

Mikromobilität

Seminar Kommunikation und Multimedia WS 2002/2003

Justus von Richthofen <j.richthofen@tu-bs.de>

Betreuer: Marc Bechler
Institut für Betriebssysteme und Rechnerverbund
Technische Universität Braunschweig

1. Abstract

Die Entwicklung der Technologien in der drahtlosen Kommunikation hat in letzter Zeit große Fortschritte gemacht, so dass es immer mehr Internetnutzer gibt, die drahtlos an das Internet angebunden sind. Drahtlose Netzwerke sind die Technologie der Zukunft, da sie flexibler und mittlerweile auch günstiger als drahtgebundene Netzwerke sind. Mikromobilität beschäftigt sich speziell mit der mobilen drahtlosen Kommunikation in geographisch begrenzten Räumen, in denen der mobile Nutzer häufig die Basisstation wechselt (z.B. Autofahrer auf der Autobahn). Um die verschiedenen Probleme, die bei drahtlosen Internetanwendungen derzeit und zukünftig auftreten können, zu bewältigen, wurde in letzter Zeit viel an der Entwicklung spezieller Mikromobilitätsprotokolle gearbeitet. Ziel ist es, dem drahtlosen Internetsurfer mindestens dieselben Leistungen zu liefern, die ein drahtgebundener Internetsurfer genießt. Große Probleme bereiten vor allem die Weitergabe (auch Handoff oder Handover) von einer Basisstation zur anderen, denn diese führt häufig zur verzögerten Ankunft einer Nachricht beim Empfänger oder sogar zum Verlust der Nachricht. Bei den immer populärer werdenden Echtzeit-Anwendungen (z.B. „Voice over IP“ oder Videokonferenz), ist es äußerst wichtig, Verzögerung und Paketverlust zu minimieren. In dieser Arbeit werden die wesentlichen Lösungsansätze für die erwähnten und weitere Probleme vorgestellt, bewertet und verglichen. Zuletzt wird noch ein Ausblick in die Zukunft gegeben.

2. Einleitung

In den letzten Jahren hat eine rasante Entwicklung im Bereich des drahtlosen Internetzugangs stattgefunden. Immer mehr Geräte besitzen die Fähigkeit, z.B. über Funk mit dem Internet zu kommunizieren, ohne auf einen Kabelanschluss angewiesen zu sein. Von Laptop und PDA bis hin zu Autos und Haushaltsgeräten (embedded systems) wird mittlerweile fast alles per WLAN, Bluetooth oder ähnlichen Funktechniken an das Internet angebunden. Bereits im Jahre 2000 war über 20% der verkauften PCs portabel [1] und auf der CeBIT 2002 war die drahtlose Kommunikation als der Trend der Zukunft zu erkennen.

Die Benutzer mobiler Endgeräte wollen denselben Service zur Verfügung haben wie an einem stationären Endgerät (z.B. ein PC), das per Kabel an das Netz angebunden ist. Hier zeigen sich die ersten Probleme, denn die heutigen Internet-Protokolle (IPv4) wurden damals nicht für diese Anforderungen ausgelegt, weil der Trend zur drahtlosen Kommunikation noch nicht zu erkennen bzw. die Technik noch nicht vorhanden war.

Es stellt sich beispielsweise die Frage, wie drahtlose Echtzeitanwendungen (z.B. Voice over IP) beim Wechsel der Basisstation ohne Unterbrechung der Kommunikation realisiert werden können, oder wie die Sicherheit des Informationsaustausches gewährleistet werden kann bei gleichzeitiger Minimierung der Steuerungsdaten für das Netzwerkmanagement. Diese Daten

werden auch als Verwaltungsinformation (Networkoverhead) bezeichnet. Dazu gehören beispielsweise IP-Header, die jedem Datenpaket vorangestellt sind, sowie Nachrichten zur Koordination des Netzwerkverkehrs.

Mikromobilität beschäftigt sich speziell mit der mobilen drahtlosen Kommunikation in geographisch begrenzten Räumen, in denen der mobile Nutzer häufig die Basisstation wechselt (z.B. Autofahrer auf der Autobahn). Schon seit längerem haben sich Wissenschaftler mit den Problemen beschäftigt, die bei mobilen Endgeräten in WANs und LANs auftreten. Eine erste Lösung für diese Probleme ist Mobile IPv4, das es einem Client ermöglicht, sich im Internet mit einer statischen IP-Adresse zu bewegen und trotzdem auf der ganzen Welt unter dieser IP-Adresse erreichbar zu sein.

Mikromobilitäts-Protokolle gehen noch einen Schritt weiter, denn Mikromobilität bietet schnelle, nahtlose Vernetzung in geographisch begrenzten Räumen, d.h. die Protokolle werden dort eingesetzt, wo mobile Netzteilnehmer so häufig ihren Ort wechseln, dass nicht einmal das Mobile-IP-Protokoll den Ansprüchen des Benutzers gerecht werden kann (siehe Kapitel 3). Problematisch bei der Weitergabe (Handover oder Handoff) des mobilen Clients von einer Basisstation zur anderen ist die oft auftretende Verzögerung (Delay) und der Paketverlust. Verzögerung bezeichnet die Zeit, die ein Paket vom Zeitpunkt des Absendens bis zum Zeitpunkt des Empfangens benötigt. Die physikalische Distanz zwischen zwei Endpunkten ist bereits ein wichtiger Faktor bei der Verzögerung. Wie lange ein Signal benötigt, um von einem Ende des Netzes zum anderen zu gelangen, nennt sich „Propagation“. Der hier entstehende Propagation-Delay ist proportional zur Lichtgeschwindigkeit und bezeichnet die Zeit, die ein physikalisches Signal benötigt, um Kupfer, optische oder kabellose Medien zu überbrücken. So ist der Propagation-Delay zwischen München und Sydney wesentlich höher als zwischen München und Frankfurt. Jedes Netzwerk-Gerät zwischen den Gesprächspartner führt zu weiteren Verzögerungen. Das Datenpaket braucht Zeit, um Router, Firewalls, Basisstationen oder andere Geräte zu passieren. Bei einigen Geräten ist der hinzugefügte Delay relativ konstant und damit einfach berechenbar. Bei anderen wiederum, insbesondere Router zählen hierzu, vergrößert sich die Verzögerung mit wachsender Paketmenge.

