Mobile & Cellular IP

Lei Wang, Rainer Holzmann

Hauptseminar „Dienste & Infrastrukturen mobiler Systeme“
Wintersemester 03/04
Institut für Informatik
Ludwig Maximilians Universität München
{wangl | holzmann}@informatik.uni-muenchen.de

Zusammenfassung. In dieser Seminararbeit werden die grundlegenden Eigenschaften von Mobile & Cellular IP vorgestellt. Der erste Teil beschäftigt sich mit Mobile IP, einem Protokoll zur Unterstützung von Makromobilität. Dabei wird das Protokoll detailliert in seiner Funktionsweise erläutert und neben Sicherheitsaspekten auch auf Mobile IPv6 eingegangen. Im zweiten Teil der Arbeit wird Cellular IP vorgestellt.

Lei Wang

1. Beschreibung von Mobile IP

1.1 Was ist Mobile IP?

Wer den Ausdruck „Mobile IP“ zum ersten Mal hört, denkt eventuell daran, dass es sich um eine Erweiterung von IP handeln könnte, mit der man mobile Geräte (Mobiltelefone, PDA´s, Notebooks, etc.) in das Internet integrieren kann. Obwohl der Begriff dies nahe legt, ist es nicht ganz richtig: Bei Mobile IP geht es eben nicht darum, dass Geräte, die während der Kommunikation im Netz schnell ihren Standort wechseln (wie z.B. Mobiltelefone), integriert werden, sondern vielmehr darum, ein Geräte unabhängig von seinem Standort mit ein und derselben IP-Adresse zu erreichen, Solange Kommunikation stattfindet, muss diese Geräte allerdings seinen Standort „beibehalten“. Im Kapitel 2 wird zeigen, dass Mobile IP aber genau die Grundlage liefert, mit der man die Integration „wirklich“ mobiler Geräte realisieren kann.
Der Grundgedanke von Mobile IP ist also die transparente Integration mobiler Host in beliebige Netzwerke, die Mobile IP unterstützen. Das heißt, dass andere Geräte den mobilen Host unter einer einzigen IP-Adresse erreichen können, sogar falls der mobile Host in einem anderen Netzwerk angeschlossen ist. Dabei redet man vom Heimatnetzwerk (Home Network), wenn man das Netzwerk meint, welches dieselbe Netz-ID trägt wie die IP-Adresse des mobilen Gerätes. Jedes andere Netzwerk, in welchem ein Gerät unter Verwendung von Mobile IP angeschlossen werden kann, wird Fremdnetzwerk (Foreign Network) genannt.
Zusammenfassend lässt sich sagen, dass ein Gerät mit Mobile IP jederzeit unter einer einzigen IP-Adresse erreichbar ist und sogar das Netzwerk wechseln kann, ohne offene Verbindungen zu verlieren, solange während des Wechsels kein Datenaustausch stattfindet.

1.2 Entstehung von Mobile IP

Angenommen, ein mobiler Host wird von seinem Standort im Internet entfernt und soll an einer anderen Stelle wieder angeschlossen werden (Roaming), wie in Abbildung 1 dargestellt. Um die Kommunikation mit diesem Host zu erhalten, muss der Host in Subnetz C mit neuer IP Adresse, Netzmaske und dem Default Router neu konfiguriert werden.

Das Problem in heutigen Internet-Protokollen liegt darin, dass ein Knoten immer am selben Punkt mit dem Internet verbunden ist; wechselt ein Knoten seinen Standort, ohne seine IP Adresse zu ändern, können existierende Routing-Protokoll-Datenpakete nicht mehr an die Knoten zugestellt werden.

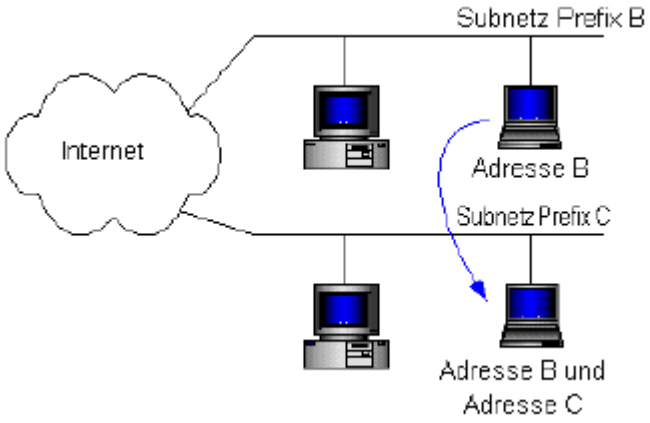


Abbildung 1: Netzwechsel eines Mobile Knotens

Es gibt nun folgende Möglichkeiten, um das Problem zu lösen:

- Dem mobilen Knoten wird eine passende IP Adresse zugewiesen. Wird beispielsweise DHCP (*Dynamic Host Configuration Protocol*) verwendet, so geht diese Zuweisung automatisch, andernfalls entsteht an dieser Stelle Administrationsaufwand. Außerdem wird der mobile Knoten unter seiner alten IP Adresse nicht mehr gefunden, Name-Server-Einträge müssen dann angepasst werden.

- Es könnte für alle mobilen Knoten eine Route installiert werden, so dass Datagramme für diesen Hosts explizit an das richtige Netzwerk weitergeleitet werden. Aber auch diese Lösung ist aufwendig.

Diese Nachteile führten dazu, dass Mobile IP entwickelt wurde.

2. Funktionsweise

2.1 Wichtige Begriffe

Mobile IP definiert drei funktionale Entitäten, in denen die Mobilitätsprotokolle implementiert werden müssen [2]:

2.1.1 Mobiler Host
Darunter versteht man einen mobilen Rechner, der seine Position im Netzwerk ändert und dabei eine permanente IP-Home-Adresse besitzt.

2.1.2 Home Agent
Das ist ein im Heimatnetzwerk des Mobile Host installierter Rechner. Er hat daher denselben IP-Netzwerkanteil wie der Mobile Host. Er empfängt die Nachrichten, die für den mobilen Knoten bestimmt sind, und leitet diese an den Mobile Node weiter. Außerdem wird er laufend vom mobilen Knoten über seinen derzeitigen Aufenthaltsort informiert.

2.1.3 Foreign Agent
Das ist ein Router eines fremden Netzwerkes, in dem sich der mobile Rechner gerade aufhält. Er empfängt die Nachrichten des Home Agents und leitet diese an die mobile Station weiter.

Um den Aufenthaltsort eines mobilen Rechners bestimmen zu können, benötigt man zwei
Adressen:

2.1.4 Home Adress
Das ist die IP Adresse, die der mobile Knoten von seinem Heimatnetz zugeordnet bekommt. Unter dieser Adresse ist er seinen Kommunikationspartnern bekannt und behält sie auch, wenn er sich durch das Netzwerk bewegt. Das Netzwerkpräfix der Heimatadresse des mobilen Rechners definiert seinen Anschluss an das Netzwerk.

2.1.5 Care-of-Address (COA)
Jedes Mal, wenn der mobile Knoten ein neues Netzwerk besucht, erhält er eine für das fremde Netz spezifische temporäre IP-Adresse. Diese bestimmt den derzeitigen Standort des mobilen Rechners und stellt jene Adresse dar, zu der die Nachrichten, die für den mobilen Rechner bestimmt sind, weitergeleitet werden. Diese Adresse wird also niemals als IP Source bzw. Destination Adresse verwendet.

Man kann hierbei zwei verschiedene Typen unterscheiden:

Foreign Agent Care-of-Adress: Darunter versteht man eine IP-Adresse des Foreign Agent, der eine Schnittstelle zu jenem Netz besitzt, in dem sich der mobile Knoten gerade befindet. Es kann sich dabei um eine beliebige IP-Adresse handeln, solange der Foreign Agent eine Verbindung zum jeweiligen Fremdnetz bereitstellt. Die Care-

of-Adresse eines Foreign Agent kann von mehreren mobilen Rechnern gleichzeitig verwendet werden.

Collocated Care-of-Adress: Diese IP-Adresse wird dem mobilen Knoten direkt zugewiesen und wird dann angewendet, wenn kein Foreign Agent zur Verfügung steht. Die Netzwerk- Präfixe müssen mit dem Fremdnetz übereinstimmen und jede coloccated COA kann nur einmal vergeben werden.

2.2 Wie funktioniert Mobile IP?

Mit Mobile IP wird es möglich, dass ein Rechner sich beliebig von einem Netz zum anderen bewegt, ohne seine offizielle Adresse wechseln zu müssen. Ganz gleich, an welcher Stelle er sich aufhält und über welche Wege er erreichbar ist, seine Adresse aus dem Heimatnetz, so genannt „Home Adress“ ist überall gültig.

Im Grunde löst Mobile IP das oben angesprochen Problem, indem es einem mobilen Rechner zwei IP Adressen zur Verfügung stellt, und zwar einerseits die statischeHeimatadresse und andererseits die so genannte, mit Veränderung des Rechnerstandortes veränderbare Care-of Adresse, die eine mobile Station von dem gerade besuchten Fremdnetz zugewiesen bekommt (durch statuslose Autokonfiguration oder DHCP), wenn sie nicht an ihrem Heimatnetz angeschlossen ist.

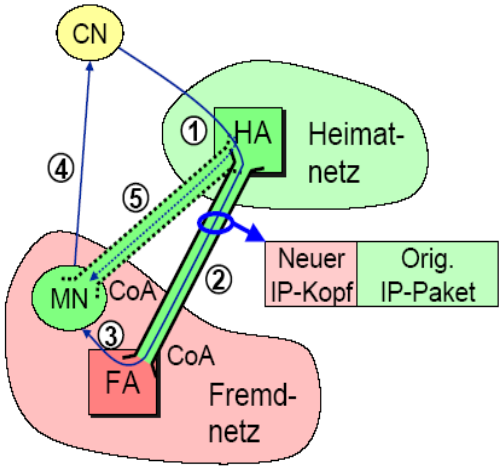


Abbildung 2: Funktionsweise von Mobile IP

Funktionsweise:

1. Pakete von „Correspondent Node“ (CN) zum mobilen Rechner (Mobile Node, MN) werden vom Heimatagenten (HA) abgefangen

2. Der HA tunnelt die Pakete zur Care-of Address (CoA), wenn ein Foreign Agent (FA) existiert

3. Der FA liefert die Pakete an den MN aus

4. In der Rückrichtung MN –> CN: kein Tunnel

5. Alternative: kein FA, MN erhält „co-located CoA“ (z.B. über DHCP oder PPP)

Ein mobiler Rechner ist also immer über seine Heimatadresse zu erreichen. Ist er im eigenen Netz, so funktioniert das automatisch. Ist er jedoch in einem Fremdnetz, muss der mobile Rechner ein Paket, das die zur Zeit benutzte Care-of Adresse enthält, an den Router in seinem Heimatnetz übermitteln, der dann über diese Bindung die Pakete nachsenden kann (Registrierung). Ab diesem Zeitpunkt erreichen alle Pakete, die an die ursprüngliche Heimatadresse gerichtet waren, den mobilen Rechner über einen Tunnel seines Heimatagenten.

2.3 Protokolle

Im Folgenden möchten wir auf die wesentlichen Komponenten von Mobile IP detaillierter eingehen: Agent Discovery, Erkennung von Zugangspunktänderung, Registrierung und Tunneling von Care-of Adressen.

2.3.1 Agent Discovery

Dieser Prozess beschreibt den Vorgang, in welchem der mobile Rechner seine derzeitige
Lokation bestimmt und eine Care-of Adresse zugewiesen bekommt.

Hierbei werden zwei verschiedene Formen von Nachrichten verwendet:

- Agent Advertisements werden periodisch, in regulären Intervallen sowohl von Home Agents als auch von Foreign Agents übermittelt, um dem mobilen Rechner zu ermöglichen, herauszufinden, ob er sich in seinem Heimatnetz oder in einem Fremdnetz befindet.

- Agent Solicitations werden vom mobilen Rechner gesendet, falls dieser Bedarf an einer Zuweisung einer Care-of Adresse hat und nicht auf die periodische Versendung der Agent Advertisements warten möchte. Diese Solicitation wird in Folge dann von einem Foreign bzw. Home Agent in Form eines Agent Advertisements beantwortet.

Stellt ein mobiler Knoten nach der Auswertung des Inhaltes der Agent Advertisment fest, dass er sich in seinem eigenen Heimatnetz befindet (das Netzwerkpräfix der Adresse vom Home Agent entspricht dem Netzwerkpräfix der Heimatadresse des mobilen Rechners), verhält er sich wie ein fixer Host und macht keinen Gebrauch von Mobile IP. Wird jedoch ersichtlich, dass er sich in einem Fremdnetz befindet, wird weiter überprüft, ob der mobile Rechner seine Position seit dem letzten Empfang eines Agent Advertisements verändert hat. Trifft dies zu, so benötigt der Rechner eine neue Care-of Adresse und es folgt der Schritt der Registrierung.

Allgemein kann man sagen, dass ein sich in einem Fremdnetz befindender mobiler Rechner eine Care-of-Adresse vom Fremdagenten erhält. Wird ihm jedoch keine

Adresse zugewiesen, dann versucht er über DHCP eine so genannte collocated-Care-of Adresse zu erhalten. Wenn allerdings auch dieser Versuch zu einer zusätzlichen Adresse zu gelangen scheitert, bleibt nur noch die manuelle Eingabe der IP Adresse als Lösung.

