Le Multicast Sans Fil dans un Environnement IP

Neda Nikaein, Christian Bonnet

Institut Eurécom,
2229 Route des Crêtes, BP 193,
06904 Sophia Antipolis Cedex, France
E-mail: {nikaein, bonnet}@eurecom.fr
Fax: (+33) 4 93 00 26 27

Résumé

Dans cet article, nous discutons le mécanisme d'IP multicast dans le contexte des réseaux d'accès sans fil. Par ailleurs, les problèmes rencontrés dans ce type de réseau tel qu'une bande passante limitée et des contraintes de consommation de puissance pour les terminaux mobiles exigent d'apporter des modifications aux protocoles existants dans les réseaux filaires. Par conséquent, nous analysons les problèmes rencontrés lors de l'application du protocole IGMP (Internet Group Management Protocol) aux réseaux locaux sans fil. Nous proposons un protocole spécifique de gestion de groupe pour les réseaux sans fil nommé WGMP (Wireless Group Management Protocol). Nous effectuons une évaluation de performance de notre protocole en nous basant sur le critère d'*overhead.* Les résultats obtenus sont comparés a ceux relatifs aux protocoles déjà existants.

1. Introduction

La communication multicast consiste à envoyer un paquet à plusieurs destinations par le biais d'une seule transmission. Elle intervient dans le cas où plus de deux utilisateurs veulent échanger des informations [4]. L'avantage d'une communication multicast réside dans son utilisation efficace de la bande passante et des ressources du réseau. La source diffuse ainsi des données à tous les récepteurs. Des applications multicast sont de plus en plus utilisées. Nous notons principalement l'existence des applications audio/vidéo conférence et des jeux distribués. Il est donc important que les réseaux sans fil puissent fournir des services multicast similaires aux utilisateurs.

L'Internet est en train d'évoluer d'un modèle de service *best-effort* classique à un modèle de service intégré, capable d'offrir plusieurs applications multimédia et temps réel. La gestion de mobilité dans IPv6 [1], [5], [7], et IP mobile [6] ont fait du protocole IP un protocole adapté

aux environnements mobiles. Par conséquent, IP est une des technologies clés pour les réseaux mobiles.

IP supporte des applications multicast par l'intermédiaire d'une série de mécanismes constituant IP multicast. IP multicast comprend deux mécanismes: un mécanisme de gestion de groupe dans un réseau local et un mécanisme de routage des paquets vers les récepteurs localisés dans les autres réseaux. La nature différente du support de transmission (interface radio) entraîne l'émergence de nouveaux besoins pour les applications multicast. En effet, les caractéristiques principales d'un réseau sans fil sont la limitation de la bande passante, les pertes des paquets dues aux erreurs bit du canal radio et les contraintes de consommation d'énergie au niveau des terminaux mobiles. Les caractéristiques relatives au monde sans fil n'ont pas été prises en comptes dans la conception du protocole de gestion du groupe d'IP multicast. Dans ce contexte, nous proposons dans cet article un mécanisme de gestion de groupe pour un réseau local sans fil.

Notre article comprend cinq principales sections. La section 2 présente l'architecture de base d'un réseau d'accès sans fil basé sur IP. La section 3 décrit de manière détaillée le mécanisme d'IP multicast. La section 4 introduit notre protocole de gestion de groupe pour les réseaux sans fil. Le problème de mobilité dans les communications multicast est étudié en section 5. La section 6 est dédiée à la comparaison de performance de notre protocole avec les protocoles de gestion de groupe d'IP multicast en se basant sur le critère d'*overhead*.

