

DATENÜBERTRAGUNG IN FUNKNETZEN

Maßnahmen zur Qualitätssicherung

Die Datenübertragung per Funk unterscheidet sich fundamental von der in ISDN- oder lokalen Netzen. Denn Funkkanäle sind, bedingt durch die physikalischen Eigenschaften des Übertragungsmediums, nicht als zuverlässige Datenübertragungswege zu betrachten, was sich unter anderem in häufigen Verbindungsabbrüchen äußert. Welche Störeinflüsse in der Luft wirken und welche Ansätze es gibt, um mobile Datenverbindungen "sicherer" zu machen, zeigt dieser Beitrag.

Die Ausbreitung von Funkwellen an der Erdoberfläche wird von einer ganzen Reihe von Faktoren beeinflusst, beispielsweise durch die Topografie oder Bebauung. Bei den quasi optischen Ausbreitungsbedingungen der Funkwellen in den heute genutzten Frequenzbereichen ist der Sichtkontakt zur ortsfesten Antenne ein gewisses wenn auch nicht hinreichendes Qualitätsmerkmal. Reflexionen und Beugungen von Funkwellen ermöglichen den Empfang auch außerhalb eines direkten Sichtbereichs. Die gleichen Effekte führen jedoch auch zu Störimpulsen. In unmittelbarer Umgebung eines Reflexionsminimums sind einfallende und reflektierte Wellen von vergleichbarer Intensität, und die Empfänger demodulieren beide Signale. So entstehen

Empfangsstörungen, die bei digitaler Information durch hohe Bit-Fehlerraten bei der Übertragung gekennzeichnet sind.

Noch plausibler ist die Anfälligkeit des Mediums Datenfunk bei der Betrachtung bewegter Empfänger. Feldstärkenschwankungen führen hier häufig zur vollständigen Signalauslöschung, das heißt zum Verbindungsabbruch, dessen Dauer unter anderem von der Geschwindigkeit des Empfängers abhängt. Funkschatten hinter Gebäuden oder Bäumen sowie der Aufenthalt in Tunneln oder Tiefgaragen bewirken mehr oder weniger lange Unterbrechungen. Aus Sicht der Datenverarbeitung sind Funkverbindungen daher als unzuverlässige Verbindungen zu qualifizieren. Im Moment eines Funkabbruchs

existiert das Netzwerkmedium der Übertragung einfach nicht mehr.

Alltägliche und teilweise nur Minuten andauernde Störungen der Mobilfunkkommunikation sind für übliche LAN-basierte EDV-Anwendungen Katastrophen, die zum Verlust der Applikationsverbindung führen. Alle für den LAN-Einsatz entworfenen Anwendungen gehen davon aus, dass eventuelle kurze Unterbrechungen in der Kommunikation auftreten können, die aber im Sekundenbereich wieder korrigiert sind. So sind die TCP/IP-Protokolle beispielsweise darauf ausgelegt, Verbindungsabbrüche bis zu einem maximalen Ausfall von drei Minuten ohne größere Störung der Anwendung zu behandeln. Danach erfolgt ein unkoordinierter Abbruch der aktivierten Datenübertragung, und inkonsistente Zustände von Datenbanken oder Host-Anwendungen können die Folge sein. Im Gegensatz zu Leitungsnetzen, wo Verbindungsabbrüche äußerst selten sind, kann ein Abbruch der Datenübertragungssession für Mobilfunkanwendungen also nicht akzeptiert werden. In einem Umfeld, in dem die Ausbreitung von Funkwellen die Stabilität der genutzten Datenverbindung bestimmt, führt dieses Verhalten zwangsläufig zu massiven Problemen in der Systembetreuung und natürlich auch in der Abwicklung des aktuellen Geschäftsvorgangs. Die Session muss in diesem Fall logisch aufrechterhalten werden, um ein korrektes Verhalten der beteiligten Programmsysteme zu ermöglichen. Da sich eine Unter-

brechungssituation im Funk meist innerhalb kurzer Zeit von selbst "repariert", ist also nicht von einem Abbruch, sondern lediglich von einem vorübergehenden Defekt auszugehen.

