Ad-hoc-Netzwerke und Routing in Ad-hoc-Netzwerken

Manuel Beetz, Marcus C. Gottwald
{beetz|gottwald}@inf.fu-berlin.de

Herbst 2001

$Id: adhoc.tex,v 1.68 2002/02/01 17:39:16 beetz Exp $

Zusammenfassung

Bei den vorliegenden 42 Seiten handelt es sich um die schriftliche Ausarbeitung der von den Autoren zusammengetragenen Informationen zu den im Titel genannten beiden Themen. Es wird keinerlei Anspruch auf Vollständigkeit oder Korrektheit aller genannten Fakten erhoben.

Entstanden ist diese Arbeit im Rahmen des Seminars *Mobilkommunikation* von Prof. Dr.-Ing. Jochen Schiller am Institut für Informatik der Freien Universität Berlin im Wintersemester 2001/02.

Bluetooth ist eingetragenes Warenzeichen der *Bluetooth SIG, Inc (Bluetooth Special Interest Group).*

WPAN und *Wireless Personal Area Network* sind eingetragene Warenzeichen der *Institute of Electrical and Electronics Engineers, Inc. (IEEE).*

Diese und andere Warenzeichen werden in diesem Dokument ohne besondere Kennzeichnung verwendet.

Inhaltsverzeichnis

Abbildungsverzeichnis

Teil I

Ad-hoc-Netzwerke

Marcus Gottwald und Manuel Beetz

1 Hintergrund/Einführung

Sogenannte *Ad-hoc-Netzwerke* sind Netzwerke, die sich dadurch auszeichnen, dass sie nicht durch eine permanent vorhandene, gleichbleibende Infrastruktur definiert sind. Das zweite entscheidene Kriterium für die Einstufung als Ad-hoc-Netzwerk ist die Fähigkeit zur Autokonfiguration. Es soll kein administrativer Eingriff notwendig werden, um einen Beitritt zu einem Ad-hoc-Netzwerk durchzuführen, solange ggf. alle notwendigen Parameter (wie Netzwerkname, Kennwörter etc.) bekannt sind und dem System zur Verfügung gestellt wurden.

Es gibt *mobile* und *immobile* Ad-hoc-Netzwerke. Die Bezeichnung „mobil“ bezieht sich dabei auf die Bewegung der Teilnehmer, der sogenannten *Nodes* oder *Stationen*. Ein immobiles Ad-hoc-Netzwerk kommt z.B. dann zustande, wenn einigermaßen fest installierte Rechner ohne permanente Netzwerk-Infrastruktur nicht immer alle gleichzeitig angeschaltet sind. Ein weiteres Beispiel ist das Aufstellen transportabler Teile von Netzwerkinfrastruktur an einem Katastrophenort. *Immobile* Ad-hoc-Netzwerke unterscheiden sich hauptsächlich darin von *mobilen* Ad-hoc-Netzwerken, dass sich die Qualität der (Funk-)Verbindung zwischen zwei Nodes meist nicht stark ändert.

Mobile Ad-hoc-Netzwerke werden üblicherweise als *MANET* (Mobile Adhoc Network) bezeichnet.

Es gibt *wired* und *wireless* Ad-hoc-Netzwerke. „Wired“ bezieht sich auf die Art der Datenübertragung im Netzwerk auf Schicht 1. Wired Ad-hoc-Netzwerke sind recht selten[1]. und für die weitere Betrachtung irrelevant. Wir werden den meistverbreiteten Typ von Ad-hoc-Netzwerken, ein mobiles und schnurlos kommunizierendes Netzwerk, betrachten.

2 Anwendungen

Typische Anwendungsfälle lassen sich nur schwer kategorisieren, daher stellen wir hier nur eine bunt gemischte Auswahl vor.

2.1 Conferencing

Gerne genutzt würden Ad-hoc-Netzwerke z.B. bei großen Konferenzen. Könnten sich die Teilnehmer darauf einigen, welchen Standard sie benutzen wollen, so wäre es ohne großen Aufwand möglich, mittels mitgebrachter – oder auch an die Teilnehmer ausgegebener – Geräte ständig an fast

[1] „Kids, die Gameboys koppeln `;-)`“, Schiller 2001

jedem Ort, an dem sich ausreichend viele Konferenz-Teilnehmer aufhalten, ein Netzwerk zur Verfügung zu haben. Der Austausch von Daten, die Demonstration von Client/Server-Anwendungen oder ähnlichem wäre problemlos möglich.

2.2 Home Networking

Mobile Geräte ersetzen immer häufiger fest installierte Hardware. Sehr beliebt ist der Kauf von Notebooks als Einsteiger-Gerät anstelle eines PCs. Ein Vorteil, der gerne angeführt wird, ist die Verwendbarkeit desselben Geräts sowohl zu Hause als auch an der Arbeitsstelle, wie auch bei Freunden oder Bekannten. Oft übersehen wird dabei der Aufwand, der mit der Anpassung der Netzwerkkonfiguration verbunden ist. Sofern ein Netzwerkanschluß erwünscht ist, können Ad-hoc-Netzwerke hier einen großen Teil der Arbeit abnehmen.

Das jedenfalls behauptet Perkins in [Perkins, Seite 9f]. Recht hat er damit zwar, allerdings wird derzeit vorrangig IP für Datenübertragung benutzt, dessen Konfiguration ebenfalls automatisiert werden muss. Eine Lösung für Datenübertragung allein mittels eines MANETs, das die Arbeit der Schichten 2 und 3 übernimmt, ist derzeit für PCs nicht in Sicht.

2.3 Personal Area Networks

Als *Personal Area Networks* (PANs) bezeichnet man Netzwerke, die in Abständen von maximal wenigen Metern um eine Person herum ihre Anwendung finden. Ein typischer Vertreter ist *Bluetooth*. Um die Entwicklung und Verbreitung solcher Netze hat sich besonders die IEEE (http://www.ieee.org) bemüht gemacht.

In PANs können sich z.B. Mobiltelefone, PDAs und Notebooks verständigen, um gegenseitig Ressourcen nutzen und zur Verfügung stellen zu können. Durchaus schon angedacht und erprobt ist die Kommunikation zwischen Hemd und Hose zwecks farblicher Abstimmung oder auch der Kaffeemaschine und der Armbanduhr zwecks Ermittlung individueller Vorlieben.

Ein derzeit wohl aufgrund des voraussichtlichen Aufwands wieder vernachlässigtes Gebiet der Anwendung für PANs ist die Nutzung durch Privatpersonen im alltäglichen Einkauf. Bekannte Szenarien sind der Einkaufswagen, der mitzählt, und die Möglichkeit des bargeld- und berührungslosen Bezahlens.

2.4 Emergency/Disaster

Schnell ersichtlich ist der Vorteil von Ad-hoc-Netzwerken für Krisenhilfsdienste, Feuerwehr, Polizei und ähnliche Einrichtungen. Das Netzwerk bildet sich automatisch mit und aus allen kooperierenden erreichbaren Teilnehmern. Bei Verwendung geeigneter Protokolle auf höheren Schichten ist so eine einfache Kommunikation zwischen allen Beteiligten und der Zugriff auf aktuelle relevante Daten möglich.

Für die Zivilbevölkerung ist der Einsatz von Ad-hoc-Netzwerken im Katastrophenfall unter Umständen die einzige Möglichkeit, Kontakt zu einem

weiterhin bestehenden Teil eines Netzwerkes aufzunehmen. Wird festinstallierte Netzwerkinfrastruktur beschädigt, können sich selbst konfigurierende Teile eine solche Lücke überbrücken.

2.5 Verkehr

Die Verwendung von Komponenten, die zur Bildung von Ad-hoc-Netzwerken fähig sind, in Automobilen ist der derzeit wohl am besten durch die Wirtschaft geförderte Anwendungsfall. Fahrzeuge, die in der Lage sind, selbständig schnurlose Netzwerke zu bilden und über geeignete Protokolle Daten auszutauschen, können sich gegenseitig über Reisegeschwindigkeit, Staus, Radar-Kontrollen oder die Wetterlage verständigen. Insbesondere Kommunikation zwischen Fahrzeugen, die sich entgegenkommen, eröffnet diverse Möglichkeiten. Untersuchungen über technische Voraussetzungen werden z.B. von DaimlerChrysler[Briesem] unterstützt.

Ist die Möglichkeit der fahrzeugübergreifenden Ad-hoc-Kommunikation erstmal gegeben, so erscheint es nicht unwahrscheinlich, dass die Nutzung auf privat erstellte Inhalte ausgedehnt wird. Perkins[Perkins, Seite 13] erwähnt dazu den nicht unwahrscheinlichen Fall, dass das Besuchen von Websites fremder Autos zum Lieblings-Zeitvertreib während langer Autobahnfahrten werden könnte...

2.6 Terminodes

Eine schon vor langer Zeit aufgekommene Idee ist die Nutzung Relay-fähiger Funkstation für den privaten Aufbau IP vermittelnder Netze. Projekte in diversen Großstädten (so z.B. in Berlin von Prenzlnet[Prenzl] und WaveWAN[WaveWAN]) sind bei dem Versuch gescheitert. Grund für das Scheitern sind zumeist unverhältnismäßig hohe Anschaffungskosten, die bereits von Anfang an von jedem der Teilnehmer getragen werden müssen. Ein weiterer Grund scheint die (rechtlich und technisch nicht vollkommen unbegründete) Angst davor, jemand anderen seine Hardware nutzen zu lassen, zu sein.

Ein weiterer Vorschlag in dieser Richtung basiert auf der Verwendung von Ad-hoc-Netzwerken. Ein erklärtes Ziel des Projektes *Terminodes* (von „Terminal+Node“) ist die Verbreitung des Konzepts, dass ein Teilnehmer gleichzeitig Router bzw. Bridge ist.[Term] In der Schweiz sollen möglichst flächendeckend mobile Geräte in Betrieb genommen werden, die über Ad-hoc-Prinzipien kommunizieren können und den Aufbau teurer Infrastruktur vermeiden lassen.

2.7 Electronic Dust

Als *Electronic Dust*, auch *Elektronische Wolken* genannt, bezeichnet man kleinste elektronische Geräte, die insbesondere mit Sensoren jeglicher Art ausgestattet sind und ein Schwarm- oder Nebelverhalten zeigen. Diese Geräte können sich nur selten selber fortbewegen und werden in großen Wolken meist aus der Luft ausgesetzt.

Stattet man solche Geräte mit der Fähigkeit zur Bildung von Ad-hoc-Netzwerken aus, so kann z.B. die Sendeleistung und Energieversorgung

gering ausfallen, wenn einige wenige Geräte mit stärkerer Leistung eine Gateway-Funktion übernehmen. Auch könnten sich die Geräte gegenseitig mitteilen, wo sich für sie selbst gefährliche Stoffe oder Temperaturen befinden. Selbst Szenarien wie Cluster-Bildung zur gemeinsamen algorithmischen Analyse der Befunde sind möglich.

Die Überlegungen zu Electronic Dust sind bisher reine Theorie. Es existieren Ideen und Prototypen für kleine Geräte und Fortbewegungsmethoden, eine Übersicht über das Thema findet sich bei [Mehling].

2.8 Militärische Nutzung

Ganz offensichtlich treffen auf die Anforderungen militärischer Einrichtungen nicht nur die schon vorgestellten Anwendungsgebiete zu, sondern auch diverse weitere Vorzüge von Ad-hoc-Netzwerken.

Ein großes Problem für das Militär ist, dass für eine qualitativ hochwertige Kommunikation mit Freqenzen über 100 MHz eine direkte Sichtverbindung (line of sight, LOS) erforderlich ist [Perkins, Freebersyser & Leiner, Seite 31].

Ist diese nicht gegeben, muss eine Relay-Station eingesetzt werden. In Ad-hoc-Netzwerken kann meist jeder Teilnehmer Pakete für andere Teilnehmer weiterleiten, so dass keine spezielle Infrastruktur errichtet werden muss und „das Netz“, also die Summe aller Teilnehmer, äußerst mobil ist.