2.3.2 Erkennung von Zugangspunkänderungen

Ein mobiler Host soll am RouterAdvertisment erkennen, ob er den Zugangspunkt gewechselt hat. Wenn ein mobiler Host nach abgelaufener LIFETIME keine neuen Advertisments mehr von seinem Foreign Agent empfängt, so wird festgestellt, dass der mobile Host den Zugangspunkt verlassen hat. Um einen neuen Agent zu finden oder sich bei einem Agent zu registrieren, wird der mobile Host dann eine Solication-Message aussenden.
Wenn aber kein Foreign Agent vorhanden ist, kann man den mobilen Host nicht informieren, dass seine colocated Care-of Adresse schon nicht mehr gültig ist.

2.3.3 Registrierung

Einem mobilen Rechner stellt sich die Aufgabe der Registrierung immer dann, wenn er seine Position im Netzwerk verändert hat oder auch – aufgrund einer vorhandenen Lifetime-Angabe – wenn die existierende Registrierung abläuft.

Registrierungsprozess

Die Registrierung besteht aus dem Austausch der beiden Nachrichten: Registration Request und Registration Supply. Hier sieht man die drei häufigsten Szenarios für den Registrierungsprozess:

Fall 1: Registrierung eines mobilen Rechners in einem fremden Netz mit einer collocated
Care-of Adresse (weil kein Foreign Agent im Fremdnetz präsent ist) (Abbildung 4)

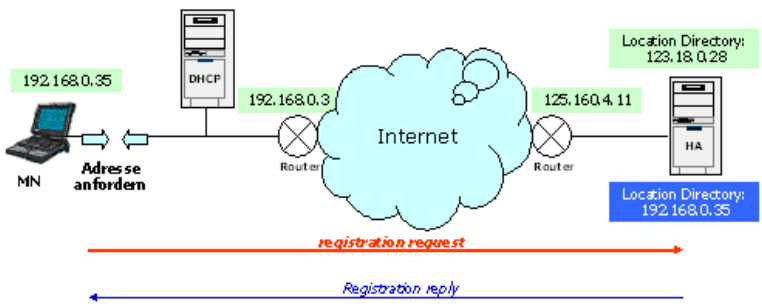


Abbildung 3: Registrierung mittels colocated Care-of Adresse

Dieser Registrierungsvorgang ist recht einfach: Der mobile Rechner benutzt also eine colocated Care-of Adresse, die Registrierung wird direkt von dem mobilen Knoten an den Home Agent gesendet. D.h, der mobile Knoten braucht nur dem Home Agent mitzuteilen, an welche Adresse er die Pakete senden soll.

Fall 2: Registrierung eines mobilen Rechners in einem Fremdnetz über einen Foreign Agent (Abbildung 5)

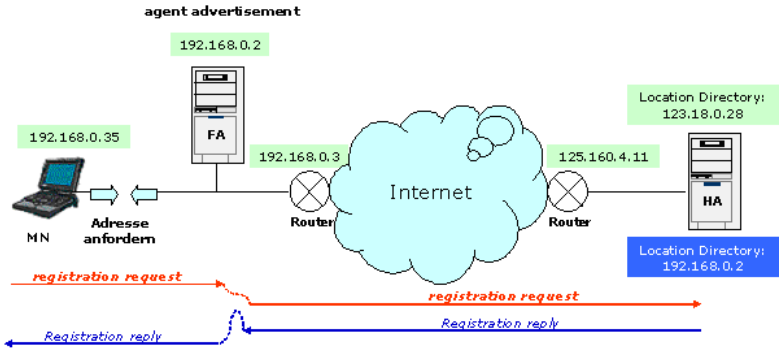


Abbildung 4: Registrierung über Foreign Agent (Care-of Adresse)

Der Unterschied zwischen dem Vorgehen mit Foreign Agent und dem ohne besteht darin, dass der Foreign Agent dem Home Agent seine eigene Adresse, und nicht die Adresse des Mobilen Hosts, mitteilen muss. Alle Pakete werden dann zunächst vom Home Agent an den Foreign Agent geschickt, nach dem Auspacken der Pakete leitet der Foreign Agent sie an das Mobile Host weiter.

Fall 3: Ein mobiler Rechner de-registriert sich nach seiner Rückkehr ins Heimatnetz (Abbildung 6)

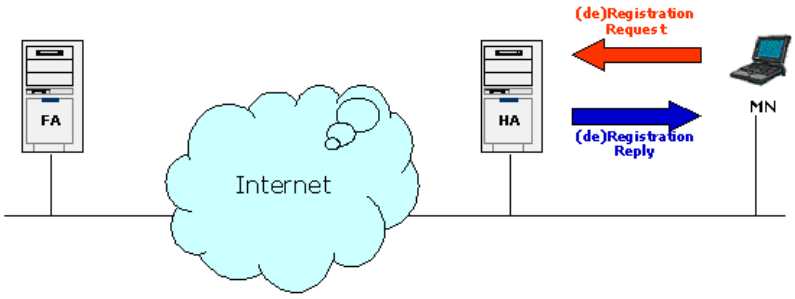


Abbildung 5: De-Registrierung

Wenn der mobile Rechner mit seinem Heimatnetzwerk verbunden ist, de-registriert er sich bei seinem Home Agent.

Eine Registrierungsanfrage kann auch als vom mobilen Rechner gesendet „binding update“ bezeichnet werden. „binding“ enthält die zusammengefasste Information über die Heimatadresse, die Care-of Adresse und die Dauer der Registrierung.

2.3.4 Tunneln

Nach den obigen zwei Operationen (Agent Discovery & Registrierung) können wir zum Mittelpunkt unserer Mechanismen kommen: Tunneling Operationen. Sie bestehen aus zwei Vorgängen: Encapsulation und Decapsulation.

Voraussetzung: Ein mobiler Rechner hat sich bereits bei seinem Home Agent registriert und hat seine Care-of Adresse bekannt gegeben. Nun werden von einem externen Host die Pakete an die Heimatadresse des mobilen Rechners versendet. Der Home Agent (Anfang des Tunnels) fängt diese Pakete ab und „verpackt“ sie in neue Pakete, welches als Zieladresse die Care-of Adresse (Ende des Tunnels) beinhalten.

Die neu erzeugten Pakete werden dann zur Care-of Adresse geroutet, aber hier müssen wir natürlich die zwei Fälle unterscheiden: In Falle einer Foreign Agent COA fängt der Foreign Agent die vom Home Agent gesendeten Pakete ab, entfernt den äußeren Header und leitet die Originalnachricht an den MN weiter. Im Falle einer collocated COA ist der mobile Knoten selbst für den Erhalt des verkapselten Paketes verantwortlich. Dieser Vorgang wird als Encapsulation bezeichnet, Internet Standard für die Encapsulation ist die so genannte „IP-in-IP Encapsulation“. Es wird von jedem Mobile IP Protokoll unterstützt und alle Home und Foreign Agents müssen dieses Verfahren implementiert haben.

In der folgenden Abbildung ist der Tunneln-Vorgang zu erkennen:

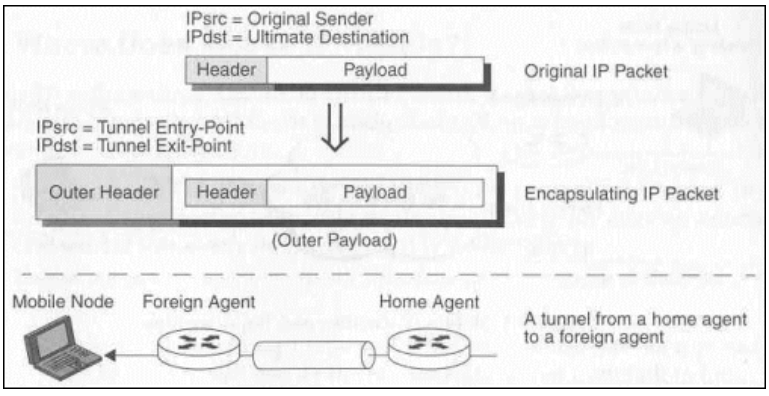


Abbildung 6: Ver-/Entkapseln

- Der innere Header besteht aus der Zieladresse des mobilen Rechners und der Quelladresse des Sendes des ursprünglichen Datagrams.
- Der äußere Header beinhaltet die Care-of Adresse des mobilen Knoten als Zieladresse und als Quelladresse die Adresse des Home Agent.

Zwischen dem inneren und äußeren Header entstehen redundante Daten; bei mobilen Knoten mit geringer Bandbreite macht „Minimal Encapsulation“ Sinn; diese doppelten Felder sollen durch diese Verfahren vermieden werden.

Um die Pakete zu versenden, besteht noch eine dritte Möglichkeit: Die Anwendung der Generic Record Encapsulation (GRE) [Hanks94a]; bei GRE stehen neben IP auch andere Protokolle (XNS, Novell IPX…) zur Verfügung.

Als Decapsulation wird das „eingepackte“ Paket „ausgepackt“, wodurch das ursprüngliche Paket wiederhergestellt wird. In Abbildung 7 wird der Tunneling Prozess (mit oder ohne FA) dargestellt.

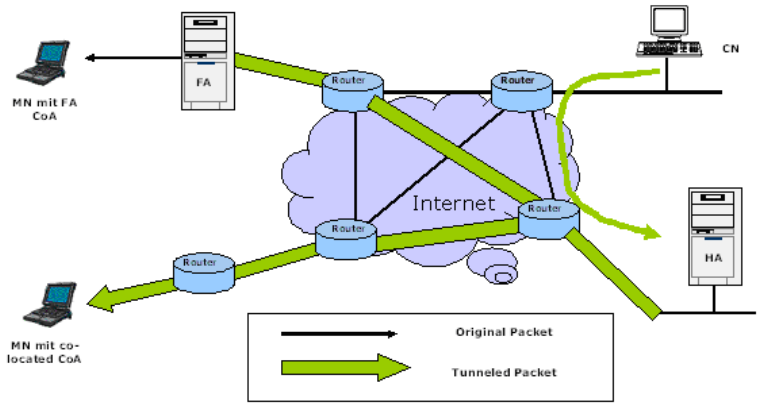


Abbildung 7: Tunneling

2.4 Sicherheitskonzepte

2.4.1 Authentisierung

Jeder MH, FA und HA muss für Security Association (SA) fähig sein, indiziert nach deren Security Parameter Index (SPI) und IP Adresse[6]. Eine Sicherheitsbeziehung beinhaltet:

1. Welches Verfahren zur Authentisierung (bzw. Verschlüsselung) benutzt wird
2. Parameter für die Verfahren
3. Aktuelle Schlüssel
4. Wie lange ein Schlüssel gültig bleibt
5. Den Modus: werden Pakete getunnelt oder transparent übermittelt

Dadurch kann der Mobile Knoten überprüfen, ob er sich wirklich bei seinen Heimatagenten registriert hat, denn ein falscher Heimagent könnte die Kommunikation abhören bzw. beeinflussen. Bei der Registrierung ist die Authentisierung sehr wichtig: Dies wird dadurch erreicht, dass zwischen jedem mobilen Rechner und seinem Home Agent eine Sicherheitsverbindung herrscht, Message Digest 5 mit 128-bit Schlüsseln (MD5 hash) wird verwendet, um fälschungssichere digitale Signaturen im Bereich der Registrierung zu gewährleisten[6]. Außerdem gibt es bei Mobile IP in der Registrierungsnachricht ein spezielles Identifikationsfeld (enthält entweder Zeitstempel oder zufällige Nummer, sieh Abbildung 1), das sich bei jeder neuen Registrierung ändert und somit die Einzigartigkeit gewährleistet.

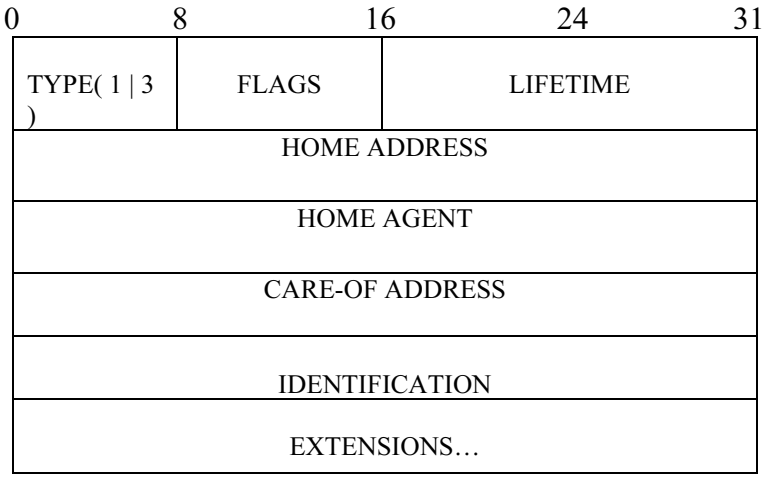


Abbildung 8: Format einer Mobile IP Registrierungs-Nachricht

Das LIFETIME Feld gibt an, wie lange die Registrierung gültig bleibt (0 bedeutet sofortige Deregistrierung, 1 bedeutet unendlich). In manchem Fall (Registrierung über

FA) können beide jeweils die LIFETIME einschränken. IDENTIFICATION ist eine 64-bit Zahl, die von dem mobilen Rechner generiert wird.

