



HAL
open science

Quality of service support and topology control in mobile ad hoc networks

Rabah Meraihi

► **To cite this version:**

Rabah Meraihi. Quality of service support and topology control in mobile ad hoc networks. domain_other. Télécom ParisTech, 2005. English. NNT: . pastel-00001166

HAL Id: pastel-00001166

<https://pastel.hal.science/pastel-00001166>

Submitted on 10 May 2005

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Thèse

présentée pour obtenir le grade de docteur

de l'Ecole nationale supérieure
des télécommunications

Spécialité : Informatique et Réseaux

Rabah MERAIHI

Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc

Guy Pujolle	Rapporteurs
Stéphane Ubéda	
Christian Bonnet	Examineurs
Andrzej Duda	
Philippe Jacquet	
Michel Riguidel	Directeurs de thèse
Samir Tohmé	
Gwendal Le Grand	Co-encadrant

Ecole nationale supérieure des télécommunications

Résumé

Avec le déploiement de la technologie WiFi ces dernières années, les réseaux locaux sans fil connaissent un grand succès auprès des institutions et les réseaux ad hoc suscitent un réel intérêt auprès de la communauté de R&D.

Parallèlement, avec l'émergence des services multimédias dans les réseaux mobiles, des travaux pour l'introduction de la qualité de service dans les réseaux ad hoc ont été proposés. Les études existantes sont souvent basées sur des hypothèses limitées et inadaptées aux propriétés des réseaux ad hoc.

Dans cette thèse, nous proposons d'abord un protocole de routage avec différenciation de terminaux qui maximise les liens sans fil de haute qualité. Le but d'une telle approche est de prendre en compte l'hétérogénéité des nœuds dans les réseaux ad hoc et de supporter les situations où des terminaux mobiles peuvent accepter ou refuser la fonction de routage. Notre proposition apporte une solution aux variations des capacités des liens sans fil en routant les paquets de préférence à travers les routeurs collaboratifs ayant une grande capacité de transmission dans le but de maintenir une meilleure qualité de lien (grand débit) des routes dans le réseau.

Nous prouvons ensuite la nécessité d'une gestion multicouches de la qualité de service dans un tel environnement. Cela permet de définir une stratégie de QoS en plusieurs couches de communication dans le but de prendre en considération les contraintes liées aux spécificités des réseaux mobiles ad hoc. Une combinaison des mécanismes de qualité de service au niveau IP et MAC (IEEE 802.11) est étudiée. De plus le principe de routage avec différenciation de terminaux décrit ci-dessus a été combiné avec la gestion de la qualité de service IP et MAC.

Un autre volet de la thèse traite l'aspect de contrôle de topologie dans les réseaux ad hoc. Il consiste à contrôler la morphologie du réseau en utilisant la mobilité d'un ensemble de routeurs dédiés. Le principe est d'utiliser positivement la mobilité, qui est habituellement subie dans le réseau, afin d'améliorer les performances de ce dernier. Ainsi, des stratégies de déploiement des routeurs dédiés sont étudiées (dans un réseau ad hoc autonome ou interconnecté à une infrastructure) dans le but d'offrir une meilleure connectivité ou pour assurer un meilleur support de la qualité de service des applications temps réel. Pour les deux stratégies, le problème a été formulé comme un problème de programmation linéaire entière mixte.

Cette thèse a été réalisée dans le cadre du projet ITEA Ambience. Dans ce contexte, nous avons entre autres contribué à la réalisation d'une plate-forme, qui illustre un exemple d'applications des réseaux ad hoc où des mécanismes décrits dans les parties précédentes sont utilisés afin d'améliorer les performances du système et répondre aux besoins des utilisateurs mobiles, dans un contexte hétérogène sécurisé.

Mots-clés :

Qualité de service, IEEE 802.11, Différenciation de services, Hétérogénéité des nœuds, Routage ad hoc, Contrôle de topologie, Routeurs dédiés, Connectivité.

Table des matières

Résumé	i
Table des matières	ii
Table des figures	v
Liste des tableaux	viii
Liste des abréviations	ix
Introduction générale	1
1 QoS et contrôle de topologie dans les réseaux ad hoc	5
1.1 Réseaux ad hoc : Généralités	5
1.1.1 Introduction et historique	5
1.1.2 Propriétés et spécificités des réseaux ad hoc	7
1.1.3 Domaines d'application des réseaux ad hoc	8
1.1.4 Réseaux ad hoc et réseaux 4G	9
1.1.5 Topologie du réseau ad hoc et interconnexion avec une infrastructure	10
1.1.6 Le routage dans les réseaux ad hoc	15
1.1.7 La couche MAC 802.11 dans les réseaux ad hoc	18
1.2 Qualité de service dans les réseaux ad hoc	21
1.2.1 Introduction	21
1.2.2 Différenciation de service au niveau de la couche MAC	22
1.2.3 Protocole de routage avec qualité de service	24
1.2.4 Protocole de réservation de ressources : INSIGNIA	27
1.2.5 Modèle de qualité de service pour les réseaux ad hoc	28
1.2.6 Discussion	30
1.3 Contrôle de topologie dans les réseaux mobiles ad hoc mobiles	32
1.3.1 Introduction	32
1.3.2 Contrôle de topologie basé sur la puissance de transmission	33
1.3.3 Techniques de Clustering	34
1.3.4 Déploiement des réseaux de senseurs	38
1.4 Discussion et conclusion	39

2	Routage avec différenciation de terminaux	41
2.1	Introduction	41
2.2	Exposition des problèmes	42
2.3	Notre proposition	45
2.3.1	Principe	45
2.3.2	Extension du protocole DSR pour la différenciation de terminaux	46
2.3.3	La phase de découverte de routes	46
2.3.4	La phase de la sélection de la route	48
2.4	Simulations et analyse des performances	48
2.4.1	Modèle de simulation	50
2.4.2	Cas d'une topologie statique	51
2.4.3	Cas d'une topologie dynamique	53
2.5	Conclusion	54
3	Gestion multicouches de la Qualité de Service	57
3.1	Introduction	57
3.1.1	Le Modèle OSI et les contraintes liées aux réseaux mobiles sans fil	58
3.1.2	Approche intercouches (crosslayer)	59
3.1.3	La QoS suivant les différentes couches du modèle OSI	60
3.2	Notre proposition : Combinaison de la qualité de service IP et MAC	63
3.3	Simulations et analyse des résultats	64
3.4	Gestion multicouches et Routage avec différenciation de terminaux	71
3.4.1	Scénario de simulation étudié	72
3.4.2	Résultats	74
3.5	Conclusion	76
4	Contrôle de topologie orienté stratégie	79
4.1	Introduction	79
4.2	Modélisation	80
4.2.1	Contrôle de topologie orienté connectivité	80
4.2.2	Déploiement des routeurs mobiles orienté qualité de service	85
4.2.3	Cas d'un réseau ad hoc interconnecté à une infrastructure fixe	87
4.2.4	Fonctionnement général	87
4.3	Contrôle de topologie dans un environnement mobile	89
4.3.1	Extension du modèle dans un environnement ad hoc dynamique	90
4.4	Simulations et résultats	91
4.4.1	Connectivité	92
4.4.2	Déploiement orienté QoS	94
4.4.3	Déploiement dynamique	96
4.5	Conclusion	97
5	Plate-forme	99
5.1	Introduction	99
5.2	Le projet AMBIENCE	100

5.3	Présentation générale de la plate-forme	101
5.3.1	Architecture globale	102
5.3.2	Identification biométrique basée sur la voix	103
5.3.3	Système de localisation ZigBee	104
5.4	Architecture Client/Serveur	105
5.4.1	Les services	106
5.4.2	La sécurisation de l'échange des données	106
5.4.3	Le Client	107
5.4.4	L'interface utilisateur graphique de l'iPAQ (Graphical User Inter- face)	108
5.4.5	Principe de fonctionnement général entre le client et le serveur . . .	109
5.5	Architecture réseau	109
5.5.1	Le routage ad hoc	110
5.5.2	Les routeurs mobiles	111
5.6	Les applications GNetWatch et NetSim	112
5.7	Conclusion	114
	Conclusions et perspectives	114

Table des figures

1.1	Réseaux 4G	10
1.2	Extension d'une infrastructure en utilisant un réseau ad hoc	11
1.3	Méthode d'accès DCF	19
1.4	Le modèle FQMM	29
1.5	Le modèle SWAN	30
1.6	Le modèle iMAQ	31
1.7	Méthode de clustering dans les réseaux ad hoc	35
2.1	Hétérogénéité des nœuds dans les réseaux ad hoc	42
2.2	Variations de la capacité du lien en fonction de la distance	43
2.3	Puissance reçue en fonction de la distance dans un milieu avec obstacles, pour différentes puissances d'émission P_e	43
2.4	Nombre de sauts Vs débit des liens	44
2.5	Principales classes utilisées dans l'implémentation NS-2 du protocole DSR	47
2.6	Extension de la structure du message Route_Request	47
2.7	Diagramme de séquence représentant la sélection de routes	49
2.8	La structure du nœud mobile dans NS-2 en utilisant le protocole DSR ou un autre protocole (DSDV)	49
2.9	Taux de paquets reçus avec DSR vs DSR modifié	52
2.10	Délai bout en bout obtenu avec DSR vs DSR modifié	52
2.11	Taux de paquets reçus obtenu avec la mobilité pour DSR vs DSR modifié	53
2.12	Délai bout en bout obtenu avec la mobilité pour DSR vs DSR modifié	54
3.1	Modèle en couche OSI	58
3.2	Mécanismes de qualité de service	62
3.3	Débit et délai des trafics temps réel sans mécanismes de QoS	66
3.4	Débit des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)	66
3.5	Délai des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)	67
3.6	Débit et délai des trafics temps réel sans mécanismes de QoS	68
3.7	Débit des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)	68

3.8	Délai des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)	68
3.9	Débit et délai des trafics temps réel sans mécanismes de QoS	70
3.10	Débit des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)	71
3.11	Délai des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)	71
3.12	Combinaison de la QoS IP et MAC avec un routage avec différenciation de terminaux	72
3.13	Topologie utilisée dans la simulation	73
3.14	Débit avec et sans différenciation de terminaux	74
3.15	Délais avec et sans différenciation de terminaux	75
3.16	Débits avec différenciation de service IP et/ou MAC	75
3.17	Délais avec différenciation de service IP et MAC	76
3.18	Délais avec QoS IP&MAC + différenciation de terminaux	77
3.19	Débits avec QoS IP et MAC + différenciation de terminaux	77
4.1	Topologie du réseau ad hoc avec et sans déploiement des routeurs mobiles	81
4.2	Fonctionnement général du contrôle de topologie	88
4.3	Déploiement dynamique des routeurs mobiles	90
4.4	Outils utilisés dans les simulations	92
4.5	Exemple de déploiement orienté connectivité des routeurs dans un réseaux ad hoc autonome	92
4.6	Déploiement des routeurs dans un réseau autonome ou interconnecté à une infrastructure	93
4.7	Nombre optimal de routeurs dans un réseau ad hoc à 30 nœuds	94
4.8	Nombre optimal de routeurs dans un réseau ad hoc à 60 nœuds	94
4.9	Nombre optimal de routeurs dans un réseau ad hoc à 100 nœuds	95
4.10	Délai moyen obtenu dans chaque approche	95
4.11	Taux de paquets reçus dans chaque approche	96
5.1	Architecture globale de la plate-forme	102
5.2	Etape <i>offline</i> de l'identification biométrique	104
5.3	Système de localisation ZigBee	105
5.4	Architecture Client/Serveur	106
5.5	Architecture du serveur	107
5.6	Exemple de la fonctionnalité <i>Find</i> et <i>map</i>	108
5.7	Architecture réseau basée sur les routeurs mobiles	110
5.8	Routeur mobile (SPIF)	111
5.9	Architecture de GNetWatch	112
5.10	Applications graphiques pour monitorer les utilisateurs mobiles	113

Liste des tableaux

2.1	Longueur de route	44
2.2	Paramètres utilisés dans le modèle de simulation	50
3.1	Paramètres du modèle de simulation	65
3.2	Paramètres du modèle de simulation	73
4.1	Liste des données et variables utilisées	85

Liste des abréviations

ATM	Asynchronous Transfer Mode
AODV	Ad hoc On Demand Distance Vector routing protocol
CBR	Constant Bit Rate
CBRP	Cluster Based Routing Protocol
CEDAR	Core Extraction Distributed Ad hoc Routing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DAD	Duplicate Address Detection
DARPA	Defense Advanced Research Projects Agency
DCF	Distributed Coordination Function
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DSDV	Distance Source Distance Vector routing protocol
DSR	Dynamic Source Routing protocol
FTP	File Transfer Protocol
GPS	Global Positioning System
HiperLan	High Performance Local Area Network
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IntServ	Integrated Services
IP	Internet Protocol
ITU	International Telecommunication Union
LAN	Local Area Network
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
OLSR	Optimized Link State Routing
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCF	Point Coordination Function
PRNet	Packet Radio Network
QoS	Quality of Service
RFC	Request For Comments

RSVP	Resource Reservation Setup Protocol
RTS	Request To Send
SURAN	Survivable Radio Networks
TBRPF	Topology Broadcast based on Reverse-Path Forwarding
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol
ZRP	Zone Routing Protocol

Introduction générale

On assiste ces dernières années à une importante évolution dans la société de l'information, conduite par la commercialisation et l'émergence des appareils de communications (tels que les téléphones cellulaires, les ordinateurs portables, les assistants personnels, ...etc.) et la convergence des réseaux fixes et mobiles. L'utilisateur passe ainsi de l'âge de l'ordinateur personnel à l'âge de l'ubiquité du traitement à travers plusieurs infrastructures. Il a accès à l'information n'importe où et n'importe quand.

Un utilisateur mobile peut consulter son courrier électronique, naviguer sur Internet dans les aéroports, les gares ou dans d'autres lieux publics. Dans une conférence, les chercheurs peuvent transférer des fichiers et d'autres types d'information grâce à leurs appareils électroniques via des réseaux locaux sans fil ; dans sa maison, une personne peut synchroniser des données et échanger des fichiers entre différents terminaux.

Comme pour les réseaux mobiles, l'intégration des services multimédias dans les réseaux ad hoc a suscité ces dernières années un réel intérêt. Notant que les problématiques posées dans le contexte particulier des réseaux ad hoc sont différentes et plus complexes que celles rencontrées dans le monde filaire. Pour cela, plusieurs travaux pour le support de la qualité de service ont été proposés. Ils sont globalement classés par couche de protocole, et se focalisent essentiellement sur des problèmes liés à une couche particulière de la pile OSI indépendamment des autres couches . De plus, face à la prolifération et la commercialisation d'équipements mobiles hétérogènes, particulièrement en termes de capacité de transmission, il serait alors incorrect de supposer que tous les nœuds sont homogènes dans les protocoles et les solutions développés pour les réseaux ad hoc.

Dans le cadre de nos travaux, nous nous sommes intéressés à la nécessité d'une interaction inter-couches de la qualité de service dans les réseaux mobiles ad hoc. La communication entre les couches permet de mieux garantir et de satisfaire les besoins des applications multimédias temps réel. Parallèlement, nous avons étudié un protocole de routage qui permet de prendre en considération la réalité des réseaux ad hoc en termes d'hétérogénéité.

Un autre paramètre important dans les réseaux ad hoc est la topologie. Dans les approches de contrôle de topologie existantes, l'idée est d'agir sur des paramètres comme

la puissance de transmission des nœuds pour obtenir une topologie réseau désirée. Dans notre proposition, contrairement aux autres approches, nous agissons sur la mobilité d'un sous-ensemble de routeurs dédiés afin d'assurer une meilleure connectivité ou de contrôler le diamètre du réseau pour fournir des liens sans fil stables.

Organisation de la thèse

La thèse est organisée comme suit :

Dans le premier chapitre nous commençons par présenter une étude bibliographique sur les réseaux mobiles ad hoc, ainsi que les solutions existantes sur la qualité de service et le contrôle de topologie.

Notre proposition d'un protocole de routage avec différenciation de terminaux est exposée dans le chapitre 2. Après avoir présenté nos motivations, nous décrivons l'ensemble d'extensions nécessaires à effectuer sur le protocole de routage ad hoc classique DSR afin de tenir compte de la métrique de l'hétérogénéité des nœuds dans le calcul de la route. Un ensemble de simulations, sous différents scénarii de mobilité et de trafics, est réalisé à l'aide de l'outil de simulation Network Simulator 2 (NS-2). Les résultats obtenus montrent une meilleure utilisation des ressources du réseau et une sélection de route améliorée en terme de capacité des liens.

Dans le chapitre 3 nous allons d'abord montrer la nécessité d'une gestion multicouches dans les réseaux mobiles sans fil et particulièrement dans les réseaux ad hoc. Ensuite, nous allons proposer de combiner la différenciation de services au niveau de la couche IP et celle de la couche MAC. Pour cette dernière, nous avons recours à une modification de la couche IEEE 802.11. Nous allons également montrer que cette gestion multicouches de la qualité de service combinée avec un protocole de routage avec différenciation de terminaux assure un meilleur support des applications temps réel. Un ensemble de simulations est réalisé pour illustrer l'amélioration obtenue.

Une nouvelle approche de contrôle de topologie dans les réseaux ad hoc est détaillée dans le chapitre 4. Son principe est basé sur le déploiement d'un sous ensemble de nœuds mobiles dédiés, afin de contrôler et d'obtenir une topologie de réseau désirée. Les deux stratégies de déploiement sont décrites et modélisées (en collaboration avec M Nicolas PUECH) sous forme de problèmes de programmation linéaire entière mixte. Les deux configurations où le réseau ad hoc est autonome ou utilisé comme extension d'une infrastructure sont traitées. Les problèmes sont résolus à l'aide du solveur CPLEX, et des simulations de ces approches de contrôle de topologie sont effectuées pour montrer la valeur ajoutée d'une telle proposition.

Dans le chapitre 5, nous présentons la plate-forme que nous avons réalisée dans le

cadre du projet européen Ambience. L'objectif ainsi que les outils adoptés dans cette plate-forme sont détaillés. Ce chapitre illustre un exemple d'application des réseaux ad hoc où des mécanismes décrits dans les chapitres précédents sont utilisés afin d'améliorer les performances du système et répondre aux besoins des utilisateurs mobiles, dans un contexte hétérogène sécurisé.

Chapitre 1

QoS et contrôle de topologie dans les réseaux ad hoc

1.1 Réseaux ad hoc : Généralités

1.1.1 Introduction et historique

Les équipements mobiles deviennent de plus en plus petits et puissants en terme de capacité de traitement et de stockage de données. De plus, ils sont dotés d'une multitude de fonctionnalités qui permettent d'assurer différents types d'applications et de services. Parmi les applications et services offerts via un équipement mobile, figurent les services de connexions et les services de données correspondants. Ces derniers représentent le service le plus demandé par les utilisateurs mobiles. Par exemple, les connexions entre deux téléphones mobiles cellulaires sont assurées par les BSC et les MSC ; les ordinateurs portables sont connectés à Internet via des points d'accès fixes.

Il y a, en outre, des situations spécifiques où les besoins de connexions des utilisateurs ne sont pas assurés par le réseau dans une zone géographique donnée. Dans cette situation fournir la connectivité est un réel défi. Récemment, de nouvelles alternatives pour fournir les services ont été proposées. Elles sont basées sur le fait d'avoir des stations mobiles interconnectées les unes aux autres grâce à une configuration autonome, créant ainsi un réseau ad hoc flexible et performant. Parallèlement, le réseau ad hoc peut être utilisé pour l'extension d'un réseau filaire. Dans ce cas, les nœuds mobiles peuvent avoir accès à l'Internet à travers une passerelle, pour étendre les services de l'Internet au-delà de l'infrastructure filaire.

Dans le domaine des réseaux ad hoc, les réseaux de senseurs (ou de capteurs) repré-

sentent un champ important de recherche [110] [111] [112]. Un réseau de senseurs est composé d'un grand nombre de nœuds mobiles aléatoirement distribués sur le terrain à étudier, dont les tailles et les capacités sont très réduites, et dont l'objectif est de collecter les informations. Le routage ad hoc constitue la base des réseaux de senseurs. Cependant, les solutions proposées dans les réseaux ad hoc sont généralement inadaptées aux spécificités des réseaux de senseurs, vu le type d'application spécifique de ces réseaux et la fonction principale des nœuds qui est collecter l'information. De plus, les communications dans les réseaux de senseurs sont souvent à un saut et consistent à remonter l'information à une entité centrale.

Historiquement, les réseaux mobiles ad hoc ont été d'abord introduits pour l'amélioration des communications dans le domaine militaire. Dans ce contexte, il n'existe pas d'infrastructure existante pour relier les communications, vue la nature dynamique des opérations et des champs militaires.

Les premières applications dans les réseaux ad hoc sont apparues avec le projet PRNet (Packet Radio Network) [67] en 1972. Ce projet a été inspiré par l'efficacité la technologie par commutation de paquet, le partage de la bande passante, le routage store-and-forward, et ses applications dans l'environnement mobile sans fil.

SURAN (Survivable Radio Networks) [113] a été développé par la DARPA en 1983 pour dresser les principaux problèmes du projet PRNet dans le domaine de la scalabilité, la sécurité, la capacité de traitement et gestion d'énergie. Les objectifs étaient de proposer des algorithmes qui peuvent supporter jusqu'à une dizaine de milliers de nœuds, tout en utilisant des mécanismes radio simples, avec une faible consommation d'énergie, et un faible coût. Ce travail a amené à la conception de la technologie LPR (Low-cost Packet Radio) [68] en 1987, dotée d'une couche radio DSSS (Direct Sequence Spread-Spectrum) avec un processeur pour la commutation de paquets intégré (Intel 8086). De plus, une famille de protocoles pour la gestion du réseau a été développée, et une topologie hiérarchique du réseau basée sur un clustering dynamique est utilisée pour remédier au problème de la scalabilité. Des améliorations pour l'adaptabilité de la couche radio, la sécurité et l'augmentation de la capacité ont été proposées.

L'évolution des infrastructures du réseau Internet et la révolution de la micro informatique ont permis de rendre faisables et applicables les idées initiales des réseaux radio de paquets. Le programme GloMo (Global Mobile) [115] initié par la DARPA en 1994 avait comme objectif de supporter les communications multimédia n'importe quand et n'importe où à travers des équipements sans fil.

Tactical Internet (IT) [67] est l'une des implémentations des réseaux sans fil ad hoc grandeur nature développée par l'armée américaine en 1997, utilisant des débits de plusieurs dizaines de kilobits par seconde.

Un autre déploiement a été réalisé en 1999, avec ELB ACTD (Extending the Littoral

Battle-space Advanced Concept Technology Demonstration) [116] qui permet de démontrer la faisabilité de concepts militaires pour les communications des bateaux en mer aux soldats sur la terre par l'intermédiaire d'un relais aérien. 20 nœuds dans le réseau ont été considérés.

La suite de ce chapitre est organisée en trois parties. Nous allons dans un premier temps présenter les caractéristiques et les contraintes liées à l'environnement des réseaux ad hoc. En particulier les problèmes d'adressage, de routage et d'interconnexion avec d'autres types de réseaux. Dans la deuxième partie, nous détaillerons les principales solutions proposées pour fournir la qualité de service dans les réseaux ad hoc. Nous passerons en revue dans la troisième partie les approches et techniques de contrôle de topologie existantes.

1.1.2 Propriétés et spécificités des réseaux ad hoc

En général, un réseau ad hoc mobile (MANET : Mobile Ad hoc NETWORK) est considéré comme un système autonome dynamique composé de nœuds mobiles interconnectés par des liens sans fil, sans l'utilisation d'une infrastructure fixe et sans administration centralisée [117]. Les nœuds sont libres de se déplacer aléatoirement et s'organisent arbitrairement. Par conséquent, la topologie du réseau peut varier de façon rapide et surtout imprévisible.

Un réseau ad hoc peut être autonome ou connecté à une infrastructure fixe. La route entre un nœud source et un nœud destination peut impliquer plusieurs sauts sans fil, d'où l'appellation de 'réseaux sans fil multi-sauts'. Un nœud mobile peut communiquer directement avec un autre nœud s'il est dans sa portée de transmission. Au delà de cette portée, les nœuds intermédiaires jouent le rôle de routeurs (relayers) pour relayer les messages saut par saut.

Les réseaux ad hoc héritent des mêmes propriétés et problèmes liés au réseaux sans fil. Particulièrement, le fait que le canal radio soit limité en terme de capacité, plus exposé aux pertes (comparé au médium filaire), et sujet à des variations dans le temps. Le canal est confronté aux problèmes de 'station cachée' et 'station exposée'. En outre, les liens sans fil sont asymétriques et pas sécurisés.

D'autres caractéristiques spécifiques aux réseaux ad hoc conduisent à ajouter une complexité et des contraintes supplémentaires qui doivent être prises en compte lors de la conception des algorithmes et des protocoles réseaux, à savoir :

L'absence d'une infrastructure centralisée : chaque nœud travaille dans un environnement pair à pair distribué, et agit en tant que routeur pour relayer des communications, ou génère ses propres données. La gestion du réseau est ainsi distribuée sur l'ensemble des éléments du réseau.

La mobilité des nœuds et maintenance des routes : la mobilité continue des nœuds crée un changement dynamique de topologie. Par exemple, un nœud peut rejoindre un réseau, changer de position ou quitter le réseau. Ce déplacement a naturellement un impact sur la morphologie du réseau et peut modifier le comportement du canal de communication. Ajoutons à cela la nature des communications (longues et synchrones, courtes et asynchrones, ...). Les algorithmes de routage doivent ainsi résoudre ces problèmes et supporter la maintenance et prendre en charge en un temps limité la reconstruction des routes tout en minimisant l'overhead généré par les messages de contrôle.

L'hétérogénéité des nœuds : un nœud mobile peut être équipé d'une ou plusieurs interfaces radio ayant des capacités de transmission variées et opérant dans des plages de fréquences différentes. Cette hétérogénéité de capacité peut engendrer des liens asymétriques dans le réseau. De plus, les nœuds peuvent avoir des différences en terme de capacité de traitement (CPU, mémoire), de logiciel, de taille (petit, grand) et de mobilité (lent, rapide). Dans ce cas, une adaptation dynamique des protocoles s'avère nécessaire pour supporter de telles situations.

La contrainte d'énergie : Les équipements mobiles disposent de batteries limitées, et dans certains cas très limitées tels que les PDA, et par conséquent d'une durée de traitement réduite. Sachant qu'une partie de l'énergie est déjà consommée par la fonctionnalité du routage. Cela limite les services et les applications supportées par chaque nœud.

La taille des réseaux ad hoc : elle est souvent de petite ou moyenne taille (une centaine de nœuds) ; le réseau est utilisé pour étendre temporairement un réseau filaire, comme pour une conférence ou des situations où le déploiement du réseau fixe n'est pas approprié (ex : catastrophes naturelles). Cependant, quelques applications des réseaux ad hoc nécessitent une utilisation allant jusqu'à des dizaines de milliers de nœuds, comme dans les réseaux de senseurs [67]. Des problèmes liés au passage à l'échelle tels que : l'adressage, le routage, la gestion de la localisation des senseurs et la configuration du réseau, la sécurité, ...etc., doivent être résolus pour une meilleure gestion du réseau.

1.1.3 Domaines d'application des réseaux ad hoc

Les premières applications des réseaux ad hoc concernaient les communications et les opérations dans le domaine militaire. Cependant, avec l'avancement des recherches dans le domaine des réseaux et l'émergence des technologies sans fil (ex : Bluetooth, IEEE 802.11 et Hiperlan) ; d'autres applications civiles sont apparues. On distingue :

- Les services d'urgence : opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire,
 - Le travail collaboratif et les communications dans des entreprises ou bâtiments : dans le cadre d'une réunion ou d'une conférence par exemple,
-

- Home network : partage d'applications et communications des équipements mobiles,
- Applications commerciales : pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur,
- Réseaux de senseurs : pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, ...etc.) ou domestiques (contrôle des équipements à distance),
- Réseaux en mouvement : informatique embarquée et véhicules communicants,
- Réseaux Mesh : c'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

En plus, dans un LAN, un réseau ad hoc fournit une solution pour étendre une couverture sans fil avec un moindre coût. Dans un WAN (ex : UMTS), il permet d'accroître la capacité globale du réseau sans fil. En fait, plus de bande passante agrégée peut être obtenue en réduisant la taille des cellules et en créant des pico-cellules. Afin de supporter une telle architecture, les opérateurs disposent de deux options : déployer plus de stations de base (une station de base par cellule), ou utiliser un réseau ad hoc pour atteindre la station de base. La deuxième solution est clairement plus flexible et moins coûteuse.

1.1.4 Réseaux ad hoc et réseaux 4G

Fondé sur un cœur de réseau IP, le futur système de télécommunication 4ème génération (4G) représente la convergence entre le réseau 3ème génération (type UMTS) et les diverses technologies radio complémentaires. L'objectif est de fournir aux utilisateurs des services sans interruption dans un environnement hétérogène. Les utilisateurs mobiles peuvent accéder ou échanger des informations indépendamment de leurs positions, du temps et en utilisant des équipements différents en terme de capacité. Les réseaux 4G sont des réseaux hybrides qui intègrent différentes topologies et plates-formes réseaux.

Il existe deux niveaux d'intégration : l'intégration des différents types de réseaux sans fil hétérogènes avec leurs techniques de transmission (wireless LAN, WAN, PAN ainsi que les réseaux ad hoc); et l'intégration des réseaux sans fil avec l'infrastructure fixe, l'Internet et le réseau téléphonique fixe. Cependant, beaucoup de travail demeure pour permettre une intégration sans couture, comme par exemple l'extension du protocole IP pour le support des stations mobiles.

Un réseau sans fil 4G tout IP est indépendant des technologies d'accès radio, où le cœur du réseau peut être doté de protocoles et services déjà existants, comme la voix et la donnée, comme les protocoles de voix sur IP (VoIP, SIP, H.323, ...etc.). Il offre un débit allant jusqu'à 100 Mbps. Parallèlement, les terminaux mobiles sont plus 'intelligents', en termes de leur position (comme le GPS dans l'environnement extérieur) et leurs besoins de services.

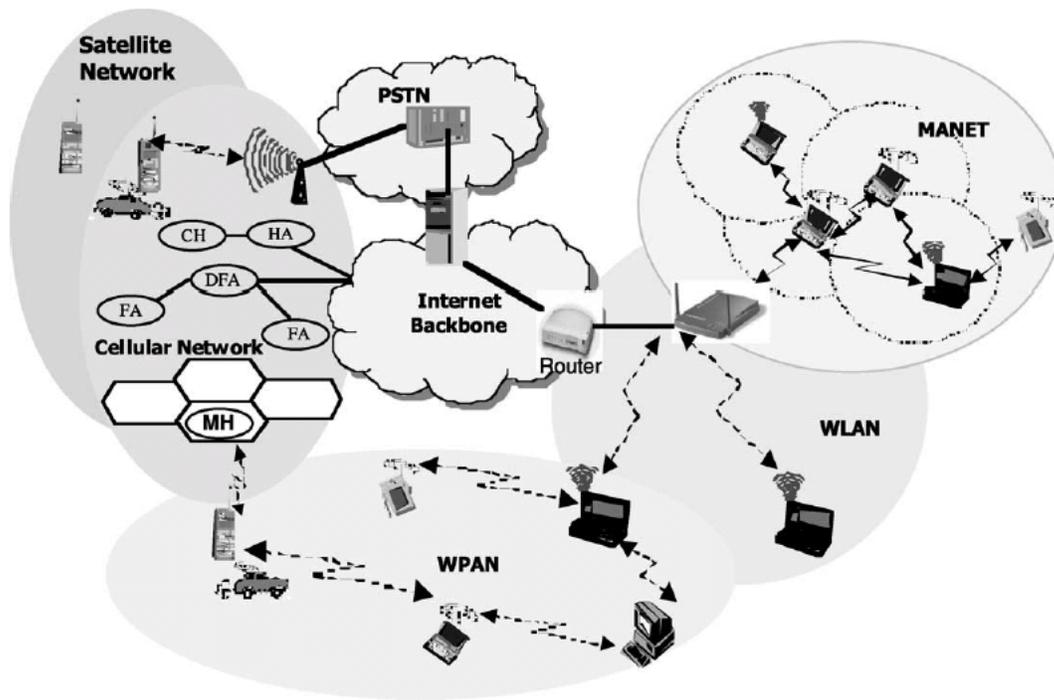


FIG. 1.1 – Réseaux 4G

Dans la section suivante nous nous intéressons aux problèmes de configuration et d'adressage quand le réseau ad hoc est utilisé pour étendre un réseau filaire. Quelques solutions existantes pour résoudre ces problèmes seront décrites.

1.1.5 Topologie du réseau ad hoc et interconnexion avec une infrastructure

Une fonctionnalité importante qui doit être intégrée dans les réseaux ad hoc est la capacité de se relier aux réseaux filaires, dans le but d'avoir accès aux services de l'Internet via une passerelle. Il est aussi nécessaire d'avoir une passerelle capable d'effectuer certaines translations d'adressage. Si l'interconnexion se fait au niveau du lien, ce qui est normalement le cas à moins qu'il y ait un raccordement au réseau externe via un routeur, le réseau ad hoc doit s'autoconfigurer de manière à coopérer avec le système d'adressage utilisé dans le réseau fixe (pour avoir le même préfixe d'adresse et masque de sous réseau). L'interconnexion avec les réseaux fixes consiste à donner aux nœuds du réseau ad hoc la possibilité de fonctionner comme s'ils faisaient partie d'un bus fixe Ethernet.

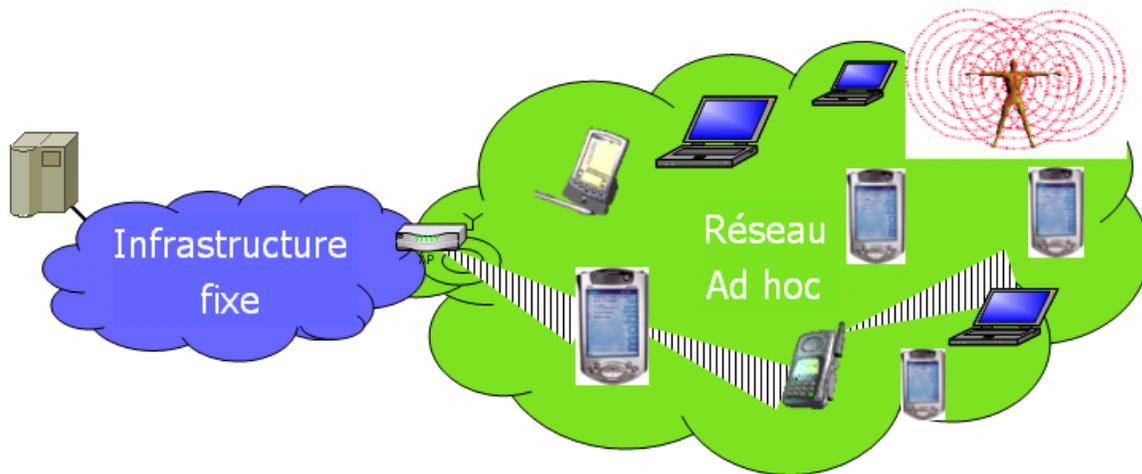


FIG. 1.2 – Extension d’une infrastructure en utilisant un réseau ad hoc

Problème de configuration et d’adressage

Il y a deux catégories de problèmes qui surgissent quand on considère l’interconnectivité des réseaux mobiles ad hoc dans les situations décrites ci-dessus. Ces deux catégories sont assez indépendantes, et des solutions doivent être mises en œuvre pour l’une sans affecter l’autre de façon considérable. La première catégorie concerne le schéma d’adressage à adopter, et la seconde concerne le mécanisme ou le protocole de configuration qui permet à ces adresses d’être assignées aux diverses machines dans le réseau.

Il est nécessaire de fournir des solutions robustes aux deux problèmes dans des situations et des environnements divers. Les réseaux fixes - s’ils ne sont pas configurés manuellement - sont configurés avec un serveur DHCP [118] qui alloue des adresses aux machines qui joignent le réseau. En l’absence de cette entité, il est clair qu’afin d’assigner une adresse à une machine souhaitant rejoindre le réseau, chaque autre machine qui fait partie du réseau doit connaître cette attribution et l’approuver afin d’empêcher la duplication d’adresse. Ceci implique la génération de beaucoup plus de trafic de signalisation dans l’attribution d’une adresse, et ainsi une quantité substantielle de la bande passante est consommée. Si un réseau contient deux adresses identiques, les algorithmes de routage deviennent invalides, notamment à cause des boucles dans les routes. Pour ce, le protocole de configuration doit être robuste même aux dépens d’une utilisation élevée de la bande passante.

DAD (Dual Address Detection)

Une méthode rudimentaire proposée par le groupe de travail Zeroconf de l'IETF est connue comme une méthode de détection d'adresse duelle [53]. Ici un nœud souhaitant joindre un MANET sélectionne une adresse d'une gamme indiquée puis diffuse un RREQ (Route Request) pour cette adresse au reste du réseau. Si aucun RREP (Route Response) n'est reçu au cours d'un certain temps, le nœud essaie encore jusqu'au temps de RREQ RETRIES pour prendre en compte la possibilité que le message reçu a été perdu le long de la route. Dans ce cas, un problème peut apparaître : quand un nœud attend une réponse, il doit d'abord avoir une adresse. Il est ainsi préférable durant la phase d'attribution d'adresse permanente d'assigner une adresse obtenue aléatoirement à partir d'un intervalle d'adresses spécifiquement réservé. Du moment qu'aucune adresse appartenant à cet intervalle n'est sélectionnée comme adresse permanente, et que la plage d'adresse temporaire est suffisamment large, la probabilité que deux nœuds sélectionnant la même adresse durant la phase d'affectation d'adresses permanentes (quelques secondes au maximum) est assez petite, voire négligeable.

Address Auto-configuration for IPv6

Dans les réseaux filaires sans aucun serveur de configuration tel que DHCP [49], IPv6 Stateless Address Autoconfiguration (SAA) est habituellement utilisé par les nœuds pour obtenir une adresse IPv6 routable [54]. IPv6 SAA consiste fondamentalement en trois phases : construction d'une adresse 'link-local', détection d'adresse double, et la construction d'une adresse 'site-local' pour l'usage local

Cependant, ce protocole tel que présenté ne peut pas être directement appliqué aux réseaux ad hoc, car il y a une disparité entre la portée d'adresse et la topologie du réseau. Afin d'atteindre sa destination, un message peut utiliser un chemin multi-sauts, dans ce cas, l'utilisation des adresses link-local violera le terme "link-local" puisque l'adresse ne doit être valide non uniquement pour ses voisins immédiats. [50] et [53] proposent d'utiliser SAA dans MANET en utilisant l'adresse site-local. Dans [53], un nœud entrant dans le réseau prend aléatoirement un identificateur de sous-réseau et le concatène avec le préfixe site-local et son identificateur d'interface de 64 bits (adresse MAC). Le nœud doit alors vérifier l'unicité de l'adresse résultante : fec0 :0 :0 : :. Ceci est fait par une méthode DAD modifiée. Ainsi, l'identificateur de sous-réseau est simplement considéré comme une extension de l'identificateur d'interface, et chaque nœud peut avoir un identificateur différent de sous-réseau.

Dans [55], le mécanisme proposé est également basé sur les principes de SAA. Il définit un nouveau format pour des messages de NDP (Neighbor Discovery Protocol) et un mécanisme différent de génération d'adresses. Un nœud du réseau exécutant la configuration automatique prend deux adresses. Par défaut, l'adresse demandée est créée en enchaînant

un nombre de nœuds aléatoire au préfixe du réseau. Le préfixe initial du réseau ad hoc est employé pour choisir l'adresse provisoire. Le nœud envoie une demande d'adresse (AREQ un message de sollicitation de voisin modifié) et attend la réponse d'adresse (AREP est une réponse de voisin modifiée) si l'adresse demandée est déjà employée dans le réseau. Dans le cas où un autre nœud possède l'adresse demandée, un message AREP est envoyé au créateur du message AREQ en utilisant l'adresse provisoire. Un champ est ajouté à l'en-tête du message NDP pour indiquer que ce message devrait être envoyé à travers un réseau multi-sauts. La limite de sauts peut être fixée dans l'en-tête IPv6 afin de borner le diamètre du réseau ad hoc.

Distributed Dynamic Host Configuration Protocol (DDHCP)

Aucun des protocoles décrits jusqu'ici ne fournit les mécanismes complets pour assurer un MANET entièrement fonctionnel. Le protocole (DDHCP) [52] est une solution plus complète qui tient compte du fait qu'il y a souvent des pertes de messages pendant l'attribution d'adresses en raison de la nature du lien physique entre les nœuds. En outre, il propose également un mécanisme pour renvoyer des adresses libérées à un ensemble d'adresses disponibles pour la réutilisation. L'idée générale derrière les diverses fonctionnalités du protocole est qu'un nœud souhaitant rejoindre le réseau essaye d'entrer en contact avec un nœud déjà dans le réseau et lui demande à effectuer l'attribution d'adresse en son nom. Le nœud se joignant est connu comme le demandeur et le nœud effectuant l'attribution d'adresse est connu comme initiateur. Puisque l'initiateur fait déjà partie du réseau, il peut être atteint par les autres nœuds déjà dans le réseau et peut recevoir ainsi toutes les réponses envoyées. L'initiateur est donc une sorte de procuration pour le demandeur jusqu'à ce qu'il lui assigne une adresse IP permanente et devienne lui-même un nœud faisant partie du réseau ad hoc.

