Zeitschrift: Horizonte : Schweizer Forschungsmagazin
Herausgeber: Schweizerischer Nationalfonds zur Förderung der Wissenschaftlichen Forschung
Band: - (2004)
Heft: 60

Artikel: Netze der Zukunft
Autor: Dessibourg, Olivier
DOI: https://doi.org/10.5169/seals-551277

VON OLIVIER DESSIBOURG

Netze der Zukunft

Sich selbst organisierende Netzwerke aus Mobiltelefonen, Laptops oder Sensoren könnten fest installierte Antennen ersetzen. An diesem Ziel arbeitet der Nationale Forschungsschwerpunkt «Mobile Informations- und Kommunikationssysteme» an der ETH Lausanne.

Über weite Entfernungen miteinander zu sprechen, egal ob im Zug, während einer Bergtour oder mitten in einem klassischen Konzert – diese Privilegien ermöglichen uns die Mobiltelefone, die über ein Netz von fest installierten Antennen miteinander verbunden sind. Was aber, wenn diese Antennen durch starke Erdbeben oder Stürme beschädigt würden? Pieeep... die Kommunikation würde gekappt.

Eine einfache Idee könnte Abhilfe schaffen: Warum nicht die wachsende Anzahl der Mobiltelefone selbst als Antennen benutzen, um Signale zu übermitteln? Wenn also beispielsweise Hans seine Grossmutter am anderen Ende der Stadt anruft, greift sein Handy auf andere mobile Telefone zurück, die sich zwischen den beiden befinden. Gerade so, wie man von Stein zu Stein hüpft, um einen Fluss zu überqueren. Fest installierte Antennen wären überflüssig, und zudem würde der Elektrosmog wegfallen, den sie erzeugen. Doch so einfach das Konzept eines dezentralen, «sich selbst organisierenden» Netzwerks ist, seine Realisierung birgt Schwierigkeiten. Seit 2001 beschäftigen sich mehrere Forschergruppen des Nationalen Forschungsschwerpunkts «Mobile Informations- und Kommunikationssysteme» (NFS MICS) an der ETH Lausanne mit diesen Problemen. Sie müssen verschiedene Anforderungen berücksichtigen: «eine ausreichende Qualität der Datenübertragung, eine kurze Übermittlungszeit der Information von wenigen Mikrosekunden, eine garantiert vertrauliche Übertragung und so weiter», zählt Jacques Bovay auf, der Koodinator des NFS MICS. Um allen Anforderungen Rechnung zu tragen, befassen sich die Forschenden mit technischen, theoretischen, energetischen und sogar ökonomischen Aspekten.

Natürlich existieren diese neuartigen Netze noch nicht, die über jegliche für die Fernkommunikation geeigneten Apparate wie Laptops, elektronische Agenden, Sensoren etc. funktionieren. Aber mit jedem neuen Forschungsergebnis verbessern sich die theoretischen Grundlagen. Nach und nach werden Fragen wie die kritische Dichte der Schnittstellen im Netzwerk, das Weiterleiten von Datenpaketen auf einer Route innerhalb eines Netzwerks (Routing), der Energieverbrauch der Schnittstellen oder die Sicherheit beant-