Von vielen verschiedenen Ansätzen zur Mikromobilität haben sich drei als besonders geeignet herauskristallisiert: Hierarchical Mobile-IP, Cellular IP und HAWAII. Die Protokolle werden zur Zeit von der IETF Mobile-IP Working Group auf ihre Eignung untersucht.

Zunächst werden die Anforderungen an Mikromobilitätsprotokolle besprochen und danach in Kapitel 3 die drei wesentlichen Protokollansätze ausführlich dargestellt. Am Ende kommen die Schlussfolgerung mit Bewertung der einzelnen Lösungen sowie ein Ausblick mit Bewertung von Zukunftschancen der Mikromobilitäts-Protokolle.

2. Anforderungen an Mikromobilitätsprotokolle

Im Allgemeinen sollten Mikromobilitätsprotokolle gewährleisten, dass der Datenverkehr möglichst selten unterbrochen wird, dass die Netzwerkressourcen effizient genutzt werden und dass das Netz gut skalierbar und zuverlässig ist.

Unterbrechungen im Datenverkehr treten häufig während der Weitergabe (2.1) von einer zur anderen Basisstation auf oder, wenn die Verbindungsqualität schlecht ist. Da Netzwerkressourcen gerade im Funkbereich ein knappes Gut sind, muss damit sparsam umgegangen werden. Der Datenverkehr besteht aus Verwaltungsinformationen (z.B. IP-Header und sonstige Steuerdaten) und Nutzdaten (z.B. Video-Stream). Um möglichst viele Nutzdaten übertragen zu können, muss der Anteil an Verwaltungsinformationen möglichst niedrig gehalten werden. Skalierbarkeit beschreibt die Eigenschaft eines Netzes, sich flexibel erweitern zu lassen ohne dass dadurch die Performance der Anwendungen leidet. Skalierbarkeit ist einer der wesentlichen Erfolgsfaktoren des Internets denn wäre sie nicht gewährleistet gewesen, hätte nicht solch ein rapides Wachstum des Internets erreicht werden können. Deshalb ist Skalierbarkeit auch für Mikromobilitätsprotokolle eine wichtige

Eigenschaft, die sie besitzen sollten. Zuverlässigkeit ist ein weiterer wesentlicher Aspekt, er beschreibt den Umfang, in dem von einem Netz erwartet werden kann, dass es die beabsichtigte Funktion mit der erforderlichen Genauigkeit ausführt. Zuverlässigkeit lässt sich weiter aufteilen in Korrektheit, Robustheit (Toleranz gegenüber Fehlbedienung) und Ausfallsicherheit (Fehleranfälligkeit).

Um den Anforderungen des Benutzers, der mobil mit dem selben Service das Internet nutzen möchte, wie wenn er an einem per Kabel angebundenen statischen PC sitzt, gerecht zu werden, müssen vier wesentliche Probleme gelöst werden: die Weitergabe zwischen den Basisstationen (2.1), die ständige Erreichbarkeit (2.2), die Sicherheit (2.3) sowie der Quality of Service (2.4).

2.1 Fast Handoff (schnelle Übergabe)

Der Handoff von einer zur nächsten Basisstation ist ein Schlüsselereignis in der Mikromobilität. Er findet normalerweise auf der Ebene 2 (Data Link Layer) des OSI-Referenzmodells statt, muss aber auch von der Ebene 3 (Netzwerkschicht) unterstützt werden, um ideal zu funktionieren. Dabei stellen sich zwei Anforderungen: kein Verlust von IP-Paketen sowie möglichst wenig Verzögerung. Gerade bei Echtzeitanwendungen ist es sehr wichtig, dass die laufende Kommunikation beim Handoff zwischen zwei Basisstationen ohne Unterbrechung erfolgt, damit nicht wichtige Informationen verloren gehen.

2.2 IP-Paging [4]

Für das mobile Gerät selbst ist darüber hinaus das Vorhandensein eines Paging-Mechanismus von zentraler Bedeutung. Wie Desktop PCs innerhalb eines LANs soll auch das mobile Gerät ständig erreichbar sein, wenn es beispielsweise als Datenserver dienen soll. Im Gegensatz zu fest stationierten, verfügen die mobilen Geräte im Normalfall über keine externe Stromversorgung. Da Batterien und Akkus nur über eine begrenzte Zeitspanne ihre Energie abgeben können und das Senden von Daten oft erhebliche Energiemengen verschlingt, wird besonders hier nach Optimierungen gesucht. Das mobile Gerät soll in die Lage versetzt werden für das Netz erreichbar zu sein, ohne dabei aktiv seinen Standort bekannt geben zu müssen.

Dem Netzwerk muss dafür jedoch die Position des Gerätes bekannt sein. Dies setzt auf der einen Seite voraus, dass das Netzwerk jegliche Positionsänderung protokolliert und speichert. Auf der anderen Seite muss es einen Mechanismus geben, ein gesuchtes mobiles Gerät aufzufinden. Bewegt sich das mobile Gerät, ohne dass es zu diesem Zeitpunkt Verbindungen zu anderen Rechnern geöffnet hat, so soll es trotz dieser Bewegung weiterhin erreichbar bleiben, ohne sich an einer neuen Basisstation registrieren zu müssen. Dies schont die Batterien, verursacht jedoch zugleich das Problem, dass das Netz nichts von dieser Bewegung mitbekommt und nicht mehr weiß, wo sich das Gerät aufhält.

