Mobiler Datenfunk

Technik der Systemintegration

MOBILE*manager*

von Dipl.-Phys. Rudolf Leibbrand

Inhaltsverzeichnis

Zusammenfassung

Mit Laptop und PC von unterwegs auf Firmendaten zugreifen ist eine Aufgabe, die höchste Anforderungen an Stabilität und Integrität des Übertragungsverfahrens stellt.

Mobilfunkkanäle unterliegen Störungen und Unterbrechungen hervorgerufen durch die Physik der Wellenausbreitung im urbanen Umfeld.

Der Bericht stellt eine Lösung vor - **MOBILE***manager* -,

- die sichere Datenverbindungen im Mobilfunkumfeld garantiert,
- die höchste Sicherheit für Vertraulichkeit und Integrität der Unternehmensdaten garantiert,
- und die mit vorhandener Anwendungssoftware kompatibel ist.

Durch Virtual Private Networking läßt sich die vorgestellte Lösung problemlos in komplexe Remote Access Systeme integrieren.

MOBILE*manager* funktioniert hervorragend mit allen paket- und leitungsvermittelten Mobilfunksystemen. Mit **MOBILE***manager* ausgestattete PCs kommunizieren aber ebenso gut über ISDN–, X.31-, und Modemverbindungen.

Mobiler Datenfunk - Technische Voraussetzungen

Mobile Kommunikation wird zu einem immer wichtigeren Wettbewerbsfaktor im globalen Markt. Schnellere und aktuellere Information, stärkere Kundenbindung und bessere Servicequalität sind die bewegenden Ziele. Effizienter Einsatz mobiler Mitarbeiter und Ressourcen ist das Gebot der Stunde.

Digitale zellulare Mobilfunknetze - primär GSM und GSM 1800 - haben sich in weiten Teilen der Welt durchgesetzt. Ihr Erfolg im Markt für Sprachdienste ist gewaltig. Die Zuwachsraten für neue Teilnehmer sind enorm.

Marketingexperten sind sich einig in der Meinung, daß nach den Sprachdiensten die Datendienste zum großen Erfolg werden. Der Internetboom zeigt deutlich, welche Voraussetzungen erfüllt sein müssen, um mobilen Datenfunkdiensten zum Durchbruch auf breiter Front zu verhelfen.

- Wir brauchen Anwendungen für Menschen unterwegs.
- Wir brauchen sichere, zuverlässige Zugänge zum DV-Netzwerk des Kunden bzw. zum Internet.
- Die Integrität der Unternehmensdaten muß garantiert werden.
- Wir müssen den Anwender vor der Problematik manchmal unzuverlässiger Funkverbindungen in Schutz nehmen.
- Das Übertragungsverfahren soll die Kosten für die grundsätzlich teuren Mobilfunkdienste durch intelligentes Connection Management minimieren.

Mobiles Computing

"Es ist einfacher, billiger und umweltfreundlicher, Informationen anstelle von Menschen zu bewegen."

Heute sind mobile elektronische Post und mobiles Fax die beiden Hauptanwendungen, die weite Akzeptanz finden werden, sowie die Punkte 2 und 3 (siehe oben) gelöst sind. Elektronische Post gibt es in verschiedenen Spielarten. Neben Unternehmenslösungen wie Lotus Notes und Microsoft Exchange müssen öffentliche Systeme wie X.400 und Internet Mail in Mobilfunknetzen unterstützt werden.

Erweitert man die E-mail Systeme um die häufig erforderlichen Datenbankzugriffe und Hostanwendungen, die heute im Unternehmenseinsatz sind, so ergibt sich eine Vielzahl äußert nützlicher Anwendungen für den mobilen Einsatz. Wir brauchen gar nicht auf die mobile "Killer"-Anwendung zu warten. Die Anforderungen für mobiles Computing sind bereits klar definiert, das Marketing für den mobilen Datenfunk kann beginnen.

Die Verfügbarkeit mobiler Datenfunkdienste wird neue Kategorien von Angeboten für den mobilen Menschen stimulieren, die Aktivitäten im Bereich der Navigationsunterstützung, Tourenplanung, und Flottensteuerung sind erste Vorboten.

Wettbewerbsvorteile durch Einsatz mobiler Datenkommunikation

Zeit- und Kostenersparnis bei der Beschaffung aktueller Unternehmensdaten stehen im Mittelpunkt des Interesses bei der Einführung mobiler Datenübertragung. Keine Wartezeiten mehr auf telephonische Informationen - der Auskunftsplatz ist ja meistens besetzt oder nicht erreichbar - keine Fehler mehr, wie bei der mündlichen Übermittlung, sind die Vorteile des mobilen Computing. Und da der Datenaustausch im Vergleich zum Gespräch blitzschnell ist, werden Handygebühren gespart.

Die Mitarbeiter im Außendienst werden also auf mannigfache Weise effizienter:

- durch weniger Wartezeit, weniger nutzloses Telephonieren,
- durch aktuellere, schnellere und präzisere Information,
- durch höhere Qualität bei der Arbeit mit dem Kunden.
- Fahrten, die der Informationsbeschaffung dienen, entfallen.