ANANAS : A New Ad hoc Network Architectural Scheme

L'architecture d'ANANAS [48] propose de séparer les niveaux : 2, 2.5 (niveau ad hoc) et le niveau 3 (IP). Cette politique implique l'existence de deux systèmes d'adressage séparés : un pour le niveau ad hoc et un pour le niveau IP. L'utilisation d'une couche supplémentaire d'adressage dans le MANET exige l'établissement d'une 'interface virtuelle'. Cette interface virtuelle est employée pour faire le lien entre la couche d'adressage ad hoc et la couche d'adressage IP.

Dans cette approche, l'adressage IP n'a besoin d'aucun schéma de configuration spécifique puisque le niveau ad hoc est transparent du point de vue du niveau IP. Le niveau IP voit juste un bus Ethernet auquel tous les nœuds du réseau sont attachés. Comme le niveau ad hoc est vu comme une couche Ethernet simple, il supporte pleinement les services IP. Différents réseaux ad hoc sont alors considérés par la couche IP comme des

liens Ethernet différents, ainsi, le routage entre plusieurs réseaux ad hoc est une tâche de cheminement IP. La mobilité entre les réseaux ad hoc est donc assurée par le protocole Mobile IP.

Interconnexion à une infrastructure

[55] et [56] décrivent des solutions pour relier un réseau ad hoc à une infrastructure. Dans le Draft IETF sur la connectivité globale dans MANETs [55], quand un nœud veut accéder à l'Internet, il doit découvrir une passerelle Internet effectuant de ce fait une découverte de passerelle Internet. On suppose que tous les nœuds du réseau ad hoc ont déjà une adresse IP. Cette adresse peut être une adresse IPv6 mère ou une adresse obtenue à partir du préfixe du réseau après un DAD ou une adresse provisoire choisie du préfixe initial du réseau. Le mécanisme de découverte de passerelle Internet utilise des messages NDP modifiés : Router Solicitation et Router Advertisement.

Afin de trouver une passerelle, un nœud doit diffuser un MANET Router Solicitation à l'adresse de la passerelle Internet, en utilisant des valeurs limitées de nombre de sauts, afin d'empêcher le message de circuler trop longtemps. Si le nœud de réception est une passerelle Internet, il envoie un message MANET Router Advertisement à l'expéditeur de sollicitation de routeur. Ce message inclura le préfixe global de la passerelle et l'adresse de la passerelle Internet. La passerelle doit à son tour enregistrer l'adresse globale du demandeur dans sa table de routage. Autrement, les nœuds intermédiaires relayent seulement les messages.

Quand le nœud reçoit des réponses des passerelles Internet indiquant leur présence dans le réseau, il doit élire l'un d'entre eux comme son point d'accès. Ensuite, il devrait produire une adresse IPv6 globale en employant le préfixe global et ses 64 bits d'identificateur d'interface. Puisque le nœud a déjà fait un DAD pour l'adresse site-local (basée sur le préfixe du réseau), l'adresse globale à partir de l'adresse site-local sera également unique.

Quand un paquet est envoyé à l'Internet, il est recommandé d'utiliser l'option de routage IPv6 comme suit : l'expéditeur utilise l'adresse de la passerelle Internet dans le champ destination de l'en-tête IPv6, et l'adresse de la destination réelle dans l'en-tête de routage. Cette méthode est recommandée pour plusieurs raisons : si l'expéditeur

ne sait pas que le nœud destinataire est dans le MANET, il enverra le paquet à la passerelle. Si la passerelle détecte que le nœud destinataire est dans le MANET, il enverra un ICMP réorientant le message d'erreur à l'expéditeur. Après réception du message d'erreur, le nœud peut envoyer une demande de route vers la destination. Sans l'option de routage incluse dans l'en-tête, un nœud intermédiaire peut envoyer le paquet directement au nœud destinataire et cela sans que la source ne sache que la destination soit à l'intérieur du MANET. Si la passerelle détecte que le nœud destination est dans le réseau ad hoc, elle

envoie un message d'erreur au nœud source. Une fois ce message d'erreur reçu, le nœud envoie une demande de route pour la destination pour avoir une route. S'il y a plusieurs passerelles dans le réseau ad hoc, le nœud peut choisir la meilleure passerelle Internet, en terme de distance (nombre de sauts) par exemple.

Dans ce qui suit nous étudions la fonction de routage dans les réseaux ad hoc et décrivons quelques protocoles de routage spécialement conçus pour un tel environnement.

1.1.6 Le routage dans les réseaux ad hoc

Le but principal des protocoles de routage est l'établissement et la maintenance des routes, pour que les messages soient correctement délivrés dans le réseau. Les caractéristiques des réseaux ad hoc rendent l'utilisation des protocoles filaires classiques [83] [82] inadéquate. Les protocoles de l'Internet ont été conçus pour des réseaux ayant des topologies statiques, et sont exécutés par des nœuds dotés de suffisamment de ressources.

Les protocoles de routage dans les réseaux ad hoc opèrent dans des réseaux dont les changements de topologie sont fréquents, et sont exécutés sur des équipements ayant des contraintes de ressources (de batterie, de mémoire, de CPU, ...etc.).

Ces dernières années, plusieurs protocoles de routage ad hoc ont été proposés, soit en modifiant les protocoles de routage de l'Internet, soit en élaborant de nouvelles approches de routage. Ils sont classés comme suit : proactifs, réactifs ou hybrides. Dans les algorithmes de routage proactifs, chaque nœud dans le réseau doit avoir et maintenir des informations de routage et les stocke dans des tables. Le protocole maintient la consistance de ces tables, en envoyant périodiquement des mises à jours à travers le réseau. Ce type d'algorithmes peut être plat ou hiérarchique (OLSR [66] par exemple).

Dans le cas où un protocole de routage réactif est utilisé, les routes sont créées à la demande, c'est à dire, lorsqu'un nouveau trafic est lancé, suivant le principe de requête-réponse. Quand un nœud veut initier une communication avec un autre nœud, il commence un processus de découverte de route (Route Discovery). Une fois la route trouvée, elle est maintenue par une procédure de maintenance de route, jusqu'à ce que la route ne soit plus utilisée. Des exemples des protocoles de routage réactifs sont : AODV [69] et DSR [106]. Ils visent tous à trouver le chemin le plus court entre une source et une destination en tenant en compte de l'état du nœud et de la configuration du réseau quand une route est demandée.

En plus des protocoles de routage réactifs et proactifs, il existe une famille de protocoles de routage qui mixe les deux et sont dit 'hybrides' (exemple : ZRP [71]). Nous allons décrire dans ce qui suit des exemples de protocoles de routage proactifs, réactifs et hybrides.

OLSR : Optimized Link State Protocol

OLSR [66] est un protocole de routage proactif. Il est considéré comme une optimisation du protocole à état des liens filaire pour les réseaux mobiles ad hoc. Son innovation réside dans sa façon d'économiser les ressources radio lors des diffusions. Ceci est réalisé grâce à l'utilisation du concept des relais multi-points dans lequel chaque nœud choisit un sous-ensemble de ses voisins qu'il appellera "MPR" (multi-point relais) pour retransmettre ses paquets en cas de diffusion. En se basant sur la diffusion sur les MPRs, tous les nœuds du réseau sont atteints avec un nombre réduit de répétitions.

Comme dans le paradigme proactif, des messages de contrôle périodiques doivent être utilisés pour le maintien des tables de routage et de voisinage. Dans OLSR, principalement deux types de messages sont introduits : "Hello" et "TC"(Topology Control). Périodiquement, chaque nœud diffuse localement un message Hello contenant des informations sur son voisinage et l'état des liens. Ceci permet à chaque nœud de prendre connaissance de son voisinage à un et deux sauts. L'ensemble MPR est alors construit dans chaque nœud de façon à contenir un sous-ensemble de voisins à un saut qui couvre tous les voisins à deux sauts. Afin de construire les tables nécessaires au routage des paquets, chaque nœud génère périodiquement un paquet TC contenant la liste de ses voisins l'ayant choisi comme MPR. Le message TC est diffusé dans l'ensemble du réseau. Seuls les voisins MPR rediffluent un paquet TC reçu pour éviter l'inondation. Cette technique prometteuse réduit considérablement l'overhead généré par le trafic de contrôle. A la réception d'un message TC, la table de topologie peut être construite. Basé sur la table de topologie, chaque nœud peut calculer la table de routage qui permet d'acheminer les paquets vers n'importe quelle destination dans le réseau.

AODV : Ad hoc On Demand Distance Vector

AODV [69] est un algorithme de routage à la demande, c'est-à-dire qu'il ne construit de routes entre nœuds que lorsqu'elles sont demandées par les nœuds sources, et ce pour réduire le nombre de diffusions de messages. AODV utilise les principes des numéros de séquence afin de maintenir la consistance des informations de routage. Les numéros de séquence permettent d'utiliser les routes les plus récentes. Il utilise une requête de route dans le but de créer un chemin vers une destination. La route peut ne pas exister si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré ou il est devenu défaillant. Cependant, AODV maintient les chemins d'une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché. Afin de maintenir des routes cohérentes, une transmission périodique du message "HELLO" est effectuée. Si au bout d'un certain temps aucun message "HELLO" n'est reçu à partir d'un nœud voisin, le lien en question est considéré défaillant. Le protocole AODV ne présente pas de boucle de routage, et offre une convergence rapide quand la topologie du réseau ad hoc change.

DSR : Dynamic Source Routing Protocol

Le protocole DSR [106] est basé sur le principe de diffusion à la demande pour calculer une route vers une destination. Il utilise un routage par la source, et se base principalement sur deux mécanismes coopératifs : 'la découverte de route' et 'la maintenance de route'. Il permet aussi l'existence de plusieurs routes vers la destination. A partir des informations de routage qui sont incluses dans les paquets de données, les nœuds appartenant à la route, ainsi que leurs nœuds voisins, peuvent les collecter et les mettre dans leurs caches pour une utilisation ultérieure. Chaque nœud dans le réseau envoyant ou relayant un paquet est responsable de confirmer son acheminement vers le prochain nœud en recevant un acquittement. Si un nœud détecte une cassure de route, un message d'erreur de route est retourné à la source. Lors de la réception d'un message d'erreur de route, la source supprime la route défaillante de son cache. Si un chemin alternatif est disponible, il peut être employé pour des données restantes à la destination, autrement, une nouvelle découverte de route est lancée. Comme AODV, DSR bufférisé les paquets IP dans le nœud de source quand la découverte de route est effectuée.

TBRPF : Topology Dissemination Based on Reverse-Path Forwarding

TBRPF [70] est un protocole de routage proactif à état de lien. Chaque nœud exécutant TBRPF calcule un arbre de source fournissant des routes à tous les nœuds accessibles. Il se base sur l'information partielle de topologie stockée dans sa table de topologie, en utilisant une modification de l'algorithme de Dijkstra. Pour réduire l'overhead, chaque nœud rapporte seulement une partie de son arbre de source aux voisins. TBRPF emploie une combinaison de mises à jour périodiques et différentielles pour tenir tous les voisins au courant de la partie rapportée de son arbre de source. Chaque nœud a également l'option pour rapporter l'information additionnelle de topologie (jusqu'à la topologie complète), pour fournir la robustesse améliorée dans les réseaux fortement mobiles. TBRPF effectue la découverte de voisins en utilisant des messages HELLO différentiels, qui rapportent seulement des changements sur l'état des voisins. Par conséquent, les messages HELLO sont beaucoup plus petits que ceux utilisés dans d'autres protocoles de routage à état de lien tels que OSPF.

ZRP : Zone-Based Hierarchical Link State Routing Protocol

ZRP [71] est un exemple de protocole hybride qui combine des approches proactives et réactives, essayant de ce fait de rassembler les avantages des deux approches. ZRP définit autour de chaque nœud une zone qui contient les nœuds voisins à un nombre donné de sauts du nœud. Des algorithmes proactifs et réactifs sont employés par le nœud pour acheminer les paquets, respectivement, dans et en dehors de la zone.

Normalisation

Le groupe de travail MANET (Mobile Ad hoc NETwork) [84] à l'IETF (Internet Engineering Task Force) a normalisé les protocoles de routage proactifs : OLSR (RFC 3626) et TBRPF (RFC 3684) ainsi que le protocole réactif AODV (RFC 3561). Le protocole DSR (<draft-ietf-manet-dsr-10.txt>) est, quant à lui, en cours de normalisation.

Dans la section suivante nous présentons les principaux standards utilisés dans les réseaux ad hoc pour les transmissions sans fil.

1.1.7 La couche MAC 802.11 dans les réseaux ad hoc

Le protocole IEEE 802.11 [44] peut opérer suivant deux configurations du réseau sans fil local : réseau à infrastructure ou réseau autonome. Dans la première configuration, un contrôleur centralisé est utilisé pour chaque cellule, souvent représenté par un Point d'Accès (AP). Le point d'accès est connecté au réseau filaire et peut donc fournir aux stations mobiles l'accès à Internet entre autres. Dans la deuxième configuration, le réseau est un système pair à pair constitué de stations qui s'autoconfigurent pour former un réseau temporaire.

Actuellement, les standards IEEE 802.11 et Bluetooth sont principalement utilisés dans les réseaux ad hoc pour le support des communications sans fil.

Description de la couche MAC IEEE 802.11

Nous avons utilisé dans notre thèse la couche MAC du standard IEEE 802.11[44]. Sa méthode d'accès basique est la 'Distributed Coordination Function' (DCF) qui se base sur l'utilisation de CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) pour supporter les transmissions asynchrones de données. La deuxième fonction d'accès, optionnelle, est la PCF (Point Coordination Function) sert à supporter les trafics synchrones, i.e. trafics temps réel. Cette dernière est utilisée en mode infrastructure. Pour les réseaux Ad Hoc, la première fonction est utilisée.

Le principe de la fonction DCF consiste à écouter le canal pour voir si un autre nœud est en train d'émettre. Le nœud doit s'assurer que le médium est libre pour une certaine durée (DIFS) avant d'émettre. Si le canal est occupé, la transmission est différée d'un temps de Backoff, choisi aléatoirement dans une fenêtre appelée Contention Window (CW). La valeur du Backoff ne sera décrémentée que si le médium est libre. Cependant, si au moins deux stations émettent simultanément, une collision peut apparaître et sa détection par la station émettrice n'est malheureusement pas possible. Pour cela, un ac-

quittement (ACK) est utilisé pour informer la station émettrice que la trame est reçue avec succès.

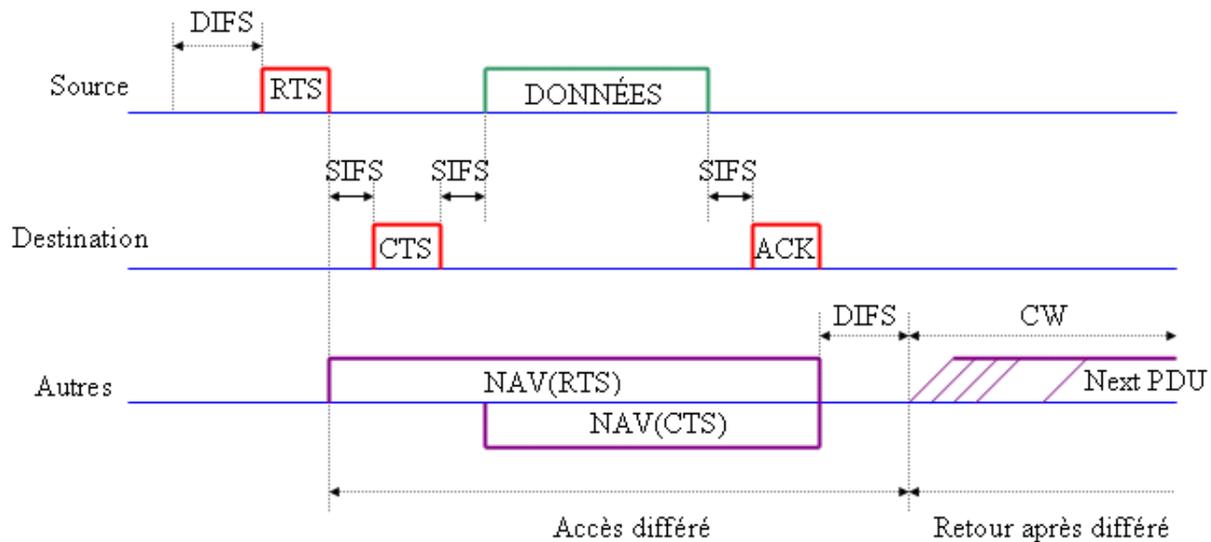


FIG. 1.3 – Méthode d'accès DCF

De plus, un principe RTS/CTS (Request To Send / Clear To Send) est utilisé pour résoudre le problème des stations cachées. Avant d'émettre, une station envoie un message RTS pour réserver le canal, la destination répond par un message CTS s'il est prêt à recevoir. Ainsi, le canal est réservé pour la durée de la transmission. Les messages RTS/CTS et ACK sont prioritaires à l'accès au médium, car ils disposent d'un temps d'attente IFS (Inter Frame Space) inférieur à celui des paquets de données.

Bluetooth

Le standard Bluetooth [72] a été initié par Ericsson et un groupe de travail (SIG : Special Interest Group) réunissant plusieurs grands industriels dont 3Com, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, Toshiba, ...etc. Les dispositifs Bluetooth peuvent former des réseaux piconet de quelques dizaines de mètres, composés d'un maximum de sept 'esclaves' et un 'maître', capables de rendre de multiples services et d'inspirer de nombreux modèles d'application, dont la téléphonie sans fil, l'accès à Internet et divers services comme l'échange de fichiers, la synchronisation de données et l'impression.

Le groupe de travail IEEE 802.15 a pris en compte les spécifications de Bluetooth pour la standardisation des réseaux personnels (WPAN : Wireless Personal Area Network).

Après avoir présenté les propriétés et spécificités des réseaux ad hoc, nous décrivons

dans la partie suivante les solutions existantes pour fournir la qualité de service dans ce type de réseau.

1.2 Qualité de service dans les réseaux ad hoc

1.2.1 Introduction

Dans cette partie nous allons présenter les principaux travaux de recherche traitant la qualité de service dans le contexte particulier des réseaux ad hoc.

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et les ressources du réseau utilisées d'une façon optimale.

La qualité de service QoS (Quality of Service) peut être définie comme le degré de satisfaction d'un utilisateur des services fournis par un système de communication. La QoS est définie dans [73] comme la capacité d'un élément du réseau (ex : routeur, nœud ou une application) de fournir un niveau de garantie pour un acheminement des données.

Le RFC 2386 [74] caractérise la QoS comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination. Ces besoins peuvent être traduits en un ensemble d'attributs pré-spécifiés et mesurables en terme de :

- Délai de bout en bout,
- Variance de délai (gigue),
- Bande passante,
- Pertes de paquets.

Suivant le type de l'application, les besoins de QoS sont différents. Par exemple, pour les applications temps réel, comme la voix et la vidéo, le délai de bout en bout d'un paquet doit être limité, autrement le paquet est inutile. Les applications non temps réel, comme le transfert de fichier ou la messagerie, quant à elles se focalisent sur la fiabilité des communications.

Le support de la qualité de service a été largement étudié dans les réseaux filaires. Le réseau ATM (Asynchronous Transfert Mode) a considéré le support de la QoS pour les trafics en plusieurs classes. Des solutions ont été proposées par l'IETF pour améliorer le réseau Internet afin de fournir la QoS aux communications multimédia. Des mécanismes ont été fournis pour gérer efficacement les ressources réseau (bande passante, mémoire tampons) pour répondre aux exigences des applications.

Dernièrement, avec l'émergence des services multimédia temps réel, et les champs variés des applications des réseaux ad hoc, la qualité de service dans les réseaux ad hoc est devenu un thème de recherche qui a suscité beaucoup d'intérêts. Dans ce contexte, des travaux pour l'introduction des applications multimédia dans les réseaux ad hoc ont été

proposés. Cependant, il est très difficile de garantir une quelconque qualité de service à une application temps réel dans un réseau ad hoc, car il faut prendre en considération les spécificités de ces réseaux, à savoir : la bande passante limitée, le changement dynamique de la topologie en fonction du temps, ainsi que le manque d'information complète sur l'état du réseau. En outre, la communication entre les stations mobiles étant par voix radio, la qualité du lien sans fil reste peu fiable, et susceptible à des variations suivant la configuration et l'état du réseau.

Dans ce qui suit nous allons présenter quelques travaux de QoS dans les réseaux ad hoc pour garantir une qualité de service pour les applications temps réel. Les approches existantes dans la littérature peuvent être classifiées suivant la couche où suivant les mécanismes de qualité utilisés (ex :les modèles de qualité de service intégrant plusieurs fonctionnalités). Dans le reste de cette partie, nous allons présenter les solutions proposées au niveau MAC, puis les protocoles de routage avec le support de la QoS. Le protocole de réservation de ressource INSIGNIA sera décrit, suivi des modèles de qualité de service développés spécialement pour les réseaux ad hoc.

1.2.2 Différenciation de service au niveau de la couche MAC

Récemment, des schémas de différenciation de service au niveau MAC ont été proposés. Néanmoins, ils sont souvent basés sur un contrôle centralisé. Dans les réseaux sans fil multi sauts, un contrôle distribué est nécessaire. Le protocole MACA/PR (Multihop Access Collision Avoidance with Piggyback Reservation) [75] propose de fournir des garanties de bande passante pour les applications temps réel via une réservation. Il permet d'établir des connexions temps réel à un saut seulement. Il utilise un dialogue RTS/CTS (Request To send/ Clear To Send) avec acquittement, et différencie la politique d'accès au médium selon la nature des flux. Pour le trafic prioritaire, une seule demande d'autorisation à transmettre (RTS-CTS) au début du flux est utilisée (jusqu'à perte d'un paquet). Dans chaque paquet, des informations sur l'ordonnancement du paquet suivant sont incluses pour empêcher les voisins d'entrer en collision avec les prochains paquets.

Dans la section suivante nous nous intéressons aux mécanismes de différenciation de service proposés pour le protocole IEEE 802.11.

Différenciation de service basée sur la fonction DCF du protocole 802.11

Dans le but d'améliorer la méthode d'accès DCF du protocole 802.11, les techniques suivantes ont été proposées :

Fonction de backoff différente [28] [76] : le principe est d'attribuer des valeurs de fenêtres de contention (CW) supérieures pour les stations les moins prioritaires et

inversement, permettant ainsi de donner plus de chance à une station prioritaire d'accéder au canal.

Différents DIFS [28] : dans le standard IEEE 802.11 de base les trames ACK ont une priorité sur les trames RTS, en attendant un temps SIFS qui est inférieur à DIFS (pour RTS). Dans cette technique de différenciation, la même idée est utilisée, où chaque station mobile dispose de sa propre valeur de DIFS qui définit son niveau de priorité pour l'accès au médium,

Distributed Fair Scheduling [77] : dans ce schéma d'accès la valeur du backoff générée avant un envoi, est proportionnelle à la longueur de la trame de donnée et inversement proportionnelle au poids du flux,

BlackBurst [33] [32] : il impose des conditions telles qu'un intervalle constant pour accéder au lien et la possibilité de bloquer le canal pendant une période de temps,

Différent longueur maximale de trame [28] : où chaque station a une priorité qui lui permet d'envoyer des trames ayant une taille maximale différente,

Différenciation des valeurs de CWmin de la fenêtre de contention : il utilise des valeurs de CW_{min} et CW_{max} différentes, où $CW_{min}(highprio) < CW_{min}(lowprio)$, et $CW_{max}(highprio) < CW_{max}(lowprio)$.

D'autres approches [29] utilisent une différenciation basée sur les flots ou sur les files au lieu d'une priorité affectée par station mobile. L'étude réalisée dans [30], montre que l'utilisation du paramètre DIFS pour la différenciation de service montre de bons résultats.

Un mécanisme de priorité pour la fonction DCF de la couche MAC 802.11 a été étudié dans [28]. Il consiste à différencier les trafics, et introduire une priorité en modifiant les paramètres de la fonction d'accès DCF. Son principe consiste à associer des DIFS ou des temps de backoff plus courts pour les flux prioritaires. Ainsi, les flux prioritaires auront une plus grande probabilité d'accéder au médium que les autres. D'autres paramètres de la fonction DCF peuvent aussi être utilisés pour différencier des services.

IEEE 802.11e

Actuellement en cours d'évaluation, la spécification du draft IEEE 802.11e [31] propose le support de la QoS dans les réseaux sans fil avec une nouvelle fonction de contrôle EDCA (Enhanced Distributed Channel Access), considérée comme la nouvelle version de la fonction DCF, et une fonction de coordination hybride (HCF). EDCA introduit quatre catégories de trafics (TC). Les priorités sont contrôlées par les stations en modifiant le schéma d'accès de base (DCF). Plus flexible que la fonction PCF, HCF est utilisée par les points d'accès pendant la période d'accès contrôlée (CAP), qui peut commencer à n'importe quel moment durant 'la superframe'. Autrement dit, ça lui permet d'avoir accès au médium pour faire passer un trafic ayant des contraintes de QoS.

Nous présentons dans la section suivante le principe du routage avec qualité de service

et passons en revue les protocoles avec QoS existants.

1.2.3 Protocole de routage avec qualité de service

Les algorithmes de routage traditionnels discutés dans les sections précédentes ont été proposés pour router les données sans tenir compte des contraintes spécifiques ou à des demandes des utilisateurs. Ainsi, ils sont inadaptés aux applications qui nécessitent le support de la qualité de service.

Contrairement aux protocoles 'au mieux' (Best Effort), le but des protocoles de routage avec support de la qualité de service [9] [51] [100] [80] [114] est de trouver une route ayant suffisamment de ressources pour satisfaire les besoins de QoS d'une communication, tout en optimisant l'utilisation des ressources disponibles.

Les métriques de QoS peuvent être additives, concaves ou multiplicatives. La bande passante est une métrique concave, alors que le délai et la gigue sont des métriques additives. La disponibilité d'un lien, basée sur des critères comme la probabilité de perte du lien quant à elle est une métrique multiplicative.

Une métrique additive A_m est définie comme : $\sum_{i=1}^h (L_i(m))$ où $L_i(m)$ est la valeur de la métrique m sur le lien L_i et $L_i \in P$. h représente la longueur du chemin P . Une métrique concave définit la valeur minimale sur un chemin P et représenté comme : $C_m = \min(L_i(m), L_i(m) \in P$. Une métrique multiplicative représente le produit des valeurs des métriques de QoS, elle est définie comme : $M_m = \prod_{i=1}^h L_i(m), L_i(m) \in P$. Pour trouver une route qui satisfait une métrique concave, les ressources disponibles dans chaque lien doivent être au moins égales à la valeur désirée de la métrique.

Trouver un chemin optimal assurant des contraintes multiples peut être un problème NP-Complet, dans le cas où il inclut deux métriques additives ou plus [119] [120].

Contrairement aux réseaux filaires, les changements de topologie dans les réseaux ad hoc exigent de recalculer les routes avec QoS, et répondre assez rapidement sans dégrader leur niveau de QoS. Par conséquent, des ressources additionnelles sont consommées (bande passante, batterie, ...etc.).

CEDAR (Core-Extraction Distributed Ad hoc Routing Algorithm)

CEDAR [9] est un protocole de routage réactif avec qualité de service basé sur une élection dynamique d'un cœur de réseau stable. Des informations sur les liens stables disposant d'une grande bande passante sont propagées entre les nœuds du cœur. Le calcul des routes est effectué par les nœuds du réseau cœur en utilisant des informations locales.

Utilisé dans des réseaux de petite à moyenne taille (de dizaines à des centaines de nœuds), il est basé sur trois composantes essentielles :

- Extraction d'un cœur du réseau : un ensemble de nœud est dynamiquement choisi pour calculer les routes et maintenir l'état des liens du réseau. L'avantage d'une telle approche est qu'avec un ensemble réduit de nœuds les échanges d'informations d'état et de route seront minimisés, évitant ainsi des messages supplémentaires circulant dans le réseau. En outre, lors d'un changement de route, seuls les nœuds du cœur serviront au calcul,
- Propagation d'état de lien : le routage avec qualité de service est réalisé grâce à la propagation des informations sur les liens stables avec une grande bande passante. L'objectif est d'informer les nœuds distants sur les liens de grande capacité, alors que les liens de faible capacité reste connus au niveau local (les nœuds n'ont pas une information sur la topologie globale du réseau),
- Calcul de route : celui-ci est basé sur la découverte et l'établissement d'un plus court chemin vers la destination satisfaisant la bande passante demandée. Des routes de 'secours' sont utilisées lors de la reconstruction de la route principale, quand cette dernière est perdue. La reconstruction peut être locale (à l'endroit de la cassure), ou à l'initiative de la source.

Au lieu de calculer une route avec un minimum de saut, l'objectif principal de CEDAR est de trouver un chemin stable pour garantir plus de bande passante. Dans ce protocole de routage, les nœuds du cœur du réseau auront plus de trafics à gérer, en plus des messages de contrôle (pour la découverte et la maintenance des routes). En outre, en cas de forte mobilité, la convergence de l'algorithme est difficile à atteindre.

Autres protocoles de routage avec QoS

Ticket-Based QoS Routing [78] est un protocole de routage distribué, qui autorise des informations d'état imprécises durant la phase de calcul de la route. Il permet de réduire la quantité des messages de routage diffusée pour la découverte de la route, en publiant un certain nombre de 'tickets logiques'. Chaque message de découverte (ou d'observation) de route doit avoir au moins un ticket. Quand un message arrive à un nœud, il peut être divisé en plusieurs messages d'observation, qui sont relayés vers les prochains sauts. Chaque message 'fils' contiendra un sous ensemble des tickets de son message 'père'. Evidemment, un message ayant un seul ticket ne peut être divisé. Lors de l'arrivée d'un message de découverte de route à la destination, le chemin saut par saut est connu et les informations de délai ou de bande passante peuvent être utilisées pour effectuer la réservation de ressources pour la route répondant aux besoins de QoS. Le nombre de tickets généré est fonction de la précision des informations d'états disponibles à la source et les besoins de QoS de la communication. Plus de tickets sont publiés dans le but d'augmenter la chance de trouver un chemin désiré.

Dans les réseaux filaires, une distribution de probabilité, selon des informations sur le délai ou la bande passante, peut être calculée. Cependant, cela reste inapproprié dans les réseaux ad hoc où les liens sans fil sont sujets à des cassures, où les informations d'états sont imprécises. Pour cela, un modèle simple a été proposé pour l'algorithme Ticket Based. Il utilise l'historique et l'estimation des variations du délai, et une formule de lissage pour calculer le délai courant. Pour s'adapter aux changements de topologie, l'algorithme autorise différents niveaux de redondance de route. Il utilise aussi des techniques de réparation et de reroutage pour la maintenance des routes. La réparation des routes se fait en utilisant des reconstructions locales.

Un algorithme de calcul et d'allocation de bande passante de bout en bout basé sur la couche TDMA a été proposé dans [79]. Dans ce cas, un nœud source peut déterminer la disponibilité des ressources pour le support des besoins de QoS vers n'importe quelle destination dans le réseau ad hoc. Cette approche est particulièrement utile pour un mécanisme de contrôle d'admission. Il propose une solution basée sur une heuristique pour connaître les slots libres dans les liens tout au long de la route, et d'assigner ces slots à chaque saut.

Contrairement aux autres protocoles avec QoS, qui essayent de trouver un seul chemin entre la source et la destination, [75] a proposé Multipath QoS Routing Protocol, qui permet de trouver plusieurs routes qui fournissent collectivement suffisamment de ressources. Ce protocole adopte aussi l'idée de distribution de tickets (voir section TBPR). Ce type de routage est adapté aux réseaux ad hoc ayant une bande passante limitée, où une seule route avec QoS semble être très difficile à assurer.

Une extension du protocole de routage réactif AODV pour le support de la qualité de service a été proposée dans [80]. Elle consiste à étendre les paquets 'route request' et 'route response' durant la phase de découverte de la route. De plus, les informations suivantes sont ajoutées dans la table de routage : bande passante minimale, délai maximum, et la liste des sources qui ont demandé des garanties de délai ou de bande passante. Si un nœud détecte que la QoS demandée n'est pas satisfaite alors il envoie un message à la source ayant initiée cette demande de QoS, pour l'informer.

[114] propose un algorithme de routage qui prend en compte des métriques et des contraintes du niveau réseau et du niveau application pour mieux répondre aux besoins de qualité de service.

Un autre mécanisme utilisé pour le support de la qualité de service est la réservation de ressources. La section suivante détaille le fonctionnement du protocole de signalisation INSIGNIA [1].

1.2.4 Protocole de réservation de ressources : INSIGNIA

INSIGNIA [1] est un protocole de signalisation spécialement conçu pour les réseaux ad hoc. Il établit une réservation de bande passante orientée flux dans le but de supporter des services temps réel adaptatifs. Il est basé sur un système de signalisation 'In-band', où les messages de contrôle sont encapsulés comme une option dans les paquets de données IP. Ceci permet de réduire l'overhead généré par les messages de signalisation, contrairement à une signalisation out-band explicite (comme RSVP [7] par exemple).

Ce protocole supporte deux types de services (temps réel et best effort). Il offre des algorithmes de réservation, restauration et d'adaptation rapides pour répondre aux changements de topologie du réseau et aux dégradations des liens sans fil. La demande de réservation est effectuée lors de l'envoi du premier paquet de données, et est rafraîchie par le passage des paquets de données. Le destinataire informe périodiquement la source de l'état de la route en envoyant des rapports de QoS (QoS Reporting), qui contiennent des statistiques sur la latence, le taux de perte et le débit. Ces informations peuvent donc servir pour la source à réguler son débit d'émission. Dans un cadre général, et dans le but de fournir des services temps réel adaptatifs, [2] propose un modèle de gestion de flots (flow management model), qui consiste en une architecture de contrôle au niveau IP, permettant d'adapter la session de l'utilisateur au service disponible sans signalisation explicite entre la source et la destination. Il comprend les fonctionnalités suivantes :

- Signalisation in-band (INSIGNIA) se charge d'établir, de terminer, de restaurer et d'adapter les réservations des flots,
- Le module packet forwarding classe les paquets entrants. Les messages de signalisation sont remis à INSIGNIA tandis que les paquets sont, soit passés aux couches supérieures, soit retransmis vers le destinataire,
- Le module *routingprotocol* s'occupe de la mise à jour de la table de routage selon la topologie du réseau et la met à disposition des autres modules,
- Le contrôle d'admission alloue la bande passante aux flots en se basant sur les débits minimal et maximal spécifiés dans la requête et sur l'utilisation, et la capacité du canal. Il décide entre l'acceptation ou le rejet d'un nouveau flot,
- Le module packet scheduling se charge de l'ordonnancement des paquets,
- Le module MAC contrôle l'accès au support en tenant compte de la QoS.

L'un des inconvénients d'une telle approche est le fait d'avoir des informations sur les trafics dans chaque nœud ce qui pose des problèmes de capacité des nœuds, et la difficulté de passage à l'échelle avec l'augmentation du nombre de flux. En outre, cette approche n'offre que deux types de service temps réel et best effort. Finalement, INSIGNIA ne supporte que les applications multimédia adaptatives, et la réservation de ressource ne peut être établie que lorsque le trafic est lancé.

Dans ce qui suit nous allons décrire quelques modèles de qualité de service proposés

pour les réseaux ad hoc. En particulier, les modèles FQMM [4], SWAN [5] et iMAQ [6] seront présentés.

1.2.5 Modèle de qualité de service pour les réseaux ad hoc

Les modèles de qualité de service IntServ/RSVP [7] et DiffServ [8] ont été proposés par l'IETF pour fournir des garanties aux besoins des services temps réel dans les réseaux filaires. D'un côté, l'application du modèle IntServ dans MANET s'avère inadaptée à l'environnement ad hoc. Ceci est justifié du fait que les capacités des nœuds mobiles sont trop variables et limitées pour supporter un traitement complexe et gérer les réservations ainsi que les états des communications en cours. De plus, une réservation dans les réseaux filaires est différente de celle d'un réseau mobile sans fil, car les liens sont partagés, limités, et susceptibles à des variations spatio-temporelles. D'un autre côté, le modèle DiffServ semble le mieux adapté aux réseaux mobiles. Pour résoudre le problème de passage à l'échelle, ce modèle utilise une granularité par classe, où aucune signalisation pour la réservation de ressources n'est utilisée. Cependant, dans ce modèle le cœur du réseau est supposé bien dimensionné, et un administrateur de domaine est nécessaire. Ces deux contraintes restent difficiles à satisfaire.

Flexible quality of service model for MANETs (FQMM)

Le modèle FQMM [4] repose sur une architecture réseau plate (non hiérarchique), constituée d'une cinquantaine de nœuds mobiles, formant un domaine DiffServ. Il combine les propriétés des modèles filaires IntServ et DiffServ, en offrant une méthode d'approvisionnement hybride : par flux, pour les trafics prioritaires, et par classe pour les autres trafics. Dans le réseau, les nœuds peuvent avoir des rôles différents suivant les trafics existants : nœud d'entrée du trafic, intermédiaire ou de sortie. Les nœuds d'entrée permettent de marquer et classifier les paquets, qui seront ensuite relayés par les nœuds intermédiaires suivant leurs PHB (Per Hop Behavior) [121], jusqu'à arriver au nœud destinataire. Ce modèle repose essentiellement sur la couche IP, où les fonctionnalités sont séparées en deux grands plans [3] : le plan relayage de données et le plan contrôle et gestion. Les techniques d'ordonnement et de gestion de mémoires tampons sont étudiées. Dans ce modèle, le protocole de routage est supposé fournir des routes ayant suffisamment de ressources.

L'avantage d'une telle approche est la possibilité d'interfacer le réseau avec l'Internet, vu les mécanismes de qualité de services offerts qui sont proches des protocoles filaires. Cependant, plusieurs mécanismes ainsi que l'interaction avec la couche MAC restent à définir pour s'adapter aux conditions variables du réseau ad hoc.

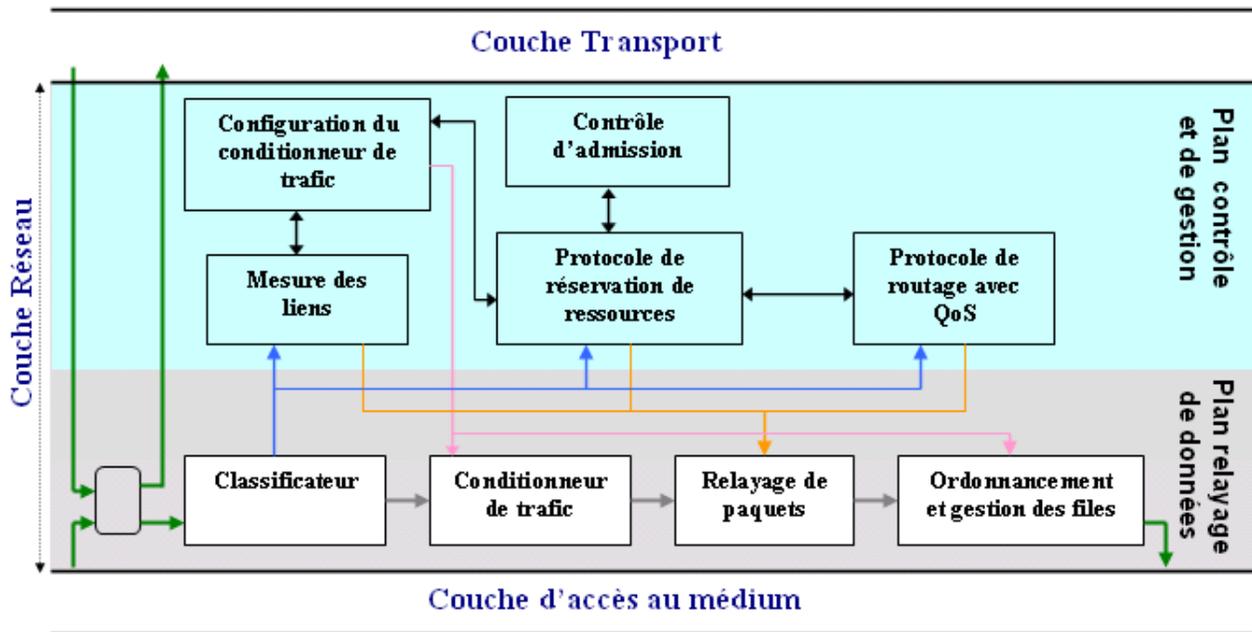


FIG. 1.4 – Le modèle FQMM

Service differentiation in wireless ad hoc networks (SWAN)

SWAN [5] est un modèle réseau sans état basé sur des algorithmes de contrôle distribués dans le but d'assurer une différenciation de services dans les réseaux ad hoc. Il offre la priorité (au niveau paquet) aux trafics temps réel en contrôlant la quantité de trafics best effort acceptée par nœud. Pour accepter un nouveau trafic temps réel, le contrôle d'admission sonde la bande passante minimale disponible sur la route (valide et obtenu par un protocole de routage). Une décision à la source est alors prise suivant la bande passante obtenue. Pour maintenir la qualité de service des trafics déjà acceptés, le débit des trafics best effort est régulé en utilisant les mesures de délais au niveau MAC comme paramètre. Un classificateur et un *shaper* permettent de différencier les deux types de trafic. En cas de congestion, les bits ECN (Explicit Congestion Notification) de l'entête des paquets IP sont positionnés pour permettre à la source de re-initier le contrôle d'admission. Si la route ne dispose pas d'assez de bande passante, le trafic est supprimé. Ainsi, SWAN permet de fournir une QoS logiciel (soft QoS).