Für den Fall, dass nun Datenpakete zugestellt werden müssen, dient das „Paging“. Über einen Broadcast kann das Gerät gerufen werden, um dessen neue Position zu ermitteln. Dabei werden zunächst nur alle Basisstationen in unmittelbarer Nähe der zuletzt bekannten Positionen diese Such-Broadcasts verschicken, bevor die Suche auf größere Gebiete ausgedehnt wird.

Alternativ teilen andere Protokolle das Netzwerk in verschiedene Paging-Bereiche ein. Anhand von empfangenen Broadcasts kann das mobile Gerät erfahren, in welchen Bereich es sich aufhält. Beim Wechsel zwischen zwei Basisstationen innerhalb des selben Paging-Bereichs kann es sich dann passiv verhalten und registriert sich erst wieder aktiv, wenn es sich in einen neuen Paging-Bereich bewegt.

2.3 Security

Ein Ziel von Mikromobilitätsprotokollen ist die Unterstützung schneller Handoffs bei mobilen Hosts. Dem entgegen wirken die Anforderungen an die Sicherheit während des Handoffs, da Mechanismen für die Sicherheit meist Netzwerk- oder Rechnerressourcen in Anspruch nehmen. Sicherheitsfunktionen sollten demnach einen schnellen Handoff unterstützen und Verwaltungsinformationen minimieren. Bisher gibt es hierfür noch keinen einheitlichen Standard. Die Authentifizierung bei der Ortsaktualisierung des mobilen Hosts ist unbedingt notwendig, um Hackern keine Angriffsfläche zu bieten.

Das Protokoll muss dafür sorgen, dass Authentifizierung (Benutzeridentifizierung), Autorisierung (Rechtevergabe) und Accounting (Rechnungskontrolle, Nutzungsanalyse, Abrechnung, etc.) (AAA) [5] geregelt und verfügbar sind. Dies wird in einigen Vorschlägen durch Session-Keys (Sitzungsschlüssel) gewährleistet, die bei der Weitergabe des mobilen Hosts von einer zur anderen Basisstation weitergeleitet werden.

2.4 Quality of Service (QoS)

QoS ist die Bereitstellung einer garantierten Dienstgüte in Bezug auf Geschwindigkeit und Zuverlässigkeit also beispielsweise die dauerhafte Bereitstellung eines Datenkanals zur Übertragung von Videodaten für eine Live-Konferenz. Bisher hat es kaum Untersuchungen gegeben, die sich mit QoS in der Mikromobilität beschäftigt haben, weil sich noch nicht einmal im drahtgebundenen Netzwerk ein Standard für QoS herausgebildet hat. In Ansätzen sind Funktionen für QoS in einigen Lösungen bereits vorgesehen.

3. Mikromobilitätskontrolle

Viele Internetnutzer besitzen mittlerweile einen Laptop oder ein sonstiges tragbares Gerät und wollen dauerhaften Zugang zum Internet haben, egal von welchem Ort. Dies ist aber aufgrund des IP-Adressierungssystems leichter gesagt als getan, denn Router auf der ganzen Welt haben in ihren Routingtabellen stehen, auf welchem Wege welche IP-Adresse erreicht werden kann. Wenn sich der Mobile Node (MN) plötzlich in einem anderen Subnetz befindet, würden die IP-Pakete nicht bei ihm ankommen, da die Routing-Informationen in den Routern nicht mehr stimmen. Es wäre keine gute Lösung, dem MN eine neue IP Adresse zu geben, da z.B. Anwendungen, Datenbanken o.ä. des Correspondent Nodes (CN) die ursprüngliche IP-Adresse gespeichert haben, um auf den MN zugreifen zu können. Um diese Probleme in den Griff zu bekommen, wurde Mobile-IP von einer Working Group des IETF entwickelt. Mobile-IP ist der derzeitige Standard für Makromobilität, d.h. für Mobilität nicht innerhalb sondern zwischen Netzen oder Domänen. Mobile-IP ist die Grundlage für Mikromobilitätsprotokolle und wird deshalb hier detailliert erläutert.

3.1 Grundlage: Mobile-IP (MIP)

Jedes Netz, das seinen Nutzern Mobilität ermöglichen will, muss bei MIP [1,16] einen „Home Agent“ (HA) bereitstellen, und jedes Netz, das fremden Nutzern Mobilität ermöglichen will, benötigt einen „Foreign Agent“ (FA). Wenn ein MN nun in einem fremden Netz auftaucht, kontaktiert er zuerst den FA und registriert sich. Der FA wiederum kontaktiert den HA des MN und gibt ihm eine „care-of address“ (CoA), was normalerweise die IP-Adresse des FAs ist. Wenn nun ein Paket für den MN in seinem Heimatnetz eintrifft (Abb.: 1, Schritt 1), versucht der Router, den MN dort zu erreichen. Befindet der sich derzeit nicht im Heimatnetz so leitet der Router die Pakete an den HA weiter, der die Pakete zur CoA tunnelt, indem er jedes IP-Paket in ein neues IP-Paket mit der CoA als Destination-IP einpackt (Abb.: 1, Schritt 2). Der FA entpackt das Paket und liefert es an den MN aus (Abb.: 1, Schritt 3). Die Antwort erfolgt nicht über einen Tunnel, sondern direkt (Abb.: 1, Schritt 4). Für den Fall dass es

keinen FA gibt, ist der MN selbst der FA, d.h. die Pakete werden vom HA direkt zum MN getunnelt (Abb.: 1, Schritt 5).