2. Architecture Générale du Système

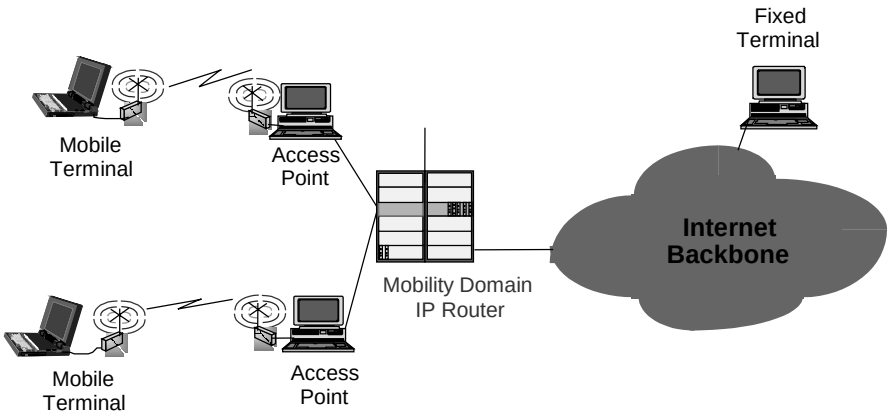


Figure 1: L'architecture générale du système

La figure 1 montre le modèle architectural pour un réseau d'accès IP sans fil. Le modèle est composé de trois éléments : Terminal Mobile (MT: Mobile Terminal), Point d'accès (AP: Access Point) et le routeur IP qui possède les fonctionnalités nécessaires pour la gestion de la mobilité (M-routeur : Mobility Domain IP router).

Le MT est une machine IP standard avec un adaptateur radio pour accéder au réseau sans fil. L'AP comprend toutes les fonctionnalités du contrôle liées à l'interface radio. Il est le point de connexion entre le monde sans fil et le monde filaire. Le M-routeur gère un ou plusieurs APs. Tous les APs qui sont connectés au même M-routeur appartiennent au même domaine IP. La mobilité au sein d'un sous-réseau IP est gérée par la couche liaison dans les APs et elle est complètement transparente à la couche réseau. La mobilité entre différents sous-réseaux IP est gérée par les modules de gestion de mobilité d'IPv6. En IP, un mobile possède deux adresses: une adresse IP temporaire nommé *care-of-address* et une adresse permanente appellé *home address*. Le *care-of-address* change à chaque fois que le mobile change de réseau. Le *home address* par contre ne change pas; c'est l'adresse obtenue par le MT lors de son enregistrement dans son réseau d'origine (*home network*). Chaque réseau doit avoir un routeur appellé *home agent* (HA) qui garde la position courante de chaque MT qui s'est enregistré dans son domaine. Le HA est capable de renvoyer des données vers les mobiles qui sont dans un réseau autre que le sien. Dans notre architecture, nous considérons que le M-routeur englobe aussi les fonctionnalités du HA alors que généralement ce dernier peut aussi être une entité séparée.

3. IP Multicast

IP identifie un groupe par une adresse IP abstraite de type D. Une source peut envoyer des données à une adresse du groupe sans connaître les membres du groupes. IP multicast utilise le protocole IGMP (Internet Group Management Protocol) [2] pour localiser des membres d'un groupe dans un réseau local. Le protocole IGMP est exécuté par un routeur qui prend en charge la gestion du groupe dans son réseau local. Ce routeur est appellé routeur multicast. Ce dernier a besoin d'avoir une connaissance permanente des groupes existants dans son réseau local. Un paquet multicast est envoyé dans un réseau local si le groupe auquel le paquet est destiné a au moins un membre dans ce réseau local. IP suppose que la couche de liaison distribue le paquet aux membres du groupe multicast. La communication multicast dans le contexte d'une interconnexion de réseaux est assurée grâce aux protocoles de routage multicast. Ces protocoles ont besoin de la liste de présence des groupes de chaque réseau afin de construire un arbre multicast pour la transmissions de trafic multicast. IGMP fournit cette liste aux protocoles de routage multicast.

IGMP est basé sur un modèle *soft state* où les informations doivent être actualisées d'une façon périodique. Le routeur multicast envoie périodiquement un message *query* à l'adresse de diffusion de son réseau local. A la réception d'un message *query*, chaque machine envoie

un message *report* pour chaque groupe auquel elle participe. Un message *report* pour un groupe est envoyé à l'adresse du groupe afin que chaque membre de groupe puisse l'entendre. A la réception du premier message *report* par un groupe, les autres membres du groupe suppriment leur message de *report* décrivant leur état d'adhésion pour ce groupe. Le routeur multicast met à jour sa liste d'adhésion de groupe après réception de chaque message *report*. Si aucun message *report* n'est reçu après plusieurs messages *query*, le routeur suppose qu'il n'y a aucun membre dans ce groupe dans le réseau local. Il procède ensuite à la suppression de ce groupe de sa liste.