Un flux prioritaire admis n'est pas sûr d'avoir des garanties pour l'entière durée de la communication, et peut à tout moment être violé par d'autres demandes de trafics. Un mécanisme de contrôle de débit des flux best effort n'est pas à lui seul suffisant pour offrir des garanties aux applications temps réel. En outre, dans cette approche, le protocole de routage ainsi que la couche d'accès au médium sont de type best effort.

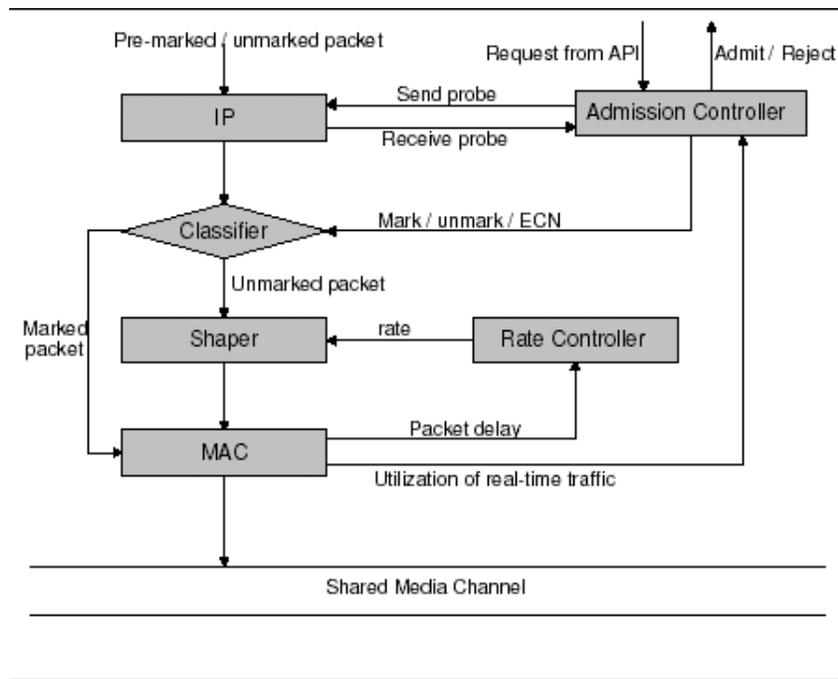


FIG. 1.5 – Le modèle SWAN

Modèle iMAQ

Le modèle iMAQ [6] fournit le support des transmissions des données multimédia dans un MANET. Le modèle inclut une couche ad hoc de routage et une couche de service logiciel (Middleware). Dans chaque nœud, ces deux couches partagent les informations et communiquent afin de fournir les garanties de QoS aux trafics multimédia. Le protocole de routage est basé sur la prédiction de la position des nœuds (predictive location-based) et orienté QoS. La couche Middleware communique également avec la couche application et la couche réseau et essaye de prévoir le partitionnement du réseau. Pour fournir une meilleure accessibilité aux données, il réplique les données entre les différents groupes du réseau avant d'effectuer le partitionnement.

1.2.6 Discussion

Les différentes approches décrites ci-dessus permettent d'offrir des mécanismes de QoS afin d'effectuer une différenciation de services entre les trafics, et une allocation de ressources tout en assurant une utilisation optimale et équitable. Des paramètres comme la mobilité, la capacité du canal sans fil limitée ainsi que la consommation d'énergie ont été explorés.

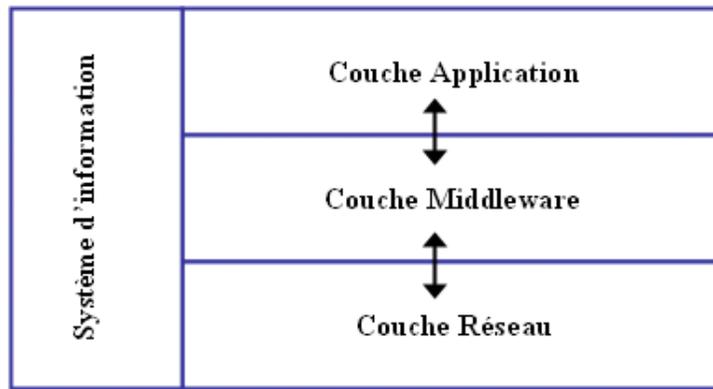


FIG. 1.6 – Le modèle iMAQ

Cependant, quelques contraintes méritent d'être étudiées et prises en compte dans l'élaboration des solutions de QoS. Par exemple, les solutions existantes supposent généralement que les nœuds mobiles d'un réseau ad hoc sont homogènes en terme de capacité de traitement ou de transmission contrairement à ce qu'on constate dans réalité. Il est à noter également que la majorité des solutions existantes se focalisent sur une couche de la pile OSI sans se préoccuper d'autres aspects liés aux autres couches.

En outre, dans les protocoles de routage existants (avec ou sans support de la qualité de service), les nœuds mobiles sont tous considérés comme routeurs, ce qui peut s'avérer inexact dans le cas où un utilisateur mobile décide de ne pas collaborer dans cette tâche et refuse, pour des raisons de batterie ou par simple égoïsme, que cette fonctionnalité soit exécutée par son équipement mobile.

Dans la partie précédente nous avons détaillé les solutions existantes dans la littérature pour fournir la qualité de service dans les réseaux ad hoc. Dans la partie suivante nous nous focalisons sur le contrôle de topologie dans les réseaux mobiles ad hoc.

1.3 Contrôle de topologie dans les réseaux mobiles ad hoc mobiles

1.3.1 Introduction

En raison de la mobilité inhérente dans l'environnement ad hoc, la topologie du réseau joue un rôle principal dans le fonctionnement des protocoles de routage, sur la capacité ainsi que sur la performance du réseau d'une manière générale. Le contrôle de topologie [17] [18] [65] [86] dans les réseaux ad hoc est un domaine de recherche récent. Il vise à maintenir une topologie adéquate en maîtrisant les liens à inclure dans le réseau. Le but est d'atteindre un ensemble d'objectifs comme : réduire les interférences, réduire la consommation d'énergie, ou augmenter la capacité efficace de réseau.

Vues les capacités limitées des équipements mobiles en terme de batterie, les premiers travaux pour le contrôle de topologie dans les réseaux ad hoc utilisent la consommation d'énergie comme métrique, et sont basés sur l'ajustement de la puissance de transmission des nœuds. Ces techniques de contrôle peuvent être centralisées ou distribuées. Dans les algorithmes de contrôle de topologie centralisés [17] [58], une entité centrale calcule la puissance de transmission en utilisant la position des nœuds du réseau afin de réaliser une topologie avec une forte connectivité. Dans les algorithmes distribués [18] [63], les nœuds mobiles ajustent leur puissance de transmission suivant des informations locales pour maintenir un nombre défini de voisins.

Une autre approche pour contrôler la topologie du réseau ad hoc est basée sur l'utilisation d'un sous-ensemble des nœuds de réseau pour servir de 'Cluster Head' (super nœud) dotés de fonctionnalités additionnelles [15] [57]. Cette approche, souvent appelée 'Cluster Based Protocol', qui consiste à élire un ensemble de cluster-heads, où chaque nœud mobile est associé à un cluster-head. L'élection permet de réduire la maintenance de la topologie dans les réseaux ad hoc. Cependant, elle a un impact négatif sur les cluster-heads, parce que ces derniers consomment leur énergie plus rapidement qu'un nœud classique. Une solution est de considérer l'équilibrage des charges dans l'algorithme d'élection. Le but d'une telle approche est de réduire la surcharge additionnelle du réseau et complexité de la maintenance, et de simplifier des fonctions essentielles comme : le routage, le contrôle de puissance, la sécurité, . . .etc.

En outre, des solutions pour la couverture et le déploiement des réseaux de senseurs ont été étudiées pour gérer la topologie des réseaux dans ce contexte.

Dans la suite de cette partie, nous nous intéressons aux approches de contrôle de topologie existantes, qu'elles soient orientées énergie ou QoS. Puis, nous décrivons le principe de fonctionnement des techniques orientées clusters. Ensuite, le problème de déploiement dans les réseaux de senseurs est traité. Une sélection des solutions proposées

dans la littérature est présentée pour chaque approche.

1.3.2 Contrôle de topologie basé sur la puissance de transmission

Dans ces techniques, le contrôle de topologie est défini comme le problème d'assigner les puissances de transmission aux différents nœuds du réseau afin que la topologie du réseau atteigne certaines propriétés de connectivité et que la consommation d'énergie des nœuds soit optimisée.

On distingue deux catégories de contrôle de topologie : centralisées et distribuées. Dans les techniques centralisées, toutes les positions des nœuds sont supposées connues par une entité centralisée qui calcule leur puissance de transmission. Cependant, ces algorithmes sont confrontés au problème du passage à l'échelle quand le nombre de nœuds dans le réseau augmente où une grande quantité d'information doit être collectée et remontée à la station centrale. Les algorithmes distribués sont quant à eux scalables et adaptés à la mobilité des nœuds, vu que seules des informations locales suffisent pour calculer la puissance appropriée.

Un des premiers travaux sur le contrôle de topologie dans les réseaux multi sauts peuvent être trouvés dans [65] [85]. Dans [65], Hou et al ont étudié le rapport entre la portée de transmission et le débit. Un modèle analytique a été développé pour permettre à chaque nœud d'ajuster sa puissance de transmission, de réduire l'interférence et par conséquent de réaliser un débit élevé. Dans [85], un algorithme distribué a été développé pour que chaque nœud ajuste sa puissance de transmission et construise une topologie fiable avec un haut débit. La réduction de la consommation d'énergie n'était pas étudiée dans ces deux travaux. Dans la suite de cette section nous décrivons quelques algorithmes basés sur la puissance de transmission.

[17] décrit deux algorithmes centralisés dont la topologie induite est 1 – *connected* ou 2 – *connected*, respectivement, où le critère d'optimisation est MINMAX. C'est à dire, réduire au minimum la puissance maximum utilisée par n'importe quel nœud. En plus, deux heuristiques distribuées ont été proposées, à savoir : LINT (Local Information No Topology) et LILT (Local Information Link-state Topology), pour ajuster de manière adaptative la puissance de transmission des nœuds afin maintenir une topologie connectée en réponse aux changements de topologie. Mais, ni LINT ni LILT ne peuvent garantir la connectivité du réseau. Ce travail est généralisé dans [58] dans le but prouver que, si la propriété désirée de topologie est 'monotone', et si le but d'optimisation est MINMAX, alors la détermination de puissance peut être calculée dans un temps polynomial. Ici, une propriété est 'monotone' si elle est toujours la même lorsqu'un nœud augmente sa puissance de transmission. Une étude générale est également présentée dans [58] pour des algorithmes d'approximation quand l'objectif est MINTOTAL et la propriété est monotone. Notant que la minimisation de la puissance totale est un problème NP-complet,

même pour la propriété de 1-connected [87].

Une méthode distribuée basée cône a été développée dans [18]. Chaque nœud augmente graduellement sa puissance de transmission jusqu'à ce qu'il trouve un nœud voisin dans chaque direction, formant ainsi un cône. Par conséquent, la connectivité globale est garantie avec la puissance minimum pour chaque nœud. Huang et al ont étendu ce travail au cas où des antennes directionnelles sont utilisées [88]. Marsan et al ont présenté une méthode dans [89] pour optimiser la topologie d'un réseau Bluetooth, qui vise à réduire la charge de trafics maximum des nœuds, réduisant de ce fait au minimum la puissance maximale des nœuds.

Singh et al ont étudié cinq métriques différentes pour un routage efficace [90], comme la réduction d'énergie consommée par un paquet, la réduction de la variance du niveau de consommation d'énergie des nœuds, la minimisation du coût par paquet et ainsi de suite. Kawadia et al ont proposé une méthode de clustering pour un routage dans les réseaux non homogènes [91], où des nœuds sont distribués dans les clusters. Le but est de choisir le niveau de puissance de transmission, de sorte que des niveaux de puissance bas puissent être employés pour des communications intra-cluster et des puissances élevées pour celles inter-cluster. Dans [92], Wieselthier et al ont étudié le problème d'ajustement de la puissance d'énergie de chaque nœud tel que le coût en énergie de l'arbre de broadcast/multicast soit réduit au minimum.

Dans [22] un mécanisme de contrôle de topologie orienté QoS est proposé. Il permet de satisfaire les besoins de qualité de service en minimisant la puissance de transmission maximale des nœuds mobiles. Les paramètres de δ étudiés sont le délai (en terme de nombre de sauts) et le taux d'acheminement des paquets. Dans ce cas, les demandes d'applications temps réel peuvent être assurées et la durée de vie du réseau prolongée. Dans cette étude deux cas sont considérés :

- les paquets d'un trafic peuvent être acheminés à travers plusieurs routes
- les paquets d'un trafic doivent emprunter la même route de la source à la destination

Dans le premier cas, le problème est formulé comme un problème de programmation linéaire mixte en tenant compte de la bande passante seulement. Dans le deuxième, il est aussi formulé comme un problème de programmation linéaire mixte où le délai de bout en bout et la bande passante sont considérés.

1.3.3 Techniques de Clustering

Dans les réseaux filaires, Kleinrock et Kamoun [93] ont étudié une approche de routage hiérarchique dans le but de réduire la taille de la table de routage dont la taille est fonction de la structure de clustering utilisé. Dans les réseaux mobiles ad hoc Linked Cluster Architecture (LCA) [94] est un des premiers travaux sur le clustering dans ce type de réseau. Gerla et son équipe ont développé plusieurs protocoles de clustering [95]

[96] [97] [98]. Dans ces approches, le clustering consiste à classer les nœuds du réseau d'une manière hiérarchique en classes équivalentes suivant certains paramètres : adresse, zone géographique, . . .etc.

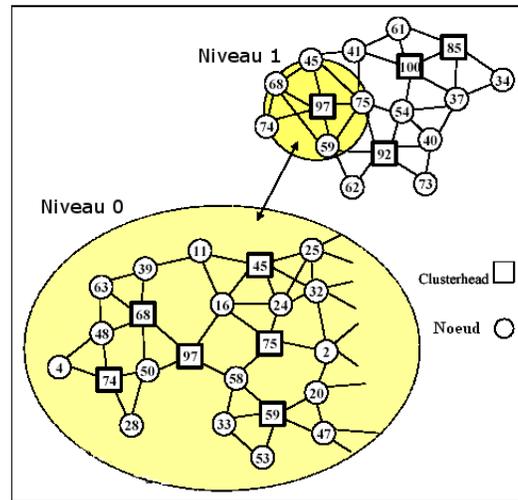


FIG. 1.7 – Méthode de clustering dans les réseaux ad hoc

Un sous ensemble de nœuds est élu, d'une manière complètement distribuée, pour jouer le rôle de d'un coordinateur local. Les Cluster-heads peuvent être utilisés pour :

- contrôler l'ordonnancement du canal,
- contrôler la consommation d'énergie,
- maintenir la synchronisation des trames,
- améliorer la réutilisation des codes et du temps,
- ainsi que pour servir de diffuseur régional.

La détermination de la taille d'un cluster est une tâche difficile, car elle est fonction de la réutilisation du canal, de la puissance de transmission des nœuds, des interférences et suivant les aspects géographiques. Un des buts du clustering est la maintenance des informations de la topologie du réseau et la réduction de l'overhead généré par la découverte de route, la réduction de la consommation d'énergie et l'amélioration de la bande passante du réseau (capacité des liens sans fil).

Un algorithme de clustering est basé sur les étapes suivantes :

Formation (élection) des cluster-heads : le réseau est ainsi divisé en plusieurs clusters, La phase d'élection ou de 'cluster set up phase' utilise des heuristiques comme le plus grand/plus petit ID dans le voisinage, le degré de connectivité, la zone géographique, la puissance de transmission ou la vitesse de déplacement (ex : utiliser les nœuds les moins mobiles), ou bien en utilisant un poids pour chaque nœud qui représente une combinaison des derniers attributs,

Communication entre les cluster-heads : dans un cluster, chaque deux nœuds sont à 2 sauts de distance entre eux. De plus, comme les cluster-heads ne sont pas directe-

ment reliés, des nœuds passerelles sont aussi élus et utilisés pour les communications entre cluster-heads,

maintenance des cluster-heads : dans le but de s'adapter aux changements de topologie fréquents dans le réseau, une mise à jour des cluster heads élus est dynamiquement réalisée.

Ci-dessous un exemple d'algorithme de clustering basé sur le plus petit ID (utilisé dans Adaptive Clustering for Mobile Wireless Networks, de Chunhung Richard Lin et Mario Gerla)

T : l'ensemble des ID des voisins à un saut et ID du nœud courant

```

{
  si (my_id ==min(T)){
    my_cid = my_id ;
    diffuser cluster(my_id, my_cid) ;
    T= T - {my_id};
  }

  for (;;){
    à la réception du cluster(id,cid){
      mettre le cluster ID du noeud id à cid;
      si(id ==cid ET my_cid==UNKNOWN OU my_cid > cid) my_cid = cid;
      T = T - {id};
      si (my_id==min(T)){
        si(my_cid== UNKNOWN) my_cid=my_id;
        diffuser cluster(my_id, my_cid);
        T=T - {my_id};
      }
    }
    si ( T==vide) stop;
  }
}

```

Clustering multi niveau (hiérarchique)

Le clustering hiérarchique adopte le même principe en assignant dynamiquement des Cluster ID avec plusieurs niveaux de clustering. Un cluster peut dynamiquement se fusionner ou s'éclater en fonction du nombre de nœuds dans un cluster. Cependant, vu la difficulté de prévoir le temps nécessaire pour propager les messages de contrôle de clustering à travers les nœuds, et le grand temps de convergence de l'algorithme de clustering, ce

type d'approche dégrade rapidement les performances du réseau, vu le trafic additionnel nécessaire pour la maintenance des informations de topologie. Ajoutons à cela la difficulté et la complexité d'implémentation dans un cas réel.

Quelques approches de clustering

Dans le protocole CGSR (Cluster-head Gateway Switch Routing) [99], les paquets sont routés alternativement entre les leaders des clusters et les passerelles. Les auteurs de ce protocole ont défini des extensions qui peuvent être ajoutées, telles que l'ordonnancement des codes, le contrôle d'accès radio et la réservation du canal. De plus, ils définissent l'algorithme LCC (Least Cluster Change), qui est conçu pour réduire le nombre de changements de cluster heads dans le réseau.

Le protocole Landmark Routing [102] permet de construire une topologie hiérarchique basée sur des Landmarks. Un landmark est un routeur dont la position est connue par les nœuds voisins (jusqu'à un certain rayon). Une hiérarchie de ces landmarks est construite en augmentant leur portée de transmission. Les nœuds ont des adresses hiérarchiques basées sur le landmark avec qui ils sont connectés. Quand un paquet est envoyé d'un nœud source à un nœud destination, il est envoyé au plus bas niveau de la hiérarchie avec lequel les deux nœuds sont associés. A l'approche du paquet de la destination, la granularité des informations du routage de cette destination s'améliore, et ainsi le paquet peut être exactement acheminé à la destination.

Dans [103], les auteurs ont proposé un schéma de clustering avec une taille de cluster entre k et $2k-1$ nœuds. Cet algorithme distribué commence par créer un arbre couvrant le réseau entier. La formation de clusters est de bas en haut, où les sous arbres sont regroupés en clusters qui répondent aux besoins de taille.

Récemment, une architecture basée sur un backbone mobile a été proposée dans [61] [62]. Un protocole pour maintenir le backbone stable (MBNP) a été développé. Il utilise un mécanisme d'élection des BNs (Backbone Node) parmi les BCNs (Backbone Capable Node) et de reconvertir les BNs en BCNs à nouveau, dans le but de réduire le nombre de BN actifs pour optimiser les ressources et l'énergie. La conversion de BCNs en BNs est utilisée pour construire le cœur du réseau et fournir une connectivité désirée. On distingue deux types de nœuds mobiles : les nœuds réguliers qui disposent d'une capacité de communication et de traitement limitée ; et les nœuds BCNs, à partir desquels les BNs sont élus, et qui ont des ressources importantes et utilisent plusieurs modules radio. Les BNs sont élus afin d'assurer des objectifs de qualité de service.

Une approche plus récente de clustering hiérarchique est le système MMWN (Multihop Mobile Wireless Networks [104]). Le système divise les nœuds en commutateurs (switchs) et nœuds finaux, où seulement les switchs peuvent servir de routeur de paquets. Un réseau

ad hoc est un cas spécial où tous les nœuds sont des commutateurs. Chaque point final est associé à exactement un commutateur, et les commutateurs sont groupés ensemble pour former des clusters. L'approche MMWN exige de tous les clusters d'être disjoints. Les fusions des clusters se produisent quand le nombre de commutateurs dans un cluster tombe au-dessous d'un certain seuil, N_{merge} . De même, les décompositions des clusters se produisent quand le nombre de commutateurs devient plus grand que le seuil, N_{split} .

La section suivante illustre quelques exemples de déploiements de réseaux de senseurs qui permettent d'atteindre des topologies spécifiques répondant à des critères de couverture.

1.3.4 Déploiement des réseaux de senseurs

Les problèmes de couverture maximale surgissent dans une variété d'applications pratiques dans de nombreux domaines, qui demandent de savoir construire et traiter de manière efficace des objets de nature géométrique. Citons, parmi d'autres, la robotique, la vision par ordinateur, l'informatique graphique, l'imagerie médicale, la réalité virtuelle et la conception assistée par ordinateur. Dans [11], ils proposent une méthode heuristique pour résoudre le problème maximum de couverture, appelée 'greedy randomized adaptive search procedure'. La qualité de la solution est mesurée en utilisant une borne supérieure obtenue par la résolution d'un problème de programmation linéaire. Le problème de couverture et de déploiement ont été également étudiés récemment dans le contexte des réseaux de senseurs [13] [20]. Une couverture déterministe peut être obtenue quand un réseau statique doit être déployé dans un secteur prédéfini. [105] est un des premiers travaux à identifier l'importance de géométrie combinatoire et les diagrammes de Voronoi pour la couverture des réseaux de senseurs.

Le déploiement des senseurs ressemble au problème de la galerie d'art [12], qui consiste à déterminer le nombre d'observateur nécessaires pour couvrir une salle de galerie d'art de telle sorte que chaque point soit visible par au moins un observateur. Ce problème a été résolu d'une manière optimale dans un espace 2D, et a été défini comme problème NP-complet dans le cas du 3D. Un placement basé grille des senseurs pour une surveillance efficace [13]. Les senseurs sont placés aux points de grille tels que chaque point de grille est couvert par un sous-ensemble unique de ces senseurs. Le problème de placement a été formulé en termes de minimisation de coût sous les contraintes de couverture. Ceci est développé en un modèle de programmation entière (ILP) pour résoudre le problème de déploiement. Une approche 'diviser pour régner' a été également utilisée pour résoudre les grandes configurations (nombre de points de grille > 50), où le modèle en ILP nécessite un grand temps d'exécution.

[20] a proposé un algorithme polynomial optimal pour résoudre la meilleure couverture. Cet algorithme est basé sur une combinaison des techniques de la géométrie combinatoire

et de la théorie des graphes, particulièrement les algorithmes de recherche de graphe et le diagramme de Voronoi [122].

1.4 Discussion et conclusion

Dans la partie précédente -Contrôle de topologie- nous avons exposé les différents travaux traitant le contrôle de topologie dans les réseaux ad hoc. Cela revient à contrôler un ensemble de paramètres, comme la puissance de transmission par exemple, pour aboutir à une topologie désirée. Une autre solution consiste à regrouper les nœuds mobiles en clusters, gérés par des cluster-heads. Le problème du déploiement dans les réseaux de senseurs a été traité.

Comme pour les protocoles de routage, les travaux basés sur les clusters supposent que tous les nœuds dans le réseau sont considérés comme homogènes. Néanmoins, les cluster heads n'ont pas de matériels ou de capacité de traitement spécifique. Dans le cas où des fonctionnalités (coûteuses en termes de ressources et de batterie) sont implémentées dans les cluster heads, ces derniers peuvent vite devenir des goulets d'étranglement. Parallèlement, dans la phase de reconstruction des clusters, un overhead de communications et de calculs est généré. De plus, quand le degré du nœud est pris comme paramètre dans l'algorithme de clustering, lors du changement de topologie les cluster-heads ont tendance à changer et ne pas rester stables. D'un autre côté, quand le ID le plus petit est utilisé, les nœuds ayant des petits ID auront plus de chance à demeurer des cluster heads pour une longue durée, ce qui entraîne une baisse de batterie importante.

Dans notre thèse (chapitre 4) nous nous intéressons au principe du contrôle de topologie à partir d'un point de vue différent en se basant particulièrement sur une représentation hiérarchique du réseau mobile ad hoc et en tenant compte de l'hétérogénéité des nœuds mobiles. Un ensemble de routeurs dédiés déplaçables est utilisé dans le but de contrôler la topologie du réseau et d'offrir un cœur de réseau stable.

Dans le chapitre suivant nous allons d'abord présenter notre proposition de routage à différenciation de terminaux dans les réseaux ad hoc.

Chapitre 2

Routage avec différenciation de terminaux

2.1 Introduction

Dans les réseaux mobiles ad hoc où les nœuds ne sont pas tous voisins directs, les nœuds intermédiaires servent de relais afin d'acheminer les données d'une source à une destination. Le calcul de la route est réalisé grâce à un protocole de routage. Le critère de choix de la route, le plus communément utilisé, est le nombre de sauts. Bien que facile à calculer, cela peut influencer sur les performances du réseau. En effet, l'utilisation d'un algorithme de routage à sauts minimum implique que les routes les plus courtes soient fréquemment sollicitées, conduisant à des congestions, particulièrement dans les réseaux sans fil ayant une bande passante déjà limitée.

Par ailleurs, les terminaux mobiles existant sur le marché sont de plus en plus hétérogènes, c'est à dire, composés de différents types d'équipements avec différentes capacités de transmission et de traitement. Aussi, un protocole de routage efficace doit prendre en considération ce critère dans la sélection des routes.

En plus de l'hétérogénéité des capacités de transmission des nœuds dans le réseau, un point important à prendre en considération est la propriété 'multidébits' des cartes sans fil. Le débit offert par ces cartes est fonction de la distance (portée de transmission) et des interférences. Par conséquent, les communications à longues distances ont des débits faibles, contrairement à celles à portées réduites. Cette propriété fournit une meilleure flexibilité, certes, mais ne garantit pas un haut débit et une longue distance de communication simultanément.

Nous présentons dans ce chapitre une proposition d'un protocole de routage avec

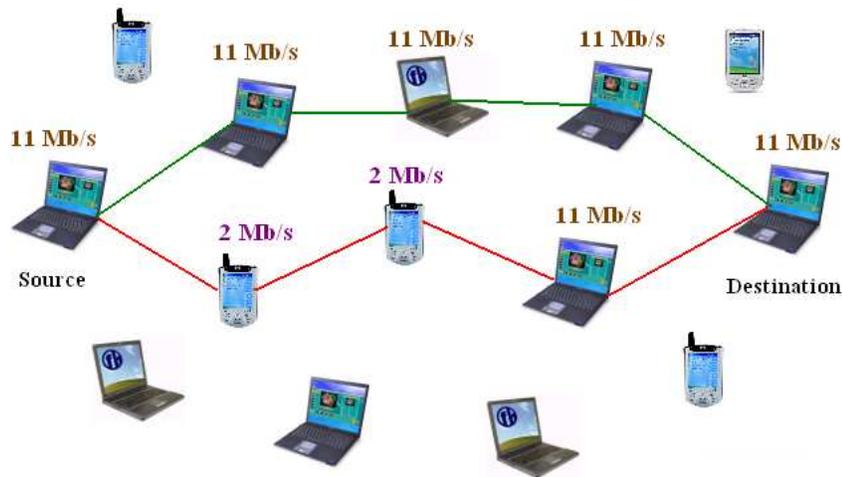


FIG. 2.1 – Hétérogénéité des nœuds dans les réseaux ad hoc

différenciation de terminaux qui prend en compte l'hétérogénéité des nœuds mobiles. La section 2 illustre les problèmes liés aux protocoles de routage classiques. Dans les sections 3 et 4 nous allons respectivement décrire le principe de fonctionnement ainsi que les modifications à apporter dans le protocole de routage DSR afin de supporter la différenciation de terminaux. A l'aide de simulations, une évaluation des performances de notre approche sera présentée dans la section 5.

2.2 Exposition des problèmes

Capacité des routes

En réseaux sans fil hétérogènes supportant des équipements de transmission différents, le choix des routes ayant le minimum de sauts a typiquement comme conséquence des chemins où les liens fonctionnent à bas débit. En effet, un minimum de nœuds intermédiaires entre la source et la destination, correspond à l'existence de liens plus longs pour couvrir la même distance. Sachant que la distance entre les nœuds est l'un des facteurs qui influence sur la qualité du canal, les liens longs ont une mauvaise qualité, et fonctionnent ainsi à bas débits (voir les figures 2.2 2.3 obtenues à partir de mesures réelles effectuées dans notre département [126]). Non seulement les liens à bas débits produisent une mauvaise route pour les communications qu'ils transportent, mais affectent également les flux avoisinants car le canal sans fil est partagé. En effet, un lien long signifie que la vitesse de transmission

des paquets est lente, ce qui implique que tous les nœuds dans la portée d'interférence de la transmission doivent reporter leurs communications pour une durée plus longue. Par conséquent, les transmissions lentes réduisent le débit global du réseau [36].

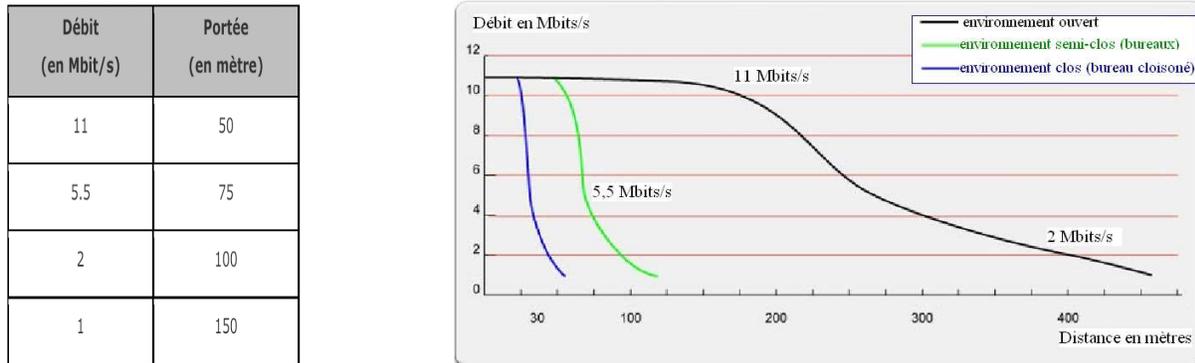


FIG. 2.2 – Variations de la capacité du lien en fonction de la distance

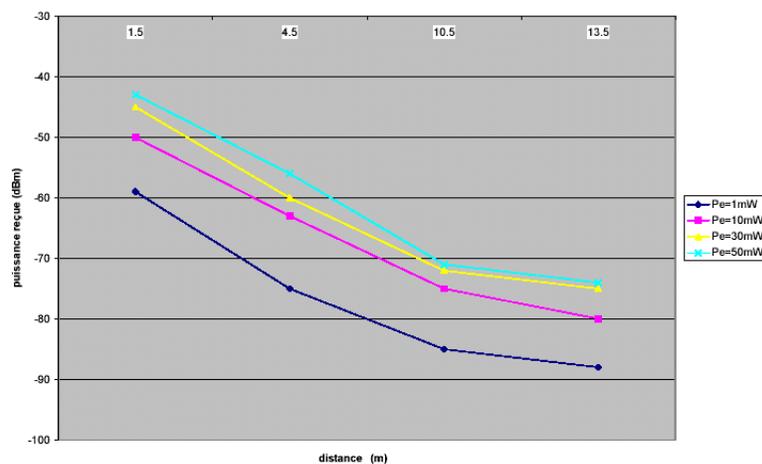


FIG. 2.3 – Puissance reçue en fonction de la distance dans un milieu avec obstacles, pour différentes puissances d'émission P_e

Connectivité

Les liens de communications fournis par un protocole de routage du plus court chemin étant distants, ils sont plus susceptibles à des coupures suite la mobilité des nœuds (même en cas de petits déplacements). Ces liens sont ainsi plus vulnérables aux pertes, générant des changements de routes fréquents, ce qui implique une détérioration des communications en cours et une charge de contrôle additionnelle dans le réseau.

Le débit du lien sans fil se dégrade de 11 à 5.5, 2 ou même 1Mb/s, lors d'une transmission de trame non réussie, provoquant ainsi une dégradation de performance. Cette dégradation n'est pas juste liée au nœud utilisant un débit réduit, mais aussi à tous les nœuds voisins (à l'intérieur de sa zone de transmission). Ceci est lié à la méthode d'accès au médium (CSMA/CA dans le DCF de IEEE 802.11) qui offre une probabilité d'accès au médium équitable entre tous les nœuds. De cette manière, lorsqu'un nœud monopolise le médium pour une longue période à cause de son faible débit, il pénalise les autres terminaux utilisant un débit supérieur [36].

Un nœud qui est déjà loin de la source, et qui va devenir hors de sa portée de transmission dans un délai réduit, générera les mécanismes de découverte de route, consommant ainsi plus de ressources réseau déjà limitées.

Routes avec moins de sauts	Routes avec plus de sauts
Liens avec une grande distance	Débit bas au niveau de chaque saut
Moins de nœuds voisins interférents	Courte distance des liens
Débit élevé au niveau de chaque saut	Plus de nœuds voisins interférents

TAB. 2.1 – Longueur de route

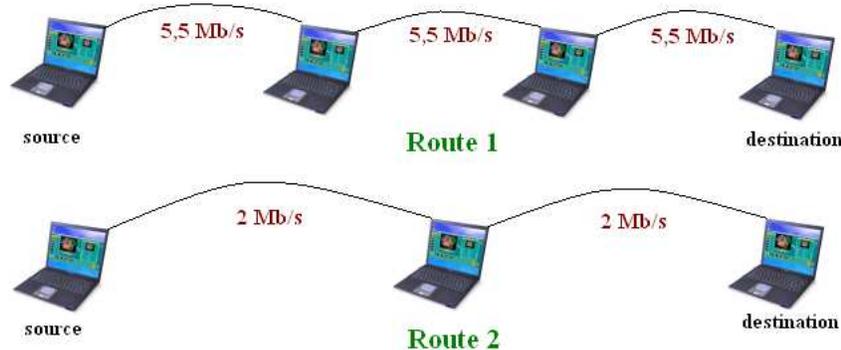


FIG. 2.4 – Nombre de sauts Vs débit des liens

Terminaux mobiles collaboratifs

Une des hypothèses de tous les protocoles de routage dans les réseaux ad hoc est que les nœuds mobiles sont à la fois terminaux et routeurs. Dans de tels protocoles de routage un nœud n'est pas supposé refuser d'effectuer la fonction de relayage, car tous les nœuds sont obligés d'être collaboratifs. Par ailleurs, quand un terminal joue le rôle de routeur, il subit une dégradation de batterie et une charge de traitement additionnelle.

2.3 Notre proposition

Notre étude considère un réseau ad hoc hétérogène, composé de stations mobiles ayant différentes capacités de transmission, et hiérarchique. Nous considérons deux types de nœuds :

les routeurs : ce sont les nœuds qui ont pour tâche de relayer les paquets,

les terminaux : tels que les PDA, portables, ...etc. qui sont généralement dotés de faible batterie, et pas dédiés pour le relayage des données.

Afin de pallier les problèmes cités, nous proposons un routage basé sur le choix des nœuds dotés d'un haut débit pour offrir une meilleure qualité de lien dans le réseau ad hoc. Ce choix a comme conséquence la stabilité des liens sans fil, qui représente une condition indispensable pour un support de la qualité de service, comme nous allons le voir dans les prochaines sections.

Il arrive qu'une route optimale en terme de nombre de sauts dégrade la capacité du lien du réseau ou des nœuds voisins, à ce moment là, une route plus longue offrant une bonne qualité de lien (consomme plus de ressources), elle apporte en contre partie une bande passante stable et meilleure pour le réseau ad hoc. De plus, notre proposition utilise principalement des équipements dédiés au routage (et qui possèdent un CPU relativement puissant). Le délai d'un paquet n'est donc pas pénalisé par le fait que l'on traverse des routeurs (type PDA) à faible capacité.

2.3.1 Principe

Pour pouvoir supporter la différenciation de terminaux, l'idée du protocole revient à faire de légères et simples modifications dans les protocoles de routage existants. Il suffit pour cela :

- Avoir la possibilité de distinguer plusieurs types de nœuds mobiles : nœuds avec une basse ou haute capacité de transmission ; ou bien entre les nœuds désirant ou refusant de supporter la fonction de routage). Une information additionnelle est alors nécessaire pour spécifier le type du nœud,
- Adapter le mécanisme de sélection de routes afin de choisir les chemins les plus courts mais aussi contenant le plus de nœuds à haut débit.

Ainsi ces modifications n'altèrent pas le fonctionnement des protocoles de routage qu'ils soient proactifs ou réactifs.

2.3.2 Extension du protocole DSR pour la différenciation de terminaux

Comme les protocoles de routage qui utilisent une découverte de route à la demande, DSR est basé sur un système de cache pour les routes, pour ne pas faire une demande de découverte de route pour les paquets suivants qu'il souhaite transmettre. Les informations du cache sont aussi utilisées pour répondre à des demandes de découverte de routes d'autres nœuds. Le système de cache est alimenté par les messages de demande de route du nœud lui-même ou des messages reçus des nœuds voisins.

Le protocole DSR n'intègre pas l'opération de découverte de routes avec celle de la maintenance, comme le font les protocoles de routage conventionnels. Quand un nœud détecte un problème de transmission, un message erreur de route est envoyé à l'émetteur original du paquet. Le message d'erreur contient l'adresse du nœud qui a détecté l'erreur et celle du nœud qui le suit dans le chemin. Lors de la réception du paquet erreur de route par l'hôte source, tous les chemins qui contiennent ce nœud sont supprimés. Ensuite, une nouvelle opération de découverte de routes vers la destination est initiée par l'émetteur.

Simplicité de l'extension

Une des raisons pour lesquelles DSR a été testé est le fait qu'il offre la possibilité d'avoir plusieurs routes dans son cache et que seules : l'ajout des types de nœuds ainsi que la modification de la procédure de sélection de route, sont nécessaires pour arriver à montrer l'intérêt de la différenciation de terminaux. Dans ce cas, aucun ajout de nouveaux messages, ou modification dans le fonctionnement du protocole lui-même ne sont effectués.

2.3.3 La phase de découverte de routes

InitiatorID : L'adresse de la source,
TargetID : L'adresse de la destination,
UniqueRequestID : Identificateur unique du message,
(Address, TYPE)List : Liste des nœuds intermédiaires (adresse et TYPE) avant la destination, *TYPE* représente la capacité de transmission du nœud (haut débit ou bas débit : 0 ou 1),
HopLimit : Nombre maximum de sauts autorisé,
NetworkInterfaceList : Dans le cas où les nœuds disposent de plusieurs interfaces,
Acknowledgementbit : Utilisé comme option pour que la destination envoie un message d'acquiescement une fois un paquet est reçu.

Les messages DSR Source Route et Route Reply sont aussi modifiés en ajoutant le

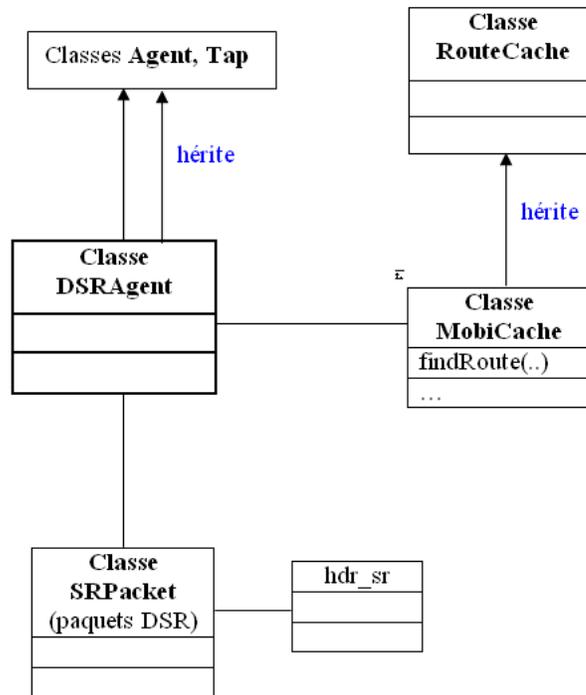


FIG. 2.5 – Principales classes utilisées dans l'implémentation NS-2 du protocole DSR

Les champs	Explication
Initiator ID	L'adresse de la source
Target ID	L'adresse de la destination
Unique Request ID	Identificateur unique du message
(Address, <i>TYPE</i>) List	Liste des nœuds intermédiaires (adresse et <i>TYPE</i>) avant la destination. <i>TYPE</i> représente la capacité de transmission du nœud (haut débit ou bas débit : 0 ou 1)
Hop Limit	Nombre maximum de sauts autorisé
Network Interface List	Dans le cas où les nœuds disposent de plusieurs interfaces
Acknowledgement bit	Utilisé comme option pour que la destination envoie un message d'acquiescement une fois un paquet est reçu

FIG. 2.6 – Extension de la structure du message Route_Request

type de nœud dans le champ 'Address'.

