



Définition et validation d'un modèle de communication supportant la communication basée contenus dans les réseaux mobiles ad hoc discontinus

Julien Haillot

► To cite this version:

Julien Haillot. Définition et validation d'un modèle de communication supportant la communication basée contenus dans les réseaux mobiles ad hoc discontinus. Réseaux et télécommunications [cs.NI]. Université de Bretagne Sud, 2010. Français. tel-00599669

HAL Id: tel-00599669

<https://tel.archives-ouvertes.fr/tel-00599669>

Submitted on 10 Jun 2011

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 / UNIVERSITÉ DE BRETAGNE SUD

UFR Sciences et Sciences de l'Ingénieur
sous le sceau de l'Université Européenne de Bretagne

Pour obtenir le grade de :
DOCTEUR DE L'UNIVERSITÉ DE BRETAGNE SUD
Mention : STIC
École Doctorale SICMA

présentée par

Julien Haillot

Laboratoire de Recherche Informatique et ses Applications
de Vannes et Lorient

Définition et validation d'un modèle de communication supportant la communication basée contenus dans les réseaux mobiles ad hoc discontinus

Thèse soutenue le 19 novembre 2010,
devant la commission d'examen composée de :

M. Claude Jard
Professeur des Universités, École normale supérieure de Cachan / Président

M. Jean-Marie Bonnin
Professeur des Universités, Télécom Bretagne / Rapporteur

M. Serge Chaumette
Professeur des Universités, Université Bordeaux 1 / Rapporteur

M. Serge Corlay
Ingénieur DGA, Direction Générale de l'Armement Maitrise de l'information / Examinateur

M. Frédéric Guidéc
Maître de Conférences HDR, Université de Bretagne-Sud / Directeur de thèse

*À mes parents,
à ma femme,
à mes enfants.*

REMERCIEMENTS

Je tiens à remercier Claude Jard qui me fait l'honneur de présider mon jury de thèse. Je remercie Jean-Marie Bonnin et Serge Chaumette d'avoir bien voulu être les rapporteurs de cette thèse. Je remercie Serge Corlay d'avoir accepté d'examiner cette thèse.

Je tiens à exprimer ma très sincère reconnaissance envers mon directeur de thèse Frédéric Guidec pour l'aide qu'il m'a apportée au cours de cette recherche. Sa motivation, son intérêt, sa patience et ses précieux conseils m'ont été d'un grand profit. Je le remercie particulièrement d'avoir dirigé ce travail de thèse, ce qui a grandement contribué à ce qu'il soit de meilleure qualité.

Je remercie aussi les membres de l'équipe CASA, pour les discussions constructives et pour la bonne ambiance qu'ils font régner dans ce groupe et dans le laboratoire. Je remercie tout particulièrement Pascale Launay qui a contribué à l'amélioration de la qualité de ce mémoire.

Je remercie tous mes collègues au laboratoire VALORIA pour les discussions et les bons moments passer avec eux à la cafet' du laboratoire. Je leur exprime ma profonde sympathie et leur souhaite beaucoup de bien.

Je remercie mes parents et mes amis pour leur soutien indéfectible, c'est avant tout grâce à eux que j'ai pu traverser cette étape.

Je dédie cette thèse à ma famille, et en particulier à ma femme Sandrine, qui m'a supporté tout au long de ces années de thèse, à ma fille Léa et à mon fils Nolann.

Ce travail a été soutenu par l'Agence Nationale de la Recherche sous contrat ANR-05-SSIA-0002-01, et par la Direction Générale de l'Armement Maitrise de l'information.

TABLE DES MATIÈRES

Introduction	7
Chapitre 1	
Communication dans les réseaux mobiles ad hoc discontinus	13
1.1 Historique	13
1.2 Réseaux mobiles ad hoc	15
1.2.1 Problématique des réseaux mobiles ad hoc	15
1.2.2 Routage dans les réseaux mobiles ad hoc	16
1.2.2.1 Routage dynamique réactif	17
1.2.2.2 Routage dynamique proactif	17
1.2.2.3 Routage dynamique hybride	18
1.2.2.4 Routage dynamique géographique	18
1.2.2.5 Autres familles de protocoles de routage	18
1.3 Réseaux mobiles ad hoc discontinus	19
1.3.1 Problématique des réseaux mobiles ad hoc discontinus	19
1.3.2 Routage dans les réseaux mobiles ad hoc discontinus	22
1.3.2.1 Communication opportuniste	22
1.3.2.2 Routage par inondation	25
1.3.2.3 Routage s'appuyant sur des historiques	26
1.3.2.4 Routage « social »	29
1.3.3 Bilan	31
1.4 Communication basée contenus	32
1.4.1 Modèle publication-abonnement	32
1.4.1.1 Modèles de souscription	33
1.4.2 Architecture générale des systèmes de communication par abonnement	33
1.4.2.1 Réseaux de couverture	34
1.4.2.2 Acheminement des événements dans les réseaux statiques ou quasi statiques	35
1.4.2.3 Acheminement des événements dans les réseaux mobiles ad hoc	37
1.4.3 Communication basée contenus dans les réseaux mobiles ad hoc discontinus	37
1.4.3.1 Acheminement épidémique (« <i>gossiping</i> »)	38
1.4.3.2 Acheminement exploitant les caractéristiques sociales des terminaux	39
1.4.4 Bilan	40

1.5	Discussion	41
Chapitre 2		
	Modèle de communication opportuniste basée sur le contenu	43
2.1	Objectifs	43
2.2	Vue d'ensemble de la proposition	44
2.2.1	Acheminement <i>Store, Carry and Forward</i>	44
2.2.2	Sélectivité des terminaux mobiles	44
2.2.3	Modulation de la sélectivité	45
2.2.3.1	Comportement égoïste	45
2.2.3.2	Comportement altruiste réactif	45
2.2.3.3	Comportement altruiste proactif	45
2.2.4	Communication multi-sauts	46
2.2.5	Exploitation de la diffusion radio	46
2.2.6	Support de la volatilité	47
2.2.7	Impact des choix de conception	47
2.3	Architecture générale du système	48
2.4	Couche supérieure de dissémination opportuniste basée contenus	50
2.4.1	Différentiation de l'information	50
2.4.1.1	Document, descripteur et identifiant	50
2.4.1.2	Profil d'intérêt et prédicat de sélection	52
2.4.2	Protocole de communication	53
2.4.2.1	Diffusion périodique du profil d'intérêt et du catalogue	55
2.4.2.2	Réception d'une annonce	59
2.4.2.3	Traitement des requêtes et diffusion de documents	63
2.4.2.4	Réception (attendue ou fortuite) de documents diffusés	65
2.4.2.5	Cache de documents	66
2.5	Couche inférieure de communication multi-sauts	67
2.5.1	Protocole de diffusion via des relais multi-points	68
2.5.2	Protocole de routage par la source	71
2.5.3	Protocole de diffusion sélective	73
2.6	Discussion	75
Chapitre 3		
	La plate-forme de communication DoD WAN	77
3.1	Vue d'ensemble de DoD WAN	77
3.1.1	Documents	78
3.1.1.1	Format des descripteurs	79

3.1.1.2	Identifiant unique d'un document	79
3.1.2	Prédicat de sélection	80
3.2	Communication multi-sauts entre terminaux voisins	81
3.2.1	Sockets de communication	81
3.2.1.1	Sockets UDP/IP	81
3.2.1.2	Pseudo-socket	81
3.2.2	Protocole de relais immédiat	82
3.2.2.1	Protocole de diffusion par inondation	82
3.2.2.2	Protocole de diffusion via des relais multi-point	83
3.2.2.3	Protocole de diffusion sélective	83
3.2.2.4	Protocole de routage par la source	84
3.3	Dissémination opportuniste basée contenus	85
3.3.1	Identifiant unique d'un terminal	85
3.3.2	Documents contenant des données de contrôle	85
3.3.3	Support de la volatilité	86
3.3.3.1	Persistance des données	86
3.3.3.2	Perception du voisinage	87
3.3.4	Interface <i>publish-subscribe</i>	88
3.3.4.1	Publication et abonnement	88
3.3.4.2	Compression et fragmentation	89
3.4	Services applicatifs exploitant DoD WAN	91
3.4.1	Service de discussion de groupes	91
3.4.1.1	Architecture du système NewsWAN	92
3.4.1.2	Administration du pseudo-serveur NewsWAN	93
3.4.1.3	Abonnement et publication dans NewsWAN	94
3.4.2	Autres exemples de services applicatifs	95
3.4.2.1	Service de partage de fichiers	95
3.4.2.2	Service de messagerie	95
3.5	Discussion	96
Chapitre 4		
Évaluation		99
4.1	Évaluation par la simulation	99
4.1.1	Conditions de simulation	100
4.1.1.1	Environnement et schéma de mobilité	100
4.1.1.2	Scénario de communication	101
4.1.1.3	Paramètres protocolaires	102

Table des matières

4.1.2	Résultats et observations	103
4.1.2.1	Vitesse de propagation des documents	103
4.1.2.2	Influence de la capacité du cache	106
4.1.2.3	Influence de la durée de vie des documents	107
4.1.2.4	Influence du mécanisme d'adaptation du catalogue	108
4.1.2.5	Influence du mécanisme d'adaptation du format l'annonce	110
4.1.2.6	Coût du relais immédiat multi-sauts	111
4.1.2.7	Influence et coût du comportement altruiste	114
4.2	Expérimentation sur postes radio de quatrième génération	115
4.2.1	Scénario d'illustration	117
4.2.2	Résultats expérimentaux	119
4.3	Bilan	121
	Conclusion et perspectives	123
	Publications personnelles	127
	Bibliographie	129

INTRODUCTION

L'essor des technologies de communication sans fil associé à la prolifération des terminaux mobiles offre de nouvelles perspectives dans le domaine des télécommunications. En effet, non seulement les terminaux mobiles peuvent aujourd'hui être connectés à un réseau d'infrastructure, et accéder ainsi au vaste monde d'Internet, mais ils peuvent aussi communiquer directement les uns avec les autres en mode ad hoc, c'est-à-dire sans recourir à une quelconque infrastructure. Un scénario alors envisageable est celui dans lequel des terminaux mobiles partagent de l'information en fonction de leurs besoins — ou intérêts —, et au gré de leurs rencontres. Le travail de thèse présenté dans ce mémoire s'inscrit dans cette perspective, puisqu'il porte sur le support de la communication basée contenus dans les réseaux mobiles ad hoc discontinus.

La communication basée contenus est un modèle de communication dans lequel l'information circule dans le réseau en fonction de l'intérêt que les terminaux y portent plutôt que vers une destination bien établie. Dans ce modèle, les terminaux du réseau affichent leur intérêt pour un certain type d'information, en *s'abonnant* afin de recevoir spécifiquement les messages contenant ce type d'information. Quant aux producteurs d'information, ils se contentent d'injecter — ou de *publier* — des messages dans le réseau, sans spécifier de destination spécifique pour ces messages. Le système de communication sous-jacent, c'est-à-dire une plate-forme intergicielle exploitant le réseau, est alors en charge de délivrer chaque message aux terminaux intéressés par son contenu. De nombreuses applications peuvent bénéficier d'un tel modèle de communication, comme par exemple des applications nécessitant du partage de ressources ou de la découverte de services.

Les réseaux mobiles ad hoc — ou MANETs (*Mobile Ad hoc NETWORKs*) — sont des réseaux constitués de terminaux mobiles capables de communiquer directement les uns avec les autres par transmission radio à courte portée, grâce à des technologies telles que Wi-Fi ou Bluetooth. La figure 1 illustre ce concept. La partie gauche de cette figure représente un MANET constitué des ordinateurs portables et assistants numériques personnels d'individus nomades. La partie droite de la figure présente un graphe modélisant ce même réseau. Les nœuds du graphe représentent les terminaux transportés par les individus, et les arêtes symbolisent la connectivité radio entre deux nœuds voisins, c'est-à-dire le fait que les deux terminaux se trouvent à portée radio l'un de l'autre.

Les MANETs ont fait l'objet de nombreux travaux de recherche au cours des deux dernières décennies. Dans un premier temps, ces travaux ont essentiellement été menés à des fins militaires. En effet, la rapidité de mise en œuvre de ce type de réseau sur le terrain est un avantage lors d'intervention dans un contexte de guerre ou de catastrophe naturelle. Depuis quelques années, des applications civiles des MANETs sont également envisagées, leur utilisation se justifiant en effet lorsque l'emploi d'un réseau d'infrastructure s'avère techniquement difficile ou économiquement peu rentable.

Les premiers travaux portant sur les MANETs ont essentiellement eu pour objectif de reproduire les conditions de fonctionnement d'Internet, c'est-à-dire le fait qu'un message puisse être acheminé — ou « routé » — de proche en proche à travers le réseau. Dans Internet, cet acheminement est assuré par des équipements dédiés baptisés routeurs, qui sont au cœur de l'infrastructure du réseau. Or un MANET ne permet pas de disposer de tels équipements dédiés. Les terminaux mobiles eux-mêmes doivent donc être mis à contribution afin d'assurer le

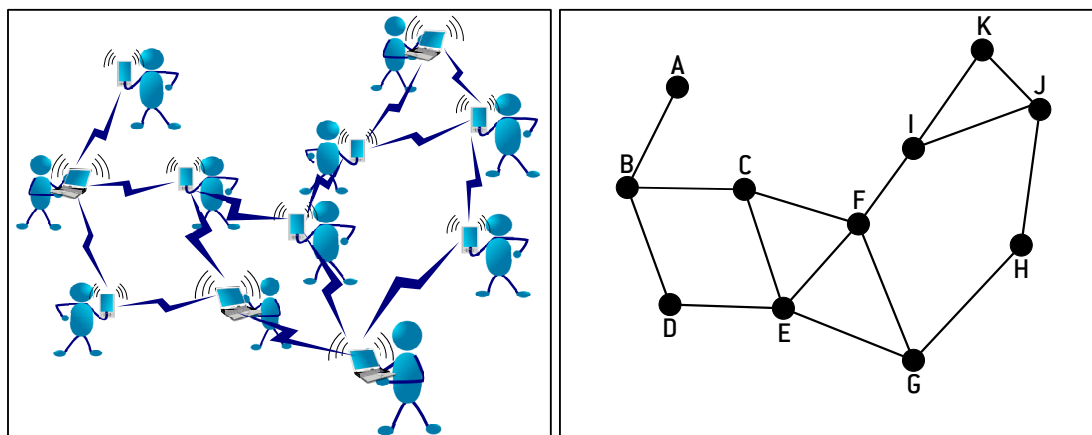


Figure 1 – Réseau mobile ad hoc, et graphe correspondant au réseau formé par ces terminaux mobiles communicants. Chaque nœud du graphe symbolise un terminal et la présence d'une arrête entre deux nœuds symbolise le fait que deux terminaux mobiles sont à portée radio l'un de l'autre.

routage des messages entre émetteurs et destinataires. Considérons par exemple le réseau de la figure 1. Lorsque le terminal A souhaite envoyer un message au terminal J, une route depuis A jusqu'à J doit impérativement être identifiée pour que la transmission puisse avoir lieu. Dans le cas présent, une telle route entre A et J pourrait passer par les terminaux B, C, E, G, et H ou encore par B, D, E, F et I. En l'absence d'une route exploitable, le message est considéré comme étant irrémédiablement perdu. Chaque terminal doit donc jouer à la fois le rôle de routeur (en collaborant avec les autres terminaux afin de déterminer les routes nécessaires à l'acheminement des messages) et d'entité applicative (en envoyant et recevant des données applicatives).

La mobilité des terminaux dans un MANET introduit une dynamique de la topologie du réseau. Une route ayant permis l'acheminement d'un message à un moment donné peut ne plus être exploitable quelques instants plus tard. Les protocoles de routage utilisés par les terminaux mobiles doivent prendre en compte cette dynamique afin de tolérer les fréquents changements de topologie du réseau.

La plupart des travaux réalisés dans ce domaine ces dernières années reposent sur des hypothèses qui ne sont pas toujours vérifiées dans la pratique. En effet, ils supposent une densité et une répartition géographique favorable des terminaux, ainsi qu'une mobilité modérée de ces terminaux. Un MANET présentant de telles propriétés présente l'avantage d'être connexe, c'est-à-dire qu'une route peut être trouvée à tout instant entre toute paire de terminaux. Dans de telles conditions les protocoles de routage évoqués plus haut peuvent jouer leur rôle. Dans la pratique les MANETs ne présentent pas toujours des propriétés aussi favorables. Un MANET peut en effet être non-connexe de manière épisodique ou chronique. La figure 2 présente à titre d'exemple le cas d'un MANET similaire à celui de la figure 1 mais dans lequel les distances entre terminaux sont telles que le graphe modélisant le réseau n'est pas connexe. Ce graphe apparaît alors comme une collection de sous-graphes connexes — ou îlots de connectivité — au sein desquels le routage est possible, mais entre lesquels aucun routage n'est envisageable à travers la seule

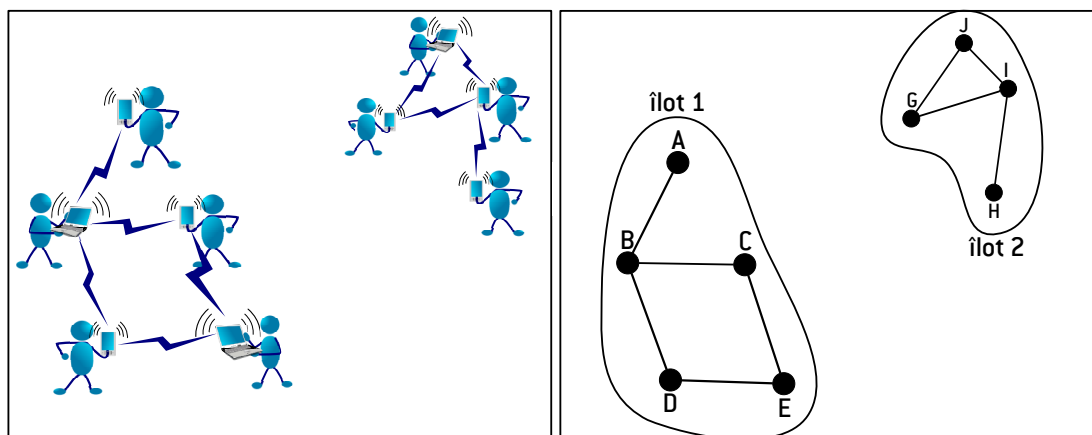


Figure 2 – Exemple de réseau mobile ad hoc discontinu formé par des individus nomades équipés de terminaux communicants. Le graphe représentant ce réseau est fragmenté en deux sous-graphes que l'on nomme « îlots de connectivité ».

utilisation des protocoles mentionnés précédemment. L'expression « réseau mobile ad hoc discontinu » — ou DMANETs (*Disconnected Mobile Ad hoc NETWORKs*) — est utilisée dans la littérature pour désigner ce type particulier de réseau.

Dans un DMANET, les protocoles de routage dynamique conçus pour les MANETs connexes ne permettent pas d'obtenir des résultats satisfaisants. Depuis quelques années, l'activité de recherche a donc été étendue afin de prendre en compte les spécificités des DMANETs. L'approche adoptée consiste à mettre à profit la mobilité des terminaux afin de tenter de rétablir une certaine forme de connectivité entre les îlots déconnectés du réseau. Par exemple, dans le cas présenté dans la figure 2, lorsque le terminal A souhaite envoyer un message au terminal J, il est nécessaire qu'un terminal en mouvement transporte physiquement ce message depuis l'îlot 1 jusqu'à l'îlot 2, lui faisant ainsi franchir une distance qui ne peut être couverte par voie radio. La figure 3 illustre ce mécanisme, le terminal C jouant ici le rôle de mule de données (*data mule*) entre les deux îlots. Pour mettre en œuvre un tel mécanisme, les terminaux mobiles doivent pouvoir stocker temporairement des messages en transit dans le réseau avant de les réémettre plus tard au moment opportun. L'expression de « communication opportuniste » (*Opportunistic Networking*) est utilisée dans la littérature pour désigner le mode de communication résultant de cette approche. La notion d'opportunisme fait ici référence à l'exploitation opportuniste de contacts radio occasionnels — et souvent non planifiés — entre les terminaux mobiles afin d'assurer l'acheminement des messages à travers un DMANET.

Le support du modèle de communication basée contenus dans des DMANETs n'a pas fait l'objet de beaucoup d'études jusqu'à ce jour. Ce modèle de communication asynchrone, qui permet un fort découplage entre producteurs et consommateurs d'informations, se satisfait pourtant fort bien de la nature discontinue et non-prévisible de ces réseaux. Le travail réalisé dans le cadre de cette thèse porte sur la conciliation des propriétés des DMANETs avec les exigences de la communication basée contenus. Ce travail s'est soldé par la définition d'un modèle de communication s'appuyant sur une combinaison judicieuse des principes de la communication basée

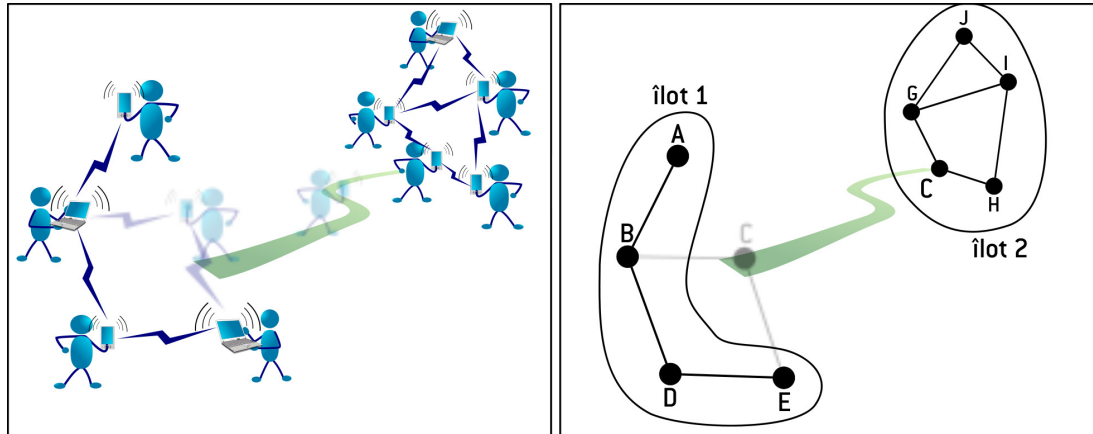


Figure 3 – Illustration de la communication opportuniste dans un réseau mobile ad hoc discontinu. Le terminal C joue ici le rôle de mule de données en transportant un message émis par un terminal de l'îlot 1 à destination d'un terminal de l'îlot 2.

contenus et de la communication opportuniste, ainsi que par la mise en œuvre de ce modèle sous forme d'une plate-forme logicielle.

ORGANISATION DU MÉMOIRE

Ce document est organisé en quatre chapitres. Le premier chapitre précise le domaine d'étude de notre travail. Après un état de l'art sur les protocoles de routage conçus pour assurer l'acheminement dans des MANETs et DMANETs, ce chapitre présente le modèle de la communication basée contenus ainsi que les quelques travaux ayant porté sur la définition d'un support pour la communication basée contenus prenant en compte les propriétés particulières des DMANETs.

Après avoir dressé les contours du domaine d'étude et les objectifs de ce travail de thèse, le deuxième chapitre de ce document présente notre proposition. En nous appuyant sur le modèle de la communication opportuniste, nous définissons un protocole permettant la dissémination sélective dans un DMANET d'informations structurées — ou *documents* — en fonction de leur contenu. Dans ce chapitre sont détaillés l'architecture générale du système, et les mécanismes permettant la sélection, ainsi que l'échange opportuniste de documents au gré de rencontres occasionnelles et non planifiées entre terminaux mobiles.

Le troisième chapitre présente la plate-forme intergicielle DoDWAN (*Document Dissemination in mobile Wireless Ad hoc Networks*). Ce prototype met en œuvre le protocole de communication proposé dans le chapitre 2 et supporte un mode de communication par publication-abonnement. Ce mode de communication convient naturellement à la communication basée contenus et à de nombreuses applications envisageables dans les DMANETs. Plusieurs services applicatifs exploitant le modèle de communication supporté par DoDWAN sont également décrits dans ce chapitre.

Les performances du protocole de communication défini dans le cadre de ce travail de thèse ont été évaluées à travers deux types de campagnes : la simulation et l'expérimentation. Le quatrième chapitre de ce mémoire présente des résultats obtenus lors de l'évaluation de notre protocole par simulation, ainsi que des résultats obtenus lors d'une expérimentation de notre protocole sur une plate-forme de test composée de PR4G, qui sont des postes radio utilisés dans les réseaux tactiques de l'armée française. Nous avons pu réaliser cette expérimentation originale car les travaux réalisés dans le cadre de cette thèse ont été financés par la DGA (Direction Générale de l'Armement). Les résultats présentés dans ce chapitre attestent de l'efficacité et de la robustesse du protocole proposé, et montrent la pertinence des choix que nous avons réalisés lors de sa conception.

Nous concluons ce document en rappelant le contexte et, en confrontant les objectifs initiaux aux contributions de ce travail de thèse. Nous évoquons également quelques perspectives de recherche découlant de nos travaux.

COMMUNICATION DANS LES RÉSEAUX MOBILES AD HOC DISCONTINUS

Dans ce chapitre, nous dressons un état de l'art des travaux réalisés dans le domaine des réseaux mobiles ad hoc (MANETs : *Mobile Ad Hoc Networks*). Nous commençons par préciser ce qu'est un MANET, et soulignons les problèmes inhérents à ce type de réseau (paragraphe 1.2). Nous présentons ensuite un panorama des travaux réalisés au cours des deux dernières décennies en vue d'assurer le routage de messages au sein des MANET, en soulignant que les solutions proposées ne sont toutefois applicables que dans des réseaux présentant une connexité favorable. Dans le paragraphe 1.3.1, nous montrons que, dans des MANETs déployés en conditions réelles, des terminaux mobiles peuvent se trouver isolés de manière chronique ou intermittente (le réseau se présentant alors sous la forme d'un ensemble discontinu d'îlots), et que dans de telles conditions les protocoles de routage « traditionnels » sont inadaptés. Dans le paragraphe 1.3.2, nous introduisons le concept de communication opportuniste, et montrons qu'il permet de tolérer la connectivité partielle dans les MANETs discontinus. Nous présentons les principaux travaux réalisés dans ce domaine, en soulignant qu'ils visent pour la plupart à permettre un routage des messages en fonction de leur destination.

L'objectif de ce travail de thèse étant de supporter la communication basée contenus dans des DMANETs, nous présentons dans le paragraphe 1.4 ce mode de communication atypique. Nous dressons un panorama de travaux récents visant à réaliser ce type de communication, en distinguant les solutions applicables dans des réseaux connexes (Internet ou MANET) de celles ciblant plus spécifiquement les MANETs discontinus (paragraphe 1.4.3). Pour clore ce chapitre nous discutons des différentes approches exposées, en nous efforçant de faire ressortir les atouts et les inconvénients de chacune d'entre elles. L'objectif est ici d'identifier les limitations des solutions présentées, tout en retenant les points forts dont nous pouvons nous inspirer dans nos propres travaux.

1.1 HISTORIQUE

La notion de réseau ad hoc est née il y a plusieurs dizaines d'années dans un cadre d'applications militaires, notamment grâce aux projets successifs menés par la DARPA¹ aux États-Unis.

1. La DARPA (*Defense Advanced Research Projects Agency*) est une agence du département de la Défense des États-Unis en charge de la recherche et du développement des nouvelles technologies destinées à un usage militaire.

L'objectif principal de ces travaux était de fournir aux forces armées américaines un système de communication s'appuyant sur des transmissions par ondes radio, capable de s'auto-configurer, et de s'auto-réparer en cas de perte d'éléments constituant. En outre, dans les réseaux tactiques, certains éléments doivent pouvoir être mobiles (e.g. équipements embarqués dans des véhicules ou transportés par des fantassins) et capables d'offrir des services de communication par voix et par données entre ou pendant les déplacements.

Dès les années 1970, la DARPA a financé un projet portant sur le développement d'un réseau à commutation de paquets s'appuyant sur des transmissions par ondes radio. Ce projet nommé ALOHA (*Areal Locations of Hazardous Atmospheres*) a non seulement permis la naissance du premier réseau ad hoc radio mais a aussi permis de fixer les bases du standard Ethernet (IEEE 802.3). Suite à ce succès, les projets dans ce domaine se sont multipliés. À partir des années 1980, les projets PRNet [JT87] (*Packet Radio Network*), SURAN [Bey90] (*Survivable, Adaptive Networks*) et LPR [BFQ87] (*Low-cost Packet Radio*) ont permis le développement de postes radio de faible encombrement et peu coûteux, de protocoles radio de plus en plus robustes et sécurisés (partage d'accès au médium, chiffrement, étalement de spectre, etc.), et des premiers protocoles de routage dynamique pour réseaux ad hoc dans lesquels les terminaux sont mobiles. Par la suite, durant les années 1990, la DARPA s'est intéressée à l'intégration des réseaux mobiles ad hoc dans les réseaux tactiques exploitant la suite de protocoles Internet à travers les projets GloMo [LRS96] (*Global Mobile Information System*) et TI (*Tactical Internet*). L'adaptation de ces protocoles a notamment permis la numérisation du champs de bataille. Aujourd'hui chaque véhicule, chaque fantassin dispose d'un moyen de communication radio lui permettant d'être en contact permanent avec la chaîne de commandement et les systèmes d'armes.

C'est à partir du milieu des années 1990 que la possibilité d'une utilisation civile des réseaux exploitant des transmissions par ondes radio est apparue. Ces années sont marquées par l'apparition sur le marché de technologies de communications sans fil comme par exemple Wi-Fi (IEEE 802.11) et Bluetooth (IEEE 802.15.1). Depuis leur apparition, ces différentes normes n'ont cessé d'évoluer, et d'autres ont été développées pour des besoins particuliers, comme par exemple la norme ZigBee (IEEE 802.15.4) pour les réseaux de capteurs.

La technologie Wi-Fi permet de connecter un terminal mobile à un réseau d'infrastructure, en déployant des points d'accès capables de jouer le rôle de passerelles entre le monde sans fil et le monde filaire. Ce mode de fonctionnement dit « mode infrastructure » est privilégié par les utilisateurs, il permet l'accès sans fil à un réseau d'entreprise et à l'Internet. Par exemple, les boîtiers ADSL qui équipent maintenant un foyer français sur deux incluent chacun un point d'accès Wi-Fi. Ce dernier permet de connecter à Internet chaque équipement situé à portée radio. Le déploiement de points d'accès Wi-Fi permet également à une entreprise d'étendre son réseau local à moindre coût. Il suffit pour ce faire de placer correctement quelques points d'accès dans l'entreprise, sans faire de travaux pour déployer de nouveaux câbles.

Les standards Wi-Fi, Bluetooth et ZigBee permettent également de déployer des réseaux dits « ad hoc », c'est-à-dire des réseaux dans lesquels des équipements situés à portée radio les uns des autres peuvent communiquer directement, sans avoir à dépendre pour ce faire d'un quelconque élément d'infrastructure. La norme Bluetooth est particulièrement adaptée pour connecter « sans fil » des périphériques tels qu'imprimantes, claviers et souris à un ordinateur.

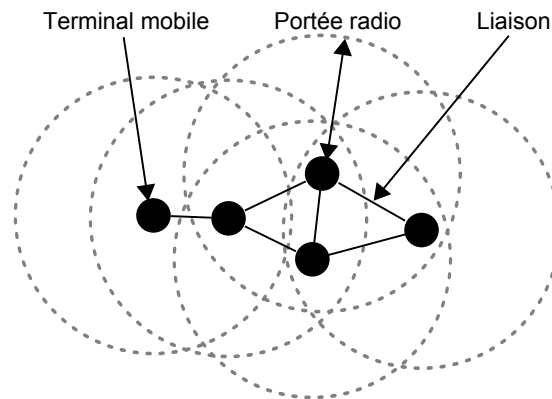


Figure 1.1 – Illustration d'un réseau ad hoc sous forme de graphe dans lequel les nœuds symbolisent les terminaux mobiles et les arêtes symbolisent la connectivité radio entre deux terminaux voisins

La norme ZigBee est généralement utilisée dans les réseaux de capteurs et dans certaines applications de domotique ou de surveillance de bâtiments. La norme Wi-Fi en mode ad hoc permet à des terminaux situés à portée radio les uns des autres de communiquer. Le recours à ce mode de communication se justifie dès lors que l'utilisation d'une infrastructure pour le support des communications s'avère soit techniquement difficile, soit économiquement peu rentable comme c'est par exemple le cas dans les réseaux de capteurs, les réseaux inter-véhicules, ou les réseaux tactiques militaires.

1.2 RÉSEAUX MOBILES AD HOC

1.2.1 PROBLÉMATIQUE DES RÉSEAUX MOBILES AD HOC

Les réseaux mobiles ad hoc sont généralement considérés comme des systèmes autonomes et dynamiques. Un MANET est constitué d'un ensemble de terminaux mobiles ou non en fonction de la nature du réseau (réseau de capteurs fixes, réseau de communication entre fantassins, réseau inter-véhiculaire, etc.). Ces terminaux sont interconnectés par des liaisons sans fil, indépendamment d'une infrastructure de communication et d'une administration centralisée. La figure 1.1 illustre ce concept. Dans cette figure, chaque terminal mobile est représenté par un nœud du graphe, et la portée radio d'un terminal est représentée par un cercle en pointillés. Lorsque deux terminaux sont à portée radio l'un de l'autre, une liaison peut être établie entre eux et qui peut leur permettre d'échanger des messages. Sur la figure la présence d'une liaison entre deux terminaux mobiles est représentée par une arête entre les nœuds correspondants.

Pour que des terminaux situés hors de portée radio les uns des autres puissent malgré tout s'échanger des messages, les terminaux mobiles doivent collaborer afin de « router » chaque message de proche en proche à travers le réseau depuis son émetteur jusqu'à son destinataire. Pour permettre ce type de communication multi-sauts, les terminaux doivent être capables de s'auto-organiser afin d'assurer la fonctionnalité principale attendue d'un réseau, c'est-à-dire le

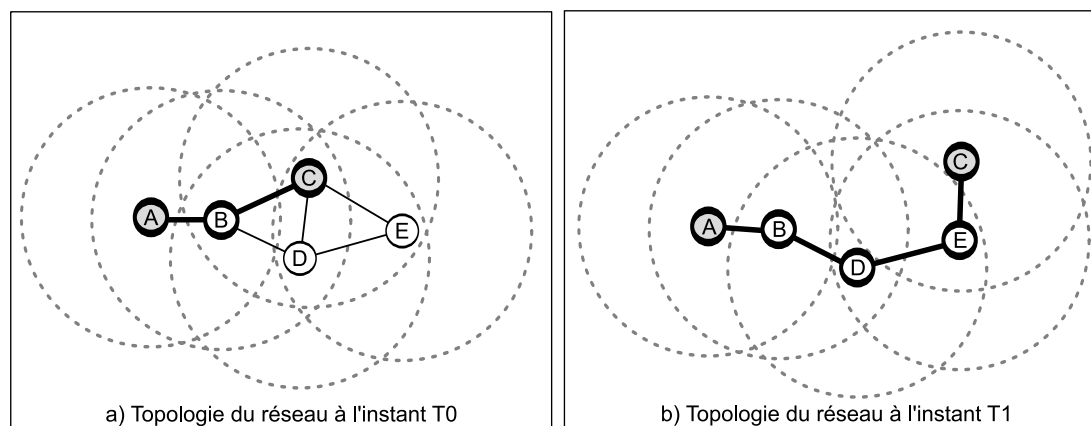


Figure 1.2 – Illustration de l'évolution de la topologie d'un réseau mobile ad hoc

routing de messages — classement de paquets IP — de bout en bout dans le réseau. Les terminaux doivent donc mettre en œuvre des protocoles de **routing dynamique** afin d'assurer la découverte des routes permettant l'acheminement des messages jusqu'à leurs destinataires.

Les terminaux qui participent à un MANET sont généralement libres de se déplacer ; cette mobilité des terminaux provoque des modifications fréquentes — et la plupart du temps imprévisibles — de la topologie du réseau. Les protocoles de routage dynamique conçus pour les réseaux filaires, par exemple OSPF [Moy98] (*Open Shortest Path First*) et RIP [Mal98] (*Routing Information Protocol*), ne sont pas adaptés à la dynamique qui caractérise les MANETs. La figure 1.2 illustre le problème lié à la mobilité des terminaux et aux changements de la topologie du réseau qu'elle implique. Considérons la topologie présentée dans la figure 1.2-a. Lorsque le terminal A souhaite envoyer un message au terminal C, une route entre A et C doit impérativement être trouvée afin que la transmission puisse avoir lieu. Dans le cas présent, cette route peut par exemple passer par le terminal B, comme illustré sur la figure. Quelques instants plus tard (figure 1.2-b), alors que le terminal C s'est déplacé, A souhaite de nouveau lui transmettre un message. Le chemin exploité lors de l'envoi du premier message ne permet plus d'atteindre C. Une nouvelle route reliant de bout en bout les terminaux A et C doit alors être identifiée. Les changements dynamiques de la topologie du réseau nécessitent donc de remettre sans cesse en question les routes qui ont pu être identifiées jusqu'alors, ces routes pouvant être devenues inutilisables.

1.2.2 ROUTAGE DANS LES RÉSEAUX MOBILES AD HOC

Au cours des deux dernières décennies, de très nombreux protocoles de routage dynamique pour réseaux mobiles ad hoc ont vu le jour. Ces protocoles ont tous pour vocation de tenir compte de la dynamique des réseaux pour lesquels ils ont été conçus. À la fin des années 1990, le groupe de travail MANET a été constitué au sein de l'IETF² en vue de standardi-

2. L'IETF (*Internet Engineering Task Force*) est un groupe international ouvert à tous contrôlé par l'IAB (*Internet Architecture Board*), et dont l'objectif est l'élaboration de standards pour Internet.

ser certains de ces protocoles. Les objectifs de ce groupe de travail ont été déterminés dans la RFC 2501 [CM99]. Ce document précise notamment ce qu'est un MANET, et les difficultés inhérentes à ce type de réseau, c'est-à-dire la topologie dynamique, les contraintes en termes de bande passante, d'énergie, de sécurité, et de passage à l'échelle. Quelques critères qualitatifs et quantitatifs sont également proposés pour évaluer la performance d'un protocole dans un contexte précis, déterminé par la densité, la connectivité moyenne, la rapidité des changements de topologie, etc.

Le groupe MANET a entrepris de recenser et évaluer les multiples protocoles développés jusqu'à ce jour en les classant en deux principales catégories : les protocoles de routage dynamique **réactifs** et **proactifs**.

1.2.2.1 ROUTAGE DYNAMIQUE RÉACTIF

Dans le routage réactif (*on-demand routing*), la route permettant l'acheminement d'un paquet IP n'est découverte que sur demande. Si un terminal doit router un paquet IP vers une destination pour laquelle il ne dispose d'aucune entrée dans sa table de routage, alors il diffuse un message de contrôle (*Route Request*) invitant les terminaux du réseau à mettre à jour leur table de routage pour cette destination précise. La mise à jour des tables de routage est réalisée grâce à un second message de contrôle (*Route Reply*) envoyé par le destinataire lui-même au terminal cherchant à l'atteindre. Ce message contient la route devant être suivie par le paquet IP à transmettre (*source routing*). De façon générale, les protocoles réactifs ont pour avantage de n'impliquer qu'un surcoût directement lié aux flux de données circulant entre les terminaux. En contrepartie, les protocoles de cette catégorie impliquent un temps de latence élevé avant qu'une route puisse être utilisée pour la première fois ou suite à des changements de la topologie. Le groupe de travail MANET a retenu le protocole DYMO [CP10] (*Dynamic MANET On-demand*), qui succède au protocole AODV [PBRD03] (*Ad hoc On-Demand Distance Vector*), en tant que protocole réactif de référence en vue d'une standardisation par l'IETF.

1.2.2.2 ROUTAGE DYNAMIQUE PROACTIF

Dans le routage proactif (*table-driven routing*), chaque terminal maintient en permanence à jour sa table de routage, de sorte que lorsqu'il doit router un paquet IP la route puisse être déterminée immédiatement. Pour ce faire, les terminaux diffusent périodiquement des messages de contrôle contenant tout ou partie de leur propre table de routage, qu'ils mettent à jour en fonction des informations reçues de leurs voisins. De manière générale, les protocoles de routage proactifs offrent de bonnes performances tant que les routes déterminées sont à jour. En effet, en plus d'introduire un surcoût élevé et constant à cause du trafic de contrôle incessant sans lequel ils ne pourraient fonctionner, les protocoles de routage proactifs présentent souvent des temps de réaction assez longs face aux changements de topologie (correction des tables de routage). Le protocole OLSRv2, qui succède à OLSR [CJ03] (*Optimized Link State Routing*), a été sélectionné par le groupe MANET comme protocole proactif de référence en vue d'une standardisation par l'IETF.

Les modèles de routage dynamique proactif et réactif présentent chacun des avantages et des inconvénients. Certains protocoles dits « hybrides » combinent ces deux approches afin de tenter de compenser les faiblesses de l'une par les qualités de l'autre.

1.2.2.3 ROUTAGE DYNAMIQUE HYBRIDE

Un exemple de protocole de routage hybride est le *Zone Routing Protocol* ou ZRP [Haa97]. ZRP est basé sur le constat qu'un changement de topologie dans le voisinage proche d'un terminal est a priori plus important (du point de vue de ce terminal) qu'un changement lointain. ZRP découpe donc le réseau en deux zones de routage (*Zone Routing*) autour de chaque terminal : une zone « IntrAzone » couvrant le voisinage proche d'un terminal (qui est exprimée en nombre de sauts) et une zone « IntErzone » constituée des terminaux situés hors de l'intrazone. ZRP utilise un protocole de routage de type proactif nommé IARP (*IntrAzone Routing Protocol*) dans l'intrazone et un protocole de routage réactif nommé IERP (*IntErzone Routing Protocol*) dans l'interzone. Grâce à l'utilisation du protocole proactif IARP, chaque terminal perçoit la topologie du réseau dans son intrazone et est en mesure de déterminer une route lui permettant d'atteindre chacun des terminaux situés à l'intérieur de celle-ci. Pour envoyer un message à un terminal situé en dehors de son intrazone, un terminal s'adresse aux terminaux situés en bordure de cette zone afin d'obtenir une route vers ce terminal, grâce à l'exploitation du protocole réactif IERP.

1.2.2.4 ROUTAGE DYNAMIQUE GÉOGRAPHIQUE

Pour améliorer les performances des protocoles de routage dynamique pour les MANETs, d'autres protocoles exploitent la position des terminaux pour améliorer ou assurer l'acheminement des messages à travers le réseau. Un protocole de routage est dit géographique lorsque les décisions de routage prennent en compte la position des terminaux. Le routage géographique nécessite que les terminaux soient capables d'estimer leur propre position (absolue ou relative), et que lors de l'envoi d'un message l'émetteur soit en mesure d'estimer la position du destinataire. Parmi les propositions de routage géographique, on peut distinguer deux catégories principales : une première catégorie dans laquelle les positions des terminaux sont exploitées afin d'améliorer les performances de protocoles de routage dynamique existants, comme par exemple LAR [KV00] (*Location Aided Routing*), et une seconde catégorie dans laquelle la position des terminaux est l'unique information exploitée pour acheminer les messages (Geo-Cast [KV99], GPSR [KK00], GRA [JPS01]). L'exploitation de la position des terminaux s'avère intéressante pour certains scénarios, comme en particulier le cas des réseaux véhiculaires. Les véhicules se déplaçant généralement le long d'axes routiers pré-existants, il est possible de déterminer la future position d'un véhicule et ainsi d'acheminer des messages de manière plus efficace.

1.2.2.5 AUTRES FAMILLES DE PROTOCOLES DE ROUTAGE

En plus des grandes catégories de protocoles évoquées ci-dessus, il existe de nombreuses autres approches proposées dans la littérature pour permettre aux terminaux d'un réseau mobile

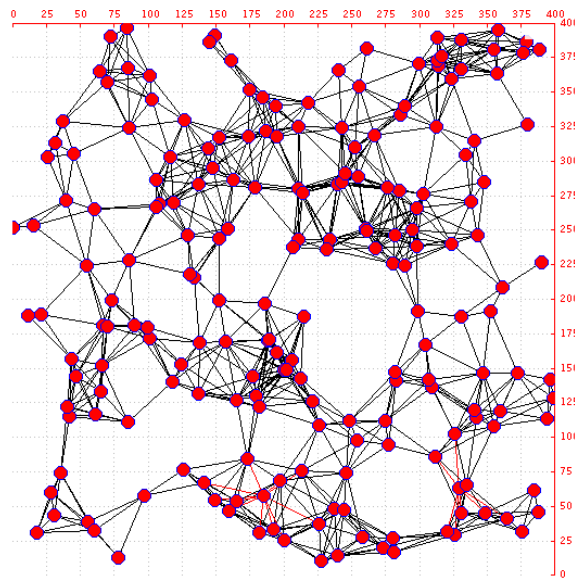


Figure 1.3 – Exemple de réseau mobile ad hoc composé de 200 terminaux mobiles communicants. La densité et la répartition géographique des terminaux dans l'environnement permettent de connecter chaque paire de terminaux mobiles.

ad hoc de s'échanger de l'information.

De manière non exhaustive on peut par exemple citer les protocoles mettant en œuvre des stratégies de gestion d'énergie, les protocoles réalisant de la différenciation de service pour fournir un support de qualité de service, des protocoles intégrant des mécanismes de sécurité, des protocoles de diffusion (*broadcast*) ou de diffusion sélective (*multicast*), etc.

1.3 RÉSEAUX MOBILES AD HOC DISCONTINUS

1.3.1 PROBLÉMATIQUE DES RÉSEAUX MOBILES AD HOC DISCONTINUS

Les travaux présentés dans le paragraphe précédent ont tous pour objectif de proposer des protocoles de routage dynamique permettant aux terminaux d'un MANET de communiquer les uns avec les autres. Ces travaux ont pour caractéristique commune de supposer des réseaux mobiles connexes. Pour ce faire, ils reposent sur des hypothèses de densité et de répartition géographique favorables des terminaux mobiles dans l'environnement.

Un exemple d'un tel MANET est proposé dans la figure 1.3. Ce réseau factice est constitué de 200 terminaux mobiles équipés d'interfaces de communication sans fil ayant une portée radio de 100 mètres qui sont répartis de manière aléatoire dans un espace ouvert de 1.6 km^2 . Ce réseau présente l'avantage d'être un réseau connexe, dans lequel les protocoles de routage dynamique évoqués dans le paragraphe 1.2.2 peuvent effectivement jouer leur rôle, dans la mesure où il est possible d'identifier à tout moment au moins un chemin de bout-en-bout reliant toutes paires de terminaux.

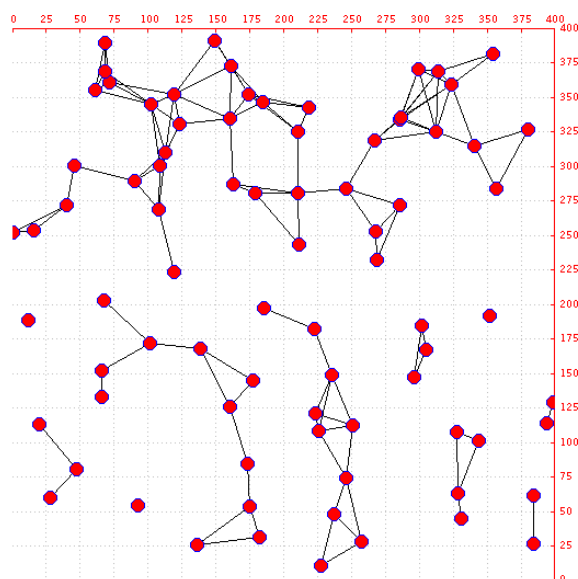


Figure 1.4 – Exemple de réseau mobile ad hoc discontinu composé de 80 terminaux mobiles communicants. La distribution clairsemée des terminaux se traduit par un partitionnement du réseau en sous-graphes connexes (ou « îlots ») aux contours fluctuants.

Les réseaux mobiles ad hoc déployés en conditions réelles ne présentent pas toujours des caractéristiques aussi favorables. Une répartition clairsemée ou irrégulière des terminaux mobiles dans l'environnement peut en effet provoquer le partitionnement du réseau en sous-graphes ou îlots. De tels réseaux mobiles ad hoc sont alors caractérisés par une connectivité partielle des terminaux. Ils sont généralement identifiés par le terme de MANET discontinus (DMANET : *Disconnected Mobile Ad hoc NETWORKs*).

