"Terminodes": vers des réseaux auto-organisés, dépourvus d'infrastructure

Autor(en): **Hubaux, Jean-Pierre**

Objekttyp: **Article**

Zeitschrift: **Ingénieurs et architectes suisses**

Band (Jahr): **127 (2001)**

Heft 04

PDF erstellt am: **02.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-80021

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Prof. Jean-Pierre Hubaux, chef du Département
de systèmes de communication,
EPFL, 1015 Lausanne

«Terminodes»: vers des réseaux auto-organisés, dépourvus d'infrastructure

Dans la jungle des nouveaux vocables - flanqués d'un nombre grandissant d'abréviations chic (WAP, UMTS, WLAN) - dont nous gavent les technologies de la communication, en voici un à consonance poétique: «terminodes». Ode aux terminaux, aux terminaux intelligents? Cette création lexicale fleurant bon le pragmatisme anglo-saxon est une contraction des mots «terminal» et «node»[1], pour désigner le cumul d'une fonction de terminal et de réseau dans un même équipement, qu'il soit téléphone mobile, système de mesure ou autre. La notion de «terminode» est intimement liée à l'auto-organisation; elle vise à s'affranchir de tout dispositif centralisé, commutateur, routeur, antenne fixe ou satellite. A l'instar des fourmis qui, de proche en proche, transmettent une information olfactive tout en vaquant à leurs tâches, les terminodes font rebondir un signal, d'appareil en appareil, jusqu'à son lieu de destination, assurant le routage et les autres fonctions du réseau indépendamment de toute infrastructure fixe.

L'auto-organisation des usagers, au service de la créativité

Avec la généralisation de l'Internet, l'implication et le degré de responsabilité des usagers des réseaux de communication se sont considérablement développés: désormais, ils ont la possibilité de développer et de modifier les applications qui tournent sur leurs propres machines. Cette liberté a stimulé la créativité, entraînant la mise au point et le déploiement d'un grand nombre de nouveaux services et applications. Par ailleurs, le développement explosif des réseaux cellulaires a apporté la mobilité. Alliée au remarquable progrès de la technologie, cette évolution a déjà profondément modifié la façon dont nous vivons et travaillons.

A l'aube du nouveau millénaire, un changement d'une ampleur au moins équivalente va se produire: l'émergence de réseaux sans infrastructure, auto-organisés. L'auto-organisation est le signe distinctif d'un réseau fonctionnant uniquement par l'action de ses propres usagers. Parallèlement, la miniaturisation permettra de mettre au point des réseaux de capteurs, qui seront également appelés à s'auto-organiser pour communiquer les uns avec les autres.

Les réseaux mobiles *ad hoc*

Evolution des réseaux cellulaires

Comme leur nom l'indique, les réseaux cellulaires sont organisés en cellules, dont chacune est couverte par le champ d'action d'une antenne. Cette dernière assure la connectivité entre le réseau fixe et les mobiles qui se trouvent dans la cellule. Le déploiement de ce type de réseaux requiert donc un important effort de planification, exigence qui va évidemment à l'encontre des besoins de déploiement rapide, tels que ceux rencontrés par les militaires sur les théâtres d'opération. Pour répondre à ces contextes particuliers, les réseaux mobiles *ad hoc* ont été mis au point dans les années 70. Déjà, les informations y étaient transmises de terminal en terminal jusqu'à atteindre leur destination. Plus récemment, d'autres applications ont été identifiées pour ces réseaux, telles que le déploiement d'équipes de secours après une catastrophe.

De par leur nature, les réseaux mobiles *ad hoc* présentent un certain nombre de caractéristiques communes. Premièrement, ils fonctionnent sans infrastructure fixe. Ensuite, ils se doivent d'être hautement coopératifs: les mécanismes de fonctionnement étant répartis sur les différents nœuds, toute opération est le résultat de la collaboration d'un ensemble de nœuds, qui sont généralement alimentés par batterie. De plus, la topologie peut être très dynamique, mettant en péril la stabilité des liens et des routes, tandis que les liens eux-mêmes sont généralement sans fil, ce qui oblige à en étudier soigneusement la fiabilité et le débit. Enfin, la sécurité est difficile à assurer, du fait de la vulnérabilité des liens radio et de la faible protection physique des nœuds.

Nous détaillons ci-après quelques-uns des grands défis techniques que pose ce genre de réseau.