Der Kunde gewinnt - er wird zufriedener, er wird besser bedient und informiert als je zuvor. Die Kompetenz seines Gesprächspartners und des dahinterstehenden Unternehmens wird ihn überzeugen.

DV-Zugangstechnologie

Die Anwendungsarchitektur eines mobilen Datenfunksystems besteht aus mobilen Client-Anwendungen im GSM-Netz und ortsfesten Server- oder Hostanwendungen im Unternehmensnetzwerk.

Server-Rechner und Hostsysteme befinden sich meist gut geschützt in Unternehmensrechenzentren. Die dort gespeicherten Daten sind vertraulich, und die Sicherstellung ihrer Vertraulichkeit und ihrer Integrität sind für die Unternehmen lebenswichtig. Der Zugriff auf diese Systeme und die dort gespeicherten Daten ist normalerweise strikt überwacht und auf autorisierte Benutzer eingeschränkt. Konsequenterweise erscheint vielen DV-Verantwortlichen der Zugriff auf diese Daten mittels öffentlicher Netze eher als Frontalangriff auf die Sicherheit und Integrität der Unternehmensdaten, denn als neue Dimension der Geschäftstätigkeit.

Konsequenterweise müssen wir zwei zentrale Forderungen an die Zugangstechnologie stellen:

- Die kommunikationstechnischen Voraussetzungen für den Datenübergang aus den GSM-Netzen ins Unternehmens - LAN müssen geschaffen werden.
- Sicherheit und Integrität des Unternehmensnetzes müssen garantiert werden, wenn wir Datennetze von Unternehmen mit öffentlichen Mobilfunknetzen verbinden.

Zur Lösung der reinen Kommunikationsaufgabe gibt es im Markt eine Reihe von Lösungen. Ebenso gibt es Lösungen zur Sicherstellung von Datensicherheit und Datenintegrität d.h. zum Schutz des Unternehmensnetzes gegen unberechtigte Zugriffe.

Firewalls lösen die Sicherheitsprobleme. Sorgfältig administriert können sie zuverlässig zwischen erwünschten Nutzern und unerwünschten Eindringlingen unterscheiden. Sie können ferner alle Transaktionen - insbesondere die unerwünschten protokollieren.

Remote Access Router - insbesondere solche, die neben ISDN analoge Modems bedienen können - sind in mehreren Varianten im Markt verfügbar, um die kommunikationstechnischen Aspekte des Zugriffs auf Unternehmensdaten von unterwegs zu lösen. Besondere Sorgfalt ist bei der Auswahl eines Routers für den Zugang von und zu GSM-Netzen erforderlich. GSM-Netzbetreiber bieten einen ISDN-Zugang mit V.110 Datenratenadaption an, um die GSM-Datenrate von 9600 bps auf die ISDN-Geschwindigkeit von 64.000 bps anzupassen. Bei der Verwendung von Callback gilt es zu berücksichtigen, daß für GSM zwischen Sprachrufnummer und Datenrufnummer unterschieden werden muß.

Der mobile Funkkanal

Als Handybenutzer kennt man die Unzulänglichkeiten mobiler Funkkanäle, die zum gelegentlichen Abbruch eines Gespräches führen. Als Rundfunkhörer ärgert sich jeder über die periodischen Rauscheinbrüche die beim Fahren in bebauten Stadtregionen üblich sind.

Ein terrestrischer Mobilfunkkanal ist eben keinesfalls ein kontinuierliches Medium wie etwa ein Kabel. Er unterliegt Störungen und er ist den Mechanismen der Mehrwegeausbreitung unterworfen, die im urbanen Umfeld keine kontinuierliche Signalversorgung zulassen.

Die Diskontinuität der Mobilfunkkanäle ist der eigentlich neue kommunikationstechnische Aspekt beim Fernzugriff auf Datenbestände. Diese Diskontinuitäten führen zu schweren Bündelstörungen und zum gelegentlichen Übertragungsabbruch. Dieses Phänomen war bei Modem- oder ISDN-Verbindungen nicht bekannt, deshalb mußte das Verhalten der Funkkanäle mit großer Sorgfalt analysiert werden, um eine Lösung zu entwickeln, die den Bedürfnissen moderner EDV-Anwendungen, den Server- und Hostsystemen und schließlich den Anwendern gerecht wird.

Übertragungsprotokolle

In der Welt der Datenübertragung verwendet man sogenannte Protokolle, um mit den Widrigkeiten der Übertragungswege fertig zu werden. Diese Protokolle stellen sicher, daß die am Ziel empfangenen Daten eine originalgetreue Kopie des ursprünglich Gesendeten sind. Es war daher das Ziel, ein für den mobilen Datenfunk geeignetes Übertragungsprotokoll zu entwickeln, welches die Daten-integrität im diskontinuierlichen Mobilfunkkanal sicherstellen kann.