Bei miltitärischer Verwendung eines MANETs kommt insbesondere ein weiterer großer Vorteil hinzu: Es läßt sich schwer stören. Der Ausfall (also die Nichterreichbarkeit) eines oder mehrerer Komponenten für den normalen Betrieb ist bereits vorgesehen. Sofern nicht alle zur Kommunikation verwendeten Frequenzen gestört werden, kann das Netz weiter betrieben werden.

3 Herausforderungen

3.1 Energieverbrauch/-versorgung

Die größte Herausforderung für mobile schnurlose Netzwerke besteht in der Versorgung der Endgeräte mit ausreichend viel Energie. Üblicherweise handelt es sich um kleine, leichte Geräte, die unabhängig von Stromnetz und Witterungsbedingungen betrieben werden können sollen.

Während die ständig angepriesene und stetig fortschreitende Entwicklung von Brennstoffzellen Linderung verspricht, bleibt es eines der wichtigsten Ziele, den Energieverbrauch eines solchen Geräts nicht unnötig zu steigern.

3.1.1 Weiterleitung (Forwarding)

Damit jeder Teilnehmer eines Ad-hoc-Netzwerkes mit jedem anderen Teilnehmer kommunizieren kann, auch wenn sich der gewünschte Kommunikationspartner nicht in direkter Funkreichweite befindet, muss ein weiterer Teilnehmer als sogenannte *Relay-Station* verwendet werden. Man spricht bei dem Vorgang der Paketvermittlung von *Routing*.

Wird eine Station als Relay verwendet, so kostet es diese Station Prozessorzeit und vor allem Energie. Der Empfang der Pakete, die Analyse und insbesondere der erneute Versand zehren vom bei mobilen Geräten oft geringen eigenen Energievorrat, so dass ein weites Feld der Untersuchung z.B. darin besteht, herauszufinden, zu welchem Zeitpunkt eine Station mit wieviel Energiereserven entscheiden sollte, für andere Stationen nicht mehr als Relay zur Verfügung zu stehen.

3.1.2 Beaconing

Nur wenige Energiesparmaßnahmen lassen sich durch theoretische Überlegungen finden. Meist wird eine günstige Änderung im Labor eines Hardware-Herstellers gefunden und erst später dokumentiert.

Ein recht gut durchleuchtetes Hardware-fernes Thema im Bereich des Energieverbrauchs ist das *Beaconing* (engl. beacon = Leuchtturm, Signalfeuer). Beaconing wird in MANETs verwendet, um Routing-Informationen zu verbreiten und/oder Nachbarstationen über die eigene Existenz zu informieren.

C-K. Toh und Vasos Vasillin haben dieses Thema eingehend untersucht [Perkins, Toh & Vassillin, Seite 299], und sind zu mehr oder weniger interessanten Ergebnissen gekommen. Die bemerkenswertesten Erkenntnisse sind sicherlich die, dass der Empfang von Beaconing-Signalen bei einem ansonsten unbeschäftigen Notebook-Computer nur äußerst geringe Auswirkungen auf den Energieverbrauch hat und dass eine deutliche Vergrößerung des Beaconing-Intervals (im Test zwischen 50ms und 15sec) nicht die erwartete Ersparnis an Energie erbringt.

3.2 Abdeckung (Coverage)

Ein besonderes Problem von Ad-hoc-Netzwerken ist die deckende Versorgung einer Fläche. Möchte man als Nebeneffekt der Bildung des eigentlichen Ad-hoc-Netzwerkes auch Anschlüsse an weitere Netze gebildet haben, so muss für bestimmte Flächen eine Abdeckung gewährleistet werden.

Bewegen sich Teilnehmer in überschaubarem Maße, so können maximale Abstände errechnet werden. Bleiben diese Abstände jedoch tatsächlich über längere Zeit maximal, können schnell Probleme durch den erhöhten Energiebedarf entstehen.

Ein weiteres Problem ist die Asymmetrie der Funkverbindungen. Ein Teilnehmer kann unter Umständen mit maximaler Leistung senden, seine Daten erfolgreich zum Partner übertragen, aber von jenem keine Daten empfangen. Die Berechnung einer optimalen Verteilung von Teilnehmern und Regulierung der jeweiligen Sendeleistung wird hierdurch stark erschwert.

3.3 Netzwerk-Verkehr

Eine typische Eigenschaft paketvermittelter drahtloser Datenübertragungsstrecken ist, dass im Vergleich zu kabelgebundenen Übertragungen viele Pakete verlorengehen. Wie bei jeder drahtlosen Datenübertragung kann

es natürlich auch bei Ad-hoc-Netzwerken auf der Bitübertragungsschicht zu den üblichen Problemen mit Abschattung, Reflexion, Streuung und Beugung [Schiller, Seite 64f] kommen.

Alle heutzutage verwendeten Standards zur mobilen Funkkommunikation, die auch die Bildung von Ad-hoc-Netzwerken unterstützen, wie z.B. 802.11 und Bluetooth, unterstützen die gesicherte und reihenfolgetreue (also verbindungsorientierte) Übertragung von Paketen auf Schicht 2.

3.4 Vermittlung und Wegewahl (Routing)

Da sich die Anordnung der Teilnehmer – und insbesondere dadurch die Erreichbarkeit – schnell und häufig ändern kann, ist das Ermitteln des korrekten Routings eine der am besten untersuchtesten und gleichzeitig weiterhin in der Entwicklung befindlichen Themengebiete der Informatik. Es fließen sowohl Wissen über die technischen Voraussetzungen und Eigenheiten, Erfahrung mit Netzwerken, Netzwerkverkehr und Routing als auch graphentheoretische Aspekte ein.

Mehr zu diesem Thema in Teil II dieser Arbeit.

3.5 Sicherheit

3.5.1 Sicherheit der Daten

Immer stärker in das öffentliche Interesse rückt die Sicherheit jeglicher Art von Datenübertragung. Sicherheit ist immer die Summe aus Vertraulichkeit, Integrität und Verfügbarkeit [Feder, Seite 5].

Vertraulichkeit ist der offensichtlichste und deshalb mit besonderer Aufmerksamkeit bedachte Teil der Sicherheit. Üblicherweise sehen Standards den Einsatz von Verschlüsselungsmechanismen vor, die Stärke der Mechanismen muss jedoch meist in Hinblick auf die in mobilen Geräten zur Verfügung stehende Rechenleistung beschränkt werden.

Eine solche Verschlüsselung kann sich auf die Strecke zwischen Absender und Empfänger beziehen oder auf die Strecke zwischen zwei aufeinanderfolgenden Knoten, die die Daten auf dem Weg vom Absender zum Empfänger passieren. Im ersten Fall passiert folgendes: Der Absender verschlüsselt die Nutzdaten so, dass nur der Empfänger sie entschlüsseln kann; die Informationen über die Identität des Empfängers muss jedoch im Klartext mitgegeben werden. Im zweiten Fall wird ein netzweit gültiger Schlüssel verwendet, so dass eine weiterleitende Station zwar die Nutzdaten sieht, ein nicht am Ad-hoc-Netzwerk Beteiligter jedoch keine Informationen bekommen kann.

Integrität wird in Ad-hoc-Netzwerken auf unterster Ebene durch einfache Prüfsummen-Verfahren gewährleistet, darüber – in Schicht 2 – zumeist gleichzeitig mit Vertraulichkeit durch einen Verschlüsselungsmechanismus.

Eine Verfügbarkeitsbetrachtung stellt sich für Ad-hoc-Netzwerke in Hinblick auf die zur Übertragung genutzten Frequenzen (Schicht 1, Bitübertragungsschicht) und insbesondere für mögliche Angriffe auf das dynamisch angepaßte Routing.

Gegen eine Störung auf einem breiten Frequenzband gibt es keinen Schutz. Üblicherweise wird eine Spread-Spectrum-Technik angewandt, um die Auswirkungen von Störungen in schmalen Frequenzbändern zu minimieren.

Bei öffentlichen oder halb-öffentlichen Ad-hoc-Netzen, von denen in vielen Visionen geträumt wird, um ganze Länder zu vernetzen ohne ein einziges Kabel verlegen zu müssen, muss davon ausgegangen werden, dass ein Angreifer als gleichberechtigter Teilnehmer im Netz agiert. Es ist für ihn so problemlos möglich, fehlerhafte Routing-Informationen zu verbreiten, Pakete zu duplizieren oder mittels Überstrahlen des Originals und verschicken einer abgeänderten Version den Inhalt eines Paketes zu verändern.

Es bleibt in Ad-hoc-Netzwerken also unerläßlich, auf höhreren Schichten Sicherheitsmechanismen zu verwenden, wenn nicht sichergestellt werden kann, dass kein Unbefugter Zugang zum Netz erlangt.

3.5.2 Sicherheit für mobile Teilnehmer

Ein Teilnehmer in einem Ad-hoc-Netzwerk ist durch die Fähigkeit und Bereitschaft zum Weiterleiten von Paketen in seiner Sicherheit gefährdet. Das größte Risiko ist sicherlich die Bombardierung mit Paketen, die unnützerweise über den zu beeinträchtigenden Teilnehmer verschickt werden. Die meisten der verwendeten Routing-Algorithmen lassen aus Sicht des weiterleitenden Teilnehmers keine Entscheidung darüber zu, ob er sinnvoller- oder unsinnvollerweise als Relay verwendet wird. In jedem Fall wird aber eine Analyse der Pakete stattfinden, was nach dem eigentlichen Empfang weitere Energie verbraucht.

Auch Schwachstellen einer Implementierung werden bei einer solchen Attacke eher aufgedeckt. Weiterhin ist es einem Teilnehmer u.U. einfach nicht möglich, unentdeckt zu bleiben (wie es bei einem drahtgebundenen Netzwerk oft möglich ist), da er als Router zur Verfügung stehen soll. Ein unbekanntes Ziel wäre jedoch viel seltener einem Angriff ausgesetzt.

3.5.3 Sicherheit für vorhandene Infrastruktur

Hat ein Ad-hoc-Netzwerk bzw. ein Teilnehmer des Netzwerkes eine Verbindung zu fest installierter Infrastruktur, so ist dieses fest installierte Netz ebenfalls größeren Gefahren ausgesetzt als sonst üblich. Schafft es ein Unbefugter, Teilnehmer des Ad-hoc-Netzwerks zu werden, so ist ihm üblicherweise der Angriff auf verbundene Netze stark vereinfacht.

In den meisten Fällen wird heute dazu übergegangen, Teilnehmern von Funk-Netzwerken nur nach weiterer Authentifizierung, zum Beispiel durch einen VPN-Mechanismus, Zugriff auf angrenzende Netze zu gewähren.

Bei Ad-hoc-Netzwerken, deren Bestimmung die unkomplizierte, automatische Vernetzung mittels kleiner, einfacher Geräte ist, tritt hier ein Interessenkonflikt auf. Nur in wenigen Fällen wird daher in solchen Fällen auf sich dynamisch restrukturierende Netze zurückgegriffen.

4 Techniken

4.1 IEEE802.11

Die Arbeitsgruppe 802 der IEEE beschäftigt sich mit lokalen Netzwerken, die Teilgruppe 802.11 mit drahtlosen solchen. Für 802.11 gibt es verschiedene Varianten, zur Zeit 802.11a mit bis zu 54 MBit/s in einem Frequenzband um 5 GHz und 802.11b mit bis zu 11MBit/s auf Frequenzen um 2,4GHz.

Die Verbreitung von 802.11b entsprechender Hardware wurde insbesondere von Lucent Technologies unter dem Markennamen „Wavelan“ und jetzt „Orinoco“ vorangetrieben.

802.11 sieht neben dem Ad-hoc-Modus einen Infrastrukturmodus (auch *Managed Mode*) vor. In dieser Betriebsart findet eine Datenübertragung von Punkt zu Punkt, nämlich von einem mobilen Teilnehmer zu einem meist immobilen *Access Point*, statt. Diese Access Points stellen zumeist Gateways oder Bridges in andere Netzwerke dar.

Bei 802.11 kommt zur Verschlüsselung der übertragenen Daten das Verfahren „WEP“ zum Einsatz, welches inzwischen als gebrochen gilt [WEP] – was den Handel nicht davon abhält, weiterhin unter Angabe der Schlüssellänge von 128 Bit (von denen effektiv nur 104 benutzt werden) damit zu werben.