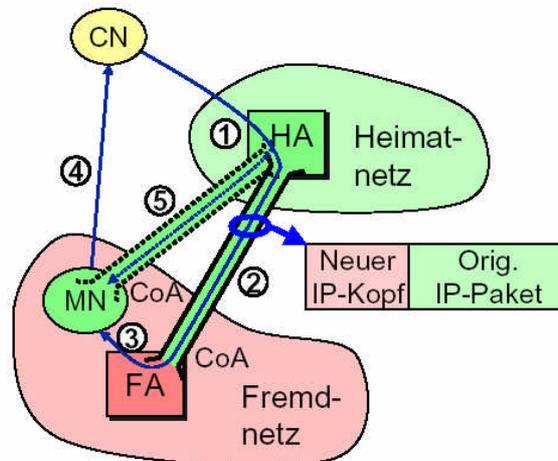


Abb.: 1 Mobile-IP (Quelle: Universität Karlsruhe (TH))

Daraus ergibt sich das sogenannte „Triangle Routing Problem“ (Abb. 2), denn alle Daten vom CN (Correspondent Node) an den MN (Mobile Node) gehen immer den Umweg über den HA. In Abbildung 2 werden die Daten immer über den Umweg Europa verschickt, obwohl sie auch direkt innerhalb der Vereinigten Staaten verschickt werden könnten. Als Lösung dieses Problems wird der Binding Cache auf der Seite des CN eingeführt. Dabei schickt der Home-Agent dem CN die Information, wo sich der MN befindet, dieser speichert sie temporär und kann die Daten nun direkt zum MN tunneln.

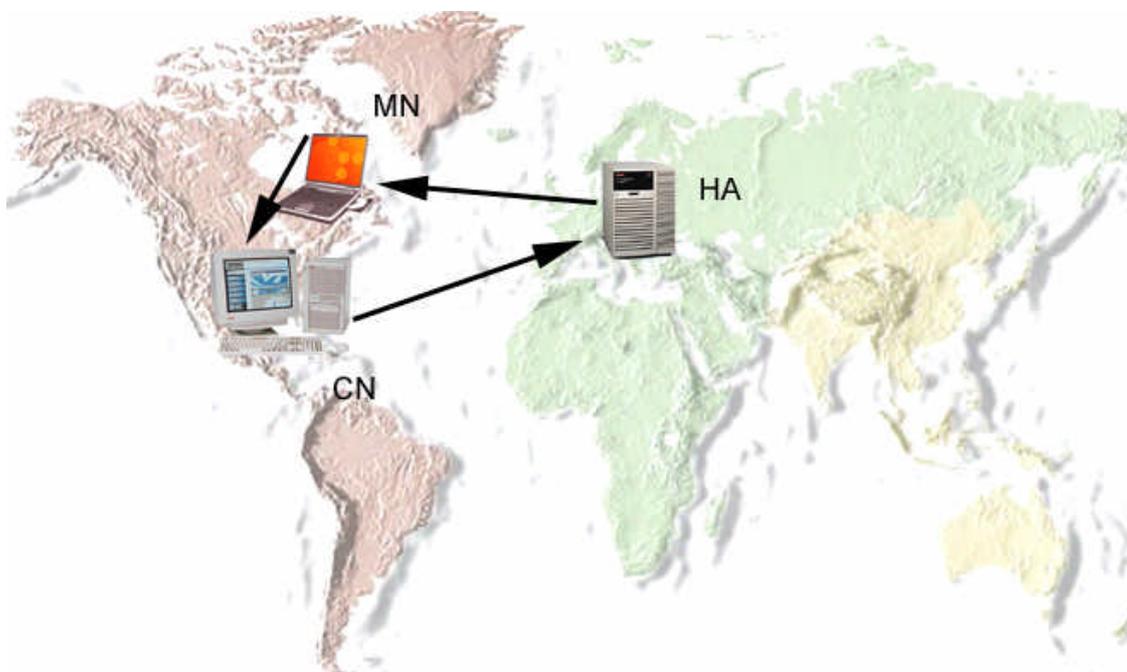


Abb. 2: Triangle Routing (Quelle: eigene Darstellung)

Auf den ersten Blick sieht der Rückweg für Pakete vom MN zu einem CN sehr einfach aus. Probleme bereiten aber die Sicherheitsmechanismen von Firewalls, die ein Paket oftmals passieren muss. Firewalls filtern verdächtige IP-Pakete heraus, wenn die Absenderadresse topologisch nicht korrekt ist. Eine Erweiterung [17] zu Mobile-IP löst dieses Problem, indem

auch auf dem Rückweg die Pakete getunnelt werden (reverse tunneling). Das erfordert allerdings, dass sowohl der MN als auch der CN tunneln kann.

Mobile-IP kann seine Stärken beim Wechsel zwischen Domänen ausspielen, genügt allerdings nicht den Anforderungen einer Mikromobilitätsumgebung, da die Verzögerung bei Registrierungsanfragen sehr groß ist und das Senden von Verwaltungsinformationen bei jedem Handoff zusätzlichen Netzwerkverkehr verursacht. Beides schränkt unter anderem den Quality of Service ein. Deswegen wurde Mobile-IP in Richtung Mikromobilität weiterentwickelt.

Die drei wichtigsten Protokolle werden im Folgenden vorgestellt. Andere Ansätze, deren Namen hier nur kurz erwähnt seien, sind z.B. Intra-Domain Mobility Management Protocol [6], 3 G Wireless [7], Edge Mobility Architecture [8], Proactive Handoff [9], Anchor Handoff [10], Session Initiation Protocol Mobility [11].

3.2 Hierarchical Mobile-IP (H-MIP)

Der „Hierarchical Mobile-IP“ Vorschlag [12] von Ericsson und Nokia benutzt eine Hierarchie von FAs, die hier Mobilitäts-Agenten (MA) genannt werden, um Mobile-IP Registrierungen lokal zu verwalten. Jeder MA besitzt eine virtuelle „care-of address“ (VCoA). Der MN schickt MIP-Registrierungsnachrichten nur an alle betreffenden MAs, um seine Ortsinformation zu aktualisieren. Diese werden bis zum Toplevel MA (auch Gateway FA genannt) getunnelt. Man kann sich dieses aus Tunneln bestehende Netzwerk als ein weiteres auf IP aufgesetztes Netzwerk vorstellen. Das Tunneln hat den großen Vorteil, dass auch Netze, die nicht Hierarchical Mobile-IP beherrschen, für den Informationsaustausch genutzt werden können.

