

Anbindung von MANETs an das Internet

Matthias Walliczek

Zusammenfassung

Bei stationären Netzwerken mit statischen IPs gestaltet sich die Anbindung an das Internet vergleichsweise einfach - normalerweise genügt die Angabe eines Default-Routers. Anders jedoch bei mobilen Ad-Hoc-Netzen: dort muss eine Vielzahl von Parametern dynamisch ermittelt und ausgehandelt werden; z.B. muss ein Gateway gesucht und gefunden werden, anschließend muss eine IP-Adresse konfiguriert werden, die ggf. in einem vom Gateway vorgegebenen Subnetz liegt und last but not least müssen die Datenpakete auch auf dem richtigen Weg zum Internet gesendet und auch korrekt empfangen werden.

In diesem Text werden einige momentan diskutierte Protokollentwürfe vorgestellt und verglichen.

1 Einleitung

1.1 Motivation

Bis 2005 werden mehr als 80% aller Notebooks im professionellen Bereich über eine drahtlose WLAN-Schnittstelle verfügen - so lautet eine Prognose des US-Analysten Gartner Dataquest [Keen03]. Selbst wenn es aber, wie ebenfalls prognostiziert, bis 2008 mehr als 167.000 Standorte mit öffentlichen WLAN-Hotspots geben wird, wird es immer noch zu viele Standorte ohne infrastrukturelle Netzanbindung per Access Point geben.

In solchen Situationen sind mobile Ad-hoc-Netze, die keinerlei feste Infrastruktur benötigen, die einzige Möglichkeit um ein Funknetz aufzubauen. Falls innerhalb dieses Funknetzes ein mobiles Endgerät (Mobile Node, MN) über einen Internet-Zugang (z.B. kabelgebunden per Ethernet oder drahtlos per GPRS) verfügt, wäre es sinnvoll, diesen Zugang auch anderen MNs innerhalb des Funknetzes zur Verfügung zu stellen.

Es könnte ebenfalls für Telefongesellschaften interessant sein, die Reichweite ihres (UMTS-) Netzes dadurch zu vergrößern, indem MNs am Rand der Zellenreichweite als Relaisstation fungieren und auch anderen außerhalb der Zelle befindlichen MNs Zugang zum Netz verschaffen. [Zitt03]

Doch selbst wenn ein MN innerhalb des WLANs über einen Internet-Zugang verfügt, reicht das allein nicht aus, um allen anderen MNs auch diesen Internet-Zugang zu Verfügung zu stellen: Zuerst braucht man ein Protokoll, damit die anderen MNs dieses Gateway überhaupt benutzen können.

1.2 Anforderungen an das Protokoll

Dieses Protokoll muss definieren, wie ein MN mit Gateway-Funktionalität (im folgenden (Internet-)Gateway genannt) von anderen MNs gefunden werden kann und ob der MN zusätzliche Adressen konfigurieren muss, und wenn ja, welche.

Die wichtigste Anforderung an dieses Protokoll ist dabei die Kompatibilität zu den bestehenden Routingprotokollen für Ad-Hoc-Netze. Diese Protokolle sorgen dafür, dass überhaupt eine Kommunikation innerhalb eines solchen Netzes stattfinden kann und ein MN auch andere MNs erreichen kann, die außerhalb der Funkreichweite der eigenen Schnittstelle liegen. In diesem Fall müssen andere MNs als Router fungieren und diese Pakete weiterleiten [Schi03]. Die so entstandene Verbindung bezeichnet man auch als Multihopverbindung [XiBe02].

Die im Moment existierenden Protokollentwürfe lassen sich dabei in zwei Gruppen aufteilen: Zum einen existieren reaktive Routing-Protokolle, bei denen keinerlei Zustände gespeichert werden und eine Route nur bei Bedarf durch das Senden von Routing-Anfragen ermittelt wird.

