



Content-Based Communication in Disconnected Mobile Ad Hoc Networks

Julien Haillet, Frédéric Guidec

► **To cite this version:**

Julien Haillet, Frédéric Guidec. Content-Based Communication in Disconnected Mobile Ad Hoc Networks. 8e conférence internationale sur les nouvelles technologies de la répartition (NOTERE'08), Jun 2008, Lyon, France. ACM, pp.162-173, 2008. <hal-00342646>

HAL Id: hal-00342646

<https://hal.archives-ouvertes.fr/hal-00342646>

Submitted on 28 Nov 2008

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.

Communication « basée contenus » dans les réseaux mobiles ad hoc discontinus

Julien Haillot
Laboratoire VALORIA
Université de Bretagne Sud
Vannes, France
Julien.Haillot@univ-ubs.fr

Frédéric Guidec
Laboratoire VALORIA
Université de Bretagne Sud
Vannes, France
Frederic.Guidec@univ-ubs.fr

RÉSUMÉ

Dans le modèle de la communication dite « basée contenus » (*CBN: Content-Based Communication*), l'information est acheminée vers les récepteurs intéressés, plutôt que vers des destinataires identifiés. Ce style de communication répond parfaitement aux besoins des applications nécessitant une API de communication de type *publish-subscribe*. Dans cet article nous nous intéressons au support de la communication basée contenus dans un réseau mobile ad hoc (MANET) à connectivité partielle ou intermittente. Nous présentons un protocole capable d'assurer l'acheminement de l'information entre des terminaux mobiles producteurs et consommateurs de cette information, en dépit de l'absence de connectivité de bout-en-bout entre ces terminaux. Des résultats de simulation sont présentés, qui attestent de l'efficacité de ce protocole dans un réseau mobile ad hoc constitué de terminaux portés par des individus évoluant dans un environnement de type campus.

Mots-clés

communication, réseau, mobile, ad hoc, basée contenus, opportuniste, tolérant les délais

1. INTRODUCTION

Les réseaux mobiles ad hoc ou MANETs (*Mobile Ad hoc NETworks*) ont fait l'objet de nombreux travaux de recherche au cours de la dernière décennie. Ces travaux ont dans un premier temps été menés essentiellement à des fins d'applications militaires, mais depuis quelques années des applications civiles sont également envisagées. La communication en mode ad hoc peut en effet se justifier dès lors que le recours à un réseau d'infrastructure s'avère soit techniquement difficile, soit économiquement peu rentable (e.g. secouristes intervenant à la suite d'une catastrophe naturelle, équipes de scientifiques travaillant en terrain désertique, systèmes de communication inter-véhicules, réseaux de capteurs, etc.).

Les premiers travaux de recherche menés dans ce domaine ont eu pour objectif principal de définir des méthodes pour

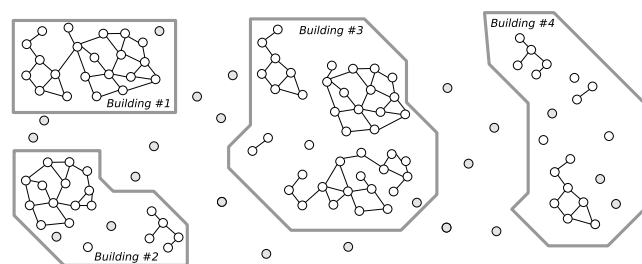


Figure 1: Illustration d'un réseau ad hoc discontinu, constitué de terminaux mobiles portés par des individus évoluant dans et entre les bâtiments d'un campus

assurer l'acheminement de messages — ou, plus classiquement, de paquets IP — de bout en bout dans un MANET. Dans cette optique, l'approche communément adoptée consiste à considérer chaque terminal mobile comme un routeur potentiel. La topologie d'un réseau constitué d'équipements mobiles pouvant varier en continu, un chemin de bout en bout, exploitable à un moment précis entre deux hôtes A et B, ne sera plus nécessairement disponible quelques instants plus tard. Le routage dans un MANET implique donc de remettre sans cesse en question les chemins de routage qui ont pu être identifiés jusqu'alors, ces chemins ayant pu devenir inutilisables ou inefficaces.

Les travaux réalisés dans ce domaine ont initialement considéré le cas des réseaux présentant des propriétés de densité et de connectivité favorables. Des protocoles de routage dynamique tels que OLSR [7], DYMO [5], etc. ne peuvent en effet être mis en œuvre, et donner des résultats satisfaisants, que dans des réseaux connexes. Des études comparatives des divers protocoles de routage dynamique développés dans cette optique sont disponibles dans [20] et [6].

Depuis quelques années, l'activité de recherche a été étendue afin de prendre en compte les problèmes spécifiques posés par des réseaux à connectivité partielle ou intermittente [3]. La figure 1 présente, en guise d'exemple, le cas d'un réseau ad hoc constitué de terminaux mobiles (e.g. ordinateurs portables ou assistants numériques personnels) transportés par des individus évoluant dans un environnement de type campus. Dans cet exemple on peut constater que le graphe représentant le réseau global n'est pas connexe. La densité des terminaux est insuffisante pour qu'on puisse trouver un chemin reliant toute paire de terminaux du réseau. On voit donc apparaître des sous-graphes connexes — on



Figure 2: Détail de la figure 1, illustrant les déplacements de quelques individus sur le campus

parlera « d’îlots » — au sein desquels les communications sont possibles (en utilisant éventuellement du routage dynamique multi-sauts), mais entre lesquels aucune communication n’est a priori possible.

De nombreux travaux ont été lancés ces dernières années en vue de s’accommoder de l’absence de connectivité de bout en bout dans les réseaux mobiles ad hoc discontinus tels que celui présenté dans la figure 1. Une étude comparative des travaux les plus récents est disponible dans [23]. En règle générale, l’approche prônée par ces divers travaux consiste à remplacer — ou compléter — les mécanismes de routage dynamique conçus pour les réseaux denses par des mécanismes permettant de tolérer les ruptures de connectivité occasionnelles ou chroniques. La mobilité des terminaux eux-mêmes est en outre mise à profit pour leur faire transporter physiquement des messages (ou paquets) à travers le réseau, contribuant ainsi à rétablir une certaine forme de « connectivité » entre des fragments autrement non connectés du réseau.

Les concepts de « communication opportuniste » (*Opportunistic Networking* [17]) et de « communication tolérant les délais » (*Delay-Tolerant Networking*¹ [11]) sont fréquemment utilisés dans la littérature pour désigner le mode de communication résultant de cette approche. En effet les échanges entre terminaux mobiles s’effectuent de manière opportuniste, à l’occasion de contacts fugitifs — et souvent non planifiés — entre ces terminaux. En outre le fait de faire transporter physiquement des messages par des terminaux en mouvement implique des temps de latence importants, qui nécessitent de la part des applications susceptibles d’exploiter ce mode de communication atypique une tolérance certaine vis-à-vis de ces délais de transmission.

De manière générale, cette approche nécessite de doter les terminaux mobiles de la capacité de stocker des messages en transit dans un cache avant de les réémettre au moment opportun. L’expression *Store, Carry, and Forward* est utilisée pour désigner ce type particulier de traitement des messages impliquant leur stockage, leur transport éventuel par des terminaux en mouvement, et leur renvoi final vers d’autres terminaux relais ou vers les terminaux destinataires.

La figure 2 illustre un cas typique dans lequel un terminal mobile transporté par un individu se déplaçant entre deux groupes de personnes (ces groupes n’étant pas à portée radio l’un de l’autre) peut contribuer à transporter des messages d’un groupe à l’autre, assurant ainsi une certaine forme de « connectivité » — non instantanée, et justifiant donc une approche « tolérant les délais » — entre ces deux groupes.