In der Welt der leitungsgebundenen Datenübertragungssysteme hat sich TCP/IP als das mit Abstand am weitesten verbreitete Datenkommunikationsprotokoll etabliert. TCP/IP ist das Übertragungsprotokoll des Internet - praktisch jeder Rechner auf der ganzen Welt kann damit kommunizieren.

Diese Tatsache ist Grund genug für den zunächst naheliegenden Wunsch, auch für die mobile Datenfunkübertragung TCP/IP einzusetzen. Falls dies nicht zufriedenstellend funktioniert, ist zumindest eine

Lösung zu fordern, die mit TCP/IP kompatibel ist. Diese Kompatibilität mit TCP/IP ist erforderlich, um die Vielzahl der für dieses Protokoll entwickelten Software-Anwendungen im mobilen Umfeld einsetzen zu können. Die Nichterfüllung dieser Bedingung würde zu gigantischen, wahrscheinlich prohibitiven Mehrkosten für mobile Datenfunkanwendungen führen - ihre Markteinführung wäre für lange Zeit behindert. Vergessen wir jedoch nicht, TCP/IP wurde für die leitungsgebundene Datenkommunikation entwickelt, d.h. für den Einsatz auf kontinuierlichen Medien.

Zellularer Mobilfunk und TCP/IP

Zunächst soll hier untersucht werden, ob TCP/IP für den Einsatz in mobilen Datenfunksystemen geeignet ist. Dazu dient eine Analyse der Funktionsweise von TCP/IP und seiner Anforderungen an die Leitungsinfrastruktur. Außerdem soll der Frage nachgegangen werden, in wieweit sich ein Transportprotokoll im Mobilfunkumfeld anders verhalten sollte als auf Leitungen.

Strukturen des Internet

Ein Internet ist eine komplexe Struktur bestehend aus Endgeräten (Computer an der Peripherie des Netzes) und Netzknoten. Die Netzknoten sorgen für die Vermittlung oder das Routing von Datenströmen durch die Netzinfrastruktur. Der Datenverkehr kann viele Netzknoten passieren auf seinem Weg von einem Endgerät zu einem anderen. Aufwendige Mechanismen dienen zur Sicherstellung der Integrität der Daten in einem Internet. Sie sollen im folgenden analysiert und auf ihre Tauglichkeit für den Einsatz im mobilen Funk untersucht werden.

Bitfehlerkorrektur

Wenn ein Datenpaket in einem Netzwerk übertragen wird, besteht grundsätzlich immer die Gefahr von Fehlern, die entweder auf einer Übertragungsstrecke oder in einem Netzknoten auftreten können. Sie entstehen meist auf Grund von thermischem Rauschen in elektronischen Bauelementen - allerdings wollen wir uns an dieser Stelle nicht weiter mit Bitfehlerkorrektur befassen, da die Übertragungsprotokolle der unteren Schichten mit diesem Problem normalerweise fertig werden. Dies gilt auch für den GSM-Mobilfunk, wo das RLP-Protokoll zuverlässig Bitfehler korrigiert.

Aus der Sicht der höheren Protokollschichten ist allerdings zu berücksichtigen, daß die Korrektur der Bitfehler Zeit braucht. Die korrigierten Datenpakete kommen also mit Verzögerung ans Ziel. Wie wir später sehen werden, kann diese Verzögerung kritisch werden, wenn sie ein bestimmtes Maß übersteigt.

Die Rolle von TCP

TCP (= Transport Control Protocol) ist das Transportsteuerungsprotokoll der Internet Protokollsuite. Seine Aufgabe ist, sicherzustellen, daß ein von der sendenden Anwendung übergebener Datenstrom zuverlässig bei der empfangenden Anwendung auf dem Zielterminal am anderen Ende des Internet abgeliefert wird. Zuverlässig bedeutet, daß der im Empfänger übergebene Datenstrom eine perfekte Kopie des Originals sein muß, es darf nichts fehlen, es darf nichts verändert sein und es darf nichts hinzugefügt worden sein. (Es darf z.B. nicht passieren, daß auf Grund einer verlorenen Quittung ein Datenpaket dupliziert wird). Ebenso muß die korrekte Reihenfolge der Daten wiederhergestellt werden.

Zur Erfüllung seiner Aufgabe teilt TCP den von der Anwendung übergebenen Datenstrom in IP-Pakete (= Internet Protocol) auf, versieht die Datenpakete mit Ziel- und Absenderadresse, numeriert sie, führt eine CRC Prüfung aus und hängt die CRC - Information an das jeweilige Datenpaket an. Mit diesen Informationen versehen kann jedes IP-Datenpaket im Internet eindeutig identifiziert und auf seine Integrität geprüft werden.

Es ist wichtig, zu verstehen, daß TCP eine größere Anzahl von IP-Datenpaketen hintereinanderweg versendet ohne auf eine Empfangsquittung zu warten. Diese Anzahl wird Fenster genannt; sie ist ein kritischer Parameter für die optimale Funktion von TCP in einem komplexen Netzwerk.