Andererseits gibt es auch proaktive Protokolle, bei denen jeder MN versucht, durch den kontinuierlichen Austausch von Routing-Tabellen einen möglichst aktuellen Zustand des Netzes zu ermitteln und auf dieser Basis Routen zu errechnen, ohne dann irgendwelche Anfragen senden zu müssen.

Ebenfalls wichtig ist die Zusammenarbeit mit Mobile IP, einem anderen Protokoll in der Kategorie mobile Kommunikation. Mobile IP ermöglicht den Endgeräten, weltweit unter derselben IP-Adresse erreichbar zu sein und so beim Wechsel von einem Netz in ein anderes Netz die Schicht 4-Verbindungen aufrecht erhalten zu können. Wichtig ist dieses Feature insbesondere dann, wenn der MN selber Dienste anbietet, die andere Hosts im Internet nutzen möchten und deshalb eine Verbindung vom Internet zum MN aufbauen wollen.

Eine wichtige Anforderung an jedes Protokoll für mobile Kommunikation ist die Berücksichtigung der begrenzten Ressourcen, die ein mobiles Endgerät auszeichnen; insbesondere mit Strom und CPU-Last sollte sparsam umgegangen werden. Das bedeutet zum Beispiel, dass ein Protokoll möglichst wenig Datenübertragungen verlangen sollte.

Um zukunftsfähig zu sein, sollten die Protokolle auch IPv6 unterstützen, bzw. ausschließlich darauf aufbauen. Dabei sollte jedoch beachtet werden, dass IPv6 bezüglich Mobile IP zahlreiche Änderungen bedeutet: Da bei IPv6 die *Care-Of-Address* mittels der automatischen Adresskonfiguration oder mittels DHCPv6 gelernt wird, sind dort keine *Foreign Agents* vorgesehen [Brau99]. Auf die Tunnel-Technik kann ebenfalls verzichtet werden, da die beiden Adressen des MN, d.h. die *Care-Of-Address* und die Home-Adresse, in den Routing-Header aufgenommen werden können.

1.3 Aktueller Stand

Im Moment befinden sich im Wesentlichen zwei verschiedene Protokollentwürfe in der Diskussion: Zum einen liegt mit MIPMANET [JALJ⁺00] der Entwurf eines Protokolls vor, bei dem versucht wird, das Mobile IP-Protokoll so zu erweitern, dass es auch in Ad-Hoc-Netzen funktioniert. Zum anderen existiert ein Internet-Draft namens „Global connectivity for IPv4/IPv6 Mobile Ad Hoc Networks“, der ein eigenes und unabhängiges Verfahren vorstellt, das allerdings kompatibel zu Mobile IP ist. Dieses Protokoll existiert unter dem Namen Globalv4 [BRSP01] in einer Version für IPv4 bzw. unter dem Namen Globalv6 [WMPN⁺03] für IPv6.

Der folgende Text zeigt anhand eines chronologischen Ablaufes die Initialisierung und anschließend den laufenden Betrieb der beiden Protokolle.

2 Auffinden eines Gateways

Bevor irgendwelche Daten ins Internet übertragen werden können, muss zunächst ermittelt werden, ob im lokalen Funknetz ein Gateway vorhanden ist. Dabei gibt es zwei grundsätzlich verschiedene Vorgehensweisen: aktiv oder passiv [XiBe02].

2.1 Passives Auffinden

Passiv meint, dass das Gateway regelmäßig *Router Advertisement*-Nachrichten per Broadcast sendet, um seine Anwesenheit bekannt zu geben. Diese Nachrichten werden von allen MNs innerhalb der Funkreichweite empfangen und können von diesen anschließend weitergesendet werden, damit sie auch von MNs empfangen werden können, die außerhalb der direkten Funkreichweite liegen. Da ein Gateway jedoch typischerweise eine höhere Sendeleistung als ein MN hat, kann es theoretisch passieren, dass ein MN zwar das *Router Advertisement* empfängt, selber jedoch keine Verbindung zu diesem Gateway aufbauen kann [XiBe02].

