Supprimer le protocole Neighbor Discovery dans les réseaux de capteurs

Laurent Toutain[*] [1] — **Kevin Perros**[*] [2] — **Joongsoo Lee**[**] [2]

[*] *ENST Bretagne,*
CS 17607, Cesson Sévigné 35576 Cedex - France,
Tel. : +33-2-99-12-70-52, Fax : +33-2-99-12-70-30
{Laurent.Toutain, Kevin.Perros}@enst-bretagne.fr

[**] *Information and Communications University,*
Munjiro 119, Yuseong-gu, Daejeon, Korea
Tel. : +82-42-866-6251, Fax : +82-42-866-6154
jslee@icu.ac.kr

RÉSUMÉ. *Cet article propose de nouveaux mécanismes pour réduire l'utilisation du protocole de découverte de voisins* Neighbor Discovery, *en particulier des* Router Advertisement, *dans un réseau de capteurs sans fil doté d'une pile IPv6. Les* Router Advertisement *sont des messages relativement longs, envoyés périodiquement sur le lien pour attester de la disponibilité du routeur. Les spécificités des réseaux de capteurs par rapport aux réseaux IPv6 classiques font qu'il n'est pas toujours nécessaire d'utiliser ces messages. Les mécanismes que nous proposons peuvent également être utilisés pour détecter les* handovers *dans les applications de mobilité.*

ABSTRACT. *This paper proposes new mechanisms to reduce the need of Neighbor Discovery, especially Router Advertisement in a Sensor Wireless Network implementing an IPv6 stack. Router Advertisement are relatively long messages, sent periodically on the link to show the availability of the router. Since Sensor Network Traffic differs from other form of traffic, it is not always necessary to send these messages on that kind of links. The proposed mechanisms can also be used for handover detection in mobility applications.*

MOTS-CLÉS : *6lowpan, Découverte de Voisins, Économie d'Énergie, Mobilité IPv6, Réseaux de Capteurs Sans Fil*

KEYWORDS: *6lowpan, Neigbor Discovery, Power Saving, IPv6 Mobility, Wireless Sensor Network*

1. Ce travail s'inscrit dans le projet "TINY 6" du programme "STIC-ASIE" soutenu par le MAEE, l'Institut Telecom et l'INRIA.
2. Ce travail s'inscrit dans le projet "MoMo" soutenu par le MIC (Ministry of Information and Communication) coréen et publié avec l'autorisation de la NIA (National Information Society Agency) de Corée.

2e soumission à *CFIP 2008*, le 8 février 2008.

1. Introduction

Le protocole *Neighbor Discovery* (NDP) [NAR 07] est utilisé par un équipement IPv6 pour dialoguer avec ses voisins dans le but d'établir la relation entre l'adresse IPv6 et l'adresse MAC. NDP est aussi largement utilisé pendant le démarrage de la machine pour auto-configurer les interfaces. Une grande majorité des équipements l'utilisent pour construire leur adresse globale et trouver le routeur par défaut. Le processus est le suivant : un équipement activant son interface réseau crée une adresse lien-local et, après avoir vérifié son unicité, envoie en *multicast* un message *Router Sollicitation* (RS) vers le groupe bien connu des routeurs du lien (`FF02::2`). Les routeurs répondent directement à l'équipement avec un message *Router Advertisement* (RA) qui peut contenir les préfixes utilisés sur le lien. L'équipement y concatène son identifiant d'interface (IID) pour produire son adresse globale. Il sélectionne aussi le routeur comme son routeur par défaut. De cette manière, l'équipement obtient une connectivité de niveau 3 et est capable d'émettre et de recevoir des paquets sur le réseau mondial. Les autres paramètres comme le résolveur DNS peuvent être appris grâce au protocole DHCPv6, ou, dans le cadre de standardisations récentes [JEO 07], peu être inclus dans les RA.

Les routeurs produisent également périodiquement des messages RA à l'adresse *multicast* bien connue des nœuds du réseau (`FF02::1`) pour :

– prouver aux équipements que le routeur est toujours actif ;

– indiquer sur quel réseau les équipements sont connectés.

