RFC 7416 : A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 6 janvier 2015

Date de publication du RFC : Janvier 2015

https://www.bortzmeyer.org/7416.html

Le protocole de routage RPL ("*Routing Protocol for Low power and lossy networks*") est conçu pour des objets connectés, nombreux, mais pas gérés, et qui doivent s'organiser tout seuls pour trouver un chemin dans le réseau. Ces objets peu intelligents soulèvent souvent des problèmes de sécurité spécifiques : ils ne sont pas gérés par un administrateur système compétent, ils ont des capacités de calcul limitées, ce qui réduit le recours à la cryptographie, ils ont une interface utilisateur réduite au minimum, ce qui fait qu'entrer une clé WPA est très pénible, etc. Ce nouveau RFC documente les problèmes de sécurité de RPL.

C'est que l'Internet des Objets est à la mode. On voudrait que chaque brosse à dents soit connectée à l'Internet, et qu'elle discute avec le tube de dentifrice et le frigo sans qu'un humain n'ait besoin de configurer manuellement le routage. On a des solutions techniques pour cela, celle qui est au cœur de ce RFC étant le protocole de routage RPL, normalisé dans le RFC 6550 [1]. Mais si ces solutions permettent au LLN ("*Low-power and Lossy Network*", réseau limité en capacité et en énergie, cf. RFC 7102) de fonctionner, elles ne garantissent pas sa sécurité. Or, ces réseaux d'objets ont souvent des exigences sérieuses en sécurité (pensez à la distribution d'électricité, par exemple). Les RFC 6574 et RFC 7397 avaient déjà abordé ce problème. Ici, on n'examinera pas l'ensemble des problèmes de sécurité des LLN, on se concentrera sur le routage.

Pour une introduction générale aux problèmes de sécurité du routage, on peut aussi consulter le RFC 4593 (qui détaille notamment les types d'attaquants) et l'article de C. Karlof et D. Wagner, « "*Secure routing in wireless sensor networks : attacks and countermeasures*" <http://nest.cs.berkeley.edu/papers/sensor-route-security.pdf> ». La section 4.3 de notre RFC se focalise sur les problèmes spécifiques aux LLN (déjà abordés dans les RFC 5548, RFC 5673, RFC 5826 et RFC 5867) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6550.txt

— Les machines connectés au LLN (les objets) ont des ressources limitées en énergie (batterie de capacité limitée), mémoire et CPU. Comme toujours, la sécurité sera un compromis et, dans le cas d'un LLN, un compromis difficile : il va falloir faire de sérieux sacrifices.
— Les LLN sont a priori de grande taille. Il ne s'agit pas de quelques ordinateurs qu'on a configurés manuellement mais de centaines ou de milliers d'objets dispersés sur le site. Toute solution de sécurité qui nécessiterait une action compliquée de configuration sur chaque objet est vouée à l'échec.
— Les objets sont censés fonctionner de manière autonome, et se débrouiller seuls, dans un réseau qui n'est pas géré et évolue sans cesse.
— La sécurité physique est très minimale. Les objets sont placés à des endroits divers, parfois éloignés, sans qu'on puisse forcément les enfermer dans une cage.
— Certains objets s'endorment de temps en temps, pour économiser l'énergie. Cela complique sérieusement le déploiement de certaines solutions de sécurité. Par exemple, si on distribue de nouvelles clés cryptographiques, les nœuds endormis ne les auront pas eues.

Malgré ces conditions difficiles, on voudrait que RPL obtienne :

— Des données de routage quand il en a besoin (disponibilité),
— Des données de routage non modifiées en route (intégrité),
— Des données de routage qui viennent bien des machines autorisées (authenticité),
— Et, même si c'est nettement moins important, des données de routage qui ne sont pas publiées à tous les vents (confidentialité).

La section 6 de notre RFC énumère les attaques possibles, en insistant sur celles spécifiques aux LLN (ou qui sont plus graves pour un LLN). D'abord, il y a le risque d'usurpation d'un nœud existant. Une machine méchante peut arriver, se glisser dans le réseau, et communiquer en prétendant être un des nœuds légitimes. Rappelez-vous que, dans RPL, n'importe quel nœud peut être routeur et donc annoncer des routes. Un usurpateur peut ainsi détourner le trafic destiné à un autre nœud. Ce détournement peut avoir de sérieuses conséquences, même si on a déployé une sécurité applicative (par exemple en utilisant TLS systématiquement) : le méchant peut retarder des messages, les re-jouer, etc. Même si les techniques de sécurité utilisées empêchent ce méchant d'usurper l'identité d'une machine existante, on peut quand même avoir des attaques où le méchant usurpe une identité, n'importe laquelle, non plus dans le but de se faire passer pour tel ou tel nœud mais simplement pour exploiter les droits d'un membre du LLN. Là encore, il peut annoncer des routes (détournant par exemple tout le trafic vers lui). Enfin, si le réseau est très ouvert (n'importe qui peut s'y joindre, identité ou pas), des attaques par épuisement des ressources peuvent avoir lieu. Rappelez-vous que, dans un LLN, certaines ressources sont sévèrement limitées, comme la capacité des batteries. En envoyant beaucoup de messages sans intérêt (spam), un attaquant pourrait priver pas mal de membres du LLN d'énergie.

