we list routing solutions adapted, or even initially proposed for vehicular ad hoc networks.

This chapter is an introduction for our proposal described in Chapter 5 and its application to the routing process described in Chapter 6.

The remainder of this chapter is organized as follows. In Section 3.2 we list the main issues and the main requirements that should be considered when designing any routing protocol for ad hoc networks. In Section 3.3, we briefly present few of the main existing routing protocols proposed for MANETs, classifying them into two big categories, and in Section 3.4 we present some routing protocols proposed for VANETs. Finally, Section 5.5 provides a summary of this chapter.

3.2 Issues and Requirements in Designing Data Routing Protocols

A routing protocol is responsible of finding a route in the network between a pair of nodes, while respecting criteria such as minimum hop length, minimum power required, maximum

path and link lifetime, minimum processing power and bandwidth, etc. The major issues and requirements that a routing protocol should face are listed in what follow.

3.2.1 Mobility

Nodes' mobility is one of the important criteria of an ad hoc network. The mobility of the nodes makes the network topology changes, which results in frequent breaks in routing routes. A route which breaks, often results in routes reconstruction and packet loss, thus in addition resources consumption. Because of this mobility, even resources reservation is almost impossible. A good routing protocol should consider all these issues and all there related direct or indirect impacts on the network.

3.2.2 Bandwidth limitation

As said previously, a route is composed by different couple of nodes connected via wireless links. A wireless link can be shared at the same time between two routes or even more. The wireless link has a limited bandwidth due to its physical characteristic. This bandwidth is shared between all communications passing through the related wireless link. Thus, more the number of communications passing through a wireless link is higher, less is the available bandwidth for each communication. This issue should be taken into account when designing a routing protocol.

3.2.3 Resource limitation

There are three main limited resources in ah hoc networks: battery lifetime, storage space, and processing power, knowing that nodes in ad hoc networks are mostly mobile and portable. Even with today technologies, when nodes can be equipped with enough storage space and processing power, the batteries limitation is still a problem and an issue to manage in some specific situations, such as networks with very small communicating nodes.

3.2.4 Minimum route acquisition delay

In ad hoc networks, when a node wants to reach a destination in the network, it must find a route to it. The duration of time spent to find this route is called the route acquisition time or delay, and should be as small as possible. Less the route acquisition delay is, better the related routing protocol is.

3.2.5 Quick route reconfiguration

In ad hoc networks, after finding a route, the source node, and even intermediate nodes in some situations, has to maintain this route for short or a long period depending on the routing scheme. And because of the mobility of nodes, a route is suspected to breaks frequently, which often results in the necessity of re-finding a new route. Such process should be done by a fast and efficient procedure.

3.2.6 Loop-free routing

Because of the random movement of nodes in ad hoc networks, loops in the routes can be formed. This loops results in additional useless transmissions. Thus, this must be avoided as much as possible by any routing protocol.

3.2.7 Distributed routing approach

Ad hoc networks are totally distributed, and should be able to work anywhere without the presence of any centralized management. In such distributed environment, a centralized routing approach causes a considerable bandwidth consumption. Thus, any routing protocol proposed for such networks should work in a totally distributed manner.

3.2.8 Minimum control overhead

Any routing protocol management consists on two steps. Neighbors discovering and routes building and maintenance. This is done based on control messages exchanged in the network. These messages are called control packets or control messages. They are exchanged in the network in a reactive or proactive manner depending on the routing scheme. More the quantity of control packets sent in the air is important, more transmission collisions and bandwidth consumption occur, resulting in decreasing the throughput in the network. Thus, the quantity of control packets should be reduced as much as possible..

3.2.9 Scalability and Provisioning of QoS

A routing protocol should be able to work with large size networks in terms of number of nodes. More the number of nodes involved in the network is high, more the routing overhead could be high. So, to scale well with large network a good routing protocol should minimize as much as possible the routing overhead.

Some applications need the routing protocol to be able to provide a certain level of Quality of Service (QoS). The QoS parameters can be bandwidth, delay, jitter, packet delivery ratio, or throughput.

3.3 Data Routing Protocols for MANETs

In the previous section we have discussed the main issues and requirements in designing a routing protocol for an ad hoc network. Now, in this section we review few existing routing protocols that have been proposed for ad hoc networks. We focus on two main schemes of routing protocols: topology-based and position-based routing schemes, with presenting one or two routing examples in each scheme.

3.3.1 Review and Classification of Routing Protocols

Routing protocols proposed for ad hoc networks can be classified in various manners. For example, the authors of [13] classified existing routing protocols into four categories as shown in Figure 3.1, and that based on the following criteria:

- Routing information update mechanism: the manner of updating the routing information can be done in proactive or reactive manner, or even in a mixture manner (hybrid) where both reactive and proactive schemes are used.
- Use of temporal information for routing: a routing protocol can use some temporal information of the network, such as the past or the future status of the communication links.
- Routing topology: depending on the network size, the routing topology may be managed in a hierarchical or flat manner. In case of large network, such as Internet, a hierarchical scheme is used to reduce the state information maintained at the core routers.
- Utilization of specific resources: routing protocols may be classified based on the use of some specific resources, such as the geographical information of the network or the power consumption.

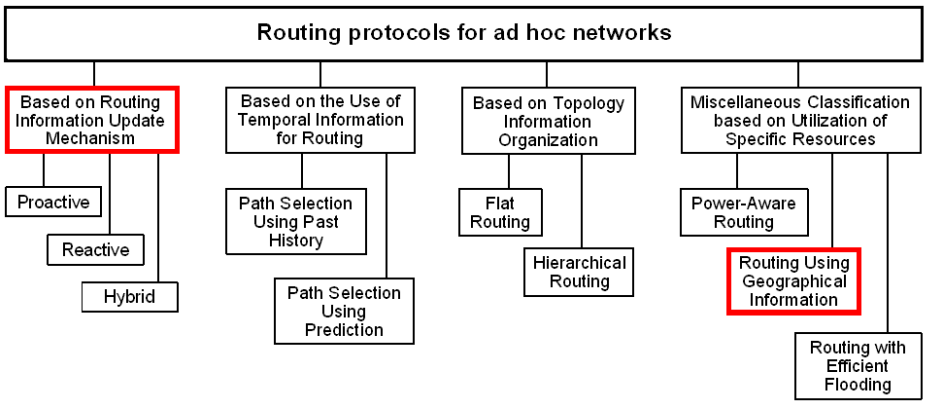

Figure 3.1: Classification example of routing protocols [13].

In the rest of this work we focus only two classes of unicast routing protocols: topology-based and position-based routing schemes, as shown in Figure 3.2. With respect to this classification we present the routing protocols of our interest in what follows.

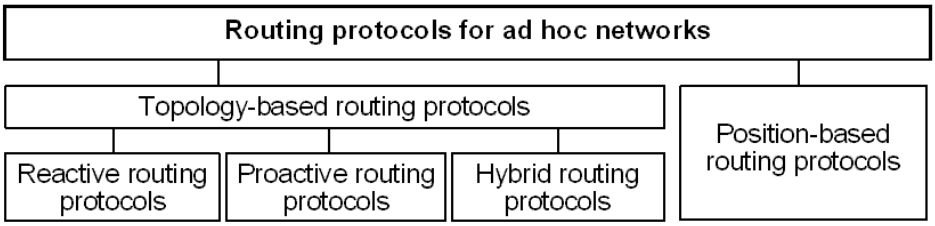

Figure 3.2: Our classification for routing protocols.

3.3.1.1 Topology-based routing scheme

A topology-based routing protocol maintains a routing table locally in each node in the network. This table which should offer efficient routes to destinations, contains a global or a

partial information of the network topology. Since the network topology is dynamic, this table should be frequently updated. This update can be done in a reactive or a proactive mode, or even in a mixture of both reactive and proactive modes at the same time (hybrid mode). Thus, topology-based routing protocols can be classified based on the routing information update mechanism into three major categories as follow.

3.3.1.1.1 Reactive approach In reactive routing mode, called on-demand routing mode as well, the routing table at every node is updated only when needed. When a sender node wants to reach a destination node in the network, and it does not know the route to this end, it starts a route finding process. Routing protocols working in this mode are called reactive routing protocols.

Withing reactive routing, to find a route to a destination node, the source floods a Route Request (RREQ) packet in the network. And once receiving this packet, the destination node, or even an intermediate node that knows the route to the desired destination, replays by sending a Route Replay (RREP) packet back to the source node. The replay packet carries the route traversed by the received RREQ packet.

The Ad hoc On-Demand Vector (AODV) routing protocol [14] is one of the famous reactive routing protocols. In AODV, a source node "S" that does not have any available route to a destination node "D", when having data to send to this destination must initiate a RREQ packet. This RREQ packet is flooded through the network. Each node, upon receiving a RREQ packet, rebroadcasts the packet to its neighbors if it has not already forwarded it, or if it is not the destination node, provided the packet's Time to Live (TTL) counter has not exceeded.

The RREQ packet carries the source identifier ($SrcID$), the destination identifier ($DestID$), the source sequence number ($SrcSeqNum$), the destination sequence number ($DesSeqNum$), the broadcast identifier ($BcastID$), and the TTL. The $DesSeqNum$ indicates the freshness of the route that is accepted by the source. When receiving a RREQ packet, a node replays to the source node by sending a RREP, if and only if it is the destination node, or if it is an intermediate node and it has a valid route to the desired destination, otherwise it forwards the RREQ. The intermediate node is able to determine whether the route it has is valid or not by comparing its own sequence number with the $DesSeqNum$ in the RREQ packet. The same RREQ, if received more than one time, is discarded. An intermediate node is able to know whether the RREQ is already processed or not by comparing the $BcastID$ and $SrcID$ pair. Each intermediate node enters the address of the previous node and its $BcastID$ while forwarding the RREQ packet. A timer is used to delete this entry in case a RREP packet is not received before the expiration time. When receiving a RREP packet, an intermediate node stores as well the information about the node from which the packet is received. This node is considered as next hop when forwarding data to the destination node which initiated the related RREP packet.

Let us consider the example shown in Figure 3.3. This example shows how the source node "S" finds the route to the destination node "D" when using AODV. Assuming that "S" wants to reach "D" and it does not have a route to it, thus it initiates a RREQ packet, with a $DesSeqNum = 3$ and a $SrcSeqNum = 1$ for example.

Once receiving the RREQ from "S", nodes "1" and "2" forward the packet to their neighbors: "3", "4", and "5". With the assumption that both "5" and "3" have already a route to the destination "D" through 10-S and 6-S respectively, if the $DesSeqNum$ at intermediate node

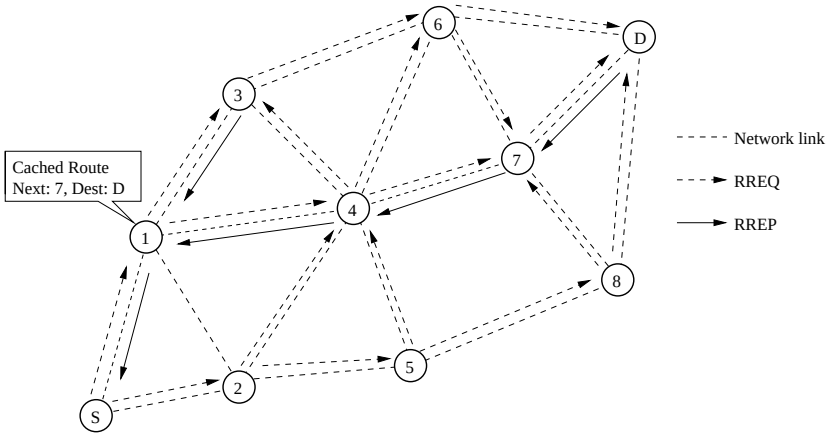

Figure 3.3: Routes building in AODV.

"5" is 1 and is 4 at intermediate node "3", then only node "3" is allowed to replay along the cached route to the source node "S". This is because the cached route at "3" is older when compared to the $DesSeqNum$ in the RREQ packet.

If the destination node "S" receives the RREQ, it initiates a RREP packet to the source as well. Thus, more than one RREP may reach the source node. Each intermediate node, when receiving a RREP packet, update its routing table with the latest $DesSeqNum$, and the routing information also if the new proposed route is shorter in terms of hops.

If the current route breaks, AODV has a mechanism to rebuild a new route. Suppose the link between the nodes "1" and "4" breaks (refer to Figure 3.4). Both "1" and "4" are able to detect that the communication link between them is broken, by observing the periodic beacons for example. Once "1" and "4" learn that the link is broken, they inform the end nodes (i.e., source and destination nodes) by sending to them a RREP packet with the hop count set as ∞. If the source node still needs the related route, when learning that the route is broken, it re-initiates the route-finding process with the new $BcastID$ and the previous $DesSeqNum$.

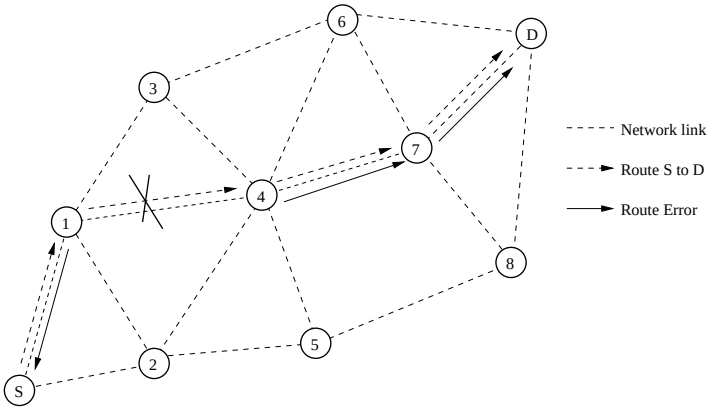

Figure 3.4: Routes maintenance in AODV.

Dynamic Source Routing (DSR) protocol [15] is another famous reactive routing protocol. DSR also establish a route only when needed, by a route finding process which is based on

the RREQ dissemination mechanism. The major difference between DSR and AODV stems out from the fact that in AODV the source node and the intermediate nodes store only the next-hop information corresponding to each flow for data packet transmission. However, DSR uses source routing in which a data packet carries the complete route to be traversed until the destination.

In reactive routing mode, we do not take the initiative to find a route to a destination, until it is required. We attempt to discover routes only on-demand by flooding our query in the network. This type of protocols reduces the routing overhead at the cost of increased latency in finding the routes. Some routing protocols act in a proactive mode in which the latency is reduced, by immediately providing the required routes when needed, at the cost of routing overhead which is considerably increased. This type of routing is described in follow.

3.3.1.1.2 Proactive approach In proactive routing mode, called on-demand and table-driven routing modes as well, each node in the network maintains a a global view of the whole network topology in form of a table, which is periodically updated. Routing protocols working in this mode are called proactive routing protocols.

Various proactive routing protocols have been proposed for mobile ad hoc networks. The Destination Sequence Distance-Vector (DSDV) routing protocol [16] is one of the first proposed protocols acting in this mode. In DSDV, routes to all destinations are readily available at each node in the network. The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology. The tables are also forwarded if significant changes happen in the local topology.

The Optimized Link State Routing (OLSR) protocol [17] is another proactive routing protocol. OLSR is based on periodic exchange of control messages. Some messages are sent locally to enable a node to know its local neighborhood, and some messages are sent in entire network which permits to exchange the knowledge of topology among all the nodes in the network.

In a pure link state protocol, all links with neighbors are declared and flooded in the entire network. OLSR protocol is an optimization of a pure link state protocol. First, it reduces the size of control packets: instead of selecting all links, it declares only a subset of links with its neighbors who are its multi-point relay selectors. Secondly, it minimizes flooding of the control traffic by using only the selected nodes, called Multi-Point Relays (MPRs), to diffuse its messages in the network. Only the MPRs of a node that retransmit its broadcast messages. This technique significantly reduces the number of retransmission in a flooding or broadcast procedure.

The idea behind MPRs is to minimize the flooding of broadcast packets in the network by reducing duplicate retransmissions in the same region. Each node in the network selects a set of nodes in its neighborhood, which retransmits its packets. This set of selected neighbor nodes is called the MPRs of that node. The neighbors of the node "i", when receiving broadcast messages from this node, they process them but they never retransmit them. Each node in the network maintains a set called MPR Selectors, which lists the neighbor nodes that have selected it as MPR. This allows a node in the network to know if it is MPR or not of a neighbor, which allows it to know either it retransmits or not broadcast messages received from this neighbor. This MPR Selectors set is changed periodically by the mean of the Hello messages, in which a node indicates its MPRs.

A node selects its MPR set among its one-hop neighbors. This set is selected in the manner

that, when flooding a message through the nodes in this MPR set, all two-hops neighbors receive this message in an optimal manner. i.e., the MPR set must satisfy the following conditions: (1) every node in the two hop neighborhood must have a bidirectional link toward this MPR set. (2) The MPR set should be as smaller as possible. Figure 3.5 shows the MPR nodes selection for node "i".

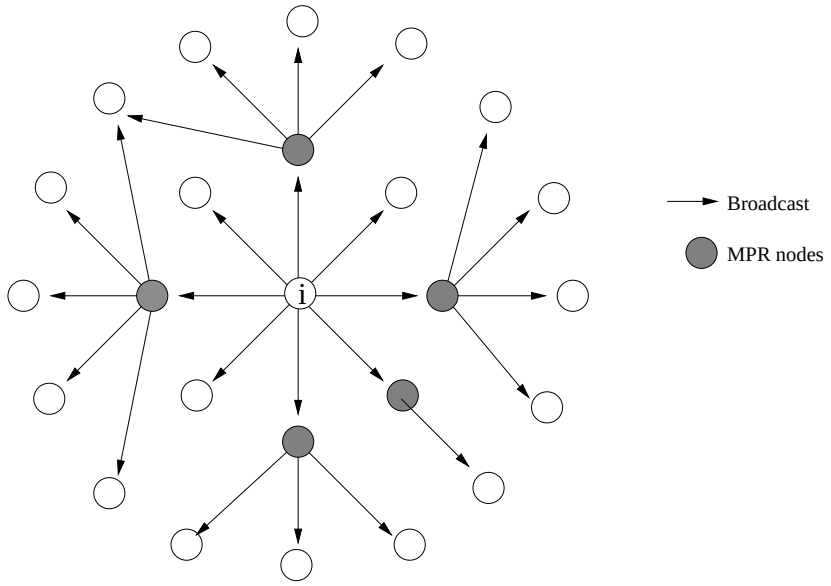

Figure 3.5: MPR nodes selection by node “i”.

In OLSR, each node in the network periodically broadcast a Topology Control message (TC-message). This message contains the information about one-hop neighbors which have been selected by the sender as a MPR. Upon receipt of this MPR Selectors' information through the TC-messages, each node gets a global view on the topology network, and thus calculates a route to each known destination. Therefore, the route is a sequence of hops through the MPR nodes from a source to a destination.

The OLSR functionality are resumed in the following four points:

- *Neighbors discovery:* each node in the network periodically broadcasts a hello message containing the information about its neighbors and their link status. The link status can be “Bi-directional”, “Uni-directional”, or “MPR”. The Hello messages are received by all one-hop neighbors since they are transmitted in a broadcast mode. These Hello messages allow each node in the network to learn the knowledge of its neighbors up to two hops. The information in received Hello messages are saved in a neighbor table, which is necessary to perform the selection of the MPR nodes. A node should indicate in its hello messages its MPR neighbors by setting their link status to “MPR”. This allows each node in the network, when receiving a Hello message from a node “i”, to know whether this node has selected it as MPR or not. Each node in the network lists all neighbors that selected it as MPR in its MPR Selector set.

A node considers the link status to a neighbor node as bi-directional if its address is announced in the hello messages coming from this neighbor.

- *MPR nodes selection:* based on the information available in the neighbor table, a node selects its MPRs among the one-hop neighbors. A neighbor can not be selected as MPR if its status is not seen as bi-directional. The one-hop neighbor nodes selected as MPR by a node "i" should satisfy the fact that, the union of the on-hop neighbor sets of these selected nodes must include all the two-hop neighbors of the node "i". And also, an MPR set must be reduced as much as possible.
- *MPR nodes information declaration:* each node in the network should periodically declare its MPR information to the whole network. To accomplish this, each node periodically initiates a TC-message and floods it in the network through its MPRs. This TC-message contains information on the one hop-neighbors that are seen as MPR Selectors.
- *Routing table construction:* by periodically receiving TC-messages from all nodes in the network, each node is able to get a global view on the whole network topology. From this global view, each node is able to build a local routing table in which a route is available to each known destination.

The availability of a route to any destination in the network at anytime, reduces much considerably the delay in the route setup process. But, this costs much in terms of routing overhead [18], caused by the important quantity of control messages sent in the air to build and maintain routing tables at each node in the network. Which makes routing protocols acting in a proactive manner suffer from dens and large network.

3.3.1.1.3 Hybrid approach Some unicast topology-based routing protocols use a mixture of the two techniques previously described (reactive and proactive techniques), i.e., they keep routes available for some destinations (up to m hops) all the time, and discover routes for other destinations only when required. This is called a hybrid mode. The Zone Routing Protocol (ZRP) [19, 20] is a well routing protocol example which acts in a hybrid manner. In ZRP, each node uses a proactive approach within a limited zone in the m-hops neighborhood, and uses a reactive approach to reach nodes beyond this zone. Figure 3.6 shows an example of a networks where ZRP is used, with m set to 2 (i.e., each node uses a proactive scheme with neighbors up to 2 hops, and a reactive scheme with farther nodes). Within ZRP, when a source node (node "S" in our example) has a data packet to send to a destination node (node "D" in our example), it checks whether the destination node is within its proactive zone or not (i.e., in its 2-hops neighbors set). If the destination belongs to its proactive zone, it delivers the packet directly. Otherwise, it sends a unicast route request to each of its peripheral nodes (second hop neighbors). In our example, the route request reaches the destination through nodes: "1" and "2". When receiving a route request, a peripheral node (node 2) replays to the source node if the requested destination belongs to its proactive zone, otherwise it forwards the request to its peripheral nodes, and so on until the destination is found.

A hybrid routing protocol, such as ZRP, combines the best features of both proactive and reactive approaches. Thus reduces the routing control overhead caused by the flooding of the control messages in the whole network in basic reactive routing schemes and the periodic

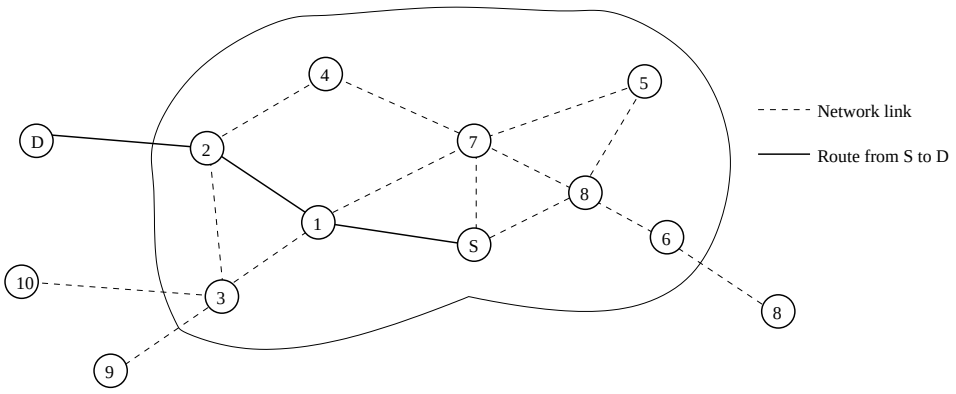

Figure 3.6: ZRP process example.

flooding of control messages in proactive routing schemes. But, due to a large overlapping of nodes' proactive zone, hybrid approaches tend to produce higher control overhead.

3.3.1.2 Position-based routing protocols

To reduce the routing overhead and/or to decrease the routing delay, some routing protocols propose to use the geographical information of nodes, or even of the network environment. The geographical information may be the physical location of the nodes involved in the network, which can be calculated in relation with some reference point or by using a dedicated location system such as GPS. In such routing schemes, in most cases there is no need for maintaining any routing table. When needed, based on position information the next forwarder is selected among neighbors to forward a data packet toward the destination. This kind of routing protocols is explained in more details in the next section and is the most interesting for VANETs.

3.4 Data Routing Protocols for VANETs

In the previous section we have presented in a brief manner the data routing process in MANETs, with listing and describing some unicast topology-based routing protocols that are proposed for such networks. These topology-based routing protocols, works well in MANETs' characteristics, even they still show some scalability and security weakness. They show more weakness when the network topology changes very fast and very often, because that the nodes are vehicle such as in vehicular ad hoc networks.

Topology-based routing protocols consist on maintaining at each node a local routing table, which is updated only when needed in the reactive mode and periodically in proactive mode. This scheme can not face the fast and the frequent topology changes [21]. In proactive mode, when the topology changes very fast, the routing tables lifetime becomes very short. Thus, each node has to flood the network with its information more frequently, which reduces the network performances from all points of view. In reactive mode, when the topology changes very fast and very often, the found routes like to be not available anymore in a very short time, which makes involved nodes restart looking for a new route very frequently, which again reduces the network performances.

In [22] authors did intensive simulations to test unicast topology-based routing protocols in vehicular network environements. They used a city mobility model like scenario in their simulations. And their studies resulted in the fact that some of the unicast topology-based routing protocols are totally unsuitable for vehicular networks, and some other are promising. In [21] authors have done other simulation-based studies to evaluate and compare the performances of position-based and topology-based routing protocols in highway like scenarios. Their studies' results show clearly that position-based routing protocol are largely more suitable for such scenarios than topology-based routing protocols.

So, in what follows we list some routing schemes that have a good potential to support the vehicular networking characteristics.

3.4.1 Routing Protocol Candidates for VANETs

In contrast to topology-based, position-based routing protocols do not need to establish or to maintain any route from a source to a destination. In position based routing protocols, each intermediate node takes the decision to which neighbor the data packet should be forwarded, based on its own physical position, its neighbors positions, and the packet's destination position information which should be included in the packet by the sender node. Thus, position routing eliminate some of the limitations in topology-based routing schemes.

In position-based routing protocols, each node is supposed to be able to get its own physical position at anytime, which is possible by using some localization system such as GPS [5, 6, 7] or Galileo [8], or any other type of positioning system [23]. The sender node should be able to get the physical position of all its one-hop neighbors, and of the destination node as well. The position information of the neighbors is learned through periodic one-hop broadcasts (beaconing). These periodic beacons contain the position of the sender. The position information of the destination node is learned through a location service. Thus, a position-based routing protocol is mainly composed by two blocks: Location Service block and Packet Forwarding block. Different location services and different forwarding systems exist, and main of them are briefly introduced in what follows.

3.4.1.1 Location Services

In position-based routing protocols, when a node wants to reach a destination in the network, it needs to know its physical position. Finding the position of the destination is the task of the *Location Service*. In centralized networks, such as cellular networks, the base station, or any other central entity, is responsible on this location service since it has the knowledge on the location of all nodes in the network. Using the same concept in ad hoc networks is not easy to achieve or even impossible because all nodes in the network should first be able to localize this location server entity. Ad hoc networks are dynamic and the localization of the location server node is not easy to achieve. Thus, the location service in such networks should be as decentralized as possible.

Any location service may fails to localize a desired destination node in one of the following cases:

- *Network partitioning:* the desired destination node may be located in a different network partition than the source node. In this situation the location service will fails to provide the localization of the desired node.

- *Inactive Node:* a node which is inactive, can not be localized by the location service.
- *Large Distance:* when the distance between the source and the destination nodes in terms of hops is greater than the the maximum Time to Live (TTL) of the location service, the localization of the destination will fails.

In the following we list the main decentralized location services.

Distance Routing Effect Algorithm for Mobility: Within the location service part in the Distance Routing Effect Algorithm for Mobility (DREAM) [24], each node in the network maintains a location table which contains the position information of all other nodes involved in the network. To achieve that, each node regularly floods the network with information to update its position information maintained by other nodes. A node controls the accuracy of its position information at other nodes by two means:

- by the frequency with which it sends its position information updates, which is relative to the node movement speed (i.e., higher is the speed, higher is the updates frequency).
- by indicating how far a position update my travel in the network before it is discarded.

Reactive Location Service: As in DREAM, the Reactive Location Service (RLS) [25] floods the network but only when needed (i.e., when a location of some node is needed). RLS is only active if a node "S" needs to discover the location of another node "D". The request is flooded to all nodes in the network by "S". Upon receiving the request, "D" initiates an answer and sends it back to "S".

In more details, when a source node "S" wants to know the location of a destination node "D", it initiates a request packet. This request packet contains the source node's ID and its location. To avoid infinite packet looping and duplication during its flooding, the request packet is marked with a sequence number which is set up by the source node. When receiving a request packet, an intermediate node forwards it only if it was not already processed, which is known by comparing the sequence number in the request packet with the sequence number in the cache. Once receiving the request, the destination replays by sending a replay packet. The replay packet contains the ID of the source node and its location (got from the request packet), and the location of the destination. The replay packet is send back to the source node by mean of the underlying routing protocol (e.g., Greedy unicast routing).

This location scheme reduce the control overhead by the cost of increasing the latency in finding the desired location.

Homezone Location Service: In contrast to both DREAM and RLS, Homezone location service [26] does not flood the whole network. In Homezone, to each node "S" in the network it is assigned an area via a hash function. This area is called the Homezone of "S". Each node sends its position updates to all nodes in its homezone. To know the location of a node "S", first the hash function is used to know the Homezone of this node "S", then a request is sent to this Homezone to get an answer from one of the nodes in this area. This approach has a major disadvantage in the fact that a node, because its unlimited movement, may be far away from its Homezone which results in long travel distance in position updates. This can lead to high network load and latency.

Grid Location Service: The Grid Location Service (GLS) [27] is a location service built upon a number of location servers distributed throughout the network. Initially, the area covered by the network is arranged into a hierarchy of grids with squares of increasing size as shown in Figure 3.7. The smallest square is called an order-1 square. Four order-1 squares make up an order-2 square, four order-2 squares make up an order-3 square, and so on.

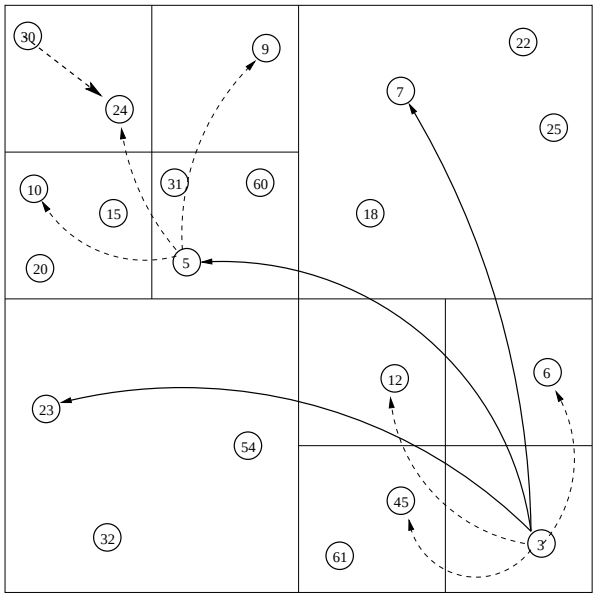

Figure 3.7: Grid Location Service example.

A node chooses its location servers by selecting a set of nodes with the least ID greater than its own ID. Each node maintains a local table which contains the information about all other nodes within the local first-order square. This table is built based on periodic position information broadcasts which are scoped to the area of the first-order square. In Figure 3.7 for example, when the node "3" wants to declare its position, it sends its position updates to all nodes located in the same square as itself, and to nodes with the nearest ID in each of the three surrounding first-order squares, and in the three surrounding second-order squares. Thus, these position information are available at the nodes 6, 12, and 45 in the first-order squares and at the nodes 5, 7, and 23 in the second-order squares. The same is done with all higher-order squares until covering all the network. Thus, the overhead cosed by a position declaration for a given node decreases logarithmically with the distance from that node.

To explain how a node can localize another node in the network with GLS, let us consider the same example shown in figure 3.7. We assume that node "30" wants to know the position of the node "3". The node "5" is the nearest node to "30" which knows the location of the node "3", but the node "30" does not know that. Thus, the node "30" asks directly to the node located in the same square and which has the ID the nearest to destination ID which is the node "24" in our example. The node "24" dos not know the location of the node "3", thus it asks to the three nodes in the three surrounding first-square that have the IDs the closest to "3", respectively nodes "5", "9", and "10". The same process is repeated until a node who knows the location of the destination is found. In our example, the node "5" knows the location of "3" and can replay to the node "30".

Hierarchical location service The Hierarchical Location Service (HLS) [28] partitions the area containing the ad-hoc network into cells as shown in Figure 3.8. This partitioning must be known to all participating nodes. The shape and size of the cells can be chosen arbitrarily according to the properties of the network. The only prerequisite is that a node in a given lowest-level cell must be able to send packets to all other nodes in the same cell. The cells are grouped hierarchically into regions of different levels. A number of cells forms a region of level one, a number of level-one regions forms a level two region and so on.

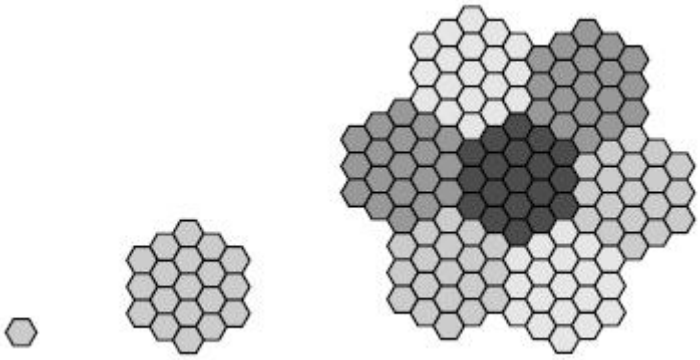

Figure 3.8: Cell and region levels organization in HLS.

HLS places location information for a node "S" in a set of Responsible Cells (RCells). "S" updates a RCell by sending position updates to an arbitrary selected node within or close to this cell. This selected node becomes a location server for "S". Each node in the network selects one RCell in each level in the hierarchy by using some hash function. A location server node, when leaving a RCell, should transfer the information it maintains to the cell it just left. This information are treated like an update: the handover packet is forwarded to a node in or close to this cell which becomes the new location server.

