

Kabellos im riskanten Geschwindigkeitsrausch

Neue Funktechnologien versprechen die kabellose Freiheit und riesige Bandbreiten für mobile Internetnutzer. In der allgemeinen Begeisterung für die stetig steigende Performance geht eines allerdings oft vergessen: die Anfälligkeit der Drahtloskommunikation für Sicherheitsattacken.

Von Simon Wepfer*

Der kabellose Luftkampf geht in eine weitere Runde: Wimax (Worldwide Interoperability for Microwave Access) funkt als WLAN-Hotspot (Wireless Local Area Network) für Langstrecken, und neue Datenbeschleuniger für UMTS-Netze (Universal Mobile Telecommunications System) versprechen Durchsätze, die bisher vor allem die Betreiber mit volumenbasiertem Verrechnungsmodell erfreuen.

Wimax liegt in der Luft

Bei Wimax handelt es sich, salopp ausgedrückt, um einen riesigen Hotspot mit Reichweiten von bis zu 50 Kilometern und Übertragungsraten von bis zu 70 Mbit/s. Doch die Zahlenangaben sind mit Vorsicht zu geniessen, denn diese Reichweiten gelten nur bei Sichtkontakt zwischen Sender und Empfänger. Gemäss Intel wird eine durchschnittliche Wimax-Basisstation Entfernungen von fünf bis acht Kilometern überbrücken. Zudem teilen sich die Nutzer die verfügbare Bandbreite. Wimax ist also eher dazu geeignet, schlecht erschlossene Randregionen mit Internetkonnektivität zu versorgen.

Wimax ist nicht mobil, die Verbindung bricht also ab, wenn sich der Empfänger bewegt. Abhilfe soll «Wimax Mobile», offiziell bezeichnet als IEEE 802.16e, schaffen – ein Standard, der auch mobile Empfänger bedienen soll. Wimax operiert wie WLAN im Mikrowellenbereich und bedarf bei hoher Leistung einer Konzession. Das Bakom (Bundesamt

* **Simon Wepfer** ist Consultant bei der Security-Spezialistin Oneconsult.

für Kommunikation) hat vor wenigen Wochen begonnen, den Weg für die Vergabe der einschlägigen schweizerischen Konzessionen zu öffnen. Mit der Vergabe ist in der zweiten Jahreshälfte 2005 zu rechnen. Zu diesem Zeitpunkt sollten laut Aussage der Hersteller erste Wimax-Komponenten auf dem Markt sein.

Protokolle für UMTS

HSDPA respektive HSUPA sind von Nokia entworfene Protokollsätze für UMTS. Die Akronyme stehen für High Speed Downlink – respektive Uplink – Packet Access und ermöglichen theoretische Bandbreiten von bis zu 14,4 Mbit/s in Empfangsrichtung und 5,8 Mbit/s in Senderichtung. In von Motorola durchgeführten Feldtests wurde allerdings ein Downlink-Datendurchsatz von 3,6 Mbit/s erzielt.

Da es sich bei HSDPA und HSUPA um reine Protokolle handelt, können die bestehenden UMTS-Netze via Software-Upgrade aufgerüstet werden. Die Protokolle verwenden optimierte Algorithmen zur Codierung und Modulation und verteilen zudem die Netzwerklast. In der Schweiz will die Telekommunikationsanbieterin Orange diesen Standard bereits im nächsten Jahr aufschalten.

Drahtlos auf Kurzstrecken

Für kürzere Distanzen bis wenige hundert Meter eignen sich die Funktechnologien Bluetooth und der Wimax-Vorgänger WLAN. Bluetooth arbeitet in einem global verfügbaren Frequenzband bei 2,4 GHz, was einen gewichtigen Vorteil bezüglich der Kompatibilität bringt.

Seit einigen Monaten sind erste Chips mit dem schnelleren Bluetooth 2.0+ EDR (Enhanced Data Rate) erhältlich.

Diese erlauben einen Nettodurchsatz von 2,2 Mbit/s und sind damit rund dreimal so schnell wie herkömmliche Bluetooth-1.0-Geräte. Der neue Bluetooth-Standard ist abwärtskompatibel. Die Reichweiten hingegen haben sich nicht geändert: Sie bewegen sich je nach Sendeleistung zwischen zehn (Klasse 3) und hundert Meter (Klasse 1).

