UNIVERSITÉ DE SHERBROOKE
Faculté de génie
Département de génie électrique et génie informatique

COMMUNICATION CONTINUE EN MODE INFRASTRUCTURE DANS LES RÉSEAUX VÉHICULAIRES UTILISANT IEEE 802.11P

Mémoire de maîtrise
Spécialité : Génie électrique

Balkrishna Sharma GUKHOOL

Jury: Soumaya Cherkaoui (directeur)
Daniel Dalle
Ahmed Khoumsi

Sherbrooke (Québec), Canada
Décembre 2009

Library and Archives
Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-65609-9
Our file Notre référence
ISBN: 978-0-494-65609-9

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

RÉSUMÉ

Les *handovers* sont des phénomènes inévitables dans les réseaux sans-fil mobiles. Lors du passage d'une station mobile d'un point d'accès à un autre, le *handover* affecte la qualité des transmissions, et ainsi, il est néfaste à la performance des réseaux sans-fil. De nombreuses techniques de réduction du délai lié au *handover* ont été proposées, mais la plupart ne sont pas adaptées aux attentes du nouveau type de réseau sans-fil mobile qu'est le réseau véhiculaire.

Ce travail propose donc l'implémentation d'une méthode de réduction du délai encouru lors d'un *handover* dans les réseaux véhiculaires qui opèrent sous une technologie d'accès sans-fil adaptée pour les besoins des réseaux véhiculaires. Le travail est composé de deux blocs : le premier est l'implémentation d'IEEE 802.11p, qui est une variante de la norme générique d'IEEE 802.11 et qui est développée spécialement pour l'accès dans les réseaux véhiculaires, dans un simulateur de réseaux. L'autre partie concerne le choix d'une méthode de réduction du délai lié à l'étape de la recherche du *handover*. En tenant compte des réalités technologiques, le choix s'est porté sur une technique préconisant l'utilisation des *cache* pour contenir et diffuser de l'information sur les points d'accès avoisinants.

La méthode proposée a été testée et a donné de très bons résultats réalistes. L'intégration des modules complémentaires pour refléter l'ensemble de la technique proposée au niveau du simulateur s'est aussi faite sans problèmes majeurs.

Mots-clés : *handovers*, réseau véhiculaire, IEEE 802.11p, *cache*

REMERCIEMENTS

Comme tout autre projet de recherche, ce mémoire n'aurait pas vu le jour sans l'aide, la collaboration et le soutien des certaines personnes que je tiens particulièrement à remercier.

Tout d'abord, je tiens à remercier ma directrice, la professeure Soumaya Cherkaoui pour m'avoir offert ce projet et qui a su me guider afin d'aboutir à ce présent travail.

Je profite de l'occasion pour exprimer ma gratitude envers les membres de mon jury, les professeurs Daniel Dalle et Ahmed Khoumsi, pour avoir accepté d'être les évaluateurs de ce mémoire.

Je suis infiniment reconnaissant envers mes parents et ma sœur, et mes collègues de bureau pour l'encouragement et le soutien qu'ils m'ont accordé tout au long de mon programme.

TABLE DES MATIÈRES

CHAPITRE 1: INTRODUCTION 1
  1.1 Contexte et problématique 1
  1.2 Solution proposée 2
  1.3 Contributions de la mémoire 3
  1.4 Plan de la mémoire 4
CHAPITRE 2: LE HANDOVER 5
  2.1 Les étapes entourant le handover 5
  2.2 La recherche 6
    2.2.1 Les délais dus à la recherche 7
  2.3 L'authentification 8
    2.3.1 Les délais dus à l'authentification 8
  2.4 La réassociation 9
    2.4.1 Les délais dus à la réassociation 9
CHAPITRE 3: TECHNIQUES POUR RÉDUIRE LES DÉLAIS LORS DU *HANDOVER* ... 11
  3.1 Réduire le délai associé à la recherche 12
  3.2 Réduire les délais associés à l'authentification et à la réassociation 17
CHAPITRE 4: ARTICLE DE CONFÉRENCE LCN ON-MOVE OCTOBRE 2008 21
  Avant-propos 21
  4.1 Abstract 23
  4.2 Keywords 23
  4.3 Introduction 23
  4.4 Vehicular Access Technologies 24
    4.4.1 Dedicated Short Range Communications (DSRC) 24
    4.4.2 Wireless Access in Vehicular Environments (WAVE) 24
    4.4.3 IEEE 802.11p 25
  4.5 Characteristics of IEEE 802.11p 25
    4.5.1 The WAVE Approach 26
    4.5.2 WAVE operations 26
    4.5.3 WAVE PHY specifications 27
  4.6 How DSRC Works 27
  4.7 IEEE 802.11p implementation in NS-2 27
    4.7.1 The physical layer 28
    4.7.2 The MAC layer 29
  4.8 Simulation 31
    4.8.1 Simulation Setup 31
  4.9 Results 32
  4.10 Future work 33
  4.11 Conclusion 33
CHAPITRE 5: ARTICLE DE CONFÉRENCE WOCN AVRIL 2009 34
  Avant-propos 34
  5.1 Abstract 36
  5.2 Keywords 36
  5.3 Introduction 36
    5.3.1 IEEE 802.11p 37
    5.3.2 Handoffs in IEEE 802.11-based networks 37

5.4 NS-2 38
  5.4.1 Handoff in NS-2 38
5.5 Implemented Handoff Model 40
5.6 IEEE 802.11p Handoff in NS-2..40
5.7 40
  5.7.1 Management Frames..40
  5.7.2 Handoff mechanism..41
5.8 Simulation..41
  5.8.1 Simulation Setup..41
  5.8.2 Discussion..45
5.9 Conclusion..49
CHAPITRE 6: ARTICLE DE REVUE IJUWBCS..50
Avant-propos 50
6.1 Abstract..52
6.2 Keywords..52
6.3 Introduction 52
6.4 IEEE 802.11p..53
6.5 Handoffs in IEEE 802.11 wireless networks..54
6.6 Handoff Model in NS-2..55
6.7 IEEE 802.11p handoff implementation in NS-2 56
  6.7.1 Proactive Caching..56
  6.7.2 Management Frames..59
  6.7.3 Handoff Mechanism 60
6.8 Simulation..61
  6.8.1 First simulation set..62
  6.8.2 First simulation set results 63
  6.8.3 Second simulation set..69
  6.8.4 Second simulation set results..70
6.9 Conclusion and future work 75
6.10 Acknowledgement..75
CHAPITRE 7 : CONCLUSION..76

LISTE DES FIGURES

FIGURE 1.1: UN RÉSEAU VÉHICULAIRE 2

FIGURE 2.1: LES PHASES DU HANDOFF ET LEURS DÉLAIS ASSOCIÉS 5

FIGURE 2.2: L'ARCHITECTURE IEEE 802.11 10

FIGURE 3.1: LES ÉCHANGES DE MESSAGES POUR LA PROCÉDURE DE HANDOVER DANS LES RÉSEAUX 802.11 11

FIGURE 3.2: LE *NG PRUNING SCHEME* 13

FIGURE 3.3: MODE D'OPÉRATION DE SYNCSCAN 15

FIGURE 3.4: OUVERTURE DE SESSION AU POINT D'ACCÈS 4 18

FIGURE 3.5: *HANDOVER* DE LA SESSION DE COMMUNICATION DU POINT D'ACCÈS 4 AU POINT D'ACCÈS 2 18

FIGURE 3.6: LA MÉTHODE PNC 19

FIGURE 4.1: WAVE PROTOCOL STACK 25

FIGURE 4.2: IEEE 802.11 MODEL IN NS-2 28

FIGURE 4.3: SIMULATION SETUP 31

FIGURE 4.4: GRAPHICAL REPRESENTATION OF THE RESULTS OBTAINED 32

FIGURE 5.1: WAVE PROTOCOL STACK 37

FIGURE 5.2: EXCHANGE OF MANAGEMENT FRAMES DURING HANDOFF 38

FIGURE 5.3: IEEE 802.11 MODEL IN NS-2 39

FIGURE 5.4: SIMULATION SETUP 42

FIGURE 5.5: MEAN RTT FOR VEHICLE SPEED OF 60 KM/H 44

FIGURE 5.6: MEAN RTT FOR VEHICLE SPEED OF 140 KM/H 44

FIGURE 5.7: MEAN RTT FOR VEHICLE SPEED OF 200 KM/H 45

FIGURE 5.8: PERCENTAGE OF PACKET LOST FOR DIFFERENT SPEEDS FOR A CBR/UDP APPLICATION 45

FIGURE 5.9: RTT OF ICMP REQUESTS FOR VEHICLES MOVING AT 60 KM/H WITH AN ADDED TRAFFIC LOAD 46

FIGURE 5.10: RTT OF ICMP REQUESTS FOR VEHICLES MOVING AT 140 KM/H WITH AN ADDED TRAFFIC LOAD 46

FIGURE 5.11: RTT OF ICMP REQUESTS FOR VEHICLES MOVING AT 200 KM/H WITH AN ADDED TRAFFIC LOAD 47

FIGURE 5.12: RTT OF ICMP REQUESTS RECEIVED FOR VEHICLES MOVING AT 60 KM/H WITH AN INCREASING VEHICLE DENSITY 47

FIGURE 5.13: RTT OF ICMP REQUESTS RECEIVED FOR VEHICLES MOVING AT 140 KM/H WITH AN INCREASING VEHICLE DENSITY 48

FIGURE 5.14: RTT OF ICMP REQUESTS RECEIVED FOR VEHICLES MOVING AT 200 KM/H WITH AN INCREASING VEHICLE DENSITY 48

FIGURE 6.1: SIMULATION SETUP FOR FIRST SET OF SIMULATIONS 63

FIGURE 6.2: MEAN RTT FOR 20 NODES AT 80 KM/H 66

FIGURE 6.3: MEAN RTT FOR 20 NODES AT 140 KM/H 66

FIGURE 6.4: MEAN RTT FOR 20 NODES AT 200 KM/H 66

FIGURE 6.5: MEAN RTT FOR 60 NODES AT 80 KM/H 67

FIGURE 6.6: MEAN RTT FOR 60 NODES AT 140 KM/H 67

FIGURE 6.7: MEAN RTT FOR 60 NODES AT 200 KM/H 67

FIGURE 6.8: MEAN RTT FOR 100 NODES AT 80 KM/H 68

FIGURE 6.9: MEAN RTT FOR 100 NODES AT 140 KM/H 68

FIGURE 6.10: MEAN RTT FOR 100 NODES AT 200 KM/H 68

FIGURE 6.11: SIMULATION SETUP FOR SECOND SET OF SIMULATIONS 70

FIGURE 6.12: MEAN RTT FOR 20 NODES AT 80 KM/H WITH HANDOFF 72

FIGURE 6.13: MEAN RTT FOR 20 NODES AT 140 KM/H WITH HANDOFF 72

FIGURE 6.14: MEAN RTT FOR 20 NODES AT 200 KM/H WITH HANDOFF 72

FIGURE 6.15: MEAN RTT FOR 60 NODES AT 80 KM/H WITH HANDOFF 73

FIGURE 6.16: MEAN RTT FOR 60 NODES AT 140 KM/H WITH HANDOFF 73

FIGURE 6.17: MEAN RTT FOR 60 NODES AT 200 KM/H WITH HANDOFF 73

FIGURE 6.18: MEAN RTT FOR 100 NODES AT 80 KM/H WITH HANDOFF 74

FIGURE 6.19: MEAN RTT FOR 100 NODES AT 140 KM/H WITH HANDOFF 74

FIGURE 6.20: MEAN RTT FOR 100 NODES AT 200 KM/H WITH HANDOFF 74

CHAPITRE 1: INTRODUCTION

Le phénomène de l'informatique omniprésente, de l'anglais *ubiquitous computing*, s'accentue chaque jour tant il y a une dépendance sur les outils technologiques de communication. Tout le monde veut avoir accès à l'information la plus récente et ce dans le plus bref délai et peu importe l'emplacement géographique. D'où l'essor que connaissent actuellement les réseaux de communication sans fil. Après l'avènement du péage sur les autoroutes, de nombreuses idées d'application que pourraient bénéficier les occupants des véhicules ont été élaborées et la nature mobile des réseaux sans fil convient parfaitement pour transmettre de l'information des sites offrant des services aux véhicules et vice-versa.

1.1 Contexte et problématique

L'exigence de la qualité et d'un temps de réponse minime est l'un des critères prépondérants au niveau des réseaux véhiculaires. Les réseaux véhiculaires consistent, entre autres, des liens de communication sans-fil établis entre des véhicules eux-mêmes, ou entre les véhicules et des infrastructures placés tout au long des routes. Plusieurs études font état de l'utilisation de diverses technologies sans-fil dans le contexte des réseaux véhiculaires. L'IEEE a créé un groupe de travail pour emmener une nouvelle version de la technologie sans-fil basée sur la norme IEEE 802.11 qui serait adaptée pour les réseaux véhiculaires; cet amendement est appelé IEEE 802.11p. Cependant, l'un des problèmes qui touchent à toutes ces technologies sans-fil reste sans doute, le *handover.*

Le *handover* survient lorsqu'une station mobile change d'association d'un point d'accès à un autre. La figure 1.1 illustre un exemple de réseau véhiculaire en milieu urbain. Le *handover* aura lieu, par exemple au niveau de la voiture qui est connecté à un point d'accès qui est relié à l'internet ainsi qu'à un réseau commercial. Lorsque la voiture s'éloigne de ce point d'accès, elle sort de sa portée ce qui fait qu'il y a une augmentation de temps de transmission qui peut même aller jusqu'à une perte de communication. Pour éviter cela, la session sera continuée à travers une association avec le prochain point d'accès sur la route qu'emprunte la voiture.

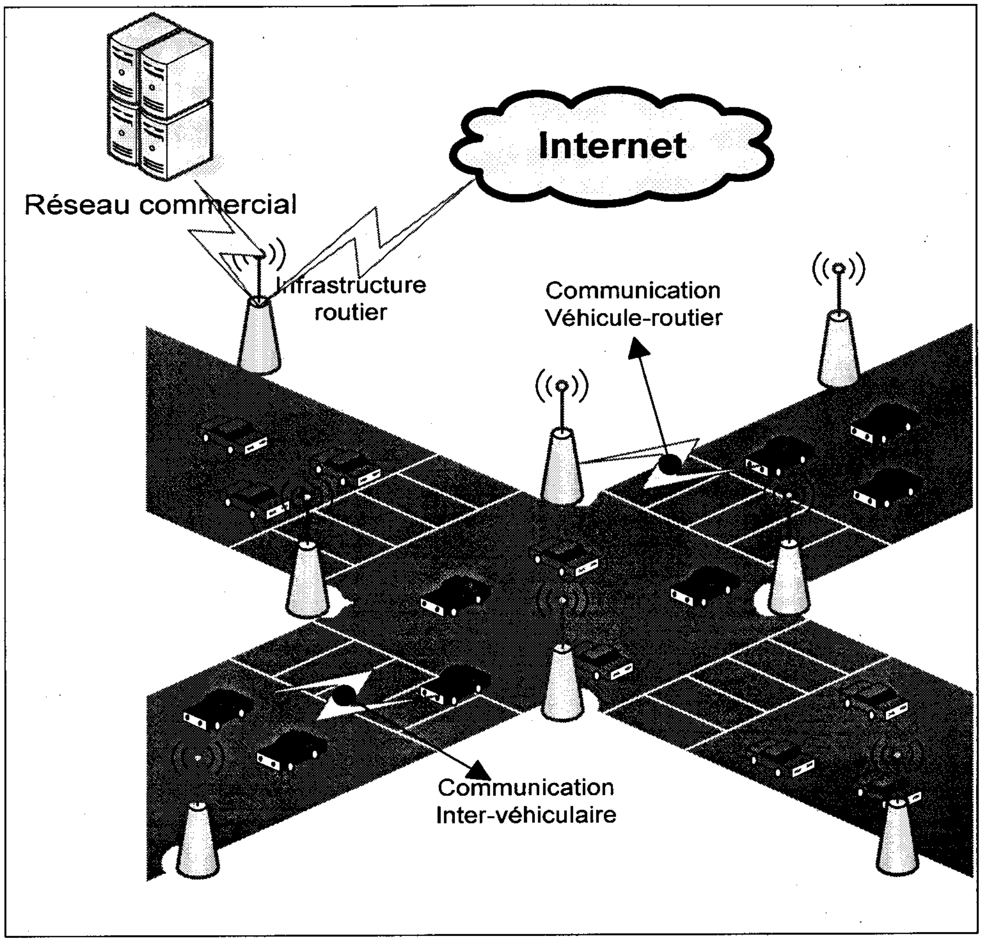

Figure 1.1: Un réseau véhiculaire

1.2 Solution proposée

Le travail développé dans ce mémoire vise la mise en application d'une technique de réduction de délai encouru lors d'un *handover*, et ce dans un environnement très spécifique, c'est-à-dire, les réseaux véhiculaires.

1.3 Contributions du mémoire

La problématique de ce travail concerne la mise en place d'une technique efficace de réduire le délai encouru lors d'un *handover* et ce, pour une communication quasi-continue de véhicule à infrastructure (*V2I*) dans un réseau véhiculaire en utilisant une variante de la norme IEEE 802.11, qui est le IEEE 802.11p.

La contribution principale est l'application d'une technique pour minimiser le délai associé à la recherche d'un nouveau point d'accès car il est le facteur le plus conséquent dans le délai encouru lors d'un *handover.* Le manque de matériel et l'implication financière font que cette technique ne peut être testée, jusqu'à présent, que dans un simulateur appropriée.

Les contributions particulières peuvent être détaillées comme suit :

- Analyse de la procédure de *handover* à la couche liaison de données dans les réseaux sans-fil utilisant la technologie d'accès générique IEEE 802.11;
- Application d'une technique de réduction de délai associé au *handover* à la couche liaison de données;
- Amélioration de la structure interne, plus spécifiquement, les couches physiques et liaison de données du simulateur de réseaux, NS-2 pour mieux satisfaire les attentes des et avoir un rapprochement vers les réseaux véhiculaires opérant en mode infrastructure;

À ce jour, et à la connaissance de l'auteur, il n'y a pas d'autres travaux qui ciblent le problème de *handover* dans les réseaux véhiculaires en utilisant la technologie d'accès IEEE 802.11p. L'originalité de ce travail tient donc de l'implémentation de la dite technologie d'accès dans NS-2 et aussi, une amélioration de la procédure de *handover*, surtout au niveau des trames échangées, dans le même simulateur.

1.4 Plan du mémoire

La mémoire s'articule en six autres chapitres. Le prochain chapitre donne une description détaillée de ce qu'est le *handover*. Le chapitre 3 définit le contexte général du travail et constitue la revue de littérature des méthodes existantes pour réduire le délai encouru lors du *handover*. Les chapitres 4,5 et 6 décrivent le travail mené pour résoudre la problématique. L'implémentation de la norme de communication IEEE 802.11p dans le simulateur, de la méthode de réduction du *handover*, ainsi que les résultats obtenus et leurs analyses sont présentés sous forme d'article. Ces chapitres sont retranscrits en langue anglaise, comme le spécifie le protocole de rédaction de l'Université de Sherbrooke. Finalement, le dernier chapitre donne les conclusions. Il revient sur la problématique, les résultats et les contributions de ce projet.

CHAPITRE 2: LE HANDOVER

Ce chapitre a pour but d'introduire les différentes étapes composantes du phénomène de *handover* dans les réseaux sans fil opérant avec l'architecture IEEE 802.11. Les informations sont issues de plusieurs articles sur le thème.

2.1 Les étapes entourant le *handover*

En général, la procédure de *handover*, comme illustrée par la figure 2.1, se déroule en trois étapes :

1. la recherche d'un nouveau point d'accès;
2. l'authentification de la station mobile;
3. la réassociation de la station mobile.

Néanmoins, ces étapes accusent chacune un certain délai car il y a des traitements qui doivent se faire à chaque niveau.

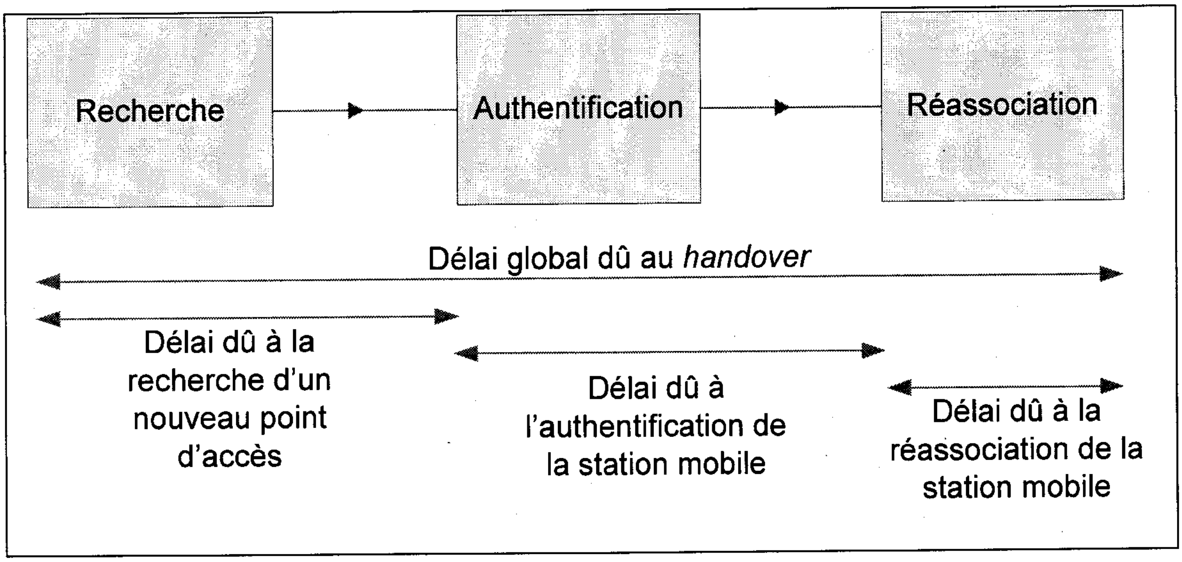

Figure 2.1: Les phases du *handover* et leurs délais associés

2.2 La recherche

La première phase est celle de la recherche ou d'observation. La mobilité de la station mobile dégrade le rapport signal bruit associé à la station de base courante, et déclenche le *handoff*. Avant de mettre un terme à la communication qui existe avec la station de base, la station mobile doit trouver de nouveaux potentiels points d'accès auxquels elle pourrait s'associer. Cette recherche est accomplie par le biais d'une fonction, qui s'appelle *scanning*, de la couche de contrôle d'accès au support ou, *Medium Access Control (MAC)*.