To localize a target node "D" in the network, "S" computes the cell which "D" would choose as responsible cell when belonging in the same level-one region, then it sends a request to this cell. When the request packet arrives at the first node "A" within the boundaries of the candidate cell, it broadcasts the request to all nodes in the candidate cell. Once receiving the request, if some node in this cell knows the location of "D" it answers to "S" through "A". Otherwise, "A" forwards the request to a corresponding cell on the next level, and so on until the request gets an answer.

3.4.1.2 Forwarding Strategies

The progress notion is used in several position-based methods. To explain this notion let us consider the example in Figure 3.9. We assume that "S" has some data to send to "D". For "S", the progress of a neighbor node "A" is defined as the projection onto the line connecting itself and the final destination "D". If the neighbor is in the direction of the forwarding through the destination, then its progress is positive, otherwise its progress is negative. In Figure 3.9, the node "A" has a positive progress and the node "B" has a negative progress.

When an intermediate node receives some data to be forwarded to a destination node, it selects a next forwarder among its neighbors. Various methods have been proposed for selecting this next forwarder [29]. Only the most important are listed in follow.

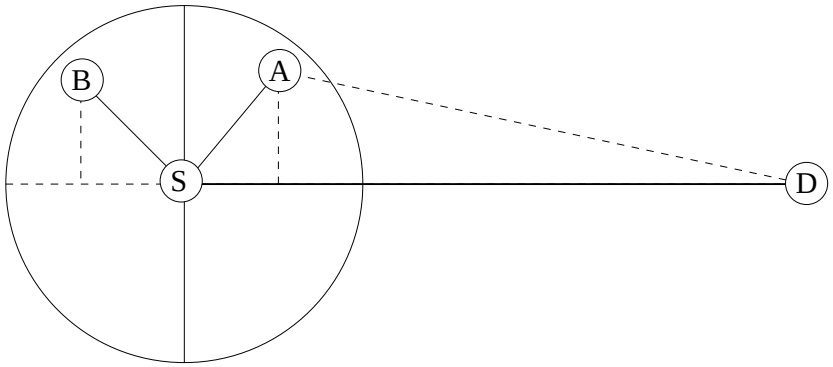

Figure 3.9: Positive and negative progress in position-based forwarding.

Random Progress Method The Random Progress Method (RPM) [30] proposes that a node selects in a random manner the next forwarder among its neighbor nodes that have a positive progress.

Most Forward within Radius The Most Forwarder within Radius (MFR) [31] selects as next forwarder the neighbor which has the greatest progress to the destination. This reduces the route length in terms of hops number when compared to the random progress method.

Nearest Forward Progress The Nearest Forward Progress (NFP) [32] selects the nearest neighbor to the sender, and then adjust the transmission power to the distance between the two nodes (between the selected and the sender nodes)..

Greedy Scheme The Greedy scheme proposed in [33] does not select randomly the next forwarder, neither the one corresponding to the greater progress. But, it selects the closest one to the destination node. Thus, the greedy scheme cares about the distance from the next hop candidate to the destination instead of the distance from the sender to the next forwarder candidate as in other schemes.

Contention-based Forwarding In a position-based forwarding system, a node has to select the next forwarder among its neighbors based on their position information. Thus, in such a system, each node has to know the position of all its neighbors. This can be achieved based on some beaconing system, which may not provide accurate information of the neighbor's positions, and may result in large overhead in highly dynamic networks. To cover this problem, authors in [34] propose a Contention-based Forwarding (CBF). CBF is a greedy forwarding scheme which does not use position beacons to determine next-forwarder node. In CBF, the forwarding node transmits a packet including the destination location as a single-hop broadcast to all neighbors, and then these neighbors contend to forward the packet. Each neighbor set up a timer based on how much progress to the destination the neighbor offers. The timer for the node with the greater progress to the destination will expire the first and that node will forward the packet first. When hearing the first forwarding, all other neighbors will suppress their packet. Simulation results in [34] show that CBF increases packet delivery ratio compared to beacon-based forwarding.

3.4.1.3 Greedy Perimeter Stateless Routing Protocol

The Greedy Perimeter Stateless Routing (GPSR) protocol [35] is a well known position based routing protocol. GPSR uses the Greedy scheme to forward packets to nodes that are always progressively the closest to the destination.

In GPSR, a data packet is marked by its originator (source node) with its destinations' locations. Thus, when receiving a data packet, an intermediate node is able to get the destination' location. Let us consider the example shown in Figure 3.10. If the intermediate node "S" knows its neighbors' locations, it calculates the distance from each one of them to the destination "D", and then it selects as next forwarder the neighbor corresponding to the shortest distance. In our example the neighbor node "2" is selected by the node "S" as next forwarder for the data destined to the destination node "D".

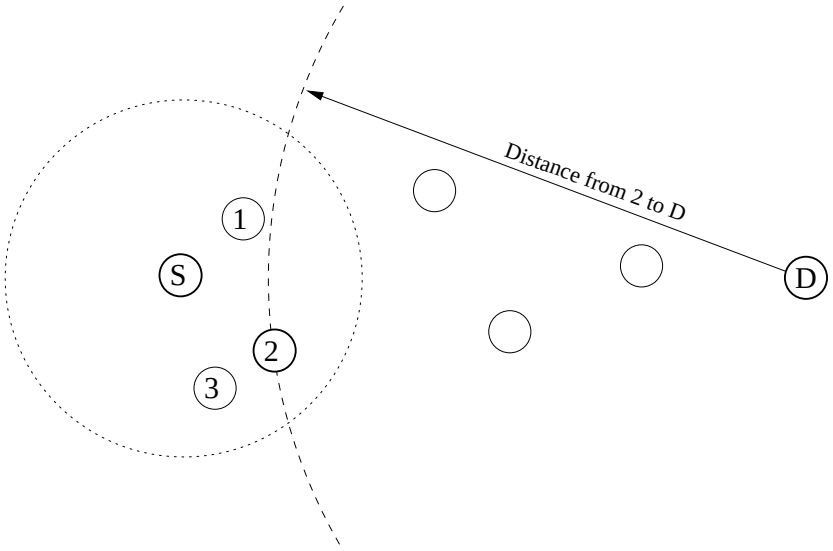

Figure 3.10: Greedy forwarding example.

It happens that no neighbor node with a positive progress to the destination is found. In such a situation the greedy forwarding fails. When such a situation happens, GPSR recovers by forwarding packets in perimeter mode, in which a packet traverses successively closer faces of a planar sub-graph of the full radio network connectivity graph, until reaching a node closer to the destination. Figure 3.11 shows an example to explain this situation.

The nodes "S" does not have any neighbor with positive progress with respect to "D" (i.e., there is no neighbor in the green region "Void"). In this situation, GPSR proposes to forward the packet to the destination "D" beyond the green region. Intuitively, "S" seeks to route around the green region (through the neighbor node "1" in our example); if a route to "D" exists from "S", it does not include nodes located within the green region.

3.4.1.4 Spatially-Aware Routing

Position-based routing protocols work well in dens networks but poorly when there are frequent topology holes due to obstacles like buildings in city scenarios. This may causes routing loops and wrong direction routing. GPSR covers such situations by forwarding in perimeter mode

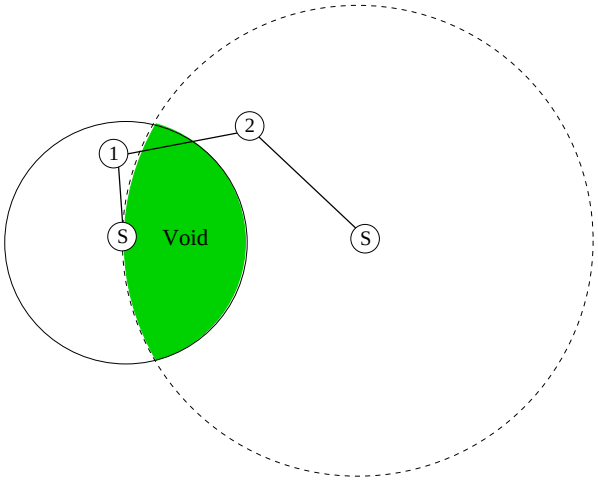

Figure 3.11: S's void with respect to D.

as said previously, but when topology holes are very frequent as in city-like scenarios, even by using a perimeter forwarding the routing protocol may suffer. To recover from such situations, the Spatially-Aware Routing (SAR) [36] proposes to combine position-based routing with topological knowledge.

SAR [36] is supported by the knowledge of the spacial environment where nodes are located. This technique makes the routing more correlated to the topological structure of the streets. The relevant spacial information have to be extracted from available geographic information systems, such as digital maps used in vehicle navigation systems.

Figure 3.12 motivates the importance of considering the spacial topological knowledge within position-based routing. It shows that by applying basic position-based routing schemes, when node "S" wants to send some packet to the destination node "D", the neighbor "1" will be selected as next forwarder, which is not the best selection because as you can see from the figure, the route through the node "1" is not connected to the destination node "D". Indeed, the best choice as next forwarder in such situation is the node "2", even it is not the closest to the destination. This choice could be possible if the node "S" has a knowledge on the surrounding environment.

Within SAR, a node "S" that has a packet to deliver to a destination node "D", computes the optimal path to the destination by using the underlying map of the city. The path here corresponds to a sequence of junctions in the city that the packet has to traverse in order to reach the destination node "D". The packet is then forwarded based on greedy forwarding until the first junction in the path, and when it reaches the first junction, it will be forwarded to the next junction, and so on until it reaches the destination.

However, there is not a guarantee that a forwarding node can always find a suitable neighbor on the desired path (junctions). To cover from such a situation, authors suggest in [36] one of the following alternative methods:

- *Suspend the packet:* the forwarder node can suspend the forwarding process and keep the packet in a specific buffer. The packet then can be forwarded when possible. The packet is drooped if the buffer is full, or after a certain delay.
- *Switch to basic greedy forwarding:* the forwarder node can decide to switch to a basic

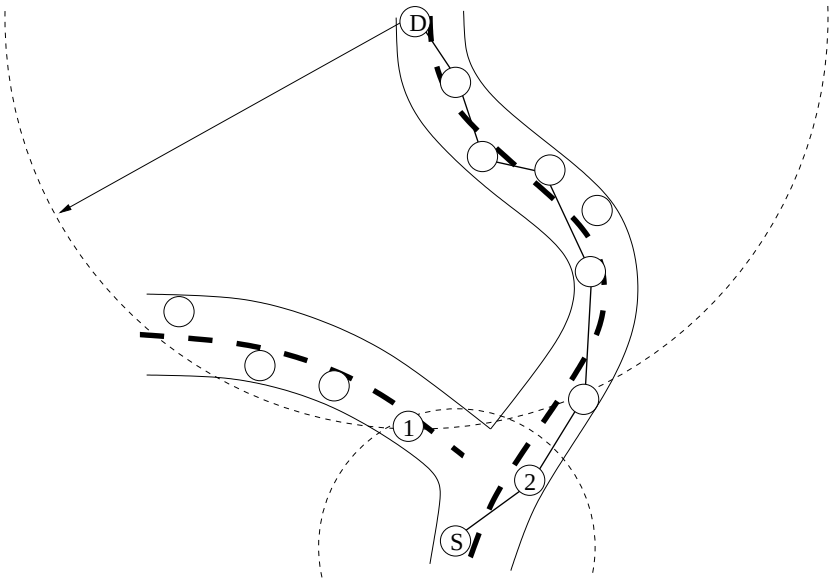

Figure 3.12: Spacial aware routing motivation.

greedy forwarding without caring about the spacial environment awareness.

- *Recompute the path (junctions):* the forwarder can as well recompute the path to the destination. It may find an alternative path along which the packet will be forwarded.

Comparison studies in [36] show that SAR handles topology hols better than generic greedy forwarding schemes.

3.4.1.5 Geographic Source Routing

The Geographic Source Routing (GSR) [37] is as well supported by a map of the city. It is similar to the Spatially-Aware Routing previously described. As SAR, GSR computes the best path (junctions) to the destination based on the map, and then selects the next forwarder based on this information. In such a routing scheme, intermediate nodes should be aware about the junctions that packets have to travel. To achieve that, GSR proposes two solutions, (1) the source node puts the set of all junctions to be traversed in the header of the packet (solution used in SAR), (2) or leave each intermediate node calculates the optimal path to the destination (set of junctions).

Simulation results in [37] show again that combining position-based and topological knowledge help in handling topology holes. Such routing scheme seems to have a good potential in vehicular networks.

3.4.1.6 Hybrid Approach

A combination of topology-based and position-based schemes is used in the Terminodes routing protocol [38]. Terminodes protocol combines two protocols, Terminodes Local Routing (TLR) and Terminodes Remote Routing (TRR). TLR is used to reach destinations located in the local area of the source node, and TRR is used to reach farther destinations, i.e. those located

outside the local area. Each node in the network has a local area, which is the set of its neighbors up to m hops.

Terminodes is inspired from the hybrid protocol ZRP [19, 20], which combines a reactive and a proactive approaches. In Terminodes, a node maintains routes to all neighbors in its local area in a proactive manner, by mean of periodic hello message exchanges. When a source node wants to reach a destination node "D", it checks whether "D" is in its local area or not. If "D" belongs in its local area, "S" delivers directly the packet to "D" using a simple distance vector routing protocol. Otherwise, if "D" is at a distance from the sender greater than m hops, the packet is sent to "D" by mean of greedy forwarding like in GPSR [35].

Authors in [38] show by means of simulations that such a combination of topology-based proactive scheme with position-based scheme improves the routing performances in terms of packet delivery ratio and routing overhead when compared to basic schemes. We believe that such schemes have also a good potential in vehicular networks.

3.4.2 Qualitative Comparison of VANET routing protocols

In vehicular ad hoc networks the topology changes very frequently and very fast, which poses new challenges for network protocols design. In this chapter we have investigated the data routing process, in basic context, and as well in vehicular ad hoc networks. We have distinguished mainly tow categories of routing protocols: topology-based and position-based routing protocols. Various studies [21] showed that topology-based are not suitable for vehicular communications comparing to position-based routing protocols. Even though, simulation results in [22] show that some topology-based routing protocols, such as AODV, are promising in city-like scenarios. However in [22], the authors did not compare with any position-based routing protocol.

In [21], based on extensive simulation studies based on realistic vehicular movement patterns, authors compares topology-based to position-based scheme. As representatives they chosen DSR as topology-based routing protocol, and GPSR as position-based routing protocol. Figure 3.13 (taken from [21]) shows their simulation results in terms of packet delivery ratio with changing the distance between the source and the destination. And we see clearly the weakness of DSR in terms of packet delivery ratio when compared to GPS. Thus, it seems that topology-based routing schemes are unsuitable for vehicular ad-hoc networks in highway environments.

Position-based routing protocols, such as GPSR, that seems the most promising for vehicular ad hoc networks, works well in dense networks and in obstacles-free environment but poorly when there are frequent topology holes due to building and road structures. Generic greedy forwarding used in GPSR fails when there is no next hop candidate with a positive progress to the destination. As recovery system in such a situation, GPSR uses a perimeter forwarding to go around the topology holes. Such a system works well, but when the topology holes are frequent or permanent, like buildings in a city scenario, such a recovery system may suffer since each packet when meeting a topology hole has to be perimetery forwarded. Using the surrounding spatial environment may help position-based routing protocols in recovering such situations, mainly in city scenarios. In [36, 37], authors propose to use a spacial model to predict and avoid forwarding failures due to permanent topology holes. The spacial model can be overlayed from a map (e.g. from the map used by the vehicle navigation system). Simulation results of both proposals show interesting and promising results, where the network performance is clearly improved in terms of packet delivery ratio and routing control overhead.

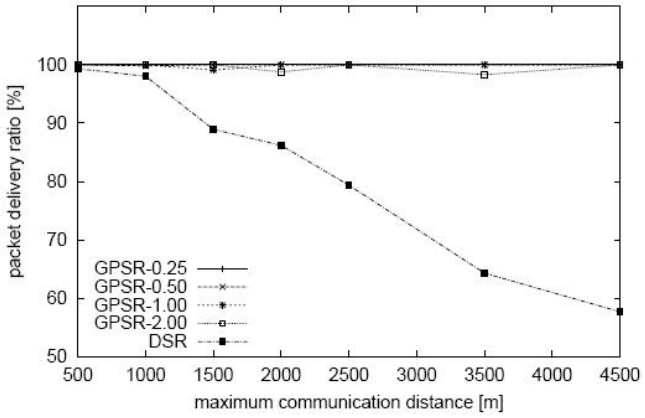

Figure 3.13: Packet delivery ratio of DSR vs. GPSR in highway environment.

Another approach that seems promising for vehicular ad hoc networks, is the combination of topology-based and position-based approaches as proposed in [38]. Topology-based routing schemes have the main problem of scalability in contrast to position-based routing schemes. Thus, it should be a good idea to use topology-based scheme just with nearest nodes (in terms of number of hops), and position-based with farther nodes. When topology-based fails, position-based can be used, and where position-based fails topology-based can be used.

3.5 Chapter Summary

In this chapter we have briefly reviewed routing protocols in generic mobile ad hoc networks, and listed and described main promising approaches for vehicular ad hoc networks. When reading this chapter, you feel the strangeness of position-based routing in the vehicular environment. Most researchers working on this topic believe on the fact that position information should be considered when designing routing protocols for vehicular networks.

Some people propose various position-based solutions with using different forwarding schemes and/or different location services. Some others [38], believe that combining topology-based with position-based approaches helps in improving the routing process, and some others [36] believe even on supporting the routing by the map of the city in order to make routing routes follow the topological paths (streets for example) in the city. Even if all those solutions show premising results by mean of simulations, we believe that still improvements are needed.

One criteria which is not taken into account in proposed solutions is the movement information of the vehicles, knowing that the movement pattern of nodes is the main difference when compared VANETs to MANETs. It is proved that considering the position of vehicles and the map of the city helps and improves the routing in vehicular networks, but what about considering the movement information (position, speed, and direction) of vehicles? We believe that they really should be taken into account as well. Thus, we propose in Chapter 5 a movement prediction concept, which aims to improve routing protocols in vehicular networks. This concept can be applied to any routing protocol to face the high-speed movement environments such as in VANETs. In Chapter 5 we give more details on this movement prediction-based concept, which we call MOPR (MOvement PRediction). And in Chapter 6, we describe how

MOPR is applied to topology-based and position-based routing protocols.

Chapter 4

Medium Access Control in Vehicular Ad hoc Networks

4.1 Introduction

In telecommunication and computer networking, a Medium Access Control (MAC), known as Media Access Control as well, allows several nodes to connect to the same physical channel to transmit over it and to share its capacity.

In wireless networks, the wireless channel is considered as a common medium, and nodes located in the same communication range should share it. Only one node is allowed to transmit over this common medium at the same time. Therefore, some specific entity in the network should be in charge of controlling the access to this medium. This entity is called a MAC protocol.

Ad hoc networks are fully distributed, which does not make easy the design of medium access mechanism. In the literature we find several MAC protocols which have been proposed for MANETs. Those protocols work fine in certain situations and certain scenarios, but they still have some weakness, specially when the nodes are highly mobile, like in VANETs.

In this chapter we briefly present main MAC protocols proposed for MANETs, and then we list some solutions that have been adapted or designed to deal with VANETs characteristics, mainly the high mobility of nodes.

The remainder of this chapter is organized as follows. In Section 4.2, we enumerate and discuss the main issues to be considered when designing a MAC protocol for wireless networks. In Section 4.3 we review the main MAC protocols proposed for MANETs, and in Section 4.4 we present some protocols proposed, or just adaptable, for VANETs. Finally, Section 4.5 provides a summary of this chapter.

4.2 Issues in Designing MAC Protocols

MANETs are totally distributed networks in which nodes share some common resources, such as the communication radio spectrum. A common resource to which only one node is allowed to access at the same time. This chapter covers the control access to this common resource, communication channel.

In wireless networks, two nodes near and in the communication range to each other, should

never transmit on the same radio channel at the same time, otherwise transmission collision occurs. To avoid this problem a centralized infrastructure can manage sharing this medium in efficient manner between nodes in its communication coverage. Unfortunately, in MANETs we do not have any centralized infrastructure, which makes sharing the medium more complicated to manage. It should be then solved in a totally distributed manner. Many MAC protocols have been already proposed to solve this problem in wireless networks [13]. When designing a MAC protocol for MANETs, there are important issues that have to be taken into account, knowing that some of these issues are more or less important when considering or not Vehicular Ad hoc Networks (VANETs) [3] and their specific characteristics (see Section 2.2).

In the next subsections the most important issues to be taken into account when designing a MAC protocol for mobile ad hoc networks are listed and discussed.

4.2.1 Bandwidth Efficiency

The radio spectrum is considered as a limited resource which concludes to a limited bandwidth. This bandwidth should be used in a efficient way by decreasing the control overhead, knowing that the bandwidth efficiency can be defined as the ratio of the bandwidth used for data transmission to the total available bandwidth. In VANETs we may have more control overhead caused by the frequent and the fast changes in the topology network due to the high mobility of vehicles.

4.2.2 Quality of Services Support

Many applications, such as video and voice communication, need for their well functionality some Quality of Service (QoS) to be guaranteed by the network. One good way to provide a good QoS consists in the bandwidth reservation, which is difficult to manage in MANETs because of that nodes in such kind of networks are almost mobile. In VANETs, providing a certain QoS may be more difficult and complex to manage when compared to such environment as in MANETs, and that because the relatively higher mobility of vehicles. Thus, the bandwidth reservation is not so easy to manage in VANETs.

4.2.3 Synchronization

Synchronization time between nodes in a wireless network is very important. In a centralized network, providing a synchronization time is easy to manage since the network has a common clock, the clock of the centralized infrastructure. This is not so easy in MANETs, that are totally distributed. Thus, synchronization should be provided in distributed way in MANETs, as in VANETs. Even in VANETs this is less difficult to manage since vehicles should be equipped with positioning systems, such as GPS, which is already able to provide a common clock in the network.

4.2.4 Hidden and Exposed Terminal Problems

The hidden terminal problem is easy to understand but not so easy to resolve. Figure 4.1-a shows three wireless nodes: "A", "B", and "C". "A" and "C" can not communicate directly via their physical layer because they are not in the communication range each one to other. But, both of them can communicate with "B" which is in their communication range at the same time. Now, suppose "A" is transmitting data to "B". Since "C" can not hear this

transmission, it can transmit at any time which can cause a transmission collision on "B" with the ongoing transmission from "A". This is what we name the hidden terminal problem, where "A" and "C" are each one hidden to the other.

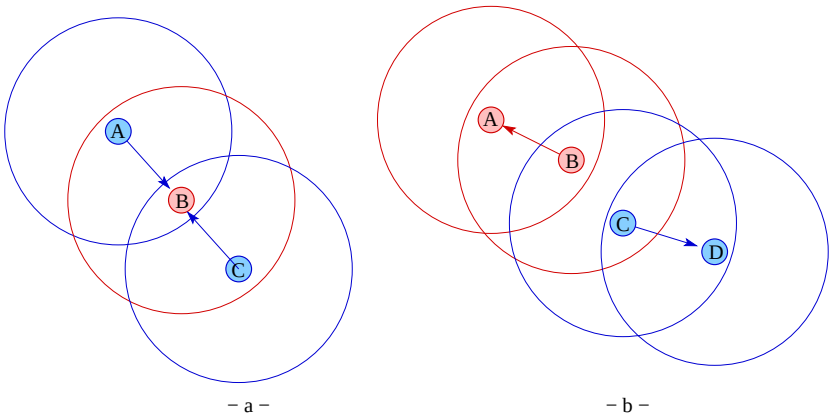

Figure 4.1: The hidden and the exposed terminals problem

The exposed terminal problem is similar to the hidden terminal problem in the sense that the problem is caused by the limitation of the communication coverage range and the common medium. Figure 4.1-b, which explains this problem, shows four wireless nodes: "A", "B", "C" and "D". When "B" is transmitting data to "A", "C" is prevented from transmitting to "D" as it believes that it will interfere with the ongoing transmission from "B" to "A". In the reality, "C" can transmit to "D" without any risk of interfering with the ongoing transmission between "B" and "A". "C" is the exposed node.

4.2.5 Error-Prone Shared Broadcast Channel

Because of the transmission radio nature, when a source node is receiving a transmission from a sender node, no other node in its neighborhood should transmit, otherwise a transmission interference can occur. That because, when a node in transmitting all nodes in its neighborhood hear this transmission. Since it often happens that nodes in the same neighborhood attempts to access to the medium at the same time, transmission collision probability is quite high in MANETs, as in VANETs. So, the role of a MAC protocol is as well reducing as much as possible these communication collisions.

4.2.6 Distributed Nature and no Central Coordination

On of the main characteristics of MANETs and VANETs is the lack of any centralized infrastructure and/or any centralized coordination. In such kind of networks, nodes should interact in a purely distributed way. Thus, the MAC protocol should carry out a good control of the channel access, based on some control packet exchanges that, again, may decrease the bandwidth.

4.2.7 Mobility of Nodes

If nodes were not mobile in MANETs, scheduling the channel access would be done in a static manner where the medium is allocated to communicating nodes in advance. Of course this

is not the case in MANETs where nodes are mobile almost of the time, and in VANETs this mobility is relatively higher and should be more seriously taken into account when designing MAC protocols.

4.3 MAC Protocols for MANETs

Thousands of works have been done around the medium access control in ad hoc networks, and many solutions have been proposed for this purpose. But, unfortunately still no solution is able to offer a perfect reliability.

4.3.1 Medium sharing methods

There are three main basic medium access methods:

- **Time Division Multiple Access (TDMA):** to allow several nodes to share the same frequency channel (medium), TDMA divides the medium into different time slots. Nodes use the medium one after one, by using a specific allocated slot in a repeated time frame. This technique allows several nodes to transmit on the same medium without transmission collisions.
- **Frequency Division Multiple Access (FDMA):** this is another way to allow different nodes to transmit on the same medium. It consists to divide the medium into different radio frequencies and make each node use an associate frequency. This is another technique to allow to have many transmissions at the same time without collisions.
- **Code Division Multiple Access (CDMA):** this is a form of multiplexing allowing multiple nodes to access the medium. It divides up a radio channel not by time as in TDMA, nor by frequency as FDMA, but instead by using different pseudo-random code sequences for each mobile.

These three different manners to split the medium can as well be coupled and used at the same time, for example, by applying TDMA on each radio frequency in FDMA.

4.3.2 Classification of MAC protocols

The existing MAC protocols can be classified in different ways based on several criteria such as time synchronization and initiation approach. In the rest of this section we give a short overview on the main existing MAC protocols with taking care to classify most of them into these three big categories:

- **Contention-based access:** in this access mode a node when having a packet to send has to contends with nodes in its neighborhood for access to the medium. In this mode no QoS can be guaranteed since no medium reservation is possible.
- **Contention-based access with reservation:** MAC protocols classified in this mode works as in contention-based access but with resources reservation. Here a node is able to make a reservation of certain bandwidth for a certain time, which make this access mode able to provide some QoS in the network, which makes it able to support real-time applications and other QoS-based applications.

- **Contention-based access with scheduling:** In this type of protocol, the MAC process is based on packet scheduling at the nodes and scheduling of the nodes. The target in this scheduling is to provide a certain ordering mechanism to guarantee some QoS differentiation or fairness. Which mean, each packet is processed following a defined order.

4.3.2.1 Contention-based Access

ALOHA [39] was the first MAC protocol proposed for packet radio networks. Its name comes from the world "Aloha" used especially in Hawaii as a greeting meaning hello and good-bay. This MAC protocol is very simple in its process, it is based on random access and process like that: when a node that has data to send, transmits them immediately, and then, if any collision occurs it retries again after a random time. The maximum throughput that this MAC protocol can reach is around 18 percent only. To improve this throughput, a slotted version of ALOHA (S-ALOHA) [39] was proposed. In this slotted version the medium is divided into several time slots. And when a node wants to access the medium it attempts to transmit at the beginning of a time slot. When compared to ALOHA, the vulnerable period of a transmission is halved in S-ALOHA, which makes the system efficiency (maximum throughput) to be doubled.

As a refinement of ALOHA, Carrier Sense Multiple Access (CSMA) [40] scheme has been proposed for wired networks. In CSMA a node senses the medium ether idle or not before transmitting. If the medium is sensed to be idle, the node can transmit, otherwise it attempts to transmit again after a random time. A collision detection was integrated to CSMA in CSMA with Collision Detection (CSMA/CD) [41]. In CSMA/CD a node is able to detect transmission collisions when they occur. Therefore, if a node detects during it transmission any collision with another transmission it stops transmitting and attempts to transmit again after a random time T. If the same transmission collides again, the sender waits twice the time T before attempting to transmit again. Even with collision detection, CSMA/CD suffers from charged networks because that the probability of the transmission collisions increases, which decreases the network performances. Another disadvantage in CSMA/CD is that collisions are detected by the sender and not by the receiver, which make it not able to solve the hidden terminal and the exposed terminal problems (see Section 4.2.4).

Multiple Access with Collision Avoidance (MACA) [42, 43] was proposed as an alternative to CSMA. It tries to overcome the hidden terminal and the exposed terminal problems based on establishing a handshake transmission between the transmitter and the receiver. In MACA, when a transmitter has a data packet to send, it asks the receiver if it is free to receive its transmission by sending a Request-to-Send (RTS) packet. When the receiver gets the RTS packet, if it is free to receive the corresponding transmission, it replies to the transmitter by sending back a Clear-to-Send (CTS) packet. Once the transmitter receives this CTS packet, it can start the transmission of its data packet without any risk of collision since all neighbors, in both its vicinity and the receiver's vicinity, are aware about the ongoing transmission through the RTS and CTS packets. The nodes in the vicinity of the transmitter, when hearing the RTS packet, do not transmit for a long enough period of time so that the sender can receive the CTS packet. The expected duration time of the data packet transmission is indicated in both CTS and RTS packets. All nodes within the vicinity of the receiver, when hearing the CTS packet, defer their transmission until the receiver receives the data packet. Based on this RTS/CTS exchange mechanism, MACA overcomes the hidden terminal problem.

In MACA the node that receives only the RTS and not the CTS should be free to transmit

even when the node from where the RTS came is transmitting. So, this node is considered as an exposed terminal (see Section 4.2.4).

MACA Wireless (MACAW) [44] has been proposed to improve the MACA performances. In addition to RTS and CTS control packets used in MACA, an acknowledgment (ACK) packet is used. In MACAW, a receiver node, when receiving the data packet, sends an ACK packet to the sender to acknowledge the well reception of the data packet. If the sender does not receive this ACK packet, it sends again the RTS packet, and when receiving this RTS packet, the receiver send back an ACK since the corresponding data packet has been already received.

To overcome the exposed terminal problem in MACA, MACAW proposes to use the additional control packet: Data-Sending (DS). The DS packet is transmitted by the sender just when receiving the CTS to make the exposed node aware about the expected duration time of the corresponding transmission. Figure 4.2 summarizes the packet exchange mechanism in MACAW, including control and data packets.

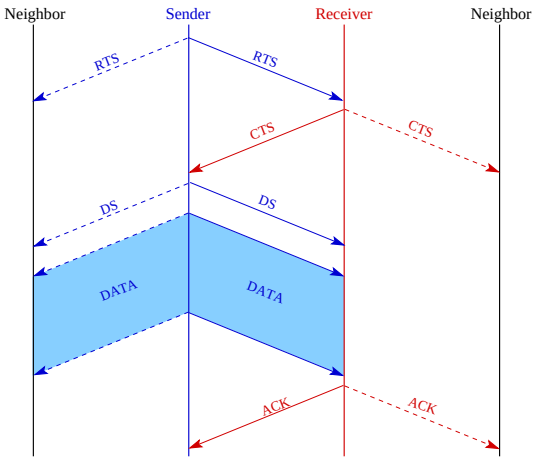

Figure 4.2: Packets exchange in MACAW

In Busy Tone Multiple Access (BTMA) MAC protocol [45] it is proposed a new way to overcome the hidden terminal problem by splitting the medium into two channels: control channel (say busy tone channel) and data channel. The first channel is used for transmitting the busy tone signal, and the second one for transmitting data packets. In BTMA, when a sender wants to transmit, it first senses the busy tone channel. If, and only if it is free, it transmits the busy tone signal on it and then starts the data transmission on the data channel. All neighbors which senses the busy tone signal, transmit it as well. Thus, all nodes in the tow-hop neighborhood of the sender are not allowed to transmit, which avoids the collisions and the hidden terminal problem. An extension of BTMA was proposed in Dual BTMA (DBTMA) [46]. DBTMA uses tow busy tones. These two busy tone channels are used to inform nodes within the neighborhood about the on going transmission. The first busy tone is used by the sender node and the second one by the receiver node.

4.3.2.2 Contention-based with reservation

In MANETs, as in VANETs, some applications like voice and video communication need some QoS to be guaranteed. As said in Section 4.3.1, MAC protocols can split the medium into different manners to make the medium seen as several physical or logical channels. Some MAC protocols allow the reservation of a channel for a dedicated transmission which makes able to provide some QoS into the network.

Five Phase Reservation Protocol (FPRP) [47] is a contention-based MAC protocol with reservation. It uses a five-phase reservation process to establish TDMA slot assignments (see Section 4.3.1). As shown in Figure 4.3, FPRP proposes to split the medium into two types of frames: Reservation Frame (RF) and Information Frame (IF). Each RF is followed by a sequence of IFs. In each IF there are N Information Slots (ISs). To each IS it corresponds a Reservation Slot (RS) in the previous RF. When a node wants to reserve an IS in the following IFs it contends in the corresponding RS. The reservation schedule generated in a RF is used in the next subsequent IFs until the next RF.

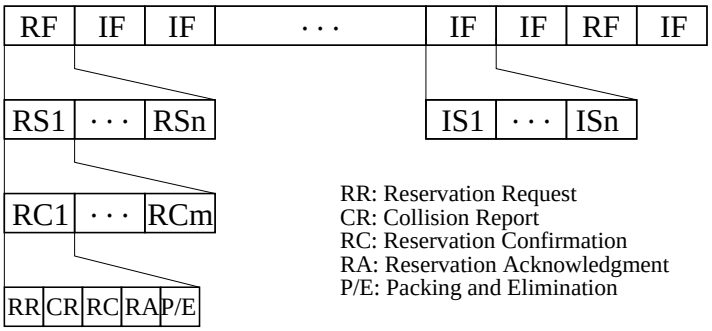

Figure 4.3: Frame structure of FPRP

Each RS is composed of M Reservation Cycles (RCs). Within each RC, one IS reservation is done through a five phase dialog between the contending node and its neighbors as in follow.