En appliquant le modèle de la communication opportuniste

tolérant les délais dans les réseaux mobiles ad hoc, on ouvre d’intéressantes perspectives dans la mesure où cette approche permet de s’affranchir de l’exigence de connectivité de bout en bout imposée jusqu’alors par les algorithmes de routage dynamique traditionnels.

Dans la suite de cet article nous nous intéressons au support de la communication dite « basée contenus » (*CBN: Content-Based Communication*² [4]) dans les MANETs discontinus. Dans ce modèle de communication, chaque unité d’information (paquet, message, document, etc.) injectée dans le réseau est censée atteindre l’ensemble des récepteurs intéressés, plutôt que des destinataires spécifiquement désignés par l’émetteur. L’information circule donc dans le réseau en fonction de l’intérêt que les nœuds du réseau y portent, plutôt que vers une destination bien établie. Ce nouveau style de communication répond parfaitement aux besoins des applications de partage d’information, d’annonce et de découverte de services, et plus généralement à toutes les applications nécessitant une API de communication de type *publish-subscribe*.

De très nombreux articles concernant la communication basée contenus ont déjà été publiés, mais ces articles décrivent pour la plupart des méthodes applicables, soit dans des réseaux câblés et stables, soit dans des MANETs connexes [9, 14, 18]. Ils proposent en général de construire et de maintenir une structure de routage dirigé par le contenu, cette structure permettant alors de router les messages depuis leurs producteurs vers tous les récepteurs intéressés.

Une exception notable vis-à-vis de cette approche est le protocole décrit dans [2]. Ce protocole ne cherche pas à bâtir une quelconque structure afin de supporter les décisions de routage. Il s’appuie au contraire sur une utilisation systématique des transmissions en diffusion, laissant aux hôtes qui reçoivent un message diffusé par l’un de leurs voisins la décision d’accepter ou non ce message en vue de le rediffuser à leur tour. Cette décision doit être prise en fonction d’une estimation de la distance séparant l’hôte considéré des récepteurs intéressés. Ce protocole ne peut donc fonctionner que dans un environnement connexe, dans lequel des chemins existent toujours entre émetteur et récepteurs.

Le cas particulier des MANETs discontinus est pris en compte dans [8]. Cet article décrit une approche dans laquelle une structure de routage multi-sauts en fonction du contenu (limitée à un certain « horizon ») est bâtie autour de chaque hôte mobile. Une fonction dite « d’utilité » (*utility function*) est utilisée pour sélectionner les meilleurs relais pour chaque type de message, et des relais mobiles peuvent aider à disséminer des messages entre des fragments non connectés du réseau.

Les sections suivantes présentent le protocole que nous avons développé, et qui reprend certaines des caractéristiques des deux protocoles évoqués ci-dessus. Plutôt que d’essayer de construire une structure de routage, notre protocole utilise des diffusions périodiques (également limitées à un certain « horizon » autour de chaque émetteur) permettant à chaque hôte mobile de se faire connaître de ses voisins, de leur faire savoir à quel type de documents ils s’intéressent (via la description de son « profil d’intérêt »), et enfin de leur proposer des documents dont il dispose et qui correspondent à leurs propres profils d’intérêt.

¹L’expression *Disruption-Tolerant Networking* est également utilisée dans la littérature.

²L’expression *Interest-Based Communication* est aussi utilisée dans la littérature.

2. VUE D'ENSEMBLE DU PROTOCOLE

Le protocole que nous avons défini repose sur le principe général du *gossiping* (ou « papotage »), dans lequel des hôtes mobiles profitent de contacts occasionnels pour échanger des informations diverses, en fonction de leurs centres d'intérêts respectifs. Ce type de protocole a d'ailleurs été formalisé avec l'algorithme *Autonomous Gossiping* (A/G) [10]. Dans la définition de cet algorithme, le schéma de dissémination de l'information est assimilé à un processus d'épidémie, chaque hôte étant plus ou moins susceptible d'être « infecté » par tel ou tel type d'information (le modèle de dissémination épidémique, introduit dans [21], repose d'ailleurs sur un principe similaire). Une différence fondamentale entre notre protocole et l'algorithme A/G est que ce dernier repose exclusivement sur des transmissions à un saut (et donc des échanges s'effectuant exclusivement entre voisins directs), alors que notre protocole peut exploiter des transmissions multi-sauts au sein d'un îlot connexe.

Pour ce faire, notre protocole se décompose en deux couches. La couche supérieure supporte la dissémination basée contenus, et dans un mode opportuniste tolérant les délais, d'éléments d'information structurés que nous désignons par le terme générique de « documents ». Cette couche assure le stockage de documents dans le cache local d'un hôte mobile, de telle sorte que cet hôte fasse office de transporteur pour les documents maintenus dans son cache lorsqu'il se déplace dans le réseau. Elle définit également les modalités d'interaction entre des hôtes voisins dans le réseau, afin que ces hôtes puissent échanger des documents en fonction de leur profils d'intérêt respectifs. Des hôtes voisins sont des hôtes qui résident — a priori temporairement — dans le même fragment connecté du réseau (ou « îlot »). L'interaction entre des hôtes d'un même îlot nécessite qu'ils soient en mesure de communiquer, en utilisant pour ce faire des transmissions à un saut ou à plusieurs sauts. La couche inférieure de notre protocole fournit les mécanismes permettant d'assurer le relais multi-sauts au sein d'un îlot.

Utilisation frugale du médium radio. Notre protocole a été conçu de manière à être aussi frugal que possible vis-à-vis des ressources qu'il consomme, et en particulier vis-à-vis de l'utilisation du médium radio. Dans cette optique, il minimise systématiquement la quantité de données transmises par chaque terminal sur le canal radio, tout en évitant les retransmissions inutiles de ces données. Il s'appuie notamment, chaque fois que c'est possible, sur des transmissions en diffusion (*broadcast*) plutôt que sur des transmissions en mode *unicast*. Ainsi, lorsqu'un hôte doit faire parvenir un message à tous ses voisins directs, cette opération est réalisée en une seule diffusion de ce message, plutôt qu'en adressant une copie de ce message successivement à chacun de ses voisins. De ce point de vue notre approche s'apparente à celle prônée dans [2] et dans [22], par exemple. Cette approche peut d'ailleurs paraître assez naturelle dans un environnement dans lequel les transmissions se font via un médium radio, puisqu'avec ce type de médium toute transmission se traduit bien par une diffusion dans l'éther. Pourtant, dans de nombreux travaux récents on ressent de la part des auteurs une certaine réticence à exploiter des transmissions en diffusion. Cette réticence est motivée par le fait qu'avec une technologie de transmission sans fils telle que Wi-Fi (alias IEEE 802.11), par exemple, l'émission d'une trame en mode *broadcast* (i.e. vers tous les hôtes voisins) est effectivement nettement moins fiable que son émission

en mode *unicast* (i.e. vers un hôte voisin explicitement désigné). Cette différence résulte du fait que, dans le protocole MAC 802.11, l'émission d'une trame en mode *unicast* implique l'utilisation d'un mécanisme d'acquiescement, avec réémission en cas de défaut d'acquiescement [1]. L'émission d'une trame en mode *broadcast*, en revanche, n'implique aucun mécanisme de ce type. Avec la technologie Wi-Fi, l'émission de trames en mode *broadcast* est donc nettement plus hasardeuse que l'émission de trames en mode *unicast*. En cas d'interférences pendant l'émission d'une trame, celle-ci peut ne pas être reçue sans que ni l'émetteur, ni le(s) destinataire(s) en soient informés. En contrepartie, l'émission d'une trame 802.11 en mode *broadcast* est nettement moins coûteuse qu'une émission en mode *unicast*, dans la mesure où elle n'implique ni trames d'acquiescement, ni réémissions éventuelles. Il en résulte une consommation moindre des ressources mises en jeu lors de la transmission (i.e. occupation moindre du médium radio, et consommation moindre d'énergie au niveau des hôtes impliqués).

