Fachhochschule Wedel
University of Applied Sciences

INFORMATIK – Seminar bei Prof. Dr. Iwanowski
im Wintersemester 2004/2005
von wi3819

Mobile Vermittlungsschicht

Frieder Kirsch
Harmsenstr. 5
22763 Hamburg

6. Dezember 2004

Inhaltsverzeichnis

1 Einleitung

Die Kommunikation im Internet ist durch die Kommunikationsarchitektur des OSI-Layer Schichtenmodell spezifiziert. Jede Schicht hat dabei im Rahmen der Kommunikation eine spezielle Aufgabe zu erfüllen. Die Vermittlungsschicht ist hierbei für die Weiterleitung der Kommunikationspakete verantwortlich. Dies geschieht an Hand der im Paketkopf angegebenen Zieladresse. Auch alle Router zwischen den Kommunikationspartnern vermitteln mit Hilfe der Zieladresse.
Durch die Mobilität einzelner Kommunikationsteilnehmer wird die Vermittlung erschwert, da sich der Standort wechseln kann und sich somit die Wege, auf denen ein mobiler Teilnehmer erreicht werden kann, ständig ändern. Mobile-IP ist ein neuer Standard zur Erweiterung des ursprünglichen Internet (Vermittlungs-) Protokoll IP Version 4, um die Probleme der Mobilität auf Vermittlungsebene zu beheben.

2 Mobile IP

2.1 Motivation

Das unaufhörliche Wachstum der Anzahl mobiler Rechner, die auf Grund ihrer Mobilität nicht auf eine uneingeschränkte Nutzung des Internet verzichten wollen, bringt einige Probleme mit sich. Die traditionelle Internetarchitektur ist nicht darauf ausgerichtet, die Mobilität zu unterstützen. Deshalb müssen Änderungen —insbesondere an den Kommunikationsprotokollen— vorgenommen und mobilitätsspezifische Erweiterungen eingeführt werden.
Das Hauptproblem ist hierbei die Vermittlung der Datenpakete, die zwischen zwei Kommunikationspartner ausgetauscht werden. Üblicherweise werden Kommunikationsteilnehmer durch ihre feste und eindeutige IP–Adresse identifiziert. Die Weiterleitung der Pakete wird von Routern durchgeführt, die mit Hilfe der IP–Adresse eingehende Pakete zu passenden Ausgängen weiterleiten, um das endgültige Ziel zu erreichen. Mittels Subnetzmasken wird das physikalische Subnetz bestimmt, in dem sich der Zielrechner befindet. Ein Router kann die Weiterleitung optimieren, in dem er nur die jeweiligen Subnetze speichert an statt jede einzelne Rechneradresse. Das Problem, was sich hieraus für die Mobilität einzelner Rechner ergibt, ist, dass sie nach einem Wechsel in ein anderes Subnetz nicht mehr erreichbar sind. Ein Rechner benötigt immer eine für das jeweilige Subnetz topologisch korrekte Adresse, bestehend aus Subnetzpräfix und Hostadresse.

2.1.1 Theoretische Lösungen

Ein naheliegender Lösungsansatz ist die Vergabe einer neuen topologischen IP–Adresse für den mobilen Rechner im fremden Subnetz, in dem er sich vorübergehend aufhält. Dies kann durch das Dynamic Host Configuration Protokoll geschehen (s. [RFC 2131]) Ein Standortwechsel ist somit gleichbedeutend mit einem Adresswechsel. Dieses Verfahren ist ausreichend, wenn der mobile Rechner allgemeine Internetdienste(HTTP,E–Mail) nur nutzen möchte, also ausschließlich als Client dient. Möchte er darüber hinaus auch internetweite Dienste selbst anbieten, also als Server vollständig in das Internet integriert werden, führt dieser Ansatz zu Problemen, da er bei einem Orts- bzw. Adresswechsel für andere Rechner nicht mehr zu erreichen ist, bis diesen die neue Adresse mitgeteilt wurde. Dies ist aber nicht Aufgabe des ursprünglichen IP-Protokolls.
Ein anderer Ansatz wäre die Anpassung der Abbildung von logischen Namen auf IP–Adressen mit Hilfe von dynamischen DNS. Die logischen Namen sind diejenigen, die man üblicherweise an Stelle der IP–Adresse in die Adresszeile des Browsers eingibt, wenn man im Internet surft. Mit Hilfe des Domain Name System werden die Namen den entsprechenden IP–Adressen zugeordnet. Die Möglichkeit der Aktualisierung der

DNS-Tabellen bei einem IP-Adresswechsel kann schnell als nicht praxistauglich wieder verworfen werden. Das Problem hierbei ist nämlich die Zeitdauer bis sich eine Aktualisierung weltweit durchgesetzt hat(bis zu 24h). Das funktioniert besonders dann nicht, wenn der Anschlusspunkt häufiger gewechselt wird und der Zugang ins Internet auch abwechselnd über verschiedene Kommunikationsmedien erfolgt(Mobilfunk, Wireless LAN,Satellit).
Häufige Adresswechsel und damit verbundene DNS-Aktualisierungen führen zwangsläufig zu Inkonsistenzen in der Zuordnung von logischen Namen und IP–Adressen. Bei Millionen von mobilen Rechnern, die ständig ihren Standort wechseln, kann niemals eine konsistente Abbildung von logischen Namen auf Adressen gewährleistet werden, da das Domain Name System mit Hilfe von zwischen gespeicherten Cache-Informationen eine gute Skalierbarkeit für die Paketweiterleitung zur Verfügung stellt. Der Aufwand für häufige und rasche Aktualisierungen ist deswegen einfach zu hoch.
Außerdem verlassen sich höhere Kommunikationsschichten (TCP/TLS) auf gleichbleibende IP–Adressen während einer bestehenden Verbindung. Der Wechsel der IP–Adresse bei bereits bestehender TCP Verbindung, die durch ein so genanntes Socket–Pair(Quelladresse,Quellport/Zieladresse,Zielport)identifiziert wird, führt zu einem Abbruch eben dieser Verbindung. Dies kann nur dadurch vermieden werden, indem die Kommunikationspartner rechtzeitig über den Wechsel der Adresse informiert werden.
Ein letzter einfacher Ansatz zur "Lösung" der Mobilitätsproblematik wäre, alle Wegwahltabellen der Router, die für die Weiterleitung der Pakete zuständig sind, so zu ändern, dass Pakete zum neuen Standort weitergeleitet werden. Bei der heutigen Anzahl der herkömmlichen Internetnutzer und stetig wachsender Anzahl mobiler Nutzer skaliert dieser Ansatz in der Praxis nicht. Router sind nämlich für eine schnelle Weiterleitung der Pakete, nicht aber für häufige Wechsel der Wegwahltabellen ausgelegt.
Router stellen wichtige Knotenpunkte für das Internet dar und stehen außerdem unter dem Schutz und der Verantwortung der jeweiligen Netzbetreiber und Systemadministratoren. Diese würden eine Gefährdung der Netzstabilität nicht zulassen, nur um einzelnen Nutzern Mobilität zu gewähren.
Da alle vorangegangenen Ansätze offensichtlich praktisch nicht durchführbar sind, führten Feldversuche und Prototypen schließlich zu einem ersten Mobilitätsstandard für das IP-Protokoll Version 4, nämlich Mobile IP. Die aktuellste Version ist [RFC 3344].