- Reservation Request (RR) phase: a node sends a RR packet when a reservation is needed.
- Collision Report (CR) phase: when a collision is detected a CR packet must be broadcast.
- Reservation Confirmation (RConf) phase: if no RConf packet has been received in the previous phase then the source node is considered to have won the contention for the corresponding SI. Thus, it sends reservation confirmation to the destination node.
- Reservation Acknowledgment (RA) phase: the destination, after receiving the RC packet, sends back to the source a Reservation Acknowledgment. All nodes in the neighborhood of the destination hear this RA which make them aware about the reservation done by the source node. By doing that, the hidden terminal problem is avoided.
- Packing and Elimination phase (P/E): In this phase, two kinds of packets are transmitted: A packing packet; which serves to make the broadcasting pattern denser in a

given slot, and an elimination packet, which is used to remove possible deadlocks (DL) between adjacent broadcast nodes (you can see [47] for more details on this phase).

FPRP is totally distributed. For a given node, the reservation process only involves nodes within two-hop neighborhood. This local reservation process makes FPRP scalable in terms of network size. FPRP is as well robust in a rapidly-changing topology since it does not need any prior information about the network.

Different contention-based MAC protocols with reservation schedule have been proposed, such as the Distributed Packet Reservation Multiple Access (D-PRMA) [48], the Soft Reservation Multiple Access with Priority Assignment (SRMA/PA) [49], and others. Most of them use the TDMA slot assignments. As in TDMA-based MAC schemes, in both CDMA-based and FDMA-based MAC schemes, the channel reservation can be provided. In CDMA-based MAC schemes, the medium is divided into several channels by using different orthogonal codes. In FDMA-based MAC schemes, by using different radio frequencies, the medium is slotted into several channels. Having several channels available in the network, make the reservation scheme possible where each node is able to reserve a specific channel for a specific period of time. Multi-Code MAC (MC MAC) [50] is a CDMA-based MAC protocol.

4.3.2.3 Contention-based with scheduling

Distributed Priority Scheduling MAC (DPS-MAC)[51] uses the distributed priority scheduling based on the basic RTS/CTS/DATA/ACK packets exchange mechanism used in the IEEE 802.11 DCF (see Section 4.4.2.1). The example in Figure 4.4 shows how this distributed scheduling mechanism works. When the source node "node 1" has data to send, it sends an RTS packets including the information of the priority index corresponding to the data packet to be sent. Once receiving this RTS packet, the destination node "node 2", if ready to receive the data packet, sends a CTS packet including the same priority index indicated in the RTS packet. All nodes in the neighborhood, including the hidden nodes, when hearing the the RTS or the CTS packets, retrieve the priority index of the data packet to be sent and create the corresponding entree in their local Scheduling Table (ST). The node 3 for example, which is a neighbor of both node 1 and the “node 2”, initially has its ST as shown in ST(a) in Figure 4.4, and when receiving the RTS sent by node 1 it adds the related entree in its ST as shown in ST(b). As shown in ST(c), another entree is add to the ST of node 3 after receiving the DATA packet sent by node 1. Finally, after receiving the ACK packet from node 1, node 3 removes the corresponding entree from its ST as shown in ST(d).

Based on this mechanism, each node in the network is able to evaluate its priority in relation with other nodes' priority.

Right now we have talked about MAC solutions proposed for MANETs, but as said in the beginning of this chapter, because of their specific characteristics (see Section 4.4.1) when compared to MANETs. These MAC solutions are not suitable as they are for VANETs. In the rest of this chapter we will not propose any MAC solution or adaptation for VANETs, but we will just select among the existing MAC solutions the ones which have a good potential to be implemented for VANETs, and the ones already proposed for such kind of networks. VANETs are still in progress and no large real implementation have been done which make the selection and the comparison of MAC protocols for these networks not so easy.

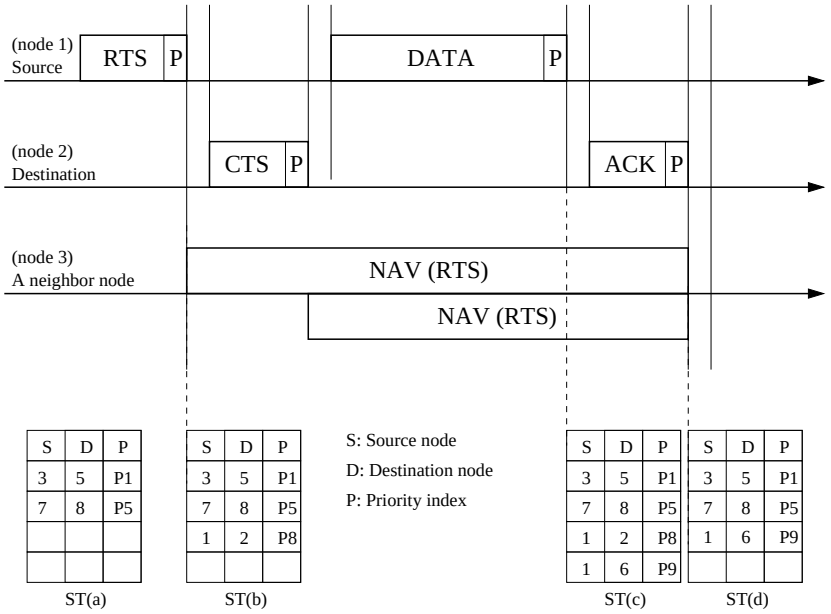

Figure 4.4: Scheduling table update in DPS-MAC.

4.4 MAC Protocols for VANETs

4.4.1 VANETs characteristics and issues for MAC protocols

Vehicular Ad hoc Networks (VANETs) [3], as well called Vehicle to Vehicle Communication (V2VC) or Inter Vehicle Communication (IVC) networks, are considered as a specific instance of MANETs, where nodes are the vehicles. Thus, one of main differences in VANETs when compared to MANETs, are defined in the characteristics of the vehicles, such as the high speed and the non limitation of energy and storage resources.

The vehicle's mobility speed, which is relatively high in VANETs, makes such kind of networks suffer on frequent and fast topology changes. This is one of the disadvantages of VANETs when compared to traditional MANETs. When talking on advantages in these networks, we have on the first plan the no limitation of energy and data resources, since vehicles are already equipped with batteries and can be equipped with power-full computers. Vehicles can be equipped with positioning systems as well, such as GPS [5, 6, 7] or Galileo [8], which allow getting own geographic positions. In contrast to nodes in MANETs, vehicles do not have a large freedom in their movement in VANETs. They move on roads following driving rules. Both roads and corresponding driving rules can be electronically represented.

All these specific characteristics make existing MAC solution already proposed for MANETs not suitable as they are for VANETs. Therefore, we do not have the same issues when designing a MAC protocol for VANETs as when designing a MAC protocol for MANETs. In Section 4.2 we presented the main issues for designing a MAC protocol for MANETs. We notice that some of these issues are less important and some other more important when considering MAC protocols for VANETs.

For both MANETs and VANETs, when designing a MAC protocol we have to think very well how to guarantee an efficiency bandwidth use, how to reduce or to avoid the hidden and the exposed terminal problems, and of course, how to make the proposed solution able to work

in a distributed way. The network synchronization is as well very important in VANETs as in MANETs, but it is more easier to guarantee in VANETs since vehicles should be equipped with a satellite positioning system, like GPS, which is able to provide a common clock in the network.

What we have to take more care about when designing a MAC protocol for VANETs are mainly the following points:

4.4.1.1 Quality of Services Support

The quality of service importance in any communication network depends directly on the application use. In VANETs, the important candidate applications would be around driver and passenger safety. Human lives depend on these safety applications, which depend on the communication network efficiency, which depends on the MAC layer. Thus, any MAC protocol proposed for VANETs should take into account the quality of services, at least for safety applications.

4.4.1.2 Mobility of Vehicles

The vehicles' mobility pattern can be the main difference when compared VANETs to MANETs. Because the high speed movement specification of vehicles, the topology network in VANETs changes frequently and rapidly. Therefore, vehicles that want to exchange some data have relatively small time to access to the channel and to establish the desired communication. Knowing that, if two vehicles move into opposite directions with a speed of 130 Km/h, the relative speed between these two vehicle becomes double, i.e. 260 Km/h. And if the radio communication range is assumed to be 250 meters for each vehicle, we conclude that these vehicles have between 3 and 4 seconds to access the channel, to establish the communication to each other, and to transfer the data.

Thus, any MAC protocol proposed for VANETs should take this into account. And should, reduce as much as possible the medium access/allocation time.

4.4.2 MAC protocol candidates for VANETs

4.4.2.1 IEEE 802.11 Standards

The wireless communication standards IEEE 802.11 [52], which was brought out in 1997, is very interesting and very famous standard in the domain of Wireless LANs (WLANs). The most famous versions of this standard are the IEEE 802.11b and the IEEE 802.11g, commercially known as WiFi (Wireless Fidelity). These two standards have got a big interest from researchers in the domain of VANETs, in both theoretical and application sides (prototypes and test beds).

The IEEE 802.11 standards work in two modes: (1) in centralized mode, where mobile terminals communicate with one or different fixed and centralized infrastructures already deployed in the network. (2) In ad hoc mode, where mobile terminals are connected each one to other without any centralized infrastructure, and in which two mobile terminals are able to communicate directly through the physical layer, when they are within the communication range to each other, or by multi-hops communication through the routing layer when they are not enough close to each other. In ad hoc mode, the network should be auto-configurable and totally distributed.

In VANETs, the IEEE 802.11 standards can be used in both modes. In centralized mode for Vehicle to Infrastructure (V2I) communications and in ad hoc mode for vehicle to vehicle (V2V) communications. Ad hoc mode can be used for V2I communications as well, when infrastructure spots, a repeater for example, play the role of an ah hoc terminal in the network.

In the OSI (Open System Interconnection) model, the IEEE 802.11 standards addresses the last two layers: data link and physical layers. The data link layer is divided into a Media Access Control (MAC) layer and a Logical Link Control (LLC) layer. In this chapter, we focus only on the MAC layer, which is almost the same used in interaction with different physical layers in all IEEE 802.11 standards.

Considering VANET environment specifications (see Section 4.4.1), the IEEE 802.11 working group is hardly working on a new standard version, named IEEE 802.11p [53]. This new standard version should deal with the VANETs characteristics. It uses a modified IEEE 802.11a with slight changes, mainly on the physical layer. It operates in the licensed 5.9 GHz band, and has almost the same MAC layer as in other standards in the family of IEEE 802.11. After having used the CSMA/CD in the IEEE 802.x wired LANs, the CSMA with Collision Avoidance (CSMA/CA) has been proposed for the WLANs (you can see Section 7.2 for more details).

4.4.2.2 AD HOC MAC

ADHOC MAC [54] was basically proposed for vehicular networks. It was proposed within the European research project CarTALK2000 which has the purpose to design novel solutions for inter-vehicle communications. ADHOC MAC has been designed to provide a reliable single and multi hop broadcast. It is totally distributed and based on dynamic TDMA mechanism that can be easily adapted to the UMTS Terrestrial Radio Access Time Division Duplex (UTRA-TDD), that has been chosen as physical target system in the CarTALK2000 project. ADHOC MAC is able to provide QoS based on time slots reservation.

To achieve the Dynamic TDMA mechanism, ADHOC MAC uses an extension of the Reservation ALOHA (R-ALOHA) [55] protocol, named Reliable R-ALOHA protocol (RR-ALOHA) [56]. R-ALOHA is capable to achieve the dynamic TDMA but in centralized networks, where a central repeater provides the status information (busy, free, or collided) of time slots. It proposes that a node which has a data packet to send contends to access a time slot by transmitting on it, and then, if the transmission is recognized as successful the slot is reserved for that node in the next subsequent frames. To apply R-ALOHA in distributed way, RR-ALOHA was proposed. RR-ALOHA makes each vehicle in the network able to reserve a slot time within two hops neighborhood, which allows it to transmit without any risk of collision and with avoiding the hidden terminal problem.

In RR-ALOHA each vehicle periodically transmits the perceived status of slots in the preceding period (frame), called Frame Information (FI). In more detail, the medium is divided into repeated successive frames, and each frame is composed by N time slots. A node that wants to transmit has to reserve a time slot that we name its Basic Chanel (BCH), that will be used for its data packet transmissions during the next subsequent of frames. The statute of a time slot (channel) is considered as busy when a transmission in this slot is recognized as successful, otherwise it is considered as free. Each vehicle in the network listens first to the FI broadcast by all active vehicles during one frame (N slots), and then marks each slots as free or busy depending to the heard transmissions during this one frame period. When a time slot is heard as busy, a vehicle puts in the corresponding slots in its FIs the ID of

the corresponding transmitter. This FIs is sent periodically every one frame period. When receiving a FI, a vehicle is able to know which time slot is reserved by which vehicle within two-hops neighborhood. When a new vehicle reaches the network, it first listens during one time frame before attempting to transmit on one free time slot. Then, if in the next frame period the same time slot is marked by its ID in the whole received FIs, it means that this time slot is considered as reserved for it by all vehicles within its two-hops neighborhood. Thus, this time slot can be considered as its BCH, and can be used for its data packet transmissions.

Figure 4.5 shows an example of FIs transmitted by vehicles in a Tow-Hop (TH) cluster, knowing that a TH-cluster is a union of One-Hop (OH) clusters having a common subset of vehicles. And a OH-cluster is a set of vehicles that are within the communication range each one to other, means, all vehicles able to communicate each to other directly at the physical layer.

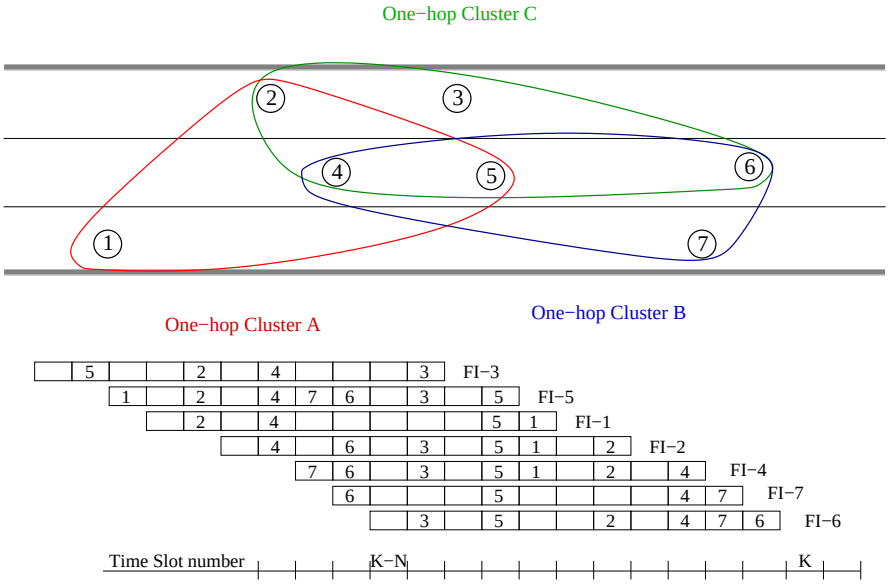

Figure 4.5: FIs propagation within TH-cluster in RR-ALOHA.

By hearing the medium, each vehicle in the network knows which time slot is reserved by which one-hop neighbor. And based on the information provided by its one-hope neighbors through their FIs, each vehicle in the network is able to know which time slot is reserved by which vehicle within two-hop neighborhood. Thus, each vehicle is aware about the whole ongoing transmissions in its two-hops neighborhood, which allows RR-ALOHA to easily overcome the hidden terminal problem, and so, to reduce transmission collisions. And, based on the dynamic TDMA mechanism with slot reservation, it can guarantee a relatively good QoS in VANETs.

4.4.2.3 Directional antenna-based MAC protocols

Directional antennas have many important benefits in MANETs as well as in VANETs. Directional antennas can provide higher system capacities by directing narrow beams toward the

users of interest, while nulling other users not of interest. This allows for lower transmission interferences, lower power levels, and more channel reuse within the same terminal neighborhood. Figure 4.6 shows how a vehicle is able to have a limited communication coverage space when using directional antennas.

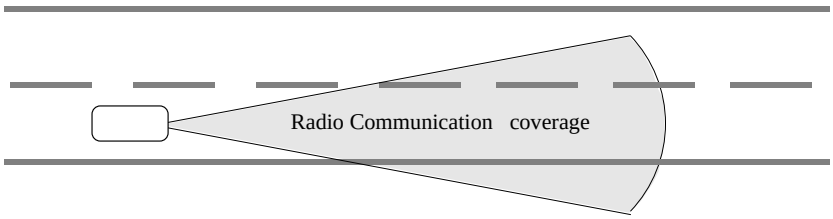

Figure 4.6: Communication coverage when using directional antenna.

In this chapter, we consider each directional antenna-based communicating vehicle as a vehicle equipped with N directional antennas, and each antenna covers an angular space of (360/N) degrees around it. Based on such kind of system, a transmitter can optimize its transmission by limiting the coverage space, which allows channels reuse and makes transmission collisions and hidden terminal problems decreases in the network. Thus, it increases the network throughput and reliability.

In some vehicular communication scenarios, directional antenna-based systems are very welcome. Vehicles move along roads, and in general cases within the same or the opposite direction. Therefor, limiting radio transmission to roads on which we are driving can be beneficial, in particular for MAC issues, when transmission collisions with vehicles moving on neighboring roads is avoided. For example, in high-way scenario, based on such kind of system transmission may be limited to only the high-way in terms of coverage space, which avoid collision with other ongoing radio communications between vehicles driving on other neighboring roads and/or high-ways.

In the following we present some MAC solutions among the many solutions which have proposed based on this directional antenna scheme.

In [57], authors suppose to have an ad hoc network of terminals equipped with M multiple directional antennas as shown in Figure 4.7. Each antenna spanning an angle of $2\Pi/M$ radians. The N antennas are fixed on each terminal with non-overlapping beam directions, so as to collectively span the entire plane. It is supposed that we can switch any one or all of the antennas to active or passive modes. When transmitting, if all antennas are active, the radio signal is transmitted in all directions like in omni-directional antennas. A node can receive a transmission from all antennas, and selects the one receiving the maximum power.

In the following we present some MAC solutions among the many solution which have proposed based on this directional antenna-based scheme.

The MAC protocol proposed here adapts the same scheme used in MACA [42, 43] to be used with directional antennas. It proposes that a terminal that has a data packet to transmit, has to find the direction of the destination in order to transmit the packet on the corresponding

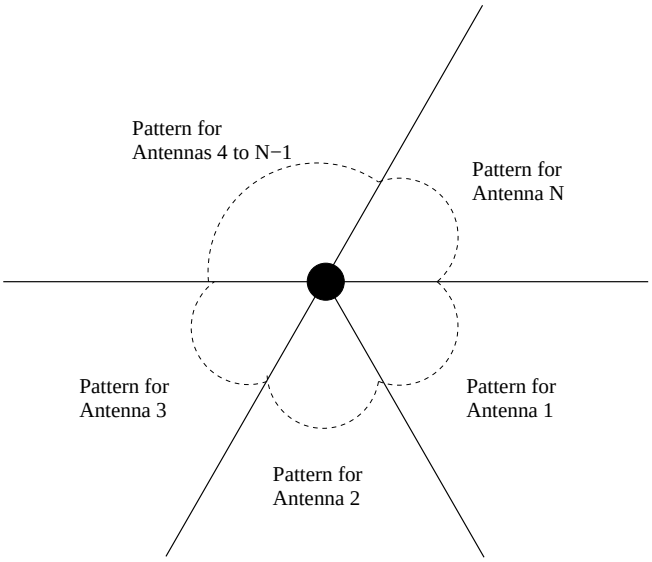

Figure 4.7: Illustration of deployment of directional antennas.

directional antenna. Same for the destination, which has to find the direction of the sender in order to know on which directional antenna the data packet will be received. To manage this task, the following process is used.

Every terminal in the network listens to ongoing transmissions in its neighborhood on all its antennas. When having a data packet to transmit, a sender first transmits an omni-direction RTS to the destination. When receiving the RTS packet, if the destination is ready to receive the transmission, it sends back an omni-direction CTS packet to the sender. Once the sender receives the CTS packet, it starts transmitting the data packet on the antenna which points towards the destination. The destination should receive this transmission on the antenna which is in the direction of the sender. To explain in more details the packet exchanges in this directional antennas-based MAC protocol, an example is shown in Figure 4.8. In this example each terminal is supposed to be equipped with four directional antennas, numbered from 1 to 4. The sender S, when having a data packet to send to D, first transmits an RTS packet to D on all its four antennas. D receives this RTS packet on its directional antenna number 2. If D is ready to receive the data packet, it transmits a CTS packet to S on all its four antennas. Once receiving the CTS packet, S transmits the data packet on its antenna 4, on which the CTS sent by D has been received. All the neighbors of S and D that hear this RTS-CTS, use the related information to prevent interfering with the ongoing data transmission.

Directional Busy Tone-Based MAC (Directional-BTMA) [58] is another MAC protocol based on directional antennas. It adapts the DBTMA [46] protocol described in Section **??** to directional antennas. The same busy tone concept used in DBTMA is again used in Directional-BTMA. As in the previously described directional MAC protocol[57], in Directional-BTMA, each terminal is supposed to have M multiple directional antennas as shown in Figure 4.7. Each antenna spanning an angle of $2\Pi/M$ radians. It is supposed that each terminal when having no ongoing transmission, keeps all its antennas sensing the channel.

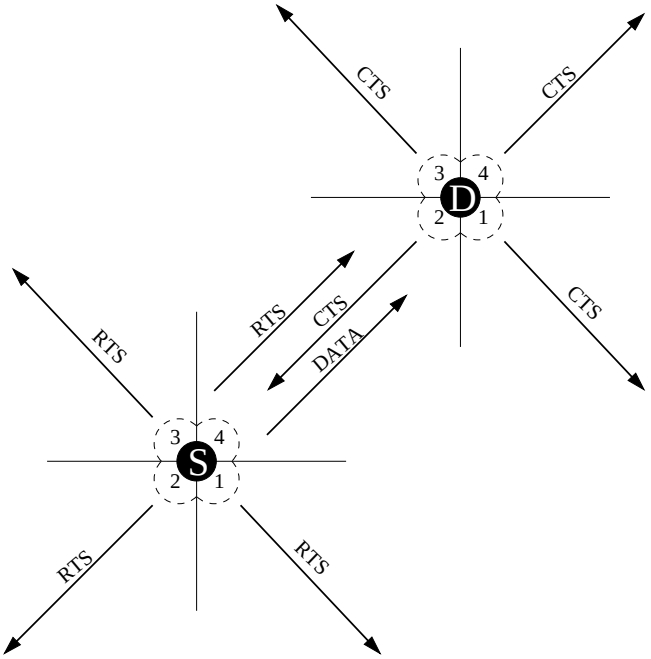

Figure 4.8: Illustration of the packet transmissions.

In order to do not interfere with ongoing transmissions in the neighborhood, a terminal that needs to send data, senses if the busy tone channel is free before sending the RTS packet on all antennas (Omnidirectional RTS). When receiving an RTS packet, if ready to receive the corresponding data transmission, the destination sends a CTS packet on all antennas (Omnidirectional CTS), and activates the busy tone on the antennas that points towards the sender. Once receiving the CTS packet, the sender activates the busy ton on the antenna that points towards the destination and starts the data packet transmission on the same antenna. All neighbors within the communication coverage of the directional antennas having the busy ton active are not allowed to transmit. This scheme can avoid transmission collisions but not in certain scenarios. For example, in Figure 4.9, terminal A is supposed to be transmitting data to B on its directional antenna. B is receiving this transmission on its directional antenna number 4, which has the busy tone activated. Terminal C is not in the transmission coverage of the directional antenna 4 of terminal B, thus it is free to transmit at any time. If terminal C gets a data packet to send to E, it can transmit it on its directional antenna 1 without any risk of collision with the ongoing transmission between A and B. Now, if this same terminal C gets a data packet to send to D, it is as well free to transmit it on its directional antenna 3 that points towards D and B. But, this transmission causes a collision on B with the ongoing transmission between A and B, even that the busy ton on the antenna 1 of B is inactive. Therefore, Directional-BTMA, as it is, is not collision-free.

In both directional antennas-based MAC protocols described above, no localization system is needed to determine on which direction a neighbor is localized in order to know the antennas which points toward it. In Directional MAC (D-MAC) protocol [59] requires that each terminal

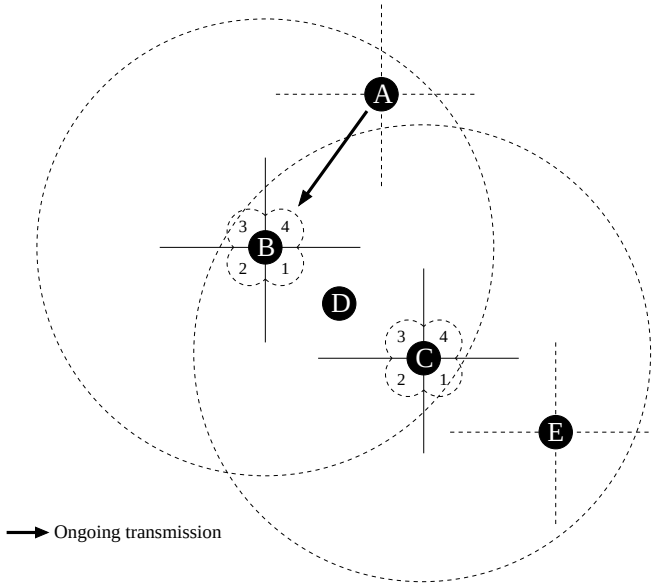

Figure 4.9: Directional BTMA: transmission collision example.

knows its neighbors' location as well as its own location. This assumption does not cause any problem in case of VANETs' applications. In VANETs it is already supposed that each vehicle knows the geographic location of itself and its neighbors. A positioning system, like GPS [5, 6, 7] and Galileo [8], can be used for that.

D-MAC uses the same handshake mechanism based on RTS-CTS packet exchange as in IEEE 802.11 MAC layer [52]. It works in two different schemes, in the first one RTS packet are directional transmitted only, and on the second one they are both directional and omnidirectional transmitted.

4.4.2.3.1 Scheme 1: using DRTS packets When the terminal B, as shown in Figure 4.10, has a data packet to send to C, first it sends a Directional RTS (DRTS) in the direction of C. Since A and C are not in the same direction, A will not hear this DRTS packet. After receiving the DRTS, C replies to B by sending him an Omnidirectional CTS (OCTS). Once receiving this OCTS, B starts the transmission of its data packet using a directional antenna. When B receives the data packet, it immediately transmits a Directional ACK (DACK).

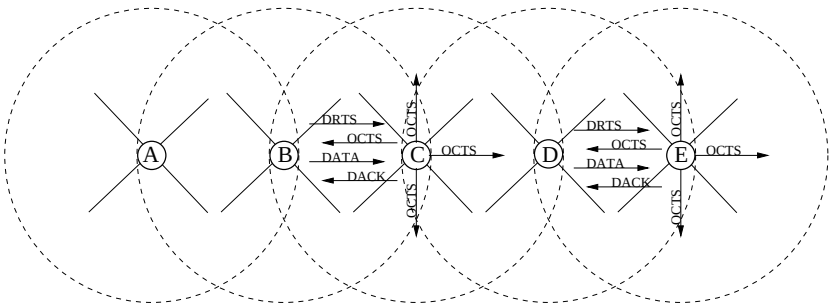

Figure 4.10: The process of the first scheme of D-MAC.

Now, suppose that during the ongoing transmission between B and C, D has a data packet to send to E. By using a directional antenna, D can transmit to E without any risk of collision on C, which is impossible when not using directional antennas. Note that C got its antenna that points towards C blocked when received the OCTS from C. So, D first sends a DRTS in the direction of E. E, if ready, sends an OCTS which authorizes D to starts the transmission of its data packet using the antenna that points towards E. Thus, D can transmit to E when C is transmitting to C without any collision.

4.4.2.3.2 Scheme 2: using both DRTS and ORTS packets In this scheme D-MAC uses both directional and omnidirectional RTS depending on the state of the antennas (blocked or not). This scheme is proposed to improve the first scheme, which may increase the the probability of control packet collisions in some cases. For example, in Figure 4.10, terminal A can not hear the DRTS sent by B to C, thus it is free to transmit to B. Therefor, if A has a data packet to send to B, it is free to send the DRTS to B, which can collide on B with the OCTS or/and DACK packets sent by C. To avoid this problem, in this second scheme of D-MAC, Omnidirectional RTS (ORTS) is sent instead of DRTS when it is possible. In more details, when a transmitter has a data packet to send, (1) if all its antenna are not blocked it transmits an ORTS, (2) otherwise it transmits a DRTS if the desired antenna is not blocked. If the desired antenna is blocked the transmission is deferred until the this antenna becomes unblocked.

Let us suppose that all antennas at terminal B (see Figure 4.10) are unblocked. When having a data packet to send to terminal C, terminal B sends transmit an ORTS. Since this ORTS is sent in all direction, A could hear it this time, and makes its antenna that points towards C blocked until the ongoing transmission between B and C finishes. Thus, when having data to send to B, A should defer its transmission until the desired antenna becomes unblocked.

D-MAC, based on directional antennas and its two schemes, increases the channel reuse with decreasing the packet transmission collisions, which improves the network throughput.

The directional antenna-based mechanism can decrease the probability of transmission collisions in the network, and can increase the channel reuse as well. Thus, can improve the network performances in terms of throughput. In VANETs vehicles movement is limited by roads, and in general cases, vehicles are moving in the same or opposite direction each one to other. This make directional antenna systems easier to be adapted for VANETs when compared to MANETs.

4.4.2.4 Other MAC solutions and improvements for VANETs

Many works have been done around communication technologies in vehicular networks, and in the context of MAC solutions, as far as we know, all proposed solution are just adaptations or extensions of the existing MAC protocols already proposed for VANETs. Above in this section we have presented some protocols and schemes that have been or may be adapted for VANETs. In the following part are presented some slight MAC extensions that have been proposed for VANETs.

In [60] a MAC extension layer is proposed for safety messages transmission. The main goal of this extension layer is to maximize the probability that a safety message is received by all

vehicles within the message range and within the message lifetime. So, the strategy here is to repeat the message a certain number of times within its lifetime. The design of this MAC extension layer is specified as a state machine that can be overlayed on IEEE 208.11 DCF.

Vehicle safety applications generate messages to be delivered to destination with a specified probability which has the following meaning. Each message has an associated intended communication range and useful lifetime (say τ). A safety message should reach all vehicles within the specified range within the specified lifetime. The packet transmission delay (say t_{trans}), which is a function of the packet size and the data rate of the radio, can be calculated. Authors in [60] propose to divide the lifetime into $n = \left\lfloor \frac{\tau}{t_{trans}} \right\rfloor$ slots. And then they pick any $k\,(1 < k < n)$ slots to transmit the packets. If at least one message is correctly received at destination the transmission is considered successful, otherwise the transmission fails. The scheme proposed here can increase the probability that a safety message is received by all concerned vehicles within desired delay, which is very important in safety-related application.

A Location-based Channel Access (LCA) protocol is proposed in [61]. LCA exploits the position information of the vehicle, easily provided by GPS or any other geo-localization system, to move the centralized scheme into ad hoc scheme. In centralized networks, the medium access it managed by the base station. Each base station has a set of channels that it allocates to terminals with in its communication coverage. Each base station covers a specific geographic plan, and two station near each to other should have different channels to allocate in order to avoid transmission collision. This is purely incompatible with ad hoc networks which are totally distributed. A great idea was inspired from this centralized scheme to be applied in LCA. In LCA, the geographic area is divided into a cellular structure, as in centralized networks. To each cell, a unique channel is associated, and used by the vehicle located in it. So, when a vehicle wants to transmit, it first gets its own position, and then it determines the cell which corresponds to this position. Once having the ID of the cell in which it is located, the vehicle obtains the corresponding channel from a locally stored cell-to-channel mapping.

This scheme allows using the cellular concept without having any base station in the network, and any centralized management. It makes allows each vehicle to get a unique channel within its neighborhood. Having each vehicle with a different physical position makes LCA scheme scalable in terms of network size because of the channel re-use. A channel cab be re-used by more than one cell if these cell are enough far each to other.

The main problem in this scheme is that it is supposed that the cell size should be small enough so that two vehicles never happen to be in the same cell. If we take into account this assumption, which is important for the well working of LCA, it will be very difficult to manage the channel allocation process. In cellular networks, there is a special mechanism to manage the the transfer of the terminal from a cell to other, say Handover. In VANETs, Vehicles movement speed is relatively high, and having the cell size so small makes handover problem very difficult, if not impossible, to manage.

4.4.3 Qualitative Comparison of VANET MAC Protocols

The MAC protocols that we have selected as candidates for VANETs in Section 4.4, can be classified into three main categories: contention-based, contention-based with reservation, and directional antenna-based.

A good MAC protocol should be selected in relation with the network characteristics, but as well, in relation with the network requirements. Network requirements refer here to the

network-related applications requirements. The characteristics of a VANET are not always the same since the network environment is not always the same. For example, the characteristics of a VANET composed by a set of a vehicles moving on a highway are not the same as for a VANET composed by a set of a vehicles moving in a city. The application requirements change as well from an application to another. Safety applications for example, have not the same requirements as video and voice communication applications. Thus, in the rest of this part of the chapter, we will try to select which scheme of MAC access is better to be used for which VANET and for which application.

The CSMA/CA scheme used in IEEE 802.11 standards, uses the contention-based access which is suitable for only burst data traffic where the available bandwidth is used effectively. Such kind of MAC schemes are not suitable for real-time communications, as video and voice communications. Safety applications need that the medium access delay be reduced as much as possible, which CSMA/CA can not guarantee when using a contention-based system and inter-frame spacings. CSMA/CA suffers from the network density in terms of number of active communicating terminals, which makes efficiency of the network decreases when the density increases. WLANs which already employ CSMA/CA in ad-hoc mode, have the same limitations as mentioned earlier.