4.2 Bluetooth

Zwischen Bluetooth und 802.11 gibt es zwei große Unterschiede: Bluetooth ist ausgelegt für Kurzstrecken-Kommunikation von wenigen Metern, was kleine Hardware ermöglicht, und Bluetooth ist einigermaßen unkompliziert, was die Hardwareherstellung günstig macht.

Als Aktionsfläche für Bluetooth ist der sogenannte *Personal Operating Space* (POS), die Fläche mit Radius 10m um eine Person, festgelegt worden.

Bluetooth ist ausschließlich für die Bildung von Ad-hoc-Netzen gedacht. Aktive Teilnehmer finden sich in sogenannten *Pikonetzen* mit jeweils bis zu acht Teilnehmern zusammen. Gruppen von Pikonetzen heißen bei Bluetooth *Scatternets* und können untereinander kommunizieren, indem einzelne Teilnehmer zwischen mehreren Pikonetzen wechseln und dabei in einem Pikonetz empfangene Daten im anderen Pikonetz aussenden.

4.3 IEEE802.15

Die 802.15 hat es sich zum Ziel gesetzt, einen Standard für Wireless LANs zu entwickeln, der die Bedürfnisse im *Personal Operating Space* (POS) abdeckt. Sie bezeichnet die betrachtete Sorte von Netzwerken als *Wireless Personal Area Networks*.

Die *Task Group 1* der 802.15 beschäftigt sich mit einem Standard, der auf Bluetooth basiert. Das übergeordnete Ziel ist, sogar eine Kommunikation zwischen 802.11-Geräten und anderen WPAN-konformen Geräten zu ermöglichen. Der Standard sollte im Dezember dieses Jahres (2001) verabschiedet werden, die Verspätung scheint derzeit nicht groß [802.15-TG1].

5 Conclusion und Ausblick

In der Theorie der Standards scheint fast alles möglich zu sein, leider gibt es derzeit keine überzeugenden Anwendungen. Vermutlich mangelt es an Attraktivität aufgrund des Fehlens einer sogenannten „Killer-Applikation“.

Es gibt unzählige Ideen und Lösungsansätze, darunter wirklich praktikable Vorschläge. Außer 802.11b (Abschnitt 4.1) und Bluetooth (Abschnitt 4.2) gibt es jedoch kaum verbreitete Implementierungen. Das Problem bei 802.11 scheint zu sein, dass es viel lieber im Managed Mode verwendet wird und dadurch seine Bekanntheit erlangte. Bei Bluetooth ist es scheinbar der fehlende Sinn, der einen Standard-Anwender davon abhält, sich ein teures Mobiltelefon zu kaufen, wenn ihm die Infrarot-Schnittstelle, die für Hersteller äußerst günstig zu beziehen ist, vollkommen ausreicht.

Andere Protokolle sind immer nur in in geringen Stückzahlen produzierte Produkte eingeflossen (Emergency/Unterhaltungstechnik, Abschnitt 2) oder sind noch nicht ausgereift genug, um in wirklich kleinen Geräten mit minimaler Energieversorgung (Electronic Dust, Abschnitt 2.7) eingesetzt werden zu können.

Bastelstube und Beschäftigungstherapie für alle Freunde von Ad-hoc-Netzwerken sind derzeit die Routing-Protokolle. Über die meisten anderen Themen ist man sich größtenteils einig und wartet auf Erfahrung.

Teil II

Routing in Ad-hoc-Netzwerken

Manuel Beetz und Marcus Gottwald

6 Hintergrund/Einführung

Ad-Hoc-Netzwerke werden aus vielen mobilen Teilnehmern gebildet. Zumeist handelt es sich bei den Geräten, die miteinander kommunizieren möchten, um kleine batteriebetriebene Computer wie Laptops oder PDAs.

Diese Geräte haben aufgrund ihres Ausmaßes und ihrer beschränkten Energieresourcen meist keine große Funkreichweite. In Ad-Hoc-Netzwerken muss daher davon ausgegangen werden, dass es nicht jeder Station möglich ist, direkt mit jeder anderen in Funkkontakt zu treten. Vielmehr kann man davon ausgehen, dass man nur einen geringen Teil der anderen Teilnehmer direkt erreichen kann. Diese Teilnehmer werden als Nachbarn bezeichnet.

Um dennoch alle Stationen in einem Ad-Hoc-Netzwerk erreichen zu können, ist man auf Routing-Dienste erreichbarer Teilnehmer angewiesen, die Daten zum entsprechenden Ziel weiterleiten können. Jede Station in einem Ad-Hoc-Netzwerk sollte daher in der Lage sein, Routing-Dienste für andere Teilnehmer anzubieten, um die Konnektivität aller Teilnehmer sicherzustellen.

Im Unterschied zu dem, was man typischerweise unter Routing versteht, wird Routing in Ad-hoc-Netzen damit nicht zuerst dazu benötigt, Konnektivität über Netzwerkgrenzen hinweg zu realisieren. Vielmehr handelt es sich um eine Wegwahl zwischen den Teilnehmern eines Netzwerkes, um von jedem Teilnehmer jeden anderen zu jeder Zeit erreichen zu können.

Besondere Herausforderungen stellen dabei folgende Besonderheiten von Ad-hoc-Netzwerken bzw. Funknetzwerken dar, die sie von anderen Netzwerken unterscheiden:

- Dynamische Netztopologie

  Teilnemer eines Ad-hoc-Netzes ändern typischerweise sehr oft und schnell ihre Position. Damit wechseln ständig die Stationen, die sich in direkter Funkreichweite eines Teilnehmers befinden.

  Ein Teilnehmer, der noch vor kurzer Zeit als Router zwischen zwei Kommunikationspartnern diente, kann seine Position derart ändern, dass er nicht mehr in der Lage ist, diese Aufgabe zu erfüllen, da er aus der Reichweite zumindest eines der kommunizierenden Geräte gelangt. Es muss eine Lösung gefunden werden, die unterbrochene Verbindung schnell über einen neuen Weg wieder herzustellen. Wenn möglich soll ein neuer Weg so schnell gefunden werden, dass eine kurzfristige Unterbrechung der Verbindung nicht auffällt.

Zum anderen ist es möglich, dass zwei Teilnehmer des Ad-hoc-Netzwerkes durch Veränderung ihrer Position plötzlich in direkte Reichweite gelangen oder es einen besseren Weg zwischen beiden gibt. In diesem Fall sollten beide Teilnehmer auch über diesen Weg miteinander kommunizieren und nicht mehr den alten Weg in Anspruch nehmen. Auch hier ist eine schnelle Anpassung der Kommunikationswege erwünscht.

Bekannte Routing-Algorithmen haben besonders mit hochdynamischen Netzwerktopologien Probleme, da Wege entweder nicht schnell genug angepasst werden oder der Anteil des Netzwerk-Verkehrs, der zur Verwaltung der Routing-Informationen benötigt wird, zu stark ansteigt.

- Asymmetrische Verbindungen

  Funkverbindungen können asymmetrisch sein. Empfängt eine Station Daten einer anderen Station, bedeutet das nicht, dass sich diese Station in der eigenen Funkreichweite befindet. Zudem können sich Funkverbindungen zwischen zwei Stationen für jede Richtung in der Qualität stark unterscheiden.

  Gründe hierfür sind zum Beispiel unterschiedliche Antennen oder die verfügbare Energie und damit unterschiedliche Sendeleistung oder auch ungleich starke Beeinflussung durch Interferenzen.

  In kabelgebundenen Netzwerken kommt dieser Effekt nur selten vor. Vorhandene Routing-Algorithmen berücksichtigen ihn daher nicht.

  Auch die meisten Algorithmen, die speziell für Ad-Hoc-Netzwerke konstruiert wurden, nutzen nur symmetrische Verbindungen und nehmen damit in Kauf, nicht den optimalen oder sogar keinen Weg zu finden, obwohl für beide Richtung ein Weg existiert.

- Interferenzen und Störungen

  In kabelgebundenen Netzwerken bestehen immer nur Verbindungen zwischen Stationen, die mit einem Kabel verbunden wurden. Man kann daher davon ausgehen, dass diese Verbindung gewollt ist. Für Funknetzwerke und damit für die meisten Ad-Hoc-Netzwerke treten Probleme auf, die dadurch entstehen, dass Signale ungewollt und nur aufgrund der physikalischen Nähe zum Sender empfangen werden. [Schiller, Kapitel 3.1.1]

  In CSMA-basierten Netzen kann das dazu führen, dass Teilnehmer, die sich in direkter Funkreichweite befinden, nicht miteinander kommunizieren können, da in der Nähe zwei andere Stationen Daten austauschen.

  Der betreffende Weg steht damit für Routing-Dienste nicht zur Verfügung. Obwohl sich die Netzwerktopologie nicht geändert hat, muss ein anderer Weg zur Kommunikation gefunden werden.

Von einem graphentheoretischen Ansatz aus gesehen, kann man sich ein Ad-hoc-Netzwerk derart vorstellen, dass jeder Teilnehmer als Knoten des Graphen dargestellt wird. Befinden sich zwei Teilnehmer des Ad-hoc-Netzwerkes in direkter Funkreichweite, verbindet man die entsprechenden Knoten mit einer Kante.

Die Suche nach dem idealen Weg zwischen je zwei Teilnehmern des Netzwerkes ergibt sich durch Auffinden der kürzesten Wege zwischen den Knoten im Graphen. Für dieses Problem stellt die Theoretische Informatik diverse Algorithmen zur Verfügung. [Cormen, Kapitel 25]

Im Allgemeinen gehen wir davon aus, dass der Weg der beste ist, der am kürzesten ist. Als Maß steht uns dafür nur die Anzahl der *Hops* zur Verfügung über die der Weg führt. Analog zur Graphentheorie kann aber durch eine Gewichtung der Kanten im Graphen durch ein anderen Kostenmaß eine andere Zielsetzung verfolgt werden. Es kann zum Beispiel die Auslastung einer Funkstrecke, deren Qualität oder die benötigte Zeit berücksichtigt werden.

Die Herausforderung an die Routing-Algorithmen stellt sich dadurch, dass es in einem Ad-hoc-Netzwerk keine zentrale Instanz gibt, die über sämtliche Informationen verfügt, um einen solchen Graphen aufzubauen und die kürzesten Wege zu ermitteln. Vielmehr muss jeder Teilnehmer seine Entscheidungen bzgl. der Wegewahl aus den ihm selbst zur Verfügung stehenden oder den ihm von den Nachbarn übermittelten Informationen treffen.

7 Verfahren

Die Aufgabe des Routing-Algorithmus ist es, zu erreichen, dass stets der kürzeste Weg zur Kommunikation zwischen zwei Teilnehmern im Netz genutzt wird.

Der Aufbau und die Pflege dieser zumeist in Tabellen gespeicherten Informationen, unterscheidet sich zwischen den verschiedenen Algorithmen. Die Ansätze, auf die Routingalgorithmen aufbauen, lassen sich in die im folgenden erläuterten Kategorien einteilen.

	Link-State	Distance-Vector
Proactive	OSPF	RIP, DSDV, FRP
Reactive	DSR	AODV

7.1 Link-State

Jeder Teilnehmer des Ad-hoc-Netzwerkes erstellt aus den ihm zur Verfügung stehenden Informationen eine Sicht auf die gesamte Netzwerk-Topologie. Aus dem daraus entstehenden Graphen ermittelt er anhand geeigneter Algorithmen der Graphentheorie für jedes Ziel etwaiger Kommunikation den kürzesten Weg und entscheidet nach diesen Ergebnissen, welchem Nachbarn er Daten zur weiteren Auslieferung weiterleitet. Angewendet wird z.B. der Algorithmus von Dijkstra. [Cormen, Kapitel 25, Single-Source Shortest Paths].

Zudem verbreitet jeder Teilnehmer Informationen über den Zustand seiner eigenen Funkverbindungen mittels Fluten im gesamten Netz. Damit können alle Teilnehmer ihre Sicht auf die Netzwerk-Topologie aktualisieren und ihre Routing-Tabellen entsprechend anpassen.