2.1.2 Ziele von Mobile IP

Die in diesem Protokoll definierten Ziele ergeben sich aus den Eigenschaften mobiler Verbindungen. Ein mobiler Rechner ist in der Regel über eine drahtlose Verbindung an das Internet angeschlossen. Diese haben zur Zeit noch eine geringere Übertragungsbandbreite als kabelgebundene Netze.
Auf Grund von Interferenzen in dem Übertragungskanal Luft und auch durch gegenseitige Übertragunsstörungen von benachbarten mobilen Rechnern ist die Fehlerrate der Übertragungen deutlich höher.

Ein weiterer wichtiger Punkt ist der Batteriebetrieb mobiler Rechner. Der Energieverbrauch sollte also so gering wie möglich gehalten werden und durch Neuerungen im Kommunikationsablauf nicht übermäßig strapaziert werden.
Das aus den Vorüberlegungen abgeleitete Hauptziel von Mobile-IP läßt sich demnach wie folgt formulieren:
Die Anzahl der Verwaltungsnachrichten, die über die mobilen Verbindungen geschickt werden (müssen), soll minimiert und die Größe dieser Nachrichten so klein wie möglich gehalten werden. Der nächste Abschnitt beschreibt weitere Annahmen und spezifiziert zusätzliche Anforderungen.

2.1.3 Annahmen und Anforderungen von Mobile IP

Makromobilität

Mobile-IP ermöglicht mobilen Rechnern das IP-Subnetz zu wechseln. Unterstützt werden Wechsel von einem Ethernet in ein anderes oder in ein Wireless LAN, solange die IP-Adresse des mobilen Rechner gleich bleibt. In der Protokollspezifikation von Mobile-IP wird die Annahme getroffen, dass ein Wechsel generell nicht häufiger als einmal pro Sekunde stattfindet. Allerdings ist diese konkrete Zeitangabe irreführend und eine Begründung dafür sucht man vergeblich.
Nach meinem Verständnis liegt das Hauptaugenmerk von Mobile-IP auf einem Wechsel des Subnetzes, was in der Praxis eher mit der Absicht geschieht, sich dort deutlich länger als eine Sekunde aufzuhalten. Der Wechsel des Subnetzes wird in der Protokollspezifikation als Makromobilitätsmanagementproblem bezeichnet. Mobile-IP ist weniger für ein Wechsel des Standortes während einer bestehender Verbindung geeignet(Mikromobilität), wie es z. B. bei Mobilfunknetzen der Fall ist, wo ein Sende-/Empfangsbereich mittels Hand-Over gewechselt werden kann.

Kompatibilität

Ein neuer Standard für Internetkommunikation kann keine Änderungen an den bereits standardisierten Anwendungen oder Netzwerkprotokollen fordern. Die bereits existierenden Internetprotokolle haben sich schon durchgesetzt und werden weltweit genutzt. Eine Veränderung darf nur aus geringfügigen Erweiterungen bestehen, um die weltweite Nutzung nicht wesentlich zu stören.
Auch muss Plattformunabhängigkeit gegeben sein, um die Integration in alle gängigen Betriebssysteme zu ermöglichen. Das ursprüngliche TCP/IP-Protokoll ist bereits schon integraler Bestandteil aller Betriebssysteme.
Auch die Router, die für die Vermittlung von Datenpaketen zuständig sind, sollten Erweiterungen auf der Vermittlungsebene ohne neue Software übernehmen können. Damit die neuen Spezifikationen von Mobile-IP mit niedrigeren Schichten des OSI-Layer Kommunikationsmodell kompatibel sind, müssen die gleichen Schnittstellen und Mechanismen wie bei IP genutzt werden. Die Fähigkeit zur Kommunikation mit herkömmlichen Systemen muss bei mit Mobile-IP erweiterten Endsystemen erhalten bleiben. Daraus folgt

also auch die Forderung nach Nutzung der gleichen Adressformate und Paketweiterleitungsmechanismen.

Transparenz

Die Erweiterungen in Mobile-IP sollten für die höheren Schichten (TCP/TLS) unsichtbar bleiben. Eventuell zeigt sich die Mobilität einzelner Rechner in einer kleineren Übertragungsbandbreite und eventuellen Störungen, trotzdem sollte der Wechsel des Zugangspunktes zum Internet generell möglich sein. Für eine TCP-Verbindung ist dabei die Beibehaltung der IP-Adresse von grundlegender Bedeutung, da eine TCP-Verbindung durch das Socket-Pair (Quelladresse/Quellport und Zieladresse/Zielport) identifiziert wird.

Skalierbarkeit und Effizienz

Die Effizienz darf durch die Einführung neuer Mechanismen nicht gefährdet werden. Das Netz sollte nicht durch eine Vielzahl neuer Signalisierungsnachrichten übermäßig belastet werden. Besondere Rücksicht muss dabei auf die geringe Bandbreite drahtloser Verbindungen genommen werden. Im Hinblick auf ein zukünftiges Multi-Milliarden-Teilnehmersystem sollte die Anzahl neuer Datenpakete so gering wie möglich gehalten werden, damit Mobile-IP über eine große Teilnehmerzahl skaliert.

Sicherheit

Die Minimalanforderung bezüglich der Sicherheit ist die Authentifizierung aller Verwaltungsnachrichten, um die rechtmäßigen Empfänger von Datenpaketen sicherzustellen. Bei Festnetzen ist der Systemverwalter für die Zuordnung von IP-Adressen zu den entsprechenden Rechnern zuständig. Bei Mobile-IP muss dies teilweise vom Protokoll übernommen werden, nämlich immer dann, wenn der mobile Rechner seinen Standort wechselt. Gemäß der Internetphilosophie sind darüber liegende Protokollschichten für weitere Sicherheiten zuständig. Das Kernnetz wird so einfach wie möglich implementiert.
Insgesamt ist also das Ziel von Mobile-IP die "Unterstützung der Endsystemmobilität unter Wahrung der Skalierbarkeit, Effizienz und Kompatibilität hinsichtlich existierender Anwendungen und Internetprotokollen"[1].