ADHOC MAC uses contention scheme with time slots reservation based on TDMA concept. Time slots reservation makes this MAC protocol able to guarantee a certain level of QoS, which is very welcome for real-time communications and any QoS-based application. One of the problems from which ADHOC MAC or any other TDMA-based system can suffer, is the time synchronization. A vehicular network is considered as an ad hoc network, which is totally distributed. In centralized networks, it is the role of the base station to provide a common clock time for synchronizing the network. Of course, this is not possible in ad hoc network, but in VANETs there is a solution to provide such common clock. In VANETs each vehicle is supposed to be equipped with a geo-positioning system, like GPS, which is able to provide additionally to the physical position, a common clock which can be used for to synchronize the network. Thus, TDMA-based MAC solutions are welcome in VANETs.

The medium access delay in ADHOC MAC, depends on the duration and the number of time slots within one time frame. To reserve a time slot in ADHOC MAC, a vehicle has to wait at least one frame time before attempting to reserve its time slot. And some times it needs to attempt many times before getting a free time slot. Thus, in case of a dense network with an important number of active vehicles, where many vehicles can attempt at the same time to reserve a time slot, the medium access delay can increase considerably because of collisions. Therefore, to be suitable for safety applications, ADHOC MAC as it is, needs some improvements in the sens of reducing the medium access delay in case of network with high density. And as well, just an optimal slotting way can be enough, i.e. find the optimal number and duration of time slots in one frame time.

Table 4.1 shows a brief comparison between IEEE 802.11 and ADHOC MAC protocols. The goal here is not to determine the better MAC protocol in all environment (urban, suburban, highway, etc), since these two MAC protocols appear both interesting for VANETs; for example IEEE 802.11 will better handle high mobility and does not need time synchronization, while ADHOC MAC should allow higher reliability, QoS and real-time compatibility. So, we believe that a combination of the IEEE 802.11 standard and the ADHOC MAC can provide a good and a more complete solution for VANETs.

	802.11 (MAC layer)	ADHOC MAC
Based on	CSMA/CA	RR-ALOHA
Implementation maturity	Mature & evolving	Medium
QoS & real time capability	Small	Medium
Mobility	Medium evolving to high	Medium
Reliability multicast/broadcast	No	Yes
Time synchronization	Not needed	Mandatory

Table 4.1: 802.11 vs. ADHOC MAC protocols

Directional antenna-based MAC protocols adapt existing MAC protocols with using direction antennas. The concept of using directional antenna is of course useful in theoretical field. It is supposed to be able to provide higher system capacities by directing narrow beams toward the vehicles of interest, while nulling other vehicles not of interest. Which provides lower transmission interferences, lower power levels, and more channel reuse within the same terminal neighborhood. But, from the practical point of view, this is not easy to manage, and such kind of technology needs specific devices (directional antennas), which are expensive and very difficult to manage. And as well, using directional antenna makes the coverage for each antenna very limited which makes the network topology changes more faster again in vehicular networks.

So, we believe that the medium access is still a big open issue in vehicular networks. Existing proposals are not suitable as they are to cover all requirements in VANETs-related applications. Safety is an important application field in VANETs. Human lives depend on the efficiency of these applications, which directly depends on the network and the MAC layers efficiency. Thus, a good MAC layer should take care on both safety application's requirements and other application's requirements. Another idea that can be used as well, is using two different MAC layers, the first used by safety applications and the second by other applications.

4.5 Chapter Summary

In this chapter we provided a general view on medium access in MANETs, focusing then on VANETs by introducing few protocols proposed in the literature to support the MAC in VANETs. What we can conclude from this chapter, is that existing MAC protocols have still several weakness when the network topology changes very fast because of the high mobility of nodes, such in vehicular networks where nodes are vehicles. Since the main difference in VANETs when compared to MANETs belongs in the relative high speed of vehicles, we believe that vehicles movement prediction in the network can be very useful to improve the MAC. Thus, our MOPR concept described in Chapter 5 can be used for that purpose. We can use the MOPR cross layer output (Movement prediction based Link Stability metric) to adapt and/or improve the existing MAC protocols in order to make theme deal better with the VANETs characteristics. In Chapter 7 we explain in detail how MOPR can improve the network performance at the MAC layer.

Chapter 5

Movement Prediction (MOPR): Cross Layer Architecture in VANETs

5.1 Introduction

From the two previous chapters (Chapter 3 and Chapter 4), we conclude that designing technical solution, such as routing and medium access protocols, for vehicular networks and any other ad hoc networks with similar characteristics (i.e., with a network topology which changes very fast and very often), faces new challenges. Existing protocols and solutions proposed for MANETs, are not always suitable, at least as they are, for ad hoc networks where the topology changes very fast and very often because of the high mobility of the nodes, such as in VANETs where nodes are vehicles. In this thesis we consider VANETs, as a promising application example of MANETs. And designing a new and dedicated technical solutions for VANETs is not our goal in this thesis, but our goal here is to make the various existing solutions more suitable and more adapted to this networks' characteristics.

The main difference between a MANET and a VANET belongs in the fact that nodes are vehicles that move faster when compared to generic node (pedestrian, or even static nodes). Let us say, the main difference belongs in the nodes movement pattern. Therefor, we believe that considering this difference is the first thing to do when trying to adapt any technical solution for such networks. The technical solutions we consider in our proposal are the data routing and the medium access.

We propose a new cross layer based on movement information prediction. This cross layer is able to provide to each node in the network a stability metric of every node in its neighborhood. This metric is useful for both access and network layers. We name this cross layer MOvement PRediction (MOPR).

The remainder of this chapter is organized as follows. In Section 5.2, we expose our motivation behind the use of the movement prediction. In Section 5.3 we explain in detail our MOPR Cross Layer. And in Section 5.4 we present the MOPR-based LS calculation test-bed with some on-road test results. Finally, Section 5.5 summarizes this chapter.

5.2 Motivation Behind Using the Movement Prediction

As said previously, our main motivation behind using the movement prediction to improve the network performances, belongs in the fact that the movement pattern is the main difference between MANET and VANET environments, and several well working networking solutions proposed for MANETs have to be adapted for VANETs.

Let us consider the example shown in Figure 5.1. This example shows the impact of nodes' movement on routing layer. On the right side of the figure, a Small vehicular network is shown at time t_0, and on the left side the same network is shown after one second of time (at time $t_0 + 1s$). We suppose that the source node "S" wants to send some data to the destination node "D". At t_0, when using a generic routing protocol, node "S" may select the blue route to reach "D" (route: S-1-3-4-D). But, at time $t_0 + 1s$, because of the movement pattern of involved vehicles, the blue route is not available anymore. The communication link $[1, 3]$ is cut since the nodes "1" and "3" are not within the communication range to each other. Thus, "S" has to re-find a new route, resulting in additional resources consumption. We notice that the green route (route: S-1-2-4-D) is still available. Why "S" did not select this route instead of the blue one from the beginning? This route seems more stable, in terms of communication lifetime.

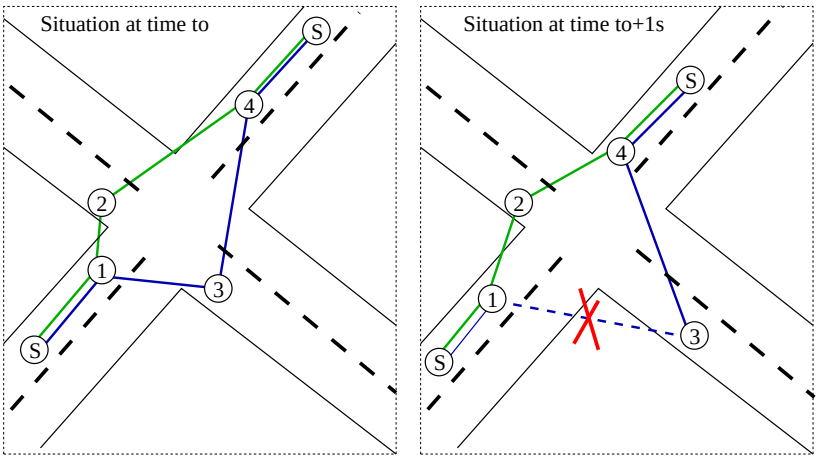

Figure 5.1: Impact of movement of nodes on data routing.

Definitely, it was better if "S" selected from the beginning the most stable route to the destination, the green one. In some scenarios, the most stable route may be longer in terms of hops, but guarantees less routing failures. The most stable route here, refer to a route which is composed by the most stable links among existing links that may be used to construct a route from the source to the destination.

On the side of the MAC layer, let us suppose that we have two nodes that want to establish a communication with a common communicating object (i.e., a neighbor node or access point). These two nodes are not moving with the same speeds relatively to the common object. Thus, if both of them have some data with the same priority to transfer to this common object, they will not have the same chance in terms of time. i.e., the node which moves with a higher relative speed will have less time to access and then to transmit its data when compared to the node which moves with a lower relative speed. This motivated us to use MOPR for avoiding

this situation, so we try to give more chance to neighbors having lower link stability when trying to access the medium.

5.3 MOPR Cross Layer

5.3.1 MOPR-based Network Architecture

Figure 5.2 shows the new network architecture, with the MOPR cross layer integrated.

The MOPR Cross Layer makes a node in the network able to affect a stability metric (say Link Stability (LS)) to each communication link with its direct neighbors. This LS is calculated by a novel algorithm which will be described in Subsection 5.3.3. This algorithm needs an input information, the movement information of the node itself and those of surrounding neighbors. The movement information of the node itself is easy to get, and can be locally available if we consider all vehicles equipped with some localization system, such as GPS or any other geo-localization system. The neighbors' movement information are not so easy to get, since they are not initially locally available. Thus, the MOPR Cross Layer architecture needs an additional mechanism to share the movement information in the neighborhood, which makes neighbor's movement information locally available for each node in the network. In Subsection 5.3.2 we provide more detail on way how the movement information is exchanged between neighbors.

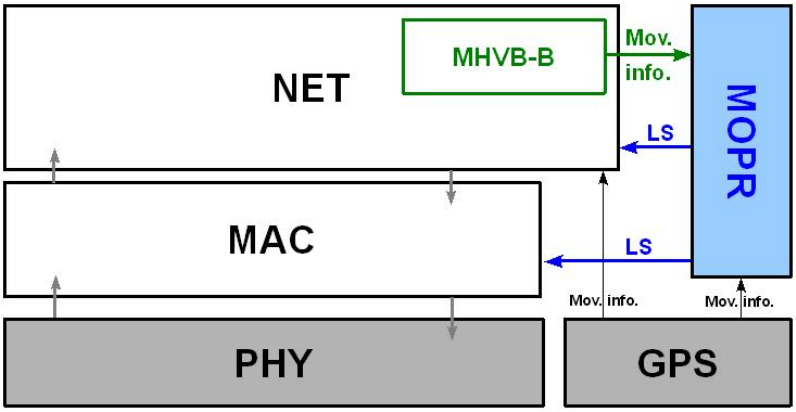

Figure 5.2: Network architecture with MOPR cross layer.

5.3.2 Neighboring Movement Information exchange

At each node i, MOPR needs the own movement information (those of i itself) to be locally available, which is provided by the GPS as shown in Figure 5.2. It needs as well the movement information of all nodes located in the neighborhood of i to be locally available. Since we are operating in ad hoc network context, any solution proposed to make neighbor's movement information locally available, should be totally distributed. In wireless ad hoc networks, several solutions can be used for sharing information between nodes in the same vicinity. But, here we distinguish mainly between two solutions operating at the network layer. The first solution is very simple, and it consists just on making each node in the network adding its own movement information in network control packets before sending them. The second solution, which is

more efficient, consists on using a separated beaconing system. These two candidates are presented in follows.

5.3.2.1 Movement Information Exchanging Through Network Control Packets

One of the solution we propose in our architecture to share the movement information in the neighborhood, consists on using the control packets at the network layer. Knowing that the MOPR cross layer is to be used at the NET and the MAC layers. Right now, at the NET layer the MOPR output (LS) is used at the data routing level. This data routing mechanism, can friendly help MOPR in exchanging the movement information in the neighborhood. Any routing protocol operating in networks such as MANETs and VANETs needs to exchange some specific control messages between nodes for its well operation. These control messages are usually responsible on neighboring nodes discovery and routing routes construction (see Chapter3 for more details). Depending on the operating manner of the routing protocol, these routing control messages are sent periodically or on-demand. Thus, when using the solution described in this paragraph, the neighbors movement information will be locally available, and updated on demand or periodically depending on the routing mechanism we use.

If the used routing protocol works in a reactive manner, such as AODV, then each node in the network, a source or an intermediate node, adds its own movement information in the routing request (RREQ) message before sending it. By doing that, each node in the network, when receiving the RREQ message, is able to get the movement information of its neighbor node from which it received the RREQ message (see Chapter 6 for more details).

Now, if the adopted routing protocol works in a proactive manner, such as OLSR, then each node adds its own movement information in the periodic Hello messages exchanged between neighbors. By doing that we make each node in the network aware about the movement information of its neighbors, thanks to the periodic reception of Hello messages.

The manner of exchanging the movement information presented in this paragraph has a main disadvantage point, that adding movement information in the routing control messages makes their size increases, which amplifies the routing overhead.

5.3.2.2 Sharing Information Through MHVB

Researchers working on Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications, are going in the sense to have some neighboring nodes discovering system, which operates at the network layer to make each node periodically aware about its neighbor nodes' movement information [62]. This information should be updated as frequently as possible. In the Car-to-Car Communication Consortium (C2C-CC) [1], they refer to some beaconing system, which makes a node in the network broadcasts its own movement information at a frequency of 0.1 to 0.5 Hz. Multi-Hop Vehicular Broadcast protocol (MHVB) [63, 64], which is proposed by HITACHI Europe Sophia Antipolis research laboratory, is one of the candidates for the C2C-CC architecture.

MHVB is a flooding protocol indeed, but optimized for VANETs usage. It efficiently disseminates movement information of the vehicles for the sake of active safety applications. It guarantees to disseminate safety messages to a certain distance from the sender, and with respect to a certain critical time. The MHVB algorithm can be adapted to operate as neighbors and neighboring information exchange system, by adjusting the critical distance of dissemination. Note that, the distance is given in real distance (e.g., meters) and not in hops number.

The three main functionalities of MHVB are describes hereafter.

Backfire algorithm

The backfire algorithm helps to identify the right forwarding node based upon its relative position from the sender; that forwarder will refrain, i.e."backfire", other potential nodes which have lesser coverage gain by their eventual forwarding. In the earlier version of MHVB protocol [64] the shape of the backfired region is a circle where, among the potential nodes able to retransmit the information, only the farthest node from the original sender retransmits the packet, so that the coverage gain is bigger, assuming message transmission in the forwarding direction. In the enhanced version of MHVB a sectoral backfire region is implemented with its angle as an extra parameter. The main advantage by implementing such a type of backfire is that by changing the angle of the sector we can modify the area covered for backfire, resulting in a "flexible" and "directional" backfiring region.

Traffic Congestion Detection algorithm

The second algorithm is based on a specific application requirement of vehicular active safety that the vehicles in the middle of traffic congestion need not transmit information as frequently as the ones which are at the edges of the traffic jam or out of it. In MHVB, this functionality is integrated and implemented in a decentralized fashion, using V2V communications. This condition helps MHVB work more efficiently. By counting the number of vehicles surrounding a concerned node, MHVB can detect whether the vehicle is situated in the middle of traffic congestion. If it is the case, it expands the interval of transmitting his own information, therefore saving bandwidth and reducing collisions.

Dynamic Scheduling

In the previous version of the protocol [63], the transmitter and the receiver modules of a node work asynchronously i.e., each node transmits information periodically based upon the delay time computed due to congestion detected by analyzing the message cache. In the case where there is no congestion detection, the transmission takes place periodically every 0.1 sec with some jitter in the transmission within [0.08, 0.1] sec. Thus the timer for the next transmission is "predetermined" ahead of one transmission interval. In this work, we modify the pre-determined time upon each reception of information of the node thus making it dynamic. Here the nodes which are at a distance farther than a threshold are made to forward the received information earlier than the other nodes in the backfire region. Thus the time which was set during the transmission by the process of congestion detection is changed during the reception. By this process the advantage is two fold. The packet is forwarded more quickly (e.g. an emergency warning message has to be transmitted as fast as possible and over a longer distance, which is the ideal condition for high speed scenarios). The second advantage is that when the nodes in the range greater than a threshold transmit information earlier, they indirectly backfire earlier nodes in the range lesser than the threshold, thus saving network resources at lesser ranges.

5.3.3 Link Stability (LS) Calculation Algorithm

As we said in previous paragraph, the movement information of neighboring nodes are the main input for MOPR to calculate the LS metric. From the realistic point of view, the movement information in VANETs can be mainly translated into the following manner: the

physical position (e.g., Latitude and longitude), the direction (e.g., Azimuth), and finally the speed. From the theoretical view, this can be different. When using the Network Simulator NS2 for example, the situation becomes quit different. And the movement information can be expressed into: position on XY plan (X and Y), speed on X access (dX), and speed on Y access (dY). Here, there is no need for direction, since the dX and dY values express the direction as well. In the rest of this section we consider the movement information from the theoretical side (i.e., Position (X, Y) and speed (dX, dY)).

In this paragraph we explain how MOPR calculates the LS metric based on the movement information. First of all, we suppose that each node in the network has locally available the movement information of itself, and of its neighbor nodes.

Let us make the following assumptions and arguments, which are important to understand the rest of this paragraph.

1. Each node has a bidirectional communication link with any other neighbor node. And two nodes are considered as neighbors, if and only if they are within a distance less than or equal to R meters from each other.

2. Each vehicle in the network moves with a constant velocity V meters/second during the LS calculation time, but initially randomly chosen.

3. $LS\,[i,j]$ is the Link Stability (LS) of the communication link between nodes i and j, with $0 < LS\,[i,j] < 1$.

4. $LifeTime\,[i,j]$ is the lifetime of the link $[i,j]$, which corresponds to the duration time in seconds that nodes i and j spend to go out of the communication range to each other with respect to their actual movement information. In other words this means, the estimated time needed, in seconds, to have the distance between nodes i and j greater than the maximum communication range R (e.g., $R = 250m$).

5. $MaxLifeTime$ is a constant in second used for Link-Lifetime normalization. To get the $LS\,[i,j]$ between 0 and 1, we divide the $LifeTime\,[i,j]$ by $MaxLifeTime$. In case of a proactive routing protocols, the $MaxLifeTime$ may be the lifetime of the concerned entry in the routing table for example, i.e. the time before a route in the routing table is considered as invalid. In case of a reactive routing protocol, it may be the estimated duration time of the oncoming transmission. In case of position-based routing protocols, the situation is little bit different since the next forwarder is selected for each data transmission packet. Thus, the $MaxLifeTime$ can be chosen equal to the neighbors discovery frequency time (i.e. the duration time between each successive of Hello message transmissions). The next forwarder is selected from the of neighbors set, which may be not enough updated because of the nodes mobility. By using the frequency time of the neighbors set update as the $MaxLifeTime$, we guaranty that the next forwarder, when selected based on MOPR, will get the highest chance to be still in the neighborhood when needed for a packet transmission.

Figure 5.3 shows an example of some vehicles connected to each other and forming a small network. As shown in this figure, by using MOPR, node i attributes to each one of its neighbors a stability metric LS (e.g., $LS[i,j] = 0.9$).

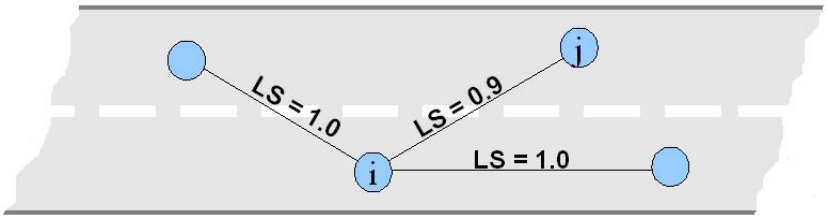

Figure 5.3: MOPR-based network example.

To understand better how this stability metric (LS) is calculated by MOPR, let us consider only the two nodes i and j. Look at Figure 5.4 which shows the same two nodes i and j on a stationary Cartesian coordinate system with orthogonal unit vectors $\hat{x}$ and $\hat{y}$ along the X and Y axes respectively, which let's the velocity of vehicle i to be $\overrightarrow{v_i} = vx_i\hat{x} + vy_i\hat{y}$ and the velocity of vehicle j to be $\overrightarrow{v_j} = vx_j\hat{x} + vy_j\hat{y}$.

The LS corresponding to the communication link $[i, j]$ in this example is calculated following Equation (5.1).

$$LS\,[i_1, j_1] = \frac{LifeTime\,[i, j]}{MaxLifeTime} \tag{5.1}$$

Since the $MaxLifeTime$ is a constant, $LS[i, j]$depends directly on the $LifeTime[i, j]$ value. Thus, the question we ask now is how to calculate the $LifeTime[i, j]$?.

If we look at Figure 5.4 again, and we suppose that $D0 < R$, and $D1 = Rmax$, then $LifeTime[i, j]$ corresponds in this example to the difference between the two instances of time t_1 and t_0. Thus, we have:

$$LifeTime\,[i, j] = t_1 - t_0 = \Delta t \tag{5.2}$$

To solve Equation (5.2), we should find t_1, knowing that t_1 is the time when D_1 becomes equal to R. Thus,

$$LifeTime\,[i, j] = \Delta t\, when\, D_1 = R \tag{5.3}$$

We have,

$$\begin{aligned} D_1^2 &= \|X_i1 - X_j1\|^2 + \|Y_i1 - Y_j1\|^2 \\ &= \|(X_i0 + Vx_i\Delta t) - (X_j0 + Vx_j\Delta t)\|^2 + \|(Y_i0 + Vy_i\Delta t) - (Y_j0 + Vy_j\Delta t)\|^2 \end{aligned} \tag{5.4}$$

From (5.4) we get:

$$D_1^2 = A\Delta t^2 + B\Delta t + C \tag{5.5}$$

$$with \begin{cases} A = (Vx_i - Vx_j)^2 + (Vy_i - Vy_j)^2 \\ B = 2\left[(X_i0 - X_j0)\,(Vx_i - Vx_j) + (X_i0 - Y_j0)\,(Vy_i - Vy_j)\right] \\ C = (X_i0 - X_j0)^2 + (Y_i0 - Y_j0)^2 \end{cases}$$

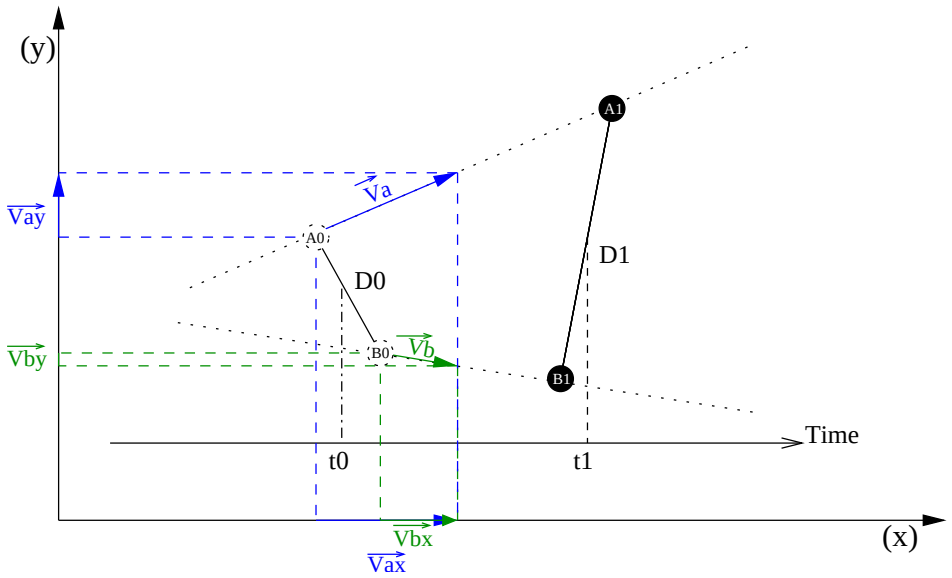

Figure 5.4: Link lifetime estimation.

So, from (5.3) we get:

$$LifeTime\,[i,j] = \Delta t \, when \, D_1^2 = R^2 \tag{5.6}$$

Finally, from (5.5) and (5.6), we get that the $LifeTime\,[i,j]$ is equal to the Δt which solves the following equation.

$$A\Delta t^2 + B\Delta t + C - R^2 = 0.$$

5.4 MOPR-based LS Calculation: Real Test-bed

The situation is always different when going to a realistic implementation from a theoretical one. We have implemented the MOPR-based LS calculation in a real testbed, and our first conclusion was that the LS calculation is done in a different way. In realistic environment we do not have an XY access as in ns2 for example, but we have the latitude and the longitude instead. In ns2, to predict the movement of a node we consider the projection of its speed on the XY access, which is not needed when going to realistic implementation. To calculate the LS of its neighbor, a node needs just to know the relative speed of this neighbor to be able to estimate the time when this neighbor is going to leave the communication range. Thus, the relative speed in our realistic implementation is calculated based only on the variation of the distance the two involved nodes.

Let us consider the example shown in Figure 5.5 to explain how LS is calculated based on MOPR in our realistic implementation.

By using some beaconing system each vehicle has locally and periodically available the positions of its neighbor. In this implementation we have used MHVB [63, 64] for this end. Each vehicle has its position (Latitude and Longitude) provided by the GPS. By having its movement information and those of its neighbor periodically available, the two vehicles

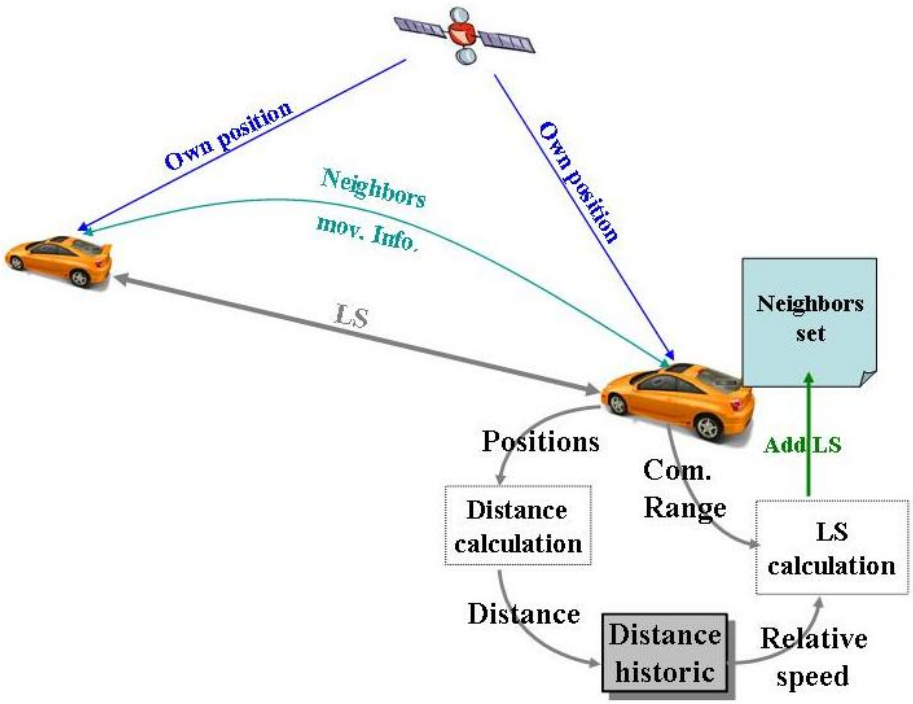

Figure 5.5: MOPR-based LS calculation in real testbed.

periodically calculate the distance to each other, and save it locally in some cache. The distances are calculated as follow.

Here we show how we calculate the distance ($Dist(Pos1, Pos2)$) between two positions: $Pos1(Lat1, Lon1)$ and $Pos2(Lat2, Lon2)$.

$$\text{We have: } \begin{cases} R = 6371km \ (earth's\, radius) \\ \Delta Lat = Lat2 - Lat1 \\ \Delta Long = Lon2 - Lon1 \end{cases}$$

$$Distance(Pos1, Pos2) = R.C \tag{5.7}$$

$$\text{with: } \begin{cases} C = 2.atan2\left(\sqrt{a}, \sqrt{1-a}\right) \\ a = sin^2\left(\Delta Lat/2\right) + cos\left(Lat1\right).cos\left(Lat2\right).sin^2\left(\Delta Long/2\right) \end{cases}$$

By periodically comparing the current distance from its neighbor with the previous distance (available in the cache), each vehicle is able to periodically get the relative speed of its neighbor. Finally, by knowing the relative speed of its neighbor and its own maximum communication range, each vehicle is able to calculate the lifetime of the communication link with its neighbor. The LS is got by normalization of the link lifetime.

We have implemented this MOPR-based LS calculation under Linux (say MOPR-LS-calculation) and tested it with using two laptops embedded in two cars. In follows we preset this implementation and relative on-road tests we have done around Sophia-Antipolis.

5.4.1 Configuration and settings

We have implemented MOPR-LS-calculation under Linux on two laptops with the following configuration:

- CPU: Pentium 4
- OS: Fedora Core 2 Linux with kernel 2.6 and GCC 3.0.
- GPS antenna: NAVILook USB Adapter GPS
- Wireless interface: IEEE 802.11b
- MaxLifeTime: 30 seconds

Each laptop is then embedded in one car as shown in Figure 5.6.

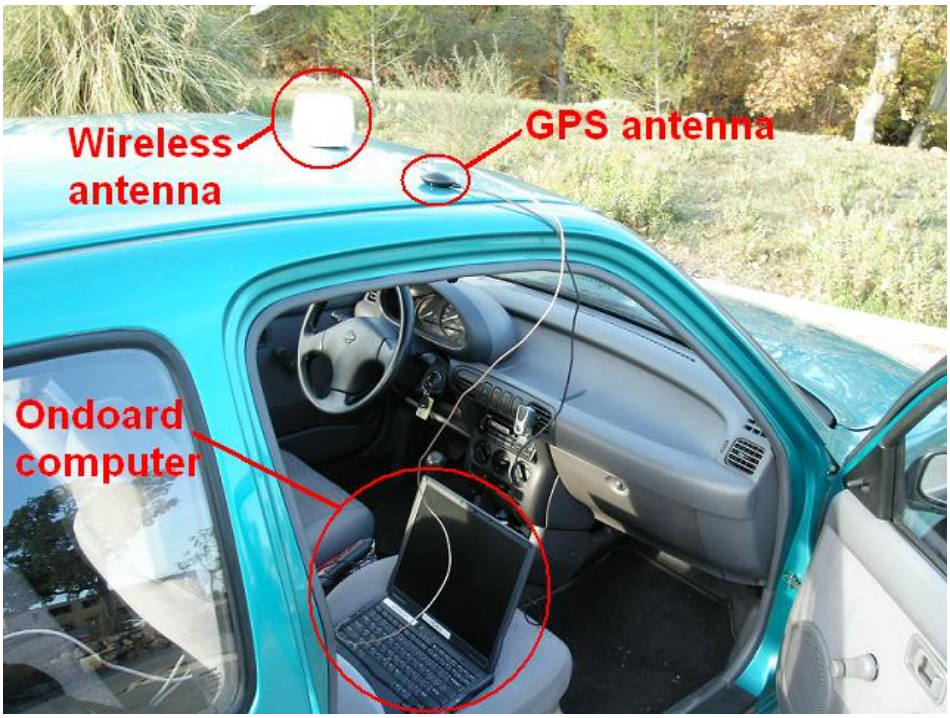

Figure 5.6: On-road testbed configuration and settings.

5.4.2 On-road tests and results

In the tests we have fixed the LS calculation frequency to 1Hz (i.e., LS is calculated every 1 second), which is the higher frequency we can set right now, because of the maximum frequency of the GPS adapters available in the market right now, which is 1Hz. Thus, MHVB beacon frequency are as well set to 1Hz (i.e., neighbor's positions are updated every 1 second).

We have used two cars (car1 and car2). Figure 5.7 shows a picture which we have taken from inside the car1, where the car2 corresponds to the green car in the same picture. The screen of the laptop embedded in the car1 shows in real time the distance between the two cars, and their corresponding lifetime and the LS, that are calculated following the formula 5.7

The first test we have done consists on keeping the two vehicles stationary at a distance of 70 meters, with our program running on both cars. Then, we observe the stability of the

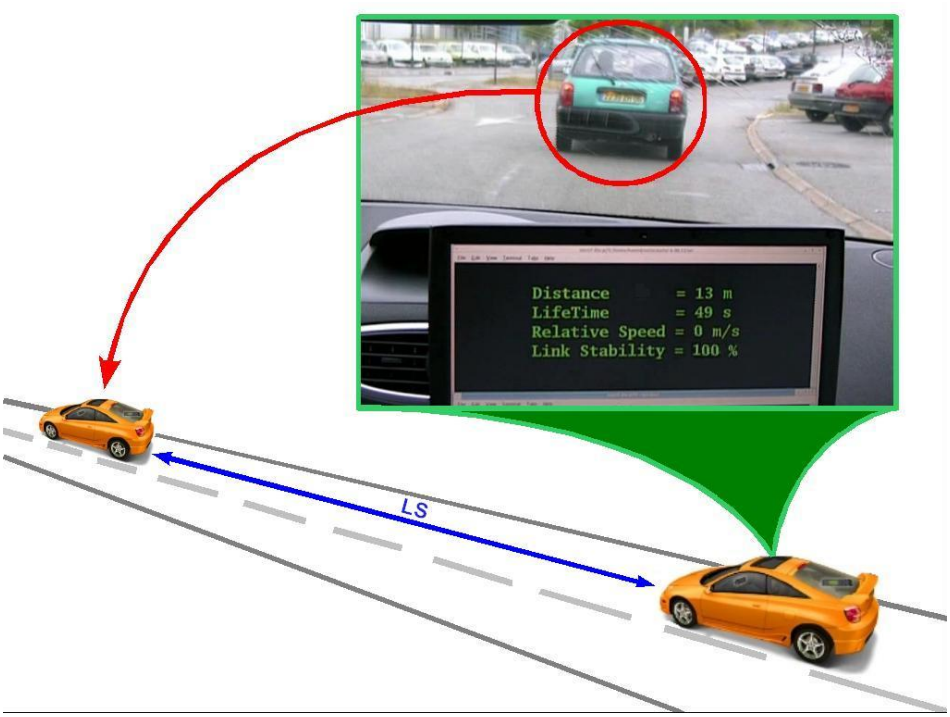

Figure 5.7: On-road tests.