Wenn ein MN mehrere *Router Response*- oder *Router Advertisement*-Nachrichten empfängt, soll er durch eine spezielle Metrik (z.B. Signalempfangsstärke, die Hopzahl, Belastung des Gateways oder eine Kombination dieser Kriterien) eine Gateway auswählen.

Beim Senden von Broadcast-Nachrichten sollte jedoch beachtet werden, dass solche Nachrichten extrem Ressourcen-hungrig sind: Da solche Nachrichten von jedem MN weitergeleitet werden müssen, verbrauchen sie bei jedem Host Batteriestrom und im ganzen Netz Bandbreite.

2.1.1 MIPMANET

Bei MIPMANET wird das Gateway als *Foreign Agent* betrachtet, der analog zu Mobile IP regelmäßig *Agent Advertisements* broadcastet. Eine *Agent Advertisement*-Nachricht stellt keinen neuen Nachrichtentyp da, sondern erweitert die in RFC 1256 definierten ICMP-Nachrichten um mobilitätsspezifische Bestandteile [Schi03] und wird auch im Festnetz von Routern zur Bekanntgabe ihrer Dienste verwendet.

Ein *Agent Advertisement*-Nachrichtenpaket besteht in der oberen Hälfte aus einem normalen ICMP-Paket, die untere Hälfte ist die notwendige Erweiterung. In dieser existieren Felder für eine Sequenznummer, die die Anzahl der bisherigen Ankündigungen anzeigt, für bestimmte Flags und mögliche *co-located Care-Of* Adressen. Über die Flags kann signalisiert werden, ob eine Registrierung beim *Foreign Agent* notwendig ist oder welche Kapselung verwendet werden soll.

Im Unterschied zu Mobile IP werden diese Nachrichten allerdings in größeren zeitlichen Abständen gesendet, um durch die dafür nötigen Broadcast-Nachrichten nicht zu viel Energie und Bandbreite zu verbrauchen: Während Mobile IP einen minimalen Abstand von einer Sekunde vorschreibt, wird bei MIPMANET mit einem Abstand von 5 Sekunden experimentiert [JALJ⁺00]. Dies bringt jedoch auch Nachteile mit sich: Das Registrieren und der Wechsel in ein neues Netz dauern länger bzw. werden instabiler.

2.1.2 Globalv4

Ebenso wie bei MIPMANET entspricht auch bei Globalv4 die Suche nach dem Gateway der Suche nach einem Foreign Agent, der seine Präsens durch *Agent Advertisements* anzeigen kann, die Mobile IP entsprechen [Perk01]. Diese Nachrichten werden wie bei Mobile IP von allen MNs weitergeleitet. Zusätzlich speichert der MN die IP-Adresse zusammen mit einer Sequenznummer; und falls er anschließend dieselbe Nachricht noch einmal erhält, braucht er dieses Duplikat nicht weiter zu verarbeiten, sondern kann es ignorieren. Nachdem er die Nachricht verarbeitet hat, sendet er sie in einer zufälligen Reihenfolge und mit zufälligem Abstand über seine Schnittstelle, um Kollisionen zu vermeiden.

2.1.3 Globalv6

Bei Globalv6 hängt das für die Suche nach einem Gateway verwendete Verfahren von dem verwendeten Routingprotokoll ab. Bei proaktiven Routing-Protokollen wird ein aus Sicht des MN passives Verfahren benutzt, bei dem das Gateway eine Nachricht namens *internet-GateWay Advertisement*, *GWADV* benutzt, die direkt entweder als Teil des Routing-Protokolls oder des *Neighbor Discovery Protocols* versendet wird.

Sobald der MN eine *GWADV*-Nachricht empfangen hat, startet er die Adresskonfiguration und das Aufsetzen der Routen.