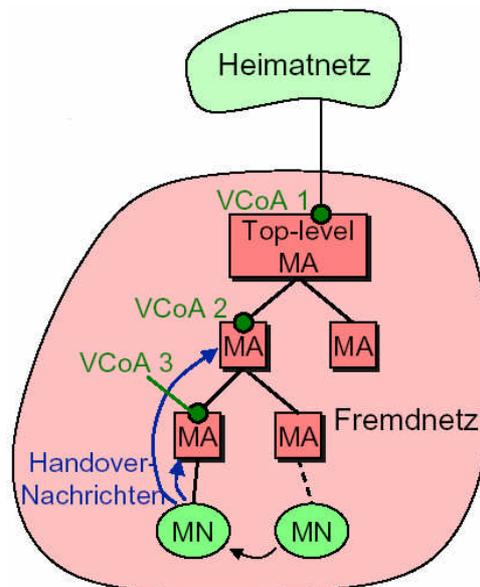


Abb.: 3 Hierarchical Mobile-IP (Quelle: Universität Karlsruhe (TH))

Ein weiterer Vorteil von Hierarchical Mobile-IP ist der minimale Verwaltungsinformationsaufwand beim Handover sowie die Tatsache, dass HAs und CNs keine genauen Bewegungsprofile erstellen können.

Nachteilig ist die Notwendigkeit, Änderungen an MN-Software vornehmen zu müssen, denn das Location Management wird von der MN Seite geregelt. Desweiteren sind die hohe Komplexität der MN-Software schlecht für die Performance des Netzes. Das Location Management läuft vollständig über (evtl. langsamen) MN-Netzzugang und stellt somit eine Verschwendung von kostbarer Bandbreite dar. Die Tunnelendpunkte sind dezentral verteilt und damit schwer administrierbar. Sie sind außerdem ein potentielles Angriffsziel für Hacker. Vor kurzem wurde in Hierarchical Mobile-IP auch Paging-Funktionen [18] eingebaut. Das Netzwerk wird dabei in verschiedene Paging-Bereiche aufgeteilt, in denen sich ein mobiles

Gerät ohne Rückmeldung bewegen kann. Wie in den anderen Protokollen auch wird beim Empfang eines für das mobile Gerät bestimmten Paketes ein Paging-Signal ausgesendet, um die aktuelle Position feststellen zu können.

3.3 Cellular-IP (CIP)

Cellular-IP [13] ist ein Vorschlag der Columbia University und Ericsson und unterstützt Fast Handoff und Paging. Das Mobilitätsmanagement und der Handoff werden im Gegensatz zu Hierarchical Mobile-IP auf der Netzwerkseite und nicht durch den mobilen Host geregelt. Um den Ort des MN bestimmen zu können, werden reguläre Datenpakete untersucht. Mit den gewonnenen Informationen können „reverse path routes“ ermittelt werden, die den Weg zum MN beschreiben. Das hat den großen Vorteil, dass es so gut wie keinen Netzwerkverkehr für die Location Updates gibt.

Der Routingmechanismus von Cellular-IP heißt „Mobile-Specific Routing“ und soll die Verwaltungsinformationen, die durch das Tunneln der Pakete mit dem notwendigen Entpacken und Packen entstehen, vermeiden (vgl. Hierarchical Mobile-IP). Dazu werden normale Routingmechanismen verwendet. Ein vom Home Agent verschicktes Paket trifft beim Router ein und wird von ihm an das mobile Gerät weitergeschickt, welches beispielsweise durch seine Heimatadresse identifiziert werden kann. Die Aktualisierung der Routingtabellen kann dabei implizit (durch Beobachtung des Netzwerkverkehrs) oder explizit (durch spezielle Pakete des mobilen Gerätes) erfolgen. Der Gebrauch von Tunneln oder Adressumschreibungen ist nicht mehr nötig, stellen dafür aber einen höheren Aufwand an die Implementierung.

Desweiteren ist in Cellular IP ein Paging-Mechanismus implementiert, der für Stromsparen und geringe Verwaltungskommunikation sorgt. Ein mobiles Gerät, das keine Verbindungen offen hat, kann die Basisstation wechseln, ohne sich umzumelden. Ein unbeschäftigter MN schickt in gleichmäßigen Abständen kurze Kontrollpakete in Form eines „paging-update packets“ an die nächstgelegene Basisstation. Das Paket wird bis zum Cellular-IP-Gateway geleitet und aktualisiert, die Paging-Caches (eine Art Positionsdatenbank), der einzelnen Knoten. Danach kann der MN wieder in den passiven Zustand wechseln. Kommt ein Paket für den MN am Router an, so wird eine Paginganfrage innerhalb eines bestimmten Radius, in dem sich das Gerät zuletzt aufgehalten hat, gesendet. Der MN kehrt vorübergehend in einen aktiven Zustand zurück, empfängt und bestätigt das Paket und sorgt so für eine Aktualisierung der Positionsdatenbank. Neben der Stromersparung für den MN kommt es hierdurch auch zu einer Verringerung des Netzwerkverkehrs.