Es läßt sich leicht erkennen, dass damit die Informationen über die Netzwerk-Topologie nicht zu jedem Zeitpunkt aktuell sind. Es kann vorkommen, dass es aufgrund veralteter Informationen zu falscher Weiterleitung von Daten kommt und dadurch vorübergehend Kreise entstehen. Diese bestehen jedoch nur solange, wie aktualisierte Informationen brauchen, um sich im gesamten Netz zu verbreiten.

Für Ad-Hoc-Netzwerke ist dieser Ansatz aufgrund der dynamischen Topologie nicht geeignet. Besonders in großen Netzwerken ist es nicht unwahrscheinlich, dass sich die Netzwerktopologie bereits wieder geändert hat, bevor die Informationen über die letzte Änderung im gesamten Netz verbreitet wurden. Hierarchische Einteilungen eines Netzes in kleinere Abschnitte machen die Verwendung von *Link-State*-Verfahren dennoch möglich.

Der in Festnetzen weit verbreitete Routing-Algorithmus OSPF verfolgt z.B. den *Link-State*-Ansatz. [RFC1247]

7.2 Distance-Vector

Bei Distance-Vector-Algorithmen speichert sich jeder Teilnehmer für jedes Ziel einen ganzen Satz von Weglängen. Jeder Teilnehmer hat die Möglichkeit, die Daten an einen beliebigen Nachbarn weiterzuleiten. Für jede dieser Möglichkeiten wird ein Wert für die Kosten des Weges gespeichert. Müssen Daten weitergeleitet werden, entscheidet der Teilnehmer sich dann für die beste, ihm zur Verfügung stehende Route und sendet die Daten an den entsprechenden Nachbarn weiter.

Um die benötigten Informationen stets aktuell zu halten, verbreiten die einzelnen Teilnehmer regelmäßig die ihnen zur Verfügung stehenden kürzesten Wege und Veränderungen ihrer direkten Funkverbindungen.

Algorithmen dieser Kategorie sind effizient zu programmieren und besonders bei großen Netzwerken sehr viel genügsamer im Speicherbedarf. Es ist keine Sicht auf die gesamte Netzwerk-Topologie notwendig. Alle zu Routingentscheidungen verwendeten Informationen werden allein durch Verständigung mit den direkten Nachbarn ermittelt. Dadurch wird das häufige Fluten des gesamten Netzwerkes unnötig.

Nachteilig gegenüber den Link-State-Algorithmen ist jedoch zu bemerken, dass sowohl kurzzeitig als auch längerfristige Kreise in der Wegewahl vorkommen können. Diese entstehen durch veraltete Routinginformationen, die zu falschen Routingentscheidungen führen können. Zusätzlich ist das *Count to Infinity*-Problem zu nennen, das die Effizienz von *Distance Vector*-Algorithmen erheblich mindert. [Tanenbaum, Seite 386]

Um dem entgegenzuwirken, werden in sämtlichen Algorithmen für Ad-Hoc-Netzwerke, die auf diesen Ansatz aufbauen, Sequenz-Nummern eingeführt, die es den Teilnehmern ermöglichen, neue Informationen über zur Verfügung stehende Wege von veralteten zu unterscheiden.

Das Routing-Protokoll RIP ist ein Vertreter der *Distance-Vector*-Protokolle und hat mit sämtlichen oben genannten Problemen zu kämpfen.

7.3 Proactive

Bei Protokollen dieser Kategorie wird die Wegwahl durchgeführt, bevor der entsprechende Weg benötigt wird. Da eine Station nicht wissen kann, mit welchem Teilnehmer sie demnächst zu kommunizieren hat, speichert sich jede Station stets zu jedem möglichen Teilnehmer im Netz einen Eintrag in der Routing-Tabelle.

Der Vorteil dieser Vorgehensweise sind die bei Bedarf sehr schnell zur Verfügung stehenden Wege. Möchten zwei Teilnehmer des Ad-Hoc-Netzwerks miteinander kommunizieren, müssen sie lediglich aus ihren gespeicherten Tabellen die notwendigen Informationen zur Weiterleitung der Daten lesen und können sofort mit der Datenübertragung beginnen.

Als Nachteil ist anzusehen, dass Wege ermittelt werden, von denen nur eine geringe Zahl tatsächlich benutzt werden. Die meisten Einträge einer Routing-Tabelle werden ungültig werden, ohne auch nur ein einziges Mal benötigt zu werden. Dieser Effekt fällt gleich doppelt negativ ins Gewicht. Zum einen müssen die Routing-Einträge gespeichert werden. Die Stationen des Ad-Hoc-Netzwerkes belegen Speicherplatz, von dem nur ein geringer Anteil relevante Informationen enthält. Zum anderen werden viele Daten zwischen einzelnen Teilnehmern und ihren Nachbarn ausgetauscht, um Wege zu finden, die nicht gebraucht werden. Damit sinkt die Kapazität des Netzwerkes, die Nutzdaten zur Verfügung steht.

Die meisten in Festnetzen eingesetzten Routing-Protokolle wie RIP und OSPF gehören zu dieser Kategorie.

7.4 Reactive

Um den für die Emittlung der Wege benötigten Netzwerkverkehr zu minimieren, werden Routing-Protokolle entwickelt, die nach Bedarf *(On Demand)* Wege zwischen zwei Stationen in einem Ad-Hoc-Netzwerk finden.

Protokolle dieser Kategorie erwarten nicht von jeder Station des Netzwerkes, dass zu jeder Zeit ein aktueller Weg zu jedem anderen Teilnehmer des Netzes bekannt ist. Vielmehr wird erst bei Bedarf, das heißt sobald Daten für eine Station zum Versand anliegen, ein kurzer und aktueller Weg zum Ziel ermittelt.

Der offensichtliche Nachteil gegenüber *Proactive* arbeitenden Protokollen ist die Verzögerung bei der Datenübertragung, die dadurch zustande kommt, dass erst ein Weg ermittelt werden muss, während dieser bei den oben beschrieben Protokollen schon vorliegt und nur aus der Routing-Tabelle gelesen werden muss. Die große Herausvorderung an Protokolle, die nach Bedarf Wege ermitteln liegt daher darin, sehr schnell einen aktuellen und optimalen Weg zu finden und damit die Verzögerung so gering wie möglich zu halten.

Die Vorteile dieser Technik sind jedoch sehr gewichtig. Der Netzwerkverkehr kann drastisch gesenkt werden. Die gesparten Resourcen stehen damit der Übertragung “echter”Daten zur Verfügung. Zusätzlich wird Strom gespart, was besonders bei Kleingeräten, wie sie in Ad-Hoc-Netzwerken zu erwarten sind, von Bedeutung ist. Teilnehmer, die zur Zeit nicht kommunizieren, brauchen keine aktuellen Routing-Informationen zu ermitteln und können z.B. in den Stromsparmodus wechseln.

Außerdem sparen Routing-Protokolle, die eine Wegwahl nur bei Bedarf ausführen, Platz in den Routing-Tabellen der Stationen, da nur wirklich benötigte Wege gespeichert werden.

8 Routing Algorithmen

8.1 Destination-Sequenced Distance-Vector

Jeder Teilnehmer des Ad-Hoc-Netzwerkes speichert sich für jede andere Station, an welchen Nachbarn er Daten weiterleiten muss, um diese auf kürzestem Weg zu erreichen.

Das DSDV-Protokoll legt fest, wie einzelne Stationen des Ad-Hoc-Netzwerkes in Zusammenarbeit mit ihren Nachbarn die richtigen Routinginformationen ermitteln können und dabei die sich schnell ändernde Netzwerktopologie angemessen berücksichtigen.

Jedem Knoten des Netzes liegt damit zu jeder Zeit ein Weg zu jedem anderen erreichbaren Knoten vor.

8.1.1 Allgemeine Funktionsweise

Jede Station des Ad-Hoc-Netzwerkes speichert sich in einer Routing-Tabelle einen Eintrag für jedes erreichbare Ziel. Diese Routing-Informationen teilt jeder Teilnehmer seinen Nachbarn in regelmäßigen Abständen mit. Besonders wichtige Veränderungen der Routing-Einträge werden sofort per Broadcast[2] allen Nachbarn mitgeteilt. Damit ist jedem Nachbarn bekannt, welche Teilnehmer über diese Station erreichbar sind. Diese können dann ihre eigenen Routing-Tabellen bei Bedarf anpassen und wiederum an ihre Nachbarn weitergeben.

Jeder Eintrag wird zusätzlich zusammen mit einer ursprünglich vom Routenziel generierten Sequenznummer gespeichert, die es jeder Station ermöglicht, neuere Informationen zur Wegewahl von alten zu unterscheiden.

Veränderungen in den Routinginformation treten auf, wenn eine Station sich aus der Reichweite einer anderen entfernt und somit von dieser nicht mehr erreichbar ist. In einem anderen Fall gelangt ein Teilnehmer in Funkreichweite einer Station, die diesen zuvor nicht erreichen konnte oder mit dem sie bisher nur durch Routing über andere Stationen kommunizieren konnte.

8.1.2 Aufbau der Routingtabelle

Jeder zu einem Ziel gespeicherte Routing-Eintrag enthält die folgenden Informationen, die an alle Nachbarn weitergegeben werden:

- **Destination**
  Je nachdem, auf welcher Schicht die Routing-Funktionalität zu Verfügung gestellt werden soll, handelt es sich hierbei um die Hardware- (Schicht 2) bzw. die Netzwerkadresse (Schicht 3) der Zielstation.

[2] Zu bedenken ist in einem Funknetzwerk, dass ein Broadcast nicht sämtliche Teilnehmer des Netzes erreicht, sondern nur diejenigen, die sich in Funkreichweite des Senders befinden. Darin besteht ein grundlegender Unterschied zu kabelgebundenen Netzwerken.

- **Metric**
  Üblicherweise handelt es sich bei der Metrik um die Anzahl der Hops auf diesem Weg durch das Netz zum angegebenen Ziel. Dieses Kostenmaß kann aber beliebig durch andere Bewertungen ersetzt werden. Beispiele hierfür wären Berücksichtigung der Auslastung oder der Qualität einzelner Funkstrecken.
- **Destination Sequence Number**
  Die Sequenznummer wird üblicherweise von der Zielstation generiert. Sie wird dann von Station zu Station weitergegeben und dient zur Unterscheidung zwischen aktuellen und veralteten Informationen.

Zusätzlich zu diesen Informationen wird bei einer Benachrichtigung der Nachbarn die Adresse des Senders und eine von ihm generierte Sequenznummer mitgeteilt. Diese Sequenznummer dient zur Unterscheidung zwischen aktuellen und veralteten Wegen zu dieser Station und wird bei der Veröffentlichung einer Route stets mitgesendet.

Jede Station, die diese Informationen erhält, kann nun ihre eigene Routing-Tabelle anpassen, falls ihr nun neuere oder bessere Wege zur Verfügung stehen.

8.1.3 Reaktion auf Veränderungen der Netzwerktopologie

In Netzwerken mit mobilen Teilnehmern werden ständig Funkverbindungen unterbrochen, da die Stationen des Netzwerkes häufig ihre Position verändern. Ein Teilnehmer eines Ad-Hoc-Netzwerkes erkennt eine getrennte Funkverbindeung entweder auf der Sicherungsschicht oder dadurch, dass ihn seit geraumer Zeit kein Broadcast dieses Nachbarn mehr erreicht hat, mit dem dieser sonst seine Routing-Einträge veröffentlicht.

Die Station, die die Unterbrechung einer Verbindung erkannt hat, aktualisiert den entsprechenden Eintrag in ihrer Routing-Tabelle. Die Sequenznummer wird inkrementiert und der Wert für die Metrik auf ∞ gesetzt.

Um den Mechanismus zu vereinfachen, wurde festgelegt, für von der Zielstation generierte Sequenznummern gerade Zahlen, für aufgrund von Unterbrechnungen von anderen Teilnehmern erstellten, ungerade Zahlen zu verwenden.

Da eine Untebrechung einer Funkverbindung eine bedeutende Veränderung darstellt, wird sofort ein Broadcast versendet. Die Nachbarn können dann sofort ihre Routing-Tabellen an die neue Situation anpassen. Steht die mitgelieferte Sequenznummer für eine neuere Information als die in der Routing-Tabelle gespeicherte, so wird auch hier der alte Eintrag durch den gerade erhaltenen mit Metrik ∞ ersetzt. Es folgt ein Broadcast an alle Nachbarn mit den neuen Werten.