2.2 Terminologie von Mobile IP

2.2.1 Mobile Node

Ein Mobile Node (MN) ist ein End- oder Zwischensystem, das den Zugangspunkt zum Internet mit Unterstützung durch Mobile-IP wechseln kann. Das mobile System behält dabei seine IP-Adresse und kann ununterbrochen mit anderen kommunizieren, solange eine Verbindung auf OSI-Layer Schicht 2 sichergestellt ist. Der MN muss dabei nicht notwendigerweise ein mobiles Endgerät (Laptop, Mobiltelefon) sein. Auch Zwischengeräte

wie z. B. leistungsstarke Router an Bord eines Flugzeuges, die den Passagieren Internetzugang ermöglichen sollen, sind denkbar.
Solange sich ein MN in seinem Heimatnetz befindet ist keine Nutzung von Mobile-IP notwendig, da er dort eine vom Netzadministrator zugewiesene topologisch korrekte Adresse besitzt.

2.2.2 Home Agent

Der Home Agent (HA) bietet dem MN im Heimatnetz verschiedene Dienste zur Unterstützung der Mobilität. Die wohl wichtigste Funktion ist die Weiterleitung der an den MN gerichteten Datenpakete, wenn dieser sich nicht im Heimatnetz befindet. Für eine genaue Beschreibung dieser und anderer Funktionen s. 2.3 und 2.4.
Der HA kann entweder auf einem beliebigen System im Heimatnetz oder auf dem für dieses Netz zuständigem Router implementiert sein. Das letztere ist die bevorzugte Lösung. Im anderen Fall sendet der Router die ankommenden Pakete ins Heimatnetz zum HA. Dieser muss eventuell feststellen, dass der Zielrechner zur Zeit nicht im Heimatnetz anwesend ist und schickt die Pakete mit der neuen Zustelladresse an den Router zurück. Dadurch wird das Heimatnetz durch eine doppelte Übertragung von Paketen unnötig belastet.

2.2.3 Foreign Agent

Der Foreign Agent (FA) ist das Pendant des Heimatagenten im besuchten Fremdnetz. Hält sich der MN vorübergehend in einem fremden Subnetz auf, so bietet ihm der FA notwendige Dienste an. So kann er z. B. eine im jeweiligen Subnetz topologisch korrekte Adresse zur Verfügung stellen, die für die Dauer des Aufenthaltes im Fremdnetz als Zustelladresse gültig ist. Außerdem ist der FA der Standardrouter für die vom MN gesendeten Datenpakete.

2.2.4 Care-Of-Adress

Die Care-Of-Adresse (COA) ist die für den Zeitraum des Aufenthaltes im Fremdnetz gültige Zustelladresse des MN. Man könnte sie auch als den aktuellen Standort und die damit verbunden Zugehörigkeit zu einem physikalischen Subnetz bezeichnen.
Die COA kann entweder bei dem FA registriert sein oder direkt bei dem MN. Im ersten Fall muss der FA die Pakete zu der tatsächlichen Position des MN im Fremdnetz weiterleiten. Im zweiten Fall kann der MN die Pakete direkt entgegennehmen und die Dienste eines FA werden nicht benötigt. Der MN kann so eine *colocated* COA von einem DHCP-Server [RFC 2131] bekommen.

2.2.5 Communication Node

Zu jeder Kommunikation gehören mindestens zwei Teilnehmer. Im Rahmen von Mobile-IP ist der Communication Node (CN) der Kommunikationspartner des MN, also derjenige welcher dem MN Datenpakete senden möchte. Befindet sich der MN gerade nicht

in seinem eigenen Subnetz, so muss der HA dafür sorgen, dass die Pakete an die COA weitergeleitet werden.

2.3 IP–Paketweiterleitung mit Mobile IP

2.3.1 Agent Discovery

Agent Advertisement

Ein Problem, welches im Rahmen von Mobile-IP gelöst werden muss, ist die Ermittlung des aktuellen Aufenthaltortes und somit Zugangspunkts des MN. In einem Fremdnetz macht ein FA mit Hilfe der so genannten Agent Advertisement Nachrichten seine Anwesenheit allen netzfremden MNs bekannt. Diese Nachrichten ähneln den ICMP-Router Advertisements und werden nur um einige mobilitätsspezifische Datenfelder ergänzt. Abbildung 2.1 zeigt einen Ausschnitt dieser Nachricht mit den für Mobile-IP relevanten Datenfeldern. Der untere Abschnitt enthält die von Mobile-IP ergänzten Felder.

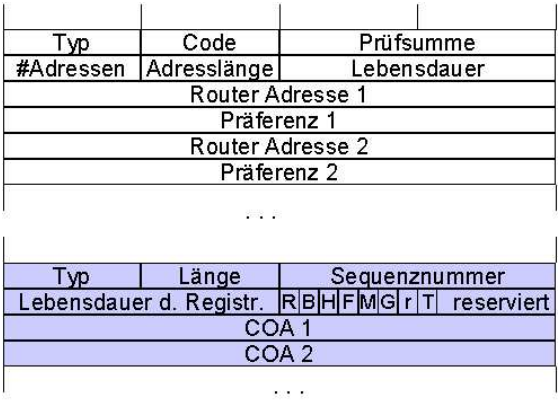


Abbildung 2.1: Agent Advertisement Nachricht [2]

Das Typ-Feld wird auf 16 gesetzt. Die Länge wird mit 6 + 4 mal die Anzahl der COAs berechnet und stellt die Anzahl Bytes dar, die von den Felder belegt werden. Sechs Bytes werden von der Sequenznummer und den darauf folgenden Feldern und Flags[1] in Anspruch genommen. Dazu werden die Adressfelder der angebotenen COAs addiert, wobei eine Adresse vier Bytes belegt.
Die Sequenznummer enthält die Anzahl der gesendeten Advertismentnachrichten nach Initialisierung (Booten) des FA.
Die Lebensdauer der Registrierung gibt die Zeitspanne in Sekunden an, in der eine auf das Advertisment folgende Registrierungsanfrage angenommen wird. Die Bedeutung der Bit-Felder ist wie folgt:

R: Registrierung über FA erforderlich, auch mit einer *colocated* COA.

[1] Bitfelder, die entweder 0 oder 1 enthalten

B: busy, der FA nimmt zur Zeit keine weiteren Registrierungen an.

H: Dienste als HA werden angeboten.

F: Dienste als FA werden angeboten.

M: Minimale Kaspelung wird unterstützt (s. 2.4.2.)

G: Generic Routing Kapselung wird unterstützt (s. 2.4.3).

T: FA unterstützt Rückwärtstunnel (s. 2.5.2).