Potenziell anfälliger

Funknetze lassen sich aufgrund des Übertragungsmediums mit einem passenden Empfänger einfacher ausspionieren als drahtgebundene Netzwerke. Sicherheitsrelevant ist zunächst die Reichweite: So birgt ein aktivierter Infrarot-Port weniger Gefahren als ein ungeschütztes Bluetooth-Gerät. Mit einem modifizierten USB-Dongle und einer Richtfunkantenne ist es gar möglich, ein Handy bei Sichtkontakt aus über 1,5 km Distanz anzusprechen.

Ein WLAN-Access-Point entspricht einem Netzwerkanschluss an der Hausmauer. Die meisten IT-Verantwortlichen haben diese Gefahr realisiert und daher Access Points im produktiven LAN verboten. Kabellose Technologien können aber auch auf andere Weise ein Sicherheitsrisiko darstellen: Die neuen Technologien sind nicht aufzuhalten und durchfluten immer mehr Cafés, Restaurants, Hotels und Bahnhöfe mit Internetanschlüssen.

Ein Problem, das auch die Sicherheitsverantwortlichen betrifft: Intern werden Sicherheitsmassnahmen zwar umgesetzt, doch wie sollen die Sicherheitsbeauftragten für das Netzwerk im Fast-food-Restaurant bürgen? Wer seinen Mitarbeitern nicht das Notebook wegnehmen oder alle Schnittstellen zukleibern will, kann nur auf das Sicherheitsbewusstsein der Benutzer zählen und sich bemühen, die Systeme auf einem aktuellen Security-Niveau zu halten.

Damit ist klar, dass das Vermeiden von Funkstrecken nicht immer eine

praktikable Lösung ist. In diesem Fall ist zu beachten, dass neben der Reichweite auch Authentifizierung und Verschlüsselung eine zentrale Rolle spielen. So lassen sich zum Beispiel verschlüsselte Funkbrücken zusätzlich über Virtual Private Networks (VPN) sichern.

Grenzen des Fortschritts

Der Geschwindigkeitsrausch in den Funknetzen hält an, und solange «High-speed-Junkies» für die mobilen Dienste bezahlen, scheint die Rechnung für die Anbieter aufzugehen, denn immer mehr Datenpakete rauschen durch den Äther. Eine gewisse Ermüdung ist inzwischen trotzdem spürbar: Der Kabelsalat wird einfach durch den Wortsalat ersetzt, den die angekündigten Technologien hinterlassen.

Doch wie viel Bandbreite braucht der Mensch wirklich? Die Vergangenheit hat das Credo aufgebaut: Es steht nie genug Bandbreite zur Verfügung. Macht man indes einen Vergleich mit der Entwicklung im flüchtigen Arbeitsspeicher, dürfte der Bandbreitenhunger jedoch bald einmal gestillt sein und nur noch

kleine Fortschritte machen. Denn der mobile Mensch von morgen wird sich Filme nach wie vor eher im Kino oder zuhause anschauen als auf dem kleinen Handydisplay.

Marktforschungsinstitute orten zudem ein technisches Problem, was die Erfolgchancen der kabellosen Kommunikationsstandards dämpfen könnte: den Energiebedarf der Geräte. Herkömmliche Batterien und Akkus, wie sie in Notebooks und PDA (Personal Digital Assistants) verwendet werden, sind nicht in der Lage, die beispielsweise von Wimax geforderte Leistung über einen längeren Zeitraum hinweg

zu liefern. Bleiben ausserdem die Fragen nach den gesundheitlichen Aspekten. Dass Mikrowellen in der entsprechenden Dosierung tatsächlich für organische Zellen ungefährlich wären, konnte bislang nicht schlüssig bewiesen werden. Tatsache ist jedoch, dass sich Elektrosmog auf die so genannten «Van der Waals»-Kräfte zwischen den Zellen auswirkt. Ein hinlänglicher Beweis für die Schädlichkeit von Elektrosmog ist dies allerdings nicht. Trotzdem: Ob die Antennen-Drahtzieher ihre Installationen auf dem eigenen Hausdach dulden würden, darf bezweifelt werden. □

Die Leistung der Funktechniken im Vergleich

	Bluetooth 2.0+ EDR	WLAN (802.11g)	Wimax	HSDPA
Max. Reichweite (Meter)	100	300	50 000*	wie UMTS
Übertragung brutto (Mbit/s)	3	54	70	14,4
Übertragung netto (Mbit/s)	2,2	12	4,5	3,6
Frequenzband (GHz)	2,4	2,4–2,4835	2–66	2

*bei Sichtkontakt