Verfügt eine Station des Ad-Hoc-Netzwerkes, die eine solche Information per Broadcast erhält bereits über einen Eintrag mit endlicher Metrik in der Routing-Tabelle, dessen Sequenznummer größer oder gleich der soeben erhaltenen ist, verfügt sie schon über eine neue Route zum Ziel. Dieser Teilnehmer sendet einen Broadcast an seine Nachbarn, um ihnen diese neue Route mitzuteilen. Das ist der zweite Fall, indem eine sofortige Benachrichtigung aller Nachbarn aufgrund einer bedeutenden Veränderung erfolgt.

Um den Netzwerkverkehr gering zu halten, wird unterschieden zwischen *full dumps*, die die gesamten Routinginformationen enthalten und *incrementals*, die nur die Veränderungen seit dem letzten *full dump* enthalten. Es werden solange *incrementals* verschickt, bis diese nicht mehr in ein Paket passen und sich damit deren Nutzen verringern würde. Anschließend wird ein *full dump* versendet, dem daraufhin wieder *incrementals* folgen können.

8.1.4 Routing-Entscheidung

Erhält ein Teilnehmer des Ad-Hoc-Netzes neue Routinginformationen, im Normalfall durch einen Broadcast eines *incrementals* eines Nachbarn, vergleicht er diese mit den Einträgen in seiner eigenen Routing-Tabelle. Ein vorhandener Eintrag wird entweder ersetzt, falls der erhaltene Eintrag eine höhere Sequenznummer hat und damit neuer ist, oder falls die Sequenznummer die gleiche ist, die neue Route aber über eine bessere Metrik verfügt.

8.1.5 Vermeidung von Fluktuationen

Es besteht die Gefahr, dass eine Station bei gleichbleibender Netzwerktopologie auf unterschiedlichen Wegen verschiedene Routinginformationen erhält und ständig zwischen diesen wechselt, da sie jede eintreffende Information für neuer bzw. besser hält. Dieser Effekt tritt auf, falls die Routinginformationen über den kürzeren Weg, d. h. mit der besseren Metrik, später eintreffen als über den Weg mit der schlechteren Metrik. Die betreffende Station übernimmt dann stets den zuerst erhaltenen Eintrag aufgrund der aktuelleren Sequenznummer. Erreicht sie dann der zweite Eintrag, wird dieser aufgrund der besseren Metrik bei gleicher Sequenznummer bevorzugt.

Im ungünstigsten Fall würden die neuen Einträge jeweils an alle Nachbarn per Broadcast weitergegeben werden, wodurch unnötiger Verkehr im Netz entstehen würde. Um diesen Effekt zu verhindern, wird zunächst zwischen Routing-Einträgen unterschieden, die für die eigene Wegewahl herangezogen werden und Routen, die veröffentlicht werden. Erst wenn eine Route als stabil gilt, wird sie veröffentlicht.

Zur Unterscheidung zwischen stabilen und nicht als stabil geltenden Routen wird zu jedem Routingeintrag zusätzlich die durchschnittliche Zeit zwischen zwei erhaltenen Aktualisierungen gespeichert. Hierdurch kann entschieden werden, ob nach Erhalt einer Route auf eine weitere gewartet wird, die die bisher bestehende bestätigen wird, oder ob die neue als stabil übernommen wird.

Zusätzlich wird dieser Mechanismus genutzt, um festzustellen, ob eine Verbindung zu einem Nachbarn weiterhin besteht. Hat man z.B. im Vergleich zur durchschnittlichen Dauer zwischen den Aktualisierungen lange keine neuen Routingtabellen erhalten, kann davon ausgegangen werden, dass die Verbindung unterbrochen wurde.

8.1.6 Eigenschaften von DSDV

Der DSDV-Algorithmus garantiert zu jeder Zeit kreisfreie Wege zwischen einzelnen Teilnehmern.

Zur Veranschaulichung kann man sich vorstellen, dass alle Wege zu einer Station einen Baum mit dem Ziel der Wege als Wurzel darstellt. Jede Sequenznummer eines Weges wird vom Ziel generiert. Von dort an wird der Baum aufgebaut.

8.2 Dynamic Source Routing (DSR)

Angenommen, man benutzt DSDV in einem Ad-Hoc-Netwzerk, das unter nur sehr geringer Last steht. Trotz des geringen Kommunikationsbedarfs tauschen ständig sämtliche Teilnehmer des Netzwerkes Routinginformationen aus und verbrauchen damit unnötig Energie. Jeder Teilnehmer versucht, zu jeder Zeit einen optimalen Weg zu jedem anderen Teilnehmer im Netz bereitzuhalten.

Das DSR-Protokoll verzichtet auf die ständige Pflege von Wegen zwischen allen Knoten im Netzwerk. Stattdessen werden Wege nur gesucht, falls Daten zu übertragen sind. Dieser Weg wird dann so lange genutzt, bis ein Problem damit auftritt. In einem solchen Fall muss ein neuer Weg aufgebaut werden.

Dieses Vorgehen macht es Teilnehmern im Netz möglich, stromsparend zu arbeiten, falls sie weder selbst kommunizieren möchten noch auf auf einer aktiven Route liegen, auf der ihre Routing-Dienste in Anspruch genommen werden. Zusätzlich wird der Speicherplatz minimiert, der benötigt wird, um die Routing-Tabellen zu speichern.

Beim Dynamic Source Routing Protocol gibt die Datenquelle den gesamten Weg für ein Datenpaket vor. Im Paketkopf jedes Pakets wird eine Liste von Stationen angegeben, über die der Weg zur Zielstation führt. In den meisten Fällen kann eine Route aus dem Cache der jeweiligen Station verwendet werden, die durch frühere Wegwahl bekannt ist. Findet sich kein Weg zur gesuchten Zielstation im Cache, muss DSR zunächst eine passende Route finden.

Die Funktionsweise von DSR wird in zwei unterschiedliche Bereiche unterteilt. Zum einen gibt es die *Route Discovery*, um einen zur Kommunikation benötigten Weg aufzubauen. Der zweite Bereich nennt sich *Route Maintenance* und befasst sich mit dem Aufrechterhalten und Pflegen eines bestehenden Weges. Beide Mechanismen werden nur nach Bedarf angewendet, es erfolgt kein periodischer Austausch von Routing-Informationen.

8.2.1 Route Discovery

Route Discovery ermöglicht es einer Station im Ad-Hoc-Netzwerk, einen Weg zu jedem erreichbaren Teilnehmer zu finden.

Findet eine Station in ihrem Cache keinen Weg zu einer gewünschten Zielstation, initiiert sie eine *Route Discovery*. Sie sendet per Broadcast einen *Route Request*, der die folgenden Informationen enthält:

- Source Address
- Destination Address
- Broadcast ID
- List of Hops

Wie in Abb. 1 zu sehen, sendet der *Initiator* einer *Route Discovery* eine Anfrage an seine Nachbarn. Der *Route Request* enthält neben seiner eigenen Adresse und der der gesuchten Zielstation eine eindeutige *Broadcast ID* und eine Liste der Stationen, über die Daten zurück zur anfragenden Station gesendet werden können. Im Beispiel in Abb. 1 enthält diese Liste zunächst nur die Adresse der Station A selbst.

Ein Empfänger einer solchen Anfrage, der selbst ebenfalls über keinen aktuellen Weg zum Ziel verfügt, leitet die Anfrage an seine Nachbarn weiter. Zuvor fügt er seine eigene Adresse in die Liste der Stationen ein, da die Quellstation von seinen Nachbarn nun über ihn erreichbar ist. Erhält eine Station die gleiche Anfrage mehrfach auf verschiedenen Wegen, was sie anhand der *Broadcast ID* erkennen kann, verwirft sie sämtliche Duplikate.

Erreicht eine Anfrage einen Teilnehmer, der selbst Ziel der Anfrage ist, antwortet dieser, indem er per *unicast* die Liste der Stationen wie in Abb. 2 an die suchende Station sendet. Er kann die Daten per *unicast* senden, da er durch die Liste die einzelnen *Hops* des Weges kennt und die Weiterleitung seines Datenpaketes entsprechend vorgeben kann. Erhält der suchende Teilnehmer die an ihn gesendete Liste, ist eine bidirektionale Kommunikation möglich, da er nun einen Weg zum gesuchten Ziel kennt.

Es ist leicht einzusehen, dass dieser Vorgang nur bidirektionale Verbindungen verwenden kann und eventuell vorhandene unidirektionale Funkstrecken nicht berücksichtigt. Steht der gefundene Weg in umgekehrter Richtung nicht zur Verfügung, muss die Zielstation nun ihrerseits als *Initiator* einer *Route Discovery* auftreten und einen Weg zum ersten Teilnehmer finden. Dem ausgesendeten *Route Request* muss zusätzlich die erhaltene Route beigefügt werden, da diese den ursprünglichen *Initiator* sonst nicht erreichen würde.

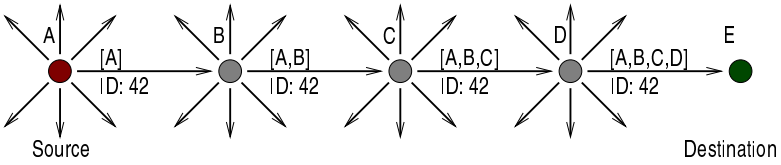

Abbildung 1: DSR Route Discovery - Route Request

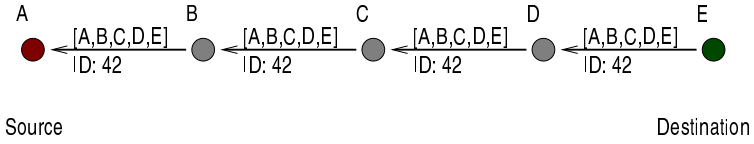

Abbildung 2: DSR Route Discovery - Route Respond

Auch nicht direkt beteiligte Stationen, die wärend einer *Route Discovery* Informationen über mögliche Wege erhalten, speichern diese in ihrem Cache. Auf diese Weise kann die Anzahl der notwendigen *Route Discoverys* verringert werden.

8.2.2 Route Maintenance

Ein funktionsfähiger Weg wird so lange genutzt, bis er durch Veränderungen der Netzwerktopologie unterbrochen wird.

Das Problem besteht nun darin, einen unterbrochenen Weg zu erkennen. Hierfür kann man sich z.B. die vorhandenen Mechanismen der Schicht 2 zu Nutze machen. IEEE802.11 erwartet Bestätigungen für versendete Pakete. Bleibt eine solche Bestätigung wiederholt aus, kann davon ausgegangen werden, dass die Verbindung unterbrochen wurde. Ähnliches gilt für die meisten anderen Funktechniken.

Stellt eine Station eines gewählten Weges zwischen den beiden Kommunikationspartnern fest, dass sie nicht in der Lage ist, das ihr zugestellte Paket dem nächsten *Hop* zuzustellen, sendet sie eine *Error Message* an den ursprünglichen Sender. Dieser löscht dann die bisherige Route aus seinem Cache und baut eine neue Verbindung auf.

Problematisch wird es wiederum bei asymmetrischen Verbindungen. Die Überprüfung, ob noch eine Verbindung besteht, kann dann nur zwischen den beiden Endpunkten der Verbindung geregelt werden. Erkennt einer der beiden Teilnehmer eine Unterbrechung, initiiert er eine neue *Route Discovery*.

Bei der Benutzung von Funktechniken wie IEEE802.11[3] kann man davon ausgehen, dass unidirektionale Funkverbindungen grundsätzlich nicht nutzbar sind, da jedes Paket schon auf Ebene 2 eine Bestätigung erwartet, die den Sender jedoch nicht erreichen kann.

8.3 Ad-Hoc On-Demand Distance-Vector

Der ständige Netzwerkverkehr der durch die Veröffentlichung und Weitergabe von Routing-Informationen entsteht, führt besonders in Funknetzwerken zu stark verringerter Effizienz.