Le dernier point est important en cas de mobilité IP car un nœud mobile peut utiliser le préfixe diffusé pour détecter un changement de réseau et produire un message d'association (*Binding Update*). Néanmoins, cette procédure est peu performante et conduit à une forte utilisation de la bande passante. Certaines mises en œuvre demandent une périodicité de quelques secondes [DAL 03]. La valeur la plus courante est de l'ordre d'une cinquantaine de secondes.

Dans les réseaux de capteurs, l'utilisation de messages périodiques peut conduire à de mauvaises performances, aussi bien en terme d'utilisation de la bande passante que pour la consommation électrique. Le but de ce papier est d'étudier les conséquences de la suppression des messages RA périodiques et d'étudier les conditions permettant la réduction des messages sollicités RS/RA tout en garantissant des communications de bout-en-bout avec les autres équipements connectés à l'Internet. Après une présentation de l'architecture IEEE 802.15.4 et du protocole 6lowpan de l'IETF, des modifications seront proposées pour réduire le besoin des messages RA périodiques et sollicités.

2. Architecture IEEE 802.15.4 et 6lowpan

IEEE 802.15.4 [IEE06] est une technologie réseau conçue pour réduire la consommation électrique. Elle est basée sur la méthode d'accès CSMA-CA avec un débit al-

lant de 20 à 250 kbit/s. Plusieurs réseaux (PAN : *Personal Area Network*) indépendants peuvent être déployés sur une même zone. Ils sont identifiés par un PANid. Chacun de ces réseaux possède un unique coordinateur (PC : *PAN Coordinator*) qui gère les attachements des capteurs au réseau, l'allocation d'adresses et optionnellement la bande passante en permettant d'écouler un trafic synchrone. Le PC assure aussi l'interconnexion avec d'autres technologies de réseaux. Dans notre cas, le PC sera mis en œuvre sur le routeur assurant l'interconnexion entre le réseau de capteurs et le réseau Internet.

Quatre types de trames sont définies par le standard : balise (*beacon*), données, acquittement et contrôle. Comme le montre la figure 1, elles commencent toutes par une séquence de synchronisation (préambule et SDF) suivi de la longueur de la trame sur 7 bits, permettant une taille maximale de 127 octets de données. Un champ contrôle donne la nature de la trame, indique la présence et la taille des adresses (16 bits ou 64 bits) et l'utilisation du PANid. Un champ séquence est utilisé pour identifier et acquitter les trames. A part les acquittements, toutes les autres trames contiennent un champ adresse composé du PANid et des adresses de la source et de la destination comme indiqué dans le champ contrôle. Seules les trames d'acquittement ne contiennent pas de données. Toutes les trames se terminent par un CRC.

Zigbee [Zig04] a été défini par le forum Zigbee pour permettre à des applications de fonctionner directement au dessus de la couche MAC. Zigbee offre des possibilités d'adressage, de routage et definit des applications. Zigbee n'est pas une architecture de bout-en-bout : les équipements connectés à l'Internet dialoguent uniquement avec le coordinateur Zigbee, qui interroge le capteur. L'approche de l'IETF avec le groupe 6lowpan est différente puisque le but est de rétablir la connectivité de bout-en-bout entre les équipements IEEE 802.15.4 et les autres équipements IPv6.

6lowpan [MON 07] est une couche d'adaptation utilisée pour transporter IPv6 au dessus d'un réseau de capteurs, et plus particulièrement sur les réseaux IEEE 802.15.4. Ce protocole n'autorise que des trames de 127 octets tandis que le standard IPv6 [DEE 98] impose une taille minimale de 1 280 octets. 6lowpan intègre un mécanisme de fragmentation pour s'adapter à cette contrainte. Il prévoit également la possibilité de compresser les en-têtes IPv6 pour éviter de transmettre les valeurs déjà connues ou contenues au niveau 2. 6lowpan définit le premier bit du champ données comme un discriminant qui indique comment les données sont structurées. Par exemple, la valeur `01 000001` indique que les octets suivants contiennent un paquet IPv6 dont l'en-tête n'est pas compressé. `01 000010` indique que l'en-tête est compressé, `10 xxxxxx` indique une encapsulation pour réseau maillé et `11 000xxx` et `11 100xxx` indiquent une fragmentation (respectivement le premier paquet et les paquets restants).