LS value we get during 100 seconds and we compare it with theoretical one. Knowing that theoretically, the LS should be equal to 100% all the time if the maximum communication range is set to 250 meters, and both cars are static and located of each other at a distance of 70 meters only. The results we have got show that the real LS is in most of time the same than the theoretical one (i.e., equal to 100%). That means the LS calculation is close to the theoretical calculation when involved vehicles are static.

Now, to see the situation when vehicles are moving, we have done some on-road tests with keeping car1 stationary on the road, and making car2 moving with a static speed (around 15km/h) on a line-straight from a point A to a point B. The point A is located at a distance of 7 meters in front of the car1, and the point B at a distance of 80 meters. In these tests we have set the maximum communication range to 80 meters at each car because of the space limitation of the site where our tests have been realized. In these tests we observe the variation of the LS values and the variation of the distance between the two cars we have got based on GPS position information (following the formula 5.7). Figure 5.8 plots the results we have got.

In Figure 5.8, the plots "LS" and "T-LS" respectively correspond to the experimental LS we have got from our tests and the theoretical LS which we should get. The plots "Distance" and "T-Distance" respectively corresponds to the experimental LS we got and the theoretical LS which we should get. As you can see, the experimental distances converge to theoretical distances. The experimental LS converge as well to theoretical values, except some time where it gives a 100% of stability when theoretical LS gives a much lower stability. Let us consider the LS value we got at time 13 seconds. At that point the experimental LS gives a 100% of stability, where theoretically it should give some stability around 42%. This situation is

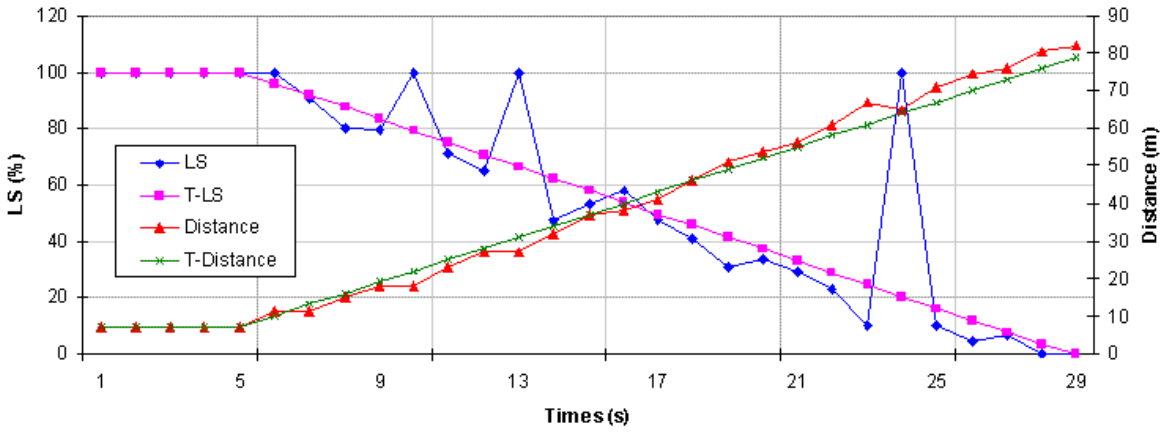

Figure 5.8: LS variation when moving with a static speed.

explained by the fact that the relative speed goes down and it guarantees a larger lifetime which makes the LS equal to 100 %. The relative speed goes down when the variation in the distance to the own position at one second ago decreases. Look at the plot "Distance" at points 12 and 13 seconds for example, where the distance shows almost the same value (around 28 m). Thus, since the relative speed used in the calculation of the experimental LS corresponds to the difference between successive distances, the relative speed here is almost null which makes the experimental LS equal to 100%.

Therefore, the unreliability in the LS calculation comes mainly from the unreliability in the relative speed calculation, which comes from the unreliability in the distances calculation. The distances are calculated based on the GPS positions of the two involved cars, following the Formula 5.7. Thus, the distance is wrong if the GPS data are wrong. Therefore, our LS reliability is sensible to GPS imprecision.

In our experimentation, when calculating the LS we do not care about the movement direction of the involved vehicles, but we consider only their relative speed which we get by comparing the current distance between them to the the same distance at one second ago. To be sure that this method for computing the relative speed not have any negative impact on the reliability of the calculated LS, we have done several on-road tests as follow. We consider only car1, which we observe during 200 seconds when driving somewhere around Sophia-Antipolis. We focus on the real speed of the car which we get directly from the GPS and the speed we get based on the distance between two successive GPS positions. Figure 5.9 shows a comparison between the two speeds.

The plot "GPSspeed" in Figure 5.9 corresponds to the speed we get from the GPS data, and the plot "Speed" corresponds to the speed which which we get by calculating the distance between the GPS position at current time and at one second ago. As we can see, both speeds converge to same values at most of time. Thus, considering the the movement direction of vehicles in the calculation of the relative speeds between them is not important since we can calculate the relative speed only based on the variation in the distances.

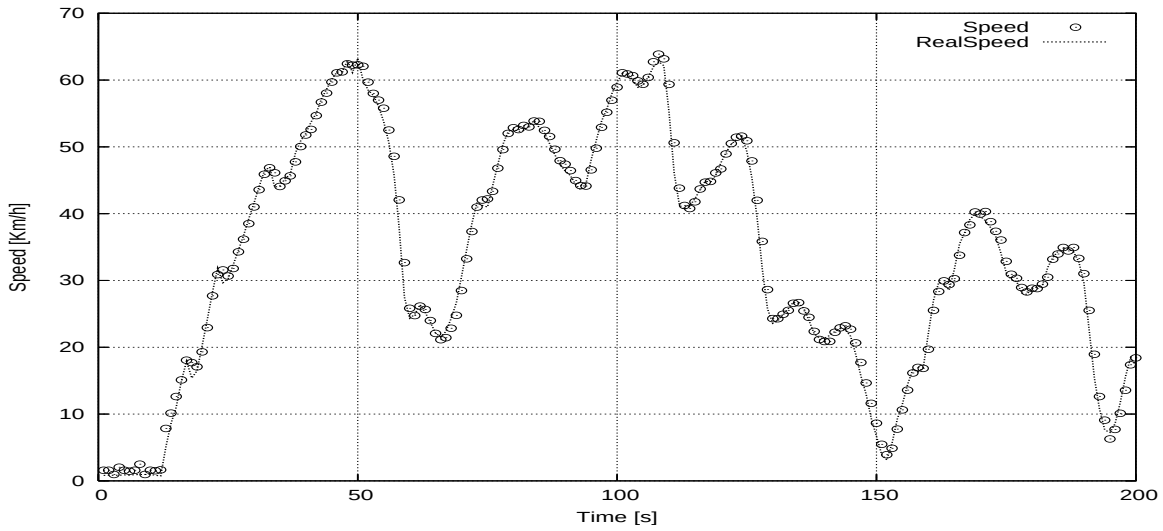

Figure 5.9: GPS speed vs. GPS distance-based speed.

5.5 Chapter Summary

In this chapter we have presented our MOPR concept. Within MOPR, after getting the movement information of the nodes located in its neighborhood by using some dedicated system (e.g., MHVB), and its own movement information locally available (thanks to GPS), each node in the network is able to attribute to each neighbor link a Link Stability (LS) metric. This LS metric is calculated by a specific algorithm which has been described in this chapter. This LS is computed by normalizing the link lifetime which is estimated on the basis of the movement information of involved neighbors.

Once this LS metric is calculated, it is given to both MAC and network layers. At the network layer, the LS is used at the level of the data routing process. The LS is used differently depending on the protocol to be improved.

We have implemented the LS calculation functionality under Linux. For validation of this implementation, we have done some on-road tests with two cars. We noticed that LS reliability depends on the reliability of the GPS data.

In Chapter 6 and Chapter 7, we show how the MOPR output (LS) helps in improving the routing layer and the MAC layer in vehicular context, respectively.

Chapter 6

MOPR-assisted Data Routing in VANETs

6.1 Introduction

From Chapter 3 we have concluded that existing routing protocols that have been proposed for generic MANETs still do not guarantee enough reliability, specially when the network topology changes very fast and very often such as in VANETs. We believe that this main feature of vehicular networks (nodes' movement pattern) should be taken into account when routing data from a source to a destination. We do not propose any new routing protocol, since many protocols that exist in the literature have already shown interesting potential to deal with VANETs' characteristics. For example, position-based routing protocols show a good potential for VANETs in [21]. Therefore, we propose to improve exiting routing protocols by considering the movement information of the surrounding vehicles. By predicting the movement of its neighbors, a vehicle is able to estimate the duration time that a neighbor is going to spend in its radio coverage, thus it is able to estimate the communication lifetime of the link formed with each neighbor.

In Chapter 5 we have presented a new concept which we called MOPR. This concept attributes to each neighbor node a Link Stability (LS) metric which is calculated based on involved nodes' movement prediction. This LS metric is useful when selecting the next forwarder node in routing data from a source to a destination (e.g., a node always selects as next forwarder the neighbor candidate which has the greater LS).

In the rest of this chapter we first explain how MOPR can improve the performances of routing protocols in networks where the topology is very dynamic. Indeed, topology-based routing protocols are not necessary the best choice for vehicular ad hoc networks, but we have implemented our proposal into this kind of routing protocols to investigate their behavior and performance when taking into account movement prediction. After having got interesting simulation results with topology-based routing protocols when using MOPR, we have tested our proposal with position-based routing schemes that are more suitable for the vehicular networks.

The remainder of this chapter is organized as follows. First, in Section 6.2 we present the implementation of MOPR on two topology-based routing protocols; the first one is AODV which is a reactive routing protocol, and the second one is OLSR which is a proactive routing protocol. Then, in Section 6.3 we present the implementation of MOPR on position-based

routing by considering the GPSR routing protocol. Finally, Section 6.4 provides a summary of this chapter.

6.2 MOPR Applied to Topology-based Routing Schemes

From Chapter 3, we distinguish two main categories of routing protocols in the topology-based family: reactive and proactive routing. In this section we present how the MOPR output (i.e., the LS information) can be beneficial for the topology-based routing protocols in vehicular contexts. We describe as well how this LS can be exploited by both reactive and proactive routing protocols in that scheme.

6.2.1 Reactive Data Routing Scheme

As a reactive routing example for the application of our concept we have chosen the Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol [14]. In AODV, when a source node "S", as shown in Figure 6.1, wants to reach a destination node "D", first it disseminates a Route Request (RREQ) message through the network, and then waits for a replay. Once receiving this request, the destination node "D" replays to the source node by sending a Route Replay (RREP) message through the route built by the RREQ packet. For more detail on AODV functionality, please refer to Chapter 3.

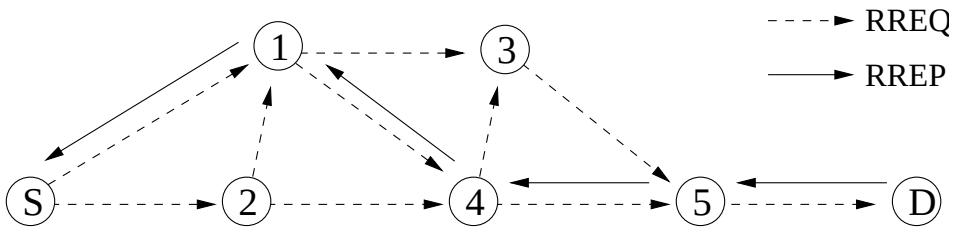

Figure 6.1: AODV functionality.

In the same example shown in Figure 6.1, you can see that different routes exist from the source node "S" to the destination "D", but AODV selects only one among those routes. This selected route is maybe the optimal one in terms of number of hops, but not necessary in terms of communication lifetime. The route selected by AODV can be composed by some intermediate nodes which are not stable, in terms of communication lifetime, because of their movement behavior. Thus, our goal from applying MOPR to AODV, or any other reactive routing protocol, is to select as much as possible the most stable route among all existing routes from the source to the destination.

Supposing we have several potential multi-hop routes from a source node (a vehicle or a static road side unit) to a destination node (another vehicle or another road side unit). We propose to choose the route which is the most stable when considering the movement conditions of the intermediate vehicles with respect to the source and the destination. The intermediate nodes can be whether moving or stationary vehicles, or even gateways along the roads.

By knowing the speeds and the movement directions of the nodes involved in the routes (including source and destination), MOPR can roughly predict their positions in the near future; eventually, by knowing the size of the data to send, it can estimate how long the transmission of each data frame will take.

Therefore, the optimal route selection for data transmission will provide the route composed by intermediate vehicles that are not likely to cause a rupture of the transmission during the transmission time because of their mobility. This approach should help as well in minimizing the risk of broken links and in reducing data loss and link-layer and transport retransmissions.

Let us consider the example shown in Figure 6.2 to explain in more detail how AODV selects the optimal route based on MOPR. The route stability of the selected route corresponds to the lowest intermediate LS.

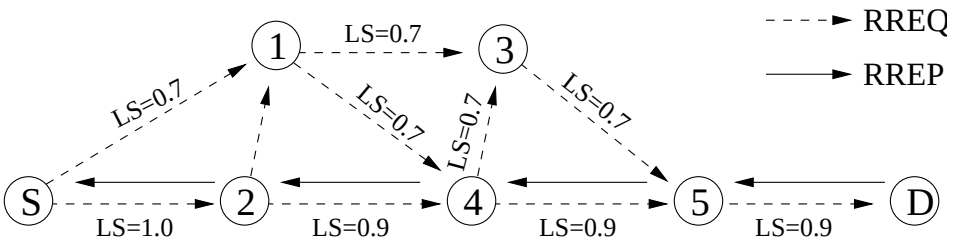

Figure 6.2: MOPR-based AODV: example.

Now, based on MOPR, AODV selects the route composed by the most stable links, knowing that, more the LS is high, more the Link stability is. In Figure 6.2, the most stable route from "S" to "D" is the one composed by the intermediate nodes: 2, 4, and 5.

6.2.1.1 MOPR-based route construction

As explained in Chapter 5, MOPR needs the movement information of all neighbors to be locally available. But, since here we are in a reactive context, the movement information sharing process can be done in a reactive manner as well. If we use the routing control packet for sharing the movement information, we propose that each node in the network indicates its own movement information in both RREQ and RREP packets.

In following we explain step by step the MOPR-based AODV process.

1. We propose to make some changes in both, RREQ and RREP packets, and the routing table as in follow:

   (a) In both RREQ and RREP packets, we add the following fields

   - *Position*: the position of the neighbor from which the packet is received.
   - *Speed*: the speed of the neighbor from which the packet is received.
   - *PS*: Path Stability (PS) from the source/destination node, with $PS \in [0, 1]$.

   (a) in the routing table, we add the following field

- PS: Path Stability (PS), indicates the stability of the corresponding route, with $PS \in [0, 1]$.

2. When having some data to send to some destination node "D", the node "S" puts its actual position and speed in the related fields (*Position* and *Speed* respectively) in the RREQ packet. Then, it transmits the packet after having set the PS field to 1.

3. When receiving a RREQ packet from node "i", the node "j" is able to get the movement information of the node "i". Thus, MOPR calculates the RS corresponding to this previous node "i", i.e. $LS[j, i]$. Then, it calculates the new PS ($newPS$).
with $newPS = \min(LS[j, i], PS)$, and PS: the PS as indicated in the received RREQ packet.
Now, "j" replaces the RS in the RREQ packet by the $newPS$.
Now, if this RREQ packet is received for the first time, it should be systematically forwarded, otherwise it is forwarded only, and only if, the new route proposed in this RREQ is more stable, i.e. the $newPS$ is higher than the one in the cached route. After that, the node "j" updates its routing table with respect to the information in the received RREQ packet. In the routing table entry corresponding to the node "S", the PS value is replaced by the $newPS$. And, in the routing entry corresponding to the neighbor "i", the PS value is replaced by $LS[j, i]$.

4. When receiving the RREQ packet, the destination node "D" proceeds as indicated in Step 3. But, instead of forwarding the RREQ packet, "D" replays to "S" by sending a RREP packet following the basic process of AODV (see Chapter 3). Before replaying, the node "D" should put its actual position and speed in the RREP packet (in appropriate fields) and set the PS field to 1.

5. When receiving a RREP packet from a node "j", the node "i" is able to get the movement information of the node "j". Thus, MOPR calculates the LS corresponding to this previous node "j", i.e. $LS[i, j]$. Then, it calculates the new PS ($newPS$) corresponding to the route to the destination node which initiated this RREP.
with $newPS = \min(LS[i, j], PS)$, and PS: the PS as indicated in the received RREP packet.
Now, "j" replaces the PS in the RREP packet by the $newPS$, and then forward it to the next node with respect to its routing table. This routing table is optimal in terms of communication lifetime, since it has been updated based on MOPR during the passage of the RREQ packets.
After forwarding the RREP packet, the node "j" updates its routing table with respect to the information contained in the RREP packet. In the routing table entry corresponding to the node "D", the PS value is replaced by the $newPS$. And, in the routing entry corresponding to the node "j", the PS value is replaced by $LS[i, j]$.

This MOPR-based manner of processing the RREQ and the RREP packets, makes the routing table at each intermediate node automatically updated with respecting the PS metric. Therefor, the data packets are sent through the most stable routes available in the network.

An interesting based on movement prediction has been proposed in [65]. In this work the authors propose to make AODV recomputs a new route before the actual route expires. This

very interesting functionality has not been included in our proposal, but we beleive strongly that it may improve the performances of the system.

6.2.1.2 Simulations

We have simulated under the network simulator ns2 [66] the AODV routing protocol with MOPR applied. As ns2 implementation of the AODV protocol, we have used the well known implementation of the Uppsala University (AODV-UU) [67]. This implementation is the most compliant with the AODV RFC 3561. In the rest of this chapter, we name the generic implementation of AODV as "AODVUU", and the MOPR-based AODV as "MOPR-AODVUU".

6.2.1.2.1 Simulation environment and scenario description For our simulations we have considered the following scenario example. We have 40 nodes (vehicles) distributed as shown in Figure 6.3. 20 nodes are horizontally distributed in a random way, and other 10 nodes are vehicle-like and randomly distributed.

The maximum radio propagation range is set to 250 meters, and the classical 802.11 MAC functionality are used, i.e. Distributed Coordination Function (DCF), Carrier Sense Multiple Access with acknowledgments (CSMA/CA with ACK) and Request-To-Send Clear-To-Send (RTS/CTS), and fragmentation, even if we suppose the messages are enough small. Traffic type is CBR, and four source/destination couples are selected randomly along the nodes horizontally distributed. Each source starts to transmit at time randomly chosen between 20s and 30s, and stops transmission at a time randomly chosen between 70s and 90s.

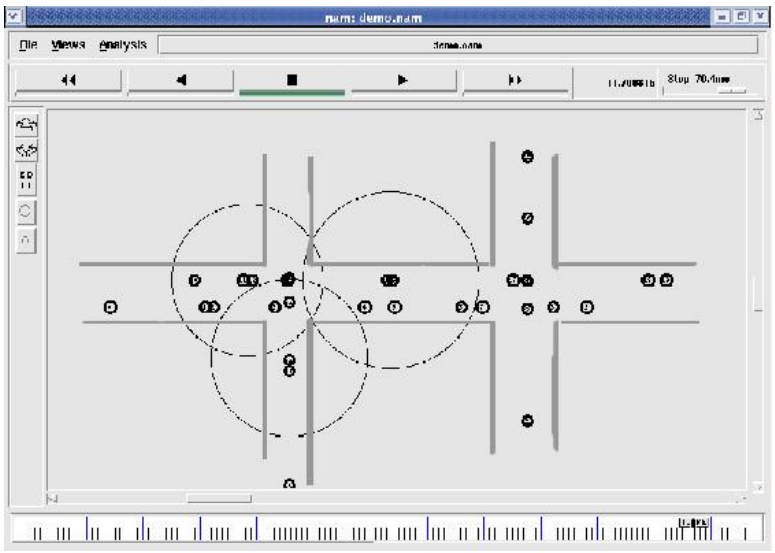

Figure 6.3: The simulated vehicular environment.

6.2.1.2.2 Simulation results and analysis The simulation results we have obtained by 1000 simulation runs and 95% of confidence interval are presented in follow.

The metrics studied are the following:

- **Packet Delivery Ratio:** defined as the number of correctly received packets at the destination over the number of packets sent by the source.

- **Routing Overhead:** defined as the number of bytes injected in the network by the routing protocol.

- **Routing Overhead Ratio:** defined as correctly received packets (in bytes) at the destination over the routing overhead (in bytes).

- **End to End Delay:** defined as the duration time that a packet takes to go from the source and arrive to the destination.

The results we have obtained are presented in two sets of plots. The first set shows the network performances versus the vehicle average speeds (randomly chosen within ranges around the X value). The second set of plots, shows the network performances versus the maximum CBR throughput for each source/destination couples, which is incremented by 0.5 Mbps each time from 0.5 Mbps to 2.5 Mbps. There are two curves in each plot in the two sets, one representing the standard AODVUU performances, and the second represents the MOPR-AODVUU performance.

Figure 6.4 shows that MOPR-AODVUU generates only little more routing overhead than AODVUU. But, the routing overhead does not have an important sens without looking to the routing overhead ratio, and Figure 6.5 shows that MOPR-AODVUU offers the same quantity of routing overhead ration than AODVUU.

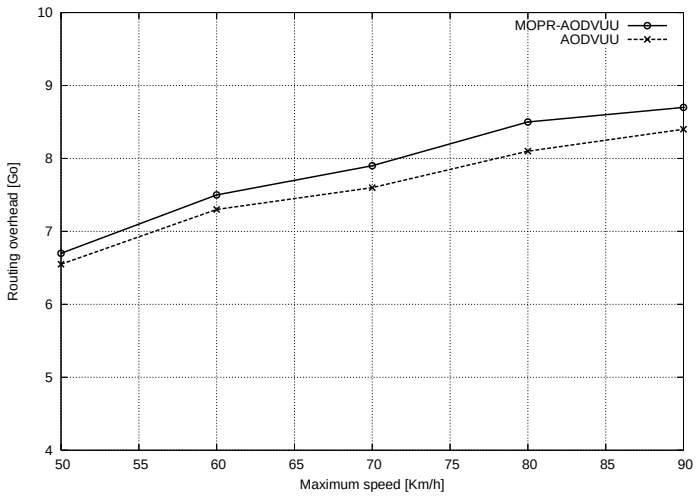

Figure 6.4: Routing overhead versus the vehicle average speeds.

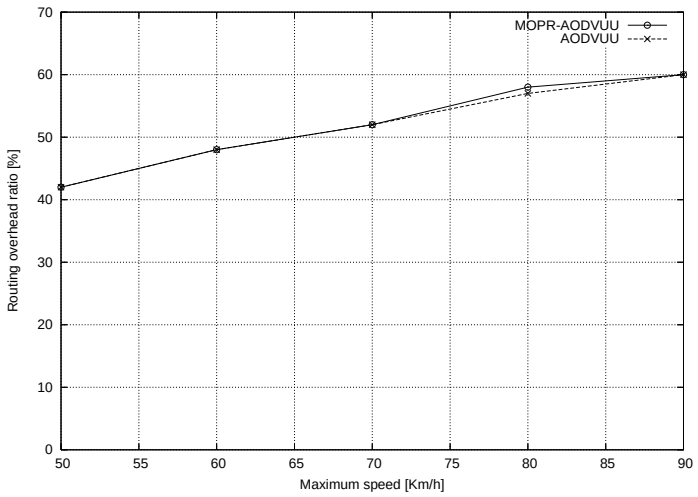

Figure 6.5: Routing overhead ratio versus the vehicle average speeds.

Figure 6.6 and Figure 6.7 show clearly that MOPR-AODV improves AODVUU in terms of delay and packet delivery ratio respectively. And Figure 6.7 shows that the the delay decreases more quickly with AODVUU when increasing the speed average. All this is simply explained by the fact that, when compared to AODVUU, MOPR-AODVUU avoids as much as possible the link failures during the data routing by selecting the most stable routes. A stable route results in less routes recalculations and less additional resources consumption.

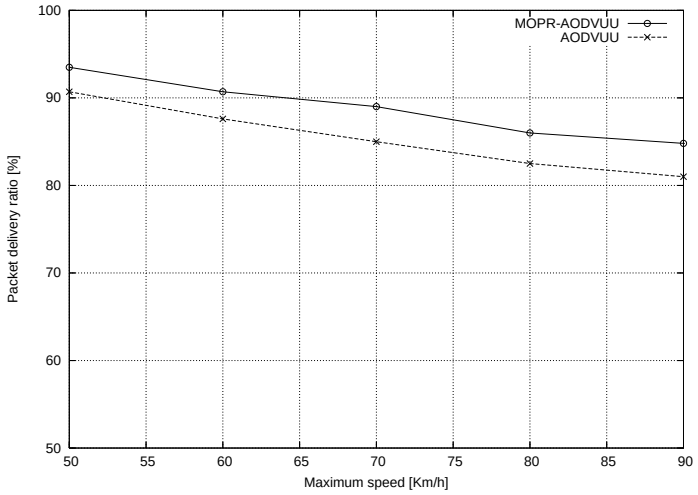

Figure 6.6: Packet delivery ratio versus the vehicle average speeds.

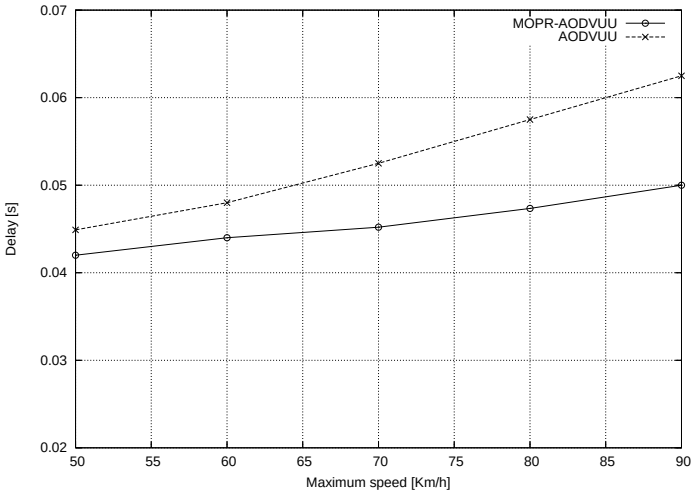

Figure 6.7: Delay versus the vehicle average speeds.

In the following set of figures we show the performances of MOPR-AODVUU vs. those of AODVUU. Up to 1.5 Mbps, Figure 6.8 and Figure 6.9 show that AODVUU when compared to MOPR-AODVUU, causes less routing overhead and less routing overhead ratio, while MOPR-AODVUU guaranties a small improvement in terms of packet delivery ratio and delay as shown in Figure 6.10 and Figure 6.11 respectively. Over 1.5 Mbps, both protocols converge to almost same values in terms of routing overhead and routing overhead ratio, when MOPR-AODVUU gets more advantages in terms of delay and packet delivery ratio when compared to AODVUU.

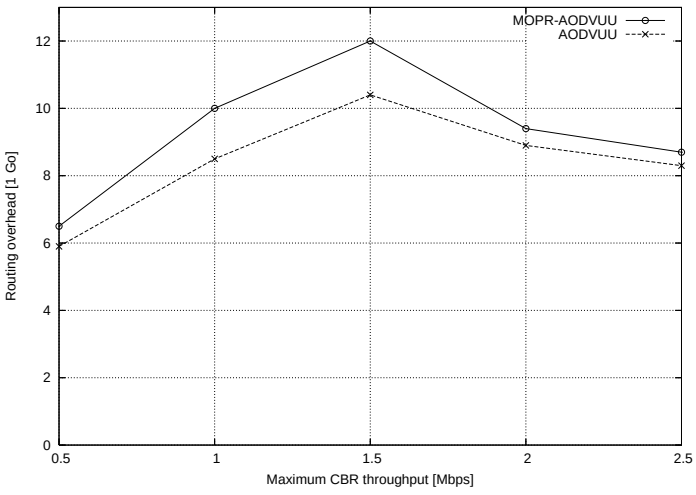

Figure 6.8: Routing overhead versus the maximum CBR throughput.

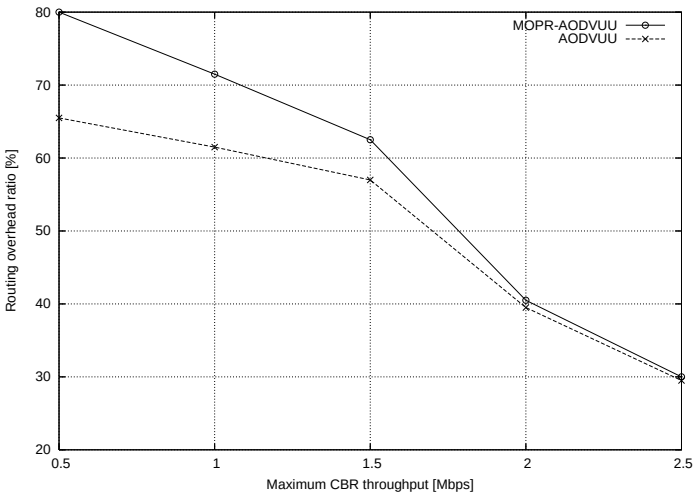

Figure 6.9: Routing overhead ratio versus the maximum CBR throughput.

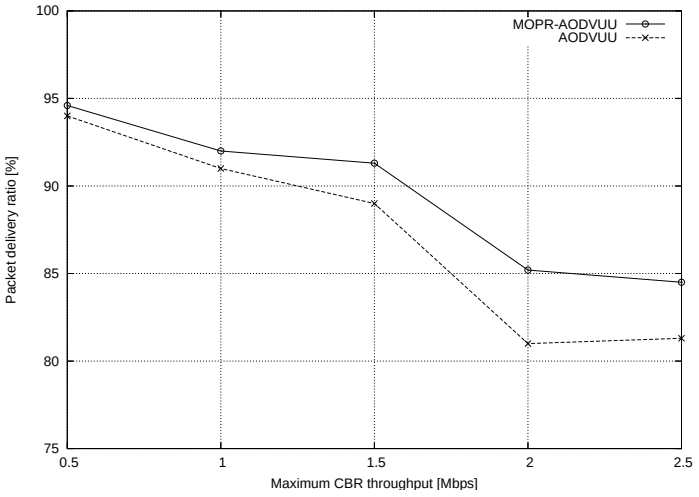

Figure 6.10: Packet delivery ratio versus the maximum CBR throughput.

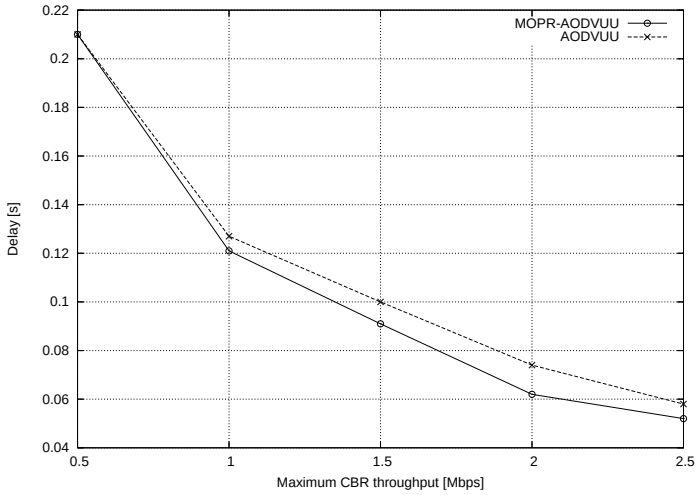

Figure 6.11: Delay versus the maximum CBR throughput.

All those simulation results show that, with increasing little bit the global data size of the whole control packets sent in the air, our algorithm improves the AODV-UU in terms of transmission quality. By decreasing the transmission link failures during the transmissions, the number of the retransmissions, and the data loss rate, it directly improves the delay and the packet delivery ratio in the whole network. Those improvements are very important for vehicular communications established by real-time applications.

In the following section we investigate the reaction of proactive routing with MOPR.

6.2.2 Proactive Data Routing Scheme

As a proactive routing example for the application of our concept we have chosen the Optimized Link State Routing (OLSR) Routing Protocol [17]. OLSR is a proactive link-state routing protocol that floods a full topology table to all nodes in the network which then compute optimal forwarding Routes locally. The main feature of OLSR is the building of a sub-graph connecting all nodes in the network in order to reduce the overhead of broadcast control message while reaching all nodes in the network. The route discovery is done through the exchanging of control messages called Topology Control (TC) messages, that allows each node in the network to have a global view on the whole network topology, then to build its routing table.

Mainly, OLSR works in two steps: Multi-Point Relay (MPR) nodes selection and routing table construction. In the first step, each node in the network selects as MPRs the shortest set of one-hop neighbors that covers all its two-hop neighbors. These MPR nodes are used for flooding the network with control messages. In the second step, each node communicates through TC messages the list of its one-hop neighbor nodes that have selected it as MPR. By receiving TC messages from different nodes in the network, a global topology information can be built locally, from which a routing table is then computed providing one route to each node in the network. For more detail on OLSR functionality, please refer to Chapter 3.

In Chapter 5 we have explained that two ways are possible to share the movement information in the neighborhood: by using the routing control packets or by using some special

system running at the network layer. Here, we are in a proactive context, thus if we use the routing control packets to do that, we will increase to much the routing overhead. Thus, we prefer to use some separate system in that case, like MHVB [63, 64]. But even that, we explain in follow how routing control packets can help in sharing the movement information in the neighborhood.

In OLSR, and most proactive routing protocols, each node in the network periodically send a Hello message to tell its neighbors about his presence. In OLSR, this Hello message contains the ID of the node who sends it with a list of its MPR Selectors. We propose that each node adds its own movement information in this Hello message before broadcasting it. By doing that, we make the movement information periodically shared in the one-hop neighborhood.

The enhancements of OLSR routing protocol using the MOPR concept have been conducted during its two main operation steps; mainly, the MPRs selection and the routing table construction phases. In the follow we explain in detail how these two phases have been improved, thanks to MOPR.