Das empfangende TCP schickt eine Quittung an den Absender. Diese Empfangsquittung enthält u.a. die Nummer des ursprünglichen Pakets, so daß das sendende TCP im Laufe der Übertragung genau informiert wird, welche Pakete erfolgreich übertragen wurden. War der ursprüngliche Datenstrom umfangreich, so durchqueren Datenpakete und Quittungen gleichzeitig und unabhängig voneinander

das Netz. So wird sichergestellt, daß TCP einen hohen Datendurchsatz in einem komplexen, weltweiten Netz erzielt , wo die Zeit zwischen dem Senden eines bestimmten Datenpakets und dem Empfang der dazugehörenden Quittung sehr lang sein kann. Diese Zeit wird Latenz genannt.

Verhalten von TCP im Fehlerfall

Wenn die dem aktuellen Fenster entsprechende Latenzzeit ohne Empfang einer Quittung verstrichen ist, d.h. nach dem Versand der in TCP voreingestellten Anzahl Datenpakete, hält TCP die Übertragung an. Das sendende TCP unterstellt dann, daß irgendwo in der Übertragungskette ein oder mehrere Pakete verloren gegangen sind, und wiederholt sämtliche Datenpakete mit einer Laufnummer größer als die des letzten quittierten IP-Pakets.

TCP garantiert einen optimalen Datendurchsatz durch die automatische Anpassung von Fenstergröße und Wiederholverzögerung an den Datendurchsatz des Netzes und die Latenzzeit. Ist das Fenster zu klein, dann verschenkt TCP Datendurchsatz d.h. es nützt die gegebene Bandbreite schlecht aus. Ist das Fenster zu groß, dann kann TCP nicht schnell genug auf Netzfehler reagieren, was ebenso zu verschenktem Datendurchsatz führt. TCP überwacht und analysiert daher ständig den Daten- und Quittungsverkehr, um die Parameter für Fenstergröße und den Retry-Timer optimal zu justieren. TCP zeigt seine beste Leistung, wenn Durchsatz und Latenz über einen größeren Zeitraum konstant bleiben!

Ein weiterer wichtiger Parameter ist der Verbindungs-Time-Out von TCP. Nach einer bestimmten Anzahl von Wiederholungen ohne Quittungen unterstellt TCP, daß die Verbindung zum entfernten Endgerät nicht mehr existiert bzw. daß das entfernte Endgerät ausgeschaltet wurde. TCP beendet dann die Übertragung mit einer Fehlermeldung an die Anwendung. Die Anwendung ihrerseits wird dann den Benutzer des Endgerätes über den Verbindungsausfall in Kenntnis setzen.

Ausbreitung der Funkwellen

Funkfelder, die sich entlang der Erdoberfläche ausbreiten, zeigen drei charakteristische Bereiche. Zunächst gibt es die Zone der kontinuierlichen Funkversorgung, die immer gegeben ist, wenn sich Mobilantenne und Feststationsantenne sehen können bei gleichzeitiger Abwesenheit reflektier-ender Flächen. Das andere Extrem ist die Zone ohne Versorgung auf Grund von Abschirmung (z.B. unter Grund oder in Stahlbetongebäuden) oder wenn die Entfernung zur nächsten Feststation zu groß ist. Die flächenmäßig größte Zone schließlich ist die, wo sich auf Grund von baulichen Hindernissen die Antennen nicht sehen können, wo aber auf Grund von Reflexionen genügend Feldstärke zur Übertragung der Informationen vorhanden ist. Diese Zone ist charakterisiert durch wild schwankende Pegel und Übertragungsqualität, kurze Unterbrechungen und durch kurzzeitige extrem hohe Bitfehlerraten.

Inkompatibilität von TCP und Mobilfunkkanal

Wenn diese Bitfehler in der fluktuierenden Zone korrigiert sind, - das RLP Protokoll des GSM-Systems leistet dies zuverlässig - ergibt sich ein Datenfunkkanal mit extrem stark variierendem Durchsatz und entsprechend variabler Latenz. Durch zusätzlich auftretende, gelegentliche Verbindungsabbrüche mit Wiederaufbauzeiten zwischen 20 und 60 Sekunden werden diese Variationen von Durchsatz und Latenz zusätzlich vergrößert.

Bedenkt man, daß die Latenzzeit in GSM-Systemen bei kontinuierlicher Funkversorgung bei rund 1 Sekunde liegt, dann ist leicht einzusehen, daß der mobile Funkkanal nur sehr schlecht mit TCP/IP harmoniert. Die oft sprungartige Variation der Latenzzeit zwischen 1 und ca. 60 Sekunden provoziert unnötige Paketwiederholungen und TCP-Verbindungsabbrüche in der Zone mit diskontinuierlicher Funkversorgung bis zu dem Punkt, wo TCP kontraproduktiv wird. Es wird einen sehr schlechten Durchsatz realisieren und gegebenenfalls auf Grund seiner internen Timer Verbindungen abbrechen, anstatt für ihre Integrität zu sorgen. Überdies tragen überflüssige Paketwiederholungen dramatisch zu Verbindungsdauer und -kosten bei.