Avant d'envoyer un paquet, DSR cherche dans son cache route l'existence d'une route vers la destination désirée. Si aucune route n'est trouvée, la source initie une phase de découverte de route en envoyant (en diffusion à ses voisins) un message ROUTE_REQUEST pour trouver une route. Quant un nœud reçoit un message ROUTE_REQUEST, il vérifie s'il est la destination du message. Sinon, il vérifie l'existence de route vers cette destination dans son cache de route. Si aucune route n'est trouvée, il ajoute son adresse ainsi que son type dans le message ROUTE_REQUEST et le diffuse à son tour aux nœuds voisins. Si le message arrive à destination et qu'une route inverse existe dans le cache route du nœud destinataire, un message ROUTE_REPLY (contenant une copie de la route accumulée dans le message ROUTE_REQUEST) est envoyé vers la source.

La liste de routes existante dans le cache des nœuds mobiles tient en compte le type du nœud appartenant à une route. Dans ce cas, pour chaque adresse de nœud est associé un type qui lui correspond.

2.3.4 La phase de la sélection de la route

Une fois que le nœud dispose des routes existantes vers une destination précise, il effectue une phase de sélection de route. Cette phase dans le protocole DSR classique consiste à choisir le chemin le plus court en évitant de passer par des liens externes (des nœuds faisant partie d'un réseau externe au réseau ad hoc DSR). Notre approche consiste à améliorer ce critère de sélection dans le but de choisir des routes avec des liens de bonne qualité. Ainsi, il sélectionne les plus courts chemins dotés de plus de liens de haut débit.

Le reste du chapitre présente les simulations réalisées avec l'outil de simulation NS-2 [34] pour évaluer les performances du protocole de routage avec différenciation de terminaux. Pour ce faire nous présentons d'abord les métriques ainsi que le modèle de simulation utilisés pour évaluer les performances.

2.4 Simulations et analyse des performances

Cette section couvre l'étude des performances du protocole de routage DSR modifié supportant la différenciation de terminaux. Il s'agit de simuler les protocoles DSR original et DSR modifié dans les réseaux ad hoc et de comparer les résultats obtenus. Pour cela une série de simulations sous différents scénarios est réalisée en utilisant l'outil de simulation NS-2 [34]. L'outil NS-2 ainsi que les intervalles de confiance sont discutés dans l'annexe. Pour le protocole DSR modifié, notre implémentation consiste à modifier le format des entêtes des paquets DSR ainsi que la méthode de sélection de routes dans le cache de

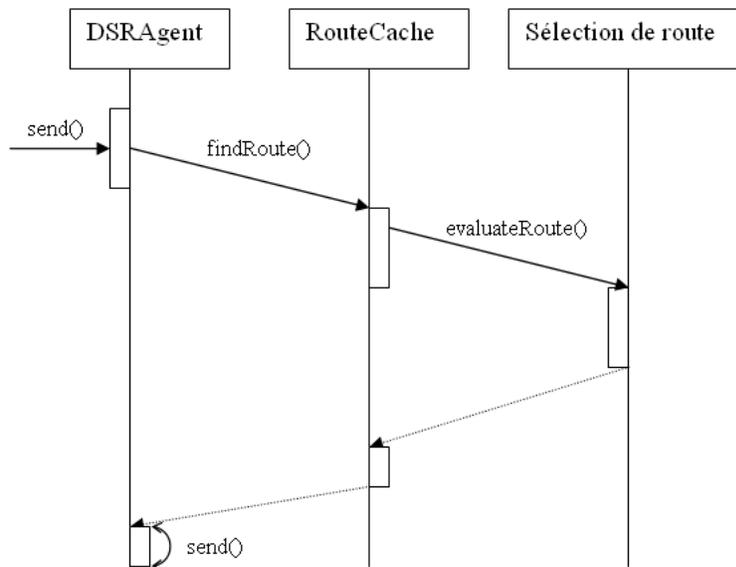


FIG. 2.7 – Diagramme de séquence représentant la sélection de routes

routes.

Un champ représentant la capacité de transmission du nœud est ajouté dans la structure du nœud mobile afin de définir le type et la capacité de transmission du nœud.

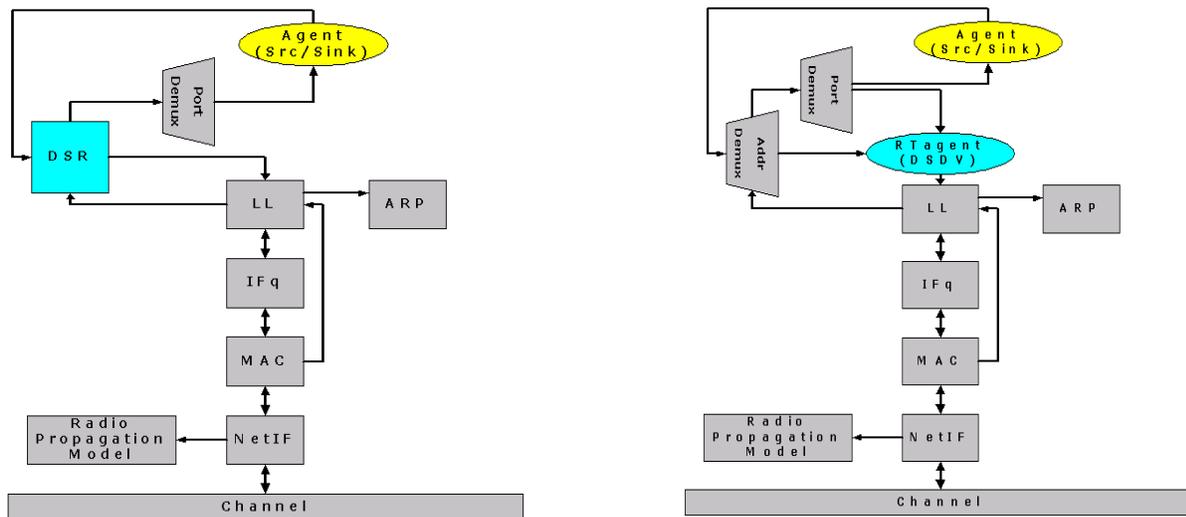


FIG. 2.8 – La structure du nœud mobile dans NS-2 en utilisant le protocole DSR ou un autre protocole (DSDV)

Pour mesurer les performances de l'extension proposée de DSR, des paramètres comme le débit, le délai bout en bout ainsi que le taux de perte sont étudiés. En outre, une comparaison avec les performances du protocole DSR classique est effectuée dans différentes conditions de mobilité et de trafics utilisés.

2.4.1 Modèle de simulation

Les principaux paramètres utilisés dans le modèle de simulation sont listés dans le tableau suivant :

Paramètre	valeur
Couche MAC	IEEE 802.11
Portée de transmission	250 mètres
Nombre de nœuds mobiles	50
Surface de simulation	$1000 \times 1000m^2$
Durée de la simulation	300 secondes
Nombre de trafics utilisés	25
Taille des paquets	1000 octets
modèle de mobilité	random-waypoint
modèle de propagation	two-ray ground

TAB. 2.2 – Paramètres utilisés dans le modèle de simulation

D'autres paramètres sont variables : nombre de sources de trafics, vitesse de déplacement des nœuds, et ce dans le but d'avoir des scénarios de trafics et de mobilités différents et proches d'une configuration réseau réelle.

A noter que dans les topologies utilisées, parmi les 50 nœuds mobiles, 30 nœuds disposent d'un débit de transmission de 2 Mb/s et le reste (20 nœuds) ont un débit de 11Mb/s. Ainsi des nœuds de différents débits sont pris en compte contrairement aux simulations qu'on rencontre dans la littérature qui définissent un seul débit pour tous les nœuds.

Pour chaque scénario étudié, 10 topologies aléatoires sont générées. Elles se caractérisent par le même nombre de nœuds, le même nombre de trafics, et le même scénario de mobilité. Ainsi, seules les positions des nœuds et les paires source-destination sont différentes. Les résultats montrés dans la section suivante représentent la moyenne des résultats obtenus pour les 10 topologies étudiées.

Nous nous intéressons dans cette partie à analyser et comparer le protocole de routage DSR classique avec le protocole DSR supportant la différenciation de terminaux. Vu qu'un protocole de routage a principalement comme rôle l'acheminement des données,

nous étudions la quantité de données acheminée entre les sources et les destinations ainsi que le délai bout en bout des paquets envoyés.

2.4.2 Cas d'une topologie statique

Dans les figures 2.10 et 2.9, nous montrons le délai bout en bout moyen des trafics lancés dans le réseau, ainsi que le taux de paquets correctement acheminés à leurs destination suivant différents scénarios de trafics. Dans ce premier cas, la mobilité n'est pas étudiée, les nœuds sont considérés comme statiques ayant des positions fixes aléatoirement obtenues.

La figure 2.9 et 2.10 montre que les deux protocoles (DSR classique et DSR supportant la différenciation de terminaux) donnent les mêmes performances (petit délai et très peu de pertes de paquets) quand le nombre de trafics générés dans le réseau est petit (moins de 10 trafics). Ceci est dû au fait que dans un réseau de faible charge, très peu de pertes sont constatées et la contention au niveau de l'accès au canal sans fil (802.11) est très réduite. Dans ce cas, les files d'attente des nœuds ne sont pas chargées et le délai de traitement dans les files est petit.

Cependant, à partir de 20 trafics générés dans le réseau, la différence entre les deux protocoles est visible et s'accroît au fur et à mesure où plus de sources sont lancées dans le réseau. Le protocole de routage avec différenciation de terminaux garantit un meilleur délai bout en bout (435 ms) ainsi qu'un taux d'acheminement supérieur (77%) malgré la charge du réseau comparé au protocole DSR classique (923 ms comme délai et 68% comme taux d'acheminement).

A noter aussi que à partir de 20 trafics, le protocole DSR montre un délai important (980 ms). Le protocole DSR modifié continue à assurer un délai bout en bout et un taux de perte inférieur jusqu'à une charge de 25 trafics. Comme attendu, sous une grande charge de trafics (à partir de 35 trafics), le délai et le taux de perte augmentent (plus 2000 ms comme délai et plus de 60% de taux de perte).

D'un côté, pour les deux configurations, les pertes ainsi que les délais élevés observés pour acheminer les paquets de données sont dus :

- au mécanisme de bufferisation utilisé par DSR dans le cas où une route n'est pas disponible. Les paquets attendent dans le buffer durant la phase de découverte de route,
- A la couche 802.11 : quand le canal sans fil est chargé, la probabilité de collision augmente où plus de retransmissions de paquets sont nécessaires pour acheminer les données à chaque saut sans fil, ce qui influence le délai du trafic en cours, mais aussi les trafics transitant par le même canal.

D'un autre côté, l'amélioration obtenue par le protocole DSR modifié par rapport à

DSR est liée au fait que des routes de haute capacité sont choisies pour le routage offrant plus de ressources et réduisant ainsi le délai et le taux de perte.

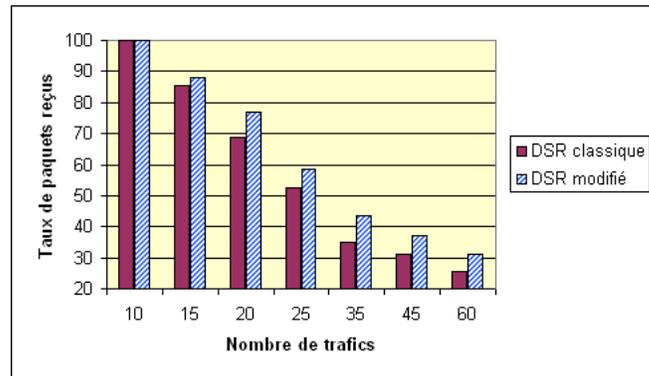


FIG. 2.9 – Taux de paquets reçus avec DSR vs DSR modifié

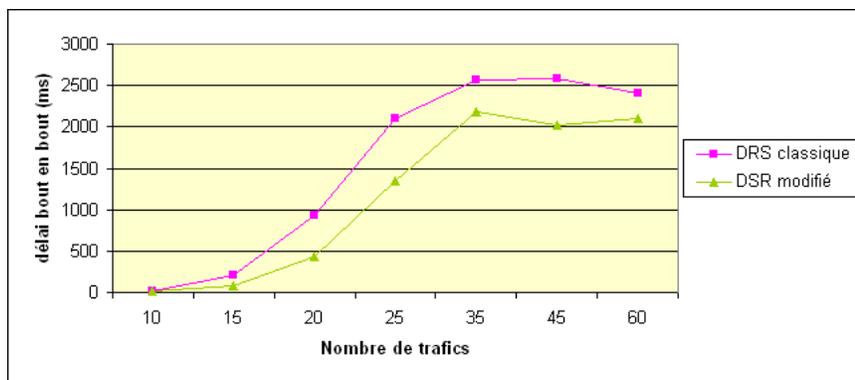


FIG. 2.10 – Délai bout en bout obtenu avec DSR vs DSR modifié

Sélection de routes

En intégrant le critère de la capacité de transmission des nœuds dans la sélection des routes, parmi les routes choisies par le protocole de routage DSR, on a constaté que 65% ont été remplacées par des routes contenant plus de nœuds à haut débit. A noter ici qu'une route sélectionnée par DSR classique peut contenir des nœuds à haut débit. Le rôle de notre extension est de chercher une meilleure route avec plus de nœuds à haut débit, le cas échéant la route est conservée.

Overhead généré par le trafic de contrôle

Dans notre proposition d'extension du protocole de routage DSR, aucun paquet additionnel n'est utilisé. On ajoute uniquement un champ dans les paquets de contrôle (ROUTE_REQUEST et ROUTE_REPLY) d'une taille d'un seul bit. Ainsi pour les simulations utilisées, la charge générée par le trafic de contrôle pour le protocole DSR modifié est identique à celle générée par le protocole DSR original.

2.4.3 Cas d'une topologie dynamique

Le but de cette partie est de montrer les résultats de simulations obtenus sous différents scénarios de mobilité (allant de 1m/s à 30m/s) dans des topologies aléatoires. A noter que dans ces scénarios de mobilité, les nœuds sont constamment mobiles, i.e "le pause duration" utilisé comme paramètre dans NS-2 est égal à 0 seconde.

Pour ces simulations, le nombre de nœuds dans le réseau est 50, 15 trafics ayant une durée d'inter arrivée de 0.25 seconde sont générés entre des sources et des destinations aléatoirement choisis.

Les figures 2.11 et 2.12 montrent respectivement le délai de bout en bout moyen correspondant à chaque scénario de mobilité, et le taux d'acheminement correct des paquets. Comme présenté dans les figures, avec une mobilité de 5 m/s les performances du protocole DSR classique se dégradent rapidement comparé au DSR modifié qui subit moins de dégradation. Lorsque la mobilité exercée sur le réseau est plus importante (10 m/s), le débit ainsi que le délai des trafics se dégradent, mais de façon moins importante dans le cas du DSR modifié. De plus les délais observés sont plus grands.

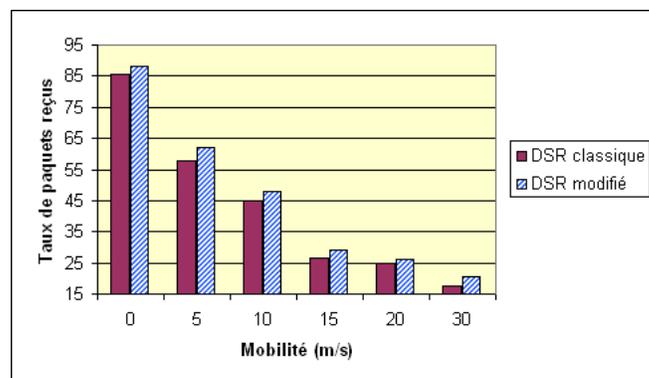


FIG. 2.11 – Taux de paquets reçus obtenu avec la mobilité pour DSR vs DSR modifié

Les changements de topologies sont naturellement fréquents quand les nœuds sont mobiles, générant ainsi plus de cassures de routes ce qui nécessite des phases de décou-

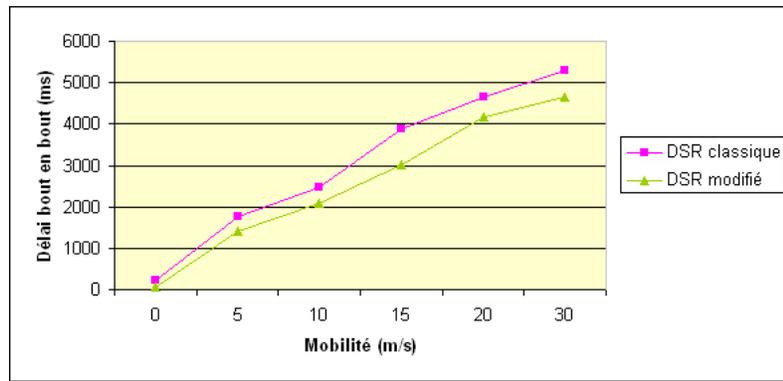


FIG. 2.12 – Délai bout en bout obtenu avec la mobilité pour DSR vs DSR modifié

verte de route répétées. Ces dernières engendrent des trafics de contrôle additionnels qui consomment plus de bande passante et laissent moins de capacité pour les trafics de données. Parallèlement, lors d'une perte de route, le mécanisme de bufferisation est déclenché ce qui se traduit par des délais importants, cela continue tant que ces phénomènes sont détectés par le protocole.

Ce comportement est aussi valable pour le DSR modifié, mais avec moins d'influence et confirme l'apport de la technique de différenciation de terminaux. Car sachant que les routes sont sélectionnées afin d'assurer des liens de haute capacité, en passant par les nœuds ayant un grand débit de transmission, le délai de transmission par saut est alors réduit et la route assure plus de capacité qu'une route classique.

De plus, la mobilité dans le cas du DSR modifié peut amener à créer de nouvelles routes qui contiennent plus de nœuds à haut débit, ce qui lui permet de mieux résister aux dégradations dues à la mobilité et aux changements de routes.

2.5 Conclusion

Dans ce chapitre nous avons présenté une nouvelle métrique pour la sélection de route dans les réseaux ad hoc hétérogènes. Dans le but d'améliorer les performances du réseau ad hoc, et particulièrement pour augmenter la capacité des routes, nous avons étudié une extension du protocole de routage classique (DSR) afin de supporter la différenciation de terminaux. Vu la simplicité de sa mise en œuvre, il nécessite peu de changements dans le fonctionnement de base du protocole DSR et donc ne nécessite pas beaucoup de changements dans le code source. Nous avons montré en utilisant des simulations que le fait de choisir des routes contenant des nœuds à haut débit améliore la capacité des routes et du réseau d'une manière générale avec et sans mobilité dans le réseau.

Nous allons présenter dans le chapitre suivant notre proposition qui montre la nécessité d'une gestion multicouches de la qualité de service dans les réseaux ad hoc. Cette proposition doit être combinée avec le principe de routage à différenciation de terminaux afin de mieux répondre aux besoins des communications temps réel.

Chapitre 3

Gestion multicouches de la Qualité de Service

3.1 Introduction

L'architecture en couches OSI (Open Systems Interconnection) pour la gestion du réseau est utilisée par l'architecture courante de l'Internet. Cette architecture a permis aux différents réseaux d'être reliés ensemble d'une manière efficace. La hiérarchie des couches fournit des abstractions naturelles faites à la hiérarchie actuelle dans les réseaux.

La couche physique traite des signaux, et fournit un service pour communiquer des bits. La couche liaison de données fournit l'abstraction d'un lien, et la capacité de transmettre et de recevoir des suites de bits, au dessus du lien. La couche réseau présente le concept d'un chemin ou d'un itinéraire . La couche transport fournit un canal bout à bout, qui pourrait être fiable ou pas, selon le protocole qui est utilisé. Les trois couches restantes sont moins clairement définies, et ont été fusionnées réellement dans l'architecture de TCP/IP qui s'est développée plus tard. Les interactions entre les couches sont contrôlées, et assurées principalement par les entêtes des protocoles que chaque couche ajoute à l'entête des paquets.

En outre, l'architecture implique également la notion des protocoles de "pair à pair" (tels que le TCP) qui négocient entre les couches correspondantes sur différentes machines. Etant donnée cette architecture, les concepteurs peuvent se concentrer sur l'élaboration des protocoles pour leur couche efficacement, avec l'assurance que le système global fonctionnera raisonnablement bien.

Dans ce chapitre, nous allons montrer les limites de l'architecture en couches dans un environnement mobile sans fil. Nous prouvons l'intérêt d'une gestion multicouches de la

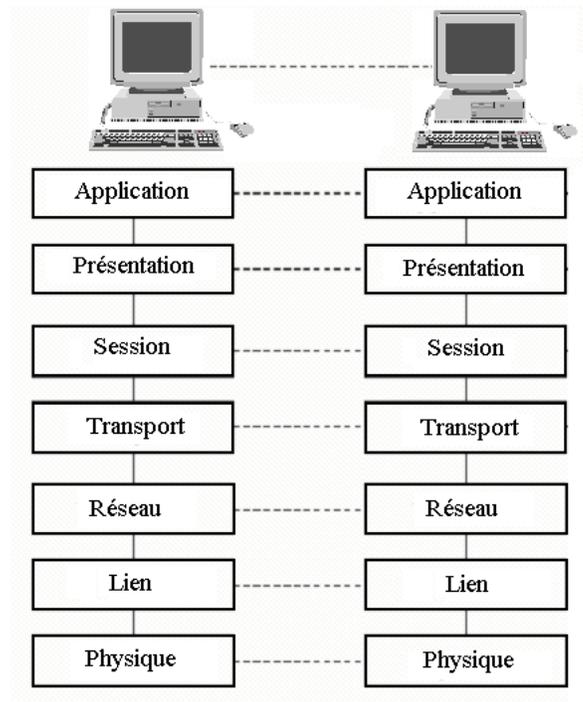


FIG. 3.1 – Modèle en couche OSI

qualité de service dans les réseaux ad hoc. Pour cela, nous effectuons une combinaison de la qualité de service IP et MAC. Un ensemble de simulations est réalisé afin d'illustrer les améliorations obtenues. Nous proposons également de combiner cette gestion de la QoS multicouches avec un protocole de routage à différenciation de terminaux (chapitre précédent) pour un meilleur support de la QoS.

3.1.1 Le Modèle OSI et les contraintes liées aux réseaux mobiles sans fil

Les conceptions architecturales réussies, par leur dominance, influencent les méthodes utilisées par les concepteurs. Le succès de l'architecture en couches des réseaux filaires a eu un grand impact sur les paradigmes de conception des réseaux. C'est devenu aussi l'architecture par défaut pour concevoir les réseaux sans fil. Cependant, il n'est pas du tout justifié que cette architecture soit a priori appropriée pour les réseaux sans fil. Cette architecture a besoin de réexamen, car l'environnement sans fil permet des modalités de communications qui sont inexistantes dans les réseaux fixes.

Pour cela, il faut étudier l'aspect constructif du schéma utilisé ainsi que les raisons pour lesquelles les approches existantes ont été empêchées dans la solution courante. D'abord,

des paquets sont transportés au dessus de plusieurs sauts. À chaque saut, le récepteur ne reçoit pas simplement le signal prévu, mais également la superposition des transmissions interférentes d'autres nœuds, plus le bruit ambiant. Les transmissions interférentes sont traitées comme un bruit, et le paquet est entièrement décodé. Cette régénération numérique d'un paquet se trouve au cœur (par opposition à l'analogique) de la révolution numérique. Le paquet régénéré est alors rediffusé au prochain nœud, où encore il sera décodé en présence aussi du bruit d'autres transmissions, ...etc.

Il y a plusieurs raisons pour lesquelles cette solution est intéressante. D'abord, les récepteurs peuvent être simples, puisqu'ils dépendent simplement du rapport signal/bruit. En second lieu, la procédure 'décodez et expédiez' avec un relayage multisauts fournit une abstraction des liens. Ainsi des protocoles pour des réseaux filaires peuvent être réutilisés pour les réseaux sans fil. Toutefois il à noter que le choix d'une architecture multisauts avec décodage et expédition à chaque nœud relais tout en traitant toute interférence comme bruit, crée certains problèmes spécifiques aux réseaux sans fil qui doivent être résolus. Par exemple, puisqu'on traite toute l'interférence comme un bruit, on veut réguler le nombre d'interférents potentiels à proximité du récepteur. Ceci nécessite un protocole de contrôle d'accès au medium par lequel on contrôle le nombre d'interférents. Ceci peut être compliqué par la présence des stations "cachées" et "exposées", d'où la nécessité d'avoir une solution distribuée en temps réel.

Un autre problème est le routage, car il nécessite des nœuds relais, où le but est de trouver une séquence de relais de la source à la destination. Ceci est différent du cas où le routage est à un saut. En outre, un contrôle de puissance est obligatoire dans ce contexte afin de maximiser la capacité des liens (réutilisation des fréquences), et réduire la consommation d'énergie des nœuds mobiles. Ainsi, on remarque que c'est le choix de l'architecture qui a créé les besoins des protocoles, en particulier : le contrôle d'accès au médium, le routage, et le contrôle de puissance, sur lesquels la communauté est entrain de travailler.

3.1.2 Approche intercouches (crosslayer)

Alors qu'une architecture en couches est simple et constitue donc un bon candidat pour une conception de base, il y a toujours le besoin d'optimiser. En effet, plusieurs occasions d'optimisation se présentent par l'interaction accrue à travers les couches. Le passé récent a ainsi vu un engouement de propositions crosslayer (intercouches) qui explorent une interaction beaucoup plus riche entre les paramètres à travers les couches. En évaluant ces propositions, la différence entre la performance et l'architecture doit être fondamentalement considérée. Ainsi une suggestion crosslayer particulière peut rapporter une amélioration en terme de performance de débits et de délais.

Si une suggestion spontanée pour une conception crosslayer peut sembler attrayante,

les interactions doivent être correctement étudiées. Contrairement à l'approche en couches, où chaque couche travaille sans se soucier du reste de la pile, une approche intercouches implique "une cassure" des couches à travers les interactions. Ces dernières affectent non seulement les couches concernées, mais également les couches non impliquées, ce qui peut éventuellement dégrader la performance du système.

En outre, un paramètre important à prendre en considération dans une approche multicouches est la stabilité du système sur une échelle de temps définie sous des conditions données.

3.1.3 La QoS suivant les différentes couches du modèle OSI

Le support de la qualité de service dans les réseaux ad hoc influence tous les protocoles utilisés dans les différentes couches OSI, à savoir : les couches physique, lien, réseau, transport et application.

La couche physique

Les conditions des canaux de transmission sont variables dans le temps, car le rapport signal/bruit dans les canaux fluctue en fonction du temps. Ceci est dû aux problèmes présentés par le canal : les effets des accès multiples, d'évanouissement, du bruit, des interférences et de la mobilité. Pour fournir la QoS dans de tels environnements, l'estimation du canal sera donc une tâche importante afin de synchroniser le récepteur et l'émetteur.

L'apport de la qualité de service pour les communications sans fil ne se limite pas à l'amélioration des techniques du canal, mais nécessite aussi une intégration avec les couches supérieures, comme les algorithmes de compression de la source au niveau applicatif. L'utilisation de schémas de compression élevés peut améliorer la qualité des communications bout en bout. Parallèlement, avec plus de protection du canal, moins d'erreurs seront observées ce qui implique un meilleur acheminement des données. Vu que la capacité du canal sans fil est limitée, le codage au niveau de la source (caractéristiques de la source) et l'état courant du canal doivent être pris en considération. AVLSI est un groupe de recherche fonctionnant avec des techniques adaptatives dans les MANETs, y compris l'information adaptative à l'état du canal. Le problème des bruits et des collisions s'accroît beaucoup plus dans les réseaux sans fil, rendant l'approvisionnement de la QoS plus complexe.

Couche lien

En raison des problèmes de synchronisation dans les réseaux sans fil, les protocoles MAC synchrones comme TDMA (Time Division Multiple Access) ou FDMA (Frequency Division Multiple Access) ne sont pas appropriés. De plus, la plupart des protocoles MAC sont conçus pour un réseau sans fil à un saut. Ce problème se produit quand deux nœuds, qui sont hors de portée de transmission l'un de l'autre, envoient au même nœud et causent une collision. Le mode d'accès asynchrone de IEEE 802.11 (DCF) [44] basé sur le CSMA/CA permet un accès distribué, propose de résoudre le problème du terminal caché en utilisant l'option de réservation RTS/CTS. Pour permettre d'assurer des services temps réel, des travaux ont été proposés (voir chapitre 1) pour assurer une différenciation de service au niveau MAC, ce que revient essentiellement à donner la priorité à certaines stations ou trafics pour accéder au canal.

Couche réseau

Aujourd'hui, la plupart des protocoles de routage proposés pour MANETs ne prennent pas en compte la QoS. Dans la majorité des cas, des messages sont acheminés à travers le plus court chemin disponible, qui peut ne pas être adapté pour les applications qui exigent des garanties de QoS. Le but primaire d'un protocole de routage orienté QoS est de déterminer un chemin d'une source à la destination qui satisfait des besoins de la QoS désirés.

Le routage n'est pas la seule composante de la couche réseau qui peut fournir de la QoS. D'autres mécanismes peuvent offrir des services qui fonctionnent mieux que l'approche dite Best Effort. Ces mécanismes, tels que le contrôle d'admission, l'ordonnancement (figure 3.2) et le lissage de trafics, doivent prendre en compte les différentes caractéristiques des MANETs comme la topologie dynamique et la qualité variable des liens.

La couche transport

La couche transport joue un rôle important pour l'acheminement des communications temps réel, en utilisant principalement UDP et TCP. Des applications temps réel comme le streaming audio/vidéo peuvent être envoyées sur le protocole UDP, qui offre un minimum de fonctionnalités réseau et plus de flexibilité, alors que d'autres applications peuvent choisir TCP qui assure la délivrance bout en bout des paquets. Dans l'Internet, TCP suppose que la majorité des pertes de paquets est due à la congestion du réseau. Cette hypothèse n'est pas vraie dans les réseaux sans fil, où la perte des paquets est essentiellement liée au bruit du canal et aux changements de routes. Quand une source TCP détecte une perte de paquets, elle active son mécanisme de contrôle de congestion, qui rend les performances

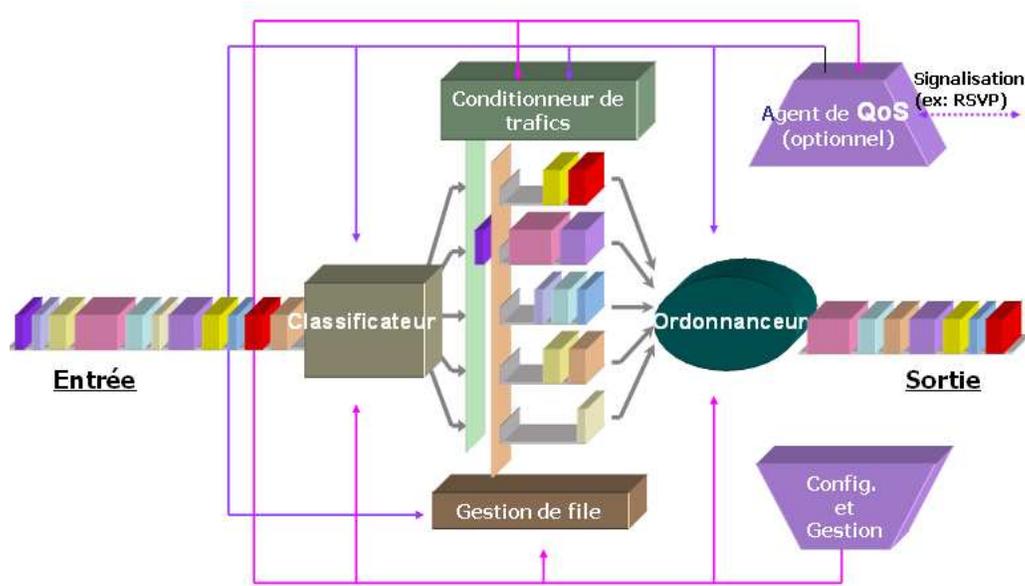


FIG. 3.2 – Mécanismes de qualité de service

des trafics TCP dans les réseaux ad hoc très limitées en terme de débit. Récemment, des travaux ont été réalisés pour améliorer les performances de TCP dans les réseaux ad hoc [109] [108]. Ils sont dépendants des mécanismes de feedback explicites pour distinguer les pertes dues aux erreurs des pertes dues à la congestion. Ainsi, une action appropriée est prise quand une perte de paquets surgit. Avoir une technique appropriée pour la gestion des ressources dans les protocoles de la couche transport, contribue à un meilleur support de la qualité de service dans les réseaux ad hoc.

La couche application

Il est très difficile de fournir la QoS dans un environnement fortement dynamique. Les applications doivent donc s'adapter à cette réalité. Une solution est d'indiquer une gamme des valeurs qu'elles peuvent tolérer. Le réseau essaye de fournir des ressources dans cette marge, et les applications doivent pouvoir s'adapter dans de telles circonstances. Plusieurs approches pour le support des applications temps réel adaptatives dans l'Internet ont été proposées [124]. Elles intègrent des mécanismes d'encodage en couche, lissage de débit, contrôle d'erreur adaptatif, ...etc. Ces solutions peuvent être modifiées et améliorées pour répondre aux spécificités des réseaux mobiles ad hoc.

Dans ce qui suit, nous allons présenter notre proposition qui consiste à fournir une différenciation de service au niveau des deux couches : réseau (pour une priorité locale des paquets) et MAC (pour l'accès au canal sans fil). Il s'agit de combiner les mécanismes de QoS des deux couches pour un meilleur support des trafics temps réel dans les réseaux

ad hoc.

3.2 Notre proposition : Combinaison de la qualité de service IP et MAC

Il est clair que réaliser une différenciation de service au niveau IP, localement dans chaque nœud, dans les réseaux filaires ou mobiles fournit une meilleure qualité de service aux applications multimédia temps réel. Cependant, dans les réseaux sans fil, où le médium est partagé entre les stations qui sont dans la même cellule, tous les nœuds ont la même probabilité pour accéder au canal. Inversement, quand seule la différenciation de service MAC est utilisée pour contrôler l'accès au lien, les paquets prioritaires peuvent être retardés par des paquets best effort à l'intérieur du même nœud. Dans ce cas, les paquets best effort peuvent aussi attendre plus de temps pour accéder au médium (d'autres paquets prioritaires d'autres nœuds sont plus prioritaires dans l'accès au lien). Par conséquent, les paquets prioritaires, bloqués par les best effort, sont encore plus pénalisés dans leur accès au lien.

Nous proposons un mécanisme de qualité de service intercouches IP et MAC qui combine la différenciation de services traitée dans les deux couches (réseau et lien) et qui bénéficie des avantages apportés par les fonctionnalités de QoS de chaque couche. Ainsi, contrairement aux modèles de qualité de service qui travaillent sur des couches d'accès au médium sans priorité, notre approche propose d'améliorer les performances et la qualité de service des applications temps réel, aussi bien dans la classification des flux en différenciant les traitements, mais aussi permettre de les privilégier pour accéder au médium. Ceci présente un apport considérable, notamment dans les réseaux avec lien sans fil, où l'accès au médium repose sur un mécanisme de compétition avec les autres nœuds.

Marquage des paquets

Au niveau de la couche IP on utilise un mécanisme proche du fonctionnement DiffServ. Chaque nœud dans le réseau ad hoc, considéré comme un domaine DiffServ, supporte les fonctionnalités d'un nœud de bordure et d'un nœud de cœur. L'opération de marquage est effectuée quant à elle au niveau des sources des trafics. Les paquets appartenant à des classes différentes sont traités dans des files séparées. Le niveau de priorité de la classe définit la probabilité de suppression des paquets de la file correspondante et sa longueur. Dans notre étude, le mécanisme de qualité de service consiste en une gestion de file d'attente des nœuds basée sur une priorité stricte entre le trafic prioritaire et le trafic best effort. La priorité est basée sur le champ DSCP.

Modification de la couche MAC 802.11

On définit deux classes de services, haute priorité (applications temps réel : sensibles au délai et à la gigue) et la classe best effort (non sensible au délai et aux pertes de paquets). Une couche MAC 802.11 modifiée est utilisée. Elle consiste à modifier la fonction d'accès DCF afin de supporter la différenciation de deux types de trafics.

Elle permet deux types de services avec une priorité simple basée sur le paramètre DIFS de la fonction de contrôle DCF. Contrairement aux paquets best effort, un court DIFS est attribué aux paquets de haute priorité. Notons que d'autres mécanismes de QoS peuvent être utilisés, par exemple la réservation de ressources ou le contrôle d'admission afin de contrôler la charge du réseau ad hoc et de fournir une qualité de service quantitative aux applications temps réel.

Le choix d'une différenciation basée sur le paramètre DIFS est justifié par son efficacité (d'après les études réalisées dans la QoS dans la couche IEEE 802.11) et aussi par sa simplicité d'implémentation.

La qualité de service est ainsi établie dans les deux couches IP et MAC et une mise en correspondance (mapping) entre les classes définies dans chaque couche est établie.

3.3 Simulations et analyse des résultats

Dans cette section, nous allons réaliser un ensemble de simulations à l'aide de NS-2 [34] (l'outil de simulation NS-2 et les intervalles de confiance sont décrits dans l'annexe), dont le but est d'illustrer que la qualité de service des flux temps réel (prioritaires) est mieux garantie lorsqu'une combinaison de la qualité de service des deux couches IP et MAC est effectuée. Les performances des trafics (temps réel ou best effort) sont exprimées en terme de débit, délai bout en bout et gigue. Les topologies réseau utilisées sont aléatoirement générées et composées de 50 nœuds mobiles (taille moyenne d'un réseau ad hoc) se déplaçant dans une surface de simulation de $1000m \times 1000m$. La charge du réseau est graduellement augmentée, en incrémentant le nombre de flux générés, afin de montrer l'apport de notre proposition dans un réseau est légèrement chargé, moyennement chargé et dans un réseau saturé.

Dans les simulations étudiées, nous nous intéressons à trois scénarios de trafics, à savoir : le trafic UDP, TCP et le trafic voix.

Les autres paramètres utilisés dans les simulations sont décrits dans le tableau suivant :

Attribut	Valeur
Modèle de propagation radio	Two Ray Ground
Portée de transmission	250 mètres
Nombre de nœuds mobiles	50
Débit des nœuds	2Mb/s
Protocole de routage	AODV
Slot Time	16 μs
SIFS Time	8 μs
DIFS Time	40 μs
DIFS1 Time (pour les paquets TR)	40 μs
DIFS2 Time (pour les paquets BE)	120 μs
Cwmin	16
Cwmax	1024

TAB. 3.1 – Paramètres du modèle de simulation

Deux types de trafics sont considérés dans notre étude : temps réel (TR) et best effort (BE). Les paquets de chaque type de trafic sont marqués à la source. Une file à priorité stricte à deux niveaux de priorité est utilisée au niveau IP. Pour une couche MAC avec qualité de service, une différenciation de service à 2 classes basée sur le paramètre DIFS est utilisée. Une valeur de $DIFS = 40\mu s$ est adoptée pour les trafics prioritaires (TR), et une valeur 3 fois supérieure ($120\mu s$) correspond aux trafics moins prioritaires (BE).

Le but de la partie suivante est d'étudier l'impact de la différenciation IP et MAC sur les performances obtenues, en fonction des trafics introduits dans le réseau, à savoir :

- des trafics UDP/CBR seuls (TR et BE)
- trafics UDP/CBR (TR) combinés avec des trafics TCP/FTP (BE)
- trafics de type voix (TR) + trafics UDP/CBR (BE)

Trafics UDP

Dans une première étape seuls les trafics UDP sont considérés. Les communications temps réel sont caractérisées par des trafics CBR (Constant Bit Rate) d'un débit de 32kb/s, d'une taille de paquet de 240 octets. Les flux best effort, quant à eux, ont un débit de 86kb/s, avec une taille des paquets de 1000 octets.

Les flux prioritaires (à partir de 3 sources choisies aléatoirement) sont d'abord lancés dans le réseau à l'instant $t=20$ seconde. Les 5 sources de flux best effort sont lancés par la suite d'une façon incrémentale dans le but de charger le réseau. A partir de $t=210$ seconde, un autre trafic BE d'un débit de 150 kb/s est lancé. La figure 3.3 montre le débit et le délai des 3 flux temps réel lorsque aucun mécanisme de QoS n'est utilisé.

Dans la première phase (avant $t=100$ secondes) où le réseau est peu chargé, les délais des paquets sont très petits et les débits sont garantis. A partir de $t=100$ le réseau commence à se charger au fur et à mesure que les flux best effort sont lancés. A ce moment là, on obtient des délais plus élevés et des pertes de paquets dues principalement aux pertes des liens causées par les congestions dans certaines régions dans le réseau. Quand le réseau est fortement congestionné, tous les trafics sont affectés, et cela se traduit par une grande perte de paquets et des délais de bout en bout beaucoup plus élevés. Lorsque les paquets réussissent à arriver à destination, ils ont souvent été retardés dans les files d'attente des nœuds, et ont subi plusieurs retransmissions au niveau de la couche MAC dues aux collisions.