Die Felder 'r' und 'reserviert' werden ignoriert sind ohne Bedeutung.
Danach folgt eine Liste der angebotenen COA Adressen. Mindestens eine muss folgen bei gesetztem F-Bit und der damit verbundenen Ankündigung von FA Diensten.
Ein FA kann für neue Registrierungen zu beschäftigt sein (B-Bit gesetzt), muss für die bereits bei ihm registrierten MNs aber weiterhin Nachrichten aussenden, damit die wissen, dass sie nicht ihren Standort gewechselt haben. Ein ausschließlich als HA tätiger Agent darf niemals das B-Bit setzen, da er für seine bei sich beheimateten MNs bei ihrer Rückkehr immer bereit sein muss, ihre Registrierungen anzunehmen.
Wenn das B(usy)-Bit gesetzt ist, muss zwangsläufig auch das F(oreign Agent)-Bit gesetzt sein. Das gleiche gilt für ein gesetztes R-Bit, womit ein FA nach einer Registrierung verlangt, auch wenn der MN eine *colocated* COA erhalten hat und sich damit eigentlich direkt bei seinem HA registrieren könnte. Ein gesetztes R-Bit hat also implizit ein gesetztes F-Bit zur Folge.
Eine Advertisement Nachricht auszusenden ohne irgendwelche Dienste anzubieten ist unsinnig, dewegen muss eines der beiden Bits F und H immer gesetzt sein.

Agent Solicitation

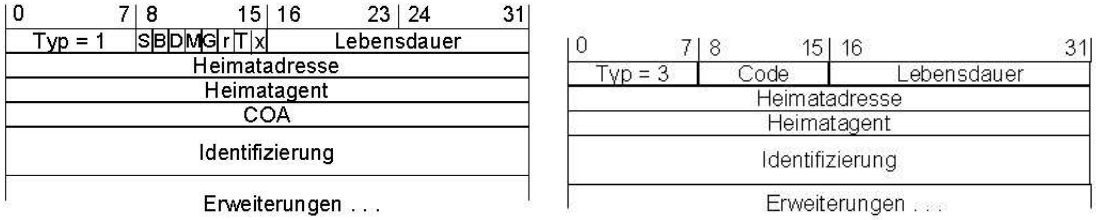
Mit Hilfe von Agent Solicitation Nachrichten kann ein MN auch aktiv die Dienste eines FA erbitten. Allerdings sollte das nur geschehen, wenn keine Agent Advertisement Nachrichten empfangen werden und auch keine IP-Adresse von einem DCHP-Server (siehe **??**) zugeteilt wird. Die Agent Solicitation Nachrichten entsprechen den ICMP-Router-Solicitation Nachrichten, mit denen ein Endsystem in einem Netzwerk nach zuständigen Routern sucht.
Werden Agent Solicitation Nachrichten nach einer gewissen Zeit nicht positiv beantwortet, so muss das wiederholte Senden verzögert werden, um das Subnetz nicht mit sinnlosen Nachrichten zu fluten. Theoretisch kann ein MN unendlich lange nach einem FA suchen. Deswegen ist dies keine bevorzugte Lösung für eine Agenten-Ermittlung.

2.3.2 Registrierung

Registration Request

Hat der MN im Fremdnetz eine COA erhalten, muss er diese bei seinem HA registieren. Dies kann entweder direkt oder über den FA geschehen. Dazu gibt es folgende einfache

Regeln. Besitzt der FA die COA für den MN und ist somit für die endgültige Zustellung von Paketen zum MN verantwortlich, muss die Registrierung über den FA laufen. Der FA leitet die Registrierung dann an den HA weiter.
Auch wenn der FA in seinen Advertisements das R-Bit gesetzt hatte, muss der MN sich über den FA registrieren.
Ansonsten darf sich der MN direkt bei seinem HA registrieren, speziell wenn er in sein eigenes Heimatnetz zurückkehrt. Abbildung 2.2 zeigt einen Ausschnitt einer Registrierungsanforderung.
Das Typ-Feld bekommt eine eins für Registrierungsanforderung. Die Bit-Felder haben



(a) Registration Request

(b) Registration Reply

Abbildung 2.2: Registrierungsnachrichten [2]

folgende Bedeutung:

S: Simultane Bindungen erwünscht, frühere Bindungen von Heimatadresse des MN zu COAs werden beibehalten.

B: Broadcast, MN wünscht den Empfang von Broadcasts[2] aus dem Heimatnetz.

D: Decapsulation, der MN besitzt eine *colocated* COA und enkapselt ankommende Pakete selbst.

M: Minimale Kaspelung soll genutzt werden (s. 2.4.2.)

G: Generic Routing Kapselung soll genutzt werden (s. 2.4.3).

T: Rückwärtstunnel wird angefordert (s. 2.5.2).

Felder 'r' und 'x' sind nicht belegt und werden ignoriert. Die Lebensdauer gibt die Zeit (in sec.) an, nach der die Registrierung ausläuft. Ein Wert von Null bedeutet Deregistrierung und Auflösung einer bestehenden Bindung von Heimatadresse des MN zu COA.
Die Heimatadresse ist die feste IP-Adresse des MN im Heimatnetz. Darunter folgt die Adresse des HA und die COA, die entweder registiert oder deregistriert werden soll.
Die Identifizierung ist eine 64-Bit Nummer zum Abgleich von Registrierungsanfragen/-anworten, um doppelte Registrierungen zu vermeiden (replay attacks). Die Erweiterungen enthalten mindestens Informationen zur Authentifizierung zwischen MN, FA und HA.

[2] an alle im Subnetz befindlichen Endgeräte gerichtete Nachrichten

Registration Reply

Die Registrierungsanwort (siehe Abbildung 2.2) wird mit einer drei im Typ-Feld gekennzeichnet. Das eigentlich Interessante ist das Code-Feld. Hier wird der Status der Registrierung angezeigt. Null steht für eine akzeptierte Registrierung. Eins bedeutet, dass die Registierung angenommen wurde, aber ohne Unterstützung von Simultanen Bindungen.
Eine Registrierung kann aber auch sowohl vom FA als auch vom HA abgelehnt werden. Dies kann unterschiedliche Ursachen und Gründe haben. Kategorien von Fehlern sind z. B. Unerreichbarkeit, mangelnde Verfügbarkeit von Diensten oder mangelhafte Anforderungsnachrichten sowie fehlerhafte Authentifizierung. Das Code-Feld beinhaltet dann die entsprechenden Fehlercodes. Die Lebensdauer hat die gleiche Bedeutung wie bei der Registrierungsanforderung.