Le mécanisme IGMP est bien adapté aux réseaux locaux classiques où on trouve un mécanisme natif de diffusion qui est disponible au niveau de couche liaison. Un réseau local sans fil diffère d'un réseau local filaire en plusieurs aspects. Un réseau sans fil est physiquement divisé en un ensemble de cellules contrôlées par différents APs. Un MT local à un AP ne peut pas recevoir les données d'un autre AP, même si les deux APs sont situés au niveau d'un même sous-réseau IP. Par conséquent, les MTs situés dans la même cellule peuvent seulement entendre les données provenant de leurs APs. Donc, le M-routeur doit envoyer un message *query* pour chaque AP afin que tous les MTs puissent entendre le message. D'autre part, le message *report* envoyé par un MT ne peut pas être entendu par les MTs des autres APs immédiatement et le M-routeur doit donc retransmettre le message à tous les APs.

Dans le protocole IGMP, pour joindre un groupe, une machine envoie un message *report* non sollicité pour ce groupe. Quitter un groupe n'exige aucune action explicite. Ceci introduit un temps d'attente entre le moment où une machine, qui correspond au dernier membre d'un groupe, part vraiment du groupe et du moment où le routeur multicast détecte la situation et arrête d'envoyer le trafic multicast pour ce groupe. IGMPv.2 [4] propose une solution pour diminuer ce temps d'attente en introduisant un nouveau message *leave*. Une machine, voulant quitter un groupe, envoie un message *leave* si elle est le dernier membre du groupe. Toutefois, même dans ce cas le routeur doit envoyer un message spécifique, *group specific query*, pour ce groupe afin de s'assurer qu'il n'y a aucun autre membre de ce groupe dans son réseau local. Puisque les messages *query* et *group specific query* d'IGMP ne sont pas envoyés d'une façon fiable, le routeur multicast doit les répéter plusieurs fois avant de valider l'absence de groupe dans son réseau local. Le nombre de fois qu'un message *group specific query* ou *query* doit être envoyé par le routeur multicast pour détecter l'absence du groupe est appellé facteur de fiabilité noté R_f (*robustness factor*).

Le facteur de fiabilité R_f peut être initialisé par l'administrateur du système selon son estimation de la perte de paquet dans le réseau local. Le choix d'une valeur optimale pour R_f est néanmoins très difficile à cause de la nature variable du taux d'erreur des liens sans fil. Divers paquets sont ainsi sujets à plusieurs taux d'erreur dûs aux phénomènes physiques comme les évanouissements. Les couches liaison comportent ainsi des mécanismes de

contrôle d'erreur pour pallier les variations élevées du taux d'erreur de l'interface radio. Par conséquent, le paquet IGMP peut être plusieurs fois retransmis dans la couche liaison avant d'être accepté. Ceci peut conduire le routeur multicast à conclure la non existence de membre dans un groupe dans son sous-réseau local, alors que la couche liaison tente de retransmettre le paquet à travers le lien radio.

Afin de diminuer le temps d'attente dans IGMP, [8] a proposé un mécanisme, basé sur des techniques de prédiction. Le routeur multicast garde un historique des derniers résultats des messages *query*. A la réception d'un message *leave*, le routeur essaie de prévoir les résultats basés sur l'historique enregistré. Il envoie également un message *report* afin de s'assurer de l'exactitude de sa prévision. Etant dans un environnement sans fil, le taux d'erreur est assez élevé. Par conséquent, la probabilité d'avoir un historique corrompu est plus élevée que sur les liens fixes, particulièrement dans le cas de l'évanouissements ou normalement cela prend un certain temps avant que le canal revienne à son état normal. Cette solution essaie de résoudre les problèmes de congestion de réseau mais elle ne supprime pas la transmission périodique des messages *query* causant la perte de bande passante et une consommation élevée de puissance dans les MTs.

