

Communications optimisées dans un réseau véhiculaire ad hoc multi-sauts

Patrick MARLIER



**Université de Technologie de
Compiègne**



France Télécom R&D

Février 2007 – Juillet 2007

REMERCIEMENTS

Si ce projet a pu se réaliser dans d'aussi bonnes conditions et susciter chez moi autant d'intérêt et de motivation, c'est grâce à plusieurs personnes que je tiens à remercier.

Je remercie tout d'abord M. Sidi-Mohammed Senouci, responsable du projet PRONTO, pour m'avoir accueilli dans son équipe et de m'avoir confié ce projet. Je le remercie pour le temps et l'intérêt qu'il a bien voulu consacrer à mon travail ainsi qu'à sa sympathie. Merci de m'avoir toujours laissé donner mon point de vue, tout en guidant mes réflexions.

Je remercie aussi M. Moez Jerbi, doctorant à France Telecom, pour son aide précieuse, ses conseils et pour m'avoir guidé pendant ce stage.

Enfin, je remercie M. Bertrand Ducourthial, suiveur UTC, qui m'a permis d'effectuer ce stage et qui s'est intéressé à mon projet.



SOMMAIRE

Remerciements.....	2
Sommaire	3
Introduction.....	5
Présentation de l'entreprise	6
1. Le groupe France Telecom	6
2. Orange Labs - France Telecom R&D	6
3. Le laboratoire CORE/M2I	8
4. L'unité de recherche et de développement R2A.....	8
5. Le projet PRONTO.....	8
Présentation du stage / Contexte	10
1. Contexte du stage.....	10
2. Objectifs du stage.....	10
3. Déroulement du stage	10
4. Présentation des réseaux de véhicules.....	10
4.1. Les types de communications	11
5. Applications des réseaux de véhicules.....	12
5.1. Applications de sécurité routière.....	12
5.2. Applications de confort	13
6. Propriétés et problématiques des réseaux de véhicules	14
7. Consortium et projets.....	15
Expérimentations de la communication inter véhicules	17
1. Etat de l'art des expérimentations	17
2. Plateforme d'expérimentations.....	18
2.1. La précédente plateforme.....	18
2.2. Objectifs de la nouvelle plateforme.....	18
2.3. Le matériel d'expérimentation	19
2.4. Les logiciels de la plateforme	19
2.5. Configuration de la plateforme	20
2.6. Acquisition de données.....	22
2.7. Analyse des données capturées	23
3. Les scénarios de tests	23
3.1. Scénarios V2V	23



3.2. Scénarios I2V	24
3.3. Scénario hybride	25
4. Les résultats et analyses	25
4.1. Expériences de communication véhicule à véhicule.....	25
4.2. Expériences de communication véhicule à véhicule multi-sauts.....	26
4.3. Expériences de communication de véhicule à infrastructure.....	28
5. Améliorations possibles de la plateforme.....	29
5.1. Le pilote Madwifi-ng	29
5.2. Implémentation d'une couche 2.5.....	29
6. Conclusions	29
Dissémination de données dans un réseau de véhicules	31
1. Introduction de la dissémination.....	31
2. Etat de l'art.....	32
2.1. Dissémination de messages d'urgence	33
2.2. Dissémination pour des applications de confort	35
3. Simulation de protocoles et évaluation des performances.....	36
3.1. Le simulateur GloMoSim	36
3.2. Le modèle de mobilité	37
3.3. Performances des solutions "DDT" et "SODAD"	38
4. Propositions pour la création d'un protocole de diffusion.....	40
Conclusion	41
Bibliographie.....	42
Annexes	44
A. Principaux sigles	44
B. Les réseaux ad hoc multi-sauts	45
C. Problématique des réseaux sans fils 802.11	47
Le choix de la norme IEEE 802.11	47
Couche Physique	47
Couche Liaison (Medium Access Control + Logical Link Control)	52



INTRODUCTION

Aujourd'hui, les télécommunications sont omniprésentes dans notre quotidien. La téléphonie mobile avec le réseau de 3^{ème} génération et Internet haut débit sans fil avec le wifi créent un nouveau besoin de mobilité. La communication doit pouvoir se faire n'importe où et n'importe quand. Cependant, à l'heure où l'on passe de plus en plus de temps dans les transports, il n'existe pas de solution fiable à faible coût.

En effet, uniquement la téléphonie mobile fonctionne dans les véhicules actuellement alors que les applications d'une communication globale sont nombreuses telles que l'amélioration de la sécurité routière et l'accès à Internet pour le passager. Les réseaux de véhicules sont donc les réponses à ce nouveau besoin grâce à un faible coût et un délai plus court. Ils ne sont cependant qu'en phase expérimentale et beaucoup de challenges doivent être encore relevés.

Ce stage s'inscrit sous forme d'une contribution à la recherche dans le domaine des réseaux véhiculaires.

Lors de ce rapport, nous allons donc rapporter en détail le déroulement du stage. Dans la section 1, nous allons tout d'abord évoquer le stage de façon générale, à travers une présentation de l'entreprise ainsi que le contexte des réseaux de véhicules. Dans la section 2, nous entrerons dans la première partie du stage qui est l'expérimentation de la communication inter véhicule avec la plateforme de tests et les scénarios effectués. Dans la section 3, nous détaillerons la seconde partie du stage avec un état de l'art du domaine de la dissémination d'informations dans un réseau de véhicules et nous comparerons des solutions existantes.



PRESENTATION DE L'ENTREPRISE

1. LE GROUPE FRANCE TELECOM

Le Groupe France Télécom est l'un des principaux opérateurs de télécommunications au monde, avec plus de 153 millions de clients répartis dans 220 pays ou territoires au 30 septembre 2006. En France, il est l'opérateur historique de télécommunications. France Télécom est devenu une Société Anonyme (SA) depuis 1996, après sa privatisation.

Les principaux marchés du groupe:

- **La vente indirecte:** Vendre des produits et des services via des partenaires-relais proches de la clientèle, c'est le principe de la vente indirecte dont l'importance au sein du Groupe va croissant.
- **le marché de la vente aux opérateurs:** Pour proposer leurs services à leurs clients, les opérateurs et les fournisseurs d'accès Internet ont besoin d'accéder la plupart du temps aux réseaux de France Télécom.
- **le marché pro:** Avec 3,3 millions d'entreprises, le marché pro représente un fort enjeu commercial et financier de par sa dimension et ses spécificités.

Avec le programme NExT (Nouvelle Expérience des Télécommunications), lancé en juin 2005, le Groupe accélère sa transformation d'opérateur intégré afin de devenir le fournisseur de référence des nouveaux services télécoms en Europe et partout où il est présent.

NExT, un programme de transformation du Groupe sur 3 ans, pour que:

- Le Groupe poursuive sa transformation d'opérateur soutenue par un modèle renouvelé de croissance profitable,
- ses clients accèdent à un univers de services enrichis et simplifiés.

La stratégie NExT:

- une vision: offrir aux clients une Nouvelle Expérience des Télécoms ; leur ouvrir l'accès à un nouveau monde de services, à une nouvelle génération de services télécoms pour changer leur vie de tous les jours.
- une ambition: devenir le fournisseur de services télécoms de référence en Europe et partout où il est présent, la référence en matière d'innovation, de qualité de services et de performance économique.

2. ORANGE LABS - FRANCE TELECOM R&D

La Division "Recherche & Développement" a pour principales missions:

- de développer des produits et services pour le groupe, en respectant la qualité de service
- de dégager de nouvelles sources de croissance,
- d'anticiper les révolutions technologiques et d'usage,



- d'imaginer dès maintenant les solutions du futur.

La R&D est la source d'innovation pour le Groupe:

- Elle alimente les "group product roadmaps" du marketing stratégique en nouvelles offres de produits et services ou évolutions d'infrastructures, à partir de ses travaux de recherche
- Elle fournit au marketing stratégique les ressources en développement nécessaires pour l'accélération de la mise sur le marché (time to market) des offres de produits/services ou nouveaux déploiements de réseaux à court et moyen terme, dans le cadre du dispositif de rapprochement R&D/ marketing/ réseaux & SI, piloté par le Technocentre (structure de projet "3 partenaires")
- Son action dans les domaines de la recherche pure et de l'anticipation lui permet de détecter et d'explorer les avancées et ruptures technologiques majeures et les nouveaux usages.
- Son expertise dans le domaine des réseaux et dans le développement et l'industrialisation des produits et des services permet de lancer des services structurants pour l'ensemble de l'industrie comme Business Everywhere ou la passerelle domestique « Livebox ».
- Elle conduit la politique d'investissement en capital risque du groupe, à travers la gestion proactive des différents fonds « Innovacom », et l'utilisation des innovations des start-up de ces fonds par le groupe.
- Elle définit et conduit la politique de valorisation de propriété intellectuelle et de licensing du groupe.
- Elle représente le groupe France Télécom dans les instances de normalisation, et défend les positions du groupe en coopération avec les divisions concernées.

En contribuant à la convergence des technologies et à l'enrichissement des services de France Télécom, cette capacité de R&D constitue pour le Groupe un avantage stratégique majeur pour anticiper les grandes ruptures technologiques, orienter l'innovation du secteur des télécommunications et inventer la nouvelle génération de services : des services de communication intégrés, innovants et simples d'utilisation.

La R&D, une mission, 2 métiers

Rechercher:

- Exceller en protection et valorisation de notre propriété intellectuelle
- Détecter les ruptures technologiques et acquérir le savoir faire
- Explorer les nouvelles technologies, services et usages

Développer:

- Réduire les délais de mise sur le marché
- Industrialiser les produits, services et les évolutions du réseau



- Concevoir les services du futur
- Améliorer les offres existantes
- Développer des partenariats stratégiques avec les industriels

Quelques chiffres clés au 31 décembre 2006:

- 3900 chercheurs ingénieurs
- 16 implantations sur 3 continents
- 512 inventions brevetées, 261 logiciels enregistrés chaque année pour un total de 8 319 brevets (au 31/12/06)
- des investissements importants en R&D avec 700 millions d'euros, soit 1,5% du CA en 2005 et une forte croissance en 2004 et 2005 : + 20 %
- un talent reconnu et citée en 2006 comme référence dans "A French Revolution in Innovation is unfolding", Forrester

3. LE LABORATOIRE CORE/M2I

Multimedia networks for non-conversational fixed/mobile services : Image, Internet" (M2I) : dirigé par Xavier Hatrisse, a pour mission d'étudier, pour les réseaux fixes et mobiles, l'ingénierie des services non conversationnels : accès à Internet et services de diffusion de l'image. Il définit, sélectionne, évalue, valide et participe à l'intégration des équipements réseaux nécessaires à ces services. Le laboratoire met en œuvre des compétences sur les équipements et architectures des réseaux de collecte fixe et mobile (BAS, NAS, SGSN, GGSN, nœud de service vidéo, réseaux ad hoc), de commande de ressources (plates-formes de commande et sondes applicatives) et d'authentification-comptage (chaîne RADIUS et ses extensions, plates-formes de facturation à l'acte, traitement du nomadisme dans le réseau). Il apporte une expertise aux entités du Groupe France Télécom afin de leur permettre de réaliser les évolutions des réseaux et des services de collecte dans un souci de qualité, sécurité et d'optimisation des investissements, charges et chiffre d'affaires.

4. L'UNITE DE RECHERCHE ET DE DEVELOPPEMENT R2A

L'Unité de Recherche et Développement (URD) R2A dirigé par Yvon Gourhant a pour thème les "Réseaux Adaptables, traitements Applicatifs et réseaux spontanés" (R2A) qui regroupe les réseaux auto-organisés tels que les réseaux pair à pair et multi-sauts. Ses missions couvrent de nombreux domaines. D'abord, cette URD développe, évalue et intègre les technologies des réseaux adaptatifs (routeurs logiciel, réseaux actifs et programmables). De plus, cette URD se concentre sur les réseaux ad hoc et réseaux de véhicules: amélioration des protocoles de routage, qualité de service, plateforme de tests et implémentations. Plusieurs projets collaboratifs sont actuellement entrain d'évoluer comme le RNRT SARAH, RNRT AIRNET, RIAM MAD GAMES, l'IST One Lab et IST MAGNET Beyond. Enfin, cette unité s'intéresse aussi dans l'évaluation d'équipements comme les sondes externes et intégrées pour les réseaux et les analyseurs de trafic capable de traiter au niveau applicatif.

5. LE PROJET PRONTO

Le projet PRONTO (PeRvasive and ubiquitOus systems & NeTwOrks) est un projet interne à Orange Labs dont le responsable est Sidi Mohammed SENOUCI. L'objectif du projet est d'étudier et



développer une expertise et des solutions pour les environnements pervasifs. En fait, les réseaux pervasifs (ou omniprésents) sont des environnements dans lequel nous sommes connectés, partout et tout le temps si nous le voulons, par l'intermédiaire de nos objets communicants classiques (ordinateurs, PDA, téléphones, etc.) mais aussi grâce à des objets multiples équipés d'une capacité de mémoire et d'intelligence. Le projet PRONTO traite plus précisément:

- les réseaux multi sauts : réseaux ad hoc, réseaux maillés, réseaux de capteurs et réseaux de véhicules
- Les systèmes embarqués

Plusieurs collaborations externes avec des universitaires nationales et internationales ont été établies dans la cadre de ce projet. Je citerai en particulier la collaboration avec l'UTC sur les réseaux fortement dynamiques.



PRESENTATION DU STAGE / CONTEXTE

Nous allons tout d'abord introduire le contexte du stage dans la partie 1, puis donnerons les objectifs dans la partie 2. Dans la partie 3, nous détaillerons le planning effectif du déroulement du stage. Dans les parties 4, 5 et 6, nous présenterons respectivement les réseaux de véhicules, leurs applications, et leurs problématiques. Enfin dans la partie 7, nous donnerons quelques projets et consortiums associés à ces réseaux.

1. CONTEXTE DU STAGE

Dans le cadre de ma dernière année d'études à l'Université de Technologie de Compiègne, j'ai dû effectuer un stage d'un minimum de 24 semaines en entreprise. En parallèle à cette dernière année, j'ai également suivi un master recherche. Le stage que j'ai réalisé chez France Télécom R&D a donc pour but de valider à la fois la dernière année d'ingénieur et le master, en mariant ces deux aspects d'ingénierie et de recherche.

2. OBJECTIFS DU STAGE

Le premier objectif de mon stage est d'expérimenter la communication sans fils 802.11 pour les réseaux de véhicules. Cette norme n'a pas été conçue pour des stations en mouvement et encore moins aux véhicules. Cette phase d'expérimentation avec une série de mesures dans différents scénarios de mobilité permet d'évaluer les possibilités du wifi et ainsi de valider le choix de cette technologie.

Le second objectif est d'étudier les mécanismes de dissémination dans les réseaux de véhicules. Pour cela, un état de l'art a été élaboré afin de comprendre les problématiques et de proposer des améliorations possibles. Le but est de disposer d'une solution de diffusion optimisée et ainsi de pouvoir développer un service autour des réseaux de véhicules.

3. DEROULEMENT DU STAGE

Le stage s'est déroulé sur 6 mois du 5 février 2007 au 31 juillet 2007 à Lannion sur le site de France Telecom R&D. Lors de ce stage, plusieurs travaux m'ont été confiés et la figure 1 illustre leurs répartitions.

	Fév		Mar		Avr		Mai		Jui		Juil	
Analyse du testbed	■											
Développement testbed		■	■			■			■		■	
Expérimentations				■	■		■		■			
Etude bibliographique	■	■			■	■	■					
Simulation								■	■	■		■
Rapport											■	■

Figure 1 : Planning effectif du stage

4. PRESENTATION DES RESEAUX DE VEHICULES

Ces dernières années, la communication inter-véhicules a attiré beaucoup de chercheurs dans le monde entier. Dans l'Union Européenne, quelques projets de recherche examinent le potentiel de réduction des accidents de la route grâce à l'initiative eSafety et il en est de même dans d'autres pays



comme les Etats-Unis ou le Japon. La communication de voiture-à-voiture (V2V), souvent mentionnée comme des **réseaux ad hoc véhiculaires** (VANETs ou Vehicular Ad hoc Networks), permet de nouveaux services pour des véhicules et crée de nombreuses opportunités pour améliorer la sécurité routière. La communication entre véhicules peut par exemple être utilisée pour aider à la conduite et proposer des services de sécurité active comme l'avertisseur d'accident, le trafic temps réel et des systèmes actifs de diffusion de l'information (de météorologie ou de navigation). Cependant, ces nouveaux services pour les réseaux de véhicules posent beaucoup de défis technologiques pour les protocoles réseaux et la sécurité des communications. Le besoin de la recherche dans ce domaine est donc en pleine expansion.

Les réseaux de véhicules ont des caractéristiques semblables à ceux des réseaux ad hoc mobiles (MANETs ou Mobile Ad hoc Networks), souvent sous forme de **réseaux multi-sauts**. Des changements de topologie du réseau arrivent fréquemment en raison de la haute mobilité des nœuds. Tous les nœuds partagent le même canal menant à la congestion dans des réseaux très denses. La nature décentralisée de ces réseaux mène au besoin de nouveaux systèmes et protocoles de diffusion de l'information. De plus, de nouvelles approches pour la sécurité de communication doivent être conçues pour adapter les besoins spécifiques du réseau et garantir des services fiables et dignes de confiance.

4.1. LES TYPES DE COMMUNICATIONS

Dans ces réseaux de véhicules, les services proposés permettent de distinguer plusieurs communications possibles, comme vous pouvez le voir sur la figure 2.