Il y a deux types de balayages dans la norme IEEE 802.11: actif et passif. Dans le mode passif, la station mobile attend la réception des trames balises. Les points d'accès envoient celles-ci toutes les 100 ms, par exemple. La trame balise contient des informations proposés par le point d'accès. Comme un point d'accès peut servir plusieurs réseaux, chaque réseau est identifié par le *Service Set Identifier* ou le SSID. En sus du nom du réseau, la trame balise contient des informations caractéristiques sur celui-ci: est-il sécurisé? Avec quelle méthode? Quels sont les débits proposés? Sur quel canal?

Chaque station souhaitant joindre un réseau particulier doit écouter sur l'ensemble des canaux si une trame de balise est envoyée, indiquant alors la présence d'un point d'accès. Ce processus est assez long en raison de l'envoi toutes les 100 ms de ces trames, il faut donc attendre au moins 100 ms par canal afin de connaître la liste exhaustive des réseaux disponibles dans l'entourage.

La norme courante IEEE 802.11 supporte plusieurs canaux; plus spécifiquement, les normes IEEE 802.11b et IEEE 802.11g, qui opèrent dans la bande ISM des 2,4 GHz, utilisent 11 des 14 canaux disponibles, alors que la norme IEEE 802.11a opère dans la bande ISM des 5 GHz, dans laquelle un total de 32 canaux sont définis. Avec le balayage passif, la station mobile doit 'écouter' sur chaque canal pour essayer de détecter le prochain point d'accès, et avec un délai de 100 ms par canal, la recherche peut s'avérer très longue.

Dans le mode actif, la station mobile essaie de trouver un nouveau point d'accès en transmettant une requête de sondage et attend une réponse de sondage de la part d'un point d'accès. Pour éviter d'attendre inutilement une réponse de sondage qui tarde à venir, la station mobile va établir une durée, déterminée par les valeurs de *MinChannelTime* et de *MaxChannelTime*. Si aucune réponse n'est obtenue à *MinChannelTime*, le prochain canal est balayé. Si une ou plusieurs réponses sont reçues à *MinChannelTime*, la station mobile arrête d'accepter les trames de réponses à *MaxChannelTime* et procède au traitement de ces réponses. Ce processus est répété pour le prochain canal.

2.2.1 Les délais dus à la recherche

Le délai causé par la recherche d'un nouveau point d'accès dépend du type de balayage utilisé. Dans le mode passif, en moyenne, ce délai peut être représenté comme une fonction de l'intervalle entre les trames balises et le nombre de canaux disponibles. Si le temps entre les trames balises est de 100 ms, le délai de recherche en moyenne avec la norme IEEE 802.11b sur 11 canaux et la norme IEEE 802.11a avec 32 canaux va être 1100 ms et 3200 ms respectivement. Il est intéressant de noter que le temps entre le changement des canaux est comparativement très négligeable; il varie entre 40 et 150 μs.

Dans le cas d'un balayage en mode actif, le délai est déterminé par les valeurs de *MinChannelTime* et de *MaxChannelTime*, qui sont dépendants du matériel. Aussi, le processus requiert le balayage de tous les canaux disponibles. Donc, le délai, D, associé à la recherche active peut être exprimé comme :

$$N \times MinChannelTime \leq D \leq N \times MaxChannelTime,$$

N étant le nombre de canaux disponibles.

La façon intuitive de réduire le délai associé à la recherche du prochain point d'accès est de réduire le nombre de canaux à chercher. En effet, le délai peut être diminué si la recherche est axée sur certains canaux seulement, au lieu de tous les canaux. Une autre méthode serait de revoir les valeurs de *MinChannelTime* et de *MaxChannelTime*.

2.3 L'authentification

L'authentification est le processus par lequel le point d'accès accepte ou rejette l'identité de la station mobile. Une fois le prochain point d'accès choisi, la station mobile va initier la procédure d'authentification en envoyant une trame d'authentification vers le point d'accès pour l'informer de son identité. Le point d'accès va ensuite envoyer, à son tour, une trame de réponse d'authentification indiquant son acceptation ou son rejet.

2.3.1 Les délais dus à l'authentification

Ce délai est encouru lorsqu'il y a des échanges de trames d'authentification. Il existe deux approches d'authentification qui sont généralement utilisées. La première c'est l'authentification à système ouvert où le point d'accès accepte toujours la station mobile sans employer une méthode d'authentification. Cette approche est souvent utilisée avec le filtrage d'adresse physique, mais ceci ne forme pas partie de la norme IEEE 802.11. La deuxième approche est l'authentification avec clé partagée, qui est basée sur le *Wired Equivalent Privacy* ou WEP. Le WEP est utilisé dans l'échange de clés de chiffrement pour sécuriser le transport de données. Le point d'accès et la station mobile sont requis d'implémenter le WEP afin de pouvoir utiliser cette deuxième méthode. L'authentification à clé partagée nécessite quatre échanges de messages comme mentionné ci-dessous :

- La station mobile fait une requête d'authentification au près de la station mobile en envoyant un message *Challenge-Request.*
- Le point d'accès renvoie un nombre aléatoire à la station mobile à travers un *Challenge-Response* message.
- La station mobile signe ce nombre aléatoire en utilisant le WEP, qui est une clé secrète pré-partagée, envoie un message *Response* au point d'accès.
- Le point d'accès vérifie que le nombre aléatoire a été signé par la bonne clé, en calculant la signature lui-même, et en comparant la valeur reçue et la valeur calculée. Une fois la vérification faite, le point d'accès authentifie la station mobile en lui envoyant un message *Approval.*

Le délai associé à l'authentification est proportionnel au nombre de messages échangés entre le point d'accès et la station mobile. Donc, le délai en utilisant l'authentification à clé partagée est plus long que celui obtenu avec une authentification à système ouvert. Si on tient compte des nouvelles techniques d'authentification utilisées dans la norme IEEE 802.11i, celles-ci génèrent un plus grand nombre de messages, et par conséquent, cela requiert un plus grand nombre d'échanges.

2.4 La réassociation

Une fois acceptée par son futur point d'accès, la station mobile va envoyer une requête de réassociation. À la différence de celle d'association, la requête de réassociation est utilisée lorsqu'une station possède déjà une association mais change de *Basic Service Set*, ou BSS. Elle envoie au nouveau point d'accès une requête de réassociation et non pas une d'association. Cela permet au nouveau point d'accès de contacter l'actuel point d'accès pour négocier l'acheminement des trames de données.

2.4.1 Les délais dus à la réassociation

La réassociation est le processus de déplacer l'association d'une station mobile d'un ancien point d'accès à un nouveau dans le même ESS. Un ESS comprend un ou plusieurs BSS interconnectés, comme l'illustre la figure 2.2; un BSS représente la couverture d'un point d'accès.

Le délai lié à la réassociation est causé par les échanges des trames de réassociation. Une fois authentifiée, la station mobile envoie une requête de réassociation et reçoit une réponse de réassociation, et ainsi se complète le *handover*. Dans un contexte sans fil, la procédure de réassociation est, plus ou moins, similaire à celle d'association; mais dans le réseau filaire, les points d'accès vont interagir pour délivrer les trames de réassociation.

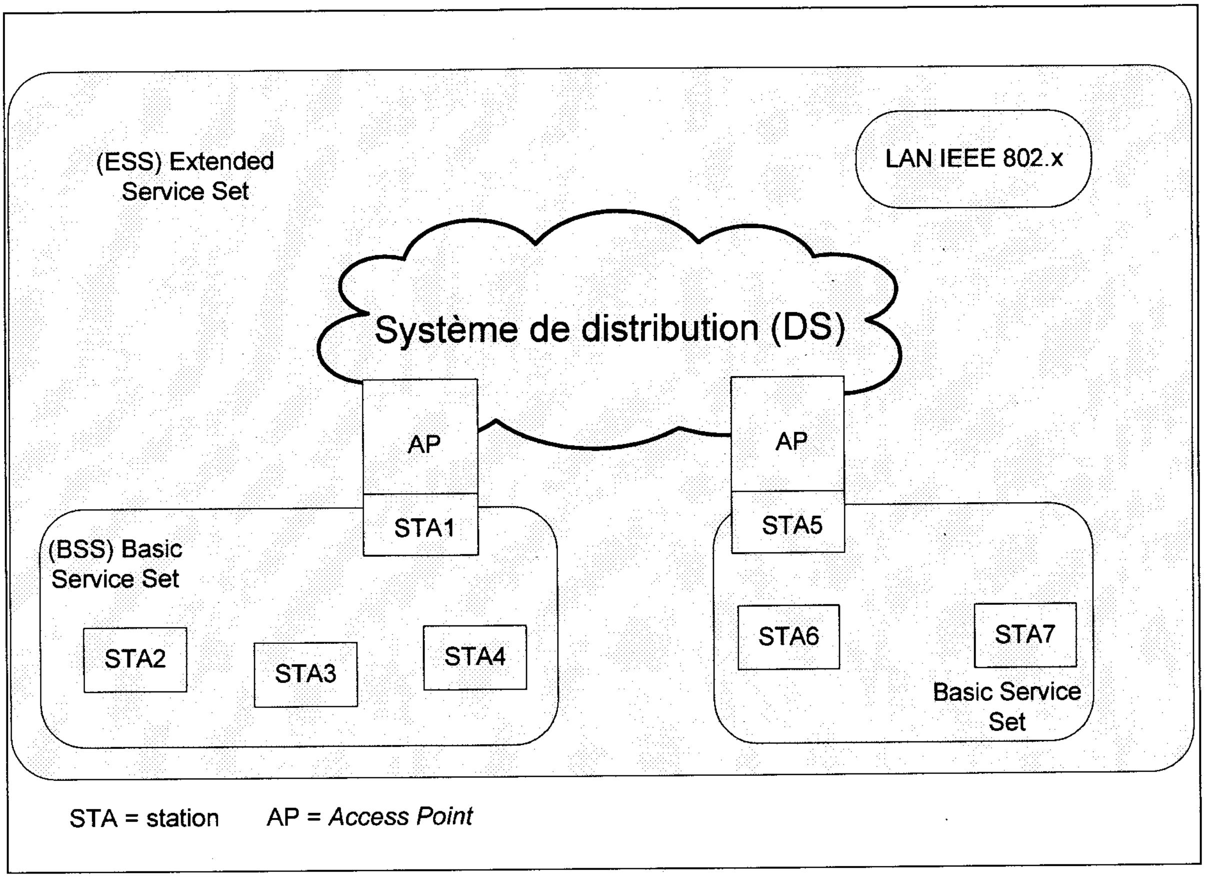

Figure 2.2: L'architecture IEEE 802.11

CHAPITRE 3: TECHNIQUES POUR RÉDUIRE LES DÉLAIS LORS DU *HANDOVER*

On peut classifier les différentes techniques proposées pour réduire le délai global associé à la procédure de *handover* en deux catégories : celles qui essaient de diminuer le délai dû à la recherche du prochain point d'accès et celles qui essaient de réduire les délais encourus lors de l'authentification et de la réassociation. Comme l'authentification et la réassociation ont les mêmes séquences d'opérations, comme l'illustre la figure 3.1 ci-dessous, ces deux procédures peuvent être considérées comme une seule.

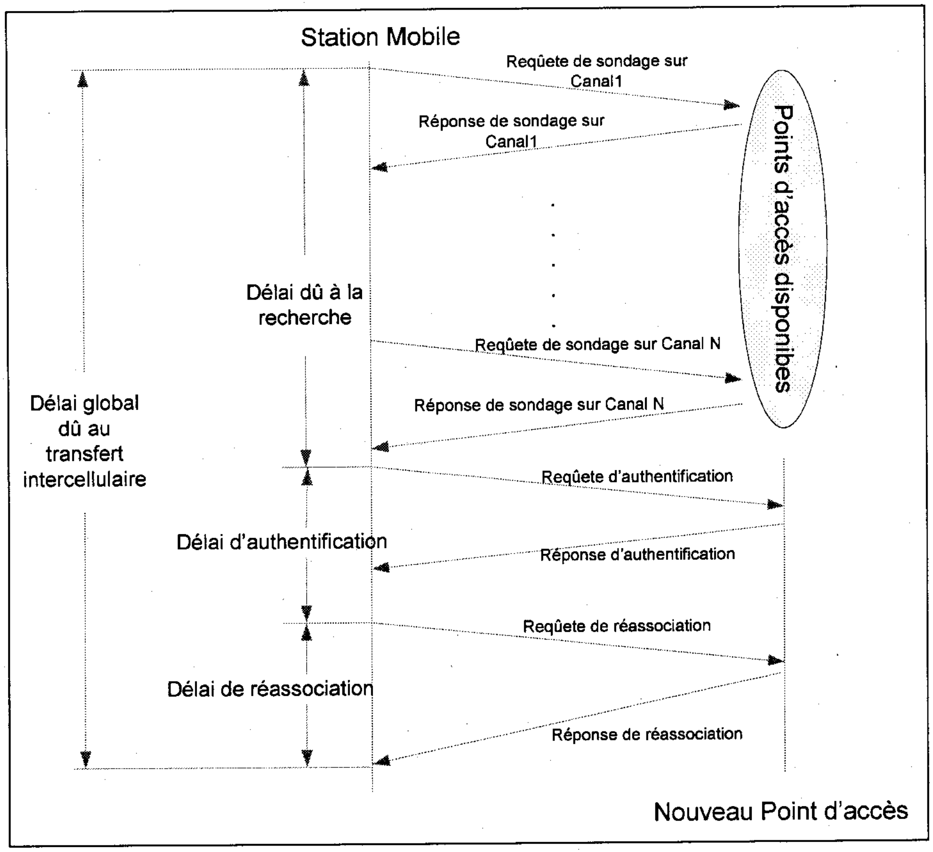

Figure 3.1: Les échanges de messages pour la procédure de *handover* dans les réseaux 802.11

3.1 Réduire le délai associé à la recherche

Mishra et al. mentionnent dans [8] que le délai associé à la recherche du prochain point d'accès est prépondérant dans le délai global de la procédure de *handover*. Donc, il est important qu'on essaie de le réduire, car ainsi, on va aussi pouvoir diminuer le temps que dure la procédure de *handover*.

Dans [11], Velayos et al. proposent une méthode rapide de détection de *handover*, qu'on appelle le *tuning scheme*. Dans cet article, les auteurs ont utilisé la distribution des pertes de trames causées par des collisions, afin de déterminer le moment optimal pour déclencher le transfert à un nouveau point d'accès. Pour réduire le temps de la procédure de *handover*, la station mobile commence la recherche d'un nouveau point d'accès dès qu'il lui semble que la raison pour laquelle il y a eu un échec dans la transmission de la trame est autre qu'une collision.

Si une transmission de trame et ses retransmissions consécutives échouent, la station mobile conclut que ceci est dû ces échecs sont causés par son mouvement, et donc, un *handover* de la liaison de communication est nécessaire. De plus, les auteurs changent la recherche en mode actif et dérivent de nouvelles valeurs pour *MinChannelTime* et *MaxChannelTime* de leurs modélisations analytiques et de leurs expériences. Plus spécifiquement, ils utilisent des valeurs inférieures à 1 ms et 10,24 ms pour le *MinChannelTime* et *MaxChannelTime* respectivement. Ainsi, en utilisant ces valeurs réduites de temps, le *tuning scheme* parvient à réduire le délai associé à la recherche du prochain point d'accèss.

Shin et al. présentent une méthode de recherche en utilisant un *neighbour graph* (NG) et un *non-overlap graph* (NOG) [12]. Cette technique, connu le *NG-pruning scheme*, se concentre sur la réduction du nombre total de canaux à balayer et aussi sur la réduction de temps passé à attendre sur chaque canal. Les auteurs suggèrent deux algorithmes : le NG et le NG-pruning. L'idée sous-jacente à ces algorithmes est de déterminer si un canal doit être balayé ou pas (fait par l'algorithme NG) et aussi, si la station mobile doit s'attendre à recevoir encore plus de messages de réponses de sondage sur un canal spécifique avant l'expiration de *MaxChannelTime* (fait par l'algorithme NG-pruning).

L'algorithme NG fait abstraction à la procédure de *handover* entre les points d'accès adjacents. L'ensemble des canaux sur lesquels opèrent les points d'accès avoisinants et l'ensemble des points d'accès avoisinants sur chaque canal peuvent être ainsi connus.

Conséquemment, la station mobile arrive à déterminer si un canal doit être balayé ou pas. L'algorithme NOG fait abstraction de la relation disjointe entre les points d'accès; deux points d'accès sont considérés disjoints seulement si la station mobile n'arrive pas à communiquer avec eux simultanément avec une qualité de connexion acceptable. Par exemple, si la distance entre deux points d'accès, *x* et *y*, est grande, une station mobile ne peut s'associer avec un seul d'entre eux. Dans ce cas, *x* et *y* sont disjoints. Donc, si la station mobile reçoit une réponse de sondage de *x*, cela implique qu'elle ne peut pas recevoir une réponse de sondage de *y*. Ainsi, avec l'algorithme NOG, la station mobile peut éliminer quelques uns des points d'accès qui sont disjoints avec le point d'accès avec lequel elle est actuellement associée.

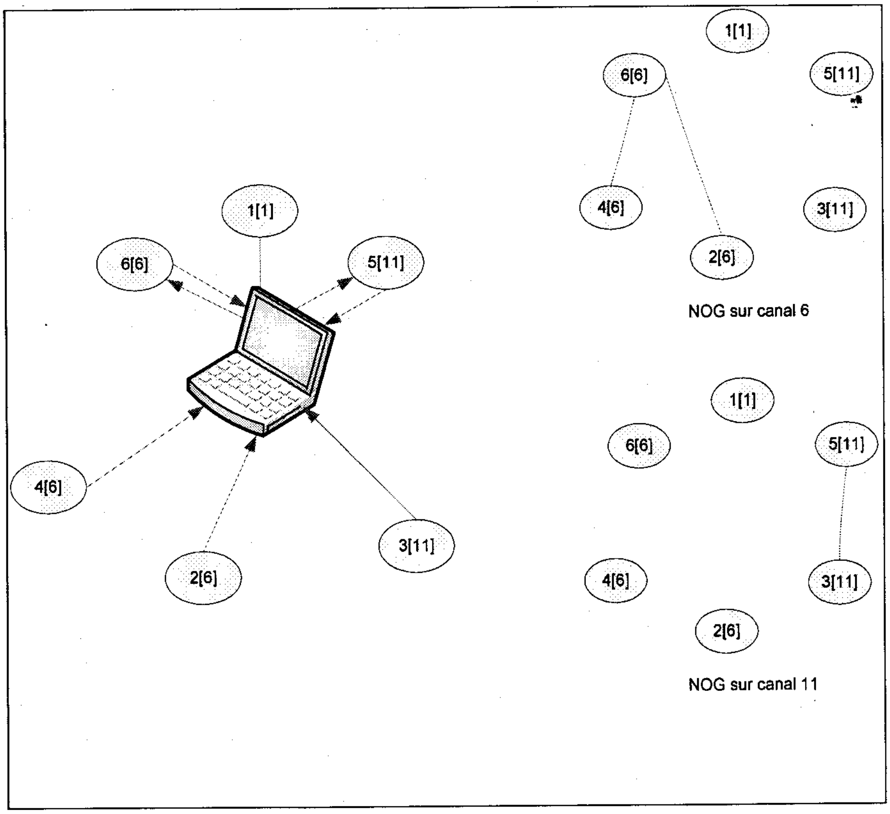

Figure 3.2: Le *NG pruning scheme*

La figure ci-dessus illustre le *NG pruning scheme*. Les points d'accès et le canal sur lequel ils opèrent sont représentés dans la figure dans le format *a*[*b*], où *a* est le point d'accès et *b* est le canal. Dans ce cas précis, seuls trois canaux sont utilisés {1, 6 et 11} et l'actuel point d'accès a cinq voisins. L'information concernant les points d'accès avoisinants peut être connue en construisant un *neighbour graph.* Ainsi, la station mobile sait qu'il y a juste deux canaux à sonder. Les NOGs sont construits pour les canaux 6 et 11 respectivement. À supposer que la station mobile sonde le canal 6 : quand elle reçoit une réponse de sondage du point d'accès 6, elle sait que c'est inutile d'attendre d'autres réponses de sondage parce que le point d'accès 6 n'est pas adjacent avec les points d'accès 2 et 4.

Shin et al. proposent dans [10] un algorithme de recherche sélective avec une cache, aussi connu comme le *channel mask scheme.* Selon cette technique, seul un sous-ensemble bien choisi de tous les canaux disponibles est sondé. La sélection du canal est faite par un *channel mask*, qui est construit quand le pilote est chargé sur la station mobile. Un balayage complet est fait initialement, et le *channel mask* est construit de l'information obtenue lors de la recherche. Dans la norme IEEE 802.11b, seul trois des onze canaux disponibles sont disjoints; donc, dans un environnement sans fil configuré en utilisant cette norme, la plupart des, sinon tous les, points d'accès fonctionnent sur les canaux 1, 6 et 11. Conséquemment, le *channel mask* est constitué en combinant les trois canaux 1, 6 et 11 et les canaux sondés durant le balayage complet initial. En utilisant ce *channel mask*, la station mobile arrive à réduire le temps qu'elle perd à sonder les canaux inexistants sur les points d'accès avoisinants. Pour mieux réduire le délai dû à la procédure de *handover*, une cache est introduite; l'idée est que chaque station mobile va utiliser la cache pour garder son historique de *handover.* Quand une station mobile s'associe avec un point d'accès, l'identité de ce dernier est insérée dans la mémoire cache. Dans l'éventualité d'un *handover*, la station mobile vérifie s'il existe dans la cache une entrée correspondante à l'adresse physique du point d'accès auquel elle veut s'associer. S'il y a une telle entrée, la station mobile peut s'associer sans avoir à faire d'autres recherches.