Es gibt also genügend Motivation, über neue Lösungen nachzudenken.

MOBILE*manager* **- Transport Protokoll für mobile Datenfunksysteme**

Die Überlegungen der vorhergehenden Kapitel und die daraus gezogenen Konsequenzen führten zur Entwicklung des Transport Protokolls für mobile Funksysteme - **MOBILE***manager*.

Dieses Protokoll funktioniert ohne die beschriebenen Time-Out / Retry Mechanismen von TCP/IP und vermeidet dadurch dessen Schwierigkeiten mit dem stark fluktuierendem Funkkanal.

Die automatischen Wiederanwahleigenschaften von **MOBILE***manager* in Verbindung mit einem intelligenten Short-Hold-Mode stellen die optimale Datenübertragung selbst unter schwierigsten Funkbedingungen sicher.

MOBILE*manager* ist mit einer Standardschnittstelle ausgestattet und verhält sich aus der Sicht der Anwendung exakt wie TCP/IP. Alle Anwendungen, die normalerweise mittels TCP/IP im Internet kommunizieren, funktionieren einwandfrei zusammen mit **MOBILE***manager*.

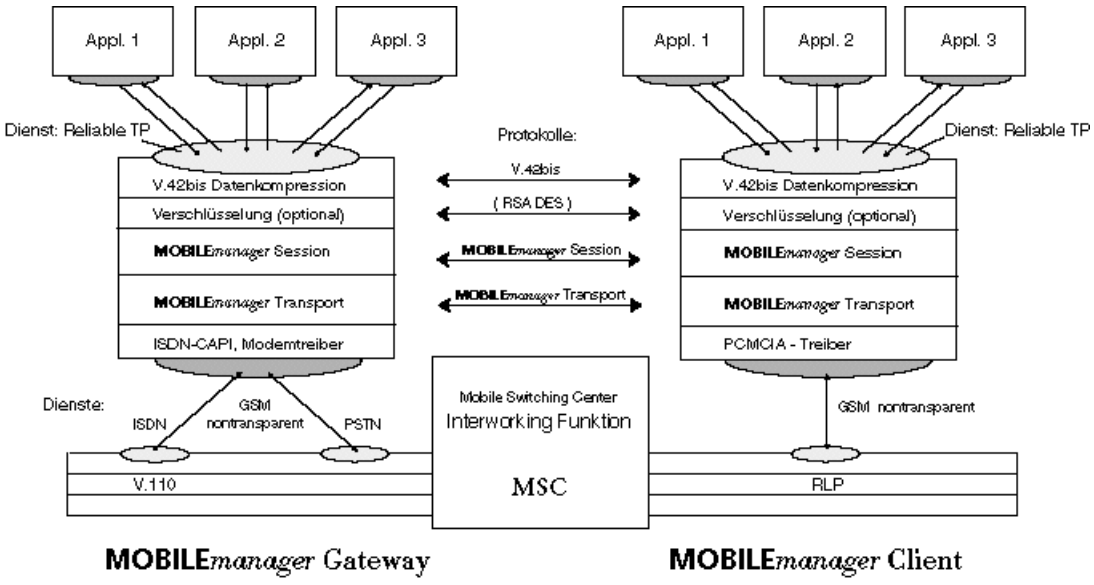

Abbildung 1: OSI-Darstellung des **MOBILE***manager* Protokolls für GSM mit optionaler Verschlüsselung

Kompatibilität mit TCP/IP

MOBILE*manager* ist ein hochspezialisiertes Transport Protokoll für den Mobilfunkkanal und seine diskontinuierlichen Übertragungsmechanismen. Die Kompatibilität und die Connectivity zum TCP/IP Protokoll des Internet wird durch zwei Maßnahmen sichergestellt.

- **MOBILE***manager* verwendet dieselbe Anwendungs-Programmierschnittstelle wie TCP/IP: Windows Sockets. Deshalb können alle Anwendungen, die für die Verwendung von Windows Sockets mit TCP/IP entwickelt sind, problemlos mit **MOBILE***manager* zusammenarbeiten. Es ist dies die überwältigende Mehrzahl aller Anwendungen.
- Am Eingang in das Unternehmensnetzwerk (oder ins Internet) wird ein Store-and-Forward Gateway eingesetzt. Dieses Gateway läßt Daten transparent aus TCP/IP in **MOBILE***manager* und umgekehrt passieren. Das Gateway ist für Anwendungen vollkommen transparent. Die mobilen Client-Anwendungen und die Server-Anwendungen im LAN kommunizieren miteinander ohne die Anwesenheit des Store-and-Forward Gateway zu bemerken.

Systemsicherheit mit **MOBILE***manager*

Die Systemsicherheit bei der Einbindung mobiler Teilnehmer in firmeninterne DV-Netze mittels **MOBILE***manager* wird durch mehrere Maßnahmen zur Teilnehmeridentifikation und durch ein Application Firewall sichergestellt.

Teilnehmeridentifikation

Autorisierte Teilnehmer werden auf drei Arten identifiziert.