2.2 Aktives Auffinden

Aktives Auffinden bedeutet, dass ein MN bei Bedarf eine *Router Request*-Nachricht entweder als Broadcast-Nachricht oder an eine Multicast-Adresse sendet, um ein Gateway zu finden. Jedes Gateway, das diese Nachricht empfängt, antwortet anschließend mit einer *Router Response*-Nachricht. Dieser Prozess sollte einerseits bei der Initialisierung eines MN stattfinden, andererseits aber auch bei einer Verschlechterung der Multihopverbindung zum Gateway. Bei Bedarf kann dieser Prozess auch regelmäßig stattfinden.

Der Prozess des Auffinden eines Gateways ist jedoch nicht nur bei der Initialisierung eines MN nötig - er wird auch im laufenden Betrieb benötigt, um bei Standortwechseln den Wechsel in ein anderes Netz festzustellen. Bei diesem sogenannten Handover muss der MN nämlich sämtliche Schritte vom Auffinden des Gateways bis zur Adresskonfiguration erneut durchlaufen.

2.2.1 MIPMANET

Bei MIPMANET kann der MN analog zu Mobile IP den *Foreign Agent* auch aktiv durch *Agent Solicitations* suchen. Jedes Gateway, dass eine entsprechende Nachricht empfängt, antwortet mit einer *Agent Advertisement*-Nachricht.

2.2.2 Globalv4

Um einen *Foreign Agent* aktiv zu suchen, kann ein MN eine *Route Request (RREQ)*-Nachricht senden. Diese Nachricht wird in dem entsprechenden Format und mit der „All Mobility Agents“-Multicastgruppenadresse 224.0.0.11 als Zieladresse per Broadcast an alle MNs in seinem Empfangsbereich gesendet. Wenn ein anderer MN diese Nachricht empfängt, überprüft dieser zuerst, ob er gerade bei einem Foreign Agent registriert ist. Ist er bei keinem Agenten registriert bzw. unterstützt er kein Mobile IP, dann broadcastet er diese Nachricht lediglich erneut. Wenn der MN jedoch bei einem Agenten registriert ist und eine Verbindung zu diesem besteht, erzeugt er eine *Route Response (RREP)*-Nachricht, die im Prinzip dem AODV-Standard entspricht [PeRD01a], jedoch eine Erweiterung für den *Foreign Agent* als Anhang hat. Diese Nachricht wird an den Sender der RREQ-Nachricht gesendet.

2.2.3 Globalv6

Da bei reaktiven Routing-Protokollen keine regelmäßigen Statusinformationen gesendet werden, muss hier der MN aktiv tätig werden und mit einer *internet-GateWay Solicitation*, *GWSOL*-Nachricht nach Gateways suchen, die dann mit einer *GWADV*-Nachricht antworten.

Als Absendeadresse bei diesen Operationen kann der MN eine beliebige routbare Adresse nehmen, zum Beispiel die Mobile IPv6 Home Adresse. Wenn er keine derartige Adresse hat, muss er eine temporäre Adresse mit dem *MANET_INITIAL_PREFIX* bilden, die er wieder löscht, sobald er Mithilfe des Gateways eine global routbare Adresse konfiguriert hat.

3 Adresskonfiguration

Für die Adresskonfiguration gibt es zwei verschiedene Autokonfigurationsmechanismen: Einen zustandsbehafteten und eine zustandslosen Mechanismus.

3.1 zustandslose Autokonfiguration

Die zustandslose Auto-Adresskonfiguration ist eine der Neuerungen, die das IPv6-Protokoll ermöglicht. Dadurch kann ein Host bereits nach Initialisierung der Schnittstelle und vor einem Auffinden irgendeines Servers eine allerdings nur lokal gültige *Link Local-Adresse* konfigurieren. Durch einen Mechanismus namens *duplicate address detection (DAD)* [PMWBR⁰¹] wird bewirkt, dass diese Adresse innerhalb des lokalen Netzes einmalig ist und damit eine eindeutige Adressierung des MN innerhalb des Netzes ermöglicht.