Si on réussit à authentifier correctement tous les nœuds du LLN, et donc à empêcher les attaques du paragraphe précédent, un méchant a encore la possibilité de modifier les informations de routage, et donc, au final, de contrôler les routes utilisées. Un nœud authentifié peut encore mentir (annoncer des routes qu'il n'a pas ou bien le contraire, c'est un exemple de comportement byzantin), mais on peut aussi imaginer une modification de l'information entre les nœuds (WiFi pas protégé, par exemple).

Enfin, si on réussit à empêcher mensonges et modifications, l'attaquant peut quand même dans certains cas lancer des attaques contre le réseau en l'empêchant tout simplement de fonctionner (attaque par déni de service). Certaines solutions aux problèmes précédents peuvent aggraver ce risque. Ainsi, si on met de la cryptographie partout, un attaquant peut envoyer des messages, certes faux et détectables, mais qu'il faudra tenter de déchiffrer, ce qui consommera des ressources.

La section 7 de notre RFC couvre les contre-mesures générales, qui peuvent être utilisées dans beaucoup de cas (la section 8 parlera des contre-mesures effectivement existantes dans RPL).

Par exemple, contre les écoutes purement passives, la solution est évidemment le chiffrement des messages de routage. Le mécanisme obligatoire en RPL est AES en mode CCM (RFC 3610). Par contre, ZigBee n'a pas de protection à ce niveau et compte sur celles du niveau 2.

Pour les attaques actives, c'est évidemment plus difficile. Une méthode d'attaque courante dans les réseaux ouverts, comme le sont souvent les LLN, est d'envoyer un grand nombre de machines joindre le réseau, pour ensuite le contrôler par la simple majorité (attaque Sybil). La solution est d'authentifier les machines, via une clé publique. Cela ne protège pas contre les byzantins. Un protocole comme OSPF, où tout le monde reçoit toute l'information, peut se défendre contre les byzantins en comparant ce que reçoivent les différents nœuds. RPL n'a pas cette possibilité et il faut donc chercher des nœuds de confiance, qui fourniront une information qu'on pourra comparer avec celle reçue des pairs (BGP a le même problème et utilise ce genre de solutions <https://www.bortzmeyer.org/alarmes-as.html>). On peut aussi utiliser des canaris, des machines qui doivent être joignables en permanence : si elles cessent de l'être après une nouvelle annonce de route, cela peut signifier une attaque. Si un nœud tente une attaque « évier » (attirer tout le trafic par des annonces de routage mensongères, pour ensuite le jeter), il faudra également le détecter et le noirlister (ne plus tenir compte de ses annonces). On pourra aussi utiliser des indications géographiques (un capteur situé dans le bâtiment A.2 pourra trouver suspect que la meilleure route vers un collecteur du même bâtiment passe par un autre bâtiment).

Et les attaques contre les batteries, surchargeant le réseau de messages à traiter pour vider les accus ? Il faudra sans doute des limiteurs de trafic (voire des quotas de trafic), des mécanismes de détection des nœuds trop bavards, etc.

Enfin, la section 8 de notre RFC décrit les méthodes déployées dans RPL. Comme vu plus haut, RPL a un mécanisme de chiffrement, pour assurer la confidentialité (section 10.9 du RFC 6550) mais qu'il n'est pas obligatoire d'activer car RPL peut se reposer sur la sécurité de la couche 2 (WPA en WiFi par exemple). C'est un peu la même chose pour l'intégrité des messages (à mon avis bien plus importante que la confidentialité, pour un protocole de routage) : si RPL peut compter sur une couche 2 sécurisée, c'est bon, sinon, RPL a son propre mécanisme d'intégrité, avec un MAC calculé, par exemple, avec AES.

Pour la disponibilité du réseau, RPL prévoit les mécanismes suivants dans ses routeurs :
— Ils peuvent limiter la cardinalité des voisins,
— Garder en mémoire plusieurs chemins pour une destination donnée (avec choix aléatoire),
— Avoir des quotas de transmission et de réception,
— Utiliser des informations extérieures à RPL pour évaluer la fiabilité d'une information RPL (comme l'utilisation de la géographie connue dans l'exemple précédent).

À noter que RPL n'a pas de mécanisme de gestion des clés cryptographiques. Celles-ci doivent être fournies et renouvelées en dehors de RPL.

Pour résumer, on peut dire que les exigences de ces réseaux d'objets (autoconfiguration, non-gestion) ne vont pas dans le sens de la sécurité et on peut donc s'attendre à pas mal de problèmes dans les années à venir.