2.4 Tunnels und Kapselung

2.4.1 IP-in-IP Kapselung

Eine Kapselung von Datenpaketen wird üblicherweise dann durchgeführt, wenn Pakete der unterschiedlichen OSI-Layer Schichten ineinander gekapselt werden. Die Nutzdaten und Header[3] Informationen werden zu der Nutzlast einer anderen Schicht, und ein neuer Paket-Header wird aufgesetzt. Bei Mobile-IP erfolgt die Kapselung auf einer Ebene, nämlich der IP-Schicht (OSI-Layer 3).
Zum einen wird dadurch erst die Weiterleitung der Pakete vom HA (Tunnelstartpunkt) zum aktuellen Zugangspunkt (Tunnelendpunkt) des MN ermöglicht und außerdem wird die tatsächliche Heimatadresse des MN vor allen anderen Vermittlungsknoten auf dem Weg durch den Tunnel geheim gehalten. Abbildung 2.3 zeigt die Standardkapselung, die von allen mit Mobile-IP erweiterten Geräten unterstützt werden muss.
Bei der IP-in-IP Kapselung wird einfach ein neuer IP-Header auf den schon vorhande-

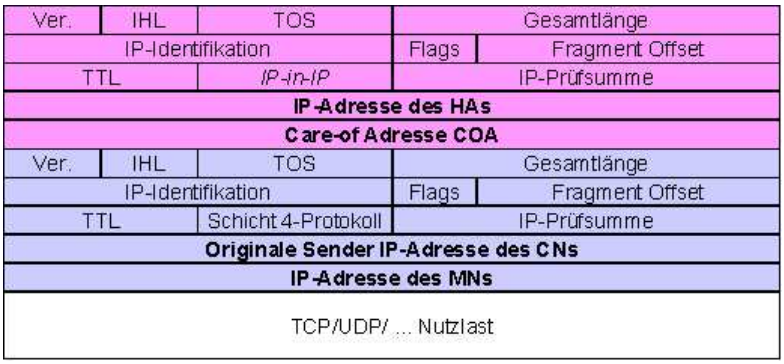


Abbildung 2.3: IP-in-IP Kaspelung [2]

nen aufgesetzt. Der neue Header enthält als Quelladresse jetzt die HA-Adresse und als

[3] Paketkopf

Zieladresse die aktuell gültige COA des MN. Dadurch werden die Pakete zu dem MN weitergeleitet. Die Datenfelder der IP-Header bleiben gleich und weisen keine Veränderung zu Standard IP-Header auf.
Allerdings haben die beiden TTL-Felder jetzt unterschiedliche Bedeutung. Diese werden standardmäßig bei jedem Passieren eines Vermittlungsknoten dekrementiert, um ein endloses Kreisen von Paketen im Internet zu vermeiden.
Das TTL des unteren Header wird allerdings nur einmal dekrementiert, egal wieviel Vermittlungsknoten zwischen dem HA und MN liegen, also anders ausgedrückt zwischen Tunnelstartpunkt und Tunnelendpunkt. Dadurch wird die Anwesenheit des MN im Heimatnetz simuliert.
Die Zahl im TTL-Feld des äußeren (oberen) Paketkopf muss mindestens groß genug sein, um alle Vermittlungsknoten innerhalb des Tunnels passieren zu können. Die Anzahl der Vermittlungsknoten im Tunnel könnte man auch als "Länge" des Tunnels bezeichnen.
Am Tunnelendpunkt wird der aufgesetzte Paketkopf während der Entkapselung einfach wieder entfernt. Weiter Spezifikationen und Beschreibungen der übrigen Felder finden sich in [RFC 2003].

2.4.2 Minimale Kapselung

Das Ziel der Minimalen Kapselung ist die Vermeidung doppelter Felder und Reduzierung von Overhead[4]. Diese kann aber nicht bei schon fragmentierten Paketen eingesetzt werden, da man an Hand Abbildung 2.4 erkennen kann, das nun im Minimal-Header kein Platz für Fragmentinformationen vorhanden ist.
Im Gegensatz zu IP-in-IP wird hier der neue minimale Header zwischen dem originalen

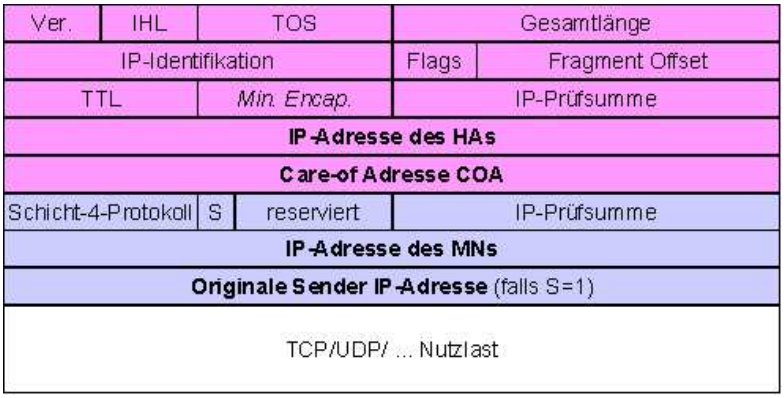


Abbildung 2.4: Minimale Kapselung [2]

Header und den Nutzdaten eingefügt. Danach wird der (originale) äußere Header modifiziert, um die Weiteleitung zum MN zu ermöglichen. Die originale Quelladresse wird durch die des HA ersetzt (Tunnelstartpunkt). Die Zieladresse wird zur aktuellen COA des MN (Tunnelendpunkt).

[4] Verwaltungsinformationen

Die originalen Quell- und Zieladressen werden in den eingefügten Minimal-Header kopiert. Sobald der Tunnelendpunkt erreicht ist, werden die Adressen aus dem minimalen Kopf in den originalen Kopf zurück kopiert und somit wiederhergestellt. Bei der Entkapselung wird der eingeschobenen Minimal-Header wieder entfernt. Für weitere Informationen zur Minimalen Kapselung siehe [RFC 2004].

2.4.3 Generic Routing Encapsulation

Generic Routing Encapsulation [RFC 1701] ist eine weitere von Mobile-IP unterstützte Kaspelungsmethode. Das Besondere hierbei ist, das mit dieser Methode generell auch eine Kapselung unterschiedlicher Protokolle möglich ist und die anderen beiden Methoden nur auf IP-Ebene kapseln.
Als weitere Besonderheit enthält GRE ein Feld, das die maximale Anzahl an Kapselungen festlegt. Dies kann helfen, wenn fehlgeleitete Tunnel dazu führen, dass ein Paket mehrfach gekapselt wird und eventuell in eine Schleife gerät.

2.5 Optimierungen

2.5.1 Binding Cache des Kommunikationspartner

Die bereits vorgestellten Techniken von Mobile-IP sind sicher nicht endgültig und weiter ausbaufähig, wenn Mobilitätsunterstützung auf IP-Ebene erforderlich ist. Man stelle sich bitte folgende Situation vor:

> Ein Deutscher und Japaner treffen sich auf Hawai. Beide haben ein Endgerät, das Mobile-IP Mechanismen unterstützt, und sie möchten miteinander kommunizieren. Wenn der Japaner jetzt Daten zum Deutschen sendet ist der Kommunikationsablauf wie folgt:
> Der Japaner sendet zum HA des Deutschen in Deutschland. Der deutsche HA stellt fest, dass sich der deutsche MN nicht im Heimatnetz befindet und tunnelt die Pakete zum aktuellen Standort in Hawai. Bei einer Antwort an den Japaner ist es ähnlich, nur, dass die Pakete jetzt nach Japan geschickt werden, bevor sie Hawai erreichen.