6.2.2.1 MOPR-based MPRs selection

As specified in the IETF RFC 3626, within OLSR a node in a one-hop neighborhood will be first selected as MPR if it covers more neighbors in the two-hops neighborhood. This basic heuristic reduces as much as possible the number of nodes in the MPR sets used for flooding the entire network, so that to enhance the overhead of the protocol. However, as the mobility of a node with the regard to the mobility of nodes in its MPR set is not taken into account, the latter heuristic may lead to non-stable links in the MPR graph used for the broadcasting of control messages.

In our proposal, the neighbor node having the best relative stability is the first selected as MPR even if it covers less neighbors in the two-hops neighborhood than another potential MPR node. We propose two ways for selecting MPRs based on MOPR: (1) MPRs are selected based only on the one-hop LS information, or (2) MPRs are selected based on both one-hop and two-hop LS information. In the following we explain in more detail how these two different MOPR-based MPRs selection ways are achieved.

6.2.2.1.1 MOPR one-hop-based MPRs selection Suppose we have a small network, with i one of nodes in that network. We have:

- $NB1hop(i)$: a set of all vehicles within the one-hop neighborhood of the vehicle i.
- $r(i)$: number of vehicles in $NB1hop(i)$.
- $GlobLS(i,j) \in [0,1]$: Global stability to the link $[i,j]$ that is the main criteria on which MOPR is based during the MPRs selection phase.

In our proposal, during the MPRs selection process, the node i first calculates for each neighbor j the global link stability $GlobLS(i,j)$, with $j \in NB1hop(i)$ as follow:

$$GlobLS(i,j) = LS(i,j)\frac{r(j)}{\sum_k r(k)} \tag{6.1}$$

with $k \in NB1hop(i)$

Finally, it selects as first MPR the neighbor j corresponding to the biggest $GlobLS(i,j)$.

6.2.2.1.2 MOPR two-hops-based MPRs selection Suppose we have the same network as above, with i one of nodes in this network. We have:

- $NB1hop(i)$: a set of all vehicles within the one-hop neighborhood of the vehicle i.
- $NB2hop(i)$: a set of all vehicles within the two-hop neighborhood of the vehicle i.
- $GlobLS(i,j) \in [0,1]$: Global stability to the link (i,j). And it is the main criteria which MOPR is based on in its MPRs selection.

In this implementation we do not consider the LS information of only the one-hop neighbors, but as well those of the two hops neighbors. Therefore, to select its MPRs set, the node i first calculates for each neighbor j the $GlobLS\,(i,j)$ as follows:

$$GlobLS\,(i,j) = LS(i,j)\frac{\sum_k LS\,(j,k)}{\sum_{l,m} LS\,(l,m)} \tag{6.2}$$

$$with \begin{cases} k \in NB1hop(i) \\ l \in NB1hop(i) \\ m \in NB1hop(l) \end{cases}$$

Finally, i selects as first MPR the candidate j corresponding to the biggest $GlobLS\,(i,j)$.

In 6.2, $LS\,(i,j)$ is locally available, thanks to the neighborhood movement information sharing system. But, $LS\,(j,k)$ which is the LS corresponding to a two-hops communication link is not locally available. Thus, we need some additional functionality to make this information available locally. For that, we propose that each node in the network to add to to each neighbor entry in its Hello messages the corresponding LS. By doing that, when receiving a Hello message from a node i, the node j, additionally to the movement information of i, gets the list of all one-hop neighbors of i with their corresponding LS information.

By applying MOPR, with both the one-hop and the two-hop based MPRs selection, the selected MPRs should be the most stable and guarantee the longest communication lifetime.

6.2.2.2 MOPR-based routing table construction

The objective of this phase is to build a routing table in each node which contains the most stable routes in terms of communication lifetime.

Within OLSR a TC message is periodically disseminated in the whole network through the MPR nodes. This TC message should contain a list of all one-hop neighbors' IDs that selected i as MPR.

Within MOPR-based OLSR, we propose that each node in the network adds to each entry (neighbors' ID) in its TC message the corresponding $GlobLS$ and then disseminates it. When receiving TC messages from all nodes in the network, a node is able to build a global topology network, with a $GlobLS$ information corresponding to each topology link (entry).

The routing table is directly built from the information given in the topology network table, in which the MOPR stability metric ($GlobLS$) is present. Thus, the routes proposed in this routing table should be the most stable in terms of communication lifetime.

In Figure 6.12 a simple example is showing how a most stable Route is selected based on MOPR. We have 10 nodes (0 to 9). Suppose that all nodes in two-hop distance regarding to

node 0 have already an available route to reach 0. Now, the node 8, for example, has choices between three routes to reach the node 0: through 4, through 5, or through 6. Among these different routes, the node 8 should selects the most stable one in order to guarantee the selection of the most stable route to reach 0. As you can see, nodes 4, 5, and 6, have different routes to reach 0 with respectively the different route stability: $RS\,(4,0) = 0.9$, $RS\,(5,0) = 0.7$, and $RS\,(6,0) = 0.6$. Node 8 has different $GlobLSs$ in regard to its neighbors 4, 5, and 6, respectively $GlobLS\,(8,4) = 1$, $GlobLS\,(8,5) = 0.9$, and $GlobLS\,(8,6) = 1$. Therefor, the best route in terms of communication lifetime that MOPR selects for 8 to reach 0 is the route passing trough 4. This selected route has the biggest Route Stability ($RS\,(8,0) = 0.9$) when compared to others. With:

$$RS\,(8,0) = Min\,(GlobLS\,(8,4)\,, RS\,(4,0)) = Min\,(1.0, 0.9) = 0.9$$

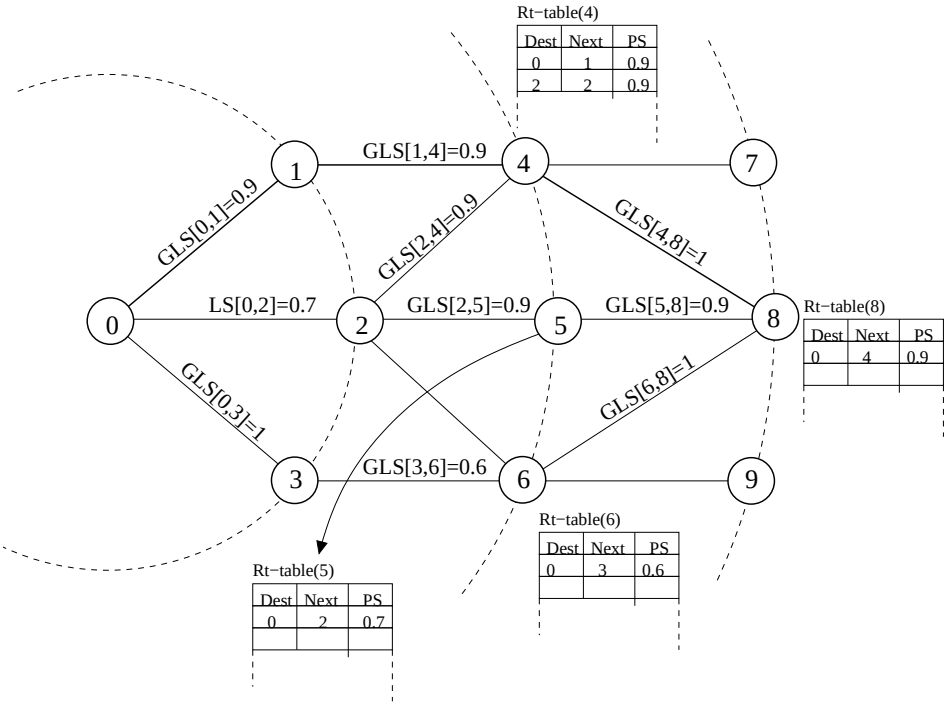

Figure 6.12: MOPR-based routing routes selection example.

As a result, the periodically updated routing table, when built based on MOPR, guarantees the best choice of to any destination by selecting the most stable routs among the available ones. In following section we present some simulation results that we have got by mean of simulations.

6.2.2.3 Simulations

We have applied MOPR to OLSR under the network simulator ns2 [66]. We considered as ns2 implementation of OLSR the one proposed by University of Murcia (UM-OLSR) [68],

which is well compliant with the OLSR RFC 3626. We name the MOPR-based OLSR implementation as MOPR-UMOLSR, and the basic implementation of OLSR as UMOLSR. The MOPR-UMOLSR implementation combines both MOPR two-hop-based MPRs selection and MOPR-based routing table construction. We suppose each node in the network has locally available the movement information of all its one-hop neighbors.

6.2.2.3.1 Simulation environment and scenario description We have considered a highway-like scenario as shown in Figure 6.13. We have 200 nodes (vehicles) moving along five km (5000 m) length highway. In each direction on this highway we have three lanes with different speed ranges, respectively: (lane1: 50-80 Km/h, lane2: 70-100 Km/h, lane3: 100-130 Km/h). In each direction we have a density of 5 vehicles every 150 m.

The maximum radio propagation rang is set to 250 meters, and the classical 802.11 Medium Access Control (MAC) functionality are used, i.e. Distributed Coordination Function (DCF), Carrier Sense Multiple Access with acknowledgments (CSMA/CA with ACK) and Request-To-Send Clear-To-Send (RTS/CTS), and fragmentation, even if we suppose the messages are enough small. Traffic type is CBR, and the two transmitting source and destination couple were selected randomly along the lane corresponding to the speed range 70-100 km/h.

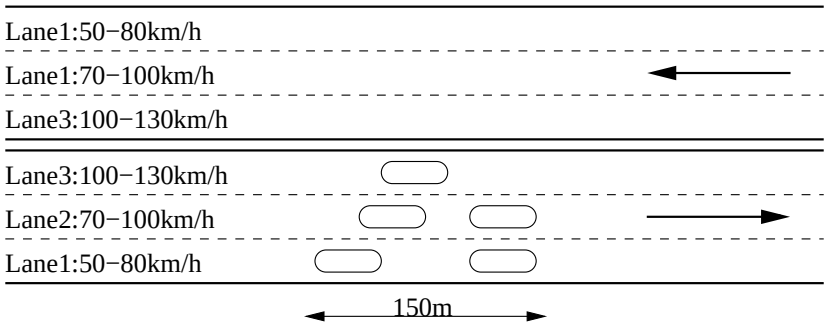

Figure 6.13: the highway scenario used for our ns2 simulations.

6.2.2.3.2 Simulation results and analysis The simulation results we have obtained by 1000 simulation runs and 95% of confidence interval are presented in follow.

The metrics studied are the following:

- **Packet Delivery Ratio:** defined as the number of correctly received packets at the destination over the number of packets sent by the source.
- **Routing Overhead:** defined as the number of bytes injected in the network by the routing protocol.
- **Routing Overhead Ratio:** defined as correctly received packets (in bytes) at the destination over the routing overhead (in bytes).
- **End to End Delay:** defined as the duration time that a packet takes to go from the source and arrive to the destination.

All graphs presented in this section show the simulation results we have obtained as a function of the maximum CBR packet size. The MOPR-UMOLSR performances are compared to those of UMOLSR.

In Figure 6.14, we see that MOPR-UMOLSR improves UMOLSR in terms of packet delivery ratio till the maximum CBR packet size reaches 1536 bytes, and that with keeping almost the same delay as shown in Figure 6.15. After 1536 bytes of maximum CBR packet size, it seems that MOPR-UMOLSR suffers little bit vs. UMOLSR in terms of delay, while guaranteeing almost the same packet delivery ratio.

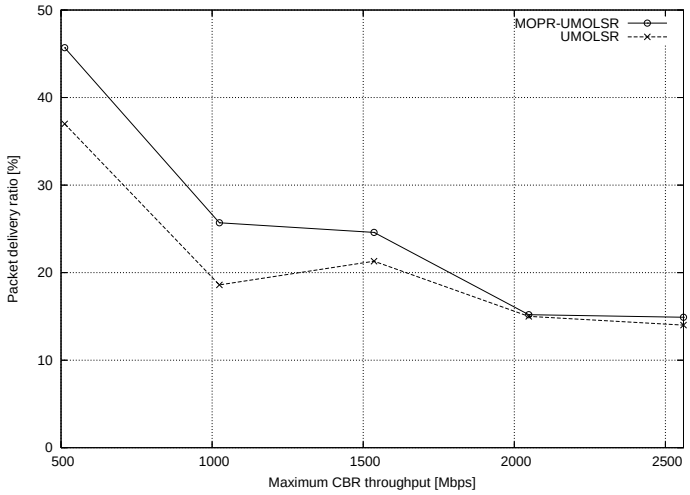

Figure 6.14: MOPR-OLSR vs OLSR in terms of packet delivery ratio.

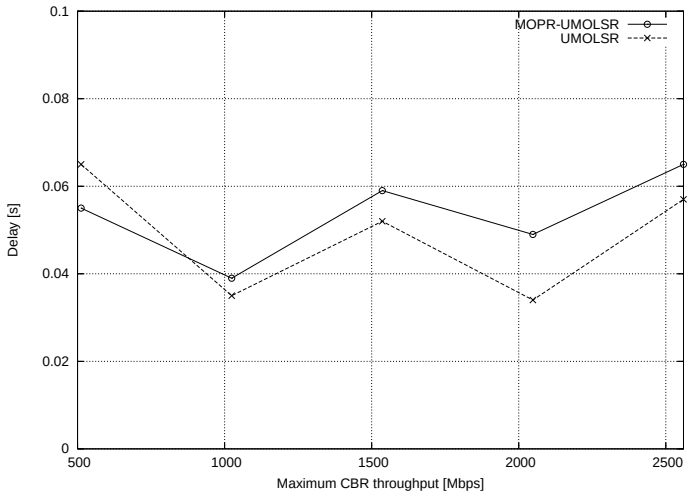

Figure 6.15: MOPR-OLSR vs OLSR in terms of delay.

In Figure 6.16 we see that MOPR-UMOLSR increases a little bit the routing overhead compared to UMOLSR, which is logical since the size of the TC messages is larger within MOPR-UMOLSR. But that is not bad since the routing overhead ratio, as shown in Figure 6.17, is almost the same for both MOPR-UMOLSR and UMOLSR.

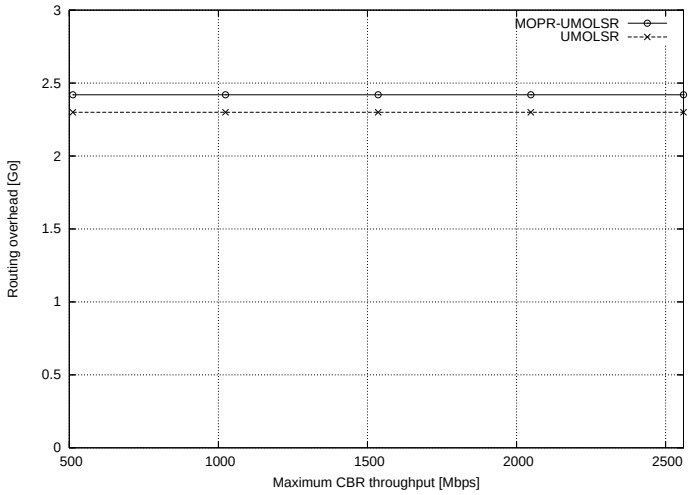

Figure 6.16: MOPR-OLSR vs OLSR in terms of routing overhead.

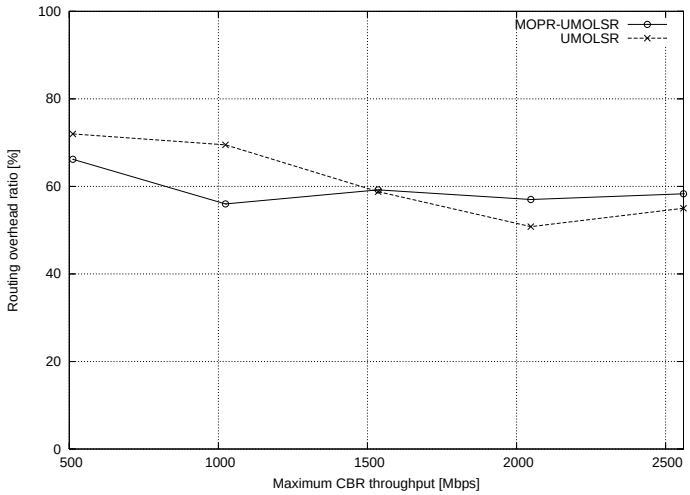

Figure 6.17: MOPR-OLSR vs OLSR in terms of routing overhead ratio.

After having shown in the previous Section the improvements on the network performances that MOPR can bring to reactive unicast routing, in this Section we have shown that MOPR improves the proactive routing as well. Thus, we have presented some promising ns2 simulation results, showing that MOPR improves the routing performances, mainly in terms of packet delivery ratio, in both reactive and proactive routing. Now, in the following section we present how MOPR can be used to improve position-based data routing in vehicular networks.

6.3 MOPR for Position-based Data Routing Schemes

Researchers working on the field of C2C/C2I communications, as in the European consortium: C2C-CC [1], believe that data routing in such networks should be based on geographic location of nodes. Extensive simulation study based on realistic vehicle movement patterns have been

done in [21] to investigate how topology-based approaches comparing to a location-based routing schemes when applied to vehicular networks. And this study shows clearly the no suitability of topology-routing schemes for vehicular networks, when compared to location-based routing schemes.

Therefore, after having shown how MOPR can improve the performances of VANETs when using a topology-based routing schemes, we have applied it to a location-based data routing scheme. As location-based routing protocol for the application of our concept, we have chosen the well known Greedy Perimeter Stateless Routing (GPSR) [35] with using HLS [28] as location service. For performances comparisons, we have considered the generic GPSR, the MOPR-based GPSR (say MOPR-GPSR), and another MOvement-based Routing Algorithm (MORA) [69].

6.3.1 MOPR-based GPSR

The GPSR protocol is described in detail in Section 3.4, but let us give a short overview of its main functionality. To enable position-based routing, a node is supposed to be aware about the physical location of all nodes located in its neighborhood. It must also be able to discover the physical location of the node it wants to communicate with, a task which is typically accomplished by some location service, as the Hierarchical Location Service (HLS) [28]. In the rest of this section, we consider GPSR as the position-based routing with using HLS as location service.

Within GPSR, when having some data to send to "D", a node "S" sends them through some intermediate nodes based on greedy forwarding. The next forwarder is selected among neighbors with positive progress to the destination, based on the physical location of both the forwarder candidate and destination node "D".

As shown in Figure 6.18, node "S" selects as next forwarder the node "i" instead of node "j", since it is the closest neighbor to the destination "D" ($Distance1 < Distance2$). So, the sender selects as next forwarder the closest neighbor to the destination which a positive progress.

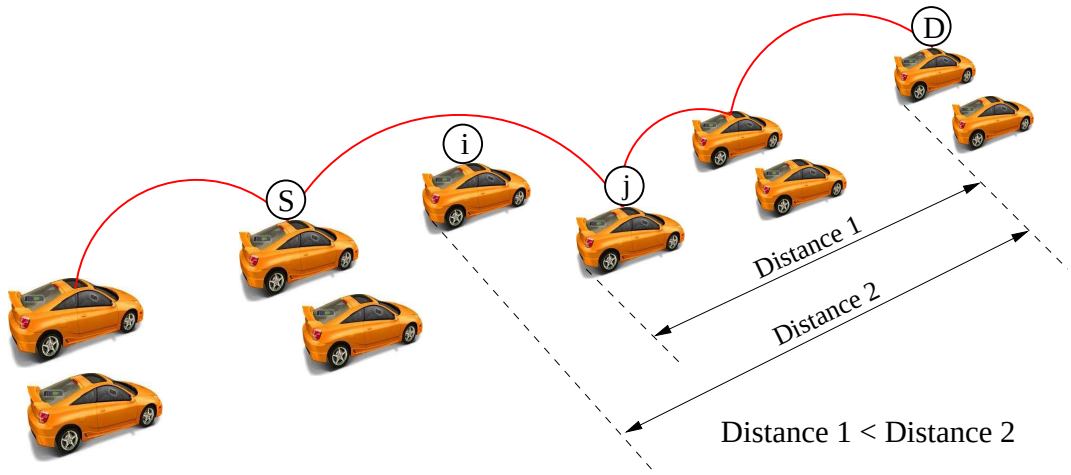

Figure 6.18: GPSR functionality: example.

In fact, there are mainly three different strategies for determining to which next-hop neighbor a given packet has to be forwarded:

- Most Forwarding within R radios (MFR) transmits packets to the neighbor closest to the destination in order to minimize the number of hops to the destination.
- Nearest with Forwarding Progress (NFP) transmits packets to the nearest neighbor of the sender which id closer to the destination.
- In Compass Routing, packets are forwarded to the neighbor closest to the straight line between the sender and destination.

Therefore, the next forwarder selection in its basic functionality is based only on distances comparison. These distances are calculated based on position information only, without considering the movement information. What happens if the selected node goes out the communication range just after having been selected or even during the transmission? The packet will get lost and a new next forwarder should be found, and some times even the destination location is recalculated. All this consume resources and reduces the performances of the network.

To avoid this situation, or at least to reduce such situations as much as possible, we propose to consider not only the position information of involved nodes, but their movement information as well. Instead of selecting as next forwarder among nodes with positive progress to the destination the one which has the shortest distance to this destination, we propose to select the most stable in terms of communication lifetime.

Let us consider the example in Figure 6.19, in which we show how the next forwarder node is selected based on MOPR in GPSR, or any other position-based routing protocol.

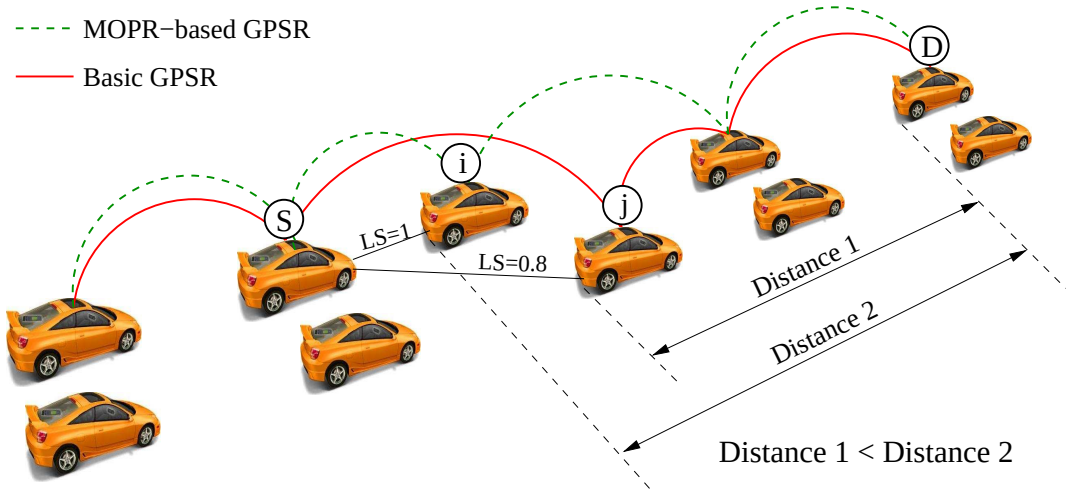

Figure 6.19: MOPR-based next forwarder selection.

The sender "S" gets from MOPR a *LS* information for each node in its one-hop neighborhood. Based on this LS information, the next forwarder is selected when applying MOPR. Here, "S" selects "j" as next forwarder instead of "i", because "j" is more stable than "i" (i.e., the *LS* corresponding to "j" is higher than that corresponding to "i").

One of the main characteristics of GPSR is its perimeter system (see Section 3.4 in Chapter 3). The greedy forwarding fails when there is no candidate neighbor with positive progress to the destination, which is caused when meeting a hole (e.g., because of obstacles). In such situation, GPSR uses a perimeter system to forward the packet around the hole until reaching

the destination or some intermediate node which has a next forwarder candidate. For the moment our proposal does not consider this situation, and when a such situation happens we switch to the basic GPSR.

In follow we present very promising results we have obtained when simulating an implementation of GPSR to which we have applied MOPR.

6.3.2 Simulations

To improve the performances of position-based routing protocols performances in VANETs based on movement information, F. Granelli et all. have proposed in [69] a Movement-Based Routing Algorithm (MORA) for vehicular ad hoc networks. In contrast to MOPR, movement information in MORA refer to movement direction only. MORA takes into account the physical location of neighboring vehicles and their movement direction when selecting the next hop for sending/forwarding packets. More details about MORA can be found in [69]. We believe that considering only the position and the movement direction is not enough for a best next forwarder selection in VANETs. The vehicles driving speed is important and should be taken into account as well. A vehicle which is almost going out the communication range should not be selected as a next forwarder, which can not be guaranteed without considering the speed.

We have simulated under the network simulator ns2 [66] the GPSR routing protocol with MOPR applied to it. For the simulation results comparison, we consider the generic GPSR implementation (refereed as GPSR), the MOPR-based GPSR implementation (say MOPR-GPSR), and the MORA-based GPSR implementation (refereed as MORA).

6.3.2.1 Simulation environment and scenario description

For our simulations we have considered a highway-like scenario as shown in Figure 6.20. We have 200 nodes (vehicles) moving along five km (5000 m) length highway. In each direction we have three lanes with different speed ranges starting from a minimum speed value of 70 km/h and a maximum speed value which we increase from 120 to 220 km/h. In each direction we have a density of 5 vehicles every 150 m.

We have used the classical 802.11 Medium Access Control (MAC) functionalities, i.e. Distributed Coordination Function (DCF), Carrier Sense Multiple Access with acknowledgments (CSMA/CA with ACK) and Request-To-Send Clear-To-Send (RTS/CTS), and fragmentation, even if we suppose the messages are enough small. Traffic type was CBR with 1024 Bytes of packet size and a 512 bps of maximum CBR rate. One transmitting source and destination vehicles are selected randomly along the middle lane (Normal vehicles' lane) in each direction.

6.3.2.2 Simulation results and analysis

The simulation results we have obtained by 1000 simulation runs and 95% of confidence interval are presented in follow.

The metrics studied are the following:

- **Packet Delivery Ratio:** defined as the number of correctly received packets at the destination over the number of packets sent by the source.
- **Routing Overhead:** defined as the number of bytes injected in the network by the routing protocol.

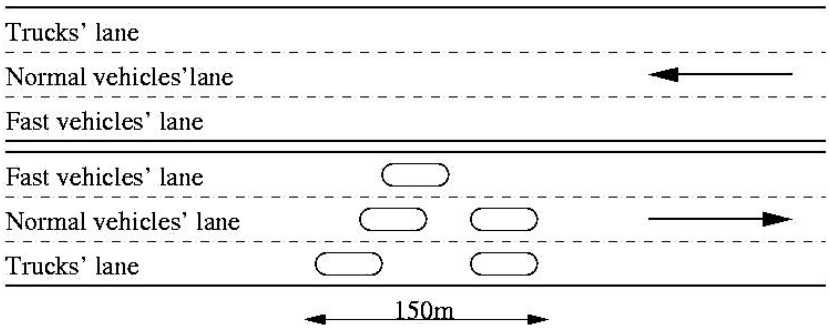

Figure 6.20: the highway scenario used for our ns2 simulations.

- **Routing Overhead Ratio:** defined as correctly received packets (in bytes) at the destination over the routing overhead (in bytes).
- **End to End Delay:** defined as the duration time that a packet takes to go from the source and arrive to the destination.

Figure 6.21 shows the Packet Delivery Ratio (PDR) obtained for each routing protocol as function of vehicles' maximum speed. It is clearly shown that both MOPR and MORA guarantee a better PDR when compared to the basic GPSR. As shown, higher the vehicles' maximum speed, higher the PDR of MOPR when compared to MORA. This means that MOPR guarantees the best PDR when the vehicles speed is higher.

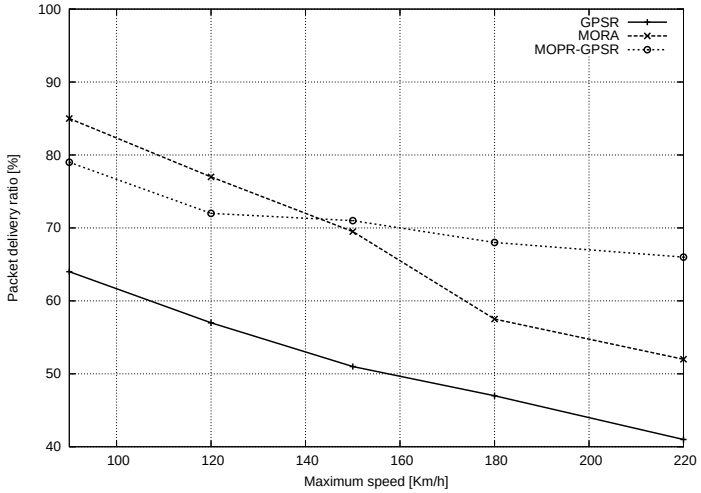

Figure 6.21: Packet delivery ratio comparison between GPSR, MOPR, and MORA.

Figure 6.22 shows the delay for each routing protocol as function of vehicles' maximum speed. And as you can see, MOPR improves the delay by at least two times when compared to both basic GPSR and MORA.

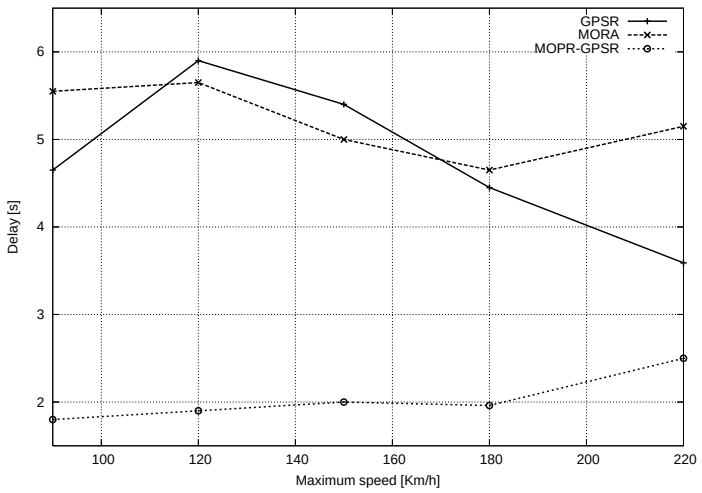

Figure 6.22: Delay comparison between GPSR, MOPR, and MORA.

Figure 6.23 shows the routing overhead as function of vehicles' maximum speed. MOPR decreases the routing overhead when compared to basic GPSR, but MORA decreases the routing overhead more. That means that MORA is the best in terms of routing overhead. But, in Figure 6.24 you can see the HLS overhead caused in the network which should be taken into account to evaluate the the real performance of our routing protocols in terms of routing overhead. And it is clearly shown that MOPR is the best in terms of HLS overhead when compared to both basic GPSR and MORA.

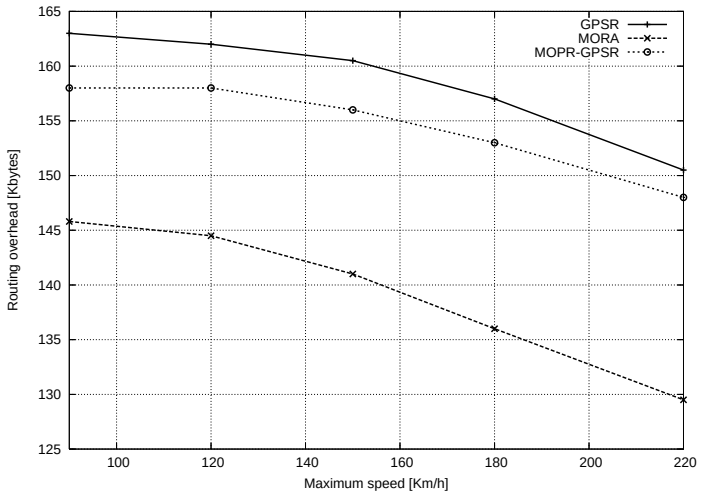

Figure 6.23: Routing overhead comparison between GPSR, MOPR, and MORA.

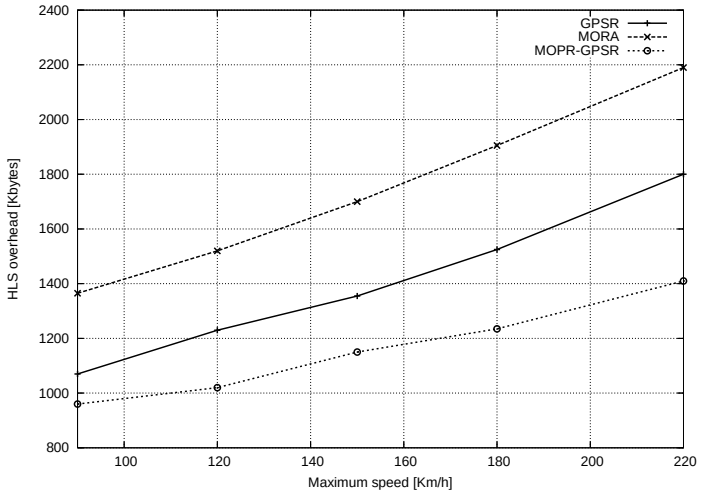

Figure 6.24: HLS overhead comparison between GPSR, MOPR, and MORA.

To evaluate the performance of any routing protocol in terms of routing overhead, it is important to look to the Routing Overhead Ratio (ROR). Figure 6.25 shows the ROR caused in our network while taking into account only the routing overhead (i.e. without counting the HLS overhead). It is clearly shown that both MOPR and MORA improve the ROR when compared to basic GPSR. And MOPR shows an almost stable ROR compared to MORA which increases when the maximum speed increases.

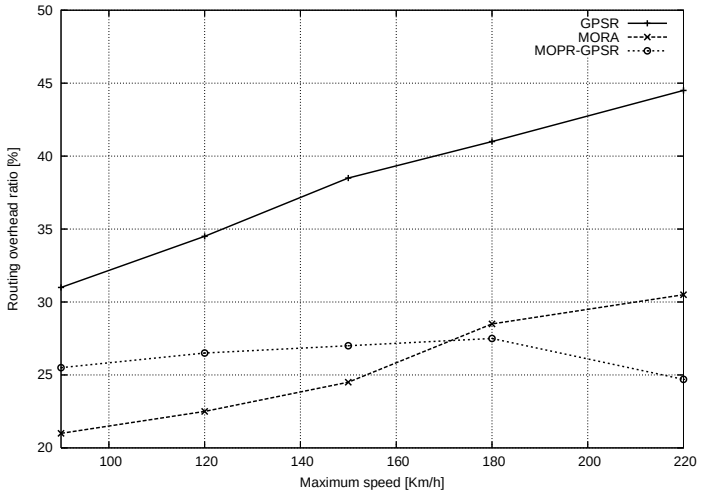

Figure 6.25: Routing overhead ratio comparison between GPSR, MOPR, and MORA.