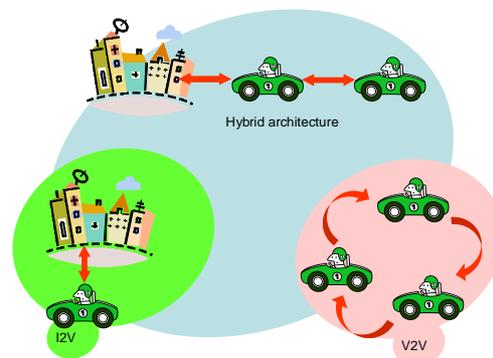


Figure 2 : Types de communication dans un réseau de véhicules.

COMMUNICATIONS DE VEHICULE A VEHICULE

Les services et les applications qui sont basées sur la simple communication inter-véhicule et n'impliquant pas d'infrastructure fonctionnent seulement dans le cas où un taux de pénétration suffisant de véhicules équipés a été atteint. En raison des longs cycles de vie des véhicules, un taux de pénétration approprié peut seulement être atteint après plusieurs années, même si toutes les voitures nouvellement produites ont été équipées en juste proportion. C'est pourquoi, les constructeurs automobiles doivent penser aux stratégies d'introduction graduelles du marché.

COMMUNICATIONS DE VEHICULE A INFRASTRUCTURE

Nous ne nous concentrons pas donc seulement sur des simples systèmes de communications inter véhicules, mais prenons aussi en compte des applications qui utilisent des points d'infrastructure (road side units ou RSUs). Ceux-ci démultiplient les services grâce à des portails Internet communs. Des services à base d'infrastructure (accès à internet, échange de données par exemple de voiture-à-domestique, communications de voiture-à-garage pour le diagnostic distant, ...) profitent aux clients

et peuvent motiver des conducteurs à investir dans l'équipement sans fil supplémentaire pour leurs véhicules.

COMMUNICATIONS HYBRIDES

La combinaison de ces deux types de communications permet d'obtenir une communication hybride très intéressante. En effet, les portées des infrastructures étant limitées, l'utilisation de véhicules comme relai permet d'étendre cette distance. Dans un but économique en évitant de multiplier les bornes à chaque coin de rue, l'utilisation de sauts par véhicules intermédiaires prend toute son importance.

5. APPLICATIONS DES RESEAUX DE VEHICULES

Une des applications de ce concept consiste à munir nos voitures et nos routes de capacités de communication permettant de rendre la route plus sûre et de rendre le temps passé sur les routes plus convivial. Cette application est appelée le **système de transport intelligents** (ITS, Intelligent transportation System).

On peut donc distinguer deux types d'applications avec les réseaux de véhicules, les applications de confort et les applications de sécurité routière. Les contraintes de ces applications sont différentes comme par exemple la vitesse de propagation de l'information. Dans le cas d'un accident, il faut prévenir les usagers dans un temps borné alors que la diffusion de publicités n'a pas cette contrainte de temps mais elle sera par contre plus consommatrice de bande passante.

Nous allons donc décrire dans les paragraphes suivants quelques applications.

5.1. APPLICATIONS DE SECURITE ROUTIERE

a) ALERTER EN CAS D'ACCIDENTS

Ce service permet, dans le cas d'un accident, d'avertir les véhicules se dirigeant vers le lieu de l'accident que les conditions de circulation se trouvent modifiées et qu'il est nécessaire de redoubler de vigilance (cf. figure 3 a). Il est nécessaire, également, en cas de densité réduite de véhicule de pouvoir conserver l'information pour pouvoir la retransmettre si un véhicule entre dans la zone de retransmission. Les messages de sécurité devront être émis à des périodes régulières. Ainsi le ou les nœuds désignés pour la retransmission des messages émettront des alertes à instants réguliers. Les messages devront être de taille réduite pour être transmis le plus rapidement possible. Les messages devront comporter les coordonnées du lieu de l'accident et les paramètres de la zone de retransmission.

b) ALERTER EN CAS DE RALENTISSEMENT ANORMAL (BOUCHON, TRAVAUX, INTEMPERIES, ETC.)

Ce service permet d'avertir les automobilistes de situations de circulation particulières (cf. figure 3 b). L'information quelque soit la nature des difficultés de circulation renseigne l'automobiliste qu'il est nécessaire de ralentir. Le message d'alerte est émis par un véhicule détectant les difficultés de circulation (freinage important par exemple, déclenchement des feux de détresse, pluie). Un véhicule banalisé effectuant des travaux peut également être à l'origine du message d'alerte. Comme pour le message d'alerte informant d'un accident, le message d'alerte informant d'un ralentissement doit être transmis aux autres véhicules de façon efficace et rapide.

c) LA CONDUITE COLLABORATIVE

La conduite collaborative est un concept qui améliore considérablement la sécurité du transport routier (réduction du nombre de victimes, cf. figure 3 d). Cette innovation est basée sur un échange



de renseignements entre des véhicules munis d'instruments (ex : capteurs) leur permettant de percevoir ce qui les entoure et de collaborer en groupes. Ces groupes de véhicules ou réseaux ponctuels, peuvent élaborer une stratégie de conduite collective qui exigerait peu ou pas d'interventions de la part des conducteurs. Depuis ces dernières années, différentes architectures de véhicules automatisés ont été proposées, mais la plupart d'entre elles n'ont peu ou pas investi le problème de communication inter véhicules. On peut aussi sur le même principe échanger des informations de trafic et de travaux afin de fluidifier le réseau routier en indiquant par exemple des itinéraires bis. La signalisation automatique est aussi envisageable avec l'avertissement de passage de véhicule d'urgence, ou encore l'avertissement d'une panne d'un feu tricolore.

5.2. APPLICATIONS DE CONFORT

a) RESEAUX COLLABORATIFS

Les réseaux collaboratifs sont en train de se développer en particulier avec les réseaux pairs-à-pairs. On peut imaginer une chaîne de radio ou de « télévision distribuée » où chaque véhicule va partager les musiques et vidéos qu'il a en sa possession pour construire un programme de diffusion continu. Les cartes collaboratives (wiki) et les petites annonces peuvent être des services distribués à base de réseaux collaboratifs. Un serveur relais (dit « proxy-cache ») peut permettre la navigation sur Internet même dans des zones sans connexion à Internet. Un système de distribution de publicités et d'informations pratiques (concerts, restaurants, ...) peut être mise en place à l'entrée des villes.

b) INTERNET DANS LES TRANSPORTS

Aujourd'hui, les hotspots (zone wifi à accès Internet) sont de plus en plus développés dans les villes, en particulier avec les initiatives des communautés (par exemple, Fon [FON]) et des opérateurs de télécommunication. En voiture, on peut imaginer acheter de la musique et de la vidéo, au niveau d'une station essence, d'une gare ou même en pleine autoroute (en passant d'une voiture à une autre jusqu'au point d'accès le plus proche). Les passagers dans la voiture pourront ainsi jouer en réseaux, ou encore même naviguer sur Internet (cf. figure 3 e).

c) GESTION DES ESPACES LIBRES DANS LES PARKINGS

Ce service permet de rassembler des informations sur la disponibilité de l'espace de stationnement dans les parkings et de coordonner entre automobilistes afin de les guider aux espaces libres (cf. figure 3 c).

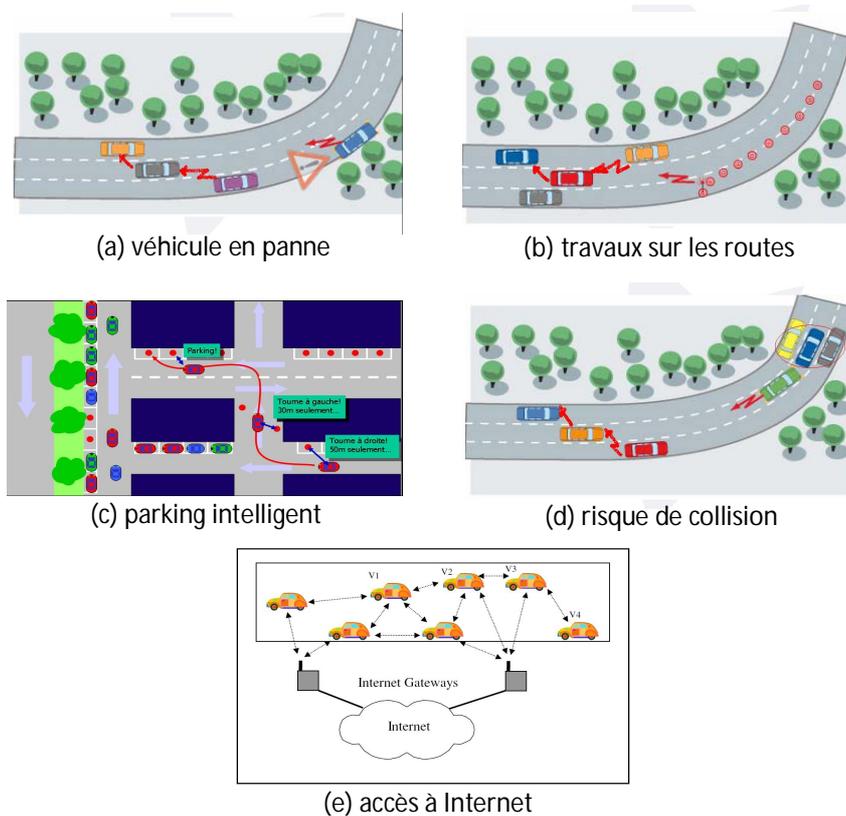


Figure 3 : Applications des réseaux de véhicules

6. PROPRIETES ET PROBLEMATIQUES DES RESEAUX DE VEHICULES

Ce type de réseau n'est autre qu'une application dédiée et spécifique des réseaux ad hoc mobiles. Cependant, les travaux de recherche étudiés et réalisés dans le domaine des MANETs ne peuvent pas être directement appliqués dans le contexte des réseaux de véhicules à cause de leurs spécificités.

Voici quelques propriétés et challenges qui distinguent les réseaux de véhicules :

- **Capacité de traitement, d'énergie et de communication** : le matériel que l'on peut embarquer dans une voiture est très différentes des terminaux mobiles tels que les PDA qui ont des contraintes de taille et de poids. On peut aussi par exemple embarquer plusieurs interfaces de communication (Wi-Fi, WiMax et Bluetooth).
- Environnement de déplacement et **modèle de mobilité** : les environnements dans les réseaux ad hoc sont souvent limités à des espaces ouverts. Les déplacements des véhicules, quant à eux, sont liés aux infrastructures routières (routes, autoroutes). Les trajectoires peuvent donc être prédictibles et l'environnement peut être urbain, rural ou autoroutier. Les contraintes imposées par ce type d'environnement, à savoir les obstacles et interférence radio, affectent le modèle de mobilité et la qualité des transmissions radio. Les protocoles et solutions doivent donc prendre en compte ces spécificités.
- Type de l'information transportée et diffusion : L'une des applications clés des réseaux de véhicules étant la prévention et la sécurité routière, l'information est destinée à un ensemble de véhicules généralement proches et limitée à une zone géographique.

- Topologie du réseau et connectivité : à la différence des réseaux ad hoc, les réseaux VANET sont caractérisés par une **forte mobilité**, liée à la vitesse des véhicules, en particulier sur autoroute. Un nœud peut rejoindre le réseau et le quitter en un temps très court, ce qui rend les changements de topologie très fréquents. Un des problèmes fréquents est le **partitionnement ou la fragmentation du réseau**, en particulier lors de la phase de déploiement de la technologie. Par ailleurs, les problématiques de **passage à l'échelle** doivent être prises en compte dans les solutions car le réseau peut devenir gigantesque (en France en 1998, il y avait 2,1 habitants par voiture).
- **Sécurité et anonymat** dans le réseau : Le problème de sécurité de la communication est important, par exemple, un message d'urgence doit pouvoir être validé ou ignoré s'il est envoyé par un nœud malicieux. Un mécanisme d'anonymat doit pouvoir assurer le respect de la vie privée.

7. CONSORTIUM ET PROJETS

Beaucoup d'activités de recherche, de développement et de standardisation de la communication automobile sont actuellement en cours. En Europe et dans le monde entier, des projets de R&D majeurs ont été amorcés pour constituer la base d'un système de transport intelligent européen. Voici une description de plusieurs projets utilisant la communication de véhicules :

- L'objectif du projet FleetNet est de développer une plate-forme de communication pour les réseaux de véhicules, de mettre en œuvre un démonstrateur, et de standardiser les solutions proposées afin d'assurer une meilleure sécurité et confort au conducteur et ses passagers.
- NoW (Network on Wheels) est un projet allemand, le successeur du projet Fleetnet (Internet on the road), qui travaille sur le développement d'un système de communication qui intègre les applications de sécurité et de confort. NOW soutient et coopère fortement avec le consortium Car2Car.
- Le consortium Car2Car s'est fixé l'objectif d'améliorer la sécurité routière, de gérer efficacement le trafic à travers l'utilisation des IVC. Les principales missions du consortium de communication Car2Car sont les suivantes : (i) la création d'un standard européen ouvert pour les communications V2V basé sur des composants LAN sans fil, (ii) développer des prototypes et des démonstrateurs des systèmes V2V pour les applications de sécurité routière, (iii) promouvoir l'attribution d'une bande de fréquence exclusive libre pour les applications de Car2Car en Europe, et (iv) développer des stratégies de déploiement et des modèles économiques pour la pénétration du marché.
- Le projet européen IST CarTalk2000 (coordonné par le constructeur Daimler Chrysler entre 2001 et 2004) avait comme but de développer des systèmes coopératifs d'aide à la conduite et de mettre en œuvre un réseau pur ad hoc sans fil auto-organisé. La technologie d'accès radio UMTS a été adoptée au dessous d'un protocole de routage multi-sauts basé sur la position.
- Le projet intégré européen PReVENT a été initié pour contribuer à la sécurité routière en développant et en démontrant des applications et des technologies préventives de sécurité routière.
- SeVeCom (Secure Vehicular Communication) s'intéresse à la sécurité des futurs réseaux de véhicules, incluant la sécurité et l'anonymat de la communication véhicule à véhicule et véhicule à infrastructure.
- SAFESPOT s'intéresse aux systèmes coopératifs pour la sécurité routière pour empêcher des accidents de la route en détectant des situations potentiellement dangereuses. Le mode de communication utilise la future norme IEEE 802.11p.



- CVIS (Cooperative Vehicle Infrastructure Systems) vise à développer un système de communication qui est capable d'utiliser une vaste gamme de technologies sans fil, des réseaux cellulaires (GPRS, UMTS), des réseaux locaux sans fil (WLAN), des réseaux micro-ondes à courte portée (DSRC) et infrarouge (IR).
- Le but de WATCH-OVER est de concevoir et de développer un système coopératif pour la prévention des accidents dans les zones accidentogènes. Le concept innovant est représenté par une plateforme embarqué et un module utilisateur. Le système est basé sur la communication faible distance et les capteurs de vision.
- GST (Global System for Telematics) développe une architecture ouverte et standardisée pour des services télématiques automobiles. Les cibles du projet sont des services orientés infrastructure comme le service d'appel de secours, l'avertissement d'accident et des services d'informations.
- COOPERS (Cooperative Systems for Intelligent Road Safety) se concentre sur le développement de d'applications télématiques innovatrices avec un but à long terme "d'une gestion de trafic coopérative" entre le véhicule et l'infrastructure.

La plupart des groupes de travail privilégie la solution de communication sans fils basée sur la norme 802.11. Peu de tests en condition réelle ont été effectués. Nous avons donc procédé à de nombreux tests afin de valider la pertinence du choix technologique.



EXPERIMENTATIONS DE LA COMMUNICATION INTER VEHICULES

Dans le but de valider le choix de la norme IEEE 802.11, nous avons procédé à de nombreux **tests en condition réelle** dans des véhicules. Ces expériences nous ont permis d'évaluer les performances ainsi que de comprendre les problèmes qui surviennent lors de la communication inter véhicules.

Une analyse de la norme 802.11 a été effectuée pour la compréhension de son fonctionnement et des mécanismes mises en jeu. Cette analyse peut être trouvée en annexe C. La problématique des réseaux ad hoc a aussi été abordée dans ce stage, on peut se référer à l'analyse faite en annexe B.

Dans la première partie, nous détaillerons un état de l'art des expérimentations des réseaux de véhicules. Dans la partie 2, nous introduirons notre plateforme de tests. Dans les parties 3 et 4, nous parlerons des scénarios de tests puis des résultats de ces expériences. Dans la partie 5, nous donnerons plusieurs améliorations possibles de la plateforme.

1. ETAT DE L'ART DES EXPERIMENTATIONS

Les expériences des réseaux de véhicules ont plusieurs fois été présentées dans la littérature et nous allons résumer quelques articles.

Dans [HULL06], les auteurs présentent les résultats d'une étude de mesure sur un ensemble de points d'accès ouverts déployés actuellement dans le secteur métropolitain de Boston. Ils mesurent le temps de connexion et la bande passante en téléchargeant avec neuf voitures se déplaçant en essayant de se connecter sur les différents points d'accès.

[GASS06] démontre la faisabilité d'utiliser directement la norme IEEE 802.11b des réseaux sans fil pour une voiture se déplaçant. Ils mesurent la performance d'un client en mouvement connecté à un point d'accès seul dans le désert de Californie, où il n'y a aucun obstacle et aucune interférence radio et aucun autre véhicule. Cet environnement leur permet de mesurer la performance dans un milieu contrôlé.

[OTT04] étudie le comportement des connexions réseaux sur un canal IEEE 802.11b à partir d'une voiture se déplaçant. Cette étude décrit des mesures TCP et UDP entre une voiture en mouvement avec une antenne externe et un point d'accès. Le but était de comprendre l'impact de la vitesse de la voiture, le taux de transmission et l'influence de la taille des paquets.