Dieses Beispiel soll folgendes Problem verdeutlichen. Obwohl sich die beiden Kommunikationspartner eventuell direkt gegenüber sitzen, werden die Pakete um die halbe Welt geschickt. Bei Millionen von mobilen Teilnehmern wäre das eine nicht aktzeptable unnötige Belastung des gesamten Netzes.
Dies kann man nun dadurch umgehen, dass ein CN die aktuelle Adresse des MN, mit dem er kommuniziert, in seinem lokalen Cache speichert. Dazu bittet er den HA des MN durch eine sogenannte Binding Request Nachricht um die neue Zustelladresse des MN. Der HA antwortet ihm mit einem Binding Update und teilt ihm darin die neue Adresse mit. Diese speichert der CN in seinem lokalen Binding Cache und kann nun Daten ohne den Umweg über den HA direkt an die Zustelladresse des MN senden.

2.5.2 Rückwärtstunnel

Ein Problem für ins Internet gesendete Pakete vom MN im Fremdnetz ist die einfache Sicherheitsfunktion der Router, nur Pakete mit topologisch korrekter Adresse durch zu lassen. Sender der MN aber Pakete mit seiner eigenen für das Heimatnetz korrekten Adresse als Absender, würden diese den Router niemals passieren und den Empfänger nicht erreichen.
Dies kann dadurch umgangen werden, dass diese Pakete ähnlich wie die ankommenden gekapselt werden, um im äußeren Paketkopf eine für das Fremdnetz passende Adresse zu enthalten. Die gesendeten Pakete nehmen den gleichen Weg wie die ankommenden, werden also erst einmal zum HA des MN gesendet, der sie dann an den CN weiterleitet. Der Nachteil hierbei ist die doppelte Dreiecksweiterleitung (triangular routing) CN zu HA zu MN und MN zu HA zu CN.
Ein weiteres Problem ist die Sicherheit. Ein Netzadministrator würde einen Rücktunnel, der nicht durch eine Firewall überprüft wird, nicht ohne weitere Sicherheitsmaßnahmen akzeptieren.
Rücktunnel sind auch notwendig, um dem MN die Teinahme an Multicast[5] seines Heimatnetzes zu ermöglichen. Sind die technischen Voraussetzungen für Gruppenkommunikation nur im Heimatnetz vorhanden, so muss ein MN mit Hilfe eines Rücktunnels seine Anwesenheit im Heimatnetz vortäuschen, um die netzspezifischen Einrichtungen nutzen zu können.
Ein letzter notwendiger Grund für den Einsatz von Rücktunnel sind die eventuellen Einschränkungen durch das TTL-Feld. Ein Rechner der im Heimatnetz durch niedrige TTL-Werte nur eine geringe Kommunikationsreichweite besitzt, kann bei einem Standortwechsel seine üblichen Kommunikationspartner nicht mehr erreichen bzw. erreicht jetzt vollkommen andere. Durch einen Rücktunnel in das Heimatnetz wird diese Problem behoben. Rücktunnel werden in [RFC 3024] beschrieben.

2.5.3 IPv6

Die Einführung der neuen Internetprotokoll Version 6 wird vieles erleichtern, auch die Mechanismen und Techniken von Mobile-IP. So ist z. B. eine Authentifizierung aller Nachrichten bereits integriert. Die Sicherheit wird nicht nur aufgesetzt, sondern wurde von vornherein bedacht.
Außerdem sind viele Verwaltungsabläufe automatisiert worden. Eine COA kann durch automatische Konfiguration (DHCPv6) zugeteilt werden. Dienste eines FA werden nicht mehr benötigt, da mit dem neuen Protokoll alle Router Router Advertisments versenden, die die speziellen Agent Advertisements des Mobile-IP für IPv4 ersetzen.
Da die neuen Adressen in IPv6 64 statt 32 Bit groß sind, geht die Anzahl möglicher Adressen in den Milliarden Bereich. Adressmangel ist kein Problem mehr und COAs sind immer *colocated*. Ein MN kann somit auch einem CN automatisch seine neue Adresse mitteilen. Der Umweg über den FA bzw. HA entfällt dann.
Zu guter letzt werden auch "sanfte" Wechsel zwischen unterschiedlichen Subnetzen un-

[5] Kommunikation mit mehreren Teilnehmern

terstützt. Pakete gehen bei einem Wechsel nicht verloren, da der MN unmittelbar nach einem Standortwechsel dem alten Router die neue COA mitteilt. Dieser kapselt eventuell noch eingehende Pakete für den MN und leitet sie an die neue COA weiter.
Nur der kombinierte Einsatz von Firewalls und Mobile-IP wird auch durch das neue IPv6 noch nicht zufrieden stellend gelöst.

2.5.4 Mikromobilität

Cellular IP

Wie schon erwähnt ist Mobile-IP eher weniger zur Lösung von Mikromobilitätsproblemen geeignet. Einige Ansätze für einen weichen Wechsel ohne Verbindungsabbruch zwischen verschiedenen Zugangspunkten werden hier kurz vorgestellt. Diese Ansätze sind weder standardisiert, noch bieten sie eine ausreichende oder optimale Lösung der Mikromobilitätsproblematik. Aktuelle Diskussionen werfen die Frage auf, ob die Schicht 2 unterhalb der Vermittlungschicht für einen reibungslosen Wechsel zwischen zwei Funknetzzellen besser geeignet ist.
Cellular IP (s. Abbildung 2.5) ermöglicht lokale Übergaben ohne Neuregistrierung. Ein CIP-Knoten verwaltet Routing-Informationen für die Weiterleitung zum MN und verhält sich wie ein FA. Die Wegwahlinformationen werden aus den Paketen gewonnen, die ein MN zum CIP-Gateway (CIPGW) sendet. Weiche Übergaben zwischen zwei Basisstationen (BS) wird durch eine Verdopplung der Pakete realisiert, die auf unterschiedlichen Wegen zum MN gelangen. Ein MN, der sich in zwei Funkzellen bewegt, ist in der Lage, Pakete sowohl über die alte als auch über die neue Basisstation zu empfangen (s. MN1 in Abbildung 2.5(a)), sofern das durch tiefere Protokollschichten unterstützt wird.
Der Vorteil von CIP ist die relativ einfache Architektur und eine weitgehende Autokonfiguration.
Nachteile ergeben sich durch einige notwendige Änderungen am ursprünglichen Mobile-IP. Dadurch ist CIP nicht transparent für existierende Systeme. Durch die simultane Weiterleitung von Paketen auf unterschiedlichen Pfaden entsteht zusätzliche Netzlast.
Ein entscheidender Nachteil ist aber die Sicherheit. Die Änderungen in Routertabellen innerhalb des CIP-Bereichs basieren auf Nachrichten des MN, denen aber nicht blind vertraut werden kann. Durch Vortäuschen falscher MN-Identitäten können andere Rechner Nachrichten empfangen, die nicht für sie bestimmt waren. Für Firmennetze ist dieser Ansatz deshalb nicht geeignet.