[9] a proposé un mécanisme explicite pour le contrôle de l'adhésion de groupe pour les liens point-à-point. Un MT envoie un message *join* quand il veut recevoir des données d'un groupe. Il envoie un message *leave* en quittant un groupe. Les messages existants de IGMPv2 *report* et *leave* peuvent être utilisés en tant que les messages *join* et *leave*. La fiabilité du protocole est assurée par le routeur qui envoie un accusé de réception en recevant un message *join* ou un message *leave*. Si le MT n'a pas reçu un accusé de réception du routeur après un certain temps, il répète sa demande. Cette approche élimine le temps d'attente. Elle est bien adaptée à un réseau sans fil en raison de son utlisation efficace de la bande passante et sa consommation optimale de puissance dans le MTs.

4. Protocole de Gestion de Groupe Sans Fil : WGMP

Le principe de base d'une communication multicast dans un réseau sans fil est d'utiliser le mécanisme de diffusion de trafic multicast à travers le support radio. L'objectif principal à atteindre est de diminuer la perte de bande passsante. Pour ce faire, nous proposons un protocole spécifique d'adhésion de groupe, que nous appellons le protocole de gestion de groupe sans fil (WGMP: *Wireless Group Management Protocol*), basé sur le mécanisme d'échange de messages *join*/*leave* décrit en [9]. Un MT envoie un message *join* ou un message *leave* afin de se rejoindre ou de quitter un groupe. Ces messages sont confirmés par un message d'accusé de réception.

Comme il a été mentionné, IGMP exige du routeur multicast de mettre à jour une liste des groupes présents dans son réseau local. Cette liste de présence de groupe n'est pas suffisante pour une transmission efficace du trafic multicast dans un réseau sans fil. Afin d'éviter la perte de bande passante, des paquets multicast doivent être expédiés seulement aux APs avec les membres actifs du groupe indiqué. Ceci exige du routeur multicast de maintenir plus d'information que la liste de groupes actuels dans son réseau local. Un MT peut être n'importe où dans son réseau local. Il peut également se déplacer vers un autre réseau local. IP Mobile propose l'utilisation d'un agent source (HA) qui est un routeur mettant à jour la localisation courante de chaque MT enregistré dans son domaine. Quand le MT est dans un réseau distant, il doit être capable de recevoir des données multicast par l'intermédiaire de son HA. L'agent HA doit connaître donc la liste de groupes auxquels le MT a souscrit.

Dans notre système, le M-routeur maintient une information de groupe (GI). Chaque groupe, qui a un membre dans le réseau local, doit avoir une entrée dans le GI. Cette entrée contient l'ensemble des adresses des MTs appartenant à ce groupe. A chaque réception de trafic destiné à un groupe, le M-routeur consulte l'entrée correspondante à ce groupe dans le GI. Il expédie alors le trafic seulement aux APs où se situent les MTs du groupe. Le M-routeur ne diffuse pas de le trafic à un groupe si son entrée est vide dans le GI. Dans ce cas, le M-routeur doit également quitter l'arbre multicast correspondant. Le GI peut être mis à jour en raison de la mobilité ou en raison des changements d'adhésion des MTs. Les changements dus à la mobilité seront discutés dans la prochaine section.

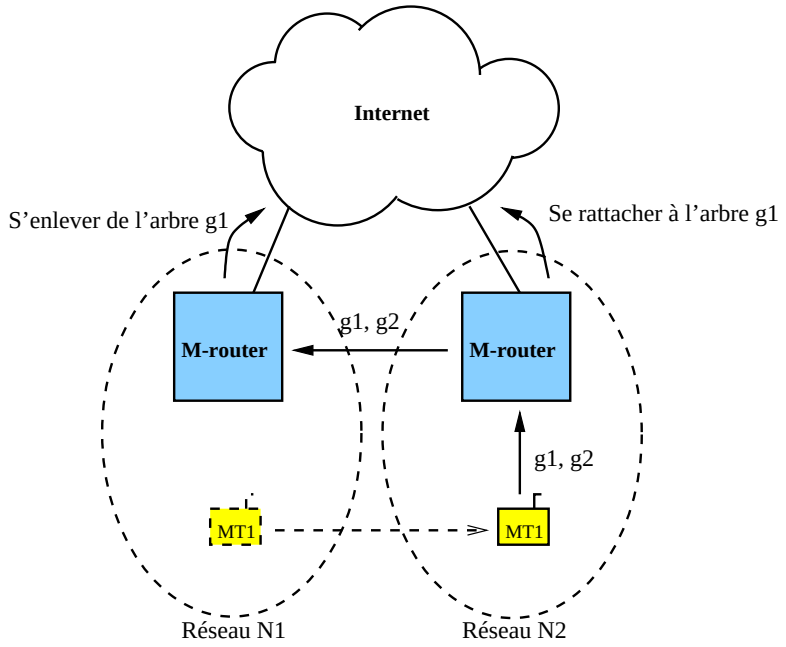
Généralement, dans les réseaux sans fil, la couche liaison détecte si un terminal mobile n'est plus actif dans une cellule donnée dû à un handover ou à une réinitialisation. Nous supposons que le WGMP est informé par les couches inférieures si un MT est éteint ou s'il est dans un autre domaine de réseau. A la réception d'un avis par les couches inférieures, WGMP effectue les modifications nécessaires dans le GI.