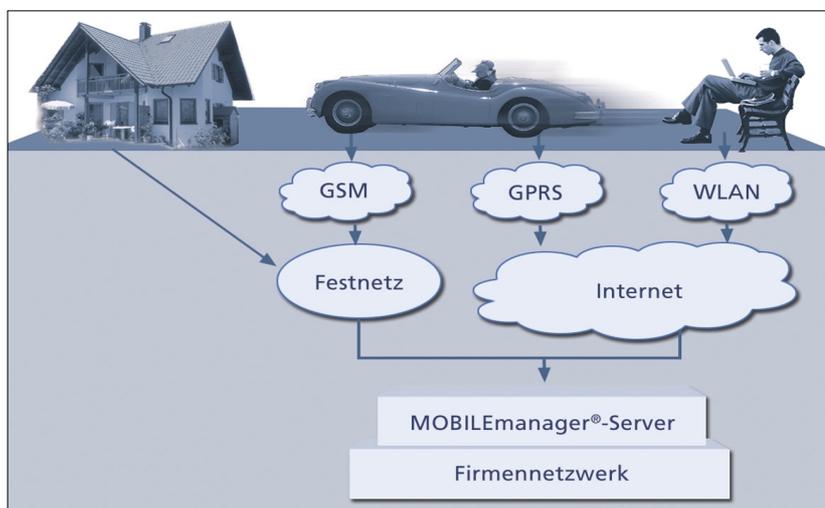
DATENÜBERTRAGUNGSPROTOKOLLE FÜR FUNKANWENDUNGEN Für die GSM-Netzwerkintegration muss daher auch im Funk eine gute Qualität beziehungsweise eine aus DV-technischer Sicht definierte Zuverlässigkeit des Übertragungsdienstes geschaffen wer-

neben einem deutlichen Protokoll-Overhead interne Timeout-Bedingungen für Verbindungsabbruch, Burst-Modus bei Retransmissions sowie fehlende Komprimierungsmöglichkeit für Daten aus integrierten Anwendungen zu nennen. Der Versuch, diese Nachteile auf Treiberebene zu umschiffen, ist ebenfalls nicht effizient, da Komprimierung und Verschlüsselung immer auf dem vollen Datenstrom am effektivsten arbeiten – nicht, wenn Pakete durch Komprimierung nur halbvoll versendet werden. Darüber hinaus

tokollen, ist nur möglich, wenn dieses dynamische Verbindungsmanagement oberhalb der Netzwerkinfrastruktur integriert wird. Dann können die vom Netzwerk bereitgestellten Qualitätsparameter zyklisch ausgewertet und in Optimierungsregeln abgebildet werden.

SCHMALBAND CONTRA BREITBAND

Typischerweise werden die hohen Bandbreiten für den Mobilfunk nicht durch die klassischen Host-Zugriffe mittels Terminalemulation à la IBM-3270 definiert. Vielmehr sind die Anforderungen an die Notwendigkeiten für den Betrieb heute üblicher, datenintensiver LAN-Anwendungen wie zum Beispiel Groupware-Programme, Intranetdienste und Ähnliches, definiert. Gerade an dieser Stelle ergeben sich der Bedarf und die Ansprüche für weitere Steigerungen aus den Möglichkeiten des LANs, und da sind in einem deutlich kleineren Zeitraum, in dem GSM von 9,6 kBit/s auf die mit UMTS zu erwartenden 2 MBit/s aufgerüstet werden wird, im LAN-Umfeld Steigerungen von 10 MBit/s auf Gigabit-Netze zu beobachten gewesen. Die Mobilfunktechnik wird also trotz deutlicher Bandbreitensteigerungen im Vergleich mit dem LAN immer ein Schmalbandmedium bleiben.