Authentifizierung wird durch eine Erweiterung des registration requests und des registration reply realisieren. Es gibt drei Erweiterungsheader für die Authentifizierung:

- Mobile-Home Authentication Extension,
- Mobile-Foreign Authentication Extension
- Foreign-Home Authentication Extension

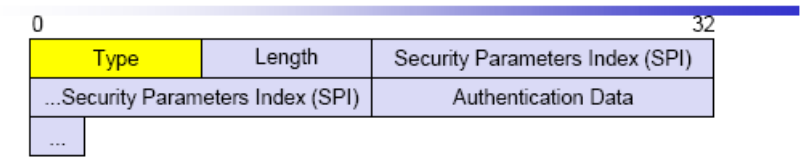


Abbildung 9: Mobile IPv4 - Authentication Extension

SPI: Der SPI identifiziert zusammen mit der (Home)-IP die Security Association
Authentication Data: Prüfwert, der durch den Authentifizierungsalgorithmus erzeugt wird.

Alle drei Erweiterungen haben das Format in Abbildung 9. Eine Mobile-Home Authentication Extension ist verpflichtend für alle Registration Requests und Replies, die anderen beiden sind optional. Falls ein Authentifizierungsheader für ein Paar von Knoten, (MH-HA), (MH-FA) oder (FA-HA) existiert, müssen ihn die entsprechenden Knoten überprüfen. Abbildung 10 veranschaulicht ein Registration request message.

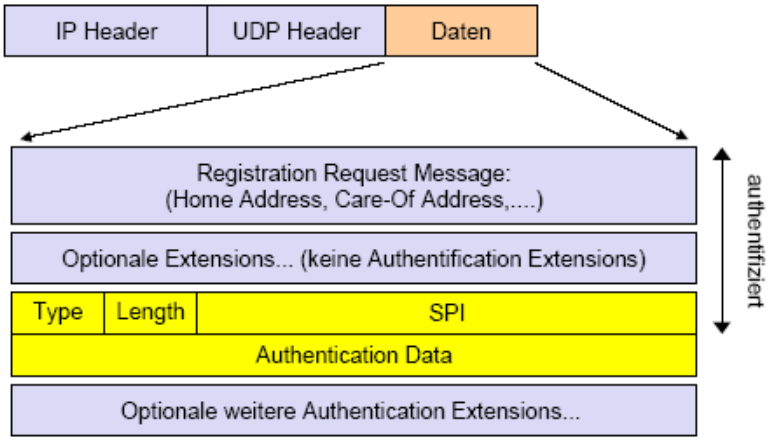


Abbildung 10: Registration request message

Ein geheime Schlüssel zwischen dem Heimatagent und dem mobilen Knoten wird vereinbart, bevor der Mobile Knoten einen registration request sendet. Innerhalb des registration request werden der geheime Schlüssel, der selbst, alle Erweiterungen des registration request und wieder der geheime Schlüssel verwendet, um mittels des MD5-Algorithmus [7] einen message digest zu erzeugen. Dieser message digest wird dann als Authentication Extension zusammen mit dem registration request zu dem Heimatagente gesendet.

2.4.2 Angriffsarten

Passives Mithören (Eavesdropping)
- Gewinnung von Informationen, die nicht für einen bestimmt sind
- Erlauschen von Passwörtern (z.B. für FTP)
- Geht oft anderen Angriffen vorraus

Wie:
- Lesen der Ethernet frames von einem anderen Computer des Netzwerks aus
- Abfangen von Funksignalen von drahtlosen Netzwerken

Denial of Service: Ein Rechner kann lahmgelegt werden
Wie:
- Flooding: ein Rechner wird mit unnützen Daten zugeschüttet. Er hat keine Resourcen mehr frei, die sinnvollen Daten zu verarbeiten.
- Einspielen falscher Informationen

Replay: Ein schon gesendetes Packet wurde abgefangen und wird nun nochmals abgeschickt (manchmal auch mit modifiziertem Inhalt)

1. Beispiel:
2. Ein Mobile Node hat seine Care-Of-Adresse gestern verändert. Das Binding Update wurde mitgehört.
3. Heute ist der Knoten in einem anderen Netz.
4. Der Angreifer schickt nun das alte abgefange Binding Update an den Home Agent.
5. Der Home Agent schickt die Daten in das falsche (alte Netz)

Man In The Middle: Erlangen von Daten
Wie:
- Der „Mittelmann“ sitzt zwischen dem Weg vom Sender zum Empfänger.
- Er gibt sich dem Sender als der eigentliche Empfänger aus, dem Empfänger als der Sender. Daten, die nun von beiden Seiten zu ihm laufen leitet er weiter.
  - ⇨ Sender und Empfänger bemerken nichts von seiner Existenz, aber alle Daten laufen über seine Rechner.

Beispiel:
Ein Mittelmann könnte sich zwischen Home Agent und Mobile Node oder auch zwischen Foreign Agent und Mobile Node setzen.

Sitzungsübernahme (Session Stealing): Zugang zu Diensten und Dateien
Beispiel:

1. Der Angreifer wartet bis der Mobile Node sich im Netzwerk angemeldet hat.
2. Er macht den Knoten funktionsunfähig (z.B.: durch DoS, Flooding)
3. Er übernimmt die Sitzung, d.h. gibt sich als Mobile Node aus und sendet/empfängt Pakete...

3. Mobile IPv6

3.1 IPv4 vs IPv6

Ein wesentlicher Unterschied zwischen IPv4 und IPv6 ist der erweiterte Adressbereich. Eine IPv4-Adresse hat 32 (4 Bytes), eine IPv6-Adresse 128 Bits (16 Bytes). Dieser Adressraum ermöglicht einerseits, ein globales hierarchisches Adressierungssystem zu schaffen, um das Routing zu optimieren und die Routingtabellen zu entlasten. Andererseits stellt das Protokoll genügend Adressen zur Verfügung, um neue Dienste und Geräte, die in Zukunft eine IP-Adresse und permanente Verbindung benötigen, in die Netze zu integrieren. Bald werden Telefone, PDA, Kühlschrän-ke, TV-Geräte, Garagentore, neue Spielgeräte und Sensorsysteme auf eine permanente IP-Adresse angewiesen sein.
In einem IPv4-basierenden Netz muss jeder Host manuell oder mittels DHCP (Dynamic Host Configuration Protocol) adressiert werden. Ein IPv6 Gerät kann automatisch erkennen, in welchem Netz es sich befindet und sich aufgrund dessen selbst für eine oder mehrere eindeutiger IPv6-Adressen konfigurieren. Selbstverständlich können nach wie vor DHCP-Server eingesetzt werden, wenn Autokonfiguration nicht erwünscht ist, oder um zusätzliche Optionen zu konfigurieren.
Auch für Verbesserungen in den Bereichen Authentifizierung, Sicherheit und Quality of Service (QoS) sind in separaten RFCs Extension Header definiert. Die Architektur erlaubt es überdies, zukünftig weitere Extension Headers zu definieren. Nicht zuletzt werden mobile Geräte in Zukunft eine IP-Adresse haben. Roamen, zum Beispiel von Wireless im Flughafen oder Hotel zu GPRS oder UMTS im Taxi wird dann mit Mobile IPv6 möglich.

3.2 Vorteile von IPv6

- Mit seiner erweiterten Funktionalität ist IPv6 effektiver als IPv4. Z.B. stellt die Knappheit der IPv4 Adressen möglicherweise ein Problem dar, falls das Netz nicht genügend Adressen anbieten kann [3].

- Mobile IPv6 benötigt weder DHCP-Server noch Foreign Agents in Fremdnetzen, um die Care-of Adresse eines mobilen Knotens zu konfigurieren.

- Mobile IPv6 kann für alle sicherheitsrelevanten Mechanismen nutzen, wie z.B. die Authentifizierung.

3.3 Mobilität in IPv6

Mit der Einführung von GPRS und UMTS wird die Anzahl mobiler Internetnutzer stetig zunehmen. Alle mobile Geräte, es dürften Milliarden werden, sollten an jedem Ort der Welt unter ihrer Heimat IP Adresse erreichbar sein. In IPv6 wurde eine spezielle Unterstützung für diese Fälle implementiert. Sie funktioniert folgendermaßen: Unterwegs ist das mobile Gerät unter einer Care-of Adresse zu erreichen, schickt nun ein anderes Gerät ein Paket an das mobile Gerät, geht dieses zunächst einen Umweg über den Home Agent und von dort an die mobile Gerät . Deren Antwortpaket enthält jedoch neben der Heimatadresse auch die Care-of Adresse, so dass nun weitere Antworten ohne Umweg direkt an die aktuell benutzte Adresse gerichtet werden können [3].

4. Mobile Anwendungen mit GPRS

Das Ziel im mobilen Internet ist das Zusammenführen verschiedener Datenströme in einem IP-Netz. Bei der Übertragung von Echtzeitdiensten wie Sprache und Video bestehen strikte Anforderungen an das Netz auf die Servicegüte (Quality of Service). In Mobilfunknetzen ist die Toleranz bei Laufzeitverzögerungen aufgrund der mobilfunkspezifischen Zugangsprotokolle und der geringeren Kapazität der Luftschnittstelle noch geringer als in Kabelgebundenen IP-Netzen. Mit der GPRS (General Packet Radio Service) -Technik ist bereits ein zentraler Bestandteil der kommenden UMTS-Netze, den Paketorientierten IP-Backbone des Kernnetzes realisiert.
Wesentlich für die Evolution vom heutigen GSM-Netz zum konvergenten All-IP-Netz sind folgende drei Entwicklungen:

- Der gesamte Datenverkehr (Daten, Sprache und Signalisierung) wird im Kernnetz über einen einheitlichen IP-Backbone geführt.

- Der gesamte Sprach- und Datenverkehr wird von Endgerät zu Endgerät über Paketvermittelte Träger geleitet.

- Die bisherige hierarchische Struktur des Funknetzes wird durch eine verteilte IP-RAN-Architektur (RAN = Radio Access Network) ersetzt.

Neu am UMTS-Netz ist die Umstellung der zahlreichen Funkzugangsnetze (Base Station Systems) auf den neuen Übertragungsstandard Wideband Code Division Multiple Access (WCDMA). Mit diesem Verfahren wird die bisherige auf Zeitmultiplexing basierende GSM-Technik durch eine auf CDMA basierende Übertragungstechnik ersetzt. CDMA ermöglicht es, alle verfügbaren Übertragungskapazitäten auf Nachfrage flexibel und effizient zuzuteilen sowie breitbandige Daten mit einer variab-

len Transferrate zu übermitteln. Darüber hinaus wird außerdem ein erheblich breiterer Frequenzbereich für die Übertragung genutzt.

Diese Mobility-Management-Funktionalität von IPv6 wird im IP-Layer angesetzt, Ferner funktioniert das Mobilitäts-Management des mobilen Knotens auch zwischen Netzwerken mit unterschiedlichen Link-Layer-Mechanismen, so dass keine besonderen Interworking-Mechanismen spezifiziert werden müssen. Mobile IPv6 ermöglicht somit eine einfache Umsetzung des Mobilitäts-Managements beim Roaming zwischen unterschiedlichen Zugangsnetzen wie beispielsweise WLAN und GPRS/UMTS. Die Zukunft soll durchgängig auf IP basierenden Mobilfunknetzen gehören. [3]

5. Zusammenfassung

- Mobile IP garantiert die Erreichbarkeit eines Hosts unter ein und derselben IP-Adresse unabhängig vom realen Aufenthaltsort dieses Hosts.

- Diese Erreichbarkeit wird transparent zu Verfügung gestellt. Andere Hosts brauchen keine spezielle Software und können mobile Hosts auf gewöhnlichem Wege erreichen.

- Mit Mobile IP alleine ist es nur möglich, Hosts einzubinden, die während der Kommunikation ihren Standort nicht ändern.

- Ein mobiler Host bekommt eine öffentliche Adresse(Primäre Adresse). Ausschließlich diese wird von externen Hosts zur Kommunikation verwendet. Des weiteren erhält der mobile Host eine sekundäre Adresse, an die ein home agent die Daten tunnelt.

- Durch Erweiterung gewisser ICMP Nachrichten kann ein mobiler Host agents finden. Diese Agents können auf ähnlichem Wege von sich aus auf sich aufmerksam machen.

- Die Transparenz des Systems hat zur Folge, dass teilweise ineffektives Routing verwendet wird.

- Erweiterungen auf Basis von Mobile IP werden bereits realisiert(z.B. Cellular IP)

Bibliographie

[1] Christian Huitema: IPv6 die neue Generation, Addision-Wesely Verlag, München, 2000

[2] Charles E. Perkins, Sun Microsystems: Mobile IP, IEEE Communications Magazine.

[3] Documet: http://www.ipv6-net.de/

[4] Charles E. Perkins, Mobile IP: Design Principles and Practices,
Adisson Wesely Longman

[5] Document: http://www.computer.org/internet/v2n1/perkins.htm#r4, 03.05.03

[6] [Wolfgang Thomas] Thema 7 :IPSec Architektur und Protokolle, Internet Key Exchange Security Protocol(IKE)

[7] [Rivest 92] Rivest, R.: The MD5 Message-Digest Algorithm RFC 1321, April 1992

Cellular IP

Rainer Holzmann

Zusammenfassung. Der drahtlose Zugang zu Diensten des Internet wird in Zukunft immer öfter genutzt werden, auch wenn es heute noch eher die Ausnahme darstellt. Es ist deutlich zu beobachten, dass die Teilnehmerzahlen an Mobilfunksystemen sich explosionsartig entwickeln, was eine enorme Herausforderung an bestehende Mobilfunknetze darstellt. Viele mobile Kunden möchten mit IP-fähigen Endgeräten eine große Anzahl von unterschiedlichsten Diensten nutzen. Dies erfordert eine paketorientierte Netzstruktur, die nahtlose Mobilität anbietet. Second- und Third-Generation-Systeme unterstützen bereits nahtlose Mobilität, sie basieren allerdings auf einer komplexen und teuren verbindungsorientierten Infrastruktur, der es an Flexibilität, Robustheit und Skalierbarkeit fehlt.