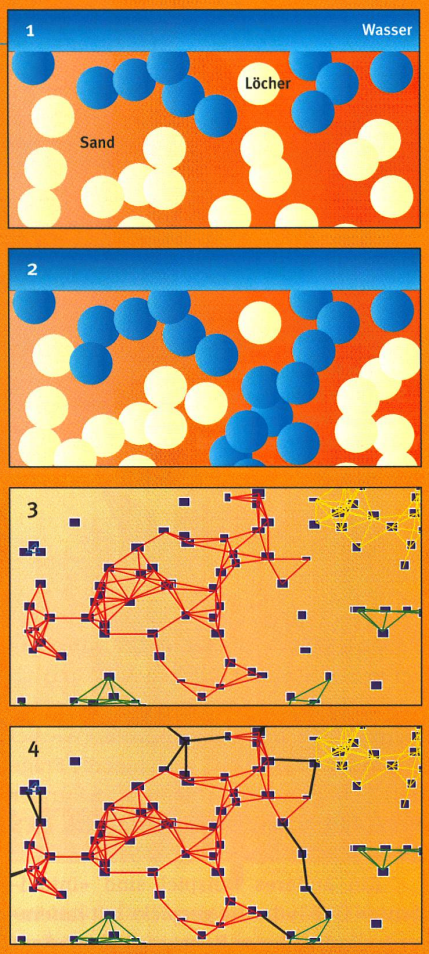
Prisma

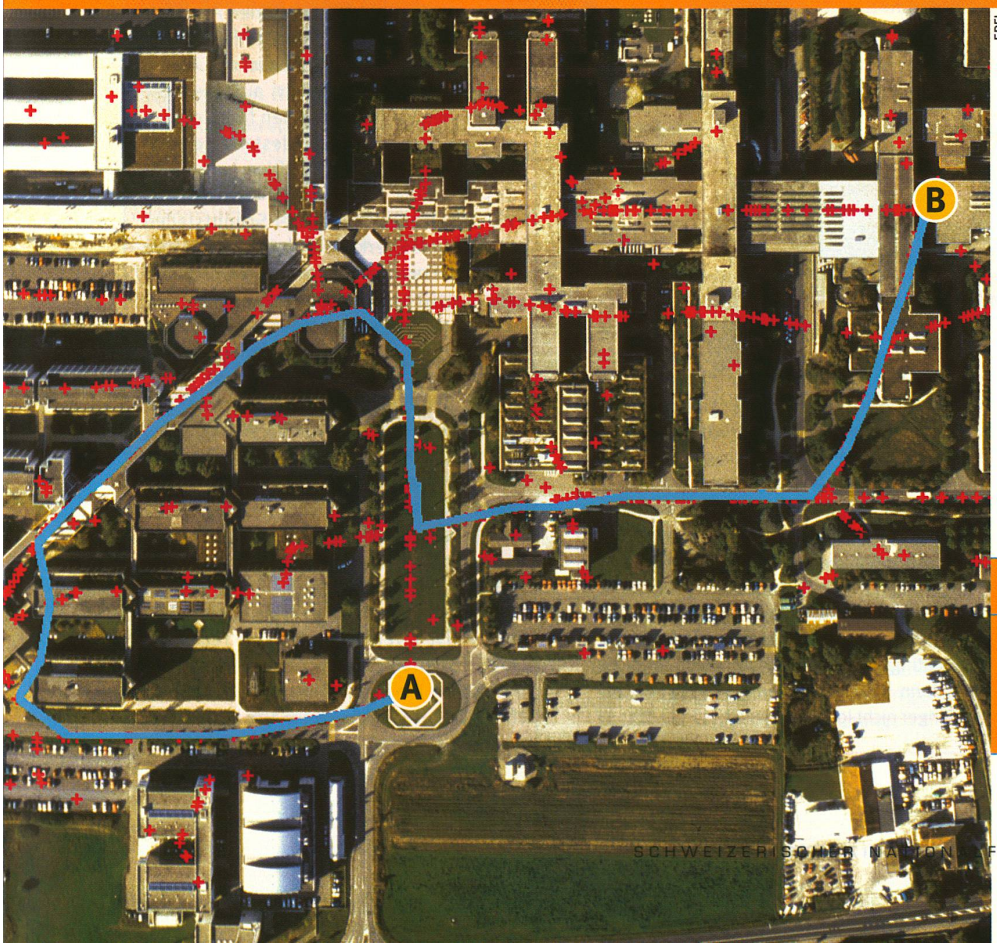
Wie Wasser durch Sand

Ein Netz mit wenigen Schnittstellen, die eine begrenzte Reichweite haben, ist schlecht verknüpft. Dies kann man ändern, indem man einerseits die Reichweite vergrössert, was aber den Energieverbrauch der Schnittstellen, beispielsweise der mobilen Telefone, erhöht. Andererseits kann man die Dichte der Schnittstellen erhöhen, aber nicht allzu sehr, denn dann häufen sich die Interferenzen. Also je dichter ein Netzwerk, desto schlechter seine Übertragungskapazität – ein Dilemma.

Um die ideale Dichte herauszufinden, lassen sich deshalb Patrick Thiran und sein Team von der ETH Lausanne vom Versickerungsprinzip inspirieren: «Wie Wasser, das durch Sand rinnt: Wenn der Abstand zwischen den Sandkörnern gering ist, wird das Wasser zurückgehalten (Abb. 1). Nimmt die Dichte der Löcher zu, versickert das Wasser (Abb. 2).»

So haben die Forscher mit komplexen, theoretischen Methoden die idealen Werte ermittelt, um die Kommunikation durch ein ganzes Netzwerk hindurch zu etablieren. «Es ist, als würden sich die fehlenden Verbindungen (schwarze Linien in der Abb. 4) genau dort bilden, wo man sie haben wollte, wenn man ein klein wenig die Reichweite der Schnittstellen erhöht», erklärt Thiran. Sein Mitarbeiter Olivier Dousse hat die Studie vertieft: «Wenn zu viele Schnittstellen vorhanden sind, kann das Problem gelöst werden, indem sie in regelmässigen Intervallen aktiviert werden. Oder indem man ihnen eine bestimmte Aktivierungswahrscheinlichkeit verleiht. Wir haben diese Wahrscheinlichkeit bestimmt, indem wir versuchten, jede einzelne Schnittstelle lokal zu betrachten, natürlich ohne den gesamten Aufbau aus den Augen zu lassen.» Was den Forschern gelungen ist: Ihre Resultate wurden anlässlich der letzten IEEE-Infocom prämiert, der grossen Konferenz der Kommunikationsspezialisten.