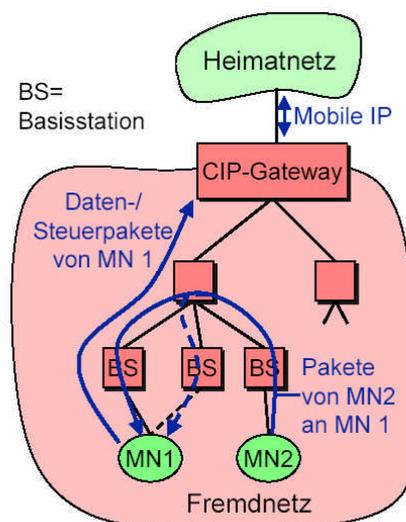


Abb.: 4 Cellular IP (Quelle: Universität Karlsruhe (TH))

Der Handoff bei Cellular-IP lässt sich unterteilen in Hard Handoff und Semisoft Handoff. Hard Handoffs reduzieren die Verwaltungsinformationen, garantieren dafür aber nicht, dass keine Pakete verloren gehen. Die Verbindung zur alten Basisstation muss erst abgebaut werden, bevor die Verbindung zur neuen Basisstation aufgebaut wird. Semisoft Handoff hingegen nutzt die Eigenschaft mancher MNs, die mit zwei Basisstationen gleichzeitig kommunizieren können. Dabei wird der Paketverlust minimiert, indem simultan zwei Verbindungen aufrechterhalten werden und Pakete automatisch von der „alten“ zur „neuen“ Basisstation weitergeleitet werden.

Ebenfalls in Cellular IP implementiert sind spezielle Session-Keys, die von jeder Basisstation bei Registrierung durch den MN unabhängig berechnet werden. Mithilfe dieser Sitzungsschlüssel kann sich der MN bei lokalen Handoffs authentifizieren. Die Unterstützung für schnelle Sicherheitsmechanismen ist damit bereits explizit enthalten und verursacht keine Verzögerungen beim Handoff.

Der Vorteil von Cellular-IP ist, dass es einfach, elegant und weitgehend selbstkonfigurierend ist. Es unterstützt private Adressen im Fremdnetz und es gibt nur einen Tunnelendpunkt (CIP-Gateway), was die Sicherheit erhöht. Ein weiterer Vorteil ist die zentrale Administrierbarkeit und die durchgängige Authentisierung aller Steuernachrichten.

Nachteilig wirkt sich aus, dass Cellular-IP vom MN und allen Knoten explizit unterstützt werden muss. Die Zuverlässigkeit ist nur eingeschränkt gewährleistet, denn wenn der CIP-Gateway ausfällt, funktioniert das ganze Netz nicht mehr.

3.4 Hawaii

Das Hawaii (Handoff-Aware Wireless Access Internet Infrastructure) Protokoll [14, 21] von Lucent Technologies [15] teilt das Netzwerk in hierarchische Domänen und beinhaltet ein spezielles Routing-Protokoll, um Mobilität innerhalb einer Domäne zu gewährleisten (Intra-Domain Mobilität). Wenn der MN in eine fremde Domäne wechselt, kommt das herkömmliche MIP zum Einsatz (Inter-Domain Mobilität).

In Abbildung 5 ist die Netzwerkarchitektur in einem Modell illustriert. Der Backbone-Router (auch Domain Root Router genannt) bietet den Zugang zur Domäne (roter Bereich).

Ebenso wie Cellular-IP beruht auch Hawaii auf dem Modell des „Mobile-Specific Routing“. Im Unterschied zu Cellular IP wird hier jedoch ein separates Routing Protokoll benötigt. Das mobile Gerät erhält eine Co-located Care-of-Address (CCoA), die auch dem HA mitgeteilt wird, und im gesamten Netzwerk beibehalten wird. Das bedeutet, dass der HA nur beim Domänenwechsel mit einbezogen werden muss.

Hawaii ist für ein großes Netz ausgelegt und sämtliche Knoten, die Hawaii implementieren, können als erweiterte IP-Router angesehen werden. Für jeden MN werden spezielle Routingeinträge (Ortsinformationen) hinterlegt. Die Verwaltung der Einträge erfolgt dabei explizit durch Steuernachrichten, die der MN verschickt.

Hawaii sieht insgesamt gleich vier verschiedene Methoden für das Handoff und die Festlegung des Routingpfads vor. Unterschieden wird dabei zum Einen der Fall, wenn das mobile Gerät das erste Mal in ein Netz wechselt, zum anderen der Wechsel zwischen zwei Basisstationen. Die letzten beiden Methoden sind vom zu Grunde liegenden Netzwerk abhängig und davon, wie der Netzbetreiber den Schwerpunkt zwischen niedriger Paketverlustrate, Handoffverzögerung und Einhaltung der Paketreihenfolge beim Handoff legt.

Einen Pagingmechanismus implementiert Hawaii auf der Basis von IP-Multicast. Wenn ein Datenpaket eintrifft, aber keine aktuellen Routinginformationen vorhanden sind, so wird ein Paging signal per Multicast an das Endgerät gesendet. Außerdem wird auch DHCP unterstützt, das einen dynamischen Bezug von IP-Adressen ermöglicht.

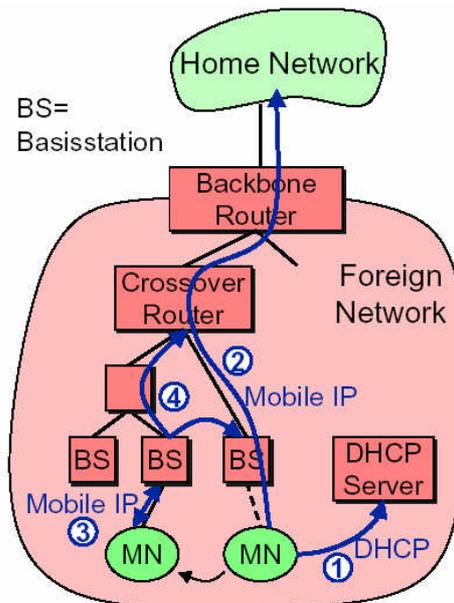


Abb.: 5 Hawaii (Quelle: Universität Karlsruhe (TH))

Größter Vorteil von Hawaii ist, dass es sich um eine Ergänzung zu Mobile IP handelt. Ein mobiles Gerät, welches bereits Mobile IP mit einigen Zusätzen wie Routenoptimierung beherrscht, kann Hawaii transparent benutzen. Ein weiterer Vorteil ist, dass (fast) keine Änderungen an MNs nötig sind und dass dynamisch zugewiesene Heimatadressen berücksichtigt werden.