- Bei jeder Verbindung (und Wiederwahl) wird der Softwareserialisierungsschlüssel übertragen und geprüft. Dies geschieht auch nach jedem funkbedingten Verbindungsabbruch.
- Falls die Verbindung über ISDN erfolgt, kann die Nummer des anrufenden Mobil-Teilnehmers durch das **MOBILE***manager* Gateway geprüft werden. Optional kann mit der ISDN-Teilnehmeridentifizierung und Rückruf gearbeitet werden (Callback). Allerdings ist zu beachten, daß sich GSM-Handies immer an Hand ihrer Sprachrufnummer identifizieren, während für den Rückruf die Datenrufnummer zu verwenden ist.
- Das **MOBILE***manager* Gateway kann die IMEI-Identifikation des mobilen Telefons überprüfen, falls diese auf der Mobilseite softwaremäßig zugänglich ist.

Application Firewall

Das **MOBILE***manager* Gateway beinhaltet einen Application Firewall. Jeder Zugriff eines autorisierten Mobilteilnehmers (siehe oben) auf einen Server und eine Anwendung im Unternehmensnetz muß explizit freigeschaltet werden. Das heißt: Es gibt im **MOBILE***manager* Gateway eine Datenbank, die für jeden berechtigten Anwender exakt festlegt, zu welcher Anwendung auf welchem Rechner er Zugang hat. Auf andere Dienste im Netz kann er von außen nicht zugreifen. Nicht autorisierte Teilnehmer erhalten gar keinen Zugriff. Unberechtigte Zugriffsversuche werden protokolliert.

Das Application Firewall besteht aus einem Store and Forward Gateway, welches oberhalb von zwei vollkommen unterschiedlichen Protokollstacks angeordnet ist: **MOBILE***manager* stellt die Verbindung zur mobilen Funkwelt her; auf der LAN- oder Internet-Seite befindet sich ein Standard TCP/IP Stack. Jede Information, die von einem mobilen Teilnehmer kommt, muß zwangsläufig den **MOBILE***manager*-Stack benutzen. Andere Protokolle sind über den Mobilfunk-Netz-zugang nicht erreichbar. Der Versuch mit irgend einem anderen Protokoll über den Mobilfunkzugang arbeiten, ist zum Scheitern verurteilt.

Da gleichzeitig keine andere Maschine im Unternehmensnetz das **MOBILE***manager* Protokoll kennt, gibt es auch keine Möglichkeit das Firewall Gateway mit Hackertricks zu umgehen. Nur ordnungsgemäß autorisierte und identifizierte Teilnehmer können das **MOBILE***manager* Gateway passieren und mit den für sie freigegebenen Anwendungen im Netz arbeiten.

Wirtschaftlichkeit

Im Umgang mit GSM Funknetzen kann man bekanntlich auf 2 Arten sparen

- man wählt den richtigen Netzzugang, ISDN Datenzugänge sind wesentlich günstiger als Modemzugänge (weil im ISDN keine Modemsynchronisationszeiten bezahlt werden müssen), Funk zu Funk Verbindungen sind günstiger als Funk - Draht Verbindungen; bei großen Teilnehmerzahlen ist die Verwendung von ISDN-Festverbindungen zum GSM-Netz empfehlenswert (Corporate Link),
- und man fasse sich kurz. Vor allem während Datenverbindungen gibt es häufig Übertragungspausen, z.B. während der Bediener seinen Bildschirminhalt bearbeitet. Ein gutes Übertragungsverfahren erkennt solche Denkpausen und legt auf. Dieser Short Hold Modus läßt sich bei **MOBILE***manager* beliebig konfigurieren um den Gegebenheiten einzelner Applikationen optimal gerecht zu werden.

Netzzugang für das Gateway

In der Vergangenheit haben wir die **MOBILE***manager* Gateways immer über Draht, vorzugsweise über ISDN an die Überleiteinrichtungen der GSM Netzbetreiber angeschlossen. Für große Installationen wird das auch in Zukunft der vorzuziehende Weg sein, insbesondere seit die Netzbetreiber kostengünstige ISDN Standleitungen für den Zugang zur Verfügung stellen.

Netzzugang über Funk

Für kleinere Installationen (bis zu einigen Dutzend Teilnehmer) kommt aber auch der direkte Zugang über das GSM-Netz in Betracht. Die Übertragungsgebühren halbieren sich dadurch ungefähr. Der Nachteil dieser Funkanbindung ist darin zu sehen, daß gegebenenfalls sämtliche Funkgeräte einer Funkbasisstation in derselben Zelle eingebucht sind. Das kann zu Besetztzuständen führen. Außerdem können sich Störungen der Zelle auf den gesamten Datenverkehr auswirken.

Für den Funkanschluß des Gateways ist eine spezielle Datenfunkbasisstation erforderlich bei der sämtliche Funktionen bis hin zur Eingabe der PIN - Nummer durch den Gateway-Rechner erledigt werden.