Ramani et al. proposent une autre solution dans [13] pour réduire le délai encouru lors des procédures de *handover.* Cette solution, appelée *SyncScan*, permet à la station mobile de surveiller continuellement la proximité des points d'accès avoisinants. En d'autres mots, la station mobile va, à intervalle régulier, sonder chaque canal pour enregistrer l'intensité de signal des canaux. Ainsi, la station mobile va maintenir une meilleure série de données sur les points d'accès avoisinants. De plus, à travers une surveillance constante sur la qualité de signal de plusieurs points d'accès, une meilleure décision quant aux *handover* peut être prise, et les délais d'authentification et de réassociation peuvent aussi être réduits. Pour réduire la perte des paquets de données pendant la surveillance périodique, le mode de sauvegarde d'énergie (*Power Saving Mode*) dans la spécification IEEE 802.11 est utilisé. Comme *SyncScan* est basé sur une surveillance régulière des points d'accès, la synchronisation du temps est très importante. Donc, pour synchroniser avec les points d'accès, le *network time protocol* (NTP) peut être modifié. Par ailleurs, si plusieurs points d'accès utilisent le même canal et génèrent des trames balises en même temps, une technique de randomisation peut être utilisée.

La figure 3.3 représente un diagramme de temps en *SyncScan*. Le paramètre *d* détermine le temps où l'envoi des trames balises se fait. Donc, tous les points d'accès opérant sur le canal 1 vont transmettre les trames balises à *T*, alors que ceux sur canal 2, vont le faire à *T* + *d*. Ainsi, la station mobile change de canal et va recevoir les trames transmises par les points d'accès. Ces opérations continuent jusqu'à ce que la station mobile apprenne l'information sur les points d'accès avoisinants.

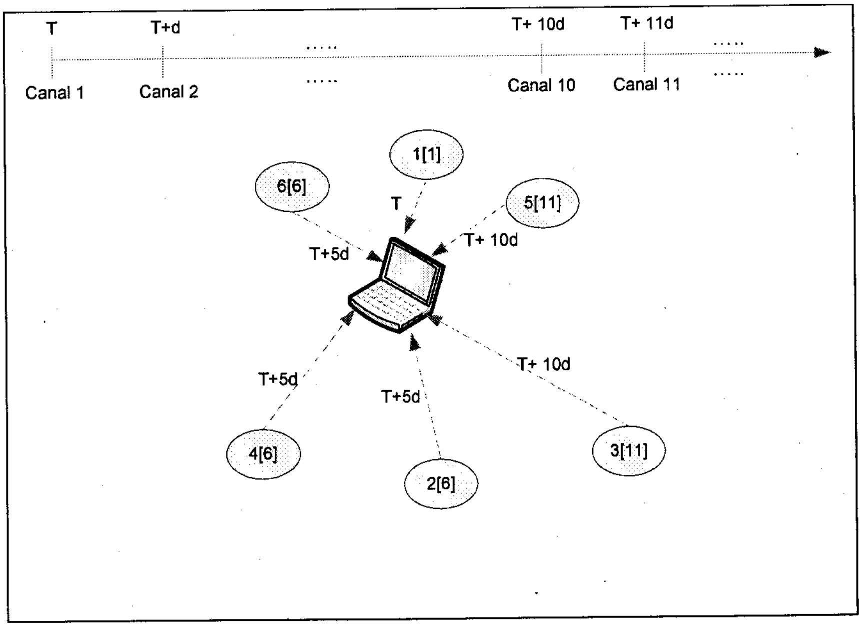

Figure 3.3: Mode d'opération de SyncScan

Brik et al. [14] introduisent une procédure de *handover* appelé *MultiScan*, qui utilise plusieurs interfaces radios. Comme *SyncScan*, *MultiScan* obtient de l'information sur les points d'accès avoisinants en sondant dès que l'opportunité se présente. Néanmoins, *MultiScan* nécessite une autre interface radio pour le sondage des canaux. L'interface primaire est associée avec le point d'accès courant et est utilisée pour la transmission des données. En même temps, l'interface secondaire sonde les canaux. Si un *handover* s'avère nécessaire, la deuxième interface est associée avec le nouveau point d'accès alors que le premier continue la transmission des données. Après la réassociation avec le nouveau point d'accès à travers l'interface secondaire, il y a un changement d'interface : le premier devient second et vice-versa. Ainsi, *MultiScan* parvient à faire un transfert de type *soft*.

3.2 Réduire les délais associés à l'authentification et à la réassociation

Bien que le délai dû sondage des points d'accès constitue une grosse partie du délai global encouru lors de la procédure de *handover*, les délais associés à l'authentification et à la réassociation doivent aussi être réduits pour atteindre des services mobiles continus. Dans la plupart des réseaux publics locaux sans fil, la technique d'authentification est basée sur un serveur central d'authentification pour assurer un service sécurisé et une meilleure gestion. Dans un tel environnement, le délai causé par la procédure d'authentification est plus long que celui observé dans des cas où l'authentification à système ouvert est utilisée. Différentes approches pour accélérer le processus d'authentification dans les réseaux IEEE 802.11 sont analysées en terme d'architecture de réseaux et de modèles de confiance par Chi et al. dans [15].

Dans [16], Pack et Choi proposent une méthode prédictive, connu comme le *FHR scheme*, pour réduire les délais encourus lors de l'authentification et de la réassociation. Les détails d'authentification de la station mobile sont distribués à plusieurs points d'accès, dépendant de son modèle de mobilité et du niveau de service. Pour prédire le modèle de mobilité de la station mobile, le concept de *Frequent Handoff Region* ou FHR est introduit; le FHR est un groupe de points d'accès qui ont les plus grandes probabilités d'être sondés par la station mobile dans un futur proche. Il est construit à partir de la fréquence que se fait le *handover*, et selon la priorité de la station mobile vis-à-vis du système centralisé. Il est peut être facilement implémenté, basé sur le modèle IEEE 802.1x [17]. Selon les mesures qui ont été faites lors des études par Schwab et Bunt [7], le nombre de points d'accès auxquels peut s'associer une station mobile est limité à deux ou trois. De ce fait, dans la méthode FHR, les détails d'authentification de la station mobile sont distribués à un sous-groupe de points d'accès avoisinants, qui sont situés à un maximum de deux bonds du point d'accès actuel.

Le triangle dans la figure 3.4 illustre le FHR du point d'accès 4. Après un *handover* du point d'accès 4 au point d'accès 2, le FHR de ce dernier est illustré par les points d'accès dans la zone elliptique de la figure 3.5.

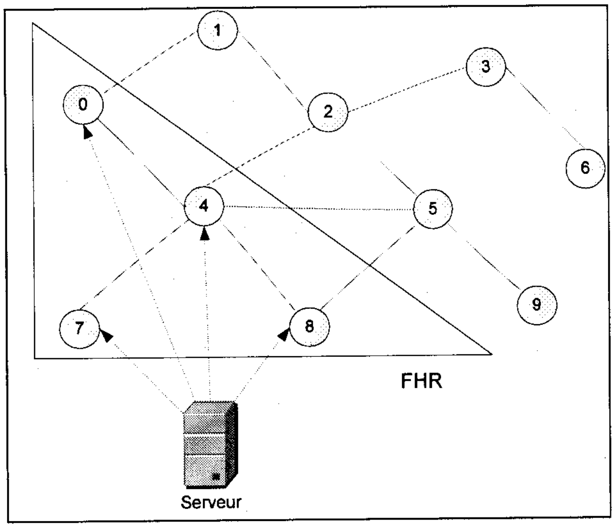

Figure 3.4: Ouverture de session au point d'accès 4

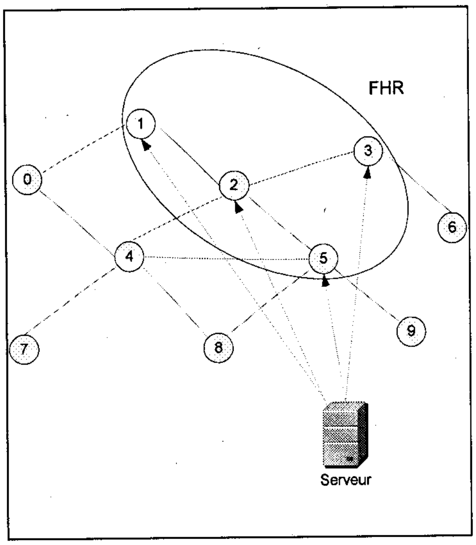

Figure 3.5: *Handover* de la session de communication du point d'accès 4 au point d'accès 2

Au lieu d'utiliser un système centralisé, une méthode proactive basée sur une structure de cache distribuée est proposée par Mishra et al. dans [18]. Elle est appelée le *proactive neighbour caching* (PNC). La méthode PNC utilise un *neighbour graph*, qui capture de façon dynamique la topologie mobile du réseau sans fil dans le but de positionner à l'avance le contexte de la station mobile. Il s'assure que le contexte de la station mobile est toujours envoyé un bond en avant, et ainsi, le délai durant le transfert peut être substantiellement diminué. Loughney et al. stipulent dans leur travail [19] que le contexte inclut l'information concernant la session de la station mobile, la qualité de service, et la sécurité. Le *neighbour graph* est construit à partir des données échangées durant le transfert de la station mobile, et il est maintenu à chaque point d'accès de façon distribuée. Le contexte envoyé est sauvegardé dans la cache et une politique de remplacement de cache peut être utilisé si toutefois la cache est remplie. La méthode PNC a été inclut dans la spécification IAPP de l'IEEE 802.11f [9], qui est la norme pour la communication entre les points d'accès.

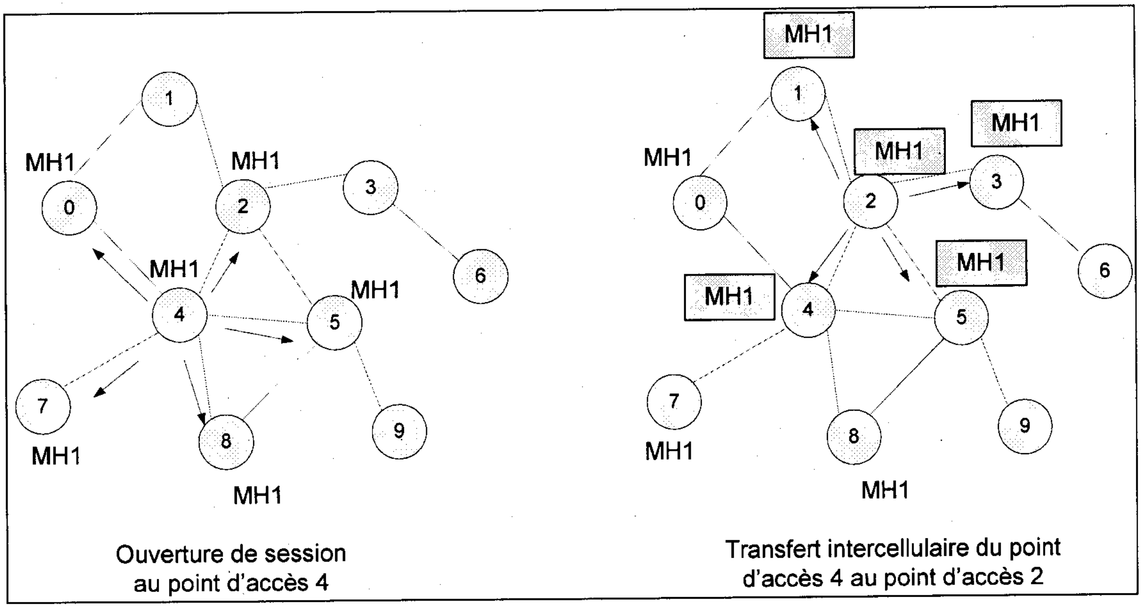

Figure 3.6: La méthode PNC

La méthode PNC préconise que le contexte de la station mobile soit envoyé à chaque nouvelle réassociation. Donc, il y aura un fort surplus de débit de signaux, surtout s'il y a plusieurs points d'accès dans le réseau sans fil IEEE 802.11. Comme indiqué dans la norme IEEE 802.11g [5], le nombre de points d'accès auxquels peut s'associer une station mobile est limité à deux ou trois. Ainsi, la diffusion du contexte de la station mobile à un sous-groupe de points d'accès avoisinants peut s'avérer suffisant pour atteindre des services mobiles continus.

La figure 3.6 illustre l'application de la méthode PNC sur le point d'accès 4. Les nœuds avec une notation MH1 représentent les points d'accès qui sont à un bond du point d'accès 4 et sont à la gauche de la figure. Lorsqu'il y a un *handover* du point d'accès 4 au point d'accès 2, les nouveaux voisins du point d'accès 2 sont déterminés par la notation grisée MH1.

CHAPITRE 4: ARTICLE DE CONFÉRENCE LCN ON-MOVE OCTOBRE 2008

Avant-propos

Auteurs et affiliation:

B.S.Gukhool : étudiant à la maîtrise, Université de Sherbrooke, Faculté de Génie, Département de génie électrique et génie informatique

S.Cherkaoui : professeure, Université de Sherbrooke, Faculté de Génie, Département de génie électrique et génie informatique

Date d'acceptation : Juin 2008

État de l'acceptation : Version finale publiée

Conférence : IEEE LCN ON-MOVE 2008

Référence : [34]

Titre français : La modélisation d'IEEE 802.11p dans NS-2

Contribution au document : Ce chapitre donne un aperçu du travail fourni pour développer un *framework* dans le simulateur de réseaux NS-2 [33], pour modéliser les comportements attendus des réseaux véhiculaires opérant avec la technologie IEEE 802.11p et bien que le modèle développé au stade de cet article soit simple, les résultats obtenus lors des simulations sont encourageants. D'ailleurs, il arrive à rencontrer parfaitement l'une des critères essentielles que toute modélisation de IEEE 802.11p doit pouvoir satisfaire, c'est-à-dire, assurer un pourcentage de paquets perdus durant un session de communication du véhicle à l'infrastructure routier inférieur à 10 %, et ceci pour des paquets long de 1000 octets et une vitesse allant jusqu'à 140 km/h. Ainsi, ce chapitre démontre non seulement que le modèle développé par l'auteur de cet écrit, sous la supervision de la professeure Cherkaoui, respecte les spécifications de la norme IEEE 802.11p mais aussi que cette norme est adaptée aux communications dans les réseaux véhiculaires.

Résumé en français : Afin de développer une plateforme pour évaluer les performances des différentes technologies sans-fil pour les réseaux véhiculaires, les auteurs ont étudié la structure interne du simulateur, NS-2, ainsi que la norme de technologie sans-fil, IEEE 802.11p. Cette plateforme vise à répliquer dans la mesure du possible les caractéristiques de la norme IEEE 802.11p dans le simulateur et avec l'aide de scénarios réalistes, a l'intention de donner une vue objective de la performance des applications destinées aux transports intelligents. Le but primaire de cette plateforme est de pouvoir satisfaire les attentes des communications du véhicule à l'infrastructure, avec une possibilité plus tard de l'étendre afin d'accommoder des communications inter-véhiculaires dans les réseaux ad hoc.

Note : À la suite des corrections demandées par les membres du jury, le contenu de cet article diffère dans la forme de celui qui a été accepté.

4.1 Abstract

In an effort to develop a simulation framework for evaluating the performance of wireless access technologies for vehicular networks, the authors have studied the internal structure of the simulator, NS-2, as well as the draft wireless technology IEEE 802.11p. This intended framework aims at replicating, as far as possible, the access technology characteristics in the simulator and with the help of realistic scenarios intends to give an objective view of the performance of applications destined for Intelligent Transport Systems. The framework is first designed to meet the requirements set for vehicle to infrastructure communications, with a view of later extending it to vehicle to vehicle communications for vehicular ad hoc networks.

4.2 Keywords

DSRC, WAVE, IEEE 802.11p, NS-2

4.3 Introduction

Vehicular networks have a major role to play in increasing the extent of pervasive computing. With services and applications specially suited for vehicular communications are being designed, it is necessary that to ensure that the communications technology used is secure, reliable and fast. In that perspective, the US FCC has allocated a block of spectrum to enhance the safety and productivity of the transportation system. From a networking viewpoint, accommodating a wireless access technology for a highly mobile and insecure environment needs time and attention, and hence, it is necessary to have the necessary framework to evaluate the performance of that access technology. An IEEE working group has started working since long on a draft amendment, IEEE 802.11p, to the legacy IEEE 802.11. This new flavour of wireless access would be dealing with security through specialized frames, reliability with a QoS feature and fast communications. This work implements most of the features described in the draft version of IEEE 802.11p [20] on the network simulator, NS-2, so as to evaluate its performance in a vehicular network context.

4.4 Vehicular Access Technologies

4.4.1 Dedicated Short Range Communications (DSRC)

DSRC is a short to medium range communications service that supports both public safety and private operations in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz) in vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication environments. Armstrong Consulting [25] mentions that DSRC is meant to be a complement to cellular communications by providing very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones are important.

4.4.2 Wireless Access in Vehicular Environments (WAVE)

WAVE is a mode of operation used by IEEE 802.11 devices to operate in the DSRC band. It is based on the IEEE P1609 series of standards, which define the architecture, the communications model, the management structure, the security and physical access features for vehicular communications. The primary architectural components are the Road-Side Units (RSUs), the OnBoard Units (OBUs), and the WAVE interface.

The IEEE P1609 series comprise of the following standards and each of them deals with a specific area.

- IEEE P1609.1 [27] is about the WAVE Resource Manager. It describes the key components of the WAVE system architecture and defines data flows and resources as well as the command message formats and data storage formats. It also specifies the types of devices that may be supported by OBUs.

- IEEE P1609.2 [28] deals with the Security Services for Applications and Management Messages. It defines the secure message formats and processing and the circumstances for using secure message exchanges.

- IEEE P1609.3 [29] is about the Networking Services. It defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange. It also describes the WAVE Short Messages (WSM), providing an efficient

WAVE-specific alternative to IP that can be directly supported by applications. It also deals with the Management Information Base (MIB) for WAVE protocol stack.

- IEEE P1609.4 [30] describes the enhancements to 802.11 MAC to support WAVE.

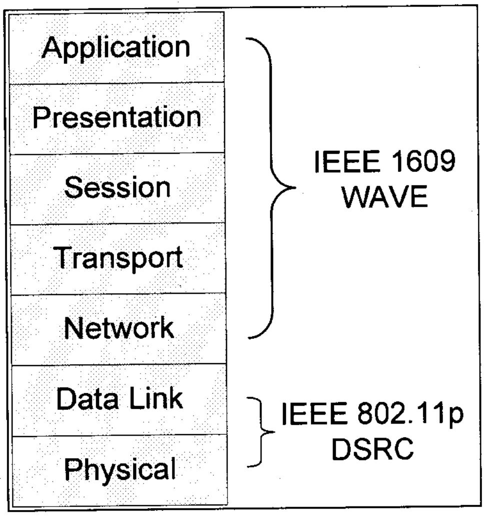

Figure 4.1: WAVE Protocol Stack

4.4.3 IEEE 802.11p

IEEE 802.11p [20] is a draft amendment to the IEEE 802.11 [2] standard to add support for WAVE. It defines enhancements to 802.11 required to support Intelligent Transport Systems (ITS) applications. It deals essentially with the data link and physical layers of the OSI model, as shown by figure 4.1; its purpose is to provide wireless communications short distances between:

- roadside and mobile radio units
- mobile units
- portable and mobile units

4.5 Characteristics of IEEE 802.11p

The changes brought to the baseline IEEE 802.11 Standard [2] are required to support longer ranges of communication (up to 1000 meters), the high mobility of the vehicles, the extreme multipath environment, the need for high quality of service in overlapping networks, and the nature of the applications to be supported.

4.5.1 The WAVE Approach

The standard [20] specifies that the total time from first signal detection to completion of frames of data exchange within order of 100 ms and that the system should operate with a Control Channel (178) and eight Service Channels. The following table shows the channel allocation for DSRC applications.

Tableau 4.1: WAVE OPERATING CHANNELS

Operating channel numbers	Channel center frequencies (MHz)	Purpose
172	5860	Safety channel
174	5870	Service channel
175	5875	Service channel
176	5880	Service channel
178	5890	Control channel
180	5900	Service channel
181	5905	Service channel
182	5910	Service channel
184	5920	Safety channel

The control channel is used for broadcasting transmissions and establishing communications whereas the service channels are used to conduct two-way communications between RSUs and OBUs and between OBUs. Thus, the extremely dynamic vehicular environment can use the same radio technology and still accommodate priority to public safety communications.

4.5.2 WAVE operations

Broadcast messages are generated by an RSU or OBU and the Provider-User connection is established when a provider transmits a Provider Service Table and a user acts on this message. It is to be noted that RSUs generate and broadcast beacons, whereas OBUs generate and broadcast action frames. On start-up, the WAVE device operates on the control channel. The service user devices listen for beacon frames containing the Extended Service Set (ESS)'s Service Set ID (SSID).

WAVE beacons include a WAVE Service Information element (WSIE), which contains the Provider Service Table (PST), the Routing Advertisement, and the Broadcast Service Information. PSTs advertise applications and identify a service channel for each application.