En concevant notre protocole nous avons donc choisi de privilégier une consommation réduite des ressources, au détriment de la fiabilité des transmissions. Nous utilisons des transmissions en mode *broadcast* chaque fois que c'est possible, tout en faisant en sorte que le protocole puisse résister aux échecs de transmissions. De manière générale les interactions entre hôtes voisins reposent sur un schéma d'échanges opportunistes plutôt que sur un schéma transactionnel strict. Ainsi, lorsqu'un hôte diffuse par exemple une annonce à l'intention de ses voisins (cet aspect du protocole sera détaillé plus loin, certains d'entre eux peuvent ne pas recevoir cette annonce, sans que ce phénomène compromette en aucune façon le bon fonctionnement de l'hôte émetteur ou des récepteurs potentiels.

3. VUE DÉTAILLÉE DU PROTOCOLE

3.1 Couche supérieure : support de la communication basée contenus

Entités manipulées par le protocole. Les principales entités manipulées par la couche supérieure de notre protocole sont décrites ci-dessous.

Documents, descripteurs, et identifiants — Un document est une unité d'information structurée, qu'un hôte peut injecter dans le réseau afin qu'il s'y propage, et soit à terme réceptionné par tout hôte affichant un intérêt pour le type particulier d'information contenue dans ce document. Un document est en fait constitué de deux parties : son descripteur, et son contenu. Le descripteur peut être vu comme une collection d'attributs fournissant n'importe quel type d'information à propos du document, comme par exemple son identifiant, son origine, sa date de production, le type et la nature de son contenu, une liste de mots-clés le caractérisant, etc. Le seul attribut dont la présence est absolument requise dans le descripteur d'un document est son identifiant. Cet identifiant doit en outre être unique, car il va permettre d'assurer les échanges entre hôtes dans le réseau, tout en leur évitant de stocker ou d'échanger des doublons. De manière générale, nous faisons l'hypothèse que le poids d'un document dépasse très 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

```

<descriptor
  id="254d3g64z36cd"
  service="filesharing"
  type="application/pdf"
  date="Fri Oct 12 09:52:11 CEST 2007"
  deadline="Sat Oct 13 14:00:00 CEST 2007"
  from="Fred"
  keywords="mobile,ad hoc,delay-tolerant,
            opportunistic,gossip-based"
/>

```

Figure 3: Exemple de descripteur de document

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 hôtes mobiles.

Un exemple de descripteur de documents est présenté dans la figure 3. Ce descripteur concerne un document diffusé dans le cadre d'un service de partage de fichiers. Le descripteur spécifie notamment quel est 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.

Cache — Nous ne faisons aucune hypothèse quant à la capacité de stockage de chaque hôte mobile. En revanche il est admis que cette capacité est a priori limitée, et qu'elle peut être différente d'un hôte à l'autre. Plusieurs travaux comparant les mérites respectifs de diverses stratégies de gestion de cache dans les réseaux tolérant les délais ont fait l'objet de publications ces dernières années (e.g. [12]). Dans nos propres travaux, nous ne cherchons donc pas à développer de nouvelles méthodes de gestion de cache. Nous supposons simplement que chaque hôte applique une politique quelconque afin de gérer son propre cache. Par ailleurs nous ne faisons pas non plus l'hypothèse que tous les hôtes d'un réseau appliquent nécessairement la même politique de gestion de cache.

Profils d'intérêt — Le profil d'intérêt d'un hôte caractérise le type de 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. Pour des raisons pratiques, nous définissons le profil d'un hôte comme un prédicat applicable à des descripteurs de documents. En appliquant ce prédicat au descripteur d'un document, un hôte peut ainsi décider s'il doit réceptionner ce document et le placer dans son cache. Un exemple de profil d'intérêt basique est reproduit dans la figure 4. Ce profil spécifie que l'hôte considéré est intéressé par tout document diffusé dans le cadre du service de partage de fichiers, dès lors que ce document est caractérisé par au moins l'un des trois mots-clés indiqués. Un hôte affichant ce profil d'intérêt se considérerait donc comme étant intéressé par le document dont le descripteur est présenté dans la figure 3.

On peut noter que le profil d'intérêt d'un hôte peut être défini, dans certains cas, directement par le propriétaire ou

```

<profile
  service="filesharing"
  keywords="sensor|vehicular|opportunistic"
/>

```

Figure 4: Exemple de spécification du profil d'intérêt d'un hôte mobile

administrateur de cet équipement. Dans d'autres cas ce sont les applications s'exécutant sur cet équipement qui peuvent être amenées à ajuster d'elles-mêmes le profil de l'hôte, en fonction de leurs propres besoins. En fait de nombreuses stratégies de définition et de gestion du profil d'intérêt d'un hôte mobile sont envisageables. Pour l'heure nous nous contentons de décrire un protocole qui a été développé tout spécialement afin de pouvoir supporter la dissémination de documents dans le réseau, tout en tenant compte des profils des hôtes constituant ce réseau.

Comme indiqué précédemment, notre protocole a été conçu de manière à être particulièrement frugal vis-à-vis des ressources consommées afin d'assurer la dissémination de documents dans le réseau. Nous nous sommes notamment efforcés de minimiser le volume des données transmises sur le médium radio, tout en évitant les retransmissions inutiles de ces données. L'interaction entre hôtes mobiles repose sur un schéma extrêmement simple, dans lequel chaque hôte informe périodiquement son voisinage de son propre profil d'intérêt, tout en proposant à ses voisins de leur fournir les documents qui sont déjà disponibles dans son propre cache. Lorsqu'un hôte découvre ainsi que l'un de ses voisins est en mesure de lui fournir un document qui l'intéresse (c'est-à-dire un document qui correspond à son propre profil d'intérêt, mais qui ne se trouve pas déjà dans son cache local), il peut adresser une requête au voisin concerné afin de se procurer le document en question. Des contacts transitoires entre hôtes mobiles sont ainsi exploités de manière opportuniste afin d'échanger des documents entre ces hôtes, en tenant compte de leurs profils d'intérêt respectifs, et des documents dont ils disposent déjà.

Annonce périodique du catalogue et du profil d'intérêt personnel d'un hôte. Chaque hôte n_i diffuse périodiquement une annonce qui combine :

- une description de son propre profil d'intérêt $prof(n_i)$
- un catalogue $cat(n_i)$, contenant les descripteurs de documents qui sont disponibles dans son cache local, et qu'il estime être susceptible d'intéresser ses voisins

Cette annonce est diffusée sous la forme d'un unique message de contrôle, dont la portée de diffusion peut être fixée explicitement par l'hôte émetteur (cet aspect est expliqué plus en détails dans la section 3.2).

En diffusant périodiquement une description de son propre profil d'intérêt, un hôte permet à ses voisins de découvrir quel type de documents l'intéresse. Inversement, en recevant le même genre d'information de chacun de ses voisins, l'hôte en question est en mesure de maintenir une vision précise de ce qui les intéresse. Le contenu du catalogue qu'il diffuse périodiquement peut ainsi être ajusté en continu, de manière à ne contenir que les descripteurs de documents qui sont effectivement susceptibles d'intéresser ses voisins. Le

coût résultant de la diffusion de ce catalogue peut ainsi être réduit au minimum, la taille du catalogue lui-même étant ajustée au plus bas afin de ne jamais proposer aux hôtes voisins des documents qui, de toute façon, ne correspondent aucunement à leurs profils d'intérêt respectifs. Un hôte disposant dans son cache d'un très grand nombre de documents s'abstiendra de diffuser un catalogue portant sur tous ces documents si seulement un très petit nombre d'entre eux — voire aucun — présente effectivement de l'intérêt pour ses voisins.