Actuellement, les réseaux de capteurs sont simples et centrés autour du coordinateur. Si l'IETF a presque finalisé la définition de la couche d'adaptation, ses travaux sur le routage n'en sont qu'à leur commencement.

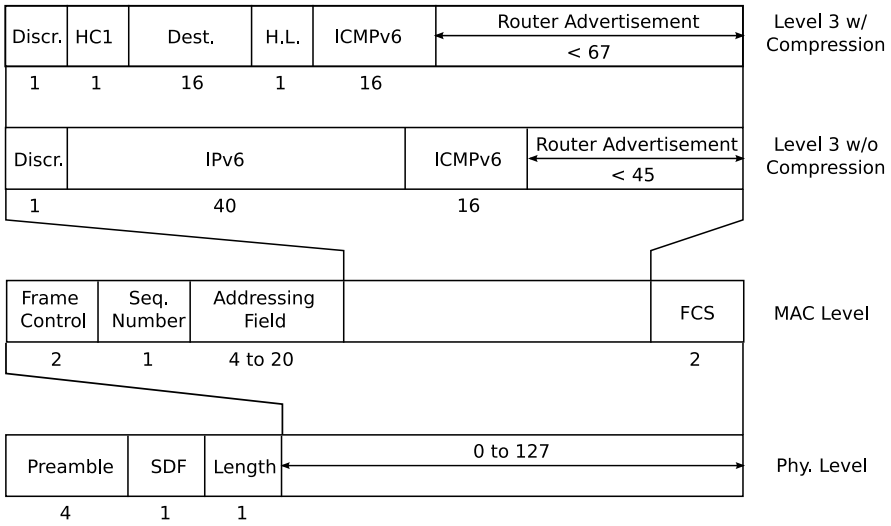

Figure 1. *Encapsulation des RA en IEEE 802.15.4*

2.1. *Compression de l'en-tête*

L'en-tête IPv6 est stable et les champs ont un comportement prévisible. Un discriminant a été défini pour les en-têtes compressés, il est suivit d'un *bitmap* indiquant quels champs doivent ou non transmis. Dans le meilleur des cas, seul le champ Nombre de Sauts (*Hop Limit*) est émis. Les adresses IPv6 source et destination peuvent aussi être compressées, si l'identifiant d'interface est dérivé de l'adresse MAC (16 ou 64 bits).

Quand une adresse de 16 octets est utilisée, son allocation est faite par le coordinateur, l'identifiant d'interface est construit en ajoutant l'adresse de niveau 2 et le PANid. Sinon l'adresse est dérivée des 64 bits de l'adresse MAC.

Dans le cas d'un message de *Neighbor Discovery*, l'adresse lien-local peut être complètement compressée. Par contre les adresses de *multicast* (tout les nœuds, tous les routeurs) ne peuvent pas l'être et les 16 octets doivent être transmis.

Les spécifications 6lowpan proposent de créer des adresses *multicast* de niveau 2 basées sur les adresses *multicast* IPv6. Dans ce cas, les derniers 13 bits de l'adresse IPv6 de *multicast* sont recopiés dans une adresse MAC de16 bits. Hui [HUI 07] propose d'étendre ce format pour y inclure la portée et le groupe. Si ce schéma était retenu, le champ adresse contiendrait l'adresse de la source (16 ou 64 bits) et l'adresse *multicast* (16 bits), ce qui aurait pour conséquence de compresser complètement l'entête. Les versions actuelles ne supportent pas cette possibilité, l'adresse de *broadcast* de 16 bits (`0xFFFF`) doit être utilisée et l'adresse de *multicast* doit être incluse dans le message.

2.2. *Compression des RA*

Quand un capteur entre dans un réseau 6lowpan, il doit construire son adresse IPv6 (soit en la demandant au coordinateur, soit en la construisant à partir de son adresse MAC-64 et en faisant un test pour s'assurer de son unicité). Comme expliqué précédemment, le nœud envoie un RS et reçoit un RA contenant le(s) préfixe(s) disponibles sur le lien et utilise le routeur ayant répondu comme routeur par défaut.

