RFC 8884 : Research Directions for Using Information-Centric Networking (ICN) in Disaster Scenarios

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 octobre 2020

Date de publication du RFC : Octobre 2020

https://www.bortzmeyer.org/8884.html

Si vous aimez les films catastrophe, voici un RFC pour vous ; il explore l'utilisation de l'ICN lors de grands désastres. N'espérez pas trouver de solutions, c'est un travail purement théorique. (Comme beaucoup de choses qui touchent à l'ICN.)

L'ICN ("*Information Centric Networking*") ? C'est quoi ? Il s'agit d'une approche des réseaux informatiques où tout est vu comme du contenu, auquel les clients veulent accéder. Les routeurs ICN vont donc se charger de récupérer l'information, sans se soucier d'où elle vient. L'ICN est décrit dans des documents comme le RFC 7476 [1] et le RFC 7927.

Parmi tous les RFC, il n'y a pas que l'ICN qui peut apporter des idées neuves en matière de robustesse lors de grandes catastrophes. Le DTN (RFC 9171), réseau acceptant les déconnexions fréquentes, est également une bonne approche. En effet, en cas de désastre, il est sûr que le réseau sera affecté, et le concept « stocke et réessaie » de DTN est donc un outil utile. Mais ICN offre des possibilités supplémentaires. D'ailleurs, le RFC 7476 (section 2.7.2) citait déjà cette possibilité d'utiliser l'ICN en cas de catastrophe. L'idée est que la couche réseau peut aider à partiellement contourner les problèmes post-catastrophe. Les applications ont leur rôle à jouer également, bien sûr, mais ce n'est pas l'objet de ce RFC.

La section 2 du RFC liste des cas d'usage. Comme déjà le RFC 7476, on commence par le tremblement de terre de Tohoku, qui avait détruit une partie importante de l'infrastructure, notamment en ce qui concerne la fourniture d'électricité. Or, après une telle catastrophe, il y a une grosse demande de

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7476.txt

communication. Les autorités veulent envoyer des messages (par exemple par diffusion sur les réseaux de téléphonie mobile), transmettre des informations, distribuer des consignes. Les habitants veulent donner des nouvelles à leurs proches, ou bien en recevoir. Les victimes veulent savoir où se trouvent les secours, les points de ravitaillement, etc.

Les gens de l'ICN étant toujours à la recherche de subventions, ils citent fréquemment les thèmes à la mode, qui promettent l'attention des pouvoirs publics. C'est ainsi que la liste des cas d'usage inclus évidemment le terrorisme (pourquoi pas la cyberguerre, tant qu'on y est ?). Dans ce cas, des difficultés supplémentaires surviennent : les attaquants peuvent effectuer des attaques par déni de service pour empêcher l'utilisation du réseau, si l'attaque elle-même ne l'a pas arrêté, ils peuvent surveiller l'utilisation du réseau pour, par exemple, découvrir des cibles intéressantes pour une nouvelle attaque, ils peuvent envoyer des messages mensongers pour créer une panique, etc. Le problème est donc plus difficile que celui d'une catastrophe naturelle.

Aujourd'hui, les réseaux existants ne permettent pas forcément de traiter les cas de catastrophes, même « simplement » naturelles. La section 3 du RFC liste les principaux défis qu'il faudrait traiter pour cela :

— On s'attend à ce que le réseau soit fragmenté par la catastrophe. Certains composants seront alors inaccessibles. Pensez à l'accès aux serveurs DNS racine si on est dans un îlot où il n'existe aucune instance de ces serveurs. Tous les systèmes centralisés seront inutilisables si on est du mauvais côté de la coupure. Par exemple, les systèmes de téléphonie mobile existants dépendent souvent de composants centraux comme le HLR. Un réseau utilisable pendant les catastrophes doit donc pouvoir fonctionner même en cas de fragmentation.
— Un service qui est très souvent centralisé est celui de l'authentification. Même quand le système peut marcher en pair-à-pair, la possibilité de l'utiliser dépend souvent d'une authentification centrale. Même quand il y a décentralisation, comme avec une PKI, il peut être nécessaire de passer d'abord par une ou plusieurs racines, qui peuvent être injoignables pendant la catastrophe. Créer un système d'authentification décentralisé est un sacré défi. Le RFC note que la chaîne de blocs n'est pas une solution, puisque celle-ci ne fonctionne plus s'il y a fragmentation (ou, plus exactement, chaque groupe de participants risque de voir sa portion de la chaîne invalidée lorsque le réseau sera à nouveau complètement connecté).
— En cas de catastrophe, il sera peut-être nécessaire de donner une priorité à certains messages, ceux liés à la coordination des secours, par exemple. C'est d'autant plus important à réaliser que la capacité <https://www.bortzmeyer.org/capacite.html> du réseau sera réduite et que les arbitrages seront donc difficiles.
— Dans un réseau sérieusement endommagé, où la connectivité risque fort d'être intermittente, il ne sera pas toujours possible d'établir une liaison de bout en bout. Il faudra, beaucoup plus qu'avec l'Internet actuel, compter sur le relayage de machine en machine, avec stockage temporaire lorsque la machine suivante n'est pas joignable. C'est justement là où DTN est utile.
— Enfin, dans la situation difficile où se trouveront tous les participants, l'énergie sera un gros problème ; peu ou pas de courant électrique, pas assez de fuel pour les groupes électrogènes, et des batteries qui se vident vite (comme dans le film Tunnel, où le héros doit surveiller en permanence la batterie de son ordiphone, et économiser chaque joule).