Réception du catalogue émis par un voisin.

Lorsqu'un hôte réceptionne une annonce contenant le catalogue d'un voisin, il examine les descripteurs contenus dans ce catalogue afin d'identifier des documents dont les caractéristiques correspondent à son profil d'intérêt, et qui ne se trouvent pas déjà dans son cache local. Si de tels documents sont effectivement mentionnés dans le catalogue, alors l'hôte récepteur de l'annonce construit une requête à l'intention de l'annonceur, cette requête contenant simplement les identifiants des documents qu'il souhaite obtenir de ce dernier. La requête est ensuite émise à destination de l'annonceur, encapsulée dans un message de contrôle émis en mode *unicast*.

Traitement des requêtes reçues des voisins. Après avoir diffusé une annonce contenant son catalogue, un hôte est susceptible de recevoir une ou plusieurs requêtes provenant de ses voisins. Ces requêtes sont traitées séquentiellement : pour chaque document demandé par un voisin, l'hôte récupère ce document du cache local, et le diffuse dans son voisinage. On peut noter que le document demandé est diffusé, plutôt que d'être adressé exclusivement au demandeur. Ce choix de conception s'explique par le fait qu'après avoir proposé à ses voisins de leur fournir un certain document, un hôte peut fort bien recevoir plusieurs requêtes pour ce même document de la part de plusieurs voisins. Dans un tel scénario, tous les voisins demandant à obtenir une copie du même document peuvent être satisfaits par une unique diffusion de ce document par l'hôte qui le leur a proposé. Ainsi, pour éviter que des requêtes successives concernant un même document entraînent des réémissions inutiles de ce document, chaque hôte maintient à jour un historique des documents qu'il a récemment diffusés à la demande de ses voisins. Cet historique est réinitialisé à chaque fois que l'hôte diffuse une nouvelle annonce contenant son profil et son catalogue. Ainsi, lorsque plusieurs voisins d'un hôte cherchent à obtenir de lui le même document, ce document est diffusé une fois et une seule sur le médium de transmission.

Réception de nouveaux documents. Tout hôte réceptionnant un document diffusé par l'un de ses voisins doit vérifier s'il est lui-même intéressé par ce document. Si c'est le cas, alors le document peut être déposé dans le cache local (s'il ne s'y trouvait pas déjà). Dès lors, tout hôte ayant décidé d'accepter un nouveau document va pouvoir jouer le rôle de transporteur mobile pour ce document, et contribuer ainsi à en assurer la dissémination dans le réseau.

On peut noter que ce modèle de communication permet à des hôtes mobiles de collecter des documents qui les intéressent sans même avoir à en faire la demande, en les interceptant simplement lors de leur diffusion sur le médium radio. Ainsi, un hôte n_i peut obtenir un document en en faisant la demande explicite à l'un de ses voisins n_j , mais il peut aussi obtenir ce document parce qu'un autre hôte n_k (qui n'est d'ailleurs pas forcément l'un de ses propres

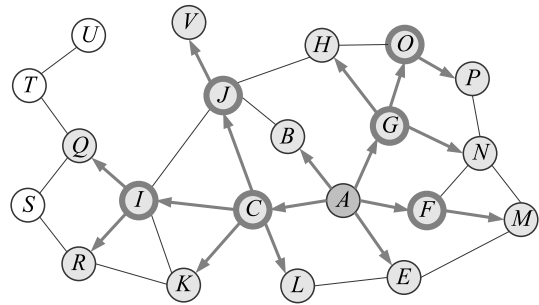


Figure 5: Illustration du mécanisme de diffusion au sein d'un îlot connexe, via des relais multi-points

voisins) en a fait la demande à n_j . Les expérimentations que nous avons menées (tant en conditions réelles qu'avec un simulateur) ont montré que cette possibilité qu'ont les hôtes mobiles d'obtenir certains documents « par hasard », sans même en avoir fait la demande, constitue une conséquence logique mais néanmoins intéressante de notre décision d'utiliser des transmissions en diffusion plutôt qu'en mode *unicast* chaque fois que c'est possible. En effet, un hôte qui obtient un document intéressant sans même en avoir fait la demande au préalable va pouvoir s'abstenir de demander ce document plus tard à un quelconque voisin. On économise ainsi un certain nombre de transmissions, ce qui dans un environnement aux ressources limitées est toujours appréciable.

3.2 Couche inférieure : support du relais immédiat des messages entre hôtes voisins

Comme expliqué dans la section précédente, la couche supérieure de notre protocole nécessite qu'un hôte soit en mesure d'envoyer des messages (contenant soit son profil et catalogue, une requête, ou un document) à ses voisins du moment. Le relais immédiat de messages (par opposition au relais différé) est donc souhaitable afin d'exploiter au mieux la connectivité transitoire existant entre des hôtes qui se trouvent appartenir — peut-être de façon extrêmement fugitive — à un même fragment connexe (îlot) du réseau. La couche inférieure de notre protocole a pour vocation de supporter ce type de relais immédiat, qu'il s'agisse de faire parvenir un message à un hôte spécifique situé dans le voisinage de l'émetteur (trafic *unicast*), ou bien à l'ensemble des voisins de cet émetteur (trafic *broadcast*).

Relais immédiat de messages à diffuser. La diffusion multi-sauts dans un MANET est réputée être une opération extrêmement coûteuse en termes de bande passante, et qui peut même à l'occasion mener au phénomène dit « d'orage de diffusion » (*broadcast storm problem*) [16]. Pour limiter le coût occasionné par la diffusion d'un message, la couche inférieure de notre protocole met en œuvre un mécanisme qui est inspiré de celui qui, dans le protocole OLSR (*Optimized Link State Routing*), est utilisé pour diffuser dans l'ensemble du réseau des informations portant sur l'état des liens de transmission [7, 19].

Concrètement, chaque hôte sélectionne périodiquement un sous-ensemble de ses voisins directs (situés à portée radio) et les enregistre en tant que relais multi-points (*MPR: Multi-Point Relays*). Il s'appuiera ensuite sur ces MPRs — et sur eux-seuls — pour diffuser des messages au delà de sa

propre portée radio. Dans OLSR, qui est un protocole de routage proactif, les MPRs sont utilisés pour diffuser efficacement sur l'ensemble du réseau — supposé connexe — des informations de contrôle relatives à l'état des tables de routage de chacun des hôtes. Ces informations sont alors utilisées localement par chaque hôte pour mettre à jour sa propre table de routage. Dans notre protocole, les MPRs ne servent pas seulement à diffuser des messages de contrôle vers l'ensemble des hôtes accessibles depuis l'émetteur, c'est-à-dire dans l'îlot auquel l'émetteur appartient. Ils vont permettre de diffuser n'importe quel type de message, et ce seulement jusqu'à une certaine distance de l'émetteur. En effet, avec notre protocole l'émetteur d'un message à diffuser a la possibilité de spécifier combien de sauts consécutif — entre hôtes voisins — ce message va pouvoir effectuer avant de cesser de se propager. La figure 5 montre ainsi un exemple dans lequel l'hôte 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. Dans cet exemple, chaque copie du message n'est autorisée à se propager que sur trois sauts consécutifs, ce qui explique pourquoi les hôtes S, T et U, qui sont situés trop loin de l'hôte A bien qu'appartenant au même îlot que lui, ne reçoivent pas son annonce. En outre, on peut observer dans la figure que seuls certains voisins de l'hôte A réémettent effectivement le message lorsqu'il le reçoivent. Dans ce cas précis, il s'agit des hôtes C, F, et G, qui font office de relais multi-points pour le premier saut réalisé par le message, et des hôtes I, J, et O, servant de relais multi-points pour le second saut du message.