4.5.3 WAVE PHY specifications

Messages are to be transferred to and from vehicles each travelling at speeds of up to 140 km/h with a Packet Error Rate (PER) of less than 10 % for Physical layer Service Data Unit (PSDU) of 1000 bytes and to and from vehicles at speeds up to a minimum of 200 km/h with a PER of less than 10% for PSDU of 64 bytes. [20]

The physical model is intended to use an Orthogonal Frequency-Division Multiplexing (OFDM) implementation as it provides WAVE with data payload capabilities of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbit/s in 10 MHz channels. Any DSRC device operating in WAVE mode should be able to transmit and receive at data rates of 3, 6, and 12 Mbit/s. Furthermore, provision has also been made for additional data payload capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s using optional 20 MHz channel combinations.

4.6 How DSRC Works

RSUs broadcast to OBUs, at a frequency of 10 times per second, the type of applications which it supports and on which channel. The OBU listens on channel 178, authenticates RSU digital signature. It executes safety applications first, if there are any, and then switches channel to execute non-safety applications. When there are no more applications to be run, the OBU returns to the control channel and listens to the broadcasts as mentioned by Bill Jones of the ITS Joint Program Office [26].

4.7 IEEE 802.11p implementation in NS-2

This implementation models communication from the vehicles to the infrastructure or the road side units and vice-versa. It is based on the actual IEEE 802.11 implementation, shown below (figure 4.2), in NS-2, as of ns-2.30 and it has also been successfully tested with and patched to ns-2.31.

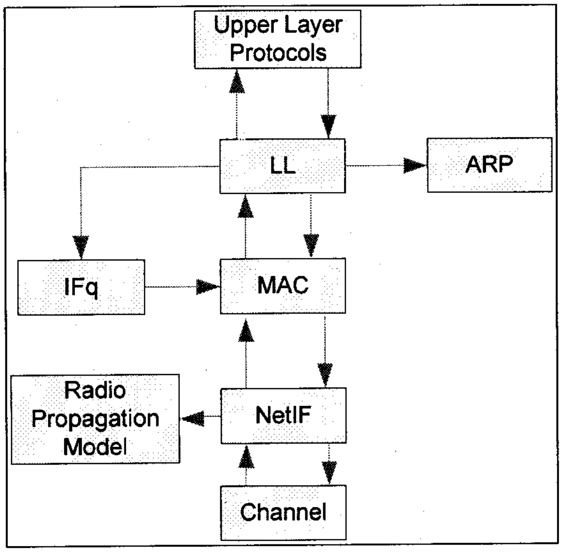

Figure 4.2: IEEE 802.11 model in NS-2

4.7.1 The physical layer

This section describes the most important changes brought to the current model.

4.7.1.1 OFDM implementation

A class called *OFDMPhy* has been defined and the corresponding simulation object has been created to integrate the ODFM properties into the physical layer of the IEEE 802.11p model. *OFDMPhy* inherits from the *WirelessPhy* class, which is already defined in NS-2, and thus, in addition to the inherited functions and attributes, also defines supplementary functions to access and modify the modulation rate used (BPSK, QPSK or QAM) and the status of the OFDM module. Just like for the inherited attributes like frequency or transmission power that can be configured in the TCL simulation script, the new attributes can also be set by TCL meaning that TCL bindings have been used to do the corresponding configurations. The MAC layer allocates bursts that can use different modulations according to distance or interference. This affects the data rate and transmission time.

The physical layer can be in different states. When in sending mode, all incoming packets are discarded. In receiving mode, packets cannot be sent. Thus, it perfectly simulates the half-duplex characteristic of IEEE 802.11p. Furthermore, the packet header contains virtual information, such as frequency and modulation, which are used to filter incoming packets.

The *node_on* and *node_off* functions enable or disable blocking all transmissions and receptions of packets, but is not currently linked to any power consumption mechanisms.

Timers

The OFDM implementation also needs different timers that do not exist in the current IEEE 802.11 model in NS-2. These required timers have thus been defined to model the OFDM properties.

Channels

Since base stations supporting IEEE 802.11p will be operating with 6 service channels, 2 safety channels and 1 control channel, it is necessary to implement a multi-channel model. In this current work base stations can have multiple channels assigned to them. The difference between the implementations of the control channel and of the service channels is that on the control channels only management frames are transmitted. A new simulation object called *ConnectionsManager* is created to help the base stations keep track of the connections they have with the various mobile nodes. A connection, in this case, consists of the MAC address of the destination node and the channel the destination node is transmitting.

Channel configuration can be done through the TCL simulation script and there is no need to recompile the NS-2 installation. This feature helps in saving time and reducing code complexity and eases the process of writing the simulation scenario.

4.7.2 The MAC layer

The *mac802_11p* is a subclass of the *Mac* class. It is an abstract class that contains the common elements of the base station (BS) and mobile station (MS). For example it stores the MAC management information base (MIB) and PHY MIB. It is the interface with other layers for sending and receiving packets. The draft standard [20] intends to make use of dynamic MAC addresses for communications in the IEEE 802.11p although no further information is provided on that feature. With respect to that, the standard includes a MAC level function to re-generate MAC address of a node, a function which is only applicable to the use of dynamic MAC addresses. In *mac802_11p*, although no dynamic MAC addressing has been used, a function to restore a node to its previous MAC object is implemented.

802.11p packet

A new simulation object is created to have the packets meet the requirements of IEEE 802.11p. For instance, an additional field has been added in the packet header to indicate whether the mobile station is operating on WAVE mode. WAVE mode is simply an indication of how it is expected that that the mobile station behaves and what are the types of services and applications available to the mobile station in that condition. Furthermore, since safety and broadcast channels should have priority over normal service channels, a priority field is introduced in the packet definition and the packet is classified to the priority channel by a MAC-level classifier.

802.11p base stations

Base stations are defined with a MAC called *mac80211_pBS* which is a subclass of the abstract class *mac802_11p*. The reason for this separation of MAC interface for base stations and subscriber stations is because those two entities will deal with different objects. The MAC used for subscriber stations is described in the next section. *mac80211_pBS* includes data about the different nodes connected, which channels they are using and also provision has been made for some future work concerning handovers in IEEE 802.11p networks. With that respect, fields containing information about the neighbouring IEEE 802.11p base stations, if there is any, are kept. This information is not currently applicable to the scope of this work.

802.11p subscriber stations

Subscriber stations are also characterized with a different MAC entity, *mac80211_pSS* that inherits from the abstract class *mac802_11p*. *mac80211_pSS* maintains a record of the current base station connected with. It also keeps track of the list of neighbouring subscriber stations in case there is the need to set up a vehicular ad hoc network. This is a step for some future work although this article does not deal with ad hoc networks. Information about the state in which the subscriber station is currently is also kept, for instance, a subscriber station can be connected. Furthermore, the basis of some foundation work on handovers is set by keeping some information about the different handover status of the subscriber stations.

4.8 Simulation

4.8.1 Simulation Setup

The simulation environment used is ns-2.31 which has been installed using the allinone version on Cygwin. The simulation is run to verify whether the IEEE 802.11p model for NS-2 meets the WAVE PHY specification of having messages transferred to and from vehicles each travelling at speeds of up to 140 km/h with a Packet Error Rate (PER) of less than 10 % for PSDU of 1000 bytes.

The setup consists of one base station and two mobile subscriber stations, as shown by figure 4.3.

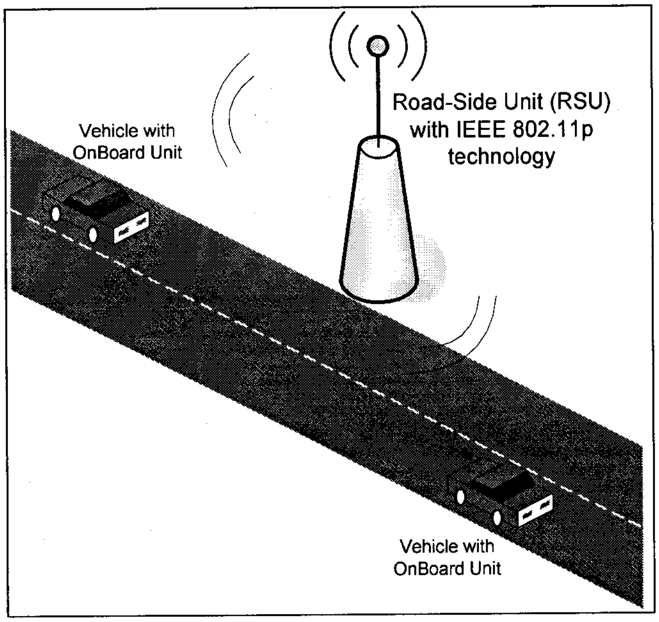

Figure 4.3: Simulation Setup

Two sets of simulation are run independently of each other. The first set has the base station and the subscriber stations defined with the IEEE 802.11p PHY and MAC, while for the second set, IEEE 802.11a values are used. IEEE 802.11a is used because it has been utilized in research previously by Cottingham et al. in [32] to replicate vehicle communications in urban region, where the speed does not surpass 70km/hr.

In both cases, the transmission range of the base station is set to 1000m to reflect DSRC standards and hence, the overall distance over which transmissions are evaluated is 2000m. The propagation model used is the Shadowing model as it is the most realistic propagation model currently available in ns-2.31 for outdoor communications [12]. ICMP messages 1000 bytes long are transmitted from each mobile node to the base station and it is the average number of packets lost, rounded to the nearest integer, that it is taken into account. The frequency of sending the ICMP echo request packets is set to 1 second. This procedure is repeated for both sets of simulation with the subscriber stations moving at speeds of 90, 100, 110, 120, 130, and 140 km/hr.

As it is of now, the current model does not support the feature to calculate the PER of transmissions. However, Awoniyi and Tobagi in [31] mention that since packet loss is a function of PER, the number of packets lost would be used as the evaluating criterion in both sets of simulation.

4.9 Results

Tableau 4.2: SIMULATION RESULTS

Speed (km/hr)	Packet loss percentage for IEEE 802.11p configuration (%)	Packet loss percentage for IEEE 802.11a configuration (%)
90	2.45	54.3
100	4.11	58.3
110	4.62	58.4
120	6.67	59.9
130	8.93	62.5
140	9.80	70.6

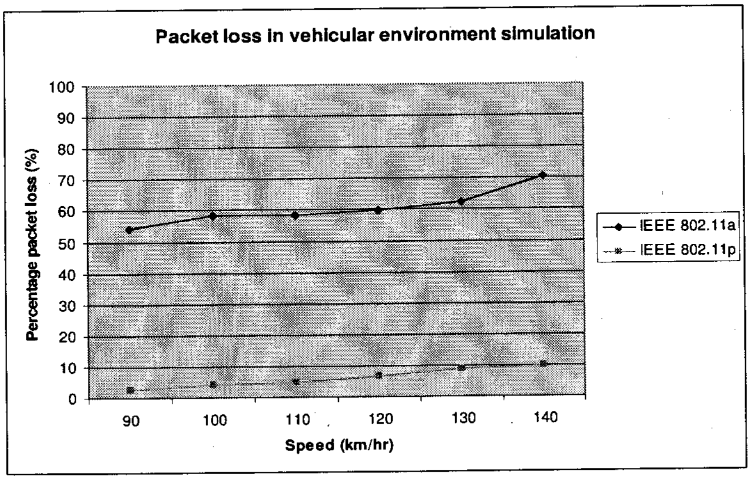

Figure 4.4: Graphical representation of the results obtained

Figure 4.4 and Tableau 4.2 show that the model emulating IEEE 802.11p gives a much improved performance as compared to the simulation configured with IEEE 802.11a parameters. The percentage of packet loss at a speed of 140 km/hr is slightly less than 10 % for packets 1000 bytes long which shows that the model is able to cater for high mobility vehicular environments and thus satisfies one of the primary prerequisites of the IEEE P802.11p draft standard.

4.10 Future work

The model is still being developed to meet all the requirements set by the IEEE P802.11p draft edition. Since the draft standard deals essentially with V2I communications, one area of interest would be to see how the model behaves with handovers and how it can be adapted to ensure a seamless handoff. Furthermore, the model is to be tested with an even higher mobility scenario. Moreover, the model has been conceived to work in a homogeneous wireless environment, just like with most of the wireless NS-2 development modules, but it could be extended to ensure that it works with other wireless access technologies, such as WiMAX, in a heterogeneous network.

4.11 Conclusion

DSRC is a promising avenue to explore for vehicular communications and, with the IEEE P802.11p standard, it seems that pervasive computing is just a few steps away from being extended to the world of vehicles. Through this paper, it has been shown P802.11p is an effective communication medium for vehicular networks especially for V2I transmissions.

CHAPITRE 5: ARTICLE DE CONFÉRENCE WOCN AVRIL 2009

Avant-propos

Auteurs et affiliation:

B.S.Gukhool : étudiant à la maîtrise, Université de Sherbrooke, Faculté de Génie, Département de génie électrique et génie informatique

S.Cherkaoui : professeure, Université de Sherbrooke, Faculté de Génie, Département de génie électrique et génie informatique

Date d'acceptation : Mars 2009

État de l'acceptation : Version finale publiée

Conférence : IEEE-IFIP WOCN 2009

Référence : [36]

Titre français : Le *handoff* dans des réseaux véhiculaires utilisant la norme IEEE 802.11p.

Contribution au document : Ce chapitre continue dans la même voie que le travail décrit durant le chapitre précédent. Le *framework* développé est étendu pour accommoder des situations de *handover*. D'abord, il a fallu faire une étude au niveau des trames existantes pour la gestion (*management frames*) pour en ajouter celles qui manquaient pour avoir un meilleur contrôle de la procédure de *handoff*. Ensuite, la technique d'utiliser des *caches* est implémentée dans le *framework* pour réduire les délais encourus lors changement de point d'accès. Ainsi, ce chapitre démontre que le modèle développé par l'auteur de cet écrit, sous la supervision de la professeure Cherkaoui, arrive à maintenir une qualité de communication plus qu'acceptable lors des sessions dans des réseaux véhiculaires où la mobilité atteint les 200 km/h et surtout lorsque le *handover* est encouru.

Résumé en français : Afin de développer un environnement de simulation pour évaluer la performance des technologies d'accès sans-fil pour les réseaux véhiculaires, les auteurs ont développé un module pour émuler les comportements et caractéristiques de la norme sans-fil IEEE 802.11p dans le simulateur NS-2. Ce modèle a été étendu pour accommoder des mécanismes pour gérer le *handover*, ceci afin de pouvoir donner un aperçu objectif de la performance des applications destinées pour les systèmes de transports intelligents. Ce modèle est, à notre connaissance, le premier qui est ouvert à la communauté de recherche tout en rencontrant les critères des communications faites en mode infrastructure, avec une attention spéciale placée sur le procédé de *handover*.

Note : À la suite des corrections demandées par les membres du jury, le contenu de cet article diffère dans la forme de celui qui a été accepté.

5.1 Abstract

In an effort to develop a simulation framework for evaluating the performance of wireless access technologies for vehicular networks, the authors have developed a simulation framework for the draft wireless technology IEEE 802.11p within the simulator NS-2 [34]. Furthermore, handoff mechanisms for the draft technology have also been added to the framework. The latter aims at replicating, as far as possible, the access technology characteristics in the simulator and with the help of scenarios intends to give an objective view of the performance of applications destined for Intelligent Transport Systems. The framework is, in our knowledge, the first framework open to the research community designed to meet the requirements set for vehicle to infrastructure communications, with special attention being paid to the handover process in the infrastructure mode of operation of IEEE 802.11p.

5.2 Keywords

WAVE; IEEE 802.11p; NS-2; Handover

5.3 Introduction

Wireless access technologies are evaluated and tested on a regular basis to determine their suitability in vehicular networks. The highly mobile nature of vehicular networks makes the continuous proper transmission of information, with regards to applications being run in those networks, a challenge. The IEEE has designated a working group to draft a amendment, IEEE 802.11p, to the legacy IEEE 802.11 standard to accommodate vehicular networks and applications. Given the limited outdoor range of current IEEE 802.11-based technologies, one of the aims of the amendment is to be able to sustain a transmission range of 1000 meters. This would undoubtedly limit the number of access points (AP) or roadside units (RSU) to be placed along the routes taken by vehicles. Nevertheless, the high speeds of those mobile units demand that the transmission of a communication session between a vehicle and a particular RSU to the next available RSU be done with the minimum disruption possible and over an acceptable duration. In this work, the authors continue to develop the IEEE 802.11p model in NS-2 [34] to involve handoff mechanisms and present a qualitative analysis of the results obtained for V2I handovers.

5.3.1 IEEE 802.11p

IEEE 802.11p [20] is a draft amendment to the IEEE 802.11 [2] standard to add support for WAVE. It defines enhancements to 802.11 required to support Intelligent Transport Systems (ITS) applications. It deals essentially with the data link and physical layers of the OSI model, as shown by figure 5.1; its purpose is to provide wireless communications short distances between:

- roadside and mobile radio units
- mobile units
- portable and mobile units

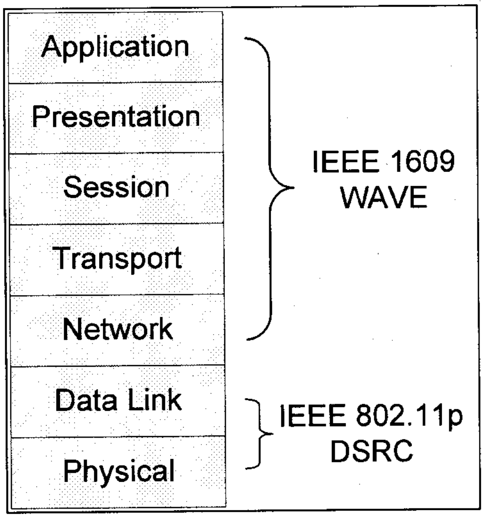

Figure 5.1: WAVE Protocol Stack

5.3.2 Handoffs in IEEE 802.11-based networks

In IEEE 802.11-based mobile networks, a handover or handoff is the process that allows a wireless mobile station to change the access point it is associated with. When a mobile unit moves out of the range of an AP into another's range, the handover occurs during which there is an exchange of management frames. This transfer, however, involves a certain latency that may give rise to disruptions in an already active communication session. The overall handoff latency can be divided into three categories:

- the probe delay, which makes up for up to 90% of the total handoff latency [8],
- the de-authentication and authentication delay
- the re-association delay.

Figure 5.2 depicts the overall exchange of frames during the handoff and the respective latencies. In this work, the authors have considered implementing a handover mechanism that deals essentially with the probe delay given the high mobility prevailing in vehicular networks.

5.4 NS-2

Network Simulator 2, or NS-2, is an open-source simulator essentially used to simulate both wired and wireless networks. It has an inherent IEEE 802.11 model that by default simulates IEEE 802.11b. Although it is a quite popular simulator, NS-2's wireless models are not very accurate and as such can give erroneous results that can lead to inappropriate conclusions.

5.4.1 Handoff in NS-2

The IEEE 802.11 baseline implementation in NS-2 is fairly simple and straightforward. In the ns-allinone-2.31 version of the simulator, a look at the aforementioned model gives an inkling of about how it operates. Figure 5.3 illustrates the different modules developed for the IEEE 802.11.

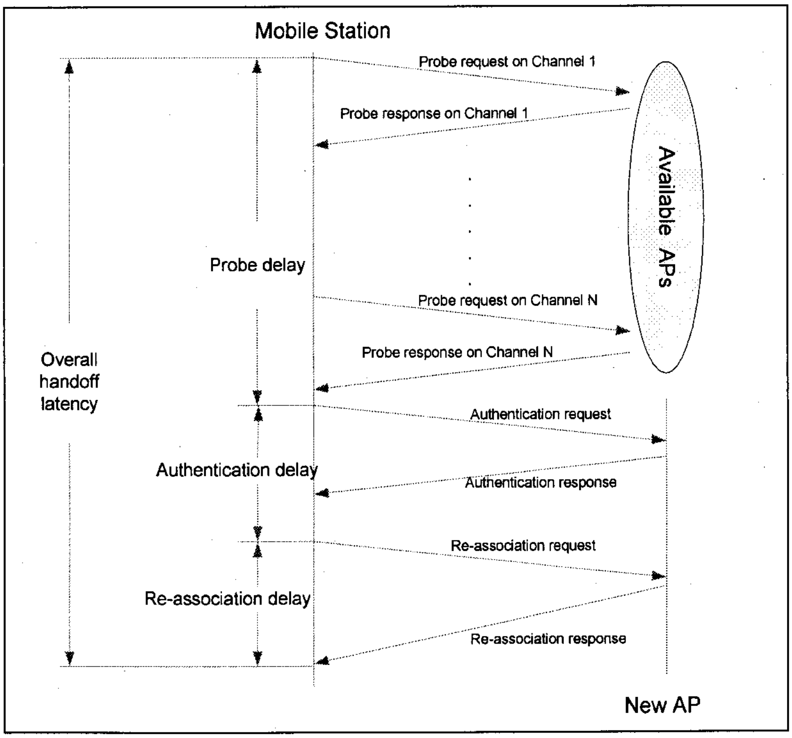

Figure 5.2: Exchange of management frames during handoff

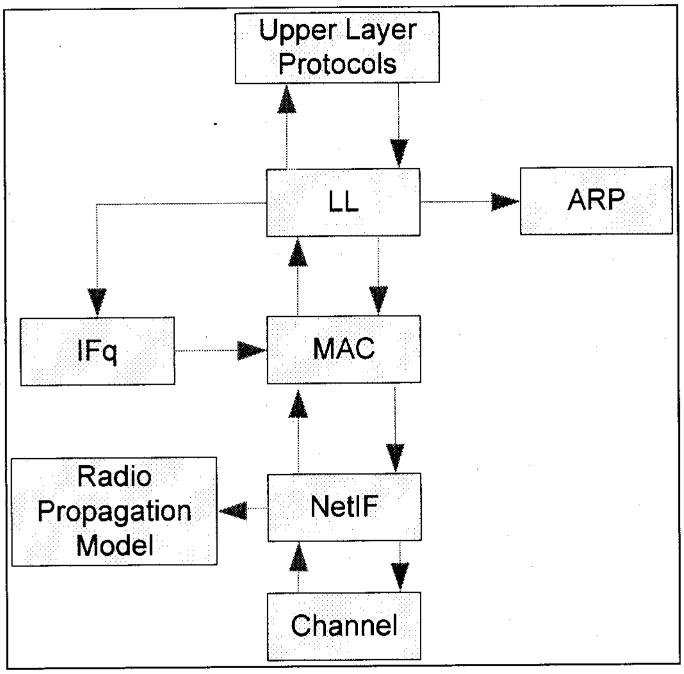

Figure 5.3: IEEE 802.11 model in NS-2

The only frames defined in the default implementation, together with the frame control field and the MAC header, are the control frames that are:

- the request-to-send (rts) frame
- the clear-to-send (cts) frame
- the acknowledgement (ack) frame

Even though a node can be assigned to be an AP, it does not necessarily function as an AP should, especially as far as handovers are concerned, due to the lack of exchange of management frames, frames which are non-existent from the start.