Mobile IP stellt eine einfache und skalierbare Lösung für die Unterstützung von Makromobilität dar, es fehlt jedoch die Fähigkeit schnelle Handoffs mit wenig Latenzzeit und einem Minimum an Paketverlust zu realisieren, sowie Paging zu unterstützen.

Cellular IP ist ein Protokoll, welches Mikromobilität in einem geographisch begrenzten Subnetz ermöglicht und das den häufigen Ortswechsel des mobilen Endgerätes beherrscht. Es vereint solche Techniken wie Paging (ermöglicht passive Konnektivität), bekannt aus bestehenden zellularen Mobilfunknetzen, mit einer effizienten Mischung aus IP Forwarding, minimalem Signalisierungsoverhead und zustandsorientiertem Location Management. In Zusammenarbeit mit Mobile IP erreicht man damit eine globale Mobilitätsunterstützung.

In dieser Ausarbeitung wird das Design, die Implementierung und eine Evaluierung von Cellular IP vorgestellt, das im Verlauf der letzten Jahre an der Columbia University mit Unterstützung von Broadcom Research, Ericsson, Fujitsu, IBM, Intel und Nortel Networks entwickelt wurde.

1 Das Cellular IP Szenario

Motivation

Um das Internet um die gewünschte Mobilität zu erweitern, haben sich die jüngsten Ansätze meistens mit dem Problem der Adressübersetzung durch Distant Location Directories oder Adress Translation Agents (beispielsweise Foreign Agent) beschäftigt [1]. Dieser Strategie folgt auch Mobile IP. Dabei werden Pakete via regulärem IP Routing zu der momentanen Care-of-Adresse (CoA) des Mobile Host (MH) gesendet. Mobile IP unterstützt keine nahtlose Mobilität, denn nach jedem Wechsel des Abdeckungsgebietes muss der MH eine neue lokale Adresse erhalten und seinem Home Agent (HA) mitteilen. Diese Mechanismen führen zu ganz erheblichem Signalisierungsoverhead innerhalb des Netzes, wodurch Mobile IP nur für Makromobilität geeignet ist [5].

Grundlagen

Die Qualität der Kommunikation im wireless LAN muss sich mit der im regulären drahtgebunden LAN messen. Schneller Zugang für bandbreitenintensive Dienste wie Multimedia erfordert immer kleinere Zellgrößen und eine steigende Anzahl an Base Stations (BSs). Dies wiederum verlangt von dem zugrundeliegenden Netz die Fähigkeit zur Unterstützung von häufigen Handoffs sowie einem Minimum an damit verbundener Latenzzeit und einem Minimum an Paketverlust. Cellular IP bietet die Konzepte für nahtlose Mikromobilität an. Mikromobilität bedeutet den Wechsel einer Funkzelle innerhalb eines Cellular IP Netzes. Der Wechsel eines Cellular IP Netzes in ein anderes wäre demnach dem Bereich Makromobilität zuzuordnen (vgl. Abbildung 1). Lokale Bewegungen des MH innerhalb des Cellular IP Subnetzes sind „transparent" zum restlichen Internet, was bedeutet, dass lokale Handoffs ohne Interaktion mit diesem stattfinden (Mikromobilität). Die Transparenz des Cellular IP Subnetzes reduziert den Signalisierungsverkehr ganz erheblich und ermöglicht damit eine Aufnahme von einer sehr großen Anzahl von Teilnehmern im Subnetz.

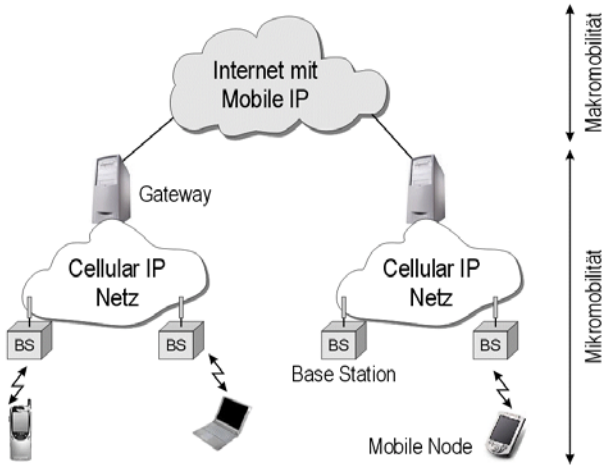


Abbildung 1: Mikromobilität

Das Cellular IP Szenario ermöglicht die Vision eines drahtlosen Zugangs zum Internet mit mehreren hundert Millionen mobiler Teilnehmer. Man geht davon aus, dass die IP-fähigen MHs ständig bereit sind, Daten sowohl zu Empfangen, als auch zu senden und damit jederzeit online sind. Tatsächlich werden die meisten Teilnehmer jedoch nicht ständig aktiv kommunizieren. Cellular IP begegnet dieser Anforderung mit der Einführung von einem Zustandskonzept für MHs ähnlich dem bei GSM [4]. Sogenannte „idle" MHs sind für das Netz erreichbar, haben jedoch seit einer gewissen Zeit aktiv keine Daten mehr gesendet und auch keine empfangen. Für das Cellular IP Subnetz reicht es, nur die ungefähre Position von idle MHs zu kennen. Die exakte Lokalisierung eines MH wird nur dann nötig, wenn Daten zum MH übertragen werden sollen. Dann muss das Netzwerk den MH in effizienter Zeit suchen und ausfindig

machen (Paging). Dabei geht der MH in den Zustand „active“ über. Die durch das Paging ermöglichte passive Konnektivität reduziert den Signalisierungsoverhead und führt damit zu weniger Verkehr auf der Luftschnittstelle. Weiterhin führt dies zu einer Reduzierung des Akku-Verbrauches beim MH.

Anforderungen

Cellular IP wurde ganz gezielt dafür entwickelt, um nahtlose Mobilität, passive Konnektivität und Paging zu unterstützen. Bei der Entwicklung standen folgende Ziele im Vordergrund: ein verteiltes Location Management ohne zentrale Steuerung, Cellular IP Routing ersetzt das gewöhnliche IP Routing, minimaler Konfigurationsaufwand für das Cellular IP Subnetz (ähnlich dem bei switched Ethernet LANs), Einfachheit und Effizienz der beteiligten Algorithmen zu Paging, Routing und Handoff, kostengünstige Implementierungen und möglichst wenig Anpassung der bestehenden Hardware, ohne dabei ein neues IP Paketformat zu definieren oder IP Tunneling einzusetzen [1], [3]. Im Folgenden werden die genauen Implementierungsdetails von Cellular IP vorgestellt. Dabei wird auf die Netzwerktopologie, das Location Management und auf Sicherheitsaspekte eingegangen. Zum Schluss wird die Geschwindigkeit des Protokolls anhand von Messungen bewertet, die durch eine an der Columbia University aufgebauten Testumgebung gewonnen werden konnten. Eine Zusammenfassung resümiert die gewonnenen Erkenntnisse.

2 Netzwerktopologie

Komponenten

Die zentrale Komponente innerhalb des Cellular IP Netzes ist die BS. Sie dient den MHs als drahtloser Zugangspunkt, ist für das Routing (dabei wird das reguläre IP Routing durch das Cellular IP Routing ersetzt, siehe Abbildung 3) von Paketen im Up- und Downlink verantwortlich und kümmert sich um alle weiteren Funktionen, die für das Cellular IP Location Management nötig sind. Die BS ist ein spezieller Cellular IP Node: sie besitzt neben den oben beschriebenen Fähigkeiten, die identisch mit denen von gewöhnlichen Nodes sind, eine drahtlose Schnittstelle.

Cellular IP Netze sind durch ein Gateway an das Internet angebunden (siehe Abbildung 2). Das Gateway weiß, welche MHs sich im Netz aufhalten. Der MH kann ein Cellular IP Netz durch den Cellular IP Network Identifier erkennen, der innerhalb eines von den BSs periodisch gesendeten Signalen (Beacon) enthalten ist. Ist der MH im Cellular IP Netz registriert, benützt er die IP-Adresse des Gateways als Mobile IP Care-of-Adresse.

Das Cellular IP Netz ist in einzelne Funkzellen unterteilt, welche zu beliebig großen und vielen Paging Areas gruppiert werden können. Beim Wechsel einer Funkzelle verschickt der MH Steuernachrichten, die bis zum Gateway geroutet werden, und löst somit einen Handoff aus. Im Gegensatz zu regulären Datenpaketen, die das Cellular IP Netz verlassen können, um zu einem entfernten Correspondent Node (Kommu-

nikationspartner) geschickt zu werden, enden Steuernachrichten am Gateway. Die damit erreichte Kapselung des Cellular IP Netzes ermöglicht spielend die Integration in das Mobile IP basierte Internet.

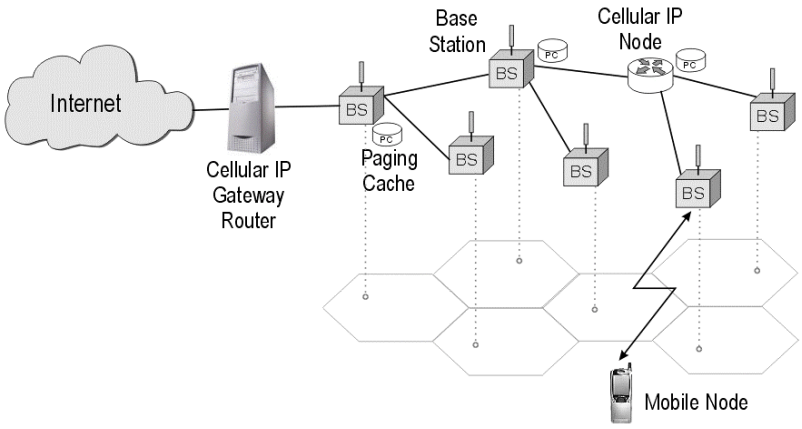


Abbildung 2: Cellular IP Netzstruktur.

Datenpfad

Im Cellular IP Netz gibt es keinen zentralen Server oder Agenten, welche ähnlich zu Mobile IP immer die aktuelle Position des MHs und die zugehörige Funkzelle wissen. Vielmehr werden Informationen, die nötig sind, um den MH ausfindig zu machen in den Cellular IP Nodes hinterlegt. Jeder Knoten weiß aber lediglich über welchen Nachbarknoten der MH erreichbar ist. Das Routing von IP-Paketen erfolgt demnach etappenweise (hop-by-hop) von Knoten zu Knoten, bis schließlich der MH selber erreicht wird. Daraus wird auch der Unterschied von Cellular IP Routing gegenüber dem regulären IP Routing deutlich: der MH wird durch seine IP-Adresse identifiziert, diese besitzt innerhalb eines Cellular IP Netzes aber keine topologische Bedeutung. Sie wird lediglich dazu benötigt, um Mappings zu erzeugen, die in den Cellular IP Knoten gespeichert werden. Ein Mapping stellt eine Verknüpfung der IP-Adresse des MH mit dem Nachbarn her, von dem das IP Paket empfangen wurde. Folgt man der Kette von gespeicherten Mappings in den Knoten für einen bestimmten MH, so ergibt sich der Datenpfad für die Up- und Downlinks.

Gemäß Mobile IP (ohne Routenoptimierung) werden die Pakete zunächst zum HA des MH geschickt. Dort werden sie verpackt und zum Gateway über ein Tunnel geschickt. Das Gateway entpackt sie und leitet sie an eine BS weiter. Innerhalb des Cellular IP Netzes werden die Pakete nicht getunnelt und es findet auch keine weitere Adresskonvertierung statt. Jedes Paket im Uplink, das das Cellular IP Netz verlässt, wird hop-by-hop bis zum Gateway geroutet und von dort weitergeschickt in das Internet (vgl. Abbildung 3).

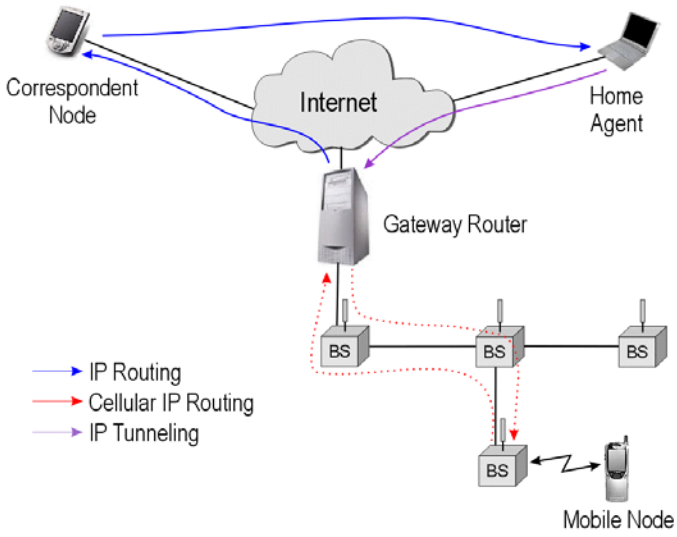


Abbildung 3: Datenpfad.