L'algorithme utilisé par chaque hôte 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 [19]. 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 hôte réémettant simplement chaque message sur le médium radio lorsqu'il le reçoit pour la première fois.

Dans l'algorithme mis en œuvre dans le protocole OLSR, chaque hôte doit diffuser périodiquement un message de contrôle visant à informer ses voisins directs (i.e. voisins à un saut) de sa présence dans le réseau, tout en leur décrivant la perception qu'il a lui-même de son propre voisinage. En recevant de tels messages de ses divers voisins, un hôte est en mesure d'identifier quels sont ses voisins à un saut et ses voisins à deux sauts, et utiliser cette information pour calculer l'ensemble des MPRs sur lesquels il va pouvoir s'appuyer pour diffuser des messages sur l'ensemble de son voisinage à deux sauts. Dans le protocole OLSR (tel que décrit par exemple dans [19]), des messages de contrôle spécifiques sont diffusés périodiquement par chaque hôte, ces messages contenant les informations requises pour le calcul des ensembles de MPRs. Dans notre propre protocole, l'information permettant le calcul de ces MPRs est transportée dans les messages de contrôle utilisés par ailleurs pour diffuser les annonces réalisées par la couche supérieure du protocole. Ainsi le calcul des ensembles de MPRs ne nécessite la diffusion d'aucun message supplémentaire dans le réseau : les deux types d'information de contrôle — requises par les deux couches du protocole — sont transmises simultanément dans

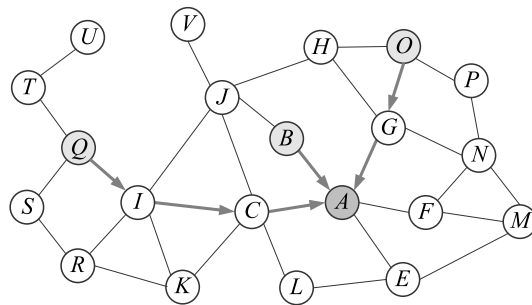


Figure 6: Illustration du mécanisme de routage par la source (*source-routing*) au sein d'un îlot connexe : ici B, O, et Q répondent à un message diffusé par A

le réseau.

Relais immédiat de messages unicast. La couche supérieure de notre protocole nécessite que les hôtes mobiles soient en mesure d'émettre une requête en réponse à une annonce qu'ils viennent de recevoir, cette requête étant bien sûr adressée à l'émetteur de l'annonce. Des messages *unicast* doivent donc pouvoir être routés vers l'émetteur d'un message qui vient tout juste d'être diffusé. Le routage par la source (dans lequel l'émetteur d'un message spécifie explicitement quel trajet ce message doit suivre dans le réseau) est approprié dans de telles circonstances. Chaque message diffusé par la couche basse de notre protocole contient un historique des hôtes par lesquels il a transité jusqu'alors. Cet historique est bien sûr mis à jour à chaque fois que le message transite par un nouvel hôte. Ainsi, lorsqu'un hôte ayant réceptionné un message diffusé estime qu'il doit y répondre, le trajet que doit suivre cette réponse peut être déduit du chemin que le message diffusé a lui-même suivi pour atteindre cet hôte. On peut noter que, pour que cette approche fonctionne dans un réseau dont tous les hôtes sont fortement mobiles, il est nécessaire qu'un message *unicast* émis en réponse à un message diffusé soit émis sans attendre. Dans de telles conditions, on peut estimer que le cheminement que le message diffusé vient de suivre est encore praticable — mais en sens inverse — pour la réponse à ce message.

Considérons de nouveau l'exemple du message diffusé par l'hôte A dans la figure 5, et supposons que les hôtes B, Q, et O décident de répondre à ce message. La figure 6 montre 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 l'hôte A.

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, et à l'aide du simulateur de réseau mobile MADHOC [13]. Quelques uns des résultats obtenus lors des simulations sont présentés ci-dessous.

Paramètres de simulation. 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) semblable à l'exemple reproduit dans la figure 1. Cet environnement est constitué de quatre bâtiments, répartis sur une superficie de $300\text{ m} \times 800\text{ m}$. Chacun des individus évoluant dans cet environnement est supposé être équipé d'un PC portable doté d'une interface Wi-Fi (IEEE 802.11).

La mobilité des individus — et donc, indirectement, celle des équipements 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 cinq bâtiments (les déplacements au sein d'un bâtiment sont donc possibles, au même titre que les déplacements entre bâtiments).

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 3 minutes. La proportion de déplacements au sein d'un même bâtiment est fixée à 40 %, contre 60 % pour les déplacements entre bâtiments. Les interfaces équipant les PC portables sont supposées avoir une portée de transmission omni-directionnelle de 40 mètres en milieu fermé (i.e. à l'intérieur d'un bâtiment), et de 100 mètres en milieu ouvert. Enfin, puisque dans la « vraie vie » un PC 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 hôte mobile (i.e. un PC portable dans le cas présent) 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.

Scénario de communication. Nous considérons un scénario dans lequel les hôtes mobiles produisent de nouveaux documents (chaque document pesant 50 ko), et les injectent dans le réseau à un rythme moyen de 1 document (par hôte) toutes les 5 minutes. Compte tenu du nombre d'hôtes constituant le réseau, ceci correspond à un rythme global de 1 nouveau document injecté dans le réseau toutes les 2.5 secondes. Chaque document porte (dans son descripteur) une étiquette qui le place dans une certaine catégorie thématique. Il y a 16 catégories distinctes, mais chaque documents s'inscrit dans seulement l'une de ces catégories.

Chaque hôte mobile affiche de l'intérêt pour 2 des 16 catégories (soit $1/8$ du trafic global), et ne souhaite donc recevoir que les documents relatifs à l'une ou l'autre de ces deux catégories. Le nombre total d'hôtes dans le réseau (i.e. 120 hôtes) a été choisi de telle sorte qu'on puisse attribuer un profil d'intérêt distinct à chacun de ces hôtes. En d'autres termes, on ne peut trouver deux hôtes dans le réseau qui affichent exactement le même profil d'intérêt, et soient donc intéressés exactement par les mêmes types de documents.

Paramètres protocolaires. Le comportement général de notre protocole est conditionné par deux paramètres essentiels. Le premier de ces paramètres est la période avec laquelle un hôte 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 hôtes dans cet environnement. Ainsi, avec les paramètres de simulation décrits plus haut, les hôtes 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 hôtes mobiles, lors d'une réactivation consécutive à un déplacement, le temps de découvrir les équipements voisins, et d'échanger des documents avec ces voisins. Une période d'annonce plus courte serait toutefois nécessaire si les hôtes mobiles étaient susceptibles de communiquer pendant leurs déplacements (comme ce pourrait être le cas, par exemple, pour des PDAs), cette période devant en outre être d'autant plus courte que les hôtes en question se déplacent rapidement (et sont donc susceptibles d'observer de très brefs contacts avec des équipements voisins). Inversement, la période d'annonce pourrait être rallongée, si les hôtes considérés étaient susceptibles de passer beaucoup plus de temps au même endroit, et donc d'observer autour d'eux un voisinage relativement stable.

Le second paramètre qui peut être ajusté dans notre protocole est le nombre de sauts admissible dans le cas du relais immédiat d'un message par la couche inférieure du protocole, et en particulier lorsqu'un hôte 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 hôte mobile, c'est-à-dire — indirectement — l'envergure du voisinage avec lequel il est disposé à échanger des documents avant de se déplacer de nouveau dans le réseau.

Vitesse de propagation des documents. Notre objectif premier est d'observer dans quelle mesure la portée du relais immédiat de messages peut influencer les performances générales de notre protocole. Le résultat attendu est que, lorsque chaque hôte 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 hôte ne peut interagir qu'avec ses voisins directs (i.e. voisins « à un saut »).