Seamless Roaming über verschiedene Medien (zum Beispiel GSM/HSCSD, GPRS, W-LAN, Festnetz) bei Erhaltung der logischen Anwendungs-Session Quelle: adisoft AG

den. Dies geschieht entsprechend dem OSI-Referenzmodell, das mit seiner logischen Schichtenstruktur alle Kommunikationsvorgänge in modernen Architekturen beschreibt, durch ein Transportprotokoll. Ein spezielles Protokoll, das die besonderen Gegebenheiten im Mobilfunk berücksichtigt, ist als Basis für den wirtschaftlichen Einsatz mobiler Techniken daher zwingende Voraussetzung.

Doch leider können die Standard-LAN-Protokolle (TCP/IP und PPP) im Funk nur als Notlösung für Spontanutzer angesehen werden. PPP und TCP sind für zuverlässige und primär breitbandige Medien entworfen. Als Konsequenz sind Verhalten definiert, die im Funk Probleme bereiten: Insbesondere sind hier

wäre eine anwendungsabhängige Konfiguration zweckmäßig, damit zum Beispiel bei Terminalemulationen nicht Pakete mit einzelnen Zeichen verschlüsselt werden, wodurch ein extremer Overhead entstehen würde.

Neben dem Argument der effizienten Paketierung der Dateneinheiten spricht der Faktor der zuverlässigen Verbindung für die Ansiedelung eines auf Funkmedien ausgerichteten Protokolls auf den so genannten höheren Schichten. Eine Trennung der logischen Session, das heißt der eindeutig identifizierte und ununterbrochene Datenstrom eine EDV-Anwendung, von der physikalischen, also dem möglicherweise temporär gestörten Übertragungsmedium und seinen Backbone-Pro-

Als Konsequenz dieser Betrachtung sind für mobile Datenanwendungen Optimierungen des Kommunikationsverhaltens im Sinne von Kosten und Antwortzeitverhalten nahezu unerlässlich. Anwendungen, die nach Murphy dazu tendieren, jegliche bereitgestellten LAN-Ressourcen zu konsumieren, müssen bei der Abbildung in mobile Netzumgebungen diesen eingeschränkten Betriebsbedingungen angepasst werden, um Akzeptanz zu finden. Jeglicher Eingriff in die Applikation verbietet sich dabei von allein. Selbst größte Konzerne werden nicht in der Lage sein, einem der marktführenden Hersteller von Applikationssystemen individuelle Funkadaptionen innerhalb eines überschaubaren Planungszeitraums abzurufen.

MÖGLICHKEITEN Die Möglichkeiten, die von offenen Gateway-Lösungen und -Protokollen geboten werden können, sind sehr eingeschränkt, aber trotzdem wirkungsvoll. Als wesentliche Funktionalität ist dabei die Kompression der Applikationsdaten zu nennen. Erfahrungen zeigen, dass die Reduktion der zu übertragenden Datenmenge je nach Art der Daten im Mittel bei zirka 60 Prozent liegt. Weiterhin ist der Umgang mit dem TCP/IP-Protokoll zu betrachten. Hier sind IP-Header-Kompression und TCP/IP-Spoofing, das heißt das Unterdrücken bestimmten Pakete bei der Datenübertragung, zu nennen. Diese Vorgehensweisen liefern in Abhängigkeit von den eingesetzten Applikationen einen Wirkungsgrad von zirka zehn Prozent gegenüber der nicht optimierten Übertragung.