Für Ad-Hoc-Netze gibt es ein spezielles Ad-Hoc-Präfix (`fec0::ffff/64`) [PMWN⁰²], mit dem jeder MN eine sogenannte *manet-local*-Adresse konfigurieren und sicherstellen kann, dass diese Adresse innerhalb des Ad-Hoc-Netzes eindeutig ist.

3.2 zustandsbehaftete Autokonfiguration

Um jedoch auch mit Stationen außerhalb des lokalen Netzwerkes kommunizieren zu können, braucht der MN eine global gültige Adresse. Dafür kann er entweder die Adresse aus seinem Heimatnetz weiterbenutzen oder er muss ggf. eine neue IP-Adresse konfigurieren, die zu dem Adressbereich des Gateways passt, nachdem er ein solches gefunden hat. Eine zustandsbehaftete Autokonfiguration kann durch DHCP [BCPD01] ermöglicht werden. Dazu benötigt man einen DHCP-Server auf dem Gateway, der die Adressen verwaltet und sie den MNs automatisch zuweist. Der MN kann diese Adresse z.B. bei der Suche nach einem Gateway lernen.

3.2.1 MIPMANET

Für MIPMANET ist dieser letzte Schritt nicht notwendig: Bei diesem Protokoll wickelt der MN sämtliche Kommunikation über seine Home-Adresse ab, also die Adresse aus seinem Heimatnetz. Da die IP-Adressen der MNs innerhalb eines Ad-Hoc-Netzes in der Regel keinen topologischen Zusammenhang haben, muss ein Ad-Hoc-Routingprotokoll grundsätzlich topologisch nicht zusammenpassende Adresse routen können und kann folglich auch diesen MN erreichen [JALJ⁰⁰].

Um von außen erreichbar zu sein, wird die IP-Adresse des *Foreign Agents* als *Care-of Address* benutzt, d.h. sämtliche Pakete werden vom *Home Agent* per Tunnel an den *Foreign Agent* gesendet, und von diesem dann an den dort registrierten MN.

3.2.2 Globalv4

Eine global routbare Adresse kann der MN bei Globalv4 auf drei verschiedene Arten bekommen: 1. er auf eine *Agent Advertisement*-Nachricht warten; 2. er kann eine solche Nachricht durch eine *Agent Solicitation*-Nachricht anfordern; 3. er kann eine *co-located Care-Of Address* durch externe Mechanismen anfordern, z.B. durch die zustandsbehaftete Autokonfiguration per DHCP.

3.2.3 Globalv6

Bei Globalv6 muss der MN nach dem Erhalt der *GWADV*-Nachricht eine global-gültige IPv6-Adresse bilden, die aus dem vom Gateway vorgegebenen Präfix und der Netzwerkkarten-ID als Host-Teil besteht. Dabei wird davon ausgegangen, dass der MN bereits die Link-Local-Adresse auf Eindeutigkeit getestet hat, und die Host-Adresse deshalb nicht erneut getestet werden muss.

Falls der MN eine mit dem *MANET_INITIAL_PREFIX* gebildete temporäre Adresse zum Suchen des Gateways benutzt hat, muss diese Adresse jetzt gelöscht werden. Außerdem müssen bei sämtlichen Durchgangs-Hosts und dem Gateway die Host-Routen für diese Adresse gelöscht werden. Dies wird durch entsprechende Routing-Protokoll-Nachrichten gemacht; bei AODV6 [PeRD01b] z.B. kann der MN eine *Route Error (RERR)*-Nachricht versenden.

Anschließend muss der MN noch folgende Routen in seine Tabelle eintragen: Zum einen eine Default-Route, deren Ziel das Gateway ist und zum anderen eine Host-Route zum Gateway, dessen Ziel der nächsten Hop ist, über den er das Gateway-Advertisement empfangen hat. Diese Einträge haben eine bestimmte Lebensdauer, die vom Gateway festgelegt wird.