The oversimplification of the default IEEE 802.11 model since there is no scanning, no beacons sent by APs amongst other things, re-emphasises the need for a better handoff model especially in the case of vehicular networks.

5.5 Implemented Handoff Model

Several handoff models have been designed and proposed to reduce the overall latency associated with the process. Given the high speeds in vehicular networks, having a handover scheme causing a minimum delay and with a low level of disruption in the communication sessions is a fundamental.

In this work, the authors have chosen to go with the handover scheme proposing a cache system at the AP. This system has already been proposed [18] and there have been other works that have proposed variants of a caching mechanism at APs to reduce the probe latency, and accordingly reduce the overall handoff delay.

5.6 IEEE 802.11p Handoff in NS-2

This implementation models communication from the vehicles to the infrastructure or the road side units and vice-versa. It is based on the work done in [34], and has been tested with the allinone version of 2.31 under both Cygwin running on Microsoft Windows XP SP2 and the Linux-based, Ubuntu.

5.7

5.7.1 Management Frames

Since any handover solution in IEEE 802.11-based technologies requires the exchange of management frames, which are not available in the NS-2 default environment mentioned above, it is necessary to define the frames that are to be involved. The following frames have been added to the *mac802_11ppkt* [34] class:

- the beacon frame, which is to be sent by the APs.
- the disassociation frame sent from the mobile node (MN) to the AP.
- the association request and response frames, sent when the MN first moves into a Basic Service Set (BSS).
- the re-association request and response frames
- the probe request and response frames, for scanning the channels and hence, the most appropriate AP.
- the authentication and de-authentication frames.

Furthermore, some other changes have been brought to already existing frames, like the addition of a QoS field and a WAVE Information Element (WIE) field in the MAC header.

5.7.2 Handoff mechanism

The management frames having been defined, the caching part of the chosen handover scheme is defined as a *struct* in C++ that contains a pointer to itself so that a dynamic list of APs can be formed. The idea is to have the APs made aware of each other presence through a wired distributed system so that two BSS can be made to form an Extended Service Set (ESS) [8]. Hence, it is assumed in this work that the communication that takes between the APs, through the wired system, is not part of the handover process and is to be dealt separately and the dynamic storage of APs enables an easy navigation through the list. The list, *ap_list*, contains information about the AP ID, and the next AP in line.

Thus, although, there are no probe frames exchanged during a handover, it remains that the first time when a MN enters a BSS, there will be a transfer of probe requests and probe response frames. In general, whether it is a first time association or a re-association, the other management frames would still have to be sent and received. All this process is dealt with within the *mac802_11p* class [34], which has been modified so that it is no longer abstract. Since the APs and MNs share the same configuration, they also now share the same class.

Thus, the handoff implementation involves a soft or make-before-break handoff, where the mobile, at a given point of time during the handover process, will be connected to the two involved access points before breaking connection with the first access point. This is to minimize the risk of having any disruption in communications as it would be detrimental to the smooth running of applications in vehicular environments.

5.8 Simulation

5.8.1 Simulation Setup

The simulation is run to verify whether the handover procedure in the IEEE 802.11p model in NS-2 is able to ensure an acceptable handover delay for speeds of 60, 140 and 200 km/h. The first speed reflects the typical mobility within urban regions while the other are meant to meet the IEEE 802.11p set requirements.

The setup consists of two base stations and one mobile station, as shown by Figure 5.4. The two access points are connected to a wired node with Ethernet cables with a capacity of 100 Mbit. The access points represent the RSUs and the mobile node represents the car with an OBU. Tableau 5.1 gives a quantitative overview of the parameters used for the simulation runs.

The simulation is divided into four sets. The first set is run to measure the mean round-trip times (RTT) of ICMP requests 64 bytes long sent from the mobile node to the wired node. Ten ICMP requests are sent each second and the mean time of the ICMP replies is calculated and shown in the figures 5.5, 5.6 and 5.7 for the respective speed of 60, 140, and 200 km/h. For each speed, many simulations have been performed and hence, the calculation of the mean RTT. For a better understanding of the handover period for the different speeds, Tableau 5.2 gives more detailed information about the different variables dependent on the speed of the mobile station.

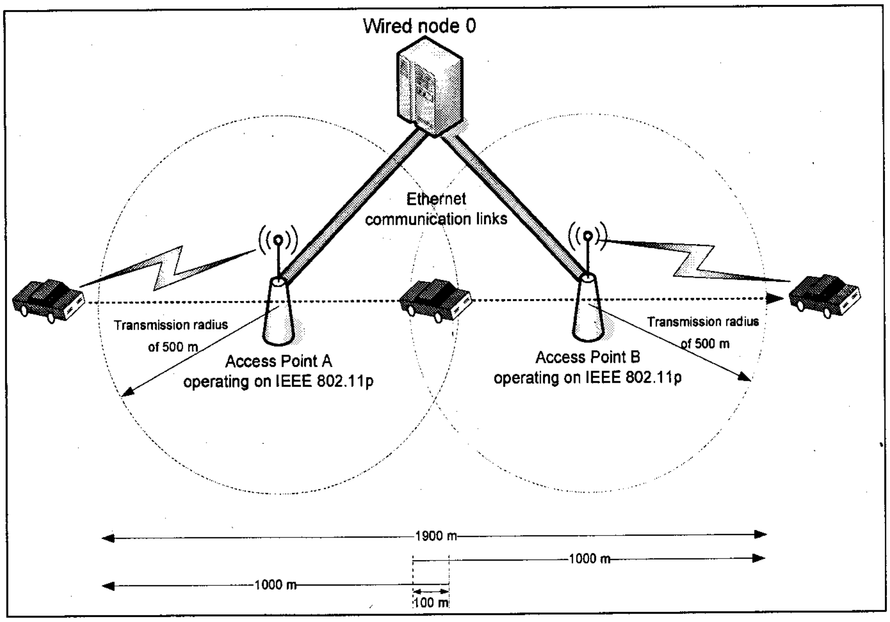

Figure 5.4: Simulation setup

Tableau 5.1: SIMULATION PARAMETERS

Parameter	**Value**
Frequency	5.88 GHz
Transmission power	0.05 W
Range	1000 m
Data rate	3 Mbit/s
Modulation	BPSK (1/2)

The second set consists of a Constant Bit-Rate (CBR) application running over UDP with packets 1000 bytes long sent at a rate of 256 kbps between the mobile node and the wired node with the access points acting as intermediary relay nodes. The aim of this second set of simulation is to quantitatively determine the percentage of packets lost during the overall communication session. This set is run for speeds of 60,140, 160 and 200 km/h. Figure 5.8 shows graphically the percentage of packet lost for the wanted speeds.

Tableau 5.2: CORRESPONDING HANDOVER PERIOD FOR DIFFERENT SPEEDS

Speed (km/h)	**Handover period**
60	Between 53.8s and 59.9 s
140	Between 23.0s and 26.0 s
200	Between 17.2s and 19.0 s

The third set consists of the addition of a traffic load on the APs. Traffic of 64 kbps CBR/UDP arrives at the APs in addition to that of the vehicle. The idea is to see how the addition of a traffic load on the APs affects the RTT of the ICMP replies received by the vehicle. Figures 5.9 to 5.11 illustrate how the RTT varies with the speed of the vehicle.

The fourth set consists of repeating the above scenario but with an increased traffic, consisting of three to five times 64 kbps CBR/UDP flows from additional surrounding vehicles. The aim is to determine how additional node traffic affects the RTT of the ICMP requests received by the first vehicle. Figures 5.12 to 5.14 depict the results obtained.

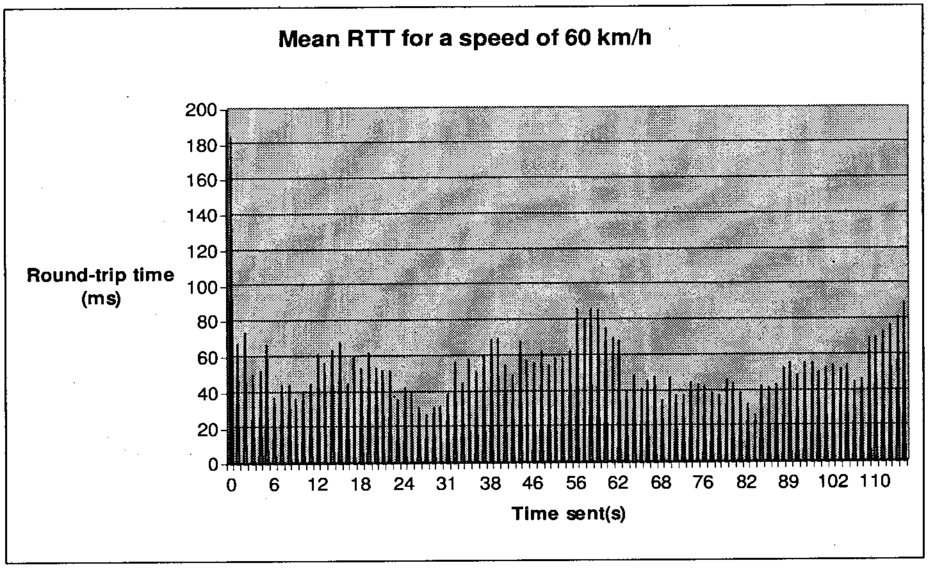

Figure 5.5: Mean RTT for vehicle speed of 60 km/h

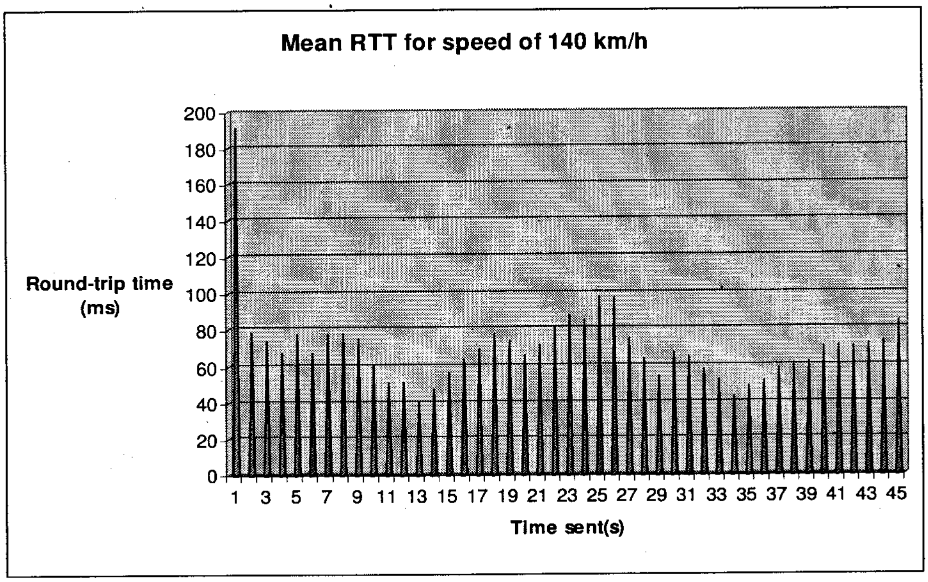

Figure 5.6: Mean RTT for vehicle speed of 140 km/h

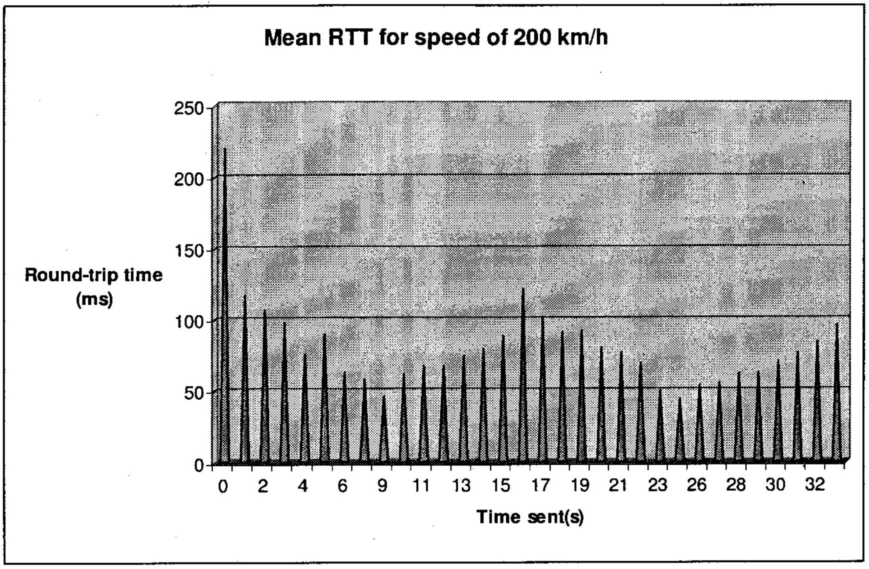

Figure 5.7: Mean RTT for vehicle speed of 200 km/h

5.8.2 Discussion

From the Figures 5.5, 5.6 and 5.7, it can be seen that there is an increase in the mean RTT during the handover zone when there is an increase in speed. This rise can be explained by the fact that an increase in mobility makes it longer for the message to reach the mobile node as the car, in this example, can cover up to 55 m in one second, for the speed of 200 km/h.

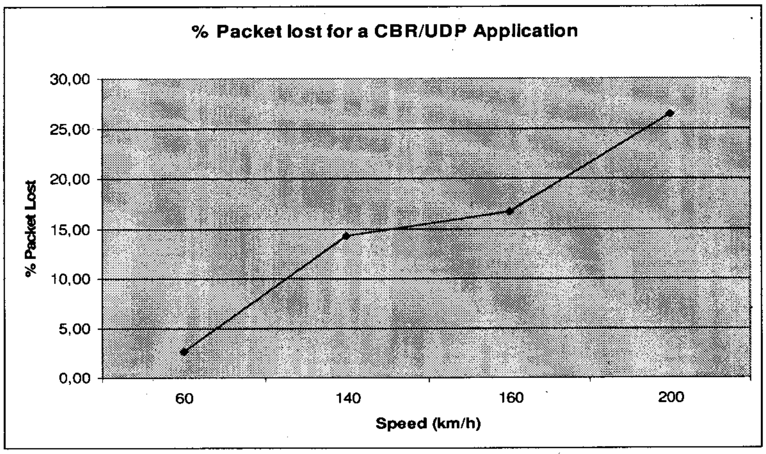

Figure 5.8: Percentage of packet lost for different speeds for a CBR/UDP application

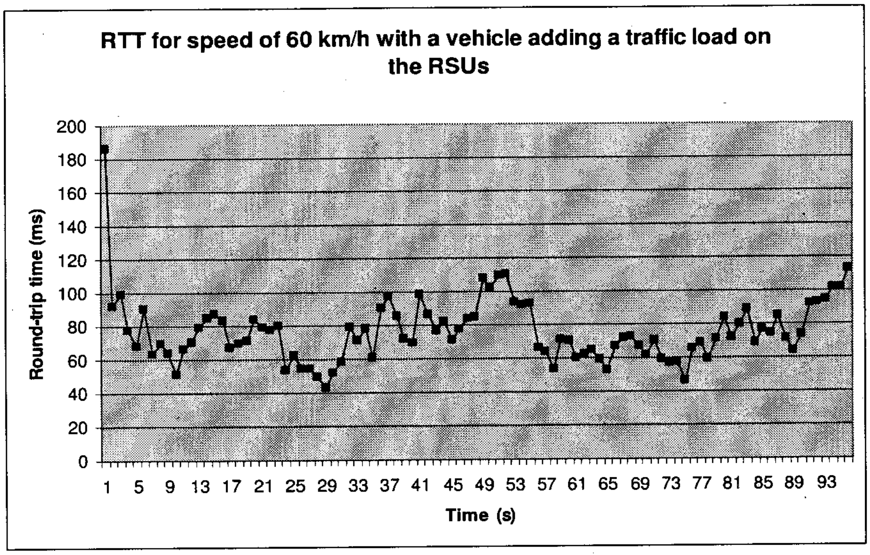

Figure 5.9: RTT of ICMP requests for vehicles moving at 60 km/h with an added traffic load

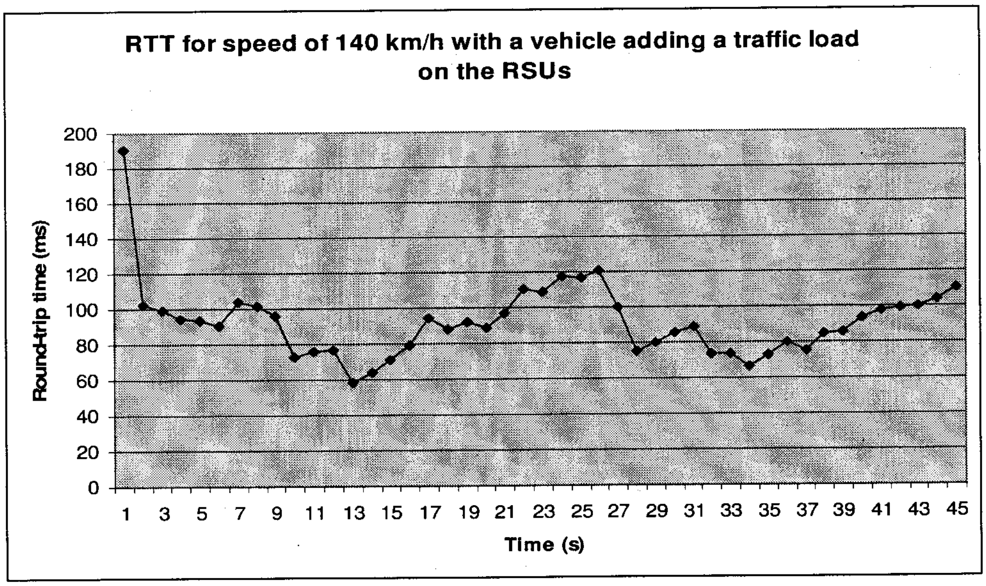

Figure 5.20: RTT of ICMP requests for vehicles moving at 140 km/h with an added traffic load

Further, it is also visible that during the first seconds of each communication session, the mean RTT is quite high with respect the mean RTT encountered during handoff. This can be accounted by the use of the caching model implemented, which is not effective when the vehicle first enters the transmission range of AP A. This IEEE 802.11p implementation models the basic behaviours of an IEEE 802.11-based technology; when the vehicle passes the closest to the APs A and B, the mean RTT drops significantly and arises as the MN moves further away.

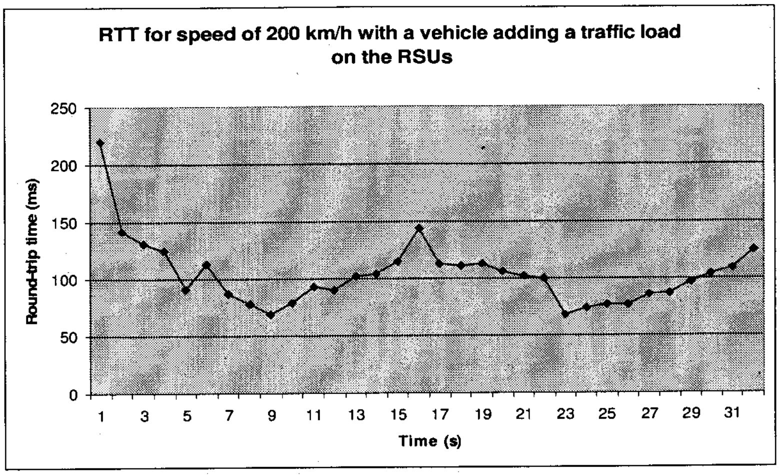

Figure 5.11: of ICMP requests for vehicles moving at 200 km/h with an added traffic load

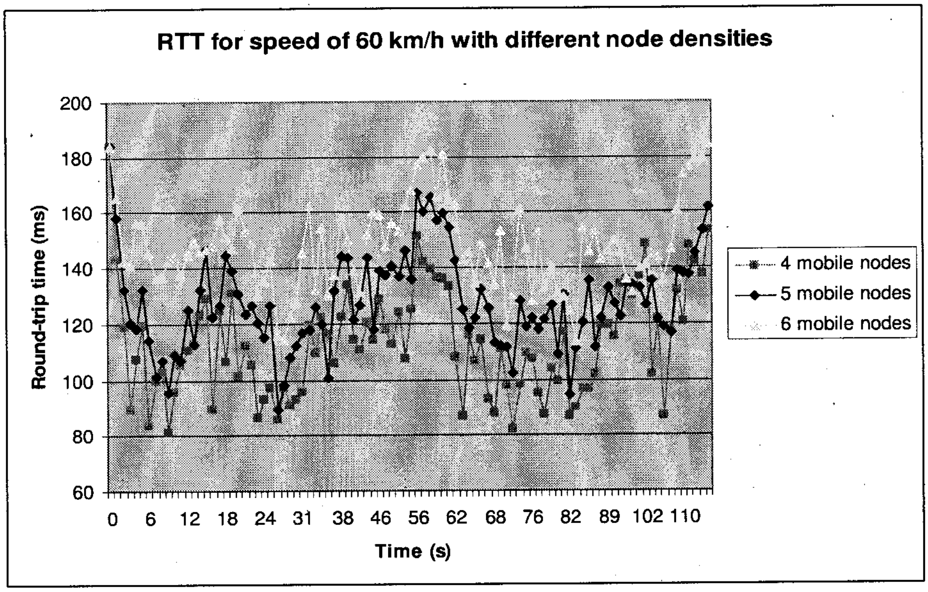

Figure 5.12: RTT of ICMP requests received for vehicles moving at 60 km/h with an increasing vehicle density

Figures 5.9, 5.10 and 5.11 show that the traffic load on the APs influences the values of the ICMP requests received by the first vehicle with significant increase in the RTT value during the handover periods for the different speeds.