Netzzugang über ISDN Standverbindung

Die GSM Netzbetreiber D1 und D2 bieten datentaugliche ISDN Standverbindungen zu ihren Überleiteinrichtungen an. Die Kosten für solche ISDN Standverbindungen variieren natürlich mit dem Abstand des Kunden zur nächsten Netzbetreibereinrichtung. Es ist also erforderlich genau zu klären, welche derartige Einrichtung am nächstgelegenen ist. Der Vorteil dieses Zuganges ist, daß auch hier der netzinterne Tarif gilt. Selbstverständlich profitieren auch die Sprachverbindungen zwischen dem Unternehmen und seinen Mitarbeitern von diesem kostengünstigen Netzzugang.

Der Betrieb eines Datenfunksystems im Callback-Modus führt auf Grund der kurzen Verbindungszeiten (es wird in Datenpausen aufgelegt) dazu, daß aus der Sicht des **MOBILE***manager* Protokolls von der ortsfesten Seite her ein Warteschlangenbetrieb möglich ist bei dem keine Besetzt-Zustände vorkommen. Wartezeiten sind für das **MOBILE***manager* Protokoll unschädlich. Den Vorteil hat der Kunde. Er kann mit weniger Standleitungen auskommen im Vergleich zu dem Fall wo sämtliche Datenverbindungen vom Mobilgerät aufgebaut werden.

MOBILE*manager* und Virtual Private Networking

Virtuelle private Netze

Virtuelle private Netzwerke (VPN) sind logische Konstrukte, die es ermöglichen, in öffentlichen, verbindungslos arbeitenden Netzen (z.B. IP-Netzen), geschützte geschlossene Benutzergruppen zu realisieren, deren Datenaustausch von fremdem Datenverkehr isoliert und vertraulich bleibt. Dabei sieht der Teilnehmer der geschlossenen Benutzergruppe den fremden Datenverkehr nicht. Sein eigener Datenverkehr kann von unerwünschten Fremden nicht mitgelesen werden. Logisch gesehen verhält sich das virtuelle private Netzwerk wie ein eigenes Netz. Sein Vorteil liegt darin, daß sich die Netzkosten auf viele andere Nutzer aufteilen, d.h. die Vorteile beim Einsatz von VPN liegen überwiegend im Bereich der Wirtschaftlichkeit.

So läßt sich auch über das Internet weltweit ein VPN realisieren, bei dem einerseits eine sehr gute Wirtschaftlichkeit, andererseits eine sehr hohe Vertraulichkeit der privaten Daten realisieren läßt.

Vorteile virtuelle privater Netze

Zu den weiteren Eigenschaften virtueller privater Netzwerke gehört die Tatsache, daß auch die Adressen der geschlossenen Benutzergruppe dem öffentlichen Netz gegenüber verborgen werden können. Dies hat viele Vorteile:

- private Adreßräume können verwendet werden,
- einem fremden Angreifer bleibt die Adresse eines VPN-Teilnehmers verborgen, ein Angriff ist damit kaum möglich,
- bei Mobilität einzelner Teilnehmer zwischen LAN und WAN kann seine IP-Adresse beibehalten werden,
- schließlich kann mit Hilfe des VPN-Ansatzes fast jedes beliebige Kommunikationsprotokoll im Internet übertragen werden; - die Beschränkung auf IP fällt weg - auch im Internet.

Damit sind die Voraussetzungen erfüllt, um auch **MOBILE***manager* über öffentliche IP-Netze zu übertragen. Dabei werden weder die hohe Sicherheit des **MOBILE***manager* Protokolls hinsichtlich der Vertraulichkeit der Daten noch seine Eigenschaft der hohen Verbindungssicherheit über mobile Funkkanäle in irgendeiner Weise angetastet.

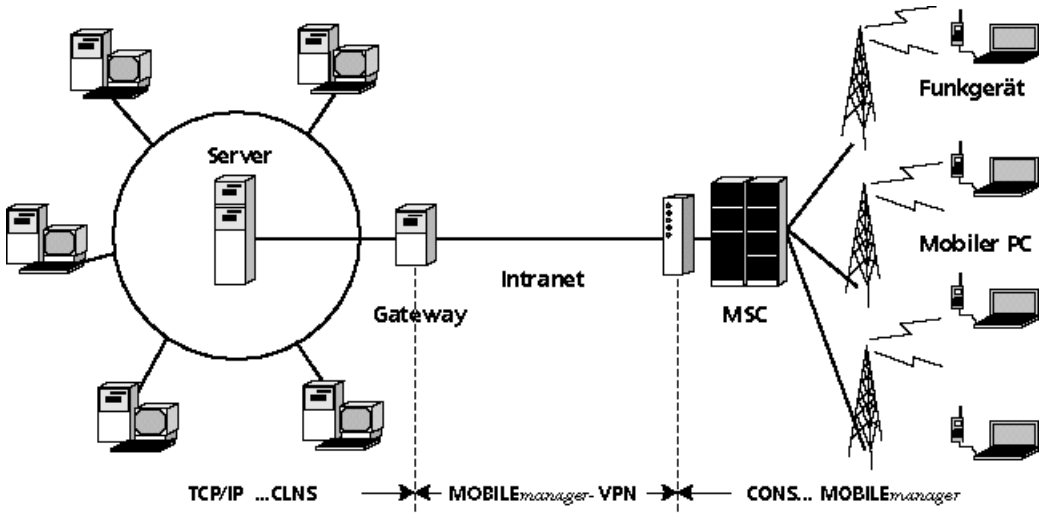

Abbildung 2: **MOBILE***manager* Systemintegration mittels einer VPN - Verbindung