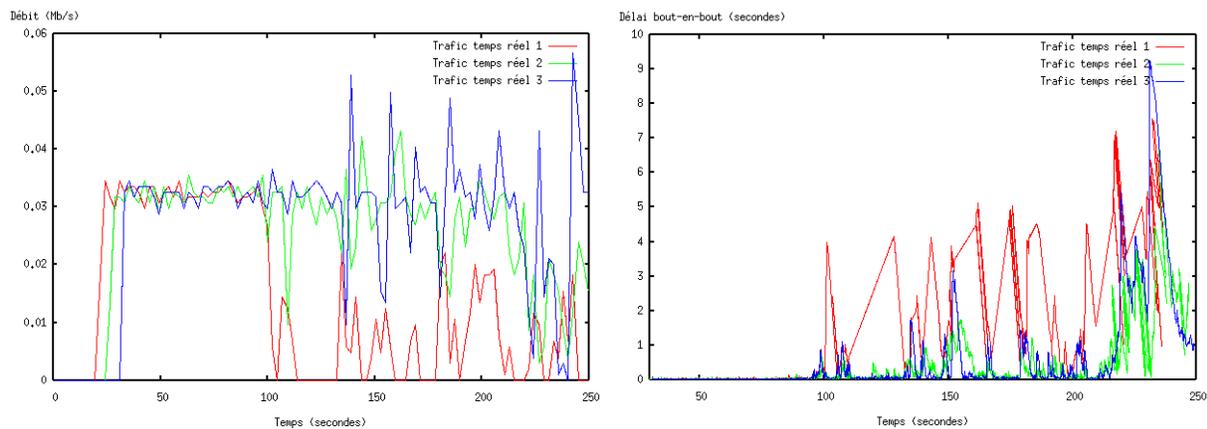


FIG. 3.3 – Débit et délai des trafics temps réel sans mécanismes de QoS

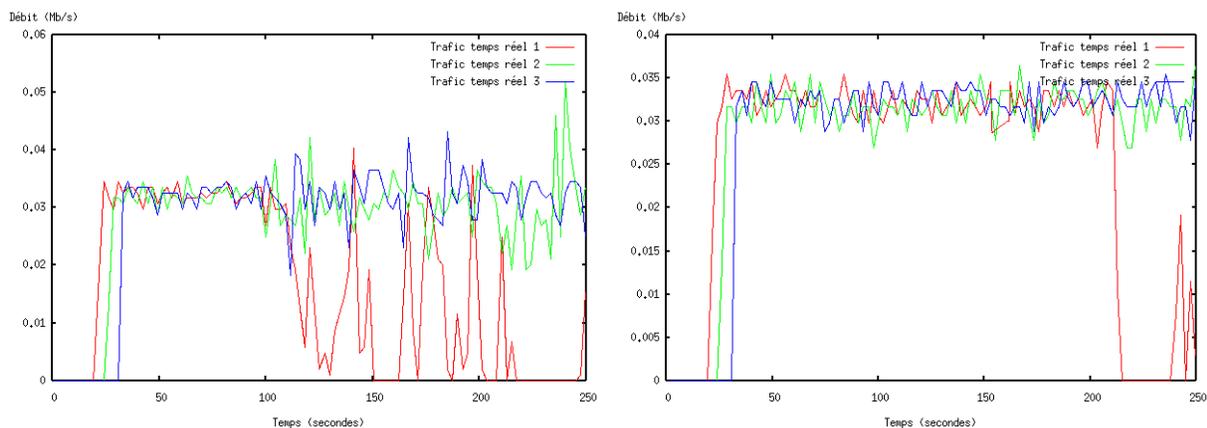


FIG. 3.4 – Débit des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)

La figure 3.4 compare le débit des trafics temps réel avec une QoS de niveau réseau seulement et avec QoS réseau+MAC. On remarque que l'utilisation de la QoS IP améliore le délai et le débit par rapport au cas précédent. Mais cela reste insuffisant pour garantir une qualité de transmission correcte des flux temps réel. Car le fait de donner la priorité aux paquets prioritaires dans les files d'attente n'empêche pas les paquets d'être perdu ou retardé au niveau de la couche MAC, qui est équitablement partagée. Contrairement à la QoS IP seulement, la QoS IP+MAC a permis de garantir des délais réduits (inférieur à 100 ms, figure 3.5) et un débit garanti (particulièrement pour les trafics temps réel 2 et 3, voir figure 3.4) et ce même dans le cas d'un réseau chargé. La priorité locale donnée aux paquets temps réel, au niveau des files d'attente, est maintenue au niveau MAC. Cela donnera une plus grande probabilité d'accès au canal sans fil et un meilleur délai de transmission.

On remarque aussi qu'à partir de $t=210$ secondes, où le réseau est fortement chargé, notre proposition offre de meilleurs résultats, bien que cela reste insuffisant pour assurer pour une bonne qualité de transmission des flux temps réel. Dans ces situations un contrôle d'admission s'avère nécessaire afin de contrôler la charge et la quantité de trafics circulant dans le réseau à un moment donné.

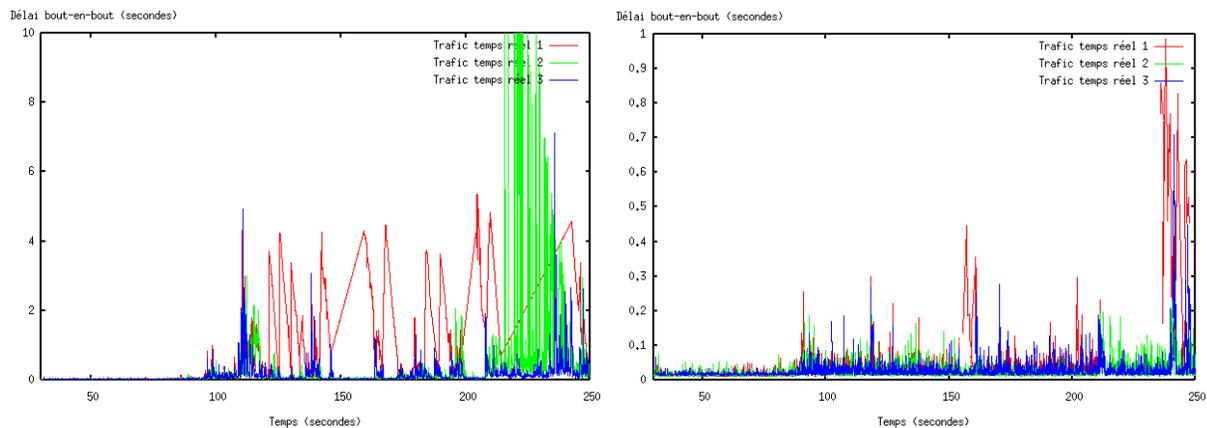


FIG. 3.5 – Délai des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)

Trafics UDP (prioritaire) combinés avec des trafics TCP (BE)

On s'intéresse dans cette section à remplacer les trafics best effort UDP par des sources FTP (TCP) ayant la même taille des paquets (1000 octets), et à observer son influence sur les performances des trafics prioritaires temps réel.

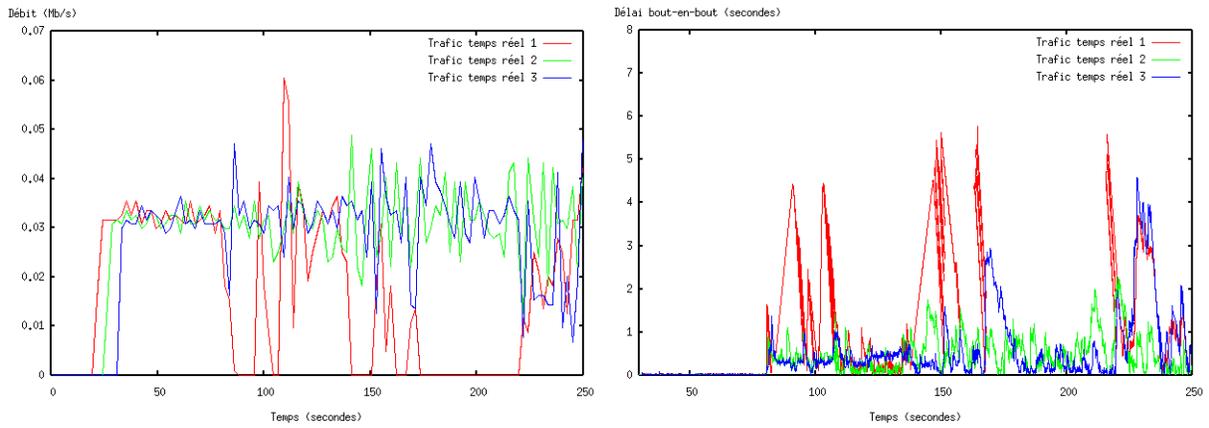


FIG. 3.6 – Débit et délai des trafics temps réel sans mécanismes de QoS

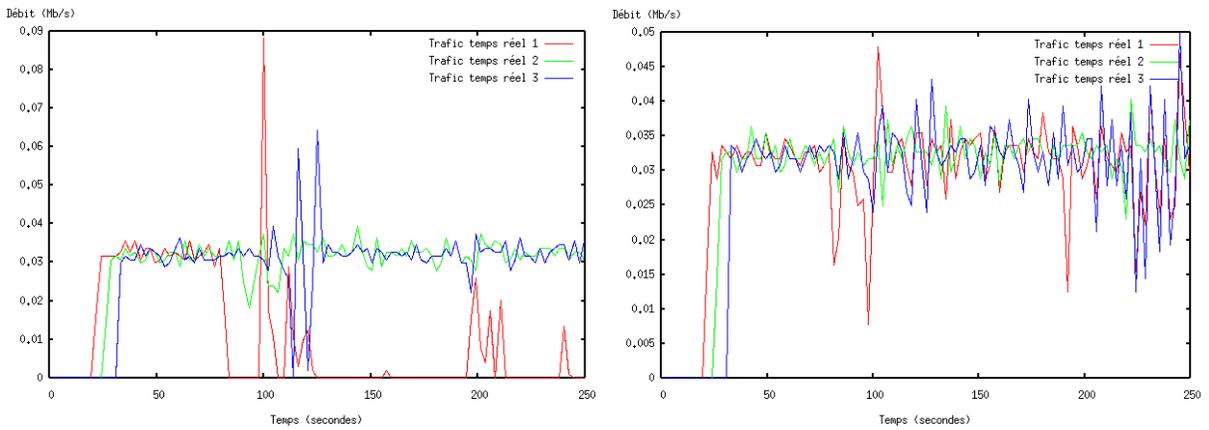


FIG. 3.7 – Débit des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)

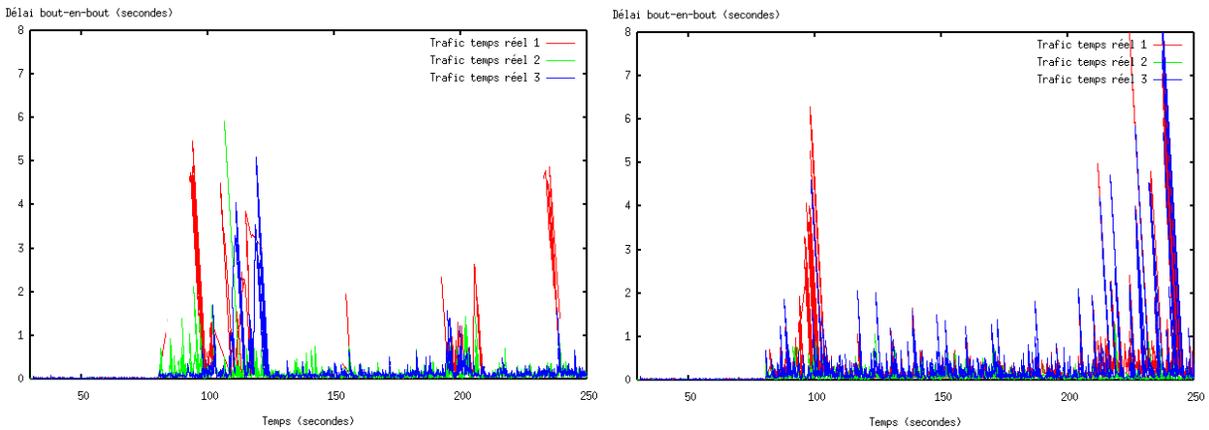


FIG. 3.8 – Délai des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)

Comme illustré dans la figure 3.6, jusqu'à la 80ème seconde, les délais et débits des trafics temps réel sont similaires à ceux obtenus dans la précédente section. Néanmoins, à partir du lancement des trafics TCP, des dégradations des délais et débits apparaissent. On constate que les délais sont instables et très variables sans l'existence d'un mécanisme de QoS.

A noter dans ce scénario, qu'il est inapproprié de le comparer avec le précédent scénario. D'une part, le débit de TCP est fonction de l'état du réseau, et adapte le temps de transmission des paquets aux conditions du réseau. D'autre part, le protocole de transport TCP nécessite des messages d'acquiescement lors des transmissions des données.

Les figures 3.7 et 3.8 montrent que l'amélioration obtenue avec la QoS IP seulement n'est pas suffisante, comparée à une différenciation IP et MAC. Car dans le cas où une QoS IP est utilisée, si les trafics TCP/FTP transitent par des nœuds différents de ceux pris par un trafic temps réel, mais qui sont voisins directs, les paquets TCP auront la même chance pour accéder au canal sans fil que les autres trafics. Dans ce cas, le protocole TCP continue à émettre avec moins d'adaptation de débit. Ce qui génère plus de perte des paquets prioritaires au niveau de la couche MAC.

On constate cependant que les trafics prioritaires ont un délai de bout en bout réduit et des débits garantis quand une gestion multicouches est utilisée.

Nous avons constaté que l'utilisation de trafics TCP/FTP perturbe le fonctionnement du réseau ad hoc et influence les autres types de trafics. Cependant l'utilisation de la gestion de la QoS IP et MAC a permis de mieux garantir le support des trafics temps réel.

Trafics de type voix combinés (temps réel) avec des trafics UDP (BE)

Dans le but de simuler des trafics de type voix, proches des modèles et des codeurs existants dans les réseaux filaires, on simule des sources ayant des propriétés proche du monde réel.

La téléphonie sur IP a connu ces dernières années un développement rapide et offre une alternative aux systèmes de téléphonie classiques. Les standards dominants pour les transmissions multimédias dans les réseaux à commutation de paquets sont les recommandations de l'ITU H.323 et H.324. L'ITU recommande pour applications sans fil le codeur G.729 à 8kb/s.

Une caractéristique du trafic audio est que le délai de bout en bout des paquets affecte

la qualité de service de la communication plus que la perte des paquets. Ce type de trafic est défini comme un processus ON/OFF (ON : pour la phase de parole, et OFF : pour le temps du silence). Les périodes ON et OFF sont générées suivant une distribution exponentielle. Dans ce cas, les paquets transmis ne sont générés que dans la période ON.

Avec la téléphonie d'IP, on peut tolérer une transmission bout à bout d'environ 150 millisecondes ainsi qu'une gigue inférieure à 100 millisecondes pour avoir une bonne qualité de communication et éviter de rencontrer des effets d'écho.

Les flux de type voix utilisés ont un débit de 32kb/s avec une taille de paquets de 250 octets. La durée de la période ON et de la période OFF est de 500 ms. Les flux audio (d'un nombre de 5) sont d'abord lancés, suivis à partir de la 80ème seconde par des trafics UDP (4 trafics d'un débit de 150kb/s) dont le but est de charger le réseau. A la 210ème seconde un autre trafic UDP (150kb/s) est généré afin de charger davantage le réseau.

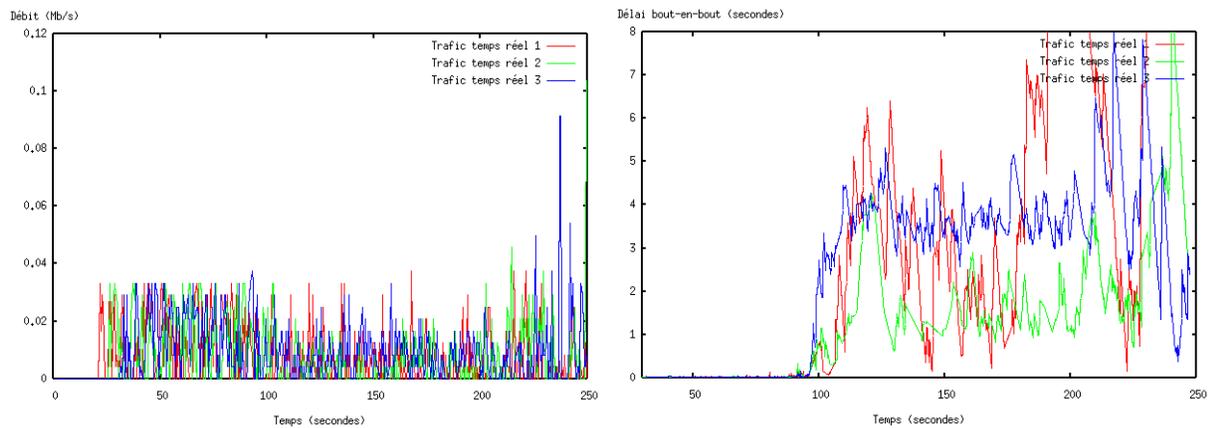


FIG. 3.9 – Débit et délai des trafics temps réel sans mécanismes de QoS

Comme pour les modèles de trafics précédents, nous distinguons les trois phases : peu chargé, chargé et très chargé. Au delà du fait que la combinaison de la qualité de service IP et MAC améliore les délais et les débits des trafics temps réel, nous constatons qu'avec l'utilisation de trafics voix (ON/OFF), plus de trafics ont pu être lancés dans le réseau. De plus, nous remarquons moins de rafales (burst) et de fluctuations dans le débit et le délai des trafics prioritaires, comparé au cas où le trafic temps réel était représenté par un UDP/CBR.

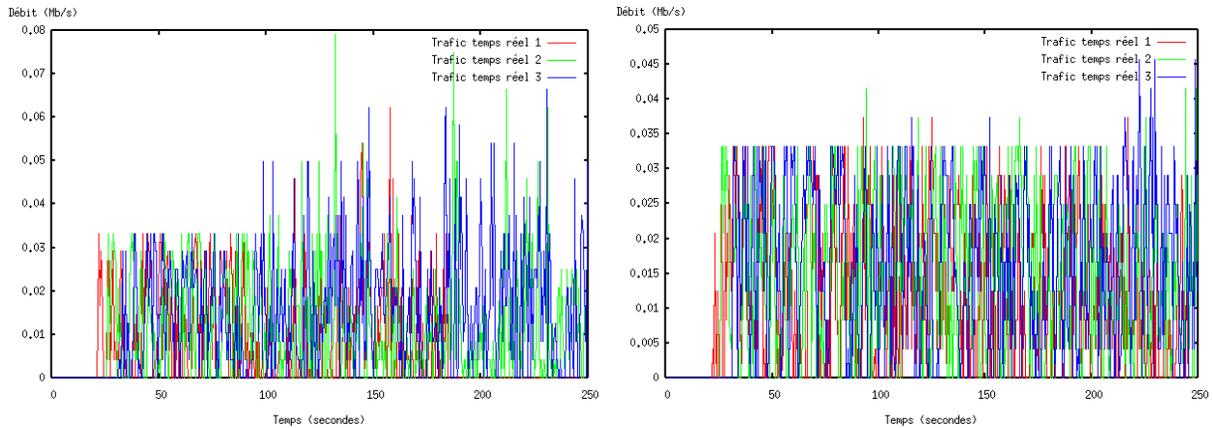


FIG. 3.10 – Débit des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)

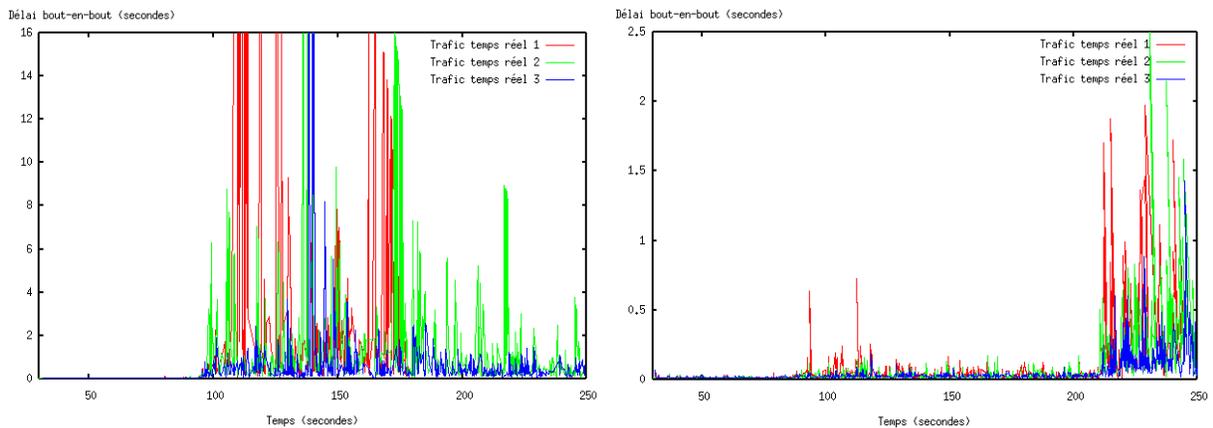


FIG. 3.11 – Délai des trafics temps réel avec une QoS IP (à gauche), et avec une QoS IP+MAC (à droite)

3.4 Gestion multicouches et Routage avec différenciation de terminaux

En plus de la combinaison de la QoS IP et MAC réalisée dans la section précédente, nous allons montrer dans cette section à travers des simulations l'intérêt de combiner la gestion multicouches IP et MAC avec un protocole de routage avec différenciation de terminaux (décrit dans le chapitre 2).

Le principe est d'offrir plus de liens sans fil de bonne qualité dans les routes sélectionnées avec le routage avec différenciation de terminaux. Ensuite, les mécanismes de QoS peuvent être envisagés pour différencier les trafics.

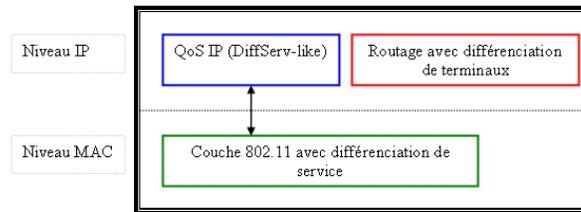


FIG. 3.12 – Combinaison de la QoS IP et MAC avec un routage avec différenciation de terminaux

3.4.1 Scénario de simulation étudié

Nous allons maintenant décrire l’environnement utilisé pour simuler les mécanismes proposés. Le modèle de simulation est réalisé en utilisant l’outil de simulation Network Simulator (NS-2) [34]. Notre modèle consiste en un réseau ad hoc connecté à une infrastructure fixe, avec 7 nœuds mobiles, se déplaçant sur une surface de 1000x1000 mètres avec une vitesse réduite. La topologie ainsi que les capacités des liens sans fil sont illustrés dans la figure 3.13. Le réseau ad hoc est composé de deux types de nœuds : routeurs intelligents (E, F), et nœuds mobiles. Les nœuds utilisent les débits définis dans le standard IEEE 802.11b. C’est à dire que lorsqu’il y a dégradation de la qualité du signal, le débit diminuera de 11 Mb/s à 5.5, 2, ou même 1 Mb/s. La qualité des liens varie en fonction du temps et de la mobilité des nœuds. Deux classes de trafics sont considérées dans la simulation :

- Données (trafic BE sans exigence de QoS) en utilisant un flux CBR (connexion UDP) à 130 kb/s.
- Trafic temps réel (avec contraintes de qualité de service) : représenté par une source de trafic CBR à 140kb/s, avec des paquets de taille de 150 octets.

Dans les simulations, un trafic prioritaire entre A à G commence à émettre à $t=15$ sec. A la 65ème seconde, un autre trafic prioritaire entre A à D est lancé, suivi d’autres flux best effort, dans le but de charger le réseau pour pouvoir mettre en évidence l’intérêt des mécanismes de QoS qu’on va utiliser dans une telle situation. L’objectif de cette étude est de comparer les performances du réseau et des applications prioritaires, selon des conditions différentes. Quatre cas sont étudiés :

- Pas de mécanismes de qualité de service,
- Différenciation de terminaux : Le protocole de routage AODV (ad hoc on demand distance vector) est modifié pour différencier les nœuds mobiles.
- QoS IP et MAC sans différenciation de terminaux : la différenciation de service IP consiste en un principe de priorité dans les files d’attente des nœuds en utilisant une priorité stricte. En outre, une couche MAC IEEE 802.11 modifiée est utilisée.
- Les mécanismes de QoS IP et MAC combinés avec la différenciation de terminaux.

Les paramètres utilisés dans le modèle de simulation sont listés dans le tableau suivant. Ils représentent les valeurs utilisées dans NS-2 pour la couche IEEE 802.11 avec une modification de la fonction DCF, en introduisant deux types de DIFS (DIFS1 et DIFS2).

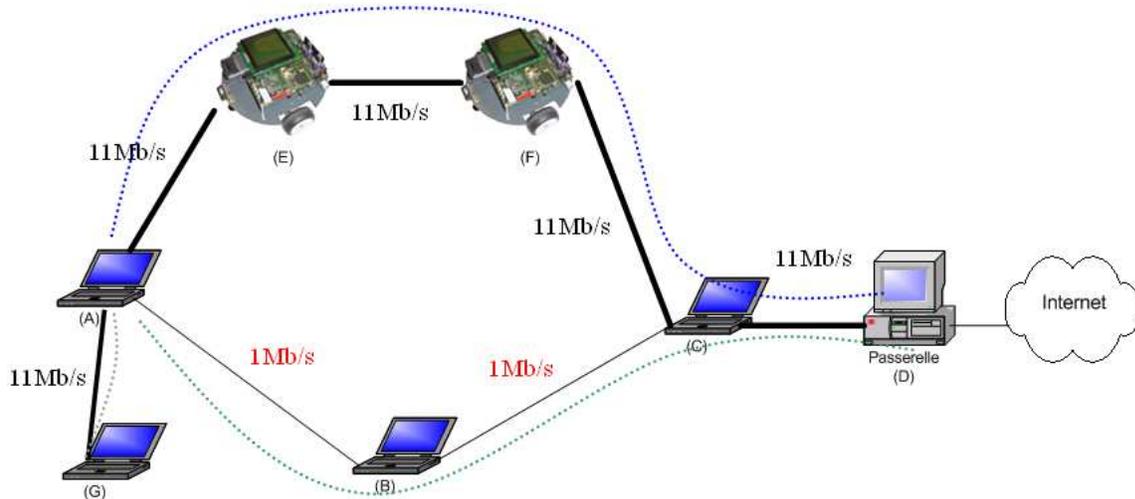


FIG. 3.13 – Topologie utilisée dans la simulation

Attribut	Valeur
Couche MAC	IEEE 802.11b
Modèle de propagation radio	Two Ray Ground
Portée de transmission	250 mètres
Nombre de nœuds mobiles	7
Débit du nœud (B)	1Mb/s
Débit des autres nœuds	11 Mb/s
Slot Time	16 μs
SIFS Time	8 μs
DIFS Time	40 μs
DIFS1 Time (pour les paquets TR)	40 μs
DIFS2 Time (pour les paquets BE)	120 μs
Cwmin	16
Cwmax	1024

TAB. 3.2 – Paramètres du modèle de simulation

Nous allons montrer que l'utilisation de la différenciation de service au niveau des couches IP et MAC garantit une bonne qualité de service pour les applications temps réel, mais reste insuffisante dans un environnement mobile ad hoc, vu la variation de la capacité du canal.

3.4.2 Résultats

Dans cette section, nous allons évaluer les performances de notre approche. La performance est mesurée en termes du délai bout en bout, gigue et débit.

Différenciation de terminaux

Avec la différenciation de terminaux (figures 3.14 et 3.15), un meilleur débit et délai (4 ms avant 65 seconde, et réduit de moitié - 230 ms - à partir de la 125ème seconde) est obtenu. Au lieu d'utiliser un protocole de routage optimisant le nombre de sauts, notre protocole fournit des routes utilisant des liens sans fil de bonne qualité (utilisant un débit élevé). Par exemple, pour un protocole de routage 'best effort' la route calculée pour le flux envoyé entre A et D est ABCD (où AB et BC utilisent des liens à 1 Mb/s qui dégradent la communication A à G qui est à 11Mb/s), alors que notre protocole avec différenciation de terminaux va fournir le chemin (AEFCD) où tous les liens sont à 11Mb/s.

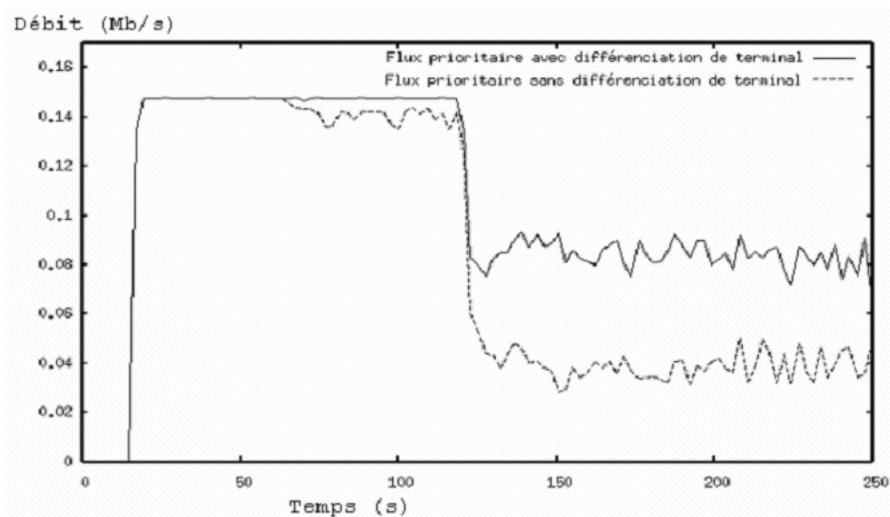


FIG. 3.14 – Débit avec et sans différenciation de terminaux

Qualité de service au niveau IP et MAC

Les résultats obtenus dans cette section (voir figures 3.16 3.17) montrent que dans l'environnement ad hoc à diffusion et variable dans le temps, la combinaison des mécanismes de QoS IP et MAC offre de meilleures performances, mais reste limitée sans l'existence de liens de bonne qualité. L'explication des résultats est identique que pour les simulations réalisées dans les sections précédentes.

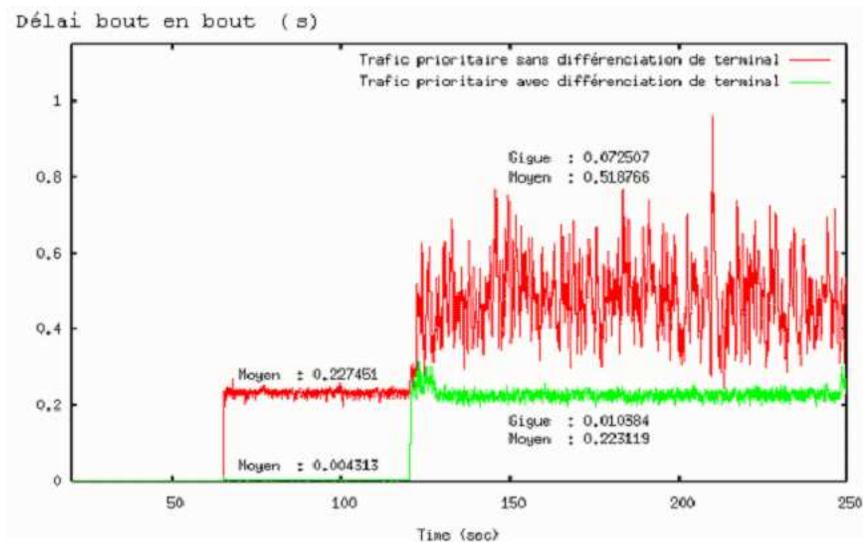


FIG. 3.15 – Délais avec et sans différenciation de terminaux

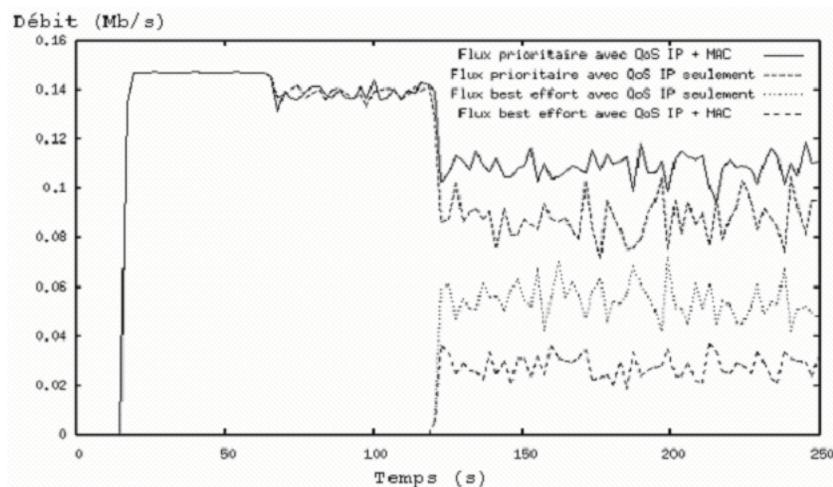


FIG. 3.16 – Débits avec différenciation de service IP et/ou MAC

Différenciation de terminaux combinée avec la QoS IP et MAC

Dans les sections précédentes, nous avons montré que :

- La différenciation de terminaux fournit des routes avec des liens stables, mais sans différenciation de flux,
- La QoS combinée au niveau IP et MAC améliore les délais et giges des trafics prioritaires. Le débit reste instable et fonction de la capacité du canal.

Maintenant, nous allons combiner les deux approches, en utilisant un algorithme de routage sensible à la qualité des liens, et une différenciation de service dans les couches

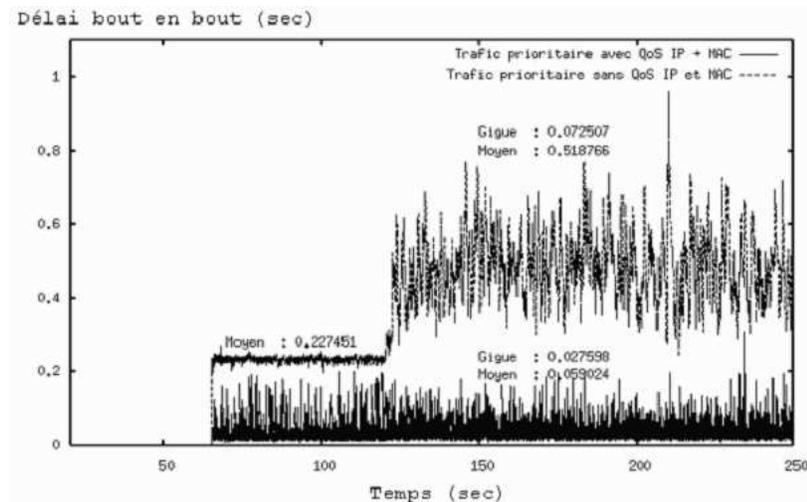


FIG. 3.17 – Délais avec différenciation de service IP et MAC

IP et MAC.

La figure 3.18 illustre le délai bout en bout des flux de haute priorité et best effort. On observe un délai (33 ms) et gigue (20 ms) réduit pour les trafics temps réel, qui permet une bonne qualité de communication. Comparé au cas où aucun mécanisme de différenciation n'est utilisé, le délai est réduit d'un facteur de 15 dans ce type de scénario. En outre, le débit des flux prioritaires (A à G et A à D) est garanti grâce à de meilleures qualités des liens. La combinaison de tous ces mécanismes fournit une meilleure performance dans un environnement ad hoc. La différenciation de terminaux assure une qualité des liens sans fil stable, de haute qualité avec un meilleur débit ; la QoS dans les couches IP et MAC réduit le délai bout en bout et la probabilité de perte des paquets des trafics temps réel.

3.5 Conclusion

Dans ce chapitre, nous avons montré quelques mécanismes de qualité de service pour supporter les applications temps réel dans un réseau ad hoc. La QoS au niveau IP et MAC permet de différencier les flux et de garantir la qualité de service des applications temps réel sensibles au délai, gigue et perte de paquets. Utiliser un protocole de routage hiérarchique avec différenciation de terminaux permet un contrôle supplémentaire sur le réseau. Il assure une stabilité des liens en prenant en compte le comportement de la couche MAC IEEE 802.11. En outre, la combinaison de la QoS IP et MAC avec le protocole de routage à liens de grande qualité améliore les performances du réseau, et des garanties de qualité de service peuvent être assurées aux flux temps réels.

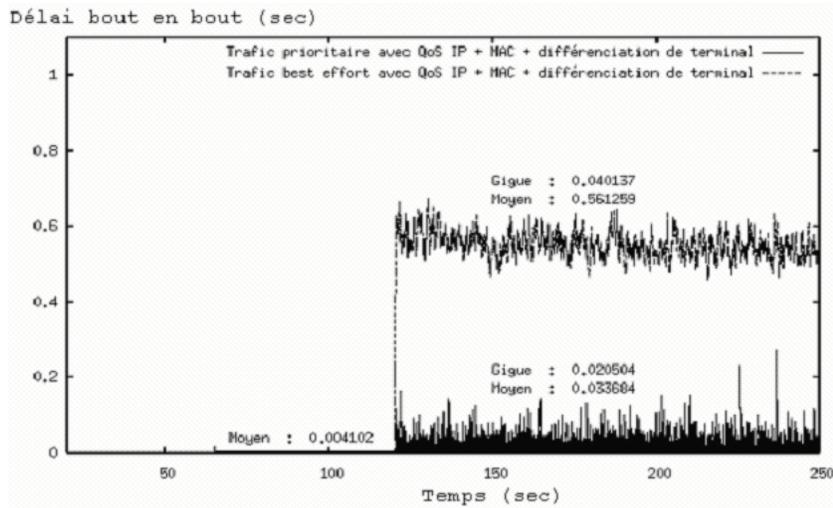


FIG. 3.18 – Délais avec QoS IP&MAC + différenciation de terminaux

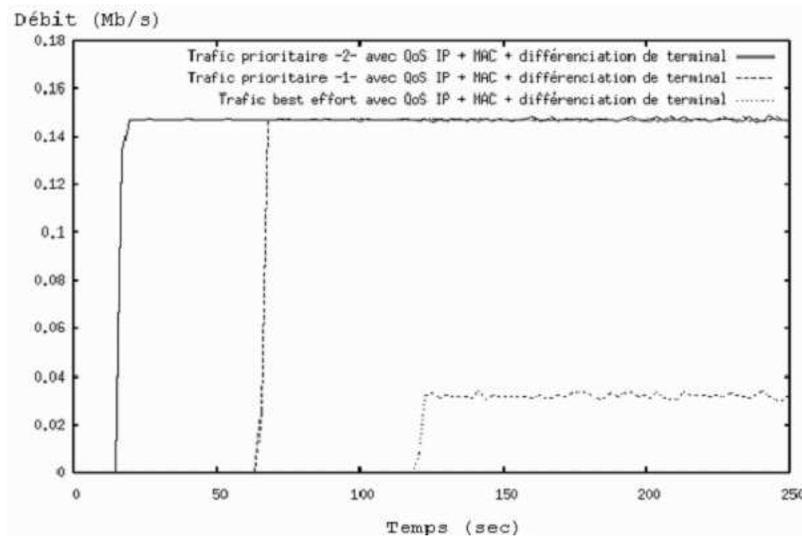


FIG. 3.19 – Débits avec QoS IP et MAC + différenciation de terminaux

Cependant, lorsque la charge du réseau augmente la combinaison des mécanismes proposés essaient de fournir au mieux la qualité de service des applications temps réel sans que cela soit garanti. C'est à dire que suivant la topologie du réseau et la nature des trafics lancés dans le réseau la combinaison de QoS proposée peut satisfaire complètement ou partiellement la qualité de service des trafics temps réel vu la qualité et la capacité des liens sans fil du réseau. Dans ce cas, un mécanisme de contrôle d'admission s'avère indispensable pour contrôler les trafics admis et éviter ainsi une surcharge du réseau. De plus, n'ayant aucun contrôle sur la topologie du réseau, il est très difficile d'assurer des liens sans fil stables vu les changements de topologie très fréquents dans les réseaux ad

hoc. Dans le prochain chapitre, nous proposons de contrôler la topologie du réseau ad hoc pour garantir des liens stables et contrôlables, sur lesquels les mécanismes de QoS peuvent être appliqués.

Chapitre 4

Contrôle de topologie orienté stratégie

4.1 Introduction

Il est certain qu'un réseau ad hoc offre des solutions flexibles aux utilisateurs mobiles sans l'existence d'infrastructure fixe. Cependant, il arrive qu'un ensemble de nœuds mobiles soit isolé du reste du réseau. Dans de telles situations, il serait inadéquat de demander à un utilisateur mobile de changer de position pour garantir la connectivité d'un autre utilisateur. De plus, lorsque le nombre de sauts et la qualité des liens des routes dans le réseau ne sont pas contrôlés, il est très difficile de garantir la qualité de service des communications temps réel en termes de délai de bout en bout et de débit. Les solutions dans la littérature ne permettent pas de répondre à ces questions. Elles se focalisent essentiellement sur la consommation d'énergie [17] [18] ou une représentation par clusters [15] [57] pour une meilleure gestion du réseau.

