Ortsbezogene mobile Dienste über heterogene Netze

Teil 1

Michael Angermann • Jens Kammann • Frank Kühndel
Patrick Robertson • Thomas Strang • Kai Wendlandt

Ortsbezogene Mobilfunkdienste haben in den letzten Jahren deutlich an Bedeutung gewonnen. Ihre Entwicklung wird zunehmend durch den Aufbau neuer allgemeiner Dienste-Plattformen unterstützt. Das System Heywow ist eine dieser Plattformen und wird vom DLR zusammen mit anderen Unternehmen und Einrichtungen entwickelt.

Das Heywow-System nutzt vor allem die Programmierbarkeit von Endgeräten und die implizite Ortung durch die Verwendung von Funksystemen wie Bluetooth. Die dabei auftretenden Fragen hinsichtlich der Nutzung heterogener Netze, Bereitstellung kontextbezogener Dienste, Sicherheit und Personalisierung machen den hohen Grad an Forschungsarbeiten in diesem Projekt deutlich.

Die Motivation und Entwicklung neuer mobiler Plattformen wurde durch drei in den letzten Jahren rasch fortschreitende Techniken und Tendenzen geprägt. Erstens beschränkte sich die Nutzung mobiler Endgeräte wie Mobiltelefon oder Personal Digital Assistent (PDA) – neben der klassischen Telefonie – im Datenbereich bisher auf den Online-Zugang zu Internetportalen über das Wireless Application Protocol (WAP) oder dem Austausch von E-Mail. Dies ändert sich mit der Einführung der neuesten Generation von Mobiltelefonen, die selbst nicht nur ein Terminal, sondern auch eine „computing platform" darstellen, und durch den Anwender oder durch Drittanbieter programmiert werden können.

Zweitens haben sich parallel zur klassischen Mobilfunkwelt Funksysteme mit kurzer Reichweite, aber hoher Bandbreite zur Reife entwickelt. Als wichtigste Beispiele seien Funk-LAN (Wireless LAN) nach IEEE 802.11 und Bluetooth genannt. Durch deren Integration mit Mobilfunksystemen eröffnen sich neue Möglichkeiten.

Drittens ist die geografische Ortung eines menschlichen Nutzers immer einfacher und kostengünstiger, was die rasche Verbreitung ortsbezogener Dienste – so genannter Location Based Services (LBS) – mit sich bringen wird. Die Kombination dieser drei Tendenzen erfordert eine Entwicklung geeigneter mobiler Informationsplattformen. Traditionelle Architekturen und Anwendungen sind nicht in der Lage, den geänderten Randbedingungen und Möglichkeiten gerecht zu werden, da sie z. B. Unterbrechungen der Netzverbindung in den meisten Fällen nicht tolerieren.

Dieser Übersichtsbeitrag gliedert sich zunächst gemäß der oben genannten drei Punkte: Nach einer Einführung in kontextsensitive Dienste und deren Repräsentation auf programmierbaren Endgeräten folgt ein Kapitel über Sicherheitsanforderungen der Verarbeitungsplattformen und geeignete Lösungsansätze hierzu. Dann folgt im zweiten Teil (im nächsten Heft) ein Abschnitt über die Verwendung heterogener Netze und insbesondere über die Verwendung so genannter Local Service Points (LSP) zur Informationsverbreitung in räumlich sehr kleinen Gebieten. Im Anschluss wird das Soft-Location-Prinzip (SoLo) zur Kombination verschiedener Positionierungsquellen eingeführt. Insbesondere in mobilen Anwendungen charakterisiert der momentane Aufenthaltsort die Situation eines Benutzers bereits relativ gut. Eine weitere Steigerung von Komfort und Effizienz lässt sich jedoch mit einer Generalisierung zu so genannten „Situation Aware Services" erreichen.

Auf einen Blick

Im Heywow-Projekt werden verschiedene neuartige Techniken untersucht, die für die Entwicklung ortsbezogener Mobilfunkdienste benötigt werden. Dazu gehören Aspekte der Programmierbarkeit mobiler Endgeräte, heterogene Netzverbindungen sowie die Bereitstellung kontextsensitiver Dienste.

Kontextsensitive Dienste auf mobilen Endgeräten in Heywow

Wie bereits betont, hat die Einführung programmierbarer Mobiltelefone wie z. B. dem Motorola-Modell Accompli 008 oder dem Siemens-Modell SL45i neue Möglichkeiten für Dienste und Dienstepattformen erlaubt. Derartige Geräte stellen nicht nur die Funktionen eines Terminals dar, sondern dienen als „computing platform". Hierzu wurde eine Variante der plattformübergreifenden Programmiersprache Java standardisiert, die in der Java2 Micro Edition (J2ME) speziell auf die Fähigkeiten und Einschränkungen mobiler Endgeräte abgestimmt wurde [1]. Dabei werden die verschiedenen Gerätetypen über Konfigurationen und Profile abgebildet, wobei Mobiltelefone und PDA als Geräte der kleinsten Leistungsklasse mit der „Connected Limited Device Configuration" (CLDC) und dem Mobile Information Device Profile (MIDP) abgedeckt werden, Tabelle 1.