4 Routing

Beim Routing innerhalb eines Ad-Hoc-Netzes müssen zunächst einmal zwei unterschiedliche Netzstrukturen bedacht werden: Beim hierarchischen Routing ist das Netzwerk in verschiedene Subnetze (*Cluster*) eingeteilt, während beim flachen Routing keine weiteren Einteilungen existieren.

4.1 hierarchisches Routing

Wenn ein MN innerhalb eines hierarchischen Ad-Hoc-Netzes Pakete an einen anderen Host senden möchte, muss er zuerst anhand der Ziel-Adresse (bzw. bei Mobile IP mit der *Care-Of-Address*) feststellen, ob dieser Host im selben Subnetz liegt [XiBe02]. Bei IPv6 muss man dazu, das Netzwerk-Präfix der Zieladresse mit dem Präfix des lokalen Netzes vergleichen. Falls der Host in einem anderen Subnetz liegt, sendet er das Paket zuerst mit dem Ad-Hoc-Routingprotokoll an das konfigurierte Gateway.

Bei einem proaktiven Protokoll kann er die innerhalb der Routingtabelle gespeicherte Host-Route nehmen und das Paket entlang dieses Pfades senden. Wird ein reaktives Protokoll verwendet, sendet der MN zuerst ein *Route Request* für die Adresse des Gateways über das Netzwerk. Wenn das Gateway über einen Multihop-Pfad mit dem MN verbunden ist, kann es die Nachricht empfangen und mit einer *Route Reply*-Nachricht antworten. Anschließend kann der MN die Daten über den etablierten Pfad zum Gateway senden. Dieses leitet sie anschließend weiter an den Empfänger innerhalb des Internets.

Wenn ein Rechner im Internet in Gegenrichtung Pakete zum MN senden möchte, sendet er sie entweder an die Home Adresse oder direkt zur *Care-Of Address*. In ersten Fall leitet der *Home Agent* das Paket weiter an die *Care-Of Address*. Nur die *Care-Of Address* wird benutzt, um die Pakete vom Gateway an den MN zu senden.

4.2 flaches Routing

Beim flachen Routing muss der MN ermitteln, ob das Ziel direkt innerhalb des Ad-Hoc-Netzes erreichbar ist oder ob das Paket an das Gateway gesendet werden muss. Wird ein proaktives Protokoll benutzt, muss der MN dazu lediglich prüfen, ob innerhalb seiner Routingtabelle ein Eintrag für eine passende Host-Route existiert.

Bei einem reaktiven Protokoll sendet er eine *Route Request*-Nachricht für die Zieladresse. Diese Nachricht wird von jedem MN weitergeleitet, bis sie schließlich ggf. beim Ziel ankommt. Dieses antwortet dann mit der *Route Response*-Nachricht. Wenn ein Gateway die Anfrage empfängt und einen Weg zum Home Agent des Ziels kennt, antwortet es ebenfalls. Der MN kann jetzt mit Hilfe spezieller Metriken den besten Pfad bestimmen. Selbst wenn Sender und Empfänger bei verschiedenen Gateways registriert sind, muss der Weg nicht zwingend über die Gateways verlaufen - wenn der Weg durchs Ad-Hoc-Netz „besser“ ist, wird er ausgewählt.

4.2.1 MIPMANET

Der entscheidende Bestandteil beim Routing mit MIPMANET ist ein Tunnel, über den der MN die Pakete zum Foreign Agent sendet. Alle Pakete, die ein MN zu Rechnern außerhalb des lokalen Netzes senden möchte, werden also gekapselt und durch das Ad-Hoc-Netzwerk zum Gateway gesendet, das sie anschließend wieder entpackt und normal weitersendet. Ob ein Host im lokalen Netz ist oder nicht, ermittelt der MN über das Ad-Hoc-Routingprotokoll; wenn ein Host lokal erreichbar ist, wird das Paket lokal zugestellt.