Verteiltes Location Management

Bei GSM/GPRS werden Steuernachrichten und Signalisierungsinformationen über getrennte logische Kanäle übertragen [6]. Bei WLAN fällt diese Struktur mit den logischen Kanälen weg. Cellular IP verbindet das Location Management geschickt mit dem Routing. Steuernachrichten sind gewöhnliche IP Pakete, die der MH überträgt. Sie werden dazu genutzt, um Mappings in den Cellular IP Knoten zu erzeugen bzw. zu aktualisieren. So können auch gewöhnliche Datenpakete zum Aktualisieren des Datenpfades verwendet werden, der durch hop-by-hop Routing und dem damit verbundenen Caching von Mappings in den betroffenen Knoten entsteht. Pakete im Downlink folgen einfach dem umgekehrten Pfad bis zum MH.

Es gibt zwei unterschiedliche Arten von Mappings: Routing und Paging Mappings. Routing Mappings beschreiben einen detaillierten Weg sowohl im Downlink, als auch im Uplink, während Paging Mappings nur in den Cellular IP Knoten eingetragen werden, die auch über einen Paging Cache (PC) verfügen. Eine exakte Lokalisierung von passiv konnektiven Mobile Hosts, also jene, die seit längerem keine Daten mehr gesendet haben, wird durch das Paging ermöglicht.

3 Location Management

Zustandsmodell

In Cellular IP wird ein Zustandsmodell eingeführt. Ein MH kann demnach entweder in dem Zustand „active“ oder im Zustand „idle“ sein (vgl. Abbildung 4). Der MH ist im Zustand active, wenn er Daten überträgt, oder Daten empfängt. Dieser Zustand ist dem Zustand „ready“ in GPRS ähnlich: ein MH ist im Zustand ready, wenn er Daten empfängt oder selber sendet.

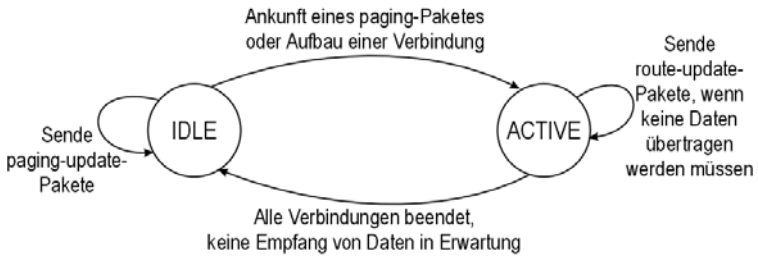


Abbildung 4: Zustandsmodell.

Der zweite mögliche Zustand eines MH ist idle. Werden alle Verbindungen beendet und auch nicht mehr auf weitere Daten gewartet, so wechselt der MH von active in idle. Wurden seit kurzer Zeit keine Daten mehr übertragen oder IP-Pakete empfangen, so ist der MH im Zustand idle. Auch hier besteht eine gewissen Ähnlichkeit zum Zustand „standby“ bei GPRS: Der Empfang und das Senden von Daten ist für einen MH im Zustand standby nicht möglich.

In GPRS wird der Zustand ready durch einen Timer überwacht. Der MH wechselt von ready in standby, wenn der Timer abgelaufen ist. Der Timer wird erneuert, wenn Daten zwischen Serving GPRS Support Node (SGSN) und MH übertragen werden. Cellular IP folgt dem gleichen Ablauf und setzt dafür den „active-state-timeout“ (ca. 5 sec) ein. Sowohl in GPRS als auch in Cellular IP sind für die Timer keine statischen Werte vordefiniert. Sie sind wesentlicher Bestandteil der Planung von Netzen.

Paging-Areas

Für gewöhnlich bleiben Hosts im LAN ständig online, auch wenn sie davon nur einen vergleichsweise geringen Teil der Zeit aktiv kommunizieren. Somit sind sie allerdings jederzeit erreichbar und können sofort auf angebotene Dienste zugreifen. Für einen mobilen Teilnehmer im drahtlosen Internet müssten periodisch Aufenthaltsinformationen gesammelt werden, damit dieser kontinuierlich erreichbar bleibt und somit dieselbe Qualität wie im LAN erwarten kann. Der MH wäre gezwungen regelmäßig Location Updates zu versenden, was in einer enormen Signalisierungslast des Netzes

und einem hohen Energieverbrauch des MH resultieren würde. Durch die Einführung von Paging in Cellular IP bleiben idle MHs passiv verbunden, das Problem der gesteigerten Netzlast wird somit vermieden. Das Cellular IP Netz ist geographisch in verschiedene Paging Areas gruppiert (vgl. Abbildung 5). Der MH kann eigene Bewegungen im Netz feststellen durch das Überprüfen des Paging Area Identifiers, der auch Bestandteil der periodisch gesendeten Beacons ist. Wenn ein MH nicht kommuniziert, so ist ein Location Update nur beim Wechsel der Paging Area notwendig. Damit brauchen idle MHs keine Location Updates durchführen und es ist auch keine Handoff-Unterstützung nötig.

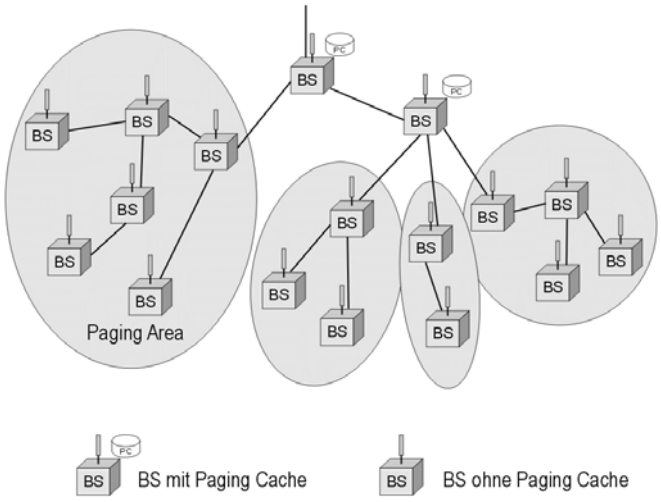


Abbildung 5: Paging Areas.

Routing und Paging Mappings

Bei der Ankunft eines eingehenden Paketes beim Gateway, wird eine Paging-Message in die gegenwärtige Paging Area des MH geschickt. Durch den Empfang dieser Nachricht sendet der MH seine Aufenthaltsinformationen in Form eines Route-Update Paketes an das Gateway und wechselt in den Zustand active. Dies stellt sicher, dass Routing Cache Mappings schnell erzeugt werden, was weiteres Paging verhindert. Route-Update Pakete und gewöhnliche Datenpakete können Mappings in PCs auch mit aktualisieren, Paging-Update Pakete jedoch nicht die Mappings in RCs. Idle MHs haben also Mappings im PC, nicht aber im Routing Cache. Dagegen besitzen active MHs Mappings in beiden Caches.

Die Knoten im Cellular IP Netz sind mit zweierlei Caches ausgestattet. Jeder der Knoten verwaltet einen Routing Cache (RC) für active MHs, in dem Routing Mappings abgelegt werden. Daneben kann ein Knoten unabhängig vom RC auch einen PC besitzen, der Paging Mappings für beide, active und idle, MHs speichert. Mappings werden von Paketen erzeugt und auch aktualisiert, die vom MH zum Gateway gesendet werden. Dabei haben die Mappings im PC einen höheren Timeout-Wert (Paging-

Timeout: ca. 3 min) gegenüber dem Timeout-Wert eines Mappings im RC (Route-Timeout: 3 sec). Die Trennung von Aufenthaltsinformationen in RC und PC ist durch das Zustandsmodell bedingt.

Idle MHs haben für einen active-state-timeout-Wert keine Daten mehr übertragen. Keine übertragenen Pakete bedeutet keine weiteren Aktualisierungen von RCs, welche dann nach Ablauf des Route-Timeouts gelöscht werden. Damit idle MHs weiterhin erreichbar bleiben, senden sie zu regelmäßigen Intervallen (durch die Paging-Update-time definiert, ca. 1 min) Paging-Update Pakete an das Gateway. Das Paging-Update Paket ist ein gewöhnliches ICMP-Paket mit der IP-Adresse des Gateways als Zieladresse. Dort angekommen wird es verarbeitet und daraufhin verworfen. Im Gegensatz zu gewöhnlichen Datenpaketen wird es nicht weitergeroutet. Route-Update Pakete unterscheiden sich zu Paging-Update Paketen nur durch einen Parameter. Die beiden erwähnten Pakete sind Steuernachrichten, die das Location Management im Cellular IP Netz ermöglichen. MHs senden ihre Paging-Update Pakete zu BSs mit besserer Signalstärke.

Paging

Normalerweise gelangen Pakete, die an den MH adressiert sind, anhand der Einträge im RC an ihr Ziel. Paging tritt nur auf, wenn ein Paket an einen idle MH adressiert wird und das Gateway oder die betroffenen BS keine gültigen RC Mappings für die Zieladresse finden können. Wenn eine BS auch keinen PC hat, wird sie das Paket an alle Nachbarknoten (bis auf den, von dem das Paket kam) weiterleiten. Existiert ein PC in einer BS, leitet diese das Paket nur weiter, wenn es dafür ein gültiges PC Mapping findet, ansonsten wird es verworfen. Gibt es im gesamten Cellular IP Netzwerk noch keine PC Mappings, so wird das erste am Gateway ankommende Paket, das an einen idle MH adressiert ist, über das gesamte Netzwerk geflutet, was kurzzeitig zu einem hohen Verkehrsaufkommen im Netz führt.

Die Konstruktion von Paging Areas bleibt dem Netzbetreiber überlassen. Wie viele BSs in einer Paging Area enthalten sind und die Verteilung von PC auf die jeweiligen BSs ist eine Konfigurationsfrage, die immer unterschiedlich ausfallen kann und an die Bedürfnisse individuell angepasst werden muss. Der Overhead, der durch Steuernachrichten verursacht wird, kann durch das Implementieren von PC in möglichst viele Cellular IP Knoten verringert werden, ist aber mit höheren Kosten verbunden.

Routing

Alle Pakete, die von einem MH abgesendet werden, gelangen zuerst unbeachtet von ihrer Zieladresse an das Gateway. Damit BS Pakete in Richtung Gateway schicken können werden die in den Knoten gespeicherten Informationen für das Routing verwendet. Diese Routinginformationen ergeben sich durch den Empfang eines Beacon-Paketes, welche das Gateway periodisch über das gesamte Netz flutet. BSs merken sich den Nachbarknoten, von dem sie das Beacon erhalten haben und erstellen daraus die Einträge im RC. Solch ein Eintrag wird Mapping genannt. Das Mapping ist ein Link von der IP Adresse des MH auf den Nachbarknoten, von dem das Paket empfan-

gen wurde [mapping(IP des MH, IP von Nachbarknoten)]. Es bleibt gültig für eine systemspezifische Zeit, die Route-Timeout genannt wird. Die Kette der gespeicherten Mappings, bezogen auf einen ganz bestimmten MH, bildet damit auch den Pfad für Downlink-Pakete, die an den gleichen MH adressiert sind. Pakete, die vom Gateway an den MH adressiert sind, werden wie im Uplink hop-by-hop, unter Verwendung der gespeicherten Mappings in den RCs, zum MH geroutet.

Solange ein MH regelmäßig Datenpakete verschickt, beinhalten die Knoten, die auf dem Pfad vom MH zum Gateway involviert sind, gültige RC Mappings. Daraus ergibt sich, dass der Versand von Daten den angenehmen Nebeneffekt hat, die Mappings in den Knoten aufzufrischen.

In Cellular IP ist der PC nur in einigen Cellular IP Knoten enthalten, im Gegensatz zum RC, der in jedem Node implementiert ist. Durch die Verwendung von zwei Caches (PC, RC) kann die Feinheit des Location Tracking für idle und active MHs unabhängig voneinander unterschiedlich ausfallen. MHs, die im Moment nicht aktiv kommunizieren, also weder senden, noch empfangen, aber immer noch erreichbar bleiben wollen für ankommende Pakete, lassen ihre RC Mapping Timer auslaufen. Dabei behalten sie ihre PCs aber aufrecht. IP Pakete, die an solche MHs adressiert sind, werden demnach über PCs zu ihnen geroutet.

	Paging Caches (PC)	**Route Caches (RC)**
aktualisiert von	allen Uplink Paketen (Datenpakete,Ppaging- und Route-Update Pakete)	Datenpaketen und Route-Update Paketen
update möglich	durch alle Update Pakete (Paging- und Route-Update Pakete)	Route-Update Pakete
update dann, wenn	Wechsel der Paging Area, oder nach Paging-Update-Time	Wechsel zu neuer Zelle, oder nach Route-Update-Time
Zustand des MH	sowohl Idle als auch Active MHs	Nur Active MHs
Aufgabe	Routing von Downlink Paketen, wenn keine RC Mappings vorhanden sind	Routing von Downlink Paketen

Abbildung 6: In der Tabelle werden die wichtigsten Parameter von PC und RC gegenübergestellt [3].