[BUCC05] expose quelques résultats expérimentaux utilisant une application multimédia dans un réseau ad hoc inter-véhicules. Deux véhicules équipés de la norme IEEE 802.11b ont testé dans uniquement deux environnements différents (urbain et autoroute). Les auteurs concluent les résultats suivants : (i) le rapport Signal/Bruit (SNR) est plus important dans une autoroute que dans une zone urbaine, (ii) la liaison est plus fiable dans une autoroute que dans une ville et (iii) la transmission optimale varie selon le scénario, puisqu'il est meilleur d'utiliser de gros paquets sur des autoroutes et utiliser une grande fragmentation avec de petits paquets dans des zones urbaines.

Les mêmes résultats sont obtenus dans [HUI01] quant au SNR et au bruit. De plus, les auteurs donnent quelques autres résultats tel que le RTT, le débit TCP et UDP, etc. Ils utilisent 3 véhicules ainsi qu'un chemin statique. De leur point de vue, le déploiement d'applications multimédia est difficile.

Dans [SING02], les auteurs ont mesuré la qualité du lien sur autoroute, dans des environnements urbains et des banlieues. Les résultats de l'étude ont montré que la banlieue est la plus favorable pour la communication inter-véhicule.



Le but des expériences dans [HULL06, GASS06, OTT04] est de comprendre les performances en termes de temps de connexion et de taux de perte quand une station mobile se connecte à des points d'accès. Tandis que les expériences dans [BUCC05, HUI01, SING02] testent des conditions d'environnements différentes. Ces expériences ne considèrent pas tous les scénarios que nous trouvons dans notre vie quotidienne ainsi que les effets de certains facteurs sur les métriques de performance. Leur objectif principal est d'avoir une vue globale de la connectivité entre seulement deux véhicules en changeant des conditions d'environnement de conduite.

Notre étude expérimentale est innovante sur plusieurs points. Tout d'abord, notre plateforme permet l'utilisation de plus de deux véhicules. De plus, nous essayons de fournir des métriques détaillées comme le débit, le délai et la puissance du signal entre trois voitures se déplaçant sans nœud stationnaire. Enfin, nous nous concentrons sur la communication multi-sauts pour étendre la couverture des points d'accès.

2. PLATEFORME D'EXPERIMENTATIONS

La plateforme a pour objectif **d'automatiser les processus de configuration, d'acquisition et de traitement**. Le module d'acquisition doit être d'autant plus simple car l'utilisateur est aussi conducteur du véhicule. Il ne doit pas effectuer de manipulation complexe pour lancer la capture des données.

2.1. LA PRECEDENTE PLATEFORME

Une première plateforme (ou testbed) a été développée précédemment à mon stage. Des premiers tests avaient été effectués mais trop de problèmes survenaient allongeant les durées des tests. Donc, ma première tâche fut d'analyser cette plateforme, d'identifier les problèmes et de les corriger.

Lors de l'analyse de l'ancienne plateforme, plusieurs erreurs ont été identifiées. Elles ont invalidé une partie des anciens résultats.

Voici quelques erreurs identifiées:

- Calcul des distances entre les nœuds
- Calcul de l'affaiblissement de parcours (pathloss)
- Calcul de la moyenne de la qualité du signal
- Désynchronisation du temps entre les données capturées et les différents nœuds

Certaines erreurs ont été identifiées plus tard durant la modification de la plateforme (ex : le choix de l'antenne d'émission et le délai inter-balise).

2.2. OBJECTIFS DE LA NOUVELLE PLATEFORME

La plateforme doit être adaptée aux matériels disponibles mais elle doit être assez générique pour faciliter son évolution lors du changement de matériels ou de logiciels. La réutilisation des précédents outils permettent un développement plus rapide et surtout une meilleure maîtrise de la plateforme. Elle doit pouvoir fonctionner avec un **réseau de plus de deux véhicules**. La synchronisation de l'heure sur les différentes machines doit être faite pour la cohérence des résultats. Pour harmoniser la plateforme, les programmes pour le traitement des données doivent être unifiés dans un même langage (AWK est facile d'utilisation et rapide dans le traitement des données de type texte). Enfin, pour en faciliter l'utilisation, nous avons décidé de proposer **une interface graphique**.

Les métriques souhaitées avec cette plateforme sont :

- Qualité du signal sous forme de RSSI (Received Signal Strength Indication) pour chaque trame émise sur chaque nœud
- Mesure du bruit
- Distance entre véhicules
- Vitesse et direction des véhicules
- Taux de perte
- Débit mesuré
- Quantité de données reçues
- Durée de connexion
- Gigue
- Temps d'aller retour (Round-Trip delay Time)

2.3. LE MATERIEL D'EXPERIMENTATION

Voici la liste du matériel utilisé lors de nos expérimentations (cf. figure 4):

- GPS Bluetooth Holux GPSlim 236 (SiRF Star III)
- PC Portable Dell D410 et D610
- carte PCMCIA Proxim ORiNOCO Gold 11b/g avec connecteur externe (8470-WD) (carte à base de chipset Atheros)
- Antenne omnidirectionnelle ORiNOCO Range Extender Antenna (2.5 dbi) connecteur MC-Card plug
- Adaptateur 12V/220V Allume cigare
- Talky Walky



Figure 4: Matériel utilisé.

2.4. LES LOGICIELS DE LA PLATEFORME

La plateforme fonctionne uniquement sous système d'exploitation Linux. Elle a été testée sur les distributions Red Hat Entreprise 4, Kubuntu 7.04 Feisty Fawn et Mandriva 2007.1. A Linux, il faut ajouter des outils réseaux comme ifconfig, ping et les wireless extension et tools [TOURR] de Jean Tourrilhes qui sont en général disponible par défaut dans les distributions linux récentes. Le pilote (driver) « madwifi modifié [MAD] » de la plateforme a besoin d'être recompilé pour chaque linux, il est donc nécessaire d'avoir les fichiers sources et entêtes de linux. Uudecode est aussi nécessaire pour le firmware de la carte sans fils (disponible dans le package sharutils de ubuntu). Les utilitaires bluetooth sont aussi nécessaires (package Bluez, incluant hcitools rfcmm) pour la connexion du GPS.

Les logiciels externes à la distribution linux sont:

- Iperf : générateur de trafic TCP/UDP [IPERF]
- GNU Plot : création de courbes de résultats [PLOT]
- TCL/TK : langage utilisé pour l'interface graphique et la synchronisation d'horloge [TCLTK]
- VLC : diffusion et affichage de vidéo [VLC]
- AWK : langage utilisé pour l'analyse des résultats [AWK]

La version de Madwifi [MADMOD] utilisée a été modifiée, par rapport à la version disponible sur Internet, pour la capture d'informations avancées telles que de la qualité du signal et le niveau de bruit. Elle modifie aussi certains paramètres de base, tels que le délai inter-balise, la désactivation de la réémission, ... Un programme nommé stanford_stat permet la récupération des informations du pilote vers un fichier.

La figure 5 permet de voir comment la plateforme s'articule avec les différents éléments.

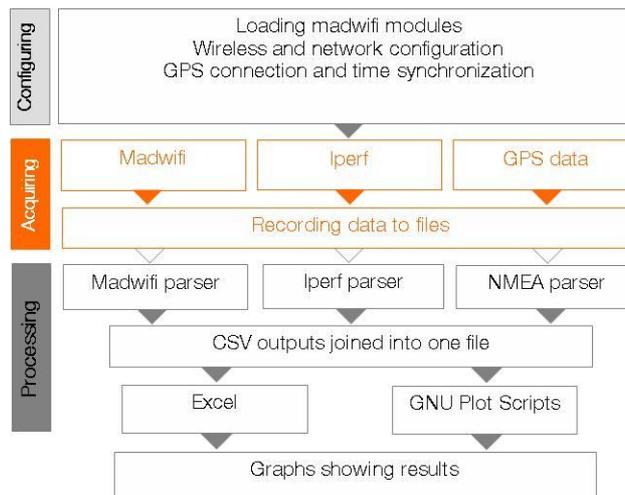


Figure 5 : Vue globale de la plateforme

2.5. CONFIGURATION DE LA PLATEFORME

De nombreux paramètres sont disponibles dans la plateforme pour s'adapter aux différents scénarios. C'est sans doute la partie la plus complexe car de nombreux paramètres entrent en jeu (cf. Figure 6).

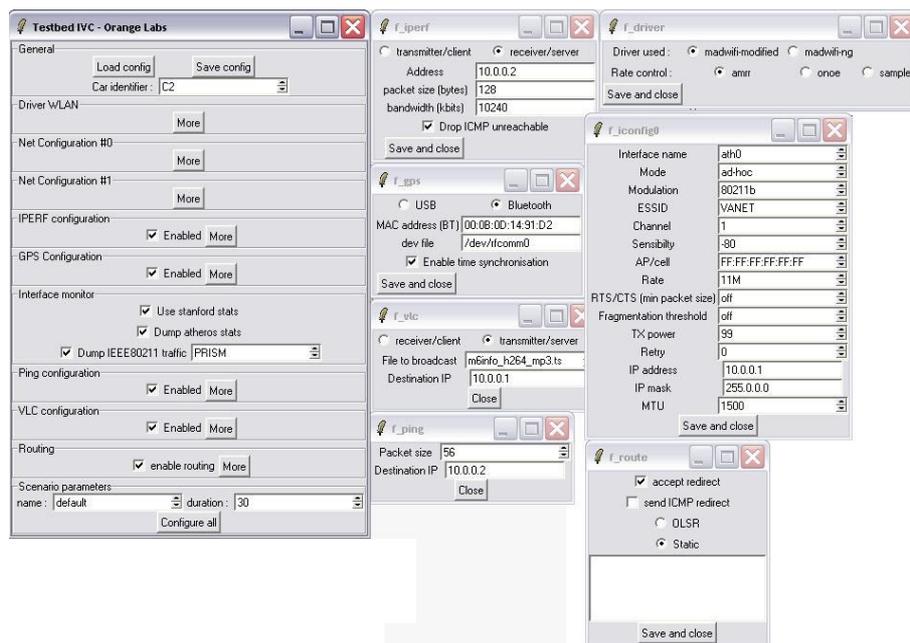


Figure 6 : Capture d'écran de l'interface de configuration

Nous allons décrire brièvement les paramètres principaux de la plateforme. Pour plus de détail sur ces paramètres, l'annexe sur la norme 802.11 peut être consultée.

LES PARAMETRES SANS FILS



Le choix du mode de fonctionnement peut être de type adhoc, station (sta), ou point d'accès (ap). Le mode « adhoc » indique un mode sans infrastructure. Celui-ci est le mode pour la communication de véhicule à véhicule. Le mode « sta » indique un mode station qui va donc se connecter à un point d'accès. Il est destiné à un réseau de véhicule à infrastructure. Le mode « ap » indique un mode point d'accès. L'interface va alors agir comme un point d'accès. On pourra ainsi se placer comme une infrastructure.

Le type de modulation permet de choisir la norme par exemple la modulation DSSS de 802.11b ou OFDM de 802.11g.

Le nom de la cellule dans un réseau avec infrastructure identifie la borne qui gère le client. Il n'est pas nécessaire de le fixer à part si on souhaite dialoguer avec une borne spécifique à un réseau. Par défaut, la borne avec la meilleure qualité de signal sera choisie. De même dans un réseau ad-hoc, il n'est pas nécessaire de le fixer. Cependant, il se peut que deux réseaux ad-hoc ayant le même ESSID ne fusionnent pas, le fixer permet de résoudre ce problème.

Le contrôle de débit peut se régler de manière automatique suivant l'algorithme choisit avec les drivers madwifi (AMRR, ONOE et SAMPLE sont disponibles). Nous pouvons aussi le fixer à un débit déterminé. Dans le madwifi modifié, l'algorithme AMRR est privilégié et désactivé par défaut.

Le mécanisme de réémission (retry) permet dans le cas de non réception d'acquittement de la trame de la réémettre. Il permet ainsi d'obtenir un plus faible taux de perte. Ce mécanisme est désactivé par défaut dans madwifi modifié. De ce fait, l'acquittement n'est pas actif en mode unicast alors que la norme 802.11 le prévoit mais cela permet de ne pas interférer avec les mesures par une réémission de la trame.

La puissance d'émission est un paramètre important pour rester dans la légalité d'émission d'ondes. Le calcul de la PIRE (Puissance isotrope rayonnée équivalente) est détaillé dans [COINCHON] et voici ce calcul pour notre matériel :

$$\text{PIRE(dBm)} = (\text{Puissance de transmission (dBm)}) - (\text{Pertes dans les câbles et connecteurs (dB)}) + (\text{Gain de l'antenne(dBi)})$$
$$\text{PIRE(dBm)} = 18 \text{ dBm (60mW, puissance maximale avec notre carte wifi)} - 3\text{dB (1dB pour le connecteur et 2 db par mètre de câble RG174)} + 2,5 \text{ dBi (gain isotrope de l'antenne)}. = 17,5 \text{ dBm}$$

Avec notre matériel, nous sommes donc bien en dessous de la puissance maximale autorisée en France de 20dBm, malgré le réglage de puissance de la carte wifi au maximum.

PARAMETRES RESEAU



A chaque voiture correspond une adresse IP dans le même réseau. Le choix du réseau est arbitraire et par défaut à 10.0.0.0/8. Dans un scénario à plusieurs voitures, il faut activer le routage sous linux grâce à l'option ip_forward qui va permettre de réémettre le paquet reçu. Avec des chemins statiques, il faut spécifier pour chaque destination le relai. De plus, il faut configurer correctement le comportement ICMP de linux en désactivant l'option send_redirects et en activant l'option accept_redirect.



PARAMETRES DU LOGICIEL IPERF



Le logiciel Iperf [IPERF] permet la **génération de trafic réseau** TCP ou UDP. Il est très utilisé dans la recherche car il est gratuit, open source et facile d'utilisation. Le premier paramètre est l'adresse IP de destination du trafic. Lorsque le mode UDP est activé, il est possible d'agir sur le débit que l'on souhaite émettre. Cependant, si ce débit est trop important et que la file de message à émettre est pleine alors iperf va réduire son émission de paquets. Il est aussi possible d'agir sur la taille des paquets envoyés, en particulier pour éviter la fragmentation au niveau IP pour satisfaire la taille maximale des données (MTU) de la couche MAC. Une option de la plateforme permet à un client d'émettre du trafic sans que le serveur soit présent. Cela est possible en inhibant les messages « ICMP unreachable ».

PARAMETRES DU LOGICIEL VIDEOLAN (VLC)



Le logiciel VideoLan [VLC] permet la visualisation et la diffusion de fichier vidéo sur un réseau. Il gère de nombreux protocoles de diffusion (RTP, MMS, ...) et de format vidéo. Pour la configuration de la plateforme, il suffit de spécifier si l'on est émetteur ou récepteur. Dans le cas de l'émetteur, il faut spécifier le fichier à émettre ainsi que l'adresse de diffusion qui peut être unicast ou multicast. Le protocole de diffusion utilisé est le RTP/UDP par défaut dans la plateforme.

SYNCHRONISATION DE L'HEURE



La fonction de synchronisation du temps est très importante dans la plateforme car elle permet de mettre en relation l'ensemble des informations reçues par les différents nœuds. Pour cela, nous utilisons l'heure donnée par le GPS car elle est très précise et identique sur les différents postes. Nous estimons l'erreur à + ou - 1 seconde, en considérant les différents intermédiaires et la variation du temps d'exécution des différentes machines.

2.6. ACQUISITION DE DONNEES

Le lancement de l'acquisition des données est très simple. Il suffit de saisir le nom de l'expérience, sa durée et de valider quand on souhaite commencer. Les différentes informations sont alors enregistrées dans des fichiers de logs. Ils sont par défaut situés dans le dossier logs puis dans celui du nom de l'expérience.

En cours d'expérience, on peut afficher en temps réel des informations de l'expérience, tel que le taux de perte, et la qualité du signal comme on peut le voir sur la figure 7.

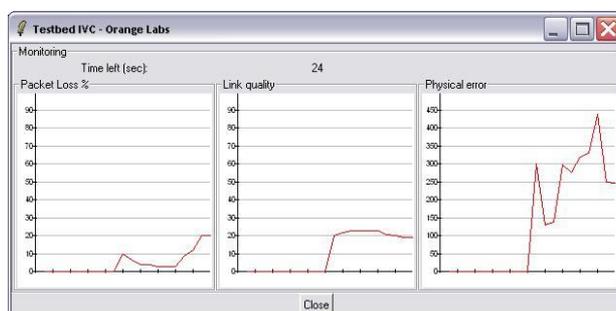


Figure 7 : Capture d'écran de l'interface du moniteur

2.7. ANALYSE DES DONNEES CAPTUREES

L'ensemble des **analyseurs de traces** sont écrits en AWK, un langage de traitement de fichier texte. Nous avons développé 4 analyseurs de traces pour les fichiers de GPS, de madwifi (stanford stat), de iperf et de ping. Les fichiers d'entrée et de sortie sont spécifiés en arguments de ligne de commande. Dans le cas d'une erreur de saisie, une aide minimale est affichée.

Un script global a été créé pour appeler l'ensemble des analyseurs et fusionner les résultats en un fichier. La fusion est faite grâce à l'utilitaire join d'Unix en utilisant la colonne d'horodatage des informations. Cela permet la **synchronisation** de l'heure pour chaque information enregistrée.

Le **tracé de courbes** est effectué grâce à GNU Plot. Des scripts pour la génération de graphes ont été créés mais ils ne peuvent être génériques car les graphes sont dépendants des scénarios et des métriques à mettre en avant.

3. LES SCENARIOS DE TESTS

Pour couvrir le maximum de situations réelles et d'applications, plusieurs scénarios ont été envisagés et nous avons choisi les plus pertinents.