Un exemple de DMANET est présenté dans la figure 1.4. Les terminaux ont la même portée radio et sont répartis sur le même espace que pour le réseau de la figure 1.3, mais les terminaux sont beaucoup moins nombreux (80 terminaux seulement pour le réseau de la figure 1.4). On peut constater sur cette figure que la réduction du nombre de terminaux sur ce même espace se traduit par le partitionnement du réseau en îlots connexes, le réseau étant globalement non-connecté.

Dans certains types de MANET le manque de connectivité entre les terminaux peut être aggravé du fait de leur volatilité. Certains terminaux mobiles peuvent en effet être tantôt actifs, tantôt inactifs du point de vue du réseau. La figure 1.5 présente un réseau présentant les mêmes caractéristiques que celui de la figure 1.4, cependant certains des terminaux sont cette fois-ci éteints ou mis en veille (dans la figure 1.5, ces terminaux sont représentés par des cercles vides), et ne sont donc pas en mesure de contribuer à l'acheminement de messages dans le réseau. On constate donc que la volatilité des terminaux est un facteur aggravant le partitionnement du réseau en îlots.

Au sein de chacun des îlots d'un MANET discontinu, les protocoles de routage dynamique tels que ceux évoqués dans le paragraphe 1.2.2 peuvent éventuellement assurer le routage de

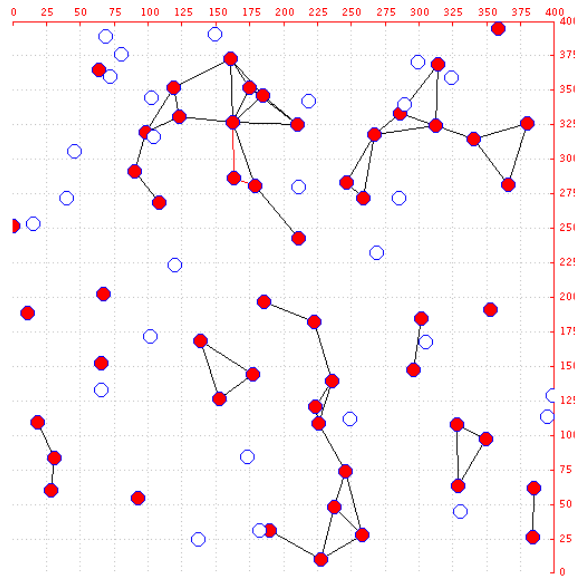


Figure 1.5 – Exemple de réseau mobile ad hoc discontinu composé de 80 terminaux mobiles communicants, les cercles vides symbolisent des terminaux éteints ou mis en veille par leur propriétaire. Cette volatilité réduit le nombre de terminaux susceptibles de participer à l'acheminement des messages.

messages. Cependant, lorsque deux terminaux se situant dans deux îlots distincts souhaitent communiquer, ces protocoles deviennent inefficaces voire inutilisables. En effet, avec ces protocoles de routage dynamique, l'émission d'un message (ou paquet IP) dans le réseau ne peut se faire que lorsqu'une route de bout-en-bout entre l'émetteur et le destinataire du paquet peut être identifiée, et que tous deux sont simultanément actifs. Tout message émis à destination d'un terminal situé dans un autre îlot que celui de l'émetteur ou a destination d'un terminal inactif, est donc irrémédiablement perdu.

Les protocoles de routage dynamique évoqués dans le paragraphe 1.2.2 ne sont donc utilisables que dans des MANETs connexes. Ils ne peuvent assurer l'acheminement de messages dans des MANETs discontinus.

Dans le cadre de ce travail de thèse nous nous sommes intéressés tout particulièrement au cas de MANETs discontinus dans lesquels les terminaux mobiles ont pour caractéristique d'être volatiles. Pour assurer l'acheminement de données dans ce type de réseaux, de nouveaux mécanismes tolérant les ruptures de connectivité temporaires ou durables entre terminaux doivent être proposés. Il s'agit alors de compléter — voire remplacer — les protocoles de routage dynamique existants par des protocoles de routage tolérant la connectivité intermittente entre les terminaux mobiles.

1.3.2 ROUTAGE DANS LES RÉSEAUX MOBILES AD HOC DISCONTINUS

Depuis quelques années, l'activité de recherche dans le domaine des MANETs a été étendue afin de prendre en compte les spécificités des MANETs discontinus. Le routage de messages dans ce type de réseaux est un sujet de recherche qui suscite un intérêt grandissant de la part de nombreuses équipes de recherche. L'approche généralement adoptée consiste à exploiter le modèle dit de « communication opportuniste » présenté ci-dessous.

1.3.2.1 COMMUNICATION OPPORTUNISTE

Bien que le concept de réseau mobile ad hoc soit étudié depuis plus d'une vingtaine d'années, une grande partie des travaux menés jusqu'à ce jour ont visé à bâtir un réseau permettant l'utilisation des standards IP, en considérant la mobilité, l'instabilité des liaisons radio et le partitionnement du réseau en îlots comme des problèmes occasionnels, n'affectant que très peu le comportement général du réseau. Le modèle de communication opportuniste [PPC06] (*Opportunistic Networking*) s'intéresse au cas où ces phénomènes sont monnaie courante, et, à ce titre, doivent être pris en compte dès la conception des protocoles de routage.

Pour rétablir une certaine forme de « connectivité » entre les îlots déconnectés du réseau, le principe fondamental qui caractérise le modèle de la communication opportuniste est d'exploiter la mobilité des terminaux. En effet, cette mobilité permet d'augmenter les performances dans l'acheminement des messages, voire de l'assurer lorsqu'un protocole de routage traditionnel ne le permet pas [GT01]. Pour ce faire, les protocoles de routage opportuniste proposés dans la littérature adoptent généralement le mode d'acheminement *store, carry and forward*. Cette technique est elle-même inspirée du principe de la communication tolérant les délais de transmission ou les ruptures de connectivité (*Delay/Disruptions-Tolerant Networking*), introduite par Kevin Fall [F⁺02]. Les travaux menés dans ces domaines sont fédérés par le DTNRG [F⁺02, CBH⁺06] (*Delay-Tolerant Network Research Group*) fondé en 2002 par l'IRTF. Ce groupe contribue à la promotion de travaux dont les champs d'application sont aussi divers que la communication dans les réseaux inter-planétaires (IPNRG³), les réseaux subaquatiques (UW-ASN⁴), les réseaux inter-véhiculaires (UMassDieselNet⁵, Drive-thru Internet⁶), les réseaux de capteurs (ZebraNet⁷) ou les MANETs discontinus (Haggle UE FP6⁸, PodNet⁹, SPINDLE¹⁰). Il est illusoire de croire qu'un unique protocole de routage puisse répondre à la totalité des besoins et des défis posés par ces domaines d'application aussi divers que variés.

3. <http://www.ipnsig.org/>

4. <http://www.ece.gatech.edu/research/labs/bwn/UWASN>

5. <http://prisms.cs.umass.edu/dome/index.php?page=umassdieselnet>

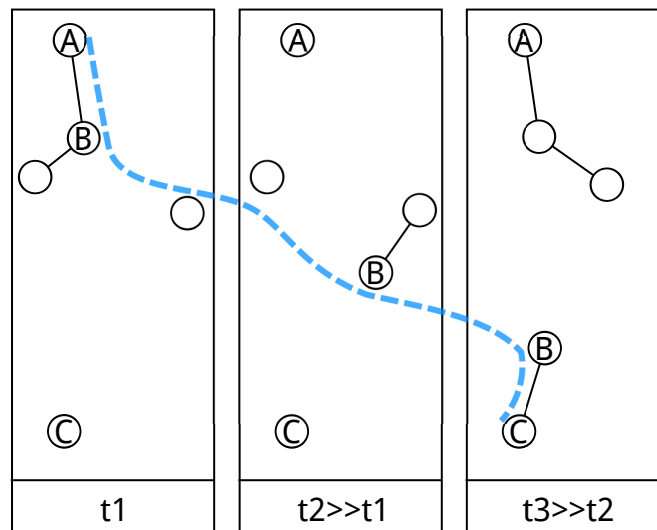
6. <http://www.drive-thru-internet.org/>

7. <http://www.princeton.edu/~mrm/zebranet.html>

8. <http://www.haggleproject.org/>

9. <http://podnet.ee.ethz.ch/>

10. <http://www.ir.bbn.com/projects/spindle/>

Figure 1.6 – Illustration du mode d'acheminement *store, carry and forward*.

Store, Carry and Forward. Le mode d'acheminement *store, carry and forward* consiste à doter tout ou partie des terminaux mobiles d'un espace de stockage leur permettant d'héberger temporairement des messages en transit dans le réseau, et à mettre à profit les contacts radio occasionnels — souvent non-planifiés — qui s'établissent au gré des déplacements des terminaux.

La figure 1.6 illustre ce mode d'acheminement. Dans le scénario présenté sur cette figure, le terminal A souhaite envoyer à l'instant $t1$ un message au terminal C. À cet instant, C est hors de portée de A, c'est-à-dire qu'aucune route de bout-en-bout permettant une communication instantanée avec C ne peut être identifiée. Le terminal A exploite alors l'opportunité qu'offre le terminal B de transporter « physiquement » le message vers son destinataire. À partir de l'instant $t1$, B stocke et transporte le message, et contribue alors à son acheminement à travers le réseau. Au cours de ses déplacements le terminal B rencontre, à l'instant $t2$, un autre terminal mobile auquel il peut éventuellement confier une copie du message émis par A. Puis il poursuit son trajet, au cours duquel il rencontre, à l'instant $t3$, le terminal C. B remet alors à C le message qui lui a été confié par A. Le terminal C reçoit donc finalement le message que A lui a envoyé, alors qu'aucune route de bout-en-bout n'a jamais existé entre émetteur et destinataire. L'acheminement de ce message a été rendu possible grâce à l'exploitation de contacts fugitifs entre terminaux mobiles, et à son transport « physique » par ces terminaux. De la sorte, ce message a cheminé le long d'une route « spatio-temporelle » (ligne en pointillés sur la figure 1.6), cette route s'étalant à la fois dans le temps et l'espace. On peut constater que la communication opportuniste peut impliquer une latence élevée puisque la vitesse de déplacement des terminaux et la fréquence de leurs contacts sont des propriétés non maîtrisables. De plus, ce mode de communication ne garantit pas la remise des messages à leur destinataire, dans la mesure où il dépend de la mobilité et des contacts entre terminaux qui sont généralement des paramètres subis. Les applications ou services exploitant ce mode de communication atypique doivent donc tolérer

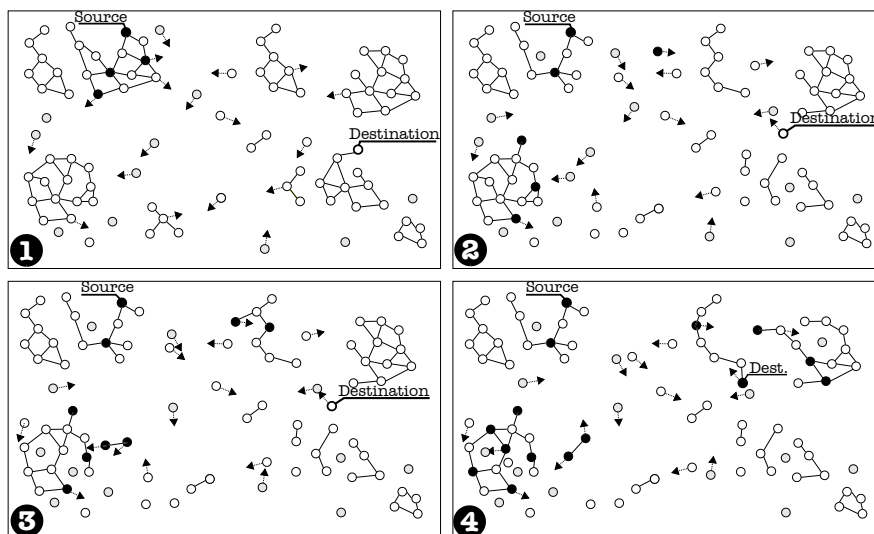


Figure 1.7 – Illustration de l'exploitation de la mobilité et des contacts fugitifs entre terminaux afin de réaliser l'acheminement d'un message depuis sa source jusqu'à sa destination. Le transport de copies par des terminaux en mouvement dans le réseau permet de rétablir une forme de connectivité entre source et destination, sur la figure les terminaux jouant le rôle de mule de données sont représentés par des ronds pleins. La quatrième partie de la figure montre que le destinataire a finalement reçu le message, bien qu'il n'ait jamais rencontré l'émetteur de ce message.

ces caractéristiques (temps de latence pouvant être élevés et pas de garantie de remise).

Une première approche pour réaliser le routage consiste à laisser le terminal émetteur d'un message le conserver, et le transporter jusqu'à un éventuel contact avec son destinataire (*Direct Transmission*) [SRJB03]. Cette solution n'est toutefois envisageable que dans le cas où source et destination entrent en contact. Dans le cas où les terminaux source et destination sont susceptibles de ne jamais entrer en contact l'un avec l'autre, l'idée est d'exploiter tout ou partie des terminaux mobiles comme relais (*data mules*), de sorte qu'ils puissent transporter et relayer le message de proche en proche, et finalement qu'un d'entre eux remette le message à son destinataire. La figure 1.7 illustre ce mécanisme.

Partant de cette idée, de nombreuses approches ont été proposées dans la littérature pour « router » les messages dans des MANETs discontinus. Les stratégies de routage diffèrent notamment sur le nombre de copies d'un message propagées dans le réseau, et sur les hypothèses formulées quant au comportement des terminaux mobiles dans le réseau. Trois grandes familles se distinguent :

- les protocoles s'appuyant sur une forme d'inondation plus ou moins contrôlée, présentés dans le paragraphe 1.3.2.2 ;
- les protocoles s'appuyant sur des historiques afin de guider le processus d'acheminement des messages, présentés dans le paragraphe 1.3.2.3 ;

- les protocoles s'appuyant sur les structures sociales liant les transporteurs entre eux pour réaliser le routage, présentés dans le paragraphe 1.3.2.4.

1.3.2.2 ROUTAGE PAR INONDATION

Le modèle le plus représentatif de cette catégorie est le protocole de **routage épidémique** [VB00] (*Epidemic Routing*). Dans ce protocole le processus d'acheminement du message est assimilé à la propagation d'une épidémie. Chaque message est considéré comme un virus, un terminal infecté par ce « virus » contaminant alors tout autre terminal rencontré. De la sorte, les chances de remettre un message à son destinataire sont augmentées, et la latence réduite à son minimum puisque le chemin « optimal » (le plus court en temps) est exploité. En revanche, un protocole de ce type entraîne un surcoût important, puisque la totalité des terminaux du réseau peut être sollicitée pour acheminer un message. En outre, cette méthode peut entraîner si elle est appliquée de manière brutale la saturation des espaces de stockage des terminaux mobiles [JP07]. De nombreuses variantes du modèle de routage épidémique ont été élaborées en vue d'éviter ce phénomène de congestion, et de réduire le coût associé à la dissémination de chaque message. Les variantes proposées dans la littérature reposent en général sur une ou plusieurs des méthodes suivantes :

Guérison du réseau (*network healing*). L'idée de base de ce mécanisme est de stopper la propagation des messages ayant atteint leur destinataire, afin de limiter stockages et transmissions inutiles. En effet, lorsqu'un message est remis à son destinataire, les terminaux porteurs de ce message n'en sont pas nécessairement informés et continuent donc de le propager. Pour éviter la surconsommation de ressources que cela entraîne, l'idée est de permettre au destinataire du message d'injecter un « antidote » dans le réseau [SH05]. La propagation de cet antidote (*passive cure* [HABR05]) indique aux terminaux mobiles transportant une copie du message original qu'il n'est plus utile de continuer à le propager.

Limitation de la portée temporelle ou spatiale d'un message. Différentes méthodes peuvent être utilisées afin de limiter la portée temporelle ou spatiale d'un message. Par exemple, [HABR05] propose d'ajouter à chaque message une date de péremption (ou durée de vie) après laquelle la propagation du message est inutile. Dans ces travaux, la durée de vie est un paramètre protocolaire fixé en fonction de propriétés supposées connues du réseau (par exemple envergure spatiale, vitesse des terminaux mobiles, fréquence des contacts, etc.). Chaque message se voit alors allouer la même durée de vie. Une approche alternative (non proposée dans [HABR05]) consisterait à ajuster la durée de vie de chaque message en fonction de son contenu.

En ce qui concerne la limitation de la portée spatiale, il est à noter qu'elle ne peut pas se faire simplement en limitant le nombre de fois qu'un message peut être relayé (comme cela est le cas pour les paquets IP dans Internet). En effet, un terminal peut se déplacer sur de longues distances avant de rencontrer un autre terminal. En revanche, lorsque les terminaux sont en mesure de déterminer leur position, il est possible alors d'associer à chaque message une zone géographique en dehors de laquelle il ne doit pas être disséminé.

Limitation du nombre de porteurs d'un message. Cette méthode vise principalement à réduire la quantité de ressources nécessaire à la livraison d'un message, tout en essayant de conserver de bonnes performances. Pour ce faire, différentes méthodes ont été proposées. Elles reposent sur une approche probabiliste, c'est-à-dire que l'envoi d'une copie d'un message à un terminal mobile est déterminé avec une certaine probabilité [ZNKT07, NTCS99], ou sur la base d'heuristiques déterministes permettant de limiter le nombre de copies propagées dans le réseau [HABR05]. Une variante intéressante dans cette deuxième catégorie est le protocole *Spray and Wait* [SPR05] qui se déroule en deux phases. Pendant la phase *Spray*, de multiples copies du message sont injectées dans le réseau par son émetteur, voire par les porteurs. Cette phase se termine lorsque L copies du message initial ont été injectées dans le réseau. Lors de la phase *Wait*, chaque terminal transportant une copie du message d'origine attend d'éventuellement rencontrer le terminal destinataire pour lui remettre le message. Cette phase se termine lorsque le message est remis à destination. Les auteurs de [SPR05] proposent un modèle analytique permettant de calculer le nombre de copies à créer en fonction du délai de livraison escompté, mais ce calcul nécessite de connaître certaines caractéristiques du réseau (envergure et nombre de terminaux participants). Ils montrent toutefois que, même si leur protocole peut sembler simple, il permet malgré tout d'obtenir des résultats satisfaisants par rapport à des approches plus complexes (comme celles évoquées par la suite), et il supporte un passage à l'échelle lorsque la densité et la connectivité du réseau augmentent.

Le modèle de routage épidémique et ses variantes évoquées précédemment permettent le routage de messages dans des réseaux dont l'évolution de la topologie est inconnue. Ils ont pour caractéristique commune d'exploiter les occasions qu'ont les terminaux de faire de « bonnes rencontres ». En effet, grâce à la propagation « virale » des messages et au hasard des contacts, certains porteurs vont contribuer de manière efficace à l'acheminement de messages à travers le réseau. En revanche, d'autres terminaux propageront des messages inutilement, ce qui peut impliquer un surcoût élevé. Il est à noter que, lorsqu'un message doit être acheminé vers un groupe de terminaux (*multicast*), voire vers l'ensemble des terminaux du réseau (*broadcast*), les protocoles de routage épidémique s'avèrent particulièrement adaptés [VB00, HABR05, SH05, SPR05, ZNKT07].

Un protocole de routage opportuniste efficace est censé combiner un taux de remise à destination élevé, un délai de remise minimum, et une faible consommation des ressources. Développer un tel protocole constitue le défi principal posé dans les réseaux mobiles ad hoc discontinus. Jain *et al.* [JFP04] montrent que grâce à l'exploitation d'informations concernant l'évolution du réseau, et en particulier l'aptitude à prévoir les futurs contacts entre terminaux mobiles, il est possible de construire des protocoles efficaces. De nombreuses approches ont été proposées dans ce sens, et sont brièvement présentées dans les deux paragraphes suivants.

1.3.2.3 ROUTAGE S'APPUYANT SUR DES HISTORIQUES

Les protocoles de routage de cette famille exploitent des informations contextuelles variées pour guider le processus d'acheminement des messages. Dans ces travaux, l'hypothèse

fondamentale est que les terminaux mobiles — et implicitement leurs transporteurs — ont tendance à exhiber des schémas de mobilité récurrents. Ces schémas peuvent être identifiés (plus ou moins automatiquement), et utilisés afin de sélectionner le ou les meilleurs porteurs pour chaque message. De la sorte, les protocoles de cette famille sont censés réduire le surcoût lié à l'acheminement d'un message en prédisant l'évolution future de la topologie du réseau à partir de son évolution passée.

Pour déterminer quels sont les terminaux mobiles qui vont contribuer de manière efficace à l'acheminement d'un message, ces protocoles reposent sur des heuristiques ou fonctions d'utilité (*utility function*) permettant à un terminal d'évaluer la probabilité qu'il a de remettre un message à un destinataire donné et s'appuient, pour ce faire, sur des historiques d'informations variées.

Le *Probabilistic ROuting Protocol using History of Encounters and Transitivity* (PROPHET) [LDS04] calcule la probabilité de remise en utilisant un historique de contacts entre terminaux mobiles. Lorsqu'un terminal doit envoyer ou relayer un message, il en confie une copie à chaque terminal qu'il rencontre qui possède une probabilité de remise supérieure à la sienne. Pour estimer cette probabilité, PROPHET utilise un historique de contacts, ainsi que la transitivité des contacts entre terminaux mobiles. La probabilité de remise d'un message à destination augmente lorsqu'un terminal rencontre fréquemment le destinataire (ou un autre terminal rencontrant fréquemment ce destinataire) et diminue entre les rencontres. PROPHET s'appuie donc sur la fréquence des contacts entre terminaux mobiles pour guider le processus d'acheminement des messages.

Cette même information est utilisée dans *Meetings and Visits* (MV) [BBL05] et MaxProp [BGJL06]. Dans MaxProp, la probabilité de remise d'un message est estimée en fonction de la similarité de trajet entre un terminal et le destinataire. La similarité de trajet est évaluée grâce aux historiques de contacts des terminaux. Le protocole de routage MV utilise, comme PROPHET, la fréquence de contact entre terminaux. La probabilité de remise d'un message à un destinataire donné est déterminée en se basant sur des informations « récentes » que sont les dates de rencontres (*meetings*) entre deux terminaux, et les dates de visites (*visits*) de zones géographiques pré-déterminées (ce qui nécessite donc de limiter la zone géographique couverte par le réseau). De la même manière que MaxProp, MV sélectionne comme bons porteurs d'un message les terminaux ayant un schéma de mobilité similaire à celui du destinataire. On notera que le schéma de mobilité du destinataire doit donc être connu, ou que sa position géographique doit être fixe.

Le protocole *MobySpace Routing* [JLC05] se base exclusivement sur les schémas de mobilité des terminaux (supposés connus) afin que l'émetteur d'un message puisse déterminer une route de bout-en-bout jusqu'au destinataire. Pour ce faire, les terminaux doivent partager une vision commune d'un espace Euclidien modélisant les schémas de mobilité de l'ensemble des terminaux du réseau. Dans cet espace, chaque axe représente un contact entre deux terminaux mobiles, et la distance le long de cet axe représente la probabilité qu'une nouvelle rencontre ait lieu entre ces deux terminaux. En théorie, ce protocole de routage permet à l'émetteur d'un message de déterminer de manière exacte quels sont les porteurs qui doivent participer à l'acheminement de son message. Lors d'une utilisation réelle de ce protocole, il sera en revanche impossible pour les terminaux de partager un état global du réseau. Les informations collectées

par les terminaux ne peuvent donc être que partielles (voire obsolètes). Par conséquent, le routage ne peut pas être optimal puisque l'espace Euclidien, grâce auquel les décisions de routage sont réalisées, n'est que partiel.

Le protocole *Spray and Focus* [SPR07] utilise la durée écoulée depuis la dernière rencontre entre deux terminaux pour prévoir une prochaine rencontre. Ce protocole est une version modifiée du protocole *Spray and Wait* [SPR05], dont la seconde phase *Focus* consiste à transférer la copie du message à un terminal ayant une probabilité de remise supérieure à celle du porteur actuel plutôt que d'attendre de rencontrer la destination (phase *Wait*). La responsabilité de remettre le message à son destinataire est alors déléguée au nouveau porteur, qui peut à son tour réaliser la même opération. À travers cette opération de routage, *Spray and Focus* permet d'acheminer un message vers une destination même si les porteurs ayant reçu une copie du message initial créé par la source ne rencontrent jamais le destinataire, ce qui serait impossible en utilisant *Spray and Wait*.

Le même type d'information est exploité dans *Last Encounter Routing* [GV03] pour estimer la probabilité de remise. Cependant, contrairement aux protocoles mentionnés précédemment, ce protocole n'achemine qu'une seule copie d'un message. L'acheminement d'un message est réalisé de proche en proche en sélectionnant les terminaux ayant rencontré le plus récemment le destinataire. L'unique copie du message « migre » alors vers le terminal destinataire en étant relayé le long d'une unique route spatio-temporelle, ce qui rend ce protocole sensible aux erreurs puisqu'il suffit d'un mauvais relais de la part d'un terminal, voire la destruction d'un relais, pour compromettre le processus d'acheminement d'un message.

Le protocole *Disconnected Transitive Communication* (DTC) [CM01] achemine lui aussi une unique copie du message original. Dans DTC, la probabilité qu'un terminal puisse délivrer un message donné est estimée en fonction de sa « proximité » (*closeness*) avec le terminal destinataire. D'une manière similaire à PROPHET, la probabilité de remise est déterminée en s'appuyant sur un historique de contacts et sur la transitivité des contacts entre terminaux mobiles. Néanmoins, DTC se distingue des protocoles mentionnés ci-dessus par le fait qu'il suppose l'utilisation d'un protocole de routage dynamique. Grâce à ce dernier protocole, les terminaux mobiles temporairement présents dans un îlot du réseau sont en contact. Lorsqu'un terminal doit envoyer ou acheminer un message à un destinataire situé en dehors de l'îlot, le message est transféré au terminal voisin présent dans l'îlot ayant la proximité la plus élevée avec le destinataire. Ce voisin stocke le message afin de le remettre plus tard, potentiellement dans un autre îlot, à son destinataire.

L'idée d'exploiter un protocole de routage dynamique dans les portions connexes du réseau est reprise dans *Context Aware Routing* (CAR) [MHM05, MM09]. Comme dans DTC [CM01], lorsqu'un terminal souhaite envoyer ou relayer un message adressé à un destinataire qui ne se situe pas dans l'îlot auquel il appartient, il sélectionne parmi les terminaux présents dans l'îlot celui qui possède la meilleure probabilité de remise du message à destination et lui transfère (délègue) le message. Pour ce faire, chaque terminal diffuse dans l'îlot un message qui indique, pour chaque destinataire connu, sa probabilité de remise. Dans CAR, cette probabilité de remise est déterminée par une fonction d'utilité qui prend en compte de multiples informations contextuelles telles que l'énergie restante, la probabilité de co-location, le taux de changement

de connectivité, etc.

Les protocoles de routage opportuniste de cette famille cherchent à prévoir les contacts futurs entre terminaux. Dans ce sens ces protocoles sont applicables uniquement dans des réseaux mobiles discontinus dans lesquels les terminaux présentent des schémas de mobilité récurrents impliquant des contacts réguliers. Cette hypothèse autorise les auteurs à développer des heuristiques permettant de prédire les contacts futurs entre terminaux sur la base d'informations (par exemple les dates de contacts entre terminaux) le plus souvent collectées, partagées et conservées par les terminaux eux-mêmes. On peut donc noter que, sans historique, ces protocoles ne sont pas opérationnels. Ils nécessitent une certaine phase d'apprentissage des « habitudes » des terminaux mobiles avant d'être opérationnels, et ne conviennent donc pas pour assurer les communications dans les réseaux déployés temporairement. Une autre question ouverte relative à l'exploitation d'historiques par ces protocoles est le passage à l'échelle de ces méthodes de prévision. À ce jour ces protocoles n'ont pas été exploités dans des réseaux de grande envergure, couvrant par exemple la population d'une ville de taille moyenne (environ 20 000 habitants). Cependant ils peuvent se révéler efficaces dans des réseaux de petite taille dans lesquels les terminaux communicants ont des comportements récurrents.

1.3.2.4 ROUTAGE « SOCIAL »

Les protocoles de routage opportuniste décrits dans le paragraphe précédent reposent sur la régularité supposée des schémas de mobilité des terminaux. L'approche proposée dans le routage social se fonde quant à elle sur le fait que la mobilité des terminaux est fonction des interactions sociales ayant lieu entre les transporteurs des terminaux. Les protocoles de cette catégorie reposent sur le fait qu'un lien social représente la force qui lie, par exemple, les membres d'une famille entre eux, ou les membres d'une communauté. Dans ces protocoles, les liens sociaux entre les propriétaires des terminaux mobiles sont placés au cœur du réseau car ils sont supposés jouer un rôle important dans la manière dont se rencontrent ces terminaux. De nombreuses études ont été menées dans ce sens ces dernières années en vue d'améliorer la connaissance sur les réseaux sociaux mobiles [HCS⁺05, MSN05, DH07a, CHC⁺07, HYCC09, YGC09, SSL10].

Dans [HC07b], Hui *et al.* proposent d'attribuer à chaque terminal mobile une étiquette indiquant son appartenance à une certaine communauté sociale. Lorsqu'un terminal envoie un message, ce message se voit également attribuer une étiquette indiquant à quelle communauté appartient son destinataire. Le message est alors relayé par l'ensemble des terminaux mobiles faisant partie de la communauté du destinataire. Les mêmes auteurs ont ensuite étudié un protocole nommé Bubble Rap [HC07a, HCY08] dans lequel les communautés sont identifiées automatiquement à l'aide d'un algorithme distribué s'appuyant sur des historiques de contacts. De la même manière que dans le protocole précédent, l'acheminement d'un message est réalisé en utilisant comme porteurs l'ensemble des terminaux appartenant à la même communauté que le terminal destinataire. En outre, si de tels terminaux ne sont pas rencontrés, Bubble Rap offre une alternative. Elle consiste à relayer le message vers un ou plusieurs terminaux ayant des « rôles centraux » dans le réseau social, c'est-à-dire les terminaux mobiles ayant les plus grands

degrés de connectivité et donc ceux qui sont supposés être les plus à même de jouer le rôle d'intermédiaire.

SimBet Routing [DH07b] exploite aussi le rôle central de certains terminaux du réseau social pour acheminer les messages. Dans ce protocole, l'acheminement est réalisé en deux phases. D'abord un message est envoyé vers un terminal jouant un rôle central, dans le but de maximiser les chances de trouver à partir de cet intermédiaire un bon relais du message. Dans SimBet un bon relais est un terminal ayant une similarité sociale avec la destination. Cette similarité est évaluée grâce à un historique de contacts entre terminaux, d'une manière proche de celle employée dans MaxProp [BGJL06].

Les protocoles de routage mentionnés précédemment proposent d'exploiter les structures sociales formées par les terminaux pour acheminer les messages jusqu'à leurs destinataires. D'autres protocoles de cette famille, présentés brièvement ci-dessous, exploitent non seulement ces structures mais aussi des informations contextuelles caractérisant la destination.

Dans [MHMC08], Musolesi *et al.* proposent de modifier la fonction d'utilité du protocole CAR [MHM05] de sorte qu'elle prenne en compte l'appartenance à une communauté sociale dans l'estimation de la probabilité de remise. En plus d'exploiter des historiques d'informations, ce protocole exploite donc l'appartenance à une communauté déclarée par son propriétaire pour guider le processus d'acheminement, qui se rapproche alors des travaux de Hui et al. [HC07a, HCY08].

Le protocole de routage HiBop [BCJP07, BCP08b] utilise des informations caractérisant socialement le propriétaire d'un terminal. Par exemple l'adresse de sa résidence, son lieu de travail, son nom, sa profession, etc. sont autant d'informations censées décrire le « profil social » d'un terminal (ou plutôt celui de son propriétaire). Lors des contacts entre terminaux, ces informations sont échangées. Ainsi, chaque terminal est en mesure de bâtir son « contexte social » en collectant et en conservant un historique de contacts avec d'autres terminaux et leurs profils. Chaque fois qu'un message est injecté dans le réseau, l'émetteur lui ajoute des méta-informations caractérisant le destinataire. Ces méta-informations sont ensuite utilisées pour calculer la similarité d'un terminal rencontré avec le terminal destinataire. Si cette similarité est élevée, c'est-à-dire que le terminal appartient à la même communauté sociale (profil similaire) que le destinataire, alors le terminal rencontré est sélectionné comme porteur d'une copie du message. Dans HiBop, à la différence des protocoles de routage social précédemment évoqués, seul le terminal émetteur décide de confier une nouvelle copie du message initial à un porteur, et ce tant que la somme des probabilités de remise des terminaux mobiles porteurs d'une copie est inférieure à une valeur seuil fixée par avance. Dans ce sens HiBop ressemble au protocole Spray and Wait, à la différence que durant la phase Spray les terminaux sont sélectionnés en fonction de leur similarité avec la destination.

Propicam [NGP07], comme HiBop, exploite le contexte d'utilisation d'un terminal et des historiques pour déterminer la probabilité de remise d'un message. Il exploite, comme HiBop, des routes composées d'un seul terminal relais sélectionné en fonction de sa similarité avec la destination. La différence entre Propicam et HiBop réside dans la manière de sélectionner les bons porteurs. Dans Propicam, lorsqu'un terminal souhaite envoyer un message il envoie à l'ensemble de ses voisins à deux sauts des informations caractérisant de son point de vue

la destination. Sur la base de ces informations, les terminaux voisins calculent et retournent leur probabilité de remise pour le destinataire donné. L'émetteur sélectionne alors parmi ses voisins ceux ayant les métriques les plus élevées, et envoie à chacun une copie du message. Il est important de noter que cet étape de sélection des bons porteurs suppose une stabilité locale du réseau.

1.3.3 BILAN

De manière générale, on peut observer que les protocoles dérivés du modèle épidémique présentent l'inconvénient de mobiliser beaucoup de ressources (terminaux transporteurs, mémoire, bande passante). Ce constat est particulièrement critique lorsqu'il s'agit d'acheminer chaque message vers un destinataire unique, le modèle épidémique étant en revanche mieux adapté à la diffusion de messages dans l'ensemble du réseau. On peut toutefois noter que ces mêmes protocoles présentent en général l'avantage d'être immédiatement opérationnels dans un réseau déployé pour une courte durée dans la mesure où ils ne nécessitent pas de phase « d'apprentissage » des propriétés du réseau. Les protocoles exploitant des informations contextuelles nécessitent en effet, pour être pleinement efficaces, que les terminaux soient en mesure d'analyser en continu des informations leur permettant de percevoir l'état global du réseau. Chaque terminal doit alors maintenir un historique des terminaux qu'il a rencontrés, et exploiter cet historique pour « prédire » les contacts futurs avec ces mêmes terminaux. Une telle approche repose sur une hypothèse forte de récurrence des contacts entre terminaux mobiles, et sur une certaine forme de stabilité du réseau. Dans les approches « sociales », cette récurrence est elle-même censée résulter des relations sociales liant les propriétaires des terminaux. On peut noter en outre qu'une approche « sociale » n'est bien sûr pas applicable dans des réseaux dont les terminaux ne sont pas transportés par des utilisateurs humains.

Avec de telles approches, on peut non seulement se demander comment un terminal s'insérant brièvement dans un réseau existant est considéré par les autres terminaux, mais aussi s'interroger sur le temps nécessaire à la prise en compte du départ ou de l'arrivée d'un terminal par les autres terminaux du réseau. D'autre part, le passage à l'échelle peut être problématique puisque chaque terminal est censé engranger et traiter une grande quantité d'information concernant tous les autres terminaux du réseau. Enfin, se pose le problème d'amorçage (*bootstrapping*) puisque, pour être en mesure de guider des messages vers leur destinataire les heuristiques utilisés par ces approches s'appuient sur des informations passées collectées par les terminaux.

Les paragraphes précédents ont été consacrés à l'acheminement de messages en fonction d'une destination visée. Dans le travail présenté dans ce mémoire nous nous intéressons plus particulièrement au modèle de communication basée contenus, qui propose non pas de « router » les messages en fonction de la destination qu'ils sont censés atteindre mais en fonction de leur contenu. Dans le paragraphe suivant nous présentons les travaux réalisés par d'autres afin de supporter la communication basée contenus, en distinguant les travaux visant les réseaux filaires (type Internet) de ceux visant les réseaux mobiles ad hoc (connexes ou discontinus).

1.4 COMMUNICATION BASÉE CONTENUS

Dans le modèle de communication basée contenus, chaque unité d'information injectée dans le réseau (paquet, événement, message, document, etc.) est censée atteindre l'ensemble des récepteurs intéressés, plutôt que des destinataires spécifiquement désignés par l'émetteur [CW01]. Dans un réseau mettant en œuvre ce mode de communication, l'information circule donc en fonction de l'intérêt que les terminaux du réseau y portent, plutôt que vers une destination bien établie.

Ce modèle de communication, bien qu'atypique, répond parfaitement aux besoins des applications de partage d'information, d'annonce, de découverte et de fourniture de services. Plus généralement, il répond aux besoins des applications distribuées nécessitant un modèle de communication de type publication-abonnement [PFGK03] (*publish-subscribe*), que nous décrivons ci-dessous. De nombreuses applications destinées à fonctionner dans des MANETs discontinus peuvent ainsi être conçues sur la base du modèle de communication pub-sub. Des exemples de telles applications sont brièvement présentés dans le paragraphe 1.4.3.

1.4.1 MODÈLE PUBLICATION-ABONNEMENT

Dans le modèle de communication par publication-abonnement (*publish-subscribe*) chaque abonné (*subscriber*) déclare ses intérêts sous forme de souscriptions (*subscriptions*). Ces souscriptions lui permettent de recevoir de manière asynchrone tous les événements (ou autres types d'unités d'informations) publiés par des éditeurs (*publishers*) qui correspondent à ses intérêts [PFGK03]. Ce modèle est un élément clé pour la dissémination d'événements dans les applications réparties. En effet, il offre un fort découplage entre les éditeurs et les abonnés en termes de :

- *temps* : les éditeurs et les abonnés n'ont nul besoin d'être simultanément présents et actifs dans le réseau pour pouvoir respectivement publier et recevoir des événements.
- *espace de nommage* : les éditeurs et les abonnés n'ont pas besoin de se connaître mutuellement. En effet, lors de la publication un éditeur ne désigne pas de destinataire(s) particulier(s). Réciproquement, lorsqu'un abonné souscrit auprès du système, il ne désigne pas spécifiquement d'éditeur(s). Les seuls éléments liant les éditeurs et les abonnés entre eux sont les événements eux-mêmes.
- *synchronisation* : les systèmes reposant sur le modèle *pub-sub* sont intrinsèquement asynchrones, les opérations de publication, de souscription et de réception d'événement n'étant pas bloquantes.

Ce fort découplage entre les éditeurs et les abonnés rend ce modèle de communication très adapté aux caractéristiques des réseaux mobiles ad hoc, et en particulier des MANETs discontinus. Le découplage temporel et l'asynchronisme du modèle de communication *pub-sub* permettent en effet de tolérer la connectivité intermittente, ainsi que la latence dans les transmissions. Le découplage dans l'espace de nommage permet en outre d'assurer les communications

dans des réseaux « ouverts » dans lesquels tous les terminaux ne se connaissent pas nécessairement les uns les autres, et dans lesquels le nombre de ces terminaux peut varier au fil du temps.

1.4.1.1 MODÈLES DE SOUSCRIPTION

Un système *pub-sub* doit fournir des opérations de base permettant aux éditeurs de publier des événements, et aux abonnés d'enregistrer ou supprimer leurs souscriptions pour des types d'événements spécifiques. Il existe différents modèles de souscription qui permettent aux abonnés de définir de façon plus ou moins précise leurs centres d'intérêt, de sorte qu'un abonné ne reçoive ensuite que les événements (ou unités d'information) qui l'intéressent.

Topic-based model. Un abonné déclare son intérêt pour un sujet (*topic*) particulier et reçoit ensuite les événements publiés concernant ce sujet. Une limitation de ce modèle de souscription est son manque d'expressivité. L'abonné d'un sujet reçoit l'ensemble des événements publiés bien qu'il puisse, en fait, n'être intéressé que par un sous-ensemble des événements reçus. Des solutions ont été envisagées pour résoudre partiellement ce problème. Par exemple, dans le système de discussion thématique *Usenet*, les groupes de discussion (*newsgroups*) sont organisés hiérarchiquement.

Content-based model. Un abonné déclare son intérêt en définissant des conditions sur le contenu des événements qu'il souhaite recevoir. La souscription est définie comme un filtre qui spécifie des contraintes portant sur le contenu même d'un événement. À la différence du modèle *topic-based* les événements n'appartiennent pas à un sujet particulier, le filtrage des événements est réalisé selon leur contenu. Ce modèle permet donc à un terminal de définir de manière très précise ce qui l'intéresse, et de recevoir uniquement des événements l'intéressant. En théorie tout type d'information caractérisant le contenu des événements peut être utilisé pour en assurer le filtrage. Pour des raisons pratiques, cependant, la plupart des systèmes mettant en œuvre ce modèle se contentent de caractériser le contenu d'un événement par des couples clés-valeurs, le filtrage reposant alors sur des combinaisons de conditions portant sur ces clés (comme par exemple dans Gryphon [SBC⁺98], Siena [CRW00], et Jedi [CDNFC98]).

Nous présentons dans les paragraphes suivants l'architecture générale des systèmes *pub-sub*, et quelques-unes des méthodes d'acheminement des événements entre éditeurs et abonnés.

1.4.2 ARCHITECTURE GÉNÉRALE DES SYSTÈMES DE COMMUNICATION PAR ABONNEMENT

Un système *pub-sub* est composé d'un ensemble de terminaux distribués sur un réseau de communication. Tout terminal participant au système se distingue par le rôle qu'il joue dans celui-ci :

- d'un côté les **éditeurs** produisent de l'information,

- de l'autre les **abonnés** consomment l'information produite par les éditeurs en fonction de leurs intérêts respectifs.

Les interactions entre éditeurs et abonnés sont gérées par le système distribué mettant en œuvre le modèle *pub-sub*. De manière générale, un ensemble de participants se coordonnent afin d'assurer l'acheminement de chaque événement publié vers chaque terminal intéressé. La communication basée contenus entre participants est donc assurée par le système *pub-sub*. Un tel système peut être décomposé en deux « couches », parfois confondues, de fonctionnalités différentes :

- une couche qui met en œuvre un **réseau de couverture** (*overlay*) dans le but d'assurer l'organisation des participants du système distribué (e.g. réseau de couverture assuré par des serveurs dédiés, réseau de couverture pair-à-pair structuré, réseau de couverture pair-à-pair non-structuré, etc.)
- une couche qui réalise le **acheminement des événements** en exploitant l'*overlay* avec pour principale fonctionnalité l'acheminement des événements des participants éditeurs vers les participants abonnés. Cette couche exploite éventuellement des caractéristiques du réseau de couverture.

1.4.2.1 RÉSEAUX DE COUVERTURE

Courtiers. Les réseaux de couverture peuvent être de différentes natures en fonction des hypothèses de travail considérées. Dans les réseaux stables de grande taille, typiquement dans Internet, les systèmes pub-sub sont en général mis en œuvre en exploitant des serveurs dédiés ou courtiers (*brokers*). Les courtiers sont connectés entre eux pour former un réseau de couverture (*overlay*) et exploitent pour ce faire les protocoles réseaux de la pile Internet. Les participants accèdent au système en se connectant à un courtier, enregistrent leurs souscriptions afin de recevoir les événements les intéressant, ou publient des événements à l'intention des abonnés. Un réseau de couverture de ce type peut reposer sur un seul et unique courtier (approche centralisée), ou sur plusieurs (approche distribuée). De tels réseaux de couverture sont maintenus par des administrateurs, et leur topologie est la plupart du temps statique (sauf lors de l'ajout ou de la maintenance d'un serveur). Des exemples de tels systèmes pub-sub sont Gryphon [SBC⁺98], Siena [CRW00], et Jedi [CDNFC98]. Dans les MANETs discontinus, cette approche n'est pas envisageable, car aucun terminal ne peut être considéré comme suffisamment stable et accessible pour assurer le rôle de courtier.

Pair-à-pair structuré. L'approche « réseau de couverture pair-à-pair structuré » ajoute à l'utilisation de courtiers la dimension d'auto-organisation du système (pas d'administration par l'homme) et la tolérance au *churn*, c'est-à-dire à l'arrivée et au départ incessants de participants dans le système. Dans cette approche, les participants s'auto-organisent et maintiennent un graphe structuré au dessus d'un espace virtuel d'adressage des événements (CAN ou *Content Adressable Network*). Chord [SMLN⁺03] et Pastry [RD01] mettent par exemple en œuvre des tables de hachage distribuées (DHT ou *Distributed Hash Tables*). Par ailleurs, des exemples de systèmes pub-sub exploitant des espaces d'adressage virtuel sont Scribe [CDKR02], et Hermes [PB02].

Dans les MANETs discontinus, de telles approches sont difficilement applicables, la forte dynamique du réseau rendant l'établissement, le maintien et l'utilisation d'un réseau de couverture structuré difficile voire impossible.

Pair-à-pair non-structuré. L'approche «réseau de couverture pair-à-pair non-structuré» consiste à bâtir des réseaux de faible envergure (ou *clusters*), organisés entre eux à l'échelle du réseau global. Ces petites structures permettent d'optimiser les communications entre les participants. Cette approche tolère assez bien une topologie fluctuante et peut donc être appliquée dans des réseaux mobiles. Différentes techniques sont utilisées pour le routage des événements dans ce type de réseau de couverture. Généralement, ces techniques se fondent sur les principes de l'inondation ou de *gossiping* (présenté dans le paragraphe suivant) car il est difficile de maintenir des structures permettant le routage des événements dans des environnements très dynamiques tels que les MANETs. Des exemples de systèmes pub-sub exploitant des réseaux de couverture pair-à-pair non structurés sont *TERA* [BBQ⁺07], *SUB-2-SUB* [VRKS06], et *SpiderCast* [CMTV07].

1.4.2.2 ACHÉMINEMENT DES ÉVÉNEMENTS DANS LES RESEAUX STATIQUES OU QUASI STATIQUES

L'acheminement des événements constitue la tâche la plus importante à remplir par un système pub-sub. Il existe différentes approches permettant de réaliser ce routage.

Acheminement par inondation. La façon la plus simple de réaliser l'acheminement des événements consiste à « inonder » le réseau des événements publiés par les éditeurs, et à laisser les abonnés filtrer ces événements en fonction de leurs propres souscriptions en ne retenant que les événements qui les intéressent. Cette approche introduit toutefois un surcoût élevé car tous les participants du réseau reçoivent la totalité des événements publiés, même s'ils n'y portent aucun intérêt. Pour réduire ce surcoût, l'approche inverse peut être adoptée. Elle consiste à inonder le réseau des souscriptions associées aux identités (adresses topologiques) des participants, afin que chaque éditeur connaisse l'ensemble des abonnés potentiellement intéressés par les événements qu'il publie. De la sorte, les événements sont directement filtrés par leurs producteurs, qui envoient alors chaque événement uniquement aux abonnés intéressés. Même si cette approche permet de réduire le coût lié à l'inondation des événements, elle est difficilement applicable dans des systèmes dans lesquels les souscriptions ou les participants évoluent constamment et rapidement [CRW01].

Ces deux méthodes de routage introduisent un surcoût non négligeable, et se prêtent donc mal à un passage à l'échelle. Des approches s'appuyant sur un sous-ensemble de participants ont donc été développées afin de gérer de façon plus fine le routage des événements.

Acheminement par filtrage. Dans l'acheminement par filtrage des événements ces derniers sont acheminés uniquement vers les abonnés intéressés. Généralement, cette approche est exploitée dans les systèmes reposant sur des courtiers ou des réseaux de couverture pair-à-pair

structurés Siena [CRW00] et Rebeca [FGKZ03]. Pour déterminer les chemins permettant la remise des événements, chaque participant doit stocker des informations concernant toutes les souscriptions de ses voisins dans le réseau de couverture. Cependant, à la différence de ce qui se passe dans l'approche par inondation des souscriptions, un participant ne communique directement qu'avec ses voisins directs, ce qui réduit le surcoût dû à la mise à jour des souscriptions. La connaissance des souscriptions permet, lors de la publication d'un événement, de l'acheminer uniquement vers les abonnés intéressés par son contenu.