The ROR is important, but in such kind of routing protocol, the global ROR (while taking into account the HLS overhead as well) is more important. Figure 6.26 shows clearly how

MOPR improves the network performance in terms of global ROR by about two times when compared to both basic GPSR and MORA.

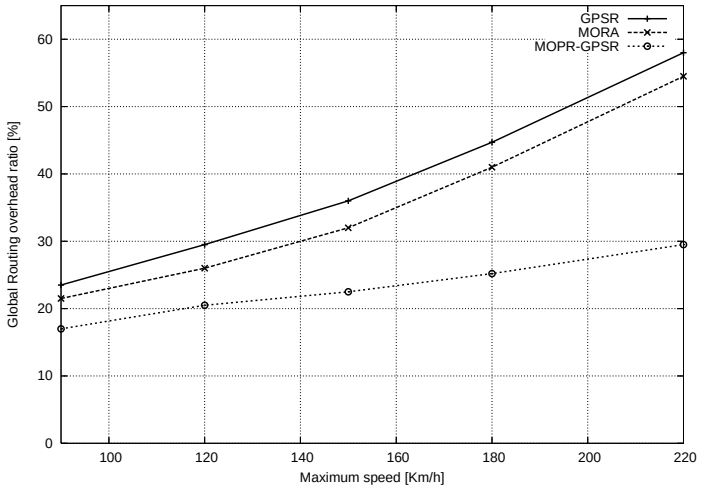

Figure 6.26: Global routing overhead ratio comparison between GPSR, MOPR, and MORA.

All simulation results presented here show that MOPR improves the routing performances from all sides. Consequently, MOPR shows a big potential with position-based routing in VANETs.

6.4 Chapter Summary

In the first section of this chapter we have presented the application of our MOPR concept to the two topology-based routing protocols: AODV as reactive protocol and OLSR as proactive protocol. We know very well that such kind of routing is not the best choice for vehicular networks where the network topology changes very often and very fast. But, we wanted from these applications just to know the performance of our approach with such routing schemes. Of course we did not stop there, and we have investigated the enhancements that MOPR may add when applied to position-based routing schemes, which are up to now the most promising schemes for vehicular ad hoc networks.

We have shown very interesting and promising results that we have got by mean of simulations. The results we have got from the application of MOPR to topology-based routing protocols were interesting but not enough good, but the situation was not the same with the application of MOPR to position-based routing scheme, where the simulation results are largely more interesting and more promising.

As future works, we want to go from theoretical implementation of MOPR to real implementation. In Chapter 5 we present a first step of this future works, with few preliminary results.

Chapter 7

MOPR-assisted Medium Access Control in VANETs

7.1 Introduction

From Chapter 4 we conclude that existing MAC solutions, initially proposed for MANETs, do not guarantee enough reliability in terms of network performances, specially when the topology changes very fast and very often such as in VANETs. We believe that the main feature of such networks (nodes' movement pattern) should be taken into account when managing the access to the medium. In chapter 6 we have shown how MOPR, based on the movement information of vehicles, can improve the data routing performances in VANETs. We believe that this same concept can be used to improve the performances of the network at the MAC layer. And this is what we show in this chapter.

The relative speed of neighbors as seen by a node are different, and some times even very different. So, each neighbor spends a different duration time in the communication range of a neighbor node. This difference can be more important when nodes move faster, like in VANETs where nodes are vehicles. Sometimes, this difference concludes in some discrimination between nodes when attempting to access the medium. For example, if we have two neighbor vehicles driving with different speeds on a road, and both of them are crossing at almost the same time some common area covered by the communication range of a common neighbor (moving or a static vehicle, or even some roadside unit). The vehicle which drives faster will spend less time in the communication range of the common neighbor, thus, it will get less chance to communicate with it when compared to the other vehicle which drives with a lower speed. To avoid such discrimination, the neighbors' movement prediction (MOPR) can play a big role. Based on MOPR, we can predict the duration time each neighbor is going to stay in the communication range. Thus, we are able to give more advantage when trying to access the medium to nodes leaving the communication range sooner. The main idea behind this proposal, which we call MOPR-assisted MAC, is to give more chance when attempting to access the medium to a node which has the lower Link Stability (LS) metric (if the MaxLifetime is equal to all nodes in the network).

Our MOPR-assisted MAC concept may be applied to any MAC protocol, but in this chapter we focus only on the IEEE 802.11 DCF since it seems the main potential MAC layer to be used for C2C and C2I communications. MOPR may improve the performances of the IEEE 802.11 DCF by offering a positive discrimination at the level of the Contention Window

(CW) determination, where neighbors corresponding to lower LS will get a lower CW value.

The remainder of this chapter is organized as follows. First, in Section 7.2 we review the IEEE 802.11 MAC mechanism, and in Section 7.3 we present our MOPR-based MAC. And then, in Section 7.4 we present the performances of our contribution through simulations. Finally, in Section 7.5 we provide a summary of this chapter.

7.2 IEEE 802.11 MAC layer

The MAC layer mechanism used by the IEEE 802.11 Wireless LANs (WLANs) [52] is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which is provided by the Distributed Coordination Function (DCF). If contention-free service is required, it can be provided by the Point Coordination Function (PCF), which is built on top of the DCF. The contention free services are provided only in networks with centralized infrastructures. The carrier sensing is used to determine either the shared medium is free for use or already in use by another candidate terminal in the neighborhood. It can be managed into two manners: physical carrier sensing or virtual carrier sensing.

- The physical carrier sensing function is provided by the physical layer, where the radio channel is sensed physically. This method needs specific hardware and can not overcome the hidden terminal problem since the hidden terminal can never been heard physically.
- The virtual carrier sensing is provided by the Network Allocation Vector (NAV). As showed in Figure 7.1 . The NAV is a timer that indicates the duration time of a transmission. Each terminal, should indicate the amount of time it is expected to use the medium. Terminals in its neighborhood count down the corresponding NAV from this amount of time until zero. The carrier sensing function indicates the medium as busy until the NAV reaches zero.

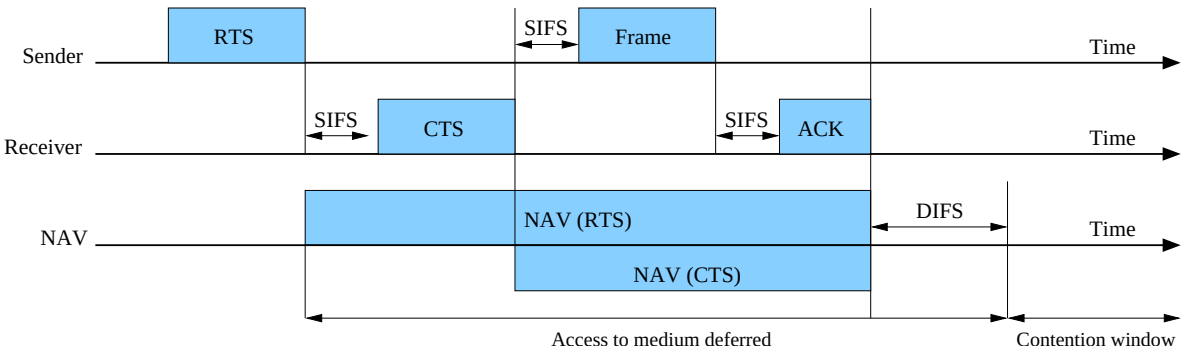

Figure 7.1: Virtual carrier sensing by the NAV.

The IEEE 802.11 WLANs uses some interval spaces named Inter Frames Spacing (IFSs). These IFSs are set between each two successive transmission frames in order to coordinate the access to the common transmission medium. All time interval are integral multiples of slot times, which are chosen judiciously using propagation delay, delay in the transmitter, and

other physical layer dependent parameters. The IEEE 802.11 uses four different IFSs as shown in Figure 7.2. Having different IFSs makes able the possibility to have different priority levels for different types of traffic. Which means, after the medium becomes idle, traffics with lower priority wait more than traffics with higher priority before attempting to access it.

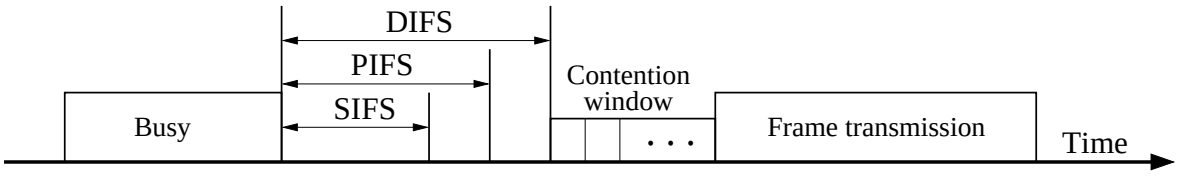

Figure 7.2: Inter-frame spacing in 802.11.

More details on these IFSs are given in follows.

- Short Inter-Frame Space (SIFS) is the shortest inter frame space. It is used for the highest priority transmission, such as RTS/CTS/ACK messages. The medium should be sensed idle for a minimum time period of at least SIFS before any transmission can be done.
- PCF Inter-Frame Space (PIFS) is used for real time services. When the medium has been sensed free of any traffic for a period greater than the PIFS, Stations operating in contention free mode may have immediate access to the medium.
- DCF Inter-Frame Space (DIFS) is longer than a PIFS, and it is used in the case of DCF transmission mode. A terminal can access immediately a medium if it senses it free for a period time longer than DIFS.
- Extended Inter-Frame Space (EIFS) is the longest one, and it is used when an error in frame transmissions occurs.

7.2.1 Medium access mechanism

When having a data packet to send in a IEEE 802.11-based VANET, a vehicle first checks neither the medium is idle or not. If it is sensed to be idle for a duration time of DIFS, the vehicle can transmit. Otherwise, it backs off and attempts again after amount of time chosen within a Contention Window (CW). The CW is set between a CWmin and a CWmax (see next Subsection to understand how the CW size is set).

The IEEE 802.11 MAC layer is principally based on the RTS/CTS/ACK packets exchange as shown in Figure 7.3 and inter-frames spacing as shown in Figure 7.1 and Figure 7.2. A vehicle, when having a data packet to transmit, checks the medium if idle or not. If the medium is sensed idle for a duration time of DIFS, an RTS packet is transmitted including the sender ID and the expected transmission duration time. If the destination vehicle is ready to receive the transmission, when receiving the corresponding RTS packet it waits for a SIFS duration time and then sends back a CTS packet to the sender. Once the sender receives this CTS packet, it waits again for a DIFS duration time and then starts the transmission of the

data packet to the destination. After receiving the data packet, the destination waits for a DIFS time and then sends an ACK packet to the sender, and set its NAV to zero. When receiving the ACK packet, the vehicle sets its NAV to zero. To reduce the risk of collision and the hidden terminal problem, all vehicles that hear the RTS or/and CTS packets, set their NAV according to the information provided in these packets.

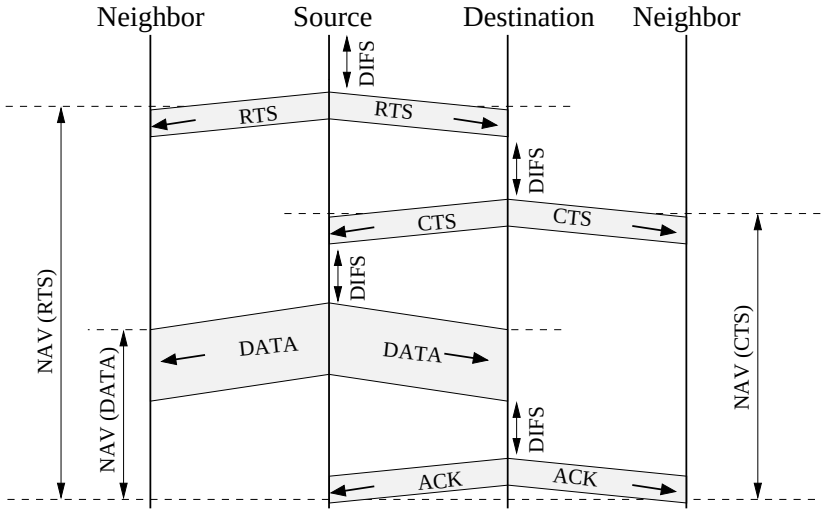

Figure 7.3: Control packets exchange in IEEE 802.11.

Thanks to the RTS/CTS/ACK packets exchange and the inter-frames spaces, 802.11 minimizes the risk of transmission collisions and the hidden terminal problems.

7.2.1.1 Contention Window size

The CW is a window of slot times set between a minimum CW (CWmin) and a maximum CW (CWmax), within which a node chooses randomly its back-off time. This back-off time is randomly chosen to avoid, or reduce, as much as possible the risque of transmission collisions. The CW is set in the beginning randomly between 0 and a CWmin, and after each time a collision occurs it is increased by doubling its size up to a CWmax.

The CW is a very important parameter and should be chosen judiciously. If the CW is too small in size, then the random values chosen by nodes within it will be close to each other which increases the probability of transmission collisions. And if the CW is too large in size, there will be unnecessary delay.Ideally the CW is set depending on the number of nodes attempting to access the medium. The CW size is set to a high value when the number of attempting nodes is high, and it is set to a low value when the number of attempting nodes is low.

The specified values of CWmin and CWmax for both IEEE 802.11b and IEEE 802.11a are given in Table 7.1.

Parameters	IEEE 802.11b	IEEE 802.11a
t_{slot}	$20\,\mu sec$	$9\,\mu sec$
SIFS	$10\,\mu sec$	$16\,\mu sec$
PIFS	$SIFS + t_{slot}$	$SIFS + t_{slot}$
DIFS	SIFS + (2 x t_{slot})	SIFS + (2 x t_{slot})
Operating frequency	$2.4\,GHz$	$5\,GHz$
Maximum data rate	$11\,Mbps$	$54\,Mbps$
CWmin	31	15
CWmax	1023	1023

Table 7.1: IEEE 802.11b and IEEE 802.11a parameters [13].

7.2.2 Toward a IEEE 802.11 physical layer for VANETs

Several IEEE 802.11 standards have been proposed. Each version is dedicated for a specific domain of application and for a specific environment. The most famous versions are the IEEE 802.11b and the IEEE 802.11g, and as well the IEEE 802.11a. Thanks to the large availability in the market of devices based on those technologies. Some versions have been proposed just as extensions or enhancement. The IEEE 802.11i for example, takes care about the security in the network communications, and the IEEE 802.11e takes care on providing a certain QoS in the network.

Both b and g versions of the IEEE 802.11 are very popular, and known under the name of WiFi. Both operate on top of an almost the same MAC layer. Like IEEE 802.11g, IEEE 802.11b uses the unlicensed 2.4 GHz band, where interferences are possible with cordless phones, microwave ovens, wireless IP cameras, and other devices using the same band. Theoretically, IEEE 802.11b data rates can reach 11 Mbps, but in the practice, due to CSMA/CA protocol overhead, it can reach only about 7.5 Mbps.

Wireless devices equipped with IEEE 802.11b and IEEE 802.11g communication technologies are compatible and can communicate each to other. The IEEE 802.11a operates on the 5 GHz frequency band which makes it incompatible with IEEE 802.11b and IEEE 802.11g. Theoretically, the maximum throughput of the IEEE 802.11a is up to 54 Mbps, but the useful one goes up to 25 Mbps at most. The 5 GHz band lets 802.11a to have the advantage of less interferences, but unfortunately, it does not let it to penetrate walls and other obstacles.

IEEE 802.11g can reach the same higher bit rate technology as IEEE 802.11a, that lets it to operate at a maximum raw data rate of 54 Mbps, which is about 25 Mbps maximum net throughput. IEEE 802.11g and IEEE 802.11b are compatible and can work together. Super G is a new proprietary feature used by some products in the market, it allows network speed to reach up to 108 Mbps by using the channel bonding over the IEEE 802.11g, that can bond two 20-MHs channels together.

7.2.3 WAVE (IEEE 802.11p)

As said above, an IEEE 802.11 working group is working on a new PHY/MAC amendment of the 802.11 standard, named IEEE 802.11p, and as well referred as Wireless Access in Vehicular Environments (WAVE) [70]. From the official IEEE 802.11 Work Plan predictions, the approved 802.11p amendment is scheduled to be published during of 2009. It should deal

with the Intelligent Transportation Systems (ITS) applications requirements, including data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). Requirements for this amendment are mostly coming from vehicular Active Safety concepts and applications (Vehicle to Vehicle (V2V) or from Vehicles to Infrastructure (V2I)), where reliability and low latency are extremely important [1]. The IEEE 802.11p is a part in the architecture defined by the IEEE 1609 standards family [71], which consists, following the annual report of the US DOT [72], of four standards as follows:

- **IEEE 1609.1** - *Resource Manager* specifies the services and interfaces of the WAVE Resource Manager application. It describes the key components of the WAVE system architecture and defines data flows and resources at all points. It also defines command message formats and data storage formats that must be used by applications to communicate between architecture components, and specifies the types of devices that may be supported by the On Board Unit (OBU) resident on the vehicle or mobile platform.
- **IEEE 1609.2** - *Security Services for Applications and Management Messages* defines secure message formats and processing. This standard also defines the circumstances for using secure message exchanges and how those messages should be processed based upon the purpose of the exchange.
- **IEEE 1609.3** - *Networking Services* defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange. It also defines Wave Short Messages, providing an efficient WAVE-specific alternative to IPv6 (Internet Protocol version 6) that can be directly supported by applications. Further, this standard defines the Management Information Base (MIB) for the WAVE protocol stack.
- **IEEE 1609.4** - *Multi-Channel Operations* provides enhancements to the IEEE 802.11 Media Access Control (MAC) to support WAVE operations.

In terms of MAC operations, WAVE is inspired from both IEEE 802.11a and IEEE 802.11e. The MAC is almost the same and based on CSMA/CA and inter-frames spacing as described above, with considering QoS. Therefore, application messages are categorized into different Access Classes (ACs), where AC0 corresponds to the lowest and AC3 to the highest priority. Within the MAC layer, a packet queue is used in each AC. During the selection of a packet for transmission, the four ACs content internally. The selected packet then contends for the channel using its selected contention parameters. The contention parameters used for the control channel (CCH) are shown in Table 7.2 (Taken from), with $aCWmin = 15$ and $aCWmax = 1023$.

At the PHY layer, WAVE should work around the 5.9 GHz spectrum, with using OFDM technology and providing vehicular wireless communications over distances up to 1000 meters theoretically, while taking into account the environment, i.e. absolute and relative high velocities (up to 200 km/h), fast multi-route finding and different scenarios (rural, highway and city). Figure 7.4 shows the WAVE spectrum allocation in the world. In north America, 70 MHz from 5,855 to 5,925 MHz have been already allocated. In Europe, the European Telecommunications Standards Institute (ETSI) has asked the European Commission to allocate 20 MHz to be used for WAVE-based safety related applications. It seems that instead of 20 MHz,

AC	CWmin	CWmax	AIFS	t_w
0	$sCWmin$	$aCWmax$	9	$264\mu s$
1	$\frac{aCWmin+1}{2} - 1$	$aCWmin$	6	$152\mu s$
2	$\frac{aCWmin+1}{4} - 1$	$\frac{aCWmin+1}{2} - 1$	3	$72\mu s$
3	$\frac{aCWmin+1}{4} - 1$	$\frac{aCWmin+1}{2} - 1$	2	$56\mu s$

Table 7.2: Enhanced distributed Channel Access parameters for the CCH [73].

30 MHz, from 5,875 to 5,905 MHz will be allocated very soon in Europe. One important open issue being in the way to use these 30 MHz in Europe. Shall Europe use as CCH the same 10 MHz as in North America (i.e. 10 MHz from 5,885 to 5,895 MHz), and the rest of the allocated spectrum as service channels (SCHs) ? or shall it uses the all 30 MHz as a CCH since they will be all used for safety-related applications where all transmitted messages has almost the same priority ? This issue is still under discussion in different European projects.

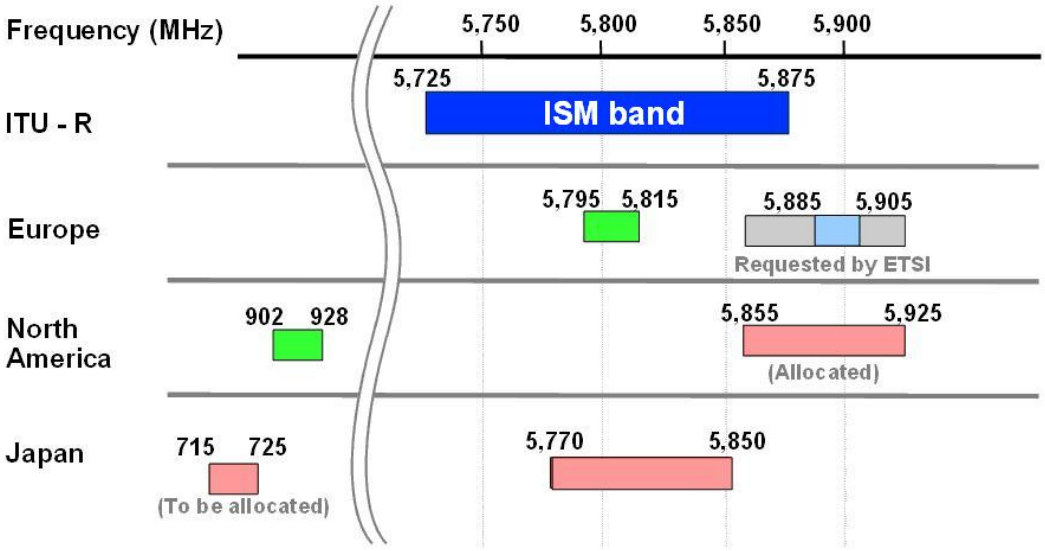

Figure 7.4: WAVE spectrum allocation.

7.3 MOPR-based IEEE 802.11 MAC

In this work we propose MOPR, which considers the movement of the vehicles to attribute a stability metric to each communication link in the network. In this section, we present how this MOPR's output (the LS metric) may be used to improve the performances of the IEEE 802.11 MAC layer. Quality of Service (QoS) notion has been introduced in the 802.11 family through the IEEE 802.11e [75]. This new version in the IEEE 802.11 family brings improvements in terms of QoS relatively to voice and video communication. It uses a new coordination function which defines four Traffic Classes (TC). For example, emails could be assigned to a low priority class, and Voice over Wireless LAN (VoWLAN) could be assigned to a high priority class. We believe that when applied to VANETs, or any other ad hoc network with high node's mobility, considering the movement information of the vehicle in this QoS

scheme is of a high importance. Thus, we propose to use the MOPR output: LS, which depends on the vehicles' movement, as a QoS metric at the level of the IEEE 802.11 MAC. This solution is done by giving more priority in the medium access to a vehicle corresponding to a communication link with lower LS when compared to another candida. And this, by adapting the CW size to the LS metric. This MOPR-based CW adaptation mechanism is described in detail in following Subsection.

7.3.1 MOPR-based CW adaptation

VANETs, because of the ad hoc mode, vehicles should attempt to access the medium to communicate with other vehicles or roadside unites. By using the basic IEEE 802.11 MAC mechanism, all vehicles have the same chance in getting access to the medium since they back-off within the same CW. Even by using the IEEE 802.11e, which offers a certain priority, the priority is set depending to application uses only. What we propose in this work is to set the priority depending on the movement information of vehicles. Again, we believe that the movement information of the vehicles are very important to consider in some situations. For example, let us consider a scenario as shown in Figure 7.5. In this scenario we have two communicating vehicles (respectively "A" and "B") driving closer to a certain communicating roadside unit (say "U"), and both "A" and "B" have the same communication range. The road side unit "U" can be another moving or stationary vehicle as well. We assume that vehicle "A" and vehicle "B" are moving within two different speeds relatively to "U", and "A" has the higher relative speed. Now, suppose that both vehicle "A" and "B" attempts to access the medium to communicate with "U". So, because of their different relative speed, vehicle "A" and the vehicle "B" will not have the same stay time in the communication range of "U", even they enter the communication range at the same time. "A" will have the lower stay time when compared to "B", because it has the higher speed. This makes the chance to get access to the medium for "A" lower than its competitor "B". Thus, to get the same chance in getting the access to the medium in that situation, some discrimination should be applied, by giving some higher priority to "A". Therefore, the movement information should be considered when managing the medium access control, mainly when the network topology changes very fast and very frequently, such as in VANETs.

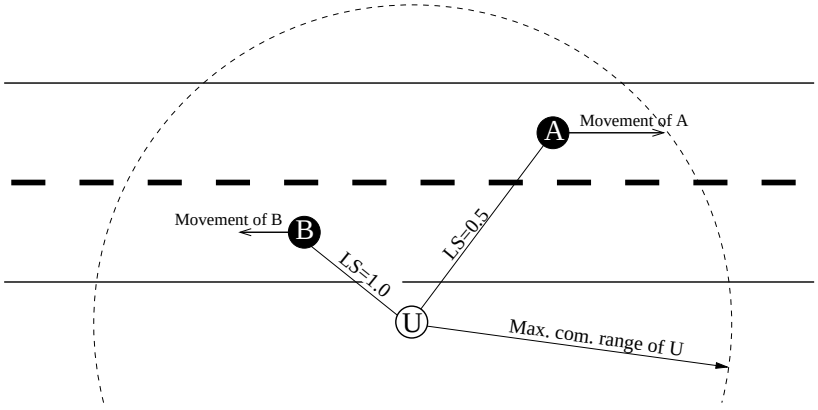

Figure 7.5: Scenario example to motivate the importance of the movement information consideration in MAC.

The MOPR-based LS metric can be used for that purpose. In the same example shown in Figure 7.5, communication link between "A" and "U" gets a lower LS when compared to the communication link between "B" and "U". Thus, to give as much as possible the same chance when accessing the medium, we should give more priority for the vehicle corresponding the the lower LS.

So, what we are proposing in this work is a sort of QoS enhancement for the IEEE 802.11 MAC, by giving more priority to vehicle with a lower LS. This priority can be set by making the vehicles with lower LS choosing a lower CW in which they back-off in case of transmission collisions. Based on MOPR, a new CW (say CWnew) is set for each vehicle. The CWnew is equal to the original CW if the concerned vehicle has LS equal to 100%, otherwise it is lower. The CWnew can be calculated following different manners, for example by using one of the following formulas,

$$CWnew = CW * LS \tag{7.1}$$

$$CWnew = CW * \cos(1 - LS) \tag{7.2}$$

$$CWnew = \frac{CW}{2} * (1 + LS) \tag{7.3}$$

Fugue 7.6 plots the CWnew values as a function of the LS values. The plot "CW" corresponds to the original CW. The plots $CWnew_1$, $CWnew_2$ and $CWnew_3$, corresponds to the new CW we get with using, respectively, Formula (7.1), Formula (7.2) and Formula (7.3). As you see, when fixing the original CW to 30 slots, the $CWnew_1$ starts from 0 time slots when $LS = 0$, but the $newCW_2$ starts from 15 time slots. So, a too small CW results in increasing the risk of transmission collisions at the level of the MAC layer. Thus, we should ovoid null and too small values of the $CWnew$. Therefore, we prefer to do not use Formula (7.1) for the calculation of the $CWnew$. Even if both Formula (7.2) and Formula (7.3) are more interesting than Formula (7.1), because of the time limitation, in the rest of this chapter we considered only Formula (7.3).

Figure 7.7 shows how the CWnew is setup respectively for the vehicles "A" and "B" in the same scenario presented in Figure 7.5). The CWnew for "A" is set to 11 and for B it is set to 15, when the original CW is set to 15. When transmission collision occurs, both "A" and "B" back-off within duration time randomly chosen in their CWnew, and then they double the original CW from which they calculate again their CWnew.

As described previously, when a transmission collision occurs, a node backs off in CW randomly chosen between 0 and the CWmin, and then in double the CWmin up it reaches the CWmax. So, another way for MOPR to improve the performances of IEEE 802.11 MAC mechanism is to adapt only the CWmax parameter.

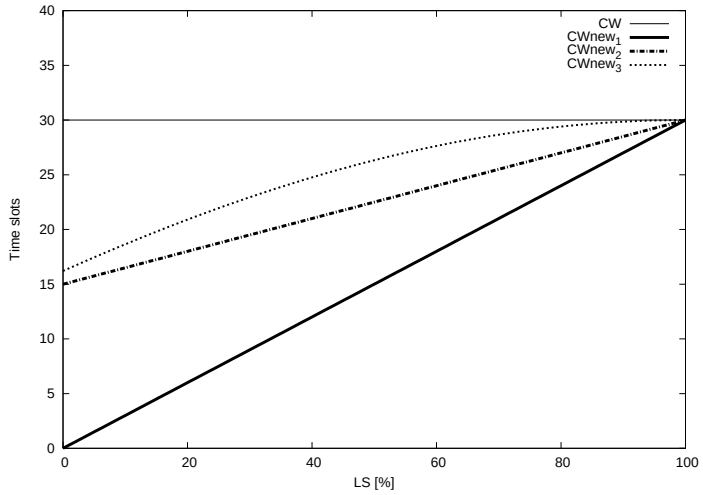

Figure 7.6: CWnew calculation

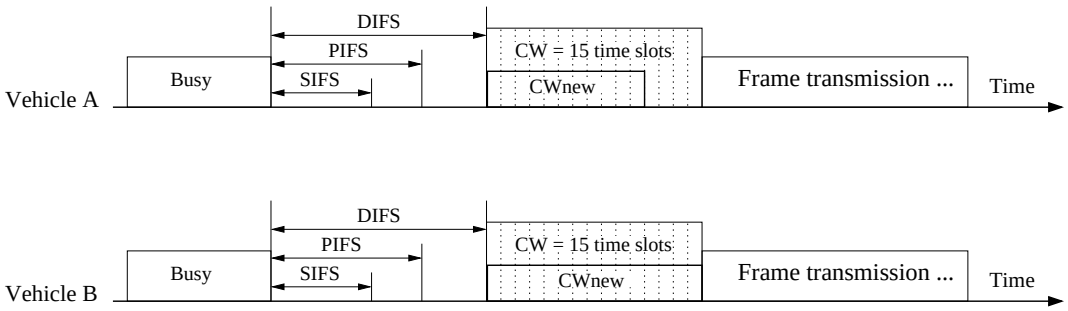

Figure 7.7: MOPR-based CW setup example.

7.4 Simulations

To validate our proposal, we have modified the ns2 implementation of the IEEE 802.11 MAC to introduce our MOPR-based CW adaptation mechanism. In this implementation (called "MOPR 802.11 MAC"), the CWnew is calculated following Formula 7.2. For performances evaluation, we have done some ns2 simulations with using separately our implementation (MOPR 802.11 MAC) and the generic 802.11 MAC (called 802.11 MAC). The simulation has been done through two steps. The first one by using a simple scenario to evaluate the improvement at the MAC layer only. And the second step by using a more realistic scenario to evaluate the performances at the MAC layer and their impact at the network layer.

In follows we present these two steps with their results that we obtained after 100 simulation runs. The metrics studied are the following:

- **Packet Delivery Ratio:** defined as the number of correctly received packets at the destination over the number of packets sent by the source.
- **End to End Delay:** defined as the duration time that a packet takes to go from the source and arrive to the destination.
- **MAC Overhead:** defined as the number of bytes injected in the network by the MAC protocol.
- **MAC Collision:** defined as the data size of the packet sent by the MAC protocol that got collided.

7.4.1 Basic simulation scenario

In this set of simulations we have considered simple scenario as shown in Figure 7.8. In this scenario we have a node "0" and some other nodes located on the same lane of a road, all 30 of them are stationary and are almost located in the communication range of the node"0". On the same road in the other lane, we have another node "A" moving from position "P1" to position "P2". Because of its movement pattern, node "A" goes out of the communication range of "0" and then comes back several times. The classical 802.11 Medium Access Control (MAC) functionalities are used, i.e. Distributed Coordination Function (DCF), Carrier Sense Multiple Access with acknowledgments (CSMA/CA with ACK) and Request-To-Send Clear-To-Send (RTS/CTS), and fragmentation, even if we suppose the messages are enough small. There is no routing protocol set in these simulations.

For performance comparisons we have done two sets of simulations. The first set with using the basic IEEE 802.11 MAC, as it is provided in the version 2.29 of ns2. And the second one with using our MOPR-based MAC implementation which is a modified version of the basic IEEE 802.11 MAC.

7.4.1.1 Simulation results and analysis

The results we got from our simulations are plotted in Figure 7.9. In this figure we see only the percentage of improvements we got by applying MOPR at the MAC layer. As you can see from the plots, by using MOPR we improve the network by 3.84% in terms of packet delivery ratio, and by 4.1% in terms of the delay. In terms of MAC overhead, MOPR does not improve

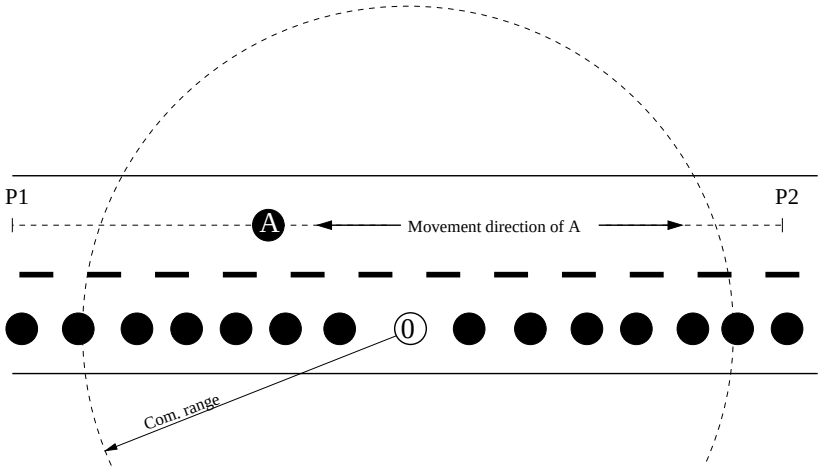

Figure 7.8: Basic simulation scenario to evaluate the performances at the MAC layer.

a lot the network performance. But, in terms of transmission collision at the MAC level, it improves the network performances by almost 5%.