Défis techniques

Le routage - soit l'acheminement optimal d'un paquet d'information de la source à la destination - est une fonction cen-

[1] Equivalent anglais de «nœud» dans les sciences naturelles et techniques. En français, l'adoption d'un mot-valise tel que «terminoeud» pourrait faire l'affaire...(si ce n'est que la rime en «ode» est perdue!)

Fig. 1: Le problème du terminal caché: supposons que le terminal A soit en train de transmettre vers B, et que C soit hors du rayon d'émission de A. Si C se met à émettre, il y a collision en B. On dit alors que A est caché de C.

trale de tout réseau. Or en matière de routage, les réseaux *ad hoc* obligent à relever deux défis essentiels. Tout d'abord - et contrairement aux solutions traditionnelles (Internet ou réseau téléphonique) où le problème consiste à transmettre rapidement l'information relative aux changements de topologie du réseau, mais en se fondant sur le fait que ces changements y sont relativement peu fréquents -, les réseaux *ad hoc* se distinguent par une topologie susceptible de changer en permanence. Ensuite, les réseaux traditionnels utilisent une base de données distribuée, maintenue par l'opérateur, qui contient des informations indispensables au routage, tandis que les réseaux *ad hoc* n'ont pas accès à de tels répertoires. Un certain nombre de solutions techniques ont été proposées et parfois réalisées; certaines d'entre elles consistent à rendre le nœud «conscient» de sa propre position géographique.

Une autre difficulté que tout réseau mobile doit résoudre consiste à gérer la mobilité de ses terminaux pour être capable de les localiser, sur la base de leur adresse. Dans les réseaux cellulaires, la localisation de tous les terminaux est stockée dans des serveurs centralisés. Bien entendu, une telle solution est exclue pour les réseaux *ad hoc*. Par conséquent, l'information de localisation doit être distribuée entre les nœuds eux-mêmes.

L'interface radio pose également des problèmes difficiles. Plusieurs aspects doivent être pris en considération. Premièrement, le signal décroît comme le carré de la distance, sinon plus. Ensuite, les protocoles généralement utilisés pour les réseaux locaux tels que Ethernet ne sont pas appropriés, du fait de la difficulté à détecter les collisions de paquets sur l'interface radio. Enfin, deux terminaux peuvent, sans le savoir, interférer l'un avec l'autre auprès d'un troisième (fig. 1).

1

Quant à la sécurité, problème de première importance dans la plupart des réseaux, elle devient cruciale dans les réseaux *ad hoc*. Plusieurs fonctions de sécurité peuvent être requises, telles que la disponibilité du service, la confidentialité, l'intégrité des données, l'authentification et la non-répudiation. Une des principales difficultés est de parvenir à gérer les clés d'encryptage de manière totalement décentralisée.

S'y ajoute enfin le contrôle de puissance, un élément toujours délicat dans les réseaux sans fil. Dans le cas des réseaux *ad hoc*, deux problèmes essentiels se posent. D'une part, la puissance d'émission doit être réglée afin de maximiser le débit global du réseau. D'autre part, comme les nœuds fonctionnent souvent sur batterie, il y a généralement lieu de minimiser leur consommation.

A ce point, il est opportun de mentionner l'émergence d'un certain nombre de produits et standards qui présentent quelque ressemblance avec les réseaux *ad hoc*. Les réseaux locaux sans fil (WLAN) tels que IEEE 802.11 ou *Hiperlan* sont désormais monnaie courante et permettent un accès au réseau par liaison radio, typiquement pour des ordinateurs portables; toutefois, ils sont généralement déployés sous la forme de liens d'accès, le relais des paquets étant assuré par des ponts ou routeurs traditionnels. Quant à *Bluetooth*, il s'agit d'une technologie économique pour la communication à courte distance (de l'ordre du mètre ou de la dizaine de mètres), dont le marché (en principe très prometteur) vise les PC, les téléphones mobiles, les montres et autres organisateurs numériques personnels. Les expériences faisant appel à cette technologie sont toutefois trop récentes pour autoriser des conclusions quant à son mode d'usage.