3.1. SCENARIOS V2V

Nous avons d'abord imaginé des scénarios simples de communication entre 2 véhicules. Une première partie des tests ont été effectués antérieurement à mon stage mais les résultats ont été erronés. Nous avons donc décidé de les reprendre pour obtenir de bonnes comparaisons avec les nouveaux scénarios. Les paramètres ont été fixés pour toutes les expériences (cf. figure 8). Ils ont été choisis pour simuler le débit d'un flux vidéo.

Modulation	802.11b, fixé à 11Mbps
Taille des paquets	560 octets
Débit	300 Kbps
Réémission	Désactivée
Transport	UDP
RTS/CTS	Désactivé

Figure 8 : Résumé des paramètres des expériences V2V

LES SCENARIOS SIMPLES A DEUX VEHICULES

Le premier scénario est le croisement de deux véhicules à différentes vitesses comme dans la figure 9. Nous avons testé à faible vitesse, environ 30km/h et à vitesse modérée, environ 50km/h.

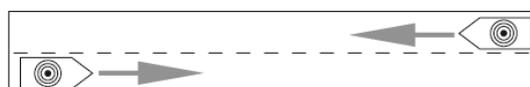


Figure 9 : Scénario de croisement

Le scénario de « passing » consiste à immobiliser une voiture au milieu d'un segment de route et une autre à le parcourir (cf. Figure 10). Cela correspond à une situation d'un croisement avec une voiture arrêté au feu rouge et l'autre passant au feu vert.

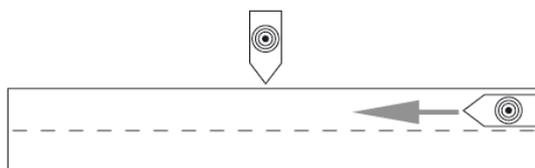


Figure 10 : Scénario de « passing »

Le scénario d'accélération permet de voir l'influence de l'accélération sur la communication. Pour cela, les deux voitures sont l'une à côté de l'autre et l'une accélère jusqu'au bout du segment de route.

LES NOUVELLES EXPERIENCES A PLUS DE DEUX VEHICULES

Ces expériences sont inédites car elles montrent la capacité des réseaux multi-sauts dans un réseau de véhicules.

Le scénario du simple saut permet de voir l'influence d'un passage par un nœud intermédiaire (cf. Figure 11). Le but étant ici d'augmenter les distances entre émetteur et récepteur en utilisant un nœud relai.

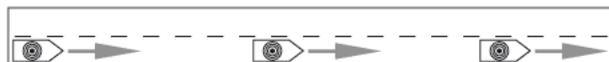


Figure 11 : scénario à 3 véhicules

Le problème de ce scénario est de forcer le passage par le véhicule relai. La solution est décrite dans la partie "Configuration réseau" de la plateforme de tests. Cette expérience a été faite avec des véhicules immobiles, puis en mouvement avec différentes vitesses.

Enfin, un scénario de chaîne de 6 véhicules (cf. Figure 12) permet d'étudier les comportements de la communication en utilisant 4 relais. Le choix des relais est fixé au départ par l'affectation de routes statiques, c'est-à-dire sans un protocole de routage dynamique de type OLSR ou AODV.



Figure 12 : scénario à 6 véhicules

3.2. SCENARIOS I2V

Les scénarios de véhicule à infrastructure sont importants car dans une phase de déploiement, les infrastructures permettent de proposer des services à tous les véhicules malgré un faible taux de pénétration.

Le scénario testé se compose d'une borne statique située sur un pont alors qu'une voiture circule sur une voie express passant en dessous. Différentes vitesses ont été testées pour tenir compte d'un maximum de situations. La borne est configurée en tant qu'émettrice continue de données avec le débit maximum.

Le véhicule est configuré comme ne connaissant pas le canal d'utilisation de la borne, ainsi nous le forçons à la découvrir par une méthode de recherche. Le but est de se rapprocher d'une condition réelle de découverte avec l'établissement d'un dialogue d'authentification et d'association avant le transfert de données.

3.3. SCENARIO HYBRIDE

Nous avons testé un scénario hybride dans le but d'étendre la couverture d'une borne émettrice. Pour cela, la borne est située sur un pont alors que deux véhicules se suivent et sont séparés d'une distance permettant la communication entre elle. D'abord, la borne se connecte directement sur la première voiture et lui envoie les données (cf. Figure 13). Lorsque celle-ci devient hors d'atteinte, un basculement de route s'effectue et les données vont alors être relayées par le second véhicule.



Figure 13 : Scénario hybride à 2 véhicules

Cependant, ce changement de destinataire n'est pas trivial car il doit prendre en compte la qualité du signal, le taux de perte, la distance, ... Ainsi pour éviter la complexité et les problèmes d'une telle solution, nous avons décidé d'effectuer un basculement manuel. La station réceptrice va ainsi indiquer à la borne de changer de chemin et de relayer les informations par le second véhicule.

Le problème de cette solution est l'utilisation de deux modes en simultanée : adhoc et station. La solution est d'utiliser « madwifi-ng » qui propose les interfaces multiples. Ainsi il est possible de créer une interface en mode ad-hoc et une seconde en mode station, à condition d'être sur le même canal. Cependant, madwifi-ng ne peut être utilisé que sur le véhicule relai car l'outil de moniteur de la qualité ne fonctionne que sur l'ancien madwifi.

Un autre problème est de trouver comment basculer d'un mode envoi direct à un mode envoi avec relai. La solution utilisée est de vérifier à tout instant les stations associées à la borne. Si le véhicule récepteur est associé alors les données lui sont envoyées directement sinon elles sont envoyées au véhicule relai. Pour indiquer le changement, le véhicule récepteur va envoyer une désassociation à la borne qui va ainsi envoyer les informations au relai.

4. LES RESULTATS ET ANALYSES

4.1. EXPERIENCES DE COMMUNICATION VEHICULE A VEHICULE

Les mêmes expériences ont été réalisées précédemment à mon stage et a fait l'objet d'un papier [VTC07] accepté à la conférence IEEE VTC 07. Cependant, les résultats avaient été biaisés à cause de petites erreurs présentes dans la plateforme. On peut confirmer maintenant que les conclusions sont proches des précédentes car les courbes gardent la même allure. Dans la figure 14 et la figure 15, on voit très bien l'influence de la distance sur la qualité du signal et le taux de perte.

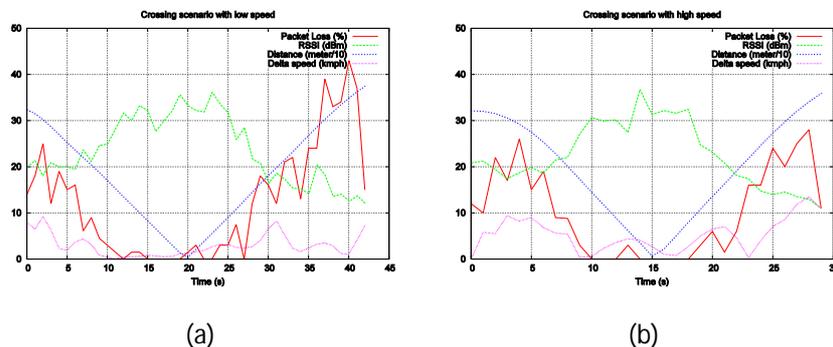


Figure 14 : Scénario de croisement à petite (a) et grande (b) vitesse

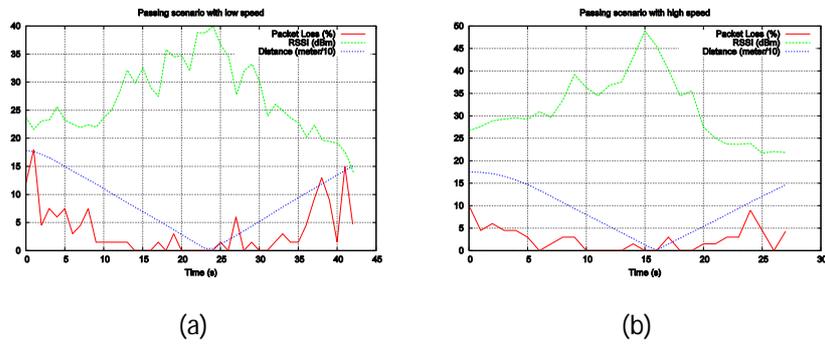


Figure 15 : Scénario de "passing" à petite (a) et grande (b) vitesse

Grâce à ces scénarios, nous avons pu voir que la communication pouvait se faire dans les conditions normales de déplacement des véhicules.

4.2. EXPERIENCES DE COMMUNICATION VEHICULE A VEHICULE MULTI-SAUTS

Les figures 16 (a) et 16 (b) correspondent aux mesures dans un scénario multi-saut statique. Ils montrent les pertes de paquets et RTT mesurés entre trois voitures statiques. Tandis que les figures 17 (a), 17 (b) et 18 (a), 18 (b) montrent les résultats obtenus avec trois voitures qui se suivent sur une autoroute et avec deux vitesses prédéterminées (50 Km/h et 90 Km/h).

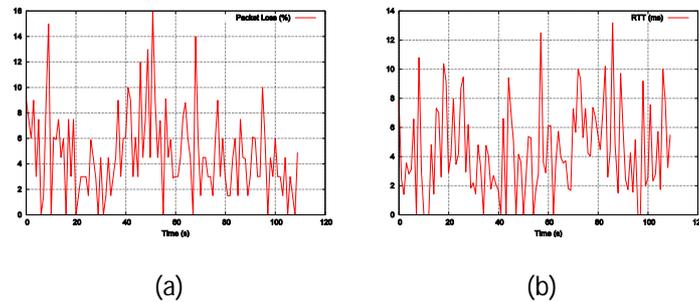


Figure 16 : Taux de perte (a) et délai d'aller-retour (b) dans un scénario statique.

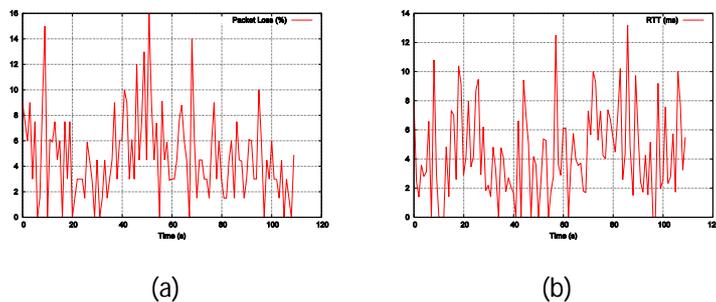


Figure 17 : Taux de perte (a) et délai d'aller-retour (b) dans un scénario de suivi (petite vitesse).

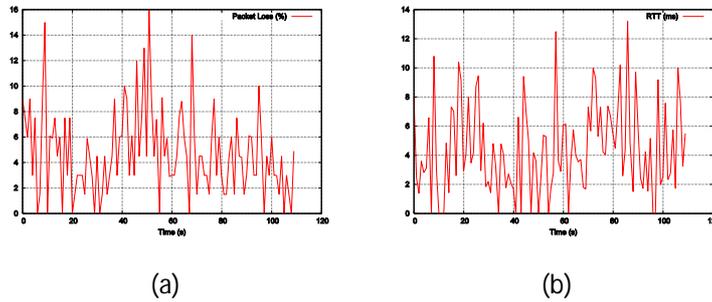


Figure 18 : Taux de perte (a) et délai d'aller-retour (b) dans un scénario de suivi (grande vitesse)

Les pertes dans le scénario de suivi sont inférieures au scénario statique malgré la mobilité de nœuds. Cette différence provient de l'environnement car sur autoroute, il n'y a ni obstacle et ni interférence d'autres systèmes radios.

La figure 19 montre un résumé des statistiques des premières d'expériences. En comparant les pertes moyennes obtenues et le délai d'aller-retour en petite ou grande vitesse, nous pouvons conclure que la vitesse affecte peu les performances des communications multi-sauts V2V.

	Average losses (%)	Average RTT (ms)	Average distance (m)
Static Scenario	4,75	4,41	87,17
Following Scenario (LS)	1,99	1,97	91,39
Following Scenario (HS)	3,48	2,04	142,05

Figure 19 : Résumé des statistiques des scénarios V2V

Les pertes moyennes dans une communication directe (0.36 %) sont inférieures à celles obtenues pour le scénario à un saut radio (3.48 % pour le scénario de suivi).

La figure 20 résume les statistiques obtenues lors de la **chaîne de communication de 6 véhicules**, c'est-à-dire en utilisant 4 relais. Le taux de perte est de 15,69% de bout en bout soit environ 3,5% de perte par émission.

Distance inter véhicule	71,93	m
Distance Total	359,64	m
Vitesse	78,69	km/h
Débit effectif	252,67	kbps
Débit émetteur	300	kbps
Taux de perte	15,69	%
RTT	7,99	ms
RSSI	42,71	
Bruit	-98,79	dB

Figure 20 : Moyenne des métriques de la chaîne de 6 véhicules

Les pertes augmentent avec le nombre croissant de sauts radio. On explique ce phénomène par l'utilisation du mécanisme de CSMA et par le problème de station caché (mécanisme RTS/CTS désactivé).

Lors de ce stage, nous avons aussi participé à un test dans un scénario à 6 véhicules avec l'Université de Technologie de Compiègne (UTC) et leur plateforme de test nommé « airplug ». Cependant, les résultats n'ont pas été concluants à cause de problèmes techniques.

Les résultats obtenus lors de tous ces tests sont encourageants car ils montrent la bonne performance de la norme 802.11 dans un réseau de véhicule avec des pertes et des délais faibles.

4.3. EXPERIENCES DE COMMUNICATION DE VEHICULE A INFRASTRUCTURE

Pour ces expérimentations, nous nous sommes focalisés sur les métriques suivantes : la puissance du signal, le taux de perte, la durée de connexion au réseau et le total de données reçues.

Nous avons exécuté plusieurs fois les essais menant à des résultats semblables. La figure 21 représente la perte de paquet et le RSSI pour le scénario simple avec point d'accès et un véhicule. La figure 22 représente les mêmes mesures pour le scénario hybride avec 2 véhicules et un point d'accès. L'impact des ponts est clairement visible.

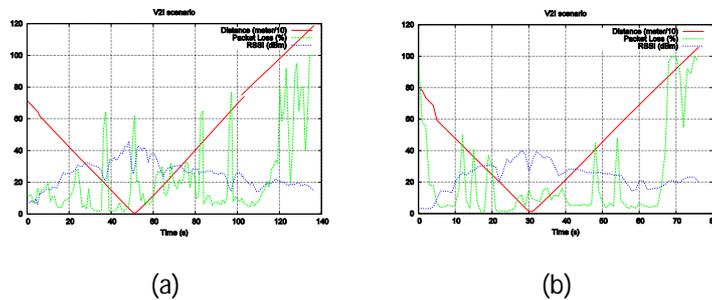


Figure 21 : Taux de perte et RSSI pour le scénario simple à basse (a) et haute (b) vitesse.

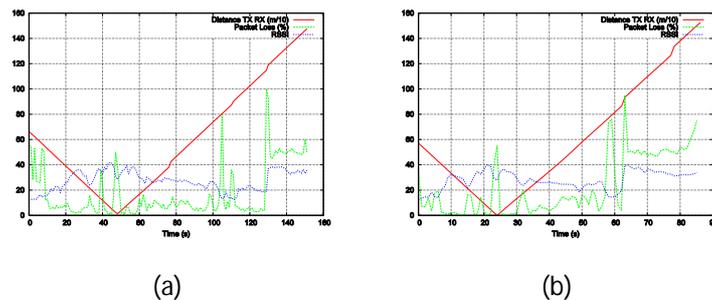


Figure 22 : Taux de perte et RSSI pour le scénario hybride à basse (a) et haute (b) vitesse.

La figure 23 montre le temps de connexion et la quantité de données transférées pour les deux derniers scénarios simple et hybride.

a)	Network connection time		Amount of data	
	high speed	low speed	high speed	low speed
Total	81	140	59,195	98,86

b)	Network connection time		Amount of data	
	high speed	low speed	high speed	low speed
direct	66	143	54,247	106,452
multihop	25	27	9,813	9,519
Total	91	170	64	116

Figure 23 : Durée de connexion (en secondes) et quantité de données (en méga-octets) transférées dans le scénario simple (a) et hybride (b)

Les résultats expérimentaux ont révélé la faisabilité du réseau ad hoc pour agrandir la zone de couverture des points d'accès. Il augmente ainsi la durée de connexion pour des voitures en mouvement de plus de 16 %. Il augmente aussi la quantité de données que la voiture peut recevoir de plus de 10 %.

Nous concluons qu'un réseau ad hoc inter-véhicule est avantageux pour étendre la connectivité des véhicules à des points d'accès fixes.

5. AMELIORATIONS POSSIBLES DE LA PLATEFORME

5.1. LE PILOTE MADWIFI-NG

La plateforme utilise principalement une version de madwifi ancienne qui a été modifiée pour capturer les informations de bas niveau tel que la qualité du signal reçu. Cette version de madwifi n'est maintenant plus maintenue et souffre de plusieurs bogues que nous avons rencontrés lors de nos tests (fusion de cellules adhoc parfois aléatoire, la dissociation en mode station entraîne le non fonctionnement du mode adhoc, qualité de signal parfois à 0, ...).

La nouvelle version du pilote madwifi permet d'instancier plusieurs interfaces de type ad hoc, station ou moniteur. Cette version est régulièrement maintenue et les codes sources sont toujours disponibles sur [MAD]. L'interface moniteur permet de capturer l'ensemble du trafic avec WireShark et de récupérer entre autre la puissance du signal (via les entêtes PRISM). Cependant, cela demande pour la plateforme la création d'un interpréteur de fichier PCAP ou bien d'un analyseur de texte après l'exécution du logiciel tshark.