Bon, ça, ce sont les problèmes. Maintenant, en quoi est-ce que l'ICN peut aider ? Plusieurs arguments sont avancés par le RFC (dont certains, à mon avis, plus faibles que d'autres) :

— L'ICN, c'est une de ses principales caractéristiques, route en fonction du nom du contenu convoité, pas en fonction d'une adresse IP. Cela peut permettre, dit le RFC, de survivre lorsque le réseau est coupé. (L'argument me semble douteux : il suppose qu'en cas de fragmentation, le contenu sera présent des deux côtés de la coupure. Mais on peut en dire autant des adresses IP. Contrairement à ce que racontent toujours les promoteurs de l'ICN, il y a bien longtemps que les adresses IP n'ont plus de rapport avec un lieu physique). C'est d'autant plus vrai si le système de résolution des noms est complètement décentralisé. (Là encore, ICN et système classique sont à égalité : l'un et l'autre peuvent utiliser un système centralisé, un système décentralisé, ou un système pair-à-pair pour la résolution de noms).

— Un point fort de l'ICN est que l'authentification et l'intégrité ne sont pas assurés par la confiance dans le serveur d'où on a obtenu le contenu, mais par une certification portée par l'objet (typiquement une signature). Certains mécanismes de nommage mettent même l'intégrité dans le nom (cf. RFC 6920). Cela permet de récupérer du contenu n'importe où, ce qui est utile si le serveur d'origine est injoignable mais que des copies circulent. On peut ainsi vérifier l'authenticité de ces copies.
— ICN utilise beaucoup les caches, les mémoires dans lesquelles sont stockées les objets. Avec l'ICN, chaque routeur peut être un cache. Là aussi, cela peut aider beaucoup si le serveur d'origine n'est plus joignable.
— Et ICN est bien adapté aux techniques à base de DTN (cf. par exemple RFC 9171), où il n'y a pas besoin de connectivité permanente : on transmet simplement le contenu en mode « stocke et fais suivre ».

En parlant de DTN, notons que DTN seul manque de certaines fonctions que pourrait fournir l'ICN. C'est le cas par exemple du "*publish/subscribe*". Dans certains cas, ces fonctions pourraient être ajoutées au DTN, comme présenté dans « "*Efficient publish/ subscribe-based multicast for opportunistic networking with self-organized resource utilization*" <https://www.researchgate.net/publication/221191155_Efficient_PublishSubscribe-Based_Multicast_for_Opportunistic_Networking_with_Self-Organized_Resource_Utilization> » (par Greifenberg, J. et D. Kutscher) ou bien « "*A Socio-Aware Overlay for Publish/Subscribe Communication in Delay Tolerant Networks*" <https://www.cl.cam.ac.uk/research/srg/netos/papers/2007_YONEKI_MSWIM.pdf> » (par Yoneki, E., Hui, P., Chan, S., et J. Crowcroft).

La section 4 du RFC précise ensuite les scénarios d'usage, et les exigences qui en découlent. Par exemple, pour le scénario « diffuser de l'information aux gens », la question de l'authentification est cruciale, de fausses informations diffusées par un malveillant ou par un plaisantin pourraient avoir des conséquences graves.

Est-ce que l'ICN peut assurer ces missions, là, aujourd'hui ? Clairement non, et la section 5 du RFC décrit tout ce qu'il reste à faire (rappelez-vous que l'ICN, c'est de la recherche fondamentale). Par exemple, dans le contexte envisagé, celui d'une vraie catastrophe, il est possible que les données doivent être transportées par des « mules », des porteurs physiques (on peut penser au RFC 1149 mais aussi, plus sérieusement, à UUCP où les messages étaient parfois transportés ainsi, notamment dans les pays du Sud). Cette proposition est envisagée dans l'article de Tagami, A., Yagyu, T., Sugiyama, K., Arumaithurai, M., Nakamura, K., Hasegawa, T., Asami, T., et K. Ramakrishnan, « "*Name-based Push/Pull Message Dissemination for Disaster Message Board*" ».

Enfin, la section 5 du RFC décrit ce qui reste à faire (l'ICN est aujourd'hui incapable d'assurer les missions décrites au début de ce RFC). La première chose serait d'évaluer en vrai les solutions ICN existantes. Un test à la prochaine catastrophe ?

À noter que le travail ayant mené à ce RFC a été fait en partie dans le cadre du projet GreenICN <http://www.greenicn.org/>.