Changement de paradigme : vers l'auto-organisation

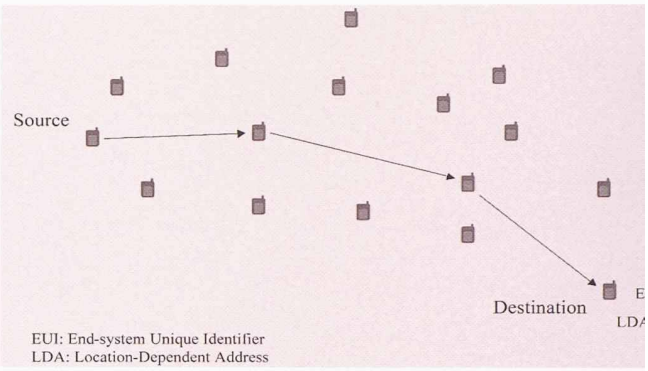
Il est communément admis que, pour fonctionner correctement, un grand système technique doit être géré par une organisation humaine. C'est le cas des chemins de fer, de la production et de la distribution d'électricité et, bien sûr, des réseaux de communication, qu'il s'agisse du réseau téléphonique, fixe ou cellulaire, ou du réseau Internet. Dans le cas d'Internet, les opérateurs se préoccupent du dimensionnement du réseau (routeurs, artères de transmission) en fonction de la charge prévue ou observée, du traitement des pannes et ainsi de suite. Cela étant, des constructions logicielles ont commencé à apparaître sur cette infrastructure, qui s'apparentent à l'auto-organisation. Dans l'ordre chronologique, on peut citer trois exemples:

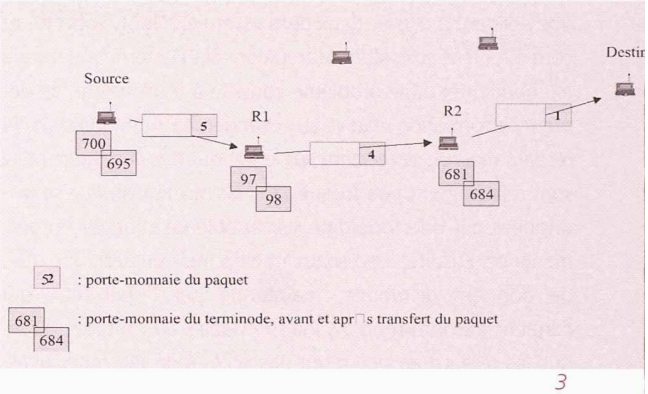
- Le *World Wide Web*, qui permet à chaque usager de tisser de nouveaux hyperliens sur la Toile, sans devoir en référer à qui que ce soit et de façon totalement décentralisée: en effet, la création d'un hyperlien se fait depuis une page Web donnée et l'information y relative demeure localisée sur celle-ci. Il faut cependant reconnaître que l'auto-organisation n'est pas totale, dans la mesure où la responsabilité de la nomenclature (et donc l'attribution des URL) reste centralisée.
- *PGP (Pretty Good Privacy)*, un système de certification des usagers qui permet à un utilisateur de certifier la clé d'encryptage publique d'un autre. Contrairement aux solutions

Fig. 2: Transfert géodésique de paquets à l'aide d'ancres: le terminode source envoie un paquet vers le terminode de destination . A chaque étape, le terminode relais est choisi de façon à se rapprocher autant que faire se peut de la destination.

Fig. 3: Monnaie virtuelle: les nuglets. *La source introduit cinq* nuglets *dans le porte-monnaie du paquet. Le premier terminode relais (R1) impute une «taxe» d'un* nuglet, *qui est prélevée dans le porte-monnaie en question. Le second (R2), prélève quatre* nuglets; *ce coût plus élevé peut être motivé par une distance au voisin plus grande.*

2





3

classiques dans lesquelles la certification est assurée par un organisme de référence, *PGP* décentralise donc cette opération. Seul le serveur de clés, sur lequel les certificats sont mis à la disposition des usagers, demeure centralisé. Mais il ne s'agit-là que d'un élément mis en place pour des raisons de commodité, et il n'est pas indispensable au principe de fonctionnement lui-même.

- *Gnutella*, enfin, est un système totalement décentralisé de publication sur le Web. Il permet à chacun de publier ce que bon lui semble (texte, images, vidéos, fichiers audios, etc.). Contrairement à *Napster*, qui comportait encore des serveurs centralisés pour faciliter la recherche d'une machine susceptible de contenir un fichier donné, *Gnutella* permet en principe de faire supporter l'effort de recherche par les machines des usagers eux-mêmes.