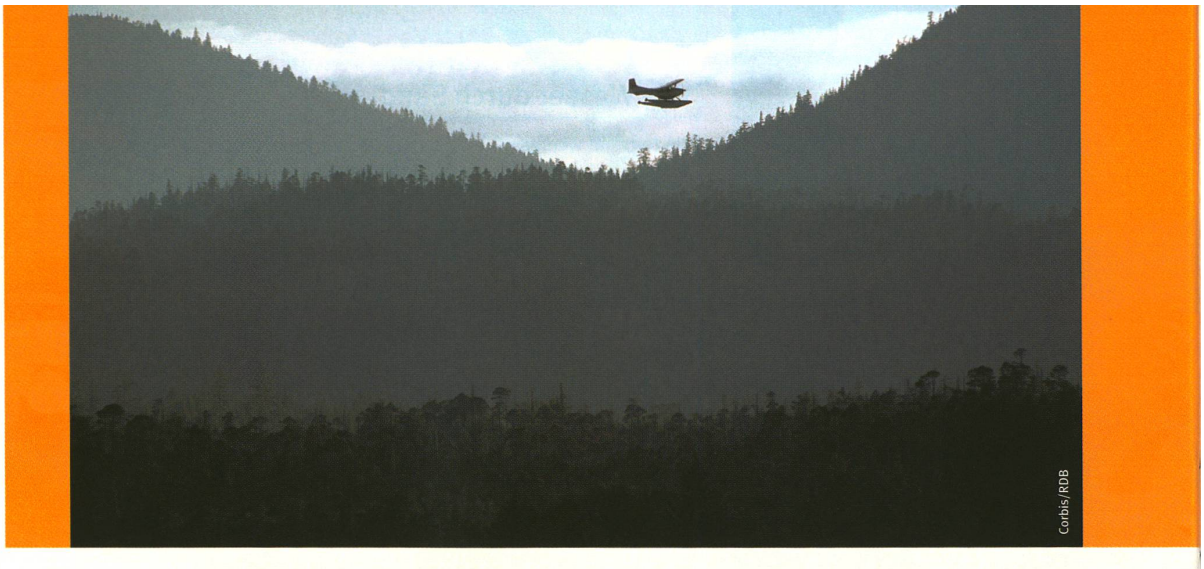


EPFL

wortet (siehe Kästen). Was die Mobiltelefone betrifft, so «ist die Vorstellung eines flächendeckenden und kostengünstigen Netzwerks von mobilen Schnittstellen utopisch. Sie werden die Festnetze nicht ersetzen, könnten aber in Zonen, in denen die Festnetze stark beansprucht werden, wie zum Beispiel an Messen oder in Städten, unterstützend mitwirken», sagt Jacques Bovay. In fünf Jahren werden wahrscheinlich andere Anwendungen entwickelt sein, «die weder mobile Elemente noch eine unmittelbare Übertragung benötigen und mit sparsameren Datenmengen auskommen». So könnten im ▶

Mobiles Netzwerk

Ein Berechnungsmodell zeigt auf, wie die Verbindung (blau) von Punkt A nach Punkt B über mobile Schnittstellen (rot) wie Mobiltelefone und Laptops laufen könnte.



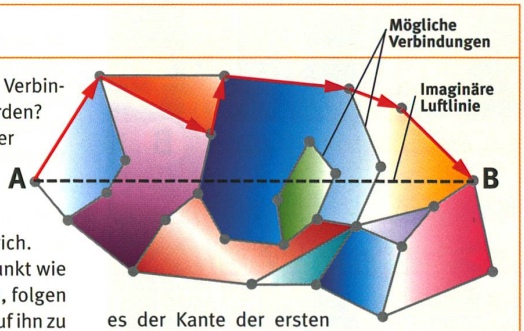
Per Flugzeug könnten Sensoren in einem Gebiet verteilt werden, die sich untereinander vernetzen und Umweltdaten aufnehmen.

Freien stationierte Netzwerke von Sensoren die Umwelt überwachen und so zum Beispiel die Ozonwerte oder andere meteorologischen Daten messen. «Wie bei den Mobiltelefonen ist auch hier die Frage der Schnittstellendichte von zentraler Bedeutung», sagt der Direktor des NFS MICS, Martin Vetterli.