DSDV skaliert z.B. nicht besonders gut, da der Netzwerkverkehr einer Station mit $O(n^2)$ steigt. n bezeichnet dabei die Anzahl aller Stationen im Ad-Hoc-Netzwerk.

Das Ad-Hoc On-Demand Distance-Vector Protokoll (AODV) verfolgt das Ziel, den Datenverkehr im Netz zu verringern, indem er die Verwaltung und Pflege der Routing-Tabellen durch periodischen Austausch von Routing-Informationen unterlässt und die Wegewahl stattdessen nach Bedarf durchführt. Stationen, die weder selbst kommunizieren möchten noch Teil eines aktiven Weges sind, der zwei andere Stationen miteinander verbindet, müssen damit keinerlei Verwaltungsaufgaben erfüllen und können z.B. in den Stromsparmodus gehen.

Die Herausforderung an die Entwicklung eines solchen Algorithmus besteht darin, trotz des verringerten Verwaltungsaufwands und der Wegwahl nach Bedarf eine geringe Latenz beim Aufbau einer Verbindung zwischen zwei Teilnehmern sicherzustellen. Zudem sollen Routing-Informationen

[3] IEEE802.11 ist von sich aus nicht multi-hop ad-hoc-fähig. Damit zwei Teilnehmer eines Netzwerkes nach IEEE802.11 miteinander kommunizieren können, müssen sie sich in direkter Funkreichweite voneinander befinden.

nur an diejenigen Teilnehmer versendet werden, die diese Einträge tatsächlich benötigen, um den für Verwaltungsaufgaben erzeugten Netzwerkverkehr weiter zu verringern.

8.3.1 Überblick Wegewahl mit AODV

Zunächst verfügt kein Teilnehmer des Ad-hoc-Netzwerkes über Informationen bzgl. des Routings. Möchte eine Station nun Daten an einen entfernten Teilnehmer senden, so muss als erstes ein Weg zwischen Quell- und Zielstation gefunden werden.

Die Ermittlung eines aktuellen Weges mit AODV geschieht in zwei Etappen. Zuerst wird der Weg ermittelt, der von der Zielstation zur Verbindung aufbauenden Station führt. Ermittelt wird der dazugehörige Weg dabei beginnend bei der Quellstation. Dieser Teil des Algorithmusses wird als *Reverse Path Setup* bezeichnet.

Anschließend wird über die gleichen Stationen die Verbindung von der Quellstation zur Zielstation aufgebaut. Dieser Mechanismus wird *Forward Path Setup* genannt.

Damit steht dann eine Bidirektionale Verbindung zur Verfügung. Die Prozess zur Ermittlung eines Weges wird als *path discovery* bezeichnet.

8.3.2 Reverse Path Setup

Wird eine Suche nach einem neuen Weg initiert, sendet der suchende Teilnehmer eine *Route Request*-Nachricht an alle seine Nachbarn.

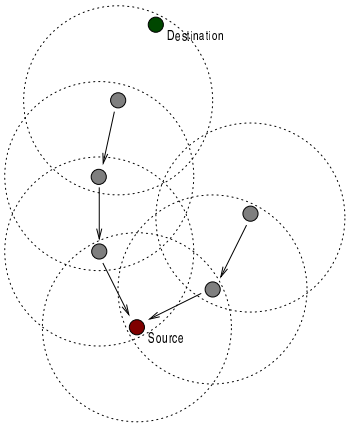

Abbildung 3: Reverse Path Setup

Eine solche Anfrage enthält die folgenden Informationen:

- **Source**
  Bei der Quelle handelt es sich um die Adresse der Station, die eine Verbindung aufbauen möchte und die Suche nach einem aktuellen Weg angestoßen hat.

Je nachdem, auf welcher Schicht das Routing im Netzwerk durchgeführt werden soll, handelt es sich hierbei entweder um eine Hardwareadresse oder um eine Netzwerkadresse.

- **Broadcast ID**

  Die Broadcast-ID der Quellstation wird mit jedem *Route Request* inkrementiert. Sie dient dazu, ältere Anfragen derselben Station von aktuellen zu unterscheiden.

- **Destination**

  Das Feld für die Zielstation enthält die Adresse des gesuchten Kommunikationspartners.

- **Source Sequence Number**

  Die Quellenfolgenummer enthält den Wert der Sequnznummer für die letzte Route, die der suchenden Station bekannt ist.

  Anhand dieser Sequenznummer ist es einem Teilnehmer möglich, zu entscheiden, ob er bereits über eine aktuellere Route als die suchende Station verfügt und er seinen Eintrag dieser Station mitteilen könnte oder ob er seinerseits ein *Route Request* versenden muss.

- **Hop Count**

  Dieses Feld enthält die Anzahl der benötigten Hops, um die Quellstation erreichen zu können.

  Er wird von jedem Teilnehmer, der ein empfangenen *Route Request* erneut sendet inkrementiert.

Eine Station, die eine *Route Request*-Nachricht erhält, ist enweder in der Lage, die Anfrage zu beantworten, falls sie über eine aktuellere Verbindung zum gesuchten Ziel verfügt als die anfragende Station. Zur Entscheidung, ob ein neuerer Weg vorliegt, wird die erhaltene Sequenznummer mit einer evtl. gespeicherten verglichen. Höhere Sequenznummern stehen für neuere Wege.

Ist es einer Station nicht möglich, eine Anfrage selbst zu beantworten, sendet sie die *Route Request* mit inkrementiertem Wert für *Hop Count* per Broadcast an alle Nachbarn weiter.

Jeder Teilnehmer, der einen *Route Request* erhält, speichert sich, von wem er diese Anfrage bekommen hat, um evtl. einen *Route Respond* an diesen weitergeben zu können. Auf diese Weise entsteht der in Abb. 3 sichtbare Pfad zur Quelle der Anfrage. Dieser Eintrag bleibt nur so lange erhalten, wie noch mit einem *Route Respond* gerechnet werden kann. Erfolgt ein Timeout, wird der Eintrag entfernt.

8.3.3 Forward Path Setup

Ist der gesuchte Teilnehmer mit dem Netz verbunden, erreicht ein *Route Request* irgendwann eine Station, die über eine aktuelle Verbindung zur Zielstation verfügt, oder die Zielstation selbst.

Eine solche Station antwortet auf die Anfrage mit einer *Route Respond*-Nachricht, die sie per unicast an den Teilnehmer sendet, von dem sie die Anfrage erhalten hat.

Ein *Route Respond*-Paket enthält die folgenden Felder:

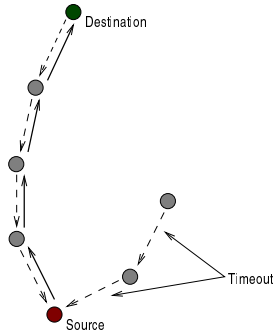

Abbildung 4: Forward Path Setup

- **Source**
  Source ist die Adresse der Station, die die Suche initiiert hat und zu der das Route Respond-Paket weitergeleitet wird.
- **Destination**
  Das Feld *Destination* enthält die Adresse des gesuchten und nun gefundenen Kommunikationspartners.
- **Hop Count**
  Dieses Feld enthält die Anzahl der benötigten Hops, um die Zielstation erreichen zu können.
  Er wird von jedem Teilnehmer, der ein empfangenen *Route Respond* erneut sendet inkrementiert.
- **Lifetime**
  Diese Feld speichert den Zeitpunkt, an dem die Route verworfen wird, falls sie nicht genutzt wird.

Jeder Teilnehmer, der eine solche *Route Respond*-Nachricht erhält, speichert in seiner Routing-Tabelle einen Eintrag für die Station, die die *Route Respond*-Nachricht generiert hat. Dabei wird die Station als *Next Hop* gewählt, von der er die *Route Respond*-Mitteilung erhalten hat. Durch die Anpassung der Routingtabelle jeder Station entsteht der *Forward Path*, wie er in 4 zu sehen ist.

Außerdem wird die *Lifetime* für die Route gemäss dem Eintrag in der erhaltenen Nachricht angepasst.

Anschließend wird die *Route Response* mit inkrementiertem *Hop Count* an den gespeicherten Vorgänger weitergeleitet.

Erreicht die *Route Respond*-Nachricht die Quellstation, ist die Verbindung hergestellt. Der Teilnehmer kann sofort mit dem Senden von Daten beginnen.

8.3.4 Pflege der Routing-Tabellen

Die Routing-Einträge bestehen aus den unten angegebenen Feldern, deren Funktion erläutert wird:

- **Destination**

  Der Wert für *Destination* enthält die Adresse des Ziels, für das dieser Routing-Eintrag angelegt wurde.

- **Next Hop**

  Für jedes Ziel wird im Feld *Next Hop* die Adresse des Nachbarn eingetragen, an den Datenpakete für das in *Destination* angegebene Ziel weitergeleitet werden sollen.

- **Metric**

  Im Feld *Metric* wird eine Bewertung der Route gespeichert. Meist handelt es sich dabei um die Anzahl der Stationen (Hops) bis zum Ziel. Der *Metric*-Wert wird benötigt, um zwei Routen miteinander zu vergleichen, falls ihre *Destination Sequence Number* identisch sind.

- **Destination Sequence number**

  Die *Destination Sequence Number* wird benötigt, um alte Routing-Informationen von neueren zu unterscheiden. Neuere Routen haben größere Sequenznummern.

- **Active Neighbors**

  Das Feld *Active Neighbors* speichert eine Liste mit den Adressen aller Nachbarn, die diese Route nutzen. Diese Nachbarn sind zu informieren, falls die Verbindung unterbrochen wird.

- **Expiration Time**

  Expiration Time gibt den Zeitpunkt an, an dem diese Route als nicht mehr aktuell angesehen wird. Wird dieser Weg genutzt, wird die *Expiration Time* ständig neu gesetzt.

Werden einer Station mögliche Routen übertragen, vergleicht sie zunächst die Werte der *Destination Sequence Number* jeder Route und wählt stets den Eintrag mit der höheren Nummer, d.h. den neueren Eintrag.

Sind die Sequenznummern beider Routen gleich, wird der Eintrag mit der besseren *Metric* gewählt, was kreisfreie Wege garantiert.

8.3.5 Reaktion auf Veränderungen der Netzwerktopologie

Verändern Teilnehmer des Ad-hoc-Netzwerkes ihre Position, die weder selbst mit einem anderen Teilnehmer kommuniziert haben, noch Teil einer aktiven Verbindung waren, ist diese Veränderung nicht relevant und löst keinerlei Reaktionen aus.

Aktive Stationen überwachen ihre genutzten Verbindungen zu ihren Nachbarn mit sog. *hello messages*, die ermitteln, ob die Funkverbindung zu ihren Nachbarn noch besteht.

Kann eine Quellstation ihren Nachbarn nicht mehr erreichen, der bisher als *Next Hop* diente, wird eine erneute *path discovery* initiiert.

Erkennt ein Teilnehmer, der Routing-Dienste leistet, eine Unterbrechung eines Weges, sendet er eine spezielle RRES-Nachricht, die eine inkrementierte Sequenznummer sowie eine Metrik vom Wert ∞ enthält und somit allen vorangehenden Stationen die Unterbrechung mitteilt.

Erreicht dieses Packet die Quellstation, startet diese eine neue *path discovery*.

8.4 Zone Routing Protokoll (ZRP)

Als Zone Routing Protokoll [ZRP] wird das Framework bezeichnet, das aus [IARP], [IERP] und [BRP] gebildet wird. ZRP nimmt eine Sonderstellung bei den vorgestellten Routing-Protokollen ein. Es versucht, die Vorteile aus *Proactive*- und *Preactive*-Ansätzen zu verbinden. Jede Station des Ad-Hoc-Netzwerkes bildet eine Routing-Zone um sich herum. Zu dieser Routing-Zone gehören alle Knoten, die mit einer festgelegten Anzahl von Hops zu erreichen ist. Die Anzahl der Hops wird als Radius der Zone bezeichnet.