In Heywow wird diese neue Fähigkeit, Programme auf dem Endgerät aus-

zuführen, vielfältig genutzt. Einerseits ermöglicht sie das Weiterarbeiten mit Diensten auch für den Fall, dass keine Online-Verbindungen möglich (z. B. auf Grund fehlender Netzabdeckung) oder erlaubt sind (z. B. im Flugzeug). Andererseits sorgen einige Heywow-Basisdienste auf dem Endgerät im Hintergrund dafür, dass dem Anwender stets aktuelle, personalisierte und auf die jeweilige Situation des Benutzers abgestimmte Informationen zur Verfügung stehen. So wird etwa eine Anwendung für Routenplanung auf dem Endgerät mit Verkehrsinformationsdiensten abgeglichen, ohne dass der Anwender aktiv in diesen Prozess eingreifen muss. Auch im Bereich Sicherheit ist die Programmierbarkeit der Endgeräte von großem Vorteil. So wird hierdurch (im Gegensatz zu WAP) eine Ende-zu-Ende Verschlüsselung auf dem Gerät ermöglicht.

Die Liste der zur Verfügung stehenden Diensten ändert sich häufig durch einen Kontextwechsel. Diese hohe Dynamik der jeweils verfügbaren Dienste wird in einem Diensteverzeichnis – Advanced Mobile Service Registry (AMSR) – verwaltet, das auf dem jeweiligen Endgerät läuft, Bild 1. Hier werden Dienstanfragen unter Verwendung von Kontextinformationen auf die jeweiligen Dienstangebote abgebildet. Kontext ist in diesem Sinne „jede Information, die dazu benutzt werden kann, die Situation einer Entität zu charakterisieren. Eine Entität ist eine Person, ein Ort oder ein Objekt, die als relevant bezüglich ... [einer Dienstnutzung] angesehen wird“ [2]. Dienste, die dabei auf den aktuellen Aufenthaltsort als Kontextinformation zurückgreifen, werden auch unter dem Oberbegriff Location Based Services (LBS) geführt.

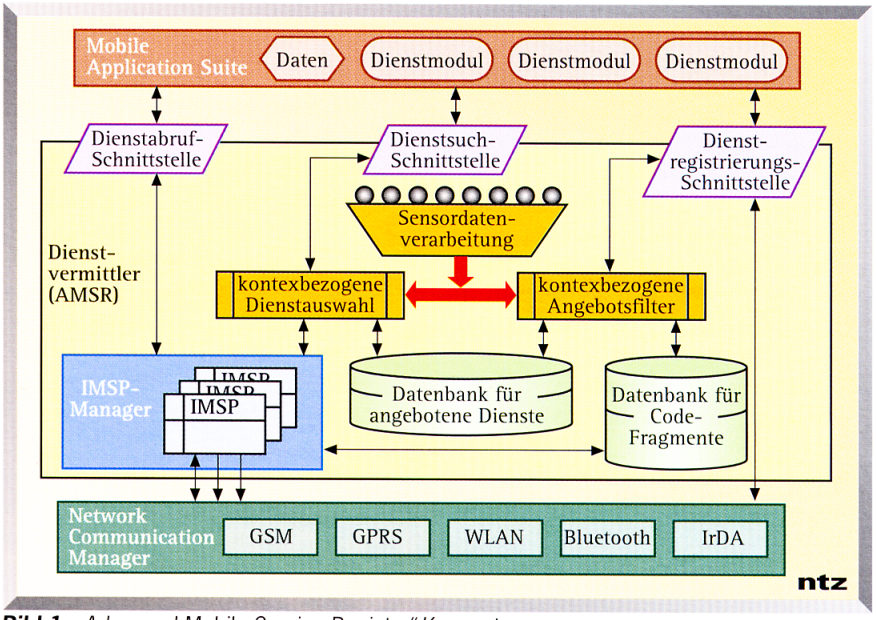

Bild 1. *„Advanced Mobile Service Registry“-Konzept*

Zur Ermittlung des aktuellen Kontexts dienen im Endgerät softwaregestützte Kontextsensoren (CS). Jeder dieser Sensoren ist für die Erfassung eines individuellen Typs von Kontextinformation durch Beobachtung einer Entität verantwortlich, und eine Menge unabhängiger Kontextsensoren definieren die so genannte Situation, in der sich ein Benutzer oder eine Anwendung gerade befindet. Kontextsensoren weisen in ihrer Art große Ähnlichkeiten mit Software-Agenten [3] auf (hoher Grad an Individualität, Anpassungsfähigkeit, autonome Handlungsweise usw.), weshalb die Kontextsensoren-Implementierung in Heywow auf einer Agentenplattform für mobile Endgeräte beruht.