Acheminement par rendez-vous. L'acheminement par rendez-vous est réalisé en deux phases : la recherche d'un abonné (dans l'espace virtuel d'adressage ou CAN puis la communication directe avec cet abonné. Dans cette approche, l'adresse topologique courante d'un participant est stockée par un autre participant qui joue le rôle de point de rendez-vous (ou ancre). Cette approche est utilisée dans les systèmes pub-sub exploitant des réseaux de couverture pair-à-pair structurés. Des exemples de systèmes bâtis sur ce modèle sont Scribe [CDKR02] et Hermes [PB02].

L'acheminement déterministe (par filtrage ou par rendez-vous) ne garantit pas la remise d'un événement à tous les abonnés. La mise à jour d'une structure de routage implique en effet des délais durant lesquels l'acheminement des événements peut être imparfait. Certains événements peuvent alors être acheminés vers des abonnés qui ne sont plus intéressés, ou ne pas atteindre de nouveaux abonnés car leurs souscriptions n'ont pas encore été prises en compte. En outre, le *churn* rend beaucoup plus prononcé le décalage entre l'acheminement des événements à un moment donné et celui qui permettrait un acheminement déterministe idéal des événements. Cette caractéristique, associée au changement dynamique de souscriptions, rend les protocoles d'acheminement déterministes peu efficaces pour la livraison des événements dans des réseaux dynamiques tels que les MANETs. Les protocoles reposant sur le principe du *gossiping* ont donc émergé comme des approches alternatives tolérant ces contraintes.

Acheminement par « gossiping ». Les approches d'acheminement des événements se fondant sur le principe du *gossiping* reposent sur des méthodes probabilistes ou pseudo-probabilistes [HHL88, HHL02, SCS02]. Les participants relaient les événements vers d'autres participants désignés au hasard. Il n'est donc pas nécessaire de construire et de maintenir des structures pour le routage des événements.

Dans certains protocoles la sélection des participants vers lesquels un événement est relayé s'appuie sur la connaissance des souscriptions des participants voisins. Conformément au principe du *gossiping*, les terminaux voisins s'échangent constamment des informations sur leurs souscriptions respectives. Grâce à ces informations, les participants sont en mesure de construire une structure de routage déterministe. Ainsi, Costa *et al.* [CP05] proposent une approche qui combine routage déterministe et probabiliste des événements. Chaque participant propage ses souscriptions dans son voisinage, et informe donc ses voisins des types d'événements qui l'intéressent. Un participant recevant un événement est alors en mesure de décider vers quels voisins il doit le relayer. Si un participant ne possède pas suffisamment d'information pour faire ce

choix, alors l'événement est relayé vers quelques participants choisis au hasard dans son voisinage. Des approches similaires sont proposées dans [VRKS06, BBQ⁺07, CMTV07]. Ces diverses approches nécessitent de la connectivité de bout en bout entre éditeurs et abonnés, et ne peuvent donc être utilisées que dans des réseaux connexes.

1.4.2.3 ACHÉMINEMENT DES ÉVÉNEMENTS DANS LES RÉSEAUX MOBILES AD HOC

Les méthodes d'acheminement des événements destinés à fonctionner dans les MANETs peuvent exploiter soit des transmissions par diffusion [BBQ⁺05] (en construisant le cas échéant des arbres de diffusion [PCM03, HGM03]), soit des protocoles de routage *multicast* dynamique [YB04]. Les approches les plus étudiées reposent sur les principes de l'inondation ou du *gossiping*, et sur des échanges par diffusion entre terminaux mobiles voisins.

Dans [BBC⁺05], l'acheminement des événements exploite une forme d'inondation contrôlée dans laquelle les événements sont routés en fonction de la « distance » séparant deux participants. Chaque terminal diffuse périodiquement un message de présence qui contient la liste de ses souscriptions. La réception de tels messages permet à chaque terminal mobile de connaître les intérêts de ses voisins et de construire (et maintenir) une table de souscriptions. La distance entre terminaux est estimée en mesurant la fréquence des annonces reçues des voisins, cette distance augmentant en cas de non réception des annonces de la part d'un voisin connu. Lors de la réception d'un événement, un terminal vérifie si une entrée de la table de souscriptions correspond. Si c'est le cas, alors le terminal diffuse cet événement après un délai proportionnel à la distance qui le sépare du terminal sélectionné. Si, par ailleurs, un participant voisin du terminal émetteur « entend » la réémission de l'événement, alors il s'abstient de le rediffuser lui-même. De la sorte, les événements se disséminent rapidement vers l'ensemble des terminaux intéressés, la transmission par diffusion limitant dans le même temps les émissions dupliquées.

Tout comme les protocoles de routage dynamique conçus pour les MANETs présentés dans le paragraphe 1.2.2, les méthodes d'acheminement d'événements destinés aux MANETs nécessitent que des chemins de bout en bout soient disponibles à tout instant entre éditeurs et abonnés, ou en d'autres termes que le réseau soit connexe à tout instant. Les protocoles de ce type ne sauraient donc fonctionner de manière satisfaisante dans des MANETs discontinus.

1.4.3 COMMUNICATION BASÉE CONTENUS DANS LES RÉSEAUX MOBILES AD HOC DISCONTINUS

Nous nous intéressons à l'acheminement d'information basée contenus dans des MANETs discontinus, dont une caractéristique majeure est la fragmentation du réseau en îlots de connectivité. Dans de telles conditions, les systèmes proposés pour les MANETs connexes sont inadaptés. En effet, la fragmentation du réseau en îlots se traduit par une impossibilité d'acheminer un événement entre des îlots distincts.

Pour assurer la propagation des événements dans l'ensemble des îlots « déconnectés » formant le réseau, on peut s'inspirer des protocoles de routage *unicast* destinés aux MANETs discontinus en permettant aux terminaux de stocker temporairement certains événements (ou messages) conformément au principe *store, carry and forward* présenté dans le paragraphe 1.3.2.1.

De la sorte, un événement peut être transporté par un terminal mobile d'un îlot à l'autre, et être relayé plus tard vers d'autres terminaux intéressés. La démarche s'apparente donc à celle présentée dans le paragraphe 1.3.2.4, si ce n'est que l'objectif est ici d'atteindre tous les terminaux intéressés plutôt qu'un ensemble de destinataires bien identifiés. Les approches proposées jusqu'à ce jour dans cette optique dans la littérature peuvent être classées en deux grandes familles :

- celles s'appuyant sur le principe du *gossiping*,
- celles s'appuyant sur l'analyse du réseau mobile ad hoc discontinu, vu comme un réseau social mobile.

1.4.3.1 ACHEMINEMENT ÉPIDÉMIQUE (« GOSSIPING »)

L'acheminement par *gossiping* repose pour l'essentiel sur des échanges entre terminaux voisins et ne nécessite pas de bâtir de structure de routage englobant l'ensemble du réseau. Il se satisfait fort bien d'une connectivité partielle entre les terminaux, et peut aisément bénéficier du « brassage » de l'information résultant du transport de messages par des terminaux mobiles.

[DQA04] définit un algorithme dit d'*Autonomous Gossiping* (A/G), permettant à des terminaux voisins de s'échanger des messages de façon opportuniste en fonction de leurs centres d'intérêt respectifs, et au gré de leurs rencontres. Dans l'algorithme A/G, le processus de dissémination de l'information est assimilé à un processus de dissémination épidémique qui n'est d'ailleurs pas sans rappeler le modèle du routage épidémique [VB00] : chaque terminal est perçu comme étant plus ou moins susceptible d'être « infecté » par certains types d'information.

Dans [LLS⁺06], Leguay *et al.* proposent aussi d'exploiter le modèle de dissémination épidémique pour distribuer des journaux électroniques. Cependant, les terminaux ne sont pas en mesure de produire et publier eux-mêmes de l'information : ils contribuent uniquement à la dissémination des journaux. Des terminaux dédiés (courtiers), *a priori* reliés à Internet, font office de sources d'informations (kiosques) auprès desquelles des terminaux mobiles peuvent se procurer les journaux en question. Les journaux sont ensuite relayés de proche en proche lorsque les terminaux entrent en contact les uns avec les autres.

PodNet [LKM07, MLKW07] est une application de « *podcasting* sans fils » permettant à des utilisateurs de terminaux mobiles d'échanger de petits fichiers audio ou vidéo. Chaque utilisateur peut inscrire son propre terminal à un certain nombre de « canaux » thématiques, dans lesquels il lui sera ensuite possible de publier des contenus. La dissémination des contenus publiés dans un canal est réalisée par l'ensemble des terminaux abonnés à ce canal. Le Brun *et al.* proposent un système assez similaire baptisé NOOS [JCNSJ07], qui permet la dissémination d'informations thématiques (flux de syndication) dans des MANETs discontinus.

[CMMP06] décrit une approche exploitant des informations contextuelles afin d'acheminer l'information, qui repose sur le protocole de routage semi-probabiliste présenté dans [CP05]. À la différence des protocoles précédents, celui-ci exploite les informations contextuelles dans le but d'identifier, autour d'un terminal, les voisins intéressés, et, parmi ceux-ci, les bons transporteurs. Dans cette approche, les souscriptions des terminaux sont propagées à un horizon h de chaque terminal (h étant défini en nombre de sauts), de sorte qu'une structure déterministe pour le routage des messages en fonction de leur contenu peut être construite et maintenue autour de chaque terminal. En plus de propager dans son voisinage la liste de ses souscriptions,

un terminal ajoute à cette liste des informations relatives à son contexte (par exemple mobilité, co-location avec des terminaux ayant des intérêts communs, énergie restante, etc.). Les informations caractérisant chaque terminal (souscriptions et contexte) sont exploitées via une « fonction d'utilité » similaire à celle développée dans CAR [MHM05]. Cette fonction d'utilité est censée permettre de déterminer dans le voisinage d'un terminal quels sont les voisins intéressés par un message donné, et quels transporteurs mobiles vont aider à propager le message vers d'autres îlots du réseau. Lorsque cette fonction d'utilité ne permet pas de sélectionner les transporteurs de manière déterministe, une sélection probabiliste est réalisée.

1.4.3.2 ACHÈMINEMENT EXPLOITANT LES CARACTÉRISTIQUES SOCIALES DES TERMINAUX

Certains auteurs se focalisent sur l'étude de stratégies d'acheminement basées contenus entre des terminaux transportés par des individus (et non par d'autres types de transporteurs, tels que véhicules, capteurs mobiles, animaux, etc.). L'idée consiste alors à essayer d'exploiter les caractéristiques des relations sociales entre ces individus afin de guider le processus d'acheminement entre éditeurs et abonnés.

ContentPlace [BCP08a] propose une approche similaire à celle développée dans PodNet, bien que le champ applicatif visé soit plus large (partage de petits fichiers audio ou vidéo, publicité, mise à jour de logiciels, etc). Les informations sont publiées dans des « canaux » thématiques auxquels les utilisateurs peuvent s'abonner. Le processus de dissémination de l'information dans ContentPlace est similaire à celui proposé dans PodNet. Cependant, ContentPlace tente d'améliorer les performances de ce processus en confiant des copies aux terminaux mobiles (intéressés ou non) susceptibles de rencontrer de nombreux terminaux d'utilisateurs abonnés. Pour ce faire, ContentPlace exploite des informations collectées et échangées par les terminaux pour analyser le réseau social formé par les utilisateurs et leurs centres d'intérêt. Grâce à cette analyse, ContentPlace est en mesure d'identifier les terminaux mobiles jouant un rôle central dans une communauté d'utilisateurs abonnés à un sujet donné.

[YHCC07] est un système *pub-sub* qui exploite le réseau « social » formé par les terminaux mobiles pour bâtir un réseau de couverture formé de terminaux jouant le rôle de courtiers entre les éditeurs et les abonnés. Ce système repose sur un algorithme distribué qui réalise une analyse des historiques de contacts entre les terminaux pour déterminer le réseau social formé par les terminaux des utilisateurs nomades. En particulier, cette analyse permet de détecter les communautés de terminaux, et les terminaux occupant une place centrale dans chacune des communautés. Les « terminaux centraux » se voient alors attribuer le rôle de courtiers. Ils sont connus de l'ensemble des membres de la communauté, et ont connaissance des identités des courtiers élus dans les autres communautés. Un terminal courtier est responsable de la dissémination des messages dans sa propre communauté. Lorsqu'un éditeur souhaite publier un message, celui-ci est envoyé au courtier qui le relaie vers les courtiers des autres communautés. En fonction des souscriptions réalisées par les utilisateurs de sa communauté, chaque courtier décide si le message doit également être disséminé dans sa communauté. L'originalité de ce travail réside dans l'approche proposée pour détecter les communautés dans les environnements mobiles (algorithmes de *clustering*). Cependant, on peut se demander si ce système peut passer à l'échelle. Les terminaux jouant le rôle de courtiers sont en effet des éléments critiques du

réseau de couverture. D'une part, ils doivent enregistrer énormément d'information sur les terminaux de leur communauté, et, d'autre part, ils doivent assurer la dissémination des messages dans leur communauté. Ils doivent en outre être constamment disponibles dans la mesure où aucune communication entre éditeurs et abonnés n'est possible en leur absence.

[CMMP08] décrit également un protocole dédié au *pub-sub*. Ce protocole est dérivé du protocole de routage *unicast* présenté dans [MHM05], mais il peut prendre en compte les centres d'intérêt (souscriptions) des utilisateurs. Il utilise un système de prédiction basé sur une métrique d'interaction sociale pour identifier les meilleurs relais mobiles pour chaque message. Dans cette approche, l'hypothèse forte sous-jacente est que chaque utilisateur a tendance à rencontrer plus fréquemment des utilisateurs ayant les mêmes centres d'intérêt que les siens. L'algorithme de routage exploite donc cette propriété pour sélectionner, en guise de porteurs pour un certain message, des terminaux mobiles qui sont fréquemment entrés en contact avec des terminaux intéressés par ce type de message dans le passé.

[MMC09] propose une approche qui s'appuie sur la même hypothèse. Toutefois, le processus de routage des messages proposé est différent dans la mesure où chaque utilisateur peut s'abonner directement auprès d'autres utilisateurs afin de recevoir les informations qu'ils publient (de la même manière que dans les sites de réseaux sociaux en ligne tels que Facebook, YouTube, etc.). L'idée de base de ce système est de construire un réseau social entre les producteurs d'information et leurs abonnés de façon à ce que, lorsqu'un utilisateur publie du contenu, celui-ci soit acheminé vers les utilisateurs intéressés. L'acheminement de l'information d'un producteur vers ses abonnés est réalisé le long de chemins s'appuyant uniquement sur les terminaux d'utilisateurs intéressés. Pour ce faire, le producteur d'un message décrit sous forme d'arbre l'ensemble des terminaux devant transporter et relayer l'information vers ses abonnés, cet arbre reproduisant les chaînes de souscriptions entre abonnés et producteur.

1.4.4 BILAN

Dans les paragraphes précédents nous avons dressé un panorama des protocoles d'acheminement développés en vue du support de la communication basée contenu. Certains d'entre eux reposent sur le principe du *gossiping*, et proposent des solutions s'apparentant au routage épidémique. Comme nous l'avons montré, de telles approches ne nécessitent pas d'apprentissage des propriétés du réseau et présentent donc l'avantage d'être immédiatement opérationnelles. De plus, il est possible de réduire le surcoût lié à la dissémination des messages, puisque cette dissémination peut ne reposer que sur des terminaux mobiles intéressés par les messages qu'ils transportent. Il faut toutefois noter que les solutions reposant sur ce modèle et proposées jusqu'à ce jour présentent quelques limitations. Il semble en effet que certaines n'ont jamais été mises en pratique, et que d'autres sont des applications spécifiques dédiées à la distribution thématique de petits fichiers vidéo, audio, etc.

D'autres solutions tentent d'améliorer les performances de l'acheminement des messages des éditeurs vers les abonnés en sélectionnant les meilleurs porteurs pour ces messages. La démarche s'apparente alors à celle développée dans le cadre de l'acheminement de message vers une destination donnée, bien que l'objectif soit ici d'atteindre l'ensemble des terminaux intéressés. De telles solutions présentent alors les mêmes inconvénients que celles développées pour

l'acheminement en fonction d'une destination (nécessité de stabilité du réseau, phase d'apprentissage, *bootstrapping*, passage à l'échelle, état global). De plus, dans certaines de ces méthodes, certains terminaux mobiles assurant un rôle central dans la dissémination des messages doivent engranger énormément d'information concernant les autres terminaux du réseau. Ces diverses approches reposent sur l'idée que des individus ayant des centres d'intérêt communs ont tendance à se rencontrer fréquemment. C'est par exemple le cas lorsque ces personnes sont des collègues de travail, des étudiants inscrits dans un même parcours de formation, ou bien encore des membres d'une même famille, d'un même club de sport, d'un même club associatif, etc. Dans certains cas, le fait que des individus affichent les mêmes centres d'intérêt n'implique pourtant aucunement qu'ils appartiennent à une même communauté. Par exemple, des individus souhaitant se tenir informés des prévisions météorologiques et des résultats sportifs ont certes des centres d'intérêts similaires, mais ceci n'implique pas qu'ils entrent fréquemment en contact les uns avec les autres. Une certaine similarité entre les profils d'intérêt des individus signifie donc qu'ils peuvent partager des informations si l'occasion se présente, mais ceci ne signifie pas forcément qu'ils présentent des schémas de mobilité ou de co-location particuliers. Dans de telles conditions, il n'est pas évident que des approches basées sur l'analyse d'historiques de contacts, notamment dans le but de découvrir les structures sociales liant les propriétaires de terminaux mobiles, soient très performantes.

1.5 DISCUSSION

Dans le paragraphe 1.2, nous avons vu que de très nombreux protocoles développés au cours des deux dernières décennies sont destinés à assurer le routage dynamique « basé destination » dans des MANETs présentant des propriétés favorables en termes de densité et de répartition géographique des terminaux. Comme nous l'avons ensuite souligné (paragraphe 1.3.1), de tels protocoles ne peuvent en aucun cas assurer seuls l'acheminement de messages dans des MANETs discontinus, qui se caractérisent par l'absence de connectivité de bout en bout et une fragmentation en multiples îlots. Il est cependant envisageable, lorsque la topologie des îlots n'évolue pas trop rapidement, d'utiliser l'un ou l'autre de ces protocoles afin d'assurer le routage multi-sauts au sein de chaque îlot. Des terminaux peuvent ainsi bénéficier de la connectivité fugace qui résulte de leur appartenance temporaire à un même îlot.

Pour rétablir une certaine forme de connectivité entre les îlots d'un MANET discontinu, le principe de la communication opportuniste (paragraphe 1.3.2) est d'exploiter la mobilité des terminaux afin de leur faire transporter les messages d'îlot en îlot. Les travaux menés dans ce domaine ont également porté pour l'essentiel sur le routage basé destination. Certains d'entre eux s'appuient sur un modèle épidémique en multipliant les copies de chaque message afin de maximiser les chances de remise à destination. D'autres s'efforcent au contraire de minimiser le nombre de copies de chaque message en sélectionnant les terminaux mobiles les plus aptes à contribuer de manière efficace à son acheminement. Cette sélection peut être effectuée de manière probabiliste ou en fonction d'informations contextuelles caractérisant l'environnement et le comportement des propriétaires des terminaux (schémas de mobilité, relations sociales, etc.).

À travers la revue de la littérature réalisée dans ce chapitre, nous avons montré que la majorité des travaux conduits dans le domaine des MANETs discontinus cherche à bâtir des systèmes permettant l'acheminement de messages en fonction de leur destination. Or comme expliqué dans le paragraphe 1.4, l'objectif de ce travail de thèse est de supporter la communication basée contenus, un style de communication atypique dans lequel l'acheminement des messages est fonction de leur contenu. Nous avons dressé un panorama des différentes approches développées pour l'organisation des participants (réseau de couverture de types courtiers, pair-à-pair structuré et non structuré) et pour le routage des messages (inondation, filtrage, rendez-vous et *gossiping*). Les solutions conçues pour fonctionner dans des réseaux dynamiques tels que les MANETs reposent majoritairement sur le principe du *gossiping* et sur des échanges par diffusion. Pour assurer le routage des messages ces approches nécessitent que des routes de bout-en-bout entre éditeurs et abonnés existent à tout instant. Autrement dit, de telles approches ne peuvent permettre seules la communication basée contenus dans les MANETs discontinus.

Dans le paragraphe 1.4.3, nous avons vu que l'emprunt du principe d'acheminement *store, carry and forward* aux protocoles de routage *unicast* conçus pour des MANETs discontinus (paragraphe 1.3.2) permet de supporter la communication basée contenus dans ces mêmes réseaux. Les travaux menés dans ce domaine se distinguent notamment par leur façon de réaliser la dissémination des messages à travers le réseau. Certains s'apparentent au routage épidémique et présentent l'avantage d'être immédiatement opérationnels, tandis que d'autres s'appuient sur les caractéristiques sociales des transporteurs des terminaux pour acheminer les messages et nécessitent une phase d'apprentissage. Nous pensons que, bien que des techniques s'appuyant sur l'analyse d'historiques puissent se révéler très efficaces dans des réseaux de petite taille (faible cardinalité de terminaux), il y a également besoin de systèmes capables de fonctionner dans des MANETs discontinus aux propriétés inconnues (réseaux de grande envergure, réseaux déployés pour une courte durée, etc.). Dans la suite de ce document, nous exposons notre proposition et proposons une solution logicielle en vue du support de la communication basée contenu dans de tels MANETs discontinus.

2

MODÈLE DE COMMUNICATION OPPORTUNISTE BASÉE SUR LE CONTENU

Dans ce chapitre, nous proposons un modèle de communication définissant les règles et modalités d'interactions entre les terminaux mobiles communicants d'un réseau mobile ad hoc discontinu. Ce modèle de communication repose sur la combinaison des principes de la communication opportuniste, de la communication basée contenus, et de la communication multi-sauts dans les réseaux mobiles ad hoc, qui sont présentés dans le Chapitre 1.

Dans un premier temps, nous rappelons l'objectif principal de cette étude (paragraphe 2.1). Ensuite, nous évoquons les principaux concepts à partir desquels une vue d'ensemble de notre proposition est dressée dans le paragraphe 2.2. Dans le paragraphe 2.3 nous présentons l'architecture générale de la solution que nous proposons. Puis, nous décrivons en détail les deux couches composant notre protocole de communication dans les paragraphes 2.4 et 2.5. Pour conclure ce chapitre nous revenons sur les points essentiels de notre contribution, et dressons un premier bilan.

2.1 OBJECTIFS

L'objectif principal de cette étude est de concevoir un système mettant en œuvre le modèle de la communication basée contenus dans des MANETs discontinus. Contrairement à ce qui est fait dans la majeure partie des travaux présentés dans l'état de l'art (Chapitre 1), l'objectif principal de ce travail de thèse consiste à concevoir une plate-forme réellement opérationnelle qui puisse certes s'interfacer avec un simulateur de réseau mobile, mais qui puisse aussi être déployée sur de « vrais » équipements mobiles et supporter le développement de véritables services applicatifs.

Avant d'aller plus loin dans la description de notre proposition, il nous semble important de préciser les caractéristiques de notre environnement cible. Le type de MANET discontinu que nous ciblons est constitué de terminaux communicants de type PDA, smart-phones ou ordinateurs portables. Ces terminaux dotés d'interfaces Wi-Fi fonctionnant en mode ad hoc sont transportés par des individus nomades, à propos desquels nous ne faisons aucune hypothèse quant à leurs schémas de mobilité ou de contacts, quant à la présence éventuelle de schémas récurrents dans leur comportement, etc. Par exemple, le réseau considéré peut être un réseau de

secours déployé temporairement suite à une catastrophe naturelle, un réseau militaire tactique dont la durée de vie est celle de la mission ou un réseau déployé dans le cadre d'un événement particulier (par exemple, exposition, manifestation sportive) dans lesquels les comportements des individus ne sont a priori pas réguliers. Dans de telles circonstances, il paraît inutile de maintenir des historiques, quelle qu'en soit la nature, pour guider le processus d'acheminement des messages. Au contraire, il paraît plus adapté d'exploiter de manière opportuniste les contacts entre terminaux afin qu'ils échangent librement des informations. Les ressources disponibles sur les terminaux communicants étant cependant rares, nous avons comme objectif de les exploiter avec frugalité, et en particulier d'être économe dans l'utilisation de la bande passante, du stockage de masse, et de l'énergie. La ressource la plus critique sur un terminal mobile est certainement l'énergie (excepté dans le cas où le terminal peut être alimenté en continu, comme par exemple dans un véhicule). Or, toute technologie de transmission radio contribue à drainer la batterie d'un terminal mobile, en particulier pendant les phases de réception et d'émission de trames radio. Nous nous efforcerons donc de limiter le nombre et le volume des messages nécessaires au fonctionnement de notre système de communication afin de limiter sa consommation. Par mesure d'économie d'énergie, le propriétaire d'un terminal (ou le système d'exploitation de ce terminal) peut l'arrêter ou le mettre en veille, interrompant ainsi le fonctionnement de la carte radio et d'autres éléments consommateurs d'énergie. Nous dirons alors que le terminal est volatile, c'est-à-dire qu'il est tantôt actif, tantôt inactif du point de vue du réseau. Nous souhaitons pouvoir supporter une telle volatilité en la prenant en compte d'emblée dans la définition de notre modèle de communication. Notre système de communication devra être réactif aux différents événements caractéristiques de la volatilité d'un terminal.

2.2 VUE D'ENSEMBLE DE LA PROPOSITION

Notre proposition repose, tout comme certaines autres propositions que nous avons évoquées dans l'état de l'art (paragraphe 1.4.3), sur les principes combinés de la communication opportuniste et de la communication basée contenus.

2.2.1 ACHEMINEMENT STORE, CARRY AND FORWARD

Le modèle d'acheminement retenu est donc le modèle *store, carry and forward* qui suppose la mise à disposition par les terminaux mobiles d'un espace de stockage dans lequel est mis en œuvre un cache. Dans nos travaux, nous ne faisons aucune hypothèse sur la capacité de stockage de chaque terminal. En revanche, il est admis que cette capacité est a priori limitée, et qu'elle peut changer d'un terminal à un autre. Nous verrons par la suite que chaque terminal applique une politique de gestion de son propre cache, et que celle-ci peut varier d'un terminal à un autre en fonction de différents critères.

2.2.2 SÉLECTIVITÉ DES TERMINAUX MOBILES

La communication basée contenus suppose que notre système offre aux services applicatifs qui vont en bénéficier un langage de souscription (paragraphe 1.4.1) leur permettant de spé-

cifier clairement le type d'information qu'ils souhaitent recevoir. Le langage de souscription que nous avons choisi de supporter est décrit dans le paragraphe 2.4.1.2. Dans notre modèle, nous cherchons systématiquement à mettre à profit la sélectivité des terminaux afin d'utiliser au mieux leurs ressources. La sélectivité d'un terminal détermine ce par quoi un terminal est intéressé, c'est-à-dire les types d'informations qu'il va chercher à se procurer lors de contacts avec d'autres terminaux. Lorsqu'un terminal récupère une information auprès d'un voisin, le système de communication met cette information à disposition des services applicatifs locaux intéressés, et en dépose par ailleurs une copie dans son propre cache. Le terminal devient alors un transporteur mobile, et peut ainsi contribuer à propager l'information entre des îlots.

2.2.3 MODULATION DE LA SÉLECTIVITÉ

La sélectivité permet une utilisation frugale des ressources puisqu'elle réduit les échanges entre terminaux, et la quantité d'information hébergée par chaque terminal dans son cache à leurs minimums. Pour autant, la sélectivité des terminaux n'implique pas nécessairement un comportement égoïste de leur part. On peut envisager des politiques d'ajustement de la sélectivité qui soient fonction de différents critères (énergie restante, capacité de stockage restante, etc.). Via de tels ajustements, un large spectre de comportements est envisageable, parmi lesquels quelques comportements particuliers auxquels nous nous sommes intéressés qui sont décrits ci-dessous.

2.2.3.1 COMPORTEMENT ÉGOÏSTE

Un terminal égoïste cherche à se procurer, lors de contacts avec d'autres terminaux, uniquement des informations présentant de l'intérêt pour des services applicatifs locaux. Un terminal égoïste héberge donc dans son cache uniquement des informations qui l'intéressent.

2.2.3.2 COMPORTEMENT ALTRUISTE RÉACTIF

Le comportement altruiste réactif étend le comportement égoïste. Un terminal altruiste réactif accepte d'héberger dans son cache des informations qui a priori n'intéressent aucun des services applicatifs locaux. Lorsqu'il reçoit des informations diffusées dans son entourage, il les enregistre dans son cache même si celles-ci ne l'intéressent pas. Un terminal altruiste réactif ne cherche donc pas à se procurer, lors de contacts avec d'autres terminaux, des informations, et il ne fournit pas d'effort particulier pour se les procurer. Un tel terminal contribue donc à la dissémination d'informations pour lesquelles il n'a a priori aucun intérêt, et qu'il va fournir sur demande à d'autres terminaux. Dans ce sens, l'adoption de ce comportement a un coût et est optionnelle dans notre protocole.

2.2.3.3 COMPORTEMENT ALTRUISTE PROACTIF

Le comportement altruiste proactif étend le comportement altruiste réactif. À la différence d'un terminal au comportement altruiste réactif, un terminal proactif cherche à se procurer des informations qui ne présentent pas d'intérêt pour des services locaux. Pour autant, un terminal

altruiste proactif ne peut pas chercher à se procurer (et de fait disséminer) toutes les informations circulant à travers le réseau. C'est le propriétaire (et administrateur) d'un terminal qui définit les types d'informations pour lesquelles son terminal va se comporter comme transporteur proactif. De la sorte, même si un aucun service applicatif n'est utilisé sur un terminal, son propriétaire peut en ajuster le comportement pour qu'il contribue malgré tout à l'acheminement d'informations à travers le réseau. L'adoption de ce type de comportement est également optionnelle dans notre protocole.

Nous verrons, dans le paragraphe 4.1.2.7, dans quelle mesure chacun de ces comportements peut influencer les performances de notre protocole.

2.2.4 COMMUNICATION MULTI-SAUTS

Une sélectivité forte, si elle permet à un terminal d'être économe quant à sa consommation de ressources, peut également rendre plus difficiles les échanges d'information entre terminaux voisins. En effet, plus un terminal est sélectif, moins il y a de chances qu'il entre en contact avec un terminal ayant des informations l'intéressant, et moins il y a de chances qu'il possède lui même des informations intéressantes d'autres terminaux. Pour aider à réduire ce phénomène, nous proposons que les terminaux d'un même îlot exploitent la connectivité temporaire présente au sein de cet îlot afin d'élargir le voisinage avec lequel ils peuvent échanger des informations. Par ce moyen, nous augmentons les chances qu'aura un terminal d'en rencontrer un autre disposant d'informations susceptibles de l'intéresser, et de fait nous augmentons le nombre de transporteurs d'informations. En revanche, les mécanismes définis dans cette optique ne doivent pas surcharger le médium radio : ils doivent permettre l'exploitation de la connectivité d'un îlot à moindre coût. Cette approche correspond à notre objectif d'utilisation frugale du médium radio pour minimiser la consommation des ressources.

2.2.5 EXPLOITATION DE LA DIFFUSION RADIO

Dans les environnements mobiles qui nous intéressent, les communications entre terminaux voisins sont réalisés par transmission radio, chaque transmission élémentaire s'effectuant par diffusion sur un canal radio partagé par tous les terminaux. Notre système de communication exploite ce mécanisme de diffusion. Ainsi, lorsqu'un terminal doit faire parvenir une information à ses voisins du moment, cette opération est réalisée en une seule diffusion plutôt qu'en adressant successivement une copie du message à chacun des voisins. En choisissant ce mode de transmission, nous privilégions une consommation réduite des ressources, mais ce choix s'effectue au détriment de la fiabilité des transmissions. En effet le standard Wi-Fi utilisé par les plateformes cibles ne fiabilise pas les transmissions en mode *broadcast*, alors qu'il cherche à fiabiliser les transmissions en mode *unicast* via un mécanisme d'acquittement et de reprise sur défaut d'acquittement. Pour prendre en compte cette contrainte notre protocole doit être conçu afin de résister aux échecs de transmissions. Pour ce faire, les interactions entre terminaux voisins reposent sur un schéma d'échange opportuniste plutôt que sur un schéma d'échange transactionnel strict.

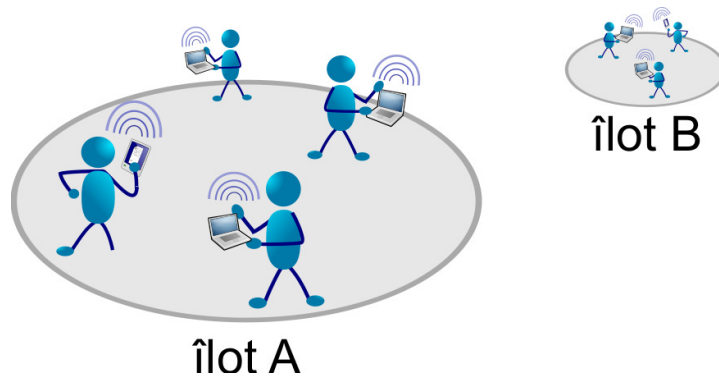


Figure 2.1 – Exemple de réseau mobile ad hoc discontinu formé de deux îlots de connectivité

2.2.6 SUPPORT DE LA VOLATILITÉ

Nous avons évoqué le fait, que pour réduire leur propre consommation d'énergie, les terminaux sont volatiles. Notre système doit donc être capable de s'accommoder des changements d'état d'un terminal hôte. Pour ce faire, il assure la persistance de données (cache, profiles d'intérêt, etc.), et met à profit sa capacité à être réactif aux changements d'état du terminal hôte pour prévenir, par exemple, ses voisins de son arrêt imminent (lors d'une procédure d'arrêt ou de mise en veille), pour prévenir ses voisins de son redémarrage, ou réaliser d'autres actions. Nous verrons par la suite comment ces réactions permettent d'améliorer de manière significative le comportement de notre système.

2.2.7 IMPACT DES CHOIX DE CONCEPTION

Pour parfaire cette vue d'ensemble, il est intéressant de préciser les conséquences résultant des choix que nous avons faits pour mettre en œuvre la communication basée contenus dans les environnements que nous ciblons.

Nous proposons de supporter un mode d'acheminement de l'information opportuniste basé contenus, dans lequel les échanges (ou le partage) d'informations transportées par les terminaux mobiles ont lieu lors de contacts occasionnels et fugitifs entre ces terminaux et sont fonction de leurs centres d'intérêts respectifs. La propagation de l'information d'un service éditeur vers d'éventuels services souscripteurs se réalise donc au gré des rencontres entre terminaux, et elle est directement dépendante de leur mobilité. Comme nous pouvons le constater sur la figure 2.1, si aucun des individus se situant dans l'îlot A ne se déplace vers l'îlot B alors aucune information hébergée par un terminal situé dans l'îlot A ne pourra être délivrée aux terminaux de l'îlot B (et inversement). Dans le cadre d'un grand nombre de scénarios, la mobilité des utilisateurs est un paramètre a priori non maîtrisable. Nous dirons alors que la mobilité des utilisateurs est subie dans notre système. Notre modèle ne peut alors garantir la remise d'une information à l'ensemble des terminaux intéressés. Le fait de ne pas pouvoir garantir la livraison d'information auprès des souscripteurs ne nous semble pas être un problème majeur dans le cas d'*applications non-critiques* envisageables dans de nombreux scénarios comme, par exemple, le partage de

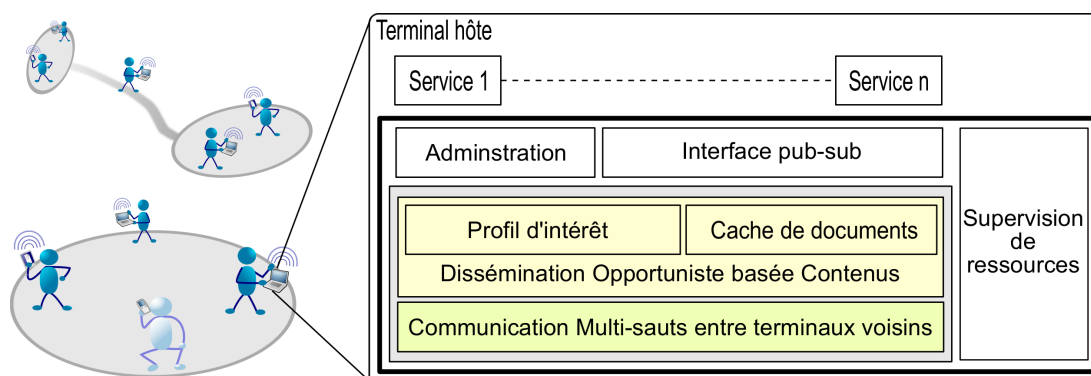


Figure 2.2 – À gauche est illustré un MANET discontinu constitué de trois îlots de connectivité formés par des terminaux mobiles. À droite est représentée l'architecture générale du système de communication déployé sur chacun de ces terminaux.

données lors d'une campagne menée par des géologues. De plus le mode de propagation de l'information qui nous intéresse ici introduit nécessairement des délais dans la communication. Les services applicatifs exploitant ce mode atypique de communication doivent prendre en compte cette caractéristique majeure. Nous supposons notamment qu'un service applicatif éditeur est en mesure de déterminer, pour chaque information publiée dans le réseau, une durée de vie pertinente pour cette information, cette durée de vie pouvant être déterminée arbitrairement ou par une analyse sémantique. Ainsi, chaque information est propagée à travers le réseau pendant une durée limitée. Cette caractéristique contribue à la préservation des ressources des terminaux, puisqu'une information n'ayant plus de sens (du point de vue applicatif) ne sera plus propagée dans le réseau.

2.3 ARCHITECTURE GÉNÉRALE DU SYSTÈME

Les choix de conception détaillés dans le paragraphe précédent nous conduisent à la définition de notre système de communication cible en termes de fonctionnalités. Dans ce paragraphe, nous présentons brièvement l'architecture générale de la plate-forme, qui est par ailleurs illustrée dans la figure 2.2.

Notre plate-forme offre à des services de niveau applicatif la possibilité d'exploiter le modèle de communication basée contenus via une **interface** (ou API) de type **publish/subscribe** (paragraphe 1.4.1). Les services applicatifs peuvent donc publier et souscrire pour la réception d'information structurées que nous désignons par le terme générique de « *documents* ». Cette notion sera précisée dans le paragraphe 2.4.1. Nous préférons utiliser ce terme puisqu'à la différence du terme « message », le terme « document » n'est pas implicitement associé à la sémantique « envoyé à destination de ... », et qu'il coïncide mieux, de notre point de vue, avec le modèle de la communication basée contenus.

Notre système permet l'hébergement et le transport des documents en transit dans le réseau par les terminaux mobiles. Le module « *Cache de documents* » est responsable de la gestion

de cet espace de stockage. Lorsqu'un service applicatif local publie un document, ce document est simplement déposé dans le cache local. Il pourra ensuite se propager d'un terminal mobile à l'autre au gré des contacts entre terminaux.

Pour pouvoir recevoir un certain type de documents, un service applicatif doit souscrire en conséquence en décrivant le type précis de document désiré dans un « *prédicat de sélection* ». Les divers prédicats de sélection exprimant les souscriptions des services applicatifs sont assemblés et forment ensemble le « *Profil d'intérêt* » du terminal dont la définition exacte sera fournie dans le paragraphe 2.4.1. La sélectivité d'un terminal est donc directement ajustée en fonction des besoins des services applicatifs, ce qui permet de réduire au minimum les échanges de documents entre terminaux mobiles, et correspond à notre principe de frugalité.

Le module « *Administration* » permet au propriétaire d'un terminal d'en ajuster le comportement sélectif. C'est en fait un pseudo-service applicatif à travers lequel le propriétaire peut activer et désactiver les options conditionnant les comportements altruiste réactif ou altruiste proactif du terminal. Il permet en outre au propriétaire de définir les types de documents pour lesquels il est prêt à se comporter comme altruiste proactif, c'est-à-dire que, au même titre qu'un autre service applicatif le module d'administration peut déposer via l'interface pub-sub des souscriptions sous la forme de prédicat de sélection.

Les deux blocs inférieurs gauche de la figure 2.2 présentent le protocole de communication. Comme cela est illustré, nous avons choisi de structurer notre protocole en deux couches aux fonctionnalités bien distinctes :

- Une **Couche Supérieure de Dissémination Opportuniste basée Contenus** (nommée CSDOC). Elle réalise la dissémination opportuniste (tolérant les délais et les ruptures de connectivité) des documents selon une approche basée sur le contenu. Elle permet l'hébergement de documents dans le cache d'un terminal, qui, lors de ses déplacements les transporte physiquement et contribue ainsi à leur propagation dans le réseau. Elle définit enfin les modalités d'interaction entre terminaux temporairement voisins afin qu'ils puissent échanger des documents en fonction de leurs profils d'intérêt respectifs. Les différents éléments constituant cette couche protocolaire sont présentés dans le paragraphe 2.4.
- Une **Couche Inférieure pour les Communications Multi-sauts entre terminaux voisins** (nommée CICM). Des terminaux voisins sont des terminaux qui résident — a priori temporairement — dans un même îlot de connectivité d'un MANET discontinu. Les interactions entre voisins nécessitent qu'ils soient en mesure de communiquer à k sauts, c'est-à-dire au delà de leurs voisins directs. La couche inférieure de notre protocole définit les mécanismes nécessaires pour assurer les transmissions à k -sauts entre terminaux voisins. Ces différents mécanismes sont détaillés dans le paragraphe 2.5.

Enfin notre système cible devant percevoir la volatilité d'un terminal, un module de « *surveillance des ressources* » lui permet d'être averti des arrêts, redémarrages, mises en veille, etc. du terminal mobile hôte. Nous verrons dans les paragraphes suivants, qui sont consacrés à la présentation détaillée du protocole de communication, comment ces événements sont pris en compte dans notre système.

<i>Descripteur du document</i>	
id	= "12"
deadline	= "2010-07-10T14:00:00"
	:
<i>Charge utile sous forme binaire</i>	
101001010010010100100100100010	
	:

Figure 2.3: Un document est composé de deux parties : un descripteur fournissant des méta-données le caractérisant et un contenu sous forme brute (binaire).

2.4 COUCHE SUPÉRIEURE DE DISSÉMINATION OPPORTUNISTE BASÉE CONTENUS

La couche supérieure de notre modèle de communication combine les principes de la communication basée contenus et de la communication opportuniste. Elle fournit :

- les mécanismes nécessaires à la différenciation de l'information en fonction de son contenu (paragraphe 2.4.1),
- un protocole de communication (paragraphe 2.4.2) définissant les règles d'interaction entre terminaux temporairement voisins. Ce protocole met en œuvre le principe d'acheminement *store, carry and forward* évoqué au paragraphe 1.3.2.1. De la sorte, il permet de tolérer le manque de connectivité caractérisant les environnements que nous ciblons.

2.4.1 DIFFÉRENCIATION DE L'INFORMATION

Dans notre modèle de communication, les participants au réseau s'échangent des documents en fonction de leurs contenus et de leurs profils d'intérêt respectifs. Cela nécessite donc que les terminaux soient capables de :

1. différencier l'information en fonction de leur contenu ;
2. spécifier les différents types d'information par lesquels il sont intéressés.

2.4.1.1 DOCUMENT, DESCRIPTEUR ET IDENTIFIANT

Un document est une unité d'information structurée, qu'un service applicatif émetteur peut injecter dans le réseau afin qu'il s'y propage, et soit à terme réceptionné par tout service applicatif affichant un intérêt pour le type d'information contenue dans ce document. Comme illustré dans la figure 2.3, un document est constitué de deux parties : son descripteur, et son contenu.

Le descripteur peut être vu comme une collection de couples attribut-valeur fournissant des informations (ou méta-informations) diverses à propos du contenu même du document. Ces informations peuvent, par exemple, être son identifiant, son origine, sa date de production, sa



<p><i>Descripteur du document D1</i></p> <p>id = "5be62d77..06f628348"</p> <p>deadline = "2010-07-10T14:00:00"</p> <p>date = "2010-07-08T09:52:11"</p> <p>service = "filesharing"</p> <p>mimetype = "application/pdf"</p> <p>publisher = "Julien"</p> <p>keywords = "mobile, ad hoc, \</p> <p>delay-tolerant, opportunistic"</p> <p><i>Charge utile sous forme binaire</i></p> 	<p><i>Descripteur du document D2</i></p> <p>id = "53875b40..d78ffb48c"</p> <p>deadline = "2010-07-12T13:15:30"</p> <p>date = "2010-07-05T13:15:30"</p> <p>service = "news"</p> <p>group = "comp.networking"</p> <p>mimetype = "text/rfc850"</p> <p>publisher = "Fred"</p> <p>keywords = "mobile, ad hoc"</p> <p><i>Charge utile sous forme binaire</i></p> 
--	--

Figure 2.4: Exemples de deux documents publiés par deux services applicatifs distincts. À gauche un document publié dans le cadre d'un service de partage de fichier, et à droite un document publié dans le cadre d'un service de discussion thématique pair-à-pair.

date de péremption, le type et la nature de son contenu, une liste de mots-clés caractérisant son contenu, etc. De nombreux attributs peuvent être présents dans le descripteur d'un document. Ils peuvent être définis librement par les services applicatifs en fonction de leurs besoins propres, et sont autant d'informations qui vont guider la dissémination du document. Des exemples de descripteurs sont présentés figure 2.4. Dans cette figure, le descripteur *D1* est celui d'un document publié dans le cadre d'un service de partage de fichiers. Ce descripteur spécifie notamment le type du contenu de ce document (un document PDF en l'occurrence), et il contient des mots-clés caractérisant ce document. On peut noter que l'identité de l'émetteur est indiquée (bien que ce ne soit pas une obligation), ainsi que les dates de production et de péremption de ce document. Dans le cas présent, le document n'est pas censé se propager dans le réseau au delà des date et heure indiquées. Le descripteur *D2*, dans cette même figure, concerne quant à lui un document publié dans le cadre d'un service de discussion thématique pair-à-pair. Dans le cas présent ce document est publié par *Fred* dans le groupe de discussion thématique *comp.networking*, et son contenu est au format texte défini dans la RFC850 (NNTP, *Network News Transfer Protocol* [Hor83]).

Dans notre modèle, deux attributs sont absolument requis : chaque document doit porter un identifiant unique, ainsi qu'une date de péremption. L'identifiant doit être unique car il permet d'assurer les échanges entre terminaux dans le réseau, tout en leur évitant de stocker ou d'échanger des doublons. La manière dont est engendré cet identifiant est présentée dans le paragraphe 3.1.1.2. D'autre part, pour chaque document injecté dans le réseau, la date de péremption doit être spécifiée. Cette information peut directement être liée à la sémantique du document (et en particulier à celle de son contenu), ou être fixée de manière arbitraire. Par exemple, si un document contient la carte météo du jour, il est évident que, le lendemain, cette information ne présentera plus aucun intérêt car les données de la carte ne seront plus valides.

Dans ce cas, la date de péremption est naturellement celle marquant la fin de la journée. La date de péremption permet de fixer la durée de vie d'un document dans le réseau, durée après laquelle sa dissémination et son stockage en cache par les terminaux ne sera plus utile.

De manière générale, nous faisons l'hypothèse que le poids d'un document dépasse nettement celui de son descripteur, qui est lui-même supérieur à celui de son identifiant. Des ordres de grandeurs typiques sont : $O(10 \text{ ko})$ pour un document, $O(100 \text{ o})$ pour un descripteur, et $O(10 \text{ o})$ pour un identifiant. Ce contraste marqué entre les poids relatifs des entités manipulées dans notre protocole est systématiquement mis à profit afin de limiter les quantités de données échangées entre les terminaux, ce qui est conforme à notre objectif de frugalité.

2.4.1.2 PROFIL D'INTÉRÊT ET PRÉDICAT DE SÉLECTION

Profil d'intérêt. Le profil d'intérêt d'un terminal caractérise le type des documents qui l'intéressent et donc, implicitement, le type de documents qu'il souhaite recevoir et pour lesquels il est également prêt à jouer le rôle de transporteur mobile. Un profil d'intérêt est un ensemble de prédicats de sélection, qui sont eux-mêmes déterminés par les services applicatifs s'exécutant sur le terminal lorsqu'ils souscrivent pour recevoir un type particulier de documents.

Prédicat de sélection. Un prédicat de sélection définit un filtre applicable à un descripteur de document. Il permet de marquer l'intérêt porté par un terminal pour le document en question.