MHs sollten in einigen Fällen ihre RC Mappings aufrechterhalten, obwohl sie nicht regelmäßig Datenpakte versenden. Ein möglicher Anwendungsfall dafür wäre, wenn MHs im Downlink einen UDP-Stream von Paketen erhalten, selber aber im Uplink keinerlei Daten zu senden haben. Das Aufrechterhalten der RC Mappings in diesem Fall würde ein erneutes, kostspieliges Paging des MH vermeiden. Damit also die

Mappings im RC gültig bleiben überträgt der MH zu regelmäßigen Intervallen (Route-Update-Time) Route-Update Pakete. Genauso wie Paging-Update Pakete verlassen sie das Cellular IP Netz nicht, sondern werden am Gateway verarbeitet und enden dort. Die Aufgabe von Route-Update Paketen besteht darin, bestehende Mappings zu ändern oder aufzufrischen bzw. neue Mappings zu erzeugen.

Die Gültigkeit eines Mappings läuft genau dann ab, wenn entweder ein Route-Update Paket oder ein normales Datenpaket vom MH nicht rechtzeitig ankommt und somit der entsprechende Timeout zurückgesetzt wird. Ist ein Mapping ungültig, wird es aus dem Cache gelöscht. Wenn der MH Daten empfängt, werden diese durch entsprechende RC Mappings zu ihm geroutet. Sind keine RC Mappings vorhanden, so wird versucht eine Route für die an den MH adressierten Pakete durch PC Mappings aufzubauen.

4 Handoff

In Cellular IP werden zwei Arten von Handoffs unterschieden. Für Applikationen, die sehr empfindlich auf Paketverlust reagieren, wird ein semi-soft Handoff angeboten. Während dieser Art von Handoff werden Pakete sowohl an die alte, als auch an die neue BS gesendet. Semi-soft Handoff konzentriert sich auf die Minimierung des Paketverlustes und damit auf eine bessere TCP- und UDP-Geschwindigkeit gegenüber dem hard Handoff.

Der Cellular IP hard Handoff basiert auf einem simplen Prinzip, bei dem weniger Wert darauf gelegt wird, den Paketverlust gegen Null laufen zu lassen. Es wird vielmehr versucht, die Signalisierungslast zu minimieren und nimmt dabei einen kleinen Paketverlust in Kauf. Auch wenn dieser Paketverlust vergleichsweise klein ausfallen mag, kann er die TCP Performance deutlich einschränken. Im folgenden werden die zwei Arten von Handoffs genauer betrachtet.

Hard Handoff

Der Handoff in Cellular IP wird grundsätzlich durch den MH ausgelöst. MHs messen die Signalqualität von den durch BSs periodisch im Netz verbreiteten Beacons, um eventuell einen Handoff zu initiieren. Der hard Handoff wird durchgeführt, in dem der MH zu einer neuen BS wechselt und dann ein Route-Update Paket losschickt. Dadurch werden neue RC Mappings auf dem Weg zum Gateway erzeugt und damit die Downlink Route zur neuen BS konfiguriert.

Wird der hard Handoff initiiert, so führt dies nicht zu einer Löschung der Mappings zwischen der Crossover und der alten BS. Die Crossover BS ist dabei der gemeinsame Vaterknoten von alter und neuer BS, der den Weg zu diesen aufteilt. Die RC Mappings werden direkt nach Ablauf des route-timeout gelöscht, bleiben auf der alten Route aber noch einige Zeit lang gültig. Diese Tatsache nützt der im Anschluss diskutierte semi-soft Handoff aus, der die Handoffdauer zu minimieren versucht, um somit den Paketverlust zu reduzieren. Ein Update in der Crossover BS führt nach Erstellen der neuen Route dazu, dass keine Pakete mehr auf der alten Route übertragen werden. Als Handoff Latenzzeit bezeichnet man hier die Zeitspanne, die zwi-

schen der Handoff Initiierung und der Ankunft des ersten Paketes entlang der neuen Route, verstreicht.
Beim hard Handoff ist die Latenzzeit gleich der Roundtrip-Zeit zwischen MH und der Crossover BS. Während der Latenzzeit gehen Pakete möglicherweise verloren. Besonders gravierend wirkt sich der Paketverlust aus, wenn die Crossover BS gleich dem Gateway entspricht (worst-case Szenario). Dennoch ist der zeitliche Aufwand für ein erneutes Schicken der Pakete im Falle eines Paketverlustes deutlich geringer als bei Mobile IP, da lediglich lokale Knoten diesbezüglich informiert werden müssen. Bei Mobile IP hingegen müsste ein eventuell weit entfernter Home Agent damit beauftragt werden.

Es gibt Überlegungen, den Paketverlust durch eine Kommunikation zwischen alter und neuer BS während des Handoff zu reduzieren. Dafür könnte die neue BS ihrer Vorgängerin eine Nachricht senden, die einen anstehenden Handoff ankündigt. Nachdem die alte BS diese Nachricht erhalten hat, werden Pakete, die sie von jetzt ab empfängt, an die neue BS und den MH geschickt. Jedoch gehen an die alte BS adressierte Pakete wiederum verloren, wenn die Benachrichtigung über den bevorstehenden Handoff noch nicht vollständig abgewickelt wurde. Ist die Zeitdauer, die für die Benachrichtigung nötig ist (Notification Time, z.B. die Roundtrip-Zeit zwischen alter und neuer BS) dabei größer als die eigentliche Dauer des Handoffs (z.B. die Round-Trip Zeit zwischen neuer und Crossover BS) führt dieser Ansatz nicht zu einer bedeutenden Verbesserung des Handoffs. Nur wenn die Notification Time deutlich kleiner ist macht sich eine Verbesserung bemerkbar. Ein weiterer Nachteil dieser Methode ist die zusätzliche Kommunikation und ein wesentlich größerer Signalisierungsoverhead, beides störende Nebenprodukte bei dem Wunsch nach einem schnellen Handoff.

Semi-soft Handoff

Diese Art von Handoff skaliert sehr gut für eine sehr große Anzahl von MHs mit jeweils häufigen Handoffs. Der MH löst den semi-soft Handoff durch das Abschicken eines Route-Update Paketes an die neue BS aus, bleibt dabei aber mit der alten BS verbunden. Das Route-Update Paket hat einen besonderen Parameter gesetzt, der anzeigt, dass ein semi-soft Handoff kurz bevor steht, deshalb nennt man dieses Route-Update Paket auch semi-soft Paket. Das semi-soft Paket erzeugt neue Mappings im RC und auch im PC. Wenn das semi-soft Update-Paket die Crossover BS (dort, wo sich alter und neuer Pfad kreuzen) erreicht, wird dort ein neues Mapping dem Cache hinzugefügt, anstatt das alte zu ersetzen. Dies ermöglicht das Senden von Paketen sowohl zur neuen, als auch zur alten BS. Während der Erzeugung neuer Mappings für die neue Route bleibt der MH mit der alten BS verbunden. Nach einem semi-soft Delay (Werte proportional zur round-trip Zeit zwischen MH und Gateway) führt der MH den eigentlichen Handoff erst aus. Das Delay stellt sicher, dass während dem Zeitpunkt, in dem der MH tatsächlich zur neuen BS wechselt, die Pakete sowohl auf der alten, als auch auf der neuen Route gesendet werden (vgl. Abbildung 7). Während dieser Zeit verbrauchen die gesendeten Pakete natürlich die doppelte Anzahl an Ressourcen, allerdings ist der Zeitrahmen dieses Prozesses im Hinblick auf die Gesamtdauer des Handoffs so gering, dass er sich nicht merkbar auf den kompletten Handoff auswirkt.

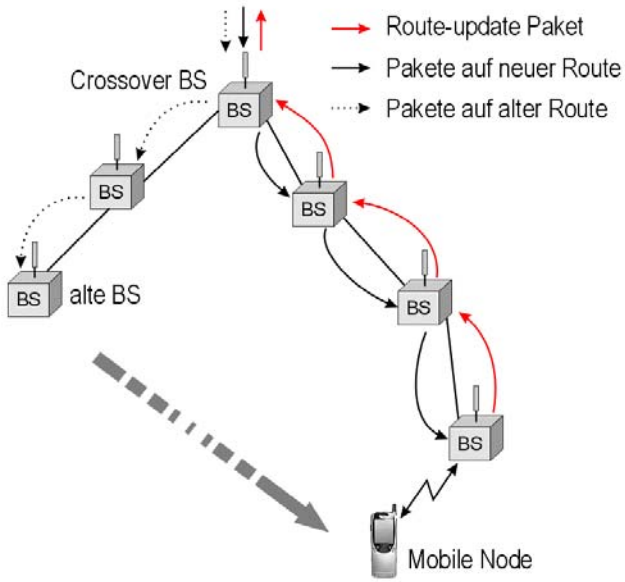


Abbildung 7: Semi-soft Handoff.

Das Aufbauen einer neuen Route bevor der MH tatsächlich zur neuen BS wechselt, sorgt dafür, dass der MH gleich nach dem semi-soft Handoff ohne Unterbrechung weiter Pakete empfangen kann. Allerdings sind die Paketströme auf der alten und neuen Route zueinander nicht synchronisiert. Hohe Netzlast oder einfach die Struktur des Netzes können die Übertragungszeiten von Crossover BS zur alten BS respektive neuen BS unterschiedlich ausfallen lassen

Liegt die neue BS hinter der alten wird der MH Duplikate erhalten, was sich für die meisten Applikationen jedoch nicht störend auswirken dürfte. Im entgegengesetzten Fall werden Pakete jedoch verloren gehen. Da eine zufriedenstellende Synchronisation zu komplex wäre, als dass sie während des semi-soft Handoffs eingesetzt werden könnte, versucht man das Problem dadurch zu umgehen, dass der Paketstrom auf dem neuen Pfad (zwischen Crossover BS und neuer BS) durch ein kurzzeitiges Delay verzögert wird. Diese Verzögerung muss dafür sorgen, dass der Zeitunterschied zwischen altem und neuem Pfad mit sehr hoher Wahrscheinlichkeit ausgeglichen wird. Idealerweise wird der Mechanismus, der den Delay steuert, in der Crossover BS implementiert. Ob der Delay angewendet wird oder nicht, entscheidet die Crossover BS mit dem Erhalt des semi-soft Update-Paketes, in dem durch ein Flag angezeigt wird, ob die Pakete den Delay passieren müssen oder nicht. Nachdem der Handoff vollständig ist, schickt der MH ein Daten- oder Route-Update Paket in Richtung Gateway. Diese Pakete sorgen dafür, dass das Delay-Flag in der Crossover BS gelöscht wird. Die Folge davon ist, dass die dort gepufferten Pakete in Richtung MH losgeschickt werden.

5 Sicherheit

Oftmals ergeben sich in mobilen Szenarien für die beteiligten Komponenten beträchtliche Sicherheitsprobleme, die man im LAN nicht vorfindet. Im WLAN ist vor allem die Tatsache, dass Datenpakete abgehört werden können, problematisch. Mobile MHs jedoch müssen häufig Informationen über ihren Aufenthaltsort über die Luftschnittstelle versenden. Die dafür verwendeten Steuernachrichten können zum entscheidenden Sicherheitsrisiko werden, wenn keine ausreichenden Schutzmaßnahmen getroffen wurden.

Cellular IP implementiert Mechanismen, um die Mobilität sicherer zu machen. Ein Schritt in diese Richtung ist, dass ausschließlich authentifizierte Kontrollpakete Cache Mappings in den Knoten des Cellular IP Netzes erzeugen oder verändern können. Route-Update und Paging-Update Pakete müssen sich also bei Bedarf im Knoten authentifizieren können. Dies verhindert Man-in-the-middle Attacken. Auf die Authentifizierung von regulären Datenpaketen wird in Hinsicht auf die Transportgeschwindigkeit bewusst verzichtet. Dies ist aber kein Nachteil, da reguläre Datenpakete existierende Mappings im Cache lediglich auffrischen, nicht aber ändern oder gar erzeugen können.

MHs verwenden in Cellular IP einen Session Key, um sich zu authentifizieren. Da ein schneller Handoff mit möglichst wenig Verzögerung gewünscht wird, muss der Session Key bei der neuen BS sofort verfügbar sein. Dafür könnte die neue BS während des Handoffs eigentlich den Session Key durch Kontaktaufnahme mit der alten BS, der Crossover BS oder einem zentralen Schlüsselverwaltungsknoten anfordern [1]. Dies würde allerdings zu erheblichem Verkehr innerhalb des Cellular IP Netzes führen. Also wird in Cellular IP Netzen ein jeweils ganz spezieller Session Key verwendet, den BSs unabhängig voneinander berechnen können. Dieser Session Key $K_{session}$ ist ein MD5-Hash über die folgenden Bestandteile

- Die IP-Adresse des MH (IP_{MH})
- Eine Zufallszahl (R_{MH}), die dem MH bei der ersten Registrierung im Netz zugewiesen wird
- Einen Cellular IP Netz-Schlüssel ($K_{network}$), der allen BS innerhalb des Netzes bekannt ist.

$$K_{session} = \text{MD5}\ (IP_{MH}, R_{MH}, K_{network})$$

Wenn ein MH den Wunsch hat, in ein Cellular IP Netz einzutreten, muss er den Registrierungsprozess durchlaufen. Dabei wird der Session Key für den MH berechnet und zusammen mit dem Zufallswert R_{MH} an ihn geschickt. Kontrollpakete enthalten diesen Zufallswert und führen neben dem Session Key zur Authentifizierung außerdem einen Zeitstempel mit sich, um Replay-Attacken vorzubeugen.