Depuis le noyau Linux 2.6.22, la norme 802.11 est gérée en natif et permet une couche MAC homogène entre les différents pilotes. Cette couche appelée « mac80211 » permet aussi la création de multiples interfaces comme le permet madwifi-ng. C'est une perspective à garder pour le déploiement d'une plateforme avec du matériel hétérogène.

5.2. IMPLEMENTATION D'UNE COUCHE 2.5

Lors des scénarios, nous nous sommes aperçus que la mise en œuvre n'était pas toujours simple. La création d'une couche de niveau 2.5, entre le niveau liaison et le niveau réseau, permettra plus de souplesse pour les tests. De plus, elle sera un début d'implémentation pour une solution pour les réseaux de véhicules.

Cette couche pourrait être « crosslayer » (utilisation d'informations de niveau différent) avec l'utilisation de la puissance du signal ou des coordonnées GPS, pour améliorer son fonctionnement. On pourrait également y intégrer un mécanisme de diffusion.

6. CONCLUSIONS

Nous avons pu voir en particulier que la perte de la ligne de vue (LOS ou line of sight) entre l'émetteur et le récepteur engendre de nombreuses pertes. De même, le fait qu'un véhicule s'intercale entre les deux voitures communicantes, augmente les pertes. La distance est aussi un facteur de perte alors que la vitesse et l'accélération ne sont que peu influentes sur la communication.

Ces expérimentations ont fait l'objet d'un article et d'un poster à la conférence UBIROADS 07 et d'un article [MOV07] accepté à la conférence MoVeNet 07.

Lors de ces expérimentations, nous avons pu aborder les problématiques de diffusion avec un mécanisme de routage simple. L'objectif de la seconde partie de mon stage est d'étudier des



mécanismes de diffusion plus complexe sous simulateur. Cette partie est détaillée dans la section suivante.



DISSEMINATION DE DONNEES DANS UN RESEAU DE VEHICULES

Le second objectif de mon stage était de travailler sur la dissémination de données. Nous allons d'abord introduire la dissémination dans les réseaux de véhicule dans la partie 1. Dans la partie 2, nous détaillerons un état de l'art de la littérature. Dans la partie 3, nous étudierons les performances de deux protocoles de diffusion. Enfin, dans la partie 4, nous donnerons quelques idées pour l'amélioration des protocoles.

1. INTRODUCTION DE LA DISSEMINATION

La dissémination d'information consiste à acheminer une information d'une source vers une ou plusieurs destinations, en assurant un délai d'acheminement réduit, une grande fiabilité et une meilleure utilisation des ressources. Les destinations ciblées par l'opération de dissémination peuvent être caractérisées par la position, l'adresse IP (cf. Figure 24), la région géographique ou autre (cf. Figure 25).

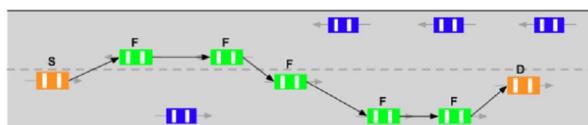


Figure 24 : Communication à destination unique (unicast)

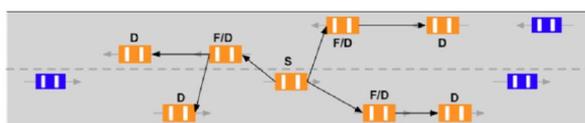


Figure 25 : Diffusion limitée aux véhicules à deux sauts radio

Dans les réseaux MANETs, les protocoles de routage utilisent l'inondation pour la découverte et la maintenance des routes. L'inondation est le protocole le plus naïf pour la diffusion dans les réseaux ad hoc. Dans celui-ci chaque nœud rediffuse systématiquement le paquet reçu une seule fois. Le problème (aussi connu dans [TSE02] comme "the broadcast storm problem") est que cette rediffusion systématique cause inutilement une consommation excessive de bande passante vu que chaque nœud va recevoir plusieurs fois la même information via le canal sans fil. De plus, dans le cas de réseaux ad hoc denses, le fait que chaque nœud rediffuse systématiquement génère un nombre important de collisions qui ne seront pas corrigés par la couche MAC (absence d'ACK lors de la diffusion). Ce qui réduit donc l'efficacité et la fiabilité de la diffusion. Pour éviter ce phénomène, la solution la plus souvent retenue est d'écarter un certain nombre de pairs par une heuristique.

Toutefois, d'autres types de diffusion mieux adaptés aux environnements IVC sont désormais possible notamment le multicast et la géo-diffusion. Le multicast est utilisé par des applications qui souhaitent transmettre des informations vers plus d'une destination. Un nœud voulant recevoir les données, doit d'abord joindre un groupe multicast. Les messages envoyés sont alors reçus par tous les membres du groupe. La géo-diffusion quant à elle adopte le même principe de fonctionnement, à la différence qu'au lieu de joindre explicitement un groupe multicast, les nœuds sont implicitement membres du même groupe s'ils sont dans la même zone géographique. Le groupe devient dans ce cas groupe géocast. Dans ce type de protocoles, la terminologie suivante est utilisée : (i) Groupe géocast : les membres d'un groupe sont définis par leur localisation géographique, (ii) Zone géocast : est l'espace géographique où l'ensemble des nœuds mobiles membre d'un groupe géocast sont localisés. Entrer dans la zone revient à joindre le groupe et vice versa, et (iii) Zone de relayage (forwarding

zone) : représente la zone où les paquets de données sont relayés. Chaque groupe géocast dispose d'une zone de relayage, et seuls les nœuds se trouvant à l'intérieur peuvent relayer les paquets. Une zone géocast peut être incluse dans une zone de relayage (cf. figure 26) ou non (cf. figure 27).

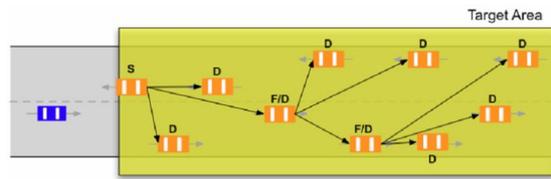


Figure 26 : Géodiffusion

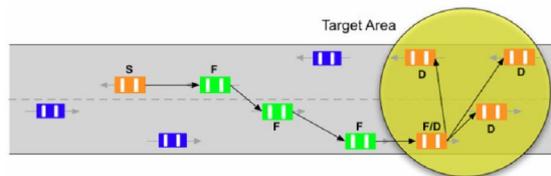


Figure 27 : Géodiffusion avec zone distante de diffusion

Lors de ce relaiage d'informations, le réseau peut être partitionné et ainsi la chaîne de communication rompue. Un mécanisme nommé "**opportunistic forwarding**" permet de résoudre ce problème en sauvegardant le message au niveau du nœud en attendant l'arrivée d'un nouveau nœud voisin. Lors qu'un nœud arrive et qu'il satisfait les conditions de transmission, la communication reprend et le message est transféré à ce nouveau voisin.

2. ÉTAT DE L'ART

Lors de l'étude de l'état de l'art de la dissémination, nous avons pu isoler deux types de dissémination avec des contraintes différentes : La dissémination de **messages d'urgence** et celle des messages relatifs aux **applications de confort**.

Un constat peut être d'ores et déjà fait dans les deux cas : plus la zone de création du message est éloignée de la réception, moins le message aura d'importance.

Un mécanisme que l'on retrouve dans de nombreux protocoles est "Distance Defer Transfer" [DDT]. Pour disséminer le plus rapidement possible, DDT propose de relayer l'information par les nœuds les plus éloignés, en supposant que les nœuds intermédiaires écoutent simplement le message. Pour élire ce nœud le plus éloigné, les récepteurs calculent la distance de l'émetteur grâce à la position insérée dans le message. Un temps d'attente inversement proportionnel à cette distance est alors enclenché avant la réémission. Ainsi, le premier à réémettre sera le nœud le plus éloigné et les autres nœuds annuleront leur réémission à la réception du message rediffusé. La formule 1 montre le calcul effectué pour borner le délai d'attente.

$$WT(d) = -\frac{MaxWT}{Range} \cdot \hat{d} + MaxWT$$

$$\hat{d} = \min\{d, Range\}$$

Formule 1 : calcul du délai d'attente dans DDT

2.1. DISSEMINATION DE MESSAGES D'URGENCE

Un message d'urgence est caractérisé par son lieu de génération, sa zone de pertinence et sa durée de validité.

Le protocole de dissémination doit donc assurer la contrainte spatiale et temporelle. En effet, il faut que tous les véhicules proches de l'alerte soient avertis de l'incident mais aussi qu'ils soient informés le plus tôt possible pour qu'ils aient le temps d'agir en conséquence.

Deux approches sont alors possibles, soit une diffusion assistée par des points d'infrastructure le long de la route soit une diffusion complètement distribuée avec une propagation de voitures en voitures avec un mécanisme de sauvegarde/réémission (store and forward).

Nous allons dans cette section résumer des solutions proposées.

a) STEID

Le protocole STEID [STEID] (Spatio-Temporal Information Dissemination) propose de résoudre les besoins en termes de fiabilité spatiale et temporelle. STEID s'assure que tous les véhicules à l'intérieur de la zone d'alerte soient informés et dans un délai suffisant pour réagir. Pour cela STEID s'exécute sur un réseau hybride de type 802.11 et de type cellulaire comme on peut le voir dans la figure 28. L'idée générale de cette architecture est d'utiliser la communication wifi pour transférer l'ensemble des alertes dans le cluster car il est peu coûteux et il s'affranchi bien du facteur d'échelle. Le réseau cellulaire est quant à lui utilisé pour améliorer la fiabilité quand le réseau est partitionné en plusieurs morceaux.

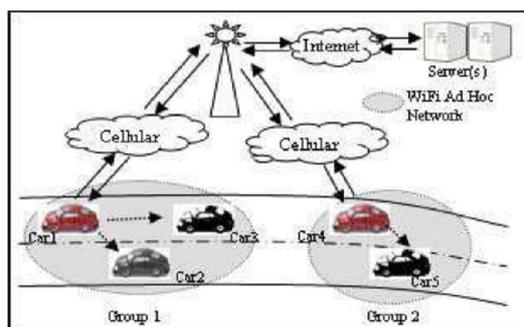


Figure 28 : fonctionnement général de STEID

Pour former un cluster, la solution propose que chaque voiture sur la route avertisse périodiquement sa présence en émettant un message "Hello" en utilisant l'interface WiFi.

A chaque cluster est élu un responsable qui va gérer l'ensemble du trafic à l'intérieur de celui-ci, il joue le rôle d'un "serveur". Il est aussi responsable de la communication entre les autres clusters. La solution propose d'utiliser DDT [DDT] pour la réémission du message. Pour augmenter la fiabilité, l'auteur propose d'ajouter au message "Hello" des informations concernant le nombre d'alertes actives ainsi que la position de l'alerte la plus proche. Cela permet via un algorithme de synchroniser les alertes avec les nœuds voisins.

Le principal inconvénient de la solution est l'émission périodique de messages qui pose des problèmes de passage à l'échelle. De plus, il ne propose ni l'algorithme d'élection, ni le maintien de nœud élu du cluster.

b) DPP

Dans [DPP], l'auteur propose une solution purement ad hoc pour la dissémination de messages d'alerte. Ce protocole, nommé DPP (Directional Propagation Protocol), utilise une direction pour la propagation de l'information. Le protocole prend en compte le phénomène de regroupement de véhicules (nommé aussi cluster) qui se produit sur les axes routiers. A l'intérieur des clusters sont élus un véhicule de tête et un véhicule de queue. Ce sont eux qui vont gérer la propagation des messages entre les différents clusters comme on peut le voir sur la figure 29. A l'intérieur d'un cluster, les véhicules n'acquittent pas les messages alors que d'un cluster à l'autre, les messages sont acquittés pour assurer une fiabilité. Pour la gestion de la fragmentation du réseau, le message peut être enregistré dans les nœuds de tête et de queue pour une future réémission jusqu'à ce que le message soit acquitté par un autre cluster.

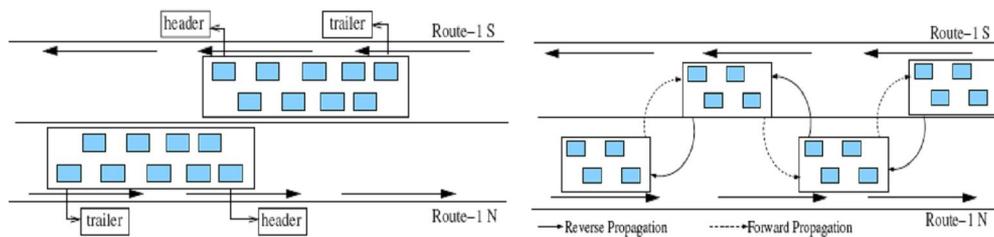


Figure 29 : Propagation de cluster en cluster

Un inconvénient de cette solution est que l'auteur ne propose pas d'algorithme d'élection des véhicules de tête et de queue alors que ce problème n'est pas trivial (utilisation de messages Hello, ou autre). Il ne propose pas non plus l'algorithme de formation et de maintien des clusters. Un autre inconvénient est que l'auteur étudie uniquement la solution dans un environnement de type autoroute et il ne compare pas son protocole avec d'autres solutions.

c) DISSEMINATING MESSAGES AMONG HIGHLY MOBILE HOSTS BASED ON INTER-VEHICLE COMMUNICATION

La solution proposée dans [BRI00] permet la dissémination dans une zone locale autour de l'initiateur. Si le message atteint un seuil de nombre de sauts alors le message n'est pas réémit. Une zone de pertinence est définie dans le message pour informer les conducteurs concernés. Pour augmenter la vitesse de propagation du message, l'auteur propose d'utiliser le mécanisme où le délai d'attente pour la réémission est inversement proportionnel à la distance de l'émetteur [DDT].

L'inconvénient de la solution est qu'elle ne prend pas en compte la fragmentation du réseau et que le choix de limiter la propagation au nombre de sauts n'est pas toujours un critère pertinent.

d) OAPB

Dans [OAPB], l'auteur propose une solution basée sur les probabilités de diffusion pour résoudre le problème du "broadcast storm". Pour cela il utilise la table des voisins à 1 et 2 sauts ainsi que la densité des nœuds environnants. Il utilise aussi le mécanisme de délai inversement proportionnel à la distance [DDT] pour essayer de propager le plus rapidement l'information.

Les inconvénients de la solution est que l'auteur a limité le nombre de nœuds à 40 ce qui ne permet pas une simulation d'une situation réelle. De plus, le surcout engendré par le maintien de la table des nœuds à deux sauts par l'émission de message "Hello" n'est pas négligeable.

e) ODAM

ODAM [BEN04] propose l'émission périodique du message d'alerte par l'initiateur. La réémission du message est limitée à la zone de risque définie dans le message. De plus, il utilise aussi le mécanisme de délai en fonction de la distance [DDT] pour réémettre uniquement à certains véhicules, les plus éloignés. Les simulations montrent que le protocole est fiable à 100% quand la distance de communication est d'au moins 200 mètres.

Cependant, la retransmission périodique par l'initiateur engendre un surcoût important et il n'est pas envisageable à large échelle. De plus, la définition de la zone de risque à la création du message limite les applications du protocole.

2.2. DISSEMINATION POUR DES APPLICATIONS DE CONFORT

Les applications de confort sont généralement plus consommatrices de bande passante avec par l'exemple le téléchargement de fichier. La propagation de message est donc sans contrainte de délai mais doit optimiser la bande passante. Une spécificité des applications de confort est que le contenu du message peut aussi être dynamique et se modifier lors du passage de nœud en nœud (par exemple pour mettre à jour une information).

a) SODAD

Le protocole SODAD [WIS05] combine une diffusion locale périodique et une couche application de sauvegarde et réémission de messages.

La diffusion locale se base sur la construction de l'information par l'intermédiaire d'une **fonction agrégation**. Chaque route est fragmentée sous forme de segments comme on peut le voir dans la figure 30. Les informations reçues sont enregistrées dans une base de données et lors de la diffusion d'un message, les informations les plus récentes et les plus pertinentes de la zone sont sélectionnées et sont insérées dans le message à diffuser.