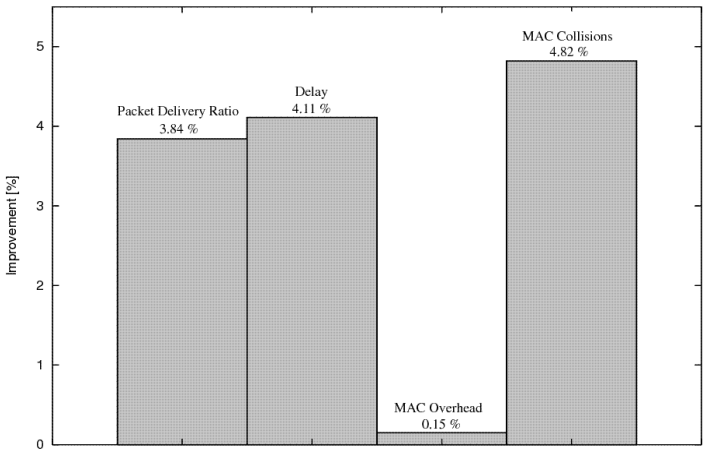

Figure 7.9: MOPR-based MAC improvements.

7.4.2 Advanced simulation scenario

For our simulations we have considered a highway-like scenario as shown in Figure 7.10. We have 200 nodes (vehicles) moving along five km (5000 m) length highway. In each direction we have three lanes with different speed ranges starting from a minimum speed value of 70 km/h and a maximum speed value which we increase from 120 to 220 km/h. In each direction we have a density of 5 vehicles every 150 m.

The maximum radio propagation rang is set to 250 meters, and the classical 802.11 Medium Access Control (MAC) functionality are used, i.e. Distributed Coordination Function (DCF), Carrier Sense Multiple Access with acknowledgments (CSMA/CA with ACK) and Request-To-Send Clear-To-Send (RTS/CTS), and fragmentation, even if we suppose the messages are enough small. Traffic type was CBR with 1024 Bytes of packet size and a 512 bps of maximum

CBR rate, and two transmitting source and destination couples are selected randomly along the middle lane (Normal vehicles' lane) in each direction. We use the GPSR as the routing protocol with the HLS as the location service.

For performance comparisons we have done two sets of simulations. The first set with using the basic IEEE 802.11 MAC, as it is provided in the version 2.29 of ns2. And the second one with using our MOPR-based MAC implementation which is a modified version of the basic IEEE 802.11 MAC.

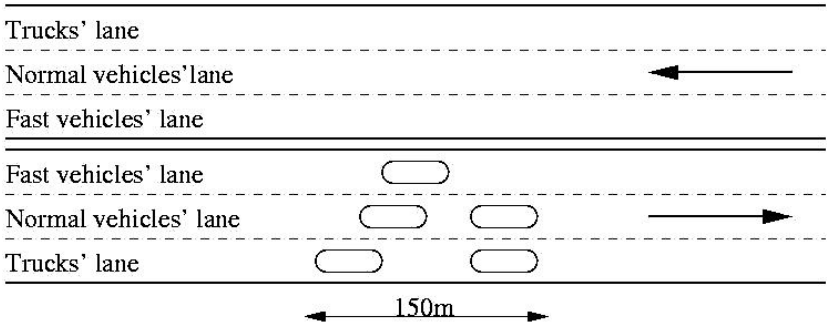

Figure 7.10: Advanced simulation scenario.

7.4.2.1 Simulation results and analysis

The results we analyze here are presented as a function of the mobility speed. Plots in Figure 7.11 compare the packet delivery ratio (PDR) of the two implementations: 802.11 MAC and our MOPR 802.11 MAC. And as you see, both implementations provide almost the same PDR. The PDR increases for both implementations when the speed increases. We think this is due to the fact the the number of packets sent over the air, in contrast to those received at the destination, decreases when the speed increases, so that the PDR appears to increase as well.

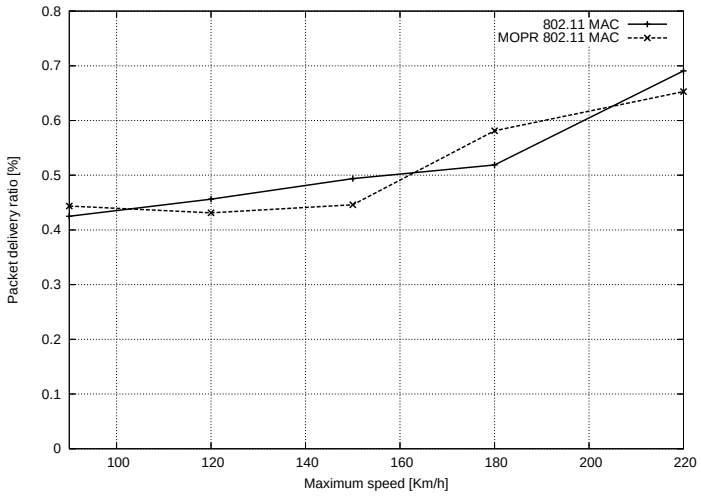

Figure 7.11: Packet delivery ratio comparison.

In Figure 7.12 we see that MOPR 802.11 MAC provides some improvement in terms of end to end delay when compared to 802.11 MAC. And this improvement gets more important when the maximum mobility speed of involved vehicles increase. Thus, when applying MOPR at the MAC layer we improve the performances of the network in terms of delay with keeping the same PDR.

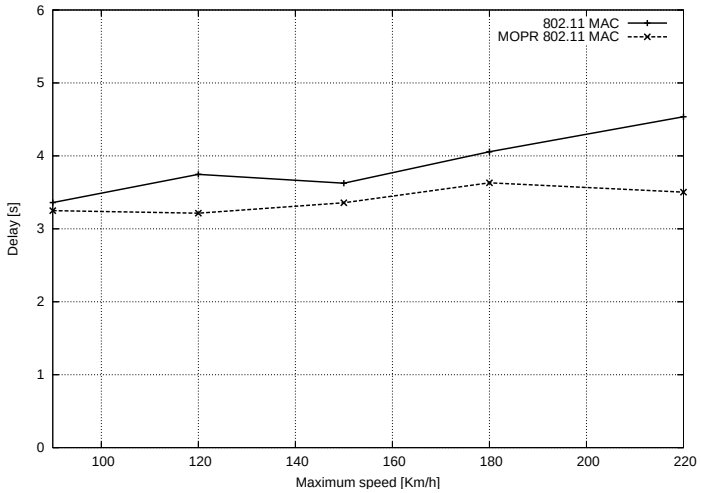

Figure 7.12: End to end delay comparison.

The performances improvements in terms of end to end delay, as shown previously, are mainly the results of the reduction of the transmission collisions as shown in Figure 7.13. In this figure we see that MOPR 802.11 MAC reduces the transmission collision at the MAC layer when comparing to the basic MAC.

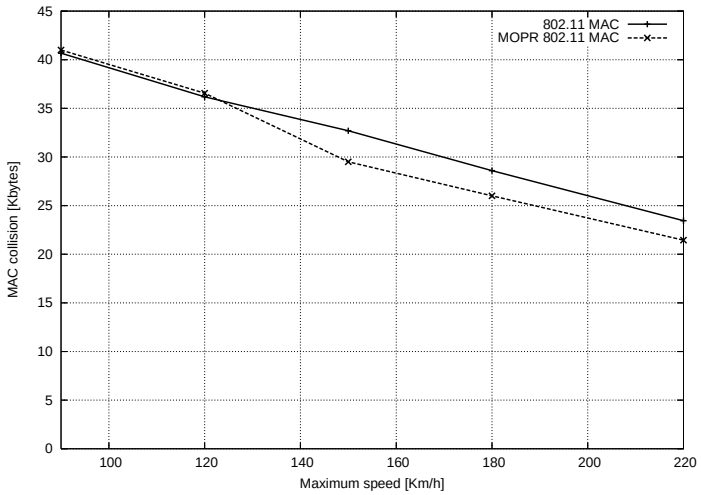

Figure 7.13: MAC collision comparison.

7.5 Chapter Summary

After having shown in the previous chapter how MOPR may improve the network from the network layer by guiding the routing protocol when selecting a route from a source to a destination, in this chapter we have shown how MOPR may bring some improvements at the MAC layer. We have presented one solution to use the MOPR output (LS) at the MAC layer. MOPR may be exploited in different ways from a MAC protocol to another, depending on the mechanism used. In case of the IEEE 802.11 MAC mechanism for example, MOPR is implemented by adapting the CW to the LS. And since LS depends on the movement information of the vehicles, the CW here becomes depended to the movement information of vehicles as well. This is the solution we considered in this chapter, but of course, MOPR may improve the IEEE 802.11 MAC mechanism by different manners. For example, if the mechanism uses some queue for incoming packet, this queue can be adapted based on LS, by giving more priority to packets coming from nodes corresponding to lower LS.

We have implemented our MOPR-based MAC by modifying the existing ns2 implementation of the IEEE 802.11 MAC. Based on ns2 simulation, we compared the network performances when using the basic IEEE 802.11 MAC and when using our MOPR-based IEEE 802.11 MAC. The results we got show little improvements with our MAC. These results, even if not enough, are promising.

Because of the time limitation we did not investigate several scenario in our simulations, which would be a follow up work.

Chapter 8

Conclusion and Perspectives

8.1 Summary of this work

Mobile ad hoc networks (MANETs) present some particularities such as the mobility, wireless interfaces, the independence from any infrastructure, etc... These wireless communication networks have been for several years of particular interest for researchers. Today, the role of this kind of networks for the industry is becoming crucial thanks to potential applications. One of the major MANET implementation families is the Vehicular ad hoc networks (VANETs), which represent a rapidly emerging class of MANETs, where nodes can be vehicles. As MANETs, VANETs are distributed and self-organizing.

VANETs have some specific characteristics when compared MANETs, such as the potential very high node speed and limited degrees of freedom in nodes' movement patterns. So the VANET topology changes very often and very quickly. Because of their characteristics, VANETs do not welcome all technologies and protocols already proposed for MANETs' data routing and Medium Access Control (MAC).

In this thesis we focus on routing and MAC only, believing that VANETs need protocols specially designed for this kind of networks. To understand well the behavior of routing and MAC mechanism in VANETs, we have reviewed the main routing and MAC mechanisms designed for MANETs, and then we have studied and listed those adapted or proposed for VANETs, or even those that have a potential in VANETs. From this review and study, we concluded that the routing and the MAC protocol which deals with VANETs' characteristics can be just an adaptation of existing protocols already proposed for traditional MANETs. And this is what we proposed in this work, a new concept which improves and adapts existing routing and MAC protocols to deal with VANETs specificity.

The mobility pattern of vehicles (nodes) is a very important parameter to consider when designing a technical solution at the network or at the MAC layer. Knowing the movement information of vehicles is possible and very easy to do with today's technologies, thanks to GPS and any other localization system. By exchanging movement information with neighboring nodes, any node in the network is able to predict their position in the near future (few seconds or even less). This may help in getting the future status of the network topology in advance, which helps in improving the routing process by choosing the most stable route, and in improving the MAC process by giving the same chance in getting access to the medium.

In this thesis we propose the MOvement PRediction (MOPR) concept, which runs as a cross layer between the MAC and the NET layers. This cross layer informs both the MAC

and the NET layers on the stability, in terms of lifetime, of neighboring links, by assigning them a metric called Link Stability (LS). This information is then used differently from layer to another layer, and from a protocol to another protocol.

To show the performances of MOPR at the NET layer, we first applied it to two topology-based data routing protocols. The first one is AODV, which is a reactive routing protocol, and the second one is OLSR, which is a proactive routing protocol. Topology-based routing is not a suitable mechanism for VANETs as is, but our implementation has been done to evaluate how MOPR reacts with such mechanisms. After getting interesting and premising results based on ns2 simulations with AODV and OLSR, we decided to investigate the application of MOPR to position-based routing mechanisms, which are very suitable for VANETs. For that implementation we have chosen the well known position-based GPSR protocol. Again, the ns2 simulations results we got proved that MOPR improves the position-based routing mechanisms in vehicular context.

To investigate performances of MOPR at the MAC layer, we considered the IEEE 802.11 MAC mechanism, which is suitable for communications in vehicular environments. Different MOPR-based solutions may be proposed to improve the IEEE 802.11 MAC, but in this work we have considered only one. It consists in using the MOPR output, the LS, to adapt the MAC Contention Window (CW). By doing that, bad discrimination between nodes attempting to access the medium can be reduced or even avoided. Making the CW size lower for neighbors corresponding to lower LS, allows us to give a certain priority to neighbors leaving the communication range sooner.

The LS is the main output of the cross layer MOPR. To go from the theoretical side to the practical side, we have done some Linux implementations of MOPR. This first Linux implementation, provides a LS to each neighbor based on own position (got from GPS antenna), and neighbors position (got from beaconing system). To validate this implementation, we have done several on-the-road tests with two cars. The main result we got from these tests is that MOPR-based LS reliability is directly related to the GPS data reliability.

After all this, we believe that considering the movement information of the nodes in VANETs is of a crucial importance.

8.2 Perspectives

In a complicated heterogeneous and distributed system, there will always be open issues and need for further improvements. The most of our contributions, touching focused topics, need further studies, especially field experiments within an operational environment. We conclude this work by listing the following interesting future directions for further research and development:

- Validation of our proposals has been done through ns2 simulations only, and some analytic study is needed to validate the performances of the MOPR-assisted routing and MAC protocols.

- The Link Stability is obtained by normalizing the lifetime we get based on movement prediction. The normalization is done by dividing the LS by a constant. It is interesting to do some mathematical studies to determine the optimal value of this constant depending on the environment and the improved protocol.

- At the MAC layer several issues are still open, due to a lack of time. In this work we investigated only the solution of adapting the CW to LS, and adapting only the CWmax to LS need to be investigated.
- The prototype we have developed is one part of MOPR, even the main part, but needs to be completed by extending the system to a routing protocol. And then, the whole system should be tested on-the-road, with several vehicles to see the impact at the routing layer.

List of Publications

Book chapters

- Hamid Menouar, Fethi Filali, and Massimiliano Lenardi, "An extensive survey and taxonomy of MAC protocols for vehicular wireless networks", in CRC Press book: Adaptive techniques in wireless networks, Summer 2008.

Journal papers

- Hamid Menouar, Fethi Filali and Massimiliano Lenardi, "A Survey and Qualitative Analysis of MAC Protocols for Vehicular Ad hoc Networks", IEEE Communication Magazine, Special issue Inter-Vehicle Communication (IVC), October 2006.

Conference papers

- Hamid Menouar, Massimiliano Lenardi, and Fethi Filali, "Movement prediction-based routing (MOPR) concept for position-based routing in vehicular networks", WiVec 2007, 1st IEEE International Symposium on Wireless Vehicular Communications, 30th September - 1st October 2007, Baltimore, USA

- Hamid Menouar, Massimiliano Lenardi, and Fethi Filali, "Improving proactive routing in VANETs with the MOPR movement prediction framework", ITST 2007, 7th International Conference on ITS Telecommunications, 6-8 June 2007, Sophia Antipolis, France

- Hamid Menouar, Massimiliano Lenardi, and Fethi Filali, "An intelligent movement-based routing for VANETs", in Proc. of the 13th ITS World Congress on Intelligent Transport Systems and Services, London, United Kingdom, 8-12 October 2006.

- Hamid Menouar, Massimiliano Lenardi, and Fethi Filali, "A Movement Prediction-Based Routing Protocol for Vehicle-to-Vehicle Communications", in Proc. of the first international workshop on Vehicle-to-Vehicle Communications (V2VCOM) (In Conjunction with MobiQuitous 2005), San Diego, California, USA, July 21, 2005.

- Hamid Menouar, Massimiliano Lenardi, and Fethi Filali, "On MAC and Routing Protocols Cooperation in Inter-Vehicle Communications", in Proc. of the 5th International Conference on ITS Telecommunications (ITST), Brest, France, June 27-19, 2005.

Bibliography

[1] CAR 2 CAR Communication Consortium (http://www.car-to-car.org)

[2] Internet Engineering Task Force Mobile Ad-hoc Networks (MANETs) working group (http://www.ietf.org/html.charters/manet-charter.html)

[3] Proceedings of the ACM international workshops on Vehicular ad hoc networks (VANET), since 2004.

[4] J. Luo and J. Hubaux, "A Survey of Inter-Vehicle Communication," School of Computer and Communication Sciences, EPFL, CH-1015 Lausanne, Switzerland, Technical Report IC/2004/24.

[5] The GPS system (http://en.wikipedia.org/wiki/GPS)

[6] B. Kaplan, "Understanding GPS," Artech House, 1996.

[7] S. Caokun, M. Hamdi, and J. Hubaux, "Gps-free positioning in mobile ad-hoc networks," In Proc. Hawaii Int. Con. on System Sciences, January 2001.

[8] The Galiliou system (http://en.wikipedia.org/wiki/Galileo_positioning_system)

[9] D. H. 859, Vehicle safety communications project task 3 final report," US Department of Transportation, Annual Report, Mar. 2005 (http://wwwnrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/index.html).

[10] R. S. Tony K. Mac, Kenneth P. Laberteaux, "A multi-channel vanet providing concurrent safety and commercial services," in Proc. of MobiCom VANET, Cologne, Germany, 2005.

[11] J. J. Blum, A. Eskandarian, and L. J. Hoffiman, "Challenges of Inter-vehicle Ad Hoc Networks," in the IEEE Transaction on Intelligent Transportation Systems, Vol. 5, No. 4, 2004.

[12] J. Luo and J-P. Hubaux, "A Survey of Inter-Vehicle Communication," School of Computer and Communication Sciences, EPFL, CH-1015 Lausanne, Switzerland, Technical Report IC/2004/24, 2004.

[13] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks - Architectures and Protocols," Pearson/Prentice Hall, May 2004 (ISBN: 0-13-147023-X).

[14] C. E. Perkins and E. M. Royer, “Ad Hoc On Demand Distance Vector (AODV) Routing,” Proc. of IEEE Workshop on Mobile Computing Systes and Applications 1999, pp. 90-100, February 1999.

[15] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad hoc Wireless Networks,” Mobile Computing, Kluwer Acadimic Publishers, vol. 353, pp. 153-181, 1996.

[16] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequence Distance-Vector Routing (DSDV) for Mobile Computers,” Proc. of ACM SIGCOMM 1994, pp. 234-244, August 1994.

[17] T.H. Clausen, G. Hansen, L. Christensen and G. Behrmann, “The Optimized Link State Routing Protocol, Evaluation through Experiments and Simulation,” IEEE Symposium on Wireless Personal Mobile Communications, September 2001.

[18] S. R. Das, R. Castaneda, and J. Yan, “Simulation based performance evaluation of mobile, ad hoc network routing protocols,” ACM/Baltzer Mobile Networks and Applications (MONET) Journal, pp. 179-189, July 2000.

[19] Zygmunt J. Haas , Marc R. Pearlman, ZRP: a hybrid framework for routing in Ad Hoc networks, Ad hoc networking, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, 2001.

[20] Marc R. Perlman and Zygmunt J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol," IEEE JSAC, 17(8), August 1999.

[21] Holger Füßler, Hannes Hartenstein, Dieter Vollmer, Martin Mauve, and Michael Käsemann, ”Location-Based Routing for Vehicular Ad-Hoc Networks,” in Proc. of the 8th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking (MOBICOM), pp 23-28, Atlanta, Georgia, USA, 2002.

[22] Seven Jaap, Marc Bechler, and Lars Wolf, “Evaluation of Routing Protocols for Vehicular Ad Hoc Networks in City Traffic Scenarios,” in Proc. of the 5th Int. Conf. on Intelligent Transportation Systems Telecommunications (ITST), Brest, France, 2005.

[23] Jeffrey Hightower and Gaetano Borriello, “Location sustems for ubiquitous computing,” Computing, 34(8):57-66, August 2001.

[24] S. Basagni, I. Chlamatac, V. Syrotiuk, and B. Woodward, "A distance routing effect algorithm for mobility (dream)," in Proc. of the 4th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking (MOBICOM), page 78-84, Dallas, TX, USA, 1998.

[25] M. Käsemann, H. Füßler, H. Hartenstein, and M. Mauve, “A Reactive Location Service for Mobile Ad Hoc Networks,” Technical Report TR-02-014, Department of Computer Science, University of Mannheim, November 2002.

[26] S. Giordano and M. Hamdi, “Mobility Management: The Virtual Home Region,” Technical Report SSC/1999/037, EPFL-ICA, October 1999.

[27] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," In Proc. of the 6th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking (MOBICOM) 2000, page 120-130, Boston, MA, USA, 2000.

[28] Wolfgang Kieß, Holger Füßler, Jörg Widmer, and Martin Mauve, "Hierarchical location service for mobile ad-hoc networks," in Proc. of ACM SIGMOBILE Mobile Computing and Communications Review, Volume 8, Issue 4, pp 47-58, October 2004.

[29] S. Giordano, I. Stojmenovic, Lj. Blazevic, "Position based routing algorithms for ad hoc networks: A taxonomy, in Ad Hoc Wireless Networking," X. Cheng, X. Huang and D.Z. Du (eds.), Kluwer, 2003.

[30] R. Nelson and L. Kleinrock, "The spatial capacity of a slotted ALOHA multihop packet radio network with capture," IEEE Transactions on Communications, 32, 6, 1984, pp 684-694.

[31] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals," IEEE Transactions on Communications, 32, 3, 1984, pp 246-257.

[32] T.C. Hou and V.O.K. Li, "Transmission range control in multihop packet radio networks," IEEE Transactions on Communications, 34, 1, 1986, pp 38-44.

[33] G.G. Finn, "Routing and addressing problems in large metropolitan-scale internetworks," ISI Research Report ISU/RR-87-180, March 1987.

[34] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, and H. Hartenstein, "Contention-Based Forwarding for Mobile Ad-Hoc Networks," Ad Hoc Networks 1, 2003.

[35] Karp, B. and Kung, H.T., "Greedy Perimeter Stateless Routing for Wireless Networks," in Proc. of the 6th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking (MobiCom), pp. 243-254, Boston, MA, August, 2000.

[36] J. Tian, L. Han, K. Rothermel, C. Cseh, "Spatially Aware Packet Routing for Mobile Ad Hoc Inter-Vehicle Radio Networks," in Proc. of the 6th IEEE Inter. Conf. on Intelligent Transportation Systems (ITSC '03), Shanghai, China, October 12-15, 2003.

[37] C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Herrmann, and M. Mauve, "A Routing Strategy for Vehicular Ad Hoc Networks in City Environments," in Proc. of IEEE Intelligent Vehicles Symposium (IV2003), pp 156-161 Columbus, Ohio, June 2003.

[38] M. Mauve, J. Widmer, H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad-Hoc Networks," IEEE Network Magazine, 2001.

[39] Ajay Chandra V. Gummalla and John O. Limb, "Wireless Medium Access Control Protocols," IEEE Communications Surveys, 2000.

[40] L. Kleinrok and F. A. Tobagi, "Packet Swiching in Radio Channels: Part I: Carrier Sense Multiple-Access Models and their Throughput-Delay Characteristics," IEEE Trans. Commun., vol. 23, no. 12, 1975, pp. 1400-16.

[41] "IEEE/ANSI Standard: Carrier Sense Multiple Access with Collision Detection," 1985.

[42] P. Karn, "MACA - A New Channel Access Method for Packet Radio," ARRL/CRRL Amateur Radio 9th Computer Networking Conference, September 22, 1990, pp. 134-40.

[43] K. Biba, "A Hybrid Wireless MAC Protocol Supporting Asynchronous and Synchronous MSDU Delivery Services," IEEE 802.11 Working Group paper 802.11/91-21, September, 1992.

[44] Vaduvure Aharghavan, Alan Memers, Scott Shenker, and Lixia Zhang, "A Media Access Protocol for Wireless LAN's," ACM SIGCOMM'94, ACM, 1994, pp. 212-25.

[45] F. A. Tobagi and L. Kleinrock, "Packet Swiching in Radio Channels: Part II: The hidden Terminal Problem in Carrier Sense Multiple-Access Modes and the Busy-Tone Solution," IEEE Trans. Commun., vol. COM-23, no. 12, pp. 1417-33, 1975.

[46] Jing Deng and Zygmunt J. Hass, "Dual Busy Tone Multiple Access (DBTMA): A New Medium Access Control for Packet Radio Networks," IEEE Trans. Commun., vol. 50, no. 6, pp. 975-85.

[47] Chenxi Zhu and M. Scott Corson, "A FIves-Phase Reservation Protocol (FPRP) for Mobile Ad Hoc Networks," ACM/Baltzer Journal of Wireless Networks, vol. 7, no. 4, pp. 371-384, Julay 2001.

[48] S. Jiang, J. Rao, D. He, and C. C. Ko, "A Simple Distributed PRMA for MANETs," Proceedings of IEEE Transactions on Vehicular Technology, vol. 51, no. 2, pp. 293-305, March 2002.

[49] Chang Wook Ahn, Chug Gu Kang, and You Ze Cho, "Soft Reservation Multiple Access with Priority Assignment (SWPA): A Novel MAC Protocol for QoS-Guaranteed Integrated Services in Mobile Ad-Hoc Networks," Proceedings of IEEE INFOCOM 1999, vol. 1, pp. 194-201, March 1999.

[50] K. T. Jin and D. H. Cho, "Multi-Code MAC for Multi-Hop Wireless Ad hoc Networks," Proceedings of IEEE Vehicular Vechnology Conference (VTC 2002), vol. 2, pp. 1100-1104, 2002.

[51] V. Kanodia, C. Li, A. Sabharwal, B. Sadeghi, and E. Knightly, "Distributed Priority Scheduling and Medium Access in Ad Hoc Networks," ACM/Baltzer Journal of Wireless Networks, vol. 8, no. 5, pp. 455-66, September 2002.

[52] Matthew S. Gast, "802.11 Wireless Networks: The Definitive Guide," O'REILLY, ISBN 0-596-00183-5, 2002.

[53] IEEE 802.11p., Trial Use Standard Wirelss Access in Vehicular Enviroments (WAVE) Multichannel Operation, for Trial Operation, November 2006.

[54] F. Borgonovo et al., "ADHOC MAC: a new, flexible and reliable MAC architecture for ad-hoc networks," Proceedings of IEEE WCNC 2003, vol. 4, no. 1, pp. 965-970, Mar 2003.

[55] W. Crowther et al., “A System for broadcast communications: Reservation ALOHA," Proceedings of Hawaii International Conference on systems Sciences, pp. 596-603, January 1973.

[56] Flaminio Borgonovo et al., “RR-ALOHA, a Reliable R-ALOHA broadcast channel for ad-hoc inter-vehicle communication networks,” Proceedings of Med-Hoc-Net, 2002.

[57] A. Nasipuri et al., “A MAC Protocol for Mobile Ad Hoc Networks Using Directional Antennas," Proceedings of IEEE WCNC 2000, vol. 1, pp. 1214-1219, September 2000.

[58] Z. Huang et al., “A Busy Tone-Based Directional MAC Protocol for Ad Hoc Networks," Proceedings of IEEE MILCOM 2002, October 2002.

[59] Y. B. Ko et al., "Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks," Proceedings of IEEE INFOCOM 2000, vol. 1, pp. 13-21, March 2000.

[60] Q. Xu et al., “Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages,” IEEE Transaction on Vehicular Technology, vol. 56, no. 2, March 2007.

[61] S. Katragadda et al., “A Decentralized Location-based Channel Access Protocol for Inter-Vehicle Communication,” Proceedings of the 57th IEEE Vehicular Technology Conference (VTC), vol. 3, pp. 1831-35, 2003.

[62] CAR 2 CAR Communication Consortium Manifesto, v1.1, September 2007 (`http://www.car-to-car.org`).

[63] T. Osafune, L. Lan, and M. Lenardi, “Multi-hop vehicular broadcast (MHVB),” International Conference on ITS Telecommunications (ITST 2006), Chengdu, China, 2006.

[64] M. Mariyasagayam, T. Osafune, M. Lenardi, “Enhanced Multi-Hop Vehicular Broadcast (MHVB) for Active Safety Applications,” ITST 2007, 7th International Conference on ITS Telecommunications, Sophia Antipolis, France, June 2007.

[65] W. Su and S. Lee and M. Gerla, "Mobility prediction and routing in ad hoc wireless networks", GlobeCom 1999.

[66] The Network Simulator NS2 (`http://www.isi.edu/nsnam/ns/`)

[67] `http://core.it.uu.se/adhoc/ImplementationPortal`

[68] `http://masimum.dif.um.es/?Software:UM-OLSR`

[69] F. Granelli, G. Boato, and D. Kliazovich, “MORA: a Movement-Based Routing Algorithm for Vehicle Ad Hoc Networks,” IEEE Workshop on Automotive Networking and Appications (AutoNet 2006), San Francisco, U.S.A., December 2006.

[70] IEEE Std. 1609.4, “IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-channel Operation”, IEEE Std. 1609.4, Nov 2006.

[71] ITS Standards Program Web Site: Standards development statuses (`http://www.standards.its.dot.gov/StdsSummary.asp?id=404,405,406,415,504,505`).

[72] Intelligent Transportation Systems Standards Fact Sheet IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE), US DOT, Jan 9, 2006 (`http://www.standards.its.dot.gov/fact_sheet.asp?f=80`).

[73] Stephan Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard," In Proc. of the 1st IEEE International Symposium on Wireless Vehicular Communications (WiVeC), September 2007.

[74] The European Telecommunications Standards Institute (`http://www.etsi.org`)

[75] Stefan Mangold, Sunghyun Choi, Peter May, Ole Klein, Guido Hiertz, and Lothar Stibor, "IEEE 802.11e Wireless LAN for Quality of Service," in Proc. European Wireless (EW'2002), vol. 1, pp. 32-39, Florence, Italy, February 2002.

List of Abbreviations

AC Access Class

ACK Acknowledgment

AODV Ad-hoc On-Demand Distance Vector

AODV-UU AODV Uppsala University

BCH Basic Chanel

BTMA Busy Tone Multiple Access

C2C Car to Car

C2I Car to Infrastructure

CBF Contention-based Forwarder

CBR CDMA Code Division Multiple Access

CCH Control Chanel

CPU Central Processing Unit

CR Collision Report

CSMA Carrier Sense Multiple Access

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD Carrier Sense Multiple Access with Collision Detection

CTS Clear to Send

CW Contention Window

CWmax Contention Window Maximum

CWmin Contention Window Minimum

D-MAC Directional MAC

D-PRMA Distributed Packet Reservation Multiple Access

DACK Directional ACK

DBTMA Dual Busy Tone Multiple Access

DCF Distributed Coordination Function

DIFS DCF Inter Frame Space

Directional-BTMA Directional Busy Tone-Based MAC

DL DeadLocks

DPS-MAC Distributed Priority Scheduling Medium Access Control

DREAM Distance Routing Effect Algorithm for Mobility

DRTS Directional RTS DS Data Sending

DSDV Destination Sequence Distance Vector

DSR Dynamic Source Routing

EIFS Extended Inter Frame Space

ETSI European Telecommunications Standards Institute

FDMA Frequency Division Multiple Access

FI Frame Information

FPRP Five Phase Reservation Protocol

GCC GNU Compiler Collection

GHz GigaHertz

GlobLS Global LS

GLS Grid Location Service

GPRS General Packet Radio Service

GPS Global Positioning System

GPSR Greedy Perimeter Stateless Routing

GSR Geographic Source Routing

HLS Hierarchical Location Service

Hz Hertz

ID Identifier

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IF Information Frame

IFS Inter Frames Spacing

IP Internet Protocol

IS Information Slot

ITS Intelligent Transportation System

IVC Inter Vehicle Communication

LAN Local Area Network

LCA Local-based Chanel Access

LLC Logical Link Control

LS Link Stability

MAC Medium Access Control

MACA Multiple Access with Collision Avoidance

MACAW Multiple Access with Collision Avoidance Wireless

MANET Mobile Ad hoc Network

Mbps Megabit Per Second

MC-MAC Multi-code Medium Access Control

MFR Most Forwarder with Radius

MHVB Multi-Hop Vehicular Broadcast

MHz Mega Hertz

MIB Management Information Base

MOPR Movement Prediction

MORA Movement-based Routing Algorithm

MPR Multi-Point Relay

NAV Network Allocation Vector

NET_layer Network layer

newRS New Route Stability

NFP Nearest Forwarder Progress

NS2 Network Simulator 2

OBU On Board Unit

OCTS Omnidirectional CTS

OH One-Hop

OLSR Optimized Link State Routing

ORTS Omnidirectional RTS

OS Operating System

OSI Open System Interaction

PCF Point Coordination Function

PDA Personal Digital Assistant

PDR Packet Delivery Ratio

PIFS PCF Inter Frame Space

PS Path Stability

QoS Quality of Service

R-ALOH Reservation ALOHA

RA Reservation Acknowledgment

RC Reservation Cycle

RCell Responsible Cell

RConf Reservation Confirmation

RF Reservation Frame

RFC Request for Comment

RLS Reactive Location Service

ROR Routing Overhead Ratio

RPM Random Progress Method

RR Reservation Request

RR-ALOHA Reliable R-ALOHA

RREP Route Replay

RREQ Route Request

RS Reservation Slot

RTS Request to Send

SCH Service Chanel

SIFS Short Inter Frame Space

SRMA/PA Soft Reservation Multiple Access with Priority Assignment

ST Scheduling Table

TC_message Topology Control Message

TDMA Times Division Multiple Access

TH Two-Hop

TLR Terminodes Local Routing

TRR Terminodes Remote Routing

TTL Time To Live

UM-OLSR University of Murcia OLSR

UMTS Universal Mobile Telecommunications System

USB Universal Serial Bus

US_DOT United Stat Department Of Transportation

UTRA-TDD UMTS Terrestrial Radio Access Time Division Duplex

V2I Vehicle to Infrastructure

V2V Vehicle to Vehicle

V2VC Vehicle to Vehicle Communication

VANET VoWLAN Voice over Wireless

LAN Local Area Network

WAVE Wireless Access in Vehicular Environment

WIFI Wireless Fidelity

WLAN Wireless Local Area Network

ZRP Zone Routing Protocol

Index