Afin de pouvoir transmettre le trafic multicast aux réseaux distants, le WGMP doit fournir la liste de groupes présents dans son réseau local aux protocoles de routage de multicast. Cette liste peut être facilement produite du GI. Un groupe est présent dans le réseau local s'il a une entrée dans le GI.

5. Mobilité et Multicast

Nous considérons d'abord le cas où un MT se déplace vers un autre AP qui est sous le même domaine IP que son ancien AP. Dans ce cas, la couche IP n'est pas au courant de la mobilité puisque le MT ne change pas d'adresse IP. Dans ce cas, aucune modification n'est nécessaire dans le GI.

La situation devient complexe si le MT se déplace vers un autre AP en dehors de son domaine de réseau actuel. Nous considérons que le protocole de gestion de groupe du réseau distant est également WGMP pour éviter des problèmes d'incompatibilité. Le handover inter-domaine est réalisé grâce aux fonctions de mobilité d'IPv6.



MT1 est le dernier membre du groupe g1 dans le réseau N1
et le premier membre du groupe g1 dans le réseau N2.

Figure 2 : Handover inter-domaine.

Reste posée une question importante concernant le mécanisme utilisé pour que le MT puisse envoyer ou recevoir le trafic multicast dans un réseau distant. En entrant dans un réseau distant, le MT a deux possibilités pour recevoir le trafic multicast. Il peut le recevoir par l'intermédiaire de son HA. Par conséquent, tous les messages *join* et *leave* venant du MT sont traités au HA. Dans ce cas, aucune modification n'est nécessaire dans le GI. Cette approche mène à un routage non optimal où tous les paquets multicast doivent d'abord être envoyés au HA et puis au réseau distant. L'autre inconvénient est que le HA va envoyer le trafic multicast d'une façon point-à-point à tous les MTs qui sont dans les autres réseaux. Ainsi, tous les avantages de communication multicast en ce qui concerne l'utilisation des ressources réseaux

sont ignorés. Cette approche n'est particulièrement pas souhaitable pour les applications temps réel à cause du retard supplémentaire engendré par le routage.

L'autre solution est que le MT envoie un autre message *join* pour ses groupes multicast dans le réseau distant. Le réseau distant exécute le protocole de gestion de groupe et fournit le trafic multicast au MT directement. Dans ce cas, le MT doit être supprimé de toutes les entrées correspondantes de GI de son réseau local. Il doit être ajouté au GI du réseau distant. Cette approche est meilleure que la précédente en raison de son routage optimal et son utilisation efficace de bande passante. Cependant, le MT risque de perdre des paquets pendant le handover. C'est dû au fait que quand un MT, qui appartient à un groupe, entre dans un réseau distant dans lequel il n'y a aucun membre de ce groupe, il ne peut pas recevoir le trafic du groupe immédiatement. Le routeur multicast local doit se joindre à l'arbre multicast de ce groupe pour pouvoir recevoir du trafic. Cette situation est montrée sur la figure 2. Les pertes de paquet peuvent être évitées par le routeur précédent jouant le rôle de HA en envoyant le trafic multicast à MT au moment de *hand-over*.