Nachteil ist, dass keine private Adressen im Fremdnetz unterstützt werden und auch die Sicherheitsprobleme von DHCP. Dezentral verteilte Tunnelendpunkte sind schwer administrierbar und stellen potenzielle Angriffspunkte dar.

3.5 Vergleich und Bewertung der Protokolle

Um die verschiedenen Mikromobilitätsansätze direkt vergleichen zu können, werden die wesentlichen Eigenschaften in Form einer Tabelle aufgeführt (Abb. 5)

	H-MIP	CIP	HAWAII
Verzögerung	hoch	mittel	mittel
Paketverlust	niedrig	niedrig	niedrig
Sicherheit	mittel	relativ hoch	relativ hoch
Zuverlässigkeit	hoch	mittel	hoch
Skalierbarkeit	sehr gut	sehr gut	sehr gut
Positionsbestimmung	spez. Datenpakete	reguläre Datenpakete	spez. Datenpakete
Tunnel	ja	nein	nein
Effizienz (Routing, Verwaltungsinform.)	schlecht	gut	mittel
Paging	Nur in Erweiterung	paging packets	IP-Multicast
Handoffperformance	gut	sehr gut	sehr gut
Kompatibilität	sehr gut	Schlecht	schlecht
OSI - Layer	„3,5“	3	3
Beteiligte Knoten	alle FAs	alle CIP Knoten	alle Router

Tabelle 1: Vergleichsübersicht MIP – H-MIP – CIP und HAWAII

Die Bewertung der unterschiedlichen Protokolle ist schwierig, da es noch keine praktische Anwendung gibt, die die Mikromobilitätsvorschläge umsetzt. Es gibt allerdings ein Programm (Columbia Micromobility Suite (CIMS)[2]) der Columbia University in New York, das eine Mikromobilitätsumgebung simuliert und Protokollvorschläge für die Mikromobilitätsprobleme testen kann. Es ist eine Erweiterung des Netzwerksimulators ns-2 [3]. In einer Simulationsstudie [19] wurde mithilfe von CIMS die Handoff-Performance von Hierarchical Mobile-IP, Cellular-IP und Hawaii getestet.

Bei abschließender Betrachtung scheint für die meisten Probleme Cellular IP die Lösung erster Wahl zu sein. Als einziges der drei Protokolle verfügt es über implizite Positionsbestimmung, verzichtet also auf die Notwendigkeit, spezielle Kontrollpakete zu benutzen. Weiterhin unterstützt es den Semi-Soft-Handoff und ist in der Lage eine Paketverlustrate von Null zu erreichen.

Auch die anderen Protokolle haben jedoch durchaus ihre Daseinsberechtigung. Zwar verhält sich Hierarchical Mobile-IP nicht annähernd so performant wie Cellular-IP, ist dafür aber so ausgelegt, dass ein Netz für Hierarchical Mobile-IP auch von anderen Anwendungen mitbenutzt werden kann. Es bietet somit die Möglichkeit ein vorhandenes Firmennetzwerk mit Mobilitätsdiensten auszustatten.

Wenn man die einzelnen Eigenschaften der vorgestellten Protokolle noch einmal miteinander vergleicht (Tabelle 1), so sind die Unterschiede zueinander eher gering. Alle Protokolle benutzen Schicht 3, die Vermittlungsschicht, um die Datenpakete an das Endgerät zu übertragen. Hierarchical Mobile IP benötigt jedoch Tunnel um ein Paket von Agent zu Agent weiterzugeben. Dabei werden die Pakete jeweils mit neuen Headern versehen und an den nächsten Agent adressiert. Dies sorgt dafür, dass die Weiterleitung auch mit in Schicht 4, die Transportschicht, hineinspielt. Dieses Verhalten von Hierarchical Mobile IP, das Wechselspiel zwischen Vermittlungs- und Transportschicht, wird in der Tabelle 1 durch den Zwischenwert von "3,5" angedeutet. Hieraus ist auch direkt ersichtlich, dass für den Einsatz dieses Protokolls bereits Router notwendig sind, die in der Lage sind Adressumschreibungen vorzunehmen.

Hierarchical Mobile IP unterscheidet sich dabei noch am stärksten von den beiden anderen Protokollen. Der Vergleich zwischen Cellular IP und Hawaii bringt nicht so große Unterschiede hervor. Im Fall von Cellular IP benutzt der MN seine Heimatadresse zur Identifikation im Fremdnetz, während er bei Hawaii eine CoA erhält.

Festzustellen bleibt, dass bereits ein Großteil der Probleme der Mikromobilität gelöst wurden und dass für verschiedene Einsatzzwecke hinreichend gute Lösungsansätze existieren. Weitere Optimierungen könnten helfen, die verschiedenen Protokolle noch performanter zu machen. Weiterhin würde eine Erhöhung der Kompatibilität dazu beitragen, die Integration in die bestehenden Netzwerke zu vereinfachen.

4. Schlussfolgerung und Ausblick

Fakt ist, dass die Zahl der mobilen Internetanschlüsse in den nächsten Jahren dramatisch ansteigen wird und damit auch die Nutzung des Internets über Techniken, die diese Mobilität ermöglichen. Deswegen ist auch ein Bedarf an entsprechenden Protokollen da, die dem Nutzer mindestens den gleichen Service liefern sollten, als wenn er an seinem stationären PC sitzt.