The effects of adding a traffic load on the APs have been shown in Figures 5.9, 5.10 and 5.11. Figures 5.12 to 5.14 show that latency of communications grows with traffic from other vehicles. A rise in the number of nodes bearing a traffic load considerably increases the delay of ICMP requests received by the first MN.

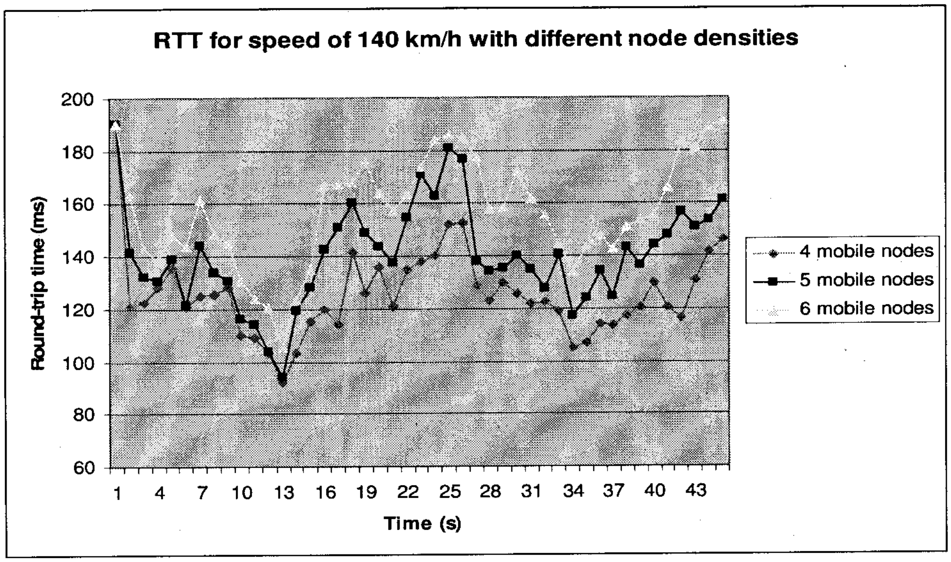

Figure 5.13: RTT of ICMP requests received for vehicles moving at 140 km/h with an increasing number of vehicles

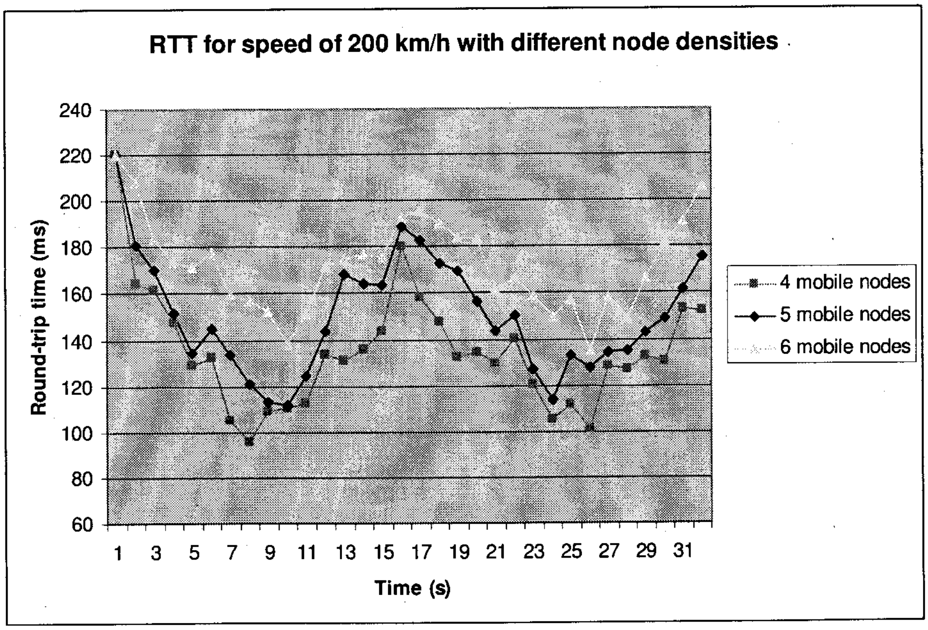

Figure 5.14: RTT of ICMP requests received for vehicles moving at 200 km/h with an increasing number of vehicles

5.9 Conclusion

In this paper we presented a simulation framework for the draft wireless technology IEEE 802.11p within the simulator NS-2 where handoff mechanisms for the draft technology have also been added. The framework is, to the best of our knowledge, the first framework open to research community designed to meet the requirements set for vehicle to infrastructure communications. Since the draft standard deals essentially with V2I communications, we were interested to see how the model behaves with handovers and how it can be adapted to ensure a seamless handoff. The first simulation experiments show how the RTT evolves with vehicle speed and AP load. Future work will target studying 802.11p performance in scenarios including realistic vehicular traffic models.

CHAPITRE 6: ARTICLE DE REVUE IJUWBCS

Avant-propos

Auteurs et affiliation:

B.S.Gukhool : étudiant à la maîtrise, Université de Sherbrooke, Faculté de Génie, Département de génie électrique et génie informatique

S.Cherkaoui : professeure, Université de Sherbrooke, Faculté de Génie, Département de génie électrique et génie informatique

Date d'acceptation : 03 décembre 2009

État de l'acceptation : Version finale acceptée et à être publiée dans la prochaine édition.

Revue : International Journal of Ultra Wide-Band and Communication Systems

Référence : [Gukhool and Cherkaoui, 2009]

Titre français : Gérer les *handovers* dans les communications véhiculaires en utilisant un modèle de 802.11p dans NS-2.

Contribution au document : Ce chapitre présente plus de détails mathématiques quant à la technique utilisée pour réduire le délai global encouru lors des *handovers*, particulièrement, pour réduire le délai associé à l'étape de recherche. De plus, le modèle développé est utilisé pour configurer des scénarios de simulation plus complexes afin de déterminer le bon fonctionnement du système proposé.

Résumé en français : Le but de ce chapitre est de démontrer comment l'utilisation d'une *cache* dans un réseau véhiculaire qui opère avec la technologie sans-fil IEEE 802.11p peut réduire le délai encouru lors de la recherche, et par conséquent, le délai global associé au processus du *handover* dans les communications en mode infrastructure. Les auteurs ont développé et testé un modèle IEEE 802.11p dans le simulateur NS-2 pour évaluer la performance des applications destinées aux réseaux véhiculaires. Suite aux résultats obtenus dans les précédents travaux des auteurs Gukhool et Cherkaoui [34][36], cet article consiste à valider le comportement du modèle face à des simulations véhiculaires plus poussées en

termes de densité et de vitesse. Ce modèle est, selon les auteurs, le premier qui est ouvert à la communauté de recherche. L'analyse des résultats des simulations valide le choix porté vers IEEE 802.11p comme étant la technologie d'accès sans-fil la plus appropriée pour les communications à courtes ou moyennes portées, lorsque comparée avec d'autres variantes de la norme générique IEEE 802.11 ainsi que l'utilisation des *cache* comme une bonne méthode de réduction des délais encourus lors des *handovers.*

Note : À la suite des corrections demandées par les membres du jury, le contenu de cet article diffère dans la forme de celui qui a été soumis.

6.1 Abstract

The focus of this article is to show how a caching mechanism can be applied to vehicular networks operating under the draft standard IEEE 802.11p to reduce the probe delay and consequently, the handover delay in vehicle-to-infrastructure (V2I) communications. The authors have developed and tested an IEEE 802.11p model within the simulator NS-2 to evaluate the performance of vehicular applications. The simulation framework is to the authors' best knowledge, the first framework open to the research community that deals with handovers in vehicular networks while operating under an access technology for vehicular environments. Simulation results analysis confirm the choice of IEEE 802.11p as the ideal technology for Data Short Range Communications (DSRC) when compared to other variants of the generic IEEE 802.11 standard as well as the technique used to reduce the handover delays, which, if left untreated, would be a serious hindrance to the optimal performance of vehicular applications.

6.2 Keywords

WAVE; IEEE 802.11p; NS-2; Handover

6.3 Introduction

The number of variants of the generic IEEE 802.11 standard [2] and other wireless standards like IEEE 802.16 is a clear indication of the growth in demand for wireless networks. Given the mobile nature of wireless access technologies and the current trend of ubiquitous computing, it is utterly normal to consider the application of such technologies to the context of vehicles to create vehicular networks. However, wireless technologies have a well documented series of problems (hidden node, etc), and when applied to the dynamic environment of vehicles, they can lead to the discovery of unknown issues and/or can increase the complexity or difficulty of existing ones. One well-known problem of wireless networks concerns the transmission of data while a mobile station is moving into or out of the range of an access point. The transition is called a handover, and usually entails a certain packet loss. Mobility being the necessary trigger behind that phenomenon, it is necessary to come up with ways to reduce, as far as possible, the delays and the packet loss encountered. Several techniques have been proposed and successfully implemented so that the access points and mobile stations can deal with handovers; but these have always concerned wireless networks with low or reduced mobility.

In the case of vehicular networks, the IEEE has designated a work group to draft an amendment to the legacy IEEE 802.11 standard called IEEE 802.11p [20]. The latter deals with wireless access in vehicular environments and proposes several novel ideas, like the implementation of control, safety and service channels, the use of the OFDM modulation technique at the physical level, specific MAC frames, an increased transmission range amongst others. However, in the infrastructure mode for vehicle-to-infrastructure (V2I) communications, the issue of handoffs is not dealt with.

The objective of this work is to demonstrate how the implementation of a handover-reduction technique adapted to V2I communications in vehicular networks operating under the draft standard IEEE 802.11p can help curb the repercussions of handovers. The paper is divided in three parts: the first one concerns the modeling of the IEEE 802.11p standard in the network simulator, NS-2, so as to generate the appropriate environment. The second part concerns the method used to reduce the delays associated with the handover. Lastly, the whole framework is then tested through the use of realistic simulation scenarios in NS-2 and a qualitative and comparative analysis of the results obtained is presented.

6.4 IEEE 802.11p

IEEE 802.11p is currently a draft amendment to the legacy IEEE 802.11 standard. It is being developed as part of data short range communications (DSRC) [25], which is basically a one-way or two-way communication channels only for automotive use and appropriate standards. DSRC essentially supports V2I and vice-versa. Its current main use in Europe and Japan is electronic toll collection (ETC), and with technological advances like the advent of IEEE 802.11p, the aim is to accommodate a wider range of ITS applications such as:

- Cooperative Adaptive Cruise Control
- Cooperative Forward Collision Warning
- Approaching emergency vehicle warning
- Infotainment

IEEE 802.11p, thus, defines enhancements to the generic 802.11 required to accommodate Intelligent Transport Systems (ITS) applications: it deals with the data link and physical layers of the OSI model whereas the upper layers of the model are catered for by the P1609 series of draft standards, and its purpose is to provide wireless communications short distances between:

- roadside and mobile radio units
- mobile units
- portable and mobile units

6.5 Handoffs in IEEE 802.11 wireless networks

In IEEE 802.11-based networks, a handover or handoff is the process that allows a wireless mobile station to change the access point it is associated with. When a mobile station moves out of the range of its current AP, the frames it receives start having a decreasing relative signal strength indicator (RSSI). Once this metric goes below a certain threshold, the mobile station initiates the first stage of the handover process, the probe/discovery phase by the use of the MAC-level function, scan. The station listens for beacon frames sent out periodically by APs at each 100 ms on assigned channels. Thus, it can create a list of neighbouring APs prioritized according to the RSSI of the beacon message received. One very important feature of wireless networks is power management: the amount of power used to scan each or selected channel(s) for beacons and processing those received is considerable. Added to that is the time issue, the timeout for listening to a specific channel is 100ms. That is why there are two types of scanning algorithms used: active scanning or passive scanning.

Passive scanning requires that the station listens to all candidate channels for the periodic beacon sent by the corresponding AP. Active scanning, on the other hand, is more of a proactive method: the station broadcasts probe request frames to the channel to force a response from the AP. Given the optimum conditions, active scanning greatly reduces the overall probe delay, when compared to the passive version.

Once, a particular AP has been chosen as the next AP with which the mobile station will be associated, the re-authentication phase, which can be broken down into two distinct processes - authentication and re-association, takes place. This is basically a transfer of credentials and other state information from the old AP. Thus, there is an exchange of management frames, and consequently, delays during the three stages:

- the probe delay, which makes up for up to 90% of the total handoff latency [8];
- the de-authentication and authentication delay;
- the re-association delay.

In vehicular networks, although power is not an issue at all, time is a critical factor. Hence, it is better to favour active scanning over passive scanning and since the probe delay is the most important factor behind total handover latency, the handover-reduction technique to be used should aim at decreasing the probe latency.

In this work, the authors have considered implementing a handover mechanism that deals essentially with the probe delay given the high mobility prevailing in vehicular networks.

6.6 Handoff Model in NS-2

Network Simulator 2, or NS-2, [33] is an open-source simulator used to simulate both wired and wireless networks. The IEEE 802.11 model for wireless local area networks that is available in all NS-2 versions simulates, by default, IEEE 802.11b. It is quite popular amongst academics and research students; nevertheless, its wireless models are not very accurate and as such can give erroneous results that can lead to inappropriate conclusions.

The IEEE 802.11 baseline implementation in NS-2 is overly simple. If the ns-allinone-2.31 version of the simulator is taken into account, the WLAN model gives an inkling of about how it operates. The model in [34] gives a more detailed description about the different components developed for the IEEE 802.11.

The only frames defined in the default implementation, together with the frame control field and the MAC header, are the control frames that are:

- the request-to-send (rts) frame;
- the clear-to-send (cts) frame;
- the acknowledgement (ack) frame.

Even though a node can be assigned to be an AP, it does not necessarily function as an AP should in the simulator, especially as far as handovers are concerned, due to the lack of exchange of management frames- frames which are non-existent from the start.

The oversimplification of the default IEEE 802.11 model since there is no scanning, no beacons sent by APs amongst other things, re-emphasises the need for a better handoff model especially in the case of vehicular networks.

6.7 IEEE 802.11p handoff implementation in NS-2

Several handoff models have been designed and proposed to reduce the overall latency associated with the process. Given the high speeds in vehicular networks, having a handover scheme causing a minimum delay and with a low level of disruption in the communication sessions is a fundamental.

In this work, the authors have chosen to favour a handover scheme proposing a cache system at the APs. This system has already been proposed in [18] and there have been other works that have proposed variants of a caching mechanism at APs to reduce the probe latency, and consequently, reduce the overall handoff delay.

This implementation models communication from the vehicles to the infrastructure or the road side units and vice-versa using 802.11p. It is based on the work done in [34] implementing the draft standard on NS-2, and has been tested with the allinone version of 2.31 under both Cygwin running on Microsoft Windows XP SP2 and the Linux-based, Ubuntu.

6.7.1 Proactive Caching

Two APs, ap_x and ap_y, share an association/re-association relation if a mobile station is able to be dissociated from one and be re-associated with the other while following a line of motion through them. An association pattern β (*sta*) for a mobile client, *sta*, is defined as $((ap_1,t_1), (ap_2,t_2), (ap_3,t_3),\ldots.. (ap_n,t_n))$, where ap_n is the AP to which sta is re-associated with at time t = n. $\{(ap_j,t_j), (ap_{j+1},t_{j+1})\}$ is such that a handoff occurs from ap_j to ap_{j+1} at time t+1. Thus, the client maintains the network logical connectivity from t = 1 to t = n.

$G = (V, E)$ is an undirected graph where V = $\{ap_1, ap_2, ap_3,\ldots, ap_n\}$ is the set of all the APs in the wireless network. An edge *e* exists between ap_m and ap_n where $e = (ap_m, ap_n)$ if they have an association/re-association relationship. The next step is to define the valid neighbouring APs. Let the set of neighbouring APs of ap_a be identified as Neigh $(ap_a) = \{ap_{neigh}: ap_{neigh} \in$ V, $(ap_a, ap_{neigh}) \in$ E$\}$. For the particular context of vehicular communications, this neighbour graph is implemented at each participating AP, that is, in a distributed manner so that each AP knows its neighbours. The caching mechanism is based on the following principle: a client *sta* with an association pattern, β (*sta*), should satisfy the reassociation relationship with any two successive APs, like ap_j and ap_{j+1}. Before defining the algorithm, the following notations are described to provide a better understanding.

1) *Contxt(sta):* Represents the context related to client *sta*.
2) *Cache(ap_k):* Denotes the cache data structure maintained at ap_k.
3) *Prop_Contxt(ap_m,sta,ap_n):* Sends the client *sta*'s context information from ap_m to ap_n.
4) *Obt_Contxt(ap_a, sta, ap_b):* ap_a obtains *Contxt(sta)* from ap_b from using IAPP Move-Notify message.
5) *Rem_Contxt(ap_o, sta, ap_{neigh}):* ap_o sends a Cache-Invalidate message to ap_{neigh} to delete *Contxt(sta)* from *Cache(ap_{neigh})*.
6) *Ins_Cache(ap_m,Contxt(sta)):* Insert the context of client, *sta*, into the cache data structure at ap_m. Perform a Least Recently Used replacement if necessary.

The algorithm can thus be defined as shown below. Assuming AP ap_m is running the algorithm, ap_i is the old AP, and *sta* is the mobile client.

```
    if sta is associated with $ap_m$, then
        for all $ap_i \in$ Neigh ($ap_m$) do
            Prop_Contxt($ap_m$,sta,$ap_i$ )
        end for
    endif
    if sta reassociates to $ap_m$ from $ap_n$ then
        if Contxt(sta) not in Cache($ap_m$ )
            Obt_Contxt($ap_i$, sta, $ap_m$)
        endif
        for all $ap_i \in$ Neigh ($ap_m$) do
            Prop_Contxt($ap_m$,sta,$ap_i$ )
        end for
    endif
if sta reassociates to $ap_n$ from $ap_m$ then
```

```
        for all $ap_i \in$ Neigh ($ap_m$) do
                $Rem\_Contxt(ap_m, sta, ap_i)$
        end for
endif
if $ap_m$ received $Contxt(sta)$ from $ap_i$ then
        $Ins\_Cache(ap_m, Contxt(sta))$
endif
```

New parameters can be added to the neighbour graph cache: in addition to the topological information on the APs, the cache would then also contain the BSSIDs, SSIDs, and channels of APs. Thus, the data structure of their neighbour cache graph is defined as such:

$$G' = (V', E),$$
$$V' = \{v_m : v_m = (ap_m, BSSID, SSID \text{ and } channel), v_m \in \mathrm{V}\},$$
$$e = (ap_m, ap_n),$$
$$NC\,(ap_n) = \{ap_k : ap_k \mathrm{\ E\ } V', (ap_i, a_{ik}) \in E\}, \qquad (1)$$

where G' is the modified neighbor graph cache and V' is the set which contains APs with BSSIDs, SSIDs, and channels. Since the BSSIDs, the SSIDs and the channels of the neighboring APs are already pre-cached, the mobile station, when performing the handoff, can go directly to the association phase and thus, greatly reduce the handover latency. The delay incurred during the scanning/probe phase of the handover procedure can be represented as the following bounded equation:

$$\mathrm{N} \times \mathrm{MinChannelTime} \leq \mathrm{Delay}_{\mathrm{probe}} \leq \mathrm{N} \times \mathrm{MaxChannelTime} \qquad (2)$$

where N is the number of channels to be scanned, and $\mathrm{Delay}_{\mathrm{probe}}$ represents the total measure probe delay.

(2) can be extended for the context of neighbour graphs such that it becomes:

$$\sum_{N'}^{i=1}(T_{\min} \times \alpha^{i} + \delta) \leq Delay_{probe} \leq \sum_{N'}^{i=1}(T_{\max} \times \alpha^{i} + \delta) \quad (3)$$

where N' is the number of cached channels, T_{min} is the minimum channel time, α^{i} is the association successful value, T_{max} is the maximum channel time and δ is the association delay. Further, it can be argued that, in the case of a successful re-association, that is, the mobile station has been able to associate itself with the next cached AP during the handover, the overall handoff delay is greatly reduced since there is now no need for entering the scanning phase. However, in case there is no successful association with a cached AP, the normal handoff procedure has to be followed starting with the probe phase. These deductions have also been reached by Mishra et al. in [18] and Li et al. in [35].

6.7.2 Management Frames

Since any handover solution in IEEE 802.11-based technologies requires the exchange of management frames, which are not available in the NS-2 default environment mentioned above, it is necessary to define the frames that are to be involved. The following frames have been added to the mac802_11ppkt class [34]:

- the beacon frame, which is to be sent by the APs;
- the disassociation frame sent from the mobile node (MN) to the AP;
- the association request and response frames, sent when the MN first moves into a Basic Service Set (BSS);
- the re-association request and response frames;
- the probe request and response frames, for scanning the channels and hence, the most appropriate AP;
- the authentication and de-authentication frames.