RS est un petit message contenant les 16 octets de l'en-tête ICMPv6 plus une option contenant l'adresse MAC de la source qui ne demande pas de compression particulière et qui est envoyée sur le groupe de *multicast* « tous les routeurs » (`FF02::2`). La norme 6lowpan ne prévoit pas d'adressage *multicast* niveau 2 dans le cas des topologies en étoile [MON 07]. Cette adresse est donc transformée au niveau 2 en adresse de diffusion généralisée, tous les nœuds du PAN reçoivent ce message et, à part le routeur, le rejettent.

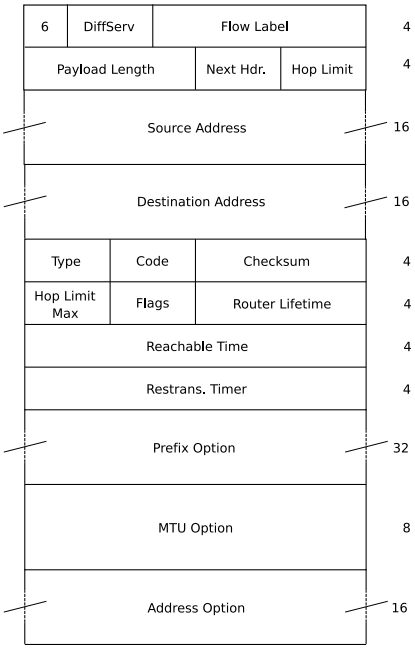

Figure 2. *Message* Router Advertisement *Complet*

La figure 2 donne le format d'un message RA pour un réseau IEEE 802.15.4 quand l'adresse MAC est codée sur 64 bits. Ce message contient :

– 40 octets pour l'en-tête IPv6 ;

– 16 octets pour l'en-tête IPv6, contenant des paramètres commun au réseau comme la valeur maximale du champ nombre de sauts, la durée en seconde pendant laquelle le routeur assurera les fonctions de routeur par défaut, des drapeaux

pour connaître l'articulation avec DHCPv6 et deux temporisateurs pour la résolution d'adresses ;

– L'en-tête ICMPv6 est suivi d'options : 32 octets pour l'option contenant le préfixe et sa durée de validité, 8 pour la valeur de la MTU recommandée sur le lien et 16 ou 8 octets pour l'adresse physique du routeur. Cette dernière option peut être omise, mais elle permet aux nœuds de trouver facilement l'adresse physique du routeur par défaut.

Comme indiqué figure 1, dans le pire des cas (les adresses sont codées sur 64 bits), seuls 45 octets sont disponibles dans une trame IEEE 802.15.4 pour transporter les options. L'option « adresse » ne peut pas être incluse, sauf si on a recourt à la fragmentation. La compression d'en-tête réduit l'en-tête IPv6 de 40 à 18 octets (HC1 + Nombre de Sauts + adresse destination) laissant assez d'espace pour toutes les options du RA. Bien entendu ce calcul n'est valable que lorsqu'un seul préfixe est transmis. Si plusieurs préfixes existent, la fragmentation sera obligatoire.

3. Suppression des RA sollicités

Si l'échange RS/RA peut être évité, cela réduira la consommation en énergie du système, principalement parce que les requêtes RS sont diffusées vers tous les équipements. Dans certain cas, un capteur initiant une session avec le monde extérieur n'a pas besoin de connaître sa propre adresse IPv6. Cette adresse peut être ajoutée par le routeur de bordure. Quand le destinataire répond, le paquet est retourné au routeur de bordure grâce au préfixe et le routeur compresse l'en-tête IPv6 et en extrait l'adresse destination qu'il place dans la trame et l'information est transmise au capteur.

Ce schéma est très similaire à celui utilisé quand, en IPv4, un adressage privé est mis en place. L'adresse privée correspond à l'IID et l'adresse publique correspond au préfixe. La différence majeure comparée à la traduction d'adresse est que si le capteur veut réellement connaître son adresse publique, il peut envoyer un message RS sur le réseau et attendre la réponse du routeur.