Weitergehende Mechanismen wie beispielsweise Applikationsdaten-Spoofing sind nicht mehr applikationstransparent

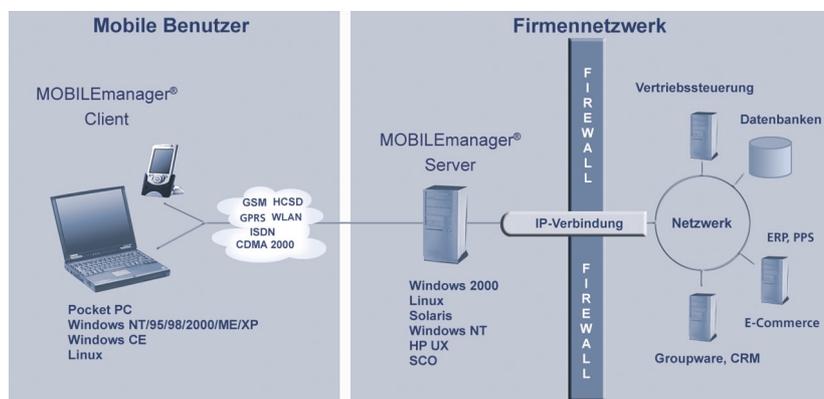
der Ausschluss von Applikationscharakteristika, das heißt exklusive Plattformlösungen, nur bedingt Erfolg haben werden. Während technische Verbindungsfragen im LAN nämlich keinerlei Betrachtung unterzogen werden, stellen Terminalemulationen beim Host-Zugriff (Onlinedialog; häufig sogar mit Zeichenecho durch den Host), Browser (Verbindungsabbau nach Aufbau einer http-Seite) und Datenbank- beziehungsweise Groupware-Anwendungen (mit potenziell längeren Antwortzeiten in der zentralen Verarbeitung der Anfragen) unterschiedliche Anwendungsklassen dar, die im schmalbandigen Remote Access über Mobilfunknetze relevant sind. So wird das Browsen durch Intranetinformatoren deutlich erleichtert, wenn bei Einsatz von GSM/HSCSD oder beim Roaming im GPRS nicht für jede Seite eine neue Verbindung initiiert werden muss. Anders herum betrachtet sind die Leerlaufzeiten des mobilen Anwenders

sind in zukunftsorientierten Gateway-Lösungen vorzusehen.

SICHERHEIT UND ANWENDERUNTERSTÜTZUNG Ein weiterer Aspekt der mobilen Datenkommunikation ergibt sich aus der Komplexität des für Kommunikationsvorgänge involvierten Netzes. Die Verbindung vom Laptop/PDA zum Mobilfunkgerät ermöglicht die Übertragung über die Luftschnittstelle zum GSM- oder WLAN-Betreiber, der dann wiederum eine Verbindung über öffentliche oder geschützte Festnetzverbindungen zum Unternehmen aufbaut, von wo aus eine Intranetverbindung zum Server mit der eigentlichen Applikation aufgebaut wird.

Für einen Anwender und damit eine Problemanalyse durch eine Hotline ist diese Kommunikationsumgebung kaum noch zu erfassen. Die Lokalisierung eines Problems ist daher in der Regel nur noch mit umfangreichen Log-Dateien oder mit technischen Detailkenntnissen beim Anwender möglich. Beide Vorgehensweisen sind im realen Einsatz nicht gegeben oder unpraktikabel. Hier ist an unterstützende Werkzeuge der Anspruch zu stellen, eine einfache Darstellung der Systemzustände, insbesondere hinsichtlich der Verschachtelung der Kommunikationsnetze, zu schaffen.