Le choix du langage (de souscription) utilisé pour construire un prédicat de sélection est un élément important dans un système de communication basée contenus. En effet, plus le langage permet de définir des expressions ou formules précises, plus il permet d'affiner la sélectivité d'un terminal (et implicitement des services applicatifs qu'il héberge). Dans notre modèle, un prédicat de sélection est une formule propositionnelle P_i qui est construite en utilisant les opérateurs de négation, de conjonction et de disjonction de propositions atomiques. Les propositions atomiques sont quant à elles des tuples de la forme $(attribut, comparateur, valeur)$. Par exemple le prédicat p_j défini par le tuple $(att_j, comp_j, val_j)$ est vraie lorsque la comparaison entre la valeur de l'attribut nommé att_j contenue dans le descripteur du document et la valeur val_j en utilisant le comparateur $comp_j$ est vérifiée. En fonction de la nature de l'attribut, il est souhaitable de pouvoir utiliser différents comparateurs. Le comparateur $comp_j$ peut être choisi parmi un ensemble d'opérateurs de base $\{=, <, <=, <>, >=, >\}$ pour des attributs de type numérique, et un opérateur d'expression régulière (*matches*) pour les attributs de type chaîne de caractères.

Le profil d'intérêt du terminal est le résultat de la disjonction des prédicats de sélection P_i qui définissent ses centres d'intérêts. Pour un terminal t_i donné son profil d'intérêt suit la formule $prof(t_i) = P_1 \vee \dots \vee P_m$ où P_i est un prédicat de sélection. De la sorte, un profil d'intérêt est applicable à un descripteur de document.

La table 2.1 illustre le profil d'intérêt d'un terminal et les prédicats de sélection qui lui sont associés. Voyons si ces prédicats de sélection peuvent s'appliquer aux descripteurs de documents

Prédicat de sélection	Expression
P_1	((service = 'news') or (service = 'filesharing')) and (keywords matches 'mobile')
P_2	(service = 'news') or (publisher = 'Fred')

Table 2.1 – Profils d'intérêt et prédicats de sélection

présents dans la figure 2.4. Le prédicat de sélection P_1 permet de sélectionner les documents $D1$ et $D2$. Il précise que l'attribut « service » d'un descripteur doit être égal soit à « news » soit à « filesharing », et que, parmi la liste de mots clés, doit se trouver le terme « mobile ». Le prédicat de sélection P_2 permet de sélectionner le document $D2$ car tous les attributs présents dans son descripteur correspondent avec l'expression. En revanche, le prédicat P_2 ne sélectionne pas le document $D1$ car la valeur de l'attribut « services » n'est pas égale à « news » et la valeur de l'attribut « publisher » n'est pas égale à « Fred ». Un terminal possédant le prédicat de sélection P_2 est donc un transporteur potentiel pour l'ensemble des documents publiés par l'éditeur « Fred » et pour l'ensemble des documents publiés dans le cadre du service de discussion thématique pair-à-pair.

2.4.2 PROTOCOLE DE COMMUNICATION

Dans ce paragraphe, nous décrivons notre protocole de communication, qui repose d'une part sur l'exploitation opportuniste de contacts fugitifs entre terminaux voisins pour échanger des documents en fonction de leurs intérêts respectifs, et d'autre part sur le transport de documents par ces mêmes terminaux pour rétablir une forme de connectivité entre îlots épars.

Avant d'aller plus loin dans la définition de notre protocole de communication, il nous semble important de présenter de manière simplifiée son principe de fonctionnement. La figure 2.5 illustre les interactions entre deux terminaux voisins. Le terminal A est intéressé par les documents correspondant au prédicat P_2 (présenté dans le tableau 2.1) et n'héberge aucun document dans son cache. Le terminal B quant à lui héberge les documents $D1$ et $D2$ dans son cache (présentés dans la figure 2.4), et est intéressé par les documents correspondant au prédicat P_1 (présenté dans le tableau 2.1).

La figure 2.5 illustre les différentes phases d'un cycle d'interaction élémentaire entre A et B.

Diffusion périodique d'une annonce. (étapes (1) et (2) de la figure 2.5). Dans les environnements que nous ciblons, les échanges de documents d'intérêt entre terminaux mobiles ne peuvent avoir lieu que lors de contacts occasionnels et fugitifs. Pour être en mesure d'exploiter ces contacts, un terminal doit tout d'abord être capable de les détecter. Notre protocole met en œuvre un mécanisme de détection de voisinage, en s'appuyant sur la diffusion périodique d'une annonce (paragraphe 2.4.2.1). Ce mécanisme permet à chaque terminal de percevoir la présence

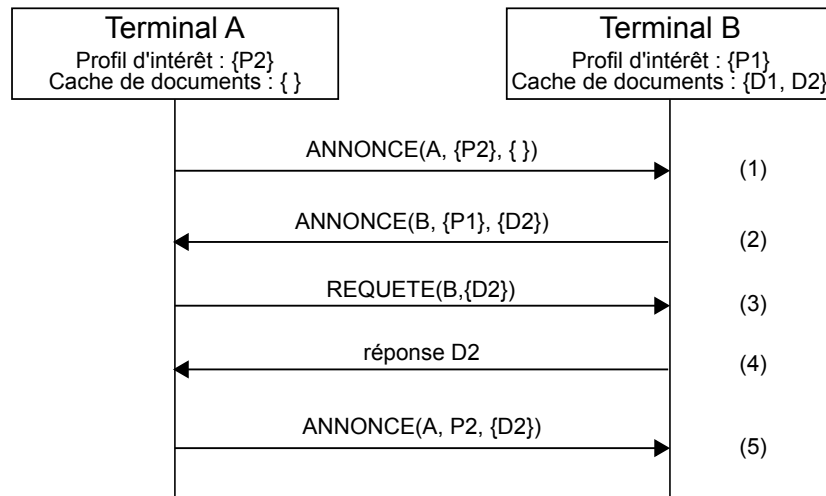


Figure 2.5 – Diagramme de séquence illustrant les interactions entre deux terminaux voisins A et B.

de ses voisins et d'en découvrir les profils d'intérêt. Par exemple, dans la figure 2.5, lorsque le terminal A diffuse une annonce, il informe ainsi le terminal B de sa présence et de son profil d'intérêt. De cette manière, le terminal B va être en mesure d'insérer dans sa prochaine annonce un catalogue de documents susceptibles d'intéresser ses voisins du moment (ici l'unique terminal A). Dans notre exemple, le catalogue construit par B contient uniquement le document *D2* qui correspond à *P2* (l'unique prédicat du profil d'intérêt de A).

Requête de documents. (étapes (3) de la figure 2.5) Lorsque le terminal A reçoit l'annonce diffusée par B, il apprend la présence d'un nouveau voisin B, et il apprend que B héberge en cache le document *D2*. En examinant le descripteur de *D2*, A constate qu'il satisfait son profil d'intérêt et qu'il ne dispose pas encore d'une copie de ce document dans son propre cache. A adresse alors une requête au terminal B, lui demandant de diffuser le document *D2* (paragraphe 2.4.2.2).

Diffusion de documents. (étapes (4) de la figure 2.5) Ayant reçu la demande de A, B extrait *D2* de son cache et le diffuse. Le document *D2* est alors réceptionné par A, qui le dépose dans son propre cache. Le terminal A devient dès lors transporteur du document *D2* (paragraphe 2.4.2.4 et 2.4.2.5), et peut ainsi contribuer à sa dissémination à travers le réseau.

Il est à noter que cette approche suppose que la connectivité entre terminaux mobiles voisins est suffisamment stable pour permettre un cycle d'interaction élémentaire complet. Par ailleurs, des terminaux mobiles voisins étant des terminaux qui résident a priori temporairement dans un même îlot de connectivité, nous avons pour objectif d'identifier dans les paragraphes suivants les besoins en terme de communication multi-sauts.

2.4.2.1 DIFFUSION PÉRIODIQUE DU PROFIL D'INTÉRÊT ET DU CATALOGUE

Variables

t_i : identifiant (unique) du terminal.
 $prof(t_i)$: profil d'intérêt du terminal.
 $ann(t_i)$: dernière annonce complète diffusée par le terminal.
 \mathcal{C} : cache de documents du terminal.
 \mathcal{T} : période d'annonce (en secondes).
 k : portée des annonces en nombre de sauts.
 $voisinage$: table du voisinage maintenue par le terminal.

```

1 répéter tous les  $\mathcal{T}$  secondes
    // Création de l'annonce
2   si nouveauContexte() alors
3        $cat(t_i) \leftarrow$  créer Catalogue( $voisinage, \mathcal{C}$ )
4        $ann(t_i) \leftarrow$  créer AnnonceComplète( $t_i, ref, ddv, prof(t_i), cat(t_i)$ )
5        $msg \leftarrow ann(t_i)$ 
6   sinon
7        $msg \leftarrow$  créer AnnonceCourte( $t_i, ann(t_i).ref, ddv$ )
8   diffuser( $msg, k$ )

```

Algorithme 1 : Construction et diffusion dans le k -voisinage d'une annonce (complète ou courte)

L'algorithme 1 présente le mécanisme de diffusion périodique d'une annonce.

Périodicité d'annonce \mathcal{T} . Une attention particulière doit être portée à la fréquence de diffusion des annonces par les terminaux, fréquence qui est un paramètre du protocole (ligne 1 dans l'algorithme 1). En effet, une fréquence trop élevée nuirait à notre démarche de conservation de l'énergie, et au bon fonctionnement de notre protocole à cause d'éventuelles collisions. Inversement une fréquence trop basse nuirait à la réactivité dans la détection du voisinage, et par conséquent à l'exploitation de contacts fugitifs pour échanger de l'information. Un compromis entre la conservation en énergie et la détection du voisinage doit être fait en fonction de critères qui sont principalement liés à la population d'individus considérée et à la technologie de transmission radio utilisée. Par exemple, nous avons constaté au cours de nos campagnes d'expérimentation qu'une période d'annonce de 15 secondes est un bon compromis dans le cas d'une population de piétons utilisant des terminaux équipés d'interfaces radio de type Wi-Fi (IEEE 802.11).

Structure d'une annonce. Tout terminal participant au réseau diffuse donc périodiquement un unique message de contrôle que nous désignons par le terme « *annonce* ». Ce message de contrôle contient :

- dans son descripteur :
 - l'identité t_i du terminal émetteur ;
 - la référence ref de l'annonce ;
 - la durée de vie des informations contenues dans l'annonce ddv .
- et en guise contenu :
 - le profil d'intérêt $prof(t_i)$ du terminal émetteur t_i ;
 - un catalogue de documents $cat(t_i)$ qui concerne des documents que t_i possède dans son cache et qui sont susceptibles d'intéresser ses voisins.

Chaque terminal doit pouvoir contrôler la portée (en nombre de sauts k) de son annonce dans son k -voisinage (ligne 8 dans l'algorithme 1). **La diffusion de message à k -sauts est donc un besoin qui doit être couvert par la couche protocolaire inférieure (CICM).** Nous verrons dans le paragraphe 2.5 comment cette couche protocolaire est définie, et quelles sont ses fonctionnalités.

Diffusion périodique d'une annonce. Le mécanisme de diffusion d'annonce permet à un terminal t_i de percevoir son voisinage. En effet, lorsqu'un terminal reçoit une annonce, cela lui permet de découvrir ou de confirmer la présence du voisin t_i dans son k -voisinage. De plus, l'annonce contient le profil d'intérêt $prof(t_i)$, ce qui permet à tout récepteur d'apprendre quels types de documents intéressent t_i . Chaque terminal perçoit ainsi son voisinage, et conserve pour chaque voisin les informations qui le caractérisent. En particulier, chaque terminal maintient une table du voisinage, dont la structure et la procédure de mise à jour sont présentés dans le paragraphe 2.4.2.2.

Dans notre protocole, les annonces périodiques s'appuient sur des transmissions par diffusion, qui ne sont en général pas fiabilisées dans les couches PHY et MAC actuelles. Il peut donc arriver qu'une annonce ne soit pas reçue par tous les voisins d'un terminal émetteur, alors qu'ils avaient pourtant déjà connaissance de ce voisin. Nous avons donc attribué une durée de vie (ddv) aux informations contenues dans l'annonce. Cette durée de vie est par défaut fixée à deux fois la période d'annonce (ligne 4 dans l'algorithme 1), ce qui permet à un terminal de « manquer » une annonce de l'un de ses voisins sans pour autant en déduire que ce voisin a disparu. Elle peut toutefois être réajustée si les conditions le justifient, par exemple dans un réseau dans lequel les taux d'erreurs de transmission sont particulièrement élevés.

Ajustement dynamique du catalogue diffusé dans chaque annonce. Grâce à la perception de son voisinage, le terminal t_i est en mesure d'ajuster le contenu du catalogue inséré dans chacune de ses annonces périodiques, de telle sorte que ce catalogue contienne uniquement les descripteurs de documents susceptibles d'intéresser ses voisins du moment (ligne 3 dans l'algorithme 1). Ainsi, t_i ne proposera jamais à ses voisins des documents qui, de toute façon, ne correspondent aucunement à leurs profils d'intérêt. De plus, les descripteurs contenus dans le catalogue sont réduits aux uniques couples attribut-valeur permettant aux voisins de décider s'ils sont intéressés ou non par un document. De la sorte, pour le descripteur d'un document

Descripteur du document D2	
id	"53875b40..d78ffb48c"
deadline	"2010-07-12T13:15:30"
date	"2010-07-05T13:15:30"
service	"news"
group	"comp.networking"
mimetype	"text/rfc850"
publisher	"Fred"
keywords	"mobile,ad hoc"

Descripteur réduit du document D2	
id	"53875b40..d78ffb48c"
service	"news"
publisher	"Fred"

Figure 2.6: À gauche le descripteur du document D2. À droite le descripteur réduit du document D2 construit en fonction du profil d'intérêt du terminal A, c'est-à-dire en fonction du prédicat P2.

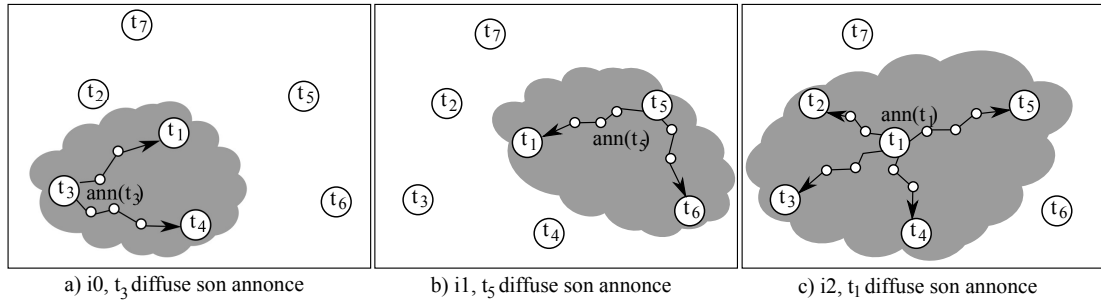


Figure 2.7 – Illustration du mécanisme de diffusion périodique d'annonce. Les nœuds figurant sur les flèches sont des terminaux mobiles contribuant à relayer les annonces. La zone grise autour d'un terminal représente la zone de diffusion couverte par son annonce. Les terminaux situés hors de cette zone grise ne reçoivent donc pas l'annonce.

donné, sont conservés uniquement les attributs présents dans les prédicats qui le sélectionnent, ainsi bien sûr que l'identifiant unique du document. Par exemple, la figure 2.6 représente, en partie gauche, le catalogue de documents inséré par le terminal B dans notre exemple introductif (figure 2.5). On note en partie droite que, si B cherche à bâtir un descripteur réduit en tenant compte du profil de son voisin A, alors seuls les attributs service et publisher sont discriminants du point de vue de A. Un catalogue bâti en combinant les descripteurs réduits des documents susceptibles d'intéresser les voisins est donc nettement plus compact qu'un catalogue constitué de descripteurs complets. De cette manière, la taille de $cat(t_i)$ proposé à chaque période est ajustée au plus bas, et le coût de la diffusion de chaque annonce est donc réduit au minimum. En effet, si un terminal héberge un grand nombre de documents dans son cache, il ne diffusera alors qu'un sous-ensemble de leurs descripteurs satisfaisant les profils d'intérêt de ses voisins, voire aucun si aucun voisin n'est intéressé par ces documents.

La figure 2.7 illustre l'ensemble du mécanisme de diffusion périodique d'annonces. À l'instant i_0 , le terminal t_3 diffuse une annonce périodique contenant son profil d'intérêt $prof(t_3)$ et

un catalogue vide, car jusqu'alors t_3 n'a reçu aucune annonce de la part de ses voisins. Cette annonce est reçue par les terminaux t_1 et t_4 qui mettent à jour la perception de leur k-voisinage en y ajoutant t_3 , et en notant que t_3 est intéressé par les documents correspondant à $prof(t_3)$. Aucun descripteur de document n'est présent dans le catalogue $cat(t_3)$. t_1 et t_4 ne l'analysent donc pas.

À l'instant i_1 , le terminal t_5 diffuse à son tour une annonce périodique contenant son profil d'intérêt $prof(t_5)$ et un catalogue vide car jusqu'alors t_5 n'a pas non plus reçu d'annonce de la part de ses voisins. L'annonce de t_5 est reçue par les terminaux t_1 et t_6 qui enregistrent alors la présence dans leur k-voisinage de t_5 , et notent que t_5 est intéressé par les documents correspondant à $prof(t_5)$. Aucun descripteur de document n'est présent dans le catalogue $cat(t_5)$, t_1 et t_6 ne l'analysent donc pas.

À son tour, à l'instant i_2 le terminal t_1 diffuse une annonce périodique contenant son profil d'intérêt $prof(t_1)$ et le catalogue $cat(t_1)$ établi en fonction des documents présents dans son propre cache (doc_1 , doc_2 , doc_3 et doc_4) et des profils d'intérêt des voisins connus à l'instant i_2 , c'est-à-dire $prof(t_3)$ et $prof(t_5)$. Cette annonce est reçue par les terminaux t_2 , t_3 , t_4 et t_5 qui enregistrent alors la présence dans leur voisinage de t_1 et notent que t_1 est intéressé par les documents correspondant à $prof(t_1)$. Ils procèdent en outre au traitement du catalogue $cat(t_1)$ qui dans le cas présent pourrait contenir les descripteurs de documents intéressants notamment t_3 et t_5 puisqu'il a été construit en tenant compte de leurs centres d'intérêt. Le traitement des catalogues est présenté en détails dans le paragraphe 2.4.2.2.

Ajustement dynamique du format des annonces. Dans certaines circonstances, la taille d'une annonce périodique peut être fortement réduite. Lorsqu'un terminal n'a observé aucun changement depuis l'annonce précédente (ligne 2 dans l'algorithme 1), il s'abstient de diffuser une annonce complète et diffuse une annonce longue portant la même référence ref que la dernière annonce complète qu'il a diffusé. Les annonces diffusées périodiquement par un terminal ont donc deux formats :

- annonce dite « courte » contenant uniquement t_i , ref et ddv ;
- annonce dite « complète » contenant t_i , ref , ddv , $prof(t_i)$ et $cat(t_i)$.

Une annonce courte permet à t_i de confirmer sa présence à ses voisins et de les informer que, de son point de vue, la dernière annonce complète (contenant $prof(t_i)$ et $cat(t_i)$) diffusée est toujours valide. Ce mécanisme d'annonce courte est exploitable uniquement lorsque, depuis sa dernière annonce complète, t_i :

- n'a détecté aucun nouveau voisin et n'a perdu aucun voisin ;
- n'a pas observé de changement dans les profils $prof(t_j)$ reçus de ses voisins ;
- n'a pas modifié son propre profil d'intérêt $prof(t_i)$;
- n'a déposé aucun nouveau document dans son propre cache local.

Ce mécanisme d'adaptation dynamique du format de l'annonce est conforme à notre objectif d'économie de ressources. Par exemple, il permet à un terminal isolé pour une durée plus ou moins courte d'économiser de l'énergie puisqu'il ne diffusera qu'une annonce très réduite afin

de se faire connaître d'éventuels nouveaux voisins. Ce mécanisme permet aussi de réduire la quantité d'information échangée sur le médium radio lorsque des voisins sont dits « stables », c'est-à-dire que les conditions mentionnées ci-dessus sont vérifiées comme cela peut être le cas dans un îlot de connectivité dans lequel tous les échanges de documents possibles au sein de l'îlot ont déjà eu lieu.

Adaptation à la volatilité des terminaux. Le mécanisme d'annonce périodique est réactif à la volatilité d'un terminal. Il doit démarrer lors de l'allumage ou de la sortie de veille du terminal hôte, lui permettant ainsi d'avertir des voisins potentiels de sa présence. L'arrêt ou la mise en veille d'un terminal entraîne l'arrêt du mécanisme de diffusion d'annonce. Lorsqu'un terminal interrompt son fonctionnement, ses voisins le considèrent toujours comme présent. Ils continuent donc d'adapter le contenu de leurs catalogues en fonction d'une table du voisinage qui est erronée puisqu'un de leurs voisins a disparu. Pour limiter ce phénomène, avant d'être mis en veille ou arrêté, un terminal diffuse un message de contrôle indiquant son arrêt imminent. De la sorte, les voisins recevant ce message suppriment son émetteur de leur propre table du voisinage, et sont alors en mesure d'ajuster le contenu de leurs catalogues.

2.4.2.2 RÉCEPTION D'UNE ANNONCE

Les opérations réalisées par un terminal suite à la réception d'une annonce complète ou courte de l'un de ses voisins sont présentées dans l'algorithme 2. De manière synthétique, ces opérations sont les suivantes :

- mise à jour de la table du voisinage,
- analyse du contenu du catalogue inclus dans l'annonce,
- si nécessaire envoi d'une requête à l'annonceur.

Table du voisinage. La table du voisinage est une table qui modélise la perception de son voisinage par un terminal. Elle permet au terminal de conserver temporairement les informations relatives à chacun de ses voisins du moment. Chaque entrée est constituée de l'identité du voisin, de la référence de la dernière annonce complète reçue de ce voisin et du profil d'intérêt contenu dans cette annonce, ainsi que de la liste des documents récemment demandés à ce voisin afin de permettre à un terminal d'éviter de demander la diffusion d'un même document à plusieurs de ces voisins. Comme nous l'avons déjà indiqué, chaque entrée possède une durée de vie indiquant dans combien de temps le voisin correspondant devra être considéré comme perdu. Ceci permet de purger automatiquement la table des informations concernant des voisins qui n'ont plus donné signe de vie depuis quelque temps. En outre, la réception d'un message de contrôle indiquant l'arrêt imminent d'un terminal voisin provoque également la suppression de l'entrée correspondante de la table maintenue par le terminal receveur.

Mise à jour de la table du voisinage. La réception d'une annonce par un terminal entraîne la mise à jour de la table. Les opérations à réaliser dépendent du format de l'annonce reçue :

Variables

$prof(t_i)$: profil d'intérêt du terminal.

\mathcal{C} : cache de documents du terminal.

$voisinage(voisin, (ref, profil, ddv, idDocs))$: table du voisinage maintenue par le terminal.

```

1  sur réception de l'annonce ann
2  si ann est complète alors
3      si ( $ann.source \notin voisinage.voisin$ )  $\vee$  ( $(ann.source \in voisinage.voisin) \wedge$ 
        ( $ann.ref \neq voisinage[ann.source].ref$ )) alors
4           $voisinage[ann.source] \leftarrow (ann.ref, ann.profil, ann.ddv, \emptyset)$ 
5           $ids \leftarrow analyserCatalogue(ann.catalogue, prof(t_i), \mathcal{C})$ 
          // Supprimer de la liste ids les documents déjà réclamés
6          pour tous les  $v \in voisinage.voisin$  faire
7               $ids \leftarrow ids - (voisinage[v].idDocs \cap ids)$ 
8           $voisinage[ann.source].idDocs \leftarrow ids$ 
9          si  $ids \neq \emptyset$  alors
10             requête  $\leftarrow$  créer Requête( $t_i, ids$ )
11             envoyer requête à ann.source
12 sinon
13     // Annonce courte
14     si ( $ann.source \in voisinage.voisin$ )  $\wedge$  ( $ann.ref = voisinage[ann.source].ref$ )
15     alors
16          $voisinage[ann.source].ddv \leftarrow ann.ddv$ 
17         si  $voisinage[ann.source].idDocs \neq \emptyset$  alors
18             requête  $\leftarrow$  créer Requête( $t_i, voisinage[ann.source].idDocs$ )
19             envoyer requête à ann.source
20     sinon
21         requête  $\leftarrow$  créer Requête( $t_i, ann.ref$ )
22         envoyer requête à ann.source

```

Algorithme 2 : Traitement réalisé lors de la réception d'une annonce (complète ou courte)

- si l'annonce reçue par un terminal est *complète*, alors il vérifie que l'annonce reçue n'a pas déjà été traitée (lignes 2-3 dans l'algorithme 2). Pour ce faire il vérifie que les informations contenues dans l'annonce reçue sont différentes de celles conservées localement en se servant de la référence de l'annonce. Dans le cas où les informations sont identiques, le traitement de l'annonce est interrompu, de sorte que le terminal ne demande pas de nouveau la diffusion de documents pour lesquels il a déjà envoyé une requête (cette partie du protocole est détaillée ci-dessous). Dans le cas contraire, le terminal récepteur met à jour l'entrée correspondant à l'émetteur de l'annonce (ligne 4 dans l'algorithme 2).
- si l'annonce reçue par un terminal est *courte*, alors il cherche à mettre à jour l'entrée correspondant au terminal annonceur (ligne 13 dans l'algorithme 2). Il vérifie donc qu'il dispose des informations contenues dans la version complète correspondant à l'annonce courte reçue en se servant de la référence de l'annonce. Si tel est le cas alors il modifie la durée de vie de l'entrée par celle de l'annonce courte (ligne 14 dans l'algorithme 2), de sorte que ce voisin ne soit pas supprimé de sa table du voisinage. Dans le cas où le récepteur ne dispose pas de la version complète correspondant à l'annonce courte, c'est-à-dire si les identifiants sont différents ou s'il ne dispose pas d'entrée concernant ce voisin, alors il adresse un requête à l'annonceur, lui demandant de diffuser immédiatement la version complète de l'annonce *ref* qu'il vient de recevoir (lignes 19-20 dans l'algorithme 2). Lors de la réception de cette requête, l'annonceur diffuse immédiatement dans son k-voisinage la version complète correspondant à l'annonce courte, ce qui permet de satisfaire l'ensemble des voisins demandeurs en une seule diffusion. Cette opération est réalisée au plus une fois au cours d'une période d'annonce afin d'éviter de répondre à de multiples requêtes, et entraîner de fait une surconsommation des ressources, ce qui serait contraire à notre principe d'économie des ressources. Cette observation est importante car elle détermine l'une des fonctionnalités requises de la couche protocolaire CICM, que nous examinons en détail dans le paragraphe 2.5.

Analyse du catalogue. Suite à la mise à jour de la perception de son voisinage, un terminal receveur peut adresser une requête à l'annonceur pour lui demander de diffuser certains documents qui lui font défaut. Voyons maintenant comment un récepteur identifie ces documents. Le traitement correspondant diffère selon le format de l'annonce reçue :

- si l'annonce est *complète*, et qu'elle contient des informations différentes de celles conservées localement, alors le terminal récepteur procède à l'analyse du catalogue $cat(t_i)$ quelle contient (ligne 5 dans l'algorithme 2). Cet examen permet au receveur d'identifier des documents proposés par l'annonceur qui correspondent à son profil d'intérêt, et pour lesquels il ne dispose pas déjà d'une copie en cache. Sachant que différents voisins peuvent proposer des documents identiques, un récepteur peut alors solliciter auprès de plusieurs voisins la diffusion du même document. Pour éviter ce phénomène surconsommateur de ressource, un terminal conserve temporairement la liste des identifiants de documents demandés à chaque voisin dans sa table du voisinage. Un terminal retient donc uniquement les identifiants de documents dont il n'a pas déjà réclamé la diffusion

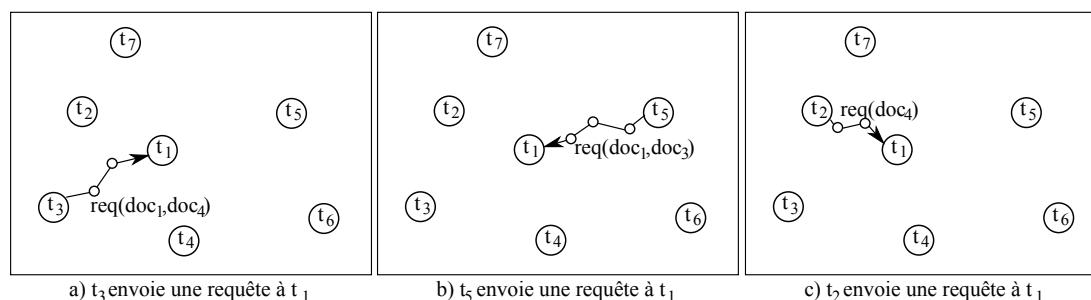


Figure 2.8 – Illustration du mécanisme de requête. Les noeuds figurant sur les flèches sont des terminaux mobiles contribuant à acheminer les requêtes vers leur destinataire.

à un autre voisin (lignes 6-7 dans l'algorithme 2). La réception d'un document entraîne bien sûr la suppression de son identifiant dans la liste des documents demandés.

- si l'annonce est *courte* et que des identifiants sont présents dans la liste associée à l'émetteur de l'annonce, alors le terminal récepteur retient ces identifiants de documents (lignes 15-17 dans l'algorithme 2). La présence d'identifiants dans la liste associée à l'annonceur indique soit que la requête n'a pas été reçue par l'annonceur, soit que le terminal récepteur n'a pas été en mesure de réceptionner toute ou partie des documents diffusés par l'annonceur. Néanmoins, ces échecs de transmission ne constituent pas des pannes, ils sont dus à la non fiabilisation des transmissions des documents entre terminaux. Notre protocole résiste à ce type d'événements, un terminal redemandera plus tard la diffusion des documents manqués au même terminal ou à un autre.

Envoi d'une requête de documents. Si des documents ont été identifiés comme manquant localement, alors un récepteur adresse à l'annonceur une requête, lui demandant de diffuser les documents désignés par la liste d'identifiants embarquée dans la requête (lignes 11, 17, et 20 dans l'algorithme 2). Cette requête est encapsulée dans un message de contrôle adressé à l'annonceur. **La couche protocolaire inférieure CICM de notre système doit donc permettre l'acheminement d'une requête vers un destinataire désigné.** Cette fonctionnalité sera examinée en détail dans le paragraphe 2.5.2.

Afin d'illustrer le mécanisme de requête de document, la séquence d'événements présentée dans la figure 2.8 fait suite au scénario de la figure 2.7 présentant le mécanisme d'annonce périodique. L'annonce diffusée par t_1 dans son k -voisinage est reçue par les terminaux t_2, t_3, t_4 et t_5 qui mettent alors à jour leur table du voisinage en y insérant le terminal t_1 et les informations contenues dans son annonce. Ils procèdent au traitement du catalogue $cat(t_1)$ qui, rappelons-le, a été construit en fonction de $prof(t_3)$ et $prof(t_5)$. Au cours de ce traitement, les terminaux t_2, t_3 et t_5 sélectionnent des documents qui leur font défaut : t_3 sélectionne les documents doc_1 et doc_4 ; t_5 sélectionne les documents doc_1 et doc_3 .

Bien que le catalogue $cat(t_1)$ ait été construit uniquement en fonction de $prof(t_3)$ et $prof(t_5)$, le terminal t_2 identifie que le document doc_4 l'intéresse et envoie donc une requête à t_1 pour

le document doc_4 . En effet, lorsque t_1 a construit le catalogue contenu dans l'annonce reçue par ses voisins, il n'avait pas connaissance du profil d'intérêt de t_2 . Toutefois, la diffusion de l'annonce contenant ce catalogue permet à t_2 d'identifier un document correspondant à son profil d'intérêt et lui manquant localement, ce qui illustre l'intérêt de la diffusion périodique des annonces contenant, entre autres les catalogues.

2.4.2.3 TRAITEMENT DES REQUÊTES ET DIFFUSION DE DOCUMENTS

Variables

$requetes(idDoc, voisins)$: historique des requêtes contenant la liste des identifiants des documents sollicités par les voisins.

Δ : délai d'attente avant diffusion de documents demandés par les voisins. Si $k = 1$, $\Delta = 0$ sinon $\Delta \approx k$

\mathcal{C} : cache de documents du terminal.

```

1 sur réception de la requête  $req$ 
2   pour tous les  $idDoc \in req.idDocs$  faire
3     si  $idDoc \notin requetes.idDoc$  alors
4        $requetes[idDoc].voisins \leftarrow req.source$ 
5     sinon
6        $requetes[idDoc].voisins \leftarrow requetes[idDoc].voisins \cup req.source$ 
7 à la fin du délai  $\Delta$ 
8   pour tous les  $idDoc \in requetes.idDoc$  faire
9      $doc \leftarrow \mathcal{C}.récupère(idDoc)$ 
10    diffuser  $doc$  vers  $requetes[idDoc].voisins$ 
```

Algorithme 3 : Traitement des requêtes effectué juste après la diffusion de l'annonce

Suite à la diffusion d'une annonce, le terminal annonceur est susceptible de recevoir une ou plusieurs requêtes, auxquelles il devra répondre en diffusant dans son k-voisinage les documents demandés (algorithme 3). Il faut toutefois noter que la diffusion globale à k-sauts d'un document sollicité par un nombre limité de voisins peut entraîner une surconsommation des ressources. Afin de limiter ce phénomène, nous proposons d'éviter la diffusion globale en utilisant à la place un protocole de diffusion sélective. Pour être en mesure de mettre ce type de protocole en place, il est nécessaire qu'un terminal diffusant un document précise la liste de ses demandeurs afin que ce document puisse leur parvenir. Un terminal annonceur doit donc attendre d'avoir reçu toutes les requêtes qui lui ont été adressées par ses voisins. Pour ce faire, suite à la diffusion de son annonce, le terminal annonceur doit attendre un certain délai Δ avant de répondre aux différentes requêtes. Ce délai d'attente est proportionnel au nombre de sauts devant être parcourus par l'annonce car les requêtes peuvent provenir de voisins distants. Durant ce délai, un annonceur examine chaque requête reçue. Pour tout document demandé, il construit la liste de terminaux demandeurs dans un historique (lignes 1-6 dans l'algorithme 3).

Cet historique est remis à zéro lorsque le terminal diffuse sa propre annonce. Une fois le délai d'attente écoulé, l'annonceur extrait du cache chaque document demandé, et le diffuse le long d'un arbre permettant de satisfaire la liste de demandeurs qu'il a identifiés (lignes 7-10 dans l'algorithme 3). La diffusion d'un document permet de satisfaire tous les voisins intéressés en une seule fois, et le traitement des requêtes après un certain délai permet d'éviter d'envoyer successivement le même document vers chaque demandeur, ce qui permet de réaliser des économies de ressources. **La couche protocolaire inférieure CICM de notre protocole doit permettre la diffusion sélective d'un document vers de multiples terminaux.** Cette fonctionnalité de la couche CICM sera examinée en détails au paragraphe 2.5.3.

Variables

$requetes(idDoc)$: historique des requêtes contenant identifiants des documents sollicités par les voisins.

Δ : délai d'attente avant diffusion de documents demandés par les voisins. Si $k = 1$, $\Delta = 0$ sinon $\Delta \approx k$

\mathcal{C} : cache de documents du terminal.

```

1 sur réception de la requête  $req$ 
2   pour tous les  $idDoc \in req.idDocs$  faire
3     si  $idDoc \notin requetes.idDoc$  alors
4        $doc \leftarrow \mathcal{C}.récupère(idDoc)$ 
5        $requetes \leftarrow requetes \cup idDoc$ 
6       diffuser  $doc$ 

```

Algorithme 4 : Traitement des requêtes avec délais d'attente nul

Lorsque les terminaux sont configurés pour ne communiquer qu'à un seul saut, c'est-à-dire uniquement avec leurs voisins direct, le délai d'attente peut être nul (algorithme 4). Dans ce cas, les requêtes sont traitées séquentiellement : pour chaque document demandé par un voisin, le terminal extrait ce document de son propre cache, et le diffuse dans son voisinage direct (lignes 2-6 dans l'algorithme 4). Il est à noter que le document demandé est diffusé plutôt qu'adressé uniquement au demandeur. En effet, ce choix se justifie par le fait qu'ayant proposé un ensemble de documents à ses voisins, un annonceur peut recevoir de la part de plusieurs voisins des requêtes pour ce même document. Pour éviter que des requêtes successives entraînent des rediffusions inutiles de ce même document, chaque terminal maintient un historique des documents récemment diffusés sur demande des voisins et consulte cet historique à chaque nouvelle demande afin d'éviter de redifuser plusieurs fois le même document sur le canal radio (ligne 3-6 dans l'algorithme 4). Cet historique est remis à zéro lors de l'émission d'une annonce. Ainsi lorsque plusieurs voisins sollicitent la diffusion du même document en réponse à la diffusion d'un catalogue, ce document est diffusé une et une seule fois sur le médium radio.

La séquence de diffusion de documents présentée dans la figure 2.9 illustre le mécanisme de diffusion sélective qui sera présenté en détail dans le paragraphe 2.5.3. Lorsque le délai d'attente est écoulé, le terminal t_1 traite les requêtes qu'il a reçues de ses voisins suite à sa dernière

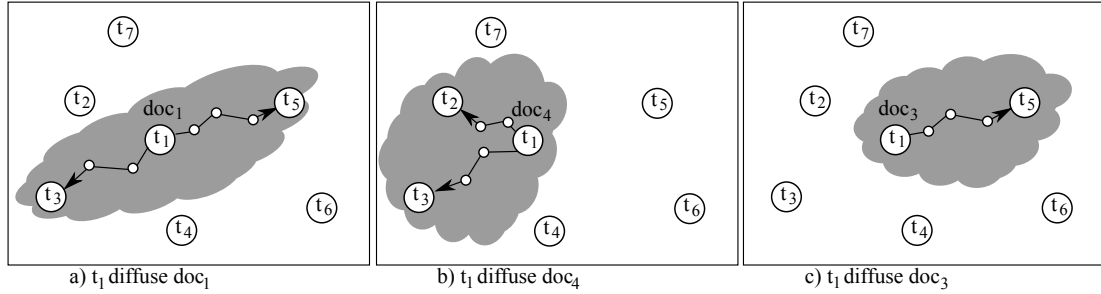


Figure 2.9 – Illustration du mécanisme de diffusion de documents à k-sauts. Les noeuds figurant sur les flèches sont des terminaux mobiles contribuant à relayer les documents vers leurs destinataires. Les terminaux situés hors de la zone grise figurant autour de chaque émetteur ne reçoivent pas les documents.

annonce. Le terminal t_1 extrait de son cache une copie de chaque document demandé. Chacun des documents doc_1 , doc_4 et doc_3 est alors diffusé le long d'un arbre permettant d'atteindre les terminaux qui en ont fait la demande. doc_1 est ainsi diffusé le long d'un arbre atteignant t_3 et t_5 , doc_4 est diffusé le long d'un arbre atteignant le terminal t_3 et t_2 , et doc_3 est diffusé vers t_5 .

2.4.2.4 RÉCEPTION (ATTENDUE OU FORTUITE) DE DOCUMENTS DIFFUSÉS

Variables

altruiste : booléen fixé à Vrai si le terminal a un comportement altruiste réactif ou proactif

$prof(t_i)$: profil d'intérêt du terminal.

\mathcal{C} : cache de documents du terminal.

$voisinage(voisin, (ref, profil, ddu, idDocs))$: table du voisinage maintenue par le terminal.

```

1 sur réception du document doc
2   pour tous les  $v \in voisinage.voisin$  faire
3      $voisinage[v].idDocs \leftarrow voisinage[v].idDocs - doc.idDoc;$ 
4    $\mathcal{C}.déposer(doc);$ 
5   si doc correspond  $prof(t_i)$  alors
6      $pubsubService.notifier(doc);$ 

```

Algorithme 5 : Réception d'un document

La diffusion des documents, à un ou plusieurs sauts, se solde par leur réception par l'ensemble des terminaux situés le long de l'arbre de diffusion. La réception par un terminal ne signifie donc pas qu'il est intéressé par ce document, mais simplement qu'un de ses voisins en a sollicité la diffusion.

L'algorithme 5 présente les opérations réalisées lors de la réception d'un document. La réception d'un document par un terminal se traduit par :

- la suppression de son identifiant de la liste des documents demandés, qui est contenue dans la table du voisinage (lignes 2-3 dans l'algorithme 5),
- la soumission du document au gestionnaire de cache (ligne 4 dans l'algorithme 5) qui prend alors la décision de l'héberger ou non (cet aspect du protocole est détaillé dans le paragraphe 2.4.2.5). Chaque terminal déposant de nouveaux documents dans son cache contribue alors à leur transport et à leur dissémination à travers le réseau,
- le relais du document vers le service pub-sub, si ce document satisfait le profil d'intérêt du terminal (lignes 5 et 6 dans l'algorithme 5). Le service pub-sub identifie les services applicatifs intéressés par le document, puis il relaie ce document vers ces services. Chaque service est alors à même de traiter le contenu du document relayé.

2.4.2.5 CACHE DE DOCUMENTS

Le cache est un espace persistant de stockage de documents, dont la capacité est a priori limitée. Sa mise en œuvre doit être robuste afin de tolérer la volatilité du terminal hôte. Sur chaque terminal, un gestionnaire applique une politique de gestion de cet espace. Il décide du dépôt ou non d'un document dans le cache, et il décide quel document doit être supprimé pour libérer de l'espace de stockage lorsque cela est nécessaire.

Dépôt en cache d'un nouveau document. La réception d'un document par un terminal et la publication d'un document par un service applicatif local se traduisent par une demande de dépôt en cache du document. Lorsque la demande de dépôt fait suite à la réception d'un document depuis le réseau, son dépôt en cache est conditionné par le niveau de sélectivité du récepteur. Bien entendu, si le document est déjà présent en cache, le cache ignore cette demande. Dans le cas contraire, un premier filtrage conditionne la suite du processus. Si le terminal est configuré pour se comporter de manière « altruiste », alors le processus de dépôt continue pour chaque document. Si le terminal est configuré pour se comporter de manière « égoïste », alors le processus continue uniquement pour les documents correspondant à son propre profil d'intérêt (qui est déterminé par les services applicatifs et qui peut évoluer au cours du temps).

Suite à cette première sélection le gestionnaire de cache vérifie si le document peut être hébergé. Si l'espace disponible n'est pas suffisant, alors il cherche à libérer de manière intelligente l'espace mémoire nécessaire à l'hébergement de ce document. Pour ce faire, une fonction de rang (R) est utilisée pour ordonner le cache. Cette fonction est définie de telle manière que les rangs attribués aux documents correspondant au profil d'intérêt sont supérieurs à ceux attribués aux documents transportés de manière altruiste. La fonction permet de déterminer le rang du document qui vient d'être reçu, et de déterminer, le cas échéant, quels documents doivent être supprimés pour libérer l'espace nécessaire. Lorsque le nouveau document a le plus faible rang ou que le volume pouvant être libéré par des documents de rang inférieur n'est pas suffisant, alors le dépôt en cache du document est impossible.

Lorsque la demande de dépôt fait suite à la publication d'un document par un service applicatif local, le processus est différent. En effet, si le document n'est pas déposé en cache alors

il ne pourra pas être propagé dans le réseau. Pour éviter ce phénomène, l'espace mémoire nécessaire au dépôt en cache d'un document venant d'être publié par un service local est libéré au besoin en supprimant les documents de plus faible rang.

D'autres événements peuvent provoquer la suppression de documents du cache. D'une part, chaque document publié par un service applicatif possède une date de péremption au delà de laquelle sa dissémination ne présente plus aucun intérêt. Lorsque cette date est dépassée, le document concerné est supprimé du cache. D'autre part, le désabonnement d'un service applicatif entraîne la mise à jour du profil d'intérêt avec la suppression du prédicat de sélection correspondant. Des documents qui intéressaient le service peuvent donc être supprimés du cache si le terminal n'est pas altruiste. Enfin, la désactivation du mode altruiste par le propriétaire du terminal provoque la suppression du cache de tous les documents ne satisfaisant pas le profil d'intérêt du terminal.

Fonction d'estimation du rang d'un document. Nous avons indiqué plus haut que l'ordonnement du cache est réalisé en exploitant une fonction R qui permet de déterminer le rang r d'un document. Dans notre modèle, cette fonction n'est pas figée : il est possible de la redéfinir à volonté. Cependant, la définition de cette fonction doit respecter la contrainte suivante : le rang affecté à un document correspondant au profil d'intérêt local doit être supérieur au rang d'un document transporté de manière altruiste. Un exemple de fonction de rang est illustré ci-dessous :

$$R(\text{document}) = \frac{\text{nombre de prédicats sélectionnant le document}}{\text{âge du document}} \quad (2.1)$$

Avec cette fonction R , le rang d'un document correspondant au profil d'intérêt local est supérieur à celui d'un document du même âge transporté de manière altruiste (puisque ce dernier ne correspond à aucun prédicat de sélection). En outre, nous supposons ici que le transport d'un document récent présente plus d'intérêt que le transport d'un document plus ancien.

2.5 COUCHE INFÉRIEURE DE COMMUNICATION MULTI-SAUTS

Comme expliqué dans la section précédente, la couche supérieure de notre protocole nécessite qu'un terminal soit en mesure d'envoyer des messages (contenant soit ses profil et catalogue, soit une requête, soit un document) à ses voisins du moment. Le **relais immédiat** de messages — par opposition au relais différé de la couche supérieure — est donc souhaitable afin d'exploiter au mieux la connectivité transitoire existant entre des terminaux qui se trouvent appartenir — peut-être de façon extrêmement fugitive — à un même fragment connexe du réseau.

La couche protocolaire inférieure de notre système a pour vocation de supporter ce type de relais immédiat, qu'il s'agisse de faire parvenir un message à un terminal spécifique situé dans le voisinage de l'émetteur (trafic *unicast*), ou bien à l'ensemble des voisins de cet émetteur (trafic *broadcast*).

Dans le tableau 2.2, nous décrivons les besoins identifiés dans la couche protocolaire CS-DOC en termes de communication multi-sauts, et les algorithmes associés. Les paragraphes

Besoins	Algorithmes requis
Un terminal doit pouvoir diffuser ses propres annonces dans son k-voisinage	Relais immédiat entre terminaux voisins de messages à un horizon de k-sauts (k étant borné) autour de l'émetteur, en exploitant des transmissions élémentaires en mode <i>broadcast</i> .
Un terminal doit pouvoir adresser une requête à l'émetteur d'une annonce	Relais immédiat entre terminaux voisins de messages adressés à un destinataire précis, en exploitant des transmissions élémentaires en mode <i>unicast</i> .
Un terminal doit pouvoir diffuser un document vers un ensemble de demandeurs ciblés	Relais immédiat entre terminaux voisins de messages le long d'un arbre de diffusion sélective, en exploitant des transmissions élémentaires en mode <i>broadcast</i> , afin d'atteindre un sous-ensemble de terminaux situés dans le k-voisinage de l'émetteur.

Table 2.2 – Besoins de la couche CSDOC en termes d'algorithmes de communication multi-sauts mis en œuvre dans la couche CICM

suivants présentent en détail les protocoles de relais immédiat que nous avons définis pour répondre à nos besoins.

2.5.1 PROTOCOLE DE DIFFUSION VIA DES RELAIS MULTI-POINTS

La couche inférieure de notre protocole met en œuvre, pour la diffusion à k-sauts de messages entre terminaux d'un même îlot de connectivité, un mécanisme inspiré du relais multi-points (MPR : *Multi-Point Relay*) [QVL02]. Ce mécanisme MPR est, à l'origine, exploité dans l'algorithme de routage proactif OLSR (*Optimized Link State Routing*) [CJ03], où il est utilisé pour diffuser dans le réseau des informations portant sur l'état des liens de transmission entre terminaux voisins. Il permet de limiter fortement le coût de diffusion d'un message, qui si l'on n'y prend garde, peut être une opération très coûteuse en termes de bande passante dans un MANET et peut même parfois engendrer le problème dit « d'orage de diffusion » (*Broadcast Storm Problem*) [NTCS99].

L'algorithme utilisé par chaque terminal pour sélectionner parmi ses voisins ceux qui vont servir de relais multi-points n'est décrit ci-dessous que très sommairement, dans la mesure où il s'agit d'un algorithme emprunté au protocole OLSR, et qu'à ce titre il a déjà été abondamment décrit et validé dans la littérature [QVL02]. Il a notamment été démontré que, dans un réseau MANET suffisamment dense, l'approche consistant à faire réaliser la diffusion par des MPRs est nettement moins coûteuse que celle qui consiste à réaliser une simple inondation, chaque terminal ré-émettant simplement chaque message sur le médium radio lorsqu'il le reçoit pour la première fois [QVL02].