Hui [HUI 07] définit un nouveau discriminant pour la compression des en-têtes appelé HC1g pour les adresses globales. Ce discriminant fonctionne de la même manière que celui standardisé par 6lowpan, mais au lieu d'ajouter le prefixe lien-local, le prefixe global du lien est inséré si un paquet IPv6 complet doit être construit. Dans notre cas, ce nouveau discriminant n'est pas nécessaire puisque les paquets doivent être transmis à l'extérieur du réseau de capteurs, l'adresse de destination contient déjà un préfixe global et son identifiant (incompressible puisqu'imprévisible). Un routeur qui reçoit ce type de paquet ajoute le préfixe du lien et l'adresse physique et la source.

Si les RA sont supprimés, le routeur par défaut doit être localisé par les capteurs. Quand le réseau de capteurs a une topologie en étoile, toutes les communications sont organisées autour du coordinateur, donc le routeur est intrinsèquement découvert. Pour les autres topologies, un protocole de routage de niveau 2 est nécessaire pour acheminer les paquets jusqu'au routeur. Dans cette optique, nous proposons d'identifier

le routeur par défaut par une adresse *anycast* bien connue. Cela veut dire que tout équipement ayant les fonctions de routeur par défaut doit être configuré avec cette adresse et que le protocole de routage à l'intérieur du réseau de capteurs doit relayer les trames vers cette adresse. Les capteurs seront configurés avec cette adresse par défaut dans leur table de routage IPv6 et relayeront tous les paquets vers cette adresse. Cette adresse *anycast* ne sera pas utilisée si un RA a fourni une autre valeur. Nous n'étudions pas le routage *anycast* niveau 2 pour les topologies en maillage dans cet article.

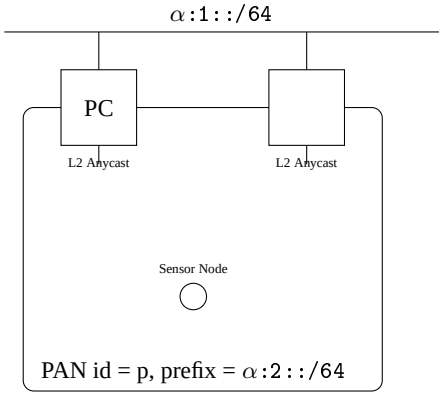

Figure 3. *Adresse* anycast *de niveau 2*

Dans le cas de plusieurs attachement au réseau de capteurs, comme représenté figure 3, plusieurs routeurs par défaut (mais un seul PC) seront actifs sur le réseau. La trame sera routée au niveau 2 vers le routeur le plus proche, réduisant ainsi la consommation du système global en limitant le nombre de sauts. Avec la découverte standard du routeur par défaut, le premier routeur répondant est choisi, le chemin peut donc être plus long, et ne changera pas, même si le capteur se déplace.

Les RA periodiques peuvent être utilisés pour détecter la mort d'un routeur. Dans le cas d'une adresse *anycast* de niveau 2, il n'est pas nécessaire de détecter la mort du routeur, puisque si un autre existe, les paquets seront redirigés vers lui. Certaines applications peuvent vouloir savoir si le routeur par défaut est toujours actif. Une solution possible serait d'utiliser les trames d'acquittement prévues dans le standard IEEE 802.15.4.

Une contrainte à cette approche peut apparaître quand les messages sont fragmentés, si le routage est instable, ou si l'équipement se déplace : certains fragments peuvent être reçus par un routeur et d'autres par un autre, rendant le ré-assemblage impossible. Néanmoins, vues la petite taille et la sporadicité du trafic, le risque est faible. Le capteur ayant un trafic avec de grands paquets peut apprendre une route par défaut grâce à la procédure standard RS/RA.

4. Gestion de la mobilité

Les RA périodiques peuvent être utilisés lors de situations de mobilité pour détecter un *handover* [DAL 03]. Si ceux-ci ne sont plus transmis, un capteur pourra prendre plus de temps pour détecter un déplacement. L'information sur le préfixe doit être résumée ailleurs. Nous proposons d'utiliser le PANid pour informer des modifications de la valeur du préfixe. Le PANid etant sur 16 bits, l'algorithme doit avoir les propriétés suivantes :

– si le capteur reste dans le même domaine (i.e. identifé par le même préfixe global) mais se déplace d'un sous-réseau vers un autre, le PANid doit changer ;

– si le capteur se déplace d'un domaine à un autre, le risque de ne pas détecter ce mouvement doit être faible.