Innerhalb seiner eigenen Routing-Zone verfolgt jeder Teilnehmer die *Proactive*-Strategie. Für jede Station, die sich innerhalb der Routing-Zone eines Teilnehmers befindet, speichert sich der Teilnehmer zu jeder Zeit einen aktuellen und optimalen Weg in seiner Routing- Tabelle. Jeder Station sind damit die Teilnehmer bekannt, die sich in der eigenen Routing-Zone befinden. Im Beispiel in Abb. 5 ist zu sehen, welche Stationen sich für einen Radius von 2 innerhalb der Routing-Zone befinden.

Für alle Stationen, die sich außerhalb der Routing-Zone befinden wird der *Reactive*-Ansatz gewählt. Nur nach Bedarf werden Wege zu diesen Knoten ermittelt. Die Stationen, die sich am Rand einer Routing-Zone befinden werden als *Bordernodes* bezeichnet.

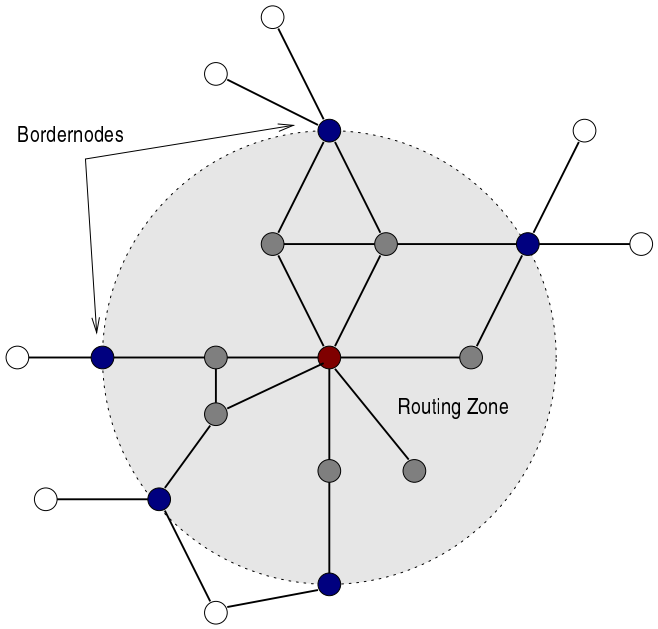

Abbildung 5: Routing Zone mit Radius 2

Der Radius einer Routing-Zone kann nach Bedarf angepasst werden. Ist der Netzwerkverkehr im Ad-Hoc-Netzwerk sehr gering, kann der Radius sehr klein gewählt werden. Damit reduzieren sich die periodisch ausgesendeten Update-Pakete. Die Teilnehmer können Strom sparen. Werden diverse verschiedene Wege benötigt, kommuniziert jede Station mit jeder anderen, ist eine Vergrößerung des Routing-Zone-Radius angebracht. Der

Radius kann ebenfalls inkrementiert werden, falls sich die Netzwerktopologie stabilisiert.

8.4.1 IntrAzone Routing Protokoll (IARP)

Proaktive Link-State-Protokolle haben den Vorteil, jederzeit einen garantiert kreisfreien Weg zu einem gewünschten Ziel anbieten zu können. Jede Station erstellt eine Sicht auf das gesamte Netzwerk und kann selbst einen geeigneten Weg berechnen. In Ad-Hoc-Netzwerken scheint dieser Ansatz ungeeignet, da sich die Netzwerk- Topologie derart schnell verändert, dass in großen Netzwetzwerken eine Station niemals eine korrekte Sicht auf das gesamte Netz erstellen kann, da sich das Netzwerk bereits wieder verändert hat, bevor die Informationen über die Netzwerktopologie die Station überhaupt erreichen. Zudem erzeugen periodisch ausgesendete Informationen gewaltigen Netzwerkverkehr.

Das Zone Routing Protokoll verwendet mit IARP den Ansatz, dass Wege von einer Station nur für einen begrenzten Bereich um die Station herum ständig aktuell und im Voraus präsent gehalten werden. Diesem Ansatz liegt zugrunde, dass das Unterbrechen von Verbindungen zwar lokal von großer Bedeutung, für enfernte Teilnehmer aber meist nicht von Belang ist. Da Stationen typischer Weise nicht auf der einen Seite des Netzwerkes verschwinden und auf der anderen Seite wieder auftauchen, kann man davon ausgehen, dass entfernte Teilnehmer ihre Daten weiterhin an den gleichen Hop weiterzuleiten haben.

Realisiert wird die Routing-Zone um einen Teilnehmer indem dieser seine periodisch ausgesendeten Updates seiner Verbindungen mit einer kleinen TTL versieht. Der TTL-Wert gibt dabei gerade den Radius für die Routing-Zone an.

Als Routing-Protokolle für diese beschränke Routing-Zone kommen beliebige vorhandene proactive Link-State-Algorithmen in Frage.

8.4.2 IntErzone Routing Protokoll (IERP)

Möchte ein Teilnehmer eines Ad-Hoc-Netzwerkes mit einem anderen kommunizieren ermittelt er zunächst, ob sich dieser Teilnehmer in seiner eigenen Routing-Zone befindet. Ist das nicht der Fall, muss zunächst ein Weg zum gewünschten Ziel gefunden werden.

Eine *Route Discovery* teilt sich *Route Request* und *Route Response* auf. Die suchende Station sendet ihre Anfrage an alle ihre Bordernodes aus. Diese ermitteln ihrerseits, ob sich der gesuchte Teilnehmer in ihrer Routing-Zone befindet. Ist das der Fall, sendet der betreffende Bordernode eine Antwort an den suchenden Teilnehmer zurück. Anderenfalls sendet die Station die Anfrage an ihre eigenen Bordernodes weiter. Das Weiterleiten an die Bordernodes ist ausreichend, da die dazwischenliegenden Stationen, den Teilnehmern stets bekannt sind.

Es kann auch hier jeder beliebige Distance-Vector-Algorithmus benutzt werden. Es muss nur jeweils angepasst werden, dass Anfragen nicht an alle Nachbarn weitergeleitet werden, sondern nur an die Bordernodes. Kommt beispielsweise DSR zur Anwendung, ist das Ergebnis einer Anfrage eine

Liste von Stationen, von denen jede Bordernode der vorangehenden in der Liste ist.

Ein weiterer Vorteil von ZRP liegt in der Benutzung der Bordernodes. Tritt eine Unterbrechung einer Verbindung zwischen zwei Stationen auf, handelt es sich um ein lokales Problem. Unter Umständen ist es einem betreffenden Knoten jedoch möglich, diese Unterbrechung zu umgehen, falls sie sich innerhalb seiner Routing-Zone befindet und er bereits über eine neue Verbindung verfügt. Mit ZRP kann man also sehr stabile und selbstreparierende Wege nutzen.

8.4.3 Bordercast Resolution Protokoll (BRP)

Bordercasting arbeitet im Gegensatz zu Broadcasting sehr viel effizienter. Jede Station weiß, ob sich eine gesuchte Station in der Routing-Zone befindet. Ist das nicht der Fall, reicht es aus, die Anfragen an die Bordernodes weiterzuleiten. Ein Fluten der Routing-Zone mit Broadcast- Paketen ist nicht notwendig.

Das Bordercast Routing Protokoll legt fest, wie Bordernodes ermittelt werden. Die Bordernodes werden wärend der Aktivität des Intrazone Routing Protokolls [IARP] gefunden. Eine Station, die ihre Routingtabelle veröffentlicht, versieht ihre Pakete mit einer TTL. Da der Wert der TTL gerade dem Radius der Routing-Zone entspricht, erkennen Stationen, an denen die TTL auf Null heruntergezählt und das Paket verworfen wird, dass sie Bordernodes der Routing-Zone des Absenders des Pakets sind. Anschließend teilen sie der betreffenden Station mit, dass sie selbst Bordernode ihrer Routing-Zone sind.

Möglich ist auch der Einsatz von multicast-Verbindungen zwischen einer Station und ihren Bordernodes. Auf diese Weise wird das Zone Routing Protokoll gut skalierbar und sehr effizient.

8.5 Fisheye Routing Protokoll (FRP)

Das Fisheye Routing Protokoll geht davon aus, dass entfernte Stationen nur die ungefähre Richtung wissen müssen, in die sie ein Paket weiterzuleiten haben. Erst in der näheren Umgebung des Zielteilnehmrs werden genaue Informationen darüber notwendig, wo der gesuchte Teinehmer zu finden ist. Wird eine Verbindung unterbrochen, ist dies zunächst nur lokal von Bedeutung. Für entfernte Stationen hat es jedoch meist keinen Einfluss auf die Routing-Entscheidungen, da sich die gesuchte Station weiterhin grob in der gleichen Umgebung wie bisher befinden wird.

FRP ist eine Link-State-Protokoll und nutzt den oben genannten Effekt aus, indem es Routing-Einträge, die entfernte Stationen betreffen, seltener veröffentlicht als die, die Stationen in der nahen Umgebung betreffen. Auf diese Weise kann der Netzwerkverkehr, der zum Verbreiten von Link-State- Informationen benötigt wird, stark reduziert werden.

9 Cluster-Based Networks

Besonders in großen Netzwerken entstehen Probleme durch Interferenzen, Kollisionen und den Speicherbedarf der Routing-Tabellen. Diesen Pro-

blemen kann man entgegenwirken, indem ein Netzwerk in kleinere administrative Einheiten *(Cluster)* eingeteilt wird. Jeder Cluster muss nun zunächst die Konnektivität aller seiner Knoten untereinander sicherstellen. Dabei sind die Stationen des Clusters vollkommen unabhängig von den Teilnehmern des restlichen Netzwerkes. Um Interferenzen zwischen Clustern zu minimieren, können bei der Kommunikation innerhalb eines Clusters Code-Muliplex-Verfahren eingesetzt werden.

Zusätzlich müssen Funkverbindungen zur Verfügung stehen, die Cluster untereinander verbinden. Diese können einen eigenen Code verwenden, was Störungen weiter verringert.

9.1 Link-Cluster Architecture

Jeder Cluster besteht aus einem *Clusterhead* allen Knoten die diesen *Clusterhead* direkt erreichen können. Einige dieser Knoten können als Gateway dienen, falls sie Funkverbindungen zu anderen *Clustern* aufbauen können.

Um ein Netzwerk in einzelne *Cluster* aufteilen zu können, müssen die Stationen in der Lage sein, *Clusterheads* zu wählen und Gateways zu ermitteln.

9.2 Clusterheads

Es gibt mehrere Möglichkeiten, geeignete *Clusterheads* zu wählen. Wir beschränken uns jedoch auf einen verteilten Algorithmus, da dieser sich für Ad-Hoc-Netzwerke am besten eignet.

Jeder Teilnehmer eines Netzwerkes zählt die Stationen, zu denen er eine bidirektionale Verbindung aufbauen kann. Anschließend teilt er seinen Nachbarn diesen Wert mit. Kann eine Station mehr direkte Verbindungen aufbauen als alle seine Nachbarn, ernennt er sich als *Clusterhead* und gründet einen neuen *Cluster*. Alle seine Nachbarn gehören nun zu diesem *Cluster* und können selbst keinen *Cluster* mehr gründen. Dieser Vorgang ist abgeschlossen, sobald jeder Teilnehmer eines Netzes einem *Cluster* angehört.

9.3 Gateways

Wie in Abb. 6 zu sehen ist, kann ein Gateway entweder Teilnehmer zweier *Cluster* sein, da er zwei *Clusterheads* direkt erreichen kann. Oder es befindet sich eine Station eines anderen *Clusters* in seiner Reichweite, die ebenfalls als Gateway agieren kann. Die Verbindung zwischen den beiden betreffenden *Clustern* wird dann über diese beiden Stationen aufgebaut.

9.4 Mobilität der Teilnehmer

Aufgrund der Mobilität der Teilnehmer eines Ad-Hoc-Netzwerkes, kann es sein, dass die gewählte Einteilung in *Cluster* angepasst werden muss. Es gibt verschiedene Ereignisse, die eine Neuordnung notwendig machen.