De façon prévisible, dès lors qu'un système est auto-organisé, des difficultés importantes apparaissent au niveau éthique et, partant, dans les relations avec l'autorité. Ainsi, depuis sa création en 1989, l'histoire du Web a été jalonnée de tentatives d'imposer des mesures de censure pour combattre certaines dérives regrettables quant au contenu. Bien entendu, les promoteurs du Web se sont toujours efforcés d'éviter que le législateur ne se mêle de restreindre la liberté d'expression; ils ont donc tenté faire rimer auto-organisation avec autodiscipline, notamment par le biais de la technique *PICS (Platform for Internet Content Selection)*. De même, les autorités (en particulier américaines) se sont montrées très nerveuses face au risque que *PGP* ne leur permette plus de décrypter certaines communications jugées «sensibles». Enfin, l'émergence de solutions de type *Napster* ou *Gnutella* remet profondément en question l'applicabilité des lois sur le droit d'auteur et bouleverse déjà le secteur de la vente des enregistements, musicaux en particulier. En dépit de ces inconvénients, l'auto-organisation recèle vraisemblablement un potentiel fantastique, dans la mesure où elle permet d'une part de s'affranchir de la tutelle d'une organisation et d'autre part de stimuler la créativité de l'individu dans des proportions initialement insoupçonnées, comme c'est le cas pour le Web.

Le projet «Terminodes»

Nous avons défini un projet de recherche à long terme, baptisé «terminodes», qui vise à étudier la mise en oeuvre des principes d'auto-organisation dans les réseaux mobiles *ad hoc*. Cette faisabilité est étudiée à différents niveaux, depuis la couche physique (ou liaison radio) jusqu'aux applications, en passant en particulier par l'organisation des mécanismes du réseau lui-même. Nous décrivons ci-après quelques-uns de ces mécanismes.

Chaque terminode possède un identifiant unique (appelé *End System Unique Identifier, EUI*), invariable. Il a par ailleurs une adresse géographique, qui correspond à sa position, appelée *Location-Dependent Address* ou *LDA*. Si le terminode est équipé d'un récepteur GPS et qu'il reçoit le signal correspondant, le *LDA* contient l'information fournie par le GPS. Autrement, un positionnement relatif est réalisé, selon un principe que nous décrivons plus loin. Le routage dans les terminodes obéit à trois exigences: opérabilité dans des réseaux de grande taille, minimisation des fonctions activées dans les nœuds intermédiaires et robustesse face aux usagers malveillants. Il se fonde sur le transfert géodésique de paquets: à chaque saut, le paquet est transféré au voisin le plus proche de la destination visée (fig. 2).

En l'absence de récepteur GPS, le positionnement géographique se fonde sur l'estimation de la distance entre terminodes voisins par des mesures appropriées (temps de propagation ou atténuation du signal). Ces mesures peuvent évidemment être entachées d'un certain niveau d'erreur, surtout lorsque deux voisins ne sont pas en vue l'un de l'autre. Le principe en est fourni par la figure 4.

Enfin, l'auto-organisation pose le problème de la volonté de collaboration des usagers. Le risque existe en effet que certains se comportent de façon égoïste, saturant le réseau par un usage excessif ou ne relayant pas les paquets d'autrui. Afin de pallier cet inconvénient, nous travaillons actuellement sur l'usage d'une monnaie virtuelle pour les terminodes, baptisée «nuglets» (en anglais, «nugget» signifie pépite et «nuglet» est un néologisme pour désigner une «très petite pépite»). Le principe en est illustré à la figure 3.

Nous nous sommes contentés de décrire ici quelques mécanismes s'appliquant au réseau. D'autres sont à l'étude, qui touchent notamment à la couche physique et aux applications. Le lecteur intéressé pourra consulter le site Web du projet (www.terminodes.org).

4

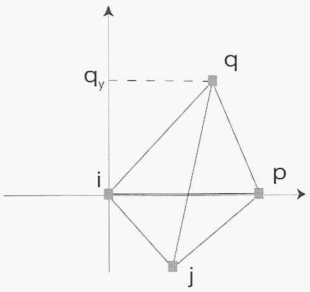


Fig. 4: Positionnement géographique en l'absence de récepteur GPS: chaque terminode s'efforce d'établir une estimation de la distance qui le sépare de chacun de ses voisins. Selon un algorithme réparti, ces données sont ensuite combinées pour construire un repère orthonormé de l'ensemble du réseau, dans lequel les coordonnées de chaque terminode sont alors exprimées. Ici, en phase initiale, le terminode i *choisit ses voisins* p *et* q.