Un algorithme comme $PANid = hash(Préfixe\ Global) + SID$, ou plus simplement l'algorithme bien connu de calcul de somme de contrôle des en-têtes IP (addition en complément à 1 des mots de 16 bits du préfixe), répondent à ces propriétés. Aucune hypothèse n'est faite sur la longueur du préfixe global, s'il est plus grand ces propriétés sont respectées.

Les propriétés du PANid ainsi obtenu sont les suivantes : si le capteur quitte un domaine pour entrer dans un autre, alors le préfixe global IPv6 et le SID changent, il y a alors une probabilité de $1/65536$ que le changement ne soit pas détecté.

Comme le coordinateur est aussi le routeur par défaut, quand un préfixe est alloué au PC, le PANid est calculé et annoncé sur le réseau de capteurs. En cas d'attachements multiples, comme le décrit la figure 3, un changement de comportement par rapport aux spécifications de la norme IEEE 802.15.4 doit être fait. Le standard stipule que chaque PC doit posséder un PANid unique : en cas de conflit entre deux PC, l'un des deux doit changer la valeur de son PANid. Nous désirons au contraire qu'un PANid soit associé à chaque préfixe. Nous proposons qu'en cas de conflit un seul routeur garde le rôle de PC, les autres pouvant servir de PC de secours.

5. Conclusion

Nous avons présenté une meilleure intégration de IPv6 dans IEEE 802.15.4 pour réduire l'utilisation du protocole *Neighbor Discovery* dans les réseaux de capteurs sans fil. Cette approche permet à l'application de choisir le comportement du réseau. Certaines applications simples n'aurons pas besoin de configurer leur niveau 3 pour pouvoir émettre sur le réseau : le PC se chargera dans ce cas de construire les en-têtes niveau 3. Dans ce cas, on diminue grandement l'énergie dépensée pour la configuration et la gestion du réseau. Les capteurs qui voudraient une connectivité IPv6 complète de bout-en-bout peuvent tout de même utiliser *Neighbor Discovery* pour cela : nous avons montré que même dans ce cas, l'envoi de messages périodiques n'est pas nécessaire. Les capteurs peuvent également bénéficier de cette approche pour détecter les *handover* en écoutant les trames IEEE 802.15.4 plutôt que les messages RA.

6. Bibliographie

[DAL 03] DALEY G., PENTLAND B., NELSON R., « Effects of Fast Router Advertisement on Mobile IPv6 Handovers », *Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC 03)*, Kemer - Antalya, Turkey, July 2003, IEEE, p. 1530–1346.

[DEE 98] DEERING S., HINDEN R., « Internet Protocol, Version 6 (IPv6) Specification. », IETF Request for Comments n° 2460, December 1998, Internet Engineering Task Force.

[HUI 07] HUI J., CULLER D., « Stateless IPv6 Header Compression for Globally Routable Packets in 6LoWPAN Subnetworks », Internet Draft n° draft-hui-6lowpan-hc1g-00.txt, June 2007, Internet Engineering Task Force.

[IEE06] IEEE, « Standard 802.15.4-2006, Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). », june 2006.

[JEO 07] JEONG J., PARK S., BELOEIL L., MADANAPALLI S., « IPv6 Router Advertisement Option for DNS Configuration », IETF Request for Comments n° 5006, September 2007, Internet Engineering Task Force.

[MON 07] MONTENEGRO G., KUSHALNAGAR N., HUI J., CULLER. D., « Transmission of IPv6 Packets over IEEE 802.15.4 Networks. », IETF Request for Comments n° 4944, September 2007, Internet Engineering Task Force.

[NAR 07] NARTEN T., NORDMARK E., SIMPSON W., SOLIMAN H., « Neighbor Discovery for IP version 6 (IPv6). », IETF Request for Comments n° 4861, September 2007, Internet Engineering Task Force.

[Zig04] « ZigBee Specification Version 1.0. », december 2004.