BS können beim Empfang eines Kontrollpaketes nun ganz einfach den Session Key berechnen, in dem sie den MD5-Hash über die im Kontrollpaket gefundene IP-Adresse des MH, sowie den übertragenden Zufallswert und dem nur ihnen bekannten Netzschlüssel bilden und den berechneten Wert mit dem empfangenen Hashwert vergleichen. Der Authentifizierungsprozess findet ausschließlich lokal in der BS statt,

ohne weitere Kommunikation mit Komponenten des Netzes. Durch dieses Verfahren wird ein schneller Handoff gewährleistet. Der Entwurf des Sicherheitskonzeptes in Cellular IP empfiehlt den Session Key in regelmäßigen Abständen zu ändern, um Brute-Force-Angriffe zu erschweren.

Im Zusammenspiel mit Mobile IP können die Sicherheitsfunktionen natürlich entsprechend umfangreicher ausfallen. Im globalen Zusammenspiel der einzelnen Cellular IP Subnetze als dynamischer Verbund in einem Mobile IP Internet können stärkere Anforderungen, die für den kommerziellen Erfolg der Protokolle unerlässlich sind, umgesetzt werden. Dabei kann bei der Authentifizierung (**A**uthentication), der Authorisierung (**A**uthorization) und einem Abrechnungssystem (**A**ccounting, **AAA**) mehr Wert auf eine global skalierbare Lösung als auf die Unterstützung eines schnellen Handoffs gelegt werden.

6 Evaluierung

Testumgebung

Das Ziel der folgenden Untersuchungen ist es, Erkenntnisse über die Geschwindigkeit und die Skalierbarkeit von Cellular IP zu gewinnen. Die Tests basieren alle auf der Testumgebung aus Abbildung 8. Cellular IP wurde dafür in FreeBSD 2.2.6 (jedoch werden Windows und Linux auch unterstützt) implementiert und getestet. Für die Verarbeitung und das Weiterleiten von IP Paketen wird der Berkeley Packet Filter's Packet Capture Library (PCAP) verwendet.

Die Testumgebung ist ein Cellular IP Netz, dessen Hauptkomponenten drei BSs (300 MHz Pentium PC) sind. Die BSs sind untereinander über 100 Mb/s full duplex Leitungen verbunden, wobei BS 1 auch als Gateway zum Mobile IP Internet dient. Als MH kommt ein 300 MHz Pentium Notebook zum Einsatz, welches mit einer 2 Mb/s WaveLAN 2.4 GHz Funkverbindung Kontakt mit den BSs aufnimmt. Diese Funkverbindung kann auf bis zu acht verschiedenen Frequenzen arbeiten, um Interferenzen zwischen benachbarten Zellen zu vermeiden. Um einen Handoff unabhängig von der Signalstärke simulieren zu können, hat der MH die Fähigkeit, seine Frequenzen dynamisch zu ändern. BSs jedoch besitzen jeweils eine statisch vergebene Frequenz. Der MH befindet sich hier in einer Region von sich überlappenden Funkzellen. Um einen Handoff manuell durchzuführen, wurde im MH eine Funktion implementiert, welche den Handoff durch Programmsteuerung auslöst, egal, wie stark die gerade gemessenen Signalqualitäten der BS sind. Die gewonnenen Erkenntnisse und Diagramme spiegeln die Ergebnisse der Testreihen vollständig wieder, die von den Entwicklern ursprünglich durchgeführt wurden [2].

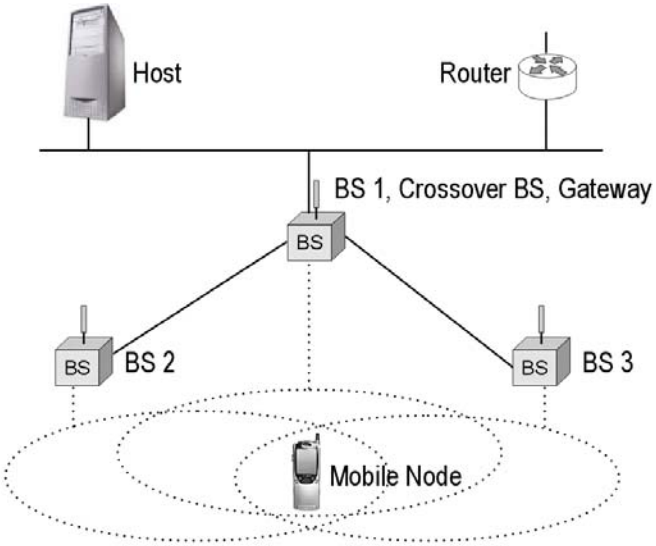


Abbildung 8: Aufbau der Testumgebung für die Geschwindigkeits- und Skalierbarkeitstests von Cellular IP.

UDP Performance während hard und semi-soft Handoff

Die Messergebnisse zu dieser Testreihe sind in Abbildung 9 zu sehen. Jeder Punkt im Diagramm ergibt sich aus dem Durchschnittswert der Paketverluste, die über 50 Handoffs hinweg gemessen wurden.

Bei den Tests zur UDP Performance während hard und semi-soft Handoff empfängt der MH ständig 100 Byte UDP-Pakete (25 bzw. 50 Pakete pro Sekunde [pps]) und führt regelmäßig im Abstand von fünf Sekunden einen Handoff zwischen BS 2 und BS 3 durch.

Für die Testreihe zum semi-soft Handoff wurde ein Delay in der Crossover BS 1 verwendet, welches die Pakete in einem Puffer solange speichert, bis das nächste Downlink-Paket dort ankommt. Erst dann wird das gepufferte Paket entlang der neuen Route zur neuen BS losgeschickt. Wenn der semi-soft Handoff komplett ist, wird das letzte Paket aus dem Puffer gelöscht und in Richtung MH geschickt. In dem Diagramm auf der folgenden Seite ist zu sehen, dass der semi-soft Handoff den Paketverlust vollständig verhindert! Besonders interessant ist dabei die Tatsache, dass es selbst bei einer sehr hohen Roundtrip-Zeit zwischen MH und Gateway ausreicht, lediglich einen 1-Paket-Puffer in der Crossover BS zu implementieren, um den Paketverlust zu eliminieren.

Für den hard Handoff fallen die Ergebnisse weniger positiv aus. Der Paketverlust beim hard Handoff ist sogar proportional zur Roundtrip-Zeit und der Downlink-Paketrate. Selbst für eine sehr geringe Roundtrip-Zeit zwischen MH und Gateway geht mindestens ein Paket verloren, im schlimmsten Fall gibt es einen Verlust von vier Paketen bei einer Roundtrip-Zeit von 80ms.

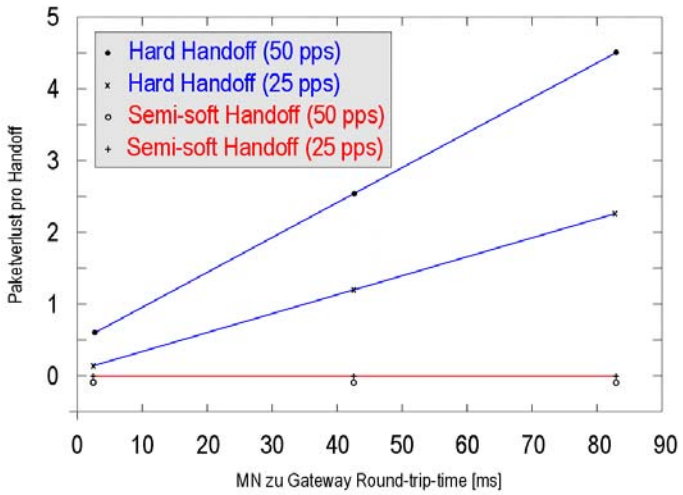


Abbildung 9: UDP-Paketverlust bei verschiedenen Handoffs (pps: Pakete/Sekunde).

TCP Performance während hard und semi-soft Handoff

Für diesen Test führt der MH wiederum regelmäßig Handoffs zwischen BS 2 und BS 3 durch und lädt dabei 16 MB Daten von einem Correspondent Node herunter. Die Messpunkte in Abbildung 10 sind dabei ein Mittelwert von jeweils sechs unabhängigen Messungen. Ziel dieser Testreihe ist es zu untersuchen wie sich der TCP Datendurchsatz in Abhängigkeit zur Anzahl der Handoffs verhält.

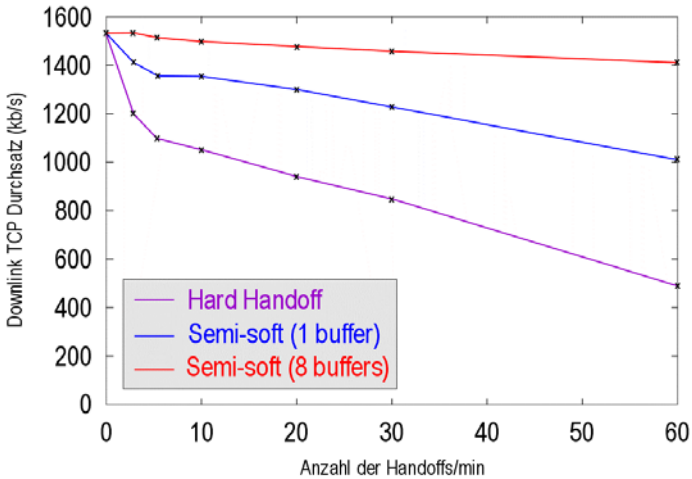


Abbildung 10: Downlink TCP Datendurchsatz beim Handoff.

Der Datendurchsatz bei keinem Handoff fällt ein wenig geringer aus als die 1,6 Mb/s bei regulärem IP Routing, da IP Routing im Kernel und Cellular IP im User-Mode implementiert ist. Hinzu kommt, dass Cellular IP in diesem Test auf PCAP basiert, welches nicht für IP Forwarding optimiert wurde.

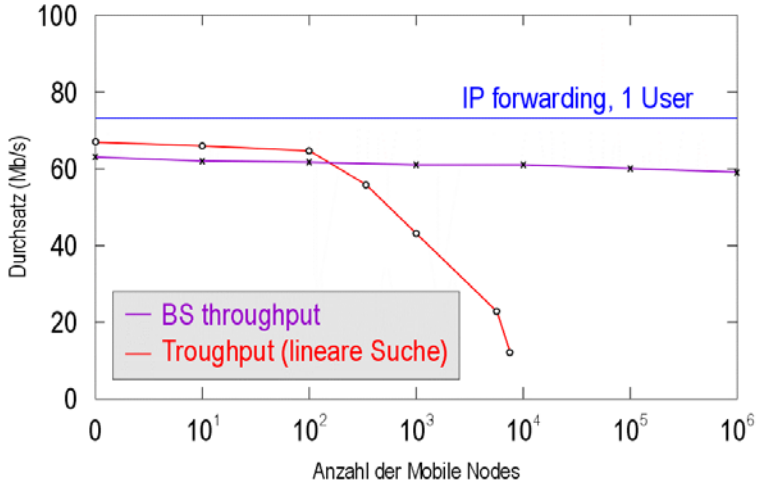
Im Diagramm lässt sich deutlich der sinkende TCP Datendurchsatz bei steigender Anzahl von hard Handoffs pro Minute aufgrund von zunehmendem Paketverlust feststellen. Der abnehmende TCP Datendurchsatz bei einer steigenden Anzahl von Handoffs pro Minute ergibt sich daraus, dass TCP vorangegangene Paketverluste durch Neuanforderung kompensieren muss und dadurch Zeit verliert. Diese Zeit summiert sich im Verlauf des Experiments: TCP kann sich von den Paketverlusten nicht mehr erholen, was zu einem kleineren TCP Datendurchsatz führt.

Die Kurve für den semi-soft Handoff bei einem 1-Paket-Puffer in der Crossover BS verdeutlicht einen akzeptablen TCP Datendurchsatz. Im Vergleich zum hard Handoff konnte hier der Paketverlust verringert werden und damit liegt der Datendurchsatz bei gleicher Anzahl Handoffs pro Minute im Vergleich zum hard Handoff viel höher. Die beiden Paketströme zwischen alter und neuer BS sind nicht synchronisiert und in der Crossover BS exsistiert nur ein 1-Paket-Puffer, wodurch der Paketverlust bei höheren Handoff-Raten nicht vollständig vermieden werden kann, wie das bei UDP der Fall war. Das Puffern von Paketen ist bei TCP an die Paketankunftszeit gebunden, die sowohl kürzer als auch unregelmäßiger in TCP-Streams ist, als es bei den Tests zu UDP war. Synchronisation ist in Cellular IP aufgrund ihrer Komplexität jedoch nicht erwünscht, also wird mit dem Ersetzen des 1-Paket-Puffers durch einen 8-Paket-Puffer die Delay-Funktion in der Crossover BS verbessert. Nun geht der Paketverlust selbst für Handoff-Raten von einem Handoff pro Sekunde gegen Null.

Skalierbarkeit

Im folgenden Test wird untersucht, ob Cellular IP auch für eine enorm große Anzahl von active MHs im Cellular IP Netz effizient funktioniert. Für jedes Paket, das in Richtung MH geleitet wird, müssen die Routing Caches der Cellular IP Nodes durchsucht werden. Mit einer steigenden Anzahl von active MHs wächst der Routing Cache, wodurch besonders effiziente Suchalgorithmen zum Einsatz kommen müssen. Sollten Routing Cache Mappings fehlen, müssen auch noch Paging Caches durchsucht werden. Jedoch aktualisieren active MHs ihre RC Mappings ständig, so dass Paging Caches für dauernde Datenübertragungen nicht mehr durchsucht werden müssen. Effiziente Suchalgorithmen widerlegen jedoch den Verdacht, dass die Anzahl der User im Cellular IP Netz begrenzt ist. Vielmehr besitzt das Netz eine Obergrenze an aktiv kommunizierenden MHs.