Dans ce chapitre nous présentons une nouvelle approche de contrôle de topologie dans les réseaux ad hoc. Elle est basée sur le déploiement d'un sous ensemble de routeurs mobiles dédiés [21] qui ont un rôle double. D'un côté, ils assurent une meilleure connectivité dans le réseau. D'un autre côté, ils garantissent un réseau ad hoc avec un diamètre limité et des liens sans fil stables qui permettent ainsi d'appliquer des mécanismes de qualité de service (comme vu dans le chapitre précédent). Le principe est de se servir de la mobilité qui est habituellement subie dans les réseaux ad hoc afin d'améliorer les performances du réseau. Des modèles relevant de la programmation linéaire entière mixte ont été établis pour décrire les déploiements.

La suite de ce chapitre est organisée de la manière suivante. Dans la section 2 nous décrivons les modèles utilisés pour réaliser le déploiement désiré. Les deux configurations où le réseau est autonome ou interconnecté à une infrastructure sont étudiées. Dans un premier temps, nous considérons le cas d'un réseau ad hoc statique, suivi du cas où

la topologie du réseau change en fonction de la mobilité des nœuds (section 3). Dans la section 4, nous décrivons l'environnement de simulation et présentons les résultats obtenus pour évaluer les performances du contrôle de topologie utilisé.

La modélisation réalisée dans ce chapitre a été effectuée sous la direction de M Nicolas PUECH, maître de conférence au département Informatique et Réseaux à L'Ecole Nationale Supérieure des Télécommunications.

4.2 Modélisation

Dans notre étude, la structure du réseau ad hoc est hiérarchique. Elle est composée de nœuds classiques et de routeurs mobiles dédiés (ex : routeurs SPIF [21]) utilisés spécialement pour le routage. Ces derniers disposent d'une grande autonomie (pas de problème d'énergie) et d'une grande capacité de transmission. On suppose aussi que tous les nœuds sont capables d'obtenir leurs positions à n'importe quel moment (ex : grâce à un dispositif GPS [19] dans un environnement extérieur ou Zigbee [125] pour un environnement intérieur). Dans le reste de ce chapitre, le terme 'routeur' désigne un routeur mobile dédié, et l'appellation station mobile ou nœud mobile est utilisée pour désigner un nœud classique.

Nous commençons dans la section suivante par modéliser le système dans le cas où le rôle confié aux routeurs dédiés est d'assurer une forte connectivité du réseau.

4.2.1 Contrôle de topologie orienté connectivité

Un réseau ad hoc est dit connecté si et seulement si il existe au moins une route entre chaque paire de nœuds mobiles. La connectivité dépend essentiellement de l'existence des routes. Elle est affectée par les changements de topologie dus à la mobilité : perte de liens, mises à jours des routes, reroutage, ...etc.

Dans le but d'assurer la connectivité, nous avons besoin de déterminer les positions vers lesquelles les routeurs mobiles doivent se déplacer afin de maximiser le nombre de nœuds couverts par ces derniers. Le déploiement des routeurs mobiles doit garantir un réseau backbone connecté.

Dans une application réaliste, l'intérêt d'un tel déploiement est son utilisation dans le cadre de déploiement des points d'accès ayant à déjà une connaissance sur la surface couverte et le nombre d'utilisateurs dans le réseau.

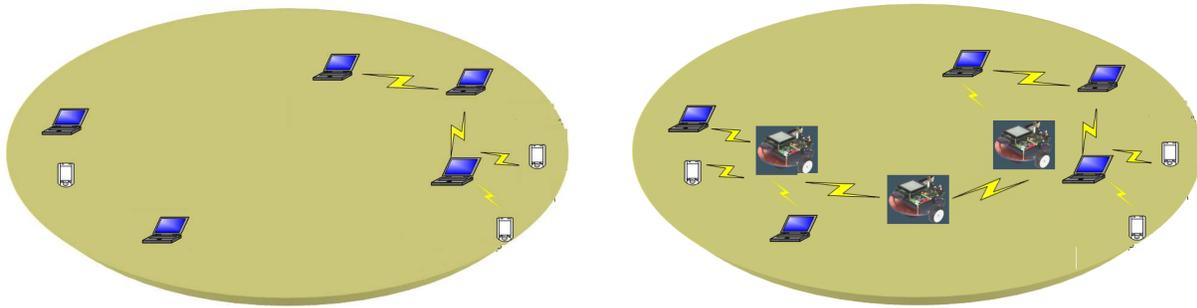


FIG. 4.1 – Topologie du réseau ad hoc avec et sans déploiement des routeurs mobiles

Pour modéliser le déploiement des routeurs mobiles en un problème de programmation linéaire mixte, nous allons d'abord identifier les différentes informations connues, à savoir le nombre et les positions des nœuds mobiles, le nombre de routeurs à déployer et la délimitation de la surface du réseau ad hoc. Ensuite, un ensemble de variables sont définies suivi de la description de la fonction objectif à maximiser (qui correspond au but du déploiement). Enfin, nous décrivons les différentes contraintes liées à la connectivité dans le réseau.

Les paramètres

Dans notre modèle nous considérons :

- N stations mobiles (SM) à couvrir par M routeurs mobiles (RM), tous localisés dans une surface rectangulaire plane $A \times B$,
- chaque nœud mobile SM_i est représenté par le point géométrique P_i de coordonnées (x_i, y_i) ,
- chaque routeur mobile RM_j est représenté par le point géométrique Q_j de coordonnées (a_j, b_j) ,
- R_r représente la portée de transmission du routeur mobile,
- R_m représente la portée de transmission de la station mobile,
- $d(J, K)$ représente la distance euclidienne entre les points géométriques J et K ($\sqrt{(x_J - x_K)^2 + (y_J - y_K)^2}$)

Pour être couvert par un routeur mobile, la distance entre la station mobile et le routeur mobile le plus proche doit être inférieure à R_m . Deux routeurs mobiles sont 'voisins' (c'est à dire adjacents dans le réseau backbone) si la distance entre eux est inférieure R_r .

La surface du déploiement est délimitée en $[x_{min}, x_{max}] \times [y_{min}, y_{max}]$, tel que :

$$\begin{aligned} x_{min} &= \min_{1 \leq i \leq N}(x_i), & x_{max} &= \max_{1 \leq i \leq N}(x_i) \\ y_{min} &= \min_{1 \leq i \leq N}(y_i), & y_{max} &= \max_{1 \leq i \leq N}(y_i) \end{aligned}$$

Les variables

Pour $i = 1, \dots, N$ et $j = 1, \dots, M$, (a_j, b_j) représentent les coordonnées du routeur RM_j ,

$$\text{Soit la variable } \lambda_{i,j} = \begin{cases} 1 & \text{si } d(P_i, Q_j) \leq R_m \\ 0 & \text{sinon} \end{cases} \quad (4.1)$$

Cette variable permet d'assurer la connectivité entre la station mobile SM_i et le routeur mobile RM_j . En d'autres termes, $\lambda_{i,j} = 1$ ssi la station mobile SM_i est couverte par le routeur mobile RM_j .

$$\text{Pour } i, j = 1, \dots, M, \quad \text{soit la variable } \mu_{i,j} = \begin{cases} 1 & \text{si } d(Q_i, Q_j) \leq R_r \\ 0 & \text{sinon} \end{cases} \quad (4.2)$$

Cette variable permet d'assurer la connectivité entre deux routeurs. C'est à dire, $\mu_{i,j} = 1$ ssi RM_i est un routeur adjacent au routeur RM_j dans le backbone formé de routeurs mobiles.

Le réseau backbone peut être représenté par un graphe dont les sommets sont les routeurs mobiles et dont la matrice d'adjacence est $(\mu_{i,j})$, $1 \leq i, j \leq M$.

Nous avons également défini la variable τ_i , telle que :
pour $i = 1, \dots, N$, $\tau_i = 1$ ssi SM_i est couverte par au moins un routeur mobile. Dans ce cas, il existe un routeur mobile (RM_j) pour lequel $\lambda_{i,j} = 1$.

Pour vérifier la connectivité du backbone (formé des routeurs mobiles), nous testons s'il y a possibilité de créer une route de n'importe quel routeur RM_s ($s = 2, \dots, M$) vers le routeur numéro 1 (RM_1). Pour cela il suffit de définir la variable suivante :

$$z_{i,j}^s = \begin{cases} 1 & \text{si la route du routeur } s \text{ vers le routeur } 1 \text{ traverse le lien } (i, j) \\ 0 & \text{sinon} \end{cases} \quad (4.3)$$

Le problème d'optimisation consiste à trouver les valeurs :

- Des positions des routeurs mobiles $Q_i(a_i, b_i)$, pour $i = 1, \dots, M$,
- De la variable $\lambda_{i,j}$, pour $i = 1, \dots, N$ et $j = 1, \dots, M$,
- De la variable $\mu_{i,j}$, pour $i, j = 1, \dots, M$

qui maximisent la fonction objectif suivante :

$$\sum_{i=1}^N \tau_i - \sum_{i,j,s} z_{i,j}^s \quad (4.4)$$

Le terme $\sum_{i=1}^N \tau_i$ représente le nombre total de stations mobiles couvertes par les routeurs mobiles (que nous voulons aussi grand que possible).

On soustrait $\sum_{i,j,s} z_{i,j}^s$ au terme précédent pour forcer les routes à être aussi courtes que possible dans le réseau coeur.

Dans ce qui suit nous allons décrire les différentes contraintes utilisées, qu'elles soient liées au domaine du déploiement, à la couverture (entre routeurs et nœuds ou entre routeurs eux mêmes), ainsi qu'aux routes à l'intérieur du backbone.

Contraintes du domaine de déploiement

Les positions des routeurs recherchées (a_i, b_i) doivent être délimitées par les localisations des nœuds.

$$a_i \in [x_{min}, x_{max}], \quad i = 1, \dots, M$$

$$b_i \in [y_{min}, y_{max}], \quad i = 1, \dots, M$$

Les variables utilisées dans notre modèle sont toutes binaires :

$$\tau_i \in \{0, 1\}, \quad i = 1, \dots, N$$

$$\lambda_{i,j} \in \{0, 1\}, \quad i = 1, \dots, N, j = 1, \dots, M$$

$$\mu_{i,j} \in \{0, 1\}, \quad i, j = 1, \dots, M$$

$$z_{i,j}^s \in \{0, 1\}, \quad i, j = 1, \dots, M, s = 2, \dots, M$$

Contraintes de couverture

Ces contraintes sont utilisées dans le but de garantir la connectivité entre les nœuds mobiles et les routeurs mobiles.

$$\lambda_{i,j} = 1 \iff d(P_i, Q_j) \leq R_m, \quad i = 1, \dots, N, j = 1, \dots, M \quad (4.5)$$

Le nœud SM_i est couvert par le routeur RM_j

$$\mu_{i,j} = 1 \iff d(Q_i, Q_j) \leq R_r, \quad i, j = 1, \dots, M \quad (4.6)$$

Le routeur RM_i est connecté au routeur RM_j

$$\lambda_{i,j} \leq \tau_i \leq \sum_{k=1}^M \lambda_{i,k}, \quad i = 1, \dots, N, j = 1, \dots, M \quad (4.7)$$

Cette contrainte permet de forcer un nœud à être couvert par au moins un routeur.

Contraintes de routes

$$z_{i,j}^s = 0, \quad i, s = 1, \dots, M \quad (4.8)$$

$$z_{i,j}^s \leq \mu_{i,j}, \quad i, j, s = 1, \dots, M \quad (4.9)$$

Cela signifie qu'il y a pas de trafics échangés entre RM_i et RM_j s'ils ne sont pas connectés.

$$\sum_{j=1}^M z_{i,j}^s - \sum_{j=1}^M z_{j,i}^s = \begin{cases} 0 & \text{si } i \neq s, i \neq 1; \quad i, s = 1, \dots, M \\ -\theta^s & \text{si } i = s; \quad i, s = 1, \dots, M \\ \theta^s & \text{si } i = 1; \quad s = 1, \dots, M \end{cases} \quad (4.10)$$

$$\text{où : } \theta^s = \begin{cases} 1 & \text{si } s = 2, \dots, M \\ 0 & \text{si } s = 1 \end{cases}$$

Ces deux dernières contraintes assurent l'existence d'une route entre chaque paire de routeurs afin de garder le backbone connecté, et assurent la conservation de flot au niveau du routeur mobile RM_i

Les contraintes de couverture étant quadratiques (distance euclidienne), nous les avons linéarisées afin d'être supportées par le solveur que nous avons utilisé (CPLEX [60]) et formulées dans un contexte de programmation linéaire entière mixte. Un exemple de modèle qui illustre la connectivité est décrit dans l'annexe en utilisant le langage AMPL [16].

Le tableau suivant résume les variables et données utilisées dans notre modèle.

Nom	Signification
N	Nombre de stations mobiles dans le réseau
M	Nombre de routeurs à déployer
(x_i, y_i)	Coordonnées des stations mobiles
R_m, R_r	Portée de transmission des stations et des routeurs
$A \times B$	Surface du réseau
$(x_{min}, x_{max}), (y_{min}, y_{max})$	Délimitation de la zone de déploiement
(a_j, b_j)	Coordonnées des routeurs mobiles
$\lambda_{i,j}, \mu_{i,j}, \tau_i, z_{i,j}^s$	Variables binaires définies

TAB. 4.1 – Liste des données et variables utilisées

La portée de transmission des routeurs mobiles R_r et celle des nœuds mobiles R_m étant constantes, la complexité du problème est principalement fonction du nombre de nœuds mobiles N et de routeurs mobiles M .

Jusque là nous avons vu la formulation du problème pour assurer la connectivité dans réseau ad hoc. La section suivante traite le déploiement permettant de limiter le diamètre du réseau.

4.2.2 Déploiement des routeurs mobiles orienté qualité de service

Dans les réseaux sans fil multisauts, les performances du réseau et le délai de bout en bout des communications dépendent principalement du nombre de sauts des routes. Ceci

est du au fait que les paquets acheminés sur une route subissent un délai au niveau de chaque nœud pour le traitement dans les files d'attente et un autre délai pour l'accès au lien sans fil partagé. Dans une topologie dynamique, les liens des routes sélectionnées sont instables et susceptibles à des variations dans le temps et dans l'espace.

Dans cette section, nous proposons de gérer la topologie du réseau en limitant le diamètre du réseau backbone. Avec un diamètre limité, nous réduisons le délai de bout en bout des communications transitant, et nous fournissons une certaine stabilité et un contrôle sur le réseau. Ainsi, l'utilisation des schémas de QoS classiques peut être ajoutée pour améliorer davantage le délai des applications temps réel.

Dans les réseaux ad hoc, le délai de bout en bout d'un nœud source MS_s vers un nœud destination MS_d transitant par H sauts est représenté comme :

$$D(s, d) = H \times (AverNodeDelay + T_{trans} + T_{prop}) \quad (4.11)$$

Où : T_{trans} : délai de transmission (longueur du paquet/débit de transmission)

T_{prop} : délai de propagation (négligeable)

$$AverNodeDelay = \frac{\sum_{k \in path(s \rightarrow d)} Nodedelay(k)}{H}$$

$$Nodedelay(k) = queue_delay(k) + MAC_delay(k)$$

Dans le déploiement orienté QoS des routeurs dédiés, les contraintes liées au diamètre du backbone sont ajoutées dans la formulation du problème : le nombre maximum de sauts, fixé à H , entre deux routeurs mobiles est fixé afin de satisfaire le pire cas. Le délai maximum toléré est étudié (100ms) et nous avons considéré le pire délai par saut, qui est fonction des longueurs des buffers, du nombre de routeurs mobiles disponible, et de la charge du réseau (quantité de trafics circulant dans le réseau). La valeur de H doit être limitée quand un plus grand délai est nécessaire pour acheminer les paquets au niveau IP (file d'attente) et au niveau MAC, quand une congestion apparaît.

Le problème est légèrement différent de celui formulé pour l'objectif de la connectivité. Une contrainte supplémentaire est ajoutée pour caractériser le diamètre du réseau backbone (fixé à H). Elle est formulée comme suit :

Contrainte du diamètre

$$\sum_{1 \leq i, j \leq M} z_{i,j}^s \leq \frac{H}{2}, \quad s = 1, \dots, M \quad (4.12)$$

Cette contrainte oblige les routes entre les routeurs mobiles les plus distants à être au maximum égale à H sauts.

4.2.3 Cas d'un réseau ad hoc interconnecté à une infrastructure fixe

Dans l'optique des réseaux 4G et l'évolution des réseaux mobile, nous considérons les réseaux ad hoc comme un moyen efficace pour étendre l'accès et les services de l'infrastructure filaire. Pour ce, nous nous intéressons dans cette section au déploiement des routeurs dans une configuration dans laquelle le réseau n'est pas autonome.

Le modèle doit prendre en considération le fait qu'au moins un routeur mobile est connecté directement à l'infrastructure via une passerelle. La formulation des problèmes est presque la même que dans le cas d'un réseau ad hoc autonome. Dans cette configuration réseau chaque routeur mobile doit avoir une route vers la passerelle fixe, il est suffisant de considérer la passerelle comme un $(M + 1)$ ième routeur mobile, ayant une position géométrique prédéfinie. Ainsi, $M + 1$ routeurs mobiles sont pris en compte dans le modèle, nous avons simplement ajouté une contrainte sur la position de la passerelle formulée comme suit :

$$\begin{cases} a_{M+1} = x_{passerelle} \\ b_{M+1} = y_{passerelle} \end{cases} \quad (4.13)$$

Dans ce cas, le problème reste formulé comme un problème de programmation linéaire entière mixte (MILP : Mixed Integer Linear Program) avec cette dernière contrainte additionnelle. La connectivité du backbone réseau ou l'objectif de QoS reste garanti comme décrit précédemment.

4.2.4 Fonctionnement général

Nous allons décrire ici les étapes suivies pour réaliser l'une des stratégies de déploiement proposées. Comme illustré dans la figure 4.2 :

- La première phase consiste à collecter les positions des nœuds. Dans ce cas, chaque nœud envoie ses coordonnées (X,Y) dans un paquet de contrôle vers une entité centralisée,
- Une fois les positions des nœuds récupérées par l'entité de calcul, cette dernière résout (avec l'outil CPLEX dans notre cas) le modèle approprié suivant la stratégie adoptée et calcule les positions des routeurs mobiles,
- La dernière étape consiste à déplacer les routeurs vers les positions désirées, accomplissant ainsi la tâche requise.

A noter que le calcul centralisé des positions des routeurs mobiles est choisi pour sa simplicité. L'entité centralisée disposant d'une grande capacité de traitement, permet d'avoir une vue sur l'ensemble du réseau.

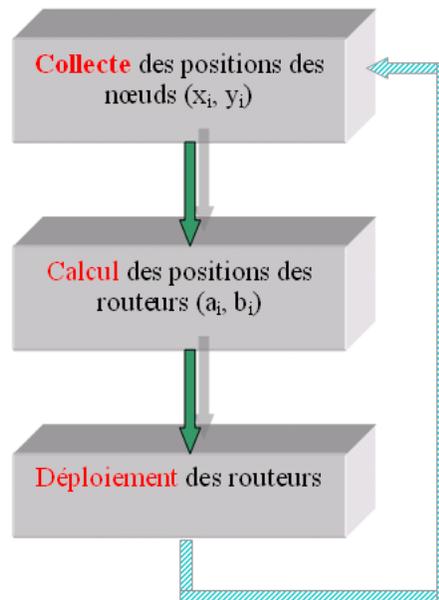


FIG. 4.2 – Fonctionnement général du contrôle de topologie

Il existe cependant le cas où des nœuds ne sont pas 'joignables' par les autres dans la première phase de collecte des positions. Dans cette situation, la solution consiste à utiliser un routeur mobile pour prospecter les nœuds isolés du réseau afin de récupérer toutes les positions, afin de pouvoir par la suite calculer les positions des routeurs.

4.3 Contrôle de topologie dans un environnement mobile

Dans la section précédente, nous avons traité le cas où la topologie du réseau est fixe. Dans cette section, le cas où les nœuds sont mobiles engendrant des changements de topologies fréquents est étudié. Le problème consiste à calculer périodiquement les positions des routeurs mobiles suite aux changements des nœuds, afin de garantir une meilleure connectivité ou un backbone de diamètre limité.

Une première idée consisterait à utiliser le même modèle défini pour le cas statique. Dans cette solution, à chaque intervalle de temps bien défini Δt , les nouvelles positions des nœuds mobiles sont réintroduites dans le modèle pour avoir les nouvelles positions des routeurs mobiles. Cette solution est certes très simple et ne nécessite aucune modification dans le modèle décrit précédemment, cependant elle ne prend pas en considération l'historique du réseau (la topologie précédente du réseau). Autrement dit, si on dispose d'un déploiement à l'instant (t_1), à l'instant ($t_2, t_2 > t_1$) le nouveau déploiement des routeurs peut :

- Engendrer de longs déplacements pour les routeurs relativement à leurs anciennes positions,
- Causer d'importantes interruptions de communications déjà en cours.

Pour remédier à ces problèmes, nous proposons de développer un autre modèle en s'appuyant sur le modèle déjà proposé pour un réseau statique afin :

1. De minimiser le déplacement effectué par chaque routeur mobile entre l'instant (t_1) et l'instant (t_2) (voir figure 4.3),
2. De conserver le maximum de communications qui étaient déjà en cours,
3. Et de garantir au même temps l'objectif désiré (connectivité ou QoS).

Pour cela, un ensemble de variables et de contraintes sont ajoutées. La fonction objectif est à son tour modifiée pour assurer un déplacement optimal des routeurs mobiles.

L'intervalle de temps pendant lequel les positions des routeurs sont mises à jour est principalement lié à la mobilité des nœuds mobiles. Un temps court correspond à une topologie très variable, où le déploiement doit s'adapter et correspondre à la morphologie du réseau.

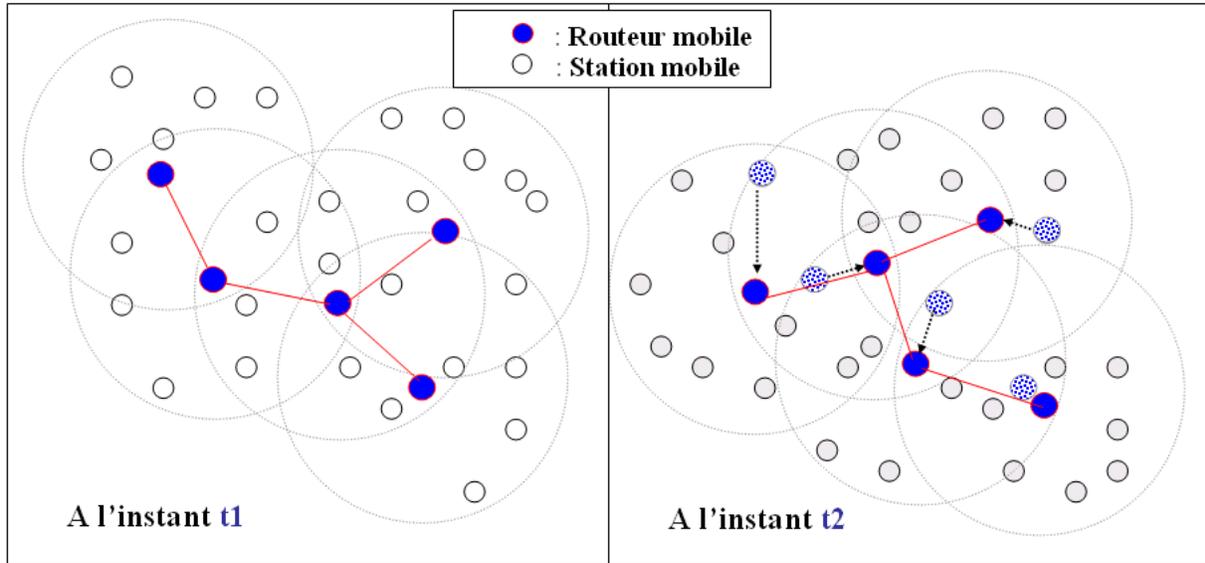


FIG. 4.3 – Déploiement dynamique des routeurs mobiles

4.3.1 Extension du modèle dans un environnement ad hoc dynamique

Il s'agit toujours de trouver les nouvelles positions des routeurs mobiles $Q(a_i, b_i)$ à l'instant t_2 , sachant qu'on dispose en plus :

- des anciennes positions des routeurs $Q^{t_1}(a_i^{t_1}, b_i^{t_1})$,
- ainsi que des valeurs de la variable $\lambda_{i,j}^{t_1}$ obtenues à l'instant t_1 , pour $i = 1, \dots, N$ et $j = 1, \dots, M$.

De plus, outre les variables et les contraintes définies dans le modèle précédent, nous allons définir :

- la variable binaire C_i qui correspond au changement de couverture (ou de connectivité) d'une station mobile par un routeur mobile, tel que : pour $i = 1, \dots, N$

$$C_i = \begin{cases} 1 & \text{si la station } MS_i \text{ reste couverte à l'instant } t_2 \text{ par le même routeur mobile} \\ 0 & \text{si la station } MS_i \text{ n'est plus couverte par le même routeur mobile à l'instant } t_2 \end{cases} \quad (4.14)$$

- afin de forcer les stations mobiles à rester couvertes par les mêmes routeurs mobiles, nous définissons la contrainte suivante :

$$0 \leq \lambda_{i,j}^{t1} \times \lambda_{i,j} \leq C_i \leq \sum_{j=1}^M \lambda_{i,j}^{t1} \times \lambda_{i,j} \quad i = 1, \dots, N \quad (4.15)$$

- La nouvelle fonction objectif à maximiser devient :

$$\left(\sum_{i=1}^N \tau_i - \sum_{i,j,s} z_{i,j}^s \right) + \sum_{i=1}^N C_i - \sum_{j=1}^M d(Q_j^{t1}, Q_j) \quad (4.16)$$

Le premier terme de la fonction est le même que dans le modèle statique que nous voulons maximiser. Nous voulons également maximiser le deuxième terme afin qu'un grand nombre de stations mobiles restent couvertes par les mêmes routeurs mobiles à l'instant t2 pour éviter les changements de routes. Le dernier terme sert à minimiser le déplacement effectué par les routeurs entre l'instant t1 et t2.

4.4 Simulations et résultats

Dans cette section, nous allons montrer l'intérêt de l'utilisation de notre approche en utilisant des simulations. CPLEX [60], un solveur des problèmes de programmation linéaire mixte, a été utilisé pour résoudre les modèles proposés. Les modèles soumis au solveur sont décrits à l'aide du langage AMPL[16].

Nous allons d'abord illustrer le résultat du déploiement des routeurs mobiles afin d'assurer la connectivité. Ensuite, nous étudions la relation entre la surface du réseau $A \times B$, le nombre de nœuds N , la portée de transmission des routeurs mobiles et le nombre optimal des routeurs (M) nécessaires pour couvrir les nœuds. On considère que le réseau est complètement couvert si le taux de nœuds couverts est supérieur ou égale à 95 %.

Pour mesurer l'impact du déploiement orienté qualité de service sur les performances des trafics (délai bout en bout et débit), l'outil de simulation NS-2 [34] est utilisé. Quand les positions des routeurs mobiles sont obtenues à l'aide du solveur CPLEX (voire figure 4.4), elles sont injectées dans le modèle de simulation NS-2. Le but de ces simulations est de montrer que le déploiement avec QoS utilisé améliore les performances du réseau ad hoc, tout en utilisant un nombre optimal de routeurs dédiés. Nous montrons à la fin un exemple de déploiement dynamique pour illustrer le déplacement intelligent des routeurs pour conserver le plus de communications en cours et réduire les distances parcourues entre chaque changement de topologie.

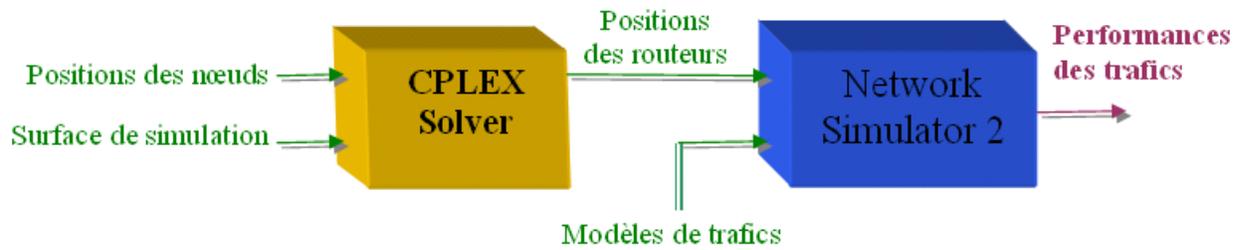


FIG. 4.4 – Outils utilisés dans les simulations

4.4.1 Connectivité

La figure 4.5 illustre un exemple de déploiement des routeurs dans un réseau autonome pour assurer la connectivité. Dans cette topologie, les paramètres suivants sont considérés : la surface de simulation est de $1000 \times 1000m^2$, le nombre de nœuds mobiles est $N=100$ (aléatoirement générés), et la portée de transmission des nœuds et des routeurs mobiles sont respectivement $R_m = 150m$, $R_r = 220m$. Nous constatons que $M=11$ routeurs mobiles sont suffisants pour assurer une connectivité globale du réseau.

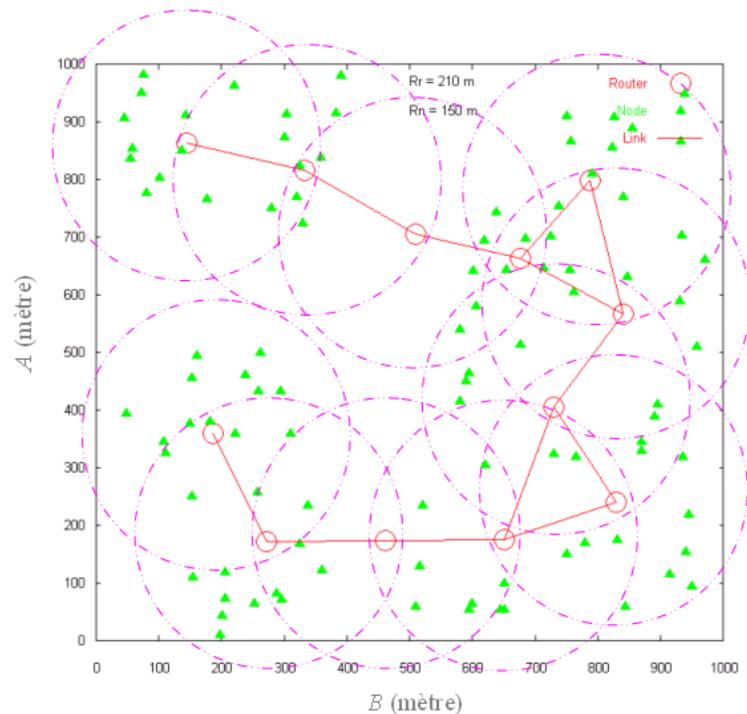


FIG. 4.5 – Exemple de déploiement orienté connectivité des routeurs dans un réseaux ad hoc autonome

Dans la figure 4.6, une autre topologie a été utilisée. On remarque que 7 routeurs sont

nécessaires pour couvrir tous les nœuds mobiles (dans un réseau de 50 nœuds situés sur une surface de $800m \times 800m$, avec un $R_m = 150m$ et un $R_r = 200m$).

Nous remarquons que le déploiement des routeurs est différent suivant que le réseau est autonome ou interconnecté à une passerelle fixe. Dans le cas d'un réseau interconnecté à une infrastructure, nous constatons qu'un routeur dédié est spécialement déployé à côté de la passerelle pour assurer l'extension et relie deux routeurs dédiés, sans qu'il ne couvre aucun nœud dans le réseau.

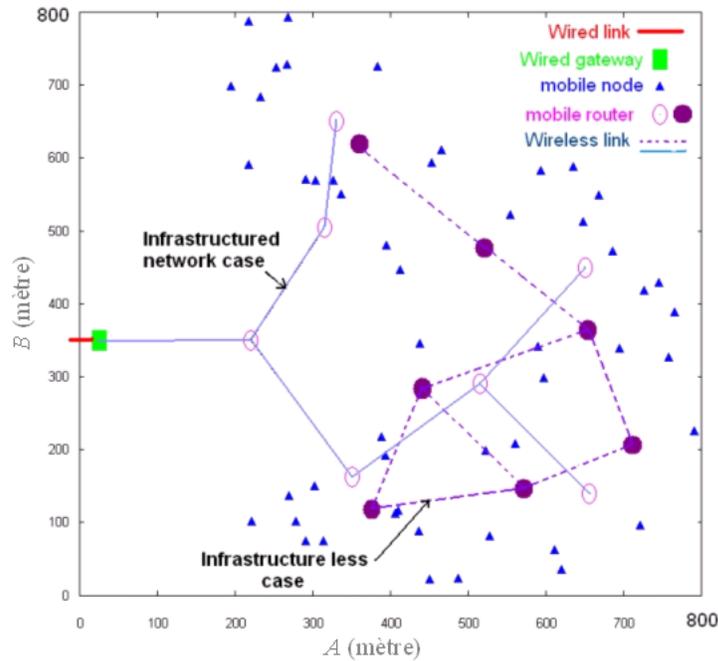


FIG. 4.6 – Déploiement des routeurs dans un réseau autonome ou interconnecté à une infrastructure

Nombre optimal de routeurs dédiés

Pour montrer la relation entre le nombre de routeurs déployés et la topologie du réseau, nous avons étudié des topologies de réseaux avec 30 (respectivement 60 ou 100) nœuds mobiles dans une surface d'une taille de $500 \times 500m^2$ (respectivement $750 \times 750m^2$ ou $1000 \times 1000m^2$). Dans chaque cas, nous avons aléatoirement généré 20 réseaux et représentons les valeurs moyennes calculées à partir des résultats obtenus. La portée de transmission des routeurs mobiles est de 150 m, 225 m ou 300 m. Sur les figures 4.7 4.8 4.9, les résultats prouvent que le nombre optimal de routeurs mobiles requis pour assurer la connectivité est proportionnel à la surface, et proportionnel au nombre de nœuds et disproportionné à la portée de transmission des routeurs mobiles. A titre d'exemple, nous trouvons que $M=15$ routeurs avec une portée de transmission R_r de 150 mètres sont

exigés pour réaliser la connectivité dans une topologie de 60 nœuds sur une surface de $1000 \times 1000m^2$. Ce nombre décroît avec une portée de transmission supérieure ($M=9$ pour une valeur de $R_r = 300m$), car quand les routeurs disposent d'une grande portée de transmission ils assurent la couverture des nœuds tout en restant couverts et distants les uns des autres.

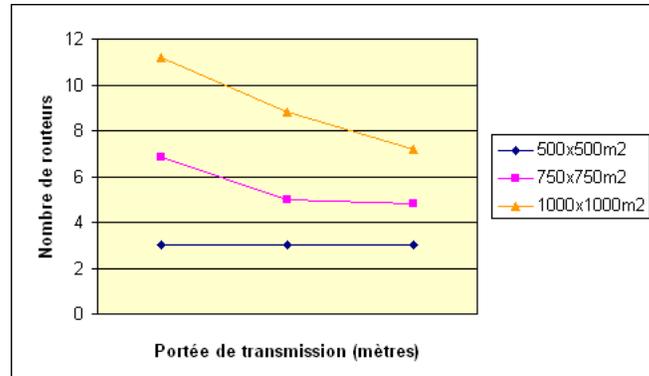


FIG. 4.7 – Nombre optimal de routeurs dans un réseau ad hoc à 30 nœuds

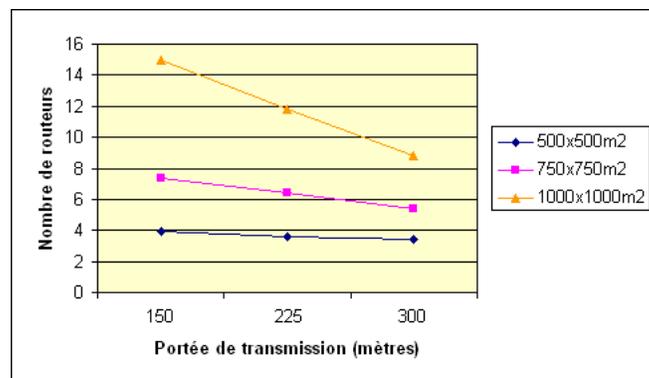


FIG. 4.8 – Nombre optimal de routeurs dans un réseau ad hoc à 60 nœuds

4.4.2 Déploiement orienté QoS

Pour montrer les performances du réseau sous le déploiement orienté QoS, nous avons effectué une série de simulations en utilisant NS-2 [34]. Il s'agit de 7 topologies de réseau de 50 nœuds aléatoirement situés sur une surface de $800 \times 800m^2$. La couche MAC IEEE 802.11 a été utilisée, où tous les routeurs mobiles disposent d'un débit de 11 Mb/s. Les autres nœuds ont (aléatoirement) un débit de 2 ou de 11Mb/s. Le protocole de routage DSDV est employé. Pour chaque topologie de réseau étudiée, les positions des routeurs mobiles sont obtenues par le solveur CPLEX suivant le modèle orienté QoS décrit dans la section précédente.

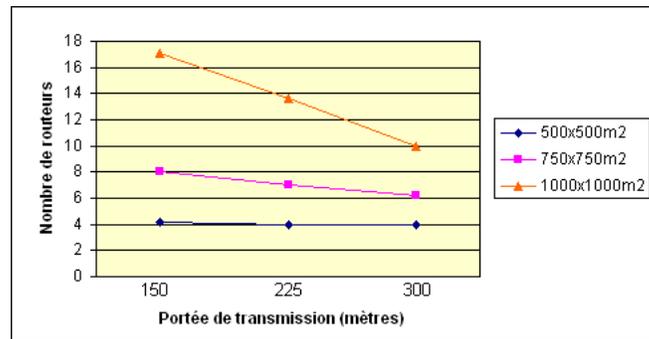


FIG. 4.9 – Nombre optimal de routeurs dans un réseau ad hoc à 100 nœuds

Pour chaque topologie réseau, nous produisons aléatoirement de 17 applications de CBR avec un débit de 32kbps et une taille de paquet de 512 bytes, pendant un temps de simulation de 300 secondes. Le but de nos simulations est de comparer la performance du réseau sous différentes conditions. La figure 4.10 et 4.11 montre le délai bout en bout ainsi que taux moyen de la livraison et de perte des paquets moyen des trafics considérés :

- Sans utiliser les routeurs mobiles,
- Avec une approche de clustering, où les nœuds mobiles élisent les nœuds ayant un débit élevé comme cluster-heads,
- En utilisant notre modèle orienté QoS,
- En utilisant un nombre fixe de routeurs mobiles uniformément distribués sur la surface de simulation, afin de couvrir entièrement la surface de simulation.

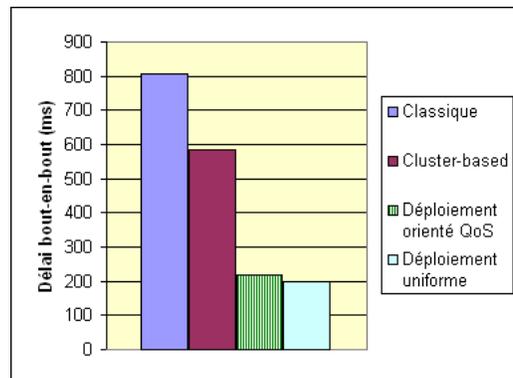


FIG. 4.10 – Délai moyen obtenu dans chaque approche

Dans le cas d'un réseau ad hoc classique, les routes utilisées pour router les paquets sont souvent de mauvaise qualité en terme de capacité de lien. Par conséquent, les itinéraires deviennent rapidement encombrés. Ainsi, le délai moyen est assez élevé (806 ms) et le débit des flux n'est pas satisfait. Pour une approche de clustering, les figures 4.11 4.10 montrent de meilleures performances. Dans une telle approche, des liens de capacité élevée peuvent être choisis pour transmettre et relayer les communications, réduisant de ce fait

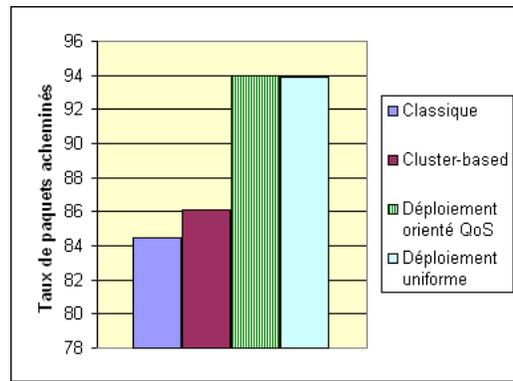


FIG. 4.11 – Taux de paquets reçus dans chaque approche

le délai et les pertes de paquets.

Quand notre déploiement est utilisé les résultats obtenus montrent encore plus d'améliorations (délai moyen inférieur à 220ms) et un taux de perte de 7 % (très bas relativement aux deux premiers cas). Dans ce cas, les routeurs mobiles sont déployés selon les positions des autres nœuds dans le réseau. Ils permettent de former un cœur de réseau de haute qualité de lien avec un diamètre limité et ils fournissent des itinéraires courts et meilleurs en capacité. En outre, puisque les routeurs mobiles sont dédiés pour le routage, ils ont une portée de transmission élevée et une capacité élevée de lien. Par conséquent, le débit et le délai des trafics transitant sont améliorés. Notez que, si une différenciation de service est effectuée à la couche IP ou MAC, les besoins des applications temps réel en terme de débit, délai bout en bout et gigue peuvent être garantis.

Dans la dernière approche, quand un grand nombre de routeurs mobiles est déployés uniformément pour couvrir la surface de simulation, on remarque naturellement des résultats améliorés. Cependant, ce déploiement n'est pas optimal en termes de nombre de routeurs. Ce déploiement est fonction de la surface de simulation indépendamment des nœuds du réseau contrairement à notre approche. Notre approche montre presque les mêmes performances, avec un nombre réduit de routeurs intelligemment déployés.