4.2.2 GlobalV6

Wenn Globalv6 zusammen mit einem reaktiven Routing-Protokoll verwendet wird, hat das Gateway trotzdem die Aufgabe, Host-Routen für alle MNs zu speichern. Zu dieser Aufgabe gehört auch, die Zieladresse zu prüfen, wenn ein MN Pakete über das Gateway senden möchte. Wenn das Gateway dabei feststellt, dass es zu dem Ziel eine Route durchs Ad-Hoc-Netzwerk finden kann, muss das Ziel offenbar auch im selben Netz liegen und müßte vom Sender auch direkt erreicht werden können. Dies wird dem Sender durch eine Kontrollnachricht mitgeteilt. Der allerdings kann diese Nachricht auch ignorieren, wenn für ihn die Route über das Gateway schneller ist.

Literatur

- [BCPD01] J. Bound, M. Carney, Charles E. Perkins und R. Droms. Dynamic host configuration protocol for IPv6 (DHCPv6). Internet Draft, Juni 2001.
- [Brau99] Torsten Braun. *IPnG*. dpunkt.verlag. 1999.
- [BRSP01] Elizabeth M. Belding-Royer, Yuan Sun und Charles E. Perkins. Global Connectivity for IPv4 Mobile Ad hoc Networks. Internet Draft draft-royer-manet-globalv4-00.txt, November 2001.
- [JALJ⁺00] Ulf Jönsson, Fredrik Alriksson, Tony Larsson, Per Johansson und Gerald Q. Maguire Jr. MIPMANET - Mobile IP for Mobile Ad Hoc Networks. *Proc. ACM MobiHoc*, 2000, S. 75–85.
- [Keen03] Ian Keene. Öffentliche WLAN-Hotspots weltweit, 2002-2008, Mai 2003. <http://www.intel.com/deutsch/ebusiness/strategies/wireless/hotspot.htm>.
- [PeRD01a] Charles E. Perkins, E. Royer und S. Das. Ad Hoc On Demand Distance Vector (AODV) Routing. Internet Draft draft-ietf-manet-aodv-09.txt, November 2001.
- [PeRD01b] Charles E. Perkins, E. Royer und S. Das. Ad Hoc On Demand Distance Vector (AODV) Routing for IP version 6. Internet Draft draft-perkins-manet-aodv6-01.txt, November 2001.
- [Perk01] Charles E. Perkins. IP Mobility Support for IPv4. Internet Draft draft-ietf-mobileip-rfc2002-bis-08.txt, September 2001.
- [PMWBR⁺01] Charles. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer und Y. Sun. IP address autoconfiguration for ad hoc networks. Internet Draft, November 2001.
- [PMWN⁺02] Charles E. Perkins, Jari T. Malinen, Ryuji Wakikawa, Anders Nilsson und Antti J. Tuominen. Internet connectivity for mobile ad hoc networks. *Wireless Communications and Mobile Computing*, 2002, S. 465–482.
- [Schi03] Jochen Schiller. *Mobilkommunikation*. Pearson Education. 2003.
- [WMPN⁺03] Ryuji Wakikawa, Jari T. Malinen, Charles E. Perkins, Anders Nilsson und Antti J. Tuominen. Global connectivity for IPv6 Mobile Ad Hoc Networks. Internet Draft draft-wakikawa-manet-globalv6-03.txt, Oktober 2003.
- [XiBe02] Jin Xi und Christian Bettstetter. Wireless Multihop Internet Access: Gateway Discovery, Routing, and Addressing. *Proc. Intern. Conf. on 3G Wireless and Beyond (3Gwireless'02)*, Mai 2002.
- [Zitt03] Martina Zitterbart. Vorlesung Mobilkommunikation, 2003. http://www.tm.uka.de/lehre/SS03/vorlesungen/V_MK_Unterlagen/mk09-1.pdf.