Le mécanisme de diffusion via les MPR repose sur un algorithme visant à sélectionner parmi les voisins directs d'un terminal un sous-ensemble minimal de voisins qui lui permet de joindre l'ensemble de ses voisins à deux sauts. La principale difficulté de ce mécanisme réside dans la sélection de ces relais. Ce sous-ensemble est nommé MPR. Par exemple, dans le réseau représenté sur la figure 2.10, le MPR du terminal A est l'ensemble constitué des terminaux C, F et G qui, lors de la diffusion d'un message à deux sauts par le terminal A, sont les seuls terminaux à relayer ce message. La figure 2.10 illustre la diffusion autour du terminal A, réalisé via le MPR et via l'inondation à deux sauts. Il est à noter que l'utilisation de la diffusion via les MPR nécessite quatre émissions du message, alors que, dans le cas de l'inondation, sept émissions sont nécessaires. D'autre part, la diffusion par les MPRs permet de réduire les multiples réceptions d'un même message par les terminaux. Ainsi dans la figure 2.10, on observe 7 réceptions avec les MPR, et 17 réceptions avec l'inondation. L'utilisation de la diffusion par MPR nous permet donc de réaliser des économies de bande passante et d'énergie à travers la minimisation des émissions et des réceptions.

Dans le protocole de routage OLSR, les MPRs sont exploités lors de la diffusion périodique dans le réseau — supposé connexe — d'informations de contrôle concernant des états de liens de transmission entre voisins. Ces informations sont utilisées par chaque terminal pour la maintenance de sa propre table de routage. L'algorithme exploité dans OLSR pour la sélection des MPRs nécessite la diffusion périodique de messages de contrôle par chaque terminal. Chaque message de contrôle contient l'identité de l'émetteur et la liste de ses voisins directs. De la sorte, chaque voisin de l'émetteur d'un message de contrôle met à jour sa propre table de voisinage, et est en mesure de calculer l'ensemble de ses MPRs. Suite à cette sélection, chaque terminal ajoute dans son message de contrôle la liste des terminaux devant se comporter comme relais multi-points des messages qu'il diffuse. Ainsi, lors de la réception d'un message diffusé, un terminal vérifie s'il est MPR de l'émetteur, et si tel est le cas, il re-diffuse alors immédiatement ce message.

Dans notre cas, nous ne souhaitons pas ajouter de nouveaux messages de contrôle pour mettre en œuvre les MPRs, car ceci entraînerait inévitablement un surcoût en termes de consommation de ressources. Nous avons défini, dans la couche supérieure de notre protocole, un mécanisme de diffusion périodique d'annonces, qui permet à un terminal de se faire connaître de ses voisins. Nous exploitons donc cette annonce périodique dans la couche inférieure de notre protocole afin de permettre à chaque terminal mobile de percevoir son voisinage direct, ainsi que son voisinage à deux sauts. Pour ce faire, la couche inférieure du protocole insère, dans le descripteur de chaque annonce diffusée, la liste des voisins directs connus de l'annonceur. Ainsi, les terminaux voisins directs d'un annonceur prennent connaissance de leur voisinage direct et de leur voisinage à deux sauts. Ces informations ainsi collectées (et mises à jour) vont permettre à chaque terminal de calculer ses propres MPRs.

À la différence de OLSR, dans notre protocole, les terminaux n'informent pas les terminaux qu'ils ont sélectionnés en tant que MPR. Lors de la diffusion d'une annonce à k -sauts radio ($k > 1$), la couche inférieure de notre protocole précise dans le descripteur de l'annonce le nombre de sauts k qu'elle doit parcourir, et la liste des terminaux devant la relayer immédiatement. Par ailleurs, c'est à cet instant que le calcul permettant de déterminer le MPR du terminal est effectué. Lorsqu'un terminal s'identifie comme MPR d'une annonce reçue, il doit rediffuser

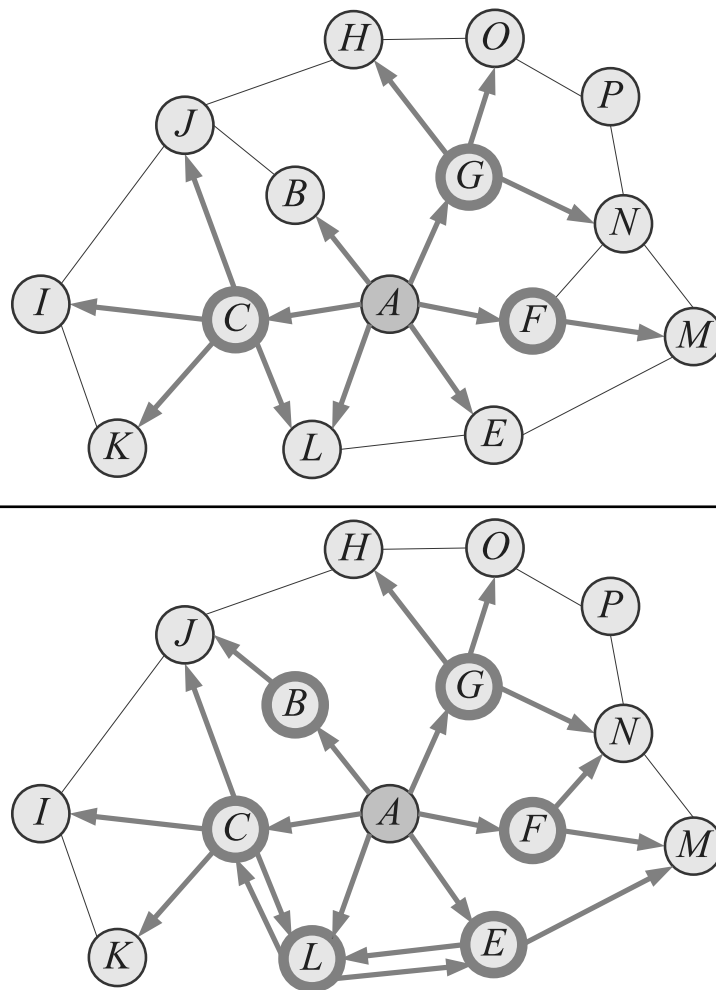


Figure 2.10 – Illustration d'une diffusion à deux sauts via l'exploitation de relais multi-points (en haut) et via une simple inondation (en bas). Pour que le message puisse atteindre l'ensemble des voisins à deux sauts du terminal A, les terminaux représentés par des cercles en gras doivent rediffuser le message émis par le terminal A.

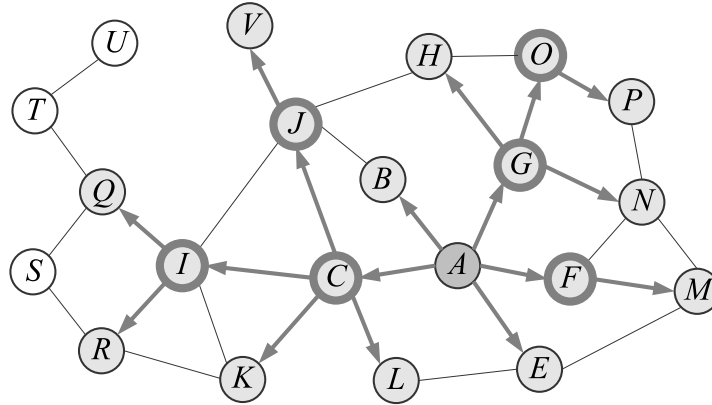


Figure 2.11 – Illustration du mécanisme de diffusion exploitant les relais multi-points

l'annonce. En outre, si le nombre de saut devant être parcourus par l'annonce est supérieur à un, alors le terminal relais remplace la liste des MPRs contenue dans le descripteur du document par ses propres MPRs, sinon il supprime la liste de MPRs contenue dans le descripteur. Finalement, il diffuse le message contenant l'annonce dans son propre voisinage.

La figure 2.11 illustre ce mécanisme. Dans cet exemple le terminal A diffuse un message, qui pourrait par exemple être une annonce contenant son profil d'intérêt et le catalogue des documents qu'il met à disposition de ses voisins. Chaque copie du message n'est autorisée à se propager que sur trois sauts consécutifs, ce qui explique pourquoi les terminaux S, T et U, qui sont situés trop loin de A bien qu'appartenant au même îlot que lui, ne reçoivent pas son annonce. On peut observer dans la figure que seuls certains voisins du terminal A réémettent effectivement le message lorsqu'il le reçoivent. Dans ce cas précis, il s'agit des terminaux C, F, et G, qui font office de relais multi-points pour le premier saut réalisé par le message, et des terminaux I, J, et O, servant de relais multi-points pour le second saut du message.

2.5.2 PROTOCOLE DE ROUTAGE PAR LA SOURCE

Notre protocole de dissémination nécessite que les terminaux soient capable d'émettre une requête en réponse à une annonce qu'ils viennent de recevoir. Bien sûr, cette requête est adressée à l'émetteur de l'annonce. Lorsqu'un terminal envoie une requête à un destinataire présent dans son k-voisinage, la couche inférieure de notre protocole doit déterminer le chemin par lequel doit transiter ce message de contrôle pour pouvoir être remis à son destinataire.

Le protocole que nous proposons pour l'acheminement des requêtes repose sur le principe du routage par la source proposé pour le routage dynamique dans les MANETs connexes. Dans ce type de protocole, l'émetteur d'un message spécifie explicitement quel trajet ce message doit suivre dans le réseau pour atteindre son destinataire. Ce type de protocole de routage nécessite une phase de découverte des routes entre terminaux sources et destinations. Dans notre cas, un terminal a besoin d'acheminer un message vers une destination précise lorsqu'il adresse une requête à un terminal ayant diffusé une annonce. Il suffit donc que la requête suive le chemin

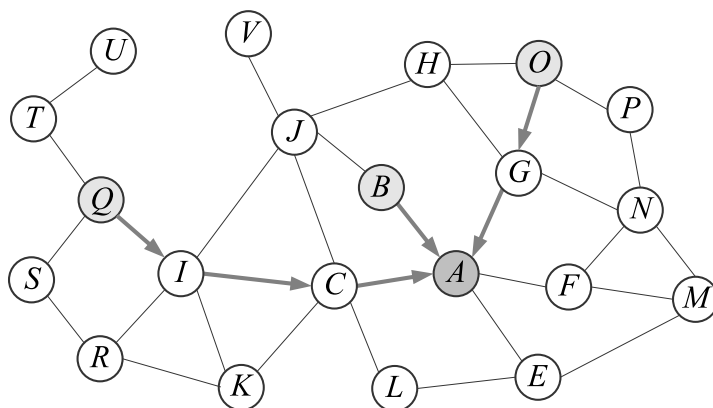


Figure 2.12 – Illustration du mécanisme de routage par la source

inverse de celui parcouru par l'annonce. Néanmoins, pour que cette approche fonctionne dans un réseau dont les terminaux sont fortement dynamiques, il est nécessaire qu'une requête soit émise sans attendre. Dans de telles circonstances, le chemin que doit parcourir la requête est encore praticable.

Pour mettre en œuvre ce principe, chaque terminal relayant une annonce ajoute son identité au début d'une liste de relais présente dans le descripteur de l'annonce. Lorsqu'un terminal reçoit une annonce, il mémorise temporairement la liste de relais dans une table de routage. De la sorte, si un terminal adresse une requête à l'émetteur d'une annonce qu'il vient de recevoir, il est en mesure de préciser dans la requête le chemin précis que celle-ci devra suivre. Ce chemin est inséré dans le message de contrôle contenant la requête de document, et indique aux terminaux identifiés qu'ils doivent relayer immédiatement le message vers le prochain terminal relais. Ainsi, de proche en proche, une requête « remonte » vers le terminal destinataire pour y être traitée.

Considérons de nouveau l'exemple du message d'annonce diffusé par le terminal A dans la figure 2.11, et supposons que les terminaux B, Q, et O décident de répondre à ce message. La figure 2.12 illustre comment ces réponses peuvent se propager en remontant le chemin que le message diffusé vient juste de « descendre », chaque réponse contenant la description explicite du cheminement qu'elle doit suivre afin d'atteindre le terminal A. Par exemple, la requête adressée à A par le terminal Q contient la route I, C. Celle-ci indique au terminal Q qu'il doit envoyer le message au terminal I, ce dernier le relaie à son tour au terminal C qui le relaie au terminal A.

Un seul événement extérieur peut nuire à l'envoi d'une requête, une route peut en effet devenir inexploitable suite à l'arrêt ou la mise en veille d'un terminal relais ou destinataire. Pour éviter d'envoyer une requête vers un terminal inactif, avant de l'émettre sur le médium, un terminal vérifie la présence du destinataire dans sa table de routage. Il est à noter que cette table de routage est mise à jour lorsqu'un terminal reçoit un message de contrôle indiquant l'arrêt d'un voisin, et que toutes les routes contenant le terminal en question sont supprimées de la table.

2.5.3 PROTOCOLE DE DIFFUSION SÉLECTIVE

Nous avons défini dans la couche inférieure de notre système un protocole de diffusion sélective. Ce mécanisme permet au terminal émetteur d'un message de « guider » ce message vers des terminaux précis, en réduisant la consommation de ressources. Ce « guidage » repose sur la définition par l'émetteur d'un message d'un arbre de diffusion permettant d'atteindre l'ensemble des destinataires de ce message. Ainsi, les terminaux impliqués dans le relais d'un message sont uniquement ceux « utiles » à son acheminement. De la sorte, les émissions et les réceptions sont réduites au strict nécessaire ce qui, en comparaison de la diffusion via les MPRs permet d'économiser des ressources. D'autre part, l'utilisation de la diffusion sélective permet de limiter les *spams* (réceptions non souhaitées), et convient donc à notre principe d'utilisation frugale des ressources.

La diffusion sélective de documents est exploitée par les terminaux pour répondre aux demandes de leurs voisins. Pour déterminer l'arbre de diffusion permettant d'atteindre un ensemble de demandeurs, un terminal doit connaître chaque chemin permettant d'atteindre chaque demandeur. De la même manière que pour le protocole de routage par la source défini dans le paragraphe 2.5.2, le chemin parcouru par une requête est embarqué dans le message de contrôle lui correspondant. De la sorte, un terminal recevant une requête apprend le chemin permettant d'atteindre un demandeur, en enregistrant dans sa table de routage le chemin contenu dans cette requête. Il est à noter que la table du voisinage d'un terminal est purgée lorsqu'il diffuse sa propre annonce périodique puisque la diffusion d'un document présuppose la réception d'une requête.

Lorsqu'un terminal répond aux requêtes de ses voisins en diffusant de manière successive des documents, il calcule pour chaque document l'arbre de diffusion permettant d'atteindre tout ou partie des terminaux ayant sollicité la diffusion de ce document, car certains d'entre eux peuvent ne plus être présents ou atteignables au moment de la diffusion du document. L'arbre de diffusion est calculé en fusionnant les chemins correspondant aux demandeurs, ces chemins étant maintenus dans la table de routage du terminal émetteur. Cet arbre de diffusion est ensuite inséré dans le descripteur du document à diffuser. Il indique à chaque terminal récepteur faisant partie de la liste des terminaux identifiés dans l'arbre de diffuser le document à son tour.

La figure 2.13 fait suite à l'exemple de la figure 2.12 dans lequel nous avons illustré le routage par la source des requêtes adressées au terminal A par les terminaux B, O et Q. Supposons maintenant que l'ensemble des requêtes soient parvenues au terminal A. Les terminaux B et O demandent la diffusion du document doc_A , et le terminal Q demande la diffusion d'un autre document doc_B .

En réponse aux requêtes de B et O, le terminal A diffuse le doc_A en indiquant qu'il doit atteindre les terminaux B et O. La couche inférieure de notre protocole détermine l'arbre de diffusion permettant de les atteindre en fonction des deux chemins de leurs requêtes respectives. A diffuse donc doc_A , qui est réceptionné par les terminaux B, C, L, E, F et G qui identifie alors qu'il doit relayer immédiatement doc_A afin qu'il puisse être réceptionné par O.

En réponse à la requête de Q, le terminal A diffuse le doc_B en précisant que son demandeur est Q. La couche inférieure de notre protocole détermine l'arbre de diffusion permettant

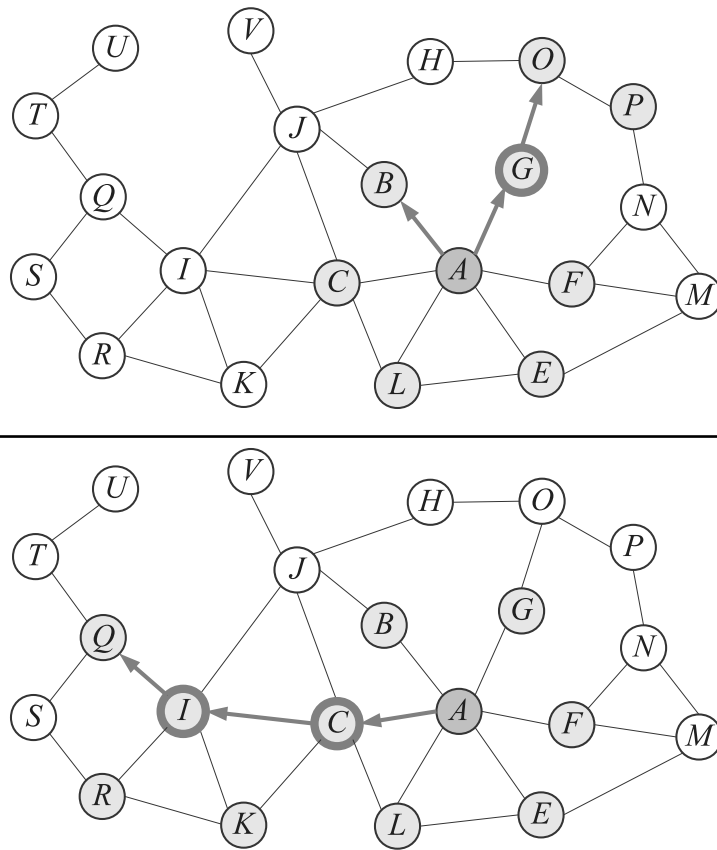


Figure 2.13 – Illustration du mécanisme de diffusion sélective exploitant des arbres de diffusion. En haut, l'arbre de diffusion exploité lors de la diffusion de doc_A . En bas, l'arbre de diffusion exploité lors de la diffusion de doc_B . Les nœuds du graphe entourés par un trait épais sont ceux désignés par A comme devant relayer les documents, tandis que les nœuds gris sont ceux recevant finalement les documents.

d'atteindre Q en récupérant le chemin depuis la table de routage du terminal émetteur. Les terminaux C et I, relaient successivement le doc_B afin qu'il puisse finalement être réceptionné par Q. Lors de son acheminement, ce document est réceptionné par les terminaux B, G, F, L, K, J et R qui n'étaient pas demandeurs du document. Néanmoins, comme nous l'avons déjà évoqué, la diffusion d'un document via les arbres est nettement moins coûteuse qu'une diffusion via les MPRs (ou par inondation). L'acheminement du document doc_B nécessite trois diffusions via les arbres contre six via les MPRs, et implique dix réceptions via les arbres contre dix-sept réceptions via les MPRs. Cet exemple montre que l'utilisation d'arbre pour la diffusion de document permet de réaliser des économies d'énergie et de bande passante.

Pour que ce mécanisme de diffusion sélective fonctionne, il est nécessaire que le délai d'attente avant le traitement des requêtes soit bien choisi. En effet, ce délai ne doit pas être trop court afin de permettre aux terminaux situés à k -sauts d'un annonceur de lui faire parvenir leurs requêtes, et il ne doit pas être trop long car les chemins suivis par les requêtes ne sont que temporairement valides. La portée de diffusion d'une annonce est un paramètre à prendre en compte lors du calcul permettant de déterminer le délai d'attente.

2.6 DISCUSSION

Dans ce chapitre, nous avons proposé un protocole fondé sur la dissémination sélective de messages en fonction de leur contenu. Dans ce modèle de communication, les messages ou plutôt les documents ne sont plus acheminés en fonction de leur destination mais en fonction de leur contenu : la communication est dite basée sur le contenu. Pour ce faire, chaque terminal dispose d'un cache permettant le stockage de document, et d'un profil d'intérêt. Le profil d'intérêt d'un terminal caractérise le type de messages qui l'intéresse et donc, implicitement, le type de messages qu'il souhaite recevoir, et pour lesquels il est également prêt à jouer le rôle de transporteur mobile. Les services applicatifs adaptent le profil d'intérêt d'un terminal en fonction de leurs propres besoins et des centres d'intérêts de l'utilisateur. Les contacts transitoires entre terminaux voisins appartenant temporairement au même îlot de connectivité sont exploités de manière opportuniste afin d'échanger des documents, en tenant compte de leurs profils d'intérêt respectifs, et de ceux dont ils disposent déjà. Avec pour objectif d'améliorer les performances de notre protocole de communication, nous avons développé des protocoles de relais immédiats inspirés de ceux proposés pour le routage dynamique dans les MANETs. Lorsque nous avons conçu ces protocoles nous avons cherché à minimiser leurs impacts sur le coût du protocole, en théorie ils permettent de le réduire de manière significative.

Nous soutenons en outre que le protocole que nous avons développé peut fonctionner sans difficulté majeure dans les environnements que nous ciblons (réseaux de grande envergure, réseaux déployés pour une courte durée, etc.), dans la mesure où il ne s'appuie justement pas sur le maintien d'historique de contacts ou de déplacements. En fait, dans notre système chaque terminal ne maintient que très peu d'information d'état concernant ses voisins à chaque instant, et oublie ces informations dès qu'un voisin passe hors de portée radio. Les principales limitations de ce système résident dans le nombre de voisins qu'un terminal peut gérer à tout instant

(mais cette contrainte est essentiellement liée aux caractéristiques mêmes de la technologie radio sous-jacente), et dans le nombre et la taille des documents qu'ils peut échanger avec ses voisins avant que ceux-ci ne soient plus accessibles.

Nous avons réalisé une implémentation de ce protocole de communication dans un intergiciel que nous avons nommée *DoDWAN* (pour *Document Dissemination in mobile Wireless Ad hoc Network*). Cette plate-forme de communication permet à d'autres logiciels d'exploiter la communication opportuniste basée sur le contenu. Le chapitre suivant fait l'objet d'une présentation de cette plate-forme et de quelques services applicatifs de démonstration.

Cette plate-forme a autorisé l'évaluation du protocole proposé au cours de plusieurs campagnes de tests, qui ont permis d'observer son comportement sous différentes conditions. Ces campagnes ont été réalisées dans des conditions d'expérimentation réelles, notamment sur une plate-forme militaire, et à l'aide d'un simulateur de réseau mobile. Les résultats expérimentaux qui attestent du fonctionnement de notre modèle sont proposés dans le chapitre 4. Dans ce chapitre, nous aurons l'occasion de présenter des résultats quantitatifs justifiant nos choix.

3

LA PLATE-FORME DE COMMUNICATION DoDWAN

L'architecture générale et le protocole de communication décrits dans le chapitre 2 de ce mémoire sont mis en œuvre dans la plate-forme intergicielle DoDWAN (pour *Document Dissemination in mobile Wireless Ad Hoc Network*). Le prototype que nous avons développé permet d'assurer la communication opportuniste basée contenus entre des services applicatifs s'exécutant sur des terminaux mobiles communicants volatiles.

Dans ce chapitre, nous présentons, dans le paragraphe 3.1, une vue d'ensemble de l'intergiciel DoDWAN, qui fournit les outils nécessaires à des services applicatifs pour exploiter le modèle de communication tel que nous l'avons défini dans le chapitre 2. Les paragraphes 3.2 et 3.3 décrivent respectivement la mise en œuvre de la couche inférieure et de la couche supérieure de notre protocole de communication. Puis, dans le paragraphe 3.4, nous présentons des exemples de services applicatifs de démonstration. Ces services applicatifs ont été développés dans le cadre de différents projets menés par l'équipe CASA du laboratoire VALORIA.

3.1 VUE D'ENSEMBLE DE DoDWAN

La plate-forme intergicielle DoDWAN, dont une vue d'ensemble est présentée dans la figure 3.1, est le résultat de l'implémentation dans le langage de programmation à objets Java du modèle de communication décrit dans le chapitre 2. Cette plate-forme s'exécutant en tâche de fond sur chaque terminal, permet à des services applicatifs de communiquer. Elle a été conçue afin d'aider à la mise en œuvre de services applicatifs capables de fonctionner dans les réseaux mobiles ad hoc discontinus et d'exploiter le modèle de communication atypique que nous proposons. Dans ce sens, DoDWAN offre une API de type *publish-subscribe* qui permet de développer aisément des services applicatifs. Cette API est présentée en détail dans le paragraphe 3.3.4.

Bien que la plate-forme de communication DoDWAN puisse être perçue comme un intergiciel orienté message (*Message Oriented Middleware*), elle se distingue toutefois d'autres produits tels que *Java Message Service* [HBS⁺02] ou *Emma* [MMH05] par le fait que les objets manipulés sont en fait des documents et non de simples messages (paragraphe 3.1.1). Dans DoDWAN, le traitement d'un document dépend des caractéristiques mêmes de ce document et

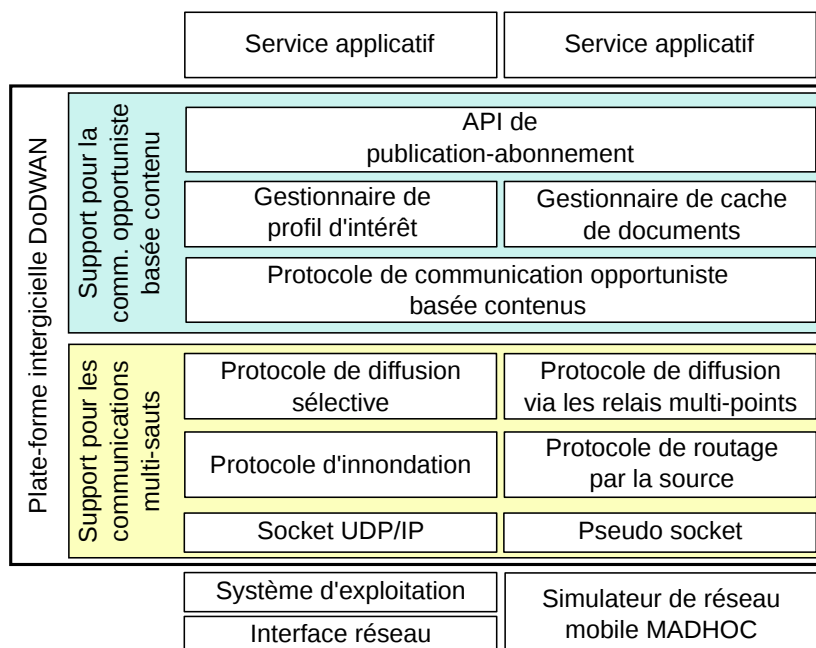


Figure 3.1 – Vue d'ensemble de la plate-forme intergicielle DoDWAN

non uniquement d'une destination désignée. DoDWAN permet aux services applicatifs de déterminer les différents types de documents les intéressant grâce à l'utilisation d'un langage de souscription présenté dans le paragraphe 3.1.2.

3.1.1 DOCUMENTS

Toutes les unités de transmission manipulées par l'intergiciel DoDWAN, c'est-à-dire à la fois celles contenant des données applicatives et celle contenant des données de contrôle (annonces, requêtes, etc.), sont des documents structurés en deux parties : un descripteur et un contenu.

Le descripteur est une collection d'attributs. Tout descripteur de document doit contenir certains attributs obligatoires : un identifiant unique (*attribut id*) qui est généré de manière automatique (paragraphe 3.1.1.2), ainsi qu'une date de péremption (*attribut deadline*) qui doit être fixée par le service applicatif publiant le document. Nous verrons plus loin que d'autres attributs prédéfinis existent, qui permettent par exemple de différencier les document contenant des données de contrôle des documents publiés par les services applicatifs, ou encore d'indiquer comment un document doit être relayé.

Des informations complémentaires caractérisant le contenu d'un document peuvent également être librement spécifiées par le service applicatif qui le publie, ces informations étant ajoutées sous la forme d'attributs complémentaires qui vont aider à guider son acheminement dans le réseau. Dans l'exemple présenté dans la figure 3.2, les attributs déterminés par le service éditeur indiquent que le document considéré a été publié dans le cadre d'un service de partage

<i>Descripteur du document D1</i> <pre> <descriptor id="5be62d77..06f628348" deadline="2010-07-10T14:00:00"> <date>2010-07-08T09:52:11</date> <service>filesharing</service> <mimetype>application/pdf</mimetype> <publisher>Fred</publisher> <keywords>mobile, ad hoc, delay-tolerant, opportunistic</keywords> </descriptor> </pre>
<i>Charge utile sous forme binaire</i>

Figure 3.2: Exemple de document publié dans le cadre d'un service de partage de fichier.

de fichier (attribut *service*), et que son contenu est un document PDF (attribut *mimetype*) qui est en outre caractérisé par les mots clés « *mobile, ad hoc, delay-tolerant, opportunistic* ».

3.1.1.1 FORMAT DES DESCRIPTEURS

Les descripteurs des documents manipulés par DoDWAN sont formatés en XML (comme illustré dans la figure 3.2) tandis que le contenu du document est au format binaire. Le langage XML étant un langage à balises, des informations formatées en XML sont presque toujours plus volumineuse que ces mêmes informations formatées dans un format binaire comparable (comme par exemple un format similaire à celui du standard pour le format des messages texte Internet ARPA [RFC822]). L'utilisation de l'algorithme de compression sans perte LZ77 [ZL77] permet de réduire cet écart. Ainsi, tout document publié par DoDWAN est systématiquement compressé afin de réduire le volume de données émis sur le médium radio. Nous avons cependant choisi d'utiliser le format XML pour des raisons qui sont précisées dans le paragraphe 3.1.2.

3.1.1.2 IDENTIFIANT UNIQUE D'UN DOCUMENT

L'identifiant unique permet de différencier les documents, notamment lors de leur mise en cache, et d'éviter à un terminal de se procurer inutilement de multiples copies d'un même document.

Dans la plate-forme DoDWAN, la génération des identifiants des documents est réalisée en calculant l'empreinte MD5 (*Message-Digest algorithm 5* [Riv92]) du document publié (descripteur et contenu), et en s'appuyant sur le fait que le condensat MD5 d'un document est unique (sous réserve de collision¹). Pour limiter le risque de collision, d'autres solutions sont envisageables comme, par exemple, l'intégration dans l'identifiant de l'adresse MAC de l'hôte émetteur (ou de son numéro IMEI s'il s'agit d'un *smartphone*), de la date d'émission prise à la milliseconde près, etc.

1. Une collision consiste à obtenir le même condensat à partir de deux documents (ou fichiers) différents, ce risque est très faible. De plus il n'existe semble-t-il pas encore d'applicatifs permettant de soumettre un document (ou fichier) afin qu'il lui soit ajouté ce qu'il faut pour que son MD5 soit égal à un MD5 de référence (forger un MD5).

```

Prédicat de sélection P1
descriptor[
    service    ='filesharing'
    and        publisher='Fred'
    and        contains(keywords,'mobile')
]

```

Figure 3.3: Exemple de prédicat de sélection, applicable à un descripteur de document, exprimé dans un langage d'interrogation de document XML XPath.

```

Descripteur réduit du document D1
<descriptor id="5be62d77..06f628348"
deadline="2010-07-10T14:00:00">
  <service>filesharing</service>
  <publisher>Fred</publisher>
  <keywords>mobile, ad hoc,\
delay-tolerant, opportunistic</keywords>
</descriptor>

```

Figure 3.4: Le descripteur réduit obtenu en appliquant le prédicat XPath P1 au descripteur XML du document D1.

3.1.2 PRÉDICAT DE SÉLECTION

Dans notre protocole de communication, la différenciation de l'information est réalisée en fonction des méta-données présentes dans le descripteur de document. Comme indiqué dans le paragraphe 2.4.1, l'intérêt d'un terminal pour un document donné est évalué en appliquant un prédicat de sélection au descripteur de ce document. Dans notre mise en œuvre, les prédicats de sélection sont des expressions XPath [CD⁺99] (*XML Path Language*). Ce langage répond parfaitement aux besoins identifiés dans le paragraphe 2.4.1.2. XPath permettant de faire des requêtes sur des documents au format XML, cette caractéristique a motivé notre choix d'une représentation XML des descripteurs de documents.

Un exemple de prédicat XPath est présenté dans la figure 3.3. Ce prédicat permet de sélectionner des documents publiés par « Fred » dans le cadre des services de partage de fichier ou de discussion thématique, à condition toutefois que ces documents soient caractérisés par le mot clé « *mobile* ».

L'application d'un prédicat XPath à un document XML permet donc de savoir si le prédicat sélectionne le document. De plus, lorsqu'un document XML correspond à un prédicat XPath, il est possible d'extraire tous les nœuds du document XML qui correspondent aux critères de sélection exprimés dans le prédicat. Cette possibilité permet de construire aisément un catalogue compact en fonction des profils d'intérêt des voisins, en ne retenant dans un catalogue que des attributs significatifs pour ces voisins

Par exemple, dans la figure 3.4 est présenté un descripteur réduit, qui résulte de l'application du prédicat P1 (figure 3.3) au descripteur du document D1 (figure 3.2). On remarque ici que

seuls les attributs correspondant aux critères exprimés dans P1 sont présents dans le descripteur réduit de la figure 3.4. De la sorte, il est aisé de construire les descripteurs réduits de documents à insérer dans le catalogue proposé dans chaque annonce complète.

3.2 COMMUNICATION MULTI-SAUTS ENTRE TERMINAUX VOISINS

La couche inférieure de notre protocole de communication a été décrite dans le paragraphe 2.5. Nous présentons les choix que nous avons faits pour la mise en œuvre de la communication multi-sauts entre équipements mobiles appartenant à un même îlot du réseau.

3.2.1 SOCKETS DE COMMUNICATION

La plate-forme de communication DoDWAN doit satisfaire deux objectifs. D'une part, elle doit permettre de développer et expérimenter des services applicatifs sur de « vrais » équipements mobiles équipés d'interfaces radio de type WiFi fonctionnant en mode ad hoc. D'autre part, elle doit permettre de tester le protocole de communication qu'elle implémente dans un environnement « virtuel contrôlé », c'est-à-dire à l'aide d'un simulateur de réseau mobile.

Pour répondre à ce double objectif, l'intergiciel DoDWAN a été conçu de sorte à ce qu'il exploite une socket de communication UDP/IP lorsqu'il s'exécute sur un équipement mobile réel, et une pseudo-socket lorsqu'il est interfacé avec le simulateur de réseaux mobiles MADHOC. Ce simulateur est décrit dans [HGB06].

3.2.1.1 SOCKETS UDP/IP

Dans la mise en œuvre actuelle, les communications entre équipements mobiles à portée radio s'effectuent à travers une pile UDP/IP standard (*Internet Protocol versions 4 et 6*). Les messages échangés entre terminaux voisins sont donc embarqués dans des datagrammes UDP (*User Datagram Protocol*). En fonction du protocole de relais immédiat multi-sauts utilisé, un datagramme UDP est soit adressé à un destinataire précis (*unicast*), soit diffusé. La diffusion est réalisée en utilisant un groupe *multicast* prédéfini, de sorte qu'un datagramme soit uniquement reçu par les équipements abonnés à ce groupe prédéfini.

Le protocole de transport UDP satisfait assez bien nos besoins. Il offre un mode de communication non-connecté et non-fiable, qui permet des échanges opportuniste entre terminaux voisins. Cependant, certains services peuvent être amenés à publier des documents volumineux, qui ne peuvent être inclus dans un seul datagramme UDP dont la taille est limitée (65535 octets). Pour pallier cette contrainte, DoDWAN supporte la fragmentation et le ré-assemblage de documents volumineux. Cette fonctionnalité sera présentée en détails dans le paragraphe 3.3.4.

3.2.1.2 PSEUDO-SOCKET

Dans la mesure où il est assez difficile d'organiser et de réaliser des campagnes d'expérimentations impliquant des dizaines, voire des centaines d'équipements mobiles, DoDWAN a été

conçu de telle sorte à ce qu'il puisse être interfacé avec le simulateur de réseaux mobiles ad hoc (discontinus ou non) MADHOC [HGB06]. Nous avons choisi MADHOC car il a été développé à l'aide du langage de programmation Java. Cette caractéristique nous a permis de développer du code nous autorisant d'émuler DoDWAN sur chaque terminal mobile simulé par MADHOC. Pour ce faire, DoDWAN met en œuvre une pseudo-socket lui permettant d'être perçu comme une application du point de vue de MADHOC. En utilisant la combinaison DoDWAN-MADHOC, nous avons réalisé un certain nombre de simulations dans le but d'observer les performances de notre protocole sous différentes conditions. Les simulations attestent du bon fonctionnement de l'intergiciel DoDWAN, puisque, au cours des expérimentations, il s'exécute « réellement » sur chaque terminal mobile simulé.

3.2.2 PROTOCOLE DE RELAIS IMMÉDIAT

La couche protocolaire inférieure de DoDWAN a pour vocation de supporter le relais immédiat de documents dans le voisinage à k -sauts d'un terminal. Cette couche implémente nos protocoles de routage immédiat de documents (paragraphe 2.5.1, 2.5.2 et 2.5.3), en exploitant les sockets de communication décrites précédemment.

Les paragraphes suivants présentent la mise en œuvre des protocoles de routage multi-sauts d'un document au sein d'un îlot connexe. Celle-ci s'appuie sur l'ajout d'attributs prédéfinis dans le descripteur du document, attributs contenant des informations caractérisant, par exemple, le type de protocole de routage à appliquer.

3.2.2.1 PROTOCOLE DE DIFFUSION PAR INONDATION

En plus des protocoles de diffusion multi-sauts décrits dans le paragraphe 2.5, nous avons développé un protocole de diffusion par inondation afin de pouvoir vérifier lors de nos expérimentations :

- si l'exploitation de la diffusion via des relais multi-points permet effectivement de réduire la consommation des ressources lors de la diffusion à k -sauts d'une annonce par rapport à l'inondation ;
- si l'exploitation de la diffusion sélective pour la diffusion des documents en réponse à des requêtes permet d'obtenir des résultats satisfaisant, et de réaliser des économies de bande passante grâce à la limitation du nombre de diffusions ;

La figure 3.5 présente les informations insérées dans le descripteur d'un document devant être diffusé en exploitant le protocole de diffusion par inondation. En l'occurrence, il s'agit d'un document diffusé initialement par le terminal *hostA*, qui est relayé ici par le terminal C et qui doit encore être diffusé sur deux sauts consécutifs par d'autres terminaux. Pour répondre aux besoins du protocole de routage par la source décrit dans le paragraphe 2.5.2, chaque document diffusé contient l'historique des terminaux qui l'ont déjà relayé. Lorsqu'un terminal diffuse à son tour un document dans le cadre de la diffusion par inondation, il modifie au passage le descripteur du document : il ajoute son identifiant à l'historique de relais et décrémente le nombre de sauts restant à parcourir.

```
<broadcast-parameters
  protocol="flooding"
  from="hostA"
  nbOfHops="2"
  history="hostA, hostC"
/>
```

Figure 3.5: Information greffées à un descripteur de document devant être diffusé par inondation.

```
<broadcast-parameters
  protocol="mpr"
  from="hostA"
  nbOfHops="2"
  history="hostA, hostC"
  mpr-set="[hostI, hostJ]"
/>
```

Figure 3.6: Informations greffées à un document dans le cadre du protocole de diffusion via des relais multi-points. Sur cette figure le document est diffusé par le terminal C.

3.2.2.2 PROTOCOLE DE DIFFUSION VIA DES RELAIS MULTI-POINT

La figure 3.6 présente les informations insérées dans le descripteur d'un document devant être diffusé en exploitant le protocole de diffusion via des relais multi-point. À la différence de la diffusion par inondation, un terminal diffusant un document via ses MPR désigne quels terminaux doivent le rediffuser à leur tour. Cette information est contenue dans le paramètre *mpr-set*.

Dans l'exemple présenté dans la figure 3.6, le terminal *hostC* relaie le document et indique aux terminaux *hostI* et *hostJ* qu'ils sont ses MPR. Ces terminaux diffuseront donc à leur tour le document, en modifiant au passage dans le descripteur l'historique des relais du document, le nombre de sauts, et l'ensemble des MPR comme cela est défini dans le paragraphe 2.5.1.

3.2.2.3 PROTOCOLE DE DIFFUSION SÉLECTIVE

La figure 3.7 présente les informations insérées dans le descripteur d'un document devant être diffusé en exploitant le protocole de diffusion sélective. L'arbre de diffusion le long duquel un document doit être diffusé est précisé par le paramètre « *tree* », il est représenté sous une forme compacte parenthésée. L'arbre de diffusion d'un document a été présenté dans le paragraphe 2.5.3.

Dans l'exemple illustré dans la figure 3.7, le terminal *hostA* diffuse un document suite à des requêtes provenant des terminaux mobiles *hostC*, *hostD*, *hostF* et *hostG*, lui demandant la diffusion du même document. Le terminal *hostA* calcule donc l'arbre de diffusion (dont lui-même est la racine et les demandeurs sont les feuilles) grâce auquel il peut satisfaire en une


```
<broadcast-parameters
protocol="tree"
tree="(hostA(hostB(hostC,hostD),(hostE(hostF(hostG))))))"
/>
```

Figure 3.7: Informations greffées à un document dans le cadre du protocole de diffusion sélective.

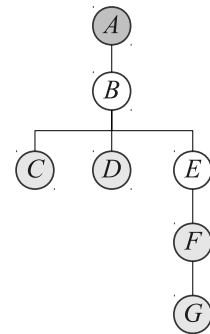


Figure 3.8 – Représentation graphique de l'arbre de diffusion

```
<unicast-parameters
from="hostG"
to="hostA"
path="hostE, hostA"
path="hostF"
/>
```

Figure 3.9: Informations greffées à un document dans le cadre du protocole de routage unicast par la source.

seule diffusion tous les demandeurs. Cet arbre, exprimé sous une forme parenthésée dans la figure 3.7, est représenté graphiquement dans la figure 3.8.

3.2.2.4 PROTOCOLE DE ROUTAGE PAR LA SOURCE

La figure 3.9 présente les informations insérées dans le descripteur d'un document adressé à *hostA* par *hostG*. En l'occurrence, ce mécanisme doit permettre à une requête de parcourir le chemin inverse de celui parcouru par l'annonce diffusée par *hostA* pour atteindre *hostG*. Ce chemin le long duquel le document doit être relayé en unicast est indiqué par la source dans le paramètre *path*.

Lorsqu'un terminal reçoit un document qu'il doit relayer en exploitant le protocole de routage par la source, le terminal adresse le document au prochain terminal en exploitant une transmission *unicast*, et, au passage, supprime son identifiant de l'attribut *path* et l'ajoute à l'historique. Dans l'exemple illustré dans la figure 3.9 le document concerné est adressé à *hostA* par *hostG* ; il est relayé par *hostF* à *hostE* qui devra le relayer vers son destinataire.

Comme nous l'avons évoqué dans le paragraphe 2.5.2, un terminal relayant une requête vérifie d'abord que le terminal vers lequel il doit relayer le message est bien présent dans son voisinage, ceci dans le but de détecter d'éventuelles ruptures de connectivité et ainsi de réduire

le nombre d'émission inutile. Toutes les ruptures ne peuvent être détectées, dans ce sens notre protocole a été développé afin de les tolérer.

3.3 DISSÉMINATION OPPORTUNISTE BASÉE CONTENUS

3.3.1 IDENTIFIANT UNIQUE D'UN TERMINAL

Notre protocole de communication opportuniste basée contenus est présenté en détails dans le paragraphe 2.4.2. Il nécessite qu'un terminal soit en mesure d'identifier ses voisins pour pouvoir leur adresser des requêtes ou des documents. Un terminal doit donc posséder un identifiant unique pour que des échanges de documents puissent avoir lieu. Lors des expérimentations que nous avons réalisées avec un nombre limité d'ordinateurs portables, nous étions en mesure d'attribuer « manuellement » à chaque terminal un identifiant unique. Cependant, nous avons envisagé le cas où l'intergiciel DoDWAN serait distribué au grand public. Dans ce cas précis, la population de terminaux est inconnue et n'est pas administrée par nos soins. Plusieurs méthodes sont alors envisageables pour permettre la génération automatique d'un identifiant unique. Ainsi, selon le type de terminal mobile communicant sur lequel DoDWAN est installé, différentes méthodes sont utilisables :

- si DoDWAN est utilisé sur des téléphones portables ou des *smartphones*, l'identité unique de l'hôte peut être son propre code IMEI (*International Mobile Equipment Identity*). En effet, le code IMEI est un numéro de série unique composé de 15 à 17 chiffres attribué à chaque téléphone portable ;
- si DoDWAN est utilisé sur des ordinateurs portables ou des PDAs, l'identité unique de l'hôte peut être sa propre adresse MAC (*Media Access Control*). En effet, l'adresse MAC est un identifiant physique stocké au niveau de l'interface réseau qui est utilisé pour attribuer mondialement une adresse unique au niveau de la couche de liaison (couche 2 du modèle OSI). Il est également possible d'utiliser comme identité l'adresse IPv6 locale (*link local*) de l'interface radio du terminal hôte. Cette adresse est en théorie unique puisqu'elle est construite à partir de l'adresse MAC du terminal.

Dans notre mise en œuvre actuelle sur ordinateur ou PDA c'est l'adresse IPv6 locale de l'interface radio que nous avons utilisée.

3.3.2 DOCUMENTS CONTENANT DES DONNÉES DE CONTRÔLE

Dans notre mise en œuvre, le trafic de contrôle nécessaire aux échanges de documents entre terminaux voisins est réalisé à l'aide de documents particuliers. Ces documents sont similaires dans leur structure aux documents publiés par des services applicatifs, mais ils contiennent dans leur descripteur un attribut particulier nommé *dodwan-protocol*. Cet attribut indique que le document contient un message de contrôle protocolaire. Par exemple, si un document contient une annonce complète, l'attribut *dodwan-protocol* prend la valeur « *announce* ». Si le document contient une requête, l'attribut prend la valeur « *request* ». Ces documents d'un genre particulier ne sont pas hébergés en cache par les terminaux, en effet ils contiennent des données de contrôle qui ne doivent pas être disséminées à travers le réseau.

3.3.3 SUPPORT DE LA VOLATILITÉ

L'intergiciel DoDWAN doit supporter les arrêts (éventuellement brutaux) et redémarrages du terminal hôte, tout en assurant la continuité du fonctionnement du protocole de dissémination opportuniste basée sur le contenu, et en permettant aux terminaux de maintenir à jour leur propre perception du voisinage.

Lors du redémarrage d'un terminal hôte, l'intergiciel DoDWAN doit donc être capable de continuer à disséminer les documents hébergés dans son cache, et de continuer à collecter des documents correspondant à son profil d'intérêt défini par le passé. Pour ce faire, nous avons mis en œuvre dans notre plate-forme de communication la persistance des données utiles au bon fonctionnement du protocole de communication qu'elle implémente. Le paragraphe 3.3.3.1 décrit les gestionnaires gérant la persistance de ces données.

Le protocole de communication, implémenté dans l'intergiciel DoDWAN, s'appuie sur la perception qu'ont les terminaux de leur voisinage afin de réaliser la dissémination sélective basée sur le contenu et le relais immédiat. Pour permettre aux terminaux de maintenir une perception « à jour » de leur voisinage, notre protocole exploite, d'une part, un mécanisme de diffusion périodique d'annonce qui permet à un terminal d'avertir des terminaux voisins de sa présence, et, d'autre part, la capacité des terminaux à percevoir leurs événements d'arrêt et de redémarrage afin qu'ils annoncent respectivement leur départ et leur arrivée. Le paragraphe 3.3.3.2 présente les réactions des terminaux à ces événements.

3.3.3.1 PERSISTANCE DES DONNÉES

Gestionnaire de cache de document. Notre modèle de communication nécessite qu'un terminal soit capable d'héberger des documents en transit dans un espace de stockage persistant et limité. DoDWAN met donc en œuvre un cache dans lequel ils sont entreposés. Pour gérer cet espace limité, un gestionnaire de cache applique une politique de gestion afin de libérer de l'espace lorsque cela est nécessaire. À ce jour, seule la fonction de rang proposée dans le paragraphe 2.4.2.5 a été implémentée dans le code de DoDWAN. Toutefois, ce gestionnaire a été développé de telle sorte à ce qu'il soit aisé d'y intégrer d'autres fonctions de rang.