4.4.3 Déploiement dynamique

Dans cette section, nous étudions un exemple de déploiement dynamique orienté connectivité dans une topologie composée de 15 nœuds mobiles se déplaçant à une vitesse de 7km/h dans une surface de $700 \times 700m^2$. Cinq trafics d'un débit de 30kb/s sont aléatoirement lancés dans le réseau. Les paramètres étudiés dans cette simulation sont : le déplacement des routeurs effectué entre chaque changement de topologie ainsi que les changements de routes dus aux déplacements des routeurs (perte de connectivité d'un

nœud avec le routeur associé).

Dans ces simulations nous n'avons pas pu résoudre le modèle, décrit pour le déploiement dynamique, avec le solveur CPLEX car les contraintes quadratiques ne sont pas supportées par ce dernier. Pour palier ce problème et pour des facteurs de temps, nous avons appliqué le modèle statique à des moments périodiques (chaque 30 secondes), et sachant que le modèle permet de fournir une multitude de solutions, nous sélectionnons manuellement les solutions qui correspondent aux contraintes liées au déploiement dynamique. Le solveur CPLEX est alors utilisé pour résoudre le modèle, et l'outil de simulation NS-2 pour la mesure de performance.

Nous comparons la distance moyenne parcourue par les routeurs mobiles avec et sans prise en compte des contraintes de mobilité. On remarque comme attendu que quand le déploiement est recalculé sans prendre en considération les anciennes positions des routeurs dans le réseau, la distance de déplacement est assez grande (214m) comparé au deuxième cas plus amélioré (72m). Car dans une telle situation, un routeur se trouvant à droite de la surface de simulation peut après quelques secondes de l'autre côté de la topologie, en effectuant ainsi un grand déplacement et un grand changement dans la topologie.

Par ailleurs, bien que le mobilité des noeuds engendre des changements de routes dans le réseau, nous constatons moins de cassure de liens (93 changements contre changements 37 durant toute la durée de simulation) quand les nœuds mobiles essayent de rester attachés aux mêmes routeurs selon nos contraintes. Comme pour la distance parcourue, les routeurs qui effectuent des déplacements optimaux risquent moins de causer des pertes de liens sans fil et par conséquent moins de changements de routes.

4.5 Conclusion

Nous avons présenté dans ce chapitre un nouveau mécanisme de contrôle de topologie. Il s'agit du déploiement d'un ensemble de routeurs mobiles dédiés de capacité élevée dans un environnement statique ou mobile. Le but de notre approche est d'assurer une forte connectivité ou un diamètre limité du réseau ad hoc. Pour chaque stratégie, le problème a été formulé comme un problème de programmation linéaire entière mixte. Les réseaux autonomes ou liés à un réseau filaire sont considérés dans notre étude. Les résultats de simulation prouvent que l'approche proposée améliore de manière significative les performances du réseau ad hoc. De plus, le temps nécessaire pour résoudre les modèles proposés est raisonnable pour des topologies allant jusqu'à une centaine de nœuds, ce qui les rendent applicables dans des déploiements réalistes.

Le modèle présenté dans ce chapitre nous permet d'avoir les positions des routeurs

mobiles. Néanmoins, la solution du MILP n'est pas unique, et offre une multitude de solutions. Dans ce cas les positions des routeurs peuvent être raffinées afin de prendre en considération non seulement la distance euclidienne comme critère, mais aussi d'autres paramètres comme la qualité des liens où la gestion d'énergie.

Un autre aspect important dans les réseaux ad hoc est l'équilibrage de charge. Notre proposition de déploiement peut ainsi être améliorée dans le but d'équilibrer la charge entre régions d'un réseau, en déplaçant des routeurs mobiles vers des zones du réseau où cela s'avère nécessaire. On peut également imaginer des situations où nos modèles peuvent être étendus dans le but d'inclure d'autres contraintes spécifiques à une application ou à une configuration du réseau ad hoc.

De plus, notre solution de contrôle de topologie se base essentiellement sur une entité centralisée qui effectue le calcul des positions. Cependant, il serait intéressant de concevoir une approche distribuée, plus adaptée à l'environnement des réseaux ad hoc. Dans une telle approche, l'objectif est de répartir la tâche de contrôle de topologie en un ensemble de contrôles de topologie régionaux.

Le chapitre suivant est consacré à la description de la plate-forme ; celle-ci a été réalisée dans le cadre du projet ITEA Ambience.

Chapitre 5

Plate-forme

5.1 Introduction

L'objectif de ce chapitre est de présenter la plate-forme que nous avons réalisée dans le cadre du projet ITEA Ambience [23]. Réalisée en collaboration avec plusieurs partenaires académiques et industriels cette plate-forme intègre plusieurs technologies de domaines différents et fournit un ensemble de services aux utilisateurs mobiles dans un environnement hétérogène tout en démontrant l'efficacité d'une partie des mécanismes proposés dans les chapitres précédents.

Le projet ITEA Ambience fait référence à un nouveau paradigme de la technologie de l'information, dans lequel le traitement de l'information est réparti sur tous les objets de l'environnement des utilisateurs. Ces derniers peuvent ainsi être assistés par une intelligence ambiante apportée par cet environnement. Cet environnement se maintient informé de leur présence et du contexte, il est sensible, adaptatif et attentif à leurs besoins, habitudes, et attitudes.

Les environnements intelligents ambiants peuvent être caractérisés par les éléments de base suivants : ubiquité, conscience (awareness), intelligence, et interaction naturelle. Ce paradigme émerge de la combinaison de possibilités technologiques nouvelles : omniprésence de capacités de traitement de l'information embarqué, disponibilité de capteurs et actionneurs en technologies banalisées, et de la tendance à un enrichissement et à une plus grande convivialité des interfaces utilisateur. Il met en œuvre des technologies de communication innovantes (réseaux ad hoc, middleware de découverte de services) permettant de former dynamiquement des réseaux en particulier sur la base d'appareils mobiles mais aussi d'appareils fixes devenant accessibles à distance. En y ajoutant des procédés d'interaction adaptatifs basés sur des nouveaux concepts (interfaces naturelles, interfaces tangibles), l'environnement numérique devrait contribuer à l'amélioration de la

qualité de vie des personnes en prenant mieux en compte leur comportement.

Dans ce qui suit, nous allons d'abord présenter le projet ITEA Ambience. Ensuite, nous détaillons l'architecture adoptée pour la plate-forme. Nous mettons l'accent par la suite sur le serveur, l'architecture réseau, le routage ainsi que les applications graphiques que nous avons développés. L'intégration avec les autres partenaires ainsi que les outils matériels et logiciels utilisés sont également décrits.

5.2 Le projet AMBIENCE

L'objectif du projet Ambience est de générer des concepts pour les environnements intelligents ambiants et de développer des architectures, des procédés et des outils utiles à de futurs développements de produits dans ce contexte. Le consortium a démontré ces concepts et technologies sur des plates-formes opérationnelles essentiellement pour des environnements d'intérieur du domaine domestique mais aussi professionnel. Les questions auxquelles le projet a tâché de répondre sont les suivantes :

Quels sont les centres d'intérêt et les besoins clés des utilisateurs ? Ce défi a été relevé en mettant en place des scénarios utiles et plaisants sur les applications et services qui ont été démontrés.

Quelle est l'architecture la plus appropriée pour un environnement intelligent ?

Le système devait notamment prendre en compte la diversité des appareils interconnectés, l'hétérogénéité des réseaux mis en œuvre, et devait être capable de tolérer une intelligence distribuée.

Comment gérer efficacement un tel système ? Il devait supporter divers types de média de type graphique, vidéo, audio, parole, manuscrit. Cette abondance d'information suppose des procédés d'indexation et de recherche d'information avancés.

Comment personnaliser ces systèmes intelligents ? Le caractère adaptatif du système a été jugé au travers de ses capacités à deviner les intuitions et les habitudes de l'utilisateur. La personnalisation s'est effectuée au travers d'un système d'apprentissage analysant les interactions entre la machine et l'utilisateur.

Le projet Ambience a été divisé en quatre groupes de travail (Work Package), dont le Work Package 1 Ubiquité dans lequel nous avons participé. Son but est d'assurer des services transparents sans couture à des utilisateurs nomades se déplaçant dans un environnement sans fil. Le travail consiste à :

- Définir les besoins du système pour la fourniture de services sans couture et transparents aux utilisateurs nomades se déplaçant dans un bâtiment ou dans des environnements d'affaires ou public à travers un ensemble de réseaux d'accès et de terminaux différents,
 - La fourniture de services adaptatifs pour des équipements physiques immergeant plus intuitifs et d'une largeur de bande plus large qu'avec celle disponible avec
-

les terminaux traditionnels. La fourniture de nouveaux services basés-réseau pour toutes sortes de dispositifs physiques,

- Évaluez la convenance des protocoles de réseau existants et émergents et les infrastructures logicielles distribuées,
- Développer une plate-forme pour le projet, probablement avec des variantes s'il y a lieu pour les différents environnements en utilisant les modules logiciels pour mettre en application cette plate-forme. Définir les besoins du système et des utilisateurs, concevoir l'architecture du système et de mettre en œuvre les applications nécessaires et les intégrer dans une plate-forme finale.

Dans le projet Ambience on distingue également le Work Package 2 pour l'identification et le positionnement, le Work Package 3 pour la gestion de la partie intelligence, ainsi que le Work Package 4 pour la partie interaction naturelle

5.3 Présentation générale de la plate-forme

La plate-forme fait partie du démonstrateur M1 'Find a meeting' que nous avons réalisé dans le cadre du groupe de travail WP1. Dans ce contexte, l'objectif est de fournir un accès omniprésent à un réseau mobile intelligent ambiant avec un support des communications temps réel. Dans un tel environnement, le réseau doit s'adapter aux variations de l'environnement et doit être sensible aux besoins des applications des utilisateurs.

Cette plate-forme permet d'assurer des services sans couture et transparents aux différents utilisateurs ayant des capacités différentes, se déplaçant dans un bâtiment ou dans un environnement public à travers différents réseaux d'accès dans un environnement complètement hétérogène.

L'application adoptée dans notre contexte est la gestion d'une conférence. Les participants disposent d'un terminal mobile (iPAQ) doté d'une application intuitive offrant plusieurs fonctionnalités. Ces dernières permettant d'aider les utilisateurs au bon déroulement de la conférence à partir de la phase d'enregistrement jusqu'à la fin des réunions.

Dès le début du projet, il est apparu le besoin d'avoir une vue globale sur l'architecture fonctionnelle de l'environnement ambiant. L'ENST a contribué, dans le cadre d'un groupe architecture, à établir un schéma sur l'organisation fonctionnelle du réseau ambiant en spécifiant des blocs aussi génériques que possible.

5.3.1 Architecture globale

La figure 5.1 illustre l'architecture générale du système. Au cœur, se trouve le serveur qui gère les applications et achemine les informations à travers tout le système. L'authentification biométrique est réalisée par reconnaissance vocale qui établit le lien entre la personne physique (participant) et l'iPAQ (application Client). Chaque iPAQ dispose d'une jaquette avec les technologies WLAN et ZigBee [125] (une technologie de positionnement développée par Philips). Ce dispositif ZigBee communique avec une infrastructure ZigBee (des balises déployées dans des endroits connus à l'avance) pour fournir une estimation de la position suivant des mesures RSSI (Received Signal Strength Information). Les messages envoyés sont acheminés vers l'iPAQ grâce au réseau local sans fil (WLAN) pour informer les participants sur les réunions et le programme de la conférence.

Le participant peut demander d'être guidé vers une salle ou une personne de la conférence. La localisation des utilisateurs est périodiquement mise à jour au niveau du serveur, engendrant ainsi une carte interactive au niveau de l'interface utilisateur lors de changement de position. Les messages sont définis au format XML pour faciliter la manipulation des données. Le client échange des messages avec le serveur sous forme de message de demande à qui le serveur répond à chaque fois, qui est une sorte de messages 'update' réguliers.

La couverture réseau est étendue au-delà de l'infrastructure fixe grâce à l'utilisation du réseau ad hoc en utilisant les autres iPAQs ou les routeurs mobiles particulièrement conçus pour prévoir la coupure de connexion et se déplacent pour entendre convenablement le réseau.

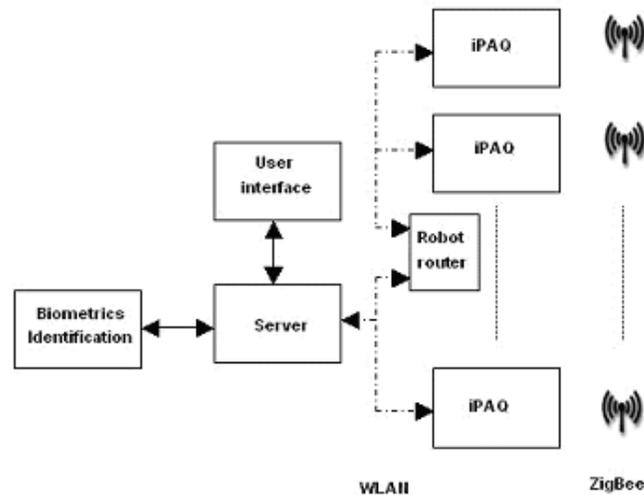


FIG. 5.1 – Architecture globale de la plate-forme

Cette plate-forme a été le fruit de la collaboration des différents partenaires du projet

spécialisés dans les technologies suivantes :

- Reconnaissance de la parole - Thales, France
- Client et système d'échange de messages XML - CCC, Finlande
- Localisation ZigBee - Philips, UK
- Analyse et gestion du réseau - LIP6, France
- Serveur - Nous (ENST Paris) , France
- Routeurs et leur déplacement - Nous (ENST Paris) , France
- Communications sans fil et routage Ad Hoc - Nous (ENST Paris), France

Dans la section suivante, nous allons décrire le phase de reconnaissance de la parole utilisée quand un nouveau participant s'enregistre à la conférence, suivie de la présentation de la technologie de localisation qui permet de suivre les positions des participants.

5.3.2 Identification biométrique basée sur la voix

La procédure *offline*

Cette phase est conçue pour produire une carte d'identité (identité biométrique) pour le délégué. Cette carte d'identité forme le lien entre le délégué physique et son profil numérique. En entrant dans le bâtiment où se déroule la conférence, le délégué s'adresse au bureau de réception. Le réceptionniste utilise 'l'application bienvenue' pour lancer le procédé d'authentification où :

1. Le délégué fournit des preuves d'identité,
2. Le réceptionniste recherche le délégué dans la base de données partagée,
3. Une fois trouvé, le délégué parle dans un microphone pour enregistrer un échantillon de sa voix,
4. 'L'application bienvenue' crée un profil biométrique de l'échantillon de voix et le stocke dans la base de données,
5. 'L'application bienvenue' extrait les données du délégué à partir de la base de données et crée un certificat X509 avec une extension biométrique. Ce certificat est la carte d'identité,
6. Le délégué reçoit une carte MMC (MultiMedia Card) avec la nouvelle identité biométrique. Ce processus est illustré sur le schéma 5.2.

Enregistrement des services

Quand le PDA, porté par le délégué, est détecté par le réseau pour la première fois, il obtient une identité utilisateur non sécurisée. La carte d'identité du délégué est utilisée pour établir une connexion SSL. L'utilisateur est incité à s'authentifier pour les services de

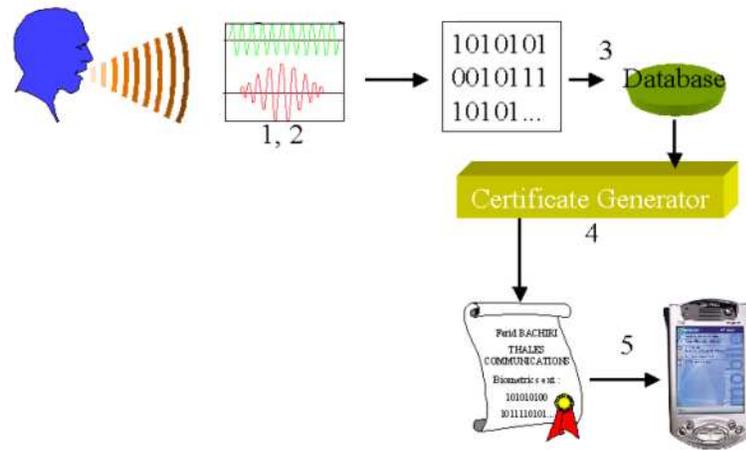


FIG. 5.2 – Etape *offline* de l'identification biométrique

la conférence en parlant dans le microphone du PDA. Quelques secondes du discours sont enregistrées. L'échantillon de voix obtenu est envoyé au serveur à travers la connexion SSL. Le serveur recherche le profil biométrique du délégué dans la base de données partagée et les propriétés biométriques sont comparées pour enfin accorder ou refuser l'accès aux services de la conférence.

5.3.3 Système de localisation ZigBee

La technologie de positionnement utilisée pour la plate-forme est basée sur le système par radio ZigBee [125]. Un certain nombre de balises de ZigBee sont installées à des positions connues fixes à travers tout le site où se déroule la conférence, de sorte qu'au moins deux balises puissent être détectées à n'importe quel un point. Une radio ZigBee est également construite dans chaque jaquette de l'iPAQ fournissant une interface série au PDA.

La radio ZigBee incluse dans la jaquette de l'iPAQ détecte les balises qui sont dans sa portée et mesure leur puissance du signal. Cette information est compilée et mise dans un message de balise par le PDA et expédiée au serveur. Le serveur utilise une table pour convertir la force de signal en portée de chaque balise fixe. Ce principe fournit des informations suffisantes pour récupérer la position de l'utilisateur, en utilisant un algorithme de triangulation. Ce processus met à jour la position de chaque iPAQ toutes les 2 ou 3 secondes. La position est alors filtrée avec des évaluations précédentes de position pour produire une position raffinée plus fiable.

La section suivante décrit le principe de fonctionnement de l'architecture Client/Serveur.

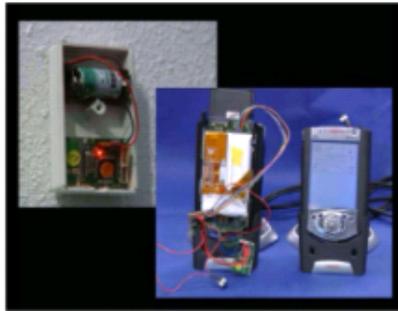


FIG. 5.3 – Système de localisation ZigBee

Nous détaillerons les composants du serveur que nous avons réalisés et nous présenterons le client développé par le partenaire CCC.

5.4 Architecture Client/Serveur

Dans la plate-forme, nous avons adopté une architecture Client/Serveur afin de rendre accessibles les applications aux utilisateurs mobiles. Pour la conception du serveur, la solution logicielle est basée sur un serveur Tomcat et un conteneur de servlets java. Ecrit en Java, Tomcat nécessite pour pouvoir fonctionner la présence d'une machine virtuelle Java, et plus précisément du SDK - Sun Développement Kit - complet. A ce titre, Tomcat est totalement portable et peut être, très aisément mis en œuvre sur un grand choix de plates-formes, tels que Unix, Linux ou Windows. Il peut fonctionner seul ou en amont d'un serveur Apache ou Microsoft.

Cette plate-forme serveur permet une grande évolutivité dans le panel des services par la facilité de développement, héritée du langage Java, des servlets et Java Server Page. A partir de la version 1.4, Java intègre directement la librairie JSSE. Celle-ci permet la gestion des connexions sécurisées par SSL. En outre, l'installation d'un serveur Tomcat est des plus simples. Robuste et fiable, il fournit un service HTML de base, et reste résolument dédié en priorité aux servlets Java. Les applications peuvent être installées manuellement ou automatiquement (fichiers WAR).

Une autre solution consisterait à utiliser le couple Apache - serveur HTML. Dans ce cas de figure, le serveur Apache sert de portail d'accès. L'interconnexion entre Apache et Tomcat s'effectue au moyen d'un connecteur logiciel JK2. Celui-ci permet à Apache de considérer Tomcat comme un de ses modules. L'intérêt de cette architecture est la grande robustesse grâce à la possibilité de faire du partage de charge automatique. Cependant, le connecteur JK2 est toujours en cours de développement. De plus, il dispose d'un en-

semble de fonctionnalités restreintes en terme d'échange d'information intra plate-forme. Ce défaut est malheureusement rédhibitoire pour le développement du serveur Ambience.



FIG. 5.4 – Architecture Client/Serveur

5.4.1 Les services

Les services offerts par le serveur sont développés sous forme de modules indépendants (classes java) et offrent aux clients les possibilités de communication suivantes :

- authentification vocale du client,
- localisation du client (ou d'autres clients connectés au réseau) par affichage d'une carte du site et positionnement,
- envoi et réception de messages courts,
- consultation de documents.

5.4.2 La sécurisation de l'échange des données

La sécurité des communications est assurée par l'utilisation de SSL et des certificats X-509 en une authentification mutuelle client - serveur et en cryptant les données échangées. Cette authentification sécurisée est gérée par Tomcat. L'accès aux services offerts par le serveur est de plus soumis à la vérification de l'identité et de l'empreinte vocale.

L'inscription, la gestion des participants, ainsi que l'échange de données, sont réalisés

au travers d'une base de données MySQL. Le système de gestion de base de données MySQL est disponible pour les principaux systèmes d'exploitation et s'intègre parfaitement à une plate-forme serveur Apache Tomcat. Cette base de données regroupe les informations principales suivantes :

- La liste des participants,
- Les paramètres vocaux des participants (pour l'authentification),
- La liste des participants présents sur le site de la conférence,
- La position géographique des participants,
- L'inscription des participants aux conférences,
- La liste des documents consultables.

La gestion des données propres à une conférence est réalisée à travers l'interface Chairman, développée en marge du serveur. La gestion technique de la base de données s'effectue grâce à l'interface de type Web fournie par PHPMyAdmin (celle-ci nécessite la présence d'un serveur de type Apache).

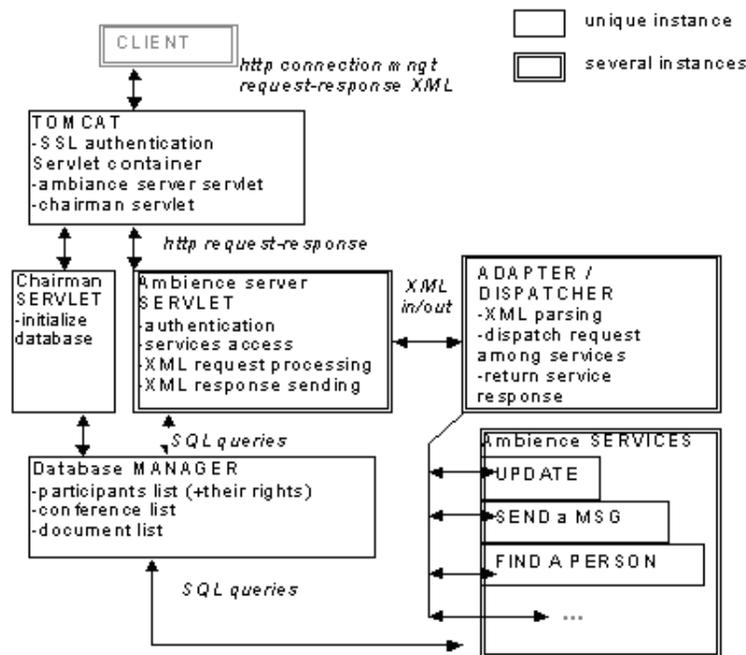


FIG. 5.5 – Architecture du serveur

5.4.3 Le Client

Dans la plate-forme, la réalisation du client a été développée par CCC. Les iPAQ où sont implantés les clients sont équipés du système d'exploitation Familiar Linux et l'environnement d'exécution Java Blackdown. L'application Client est compatible avec

l'édition Java 1.3.1. Tous les échanges de messages entre les clients et le serveur sont basés sur XML, qui peut être facilement étendu pour des besoins futurs. Le choix des standards ouverts, tels que Java et XML, donne l'avantage de la flexibilité et le support d'une grande variété d'équipements et environnements client.

5.4.4 L'interface utilisateur graphique de l'iPAQ (Graphical User Interface)

Elle est basée sur Java et permet à l'utilisateur de choisir et de commander les applications disponibles. Elle fournit une interface utilisateur simple qui permet d'alterner entre un certain nombre d'onglets, dont :

Le plan : carte d'affichage du plan local avec localisation de l'utilisateur mobile,

Information : affiche les informations d'état du système à un moment donné,

Find a meeting : fournit au client la localisation géographique de la salle de conférence,

Find a person : fournit au client la localisation géographique d'une personne participant à la même conférence,

Read a document : offre la possibilité de consulter des documents numériques correspondants à la conférence,

Send a message : permet au client d'envoyer un message à une personne ou à un groupe,

Update : permet la mise à jour régulière des informations disponibles pour le client.

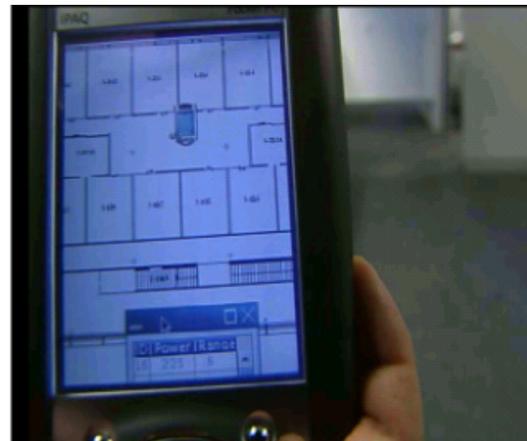
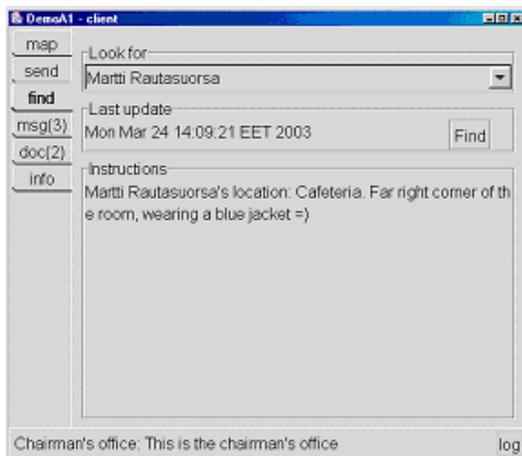


FIG. 5.6 – Exemple de la fonctionnalité *Find* et *map*

5.4.5 Principe de fonctionnement général entre le client et le serveur

A la première connexion d'un client, le serveur Tomcat réalise l'authentification SSL. Une fois celle-ci passée, la connexion sécurisée est établie. La servlet Ambience est instanciée. Le nom et le prénom du détenteur du client sont extraits du certificat SSL et comparés à la liste des participants. Dans le cas d'une concordance, la servlet Ambience autorise la poursuite de la connexion et une instance des classes Adapter et de celles correspondant à chaque service sont créés.

Le client envoie au serveur un premier message 'client update'. le serveur répond par un message 'server challenge' demandant l'identifiant vocal du client. Celui-ci renvoie une empreinte vocale, encodée en base64, et encapsulée dans un message 'client bioauth'. L'empreinte vocale est comparée à celle présente dans la base de données au moyen de la routine développée par la société Thalès. Si le client est enfin authentifié, le serveur renvoi un 'server update' contenant toutes les informations qui le concernent : liste des participants, liste des documents disponibles, et messages (éventuellement). Une fois passée toute l'étape d'authentification, les messages échangés sont de deux types :

- Les messages provoqués par une demande de service de la part du client. Il s'agit de l'envoi d'un message à un autre participant, d'une demande de localisation, de la lecture d'un document.
- Les messages automatiques. Ce sont les messages 'update' et 'beacon'.

Les messages 'update' sont régulièrement envoyés par le client au serveur. Celui-ci renvoie toutes les modifications intervenues dans la listes des clients, des documents et les nouveaux messages, depuis le dernier update. Les messages 'beacon' renvoient au serveur une liste des balises détectées par le Zigbee (paramètres : identifiant, puissance, distance). Le serveur récupère ces données pour calculer la position du client. Tout client déconnecté du réseau doit repasser par l'étape de l'authentification.

5.5 Architecture réseau

L'architecture réseau est représentée par une combinaison d'un réseau filaire et d'un réseau sans fil. Le réseau sans fil est un réseau ad hoc qui permet l'extension de l'infrastructure filaire, où la connectivité est assurée par les routeurs mobiles intelligents, à savoir les routeurs. Le réseau ad hoc conçu dans le projet Ambience correspond à la figure 5.7. Il constitue un moyen d'accès au réseau fixe même lorsque les utilisateurs ne sont pas dans la portée de transmission du point d'accès. Les routeurs mobiles constituent un cœur de réseau contrôlable dont le but est :

1. D'assurer la connectivité (routeur intelligent, aucune mobilité d'utilisateur requise),
-

2. D'étendre le réseau filaire existant,
3. D'élargir la couverture radio du réseau sans fil.

Dans ce contexte, les routeurs mobiles fournissent une certaine valeur ajoutée au réseau. Ils se déplaceront pour fournir la connectivité sans fil et l'adaptation des liens sans fil. En outre, les routeurs puisqu'ils sont consacrés au routage, peuvent supporter plusieurs interfaces sans fil afin de fournir un pont entre différentes technologies sans fil. En outre, la consommation de batterie n'est pas un problème puisque les routeurs possèdent une autonomie élevée et peuvent aller se charger quand cela est nécessaire (sur une station dédiée de rechargement).

Avoir un contrôle sur le réseau est essentiel afin de fournir une qualité acceptable des liens sans fil et d'ajouter par la suite des mécanismes de QoS dans le réseau. Par conséquent, la quantité du trafic peut être contrôlée et les liens de bonne qualité peuvent être maintenus.

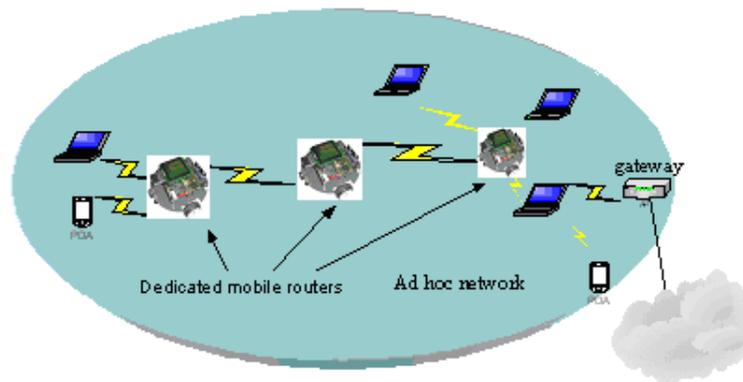


FIG. 5.7 – Architecture réseau basée sur les routeurs mobiles

5.5.1 Le routage ad hoc

Nous avons été amené à installer et configurer le protocole de routage OLSR [66] sur les différents terminaux mobiles (ordinateurs portables, iPAQ et routeurs mobiles). Une version IPv6 du protocole OLSR a été aussi développée et testée à petite échelle. Une proposition pour la modification du protocole OLSR pour le support de la différenciation de terminaux a été proposée. Deux types de terminaux sont considérés : les nœuds supportant la fonctionnalité de routage (routeur mobile ou portables), et ceux qui la supportant pas (PDA, terminaux Bluetooth). Un tel routage permettra de contrôler le réseau et d'assurer des liens sans fil de bonne qualité pour améliorer les performances du réseau en supportant les services temps réel.

5.5.2 Les routeurs mobiles

Les routeurs mobiles [21] ont été conçus et réalisés au sein du département Informatique et Réseaux (INFRES) à l'ENST. Leur architecture est ouverte et modulaire, et offre plusieurs standards de communications : Ethernet, 802.11 et Bluetooth. Elle fournit également un éventail d'interfaces d'entrée/sortie : USB, I2C, PCMCIA, 115 kbits IRDA, ISO 7816-2 Smartcard, CODEC audio 8 bits, écran d'affichage graphique à cristaux liquides.

La batterie est commandée par un circuit dédié qui maintient le processeur au courant de son niveau de charge. Quand le niveau de batterie atteint une basse limite, le routeur accomplira ses tâches critiques, et le cas échéant effectue un mouvement vers une station intelligente de réapprovisionnement en énergie. Cette station émet un rayon laser pour guider le routeur.

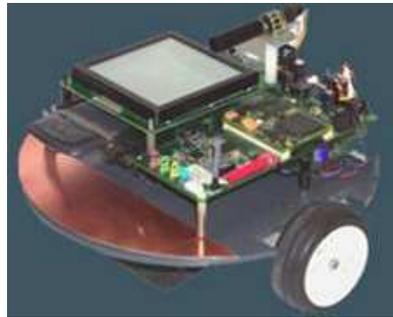


FIG. 5.8 – Routeur mobile (SPIF)

Déplacement des routeurs mobiles

L'intelligence des routeurs a été conçue autour de l'architecture InViWo [45](Intuitive Virtual Worlds), qui est un environnement de développement élaborée par l'ENST, le LIP6 et l'INRIA). Dans ce modèle, tout est représenté par un agent, le routeur lui-même est un agent. De son point de vue, le monde extérieur est composé d'un ensemble d'agents. Selon les stimuli reçus de l'extérieur et suivant son état interne, les modules comportementaux proposeront des actions à l'arbitre de l'agent. Le but de cet arbitre est de résoudre des conflits et de prendre une décision qui maximisera l'efficacité du routeur.

Quand plusieurs routeurs collaborent pour réaliser un but commun, ils échangeront des messages (vus comme stimulus par les autres routeurs) sur leurs actions prévues. Chaque arbitre tiendra compte alors d'autres routeurs pour définir sa propre stratégie, en apportant ainsi une action commune décentralisée. Le routeur garde une carte de son environnement, composée de plusieurs sous-cartes. Une de ces cartes est celle représentant

les obstacles fixes. Par exemple, le routeur essaiera de ne pas se mettre près d'un endroit dangereux (trous ou aux escaliers). En outre, il marquera quelques secteurs, ouvertures des portes par exemple, comme potentiellement dangereux.

Lors de l'élaboration d'un chemin, le routeur essaiera d'éviter les secteurs potentiellement dangereux et refusera de passer par les zones dangereuses. Une autre carte contient les environnements immédiats du routeur, avec une précision de 5cm de 5cm. Le routeur ajoutera n'importe quel obstacle qu'il peut rencontrer dans cette carte. Chaque obstacle est associé à un poids qui peut diminuer avec le temps. Cependant, si un obstacle déjà connu est de nouveau détecté, son poids sera considérablement augmenté de sorte à réduire les chances de le rencontrer ultérieurement.

5.6 Les applications GNetWatch et NetSim

Le serveur dispose également de deux applications graphiques *GNetWatch* et *NetSim* qui permettent d'avoir une vue globale sur l'état du système et sur les changements de topologie dans le réseau. *GNetWatch* (figure 5.9) est composé de deux parties (écrites en Java) : Serveur et Client, et permet de visualiser les nœuds mobiles sur un plan donné. D'un côté, le serveur permet d'effectuer la collecte des informations sur les utilisateurs mobiles et les stocke dans une base de données. D'un autre côté, le client constitue une représentation graphique du contenu de la base de données.

Quand le serveur est démarré, nous avons la possibilité soit : de représenter les événements réalisés dans le réseau ou de rejouer des scénarios déjà stockés dans le fichier de log. Les liens et les routes entre les nœuds mobiles peuvent être partiellement ou entièrement visualisés (figure 5.10 à droite).

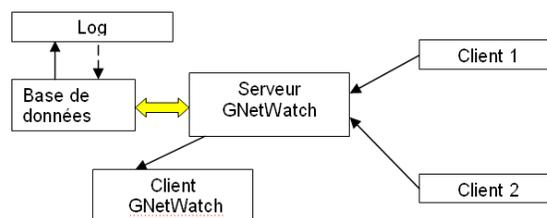


FIG. 5.9 – Architecture de GNetWatch

NetSim est aussi interfacé avec la partie *GNetWatch*. L'interface graphique '*NetSim*' permet d'afficher plus d'informations liées à l'identité de chaque client tel que les caractéristiques réseau (adresse IP, adresse de sous réseau, adresse MAC, SSID, la table de routage, puissance du signal, ...etc.), et la position (X, Y, Z) du terminal. Une représen-

tation graphique temps réel est assurée par l'application GNetWatch pour la visualisation de chaque utilisateur dans le plan de la conférence. Nous avons programmé un scénario pour l'application graphique NetSim où des utilisateurs sont créés avec des caractéristiques prédéfinies. NetSim est connecté à chaque client. Les nœuds du réseau envoient les messages à NetSim qui les affiche à son tour.

Phase d'intégration de la plate-forme

Afin de mener à bien la plate-forme finale du projet Ambience, nous avons à la fin du projet contribuer à :

- La participation à l'intégration du système de localisation développé par Philips,
- L'intégration de l'authentification vocale produite par Thalès,
- Test avec l'application client développée par CCC,
- La phase d'intégration finale des différentes parties développées par les partenaires impliqués dans la plate-forme pour une démonstration commune à la fin du projet.

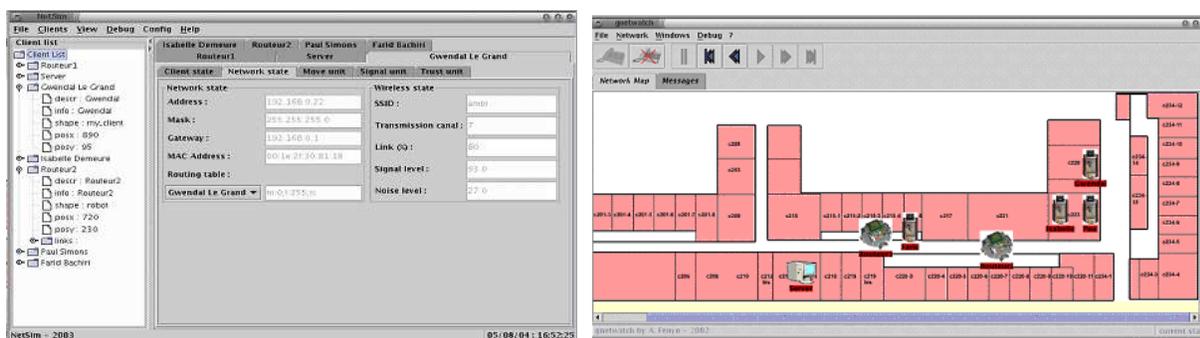


FIG. 5.10 – Applications graphiques pour monitorer les utilisateurs mobiles

Matériels et logiciels utilisés

Le développement a été réalisé sur un portable NEC (Pentium III 700MHz - 192 Mo) sous environnement linux (Red Hat 7.3). Le client a été installé sur un pocket pc iPAQ 3870, le système d'exploitation d'origine (Pocket PC 2002) a été remplacé par une distribution Linux Familiar version 0.6.1 avec la JVM diffusée par Blackdown (Java 1.3.1). 5 routeurs mobiles spif doté de la version 2.4.19 du noyau linux. Le module JSSE est nécessaire pour la gestion des communications sécurisées (SSL). Lors des deux périodes d'intégration, l'interface ZigBee (système de localisation par balise développé par Philips) a été ajoutée à l'iPAQ.

Le développement a été réalisé avec les logiciels suivants :

- Kit de développement Java 1.3.1 ;
- Base de données MySQL 3.23.53 ;
- Connecteur JDBC 3.0.

5.7 Conclusion

Dans ce chapitre nous avons présenté les différentes composantes de la plate-forme réalisée dans le démonstrateur du projet Ambience. Un ensemble de services sont offerts aux utilisateurs mobiles au sein d'une conférence. Une extension du réseau filaire est assurée par un réseau ad hoc, principalement contrôlé par des routeurs mobiles dédiés pour le routage et la gestion de la topologie. Pour garantir des services temps réel dans un tel environnement, une gestion multicouches IP et MAC est envisagée. Elle est utilisée en parallèle avec un routage avec différenciation de terminaux.

Cette plate-forme offre la possibilité de voir l'apport des différents mécanismes dans une vue globale du système, où les différentes composantes et technologies sont intégrées et interopèrent pour un fonctionnement efficace.

Le projet étant terminé en novembre 2003 et pour des contraintes de temps, la différenciation de service au niveau MAC (modification des codes des drivers des cartes sans fil) décrit dans le chapitre 3 n'a pas pu être intégrée dans la plate-forme.

Conclusion et Perspectives

Nous avons tenté à travers cette thèse d'apporter quelques solutions aux problèmes liés à la qualité de service dans les réseaux sans fil ad hoc. Notre démarche a consisté à agir au niveau des différents composants qui influencent le bon fonctionnement du réseau ad hoc.

Dans un premier temps, nous nous sommes d'abord intéressés à un autre aspect de la différenciation, appelé différenciation de terminaux. Cette tendance est née suite à l'hétérogénéité des équipements mobiles vendus sur le marché. Cette approche consiste à préférer les terminaux à haute capacité de transmission pour la fonction de routage par rapport aux terminaux de faible capacité. Une nouvelle métrique du protocole de routage est alors considérée à savoir la sélection des routes qui offrent le maximum de capacité. Le cas particulier du protocole de routage ad hoc DSR a été étudié et étendu pour supporter cette nouvelle fonctionnalité. Nous avons montré à travers des simulations intensives l'intérêt de la différenciation de terminaux dans l'amélioration des performances du réseau en terme de délai de bout en bout et de taux de perte.