De la même manière, le MT peut envoyer un datagramme à un groupe multicast de deux façon dans un réseau distant. Il peut l'envoyer soit par l'intermédiaire de son HA en utilisant son *home address* ou directement sur le réseau distant en utilisant son *care-of-address*. La première approche mène à un routage non optimal et à un retard supplémentaire étant donné que des datagrammes doivent être expédiés d'abord au HA. La deuxième approche est optimale grâce à l'optimisation du routage et du délai de transmission. Le MT doit utiliser son *care-of-address* comme son adresse IP de source en envoyant des datagrammes directement de son réseau distant. Cependant, le MT change son *care-of-address* selon son emplacement dans le réseau Internet. Par conséquent, un mécanisme est nécessaire pour que les destinataires sachent que bien que deux datagrammes multicast contiennent différentes adresses de source, ils proviennent du même mobile qui s'est déplacé à travers différents réseaux. IPv6 a présenté un nouveau champ d'en-tête appelé l'en-tête d'options de destination. Ce champ d'en-tête contient les options qui ne seront traitées qu'au niveau de la destination.

Nous proposons que le MT utilise son *home address* dans le champ d'options de destination d'un datagramme IPv6 quand il veut envoyer le trafic multicast dans un réseau distant. Les récepteurs peuvent alors identifier le mobile par son *home address*.

6. Evaluation de Performance

Dans cette section, nous comparons le protocole WGMP avec les protocoles IGMPv1 et IGMPv2 en termes d'*overhead*. [9] a déjà comparé l'*overhead* de IGMPv1 et IGMPv2 à l'approche utilisant les messages *join*/*leave* pour des liens point-à-point. Cependant, aucun paquet n'est supposé perdu. Les pertes de paquet sont assez fréquentes dans des liens sans fil.

Par conséquent, nous comparons l'*overhead* du protocole WGMP aux deux versions du protocole IGMP dans deux cas, une fois en présence des erreurs et une fois sans erreurs. Nous utilisons un mécanisme de diffusion pour la transmissions multicast dans une cellule. Les valeurs par défaut indiquées dans [5] sont utilisées pour les différents temporisateurs et variables de IGMPv1 et IGMPv2. Ces variables avec leurs valeurs par défaut sont regroupées dans le tableau 1.

T_q	Intervalle du temps entre deux messages *query* valeur par défaut 125 seconds
T_{qs}	Intervalle du temps entre deux messages *group specific query* valeur par défaut 1 seconds
R_f	Facteur de fiabilité valeur par défaut 2 seconds
T_r	Temps de réponse maximum pour un récepteur pour envoyer un message *report* valeur par défaut 10 seconds

Tableau1 : Définition des variables

Le temps T_q est l'intervalle du temps entre deux messages *query* envoyés par le routeur multicast. L'intervalle T_r est le temps de réponse maximum pour un récepteur pour envoyer un message *report* en réponse à un message *query*. En utilisant ces valeurs par défaut, IGMPv1 met $R_f\, T_q + T_r$ secondes pour noter l'absence de groupe dans le pire des cas. Ce dernier correspond à la situation où une machine quitte un groupe tout de suite après un message *quer*y. Le temps T_{qs} est l'intervalle du temps entre deux messages *group specific query*. C'est aussi le temps de réponse maximum pour un récepteur pour envoyer un message *report* en réponse à un message *group specific query*. Pour IGMPv2, le temps d'attente est $(R_f + 1)T_{qs}$ secondes. Dans les deux versions d'IGMP, quand une machine veut joindre un groupe, elle envoie deux messages de *report* non sollicités.

L'*overhead* de chaque approche comprend les messages de contrôle et les données envoyées par le routeur multicast sur son réseau local pendant le temps d'attente pour chaque groupe. Pour des raisons de simplicité, nous ne tenons pas compte de l'*overhead* engendré par les messages *query* et *report*. Par conséquent, l'*overhead* d'IGMPv1 est dû aux deux messages *report* non sollicités envoyés par chaque MT qui veut se rejoindre à un groupe plus les données envoyées par le routeur au réseau local pendant le temps d'attente d'un groupe (voir formule 6.1).

$$Overhead(IGMPv1) = 2L_p\, N + (R_f T_q + T_r)\, D_r \qquad (6.1)$$

où L_p est la taille de paquet, N est le nombre des participants du groupe et D_r est le débit du canal.