Pour vérifier que cette hypothèse est effectivement vérifiée, nous considérons dans un premier temps un scénario — fort peu 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 hôtes considérés dans la simulation, et que les documents injectés dans le réseau n'ont pas de durée de vie précise.

Le modèle de mobilité utilisé dans cette campagne de simulation (i.e. *Constrained Random Waypoint*) garantit que chaque hôte mobile entrera à un moment ou un autre en contact avec chacun des autres hôtes du réseau. Dans ces conditions, un document pouvant demeurer éternellement dans le réseau est assuré d'atteindre à terme tous les hôtes intéressés. Cependant, le temps nécessaire pour qu'un document atteigne un récepteur précis peut être nettement influencé par les paramètres de notre protocole, et notamment par l'étendue du voisinage avec lequel chaque hôte est autorisé à interagir.

Intéressons nous au temps moyen nécessaire aux documents pour atteindre les hôtes pour lesquels ils présentent

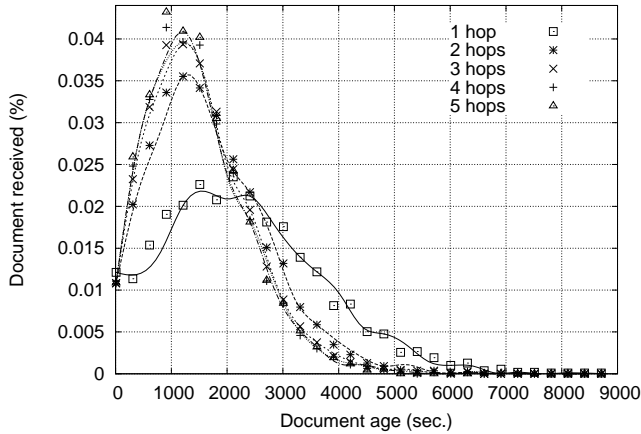


Figure 7: Distribution de l'âge des documents lors de leur réception par un hôte intéressé

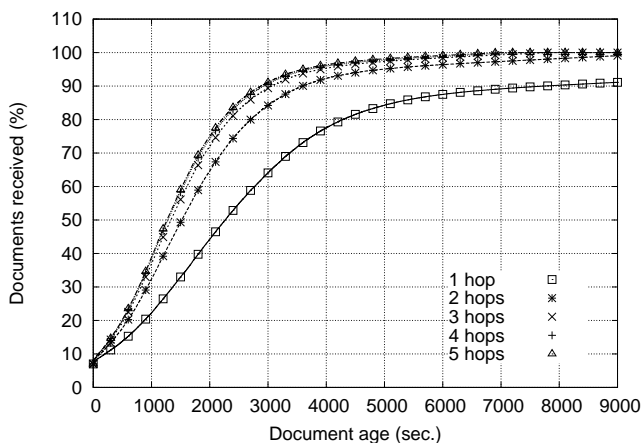


Figure 8: Distribution cumulée de l'âge des documents lors de leur réception par un hôte intéressé

de l'intérêt. La figure 7 montre la distribution normalisée de l'âge des documents lors de leur réception, et la figure 8 montre la distribution cumulée correspondante.

Considérons tout d'abord le cas où les hôtes ne peuvent utiliser que des transmissions à 1 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 hôtes intéressés en moins de 30 minutes. Au bout d'une heure, environ 75 % des documents ont atteint les récepteurs intéressés, et après environ 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 7 montre que, lorsque du relais à deux sauts est utilisé (c'est-à-dire lorsque un hôte peut atteindre, via des transmissions multi-sauts, ses voisins à 2 sauts), la plupart des documents parviennent aux hôtes intéressés en moins de 20 minutes (contre 30 minutes lorsque seules sont utilisées des communications à 1 saut). Dans ces conditions, environ 98 % des documents parviennent en fait aux hôtes intéressés en moins de 2 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 encore la sphère de communication de chaque hôte en l'autorisant à interagir avec ses voisins à 3 sauts, à 4 sauts, et à 5 sauts respectivement.

En fait, avec les paramètres de simulation utilisés dans cette campagne d'évaluation, les îlots — ou fragments connexes du réseau — pouvant se former au sein des bâtiments ont une élongation qui varie entre 0 (lorsqu'un hôte 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 hôte 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 à laquelle les documents se propagent entre les bâtiments (ou entre des zones non connectées d'un même bâtiment) dépend directement de la vitesse à laquelle les transporteurs mobiles de ces documents — c'est-à-dire, ici, des piétons — se déplacent dans la zone de simulation.

Cette première expérience confirme qu'en étendant la sphère de communication de chaque hôte mobile, notre protocole permet bien une dissémination plus rapide des documents dans chaque îlot, ce qui contribue aussi à faire croître plus rapidement le nombre d'hôtes porteurs d'un même document, et permet au final une dissémination plus rapide des documents sur l'ensemble des fragments non connectés du réseau.

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

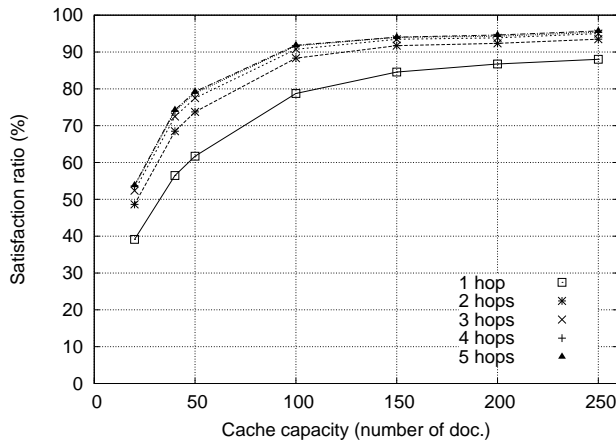


Figure 9: Variation du taux de délivrance des documents en fonction de la capacité du cache sur chaque hôte mobile

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 hôte 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 hôte mobile afin d'éviter la saturation de cache et, si cette saturation survient malgré tout, de résoudre ce problème.

Les courbes de la figure 9 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 hôte la capacité du cache entre 50 et 200 documents. Pendant ces simulations la politique de gestion de cache appliquée était telle que, lorsqu'un cache atteignait le niveau de saturation, le document le plus ancien contenu dans ce cache était supprimé afin de libérer de la place pour un nouveau document.

La figure 9 montre l'évolution du taux de délivrance (défini comme le pourcentage de documents atteignant effectivement les récepteurs intéressés), variant en fonction de la capacité du cache sur chaque hôte. On peut tout d'abord constater que les courbes présentées confirment l'intuition naturelle selon laquelle un hôte mobile doté d'un cache de grande capacité est en mesure de transporter les documents plus longtemps — 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. Dans la figure on voit notamment que le taux de délivrance augmente de manière significative lorsque la portée du relais immédiat est étendue à quelques sauts autour de chaque hôte. Considérons par exemple le cas où chaque hôte 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 hôte ne peut interagir qu'avec ses voisins directs. En revanche ce taux est accru de 10 % lorsque chaque hôte peut interagir avec ses voisins à 2 sauts, et il est encore accru de 2 % supplémentaires lorsque chaque hôte peut atteindre ses voisins à 3 sauts.