Furthermore, some other changes have been brought to already existing frames, like the addition of a QoS field and a WAVE Information Element (WIE) field in the MAC header [34].

6.7.3 Handoff Mechanism

The management frames having been defined, the caching part of the chosen handover scheme is defined as a struct in C++ that contains a pointer to itself so that a dynamic list of APs can be formed. The idea is to have the APs made aware of each other presence through a wired distributed system so that two BSS can be made to form an Extended Service Set (ESS). Hence, it is assumed in this work that the communication that takes between the APs, through the wired system or the IAPP protocol, is not part of the handover process and is to be dealt separately and the dynamic storage of APs enables an easy navigation through the list. It is a simple case of the information detailed in section 5.1. The list, ap_list, contains information about the AP ID, and the next AP in line.

Although, there are no probe frames exchanged during a handover, it remains that the first time when a MN enters a BSS, there will be a transfer of probe requests and probe response frames. In general, whether it is a first time association or a re-association, the other management frames would still have to be sent and received. All this process is dealt with within the mac802_11p class [34], which has been modified so that it is no longer abstract. Since the APs and MNs share the same configuration, they also now share the same class.

Thus, the handoff implementation involves a soft or make-before-break handoff, where the mobile, at a given point of time during the handover process, will be connected to the two involved access points before breaking connection with the first access point. This is to minimize the risk of having any major or lengthy disruption in communications as it would be detrimental to the smooth running of applications in vehicular environments.

6.8 Simulation

The simulation is divided into two sets. The context is about simulating vehicular traffic on a highway. Hence, the speeds considered are 80, 140 and 200 km/h: the last two speeds have been mentioned in the IEEE 802.11p draft standard as reference speeds. Moreover, the simulations are run both with configurations of IEEE 802.11a and IEEE 802.11p. IEEE 802.11a has been extensively used in simulators to emulate vehicular network behaviors because of the similarities it shares with the draft IEEE 802.11p, especially as far as the physical layer characteristics are concerned. They both use the Orthogonal Frequency-Division Multiplexing (OFDM) as their modulation method and their operating frequencies are within the 5 GHz band: IEEE 802.11a utilizes a frequency of 5.2 GHz whereas IEEE 802.11p operates in the range of 5.9-GHz Intelligent Transport System (ITS) band.

6.8.1 First simulation set

The first set consists of having a road-side unit (RSU) acting as the access point (AP) for the vehicular network. The AP is connected to a server offering some sort of service, for instance a Voice-Over IP (VOIP) application. The server is connected to the AP through an Ethernet backbone with a bandwidth capacity of 100 Mb. A Constant Bit-Rate (CBR) application with packets 1000 bytes long and running at a rate of 0.5 Mb per second is set up to run between selected mobile nodes and the wired node. The communication is configured to go through the AP. Thus, the AP is made to manage the connections with the forthcoming vehicles while operating under the constant workload of CBR application. The transmission diameter of the AP is set to 1 km. Vehicular density is increased from 10-a-side to 30-a-side to 50-a-side, i.e., the AP is going to accommodate 20 to 60 to 100 mobile nodes at a given point of time and for each density, the reference speeds of 80, 140 and 200 km/h would be setup.

In addition to the constant load placed on the AP, the typical vehicle-to-infrastructure (V2I) communication involves the sending of ICMP request messages from the noted mobile node to the wired node through the AP and the receipt of ICMP reply messages from the wired node to the corresponding mobile node through the AP. The frequency of sending those ICMP request messages is set to one second irrespective of the simulation mobility. The round-trip time (RTT) of the received ICMP reply messages are monitored and their average is calculated and plotted on the graphs shown in the next section.

For a configuration of 20 mobile nodes, there would be four marked cars, two-a-side, whose communication with the wired node would be monitored during their displacement. Coupled with that, is the CBR application running from one mobile node on each side of the AP to the wired node. In order to minimize the effect of a continually increasing load on the AP, the topology of the cars is designed as grid-like with a distance of five meters between each mobile node. In this particular case, the RTT of ICMP requests sent by four vehicles is averaged. In the simulation scenario with 60 mobile nodes, there are 10 marked cars, five on each side of the AP which send the ICMP requests to the wired node, and with 100 mobile nodes, there are 20 cars that send the ICMP request messages.

The first group of simulations is run to determine whether IEEE 802.11a is suited for vehicular networks with high mobility with no event of handover as compared to IEEE 802.11p. Furthermore, the IEEE 802.11p model in NS-2 developed by the authors is being put under test with more realistic vehicular scenarios. The simulation setup for the first series of simulations is shown in figure 6.1.

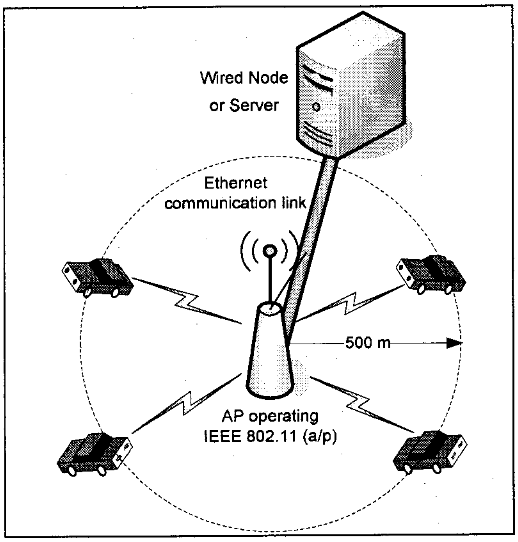

Figure 6.1: Simulation setup for first set of simulations

6.8.2 First simulation set results

IEEE 802.11a and IEEE 802.11p respective results are depicted on the same graphs. Figures 6.2, 6.3 and 6.4 depict how the mean round-trip time for the ICMP requests sent by the four marked mobile nodes vary with respect to speed. Given that the distance to be covered is set to 1000 m, at speeds of 80 km/h, 140 km/h, the corresponding time taken to travel that distance is approximately 46 s, 28s, and 19 s respectively, with the nearest point to the AP occurring at half of the above-mentioned intervals. It can be seen from the above graphs that generally, under these specific conditions and configurations, IEEE 802.11a has much larger mean round-trip time than IEEE 802.11p. For instance, from figure 6.2, at the beginning of the simulation, the average RTT encountered by vehicles operating under IEEE 802.11a is around 260 ms, whereas that for vehicles operating under IEEE 802.11p is around 180 ms. When passing the AP, the mean RTT falls down to around 100 ms for the IEEE 802.11a configuration whereas for IEEE 802.11p that value is around 75 ms. From vehicles moving at 140 km/h, the highest mean RTT value for the four ICMP request messages sent under IEEE 802.11a and IEEE 802.11p is around 275 ms and 200 ms respectively, and the lowest is around 125 and 90 ms respectively. From figure 6.4, the average RTT starts at around 285 ms for IEEE 802.11a and around 215 for IEEE 802.11p and the average RTT at the AP is approximately 140 ms for IEEE 802.11a and nearing 105 ms for IEEE 802.11p. The main observation that can be made is that even with a relatively low vehicular density with a low traffic load, an AP configured with IEEE 802.11p outperforms an AP configured with IEEE 802.11a: the mean RTT values in the IEEE 802.11p simulations are always lower than those in the IEEE 802.11a simulations. Moreover, it is shown that IEEE 802.11a-based vehicular networks do not support well high speeds.

Figures 6.5, 6.6 and 6.7 illustrate how the mean round-trip time for the ICMP requests sent by the 10 marked mobile nodes vary with respect to speed. Since the distance to be covered is set to 1000 m, at speeds of 80 km/h, 140 km/h, the corresponding time taken to travel that distance is approximately 46 s, 28s, and 19 s respectively, with the nearest point to the AP occurring at half of the above-mentioned intervals. It can be seen from the above graphs that generally, under these specific conditions and configurations, IEEE 802.11a has much larger mean round-trip time than IEEE 802.11p. For instance, from figure 6.5, at the beginning of the simulation, the average RTT encountered by vehicles operating under IEEE 802.11a is around 275 ms, whereas that for vehicles operating under IEEE 802.11p is around 215 ms. When passing the AP, the mean RTT falls down to around 115 ms for the IEEE 802.11a configuration whereas for IEEE 802.11p that value is around 95 ms. From vehicles moving at 140 km/h, the highest mean RTT value for the ten ICMP request messages sent under IEEE 802.11a and IEEE 802.11p is around 285 ms and 235 ms respectively, and the lowest is around 135 and 105 ms respectively. From figure 6.7, the average RTT starts at nearly 300 ms for IEEE 802.11a and around 260 ms for IEEE 802.11p and the average RTT at the AP is approximately 175 ms for IEEE 802.11a and nearing 145 ms for IEEE 802.11p.

It can be observed that with an increased vehicular density and a more significant traffic load, IEEE 8021.11p-based vehicular communications perform better than IEEE 802.11a-ones. Not only are the mean RTT values from the simulations significantly lower when configured with IEEE 802.11p than when configured with IEEE 802.11a, but also the IEEE 802.11p-based communication sessions last longer during the motion of the mobile nodes. This is shown in the figures 6.6 and 6.7, whereby the mean RTT values obtained with IEEE 802.11a stop abruptly without continuing till the end of the trip. This is because the packets sent have been lost as the IEEE 802.11a-configured AP is not able to deal with high speeds since IEEE 802.11a was developed with an indoors environment in mind –where the mobility is quite low, rather than for outdoors performance. Moreover, previous work done, namely by Cottingham et al. in [32] where IEEE 802.11a has been used as the access technology for vehicular communications, have been essentially limited to urban environments where the speed would not go beyond 70 km/h.

Figures 6.8, 6.9 and 6.10 depict how the mean round-trip time for the ICMP requests sent by the 20 marked mobile nodes vary with respect to speed. Since the distance to be covered is set to 1000 m, at speeds of 80 km/h, 140 km/h, the corresponding time taken to travel that distance is approximately 46 s, 28s, and 19 s respectively, with the nearest point to the AP occurring at half of the above-mentioned intervals. It can be seen from the above graphs that generally, under these specific conditions and configurations, IEEE 802.11a has much larger mean round-trip time than IEEE 802.11p. For instance, from figure 6.8, at the beginning of the simulation, the average RTT encountered by vehicles operating under IEEE 802.11a is around 285 ms, whereas that for vehicles operating under IEEE 802.11p is around 250 ms. When passing the AP, the mean RTT falls down to around 125 ms for the IEEE 802.11a configuration whereas for IEEE 802.11p that value is around 105 ms. From vehicles moving at 140 km/h, the highest mean RTT value for the twenty ICMP request messages sent under IEEE 802.11a and IEEE 802.11p is around 295 ms and 270 ms respectively, and the lowest is around 145 and 120 ms respectively. From figure 6.9, the average RTT starts at nearly 340 ms for IEEE 802.11a and around 290 ms for IEEE 802.11p and the average RTT at the AP is approximately 185 ms for IEEE 802.11a and nearing 155 ms for IEEE 802.11p.

It is again observed that with a much greater vehicular density and more traffic load, IEEE 8021.11p-based vehicular communications still perform better than a IEEE 802.11a-based one. The mean RTT values from the simulations significantly lower when configured with IEEE 802.11p than when configured with IEEE 802.11a, and also the IEEE 802.11p model in NS-2 ensures that the communication session lasts during the motion of the mobile nodes. In Figures 6.9 and 6.10, the mean RTT values obtained with IEEE 802.11a plots are discontinued in the figures because the packets sent are lost.

A general remark is that, at typical highway vehicular velocities, IEEE 802.11p has significantly better results than that of IEEE 802.11a. Vehicular density impact on communications in the IEEE 802.11a model worsens at medium to high vehicle speeds.

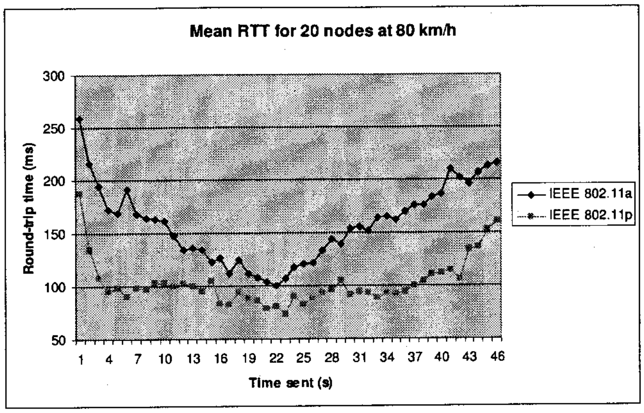

Figure 6.2: Mean RTT for 20 nodes at 80 km/h

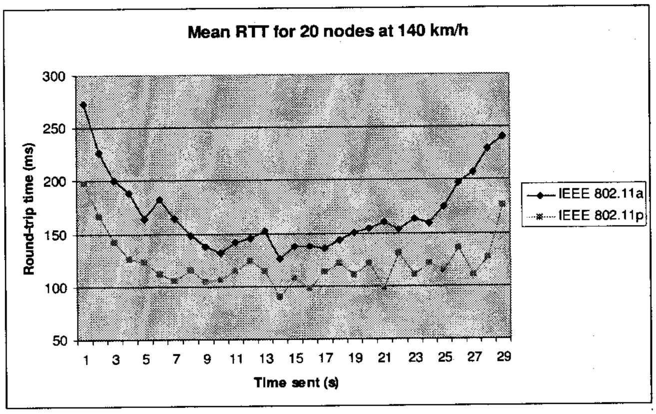

Figure 6.3: Mean RTT for 20 nodes at 140 km/h

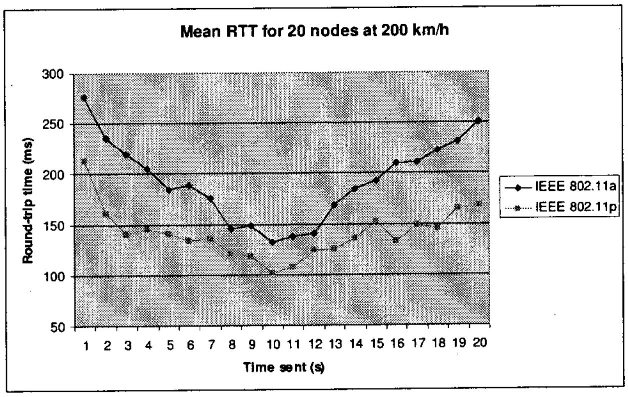

Figure 6.4: Mean RTT for 20 nodes at 200 km/h

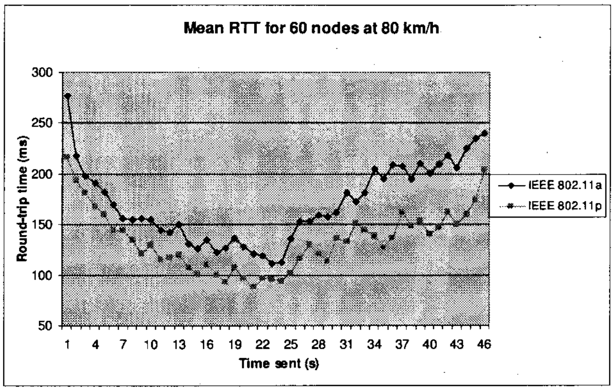

Figure 6.5: Mean RTT for 60 nodes at 80 km/h

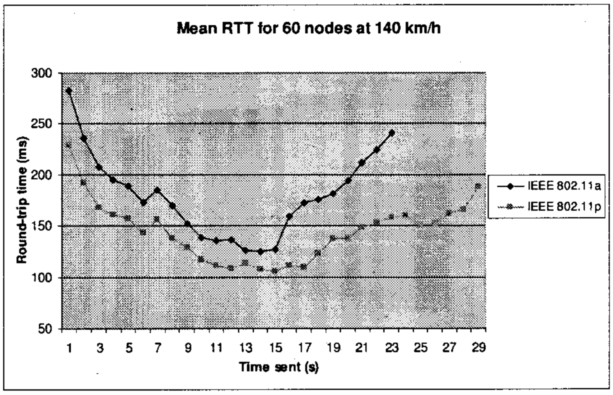

Figure 6.6: Mean RTT for 60 nodes at 140 km/h

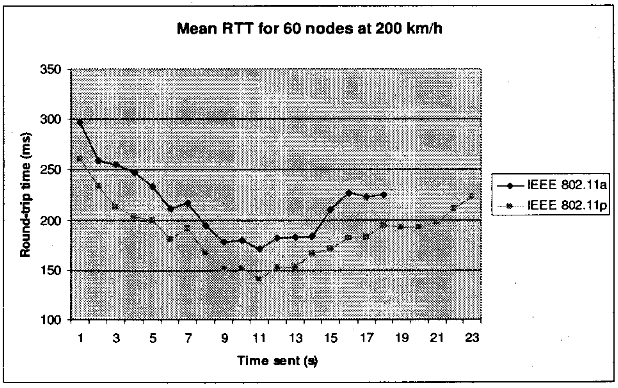

Figure 6.7: Mean RTT for 60 nodes at 200 km/h

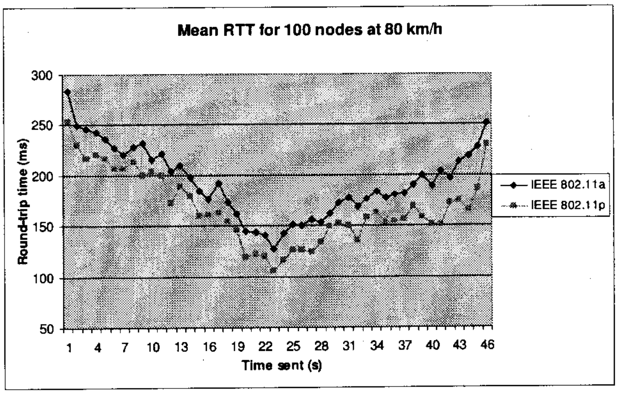

Figure 6.8: Mean RTT for 100 nodes at 80 km/h

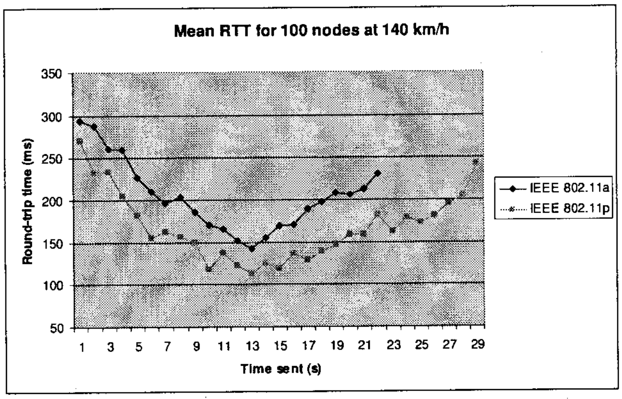

Figure 6.9: Mean RTT for 100 nodes at 140 km/h

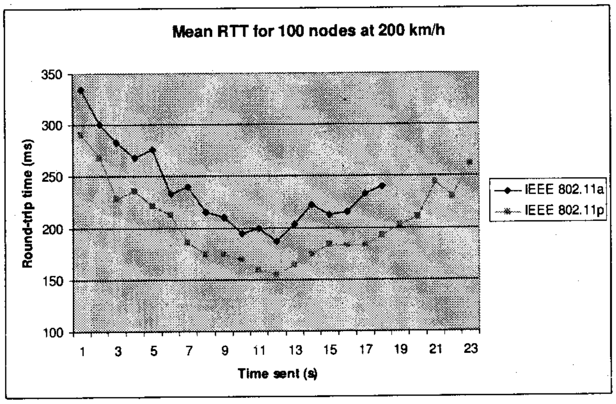

Figure 6.10: Mean RTT for 100 nodes at 200 km/h

6.8.3 Second simulation set

The second set of simulation follows the same basic configuration as the first one, with the addition of another AP to simulate handoffs for moving vehicles. There are two RSUs acting as APs, and they are both connected to a wired node through a 100 Mb-Ethernet cable. A CBR application with 1000-byte long packets sent at a rate of 0.5 Mb per second is configured to run between the wired node and two mobile nodes, one on each side of the road. The transmission diameter of the AP is set to 1 km. Vehicular density is increased from 10-a-side to 30-a-side and then to 50-a-side, i.e., the APs are going to accommodate 20 to 60 to 100 mobile nodes at a given point of time and for each density, the reference speeds of 80, 140 and 200 km/h would be setup.

To monitor the handover effect in the V2I environment, some marked mobile nodes are configured to send ICMP request messages to the wired node through the corresponding AP at a frequency of each second of motion. Depending on the average round-trip time of the received ICMP reply messages, the handover period is to be determined and the handoff period communication results will be analyzed. The handover zone is set up to cover approximately 20 % of the coverage zone of an AP, that is, the handover region is around 200 m long.