L'*overhead* d'IGMPv2 est dû aux deux messages de *report* non sollicités, à un message de *leave*, de R_f messages de *group specific query* et les données inutilisées envoyées pendant le temps d'attente. L'*overhead* d'IGMPv2 est calculé grâce à la formule (6.2).

$$Overhead(IGMPv2) = 2L_p N + (R_f + 1)L_p + (R_f + 1)T_{qs} D_r \qquad (6.2)$$

Dans WGMP, l'*overhead* est seulement dû aux messages de contrôle puisqu'il n'y a aucun temps d'attente dans le cas où il n'y a pas de perte de paquet. Les messages de contrôle de WGMP se composent d'un message *join*, d'un message *leave* et de deux accusés de réception (voir formule 6.3).

$$Overhead(WGMP) = 4L_p N \qquad (6.3)$$

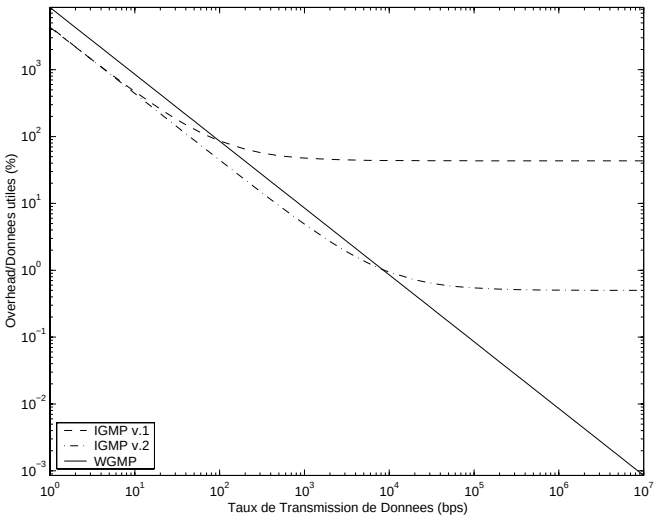


Figure 3: γ en fonction de taux de transmission pour différents protocoles de gestion de groupe sans perte de paquet.

Nous définissons le paramètre γ comme étant l'*overhead* de chaque protocole divisé par la volume de l'information utile. La figure 3 montre l'évolution de ce paramètre pour chaque approche en fonction de débit de transmission. Nous supposons qu'il n'y a pas de perte de paquet. Nous avons fixé la durée d'adhésion à 10 minutes et le nombre des participants à 50

MTs. Nous supposons que tous les messages de commande ont la même taille, 256 bits, dans tous les protocoles comme dans [9].

Comme le montre la figure 3, avec des débits bas, l'*overhead* est dû aux messages de contrôle pour les protocoles IGMPv1 et IGMPv2. Au fur au mesure que le débit augmente, l'*overhead* dû aux messages de contrôle devient négligeable et l'effet du temps d'attente devient dominant. Dans WGMP, l'*overhead* diminue d'une façon linéaire quand le débit augmente. C'est dû au fait que l'*overhead* de WGMP est indépendant de débit (4 messages de contrôle pour chaque participant). Nous constatons que l'*overhead* de WGMP devient inférieur a ceux des deux versions d'IGMP à partir de 10 Kbps, ce qui montre que WGMP est un bon choix pour les réseaux d'accès sans fils où le débit est souvent assez élevé.

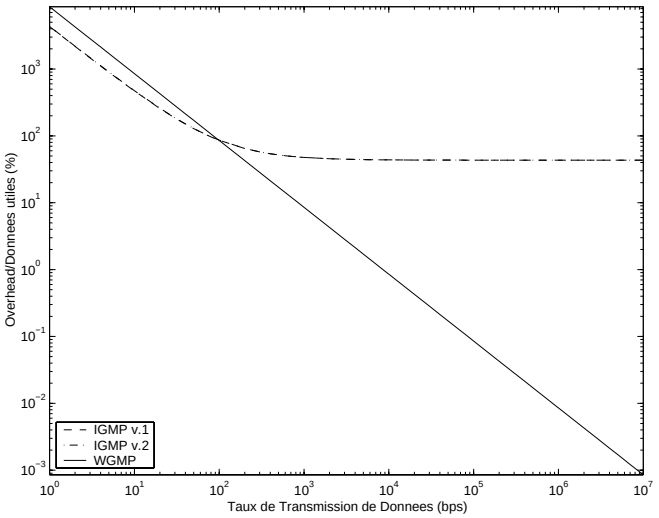


Figure 4: γ en fonction de taux de transmission pour différents protocoles de gestion de groupe avec perte de paquet .