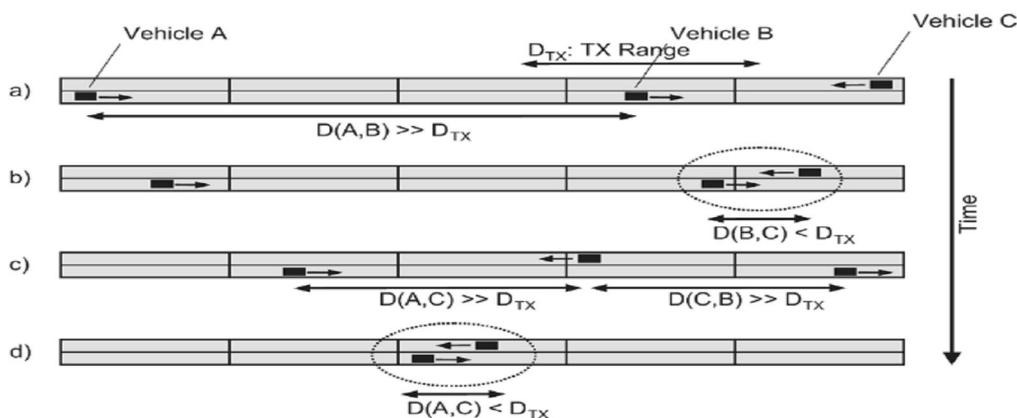


Figure 30 : Fragmentation des routes et connectivité au cours du temps

L'auteur présente aussi un autre mécanisme qu'il appelle la diffusion adaptative. La vitesse à laquelle un véhicule envoie des messages s'adapte à l'environnement actuel en observant deux types d'événements. Si le nœud a reçu de vieilles informations alors le temps entre chaque diffusion va être diminué. À l'inverse, si le nœud reçoit des informations identiques à celle qu'il a enregistré alors le délai de diffusion va augmenter.

b) MDDV

MDDV (Mobility-Centric Data Dissemination Algorithm for Vehicular Networks) [WUH04] est un algorithme de diffusion qui, contrairement aux autres algorithmes géographiques, considère que les véhicules ne disposent pas des positions des véhicules voisins. Le réseau routier est modélisé comme un graphe orienté où les nœuds représentent les intersections, et les liens les segments routiers. Un poids est associé à chaque lien pour refléter la distance et la densité de trafic correspondante. MDDV utilise une trajectoire de relaying spécifiée comme le chemin ayant la plus petite somme des poids d'une source vers la 'région destination' dans le graphe orienté.

c) UMB

Urban Multi-Hop Broadcast Protocol [KOR04] est un algorithme de diffusion qui modifie la couche d'accès 802.11 pour l'adapter au contexte des IVC dans le but de réduire les collisions et d'utiliser efficacement la bande passante. Cette adaptation utilise un mécanisme de RTS/CTS couplé au mécanisme de type DDT qui permet d'éviter le problème de la station caché en mode de diffusion. UMB comprend deux phases : la première appelée diffusion directionnelle où la source sélectionne un nœud dans la direction de diffusion pour effectuer le relaying des données sans aucune information sur la topologie, et la deuxième diffusion aux intersections, pour disséminer les paquets dans toutes les directions, en installant des répéteurs vers tous les segments de route.

d) RBM

Dans RBM (Role-Based Multicast) [HOM00], les auteurs proposent un protocole de multicast où chaque nœud maintient deux listes : une liste de voisins et une liste des nœuds émetteurs. En fonction des contenus de ces deux listes, un nœud décide ou pas de rediffuser le message après un certain temps. Dans cette approche, le protocole suppose l'existence d'une couche liaison qui maintient la liste des nœuds voisins.

3. SIMULATION DE PROTOCOLES ET EVALUATION DES PERFORMANCES

La simulation de protocoles est essentielle pour la création d'un protocole réseau. Elle permet de concevoir, implémenter et "valider" un protocole. Les nouveaux protocoles peuvent être testés à moindre coût et ainsi anticiper les problèmes qui pourront se poser dans le futur afin d'implémenter la technologie la mieux adaptée aux besoins. Le facteur d'échelle est plus facilement pris en compte et la difficulté d'effectuer des mesures directes sur un système réel est ainsi évitée.

La simulation permet aussi la comparaison des protocoles et montrer qu'un protocole est plus performant qu'un autre. Cependant, le simulateur ne prouve en aucun cas la validité d'un protocole et ses performances. En multipliant les simulations et les scénarios, on peut obtenir une évaluation du protocole relativement fiable.

Dans la première section, nous donnerons des détails sur l'outil de simulation GloMoSim. Dans la seconde section, nous expliquerons les modèles de mobilité qui sont importants dans les réseaux de véhicules. Enfin dans la section 3, nous parlerons de l'implémentation des protocoles de diffusion et des résultats obtenus.

3.1. LE SIMULATEUR GLOMOSIM

GloMoSim (Global Mobile Simulator) [GLOMO] est un simulateur de réseaux purement sans fils. Il implémente une couche de propagation radio et aussi en particulier la couche physique et liaison d'IEEE 802.11. Développé par UCLA University of California, il est disponible gratuitement pour l'ensemble des universitaires. Il a été conçu en utilisant la capacité de la simulation parallèle fournie

par Parsec. Pour information, la version commerciale nommé QualNet implémente de nombreuses couches non disponibles dans GloMoSim.

Malheureusement, il souffre de plusieurs bogues non corrigés et l'utilisation du pré-compilateur parsec ne permet pas un débogage efficace. Nous avons du corriger quelques bugs identifiés car GloMoSim ne semble plus être maintenus par les concepteurs, la dernière version datant de 2003.

3.2. LE MODELE DE MOBILITE

La mobilité est très importante dans la simulation de réseaux de véhicules. En effet, c'est elle qui va déterminer si deux pairs sont proches et peuvent communiquer et une des spécificités des réseaux de véhicules est que le déplacement des véhicules est caractérisé par les infrastructures (routes, feux tricolores, carrefour, ...). La prise en compte des dépassements, des bouchons est très importante pour la représentation de la réalité.

Afin de définir un modèle de mobilité adéquat pour les réseaux de véhicules, on distingue les environnements suivants :

- Autoroute : environnement ouvert caractérisé par une grande vitesse de déplacement (avec des limites : vitesse min et vitesse max), avec des dépassements de véhicules, et une densité de nœuds fonction de l'heure de la journée;
- Ville : vitesse modérée avec une probabilité d'intersection plus grande. Il existe des endroits d'arrêt aux feux, une grande densité de voitures, et l'existence de certaines routes plus fréquentées que d'autres (routes principales, endroit commercial ou touristique par exemple);
- Rase campagne : caractérisé par des vitesses moins importantes avec une densité de voitures plus faible.

Pour les réseaux ad hoc mobiles, le modèle Random Way Point (RWP) [JOH96] est l'un des modèles de mobilité les plus répandus et utilisés dans les simulations. Dans ce modèle, chaque nœud choisit individuellement une destination aléatoire dans la limite géographique du réseau et choisit également une vitesse aléatoire de déplacement (comprise entre une vitesse minimum et maximum). Une fois que le nœud a atteint la destination, il effectue une pause pendant une période de temps. Après ce temps de pause, le nœud répète le processus, en choisissant une destination et une vitesse aléatoire différentes. Dans ce cas les nœuds mobiles se déplacent aléatoirement et indépendamment les uns des autres.

Un autre modèle disponible dans GloMoSim est le Trace File qui permet de prendre des positions pré-calculées par un autre logiciel. C'est cette méthode qui a été utilisée lors de nos simulations en utilisant le logiciel VanetMobiSim/CanuMobiSim [VMSIM].

CANU Mobility Simulation Environment (CanuMobiSim) est une plateforme flexible pour la modélisation de la mobilité. Cette plateforme est mise en œuvre comme une application JAVA autonome et, ainsi, peut être utilisée avec presque n'importe quel outil de simulation et d'émulation pour des réseaux mobiles (format NS-2, GloMoSim, et QualNet). Pour simuler le mouvement, il fournit plusieurs modèles de la physique et de la dynamique automobile. De plus, la structure contient plusieurs modèles de mobilité aléatoires, comme le mouvement Brownien ou le mouvement "Random Waypoint".

VanetMobiSim [VMSIM] est une extension pour CanuMobiSim. L'extension VanetMobiSim se concentre sur la mobilité automobile et dispose de nouveaux modèles de mouvement automobiles réalistes aux niveaux tant macroscopiques que microscopiques. Au niveau macroscopique,



VanetMobiSim peut produire des cartes routières en utilisant le diagramme de Voronoï comme sur la figure 31. Il ajoute aussi la gestion des routes à plusieurs voies de circulation, des flux unidirectionnels, et des contraintes de vitesse aux intersections et des feux de signalisation. Au niveau microscopique, VanetMobiSim met en œuvre de nouveaux modèles de mobilité, permettant la prise en compte des véhicules voisins (ralentissement, distance de sécurité, ...).

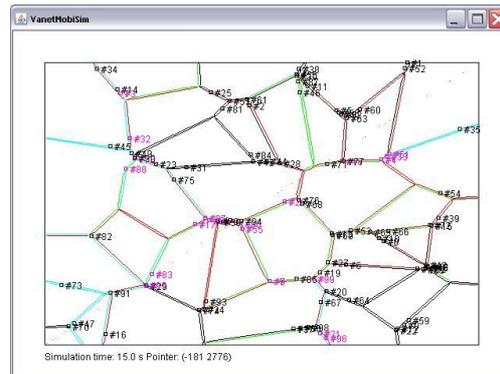


Figure 31 : Capture d'écran de l'interface graphique de VanetMobiSim

3.3. PERFORMANCES DES SOLUTIONS "DDT" ET "SODAD"

Nous avons décidé d'implémenter les solutions DDT et SODAD, deux solutions simples, pour comprendre les enjeux d'une solution de diffusion optimisée. L'implémentation d'un protocole de diffusion peut s'effectuer à différent niveau du modèle OSI. Notre choix est de l'implémenter au niveau réseau car c'est celui qui semble le plus pertinent. Les métriques que nous avons essayé de mettre en avant sont le nombre de rediffusions, la distance parcourue par le message, et le délai mis par le message pour parcourir cette distance.

Pour toutes les simulations, nous avons utilisé un environnement urbain avec 300 véhicules sur une surface 2500m². Le déplacement des véhicules est aléatoire sur une topologie fixe de routes. Un nœud qui est situé au milieu de la carte génère des messages de 100 octets toutes les secondes.

Distance Defer Transfer

Nous avons configuré la solution DDT pour limiter le nombre de sauts radio et pour que le délai d'attente maximum soit limité à 10 ms.

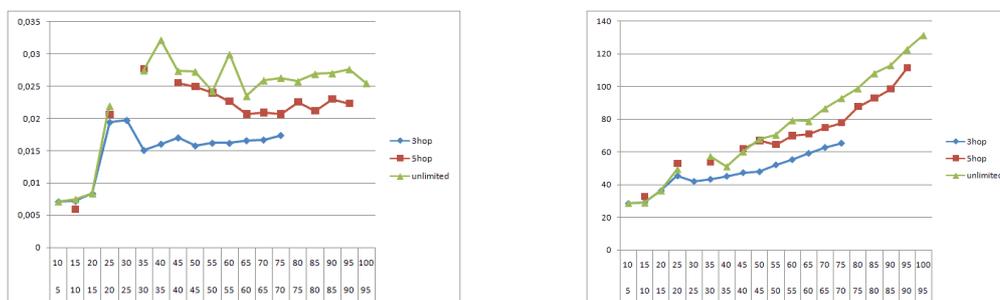


Figure 32 : délai (en secondes) de propagation du message et nombre de retransmission pour la solution DDT en fonction du pourcentage de nœuds informés et du nombre de sauts

Lors des simulations de la figure 32, nous avons remarqué que la limitation du nombre de saut radio dans DDT permet de « borner » les délais. Cette limitation permet aussi de délimiter une zone informée par le message. Elle permet aussi de réduire le nombre de retransmission mais le nombre de nœuds informés en est donc diminué.

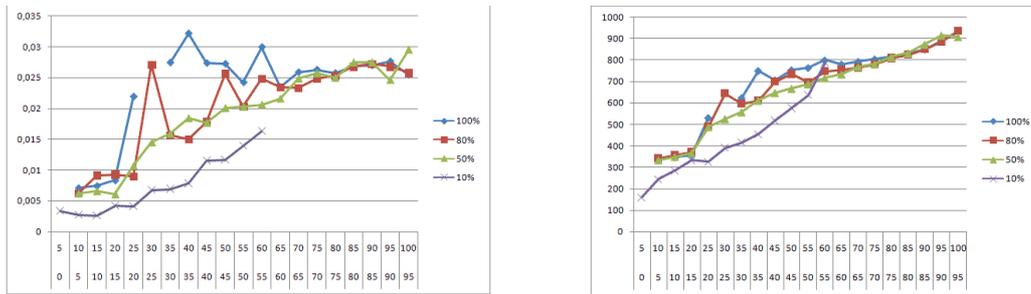


Figure 33 : délai (en secondes) et distance moyenne (en mètres) du parcours des messages pour la solution DDT en fonction du pourcentage de noeuds informés et du taux de pénétration

La distance parcourue par les messages dépend de la taille du cluster car DDT ne propose pas de solution pour la fragmentation du réseau. Le taux de pénétration influe sur la taille du cluster et par conséquent sur la distance parcourue par le message.

pénétration	informé (%)	retransmission	délai (sec)	distance moyenne (mètre)	distance maximum (mètre)
100%	87,62	109,27	0,0261	836,80	1612,09
80%	83,02	86,13	0,0251	809,43	1566,29
50%	67,44	50,18	0,0221	731,31	1451,44
10%	27,81	7,29	0,0057	376,29	649,56

Figure 34 : Tableau des moyennes de la solution DDT

Sur la figure 34, on observe que les délais sont faibles avec des taux de pénétration différents car la durée des transmissions radio est la cause principale du délai.

SODAD

La dissémination de SODAD s'effectue avec l'émission d'un paquet des 10 derniers messages reçus toutes les secondes.

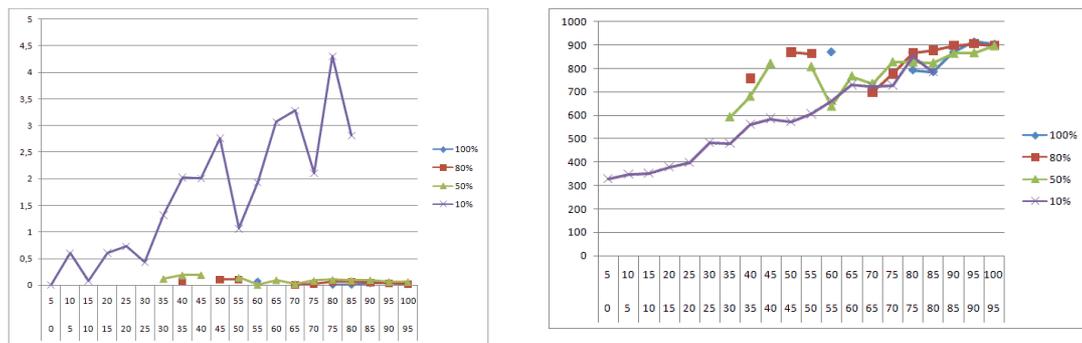


Figure 35 : SODAD et taux de pénétration en fonction du pourcentage de noeuds informés

Les délais sont assez faibles avec des taux de pénétration élevés mais le délai augmente à plusieurs secondes quand le réseau est très fragmenté (i.e. un taux de pénétration faible).

Pénétration	Noeuds informés (%)
100%	98.97
80%	98.39
50%	94.12
10%	36.51

Figure 36 : performance de SODAD en fonction du taux de pénétration

La figure 36 montre que SODAD permet un taux important de nœuds informés même avec un taux de pénétration de 50% en s'affranchissant des problèmes de fragmentation du réseau.

4. PROPOSITIONS POUR LA CREATION D'UN PROTOCOLE DE DIFFUSION

« DDT » est un mécanisme retenu dans beaucoup de solutions malheureusement il ne traite pas ces problèmes. D'abord, « DDT » ne prend pas en compte **l'asymétrie de la communication** dans les réseaux ad hoc sans fils. Un nœud A peut communiquer avec le nœud B mais à l'inverse, il arrive que le nœud B ne puisse pas atteindre le nœud A à cause d'interférences. De plus, « DDT » permet de choisir le nœud le plus éloigné mais à cause la distance c'est aussi le nœud avec lequel la communication est la **moins fiable** et la plus facilement rompue. Enfin, elle suppose que chaque véhicule dispose d'un **moyen de géo-localisation**. Nous proposons d'utiliser la qualité du signal du message reçu pour calculer le délai d'attente afin de s'affranchir de certains problèmes de « DDT ».

Pour les mécanismes proactifs, nous proposons d'utiliser les informations de **vitesse du nœud** et de **densité** pour calculer la période d'émission de message « Hello ». Plus un nœud se déplace rapidement, plus sa période d'émission est diminuée. Cela permet d'établir plus rapidement une connexion pour les nœuds rapides. De même, plus la densité des nœuds (nombre de messages « Hello » reçus) est importante, plus la fréquence d'émission est faible. Cela évite la congestion dans des cas de haute densité de véhicules (ex : bouchons, parking).

La fragmentation du réseau est un phénomène très répandu dans les réseaux de véhicules. Ainsi, toute solution devra présentée un mécanisme permettant la gestion de ce partitionnement tel que le « store and forward » ou l'utilisation d'infrastructure.

CONCLUSION

Ce stage m'a permis de mieux connaître le monde de la recherche et j'ai pu y découvrir une équipe motivée avec laquelle j'ai beaucoup apprécié travailler. Ce projet de recherche mêle à la fois la recherche et l'ingénierie avec la perspective d'applications pour l'opérateur de télécommunication ce qui m'a permis de montrer mes capacités en tant qu'ingénieur mais aussi en tant que chercheur.

Le domaine des réseaux de véhicules a un énorme potentiel de développement et permettra une avancée technologique importante dans les transports. Ce futur réseau et ce stage me donne envie de continuer dans ce domaine pour y apporter ma contribution.