Lorsque l'intergiciel DoDWAN s'exécute sur de « vrais » équipements mobiles, le gestionnaire de cache de documents est responsable du stockage sur disque des documents. Ce dernier est réalisé de la façon suivante : une première zone est réservée à l'hébergement des descripteurs de documents, et une seconde à l'entreposage des charges utiles. De la sorte, lors du redémarrage d'un terminal, le gestionnaire de cache ne recharge en mémoire que les descripteurs des documents. La charge utile d'un document est chargée en mémoire uniquement lorsque ce document doit être délivré à un service local ou lorsqu'il doit être diffusé sur le médium radio.

Pour que la persistance du cache de documents soit assurée en cas d'arrêts brutaux d'un terminal (par exemple un plantage système), le stockage sur disques est réalisé en continu, c'est-à-dire que, lorsque le gestionnaire de cache décide d'héberger un nouveau document, celui-ci est immédiatement enregistré sur disque.

Gestionnaire de profil d'intérêt. Le gestionnaire de profil d'intérêt gère les abonnements réalisés par les services applicatifs locaux à travers l'interface *publish-subscribe*. Il permet l'ajout, la suppression et la modification d'un prédicat de sélection du profil d'intérêt. Pour ce faire, à chaque prédicat de sélection est associée une clé, qui est transmise au service applicatif lors de son abonnement via l'interface de *publish-subscribe*. Lorsqu'un service applicatif souhaite modifier ou supprimer l'un des ses abonnements, il précise la clé correspondant à cet abonnement ainsi que le nouveau prédicat de sélection.

Le gestionnaire de profil d'intérêt est responsable de la persistance du profil d'intérêt du terminal hôte. Pour tolérer la volatilité d'un terminal, les opérations d'ajout, de suppression et de modification d'un prédicat de sélection au profil d'intérêt provoquent immédiatement son stockage sur disque. De la sorte, lorsqu'un terminal hôte redémarre, son profil d'intérêt est chargé par DoDWAN depuis le disque. Le terminal continue donc à collecter des documents correspondant aux centres d'intérêts définis par le passé.

3.3.3.2 PERCEPTION DU VOISINAGE

DoDWAN doit être sensible à la mise en veille et à la sortie de veille du terminal hôte. De manière générale, la mise en veille et le redémarrage d'un terminal hôte donnent lieu à la production d'événements ACPI². Ces événements peuvent être capturés par DoDWAN dans le but de réaliser différentes opérations selon le type d'événement.

Lors de la mise en veille ou de l'arrêt d'un terminal, l'événement ACPI reçu par DoDWAN l'informe de l'arrêt imminent du système hôte. DoDWAN réagit à cet événement en diffusant immédiatement un message de contrôle dans le k-voisinage. Ce message de contrôle indique aux terminaux voisins que le terminal émetteur ne sera plus actif. La réception d'un message de ce type par un terminal lui permet de mettre à jour sa perception de son voisinage.

Lors de la réactivation d'un terminal suite à une phase de veille, l'événement ACPI capturé par DoDWAN l'informe de la réactivation du terminal hôte. DoDWAN procède alors au réamorçage du mécanisme d'annonce périodique : il diffuse immédiatement une annonce complète, indiquant sa présence à d'éventuels voisins.

Permettre à l'intergiciel DoDWAN de capturer les événements ACPI du système hôte n'est pas chose aisée, car l'API Java ne fournit pas les outils nécessaires. Un système permettant à DoDWAN d'être sensible aux événements ACPI est donc nécessaire. À ce jour, DoDWAN n'est réactif à ces événements que lorsque le système d'exploitation utilisé est basé sur un noyau Linux, et que le démon *acpid*³ est actif. Ce démon permet un traitement sélectif des événements ACPI. Lorsqu'un événement survient, il exécute les scripts prévus.

2. Le terme anglais Advanced Configuration and Power Interface (ACPI) désigne une norme co-développée par Hewlett Packard, Intel, Microsoft, Phoenix Technologies et Toshiba (<http://www.acpi.info>). Le but de cette norme est de réduire la consommation d'énergie d'un ordinateur en mettant hors tension certains éléments. La mise hors tension de périphériques matériels est réalisée par le système d'exploitation à travers une interface permettant l'envoi de signaux. Cette interface permet aussi au matériel d'envoyer des signaux au système d'exploitation, par exemple lorsque l'utilisateur appuie sur le bouton de mise en veille.

3. <http://acpid.sourceforge.net>

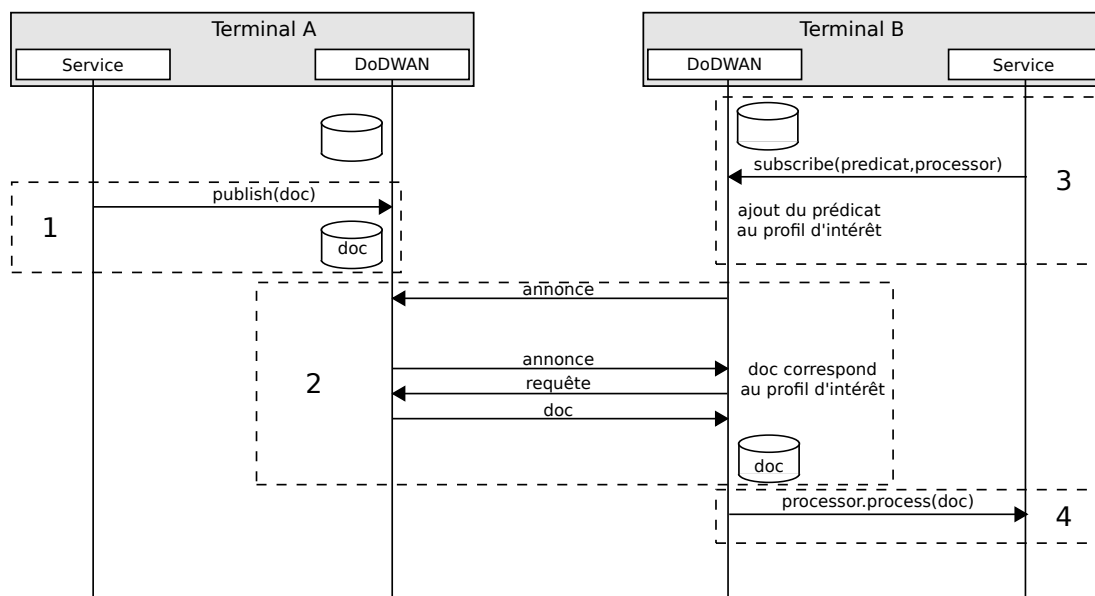


Figure 3.10 – Diagramme de séquence simplifié présentant les interactions entre services applicatifs et DoDWAN via l'interface *publish-subscribe*.

La transmission des événements ACPI de mise en veille, de réactivation et d'arrêt à DoDWAN est réalisée de la manière suivante. DoDWAN met en œuvre une console depuis laquelle il attend de recevoir les consignes de mise en veille et de réveil. Selon le type d'événement, un script est exécuté et envoie une consigne sur la console de DoDWAN. Par exemple, lors de la réception d'un événement ACPI de mise en veille, le démon *acpid* exécute un script qui envoie la consigne de mise en veille à DoDWAN.

Il est toutefois important de noter que si DoDWAN doit s'exécuter sur une plate-forme sur laquelle les événements ACPI ne sont pas utilisables alors il faudra soit développer une autre moyen techniques permettant de percevoir la volatilité du terminal, soit admettre que le protocole mis en œuvre dans DoDWAN fonctionne de manière dégradée.

3.3.4 INTERFACE PUBLISH-SUBSCRIBE

Le protocole de communication mis en œuvre dans la plate-forme DoDWAN est accessible aux services applicatifs via l'interface *publish-subscribe*. Grâce à cette interface les services applicatifs s'exécutant sur un terminal sont en mesure de publier des documents et de souscrire pour recevoir des types particuliers de documents.

3.3.4.1 PUBLICATION ET ABONNEMENT

La figure 3.10 présente, de manière simplifiée, les interactions entre service applicatif et DoDWAN ainsi qu'entre les terminaux voisins A et B.

Publication. Lorsqu'un service applicatif publie un document contenant des données applicatives, le document est simplement déposé dans le cache local du terminal (étape 1 de la figure 3.10). Dès lors, grâce au protocole de dissémination implémenté dans l'intergiciel DoD-WAN, ce document pourra se propager dans le réseau vers des terminaux mobiles sur lesquels des services applicatifs se sont abonnés pour recevoir ces documents (étape 2 de la figure 3.10).

Abonnement. Pour pouvoir recevoir un certain type de documents, un service applicatif doit s'abonner en précisant les caractéristiques du type de documents désiré à l'aide d'un prédicat de sélection et doit indiquer quel élément sera responsable du traitement des documents satisfaisant chacun de ses intérêts (étape 3 de la figure 3.10). L'abonnement réalisé par le service est relayé au gestionnaire de profil d'intérêt, qui l'insère dans le profil d'intérêt du terminal. Dès lors le terminal en question va chercher à se procurer, lors de contacts fugitifs, des documents correspondant au prédicat de sélection fournit par le service applicatif.

Réception d'un nouveau document. Lors de la réception d'un nouveau document (depuis le réseau ou publié localement), l'interface *publish-subscribe* est responsable du relais du document vers chaque service applicatif local intéressé pour qu'il puisse traiter le document en question (étape 4 de la figure 3.10). De plus, lors de son abonnement un service applicatif est notifié des documents hébergés en cache et qui satisfont ses intérêts. Un service applicatif peut alors décider de récupérer tout ou partie des documents identifiés pour les traiter.

Les abonnements réalisés par les services applicatifs s'exécutant sur un terminal mobile sont enregistrés dans son profil d'intérêt par le gestionnaire de profil d'intérêt, un abonnement est donc persistant. Cependant, il se peut qu'un service souhaite modifier son abonnement. Pour ce faire, pour chaque abonnement il reçoit une clé qu'il doit conserver. Lorsqu'il souhaitera se désabonner ou modifier son abonnement il devra fournir cette clé afin de permettre au gestionnaire de profil d'intérêt de modifier le profil du terminal mobile en conséquence.

En outre, les services applicatifs utilisant DoD-WAN pour communiquer ne sont pas nécessairement actifs en même temps que DoD-WAN. C'est-à-dire qu'un service applicatif peut s'abonner pour un certain type de document, recevoir et traiter des documents, puis décider de s'arrêter (sans se désabonner). Cependant lorsqu'un service applicatif interrompt son fonctionnement, il indique à DoD-WAN d'arrêter de lui relayer des documents correspondant à ses intérêts. Pour ce faire, il utilise les clés fournies lors de ses abonnements. Lors de son redémarrage, le service applicatif en question devra indiquer à DoD-WAN qu'il doit à nouveau lui relayer les documents correspondant à ses abonnements. Pour ce faire, le service applicatif précise à DoD-WAN les clés correspondant à ses abonnements, DoD-WAN procède ensuite comme s'il s'agissait d'un nouvel abonnement.

3.3.4.2 COMPRESSION ET FRAGMENTATION

Compression. Lorsqu'un service applicatif publie un document, le contenu de ce document est systématiquement compressé dans le but de réduire la quantité de ressources consommées

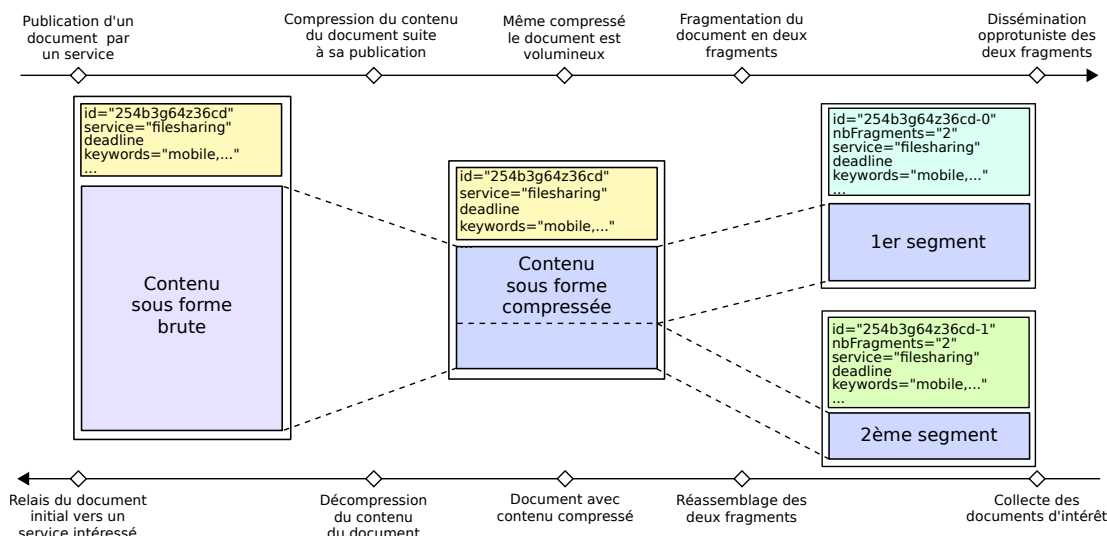


Figure 3.11 – Processus de compression et de fragmentation d'un document publié par un service

lors son stockage en cache et lors de sa diffusion sur le médium radio. Le taux de compression est directement lié au type de contenu du document. Par exemple, un descripteur de service XML permet d'obtenir un taux de compression bien supérieur à celui obtenu lors de la compression d'une image au format JPEG. Les documents que les terminaux mobiles hôtes échangent et hébergent dans leur cache se présentent donc sous forme compressée. Lorsqu'un document est relayé par l'interface *publish-subscribe* à un ou plusieurs services applicatifs locaux intéressés, le contenu du document est décompressé.

Fragmentation. Certains services peuvent être amenés à publier des documents dont le contenu est volumineux, même sous forme compressée. Ces documents ne peuvent être transmis en une seule fois sur le médium radio, c'est-à-dire qu'ils ne peuvent être inclus dans un datagramme UDP. Pour permettre la dissémination de tels documents DoDWAN supporte la fragmentation et le ré-assemblage, comme cela est illustré par la figure 3.11. Lorsqu'un document est publié par un service local, DoDWAN vérifie si la taille du document est inférieure à une valeur seuil qui détermine la taille maximale d'un document pouvant être émis par DoDWAN, c'est-à-dire une valeur inférieure ou égale à la charge maximale pouvant être incluse dans un datagramme UDP. Si la taille du document dépasse cette valeur seuil, son contenu est alors fragmenté par la source en segments distincts. Ces segments sont encapsulés dans des fragments du document dont les descripteurs conservent les mêmes caractéristiques que le descripteur du document initial, c'est-à-dire qu'ils conservent les mêmes attributs (date de péremption, mots clés, ...). Les fragments du document initial peuvent alors se propager dans le réseau indépendamment les uns des autres. Ils seront, à terme, collectés par les terminaux intéressés, au niveau desquels le réassemblage des multiples segments permettra de reconstituer le document initial.

Chaque segment contenu dans un fragment de document est identifié afin qu'un terminal disposant de l'ensemble des fragments de document puisse réassembler les segments dans le

bon ordre et reconstruire le contenu du document initial. Deux informations sont donc utiles à un terminal récepteur : le nombre de fragments de document et le numéro de séquence du segment contenu dans un fragment. Ces deux informations sont ajoutées dans le descripteur d'un fragment de document. Par exemple, le premier fragment présent dans la figure 3.11 contient dans son descripteur, en plus des attributs présents dans le descripteur du document initial, le nombre de fragments (« nbFragments=2 »), indiquant qu'il y a deux fragments, et un identifiant unique (« id=254b3g64z36cd-0 », indiquant le numéro de séquence du fragment « 0 » et l'identifiant du document initial « 254b3g64z36cd »).

Le réassemblage d'un document fragmenté a lieu uniquement lorsqu'un terminal dispose de l'ensemble de ses fragments et que ce document doit être relayé vers un ou plusieurs services applicatifs locaux intéressés. Ce mécanisme est illustré dans la figure 3.11. La première étape consiste en la reconstitution du contenu sous forme compressée, c'est-à-dire la concaténation des segments dans le bon ordre, et la reconstitution du descripteur initial du document. Ce dernier est obtenu en supprimant du descripteur l'attribut « nbFragments » et en supprimant de l'attribut « id » le numéro de séquence du fragment. Le contenu du document est alors décompressé, et le document est relayé vers les services applicatifs locaux intéressés.

On peut noter qu'avec cette caractéristique contribue à assurer la robustesse du système, dans la mesure où il n'est pas nécessaire qu'un terminal mobile dispose de l'ensemble des fragments d'un document pour pouvoir contribuer à sa dissémination dans le réseau.

3.4 SERVICES APPLICATIFS EXPLOITANT DODWAN

Pour démontrer la faisabilité du développement et de l'utilisation de services applicatifs qui utilisent le mode de communication proposé dans DoDWAN, nous avons développé de multiples applications de démonstration. Plusieurs services applicatifs pour réseaux mobiles ad hoc discontinus ont ainsi été mise en œuvre, sur la base d'une architecture pair-à-pair exploitant un modèle de communication opportuniste basée contenus.

3.4.1 SERVICE DE DISCUSSION DE GROUPES

NewsWAN (*News distribution in Wireless Ad hoc Networks*) est un service de discussion permettant aux utilisateurs de terminaux mobiles communicants de publier librement des articles dans des rubriques thématiques appelées forums ou groupes de discussion, et de s'abonner à certains forums afin de recevoir de façon asynchrone l'ensemble des articles qui y sont publiés. Ce service de discussion thématique se prête donc bien à une utilisation dans des réseaux mobiles ad hoc discontinus et à l'exploitation du modèle de communication basé contenus proposé par l'intergiciel DoDWAN.

NewsWAN s'inspire fortement du service Usenet (contraction de User Network) créé dans les années 1980. Cependant, contrairement à Usenet, NewsWAN ne repose pas sur un modèle client-serveur mais sur un modèle pair-à-pair : les terminaux des utilisateurs peuvent s'échanger directement des articles, sans avoir pour ce faire à passer par un quelconque serveur.

Avec ce système, un utilisateur est en mesure d'envoyer et de recevoir des articles de la même manière que sur le système Usenet. Nous avons conservé les applications standards dédiées à l'utilisation de Usenet (c'est-à-dire un programme client nommé *newsreader* tel que Thunderbird) afin de ne pas changer les habitudes des utilisateurs et de ne pas avoir à développer une application cliente dédiée à NewsWAN. Un client classique peut donc être utilisé pour accéder aux forums de discussion, même si le système qui maintient ces forums opère d'une façon différente de Usenet.

Dans un MANET discontinu, aucun terminal ne peut être considéré comme suffisamment stable et accessible pour jouer le rôle d'un serveur dédié comme dans le système Usenet. Par conséquent, le newsreader s'exécutant sur le terminal d'un utilisateur ne peut pas être associé avec un serveur distant. La solution que nous avons adoptée consiste à faire tourner sur chaque terminal mobile un pseudo-serveur, avec lequel le newsreader peut interagir par des sessions NNTP (*Network News Transfer Protocol*) locales lorsqu'un utilisateur souhaite envoyer ou recevoir des articles, et s'abonner ou se désabonner d'un newsgroup.

Dans l'architecture standard Usenet, les serveurs sont administrés par du personnel dédié qui décide de la création d'un forum, de l'hébergement local de forum, et des serveurs avec lesquels ils doivent se synchroniser. Dans le système NewsWAN, le propriétaire d'un terminal « administre » lui-même le pseudo-serveur de son terminal.

Les terminaux mobiles étant contraints en ressource mémoire, il est impensable qu'un terminal puisse héberger l'ensemble des forums. L'utilisateur définit avec soin des forums qu'il décide d'héberger localement et ceux auxquels il souhaite s'abonner grâce à son application cliente. Pour réaliser cette tâche les administrateurs de serveurs Usenet utilisent une liste des forums existants et sélectionnent dans cette liste les forums qu'ils souhaitent voir hébergés sur leurs serveurs. Cette approche n'est pas applicable dans le cas du système NewsWAN, aucun terminal dans un réseau mobile ad hoc discontinu ne pouvant servir de point central maintenant les listes des newsgroups. À la place d'un tel mécanisme, un mécanisme de découverte est mis en œuvre afin de permettre aux utilisateurs de prendre connaissance de l'existence de nouveaux newsgroups créés par d'autres utilisateurs.

3.4.1.1 ARCHITECTURE DU SYSTÈME NEWSWAN

La figure 3.12 présente l'architecture générale d'un hôte exécutant NewsWAN. Le couple DoD WAN-NewsWAN s'exécute en tâche de fond sur chaque terminal participant au système de discussion thématique. Il y a donc deux couches constituant le système :

- Une couche haute qui est en charge de la gestion des forums et des interactions avec l'application cliente de l'utilisateur à travers des sessions NNTP.
- Une couche basse qui permet l'interaction avec les autres pseudo-serveurs NewsWAN s'exécutant sur des terminaux voisins.

En pratique, lorsque deux terminaux mobiles entrent en contact radio, ils exploitent cette opportunité pour échanger des articles appartenant aux forums de discussion par lesquels leurs propriétaires respectifs sont intéressés. Le protocole de communication mis en œuvre dans

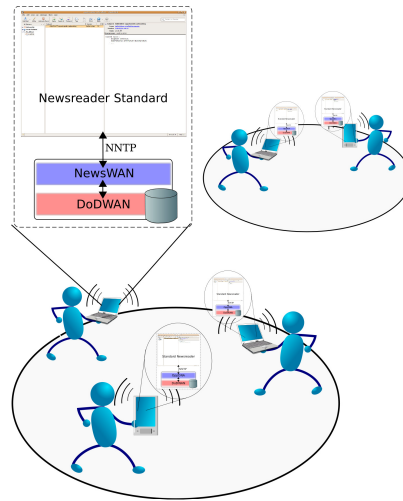


Figure 3.12: Architecture d'une instance de NewsWAN

DoDWAN répond parfaitement à ce besoin d'échange opportuniste basé contenus parce qu'il met à profit chaque contact fugitif afin de permettre à des terminaux d'échanger des documents en fonction de leurs centres d'intérêt respectifs.

Lorsqu'un utilisateur publie un article dans un forum, cet article est simplement passé depuis le programme client à NewsWAN, grâce à une session NNTP standard. Cet article est alors converti dans le format supporté par DoDWAN. Grâce à cette opération l'article peut se disséminer à travers le réseau, en étant relayé de façon opportuniste vers chaque terminal dont le propriétaire est abonné au forum de discussion auquel cet article appartient. Inversement, lorsque DoDWAN obtient de la part d'un voisin un article intéressant le propriétaire du terminal, la couche supérieure (c'est-à-dire NewsWAN) est notifiée de cette réception et l'article est rendu accessible à l'utilisateur depuis son application cliente.

3.4.1.2 ADMINISTRATION DU PSEUDO-SERVEUR NEWSWAN

Le profil d'intérêt qui détermine les types de documents que l'intergiciel DoDWAN doit chercher à récupérer depuis des terminaux voisins doit être établi selon les préférences de l'utilisateur de NewsWAN.

Dans le système Usenet, l'application cliente enregistre les abonnements d'un utilisateur pour des forums de discussion, et récupère les articles de ces forums depuis le serveur. Cependant, un utilisateur ne peut pas ordonner au serveur de créer ou s'abonner à un forum car les forums hébergés par un serveur sont contrôlés par son administrateur. Pour le système NewsWAN une méthode doit donc permettre à un utilisateur de configurer les newsgroups hébergés par le pseudo-serveur local. La solution que nous avons adoptée pour l'administration repose sur l'utilisation d'un forum de discussion dédié à l'administration du pseudo-serveur (le forum *newswan.admin*). En publiant dans ce forum des articles respectant un format spécifique, un utilisateur donne des instructions à NewsWAN.

Par exemple, si un utilisateur souhaite créer le forum de discussion *comp.networking*, il publie dans *newswan.admin* un article dont le corps contient une description du sujet couvert par le forum à créer, et dont le champ *Subject* est formaté comme suit : **Subject: ANNOUNCE comp.networking [2j]**. NewsWAN interprète alors le champ *Subject* comme une consigne l'invitant à créer localement le forum de discussion *comp.networking*, et précisant que tout article envoyé dans ce forum se verra attribuer une durée de vie de 2 jours par défaut, c'est-à-dire que DoDWAN disséminera les articles appartenant à ce forum uniquement durant 48 heures.

Afin de permettre la découverte des forums de discussion par les utilisateurs, le programme NewsWAN est abonné au forum *newswan.admin*. NewsWAN collecte donc tous les articles annonçant la création d'un nouveau forum. En consultant le forum *newswan.admin*, un utilisateur prend connaissance des forums existants et des sujets qu'ils couvrent. Un utilisateur qui découvre l'existence du forum *comp.networking* peut décider de s'y abonner à l'aide de son *newsreader*. Lorsque le pseudo-serveur identifie qu'à travers son application cliente un utilisateur s'abonne à un nouveau forum non hébergé localement, il réalise alors un abonnement auprès de DoDWAN afin de pouvoir recevoir les articles appartenant à ce forum. Le profil d'intérêt du terminal local est alors modifié. Dès lors DoDWAN cherche à obtenir les articles du forum de discussion *comp.networking*. Le terminal de l'utilisateur devient un transporteur pour l'ensemble des articles de ce forum, et à son tour pourra les fournir à des utilisateurs intéressés qu'il rencontrera au gré de ses déplacements. À l'inverse, le désabonnement d'un utilisateur à un forum entraîne au niveau de DoDWAN la suppression du prédicat de sélection correspondant du profil d'intérêt (arrêt de la collecte des articles publiés dans ce forum) et au niveau de NewsWAN la destruction des articles présents dans ce forum.

Si la création d'un forum est possible sa suppression est impossible. En effet, à partir du moment où un utilisateur crée un nouveau forum sur son terminal, l'information concernant l'existence de ce forum va commencer à se propager de proche en proche, au gré des contacts entre terminaux mobiles comme cela est décrit dans le mécanisme de découverte. Certains utilisateurs vont donc (potentiellement) s'abonner à ce forum et y publier des articles. Le nouveau forum n'est pas la « propriété » exclusive de l'utilisateur qui l'a créé initialement : il appartient collectivement à tous les utilisateurs qui y sont abonnés. Si un utilisateur ne souhaite plus recevoir les articles publiés dans un certain forum, il lui suffit de s'en désabonner. Si tous les utilisateurs se désabonnent d'un même forum, alors cela équivaut, de fait, à la disparition de ce forum.

3.4.1.3 ABONNEMENT ET PUBLICATION DANS NEWSWAN

Du point de vue de l'utilisateur, les procédures d'abonnement, de désabonnement et de publication d'un article dans un forum de discussion thématique sont identiques à celles réalisées lorsqu'il utilise le système classique Usenet. Cependant, comme nous venons de le présenter l'abonnement et le désabonnement à un forum entraînent des modifications du profil d'intérêt de DoDWAN.

Lorsqu'un utilisateur publie un article dans un forum de discussion, cet article se voit attribuer la durée de vie par défaut du forum. Dans certains cas, l'utilisateur peut décider d'attribuer

lui-même une durée de vie à son article. Pour ce faire, il lui suffit d'ajouter à la fin du sujet un paramètre indiquant la durée de vie de l'article concerné. La durée de vie attribuée aux articles publiés peut être spécifiée de différentes façons. Les expressions suivantes sont par exemple toutes équivalentes pour exprimer une durée de vie de 2 jours, 8 heures, et 30 minutes : [02:08:30], [2:8:30], [2 jours 8 heures 30 minutes], [2 j 8 h 30 m], ou [2j8h30m].

3.4.2 AUTRES EXEMPLES DE SERVICES APPLICATIFS

Sur la base de l'architecture présentée dans le paragraphe précédent, d'autres services applicatifs de démonstration ont été développés. Il s'agit d'un service de partage de fichiers basé contenu et d'un service de messagerie, tout deux capables de fonctionner dans des réseaux mobiles ad hoc discontinus.

3.4.2.1 SERVICE DE PARTAGE DE FICHIERS

FishWAN (*File SHaring in Wireless Ad hoc Networks*) est un service de partage de fichiers en mode pair-à-pair. Il possède de ce fait un grand nombre de caractéristiques communes avec les logiciels populaires utilisés sur Internet (Emule, Kaaza, etc.). Il permet à un utilisateur de mettre des fichiers qu'il possède à disposition d'une communauté d'utilisateurs (c'est-à-dire de publier des fichiers) et réciproquement, d'obtenir de nouveaux fichiers d'autres utilisateurs de la communauté (c'est-à-dire de s'abonner pour recevoir des types particuliers de fichiers).

L'intérêt de ce service de partage est de montrer comment la communication opportuniste basée contenus peut-être utilisée par des utilisateurs afin de partager de fichiers dans des réseaux mobiles ad hoc discontinus. Lors de la publication d'un fichier par un utilisateur, ce dernier peut fournir autant de méta-données qu'il souhaite pour caractériser ce qu'il publie. Ces méta-données sont ensuite associées au document publié par le service applicatif. Les utilisateurs souhaitant recevoir un type particulier de fichiers, décrivent comment sont caractérisés ces documents par une liste de méta-données.

Le partage se fait de façon asynchrone, l'utilisateur de FishWAN spécifie les types particuliers de fichiers qui l'intéressent, et les reçoit ensuite en continu. Le processus de récupération du fichier pouvant prendre un certain temps, ce type de partage de fichier est le plus souvent incompatible avec une utilisation interactive. L'utilisateur est notifié de la réception d'un fichier à la fin du processus de récupération.

3.4.2.2 SERVICE DE MESSAGERIE

MailWAN (*Mail exchange in Wireless Ad hoc Networks*) est un service qui permet aux utilisateurs de terminaux mobiles communicant d'échanger des courriers électroniques en l'absence de toute infrastructure de communication. Ce service montre qu'il est possible de réaliser des communications orientées destinations à l'aide du modèle de communication offert par l'intergiciel DoDWAN même si le modèle de communication proposé par DoDWAN est orienté contenus. De plus, ce service de messagerie correspond à une utilisation dans un environnement discontinu, le transport du message pouvant être assimilé à celui d'un courrier papier.

MailWAN s'inspire du service de messagerie électronique existant sur Internet, le format des messages et des adresses électroniques est identique. Cependant, contrairement au service de messagerie sur Internet qui fonctionne selon un modèle client-serveur, MailWAN repose sur un modèle pair-à-pair : les terminaux mobiles s'échangent directement les courriers électroniques, sans passer par un quelconque serveur.

Pour ce faire, la structure de l'adresse électronique d'un utilisateur n'identifie plus un compte utilisateur sur un serveur hébergeant le service de messagerie électronique, mais elle identifie un utilisateur appartenant à une communauté d'utilisateurs. Par exemple, l'adresse électronique `yves.mahéo@casa.valoria.univ-ubs` indique que le courrier électronique est adressé à Yves Mahéo qui fait partie de la communauté `casa`, qui est un sous-groupe de la communauté `valoria`, qui est elle-même un sous-groupe de la communauté `univ-ubs`. Pour que ce message puisse être reçu par son destinataire, il pourra être relayé par les utilisateurs disposés à le faire. Pour ce faire, le service MailWAN met à disposition de l'utilisateur une interface d'administration qui lui permet de définir pour quels groupes il est prêt à jouer le rôle de transporteur altruiste proactif (mode de transport défini dans le paragraphe 2.2.3). Par exemple, un utilisateur indiquant qu'il est prêt à transporter et relayer les courriers électroniques de la communauté `valoria` sera un bon porteur du message envoyé à Yves Mahéo.

Lorsqu'un utilisateur envoie un courrier électronique, il peut préciser la date de péremption d'un message afin de limiter sa propagation dans le temps en fonction, par exemple, de la sémantique du message. Si l'utilisateur n'indique pas de date de péremption, le message se voit attribuer une date de péremption en fonction de sa date d'envoi et d'une durée de vie par défaut.

3.5 DISCUSSION

Dans ce chapitre, nous avons présenté la mise en œuvre du protocole de communication décrit dans le chapitre 2 de ce mémoire de thèse. Cette mise en œuvre dans la plate-forme intergicielle DoDWAN correspond à notre objectif d'évaluation par la pratique de notre protocole de communication.

La plate-forme de communication DoDWAN⁴ est aujourd'hui distribuée sous la forme d'une librairie Java. Elle représente environ 35 000 lignes de code. On peut noter que l'intergiciel DoDWAN a été téléchargé de nombreuses fois, et qui est actuellement utilisé dans différents projets, comme par exemple dans un jeu d'échec⁵ développé en Java.

DoDWAN peut être déployée sur de « vrais » équipements mobiles. Pour l'heure, suite aux travaux menés dans cette thèse, cette plate-forme de communication a notamment été déployée et utilisée sur une trentaine d'ordinateurs portables équipés d'interface réseau de type Wi-Fi, dans le cadre de campagnes d'expérimentations en conditions réelles baptisées DITADHOC⁶ et DoDWAN-Expe⁷. Par ailleurs, l'intergiciel DoDWAN a évolué dans le cadre de ces deux projets. Il a notamment été conditionné sous la forme d'un bundle OSGi, et sous la forme d'un

4. <http://www-valoria.univ-ubs.fr/CASA/DoDWAN/>

5. <http://echecs.parlenet.org/>

6. <http://www-valoria.univ-ubs.fr/CASA/DITADHOC/>

7. <http://www-valoria.univ-ubs.fr/CASA/DODWAN-EXPE/>

paquet Debian en vue de faciliter son déploiement et sa diffusion dans les environnements Linux Debian et dérivés.

Les différents services applicatifs proposés lors de ces expérimentations réelles, qui ont fait suite aux travaux présentés dans ce mémoire, nous ont permis de valider par l'expérimentation la faisabilité et l'utilisabilité de notre protocole de communication, et des services applicatifs de partage de fichiers, de messagerie et de discussion thématique.

Dans le chapitre suivant, nous présentons des résultats expérimentaux obtenus à l'aide du couple MADHOC-DoDWAN, et lors d'une expérimentation de notre plate-forme sur des postes de communication utilisés dans le cadre des réseaux tactiques militaires.

4

ÉVALUATION

Notre protocole a été évalué au cours de plusieurs campagnes de tests, qui nous ont permis d'observer comment il se comporte dans différentes conditions. Ces campagnes ont été réalisées à la fois dans des conditions d'expérimentation réelles impliquant une douzaine d'ordinateurs portables au sein du laboratoire Valoria de l'Université de Bretagne Sud, et à l'aide du simulateur de réseau mobile MADHOC (*Metropolitan ad hoc network simulator*).

Dans ce chapitre nous présentons les résultats d'expérimentation de notre protocole de communication selon deux axes. D'une part, dans le paragraphe 4.1 nous présentons les résultats obtenus lors de l'évaluation de notre protocole de communication à l'aide du simulateur de réseaux mobiles ad hoc MADHOC [HGB06]. D'autre part, dans le paragraphe 4.2 nous présentons les résultats de l'expérimentation de la plate-forme de communication DoDWAN sur un banc de test constitué de plusieurs postes radio de type PR4G, qui sont des postes de radiotransmission utilisés par l'armée française.

4.1 ÉVALUATION PAR LA SIMULATION

Notre protocole de communication a été implémenté en Java, et embarqué dans la plate-forme intergicielle DoDWAN qui a été présentée dans le chapitre 3. Dans la mesure où il est assez difficile d'organiser et de réaliser des campagnes d'expérimentations impliquant des dizaines, voire des centaines de terminaux mobiles, DoDWAN a été conçu de telle sorte qu'il puisse être interfacé avec le simulateur MADHOC [HGB06]. Ce simulateur a été développé par le laboratoire LITIS de l'Université du Havre. Il permet de simuler des réseaux mobiles ad hoc (discontinus ou non) de très grande taille (jusqu'à plusieurs dizaines de milliers de nœuds) dans lesquels les terminaux peuvent suivre différents modèles de mobilité [HGD⁺06].

En utilisant la combinaison DoDWAN-MADHOC, nous avons réalisé un certain nombre de simulations dans le but d'observer les performances de notre protocole sous différentes conditions. Les paramètres utilisés lors de ces simulations ont été déterminés grâce à l'expérience acquise lors des expérimentations réelles que nous avons réalisées avant d'entamer les simulations. Le paragraphe 4.1.2 présente des résultats obtenus en réalisant une série de simulations, avec les paramètres de simulation et le scénario de communication décrits ci-dessous.

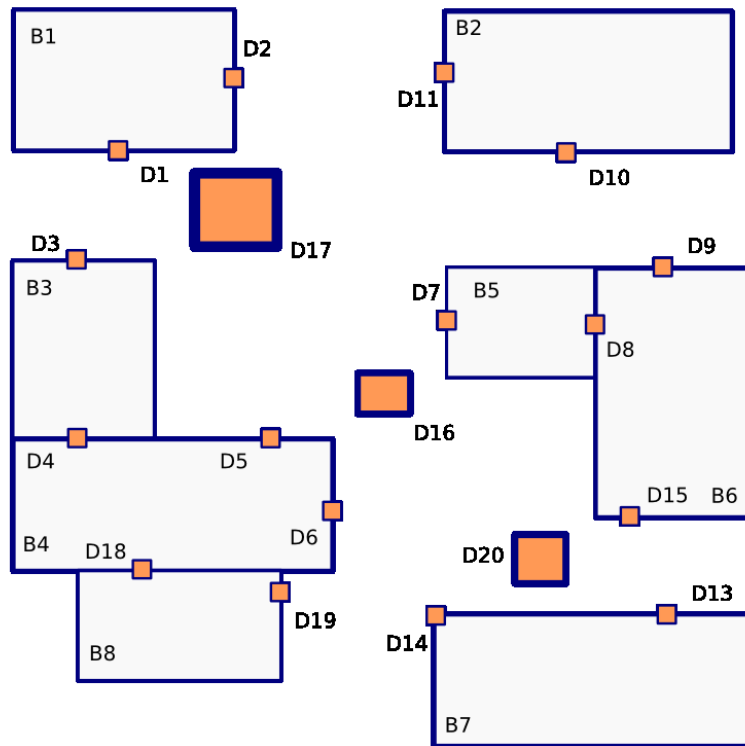


Figure 4.1 – Exemple d'environnement de type « campus » au sein duquel une population de terminaux mobiles communicants peut évoluer. Les bâtiments du campus sont représentés par les rectangles vides, tandis que les portes et points de passage obligatoires sont représentés par des rectangles oranges.

4.1.1 CONDITIONS DE SIMULATION

Dans les paragraphes suivants nous précisons les conditions de simulation utilisées pour obtenir les résultats présentés dans le paragraphe 4.1.2. Ces conditions précisent les paramètres qui caractérisent l'environnement au sein duquel les terminaux mobiles évoluent, le schéma de mobilité suivis par les terminaux dans cet environnement, ainsi que le scénario de communication précisant les conditions de publication des documents partagés par les terminaux mobiles.

4.1.1.1 ENVIRONNEMENT ET SCHÉMA DE MOBILITÉ

Nous considérons un scénario de simulation dans lequel une population de 120 individus évolue dans un environnement de type « campus » (ou dans l'enceinte d'une entreprise) comme illustré dans la figure 4.1. Cet environnement est constitué de plusieurs bâtiments, répartis sur une superficie de 800 mètres × 800 mètres, et identifiés par les étiquettes B1, B2, etc. Pour entrer et sortir d'un bâtiment un individu doit obligatoirement passer par une porte. Par exemple, les

portes D13 et D14 permettent d'entrer et de sortir du bâtiment B7. De plus, les déplacements des individus d'un bâtiment à un autre sont contraints. Pour ce faire nous avons définis les chemins devant être suivi par les individus évoluant dans cet environnement. Par exemple, pour passer du bâtiment B8 à B5, un individu peut emprunter plusieurs chemins alternatifs : B8-D19-D16-D7-B5 ou B8-D18-D5-D16-D7-B5.

Chacun des individus évoluant dans cet environnement est équipé d'un ordinateur portable doté d'une interface Wi-Fi fonctionnant en mode ad hoc. La mobilité des individus — et donc, indirectement, celle des terminaux qu'ils transportent — est simulée en utilisant une variante du modèle *Random Waypoint* traditionnel : un individu peut rester immobile dans un bâtiment pendant un certain temps, avant de se déplacer vers une destination choisie au hasard dans l'un quelconque des bâtiments. Les déplacements au sein d'un bâtiment sont donc possibles, au même titre que les déplacements entre bâtiments en exploitant les chemins prédéfinis.

Pour obtenir les résultats décrits plus loin, les paramètres de mobilité suivants ont été utilisés : la vitesse de déplacement des individus peut varier entre 0.5 m/s et 2 m/s (ce qui correspond à des vitesses de déplacements typiques pour des piétons). Un individu peut rester immobile entre deux déplacements consécutifs, pour une durée se situant entre 30 secondes et 5 minutes. La proportion de déplacements au sein d'un même bâtiment est fixée à 40 %, contre 60 % pour les déplacements entre bâtiments, c'est-à-dire qu'il y a 60 % de chance qu'un terminal se déplace en direction d'un autre bâtiment. Les interfaces équipant les terminaux mobiles sont supposées avoir une portée de transmission omni-directionnelle de 40 mètres en milieu fermé (c'est-à-dire à l'intérieur d'un bâtiment) et de 100 mètres en milieu ouvert. Enfin, puisque dans des conditions d'utilisation réelles un ordinateur portable est en général éteint ou mis en veille lorsque son propriétaire se déplace, le modèle de mobilité utilisé tient compte de cette observation. Avec ce modèle, un ordinateur portable est considéré comme étant éteint et donc incapable de communiquer avec tout autre équipement lorsque son propriétaire est en mouvement, et comme étant allumé et donc apte à interagir avec les équipements voisins lorsque son propriétaire est à l'arrêt.

4.1.1.2 SCÉNARIO DE COMMUNICATION

Nous considérons un scénario dans lequel les terminaux mobiles produisent de nouveaux documents, et les injectent dans le réseau à un rythme moyen de 1 document (par terminal) toutes les 5 minutes. Chaque terminal injecte des documents dans le réseau pendant une durée de une heure. Les charges utiles (ou contenus) des documents injectés par les terminaux dans le réseaux sont de types différents, et de tailles différentes.

Chaque document porte, dans son descripteur, une étiquette qui le place dans une certaine catégorie thématique. Il y a 16 catégories distinctes, mais chaque document s'inscrit dans seulement l'une de ces catégories. D'autres informations sont insérées dans le descripteur de chaque document injecté, par exemple, lorsque le document à injecter dans le réseau contient une photographie, des attributs spécifiques précisant les caractéristiques de cette photographie sont ajoutés au descripteur du document (type du fichier, taille du fichier, date de publication, noms des personnes figurant sur la photographie, dimension de la photographie, etc.).

Chaque terminal mobile affiche de l'intérêt pour 2 des 16 catégories, c'est-à-dire pour 1/8 du trafic global généré par les terminaux mobiles, et ne souhaite donc recevoir que les documents relatifs à l'une ou l'autre de ces deux catégories. Le nombre total de terminaux dans le réseau, fixé à 120, a été choisi de telle sorte qu'on puisse attribuer un profil d'intérêt distinct à chacun des terminaux évoluant dans la simulation. En d'autres termes, on ne peut trouver deux terminaux dans le réseau qui affichent exactement le même profil d'intérêt, et soient donc intéressés exactement par les mêmes types de documents.

4.1.1.3 PARAMÈTRES PROTOCOLAIRES

Le comportement général de notre protocole est conditionné par quelques paramètres.

Le premier de ces paramètres est la période avec laquelle un terminal mobile va diffuser des annonces contenant son profil d'intérêt et le catalogue des documents qu'il propose à ses voisins. Une valeur convenable pour cette période peut être déduite des conditions dans lesquelles le protocole doit être utilisé, et notamment des caractéristiques de mobilité des terminaux dans cet environnement. Ainsi, avec les paramètres de simulation décrits plus haut, les terminaux mobiles sont supposés être transportés par des piétons, et n'être actifs que lorsque leurs propriétaires sont immobiles. Dans de telles conditions, il n'est pas nécessaire d'adopter une période d'annonce très courte. En l'occurrence, une période d'annonce de 15 secondes suffit pour laisser aux terminaux, lors d'une réactivation consécutive à un déplacement, le temps de découvrir les terminaux voisins, et d'échanger des documents avec eux. Une période d'annonce plus courte serait toutefois nécessaire si les terminaux mobiles étaient susceptibles de communiquer pendant leurs déplacements (comme ce pourrait être le cas, par exemple, pour des smartphones), cette période devant en outre être d'autant plus courte que les terminaux en question se déplacent rapidement, et qu'ils sont donc susceptibles d'observer des contacts de courte durée avec des équipements voisins. Inversement, la période d'annonce pourrait être rallongée si les terminaux considérés étaient susceptibles de passer beaucoup plus de temps au même endroit, et donc d'observer autour d'eux un voisinage relativement stable.

Le deuxième paramètre qui peut être ajusté dans notre protocole est le nombre de sauts admissible dans le cas du relais immédiat par la couche inférieure du protocole (paragraphe 2.5), et en particulier lorsqu'un terminal diffuse une annonce à l'intention de ses voisins. En ajustant ce paramètre, on peut en effet déterminer l'étendue de la « sphère de communication » au centre de laquelle se trouve chaque terminal mobile, c'est-à-dire l'envergure du voisinage avec lequel il est disposé à échanger des documents avant de se déplacer de nouveau dans le réseau.

Un troisième paramètre, qui influe sur le protocole de diffusion sélective défini dans la couche inférieure (paragraphe 2.5.3), est le délai d'attente avant la diffusion des documents par un terminal. Rappelons que suite à la diffusion d'une annonce un terminal est susceptible de recevoir plusieurs requêtes pour un même document en provenance de différents voisins. En cherchant à limiter le coût de la diffusion du document nous avons décidé, lors de la conception du protocole, d'exploiter des arbres de diffusion. Cette approche nécessite qu'un terminal venant de diffuser une annonce attende un certain délai pour pouvoir recevoir toutes les requêtes de documents, et pouvoir diffuser chaque document demandé de façon à satisfaire tout les demandeurs à la fois. Ce délai d'attente doit donc permettre à une annonce d'être relayée par les

terminaux dans la sphère de communication du terminal annonceur, aux récepteurs de l'annonce de la traiter, et le cas échéant aux requêtes de remonter depuis ceux-ci vers l'annonceur. Dans nos simulations, la sphère de communication d'un terminal a une étendue maximale de 5 sauts. Le relais de l'annonce sur 5 sauts est de courte durée, en effet, les délais de transmission et de traitement pour le relais immédiat sont très faibles, notamment car le protocole de communication ne s'appuie pas sur des transmissions fiabilisées. Une annonce mettra au plus quelques dizaines de millisecondes pour être relayée dans la sphère de communication du terminal annonceur. De plus, le traitement d'une annonce par un terminal est instantané, si des documents sont identifiés comme faisant défaut la requête est donc adressée à l'annonceur immédiatement après la réception de son annonce. Cette requête remontera au maximum 5 sauts pour être reçue par son destinataire, les délais de transmission et de relais de la requête étant très faibles, elle mettra quelques dizaines de millisecondes avant d'être reçue par l'annonceur. Le simulateur fonctionnant en temps discret, nous avons calculé le délai d'attente en fonction du pas de simulation (fixé à 100 millisecondes) et du nombre de sauts total devant être parcouru par l'annonce puis par la requête (maximum 10 sauts). Par exemple, lorsque le nombre de sauts est fixé à trois, nous avons fixé le délais d'attente à 600 millisecondes.

4.1.2 RÉSULTATS ET OBSERVATIONS

Dans les paragraphes suivants, nous présentons des résultats obtenus en réalisant une série de simulations, en exploitant les conditions de simulations évoquées précédemment. En particulier, ces résultats nous permettent de vérifier si les choix réalisés lors de la conception de notre protocole de communication satisfont nos objectifs.

4.1.2.1 VITESSE DE PROPAGATION DES DOCUMENTS

Notre objectif premier est d'observer l'impact de la portée du relais immédiat multi-sauts sur les performances générales de notre protocole. Le résultat attendu est que, lorsque chaque terminal mobile est autorisé à utiliser le relais multi-sauts afin d'accroître la population des voisins avec lesquels il peut interagir, la dissémination des documents dans le réseau s'effectue plus rapidement que lorsque chaque terminal ne peut interagir qu'avec ses voisins directs.

Pour vérifier que cette hypothèse est effectivement satisfaite, nous considérons dans un premier temps un scénario non réaliste dans lequel les documents peuvent se propager éternellement dans le réseau. Pour ce faire, nous supposons que la capacité du cache est illimitée sur chacun des terminaux considérés dans la simulation, et que les documents injectés dans le réseau n'ont pas de durée de vie précise.

Les résultats présentés ci-dessous ont été obtenus en réalisant des simulations de quatre heures (en temps simulé). Le modèle de mobilité utilisé dans cette campagne de simulations « garantit » que chaque terminal mobile entrera à un moment ou un autre en contact avec chacun des autres terminaux du réseau. Dans ces conditions, un document pouvant demeurer éternellement dans le réseau est censé atteindre durant la simulation tous les terminaux mobile intéressés.