Mikromobilität und die entsprechenden Protokolle befinden sich zur Zeit noch im Forschungsstadium und es gibt noch keine testreifen Implementierungen der Protokolle. Es scheint, dass Cellular-IP die besten Fähigkeiten besitzt, um der de facto Standard für Mikromobilität zu werden.

Es wurden bisher schon eine Menge Probleme der Mikromobilität gelöst, dennoch ist hier sicher noch kein Ende der Entwicklung erreicht. Die Community des IETF beschäftigt sich zur Zeit intensiv mit den Vorschlägen und wird sie bewerten. Durch die Diskussionen wird

früher oder später ein Standard herausgearbeitet, der sich bisher noch nicht herauskristallisiert hat. Viele Faktoren gibt es noch abzuwägen. Auf der einen Seite muss die Performance und Kompatibilität der bestehenden Lösungen hinterfragt werden, auf der anderen Seite aber auch der Aufwand in der Implementierung. Der Wunsch nach weiteren Optimierungen bleibt: Eine noch bessere Performance und eine gesteigerte Kompatibilität würde weitere Verbesserungen mit sich bringen. Auch einige Fragen bleiben noch offen: welche Art des Handoffs ist zu wählen, wie zuverlässig ist eine Lösung in Bezug auf Netzwerkverkehr und einer Vielzahl mobiler Geräte. Weitere Forschungen auf diesem Gebiet sind nötig, um auch in zukünftigen Netzwerken das Problem des Mobilitätsmanagements angemessen zu lösen.

5. Literaturverzeichnis

- [1] **Schiller, Jochen (2000):** Mobilkommunikation, Techniken für das allgegenwärtige Internet
- [2] **Comet Group Columbia University(2002):**
<http://www.comet.columbia.edu/micromobility/software.htm>, abgerufen am 10.01.2003
- [3] **The Network Simulator ns-2:** <http://www.isi.edu/nsnam/ns/>, abgerufen am 10.01.2003
- [4] **J. Kempf (2001):**, IP Paging, RFC 3132: <http://www.faqs.org/rfcs/rfc3132.html>,
abgerufen am 7.1.2003
- [5] **S.Glass, T. Hiller, S. Jacobs, C. Perkins (2000):** Mobile IP Authentication, Authorization, and Accounting Requirements, RFC 2977:
<http://www.ietf.org/rfc/rfc2977.txt?number=2977>, abgerufen am 7.1.2003
- [6] **Archan Misra et al. (2001):** IDMP, Internet-Draft,
<http://comet.ctr.columbia.edu/micromobility/pub/draft-misra-mobileip-idmp-00.txt>, in Arbeit
- [7] **Yingchun Xu et al (2000):** Mobile IP Based Micro Mobility Management Protocol, Internet-Draft: <http://comet.ctr.columbia.edu/micromobility/pub/draft-ietf-mobileip-3gwireless-ext-05.txt>, in Arbeit, November 2000
- [8] **A. O'Neill, G. Tsirtsis (2000):** Edge Mobility Architecture, Internet-Draft,
<http://www.comet.columbia.edu/micromobility/pub/draft-oneill-ema-02.txt>, in Arbeit, Juli 2000
- [9] **Pat R. Calhoun (2000):** Foreign Agent Assisted Handoff, Internet-Draft,
<http://comet.ctr.columbia.edu/micromobility/pub/draft-calhoun-mobileip-proactive-fa-03.txt>, in Arbeit, November 2000
- [10] **Gopal Dommety (2000):** Local and Indirect Registration for Anchoring Handoffs, Internet-Draft, <http://comet.ctr.columbia.edu/micromobility/pub/draft-dommety-mobileip-anchor-handoff-01.txt>, in Arbeit, Dezember 2000
- [11] **F. Vakil et al. (2001):** Mobility Management in a SIP Environment, Internet-Draft,
<http://comet.ctr.columbia.edu/micromobility/pub/draft-itsumo-sip-mobility-req-02.txt>, in Arbeit, Dezember 2000
- [12] **Eva Gustafsson, Annika Jonsson, Charles E. Perkins (2002):** Mobile IP Working Group: Mobile Ipv4 Regional Registration (Internetdraft) <http://www.ietf.org/internet-drafts/draft-ietf-mobileip-reg-tunnel-07.txt>, Oktober 2002
- [13] **Cellular IP:** <http://www.comet.columbia.edu/cellularip/> , abgerufen am 8.1.2003
- [14] **R. Ramjee et al. (1999):** IP micro-mobility support using HAWAII, Internet-Draft,
<http://comet.ctr.columbia.edu/micromobility/pub/draft-ietf-mobileip-hawaii-00.txt>, abgerufen am 5.1.2003
- [15] **Lucent Technologies:** <http://www.lucent.com/>, abgerufen am 6.1.2003
- [16] **Tanenbaum, Andrew S. (2003):** Computer Networks, Fourth Edition

-
- [17] **G. Montenegro (1998):** Reverse Tunneling for Mobile-IP, RFC 2344,
<http://www.ietf.org/rfc/rfc2344.txt?number=2344>
- [18] **H. Haverinen and J. Malinen (2000):**, Mobile ip regional paging, Internet-Draft,
<http://www.comet.columbia.edu/micromobility/pub/draft-haverinen-mobileip-reg-paging-00.txt>
- [19] **Campbell, A.T. et al. (2002):** Comparison of IP Micro-Mobility Protocols
<http://www.comet.columbia.edu/cellularip/pub/pcs2001.pdf>, abgerufen am 08.01.2003
- [20] **Columbia IP Micromobility Homepage: CIMS,**
<http://comet.ctr.columbia.edu/micromobility/>, abgerufen am 08.01.2003
- [21] **Ramjee, R. und La Porta, T und Thuel, S. und Varadha, K. (2002):** HAWAII
A Domain-based Approach for Supporting mobility in Wide-area Wireless networks