BIBLIOGRAPHIE

- [AWK] AWK Programming Language <http://www.gnu.org/>
- [COINCHON] Calcul de liens par M. Coinchon http://www.swisswireless.org/wlan_calc_fr.html
- [FON] Communauté FON <http://www.fon.com/>
- [GLOMO] GloMoSim Simulator <http://pcl.cs.ucla.edu/projects/glomosim/>
- [IPERF] IPERF Traffic generator, <http://dast.nlanr.net/Projects/Iperf/>
- [MAD] Multi-band Atheros driver for wifi (madwifi), <http://madwifi.org/>
- [MADMOD] Madwifi modifié par A. Vyas de l'université de Stanford.
- [PLOT] GNU Plot <http://www.gnuplot.info/>
- [TCLTK] TCL/TK <http://www.tcl.tk/>
- [TOURR] Wireless for linux. http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/
- [VLC] VideoLanClient, <http://www.videolan.org/vlc/>
- [VMSIM] VanetMobiSim <http://vanet.eurecom.fr/>
- [BEN04] Benslimane, A.: Optimized Dissemination of Alarm Messages in Vehicular Ad-hoc Networks (VANET). In Proceedings of the 7th IEEE International Conference, Toulouse, France, June 2004.
- [BRI00] L. Briesemeister, L. Schäfers and G. Hommel: Disseminating Messages among Highly Mobile Hosts based on Inter-Vehicle Communication. In Proceedings of the IEEE Intelligent Vehicles Symposium 2000, pages 522–527, Piscataway, NJ, USA, October 2000.
- [BUCC05] P. Buccioli, E. Masala, N. Kawaguchi, K. Takeda, J.C. De Martin, "Performance Evaluation of H.264 Video Streaming over Inter-Vehicular 802.11 Ad Hoc Networks", Proc. of 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Berlin, Germany, Sep. 2005.
- [DDT] M.-T. Sun and al. Gps-based message broadcast for adaptive intervehicle communications. VTC Fall 2000.
- [DPP] Little, T.D.C. and A. Agarwal: An Information Propagation Scheme for VANETs. MCL Technical Report 07-01-2005, Department of Electrical and Computer Engineering, Boston University, Boston, USA, July 2005.
- [GASS06] R. Gass, J. Scott, and C. Diot. Measurements of In-Motion 802.11 Networking. In Proc. WMCSA, Apr. 2006.
- [HOM00] L. Briesemeister, G. Hommel, « Role-based multicast in highly mobile but sparsely connected ad hoc networks », Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, Boston, Massachusetts, 2000.
- [HUI01] Fay Hui, "Experimental Characterization of Communications in Vehicular Ad Hoc Networks", Thesis Master of Science in Computer Science, University of California Davis, 2001.



[HULL06] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, S. Madden: A measurement study of vehicular internet access using in situ Wi-Fi networks. MOBICOM 2006: 50-61.

[JOH96] D.B. Johnson and D.A. Maltz. « Dynamic source routing in ad hoc wireless networks ». Mobile Computing, Tomasz Imielinski and Hank Korth editors, Kluwer Academic Publishers, vol 353, p. 153-181, 1996.

[KOR04] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner , « Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems », Proceedings of First ACM Workshop on Vehicular Ad Hoc Networks (VANET 2004), p. 76-85, Philadelphia, PA, USA, Octobre 2004.

[MOV07] Patrick Marlier, Moez Jerbi, and Sidi Mohammed Senouci, " Experimental Assessment of V2V and I2V Communications " International Workshop on Mobile Vehicular Networks (MoVeNet 2007) October 12, 2007, Pisa, Italy

[OAPB] Alshaer, H. and E. Horlait: An Optimized Adaptive Broadcast Scheme for Inter-vehicle Communication. In Proceedings of the IEEE Vehicular Technology Conference (IEEE VTC2005-Spring), pages 2840– 2844, Stockholm, Sweden, May 2005.

[OTT04] J. Ott and D. Kutscher. Drive-thru internet: IEEE 802.11b for automobile users. In IEEE INFOCOM, 2004.

[SING02] J.P. Singh, N. Bambos, B. Srinivasan, and D. Clawin. Wireless lan performance under varied stress conditions in vehicular traffic scenarios. In Proceedings. IEEE 56th Vehicular Technology Conference, Fall 2002, volume 2, pages 743– 747. IEEE, 2002.

[STEID] J. Nzoonta and C. Borcea, STEID: A protocol for emergency information dissemination in vehicular networks, Draft, 2006.

[TSE02] Y.C. Tseng, S.Y. Ni, Y.S. Chen, and J.P. Sheu. « The broadcast storm problem in a mobile ad hoc network », Wireless Networks, 8(2/3), p. 153-67, 2002.

[VTC07] Moez Jerbi, Sidi-Mohammed Senouci, and Mahmoud Al Haj, "Extensive Experimental Characterization of Communications in Vehicular Ad Hoc Networks within Different Environments", IEEE 65th Vehicular Technology Conference VTC2007-Spring.

[WIS05] Wischhof, L., A. Ebner and H. Rohling: Information Dissemination in Self-organizing Intervehicle Networks. IEEE Transactions on Intelligent Transportation Systems, 6(1):90–101, March 2005.

[WUH04] Hao Wu, Richard Fujimoto, Randall Guensler and Michael Hunter: MDDV: A Mobility-centric Data Dissemination Algorithm for Vehicular Networks. In Proceedings of the Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET '04), pages 47–56, New York, NY, USA, 2004. ACM Press.

ANNEXES

A. PRINCIPAUX SIGLES

ACK	Trame d'acquittement	LAN	Réseau local (Local Area Network)
AP	Point d'accès (Access Point)	LLC	Logical Link Control
BSS	Basic Service Set	MAC	Medium Access Control
C2C	Voiture à voiture (Car to Car)	OFDM	Orthogonal Frequency Division Multiplexing
CRC	Cyclic Redundancy Code	OSI	Open System Interconnection
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	PCF	Point Coordination Function
CTS	Clear To Send	PHY	Physical
DCF	Distributed Coordination Function	PIFS	PCF IFS
DIFS	DCF IFS	QoS	Qualité de service (Quality of Service)
DS	Distribution System	RTS	Ready To Send
DSSS	Direct Sequence Spread Spectrum	RVC	Communication véhicule à infrastructure (Roadside-to-Vehicle Communication)
EIFS	Extended IFS	SIFS	Short IFS
FCS	Frame Check Sequence	V2I	Communication véhicule à infrastructure (Vehicle to infrastructure)
FHSS	Frequency Hopping Spread Spectrum	V2V	Véhicule à Véhicule (Vehicle to vehicle)
I2V	Communication infrastructure à véhicule (Infrastructure to vehicle)	WEP	Wired Equivalent Privacy
IBSS	Independant Basic Service Set	WiFi	Wireless Fidelity
IEEE	Institute of Electrical and Electronics Engineers	WLAN	Wireless local Area Network
IFS	Inter Frame Space	WMAN	Wireless Metropolitan Area Network
IVC	Communication intervéhicule (Inter-Vehicle Communication)	WPAN	Wireless Personal Area Network

B. LES RESEAUX AD HOC MULTI-SAUTS

Les réseaux ad hoc sont souvent appelé MANET (Mobile Ad-hoc NETWORK). Voici quelques propriétés des réseaux ad hoc.

Un réseau ad hoc est un ensemble de terminaux mobiles indépendants de toute infrastructure, communiquant par onde radio (cf. Figure B.1). Les terminaux offre un service de relais qui permet d'accepter un message qui ne lui est pas destiné afin de le réémettre vers un autre terminal du réseau qui est hors de portée de l'émetteur initial de ce message.



Figure B.1 : réseau ad-hoc minimal

Les pairs doivent alors s'auto organiser en réseau pour permettre une communication de bout en bout de manière efficace. Comme il n'y a aucune infrastructure particulière dans ces réseaux, cela implique que toute station doit être en mesure de relayer tout paquet et donc que toute station est un routeur potentiel. On parle alors de communications multi-saut, car une communication entre deux stations non à portée de communication se réalise sur plusieurs sauts radios. La mobilité des terminaux et la versatilité des communications radio rendent la topologie du réseau extrêmement variable et dynamique.

On retrouve derrière le réseau ad hoc, l'idée originale du projet PRnet de la DARPA, où le concept est d'interdire l'emploi d'une infrastructure de communication fixe pré existante. En 1995, L'Internet Engineering Task Force (IETF) crée le groupe Mobile Ad Hoc Networks (MANET) pour étudier les réseaux ad hoc dans le contexte Internet. Aujourd'hui le groupe MANET est toujours actif et développe des solutions de routage pair à pair pour des nœuds mobiles communicant en sans fils.

Les réseaux radio multi-saut sont très flexibles et simples d'utilisation, ils ne nécessitent aucun câblage et aucune installation humaine, ainsi ils ne représentent qu'un coût très faible. Les recherches principales ont portée sur les problématiques de routage, mais depuis quelques années le spectre des recherches s'est élargi allant à la mise en place de protocoles MAC adaptés à la découverte de services en passant par la gestion de l'énergie, la mise en place de qualité de service ou la sécurisation de ces réseaux.

Quelques caractéristiques des réseaux ad hoc :

- Liens asymétriques

En théorie, les liens sont symétriques, et l'affaiblissement est inversement proportionnel à la distance entre l'émetteur et le récepteur. En pratique, les liens sont asymétriques à cause de déphasages dû aux multiples réflexions du signal sur différents obstacles, de l'évanouissement (fading). On peut ainsi obtenir une bonne réception dans un sens, une mauvaise dans l'autre. La route inverse n'est pas forcément la même que la route directe. Pour le maintien des liens, il faut une mise en place d'une signalisation beaucoup plus importante que celle des réseaux fixes.

- Interférences

L'interface radio est partagée de tous les pairs, chaque donnée est réceptionnée par tous les nœuds, à des puissances variables. Les interférences s'ajoutent au bruit et détériorent les communications, en augmentant le taux d'erreur. La transmission des paquets non récupérables diminue le débit de la liaison.

- Redondance

La diffusion à tous les voisins engendre une certaine redondance car en général la destination est un voisin en particulier.

- Mobilité des nœuds

La topologie du réseau est dynamique et les routes sont modifiées assez fréquemment. Un routage dynamique est alors nécessaire mais il demande d'énormes ressources pour véhiculer la signalisation indispensable aux mouvements des nœuds. Jusqu'à présent, la plupart des routages ad-hoc se sont montrés plutôt inaptes à faire face à une forte mobilité. C'est une des problématiques au cœur des travaux de recherche. La modification de la topologie du réseau transforme le tracé des routes lors des échanges de paquets.

- Routage

Ainsi pour permettre une communication de bout en bout avec plusieurs sauts (cf. Figure B.2), il est nécessaire d'utiliser un protocole de routage dynamique adapté à ce type de réseau. Deux approches sont alors possibles, l'approche proactive et l'approche réactive. La première approche consiste à maintenir des connexions en permanence entre les nœuds, c'est ce que fait le protocole OLSR. A l'inverse, l'approche réactive recherche un chemin seulement à la demande, par exemple AODV. On trouve aussi des routages de type hiérarchique et de type géographique, en particulier dans les réseaux de véhicules.

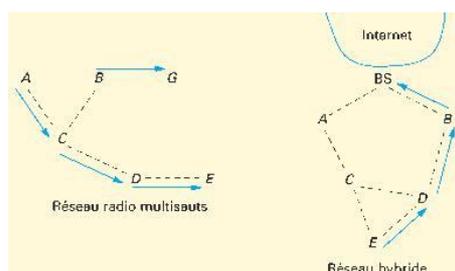


Figure B.2 : réseau ad-hoc multi-sauts

C. PROBLEMATIQUE DES RESEAUX SANS FILS 802.11

Lors de ce stage, une étude de la norme IEEE 802.11 était nécessaire pour comprendre les problèmes engendrés par cette norme. Etant très répandue, cette norme ne manque pas de documentation sur Internet. Nous allons balayer largement la norme pour maîtriser au maximum les tests.

D'abord, nous justifions notre choix pour la norme 802.11. Ensuite nous donnerons des détails de la couche Physique et de la couche Liaison comme illustré dans le schéma C.1.

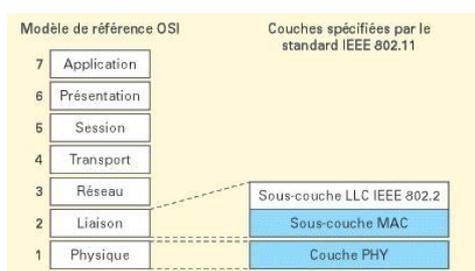


Figure C.1 : Modèle OSI et couches de la norme 802.11

LE CHOIX DE LA NORME IEEE 802.11

Cette technologie est omniprésente dans les foyers, aéroport, et dans les villes grâce aux hotspots. Elle est même intégrée à tous les ordinateurs portables et consoles de jeux d'aujourd'hui et commence à être ajoutée dans les téléphones portables. Cette popularité a fait chuter le prix des puces. En 2007, la puce wifi Marvell équipant l'iPhone coûte environ \$6¹.

Le choix du wifi s'est imposé par son coût, sa facilité d'utilisation, et aussi par sa capacité de portée du signal.

Un autre atout du standard 802.11 est de faire partie d'un ensemble cohérent de standard de communication sans fil destiné à couvrir l'ensemble des besoins. En effet, l'IEEE développe un standard pour l'interconnexion sans fil de système distant de 2 à 50 km connu sous l'appellation WMAN (Wireless Metropolitan Area Network). C'est le futur standard IEEE 802.16.

COUCHE PHYSIQUE

- **Accès et gestion du médium radio**

La norme utilise le mode CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pour l'accès au médium. Son principe de fonctionnement est d'écouter le canal (détection de porteuse) pour savoir s'il est occupé ou non et d'utiliser des temps d'attente au canal aléatoire dans un intervalle de temps appelé fenêtre de contention (Contention Window) pour essayer de départager les nœuds et autoriser un unique nœud à émettre. Le problème est qu'un matériel qui n'agit pas correctement, peut émettre en permanence en ne respectant pas les temps d'attente aléatoire (backoff).

Cette méthode nécessite également l'emploi de « trou », d'une durée minimale spécifiée entre les transmissions contiguës. Ce trou est appelé IFS (Inter Frame Space) ou espace inter trame. La figure C.2 illustre l'usage de l'IFS. Le slot time est l'unité de temps qui est fixé par la norme. Il correspond à l'intervalle minimal entre deux opérations de détection de porteuse.

¹ Source : Enquête iSuppli

La norme 802.11 prévoit deux modes de gestion du médium. Un mode distribué appelé DCF (Distributed Coordination Function) et un mode centralisé, le PCF (Point Coordination Function). Le PCF ne peut fonctionner uniquement en mode infrastructure, c'est-à-dire qu'un nœud joue le rôle d'orchestrateur, en donnant des accès alternativement aux autres nœuds. L'utilisation du PCF est optionnelle et donc peu ou pas implémentée dans les matériels 802.11. Le DCF est donc utilisé mais alors se pose le problème d'équité² d'utilisation du médium par l'ensemble des nœuds.

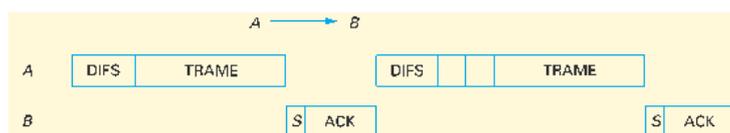


Figure C.2 : Une communication simple avec DCF

- **Codage de l'information**

Le codage de l'information en 802.11 peut se faire de plusieurs façons. En 802.11 de base, le codage utilise le DSSS (Direct Sequence Spread Spectrum). Le 802.11b utilise aussi le DSSS mais accompagné de CCK (Complementary code keying) comme méthode de modulation. Cela permet d'obtenir de meilleures performances passant de 1-2Mbits à 11Mbits. Le 802.11g et 802.11a utilisent eux le codage OFDM qui permet d'atteindre un débit théorique de 54Mbits.

- **Puissance du signal**

La portée du signal dépend de la fréquence d'utilisation et de la puissance d'émission. Cependant, ces paramètres sont légalisés et limités par les autorités de chaque pays. En France, c'est l'ARCEP (Autorité de régulation des communications électroniques et des postes) qui régule l'utilisation des fréquences. Sur la figure C.3, on peut voir les puissances autorisées pour les différentes normes 802.11.

	Intérieur	Extérieur
Bande 2400-2454 MHz 802.11b/g	100 mW	100 mW
Bande 2483,5 MHz 802.11b canal 14	100 mW	10 mW
Bande 5150-5350 MHz 802.11a	200 mW	Interdit
Bande 5470-5725 MHz 802.11h	1 W avec une régulation de la puissance de l'émetteur ou 500 mW sans	

Figure C.3 : Tableau des puissances autorisées en France (source ARCEP)

Le 802.11b et le 802.11g peuvent être utilisés en intérieur et en extérieur. A l'inverse, le 802.11a qui exploite la bande de fréquences de 5,15 à 5,35 GHz, est à utiliser exclusivement à l'intérieur des bâtiments. Par contre, les technologies (comme le 802.11h) exploitant la bande de fréquences 5,47 à 5,725 GHz peuvent être utilisées à l'extérieur comme à l'intérieur.

Pour utiliser les valeurs données dans la figure C.3, il est nécessaire de calculer la puissance isotrope rayonnée équivalente (PIRE ou EIRP, Equivalent isotropically radiated power). La PIRE est le gain dans la direction de l'antenne où la puissance émise est maximale par rapport à celle émise par

² Y. Khaled, B. Ducourthial, M. Shawky « Généralisation du problème de l'équité des trois paires dans la norme IEEE 802.11 »



une antenne isotrope (émettant parfaitement dans toutes les directions). Nous obtenons ainsi la formule suivante :

$$\text{PIRE(dBm)} = (\text{Puissance de transmission (dBm)}) - (\text{Pertes dans les câbles et connecteurs (dB)}) + (\text{Gain de l'antenne(dBi)})$$

Le passage de Watt et dB est effectué ainsi :

$$\text{dB} = 10 \log(W) ; \text{dBm} = 10 \log(\text{mW})$$

Le passage de dB en dBm s'effectue simplement en ajoutant 30. (0 dB = 10 log 1000 = 30 dBm)

La sensibilité des récepteurs est aussi un paramètre lié à la puissance d'émission. La valeur par défaut est de -80dBm. En dessous de ce niveau, la carte wifi n'essayera pas de décoder la trame la jugeant trop faible. Il est cependant possible de modifier ce paramètre pour des cas exceptionnels.

- **Les interférences**

Les ondes radio subissent différents phénomènes comme par exemple l'atténuation (fading) et les multi-chemins (multipath), qui rendent la portée de transmission radio limitée. La ligne de vue (Line of sight ou LOS) est un facteur important pour la qualité du signal.