HAWAII

Die Handoff-Aware Wireless Access Internet Infrastruktur (s. Abbildung 2.5(b)) versucht die Mikromobilitätsunterstützung für den HA und MN so transparent wie möglich zu machen.

Schritt 1: Nach Betreten eines HAWAII-Bereiches muss der MN eine *colocated* COA erhalten (z. B von einem DHCP-Server).

Schritt 2: Registrierung beim HA.

Schritt 3: Bei Eintritt in eine andere Funkzelle erfolgt eine Registrierungsanfrage an die neue Basisstation (BS) wie zu einem FA; Kombination der Konzepte von *colocated* COA und FA-COA.

Schritt 4: Basisstation (BS) fängt Registrierungsanforderung ab und sendet Aktualisierungsnachricht (Handoff update) aus, wodurch alle Router auf Wegen von alter und neuer Basisstation bis zum Crossover Router neu konfiguriert werden; nach Neukonfiguration sendet BS (wie FA) Registrierungsantwort an MN.

Der Vorteil im Vergleich zu CIP ist, dass Änderungen der Routerkonfiguration immer von der Infrastruktur im Fremdnetz selbst initiert werden. Eine Authentifikation dieser Konfigurationsnachrichten ist möglich und erhöht die Sicherheit.
Ein Nachteil ist die fehlende Unterstützung privater Adressen. Für jeden MN muss eine eigene weltweit eindeutige COA vergeben werden.

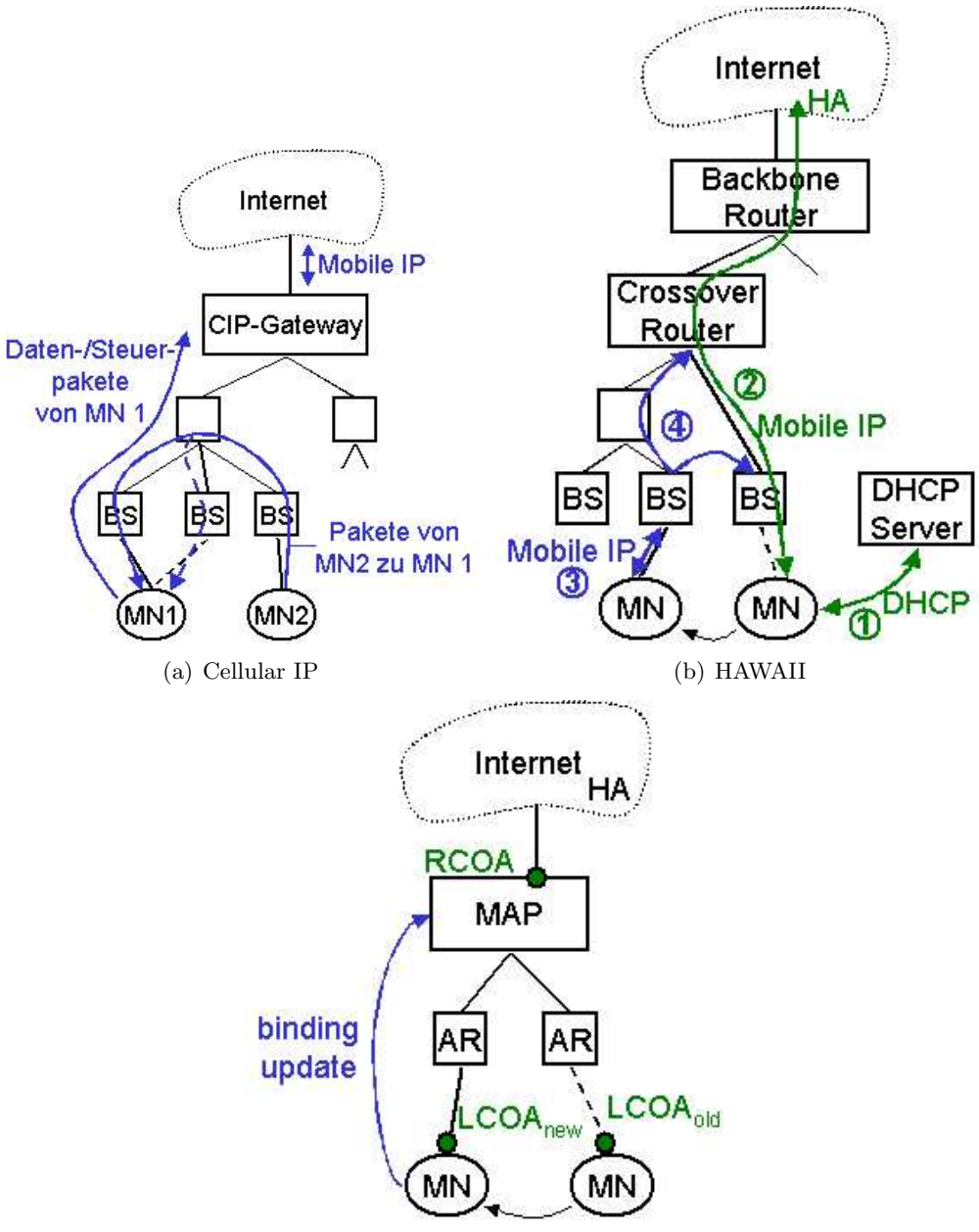
HMIPv6

Da die Einführung von Hierarchie der ganz natürliche Ansatz zur Behandlung von Mikromobilität zu sein scheint, folgt hier noch ein Ansatz, der sich auch so nennt.
Hierarchical Mobile IPv6 (s. Abbildung 2.5(c)) unterstützt Mikromobilität durch Mobility Anchor Points (MAP), die innerhalb ihres Bereiches für alle MNs verantwortlich sind. Die Link COA (LCOA) ist die lokale Adresse eines MN. Solange dieser im Bereich des MAP bleibt, ändert sich die global sichtbare Regional COA (RCOA) nicht. Der MAP hilft bei lokalen Übergaben und verbindet RCOA mit aktueller LCOA. Nur die RCOA wird bei dem HA registriert. Eine lokale Bewegung erfordert nur Neuregistrierung der LCOA bei dem MAP, und verursacht keine Neukonfiguration der Router wie das im HAWAII-Ansatz der Fall ist.
Der entscheidende Vorteil gegenüber den anderen Ansätzen ist die direkte Weiterleitung zwischen Knoten im gleichen Subnetz an Hand der LCOAs. Da bei CIP und HAWAII die MNs ihre Adressen bei einem Wechsel der Basisstationen behalten, müssen alle Pakete immer über die zuständige Basisstation vermittelt werden.