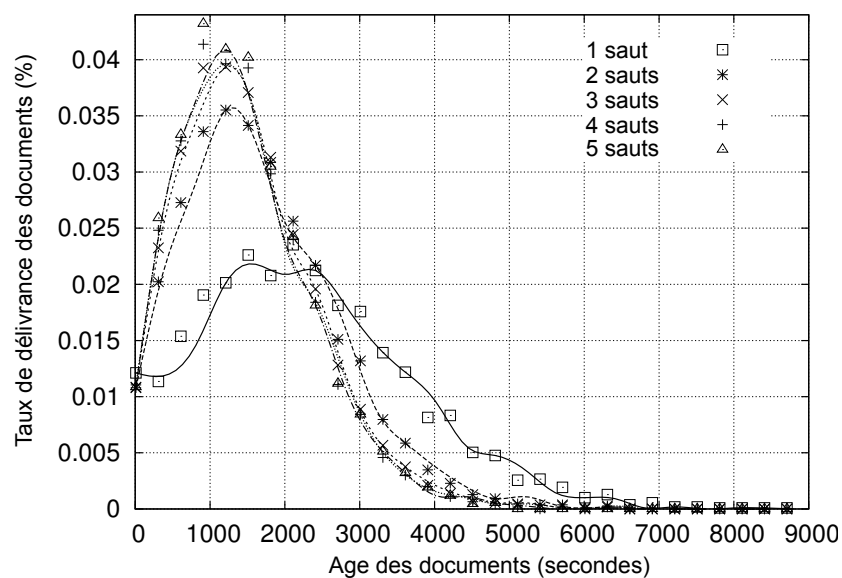


Figure 4.2 – Distribution non cumulée de l'âge des documents lors de leur réception par un terminal intéressé

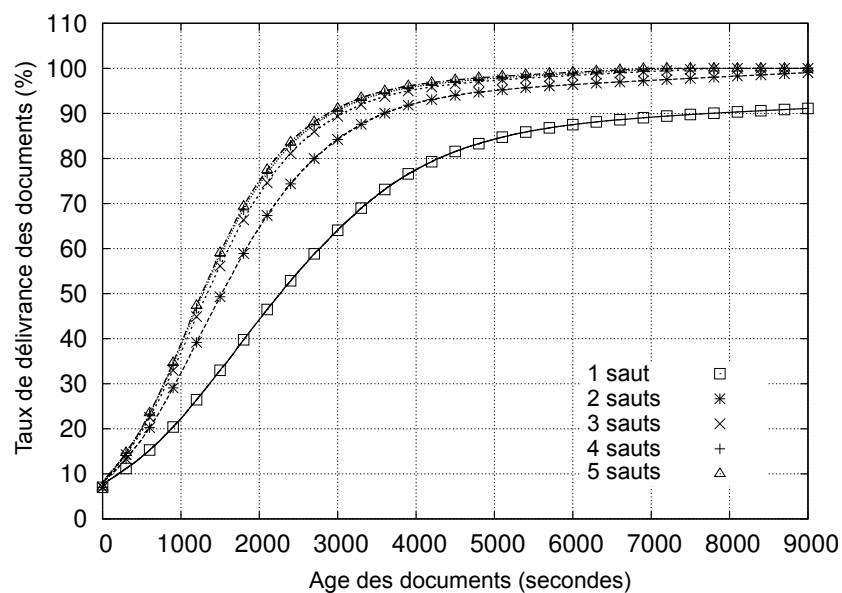


Figure 4.3 – Distribution cumulée de l'âge des documents lors de leur réception par un terminal intéressé

Le temps nécessaire pour qu'un document atteigne un récepteur précis peut cependant être influencé par les paramètres protocolaire, et en particulier par l'étendue du voisinage avec lequel chaque terminal est autorisé à interagir.

La figure 4.2 montre la distribution normalisée de l'âge des documents lors de leur réception, et la figure 4.3 montre la distribution cumulée correspondante. Intéressons nous au temps moyen nécessaire aux documents pour atteindre les terminaux pour lesquels ils présentent de l'intérêt. Considérons tout d'abord le cas où les terminaux ne peuvent utiliser que des transmissions à un saut pour interagir avec leur voisinage. En d'autres termes, il s'agit d'un cas dans lequel la couche inférieure de notre protocole ne joue aucun rôle, seules les communications entre voisins directs étant possibles. On peut constater que, dans de telles circonstances, environ 40 % des documents atteignent néanmoins les terminaux intéressés en moins de 30 minutes. Au bout d'une heure, environ 75 % des documents sont réceptionnés par les récepteurs intéressés, et après deux heures environ 90 % des documents ont atteint les récepteurs intéressés. Ces valeurs vont nous servir de référence pour évaluer l'impact du relais immédiat multi-sauts, tel qu'il est assuré par la couche inférieure de notre protocole.

La courbe de la figure 4.2 montre que, lorsque du relais à deux sauts est utilisé, c'est-à-dire lorsque un terminal peut atteindre ses voisins à 2 sauts via des transmissions multi-sauts impliquant d'autres terminaux mobiles, la plupart des documents parviennent aux terminaux intéressés en moins de 20 minutes alors qu'il faut environ 30 minutes lors de communication entre voisins directs. En utilisant des transmissions à deux sauts, environ 98 % des documents parviennent en fait aux terminaux intéressés en moins de deux heures, environ 90 % y parviennent en moins d'une heure, et environ 60 % en moins de 30 minutes.

Une amélioration similaire, quoique moins importante quantitativement, peut être observée lorsque l'on étend la sphère de communication de chaque terminal en l'autorisant à interagir avec ses voisins à 3, 4, et 5 sauts. En fait, avec les paramètres de simulation utilisés dans cette campagne d'évaluation, les îlots pouvant se former au sein des bâtiments ont une élongation qui varie entre 0 (lorsqu'un terminal isolé n'a aucun voisin) et 7 sauts, avec une valeur moyenne de 4,2 sauts. Ceci explique pourquoi le fait d'étendre la portée (théorique) du relais immédiat multi-sauts dans le paramétrage de notre protocole n'apporte pas nécessairement d'amélioration significative dans la simulation. Lorsqu'un terminal est autorisé à diffuser ses annonces jusqu'à, par exemple, 8 sauts de là, encore faut-il qu'il ait effectivement des voisins situés aussi loin de lui-même. Une raison complémentaire est que la vitesse de propagation des documents dans le réseau est directement dépendante des déplacements des terminaux entre et au sein des bâtiments constituant l'environnement de simulation et de la vitesse à laquelle les transporteurs mobiles de ces terminaux hébergeant les documents, c'est-à-dire, ici, des piétons se déplacent dans la zone de simulation.

Cette première expérience confirme qu'en augmentant la sphère de communication de chaque terminal mobile à quelques sauts, notre protocole permet bien une dissémination plus rapide des documents dans chaque îlot, ce qui contribue aussi à faire croître plus rapidement le nombre de terminaux porteurs d'un même document, et permet au final une dissémination plus rapide des documents sur l'ensemble des îlots non connectés constituant le réseau simulé.

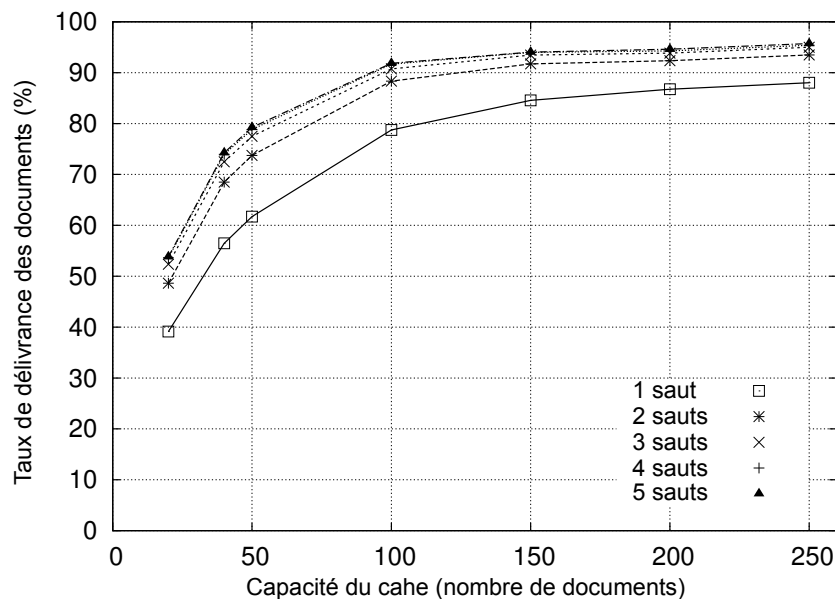


Figure 4.4 – Variation du taux de délivrance (défini comme le pourcentage de documents atteignant effectivement les récepteurs intéressés) des documents en fonction de la capacité du cache sur chaque terminal mobile et du nombre de sauts exploité lors du relais multi-sauts.

4.1.2.2 INFLUENCE DE LA CAPACITÉ DU CACHE

Dans les simulations dont les résultats ont été discutés plus haut, nous avons supposé que les documents pouvaient se propager indéfiniment dans le réseau. Cependant, une telle hypothèse n'est évidemment guère réaliste, dans la mesure où les ressources disponibles dans un réseau de type MANET sont en général limitées, et souvent même inférieures à celles dont on peut disposer dans un environnement filaire. Par exemple, le cache dans lequel un terminal mobile peut stocker des documents est forcément de capacité limitée. Une politique de gestion de cache appropriée doit donc être définie et appliquée sur chaque terminal mobile afin d'éviter la saturation de cache et, si cette saturation survient malgré tout, de résoudre ce problème.

La figure 4.4 montrent l'influence de la capacité du cache sur les performances observées lors de la dissémination de documents. Pour produire ces résultats nous avons mené une nouvelle campagne de simulations, en faisant varier sur chaque terminal la capacité du cache entre 20 et 250 documents. Pendant ces simulations, d'une durée de deux heures en temps simulé, la politique de gestion de cache appliquée exploitait la fonction de rang que nous avons définie au paragraphe 2.4.2.5 : lorsqu'un cache atteignait le niveau de saturation, le document ayant le poids le plus faible était supprimé afin de libérer de la place pour un document de poids plus élevé.

Les résultats présentés figure 4.4 présentent les taux de délivrance (défini comme le pourcentage de documents atteignant effectivement les récepteurs intéressés), variant en fonction de la capacité du cache sur chaque terminal. On peut tout d'abord constater que les chiffres présentés confirment l'intuition naturelle selon laquelle un terminal mobile doté d'un cache de

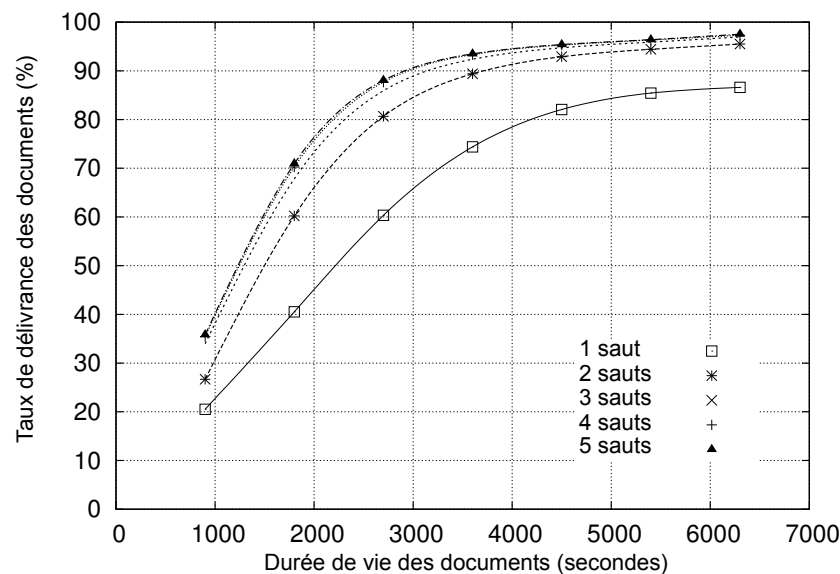


Figure 4.5 – Variation du taux de délivrance des documents en fonction de la durée de vie accordée à chaque document

grande capacité est en mesure de transporter les documents plus longtemps et donc plus loin dans le réseau.

On peut également observer l'influence de l'utilisation du relais immédiat multi-sauts sur la dissémination des documents. On peut remarquer que le taux de délivrance augmente de manière significative lorsque la portée du relais immédiat est étendue à quelques sauts autour de chaque terminal. Considérons, par exemple, le cas où chaque terminal ne dispose que d'un cache capable de stocker 100 documents. Dans ces conditions, les documents injectés dans le réseau ne parviennent, en moyenne, qu'à 78 % des récepteurs intéressés si chaque terminal ne peut interagir qu'avec ses voisins directs. En revanche, ce taux est accru de 10 %, lorsque chaque terminal peut interagir avec ses voisins à 2 sauts, et il est encore accru de 2 % supplémentaires lorsque chaque terminal peut atteindre ses voisins à 3 sauts.

4.1.2.3 INFLUENCE DE LA DURÉE DE VIE DES DOCUMENTS

Une autre manière d'éviter que les documents demeurent éternellement dans le réseau est de donner à chaque document une durée de vie précise, lors de son injection dans le réseau. Ainsi, dès qu'un document devient obsolète, toutes ses copies sont automatiquement supprimées des caches dans lesquelles elles pouvaient être stockées. Cette méthode peut d'ailleurs être utilisée soit en remplacement, soit en complément de celle qui consiste à limiter la capacité des caches sur les terminaux mobiles.

Les résultats présentés dans la figure 4.5 montrent l'influence de la durée de vie des documents sur l'efficacité de leur dissémination. Ces résultats ont été obtenus avec des caches de capacité illimitée, afin que les deux types de contraintes (durée de vie des documents et capacité

des caches) n'interfèrent pas pendant les simulations. Comme pour l'évaluation de l'impact de la capacité du cache sur les performances du protocoles, les simulations réalisées dans le cadre de cette évaluation avait pour durée deux heures en temps simulé, et respectaient les conditions de simulation présentées dans le paragraphe 4.1.1.

La figure 4.5 met en évidence l'évolution du taux de documents parvenant aux récepteurs intéressés en fonction de la durée de vie attribuée à ces documents. Comme on pouvait s'y attendre, le taux de délivrance s'accroît avec la durée de vie des documents. Cependant, on peut constater que, cette fois encore, l'utilisation du mécanisme de relais immédiat multi-sauts permet une amélioration significative des performances. Ainsi, lorsque les documents ont une durée de vie de seulement 30 minutes, ils ne sont reçus, en moyenne, que par 30 % des récepteurs intéressés si seuls les échanges entre voisins directs (à 1 saut) sont possibles. Ce taux est accru de 20 % lorsque chaque terminal peut atteindre ses voisins à 2 sauts, et il l'est encore de 7 % lorsque chaque terminal peut atteindre ses voisins à 3 sauts.

Il est à noter que le fait de limiter la durée de vie des documents n'est pas tout à fait équivalent au fait de limiter la capacité du cache sur chaque terminal, bien que ces deux approches puissent être utilisées pour réguler la quantité de documents en cours de dissémination dans le réseau. En fait, la capacité du cache sur un terminal donné résulte en général directement de la quantité de ressources de stockage disponible sur ce terminal. Il s'agit donc pour l'essentiel d'une contrainte liée à la gestion même de ce terminal, en fonction des ressources dont il dispose. En revanche, la durée de vie octroyée à un document doit être déterminée par l'émetteur de ce document. Elle peut être fixée soit sur la base d'une estimation du temps nécessaire à ce document pour atteindre tout ou partie des terminaux qu'il va intéresser, soit sur la base d'une estimation de la durée pendant laquelle les informations contenues dans ce document doivent être considérées comme étant pertinentes pour les terminaux récepteurs. Dans le premier cas, la décision est d'ordre stratégique et nécessite une certaine connaissance des caractéristiques du réseau, telle que son envergure, les schémas de mobilité des terminaux, les fréquences des contacts, etc. Dans le second cas, elle est plutôt d'ordre sémantique, puisqu'elle conditionne la persistance des documents dans le réseau en fonction des informations qu'ils apportent aux récepteurs.

4.1.2.4 INFLUENCE DU MÉCANISME D'ADAPTATION DU CATALOGUE

Dans le chapitre 2 nous avons affirmé que notre protocole a été conçu de manière à consommer aussi peu de ressources que possible. Nous avons notamment expliqué que le catalogue inséré par chaque terminal dans ses annonces périodiques est construit en tenant compte des profils d'intérêt des terminaux voisins.

La figure 4.6 montre comment la taille du catalogue devant être inséré dans chaque annonce par un terminal particulier évolue au fil du temps, en fonction du voisinage actuel de ce terminal, des profils d'intérêt de ses voisins du moment, et bien sûr des documents présents dans son cache. Ces résultats ont été obtenus au cours d'une simulation pendant laquelle la capacité du cache sur le terminal considéré était fixée à 100 documents. En outre, chaque document produit pendant la simulation avait une durée de vie fixée à 60 minutes, la portée du relais multi-sauts était limitée à 2 sauts et la simulation durait deux heures en temps simulé.

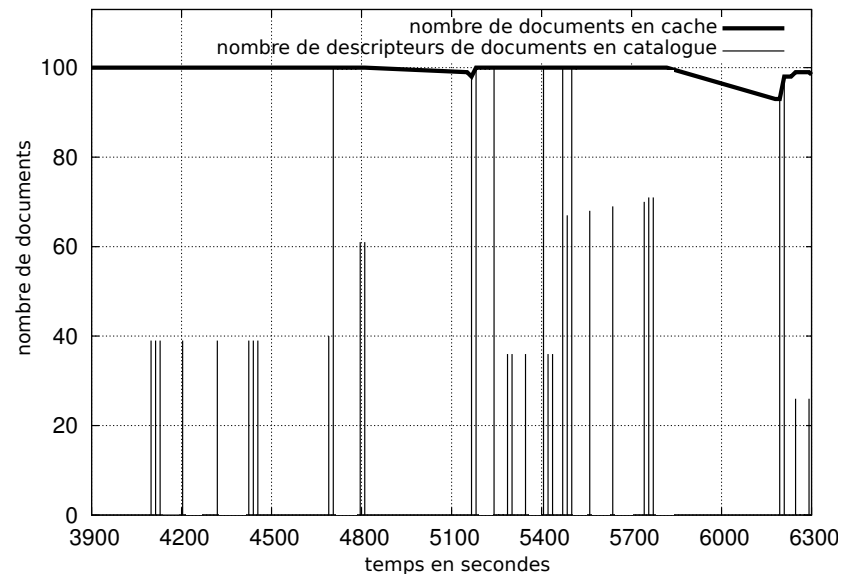


Figure 4.6 – Évolution de la taille du catalogue et du niveau d’occupation du cache sur un terminal mobile particulier au cours de la simulation

On peut constater dans la figure 4.6 que, pendant la durée d’exécution observée, le cache est presque constamment plein. Les documents sont supprimés du cache dès qu’ils deviennent obsolètes, mais ils sont rapidement remplacés par de nouveaux documents reçus de terminaux voisins. Pourtant le nombre de descripteurs insérés dans le catalogue diffusé toutes les 15 secondes par le terminal observé est souvent bien inférieur au nombre de documents disponibles dans le cache, et tombe même fréquemment à zéro. Dans ce dernier cas le catalogue inséré dans l’annonce est alors vide ou les conditions sont réunies pour que le terminal diffuse une annonce courte.

Ces observations confirment que le terminal considéré ici bâtit bien son catalogue en fonction des profils d’intérêt de ses voisins, et qu’il est capable de s’adapter dynamiquement à la stabilité de son voisinage en évitant de diffuser des annonces complètes et donc de bâtir inutilement de nouveaux catalogues. Parfois il n’a aucun voisin (et le catalogue accompagnant l’annonce de présence qu’il diffuse malgré tout pour signaler sa présence est donc vide), et parfois ses voisins affichent des profils d’intérêt qui ne correspondent pas du tout avec les documents qu’il transporte. Parfois seul un nombre limité de documents qu’il héberge dans son cache sont susceptibles d’intéresser ses voisins. Enfin, parfois le voisinage d’un terminal est suffisamment stable pour qu’il diffuse une annonce courte, en évitant ainsi de bâtir inutilement un catalogue.

En adaptant continuellement le contenu du catalogue diffusé à l’intention de ses voisins, un terminal peut donc contribuer à réduire de manière significative le poids de ses annonces périodiques, et par conséquent la quantité de travail imposée aux voisins lorsque ceux-ci doivent recevoir et analyser ces annonces. Bien sûr, nos efforts en vue de réduire la taille des catalogues s’avèrent plus rentables lorsque chaque terminal héberge un grand nombre de documents dans

Mécanisme d'adaptation de l'annonce	Volume en kilo octets du trafic de contrôle	Nombre de message de contrôle	Satisfaction en pourcentage
Désactivé	36 407 (x1)	63 593 (x1)	75.3 (x1)
Activé	30 480 (x0.71)	78 219 (x1.23)	74.4 (x0.99)

Table 4.1 – Comparaison du volume de trafic de contrôle nécessaire au fonctionnement du protocole de communication lors de l'activation du mécanisme d'adaptation de l'annonce.

son cache, et est en même temps confronté à des voisins aux profils d'intérêt sélectifs.

4.1.2.5 INFLUENCE DU MÉCANISME D'ADAPTATION DU FORMAT L'ANNONCE

Dans le chapitre 2 nous avons indiqué que dans certains cas la taille d'une annonce périodique peut être fortement réduite (paragraphe 2.4.2.1). Pour ce faire, nous avons déterminé des conditions qui lorsqu'elles sont vérifiées permettent à un terminal de s'abstenir de diffuser une annonce contenant son profil d'intérêt et un catalogue bati en fonction des centres d'intérêt des voisins et de diffuser une annonce courte dont le volume est bien inférieur.

Le tableau 4.1 montre une comparaison du volume de trafic de contrôle nécessaire au fonctionnement de notre protocole de communication, entre une version utilisant le mécanisme d'adaptation du format de l'annonce et une autre sans ce mécanisme. Ces résultats ont été obtenus en réalisant deux simulations dans des conditions identiques. Dans ces simulations, d'une durée d'une heure en temps simulé, la capacité du cache des terminaux était fixée à 200 documents, chaque document produit avait une durée de vie fixée à 60 minutes, et la portée du relais multi-sauts était limitée à 2 sauts.

Grâce à ces résultats on peut constater que, le trafic de contrôle engendré par le protocole est inférieur lorsque le mécanisme d'adaptation du format de l'annonce est utilisé. Ce mécanisme adaptatif permet effectivement de mettre à profit les périodes de stabilité du réseau pour réduire le volume des messages échangés. En effet, la version exploitant les annonces courtes permet de réduire la charge induite par le trafic de contrôle d'environ 30 %.

Les résultats montrent aussi que l'utilisation du mécanisme d'adaptation du format de l'annonce implique un plus grand nombre de messages de contrôle (environ 23 %). Cela s'explique par le fait que, lorsqu'un terminal réceptionne une annonce courte pour laquelle il ne dispose pas de la version complète, ce terminal doit alors adresser une requête à l'annonceur l'invitant à diffuser immédiatement la version complète correspondant à l'annonce courte.

On peut aussi observer que le taux de document parvenant aux récepteurs intéressés est légèrement inférieur lorsque le mécanisme d'adaptation du format de l'annonce est activé. Dans le cas présent l'écart entre les taux de délivrance des documents des deux versions du protocole est faible. Cet écart existe car le mécanisme d'adaptation du format de l'annonce introduit des délais dans l'annonce au voisinage. Ces observations confirment que le mécanisme d'adaptation

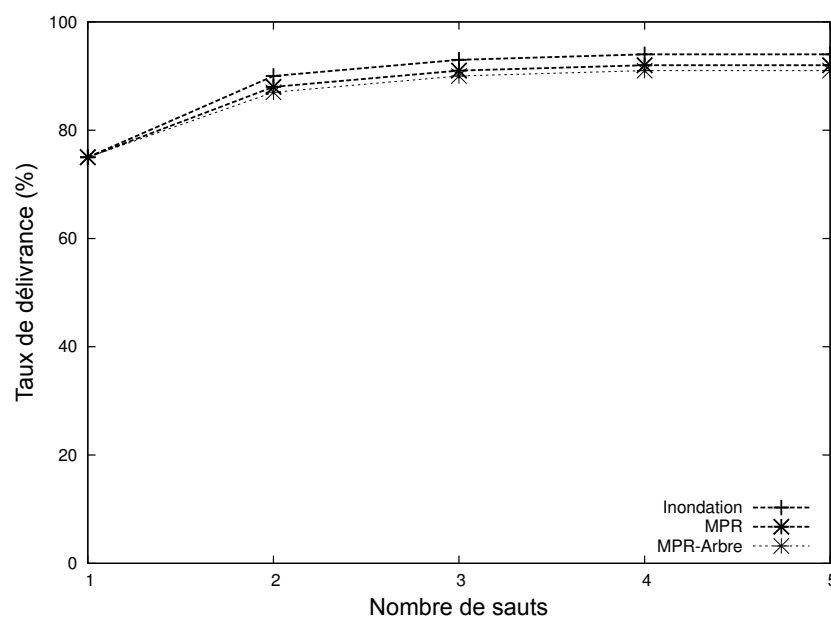


Figure 4.7 – Comparaison des modes de diffusion par inondation, via des relais multi-points et des arbres en termes de performances.

dynamique du format de l'annonce par les terminaux, bien qu'il nécessite un nombre accru de messages de contrôles, permet d'une part aux terminaux de réduire l'utilisation du médium radio (et donc implicitement de leurs ressources), et d'autre part de conserver un taux de délivrance très proche d'une version n'exploitant pas ce mécanisme.

4.1.2.6 COÛT DU RELAIS IMMÉDIAT MULTI-SAUTS

Les résultats présentés dans le paragraphe 4.1.2.1 ont montré qu'en utilisant le mécanisme de relais immédiat multi-sauts, la dissémination de documents dans le réseau peut être réalisée de façon plus rapide, et donc plus efficace. Ils montrent également qu'une faible extension de la sphère de communication de chaque terminal mobile en lui permettant par exemple d'atteindre ses voisins à 2 ou 3 sauts, peut déjà apporter un progrès significatif par rapport au cas où seuls sont possibles les échanges entre voisins directs.

L'inconvénient des transmissions multi-sauts est bien évidemment qu'elles mobilisent énormément de ressources. En effet, à chaque fois qu'un terminal relaie un message, cette opération draine la batterie de ce terminal, mais aussi celles des récepteurs voisins, tout en monopolisant le canal radio dans le voisinage de l'émetteur.

En concevant notre protocole nous avons choisi de nous appuyer sur deux protocoles de diffusion différents : la diffusion via des relais multi-points (principe emprunté au protocole OLSR) afin d'assurer la diffusion des annonces des terminaux dans leur sphère de communication, et la diffusion sélective via des arbres pour permettre à un terminal de diffuser un document vers les terminaux qui en ont fait la demande. De toute évidence, il aurait été plus simple pour

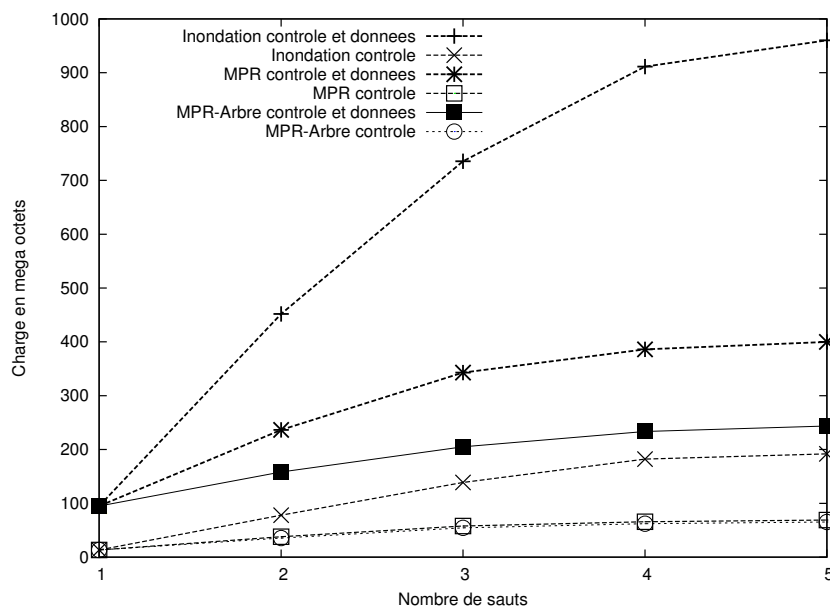


Figure 4.8 – Comparaison des modes de diffusion par inondation, via des relais multi-points et des arbres en termes de coût.

nous de mettre en œuvre un simple algorithme d'inondation pour réaliser la diffusion des annonces et des documents, ou de mettre en œuvre le même algorithme pour la diffusion des annonces et des documents. Puisque les résultats présentés plus haut montrent qu'une amélioration significative des performances de la dissémination des documents peut être obtenue en relayant les messages sur un très faible nombre de sauts (dans le scénario considéré deux ou trois sauts), on peut se demander si l'utilisation combinée de la diffusion via des relais multi-points et via des arbres de diffusion dans un tel contexte apporte un quelconque bénéfice par rapport à l'utilisation d'un unique protocole de diffusion tel que la diffusion via des relais multi-points ou via simple mécanisme d'inondation.

Pour comparer les coûts de fonctionnement respectifs des trois approches ci-dessus, des versions dégradées du protocole ont été mises en œuvre :

- la première version met en œuvre les deux protocoles de diffusion présentés dans les paragraphes 2.5.1 et 2.5.3, respectivement la diffusion via des relais multi-points et la diffusion via des arbres,
- la seconde version met en œuvre uniquement le protocole de diffusion via les relais multi-point, qui sert donc à la fois pour la diffusion des annonces et pour celle des documents,
- la troisième version met en œuvre l'algorithme de diffusion par inondation

Nous avons ensuite comparé le comportement de ces trois versions du protocole, en répétant bien sûr dans les trois cas les mêmes scénarios de mobilité et de communication.

Les résultats sont présentés dans la figure 4.7 qui montre les performances observées avec les trois approches (performances exprimées ici en termes de pourcentage de documents atteignant les terminaux intéressés), et dans la figure 4.8 qui montre le coût observé avec chaque

approche (coût exprimé ici en termes du volume des messages émis sur le canal radio, en distinguant trafic de contrôle et trafic de données). Ces résultats ont été produits en réalisant des simulations de quatre heures (en temps simulé) avec les conditions présentées dans le paragraphe 4.1.1, des caches de capacité illimitée, et des documents ayant chacun une durée de vie d'une heure.

On peut tout d'abord constater que les trois versions du protocole ne donnent pas tout à fait les mêmes taux de délivrance. Ceci est dû au fait qu'avec les deux versions de notre protocole utilisant les MPRs pour la diffusion des annonces périodiques la dissémination des documents s'effectue légèrement plus lentement qu'avec la version reposant sur le mécanisme d'inondation. En effet, un terminal dont le voisinage est modifié doit attendre quelques temps (précisément, deux cycles d'annonce consécutifs) avant de découvrir ses nouveaux voisins à 2 sauts, et donc de pouvoir adapter ses annonces à leurs profils d'intérêts respectifs. Dans la version reposant sur de l'inondation, en revanche, ce temps de latence initial n'existe pas : un terminal dont le voisinage à 2 sauts change peut immédiatement proposer un catalogue de documents susceptibles d'intéresser ses nouveaux voisins.

On observe aussi sur la figure 4.7 que le taux de délivrance de documents est légèrement inférieur avec la version standard et la version utilisant uniquement la diffusion via des MPRs qu'avec la version pratiquant l'inondation. Cette différence demeure cependant inférieure à 3 %, alors que le coût relatif lié à l'utilisation de chacune des méthodes de diffusion est fort différent. On remarque sur cette même figure que le taux de délivrance de documents est légèrement inférieur lorsque la diffusion des documents est réalisée via des arbres de diffusion. Ceci vient du fait que la diffusion via des arbres de diffusion introduit un délai d'attente avant la diffusion des documents demandés par les voisins, durant ce délai d'attente un terminal qui a sollicité la diffusion d'un document ou un terminal identifié comme devant relayer le document peut se mettre en veille et nuire à la diffusion du document. De plus, à la différence d'une diffusion via les MPRs, un document diffusé via un arbre de diffusion n'est pas réceptionné par l'ensemble des terminaux situés dans la sphère de communication du terminal émetteur mais uniquement par un nombre très limité de terminaux (c'est-à-dire les demandeurs). De ce fait, les terminaux ont moins de chance de réceptionner des documents les intéressant sans en avoir fait le demande dans la version exploitant les arbres pour la diffusion des documents.

On peut observer dans la figure 4.8 que, le volume du trafic de contrôle nécessaire au fonctionnement du protocole de communication est très nettement supérieur avec le mécanisme d'inondation qu'avec le mécanisme reposant sur la diffusion via des relais multi-points. Ce constat conforte notre décision de nous appuyer sur des relais multi-points pour assurer la diffusion des annonces tout autour d'un terminal émetteur.

De plus, on peut constater sur cette même figure que le coût occasionné par la diffusion des documents (trafic de données) est très nettement inférieur avec le protocole de diffusion sélective qu'avec l'utilisation des MPRs et de l'inondation. La diffusion via des arbres permet à un terminal émetteur d'un document de préciser vers quels terminaux ce document doit être relayé, et donc ainsi de limiter le nombre de diffusions utiles à l'acheminement du document vers les terminaux demandeurs. Alors que via l'inondation ou via les relais multi-points un document est relayé pour atteindre l'ensemble des terminaux se situant dans la sphère de communication de l'émetteur.

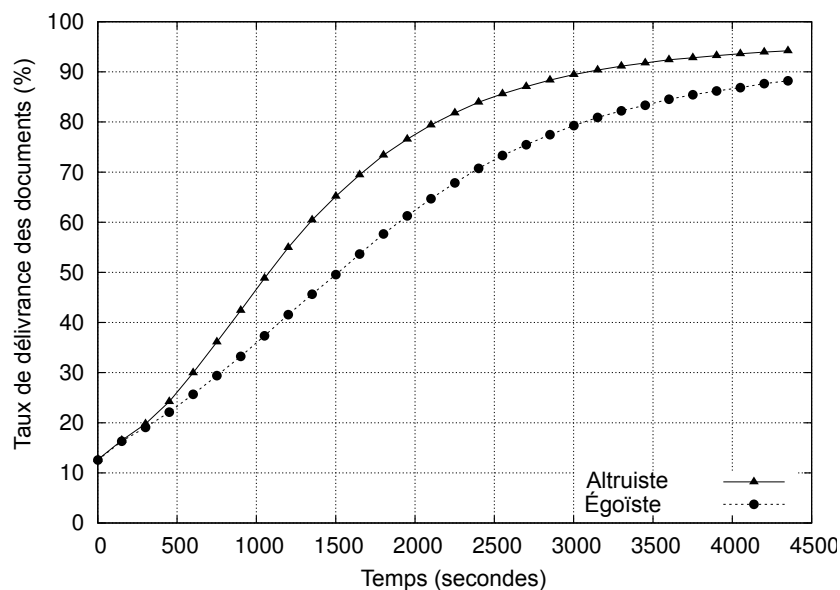


Figure 4.9 – Variation du taux de délivrance des documents selon que les terminaux mobiles se comportent de façon égoïste ou de façon altruiste

On observe sur la figure, que l'économie réalisée lors de l'utilisation du protocole de diffusion sélective est d'autant plus intéressante que la sphère de communication de chaque terminal est étendue. On peut noter que, le coût global (trafic de contrôle et trafic de données) ne croît pas énormément lorsque la sphère de communication de chaque terminal est étendue au delà de ses voisins à 4 ou 5 sauts. Ceci résulte du fait qu'avec les paramètres utilisés lors de cette campagne de simulation, l'élongation moyenne de chaque îlot dans le réseau se situe à 4.2 sauts.

4.1.2.7 INFLUENCE ET COÛT DU COMPORTEMENT ALTRUISTE

Dans le chapitre 2 nous avons proposé le principe de modulation du comportement (paragraphe 2.2.3). Nous avons expliqué que chaque terminal peut être configuré de manière à se comporter en tant que transporteur altruiste pour des documents qui ne l'intéressent pas, sans que ce comportement compromette ses chances de collecter des documents conformes à son propre profil d'intérêt. Cette possibilité n'a cependant pas été exploitée dans les simulations dont les résultats ont été présentés dans les paragraphes précédents.

Pour mesurer l'impact de l'adoption du comportement altruiste réactif par les terminaux sur les performances globale de la dissémination des documents à travers le réseau, nous avons réalisé des simulations dans lesquelles les terminaux se comportent en transporteurs altruiste ou non. Pour mémoire, nous dirons d'un terminal qu'il se comporte de façon « égoïste » lorsqu'il accepte de ne recevoir, stocker, transporter, et fournir sur demande que des documents qui satisfont son propre profil d'intérêt. Ceci correspond au comportement que nous avons observé dans tous les résultats présentés jusqu'à présent. À l'inverse, nous disons qu'un terminal est « altruiste » lorsqu'il accepte de recevoir, stocker et fournir sur demande des documents dont il

a intercepté la diffusion sur le canal radio, alors que ces documents ne correspondent pourtant pas à son profil d'intérêt.

La figure 4.9 montre comment le taux de délivrance des documents évolue au cours des simulations. Ces résultats ont été obtenus au cours d'une campagne de simulation pendant laquelle la capacité du cache sur chaque terminal était fixée à 300 documents, ce qui dans le scénario considéré était légèrement supérieur à la capacité requise pour n'héberger dans le cache que des documents satisfaisant le profil d'intérêt local. L'espace restant sur chaque terminal pouvait donc être utilisé pour transporter des documents de manière altruiste. Au cours de la simulation, chaque document avait une durée de vie fixée à 75 minutes, et la portée du relais multi-sauts était fixée à deux sauts.

On peut constater, dans la figure 4.9, que lorsque les terminaux mobiles se comportent en transporteurs altruistes, l'ensemble des documents se propage plus rapidement et donc plus efficacement vers l'ensemble des récepteurs intéressés. Par exemple, avec des terminaux égoïstes les documents peuvent être reçus en moyenne par 57 % des souscripteurs en moins de 30 minutes, alors qu'avec des terminaux altruistes ces mêmes documents sont reçus par 72 % des souscripteurs pendant la même durée.

Cette observation confirme bien entendu l'intuition selon laquelle les documents se propagent d'autant plus rapidement dans un réseau ad hoc discontinu qu'ils sont transportés par un grand nombre de terminaux mobiles. Toutefois, il est intéressant de rappeler qu'avec l'approche que nous avons adoptée, cet accroissement de performance observé grâce à l'utilisation de terminaux altruistes réactifs est obtenu à très faible coût dans la mesure où chaque terminal collecte les documents qui ne satisfont pas son profil d'intérêt en interceptant simplement des diffusions sur le canal radio. Aucune transmission supplémentaire n'est donc requise pour ce faire. En outre, comme un terminal altruiste ne supprime jamais de son propre cache de document satisfaisant son profil d'intérêt pour le remplacer par un autre document qui ne le satisfait pas, l'adoption d'un comportement altruiste au niveau d'un terminal n'affecte jamais son rôle premier, qui est d'héberger et relayer en priorité des documents satisfaisant son propre profil d'intérêt.

4.2 EXPÉRIMENTATION SUR POSTES RADIO DE QUATRIÈME GÉNÉRATION

Dans le paragraphe précédent, nous avons observé les performances de notre protocole de communication lorsqu'il est utilisé par des terminaux mobiles de type ordinateur portable disposant d'une interface radio de type WiFi. Ces travaux étant réalisés dans le cadre d'un financement DGA (Direction Générale de l'Armement), nous avons eu l'occasion d'expérimenter notre protocole de communication sur un banc d'essai composé de plusieurs PR4G (Poste Radio de quatrième Génération). Ce banc d'essai est maintenu par la DGA Maîtrise de l'information (appelée CELAR pour Centre d'électronique de l'armement jusqu'à fin 2009) qui est implémenté à Bruz au sud de Rennes.

Dans ce paragraphe nous nous intéressons donc au support des communications dans des réseaux tactiques militaires partiellement connexes. En particulier nous présentons l'expérimen-



Figure 4.10 – Photographie d'un poste radio de quatrième génération (PR4G) développé par Thalès Communications pour l'armée française.

tation de la plate-forme de communication DoD WAN sur un banc d'essai composé de plusieurs PR4G. Le PR4G (figure 4.10), développé par Thalès Communications, est un système VHF complet de radiocommunications militaires protégées. Initialement développé comme un poste radio permettant des transmissions par phonie, le PR4G a évolué pour répondre aux besoins des opérations centrées réseau, qui consistent en la numérisation du champ de bataille pour permettre au commandement de décider et d'agir efficacement. Ce système est donc devenu une radio logicielle (*SDR, Software Defined Radio*) assurant les fonctionnalités d'un routeur IP, et effectuant du routage dynamique afin de s'adapter à la mobilité des terminaux du réseau. Le PR4G est utilisé par les forces armées françaises (air, mer & terre) afin d'assurer les liaisons internes, depuis les grandes unités jusqu'au niveau des unités élémentaires (c'est-à-dire au sein des systèmes de commandement), des systèmes d'armes et des systèmes de tenue de situation tactique. Il permet des transmissions radio longue portée grâce à des puissances en émission élevées. En revanche les débits demeurent faibles en comparaison avec des technologies civiles (WiFi, Bluetooth, etc.). Enfin, les communications par phonie ou par données sont protégées contre l'écoute (procédé de chiffrement numérique intégré), contre le brouillage (recherche de canal libre), et contre la destruction par impulsion électromagnétique en haute altitude.

L'évolution des réseaux radio tactiques militaires associée à l'augmentation des débits contribue à faciliter le déploiement de réseaux sur le théâtre des opérations, et offre de nouvelles perspectives pour le partage d'informations de tenue de situation, qui sont essentielles à la prise de décision. Néanmoins, ces technologies ne permettent pas aux militaires de faire face à toutes les situations rencontrées sur le champ de bataille. En effet, dans les réseaux tactiques la connectivité peut être perturbée à cause d'un faible nombre d'unités mobiles, de la mobilité ou du déploiement lacunaire de ces unités, de masques de propagation naturel, du brouillage radio, ou encore à cause de la destruction d'unités mobiles. Les postes radio de combat ont été développés afin de tolérer des perturbations de courte durée (jusqu'à quelques minutes) entre des unités mobiles. En revanche, ils peuvent difficilement assurer les communications entre des unités subissant des perturbations de connectivité de « longue durée », c'est-à-dire des perturbations allant de la dizaine de minutes à plusieurs heures.

Assurer les communications dans des réseaux radio tactiques discontinus est donc un défi intéressant. Des applications de partage d'information tactique ont déjà été développées par le passé, comme par exemple [BCT06]. Dans notre travail de thèse, nous nous sommes intéressés

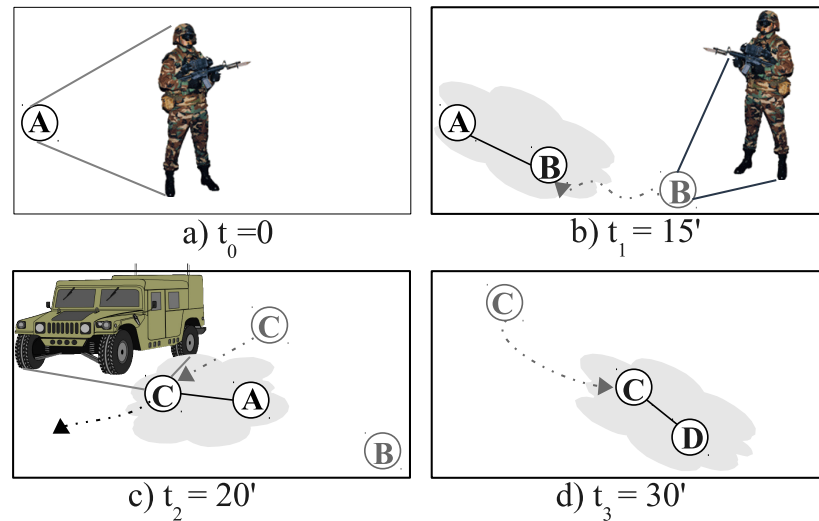


Figure 4.11 – Scénario de contacts radio entre les unités mobiles impliquées dans la mission d'observation.

particulièrement au problème de la dissémination d'information basée contenus dans les DMA-NETs. Dans le paragraphe suivant nous présentons à l'aide d'un scénario d'illustration comment le protocole de communication que nous avons implémenté dans notre plate-forme de communication DoDWAN peut être exploité dans le cadre d'une mission d'observation réalisée par des unités mobiles. Dans le paragraphe 4.2.2, nous présentons le banc d'essai expérimental composé de plusieurs PR4G que nous avons utilisés lors de cette expérimentation et les résultats expérimentaux obtenus lors de cette campagne de test.

4.2.1 SCÉNARIO D'ILLUSTRATION

Nous présentons ici un scénario qui montre comment des terminaux équipés de DoDWAN pourraient être utilisés pour assurer la diffusion d'information sur un champ de bataille. Par souci de clarté, ce scénario implique seulement un faible nombre de terminaux mobiles. Dans des conditions réelles, des dizaines de terminaux pourraient utiliser notre plate-forme pour publier et recevoir des documents. La figure 4.11 illustre le scénario de mobilité des terminaux, tandis que la figure 4.12 présente la chronologie de la communication entre ces terminaux en fonction de ce scénario.

Un fantassin A mène une mission d'observation sur la ligne de front, et est en rupture de contact radio avec son chef de groupe D. D'autres unités mobiles, un fantassin B et un véhicule C, se déplacent dans la région afin d'aider à la communication entre A et D. Les observations tactiques faites par A doivent être transférées aussi vite que possible à D, sans interrompre la mission menée par A.

À l'instant t_0 (Fig. 4.11-a), le fantassin A démarre son terminal T_A , afin de publier un document se rapportant aux conditions de combat observées (par exemple un court message texte

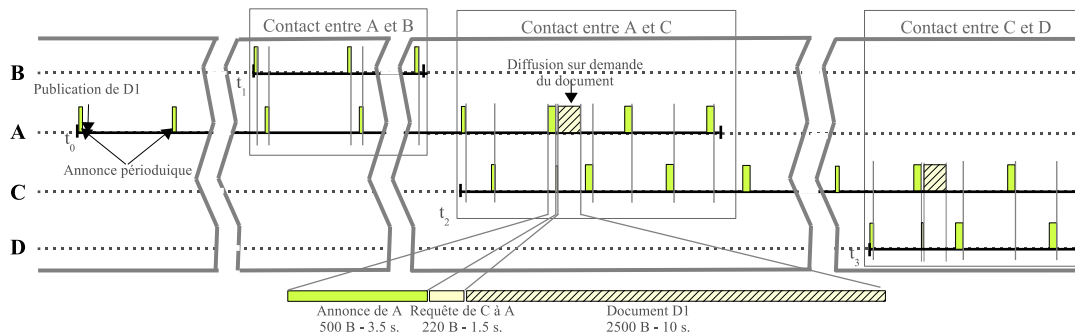


Figure 4.12 – Chronologie de la communication entre les unités mobiles conduisant la mission d'observation.

décrivant ce qu'il a observé récemment, une carte annotée, ou même une photo qu'il a prise avec un appareil photo numérique). Dès que T_A est activé, l'intergiciel DoDWAN qu'il exécute lance le mécanisme de diffusion périodique d'annonces. Le document D1 publié par A n'est pas immédiatement envoyé sur le canal radio. Il est d'abord déposé dans le cache local mis à disposition par le terminal T_A , qui contient peut-être déjà de nombreux autres documents. Puisqu'aucun autre terminal n'a été détecté par T_A dans son voisinage (ce qui signifie qu'aucun autre terminal n'est actuellement à portée radio), l'annonce diffusée par le terminal T_A contient uniquement son identité et une description de son profil d'intérêt.

À l'instant t_1 (Fig. 4.11-b), un autre fantassin B arrive à portée radio du terminal de A. Le fantassin B transporte lui aussi un terminal de communication T_B qui diffuse régulièrement une annonce indiquant son identité et son profil d'intérêt. Cependant, B n'est pas impliqué dans la mission menée par le fantassin A, et son terminal n'est donc pas configuré de manière à relayer les observations publiées par A. Lors de la réception de l'une des annonces de T_B , le terminal T_A découvre qu'il a un nouveau voisin, mais en faisant correspondre le profil d'intérêt de T_B avec les descripteurs des documents stockés dans son propre cache T_A découvre que T_B n'est intéressé par aucun des documents qu'il héberge. Le terminal T_A s'abstient donc de proposer un document à T_B , et continue d'annoncer sa présence (identité et le profil d'intérêt) sans que ses annonces ne contiennent de catalogue.