Le phénomène du « **multipath** » se produit quand le récepteur reçoit cette trame en plusieurs exemplaires suivant les différents chemins possibles empruntés par la trame. La trame d'origine et les échos produits se superposent et rendent ainsi le décodage plus difficile.

Contre le phénomène de « **fading** », on utilise une technique appelée « diversité ». Ce processus consiste à recueillir plusieurs transmissions du même message. Plusieurs types de diversités existent dont la plus utilisée est la diversité spatiale (ou diversité d'antenne). Le récepteur dispose de plusieurs antennes (minimum deux). Pour information, la longueur entre les antennes doit être un multiple de la demi-longueur d'onde de la fréquence de la porteuse. A la réception d'une trame il peut choisir la meilleure réception reçue par ses antennes, il peut aussi additionner ou combiner les signaux, ce qui améliore très sensiblement le résultat. La diversité en fréquence, consiste à envoyer une trame sous différentes fréquences et de choisir la meilleure. Ceci nécessite d'avoir un spectre de fréquence assez large.

Dans le cas de nœuds mobiles, l'effet **Doppler-Fizeau** est une interférence importante. Ce phénomène est le décalage entre la fréquence de l'onde émise et de l'onde reçue lorsque l'émetteur et le récepteur sont en mouvement l'un par rapport à l'autre ; il apparaît aussi lorsque l'onde se réfléchit sur un objet en mouvement par rapport à l'émetteur ou au récepteur.

Les objets environnants (micro ondes, émetteur TV, ...) peuvent être aussi générateurs d'ondes parasites pour le signal.

Dans le cas des réseaux véhiculaires, un autre phénomène important est la **réflexion** des ondes sur le sol (two ray ground). Il est aussi générateur d'interférence dans la communication (cf. Figure C.4).



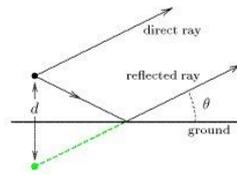


Figure C.4 : Réflexion des ondes sur le sol

Par ailleurs, le débit de transmission a aussi un impact sur la portée de communication. En effet, plus le débit est rapide, plus les techniques de codage et de modulation sont rapides et complexes (cf. Figure C.5), et meilleure doit être la qualité du signal pour pouvoir le comprendre. Par exemple, un signal trop altéré ne pourra être décodé à 11 Mb/s alors qu'il pourra éventuellement l'être à 2 Mb/s.

Technologie	Codage	Type de modulation	Débit
802.11b	11 bits (Barker sequence)	PSK	1Mbps
802.11b	11 bits (Barker sequence)	QPSK	2Mbps
802.11b	CCK (4 bits)	QPSK	5.5Mbps
802.11b	CCK (8 bits)	QPSK	11Mbps
802.11a	CCK (8 bits)	OFDM	54Mbps
802.11g	CCK (8 bits)	OFDM	54Mbps

Figure C.5 : Tableau des différents codages dans la norme 802.11

- **La zone grise**

Le phénomène de la zone grise a été découvert lors des expérimentations des protocoles de routage ad-hoc (Henrik Lundgren, Erik Nordström, Christian Tschudin "Coping with Communication Gray Zones in IEEE 802.11b based Ad hoc Networks").

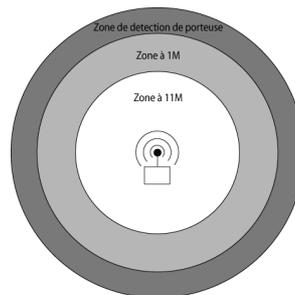


Figure C.6 : Portée du signal 802.11

La modulation et le codage étant différent pour le débit 1Mbps et 11Mbps, la distance atteinte par ces deux méthodes est différente comme on peut le voir dans le schéma C.6. De plus, la liaison peut être asymétrique. Ainsi, les protocoles de routage ne fonctionnent pas correctement croyant qu'un nœud joignable alors qu'il est hors de portée.

- **Les antennes**

Il existe différents types d'antenne avec des schémas d'irradiations différentes. La puissance d'une antenne est mesurée en dBi qui est la mesure du gain par rapport à une antenne de référence, l'antenne isotrope.

L'antenne omnidirectionnelle diffuse à 360° autour d'elle comme on peut le voir sur la figure C.7. Plus le gain d'une antenne omnidirectionnelle est important, plus la hauteur de diffusion diminue.



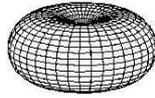


Figure C.7 : Irradiation d'une antenne omni directionnelle

L'antenne directionnelle permet des gains plus importants cependant l'inconvénient est de devoir être pointé en direction des autres antennes comme on peut le voir sur la figure C.8.

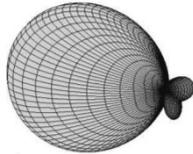


Figure C.8 : Irradiation d'une antenne directionnelle, Yagi

Les « Smart Antenna » (MIMO) sont entrain d'apparaître sur le marché et permettent une meilleure réception en utilisant un ensemble de plusieurs antennes.

- **Les canaux**

Dans la norme 802.11b et g, il y a un chevauchement des canaux comme on peut le voir sur la figure C.9. Malgré les 13 canaux disponibles, en réalité seulement 3 sont utilisables simultanément.

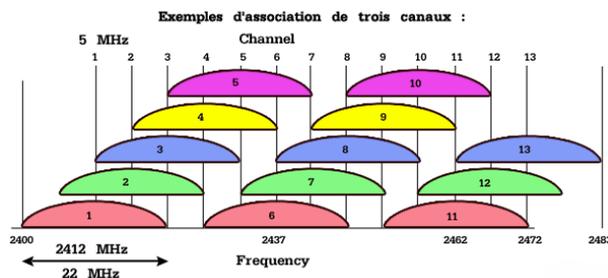


Figure C.9 : Chevauchement des canaux 802.11b/g

A la différence de cela, la norme 802.11a dispose de canaux qui ne se chevauchent pas et chacun peuvent donc être utilisés simultanément.

- **Capacité du canal**

La capacité maximale théorique du canal est de 11Mbps pour le 802.11b et de 54Mbps pour le 802.11g. Cependant, le débit effectif est toujours en dessous de cette capacité à cause entre autre des délais aléatoires (backoff), des délais d'acquittements, et des erreurs de transmission.

La durée d'attente de la réception de l'acquittement d'une trame est fixée dans la norme et elle permet par défaut des distances jusqu'à 4 km. Au delà de ce délai, le nœud émetteur pense la trame perdue et peut donc la réémettre. Plus ce délai est important, plus les performances du réseau vont alors diminuer. Dans le pilote Madwifi, il est possible de modifier ce délai grâce à l'utilitaire athctrl.

Lors d'une transmission radio, les conditions peuvent changer par une dégradation du signal causée par des interférences ou un éloignement de la station car la notion de débit est toujours liée à la notion de distance. Afin de faire accéder toutes les stations au réseau, la norme Wi-Fi utilise une fonction appelée **Variable Rate Shifting**. Cette fonction fait varier le débit de la station en fonction de la qualité du signal radio, généralement il existe quatre niveaux de débit : 11Mbit/s, 5.5Mbit/s,



2Mbit/s et 1Mbit/s (ces valeurs seuils ne sont pas standardisées et peuvent être différentes suivant les constructeurs). Il existe plusieurs algorithmes, tel que le ONOE, le SAMPLE, le AMRR qui sont disponibles dans le pilote Madwifi.

La présence dans une cellule d'un nœud lent (1Mbps) engendre un ralentissement de l'ensemble des performances de la cellule. En effet, les paquets « lents » ont la même chance d'accéder au canal que les paquets « rapides », ce qui donne une alternance en moyenne des paquets « lents » et des paquets « rapides ». Or les paquets « lents » vont occuper le médium pendant un temps beaucoup plus long que les paquets « rapides », ce qui va entraîner une chute de débit des flux « rapides ». Exemple : Des flux de 11 Mb/s peuvent obtenir des débits seulement très légèrement supérieurs à 1 Mb/s lorsqu'ils se retrouvent en compétition dans l'accès au médium avec des flux à 1 Mb/s.

Le MIMO (Multiple-Input Multiple-Output, futur norme 802.11n) permet l'utilisation de plusieurs antennes sur l'émetteur et le récepteur et l'utilisation de plusieurs canaux afin d'obtenir de meilleures performances. On arrive ainsi à plus de 200Mbps théorique avec des solutions propriétaires.

- **Les différentes normes A/B/G/P**

Les normes 802.11b et g sont compatibles dans le fait où elles fonctionnent sur les mêmes fréquences et que les équipements 802.11g peuvent aussi fonctionner en 802.11b. Ce phénomène de compatibilité était très important pour permettre le passage progressif d'une norme à l'autre. La norme 802.11a ne fonctionnant pas sur la même gamme de fréquence est incompatible avec le matériel 802.11b/g.

La norme IEEE 802.11p est dédiée aux réseaux de véhicule et elle est toujours en discussion entre les différents acteurs. La version définitive est prévue de paraître en avril 2009. Le DSRC est l'équivalent de cette norme aux Etats-Unis et ils ont de nombreux points communs (utilisation des fréquences 5.9 Ghz avec une modulation OFDM).

COUCHE LIAISON (MEDIUM ACCESS CONTROL + LOGICAL LINK CONTROL)

- **La trame MAC**

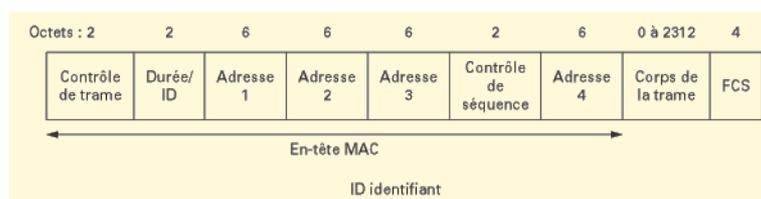


Figure C.10 : Format général de la trame MAC 802.11

La figure C.10 donne le schéma général de la trame MAC. Le champ « contrôle de trame » contient des données telles que le protocole utilisé et le type de trame transmise.

La couche MAC du protocole 802.11 offre un mécanisme de contrôle et de correction d'erreur permettant de vérifier l'intégrité des trames grâce au champ FCS. Il s'agit là d'une différence fondamentale avec le standard Ethernet. En effet Ethernet propose un système de détection d'erreurs (CRC), mais ne propose pas de correction d'erreurs, cette tâche étant laissée aux protocoles de transports de niveau supérieur (TCP). Dans un réseau sans fil le taux d'erreur est plus élevé, c'est la raison pour laquelle un contrôle d'erreur a été intégré au niveau de la couche liaison de données.

Le corps de la trame contient les données utilisateurs qui peuvent contenir jusqu'à 2312 octets. Le champ « durée/ID » contient la durée calculée pour la transmission de la trame. Cette valeur est dépendante du débit de la couche physique. Les champs « adresse » contiennent les adresses source



et destination de la trame. En plus de ces adresses, suivant le mode de fonctionnement, il contient l'adresse de la cellule ou bien des différentes adresses des relais. Le champ « contrôle de séquence » stocke le numéro de séquence et le cas échéant le numéro de fragment (si les données ont été fragmentées en plusieurs trames).

- **Les trames de gestion**

La trame d'acquiescement ACK (ACKnowledgement) est essentielle. Elle permet à l'émetteur d'une trame de s'assurer de sa bonne réception. Si elle n'est pas reçue à temps, une rémission est alors effectuée.

Les trames d'association et d'authentification permettent l'entrée d'une station au sein du réseau.

L'authentification a pour but de vérifier si la station demandant son association est autorisée sur le réseau. Ce mécanisme n'est pas nécessaire dans les réseaux fixes car il est possible d'empêcher l'accès physique à un réseau, chose qui n'est pas réalisable avec un réseau sans fil. L'authentification est basée sur l'usage d'une clef secrète partagée. Dans un réseau basé sur une infrastructure, le point d'accès envoie une question sous forme de message. Seul un possesseur de la clef secrète est capable de calculer la réponse correcte à cette question. Après vérification de la réponse par le point d'accès, la station est authentifiée auprès du réseau et peut commencer à émettre en respectant les règles établies par la couche MAC pour l'accès au médium. Ce mécanisme est d'usage optionnel. Par défaut, il n'existe pas de mécanisme d'authentification.

L'association a pour but d'enregistrer la station auprès du point d'accès. Le point d'accès attribue une adresse à la station mobile qui lui permettra d'être identifiée sur le réseau.

La trame balise (Beacon frame) est très importante car elle permet la détection du réseau et la synchronisation du réseau. La précision des transmissions et du respect des temporisateurs est une donnée essentielle dans une architecture distribuée. Dans un réseau sans fil, chaque station possède une horloge interne qui lui permet de déclencher ses processus (émission, réception). Cette horloge aussi précise soit-elle reste soumise à une dérive. Pour limiter les effets des dérives d'horloge, il est nécessaire de synchroniser l'ensemble des participants du réseau de manière périodique. Cette fonction est assurée par l'envoi cette trame particulière appelée trame balise (beacon) contenant un temps de référence. Dans une architecture basée sur une infrastructure, cette fonction est assurée par le point d'accès responsable de la cellule. Pour l'architecture ad hoc, la fonction de synchronisation doit être assurée par un mécanisme distribué.

- Le problème de la station cachée et le RTS/CTS

Comme illustré dans le schéma C.11, le problème de la station cachée se produit quand deux nœuds A et C hors de portée essayent de communiquer avec un troisième B. Au niveau du nœud B se produit alors une collision qui n'est détectée ni par A ni par C.



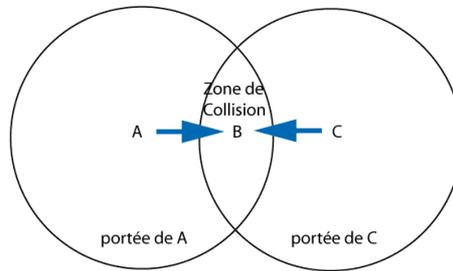


Figure C.11 : Schéma du problème de la station caché

Le mécanisme utilise des trames d'annonce RTS (Ready To Send) et CTS (Clear To Send) qui précèdent la transmission. Lorsqu'une station souhaite transmettre des trames, elle commence par envoyer une trame RTS et attend en réponse une trame CTS avant de commencer à transmettre. La station réceptrice d'une trame RTS envoie si les conditions de transmission sont réunies sa trame CTS. Ces deux trames contiennent la durée prévue pour l'échange qui va suivre.

Grâce à l'envoi de la trame RTS, toutes les stations situées dans la couverture radio de la source sont informées d'une transmission imminente et de sa durée éventuelle. Le CTS a le même rôle d'annonce mais cette fois autour du récepteur. Ces deux trames sont courtes (20 octets pour RTS et 14 octets pour CTS) et rencontrent donc une faible probabilité de collisions.

Ce mécanisme demeure inopérant pour la transmission de trames diffusées à tous les membres dites trames broadcast. En effet, le destinataire n'étant pas unique, on ne peut avoir de réponse en retour (CTS) et par conséquent des collisions sur les trames diffusées sont toujours possibles.

L'en-tête (PLCP) est toujours transmis en utilisant la modulation de base (à 1Mbps). Cela garantit à la transmission une plus grande robustesse et permet à toutes les stations, y compris celles qui ne supportent pas de mode évolué, de pouvoir comprendre les transmissions. La portée en est accrue évitant certains problèmes de stations cachées.

LES ARCHITECTURES RESEAUX

- Le mode adhoc (independant basic service set, abrégé en IBSS)

Un réseau ad hoc ne nécessite aucune infrastructure préalablement déployée pour permettre la communication entre ses membres. Chaque station opère de manière autonome afin d'assurer sa connectivité et celle avec les autres membres. La souplesse de déploiement est un atout majeur de ce type de réseau. Cette architecture est parfaitement adaptée à des besoins de communications éphémères ou sur des scènes mouvantes nécessitant un déploiement rapide et la prise en compte de la mobilité des stations. Les opérations militaires sur le terrain sont un exemple où l'architecture ad hoc montre tout son intérêt.

- Le mode infrastructure

Cette architecture est la plus utilisée. Elle est particulièrement adaptée pour assurer la connectivité dans des lieux clos tels que les halls d'aéroport et les hôpitaux. Elle repose sur un réseau dorsal sur lequel sont connectés des points d'accès.

Contrairement au réseau ad hoc où chaque station doit être capable d'effectuer toutes les opérations, ici les rôles ne sont pas identiques. Les points d'accès (AP ou Access Point) sont responsables des services d'authentification et d'association. Le système de distribution DS (Distribution System) permet d'accroître le champ d'action au-delà de la couverture radio. De même, un répéteur peut être mise en place pour augmenter la portée du signal. Cette architecture permet



aussi d'offrir aux usagers mobiles l'accès à d'autres ressources (serveurs de fichier, imprimante, etc.) ou d'autres réseaux (Internet).

- Gestion de la mobilité (Roaming)

Contrairement aux réseaux mobiles téléphoniques, il n'existe pas de gestion de changement de cellules (handover ou handoff) pour des appareils Wi-Fi en cours de transmission. Si une station se déplace elle cherchera le meilleur point d'accès pour s'associer avec lui, mais toute communication sera interrompue et non reprise par le nouveau point d'accès. Certains constructeurs, tel Lucent, ont palié à ce problème en développant un protocole propriétaire appelé IAPP (Inter-Access Point Protocol) apportant la mobilité au wifi.

Le 802.11 gère aussi la qualité de service (QoS) avec la norme 802.11e, le multimédia avec l'extension Wi-Fi Multimédia (WMM) et la sécurité avec la norme 802.1x. Elle est devenue une technologie mature qui peut être déployé dans un milieu professionnel.