Für den Test zur Skalierbarkeit wurden verschieden viele Mappings in den Routing Caches angelegt. Es ist gut zu beobachten, dass die Kurve zum Datendurchsatz im Diagramm auch für größer werdende Routing Caches (aufgrund steigender Anzahl von MHs) kaum fällt. Der BS-Datendurchsatz fällt nur geringfügig kleiner aus, als der gewöhnliche IP-Datendurchsatz. Dies kann auf die Verwendung von PCAP zurückgeführt werden. Die Wichtigkeit von effizienten Suchalgorithmen in den beteiligten



Caches macht die auf linearer Suche basierende Kurve deutlich. Die Ergebnisse zeigen, dass Cellular IP auch eine große Anzahl von MHs im Netz unterstützen kann.
Abbildung 11: Datendurchsatz in den BS.

7 Cellular IP im Vergleich mit GSM/GPRS

IP-basierte Servicetechnologien werden für die drahtlose Kommunikation immer wichtiger. Zellulare Netze werden als Standardmethode für den Zugang zum Internet oder anderen IP-basierten Netzwerken genutzt werden. Es gab bereits Ansätze, um zellulare Netze für einen paketorientierten Datenverkehr zu optimieren. Ein bekannter Vertreter dieser Ansätze ist GPRS (General Packet Radio Service), eine Erweiterung von GSM (Global System for Mobile Communications). In diesem Kapitel werden auf der Ebene der Mikromobilität kurz die Prinzipien von Cellular IP mit den angewandten Methoden in GPRS verglichen [4].

Netzwerkarchitektur

Cellular IP verwendet eine Struktur des Netzes, die der GPRS System-Architektur ähnlich ist. Beide Netzwerke sind unterteilt in mehrere Funkzellen, in denen sich mobile Teilnehmer mit Basisstationen verbinden können. Dabei dient der Serving GPRS Support Node (SGSN) als Hauptzugang zum Radio Access Network. Mittels einzelner Base Station Controller werden die Daten schließlich an die relevanten Base Stations verteilt, von wo aus sie zum MH weitergesendet werden. Der Gateway GPRS Support Node (GGSN) hingegen dient als direkte Schnittstelle zu externen IP-basierten Netzen (dem Internet und Intranets). Cellular IP ist ähnlich strukturiert. Das Gateway dient als Schnittstelle zu anderen Netzen, innerhalb des Cellular IP Netzes

selber sorgen einzelne Knoten für ein Routing der Daten zur relevanten BS, von der die Daten dann zum MH geschickt werden. In GPRS werden Datenpakete ebenfalls transparent zu externen Datennetzwerken transportiert. Dabei kommt Verschlüsselung und teilweise auch Tunneling zum Einsatz. Das GPRS Tunneling Protokoll (GTP) kommt dabei hauptsächlich zwischen GGSN und SGSN zum Einsatz. Cellular IP hingegen verwendet innerhalb des Netzes keinerlei Tunneling. Lediglich vom Cellular IP Gateway zum Home Agent werden die Daten getunnelt übertragen. Abbildung 12 zeigt die GPRS System-Architektur, die der des Cellular IP Netzes relativ ähnlich ist (Abbildung 2).

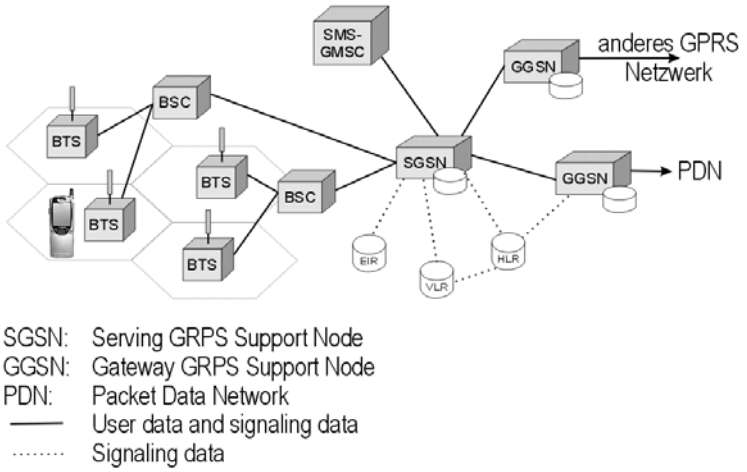


Abbildung 12: GPRS System-Architektur [6].

Eine gravierender Unterschied zwischen den beiden Netzwerken besteht jedoch hinsichtlich der Übertragungsart von Steuernachrichten. In GSM/GPRS gibt es eine feste Struktur von separaten logischen Kanälen, die zur Übertragung von Signalisierungsinformationen verwendet werden. In Cellular IP hingegen gibt es keinerlei statische Struktur von getrennten logischen Kanälen. Daten für ein verteiltes Location Management werden in den verschiedenen Cellular IP Nodes gespeichert. Route-Update und Paging-Update Pakete, sowie reguläre IP-Datenpakete werden dafür genützt, um Down- und Uplink-Routen für mobile Teilnehmer zu ermöglichen.

Protokollvergleich auf Ebene der Mikromobilität

Cellular IP implementiert einige Konzepte zur Unterstützung von Mikromobilität, die ähnlich zu Methoden sind, die in GSM/GPRS auftauchen. So gibt es in Cellular IP ebenfalls ein Zustandskonzept für MHs. Die beiden Zustände ready und standby werden in Cellular IP durch active und idle nachempfunden. Details über die Zustände beider Systeme werden in Kapitel 3 genauer besprochen.

GSM/GPRS unterstützt durch Paging einen Mechanismus, der es ermöglicht, passive Konnektivität von MHs umzusetzen. Auch Cellular IP implementiert Paging-Konzepte, die denen von GSM/GPRS sehr ähneln. Das Netz muss bei Cellular IP den Bewegungen eines active MH von BS zu BS ständig folgen, um weiterhin in der Lage zu sein, Pakete ohne Unterbrechung und ohne ein erneutes Suchen des MHs im Netz zu übertragen. Active MHs müssen das Netzwerk über jeden Handoff informieren. Diese grundlegende Eigenschaft sind kennzeichnend sowohl für Cellular IP, als auch GPRS.

Eine weitere Ähnlichkeit beider Systeme lässt sich in der Strukturierung von BS finden. In Cellular IP entsteht eine Paging Area durch die Gruppierung von mehreren BS. Idle MHs, die die Funkzellen innerhalb einer Paging Area wechseln, müssen keinerlei Steuernachrichten übertragen, um ihre neue Position mitzuteilen. Nur, wenn die neue BS sich dabei in einer anderen Paging Area befindet, wird ein Location Update nötig. Dies entspricht dem Konzept der Routing Areas bei GPRS: MHs informieren den SGSN, wenn sie eine neue Routing Area betreten, nicht jedoch wenn sie einzelne Zellen innerhalb derselben wechseln. Für die Identifizierung von möglichen Paging Areas werden in Cellular IP regelmäßig Beacons über das gesamte Netz geflutet. In diesem Paket befindet sich unter anderem ein eindeutiger Bezeichner für eine Paging Area, der es dem MH erlaubt festzustellen, ob der die Paging Area gewechselt hat oder nicht. GPRS verwendet einen separaten Broadcast-Kanal für die Übertragung solcher Informationen zur Unterscheidung von Routing Areas.

Der gesamte Netzwerkverkehr in GPRS ist in spezifische Rahmenstrukturen gegliedert. Das Routing von Datenrahmen hängt mit der Netzwerktopologie zusammen. Eine BS ist immer mit einem Base Station Controller (BSC) verbunden. Ein BSC ist direkt mit einem SGSN in Verbindung. Befindet sich ein MH im ready Zustand, so weiß sowohl der zuständige BSC, als auch der SGSN in welcher Funkzelle sich der MH aufhält. Basierend auf diesen Informationen werden die Datenrahmen zum MH verschickt. Bei Cellular IP hingegen gibt es keine zentrale Stelle im Netz, die die exakte Aufenthaltsinformation des MH kennt. Informationen werden etappenweise von Knoten zu Knoten weitergeleitet. GPRS kennt kein IP Routing für Daten innerhalb des GPRS Netzes.

Eine letzte, hier erwähnte, Gemeinsamkeit beider Systeme ist, dass der Handoff jeweils durch den MH initiiert wird. Auch in GPRS kann der MH selbstständig einen gewünschten Zellwechsel initiieren. Für die Selbständigkeit der MHs in diesem Fall gibt es keine nennenswerten Gründe, bis auf die Tatsache, dass beide Systeme darauf basieren Ressourcen je nach Bedarf anzufordern. Dafür entscheiden MHs autonom, ob die Signalqualität der momentanen BS ausreicht für eine vernünftige Übertragung der Daten.

8 Zusammenfassung

In dieser Ausarbeitung wird das Design, die Implementierung und eine Evaluierung von Cellular IP vorgestellt. Das Protokoll ist ein neuer Schritt in Richtung Mikromobilität in Umgebungen mit sehr vielen mobilen Endgeräten. Die für das Protokoll entwickelten Algorithmen sind einfach und sie skalieren gut. Deshalb reicht für eine

Umsetzung von Cellular IP momentan erhältliche PC-Hardware, Betriebssysteme und Funkverbindungen vollkommen aus. TCP- und UDP-Applikationen können dank der in Cellular IP unterstützen nahtlosen Mobilität selbst in Extremsituationen effizient und stabil ihre Aufgaben erledigen. Eine eventuell sich störend auswirkende Netzlast durch Protokolloverhead lässt sich durch eine effiziente, an die jeweilige Situation angepasste, Parametrisierung der Timeouts, sowie durch eine beliebig anpassbare Struktur der Paging Areas umgehen. Hinzu kommt, dass der im Cellular IP Netz auftretende Protokolloverhead nur innerhalb des Netzes auftritt. Diese Transparenz von Cellular IP ermöglicht eine Partnerschaft mit Mobile IP.

Sowohl Mobile IP als auch Cellular IP besitzen im Alleinbetrieb Schwächen, die einen flächendeckenden Einsatz als Grundlage zur Mobilität vieler mobiler Endgeräte unmöglich machen. Nur durch die Kombination beider Protokolle lässt sich eine flächendeckende Netzwerktopologie aufbauen, die dem mobilen Teilnehmer den drahtlosen Zugang zu Diensten des Netzes im Einklang mit hoher Bewegungsfreiheit ermöglicht. In so einem Szenario existieren viele eigenständige Cellular IP Netze nebeneinander. Verbunden sind sie durch ein Mobile IP-basiertes Internet. Die Cellular IP Gateways dienen dabei als Foreign Agents. Der MH bewegt sich innerhalb des Cellular IP Netzes transparent zur restlichen Netzwerktopologie. Sobald er dieses verlässt und in ein anderes Cellular IP Netz wechselt, wird die Adresse des neuen Gateways als care-of Adresse beim Home Agent registriert. Diese care-of Adresse ist dann wiederum für das gesamte Cellular IP Netz gültig.
Jedoch bleibt die Kommunikation mit dem Home Agent bei Mobile IP der Hauptkostenfaktor bei einer flächendeckenden Zusammenarbeit beider Protokolle. Die dafür in Mobile IP diskutierten Lösungen, wie Triangle Routing und Reverse Tunneling, bieten interessante Ansätze [5], verschwenden jedoch signifikant viel Bandbreite. In den Nachfolger Mobile IPv6, zur Zusammenarbeit mit Cellular IP, werden deshalb schon heute große Hoffnungen gesetzt.

Im Moment ist Cellular IP noch kein RFC, sondern immer noch Gegenstand laufender Entwicklungen und Forschungen. Die Entwickler beschäftigen sich mit einer passenden QoS-Erweiterung ihres Protokolls, um auch sensible Multimediadienste zu unterstützen. Des weiteren werden Forschungen über das Protokollverhalten bei Knotenausfällen betrieben. Besonderes Interesse darf dabei dem Problem der Routenkonsistenz und der Zeit, die zum erneuten „Hochfahren“ des Netzes nach einem Fehler benötigt wird, geschenkt werden.

Weiterführende Informationen zum Protokoll, sowie den Source Code, gibt es auf der Webseite der Entwickler: http://comet.columbia.edu/cellularip

Referenzen

[1] Andrew T. Campbell, Javier Gomez, Sanghyo Kim, Andras G. Valko, Chieh-Yih Wan (Columbia University New York), Zoltan R. Turanyi (Technial University of Budapest): “Design, Implementation and Evaluation of Cellular IP”, IEEE Personal Communications (August 2000).

[2] Andrew T. Campbell, Javier Gomez, Andras G. Valko: “An Overview of Cellular IP”, IEEE Personal Communications (1999).

[3] Sanghyo Kim: “Cellular IP Manual - www.comet.columbia.edu/cellularip”, Comet Group in Columbia University (1999).

[4] Sami Ala-Luukko: “Mobility Management in IETF and GPRS Specifications”, Department of Computer Science and Engineering Helsinki University of Technology (May 2000).

[5] Charles E. Perkins (Sun Microsystems): “Mobile IP”, IEEE Personal Communications (May 1997).

[6] A. Küpper, C. Linnhoff-Popien: „Mobilkommunikation II“, Institut für Informatik der Ludwig-Maximilians-Universität München (2003).