Anforderungen und Charakteristik
160 kByte bis 512 kByte Speicher für VM, CLDC- und MIDP-Bibliotheken und Anwendungen, davon • 256 kByte persistenter Speicher (z. B. Flashspeicher) für das System • 8 kByte persistenter Speicher für Programme • mind. 64 kByte RAM für Anwendungen
16- oder 32-bit-Prozessor
geringer Stromverbrauch, oft batteriebetrieben
Netz-Anschlussfähigkeit, oft drahtlose und unzuverlässige Verbindungen mit stark beschränkter Bandbreite
eingeschränkte Darstellungsfähigkeiten mit 1:1-Pixel-Seitenverhältnis, minimal • 96 · 54 Pixel und • 1 bit Farbtiefe
ITU-T-Einhand-Tastatur oder Touch-Screen

Tabelle 1. *Anforderungen und Charakteristiken von CLDC- bzw. MIDP-Geräten*

Sicherheitsaspekte von Heywow

Sicherheit ist stets ein Kompromiss zwischen zwei Gegensätzen. Das eine Extrem ist überhaupt keine Sicherheit, das ein Arbeiten ohne Beschränkungen erlaubt. Das andere Extrem ist die vollständige Sicherheit, die so restriktiv ist, dass ein Arbeiten praktisch unmöglich wird. Geschützt werden muss ein System dabei sowohl vor unbeabsichtigten Schäden wie auch vor beabsichtigten Angriffen, wobei im Folgenden nur der zweite Punkt betrachtet werden soll. Zunächst werden spezielle Sicherheitsaspekte von Heywow aufgezählt, um dann exemplarisch den Aspekt „mobiler Code“ genauer zu betrachten.

Im Mittelpunkt von Heywow stehen mobile Endgeräte, die jederzeit und überall per kabelloser Verbindung Daten und Programme laden können. Dies führt zu einer Reihe von Sicherheitsaspekten, die in dieser Form in der traditionellen kabelgebundenen Welt nicht oder zumindest nicht so intensiv auftreten:

Personalisierung bedeutet, dass der Nutzer Informationen und Dienste angeboten bekommt, die zu seinen aktuellen Bedürfnissen passen, ohne dass er ein umfangreiches Angebot von Daten und Diensten durchsuchen muss. Dazu müssen Informationen über die aktuelle Situation des Benutzers (sein Standort, seine Wünsche usw.) verfügbar sein. Das

Sicherheitssystem von Heywow muss hier verhindern, dass Unbefugte Zugriff auf diese Informationen erhalten.

Die *geringe Rechenleistung* der mobilen Endgeräte hat zur Folge, dass die Schutzmechanismen einfach gehalten werden müssen. Zum Beispiel kann nicht jede Verbindung verschlüsselt werden: Die geringe Rechenleistung reicht möglicherweise nicht für die populäre asymmetrische (Public-Key-)Verschlüsselung und Authentisierung.

Ad-Hoc-Netz bedeutet, dass sich Computer spontan – also ohne vorhergehende Konfiguration – zu einem Netz verbinden können, wobei jeder Rechner Datenpakete für andere weiterleitet. Das Sicherheitsproblem dabei ist die Frage: „Wie weit kann man den (anderen) Rechnern in einen solchen Netz trauen?" Die meist unbekannten Teilnehmercomputer an solchen Netzen könnten versuchen, das Netz zu stören, Daten auszuspionieren oder falsche Daten einzuspeisen.

Mobiler Code bedeutet, dass Programme – hier Dienste – von einem Rechner zum anderen übertragen und dort ausgeführt werden können, ohne dass der Nutzer jeden Dienst einzeln installieren muss. Dabei muss das Sicherheitssystem dafür Sorge tragen, dass die Dienste keine unerwünschten Aktionen (z. B. Ausspionieren oder Zerstören von Daten) ausführen können. Diese unerwünschten Aktionen können dabei sowohl absichtlich (z. B. Virus) wie auch unbeabsichtigt (z. B. Programmfehler) herbeigeführt werden.

Mit der Entscheidung für Java hat man sich beim Heywow-System auf eine Programmiersprache festgelegt, die „Code Mobility" und Sicherheit unterstützt. Insbesondere das Java-eigene Sandbox-Modell ist hier zu erwähnen. Dieses verhindert, dass ein Programm unerwünschte Aktionen ausführt. Bildlich ausgedrückt wird der Programmcode zusammen mit allen Objekten, die er manipulieren darf, in einen „Sandkasten" gesetzt. Auf Objekte und Ressourcen, die außerhalb dieses Sandkastens liegen, kann der Code von der Sandbox aus nicht zugreifen.