La figure 4 montre la même courbe mais avec la présence des pertes de paquet. L'*overhead* de WGMP augmente quand un message *leave* qui correspond au dernier participant d'un groupe se perd. Nous considérons ce pire cas pour WGMP et nous le comparons au même cas dans IGMPv2. La perte d'un message dans IGMPv1 n'a aucun effet sur son *overhead* puisque les messages sont transmis périodiquement de toute façon. Puisqu'il n'y a aucune retransmission pour le message *leave* dans IGMPv2, quand il est perdu, le protocole se comporte exactement comme IGMPv1. Le routeur note l'absence de groupe quand le groupe fait un *timeout* comme dans IGMPv1.

Dans WGMP, quand une machine envoie un message *leave*, elle attend un accusé de réception du routeur. S'il ne reçoit pas l'accusé de réception après un intervalle du temps *T*, elle retransmet le message *leave*. Nous supposons que les pertes des paquets sont indépendantes. Dans ce cas, la probabilité qu'une machine envoie son message *leave M* fois avant que le routeur puisse le recevoir correctement est $P(M=m)=p^{(m-1)}(1-p)$ où *p* est la probabilité de perte d'un paquet. Le nombre moyen de transmissions pour un paquet est $E[M]=1/(1-p)$. L'*overhead* moyen de WGMP peut être calculé comme suit:

$$Overhead(WGMP) = 4\ L_p\ (N-1) + (3+ E[M])L_p + E[M-1]\ T\ D_r \qquad (6.4)$$

où *T* est le temporisateur pour la retransmission. Il est fixé à deux fois la période de *roundtrip time* du réseau local. Le R_f est fixé à 2 pour les deux versions d'IGMP et le nombre des participants est encore 50 MTs. La probabilité de perte de paquet est égale à 0.01. Avec ces valeurs, nous constatons que WGMP offre moins d'*overhead* que les deux versions d'IGMP pour des débits plus haut qu'à peu près 100 bps! Il est donc mieux adapté aux environnements sans fil.

7. Conclusion

Nous avons étudié le mécanisme IP multicast et son protocole de gestion de groupe, IGMP, et nous avons vu que ce protocole est inapproprié aux réseaux sans fil. Nous avons présenté un nouveau protocole de gestion de groupe appelé WGMP pour les réseaux sans fil. Ce protocole nécessite que le routeur multicast maintienne une liste des participants par groupe dans la base de données GI. Nous avons comparé notre protocole aux deux versions d'IGMP en termes d'*overhead*. Nous avons observé que WGMP améliore l'utilisation de bande passante et qu'il est moins complexe.

Remerciement

Je voulais remercier infiniment Mlle Houda Labiod pour son aide à la rédaction de cet article en français.

8. Références

[1] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 1883, December 1995.

[2] S. Deering, "Host Extensions for IP Multicasting", RFC 1112, August 1989.

[3] C. Diot, W. Dabbous and J. Crowcroft, "Multipoint communications: a survey of protocols, functions and mechanism", IEEE JSAC, vol. 15, no. 3, April 1997.

[4] W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.
[5] D. Johnson, and C. Perkins, “Mobility Support in IPv6”, IETF Internet Draft, Work in Progress, March 1998.
[6] C. Perkins, “IP Mobility Support”, IETF Standard Track RFC 2002, October 1996.
[7] C. Perkins, and D. Johnson, “Mobility Support in IPv6”, MOBICOM’96, November 1996.
[8] L. Rizzo, “Fast Group Management in IGMP”, HIPPARCH’98 workshop, June 1998.
[9] G. Xylomenos, and G. Polyzos, IP Multicast Group Management for Point-to-point Local Distribution, Computer Communications, to appear.