Tableau I: Survol de l'évolution des réseaux

I

Type de réseau	Infrastructure	Sécurité	Applications
Réseau télécom	Opérateurs télécom	Opérateurs télécom	Opérateurs télécom (Réseau Intelligent)
Internet	Opérateurs télécom et Internet	Opérateurs Internet et usagers (PGP)	Usagers
Réseau *ad hoc* auto-organisé	Usagers + fournisseurs	Usagers + fournisseurs	Usagers

Perspectives

Comme nous l'avons vu, les réseaux mobiles auto-organisés sont susceptibles de modifier profondément la réalité des communications. Cela est illustré par le tableau I, qui fournit une vue globale de l'évolution des réseaux sur plusieurs décennies. Chaque ligne correspond à une génération de réseaux :

- les réseaux de télécommunication tels que le réseau téléphonique[2],
- Internet,
- les réseaux mobiles *ad hoc* auto-organisés.

Pour chaque génération, le tableau indique qui (usager, opérateur ou fabricant) est responsable de chacun des aspects les plus importants: l'infrastructure (y compris la facturation), la sécurité et les applications. Il illustre la tendance forte vers une augmentation de la responsabilité de l'usager. Par exemple, la colonne relative à la sécurité montre que dans les réseaux de télécommunications, les opérateurs sont responsables de cet aspect; dans l'Internet, les opérateurs de réseau (ISP) ont certes un rôle important à jouer, mais les usagers peuvent s'auto-organiser par une solution de type *PGP*; enfin, dans les réseaux mobiles auto-organisés, la sécurité est à la charge de ces derniers, qui déploient les produits qu'ils choisissent auprès des fournisseurs.

Internet a montré que lorsque les usagers peuvent faire évoluer leur propre équipement terminal en le programmant à leur guise, la créativité humaine s'en trouve formidablement stimulée et conçoit les applications puissantes que nous connaissons désormais: le courrier électronique, le Web, le commerce électronique... La globalisation est une conséquence directe de ce phénomène. S'ils sont adoptés par le marché, les réseaux *ad hoc* mobiles auto-organisés portent en eux la promesse de faire un pas de plus, en confiant aux usagers le fonctionnement du réseau lui-même.

Un autre aspect fondamental est celui de la relation que nous entretenons avec les communications. Si les échanges de personne à personne ont jusqu'ici constitué le modèle dominant, les réseaux mobiles *ad hoc* ouvrent de nouvelles possibilités, telles que la communication entre des objets ou la surveillance de l'environnement, qu'il soit naturel ou construit. Les progrès techniques rendront possible la production de millions d'équipements de ce type à très bas coût, ouvrant la voie par exemple à la surveillance fine et permanente d'ouvrages d'art (ponts, barrages) et de terrains instables. Mentionnons aussi les nombreuses applications envisageables pour les automobiles (prévention des accidents, optimisation des flux de trafic). Là encore, l'usage de ce potentiel appelle une réflexion appropriée.

Très clairement, tout au long du XXème siècle, le développement spectaculaire des technologies de communication a été soutenu par les règles classiques du capitalisme: identification des marchés et fourniture des produits et services correspondants. Nous avons probablement atteint une sorte de plateau désormais: l'être humain n'a pas tellement besoin d'être davantage saturé ou distrait par des fonctions supplémentaires sur les terminaux, qu'ils soient fixes ou mobiles, ou de s'encombrer de gadgets post-modernes supplémentaires. En revanche, les défis qui nous attendent sont de nature «globale»: favoriser l'évolution du Tiers-Monde vers le développement et la démocratie et résoudre les problèmes de l'environnement. A notre sens, les réseaux mobiles auto-organisés sont un des moyens de relever ces défis. Comment et quand? Telles sont les questions auxquelles nous entendons nous attaquer.

Remerciements

L'auteur tient à remercier Françoise Kaestli pour son aide dans la rédaction du présent article.

Références

- J.-P. Hubaux, Th. Gross, J.-Y. Le Boudec, M. Vetterli: «Toward self-organized mobile ad hoc networks: the Terminodes project»
- Site Internet du projet: <www.terminodes.org>
- Sur PGP: <www.pgp.org>
- Sur Gnutella: <www.gnutella.wego.com> et <www.gnutellang.wego.com>

[2] Pour une histoire accélérée des télécommunications, voir la grande fresque en quatre épisodes parue dans *IAS* sous la plume de Pierre Boskovitz: «Révolution planétaire: les télécommunications» (numéros 9, 10, 11 & 14 / 1996)