RFC 7181 : The Optimized Link State Routing Protocol version 2

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 avril 2014

Date de publication du RFC : Avril 2014

https://www.bortzmeyer.org/7181.html

Il existe désormais plusieurs protocoles de routage pour le problème difficile des MANETs, ces réseaux ad hoc (c'est-à-dire non organisés et non gérés) de machines diverses connectées de manière intermittente. On est loin des réseaux structurés classiques, avec leurs routeurs bien administrés qui se parlent en OSPF. Dans un MANET, le réseau doit se configurer tout seul, il n'y aura pas d'administrateur pour cela (le RFC 2501 [1] examine les différents aspects du problème des MANETs). Notre nouveau RFC décrit la version 2 d'un de ces protocoles de routage les plus répandus, OLSR, dont la version 1 était dans le RFC 3626.

OLSR v2 est incompatible avec la v1, c'est un nouveau protocole. Il garde toutefois les mêmes principes de base (qui étaient avant ceux d'HiperLAN), notamment l'utilisation de MPR, des nœuds du réseau choisis comme routeurs (dans un MANET, il n'y a pas de routeur désigné, chaque machine peut se voir affecter cette tâche, cf. section 18). Ainsi, toutes les machines n'ont pas à émettre de l'information sur leurs interfaces, seul un sous-ensemble des nœuds, les MPR, le fait (c'est particulièrement rentable si le réseau est très dense ; s'il ne l'est pas, la plupart des nœuds seront des MPR puisqu'il n'y aura pas le choix). D'autre part, OLSR v2 est un protocole proactif, il calcule les routes en permanence et elles sont toujours prêtes (contrairement à d'autres protocoles qui calculent les routes à la demande). Principales nouveautés dans OLSR v2 : d'autres façons d'évaluer le coût d'une route que le simple nombre de sauts, et davantage de souplesse dans la signalisation. Notez enfin qu'OLSR peut fonctionner sur des liens de couche 2 variés. Ces liens ne sont pas forcément fiables (par exemple, les liens radio perdent souvent des paquets).

Pour comprendre, et surtout si vous voulez mettre en œuvre OLSR v2, il va falloir lire plusieurs RFC. En effet, la structure des normes OLSR v2 est modulaire : il y a un protocole de découverte des

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2501.txt

voisins (NHDP, dans le RFC 6130), un format de messages décrit dans le RFC 5444, des TLV normalisés dans le RFC 5497, et (mais celui-ci est optionnel) les considérations sur la gigue du RFC 5148 (variations aléatoires ajoutées pour éviter que tous les messages n'arrivent en même temps). Et, naturellement, il faut ensuite lire ce nouveau RFC 7181 (113 pages).

La section 4 résume le fonctionnement du protocole. Comme les MANETs sont loin de mes domaines de compétence, je ne vais pas la reprendre complètement. Quelques points qui me semblent importants. D'abord, le routeur OLSR a plusieurs bases de données (cf. RFC 6130) dans sa mémoire : il y a sa configuration locale (ses adresses IP), sa liste d'interfaces réseau, avec les métriques de chacune (le « coût » d'utilisation), la base des voisins (très dynamique puisque, dans un MANET, les choses changent souvent, le protocole du RFC 6130 permet de découvrir les voisins, voir aussi la section 15 de ce RFC). Cette dernière base contient les volontés d'un voisin (un nœud peut indiquer sa volonté à être routeur, elle va de `WILL_NEVER` à `WILL_ALWAYS`). Et il y a bien sûr la base de la topologie, indiquant la vision du réseau de la machine (les routes qu'elle connait).

Ensuite, OLSR v2, contrairement à son prédécesseur, dispose de plusieurs métriques pour mesurer les coûts d'utilisation d'une route. Un coût est unidirectionnel (il n'a pas forcément la même valeur dans les deux directions).

Le protocole dépend d'un certain nombre de paramètres (section 5). Certains sont spécifiés dans le RFC 5498 comme le numéro de port lorsque OLSR tourne sur UDP (269).

Comme souvent avec les réseaux ad hoc, la sécurité est souvent à peu près nulle. La section 23 de notre RFC fait le point sur les risques associés à OLSR v2 et sur l'approche utilisée si on souhaite sécuriser un MANET. Premier principe, chaque routeur doit valider les paquets (pas seulement leur syntaxe mais aussi leur contenu) puisqu'il ne peut a priori pas faire confiance aux autres. Deuxième principe, la sécurité d'OLSR v2 est réglable. On peut aller de « "*open bar*" », on fait confiance à tout le monde, à l'authentification des messages par le biais de signatures attachées aux messages (RFC 7182 et RFC 7183).

Cette sécurité, si on choisit de l'activer, nécessite que les routeurs connaissent les clés cryptographiques servant à l'authentification. OLSR v2 n'a pas de protocoles de gestion de clés. Dans le contexte d'un MANET, il n'y aura souvent pas de moyen de configurer une clé avant d'installer les machines. (Rappelez-vous qu'un MANET est censé être « zéro administration »).

Il existe bien des mises en œuvre de cette version 2 de OLSR, un protocole qui avait commencé sa carrière vers 2005. Citons entre autres (attention, elles ne sont pas forcément libres) :

— nOLSRv2 <`http://www2.net.ie.niigata-u.ac.jp/nOLSRv2/`> de l'université de Niigata,
— JOLSRv2 <`http://www.herberg.name/projects/79-olsrv2-implementation/71`> (en Java), de l'École Polytechnique,
— olsrd <`http://olsr.org/`>, en C.