Die Komplexität und vor allem die verteilte Zuständigkeit von Betreibern für die einzelnen Segmente der Kommunikation zwischen einem mobilen Anwender und der Unternehmensapplikation beinhaltet eine weitere Herausforderung für die mobile Kommunikation: die Sicherheit des Kommunikationswegs gegen Manipulation und Abhören. Heute werden Mobilfunknetze weitestgehend völlig ungesichert für die Datenübertragung eingesetzt. Dieser Fakt leitet sich wahrscheinlich aus der Kenntnis um Verschlüsselungen und Frequency-Hopping-Verfahren auf der Mobilfunkstrecke ab, aber dabei werden die anderen beteiligten Netzsegmente vernachlässigt. Als Konsequenz ist eine Verschlüsselung der



Die Remote-Access-Lösung Mobilemanager von Adisoft bindet externe Arbeitsplätze über unterschiedliche Wege an ein Firmennetz an
Quelle: adisoft AG

und empfehlen sich daher nur in geschlossenen, proprietären Anwendungsumgebungen, die nicht für die Überführung in die neuen Mobilfunknetze oder -dienste vorgesehen sind. Trotzdem ist eine applikationsorientierte Betrachtung der Kommunikationsvorgänge attraktiv für das Mobile Computing. Insbesondere die Analyse des Verbindungsverhaltens der einzelnen Applikationen zeigt, dass

in Dialoganwendungen ein Kostenfaktor, der durch Short-Hold-Mechanismen, die seit Jahren aus ISDN-Umgebungen bekannt sind, in seiner Bedeutung reduziert werden kann. Nach Ablauf eines Inaktivitäts-Timers kann die physikalische Verbindung getrennt und erst bei erneuter Datenaktivität wieder aufgebaut werden. Derart unternehmensspezifische und anwendungsspezifische Anforderungen

Verbindung im Punkt-zu-Punkt-Verfahren zwischen mobilem Teilnehmer und dem adressierten Unternehmen gefordert.

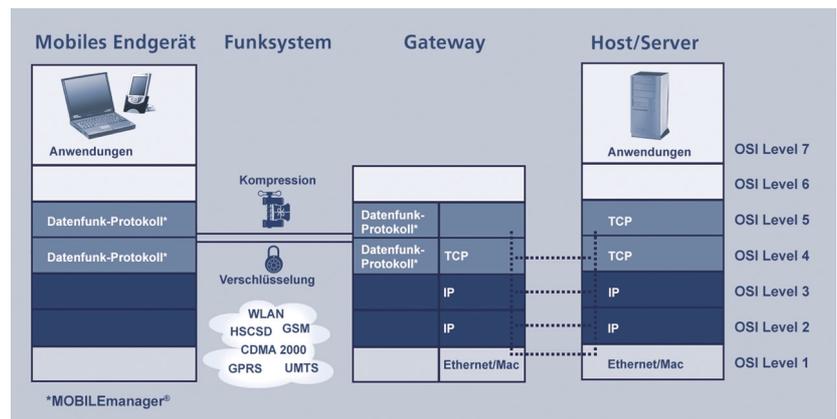
Gerade für Mobilfunknetze der 2,5 Generation (GPRS), 3G (EDGE, UMTS) und 4G (WLAN), wo als Übertragung im Backbone des Netzbetriebs Standardinternetprotokolle zum Einsatz kommen, ist ein solches Verfahren unbedingt erforderlich. Andernfalls werden die Daten bei jedem Übergang in ein anderes Netzsegment unverschlüsselt über öffentliche Netze mit hohem Angriffspotenzial transportiert. In GPRS gilt zum Beispiel, dass die übermittelten Daten und deren Verschlüsselungsmechanismen auf der Luftstrecke am Übergang zum öffentlichen Festnetz terminiert werden. Die Daten liegen danach also unverschlüsselt vor. Hier muss jeder CIO oder CSO Abhilfe schaffen, und diese ist nur mit geschützten Punkt-zu-Punkt-Verbindungen möglich.