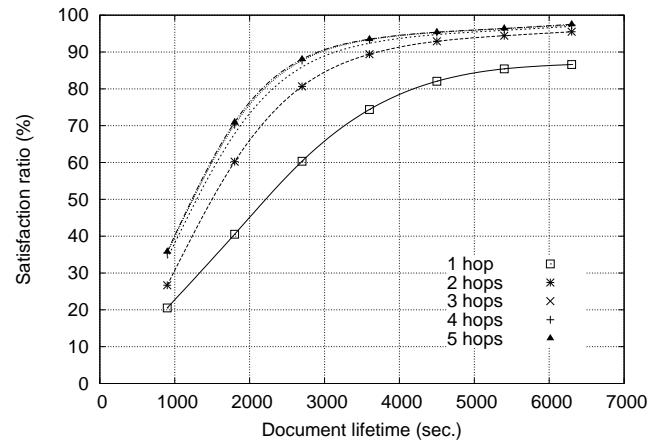


Figure 10: Variation du taux de délivrance des documents en fonction de la durée de vie accordée à chaque document

Influence de la durée de vie des documents. Une autre manière d'éviter que les documents demeurent éternellement dans le réseau consiste à donner à chaque document une durée de vie précise, lors de son injection dans le réseau. Ainsi, dès qu'un document devient obsolète, toutes les copies de ce document 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 hôtes mobiles.

Les courbes de la figure 10 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. La figure 10 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 hôte peut atteindre ses voisins à 2 sauts, et il l'est encore de 7 % lorsque chaque hôte 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 hôte, 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 hôte donné résulte en général directement de la quantité de ressources de stockage disponibles sur cet hôte. Il s'agit donc pour l'essentiel d'une contrainte liée à la gestion même de cet hôte, en fonction des ressources dont il dispose. En revanche, la durée de vie octroyée à un document doit être fixée 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 hôtes 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 hôtes récepteurs. Dans le premier cas, la décision est d'ordre stratégique et nécessite une certaine connaissance de l'état du réseau (i.e. envergure, schémas de mobilité des hôtes, 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.

Évaluation du coût du relais immédiat multi-sauts.

Les résultats précédents confirment 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 hôte mobile (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 hôte relaie un message, cette opération draine la batterie de cet hôte, mais aussi celles des récepteurs voisins, tout en monopolisant le médium radio dans le voisinage de l'émetteur.

En concevant notre protocole nous avons choisi de nous appuyer sur le principe des relais multi-points (principe emprunté au protocole OLSR) afin d'assurer la diffusion des messages. De toute évidence, il aurait été plus simple pour nous de mettre en œuvre un simple algorithme d'inondation pour diffuser ces messages. Puisque les résultats présentés plus haut montrent qu'une amélioration significative des performances de la dissémination des documents peut être obtenue — dans le scénario considéré — en relayant les messages sur un très faible nombre de sauts (typiquement deux ou trois sauts), on peut légitimement se demander si l'utilisation de relais multi-points dans un tel contexte apporte un quelconque bénéfice par rapport à un simple mécanisme d'inondation.

Pour comparer les coûts de fonctionnement respectifs de deux approches reposant, l'une sur des relais multi-points, l'autre sur un mécanisme d'inondation, nous avons mis en œuvre une version dégradée de notre protocole, dans laquelle la couche inférieure du protocole assure la diffusion de messages par inondation plutôt que via des relais multi-points. Nous avons ensuite comparé le comportement de ces deux versions du protocole, en appliquant bien sûr dans les deux cas le même scénario de mobilité et de communication. Les résultats sont présentés dans les figures 11 et 12. Ils ont été produits en réalisant des simulations de 4 heures (en temps simulé), avec des caches de capacité illimitée, et des documents ayant chacun une durée de vie d'un heure.

On peut tout d'abord constater (fig. 11) que les deux versions du protocole ne donnent pas tout à fait les mêmes taux de délivrance. Ceci est dû au fait qu'avec la version standard de notre protocole (utilisant les MPRs) la dissémination des documents s'effectue légèrement plus lentement qu'avec la version reposant sur le mécanisme d'inondation. En effet, un hôte dont le voisinage est modifié doit attendre quelques temps (précisément, deux cycles d'annonce consé-

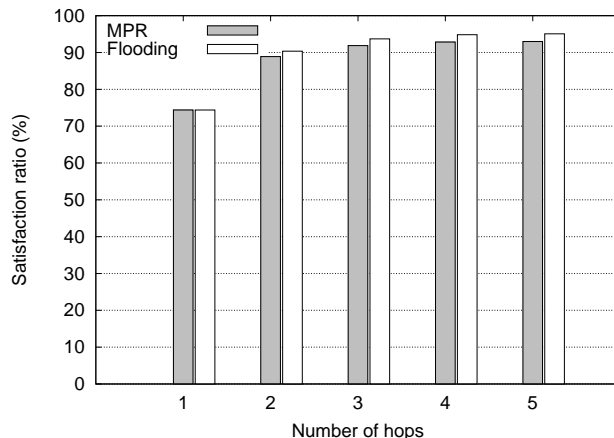


Figure 11: Comparaison entre les performances (en termes de documents remis aux récepteurs intéressés) du mode de diffusion par inondation et via des relais multi-points

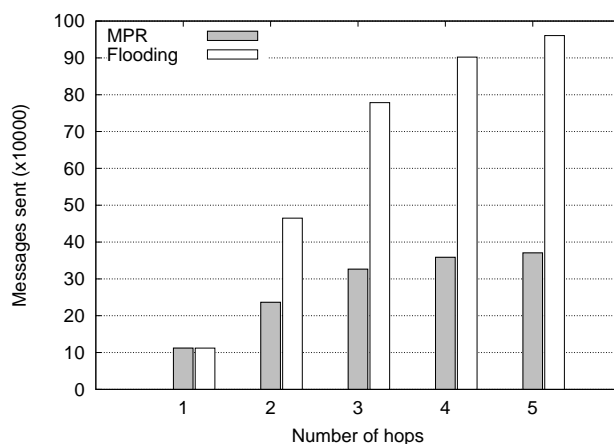


Figure 12: Comparaison entre le coût (en termes de nombres de messages émis) du mode de diffusion par inondation et via des relais multi-points

cutifs) 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 hôte dont le voisinage à 2 sauts change peut immédiatement proposer un catalogue de documents susceptibles d'intéresser ses nouveaux voisins.

Le taux de délivrance est donc très légèrement inférieur avec la version standard de notre protocole qu'avec la version pratiquant l'inondation. Cette différence demeure cependant inférieure à 3 %, alors que le coût relatif lié à l'utilisation de l'une ou l'autre méthode de diffusion est fort différent. On peut en effet observer dans la figure 12 que le nombre de transmissions élémentaires (correspondant au nombre de fois où un message est émis ou réémis sur le médium radio) est très nettement supérieur avec le mécanisme d'inondation qu'avec le mécanisme reposant sur les MPRs. Ce constat conforte notre décision de nous appuyer sur des relais multi-points pour assurer la diffusion de messages tout autour d'un hôte émetteur. Enfin on peut noter que le coût de la diffusion via des MPRs ne croît pas énormément lorsque la sphère de communication de chaque hôte 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.

5. INTÉGRATION À LA PLATE-FORME INTERGICIELLE DODWAN

Le protocole décrit dans les paragraphes précédents a été pleinement implémenté en Java, et embarqué dans la plate-forme intergicelle DoDWAN (*Document Dissemination in Wireless Ad hoc Networks*). DoDWAN est une plate-forme que nous avons conçue afin d'aider à la mise en œuvre de services applicatifs capables de fonctionner dans un réseau MANET discontinu. Elle offre une API de type *publish/subscribe*, qui permet de développer aisément des services applicatifs exploitant le modèle de communication opportuniste tolérant les délais.

DoDWAN peut en fait être perçue comme un MOM (*Message-Oriented Middleware*). Elle se distingue toutefois de produits tels que JMS (*Java Message Service*) ou Emma [15] par le fait que les objets qu'elle manipule sont en fait des documents à part entière, et non de simples messages. Le traitement accordé à ces documents par DoDWAN peut donc dépendre de leurs caractéristiques propres — en application du principe de la communication basée contenus — et non simplement de leur destination assignée.