Ensuite, nous nous sommes intéressés aux techniques de différenciation avancées. D'abord, nous avons proposé la combinaison de deux approches de différenciation connues pour leur efficacité dans l'apport de la qualité de service dans les réseaux ad hoc, à savoir la différenciation au niveau de la couche IP qui implique la priorité de la file d'attente, et la différenciation au niveau de la couche MAC qui agit sur la priorité d'accès au canal. La combinaison de ces deux niveaux de différenciation assure aux trafics temps réel la priorité au traitement par rapport aux trafics moins prioritaires au niveau du même terminal, et la priorité à l'accès par rapport aux terminaux voisins partageant le canal sans fil. Nous avons validé cette approche en utilisant l'outil de simulation NS-2 sous différents scénarios de trafics et de mobilité.

Un autre volet de notre thèse traite du contrôle de topologie dans les réseaux ad hoc. Contrairement aux approches étudiées dans la littérature, nous nous servons de la mobilité d'un ensemble de routeurs mobiles, jusqu' alors subie, afin de garantir à la fois une

meilleure connectivité et de limiter le diamètre du réseau. En limitant le diamètre du réseau, nous contrôlons ainsi les longueurs et la stabilité des routes. Lorsque la topologie du réseau est contrôlée, les mécanismes de qualités de service peuvent être déployés efficacement afin de mieux répondre aux exigences des applications temps réel. Nous nous sommes intéressés à deux configurations du réseau ad hoc à savoir les réseaux autonomes et les réseaux liés à une infrastructure. Par ailleurs, nous avons étudié le déploiement dynamique des routeurs. Lorsque les nœuds sont mobiles, cela engendre des changements de topologies fréquents. Le déploiement dynamique consiste à calculer périodiquement les positions des routeurs mobiles suite aux changements de topologie afin de garantir une meilleure connectivité ou un réseau cœur de diamètre limité.

Enfin, l'objectif du projet Ambience auquel nous avons participé, est de générer des concepts pour les environnements intelligents ambiants, de développer des architectures, des procédés et des outils utiles à de futurs développements de produits dans ce contexte. Nous avons élaboré dans le cadre de ce projet une plate-forme qui représente un exemple d'application des réseaux ad hoc pour lesquels des concepts de support de qualité de service ont été proposés. Un ensemble de services sont offerts aux utilisateurs mobiles au sein d'une conférence. Une extension du réseau filaire est assurée par un réseau ad hoc, principalement contrôlé par des robots mobiles dédiés pour le routage et la gestion de la topologie.

Toutefois, dans la continuité du travail présenté, nous pourrions approfondir notre étude afin d'améliorer les résultats obtenus. En particulier, l'étude de la gestion multicouches (réseau et lien) de la qualité de service peut être améliorée pour inclure la couche application. Dans ce cas, la couche application peut adapter le débit des flux en fonction des informations fournies par les couches basses. Parallèlement, un mécanisme de contrôle d'admission serait intéressant à étudier et permettrait de contrôler la charge du réseau et de réguler le nombre de trafics acceptés dans le réseau ad hoc.

Pour le contrôle de topologie proposé, nous nous sommes focalisés sur la modélisation du déploiement des routeurs dédiés dans un réseau ad hoc statique ou dynamique. Le modèle proposé peut être étendu afin de prendre compte d'autres contraintes (d'énergie, qualité des liens ou autres), et/ou pour définir d'autres objectifs de déploiement comme l'équilibrage de charge par exemple. De plus, une autre voie importante à explorer serait d'étudier et de concevoir une approche de déploiement distribuée plus adaptée à l'environnement des réseaux ad hoc.

Par ailleurs, pour le déploiement des routeurs dans un environnement dynamique, au lieu d'utiliser une formulation en MILP il serait également possible de trouver les positions des routeurs mobiles en utilisant des métaheuristiques telles que 'la recherche tabou' ou 'le recuit simulé' qui permettent de fournir un ensemble de solutions à notre problème de déploiement.

Finalement, la plate-forme développée dans le cadre du projet Ambience pourrait être étendue pour implémenter et évaluer les performances d'autres mécanismes de qualité de service.

Annexe

Environnement de simulations et outils utilisés

NS2 est un simulateur à événements discrets développé dans le but de recherche. Il est orienté objet (écrit en C++ et en oTCL), et il est fourni avec des outils d'analyse complémentaires eux-mêmes écrits en C/C++ ou TCL/Tk. NS2 fournit un environnement permettant de réaliser des simulations entre autre des protocoles IP, TCP, routage et des protocoles multicast dans les réseaux filaires ainsi que dans les réseaux sans fil, avec support de la mobilité des nœuds. Network Simulator 2 a été originellement développé étant que variante du "REAL network simulator" en 1989, et a considérablement évolué au cours des années. En 1995, NS-2 était développé par le projet VINT (collaboration des chercheurs à UC Berkeley, LBL, USC/ISI et Xerox PARC). Actuellement, son développement est supporté par le DARPA à travers SAMAN et par la NSF à travers CONSER, tout en incluant de nombreuses contributions extérieures, comme en particulier les codes pour les réseaux sans fil des projets Daedalus de l'UCB et Monarch de la CMU et de Sun Microsystems.

Par défaut le débit offert par la couche IEEE 802.11 est de 2Mbit/s. Cependant cette valeur peut être modifiée explicitement dans le code source. Il faut noter également que ce logiciel est constamment modifié, corrigé et étendu au fur et à mesure de l'apparition de nouveaux besoins. Ainsi, au cours du déroulement de la thèse, plusieurs versions se sont succédées, apportant leurs lots de corrections et améliorations diverses.

Intervalles de confiance

Dans les simulations utilisées, le problème est de trouver un intervalle raisonnable pouvant contenir une valeur p à déterminer. Dans le cas des sondages, l'intervalle de confiance est appelé une *fourchette*.

Calcul de l'intervalle de confiance

Supposons que X_1, X_2, \dots, X_n sont des valeurs mesurées d'une manière identique, distribuée et indépendante, ayant une moyenne μ et une variance σ^2 . la moyenne de l'échantillon est :

$$\bar{X}(n) = \frac{\sum_{i=1}^n X_i}{n}$$

et la variance :

$$S^2(n) = \frac{\sum_{i=1}^n [X_i - \bar{X}(n)]^2}{n-1}$$

Si la valeur de n est suffisamment grande, alors en utilisant le théorème de limite centrale, on peut considérer que $\bar{X}(n)$ est approximativement distribuée comme une variable aléatoire normale de moyenne μ et de variance σ^2/n . L'intervalle de confiance de $100 \times (1 - \alpha)$ pour cent de μ peut être calculé à partir de la formule suivante :

$$\bar{X}(n) \pm t_{n-1, 1-\alpha/2} \sqrt{S^2(n)/n} \quad \dots (i)$$

Où : $t_n = \frac{\bar{X}(n) - \mu}{S^2(n)/n}$ a une distribution t avec n-1 degrés de liberté

Dans l'expression (i), $t_{n-1, 1-\alpha/2}$ est le point supérieur critique $(1 - \alpha)/2$ pour la distribution t [123].

Technique d'intervalles de confiance

Il existe trois techniques couramment utilisées pour obtenir les intervalles de confiance des résultats de simulation :

- Réplication indépendante de la simulation : où des valeurs de X_i sont obtenues pour la même simulation, pour fournir plusieurs exécutions de simulations indépendantes.
- Procédure de 'Batch means' : dans cette méthode une simulation est découpée en n 'batches'. La durée de chaque 'batch' doit être suffisamment longue, de tel sorte que les exécutions des batches soient considérées indépendantes.
- Méthode régénérative : qui est basée sur la définition des états régénératifs dans un modèle récurrent. Dans un système stable non-dégénéré, il s'agit d'identifier un état dans lequel le système peut revenir de temps à autre (point de régénération). La durée séparant les visites est appelée cycle de régénération. Des mesures sur les cycles régénératifs (statistiquement indépendants) sont ainsi collectées. La méthode régénérative est plus compliquée à appliquer que les deux premières méthodes, particulièrement dans des systèmes complexes, où les durées des cycles ne sont pas connues à priori et peuvent être assez longues.

Dans notre travail, la méthode de réplication indépendante a été utilisée. Ainsi, plusieurs exécutions ont été réalisées pour chaque modèle simulé, avec des valeurs différentes des germes des variables aléatoires, pour trouver un intervalle de confiance de 95% à partir des statistiques obtenues pour des simulations données. Les simulations sont répétées avec des durées variables, jusqu'à ce que la stabilité soit atteinte, dans les résultats obtenus et dans les séquences d'évènements de la simulation. Le temps de la simulation est déterminé pour qu'un certain nombre d'évènements soit généré pendant l'exécution de la simulation pour atteindre un certain degré de magnitude des résultats.

CPLEX

CPLEX a été conçu pour résoudre des programmes linéaires ou des programmes linéaires entiers écrits en différents langages de description. Les programmes entiers peuvent être pures (toutes les variables sont entières) ou mixtes (variables continues). CPLEX offre un ensemble de bibliothèques pour la modélisation et d'autres pour faciliter son incorporation dans des applications écrites en C, Visual Basic, Fortran, ...etc. C'est un programme exécutable qui peut : lire interactivement un problème ou à partir d'un fichier décrit dans certains formats standards ; résoudre un problème, et fournir la solution interactivement ou dans un fichier texte. Le programme comprend le fichier 'cplex.exe' sur une plate-forme Windows ou 'cplex' sur une plate-forme UNIX.

AMPL (A Modeling Language for Mathematical Programming)

AMPL est un langage de modélisation algébrique complet et puissant pour décrire des problèmes d'optimisation linéaire et non-linéaire, avec des variables discrètes ou continues. Développé aux laboratoires de Bell, AMPL utilise une notation commune et des concepts

familiers pour formuler des modèles d'optimisation et pour examiner des solutions, alors que l'ordinateur gère la communication avec un solveur (solutionneur) approprié. La flexibilité et la convenance du langage AMPL permettent une modélisation et un développement de modèle rapide, en parallèle ses options de contrôle offrent particulièrement une efficacité pour des exécutions de programmes complexes.

Exemple d'un modèle pour la stratégie de connectivité

Nous présentons ici le modèle décrit ci-dessous en utilisant le langage de modélisation AMPL.

Notons également que les contraintes de couverture ont été linéarisées.

Définition des données

```
param xmin ; param xmax ; param ymin ; param ymax ;  
  
param N ;  
  
param M ;  
  
param Rr ; param Rn ; param x{i in 1..N} ; param y{i in 1..N} ;  
  
param theta {i in 1..M, j in 1..M} binary ;
```

Définition des variables

```
var a{i in 1..M} >= xmin, <= xmax ; var b{i in 1..M} >= ymin, <= ymax ;  
  
var lambda {i in 1..N, j in 1..M} binary ;  
  
var mu {i in 1..M, j in 1..M} binary ;  
  
var tau{i in 1..N} binary ;  
  
var Z {i in 1..M, j in 1..M, s in 1..M, k in 1..M} binary ;
```

Contraintes de connectivité autour des Routeurs (linéarisées)

- subject to connect1 $\{i \text{ in } 1..N, j \text{ in } 1..M\}$:

$$\lambda_{[i,j]} * x[i] \geq (a[j] - R_n) + (\lambda_{[i,j]} - 1) * x_{\max};$$
- subject to connect2 $\{i \text{ in } 1..N, j \text{ in } 1..M\}$:

$$\lambda_{[i,j]} * x[i] \leq (a[j] + R_n);$$
- subject to connect3 $\{i \text{ in } 1..N, j \text{ in } 1..M\}$:

$$\lambda_{[i,j]} * y[i] \geq (b[j] - R_n) + (\lambda_{[i,j]} - 1) * y_{\max};$$
- subject to connect4 $\{i \text{ in } 1..N, j \text{ in } 1..M\}$:

$$\lambda_{[i,j]} * y[i] \leq (b[j] + R_n);$$

Contrainte connectivité entre les Routeurs (linéarisées)

- subject to connectR1 $\{i \text{ in } 1..M, j \text{ in } 1..M : i <> j\}$:

$$a[i] \geq a[j] - R_r + (\mu_{[i,j]} - 1) * x_{\max};$$
 - subject to connectR2 $\{i \text{ in } 1..M, j \text{ in } 1..M : i <> j\}$:

$$a[i] \leq a[j] + R_r + (1 - \mu_{[i,j]}) * x_{\max};$$
 - subject to connectR3 $\{i \text{ in } 1..M, j \text{ in } 1..M : i <> j\}$:

$$b[i] \geq (b[j] - R_r) + (\mu_{[i,j]} - 1) * y_{\max};$$
 - subject to connectR4 $\{i \text{ in } 1..M, j \text{ in } 1..M : i <> j\}$:

$$b[i] \leq (b[j] + R_r) + (1 - \mu_{[i,j]}) * y_{\max};$$
 - subject to inverse $\{i \text{ in } 1..M, j \text{ in } 1..M\}$:

$$\mu_{[i,j]} = \mu_{[j,i]};$$
 - subject to connectR5 $\{i \text{ in } 1..N\}$:
-

$$\sum\{j \text{ in } 1..M\} \text{ lambda}[i,j] \geq \text{tau}[i];$$

- subject to connectR6 $\{i \text{ in } 1..N, j \text{ in } 1..M\}$:

$$\text{tau}[i] \geq \text{lambda}[i,j];$$

Contraintes de routes

- subject to route1 $\{i \text{ in } 1..M, k \text{ in } 1..M, s \text{ in } 1..M\}$:

$$Z[i,k,s,1] \geq 0;$$

- subject to route2 $\{i \text{ in } 1..M, k \text{ in } 1..M, s \text{ in } 1..M\}$:

$$Z[i,k,s,1] \leq \mu[i,k];$$

Contraintes pour la conservation des flots

- subject to conserve1 $\{s \text{ in } 1..M, d \text{ in } 1..M, j \text{ in } 1..M : j <> s \text{ } j <> d\}$:

$$\sum\{i \text{ in } 1..M\} Z[i,j,s,d] - \sum\{i \text{ in } 1..M\} Z[j,i,s,d] = 0;$$

- subject to conserve2 $\{s \text{ in } 1..M, d \text{ in } 1..M, j \text{ in } 1..M : j = s\}$:

$$\sum\{i \text{ in } 1..M\} Z[i,j,s,d] - \sum\{i \text{ in } 1..M\} Z[j,i,s,d] = -\theta[s,d];$$

- subject to conserve3 $\{s \text{ in } 1..M, d \text{ in } 1..M, j \text{ in } 1..M : j = d\}$:

$$\sum\{i \text{ in } 1..M\} Z[i,j,s,d] - \sum\{i \text{ in } 1..M\} Z[j,i,s,d] = \theta[s,d];$$

- subject to conserve4 $\{i \text{ in } 1..M, s \text{ in } 1..M, d \text{ in } 1..M\}$:

$$Z[i,i,s,d] = 0;$$

- subject to conserve5 $\{i \text{ in } 1..M, j \text{ in } 1..M, s \text{ in } 1..M\}$:

$$Z[i,j,s,s] = 0;$$

- subject to conserve6 $\{i \text{ in } 1..M, j \text{ in } 1..M, s \text{ in } 1..M, d \text{ in } 2..M\}$:

$$Z[i,j,s,d] = 0;$$

Fonction objectif :

maximize profit : $\sum_{i \text{ in } 1..N} \tau[i] - \sum_{i \text{ in } 1..M, j \text{ in } 1..M, s \text{ in } 1..M} Z[i, j, s, 1];$

Liste des publications

- R. Meraihi, G. Le Grand, S. Tohmé and M. Riguidel, 'Real time application support in an ambient network using intelligent mobile robots', in the proceedings of the European Symposium on Ambient Intelligence, LNCS 2875, October 2003, Ambient Intelligence, ISBN : 3-540-20418-0, DOI : 10.1007/b94080, Springer Verlag Heidelberg, pp. 88-100 November 3-4, 2003 - Eindhoven, The Netherlands
 - G. Le Grand, R. Meraihi, S. Tohmé and M. Riguidel, 'Intelligent ad hoc networking to support real time services', in the proceedings of the IEEE Vehicular Technology Conference (VTC 2003), 0-7803-7955/03, IEEE, Orlando, Florida, October 4-9, 2003
 - R. Meraihi, G. Le Grand, S. Tohmé et M. Riguidel, 'Gestion multicouches de la qualité de service dans un réseau ad hoc à coeur stable', Actes du 10e colloque francophone sur l'ingénierie des protocoles CFIP 2003, Hermès Science, ISBN 2-7462-0798-2, pages 461-476, Paris, Octobre 2003
 - G. Le Grand, R. Meraihi, S. Tohmé and M. Riguidel, 'Cross-layer QoS and terminal differentiation in ad hoc networks for real-time service support', in the proceedings of the Mediterranean Ad Hoc Networking Workshop (MedHOC NET 2003), (IFIP-TC6-WG6.8), Mahdia, Tunisia, June 25-27 2003
 - R. Meraihi, G. Le Grand, N. Puech, S. Tohmé, M. Riguidel, 'Improving ad hoc network performance with backbone topology control', IEEE Vehicular Technology Conference (VTC Fall 2004), Los Angeles, USA, September 26-29 2004
-

Bibliographie

- [1] S.B. Lee, and A. T. Campbell. 'INSIGNIA : In-band signaling support for QoS in mobile ad hoc networks'. In 5th Int. Workshop on Mobile Multimedia Communication (MoMuc'98), Berlin, Germany, October 1998
 - [2] S.B. Lee, A. Gahng-Seop, X. Zhang, and A.T. Campbell, 'INSIGNIA : An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks', Journal of Parallel and Distributed Computing (Academic Press) , Special issue on Wireless and Mobile Computing and Communications, Vol. 60 No. 4 pg. 374-406, April 2000
 - [3] H. Xiao, K.C. Chua and K.G. Seah, 'Quality of Service Models for Ad-Hoc Wireless Network', ECE-ICR, Wireless Communications Laboratory, Appeared in 'Handbook of Ad hoc Wireless Networks' which was published in late 2002 by CRC Press, FL, USA
 - [4] H. Xiao, K. G. Seah, A. Lo, and K. C. Chua, 'A flexible quality of service model for mobile ad-hoc networks', Vehicular Technology Conference Proceedings, 2000, VTC 2000-Spring Tokyo, IEEE : 51st, Volume : 1, Page(s) : 445 -449
 - [5] Gahng-Seop Ahn, Andrew T. Campbell, Andras Veres and Li-Hsiang Sun, 'SWAN : Service Differentiation in Stateless Wireless Ad Hoc Networks ', Proc. IEEE INFO-COM'2002, New York, New York, 2002
 - [6] K. Chen, S. H. Shah, and K. Nahrstedt, 'Cross Layer Design for Data Accessibility in Mobile Ad Hoc Networks,' Journal on Wireless Communications, vol. 21, pp. 49-75, 2002
 - [7] R. Braden, et al. 'RFC : 2205 Resource ReSerVation Protocol (RSVP)', Request for Comments, IETF, Sep. 1997.
 - [8] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss 'RFC : 2475 An Architecture for Differentiated Services', Request for Comments, IETF, December 1998
 - [9] R. Sivakumar, P. Sinha and V. Bharghavan, 'CEDAR : a Core-Extraction Distributed Ad hoc Routing algorithm', INFOCOM '99, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings, IEEE , Volume : 1 , 21-25 Mar 1999 Page(s) : 202 -209 vol.1 1999
-

-
- [10] C-C. Shen, C. Srisathapornphat, R. Liu, Z. Huang, C. Jaikaeo, and E. L. Lloyd, 'CLTC : A Cluster-based Topology Control Framework for Ad hoc Networks'. To appear in IEEE Transactions on Mobile Computing, 2004
- [11] G. C. Mauricio, C. Resende, 'Computing Approximate Solutions of the Maximum Covering Problem with GRASP'. *J. Heuristics* 4(2) : 161-177 (1998)
- [12] J. O'Rourke, 'Art Gallery Theorems and Algorithms'. New York, Oxford Univ. Press, 1987
- [13] K. Chakrabarty, S. S. Iyengar, H. Qi, E. Cho, 'Grid Coverage for Surveillance and Target Location in Distributed Sensor Networks'. *IEEE Trans. Computers* 51(12) : 1448-1453 (2002)
- [14] P. Gupta, and P. R. Kumar, 'The Capacity of Wireless Networks'. In *IEEE Transactions on Information Theory*, vol. IT-46, no. 2, 388- 404, March 2000
- [15] P. Krishna, N. Vaidya, M. Chatterjee, and D. Pradhan, 'A cluster-based approach for routing in dynamic networks'. *ACM SIGCOMM Computer Communication Review*, 49-65, Apr. 1997
- [16] R. Fourer, D. M. Gay, B-W. Kernighan, 'AMPL : A Modeling Language for Mathematical Programming'. Edition : Hardcover
- [17] R. Ramanathan and R. Rosales-Hain, 'Topology Control of Multihop Wireless Networks Using Transmit Power Adjustment'. *Infocom 2000*, 404-413, 2000
- [18] R. Wattenhofer, L. Li, P. Bahl, and Y.-M. Wang, 'Distributed Topology Control for Power Efficient Operation in Multihop Wireless Ad Hoc Networks'. *Infocom 2001*, Apr. 2001
- [19] S. Basagni, I. Chlamtac, V.R. Syrotiuk, 'Dynamic source routing for ad hoc networks using the global positioning system'. *Proc. IEEE Wireless Communications and Networking Conference*, New Orleans, September 1999
- [20] S. Meguerdichian, F. Koushanfar, M. Potkonjak, M. B. Srivastava, 'Coverage Problems in Wireless Ad-hoc Sensor Networks'. *INFOCOM 2001* : 1380-1387, Anchorage, Alaska, April 22-26, 2001
- [21] SPIF, <<http://www.enst.fr/spif>>
- [22] X. Jia, D. Li, and D. Du, 'QoS topology control in ad hoc wireless networks'. to appear in the proceedings of *IEEE INFOCOM'04*, Hong Kong, Mar 2004
- [23] Ambience project (ITEA), <<http://www.extra.research.philips.com/euprojects/ambience/>>
- [24] 2. C. E. Perkins, ed., *Ad Hoc Networking*, Addison-Wesley, Boston, 2001, pp.2-3
- [25] C.K. Toh, 'A novel distributed routing protocol to support ad-hoc mobile computing', *Wireless Personal Communication*, Jan. 1997
- [26] C.K. Toh, H. Cobb, D.A. Scott, 'Performance Evaluation Of battery Life Aware routing Schemes for Wireless Ad hoc Networks'. 2001. 0-7803-7097-1 IEEE
- [27] G. Le Grand, R. Meraihi, Cross-layer QoS and terminal differentiation in ad hoc networks for real-time service support <<http://perso.enst.fr/legrand/Publis/medhoc2003.pdf>>, to appear in the proceedings of *MedHOC NET 2003*, (IFIP-TC6-WG6.8), Mahdia, Tunisia, June 25-27 2003
-

-
- [28] I. Aad, C. Castelluccia, 'Differentiation mechanisms for IEEE 802.11', IEEE Infocom 2001, Anchorage - Alaska, April 22-26h, 2001
- [29] I. Aad and C. Castelluccia, 'Remarks on per-flow differentiation in IEEE 802.11', European Wireless 2002, Florence, Italy, February 25-28, 2002
- [30] I. Aad and C. Castelluccia, 'Priorities in WLANs', Computer networks, vol. 41/4 pp 505 - 526, February 2003
- [31] IEEE 802.11 WG, Draft Supplement to STANDARD FOR Telecommunications and Information Exchange Between Systems-LAN/MAN Specific Requirements - Part 11 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications : Medium Access Control (MAC) Enhancement for Quality of Service (QoS), IEEE 802.11e/Draft 3.0, May 2002
- [32] J. L. Sobrinho, A. S. Krishnakumar, 'Quality-Of-Service in Ad hoc Carrier sense multiple access Wireless networks', IEEE Journal on Selected Preas in Communications, pp. 1353-1368, August 1999
- [33] J. L. Sobrinho, A. S. Krishnakumar, 'Real time traffic over the IEEE 802.11 medium access control layer', Bell Labs Thechnical Journal, pp. 172-187, 1996
- [34] K. Fall, K. Varadhan, The ns manual, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf
- [35] K. Wu and J. Harms, 'QoS Support in Mobile Ad Hoc Networks,' Crossing Boundaries- the GSA Journal of University of Alberta, Vol. 1, No. 1, Nov. 2001, pp.92- 106
- [36] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, 'Performance anomaly of 802.11b'. To appear in Proceedings of IEEE INFOCOM 2003, San Francisco, USA, March 30-April 3, 2003
- [37] M. Pearlman, Z. Hass, 'Determining the optimal configuration for the zone routing protocol', IEEE selected area in communication, August, 1999
- [38] N. Roux. 'Cost Adaptive Mechanism (CAM) for Mobile Ad Hoc Reactive Routing Protocols', Master Thesis, ENST 2000
- [39] S.J. Lee, M. Gerla, 'Dynamic Load-Aware Routing in Ad hoc Networks'. Proceedings of ICC 2001, Helsinki, Finland, June 2001
- [40] S.J. Lee, M. Gerla, and C.-K. Toh, 'A Simulation Study of Table-Driven and On-Demand Routing Protocols for Mobile Ad-Hoc Networks', IEEE Network, vol. 13, no. 4, pp. 48-54, Jul. 1999
- [41] S. Jiang, D. He, and J. Rao, 'A Link Availability Prediction Model for Wireless Ad Hoc Networks', proceedings International Workshop on Wireless Networks and Mobile Computing Taipei, Taiwan, April 10-13, 2000
- [42] S. K. Das, A. Mukherjee, Bandyopadhyay, Krishna Paul, D.Saha, 'Improving Quality-of-service in Ad hoc Wireless NetWorks with Adaptive Multi-path Routing'
- [43] S. Sheng, 'Routing Support for Providing guaranteed end-to-end Quality of Service', PH.D Thesis, University of IL at Urbana Champaign, <<http://cairo.cs.uiuc.edu/papers/SCthesis.ps>>, 1999
-

-
- [44] The Institute of Electrical and Electronics Engineers, Inc. IEEE Std 802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. The Institute of Electrical and Electronics Engineers, Inc., 1999 edition
 - [45] N. Richard, 'InViWo agents : write once, display everywhere', In proc. of Web3D Symposium, March 2003, St-Malo (France)
 - [46] R. Sivakumar, P. Sinha and V. Bharghavan, 'CEDAR : a Core-Extraction Distributed Ad hoc Routing algorithm', INFOCOM '99, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings, IEEE , Volume : 1 , 21-25 Mar 1999 Page(s) : 202 -209 vol.1 1999
 - [47] J. Broch, D. Maltz, and D. Johnson, 'Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks'. Proceedings of the Workshop on Mobile Computing, Perth, Western Australia, June 1999
 - [48] G. Chelius and E. Fleury, Ananas : 'A New Ad Hoc Network Architecture', January 2002, Research Report RR-4354, Inria
 - [49] R. Droms, J. Bound, Bernie Volz, Ted Lemon, C. Perkins and M. Carney, 'Dynamic Host Configuration Protocol for IPv6 (DHCPv6)', 2 Nov 2002, Internet Draft : draft-ietf-dhc-dhcpv6-28.txt
 - [50] M. Günes and J. Reibel, 'An ip address configuration algorithm for zeroconf. mobile multi-hop ad-hoc networks. ', In Proceedings of the International Workshop on Broadband Wireless Ad-Hoc Networks and Services, Sophia Antipolis, France, September 2002
 - [51] K. Al Agha G. Pujolle H. Badis, A. Munaretto, 'QoS for Ad Hoc Networking Based on Multiple Metrics : Bandwidth and Delay', In The Fifth IEEE International Conference on Mobile and Wireless Communications Networks (MWCN 2003), 2003
 - [52] S. Nesgari and R. Prakash. 'ManetConf : Configuration of Hosts in a Mobile Ad Hoc Network'. IEEE INFOCOM, March 2002
 - [53] C. Perkins, J. Malinen, R. Wakikawa and E. Belding-Royer. 'IP Address Autoconfiguration for Ad Hoc Networks', Internet Draft : draft-ietf-manet-autoconf-01.txt, November 2001
 - [54] S. Thomson and T. Narten. 'IPv6 Stateless Address Autoconfiguration.' Request for Comments (Draft Standard) 2462, Internet Engineering Task Force, December 1998
 - [55] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, and A. Tuominen. 'Global connectivity for Mobile Ad Hoc Networks'. Internet Draft : <draft-wakikawa-manetglobalv6-03.txt>, 23 October 2003
 - [56] K. Weniger and M. Zitterbart, 'IPv6 Autoconfiguration in LargeScale Mobile Ad-Hoc Networks', Proceedings of European Wireless 2002, Florence, Italy, Feb 2002
 - [57] A.D. Amis and R. Prakash, 'Load-balancing clusters in wireless ad hoc networks'. 3rd IEEE Symposium on Application-Specific Systems and Software Engineering Technology, pages 25-32, Los Alamitos, CA, Mar. 24-25 2000
 - [58] E.L. Lloyd, R. Liu, M.V. Marathe, R. Ramanathan, and S.S. Ravi, 'Algorithmic Aspects of Topology Control Problems for Ad Hoc Networks', IEEE Mobile Ad Hoc Networking and Computing (MOBIHOC), June 2002
-

-
- [59] G. Le Grand, R. Meraihi, S. Tohmé and M. Riguidel, 'Intelligent ad hoc networking to support real time services', IEEE Vehicular Technology Conference VTC 2003, Orlando, USA, October, 2003
- [60] ILOG CPLEX 9.0 User's manual, octobre 2003
- [61] I. Rubin, X. Huang and Y. -C. Liu, 'A QoS-oriented topological synthesis protocol for mobile backbone networks', IEEE Vehicular Technology Conference VTC 2003, Orlando, USA, October, 2003
- [62] I. Rubin, X. Huang, Y. -C. Liu and H. Ju, 'A distributed stable backbone maintenance protocol for ad hoc wireless networks', IEEE Vehicular Technology Conference VTC (Spring) 2003, Jeju, Korea, April 2003
- [63] L. Li, J.Y. Halpern, P. Bahl, Y.M. Wang, and R. Wattenhofer, 'Analysis of a Cone-Based Distributed Topology Control Algorithms for Wireless Multi-Hop Networks', ACM Symp. Principle of Distributed Computing (PODC), Aug. 2001
- [64] M. Gerla, and K. Xu, 'Multimedia streaming in large-scale sensor networks with mobile swarms'. ACM SIGMOD Record, Vol 32, N4, Dec 2003
- [65] T. Hou and Victor O.K. Li, 'Transmission range control in multihop packet radio networks', IEEE Trans on Communications, vol. 34, no. 1, Jan 1986, pp.38-44
- [66] T. Clausen, P. Jacquet, 'Optimized Link State Routing Protocol (OLSR)', Request for Comments : 3626 ,October 2003
- [67] James A. Freebersyser, Barry Leiner, 'A DoD perspective on mobile ad hoc networks', Ad Hoc Networking, Addison Wesley, pp. 29-51, 2001
- [68] W. Fifer, F. Bruno, 'The low-cost packet radio', Proceedings of the IEEE 75 (1), pp 33-42, (1987)
- [69] C.E. Perkins, E.M. Belding-Royer, et S. Das. 'Ad Hoc On Demand Distance Vector (AODV) Routing', IETF RFC 3561
- [70] R. Ogier, F. Templin et M. Lewis. 'Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)', IETF RFC 3684
- [71] Z. Haas, M. Pearlman, P. Samar, 'The Zone Routing Protocol (ZRP) for Ad Hoc Networks', draft-ietf-manet-zone-zrp-02.txt, juillet 2002
- [72] Bluetooth SIG : Bluetooth Specification Version 1.1. 2001, [http://www.bluetooth.com/pdf/Bluetooth 1.1 Specifications Book.pdf](http://www.bluetooth.com/pdf/Bluetooth%201.1%20Specifications%20Book.pdf)
- [73] QoS Forum. QoS protocols and architectures. White paper of QoS Forum, July 1999. <http://www.qosforum.com>
- [74] E. Crawley, R. Nair, B. Rajagopalan, H. Sandick, 'A Framework for QoS-based Routing in the Internet', IETF RFC2386
- [75] C. R. Lin and M. Gerla, 'MACA/PR : An Asynchronous Multimedia Multihop Wireless Network'. In Proceedings of IEEE INFOCOM '97, Apr. 1997
- [76] J. Deng et RS. Chang. 'A priority scheme for IEEE 802.11 DCF access method', IEICE Transactions in Communications, vol 82-B, n 1, janvier 1999
-

-
- [77] N. H. Vaidya, P. Bahl, and S. Gupta, 'Distributed fair scheduling in wireless LAN', In Sixth Annual International Conference on Mobile Computing and Networking, Boston, USA August 2000
 - [78] S. Chen, K. Nahrstedt, 'Distributed quality-of-service routing in ad hoc networks', IEEE Journal on Selected Areas in Communications 17 (8), pp 1488-1504, (1999)
 - [79] Z. J. Haas, et al., eds., Special Issue on Wireless Ad Hoc Networks, IEEE J. on Selected Areas in Communications, Vol. 17, No. 8 (August 1999)
 - [80] C.E. Perkins, E.M. Royer, S.R. Das, 'Quality of service for ad hoc on-demand distance vector routing' (work in progress), IETF Internet Draft, draft-ietf-manet-aodvqos-00.txt, July 2000
 - [81] Antonio García-Macías, Franck Rousseau, Gilles Berger-Sabbatel, Leyla Toumi, Andrzej Duda, 'Quality of Service and Mobility for the Wireless Internet', Proc. First ACM Wireless Mobile Internet Workshop, Rome, Italy, 2001
 - [82] J. Moy, 'OSPF Version 2', Request for Comments 1247, IETF, July 1991
 - [83] C. Hedrick, 'Routing Information Protocol', Request for Comments 1058, June 1988
 - [84] Mobile Ad-hoc Networks (manet), <http://www.ietf.org/html.charters/manet-charter.html>
 - [85] L. Hu, 'Topology control for multihop packet radio networks', IEEE Trans. On Communications, vol. 41, no. 10, pp. 1474-1481, 1993,
 - [86] N. Nikaein, C. Bonnet, 'Topology Management for Improving Routing and Network Performances in Mobile Ad Hoc Networks', Kluwer/ACM MONET Journal, Vol 10, No 2, April 2005
 - [87] W.T. Chen and N.F. Huang, 'The Strongly Connecting Problem on Multihop Packet Radio Networks', IEEE Trans. Comm., vol. 37,no. 3, Mar. 1989
 - [88] Z. Huang, C.C. Shen, C. Scrisathapornphat and C. Jaikao, 'Topology control for ad hoc networks with directional antennas', IEEE 11th Conf on Computer Communications and Networks, Miami, pp.16-21, Oct 2002
 - [89] M.A. Marsan, C.F. Chiasserini, A. Nucci, G.Carello, and L.D.Giovanni, 'Optimizing the topology of Bluetooth wireless personal area networks', IEEE INFOCOM 02
 - [90] S. Singh, M. Woo and C.S. Raghavendra, 'Power-aware routing in mobile ad hoc networks', ACM MOBICOM 98, Dallas, pp.181-190, 1998
 - [91] V. Kawadia and P. R. Kumar, 'Power control and clustering in ad hoc networks', IEEE INFOCOM 03
 - [92] J.E. Wieselthier, G. D. Nguyen, and A. Ephremides, 'On the construction of energy-efficient broadcast and multicast trees in wireless networks', IEEE INFOCOM 2000
 - [93] L. Kleinrock and F. Kamoun, 'Hierarchical routing for large networks', Computer Networks 1(1), pp 155-174, 1977
 - [94] D.J. Baker and A. Ephremides, 'The architectural organization of a mobile radio network via a distributed algorithm', IEEE Transactions on Communications 29(11), pp 1694-1701, 1981
-

-
- [95] C.-C. Chiang, H.-K. Wu, W. Liu and M. Gerla, 'Routing in clustered multihop, mobile wireless networks with fading channel', in Proceedings of IEEE Singapore International Conference on Networks (SICON), pp. 197-211, April 1997
- [96] M. Gerla, T.J. Kwon and G. Pei, 'On demand routing in large ad hoc wireless networks with passive clustering', in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), September 2000
- [97] M. Gerla and J.T.-C. Tsai, 'Multicluster, mobile, multimedia radio network, Wireless Networks', 1(3), pp 255-265, 1995
- [98] C. R. Lin and M. Gerla, 'Adaptive clustering for mobile wireless networks', IEEE Journal on Selected Areas in Communications 15(7), pp 1265-1275, 1997
- [99] L. Briesemeister and G. Hommel, 'Role-based multicast in highly mobile but sparsely connected ad hoc networks', in Proceedings of the 1st Annual Workshop on Mobile and Ad Hoc Networking and Computer (MobiHOC), pp. 45-50, Boston, MA August 2000
- [100] A. Meraihi Naimi, P. Jacquet "Delay Oriented OLSR". IEEE ICTTA 2004. Syria
- [101] S. Basagni, 'Distributed clustering for ad hoc networks', in Proceedings of the 1999 International Symposium on Parallel Architectures, Algorithms, and Networks, pp. 310-315, Australia, June 1999
- [102] P.F. Tsuchiya, 'The landmark hierarchy : A new hierarchy for routing in very large networks', Computer Communication Review, pp. 35-42, August 1988
- [103] Suman Banerjee, Samir Khuller, 'A Clustering Scheme for Hierarchical Control in Multi-hop Wireless Networks', IEEE Infocom 2001, Anchorage, Alaska, April 2001
- [104] R. Ramanathan and M. Steenstrup, 'Hierarchically-organized, multihop mobile wireless networks for Quality-of-Service support', ACM/Baltzer Mobile Networks and Applications 3(1), pp 101-118, 1998
- [105] Personal communication with J. Agre, Rockwell Sciences Center. DARPA Program Review Meeting, Feb. 2000
- [106] David B. Johnson, David A. Maltz, Yih-Chun Hu, 'The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)', Internet Draft : <draft-ietf-manet-dsr-10.txt>, 19 July 2004
- [107] V. Kawadia and P. R. Kumar, 'A Cautionary Perspective on Cross Layer Design', IEEE Wireless Communication Magazine. July, 2003
- [108] K. Chandran, S. Raghunathan, S. Venkatesan and R. Prakash, 'A feedback-based scheme for improving TCP performance in ad hoc wireless networks', IEEE Personal Communications Magazine, p34-39, Feb 2001
- [109] G. Holland and N. Vaidya, 'Analysis of TCP performance over mobile ad hoc networks', ACM MobiCom, Seattle, Washington, Aout 1999
- [110] G.J. Pottie and W.J. Kaiser, 'Wireless Integrated network sensors'. Communications of the ACM 43(5) :pp 51-58, 2000
-

-
- [111] G. Asada, M. Dong, T.S. Lin, F. Newberg, G.J. Pottie, H.O. Marcy, and W.J. Kaiser, 'Wireless Integrated Network Sensors : Low Power Systems on a Chip', pp. 9-12 in Proceedings of the 24th IEEE European Solid-State Circuits Conference. Den Hague, The Netherlands : Elsevier. 1998
- [112] T.H. Lin, H. Sanchez, H.O. Marcy, and W.J. Kaiser, 'Wireless Integrated Network Sensors (WINS) for Tactical Information Systems', Proceedings of the Government Microcircuit Applications Conference. 1998
- [113] J. Westcott and G. Lauer, 'Hierarchical routing for very large networks', Proc. IEEE MILCOM '84, pp. 214-218, 21-24 October 1984
- [114] N. Nikaein, C. Bonnet, Y. Moret and I. A. Rai, '2LQoS- Two-Layered Quality of Service Model for Reactive Routing Protocols for Mobile Ad Hoc Networks', in Proceeding of SCI2002, USA, Orlando, 2002
- [115] B. Leiner, R. Ruth, A.R. Sastry, 'Goals and challenges of the DARPA GloMo program', IEEE Personal Communications 3 (6), pp 34-43, 1996
- [116] Althouse, E : Extending the Littoral Battlespace (ELB). Advanced Concept Technology Demonstration (ACTD), NATO Information Systems Technology Panel Symposium on Tactical Mobile Communications, June 1999
- [117] S. Corson, J. Macker, 'Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations', Request for Comments 2501, IETF, January 1999
- [118] R. Droms, 'Dynamic Host Configuration Protocol', IETF Request for Comments : 2131, March 1997
- [119] J.M. Jaffe, 'Algorithms for Finding Paths with Multiple Constraints', Networks, 14 :95 116, 1984
- [120] Z. Wang and J. Crowcroft, 'Qos Routing for Supporting Resource Reservation', IEEE JSAC, Sept. 1996
- [121] J.Heinanen F.Baker, W. Weiss, and J. Wroclawski, 'RFC : 2597 Assured Forwarding PHP Group', Request for Comments, IETF, June 1999
- [122] www.voronoi.com/tutorial.htm
- [123] M. Law, Averill and W. David Kelton, 'Simulation modeling and analysis', McGRAW HILL International Editions, 1991
- [124] J. Orozco and D. Ros, 'DiffServ-Aware Streaming of H.264 Video'. To appear in Proceedings of the 14th International Packet Video Workshop (PV2004), Irvine (CA), USA, December 2004
- [125] The ZigBee Alliance. <http://www.zigbee.org>
- [126] L. I. ESCOBAR, K. MAHAJAN, 'Mesures de puissance dans un réseau WiFi à l'étage A5 du bâtiment rue Dareau', rapport de brique HDIP, ENST, Mars 2004
-