À l'instant t_2 (Fig. 4.11-c), un véhicule C pénètre dans la zone de portée radio de T_A . Suite à la réception d'une annonce diffusée par le terminal T_C transporté dans ce véhicule, T_A découvre que ce terminal est intéressé par le document D1 (ce qui signifie que C est configuré pour participer à la mission d'observation réalisée par A). T_A insère donc un catalogue dans son annonce périodique. Ce catalogue contient le descripteur du document D1, et éventuellement d'autres descripteurs de documents disponibles dans le cache de T_A et qui satisfont le profil d'intérêt de terminal transporté par C. Après avoir reçu une telle annonce en provenance de T_A , T_C procède à l'analyse du catalogue de descripteur de documents qu'elle contient pour identifier les documents qui l'intéressent et qui lui font défaut. Il se trouve que le descripteur du document D1 appartient à cette catégorie. T_C adresse donc une requête à T_A , lui demandant que le document correspondant soit diffusé sur le canal radio.

Peu de temps après que le document D1 a été transmis au terminal T_C , le fantassin A met son terminal en veille et s'éloigne. Notez qu'il n'est pas nécessaire pour A de savoir que le document qu'il a publié à l'instant t_0 a bien été transféré à un ou plusieurs autres terminaux. La diffusion effective de ce document est assurée automatiquement en arrière plan par l'intergiciel DoDWAN, qui saisit toutes les opportunités pour fournir des copies des documents qu'il héberge aux terminaux intéressés.

Considérons maintenant le terminal T_C transporté dans le véhicule C. Après déplacement (qui peut être long), le terminal T_C arrive à l'instant t_3 (Fig. 4.11-d) à portée radio du terminal du chef de groupe T_D , dont le profil d'intérêt correspond bien entendu au descripteur du document D1. Sur réception d'une annonce diffusée par T_D , T_C découvre que T_D est en effet intéressé par le document D1. On peut noter que T_D a peut-être déjà reçu une copie de D1 lors d'un contact avec un autre terminal mobile. T_C propose donc D1 dans le catalogue qu'il insère dans l'annonce périodique qu'il diffuse. Ainsi il permet à T_D de décider s'il souhaite récupérer une copie du document D1. Si tel est le cas, alors T_D adresse une requête à T_C , puis T_C satisfait la demande de T_D par la diffusion du document D1 sur le canal radio.

Il est important de noter qu'avec cette approche, le document publié par T_A à l'instant t_0 a fini par atteindre les terminaux T_C et T_D , bien que T_A et T_D ne se soient jamais trouvés à portée radio l'un de l'autre et que, dans le scénario considéré, aucun chemin de bout en bout n'ait jamais existé entre eux. Le terminal T_C a effectivement servi de relais mobile pour l'information tactique embarquée dans un document publiée par A, qui avait de l'intérêt pour le chef de groupe D. Ce scénario illustre la façon dont le modèle de communication proposé par DoDWAN peut être utilisé pour assurer la diffusion de l'information dans un réseau radio militaire tactique discontinu. Il montre également comment la différenciation basée sur le contenu peut être utilisée pour diriger la diffusion de l'information dans le réseau, en permettant à chaque terminal d'être sélectif vis-à-vis des documents.

4.2.2 RÉSULTATS EXPÉRIMENTAUX

Le scénario présenté dans la section précédente a été déroulé sur un banc d'essai dédié à la simulation de réseaux radio tactiques. Ce banc d'essai est composé de 20 postes radio tactiques PR4G, développés par Thalès Communications. Ces postes radio sont connectés à un commutateur radio, qui permet de simuler différentes topologies de déploiement et différentes conditions de propagation radio à l'aide d'une matrice d'atténuation. Le principal avantage de ce banc d'essai par rapport à un environnement réel (en plein air), est que toutes les unités radio sont co-localisées et les conditions de propagation des ondes radio sont sous contrôle, ce qui facilite la conduite d'expériences répétées. Les versions actuelles du PR4G supportent jusqu'à 64 kbit/s de débit de transfert de données dans un canal de largeur 25 kHz, en sécurisant les communications par chiffrement et évocation de fréquence. Le PR4G permet également de réaliser des communications de voix et de données sécurisées grâce à une méthode de saut de fréquence propriétaire multiplex (nommée SIVD).

Notre principale motivation pour l'utilisation de ce banc d'essai était de montrer par la pratique que la plate-forme de communication DoDWAN —et plus particulièrement le protocole



Figure 4.13: Architecture d'une unité mobile utilisée lors de nos expérimentations sur des postes radio de combat (PR4G).

qu'elle met en œuvre— peut fonctionner de façon satisfaisante avec le faible débit de transmission offert par le PR4G.

Conformément au scénario décrit dans le paragraphe 4.2.1, l'expérience réalisée sur le banc d'essai implique quatre unités mobiles de communication. Chaque unité mobile, illustrée dans la figure 4.13, est composée d'un poste radio PR4G associée à un terminal de données connecté à l'interface Ethernet du PR4G. Nous avons en fait utilisé des *netbooks* (Dell Mini 9) comme terminaux de données, mais tout type d'équipement mobile embarquant la suite protocolaire IP et un environnement d'exécution Java 1.6 pourrait aussi être utilisé. Les PR4G ont été configurés pour exécuter le profil de communication dit « IP-Multiplex ». Ce profil de communication présente l'intérêt d'offrir simultanément des communications sécurisées par voix et données. En outre, le débit maximum atteignable avec ce profil est de quelques kbit/s. Bien que ce profil ne prenne pas en charge les transmissions multi-sauts (puisque aucun protocole de routage dynamique n'est utilisé), il supporte la multi-diffusion IP (*multicast*) à un seul saut radio. Ce profil correspond donc parfaitement aux besoins de notre intergiciel de communication, qui s'appuie sur des diffusions périodiques de datagrammes UDP (paragraphe 3.2.1).

Il est à noter que le routeur IP intégré au PR4G peut utiliser le champ TOS (*Type Of Service*) des paquets IP afin de fiabiliser les transmissions au niveau liaison de données, ainsi que gérer des priorités sur les paquets IP. Ces paramètres ont été utilisés au cours de notre expérience pour accroître la fiabilité des transmissions radio, et pour donner dans notre protocole la priorité au trafic de contrôle sur le trafic de données.

La mobilité des unités au cours du scénario a été simulée en ajustant la matrice d'atténuation du banc d'essai. La période d'annonce a été fixée à 60 secondes sur tous les terminaux. Le document publié sur le terminal A à l'instant t_0 était une image JPEG de 2.5 ko, avec un descripteur associé de 500 octets. Les profils d'intérêt définis sur chaque terminal pesaient environ 300 octets (après compression LZ77). La chronologie du scénario a en outre été définie comme suit : $t_0 = 0$, $t_1 = 15 \text{ min.}$, $t_2 = 20 \text{ min.}$, $t_3 = 30 \text{ min.}$

Lors de notre expérience, la progression du scénario de communication a été conforme au scénario présenté dans la figure 4.12. La compression systématique de tous les messages de contrôle et de données (c'est-à-dire des annonces, des requêtes et des documents) en utilisant l'algorithme LZ77 s'est révélée très efficace compte tenu du faible débit supporté par les modems équipant les PR4G. En effet, la plupart des messages de contrôle (qui pour rappel sont

des documents XML) ont été compressés avec un taux de compression moyen de 12:1. Nous avons par ailleurs observé des durées d'émissions variant entre 2,5 et 3,5 secondes pour chaque annonce périodique, selon que l'annonce comprenait un catalogue ou non. La durée d'émission la plus longue observée au cours de cette expérimentation a été bien entendu celle du document D1, qui a été diffusé peu de temps après t_2 par le terminal T_A en réponse à la demande de T_C , et ensuite par le terminal transporté par le véhicule C en réponse à la demande de T_D . Dans les deux cas, la diffusion de D1 a occupé le canal radio pendant environ 12 secondes.

Pour compléter ces chiffres, il convient de mentionner que la compression et les temps de décompression avec l'algorithme LZ77 n'ont jamais dépassé 10 ms sur les netbooks équipés de processeurs 1,6 GHz que nous avons utilisés durant l'expérimentation.

Dans l'ensemble, cette expérience menée sur le banc d'essai de PR4G mis à notre disposition par le CELAR, nous a confirmé que la plate-forme intergicielle DoDWAN peut fonctionner de façon satisfaisante sur des terminaux associés à des postes radio tactiques. Cette expérimentation atteste également que le protocole de communication opportuniste basée contenus mis en œuvre par l'intergiciel DoDWAN permet une diffusion efficace des informations tactiques dans un réseau radio militaire discontinu. Plus particulièrement, il a montré que la charge induite par cette diffusion est compatible avec les débits offerts par les PR4G.

Bien que ces premiers résultats soient encourageants, la question du passage à l'échelle devrait être considérée. En effet aucune expérience à grande échelle avec les postes radios PR4G n'a été effectuée à ce jour. Nous avons obtenu des résultats prometteurs lors de nos expérimentations par simulations. Ces résultats, qui ont été présentés dans le paragraphe 4.1, attestent de l'efficacité de DoDWAN pour disséminer de l'information dans des réseaux constitués de nombreuses unités mobiles.

4.3 BILAN

Dans ce chapitre nous avons présenté les résultats d'évaluation de notre protocole de communication. Cette évaluation, réalisée à l'aide du simulateur de réseau mobile ad hoc MADHOC et sur le banc de test du CELAR montre que les choix que nous avons faits lors de la conception de notre protocole permettent de satisfaire nos objectifs.

Les résultats obtenus montrent que notre protocole de communication permet à des terminaux volatiles impliqués dans un réseau déployé temporairement d'échanger efficacement des informations au gré de leurs rencontres et en fonction de leurs centres d'intérêt. Ils confirment aussi que les mécanismes développés dans la couche supérieure du protocole (la sélectivité des terminaux, l'adaptation dynamique du catalogue aux profils d'intérêt des voisins perçus, le mécanisme d'adaptation dynamique de l'annonce et la compression des données) permettent effectivement de réduire le nombre et le volume des documents échangés entre terminaux. Ils attestent enfin de l'intérêt de l'activation volontaire du comportement altruiste sur tout ou partie des terminaux. En effet, ce comportement permet d'améliorer de façon significative les performances de la dissémination des documents, sans nuire à la mission première des terminaux (qui est de collecter des documents satisfaisant leur propre profil d'intérêt), et surtout sans impliquer un surcoût élevé. Nous avons souligné que l'extension de la sphère de communication

des terminaux, obtenu via le support des transmissions multi-sauts, permet une dissémination plus efficace des documents à travers le réseau. Nous avons montré que les protocoles de diffusion que nous avons développés permettent, avec des performances comparables, de minimiser fortement l'utilisation du médium radio en comparaison à un simple mécanisme d'inondation.

Dans la seconde partie de ce chapitre, nous avons montré comment la plate-forme de communication DoDWAN peut permettre à un groupe de fantassins de partager des informations de tenue de situation dans un réseau radio tactique discontinu. L'expérimentation que nous avons menée sur le banc d'essai PR4G du CELAR confirme que le protocole de communication implémenté dans la plate-forme DoDWAN est compatible avec les faibles débits exploitables sur les PR4G. Des expérimentations plus poussées seraient cependant souhaitables afin de considérer des scénarios d'utilisation impliquant un plus grand nombre d'unités mobiles. Il serait de même intéressant de tester la plate-forme DoDWAN en conditions réelles, à l'aide d'unités mobiles PR4G déployées sur un véritable théâtre d'opérations.

CONCLUSION ET PERSPECTIVES

SYNTHÈSE

Nous avons proposé dans le cadre de cette thèse un nouveau protocole de communication s'accommodant des propriétés particulières des réseaux mobiles ad hoc (MANETs) discontinus. Ce protocole repose sur une combinaison originale du principe de la communication opportuniste et du modèle de la communication basée contenus, et reposant sur des algorithmes de relais immédiat multi-sauts inspirés des algorithmes de routage dynamique conçus pour les réseaux mobiles ad hoc connexes.

En nous appuyant sur le principe de la communication opportuniste, en particulier sur le mode d'acheminement *store, carry and forward*, nous avons conçu un protocole capable de supporter la propriété principale des MANETs discontinus, c'est-à-dire la fragmentation dynamique du réseau en îlots.

Ce protocole permet à des services applicatifs de publier des documents et de s'abonner afin de recevoir des types particuliers de documents. Il s'appuie, pour ce faire, sur la dissémination opportuniste basée contenus des documents. Contrairement à d'autres protocoles qui mettent en œuvre des méthodes complexes afin de construire des structures de routage basé contenus en fonction d'événements observés par le passé, notre protocole ne construit aucune structure de ce type. Il exploite simplement les contacts fugitifs entre terminaux mobiles, en permettant à ces terminaux d'échanger des documents en fonction de leurs profils d'intérêt respectifs tout en limitant la quantité de ressources nécessaire à leur dissémination.

Chaque terminal peut s'appuyer sur un mécanisme de relais multi-sauts afin d'échanger des documents avec d'autres terminaux situés dans le même fragment connexe du réseau que lui-même. Lors de ses déplacements dans le réseau, il participe en outre à la dissémination des documents qu'il transporte, et contribue ainsi à assurer la propagation de ces documents dans l'ensemble du réseau.

L'objectif premier poursuivi par chaque terminal est de collecter des documents satisfaisant ses propres centres d'intérêt, qui sont exprimés dans son profil d'intérêt. Il peut cependant, de manière optionnelle, adopter un comportement altruiste (réactif ou proactif) en hébergeant des documents qui ne satisfont pas son propre profil et aider à la dissémination de ces documents dans le réseau.

Ce protocole de communication a été implémenté dans le langage de programmation Java, et embarqué dans l'intergiciel DoDWAN, qui est disponible sous licence GPL. La plate-forme de communication DoDWAN se distinguant des applications développées dans d'autres travaux, comme par exemple PodNet, par le fait qu'elle n'est pas dédiée à un service applicatif particulier. La plate-forme DoDWAN a été conçue afin de permettre le développement de services applicatifs capables de tolérer les particularités des DMANETs. Comme nous l'avons présenté dans ce mémoire, nous avons développé des services applicatifs qui montrent comment notre protocole peut être exploité par des services de partage d'information et de messagerie.

Les résultats expérimentaux présentés dans ce mémoire confirment l'efficacité de notre protocole de communication pour assurer l'acheminement de documents à travers un réseau fortement fragmenté et de courte durée de vie. Ces résultats montrent également que l'utilisation

de mécanismes de relais multi-sauts contribuent à accroître la vitesse de dissémination des documents au sein des îlots du réseau, ce qui se traduit également par une efficacité accrue du transport de documents entre ces divers îlots. En ajustant la portée du relais multi-sauts réalisé autour de chaque terminal mobile, le coût supplémentaire induit par ce mécanisme peut être maintenu à un niveau raisonnable. Enfin, les simulations confirment que l'adoption d'un comportement altruiste de la part des terminaux contribue également à accroître les performances globales du système, sans que ce comportement compromette pour autant l'aptitude des terminaux à collecter en priorité des documents satisfaisant leur propre profil d'intérêt.

PERSPECTIVES

Les travaux réalisés dans le cadre de cette thèse et les résultats obtenus lors des expérimentations de notre protocole de communication opportuniste basée contenus ouvrent d'intéressantes perspectives de recherche.

Ajustement dynamique de la sphère de communication d'un terminal. Dans la version actuelle de la couche inférieure de notre protocole, le nombre de sauts autorisés dans le cadre du relais multi-sauts est fixé comme un paramètre constant. Il serait intéressant de développer des heuristiques permettant à chaque terminal mobile d'ajuster dynamiquement sa sphère de communication. Cet ajustement dynamique pourrait prendre en compte des critères relatifs à l'environnement immédiat d'un terminal mobile, comme par exemple la densité du voisinage du terminal, les profils d'intérêt de ses voisins, un historique d'échanges récents avec le voisinage, le taux d'occupation du médium radio, etc. Cependant la détermination de telles heuristiques n'est pas triviale. Il faudra en effet pouvoir déterminer de façon expérimentale les critères pertinents pour l'ajustement dynamique de la portée des communications multi-sauts.

Développement et expérimentation de fonctions de rang. Dans la version actuelle de la couche supérieure de notre protocole nous avons mis en œuvre une seule fonction de rang, c'est-à-dire celle que nous avons décrite dans ce mémoire. La plate-forme intergicielle DoDWAN a été développée de telle sorte qu'il soit possible de définir librement la politique de gestion de cache des terminaux, en particulier en redéfinissant la fonction de rang. Il serait intéressant de développer des fonctions de rang prenant en compte d'autres paramètres que l'âge d'un document et le nombre de prédicats de sélection qu'il satisfait. Une étude comparative de différentes fonctions de rang tenant compte par exemple de la popularité d'un document, de son poids, du nombre de fragments, etc. devrait être réalisée pour identifier les meilleures solutions.

Gestion de priorités lors de contacts fugitifs. Avec notre protocole, lorsque deux terminaux voisins se rencontrent ils peuvent s'échanger des documents en fonction de leurs centres d'intérêts respectifs. Un terminal peut demander à un voisin de diffuser sur le médium un nombre élevé de documents, alors que la durée du contact radio entre les terminaux ne permettra pas au demandeur d'être en mesure de recevoir l'ensemble des documents demandés. Pour éviter

ce phénomène les terminaux devraient être capables d'estimer la capacité d'un contact, celle-ci étant définie comme le taux de transmission de données multiplié par la durée de contact. Grâce à cette information un terminal ne solliciterait que la diffusion de documents qu'il jugerait prioritaire et qu'il estimerait être en mesure de recevoir. À l'heure actuelle il est difficile — voire impossible — de déterminer la durée et la capacité d'un contact entre deux terminaux à l'aide des informations que nous exploitons dans notre protocole. Par contre, il serait possible de permettre à un terminal demandeur d'affecter un rang à chaque document demandé, indiquant ainsi l'ordre dans lequel les documents demandés devront être diffusés. La gestion de priorité des demandes de documents faites aux voisins est réalisable à l'aide de la fonction de rang que nous avons développée pour la gestion du cache de document. Il serait intéressant d'évaluer l'impact de cette amélioration sur les performances de notre protocole.

Problèmes de sécurité. Nous avons conçu notre plate-forme dans le but de permettre le développement et l'expérimentation d'applications ou de services applicatifs pour MANETs discontinus. Ces applications et services applicatifs ont des besoins différents en termes de sécurité. Certains services peuvent se satisfaire d'une sécurité minimale alors que d'autres peuvent avoir besoin d'une sécurité renforcée (chiffrement, intégrité, authentification, etc.). Par exemple, le service de messagerie qui s'appuie sur le relais des messages par des groupes d'utilisateurs ne garantit pas aujourd'hui que les messages envoyés par un utilisateur ne vont pas être lus par d'autres utilisateurs que leurs destinataires, ne vont pas être modifiés avant d'être réinjectés dans le réseau, etc. L'intégration de mécanismes de sécurité dans notre modèle de communication devrait permettre de répondre à ces besoins. Il faut toutefois noter que les méthodes développées pour les réseaux connexes (qui reposent pour la plupart sur des autorités de chiffrement de type PKI) ne sont guère applicables dans les réseaux mobiles ad hoc discontinus.

Notre protocole de communication est, en l'état actuel, relativement exposé à des attaques de type déni de service, qui pourraient être facilement réalisées par un terminal malicieux via des attaques de type UDP Flooding, des requêtes systématiques pour des documents proposés en catalogue, la rediffusion de requêtes de documents, la rediffusion de documents, etc. Il est actuellement difficile de faire face à ce type de menace dans notre protocole de communication puisqu'une grande partie des échanges entre terminaux s'appuie sur de la diffusion. Une approche possible serait de développer des méthodes de répudiation, mais la principale difficulté réside ici dans le fait que le terminal répudié ne doit pas pouvoir changer d'identité, ni même être informé de sa répudiation.

Intégration de la notion de localisation. Nous avons conçu la plate-forme DoDWAN de telle sorte qu'elle puisse être configurée pour pouvoir être utilisée dans différents domaines d'applications. Dans la perspective où cette plate-forme serait utilisée par exemple dans des réseaux inter-véhiculaires, l'intégration de la notion de localisation dans notre modèle de communication devrait permettre à l'information d'être géoréférencée. De la sorte, il serait possible de limiter la portée géographique de la dissémination de l'information. Par exemple, on pourrait ainsi éviter que des informations relatives aux travaux de voiries réalisés dans une ville soient propagées dans des villes voisines, sauf sur demande explicite d'un terminal.

Évaluation des performances de notre protocole en conditions réelles. La plate-forme de communication et les services applicatifs que nous avons développés dans nos travaux de thèse permettent d'envisager des campagnes d'expérimentations de notre protocole de communication en conditions réelles, c'est-à-dire de déployer notre intergiciel et nos services sur des dizaines d'ordinateurs portables et de collecter des traces afin de mesurer les performances de notre protocole dans de telles conditions. Suite à nos travaux de thèse deux campagnes d'expérimentations en conditions réelles, l'une à l'ENS Cachan Bretagne (DITADHOC¹), l'autre à Université de Bretagne Sud (DoDWAN-Expe²), ont déjà été menées. À l'avenir nous souhaiterions réaliser de nouvelles expérimentations avec des populations d'utilisateurs plus variées (n'impliquant pas uniquement des étudiants sur un campus universitaire), dans des environnements différents, à des échelles plus larges (par exemple dans une ville comme Vannes). Nous souhaiterions aussi évaluer différents usages de notre protocole : communication basée contenus pure, communication de tribu, etc.

Ces différentes expérimentations seraient également l'occasion pour nous d'examiner le problème de la communication opportuniste sous l'angle de son acceptabilité par les utilisateurs. En effet, cette question n'a été que fort peu étudiée à ce jour. Il serait donc intéressant d'étudier comment les utilisateurs perçoivent le modèle de la communication opportuniste, et dans quelles circonstances ils seraient intéressés par son utilisation.

1. <http://www-valoria.univ-ubs.fr/CASA/DITADHOC/>

2. <http://www-valoria.univ-ubs.fr/CASA/DODWAN-EXPE/>

PUBLICATIONS PERSONNELLES

CONFÉRENCES NATIONALES À COMITÉ DE LECTURE ET AVEC ACTES

1. *Julien Haillot et Frédéric Guidec*, « Communication « basée contenus » dans les réseaux mobiles ad hoc discontinus » dans 8eme Conférence Internationale sur les NOuvelles TEchnologies de la REpartition (NOTERE), pp. 162-173, 2008.

CONFÉRENCES INTERNATIONALES À COMITÉ DE LECTURE ET AVEC ACTES

1. *Julien Haillot, Frederic Guidec, Serge Corlay et Jacques Turbert*, « *Disruption-Tolerant Content-Driven Information Dissemination in Partially Connected Military Tactical Radio Networks* » dans Proceedings of the Military Communications Conference (MIL-COM), pp. 2326-2332, Boston, USA, Octobre 2009.
2. *Julien Haillot et Frédéric Guidec*, « *A Protocol for Content-Based Communication in Disconnected Mobile Ad Hoc Networks*, » dans Proceedings of the 22nd International Conference on Advanced Information Networking and Applications (AINA), pp. 188-195, Okinawa, Japon, Mars 2008.
3. *Julien Haillot et Frederic Guidec*, « *Towards a Usenet-Like Discussion System for Users of Disconnected MANETs*, » dans Proceedings of the 22nd International Conference on Advanced Information Networking and Applications - The First IEEE International Workshop on Opportunistic Networking (WON), pp. 1678-1683, Okinawa, Japon, Mars 2008.

REVUE NATIONALE

1. *Frédéric Guidec et Julien Haillot*, « Communication « basée contenus » dans les réseaux mobiles ad hoc discontinus » dans Technique et Science Informatiques (RSTI série TSI), 30(3) :275-308, Mars 2011.

REVUE INTERNATIONALE

1. *Julien Haillot et Frédéric Guidec*, « A Protocol for Content-Based Communication in Disconnected Mobile Ad Hoc Networks » dans International Journal of Mobile Information Systems, 6(2) :123-154, 2010.

BIBLIOGRAPHIE

- [BBC⁺05] R. Baldoni, R. Beraldi, G. Cugola, M. Migliavacca et L. Querzoni : Structureless content-based routing in mobile ad hoc networks. *In Proceedings of the International Conference on Pervasive Services*, page 37—46, 2005.
- [BBL05] B. Burns, O. Brock et B.N. Levine : MV routing and capacity building in disruption tolerant networks. *In Proc. IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2005*, volume 1, page 398—408, mars 2005.
- [BBQ⁺05] R. Baldoni, R. Beraldi, L. Querzoni, G. Cugola et M. Migliavacca : Content-based routing in highly dynamic mobile ad hoc networks. *International Journal of Pervasive Computing and Communications*, 1(4):277, 2005.
- [BBQ⁺07] R. Baldoni, R. Beraldi, V. Quema, L. Querzoni et S. Tucci-Piergiovanni : TERA : topic-based event routing for peer-to-peer architectures. *In Proceedings of the 2007 inaugural international conference on Distributed event-based systems*, page 2—13. ACM New York, NY, USA, 2007.
- [BCJP07] Chiara Boldrini, Marco Conti, Jacopo Jacopini et Andrea Passarella : HiBOp : a History Based Routing Protocol for Opportunistic Networks. *In Marco Conti, éditeur : IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks WoWMoM 2007*, page 1—12, 2007.
- [BCP08a] C. Boldrini, M. Conti et A. Passarella : ContentPlace : Social-aware Data Dissemination in Opportunistic Networks. *In Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, page 203—210, 2008.
- [BCP08b] C. Boldrini, M. Conti et A. Passarella : Exploiting users social relations to forward data in opportunistic networks : The hibop solution. *Pervasive and Mobile Computing*, 4(5):633—657, 2008.
- [BCT06] L. Barrère, S. Chaumette et J. Turbert : A Tactical Active Information Sharing System for Military Manets. *In Military Communications Conference, MILCOM 2006*, page 1—7, 2006.
- [Bey90] D.A. Beyer : Accomplishments of the DARPA SURAN Program. *In A New Era Military Communications Conference MILCOM, Conference Record 1990 IEEE*, page 855—862, 1990.
- [BFQ87] F. J. Bruno, W. C. Fifer et D. M. Quinn : Low Cost Packet Radio - Advanced Technology for Packet Radio Switching Applications. *In Proc. IEEE Military Communications Conference - Crisis Communications : The Promise and Reality MILCOM 1987*, volume 2, page 0443—0448, octobre 1987.
- [BGJL06] J. Burgess, B. Gallagher, D. Jensen et B. N. Levine : MaxProp : Routing for Vehicle-Based Disruption-Tolerant Networks. *In Proc. 25th IEEE International Conference on Computer Communications INFOCOM 2006*, page 1—11, 2006.

- [CBH⁺06] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall et H. Weiss : Delay Tolerant Network Architecture. IETF Internet Draft, mars 2006. draft-irtf-dtnrg-arch-05.txt (work in progress).
- [CD⁺99] J. Clark, S. DeRose *et al.* : XPath : XML path language version 1.0. *W3C recommendation*, 16:1999, 1999.
- [CDKR02] M. Castro, P. Druschel, A.M. Kermarrec et A.I.T. Rowstron : SCRIBE : A large-scale and decentralized application-level multicast infrastructure. *IEEE Journal on Selected Areas in communications*, 20(8):1489—1499, 2002.
- [CDNFC98] G. Cugola, E. Di Nitto, A. Fuggetta et P.M. CEFRIEL : Exploiting an event-based infrastructure to develop complex distributed systems. *In Software Engineering, 1998. Proceedings of the 1998 International Conference on*, page 261—270, 1998.
- [CHC⁺07] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass et J. Scott : Impact of human mobility on opportunistic forwarding algorithms. *IEEE Transactions on Mobile Computing*, 6(6):606—620, 2007.
- [CJ03] T. Clausen et P. Jacquet : RFC 3626 : Optimized Link State Routing Protocol (OLSR). *RFC Editor United States*, 2003.
- [CM99] S. Corson et J. Macker : Mobile ad hoc networking (MANET) : routing protocol performance issues and evaluation considerations (RFC 2501). *IETF working group on Mobile Adhoc Networks, RFC Editor United States*, 1999.
- [CM01] Xiangchuan. Chen et Amy L. Murphy : Enabling disconnected transitive communication in mobile ad hoc networks. *In Workshop on Principles of Mobile Computing*, page 21—23, août 2001.
- [CMMP06] Paola Costa, Mirco Musolesi, Cecilia Mascolo et Gian Pietro Picco : Adaptive Content-based Routing for Delay-tolerant Mobile Ad Hoc Networks. Rapport technique, UCL, août 2006.
- [CMMP08] P. Costa, C. Mascolo, M. Musolesi et GP Picco : Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 26(5):748—760, 2008.
- [CMTV07] G. Chockler, R. Melamed, Y. Tock et R. Vitenberg : Spidercast : a scalable interest-aware overlay for topic-based pub/sub communication. *In Proceedings of the 2007 inaugural international conference on Distributed event-based systems*, page 14—25. ACM New York, NY, USA, 2007.
- [CP05] Paolo Costa et Gian Pietro Picco : Semi-Probabilistic Content-Based Publish-Subscribe. *In 25th International Conference on Distributed Computing Systems (ICDCS 2005)*, page 575—585, Columbus, Ohio, USA, juin 2005. IEEE Computer Society.
- [CP10] I. Chakeres et C. Perkins : Dynamic MANET On-demand (DYMO) Routing. *draft-ietf-manet-dymo-19 (work in progress)*, 2010.

- [CRW00] A. Carzaniga, D.S. Rosenblum et A.L. Wolf : Achieving scalability and expressiveness in an internet-scale event notification service. *In Proceedings of the nineteenth annual ACM symposium on Principles of distributed computing*, page 219—227. ACM New York, NY, USA, 2000.
- [CRW01] A. Carzaniga, D.S. Rosenblum et A.L. Wolf : Design and evaluation of a wide-area event notification service. *ACM Transactions on Computer Systems*, 19(3): 332—383, 2001.
- [CW01] Antonio Carzaniga et Alexander L. Wolf : Content-based Networking : A New Communication Infrastructure. *In NSF Workshop on an Infrastructure for Mobile and Wireless Systems*, numéro 2538 de LNCS, page 59—68, Scottsdale, Arizona, octobre 2001. Springer-Verlag.
- [DH07a] E.M. Daly et M. Haahr : Social network analysis for routing in disconnected delay-tolerant manets. *In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, page 32—40. ACM, 2007.
- [DH07b] E.M. Daly et M. Haahr : Social network analysis for routing in disconnected delay-tolerant MANETs. *In Proceedings of the 8 th ACM international symposium on Mobile ad hoc networking and computing*, 2007.
- [DQA04] Anwitaman Datta, Silvia Quarteroni et Karl Aberer : Autonomous Gossiping : a Self-Organizing Epidemic Algorithm for Selective Information Dissemination in Mobile Ad-Hoc Networks. *In International Conference on Semantics of a Networked World*, numéro 3226 de LNCS, pages 126--143, juin 2004.
- [F⁺02] K. Fall *et al.* : Delay tolerant networking research group. *Working group charter, Internet Research Task Force*, URL : <http://www.dtnrg.org>, 2002.
- [FGKZ03] Ludger Fiege, Felix C. Gärtner, Oliver Kasten et Andreas Zeidler : Supporting mobility in content-based publish/subscribe middleware. *In Middleware '03 : Proceedings of the ACM/IFIP/USENIX 2003 International Conference on Middleware*, page 103—122, juin 2003.
- [GT01] M. Grossglauser et D. Tse : Mobility increases the capacity of ad-hoc wireless networks. *In Proc. IEEE Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2001*, volume 3, page 1360—1369, avril 2001.
- [GV03] M. Grossglauser et M. Vetterli : Locating nodes with EASE : last encounter routing in ad hoc networks through mobility diffusion. *In Proc. INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, volume 3, page 1954—1964, mars 2003.
- [Haa97] Z.J. Haas : A new routing protocol for the reconfigurable wireless networks. *In IEEE 6th International Conference on Universal Personal Communications Record Conference Record*, volume 2, page 562—566, octobre 1997.
- [HABR05] Khaled A. Harras, Kevin C. Almeroth et Elisabeth M. Belding-Royer : Delay Tolerant Mobile Networks (DTMNs) : Controlled Flooding in Sparse Mobile Networks. *In IFIP Networking Conference, Waterloo, Ontario, CANADA*, mai 2005.

- [HBS⁺02] Mark Hapner, Rich Burrige, Rahul Sharma, Joseph Fialli et Kate Stout : *Java Message Service : The JMS API is an API for accessing enterprise messaging systems from Java programs*. Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94403 U.S.A., 2002.
- [HC07a] P. Hui et J. Crowcroft : Bubble rap : Forwarding in small world dtns in ever decreasing circles. *Univ. of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-684*, 2007.
- [HC07b] P. Hui et J. Crowcroft : How small labels create big improvements. *In Pervasive Computing and Communications Workshops*, page 65—70, 2007.
- [HCS⁺05] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft et C. Diot : Pocket switched networks and human mobility in conference environments. *In Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, page 244—251. ACM, 2005.
- [HCY08] P. Hui, J. Crowcroft et E. Yoneki : Bubble rap : Social-based forwarding in delay tolerant networks. *In Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing*, page 241—250. ACM New York, NY, USA, 2008.
- [HGB06] L. Hogue, F. Guinand et P. Bouvry : The Madhoc Metropolitan Adhoc Network Simulator. Rapport technique, University of Luxembourg, mars 2006.
- [HGD⁺06] Luc Hogue, Frédéric Guinand, Grégoire Danoy, Pascal Bouvry et Enrique Alba : Simulating Realistic Mobility Models for Large Heterogeneous MANETs. *In 9th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2006)*, page 2—6, octobre 2006.
- [HGM03] Y. Huang et H. Garcia-Molina : Publish/subscribe tree construction in wireless ad-hoc networks. *Lecture notes in computer science*, page 122—140, 2003.
- [HHL88] S.M. Hedetniemi, S.T. Hedetniemi et A.L. Liestman : A Survey of Gossiping and Broadcasting in Communication Networks. volume 18, pages 319--349. Wiley Online Library, 1988.
- [HHL02] Z.J. Haas, J.Y. Halpern et L. Li : Gossip-based Ad Hoc Routing. *In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 3, pages 1707--1716. IEEE, 2002.
- [Hor83] M. R. Horton : RFC 850 : Standard for interchange of USENET messages. *RFC Editor United States*, 1983.
- [HYCC09] P. Hui, E. Yoneki, J. Crowcroft et S.Y. Chan : Identifying social communities in complex communications for network efficiency. *Complex Sciences, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 4:351—363, 2009.
- [JCNSJ07] J.LeBrun, C-N.Chuah, S.Bhattacharya et J.Bolot : News-Feed Subscription Management for Intermittently Connected Environments. *In International Work-*

- shop on Improved Mobile User Experience (IMUx), co-located with International Conference on Pervasive Computing*, mai 2007.
- [JFP04] Sushant Jain, Kevin Fall et Rabin Patra : Routing in a Delay Tolerant Network. *SIGCOMM Computer Communication Review*, 34:145—158, 2004.
- [JLC05] Timur Friedman Jeremie Leguay et Vania Conan : MobySpace : Mobility Pattern Space Routing for DTNs. *In ACM SIGCOMM*, août 2005.
- [JP07] A. Jindal et K. Psounis : Contention-aware analysis of routing schemes for mobile opportunistic networks. *In Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking*, page 1—8. ACM New York, NY, USA, 2007.
- [JPS01] R. Jain, A. Puri et R. Sengupta : Geographical routing using partial information for wireless ad hoc networks. *IEEE Personal Communications*, 8(1):48—57, février 2001.
- [JT87] J. Jubin et J.D. Tornow : The darpa packet radio network protocols. 75(1):21—32, janvier 1987.
- [KK00] B. Karp et HT Kung : GPSR : greedy perimeter stateless routing for wireless networks. *In Proceedings of the 6th annual international conference on Mobile computing and networking*, page 243—254. ACM New York, NY, USA, 2000.
- [KV99] Y.-B. Ko et N.H. Vaidya : Geocasting in mobile ad hoc networks : location-based multicast algorithms. *In Proc. Second IEEE Workshop on Mobile Computing Systems and Applications*, page 101—110, février 1999.
- [KV00] Y.B. Ko et N.H. Vaidya : Location-Aided Routing (LAR) in mobile ad hoc networks. *Wireless Networks*, 6(4):307—321, 2000.
- [LDS04] A. Lindgren, A. Doria et O. Schelen : Probabilistic Routing in Intermittently Connected Networks. *In Proceedings of the The First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR 2004)*, Fortaleza, Brazil, août 2004.
- [LKM07] Vincent Lenders, Gunnar Karlsson et Martin May : Wireless Ad Hoc Podcasting. *In Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, juin 2007.
- [LLS⁺06] Jeremie Leguay, Anders Lindgren, James Scott, Timur Friedman et Jon Crowcroft : Opportunistic content distribution in an urban setting. *In Proceedings of the 2006 SIGCOMM workshop on Challenged networks*, page 205—212, Pisa, Italy, 2006. ACM Press.
- [LRS96] B.M. Leiner, R.J. Ruther et A.R. Sastry : Goals and challenges of the DARPA GloMo program [global mobile information systems]. *IEEE Personal Communications*, 3(6):34—43, décembre 1996.
- [Mal98] G. Malkin : RFC2453 : RIP Version 2. *RFC Editor United States*, 1998.
- [MHM05] Mirco Musolesi, Stephen Hailes et Cecilia Mascolo : Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks. *In Proceedings of the IEEE*

- 6th International Symposium on a World of Wireless, Mobile, and Multimedia Networks (WoWMoM 2005), Taormina, Italy.* IEEE press, juin 2005.
- [MHMC08] Mirco Musolesi, Pan Hui, Cecilia Mascolo et Jon Crowcroft : Writing on the Clean Slate : Implementing a Socially-Aware Protocol in Haggle. *In Proceedings of the 2nd IEEE International Workshop on Autonomic and Opportunistic Communications (AOC 2008)*, Newport Beach, California, USA, juin 2008. ACM Press.
- [MLKW07] Martin May, Vincent Lenders, Gunnar Karlsson et Clemens Wacha : Wireless Opportunistic Podcasting : Implementation and Design Tradeoffs. *In Proceedings of the second workshop on Challenged networks CHANTS*, page 75—82, New York, NY, USA, 2007. ACM Press.
- [MM09] Mirco Musolesi et Cecilia Mascolo : CAR : Context-aware Adaptive Routing for Delay Tolerant Mobile Networks. *IEEE Transactions on Mobile Computing*, 8(2):246—260, février 2009.
- [MMC09] A.J. Mashhadi, S.B. Mokhtar et L. Capra : Habit : Leveraging Human Mobility and Social Network for Efficient Content Dissemination in MANETs. *In the 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2009.
- [MMH05] Mirco Musolesi, Cecilia Mascolo et Stephen Hailes : EMMA : Epidemic Messaging Middleware for Ad hoc networks. *Personal and Ubiquitous Computing Journal*, 2005.
- [Moy98] J. Moy : RFC2328 : OSPF Version 2. *RFC Editor United States*, 1998.
- [MSN05] M. Motani, V. Srinivasan et P.S. Nuggehalli : Peoplenet : engineering a wireless virtual social network. *In Proceedings of the 11th annual international conference on Mobile computing and networking*, page 243—257, 2005.
- [NGP07] Hoang Anh Nguyen, Silvia Giordano et Alessandro Puiatti : Probabilistic routing protocol for intermittently connected mobile ad hoc network (propicman). *In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM)*, page 1—6, juin 2007.
- [NTCS99] S. Y. Ni, Y. C. Tseng, Y. S. Chen et J. P. Sheu : The Broadcast Storm Problem in a Mobile Ad Hoc Network. *In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, page 151—162. ACM/IEEE, 1999.
- [PB02] PR Pietzuch et JM Bacon : Hermes : A distributed event-based middleware architecture. *In Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops*, page 611—618, 2002.
- [PBRD03] C. Perkins, E. Belding-Royer et S. Das : RFC 3561 : ad hoc on-demand distance vector (AODV) routing. *RFC Editor United States*, 2003.
- [PCM03] GP Picco, G. Cugola et AL Murphy : Efficient content-based event dispatching in the presence of topological reconfiguration. *In Proceedings of the 23rd International Conference on Distributed Computing Systems*, page 234—243, 2003.

-
- [PFGK03] Eugster Patrick, Pascal Felber, Rachid Guerraoui et Anne-Marie Kermarrec : The many faces of publish/subscribe. *ACM Computing Surveys*, 35:114—131, 2003.
 - [PPC06] Luciana Pelusi, Andrea Passarella et Marco Conti : Opportunistic Networking : Data Forwarding in Disconnected Mobile Ad Hoc Networks. *IEEE Communications Magazine*, novembre 2006.
 - [QVL02] A. Qayyum, L. Viennot et A. Laouiti : Multipoint relaying for flooding broadcast messages in mobile wireless networks. *In Proc. 35th Annual Hawaii International Conference on HICSS System Sciences*, page 3866—3875, janvier 2002.
 - [RD01] A. Rowstron et P. Druschel : Pastry : Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. page 329—350, 2001.
 - [Riv92] R. Rivest : RFC 1321 : The MD5 Message-Digest algorithm. *RFC Editor United States*, 1992.
 - [SBC⁺98] R. Strom, G. Banavar, T. Chandra, M. Kaplan, K. Miller, B. Mukherjee, D. Sturman et M. Ward : Gryphon : An information flow based approach to message brokering, 1998.
 - [SCS02] Yoav Sasson, David Cavin et Andr  Schiper : Probabilistic broadcast for flooding in wireless mobile ad hoc networks. pages 1124--1130, 2002.
 - [SH05] T. Small et Z.J. Haas : Resource and performance tradeoffs in delay-tolerant wireless networks. *In Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, page 260—267. ACM New York, NY, USA, 2005.
 - [SMLN⁺03] I. Stoica, R. Morris, D. Liben-Nowell, DR Karger, MF Kaashoek, F. Dabek et H. Balakrishnan : Chord : a scalable peer-to-peer lookup protocol for internet applications. *IEEE/ACM Transactions on networking*, 11(1):17—32, 2003.
 - [SPR05] T. Spyropoulos, K. Psounis et C. S. Raghavendra : Spray and Wait : an efficient routing scheme for intermittently connected mobile networks. *In ACM SIGCOMM Workshop on Delay-Tolerant Networking*, page 252—259, août 2005.
 - [SPR07] Thrasyvoulos Spyropoulos, Konstantinos Psounis et Cauligi S. Raghavendra : Spray and Focus : Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility. *In Proc. Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, page 79—85, mars 2007.
 - [SRJB03] Rahul C. Shah, Sumit Roy, Sushant Jain et Waylon Brunette : Data MULEs : Modeling a Three-Tier Architecture for Sparse Sensor Networks. *In Proceedings of IEEE SNPA Workshop*, 2003.
 - [SSL10] Cecilia Mascolo Salvatore Scellato, Mirco Musolesi et Vito Latora : On Nonstationarity of Human Contact Networks. *In In Proceedings of the 2nd Workshop on Simplifying Complex Networks for Practitioners (SIMPLEX'10)*, 2010. To appear.
 - [VB00] Amin Vahdat et David Becker : Epidemic Routing for Partially Connected Ad Hoc Networks. Rapport technique, Duke University, avril 2000.

- [VRKS06] Spyros Voulgaris, Etienne Riviere, Anne-Marie Kermarrec et Maarten Van Steen : Sub-2-sub : Self-organizing content-based publish subscribe for dynamic large scale collaborative networks. *In In proceedings of the fifth International Workshop on Peer-to-Peer Systems*, 2006.
- [YB04] E. Yoneki et J. Bacon : Content-based routing with on-demand multicast. *In Proc. 23rd ICDCS Workshop-WWAN*, 2004.
- [YGC09] E. Yoneki, D. Greenfield et J. Crowcroft : Dynamics of Inter-Meeting Time in Human Contact Networks. *In Proceedings of the 2009 International Conference on Advances in Social Network Analysis and Mining*, page 356—361, 2009.
- [YHCC07] E. Yoneki, P. Hui, S.Y. Chan et J. Crowcroft : A socio-Aware Overlay for Publish/Subscribe Communication in Delay Tolerant Networks. *In Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, page 225—234, 2007.
- [ZL77] J. Ziv et A. Lempel : A universal algorithm for sequential data compression. *IEEE transactions on Information Theory*, 23(3):337—343, 1977.
- [ZNKT07] X. Zhang, G. Neglia, J. Kurose et D. Towsley : Performance modeling of epidemic routing. *Computer Networks*, 51(10):2867—2891, 2007.

Définition et validation d'un modèle de communication
supportant la communication basée contenus
dans les réseaux mobiles ad hoc discontinus

L'activité de recherche des dernières décennies dans le domaine des réseaux mobiles ad hoc (MANETs) a essentiellement visé à définir des méthodes de routage dynamique au sein de ces réseaux. La plupart des propositions faites dans cette optique reposent sur l'hypothèse que la communication entre deux terminaux mobiles n'est possible que si une route pour l'acheminement des messages peut être établie entre ces terminaux lorsque cela est nécessaire. Cette approche équivaut à considérer que la communication entre deux terminaux ne peut être réalisée que dans un réseau totalement connexe.

Depuis quelques années, l'activité de recherche dans le domaine des MANETs a été étendue afin de prendre en compte les spécificités des MANETs discontinus, c'est-à-dire des MANETs apparaissant sous la forme d'une collection de sous-réseaux connexes (on parlera d'îlots de connectivité) au sein desquels les terminaux peuvent communiquer (éventuellement en utilisant du routage dynamique), mais entre lesquels aucune communication n'est a priori possible. Le routage de messages dans ce type de réseau est un sujet de recherche qui suscite un intérêt grandissant. L'approche généralement adoptée, dite de "communication opportuniste", consiste à exploiter les terminaux mobiles comme des mules de données capables de stocker, transporter et relayer des messages entre des îlots non connectés du réseau afin qu'ils puissent à terme être remis à leur destinataire.

Dans cette thèse nous nous intéressons au support de la communication basée contenus dans les MANETs discontinus. La communication basée contenus est un modèle de communication dans lequel l'information circule dans le réseau en fonction de l'intérêt que les terminaux y portent plutôt que vers une destination bien établie. Nous pensons que de nombreuses applications peuvent bénéficier d'un tel modèle de communication, comme par exemple des applications de partage de fichiers, de distribution d'articles thématique, d'annonce et de découverte de services, etc. Dans ce manuscrit nous présentons le protocole de communication que nous avons conçu afin d'offrir ce style particulier de communication dans les MANETs discontinus ainsi que les résultats d'expérimentations que nous avons réalisées pour valider notre approche. Ce protocole repose sur une combinaison des concepts de communication basée contenus, de communication opportuniste et de communication multi-sauts pour prendre en compte les caractéristiques des MANETs discontinus.

Definition and validation of a communication model that
supports content-based communication
in disconnected mobile ad hoc networks

Research activity in the area of mobile ad hoc networks (MANETs) has aimed mainly at defining dynamic routing methods within these networks. Most proposals assume that communication between two mobile devices is possible only if a message delivery route can be established between devices when necessary. This approach is equivalent to considering that communication between two mobile devices can only be achieved in a fully-connected network.

More recently, the field has been extended to consider the specificities of disconnected MANETs, that is MANETs appearing as collections of subnets (referred to as islands of connectivity) within which terminals can communicate using dynamic routing, but among which no communication is possible. Routing in such networks is a research area that is gaining attention. The approach generally adopted, called opportunistic networking, is to leverage mobile devices as data mules, able to store, carry, and forward messages among disconnected islands in order to deliver messages to their destinations.

In this thesis I am interested in supporting content-based communication in disconnected MANETs. Content-based communication is a communication model in which information flows towards interested terminals rather than towards specifically set destinations. I believe that many applications can benefit from this communication model, such as file sharing, news articles distribution, service advertisement and discovery, etc. In this manuscript I present the communication protocol I have designed to provide this style of communication in disconnected MANETs; I also present the experiments I conducted to validate my approach. This protocol relies on a combination of content-based communication, opportunistic networking, and multi-hop communication concepts to take into account the characteristics of disconnected mobile ad hoc networks.



n d'ordre : 201

Université de Bretagne Sud

Centre d'Enseignement et de Recherche Y. Coppens - rue Yves Mainguy - 56000 VANNES

Tél : + 33(0)2 97 01 70 70 Fax : + 33(0)2 97 01 70 70