Technisch realisiert wird die Sandbox, indem jeder Klasse des Programms eindeutig Zugriffsrechte zugeordnet werden. Ruft das Programm eine Methode der Standard-Java-Bibliotheken auf – z. B. um eine Datei zum Lesen zu öffnen – so überprüft diese Methode, ob die Klasse die nötigen Rechte hat (z. B. das Recht, die Datei zu lesen). Heywow benutzt diese Sandbox im Rahmen seines Sicherheitssystems.

Der mobile Code wird über das Netz geladen, und von einer anderen Quelle erhält das System die zugehörigen Autorisierungsinformationen, **Bild 2**. Beide Datenblöcke – Code und Rechte – sind signiert, um zu verhindern, dass sie während des Transports verändert werden. Beim Start eines Dienstes wird der zugehörige Programmcode in eine neue Sandbox geladen, die mit den entsprechenden Rechten versehen wird. So ist der Computer weitgehend vor unerwünschten Effekten des mobilen Codes geschützt.

Im Heywow-Projekt bemühen wir uns, den besonderen Sicherheitsaspekten im mobilen Umfeld von vornherein Rechnung zu tragen.

* * *

Der zweite Teil im nächsten Heft erläutert die Netzaspekte und die Ortsbestimmung bei Heywow und gibt einen Ausblick auf die zukünftige „Situationsbestimmung".

Abkürzungen

AMSR Advanced Mobile ServiceRegistry, Diensteverzeichnis
CLDC Connected Limited Device Configuration, J2ME-Bibliothek zur Abdeckung von Java-Funktionen einer Gerätekonfiguration mit ähnlichen Anforderungen, hier Mobiltelefon oder PDA
CS Context Sensor, Softwaremodul zur Auswertung von Kontextinformationen
J2ME Java 2 Micro Edition, Java-Version für mobile Endgeräte
LBS Location Based Services, ortsabhängige (Informations-)Dienste
LSP Local Service Point, stellt lokal wichtige Dienste über Bluetooth oder Funk-LAN zur Verfügung, je nach Konfiguration auch als Gateway zum Heywow-Net
MIDP Mobile Information Device Profile, J2ME-Bibliothek zur Abdeckung gerätespezifischer Funktionen; ermöglicht die Zusammenarbeit zwischen verschiedenen Geräten gleicher Kategorie; setzt auf CLDC auf
PDA Personal Digital Assistent, handlicher Kleincomputer zur mobilen Nutzung
SoLo Soft Location, Kombination verschiedener Ortsinformationen
WAP Wireless Application Protocol, Netz- und Darstellungsstandard für mobile Dienste

Michael Angermann, Jens Kammann, Frank Kühndel, Patrick Robertson, Thomas Strang, Kai Wendlandt sind wissenschaftliche Mitarbeiter am Institut für Kommunikation und Navigation des Deutschen Zentrums für Luft- und Raumfahrt (DLR) in Oberpfaffenhofen.

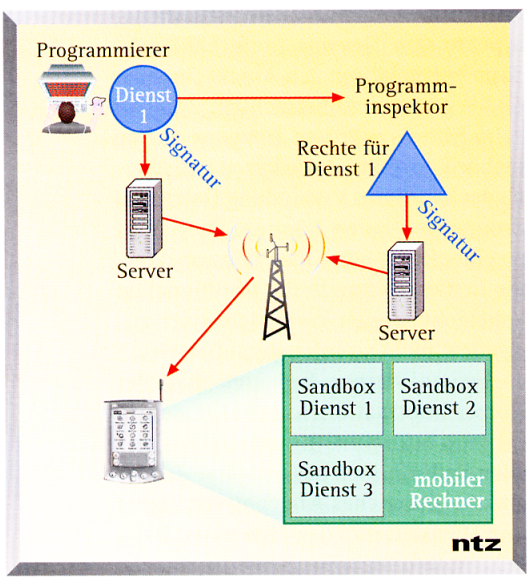

***Bild 2**. Das Sandbox Prinzip, Dienstverifizierung und Rechtevergabe*

Literatur

[1] *Riggs, R; Taivalsaari, A.; Vandenbrink, M:* Programming Wireless Devices with the Java 2 Platform, Micro Edition. Addison Wesley: 2001, ISBN 0-201-74627-1

[2] *Dey, A. K.:* Understanding and Using Context, Personal and Ubiquitous Computing. Special issue on Situated Interaction and Ubiquitous Computing 2001, vol. 5, Nr. 1

[3] *Franklin, S.; Graesser, A.:* Is it an Agent, or just a Program? A Taxonomy for Autonomous Agents. Proc. of the Third Int. Workshop on Agent Theories, Architectures, and Languages. Springer: 1996