EINSATZPRAXIS Wechselnde Arbeitsumgebungen sind ein Merkmal mobiler Anwendungen. Diese Wechsel führen jedoch zu Konfigurationsaufwänden am Endgerät und gegebenenfalls auch an den genutzten Anwendungen, wenn man die zur Verfügung stehenden Netze am jeweiligen Standort optimal für die eigenen Zwecke nutzen möchte. Es hat schließlich wenig Sinn, aus dem Home-Office mit DSL-Anschluss weiterhin GPRS-Verbindungen zu nutzen oder im Flughafen das kostenlose WLAN-Angebot zu ignorieren. Als Konsequenz ist hier eine bislang nicht bekannte Anforderung zu definieren, das so genannte "Seamless Roaming" über verschiedene Medien (zum Beispiel GSM/HSCSD, GPRS, WLAN, Festnetz) bei Erhaltung der logischen Anwendungs-Session.

AUSBLICK Professioneller Einsatz von EDV-Anwendungen im Datenfunk ist per Definition nur dann effizient, wenn kein Medienbruch in der Handhabung verschiedener Funk- und anderer Netze entsteht. Die Kompatibilität des Funkmedi-

ums muss dabei zu LAN-Umgebungen gewährleistet sein, das heißt zur TCP/IP-Socket-Schnittstelle, um Umstellungen der im Einsatz befindlichen und bewährten Applikationen zu vermeiden. Die Probleme der mobilen Datenübertragung sind klassisch im OSI-Sinne durch ein spezifisches Protokoll zu handhaben, das insbesondere eine Dienstgüte ohne Verbindungsabbrüche und das Wiederaufset-

mittels eines solchen spezifischen Gateways für RAS-Anwendungen im Businessumfeld zweckmäßig. So können, dem LAN vorgeschaltet, Funkspezifika effizient unterstützt werden: Zugriffsberechtigung, Short-Hold-Modus, Unterstützung von Mobilfunk und terrestrischen Netzen über eine einheitliche Schnittstelle und Administration. Schließlich ist trotz aller Vorteile niemand aus-



Neben dem Argument der effizienten Paketierung der Dateneinheiten spricht der Faktor der zuverlässigen Verbindung für die Ansiedelung eines auf Funkmedien ausgerichteten Protokolls auf den höheren Schichten des OSI-Modells. Quelle: adisoft AG

zen auf Sessions nach beliebiger Unterbrechungszeit ermöglicht. Als Konsequenz ist für Datenstromübertragungen in Funkmedien ein neues Transport-/Session-Protokoll gefordert, das keine Timeout-basierten Retry-Mechanismen verwendet und eine völlige Entkopplung der logischen Anwendungs-Session von den physikalischen Netzen sicherstellt. Erst wenn zuverlässige Übertragungen auch in unzuverlässigen Medien unabhängig vom Verhalten des Mediums protokolltechnisch gegeben sind, ist der Einsatz mobiler Datenübertragung zukunfts-trächtig. Bisher sind nur wenige Unternehmen weltweit in diesem Bereich so aktiv, dass ein medientransparenter Datenkanal über eine solche Protokollarchitektur genutzt werden kann, unter anderem Adisoft, Easy Access, Fenestrae, Fujitsu Siemens und IBM/Openwave. Grundsätzlich ist die Realisierung der Anbindung an die Mobilfunknetze

schließlich mit mobilen Zugriffen auf Unternehmensnetze tätig. Kosten und Bandbreite der Netze legen einen Wechsel bei entsprechender Verfügbarkeit günstigerer Arbeitsbedingungen nahe. Und wenn auch diese Wechsel anhand der kontinuierlichen Auswertung von Pegelsignalen der einzelnen Netze nach den relevanten Kriterien Kosten, Bandbreite und Sicherheit automatisch erfolgen, dann entfallen bei mobilem EDV-Einsatz zukünftig die Produktivitätskiller, die von Analysten in der aufwändigen Rekonfiguration von Laptops und PDAs bei einem Ortswechsel analysiert werden. Mit entsprechender Systemtechnik ist mobile Datenübertragung genauso unproblematisch zu nutzen wie das Unternehmens-LAN.

(Jörg Hahn/gh)

Dr. Jörg Hahn ist Vorstand Technik bei adisoft AG in Berlin.