For a configuration of 20 mobile nodes, there would be four marked cars, two-a-side, whose communication with the wired node would be monitored during their movement. Coupled with that, is the CBR application running from one mobile node on each side of the AP to the wired node. To minimize the effect of a continually increasing load on the AP, the topology of the cars is designed as grid-like with a distance of five meters between each mobile node. In this particular case, the RTT of ICMP requests sent by four vehicles is averaged. In the simulation scenario with 60 mobile nodes, there are 10 marked cars, five on each side of the AP which send the ICMP requests to the wired node, and with 100 mobile nodes, there are 20 cars that send the ICMP request messages. The simulation setup is shown in figure 6.11

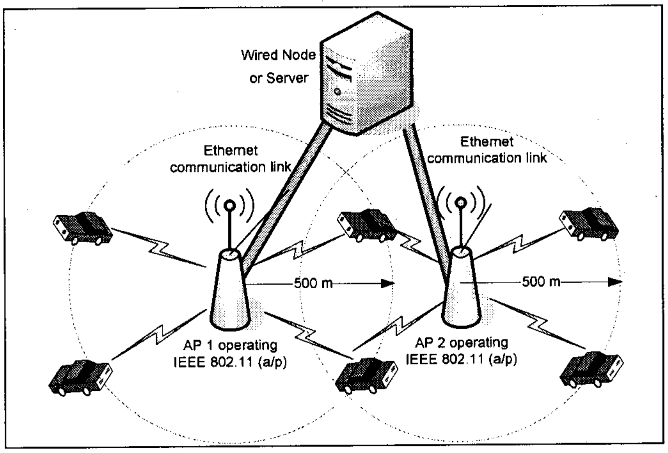

Figure 6.11: Simulation setup for second set of simulations

6.8.4 Second simulation set results

Figures 6.12, 6.13 and 6.14 depict how the mean round-trip time for the ICMP requests sent by the four marked mobile nodes vary with respect to speed. Given that the distance to be covered is set to 1800 m, at speeds of 80 km/h, 140 km/h, and 200 km/h the corresponding time taken to travel that distance is approximately 81 s, 47s, and 33 s respectively, with the handover intervals occurring between 36 s and 45 s for 80 km/h, between 20s and 26 s for 140 km/h and between 14 s and 18 s for 200 km/h. It can be seen from the above graphs that generally, under these specific conditions and configurations, IEEE 802.11a has a much larger mean round-trip time than IEEE 802.11p during the handoff. For instance, from figure 6.12, the average RTT encountered by vehicles operating under IEEE 802.11p is around 140 ms, whereas that for vehicles operating under IEEE 802.11a is around 195 ms, which is about 39% higher. For vehicles moving at 140 km/h, the highest mean RTT value for the four ICMP request messages, during the handover, sent under IEEE 802.11a and IEEE 802.11p is around 210 ms and 150 ms respectively with 802.11a corresponding value about 40% higher. From figure 6.14, the average RTT for IEEE 802.11p when changing APs reaches 180 ms while for IEEE 802.11a, it goes up to 250 ms, which is 38% higher.

Figures 6.15, 6.16 and 6.17 illustrate how the V2I behaves when the vehicular density is increased from 20 nodes to 60 nodes and consequently, when the traffic load from four to ten mobile nodes sending ICMP request messages. Again, it can be seen that IEEE 802.11a has a larger mean RTT than IEEE 802.11p during the overall communication session. If attention is paid to the handover period, then figure 6.15 shows that the average RTT under IEEE 802.11a during handoff is around 220 ms while under IEEE 802.11p, this value reaches 190 ms, which is about 16% lower. In figure 6.16, the maximum average delay encountered by vehicles configured with IEEE 802.11a is approximately 240 ms, whilst those configured with IEEE 802.11p encounter a maximum of 195 ms, a a value that is 23% lower. At 200 km/h, the average RTT reaches 275 ms for IEEE 802.11a and 200 for IEEE 802.11p, according to figure 6.17, which is about 37% lower.

Finally, for 100 mobile nodes, there are twenty marked ones that will initiate the ICMP message exchange. The results for the speeds of 80 km/h, 140 km/h and 200 km/h are illustrated in figures 6.18, 6.19 and 6.20. During the handover intervals, the average RTT reaches around 240 ms and 195 ms for IEEE 802.11a and IEEE 802.11p respectively at 80 km/h, with 802.11p outperforming 802.11a by 23%; at 140 km/h these corresponding values go up to 260 ms and 215 ms with a difference of 21%. At 200 km/h, these values reach around 285 ms and 245 ms for IEEE 802.11a and IEEE 802.11p respectively with results for the latter better by about 16%.

The main observation that can be made is that even with a relatively low vehicular density with a low traffic load, an AP configured with IEEE 802.11p as implemented in the work presented here, handles the handover better than an AP configured with IEEE 802.11a: the mean RTT values in the IEEE 802.11p simulations are consistently lower than those in the IEEE 802.11a simulations. From the previous set of simulations, it can be deduced that IEEE 802.11a does not support well high speeds. Vehicular density impact on communications in the 802.11a model worsens again at medium to high vehicle speeds when handover is involved.

We also observe during the simulation scenarios, that the communication session under IEEE 802.11a is not able to get through the handover even at low speeds. The use of a caching mechanism in the IEEE 802.11p model in NS-2, as developed in the work presented here is shown to help attenuate the ill effects of a handover at typical vehicular speeds and densities.

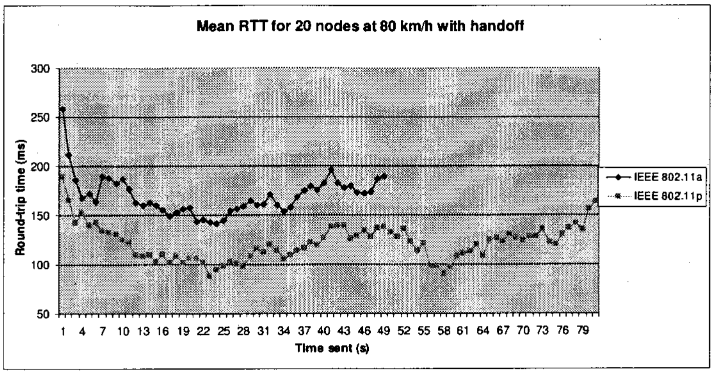

Figure 6.12: Mean RTT for 20 nodes at 80 km/h with handoff

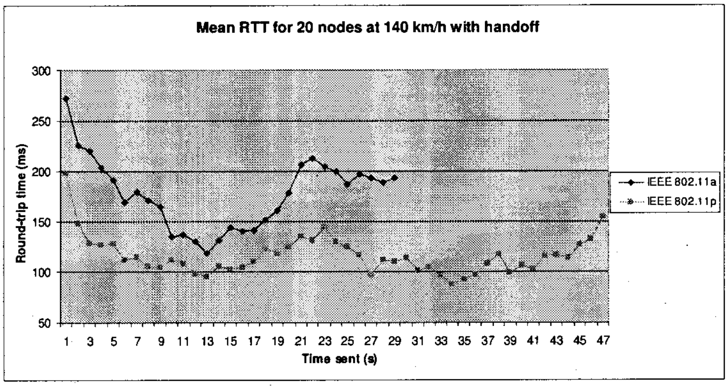

Figure 6.13: Mean RTT for 20 nodes at 140 km/h with handoff

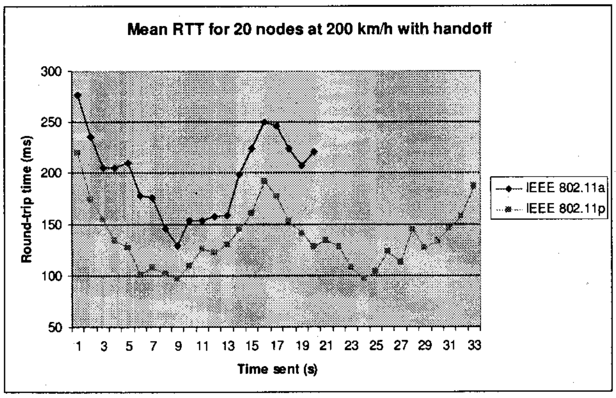

Figure 6.14: Mean RTT for 20 nodes at 200 km/h with handoff

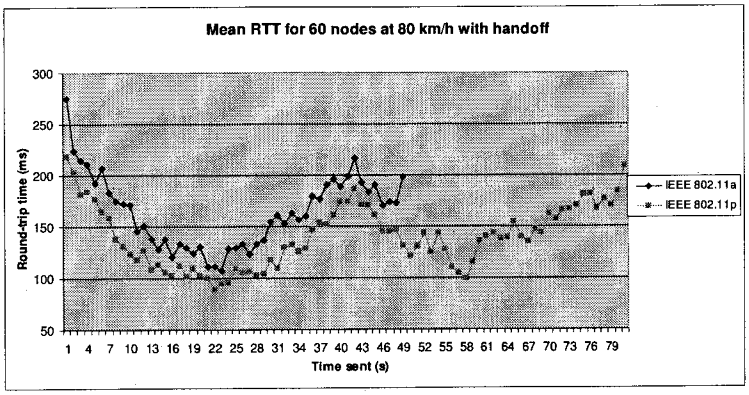

Figure 6.15: Mean RTT for 60 nodes at 80 km/h with handoff

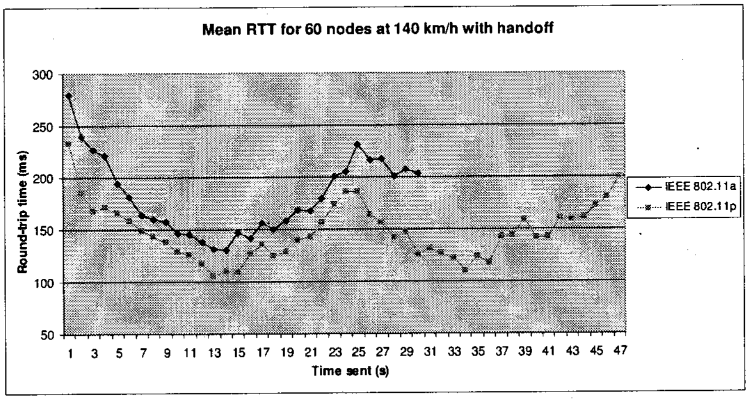

Figure 6.16: Mean RTT for 60 nodes at 140 km/h with handoff

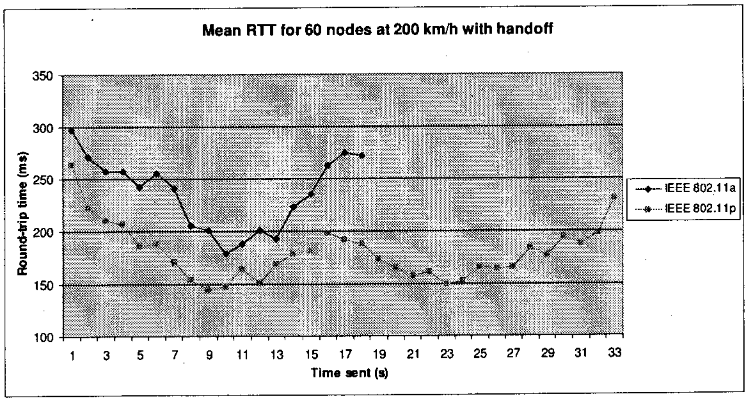

Figure 6.17: Mean RTT for 60 nodes at 200 km/h with handoff

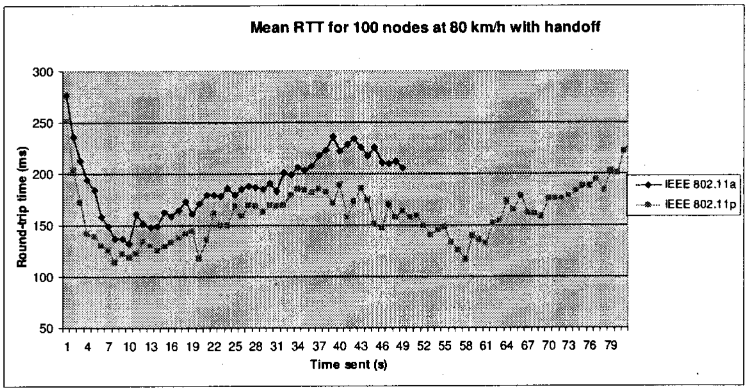

Figure 6.18: Mean RTT for 100 nodes at 80 km/h with handoff

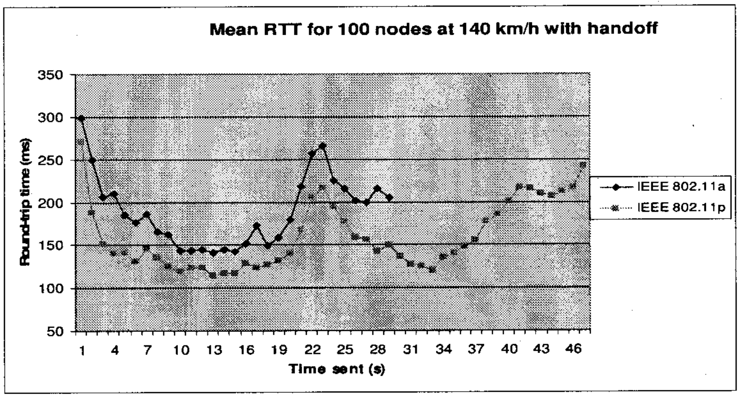

Figure 6.19: Mean RTT for 100 nodes at 140 km/h with handoff

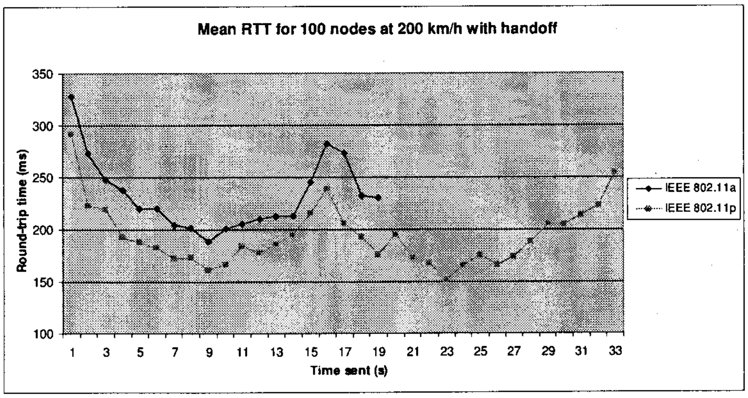

Figure 6.20: Mean RTT for 100 nodes at 200 km/h with handoff

6.9 Conclusion and future work

In this work, the authors have shown that it is necessary to have an access technology that can handle handoffs at high speeds and at densities that are typical for the V2I context. The model of handover implementation in NS-2 shown in this work handles handovers better than its closest IEEE 802.11 variant, IEEE 802.11a. It is clear from simulations that the behavior of IEEE 802.11a is not well suited to communications at speeds and densities similar to those found on a typical highway scenario. Should vehicles require V2I communication sessions that surpass the range of a single access point, it has also been shown that models such as the one implemented in this work for 802.11p, can give better results even at low vehicular densities.

6.10 Acknowledgement

This work has been supported by the Natural Sciences and Engineering Council of Canada (NSERC) as part of the AUTO21 NCE project at the Université de Sherbrooke.

CHAPITRE 7 : CONCLUSION

Dans le présent mémoire, il a été question d'un problème lié à une communication continu entre une infrastructure routière et un véhicule dans un réseau véhiculaire lors d'un *handover*, spécifiquement les délais encourus lors des différentes phases constituant le *handover*, qui affectent directement la continuité et la qualité de la session de communication.

Jusqu'à présent, les méthodes de réduction de ces délais ont été utilisées surtout dans un contexte de réseau sans-fil à basse ou moyenne mobilité. Hors, les réseaux véhiculaires, ayant une mobilité très haute, nécessitent des délais de *handoff* très faibles lorsque comparés à la moyenne. La majorité du délai global associé au *handover* est encouru lors de l'étape de recherche du prochain point d'accès. De façon générale, les technologies d'accès sans-fil traditionnel ne sont pas adaptées aux besoins et aux contraintes des réseaux véhiculaires. Outre le facteur de haute mobilité, il y a aussi d'autres critères important à considérer comme la sécurité du réseau et la capacité de la technologie d'accès à supporter des applications riches.

L'objectif du présent mémoire était de trouver une méthode de réduction du délai global encouru lors d'une procédure de *handover*, plus spécifiquement une réduction du délai associé à l'étape de recherche ou découverte du phénomène de *handover*. Cette méthode a été ensuite adaptée et testée pour les réseaux véhiculaires.

Pour arriver à cette solution, une approche scindée en deux parties a été proposée :

1. La première est le choix d'une technologie d'accès sans-fil qui puisse répondre aux attentes et besoins des réseaux véhiculaires.
2. L'utilisation des *caches* à chaque point d'accès ou, dans le cas d'un réseau véhiculaire, d'une infrastructure routière pour réduire le temps de recherche.

La première partie vise l'utilisation d'une technologie d'accès appropriée qui permettra d'optimiser la communication dans les réseaux véhiculaires. C'est pourquoi le choix s'est porté sur la norme IEEE 802.11p, qui est toujours en attente d'être adoptée. La norme IEEE 802.11p semble satisfaire les exigences de ce type d'environnement à haute mobilité grâce à ses trames spéciales pour les communications dans les réseaux véhiculaires, surtout aux couches physique et liaison de données, et en utilisant OFDM comme technique de modulation. Les trames définies sont courtes, mais contiennent que de l'information pertinente, pour réduire le temps de traitement.

La deuxième partie concerne la technique de réduction du délai associé au *handover*. Les prochains points d'accès sont stockés dans une *cache* et cette information est distribuée à chaque point d'accès pour réduire le temps de recherche. Ainsi, lorsqu'un véhicule va changer de point d'accès ou d'infrastructure routière, il va s'associer avec le prochain sans avoir à entamer une longue étape de recherche.

Pour valider la méthode proposée, la technologie d'accès IEEE 802.11p ainsi qu'une procédure de *handover*, qui utilise des *caches*, ont été implémentées dans le simulateur de réseaux, NS-2. Ainsi, l'implémentation de l'approche proposée a été utilisée pour élaborer des scénarios de simulation dont les résultats sont très satisfaisants. Toutefois, cette méthode n'est jusqu'à présent que valide pour des réseaux véhiculaires homogènes. L'extension de la même approche dans un environnement hétérogène pourrait constituer un autre projet de recherche.

BIBLIOGRAPHIE

[1] The Auto21 web page, http://www.auto21.ca

[2] IEEE 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Standard, 1999 Edition (R2003)

[3] IEEE 802.11a, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band," IEEE Standard, September 1999.

[4] IEEE 802.11b, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band," IEEE Standard, September 1999

[5] IEEE 802.11g, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band," IEEE Standard, June 2003.

[6] STALLINGS, W. (2005) Réseaux et Commnications sans fil, Paris, 2e édition, Pearson Education, 627 p.

[7] D.Schwab and R. Bunt, "Characterising the Use of a Campus Wireless Network" in Proc. IEEE INFOCOM 2001, March 2004.

[8] A.Mishra, M.Shin, and W.Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process","ACM SIGCOMM Computer Communications Review, vol.33, no.2, April 2003, pp.93-102.

[9] IEEE 802.11f, "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," IEEE Standard, July 2003.

[10] S.Shin, A.Forte, A.Rawat, and H. Schulzrine, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs", in Proc. ACM MobiWac 2004, October 2004.

[11] H.Velayos and G. Karlsson, "Techniques to reduce IEEE 802.11b MAC Layer Handover Time," in Proc. ICC 2004, June 2004.

[12] M.Shin, A.Mishra, and W.Arbaugh, "Improving the latency of 802.11 Hand-offs using Neighbor Graphs", in Proc. ACM MobiSys 2004, June 2004.

[13] I.Ramani and S.Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks", in Proc. IEEE Infocom 2005, March 2005.

[14] V.Brik, V.Mishra, and S. Banerjee, "Eliminating Handoff Latencies in 802.11 WLANs using Multiple Radios: Applications, Experience, and Evaluation", in Proc. ACM Internet Measurement Conference 2005, October 2005.

[15] K.Chi, J.Jiang, and L.Yen, "Cost-Effective Caching for Mobility Support in IEEE 802.1X Frameworks", IEEE Transactions on Mobile Computing, vol. 5, no.11, November 2006, pp. 1547- 1560.

[16] S.Pack and Y. Choi, "Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN Systems", IEE Proceedings Communications, vol.151, no.5, October 2004, pp.489-495.

[17] IEEE 802.1x, "IEEE Standards for Local and Metropolitan Area Networks for Port based Network Access Control", IEEE Standard, June 2001.

[18] A.Mishra, M.Shin, and W.Arbaugh, "Context-Caching using Neighbor Graphs for Fast Handoffs in a Wireless Network", in Proc. IEEE INFOCOM 2004, March 2004.

[19] J.Loughney, M.Nakhjiri, C.Perkins and R.Koodli, "Context Transfer Protocol (CXTP)", IETF RFC 4067, July 2005.

[20] IEEE 802.11p, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless Access in Vehicular Environments (WAVE)", Draft Edition.
[21] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns
[22] The IEEE 802.11 Official Timelines web page, http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm
[23] http://yans.inria.fr/ns-2-80211/
[24] IEEE 802.11i, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements," IEEE Standard, July 2004.
[25] Armstrong Consulting, http://www.leearmstrong.com/DSRC/DSRCHomeset.htm
[26] DSRC - Linking the Vehicle and the Road, Bill Jones, ITS Joint Program Office, U.S. Department of Transportation, 2005
[27] IEEE Standard 1609.1, Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager, 2006
[28] IEEE Standard 1609.2, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages
[29] IEEE Standard 1609.3, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Networking Services, 2007
[30] IEEE Standard 1609.4, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)- Multi-Channel Operation, 2007
[31] O. Awoniyi, F.A. Tobagi, "Packet Error Rate in OFDM-based Wireless LANs Operating in Frequency Selective Channels", INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings, April 2006. P 1-13
[32] D. Cottingham, I. Wassell, R. Harle, " Performance of IEEE 802.11a in Vehicular Context", Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th. P 854-858
[33] The ns Manual. The VINT Project, a collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC. http://www.isi.edu/nsnam/ns/doc/
[34] B.S.Gukhool, S.Cherkaoui, "IEEE 802.11p modeling in NS-2", LCN 2008. 33rd IEEE Conference on Local Computer Networks. Proceedings, October 2008. P 622-626
[35] C.S. Li,Y.C. Tseng, H.C. Chao, Y.M. Huang, 'A neighbour caching mechanism for handoff in IEEE 802.11 wireless networks.' Journal of Supercomputing, Vol. 45, March 2008. P 1-14.
[36] B.S.Gukhool, S.Cherkaoui, "Handoff in IEEE 802.11p-based vehicular networks", WOCN 2009. IEEE-IFIP International Conference on Wireless and Optical Communications Networks. Proceedings, April 2009. P 1-5.