Les communications s'effectuent à travers une pile IP standard, les messages étant embarqués dans des datagrammes UDP. Jusqu'à ce jour les expérimentations ont pour l'essentiel été menées avec des interfaces de type Wi-Fi, mais des essais réalisés avec des interfaces Bluetooth se sont également avérés concluants. DoDWAN supporte la fragmentation et le réassemblage des documents lourds, qui ne peuvent être transmis en une seule fois sur le médium de transmission. Lorsqu'un document de ce type doit être diffusé, il est découpé en segments distincts, qui sont ensuite encapsulés dans des « documents fragments », dont les descripteurs reprennent les mêmes attributs qui caractérisaient le document initial. Ces fragments peuvent alors être diffusés, et se propager dans le réseau indépendamment les uns des autres.

Ils seront à terme collectés par les hôtes intéressés, au niveau desquels le réassemblage des divers fragments permettra de reconstituer le document initial. On peut noter qu'avec cette approche un hôte peut faire office de transporteur pour certains fragments d'un document, même s'il ne dispose pas de l'ensemble des fragments qui permettraient de reconstituer ce document dans son intégralité. Cette caractéristique contribue à assurer la robustesse du système, dans la mesure où il n'est pas nécessaire qu'un hôte dispose d'un document complet pour pouvoir contribuer à la dissémination de ce document dans le réseau.

6. CONCLUSION

Dans cet article nous avons présenté un protocole capable de supporter la communication basée contenus dans des réseaux mobiles ad hoc discontinus. Contrairement à d'autres protocoles qui mettent en œuvre des méthodes complexes afin de construire des structures de routage basé contenu, 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. 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 — ou îlot — 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.

Les résultats de simulation confirment l'efficacité de ce protocole pour assurer l'acheminement des documents à travers un réseau fortement fragmenté. Ces résultats montrent également que l'utilisation de mécanismes de relais multi-sauts contribue à accroître la vitesse de dissémination des documents au sein des fragments connexes (îlots) du réseau, ce qui se traduit également par une efficacité accrue du transport de documents entre ces divers fragments. En ajustant la portée du relais multi-sauts réalisé autour de chaque terminal mobile, le surcoût résultant de ce relais peut être maintenu à un niveau raisonnable. Dans la version actuelle du protocole le nombre de sauts autorisé dans le cadre du relais multi-sauts est fixé comme un paramètre constant. Dans les travaux à venir nous prévoyons d'étudier des méthodes permettant à chaque terminal mobile d'ajuster dynamiquement ce paramètre, en tenant compte de critères relatifs à son environnement immédiat (e.g. nombre de terminaux voisins, profils d'intérêt de ces voisins, historique des échanges récents avec le voisinage, taux d'occupation du médium radio, etc.).

Crédits

Ce travail s'inscrit dans le cadre du projet SARAH (Services Asynchrones pour Réseaux mobiles Ad Hoc), financé par l'Agence Nationale de la Recherche dans le cadre du programme ARA SSIA (Actions de Recherche Amont en Sécurité, Systèmes embarqués et Intelligence Ambiante) sous le contrat ANR-05-SSIA-0002-01.

7. REFERENCES

- [1] Information Technology, Telecommunications and Information Exchange between Systems, Local and Metropolitan Area Networks, Specific Requirements

- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ANSI/IEEE Std 802.11, 1999.
- [2] R. Baldoni, R. Beraldi, M. Migliavacca, L. Querzoni, G. Cugola, and L. Migliavacca. Content-Based Routing in Highly Dynamic Mobile Ad Hoc Networks. *Journal of Pervasive Computing and Communication*, 1(4):277–288, dec 2005.
- [3] C. Basile, M.-O. Killijian, and D. Powell. A Survey of Dependability Issues in Mobile Wireless Networks. Technical report 02637, LAAS CNRS Toulouse, France, oct 2002.
- [4] A. Carzaniga and A. L. Wolf. Content-based Networking: A New Communication Infrastructure. In *NSF Workshop on an Infrastructure for Mobile and Wireless Systems*, number 2538 in LNCS, pages 59–68, Scottsdale, Arizona, Oct. 2001. Springer-Verlag.
- [5] I. Chakeres and C. Perkins. Dynamic MANET On-demand (DYMO) Routing. Technical Report draft-ietf-manet-dymo-11, IETF, Nov. 2007.
- [6] J. K. Changling Liu. A Survey of Mobile Ad Hoc network Routing Protocols. Technical report, University of Magdeburg, 2005.
- [7] T. Clausen and P. Jacquet. Optimized Link-State Routing Protocol (OLSR). Technical Report RFC 3626, Project Hipercom, INRIA, Oct. 2003.
- [8] P. Costa, M. Musolesi, C. Mascolo, and G. P. Picco. Adaptive Content-based Routing for Delay-tolerant Mobile Ad Hoc Networks. Technical report, UCL, aug 2006.
- [9] P. Costa and G. P. Picco. Semi-Probabilistic Content-Based Publish-Subscribe. In *25th International Conference on Distributed Computing Systems (ICDCS 2005)*, pages 575–585, Columbus, Ohio, USA, jun 2005. IEEE Computer Society.
- [10] A. Datta, S. Quarteroni, and K. Aberer. Autonomous Gossiping: a Self-Organizing Epidemic Algorithm for Selective Information Dissemination in Mobile Ad-Hoc Networks. In *IC-SNW'04 (International Conference on Semantics of a Networked World)*, number 3226 in LNCS, pages 126–143, Paris, jun 2004.
- [11] K. Fall. Messaging in Difficult Environments. Technical report, Intel Research Berkeley, 2004.
- [12] K. A. Harras, K. C. Almeroth, and E. M. Belding-Royer. Delay Tolerant Mobile Networks (DTMNs): Controlled Flooding in Sparse Mobile Networks. In *IFIP Networking Conference, Waterloo, Ontario, CANADA*, May 2005.
- [13] L. Hogue, P. Bouvry, and F. Guinand. The MADHOC simulator. <http://www-lih.univ-lehavre.fr/hogie/madhoc>.
- [14] R. Meier and V. Cahill. STEAM: Event-Based Middleware for Wireless Ad Hoc Network. In *International Conference on Distributed Computing Systems, Workshops (ICDCSW '02)*, pages 639–644, jul 2002.
- [15] M. Musolesi, C. Mascolo, and S. Hailes. EMMA: Epidemic Messaging Middleware for Ad hoc networks. *Personal and Ubiquitous Computing Journal*, 2005. To Appear.
- [16] S. Y. Ni, Y. C. Tseng, Y. S. Chen, and 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*, pages 151–162. ACM/IEEE, 1999.
- [17] L. Pelusi, A. Passarella, and M. Conti. Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks. *IEEE Communications Magazine*, nov 2006.
- [18] M. Petrovic, V. Muthusamy, and H.-A. Jacobsen. Content-Based Routing in Mobile Ad Hoc Networks. In *Proc. of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05)*, San Diego, California, USA, July 2005. IEEE Press.
- [19] A. Qayyum, L. Viennot, and A. Laouiti. Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks. In *35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, page 298. IEEE CS, 2002.
- [20] E. M. Royer and C.-K. Toh. A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. *IEEE Personal Communications*, pages 46–55, Apr. 1999.
- [21] A. Vahdat and D. Becker. Epidemic Routing for Partially Connected Ad Hoc Networks. Technical report, Duke University, Apr. 2000.
- [22] E. Vollset, K. Birman, and R. van Renesse. Chickweed: Group Communication for Embedded Devices in Opportunistic Networking Environments. In *3rd International Workshop on Dependable Embedded Systems, in conjunction with 25th Symposium on Reliable Distributed Systems (WDES 2006)*, Leeds, UK, October 2006.
- [23] Z. Zhang. Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges. *IEEE Communications Surveys and Tutorials*, 8(1):24–37, jan 2006.