Ein anderes Beispiel sind «intelligente» Gebäude, die gespickt mit miteinander verbundenen Sensoren sind und auf die Anwesenheit von Menschen reagieren können. Ein Start-up-Unternehmen vertreibt denn auch bereits Sensorensysteme zur Steuerung von Kälteketten. Die Befürchtung, dass solche autonomen, dezentralen Systeme Opfer von Piraterie werden oder im Chaos versinken könnten, ist für die Forscher des NFS MICS vielmehr eine Motivation. «Wir führen diese Forschung durch, um eben all diese Risiken besser verstehen zu können», betont Martin Vetterli. Er freut sich darüber, dass der NFS so viele junge Wissenschaftler miteinander vernetzt, um ein einziges Ziel zu erreichen. ■

Mit Hilfe der Oberflächen

Wie kann auf dem kürzesten Weg eine Verbindung zwischen A und B hergestellt werden? Das Routing ist wahrscheinlich eines der kompliziertesten Probleme dieser Netzwerke. «Stellen Sie sich vor, Sie haben sich in Genf verirrt», erklärt Roger Wattenhofer von der ETH Zürich. «Vielleicht finden Sie einen Anhaltspunkt wie den Jet d'eau. Um zu ihm zu gelangen, folgen Sie den Strassen, die am direktesten auf ihn zu führen.» Für mobile Netzwerke gilt dasselbe: Wenn der Ort des Empfängers bekannt ist, kann ein ähnliches Konzept für das Routing angewendet werden, selbst wenn jede Schnittstelle nur die ihr im Netzwerk am nächsten liegende kennt. «Gerät man in eine Sackgasse oder stösst auf ein Hindernis, versucht man, einen möglichst kurzen Umweg einzuschlagen», erklärt Wattenhofer. Die möglichen Verbindungen zwischen den Schnittstellen bilden nämlich eine Art Flächenmuster. Um von A nach B zu gelangen, die durch eine imaginäre Luftlinie miteinander verbunden sind, genügt,



es der Kante der ersten Fläche zu folgen, die von dieser Linie gekreuzt wird, bis zur Grenze der zweiten Fläche, die ebenfalls von dieser Linie durchschnitten wird. Und so weiter bis zum Ziel. Roger Wattenhofer und seine Kollegen Fabian Kuhn und Aaron Zollinger haben diese Technik mit weiteren Techniken kombiniert und so einen Routing-Algorithmus entwickelt, dessen mathematische Beweise zeigen, dass damit das Ziel schnell zu erreichen ist. Neben dem besseren Verständnis des Routings im Internet helfen diese Arbeiten auch dann bei der Problemlösung, wenn der Empfänger nicht lokalisierbar ist.

Sichere Kommunikation

Mobile Netzwerke müssen eine sichere Kommunikation garantieren. Jean-Pierre Hubaux und sein Team arbeiten daran.

«Ist die Sicherheit nicht garantiert, ist ein sich selbst organisierendes Netzwerk nicht denkbar», sagt Jean-Pierre Hubaux von der ETH Lausanne.

Heute wird die Sicherheit der Kommunikation im Allgemeinen direkt von den Telefongesellschaften gewährleistet. Um jedoch mobile Netzwerke zu sichern, muss man sich von einer solchen zentralen Autorität verabschieden. «Die Schnittstellen würden ihre Verschlüsselungsschlüssel und Adressen direkt untereinander austauschen; damit dies via Infrarotwellen funktioniert, müssen sie sich mindestens einmal physisch begegnet sein. Dies garantiert, dass sich die Personen wirklich kennen. Wir bezeichnen diese zwei Schnittstellen als Freunde», erklärt Hubaux. Wenn nun A und B Freunde sind und einen sicheren Kanal zwischen sich errichten, können sie kommunizieren, ohne dass die Nachricht abgehört wird. Und wenn B den Verschlüsselungsschlüssel und die Adresse von C kennt, ohne dass dies umgekehrt der Fall ist, so kann A mit Hilfe von B C kontaktieren. C hingegen kann keine sichere Verbindung zu A aufbauen, denn C kennt nicht alle nötigen Schlüssel.

Lange wurde vermutet, dass solche Sicherheitsvorschriften die Funktion autonomer Netzwerke beeinträchtigen. «Unsere Simulationen haben aber gezeigt, dass diese paarweisen Verbindungen das reibungslose Funktionieren nicht behindern. Im Gegenteil: Die Mobilität kann die Sicherheit festigen», freut sich Jean-Pierre Hubaux.