Systemkomponenten für das MOBILE*manager* VPN

MOBILE*manager* Client und **MOBILE***manager* Gateway werden ohne Modifikation für VPN eingesetzt. Durch Multihoming im Gateway wird das öffentliche und das private IP-Netz logisch getrennt. Der einzelne **MOBILE***manager*-Systemadministrator hat alle Konfigurationsmöglichkeiten für **MOBILE***manager* zur Verfügung. Er kann insbesondere die Zugriffsrechte für jeden einzelnen Anwender frei vergeben. Die Tatsache, daß der **MOBILE***manager* Server über eine VPN Verbindung am GSM- oder ISDN Netz hängt führt zu keinerlei Einschränkung in der Konfigurierbarkeit des **MOBILE***manager*-Gateway. Kundensysteme können mit privaten IP-Adreßräumen arbeiten. Eine Koordination der Adreßräume unterschiedlicher VPN-Benutzer ist nicht erforderlich.

GSM-Netzübergang

Der GSM Netzübergang in das IP-Netz mit überlagertem VPN wird realisiert mittels eines transparenten, V.110-fähigen ISDN Routers, welcher **MOBILE***manager*-Pakete transparent in IP-Pakete verpackt. Es gibt auf dem Markt mehrere Fabrikate solcher Router die hier ohne Modifikation eingesetzt werden können.

Der ISDN Router, der z.B. im Bereich eines Service Providers angesiedelt sein kann, bietet alle üblichen Methoden der Zugangskontrolle, insbesondere CLI, so daß der Service Provider seinerseits prüfen kann, daß nur berechtigte Kunden seinen Router benützen. Die üblichen Abrechnungsmethoden funktionieren weiter. Der Datenfunk Service Provider braucht kein eigenes **MOBILE***manager* Gateway.

Aus der Sicht des Endkunden bietet sich als weiterer Vorteil die Tatsache, daß **MOBILE***manager* Pakete transparent über den ISDN Router geleitet werden ohne eine Dekodiermöglichkeit für diese Pakete auf dem Router. Selbst durch Manipulation am Router können **MOBILE***manager* Nachrichten nicht in ihrer Vertraulichkeit beeinträchtigt oder gar mitgelesen werden. Der Status eines " Trusted Server " ist für den Router nicht erforderlich.

Falls **MOBILE***manager* mit Verschlüsselung eingesetzt wird, werden die verschlüsselten **MOBILE***manager*-Pakete ebenso transparent über den ISDN-Router geleitet ohne ihre Sicherheit zu kompromittieren.

Der gleiche Router kann auch für den Übergang von ISDN zum **MOBILE***manager* VPN verwendet werden. Diese Konfiguration ist immer dann besonders sinnvoll, wenn Gebühren gespart werden sollen durch die strategische Plazierung von Routern in Ortsnetzen.

Schlußfolgerung

Die **MOBILE***manager* Kombination aus optimiertem Funkprotokoll und Application Firewall bietet dem Benutzer exakt die mobile Netzzugangslösung wie wir sie eingangs gefordert haben:

- **MOBILE***manager* löst die Kommunikationsprobleme des mobilen Datenfunks.
- **MOBILE***manager* löst die Sicherheitsprobleme für den mobilen Netzzugang.
- **MOBILE***manager* befreit den Benutzer von der Unannehmlichkeit seine Anwendung nach jedem Funkloch neu starten zu müssen. Es vermeidet die hiermit verbundenen Kosten.
- **MOBILE***manager* senkt Verbindungkosten durch intelligent konfigurierbaren Short Hold Mode.

MOBILE*manager* nutzt den Funkkanal optimal aus. Optimierter Datendurchsatz kombiniert mit einem intelligenten Short-Hold-Modus spart dem Anwender Verbindungszeit. Eine Datenverbindung wird nur hergestellt, wenn wirklich Daten übertragen werden. In den Pausen - wenn der Anwender Nachrichten liest oder schreibt - wird aufgelegt ohne die logische Verbindung abzubauen.

MOBILE*manager* ist somit eine zuverlässige, sichere und wirtschaftliche Lösung für den mobilen Zugriff auf Unternehmensdaten über GSM- und andere Funksysteme.

Anschriften:

BEROTRONIKA SYSTEME GMBH
Ostpreußendamm 67
D-12207 Berlin
Telefon: 030 7079010
Telefax: 030 70790155

BEROTRONIKA SYSTEME GMBH
Kreuzberger Ring 64
D-65205 Wiesbaden
Telefon: 0611 977140
Telefax: 0611 9771450