2.6 Vermittlung in Mobilen ad-hoc Netzen

Die Vermittlung von Daten in Mobilen ad-hoc Netzen (Manet) hat im Vergleich zu leitungsgebundenen Infrastrukturnetzen ganz spezielle Probleme zu bewältigen. Der Einsatz von Manet ist z. B. bei spontanen Treffen empfehlenswert, wenn die Planung und Verwaltung einer Kommunikationsinfrastruktur zu zeitaufwendig ist. Abgelegende Gegenden können den Aufbau einer festen Infrastruktur erschweren und zu teuer werden lassen.
Auch könnte die Nutzung einer schon vorhandenen Kommunikationsarchitektur für die erforderlichen Anwendungen nicht angemessen sein. Wenn nur ein verbindungsorientiertes Telefonnetz vorhanden ist, man aber nur gelegentlich Datenpakete senden möchte, ist eine maßgeschneiderte Lösung mit ad-hoc Netzen deutlich besser, auch in Hinblick

auf die Effizienz und Kosten.
Auch bei Rettungseinsätzen in Katastrophengebieten (Erdbeben, Überschwemmung, Hurricanes etc.) bietet Manet eine sinnvolle Möglichkeit für einen schnellen Aufbau eines Kommunikationsnetzes, da die vorhandenen Kommunikationseinrichtungen nicht selten vollkommen zerstört sind. Nicht zuletzt wird die Entwicklung von Manet auch durch den Einsatz bei militärischen Operationen vorangetrieben.
In den Mobilen ad-hoc Netzen ist die Wegewahl bei der Vermittlung das entscheidende Problem. Generell sollten alle Teilnehmer die Fahigkeit zur Weiterleitung von Paketen besitzen, eine Unterscheidung von Router und Endgerät ist nur eine logische und bezieht sich immer auf konkrete Kommunikationsverbindungen.
Man kann davon ausgehen, dass diese in der Regel asymmetrisch sind, d. h. die Qualität der Empfangs- und Sendeverbindungen unterscheiden sich oder sind teilweise gar nicht vorhanden. Bei der Vermittlung von Paketen muss dies erkannt und berücksichtigt werden.
Eine Momentaufnahme des Netzes ist auf Grund dynamischer Veränderungen der Netztopologie nicht möglich. Eine zentrale Speicherung fester Wegverbindungen ist deswegen vollkommen sinnlos. Die Weiterleitung der Pakete muss der jeweiligen Situation angepasst werden und ist deswegen auch immer verbindungslos, d. h. Pakete werden in die ungefähre Richtung des Zieles verschickt, mit der Hoffnung, dieses auch zu erreichen.
Dabei ist die Wahl des besten Weges ein weiteres Problem, da durch Redundanz bis hin zur Vollvermaschung aller Teilnehmer mehrere Wege zum Ziel führen. Die Wahl des optimalen Weges kann sich nicht nur auf die Anzahl dazwischen liegender Knoten beschränken.
Wegen gegenseitigen Störungen in der Übertragung durch benachbarte Knoten und anderen Interferenzen sind Informationen der unterhalb der Vermittlungsschicht liegenden Verbindungsschicht nützlich und notwendig, um den besten Weg zu ermitteln.
Es existieren bereits einige Routing-Algorithmen-Ansätze für Manet, allerdings bietet keiner von denen die optimalste Lösung. Deswegen wird die Paketvermittlung in Manet auch in Zukunft noch ein interessanter Bereich für die Forschung und Entwicklung bleiben.



(a) Cellular IP

(b) HAWAII

(c) HMIPv6

Abbildung 2.5: Mikromobilitätsansätze [2]

3 Zusammenfassung

Der Standard [RFC 3344, IP Mobility Support for IPv4] beschreibt Techniken und Mechanismen mit deren Hilfe ein mobiles End- oder Zwischensgerät seinen Zugangspunkt zum Internet wechseln kann, ohne seine IP-Adresse wechseln zu müssen. Dies wird immer dann notwendig, wenn z. B. ein mobiler Rechner als Server für andere Rechner dient und deswegen immer unter derselben Adresse erreichbar sein sollte.
Eigentlich behält der mobile Rechner nicht wirklich seine Adresse, sondern bekommt vorübergehend eine neue Zustelladresse im Fremdnetz, da alle Knoten eine zum jeweiligen Subnetz topologisch korrekte Adresse erhalten müssen. Die Pakete, die an den mobilen Knoten gesendet werden, werden von einem Heimat-Agenten im Heimatnetz des mobilen Knoten empfangen und an die aktuelle Zustelladresse weitergeleitet.
Viele der in diesem Standard beschriebenen Funktionen und Mechanismen für die Mobilitätsunterstützung sind in dem neuen IP Version 6 Protokoll bereits integriert.
Mobile-IP ist weniger geeignet, sogenannte Mikromobilitätsprobleme zu lösen, d. h. ein Wechsel von Funknetzzellen während einer bestehenden Verbindung, ohne dass diese unterbrochen wird. Es existieren einige theoretische Ansätze, dieses Problem auf Vermittlungsebene zu lösen. Eventuell ist die darunter liegende Schicht dafür aber besser geeignet.
Mobile ad-hoc Netze, die vollkommen ohne leitungsgebundene Infrastruktur auskommen müssen, erschweren die Vermittlung von Paketen durch die Dynamik der Netzstruktur, asymmetrische Verbindungen und redundante Vermittlungsmöglichkeiten auf unterschiedlichen Wegen. Die mobile Vermittlungsschicht bietet speziell hierbei, aber auch generell noch genügend Verbesserungsmöglichkeiten und bleibt somit in Zukunft ein interessanter Bereich für die Forschung und Entwicklung, besonders in den Bereichen Sicherheit, Effizienz und Mikromobilität.

Abbildungsverzeichnis

Literaturverzeichnis

[1] Jochen Schiller, Mobilkommunikation, Pearson Studium,15. Mai 2003

[2] http://www.jochenschiller.de

[RFC 3344] C. Perkins, IP Mobility Support for IPv4, August 2002

[RFC 2003] C. Perkins, IP Encapsulation within IP, Oktober 1996

[RFC 2004] C. Perkins, Minimal Encapsulation within IP, Oktober 1996

[RFC 1701] S. Hanks, Generic Routing Encapsulation (GRE), Oktober 1994

[RFC 3024] G. Montenegro, Reverse Tunneling for Mobile IP (revised), Januar 2001

[RFC 2131] R. Droms, Dynamic Host Configuration Protocol, März 1997

Abkürzungsverzeichnis

MN: Mobile Node *deutsch* : Mobiler Knoten
HA: Home Agent *deutsch* : Heimat Agent
FA: Foreign Agent *deutsch*: Fremd Agent
COA: Care-Of-Adress *deutsch*: Zustelladresse
CN: Communication Node *deutsch*: Kommunikationspartner
Für eine ausführliche Beschreibung dieser Begriffe siehe 2.2.1 bis 2.2.5.

DHCP: Dynamic Host Configuration Protocol
ICMP: Internet Control Message Protocol
TTL: Time To Live
Manet: Mobile ad-hoc networking