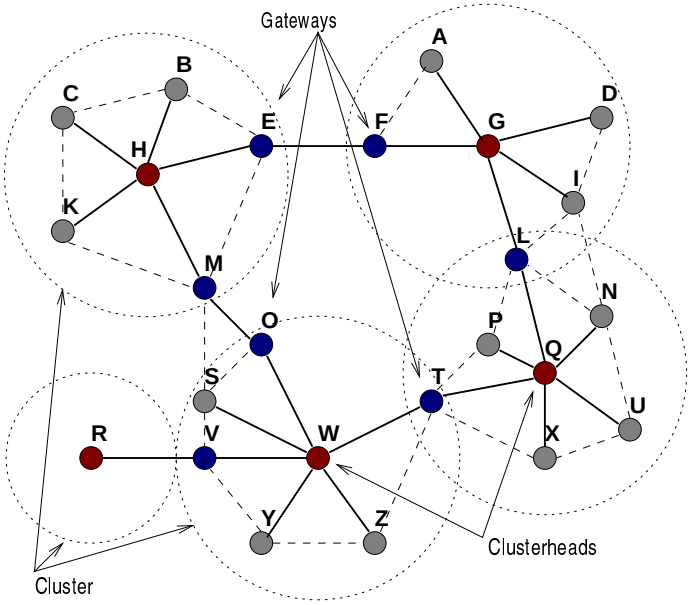

Abbildung 6: Cluster Netzwerke

- Ein Knoten verlässt einen Cluster
- Ein Knoten tritt in einen Cluster ein
- Zwei Clusterheads kommen in direkte Funkreichweite

9.5 Routing in Cluster-basierten Netzwerken

Durch die hier beschriebene Clusterbildung können Interferenzen verringert werden. Die Effizienz und Robustheit des Netzwerkes wird jedoch stark geschwächt. Es werden nur spezielle Kommunikationswege genutzt, obwohl u.U. auch andere besser geeignete Wege existieren. Daten werden zwischen Clustern nur über Clusterheads und Gateways weitergeleitet. Dieser hierdurch entstehende Kommunikationsweg wird als Backbone bezeichnet. Es kann schnell geschehen, dass ein Gateway oder Clusterhead des Backbones zum *Single Point of Failure* wird, bei dessen Ausfall der Datenaustausch zwischen Teilen des Netzes zum Erliegen kommen würde.

Um die durch Clusterbildung gewonnenen Vorteile nicht zu verlieren und dennoch ein effizientes und stabiles Netzwerk zu erhalten gibt es verschiedene Ansätze.

Alle Stationen eines Netzwerkes müssen schnell in der Lage sein, als Gateway oder Clusterhead zu agieren. Sie müssen daher schon als normale Stationen eines Clusters die Informationen ermitteln, die es ihnen ermöglichen, sofort eine dieser Funktionen zu übernehmen.

Damit die Stabilität des gesamten Netzwerkes nicht an einer einzigen Station hängt, können redundante Backbones ermittelt werden. Fällt der aktuelle Backbone aus, steht damit schnell ein neuer Weg zur Verfügung, der diese Aufgabe übernehmen kann.

10 Alternative Metriken

Bisher ist zum Vergleich zweier Wege zwischen zwei Teilnehmern eines Ad-Hoc-Netzwerkes stets die Anzahl der *Hops* auf diesem Weg als Metrik herangezogen worden.

Gerade in Funknetzwerken ist dieser Anzatz nicht immer als optimal anzusehen. Im Vergleich zu kabelgebundenen Netzwerken unterscheiden sich Funkstrecken oft stark in ihrer Qualität. Ein Weg, der länger in Bezug auf die Anzahl der zu durchlaufenden Stationen ist, kann durchaus die bessere Wahl als ein kurzer Weg mit hohen Verlustraten sein.

Es allerdings schwierig, die Qualität einer Funkstrecke bei der Wegwahl zu berücksichtigen, da auch sie starken Schwankungen unterworfen ist. Ein Versuch, ein Maß für die wahrscheinliche Qualität einer Funkstrecke zu finden verfolgt der Ansatz des *Least Interference Routing (LIR).*

Jede Station eines Ad-Hoc-Netzwerkes speichert sich, wie viele Nachbarn, sie zur Zeit empfangen kann. Mit jedem Nachbarn steigt die Gefahr von Kollisionen beim Funkverkehr, da zwei Teilnehmer, die sich gegenseitig empfangen können, sich ebensogut bei gleichzeitiger Kommunikation durch Interferenzen gegenseitig stören können.

Stehen einer Station bei der Wegwahl zwei alternative Wege zur Verfügung, wählt der Teilnehmer nun stets den Weg, für den die Summe der Nachbarn geringer und damit die Wahrscheinlichkeit einer Kollision geringer ist.

Teil III

Zusammenfassung

11 Ad-hoc-Netzwerke

Ad-hoc-Netzwerke zeichnen sich dadurch aus, dass ihre Infrastruktur nicht permanent gleichbleibend ist. Der als am wichtigsten angesehene Typ von Ad-hoc-Netzwerken ist ein *mobiles* Ad-hoc-Netzwerk, *MANET* genannt. Üblicherweise arbeiten solche Netzwerke schnurlos.

Die möglichen Einsatzszenarien sind äußerst vielfältig und reichen von privater Nutzung über Konferenzen, Straßenverkehr und Notfälle bis zum militärischen Einsatz. In jedem Fall gilt es, besondere technische Herausforderungen anzunehmen, die sich auf Themen wie Funkübertragung, Datenvermittlung, Sicherheit oder auch Energieverbrauch beziehen.

Etliche bekannte Standards zur schnurlosen Datenübertragung bieten einen Ad-hoc-Modus (z.B. 802.11b) oder sind ausschließlich dafür gedacht (z.B. Bluetooth). Der praktische Einsatz ist bisher jedoch äußerst selten zu beobachten.

12 Routing in Ad-hoc-Netzwerken

Für die Wegewahl in Ad-hoc-Netzwerken bedarf es sehr viel flexibeleren Algorithmen als in kabelgebundenen Netzen, die wenigen im Lauf der Zeit nur selten auf Veränderungen reagieren müssen. Es gibt eine Vielzahl von Ansätzen, die speziell auf die Besonderheiten von Ad-hoc-Netzwerken eingehen. Keins der vorgestellten Verfahren stellt dabei einen Königsweg dar. Ad-hoc-Netzwerke können in unterschiedlichster Form auftreten. Soll ein passender Algorithmus für ein Netzwerken zwischen Fahrzeugen und Komponenten in der Nähe der Fahrbahn aufgebaut werden, über das Informationen zur Verkehrssituation oder dem aktuellen Umfeld ausgetauscht werden sollen, steht eher die Mobilität der Teilnehmer im Vordergrund. Routing-Algorithmen müssen schnell in der Lage sein, passende Wege zwischen den Stationen zu finden. Fast unbedeutend ist dagegen das Problem des Energieverbrauchs und der Sendeleistung der Teilnehmer, deren Lösung bei vielen Routing-Algorithmen im Vordergrund steht. Anders sieht es aus wenn ein Ad-hoc-Netzwerk während einer Konferenz aufgebaut werden soll. Die Teilnehmer einer Konferenz treffen in einem Raum zusammen, diskutieren, tauschen Informationen und Daten aus und benötigen Zugang zum Internet. Oft kommen dabei PDAs zur Anwendung, die nur über wenig Energie Verfügen. Zumeist kann man davon ausgehen, dass ein Ad-hoc-Netzwerk zu diesem Zweck keine hoch dynamischen Komponenten enthält. Vielmehr werden sich einmal gefundene Routen während der Konferenz kaum ändern.

Die Anzahl der Stationen, für die ein Ad-hoc-Netzwerk zur Verfügung gestellt werden soll, ist die zweite veränderliche Komponente eines Ad-hoc-Netzwerks. Erst in einem großen Netzwerk mit einer hohen Anzahl von Stationen ist damit zu rechnen, dass die Ansätze von ZRP und FSR

zum Tragen kommen. Clusterbildung wird ebenso erst in großen Netzwerken besonders hilfreich oder notwendig werden.

Es gibt eine Vielzahl von Anwendungsmöglichkeiten von Ad-hoc-Netzwerken. Jede stellt spezielle Ansprüche an das Routing-Verfahren. Die vielen unterschiedlichen Algorithmen haben daher ihre Berechtigung. Welcher Algorithmus sich aus welchem Grund in dem ein oder anderen Anwendungsgebiet durchsetzen wird bleibt abzuwarten. Bisher[4] stehen sämtliche Algorithmen, die in dieser Arbeit behandelt werden, erst als Internet-Draft zur Verfügung und wurde bisher in keinem allgemein erhältlichen System implementiert.

[4]Februar 2002

Teil IV

Anhang

A Abkürzungen

AODV – *Ad-Hoc On-Demand Distance Vector Routing*

DSDV – *Highly Dynamic Destination-Sequenced Distance-Vecor Routing*

DSR – *Dynamic Source Routing*

LOS – *Line Of Sight*

MANET – *Mobile Ad-hoc Network*

PAN – *Personal Area Network*

PDA – *Personal Digital Assistant*

POS – *Personal Operating Space*

VPN – *Virtual Private Network*

WEP – *Wired Equivalent Privacy*

ZRP – *Zone Routing Protocol*

B Danksagung

Wir danken unseren Mamas, der Cafeteria, Linus, Linda, RMS für den Emacs, der IEEE (dafür, dass sie endlich eingesehen haben, dass ein Standard niemandem was bringt, wenn er ihn nicht einsehen kann), ...

Literatur

[802.15-TG1] IEEE 802.15, Task Group 1. http://www.ieee802.org/15/pub/TG1.html 13

[AODV] Charles Perkins, Elizabeth Belding-Royer, Samir Das. *Ad Hoc On Demand Distance Vector (AODV) Routing.* http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-09.txt, November 2001 (work in progress).

[Briesem] Linda Briesemeister. *Group Membership and Communication in Highly Mobile Ad Hoc Networks.* Dissertation TU Berlin, 2001-11-05. 8

[BRP] Zygmunt J. Haas, Marc R. Pearlman, Prince Samar. *The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks.* http://www.ietf.org/internet-drafts/draft-ietf-manet-zone-brp-01.txt, June 2001 (work in progress). 30

[Cormen] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest. *Introduction to Algorithms.* The MIT Press, 1990. 16, 17

[DSR] David B. Johnson, David A. Maltz, Yih-Chun Hu, Jorjeta G. Jetcheva. *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR).* http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-06.txt, November 2001 (work in progress).

[Feder] Hannes Federrath, Dozent. *Vorlesung Netzsicherheit, Freie Universität Berlin, 2000.* http://www.inf.fu-berlin.de/lehre/WS00/sicherheit/1SiEinf.pdf 11

[IARP] Zygmunt J. Haas, Marc R. Pearlman, Prince Samar. *The Intrazone Routing Protocol (IARP) for Ad Hoc Networks.* http://www.ietf.org/internet-drafts/draft-ietf-manet-zone-iarp-01.txt, June 2001 (work in progress). 30, 32

[IERP] Zygmunt J. Haas, Marc R. Pearlman, Prince Samar. *The Interzone Routing Protocol (IERP) for Ad Hoc Networks.* http://www.ietf.org/internet-drafts/draft-ietf-manet-zone-ierp-01.txt, June 2001 (work in progress). 30

[Mehling] Markus Mehling. *Electronic Dust.* Link fehlt noch... 9

[Perkins] Charles Perkins, editor. *Ad hoc networking.* Addison-Wesley, 2001. 7, 8, 9, 10

[Prenzl] Prenzl.net e.V.. http://www.prenzl.net 8

[RFC1247] OSPF - Open Shortest Path First 18

[Schiller] Jochen Schiller. *Mobilkommunikation.* Addison Wesley 2000 11, 16

[Tanenbaum] A. S. Tanenbaum. *Computer Networks.* 18

[Term] Terminodes.org. http://www.terminodes.org/overview.html 8

[WaveWAN] WaveWAN. http://www.wavewan.de 8

[WEP] Scott Fluhrer, Itsik Mantin, Adi Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4.* http://www.crypto.com/papers/others/rc4_ksaproc.ps 13

[ZRP] Zygmunt J. Haas, Marc R. Pearlman, Prince Samar. *Zone Routing Protocol (ZRP). IETF Internet Draft* http://www.ietf.org/internet-drafts/draft-ietf-manet-zrp-04.txt January 2001 (work in progress). 30

Index