

# Multicast Routing in Ad Hoc Netzwerken

Oliver Finger

## Abstract

Dieses Dokument befasst sich mit dem Multicast Routing in Ad Hoc Netzwerken. Zunächst wird gezeigt, was Ad Hoc Netzwerke eigentlich sind, welche Herausforderungen und Anwendungsgebiete sie beinhalten. Dann wird weiter auf die Multicast Routing Protokolle eingegangen, wobei hier zunächst herausgestellt wird, warum Multicast eigentlich wird. Darauf werden einige wesentliche Verfahren, wie das Shared Tree [5] und Source Tree Verfahren, sowie das Flooding beschrieben. Im Anschluss folgt eine Aufzählung von leitungsgebundenen Multicast Routing Protokollen, die ihre Unterscheidung in Abhängigkeit der räumlichen Reichweite finden. Man spricht dabei vom sog. Dense und Sparse Mode. Am Ende werden schließlich das Adaptive Shared Tree Multicast sowie das Forwarding Group Multicast Protokoll in leitungslosen Netzwerken angesprochen.

## 1. Einleitung

Ad Hoc Netzwerke gehören zu der Kategorie von leitungslosen Netzen und werden ausschließlich von mobilen Geräten gebildet. Dieses Netzwerk besitzt keine feste Infrastruktur und muss sich selbst organisieren. Das Routen zwischen zwei Endgeräten kann über mehrere Hops funktionieren. Hierbei wird zwischen dem „single-hop“ sowie dem „multi-hop“ unterschieden. Das „single-hop“ Verfahren zeichnet sich dadurch aus, dass alle teilnehmenden Geräte im Netzwerk selbst miteinander in Verbindung treten können, um Datenpakete auszutauschen. Beim „multi-hop“ Verfahren können alle teilnehmenden Geräte im Netzwerk über mehrer Knoten miteinander in Verbindung treten. Genau aus diesem Grund, werden Ad Hoc Netzwerke auch als „multi-hop“ Ad Hoc Netzwerke bezeichnet, da jeder Knoten gleichzeitig als Endgerät und Router funktioniert. Ad Hoc Netzwerke sind einer dynamischen Netzwerktopologie unterworfen und gerade diesbezüglich werden hohe Anforderungen an Multicast Routing Protokolle gestellt, die dieser dynamischen Struktur gerecht werden müssen.

Die größte Herausforderung für mobile drahtlose Netzwerke besteht in der Versorgung der Endgeräte mit ausreichend viel Energie. Dabei sprechen wir von Geräten, deren Praktikabilität im Vordergrund steht, d.h. sie sollen klein, leicht und unabhängig vom Stromnetz betrieben werden können. Eine weitere Herausforderung besteht im Forwarding. Hierbei sollen alle Teilnehmer eines Ad Hoc Netzwerkes mit jedem anderen Teilnehmer kommunizieren können, auch wenn der gewünschte Kommunikationspartner nicht in direkter Funkreichweite agiert. Somit muss ein Teilnehmer als Relais-Station verwendet werden, welches wiederum Energie und Prozessorleistung kostet, da die Datenpakete empfangen, analysiert und weitergeschickt werden müssen. Das Routing stellt ebenfalls ein großes Problem dar, da durch die hohe Dynamik im Netzwerk klassische Routingverfahren, die erheblich auf einer statischen Zustandshaltung in den Routingtabellen aufbauen, nicht anwendbar sind. Zudem ist das Konvergenzkriterium von entscheidender Rolle, wobei möglichst schnell, in dem dynamischen Netz, ein stabiles Routing fortgesetzt werden soll.

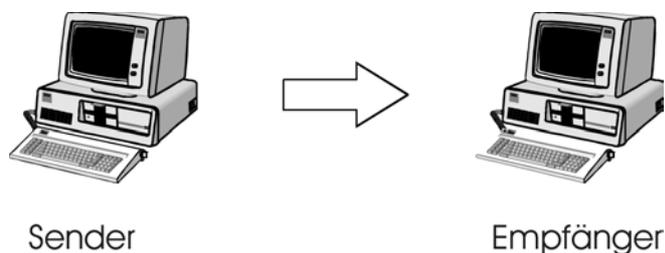
Ein weiteres Problem ist die Asymmetrie der Funkverbindungen. So ist es möglich, dass die Verbindungsqualität in beide Richtungen stark unterschiedlich sein kann. Einem Teilnehmer, dem es möglich ist mit maximaler Leistung ein Datenpaket zu übertragen, kann es passieren, dass dieser aber keine Datenpakete vom Empfänger zurück bekommt. Auf Grund der sehr

dynamischen Netzwerktopologie in mobilen Ad Hoc Netzwerken, kann es zu hohen Verlusten von Datenpaketen kommen. Die heutigen Standards zur mobilen Funkkommunikation, die auch die Bildung von Ad Hoc Netzwerken unterstützen, sorgen auch dafür, dass die Datenpakete sicher und in der richtigen Reihenfolge dem Empfänger übermittelt werden, wie z.B. : IEEE802.11 [2], Bluetooth [2]. In einem Ad Hoc Netzwerk sind die Knoten mobil und es fehlt hier an einer zentralen Koordination der Zugriffe von Knoten auf ein gemeinsam benutztes Medium. Ein Media Access Control (MAC) Protokoll muss folglich den Zugriff regeln und zugleich mögliche Kollisionen mit benachbarten Knoten vermeiden können. Sicherheit besteht aus Vertraulichkeit, Integrität und Verfügbarkeit und ist für den Nutzer des Netzwerkes von entscheidenden Interesse. Auf Grund der z.T. geringen Rechenleistung der Geräte, müssen Verschlüsselungsmechanismen beschränkt werden. Ein Teilnehmer in einem Ad Hoc Netzwerk ist jedoch durch die Fähigkeit und Bereitschaft zum Weiterleiten von Datenpaketen in seiner Sicherheit gefährdet. Des weiteren besteht die Möglichkeit, dass sich Fremde in ein drahtloses Netzwerk anbinden können, um somit Datenpakete abzufangen. Basierend auf den Vorteilen lassen sich eine Vielzahl von Anwendungsmöglichkeiten für Ad Hoc Netzwerke ableiten. Zum einen können sich die Netze schnell und dynamisch aufbauen, da sie keine Infrastruktur besitzen und zum anderen, dass die Sendeleistung niedriger sein kann als in Netzwerken mit gegebener Infrastruktur, wenn z.B. die Entfernung zum nächsten Nachbarn geringer ist als zur Basisstation.

So können Ad Hoc Netzwerk z.B. im militärischen Bereich eingesetzt werden, um Truppenverbände zu koordinieren. Einsatzgebiete im zivilen Bereich, sind in der Wirtschaft vor allem bei Konferenzen, Ausstellungen, Meetings oder Vorlesungen zu sehen. Auch im Forschungsbereich, wie der Telematik, werden Ad Hoc Netze verwandt, betrachtet man z.B. den Bereich des Straßenverkehrs, wobei daran gearbeitet wird, dass einzelne Fahrzeuge, Daten untereinander austauschen können, um den Verkehrsfluss auf den Straßen zu optimieren. Denkt man auch an das Entertainment auf Reisen bezüglich Filesharing, elektronische Spiele im Zug oder Auto, so bieten auch hier Ad Hoc Netze besondere Möglichkeiten. Des weiteren können wir auch Anwendungsbeispiel im Bereich von Katastrophenfällen finden, wenn z.B. das Telefonnetz aufgrund widriger natürlicher Umstände zusammenbricht.

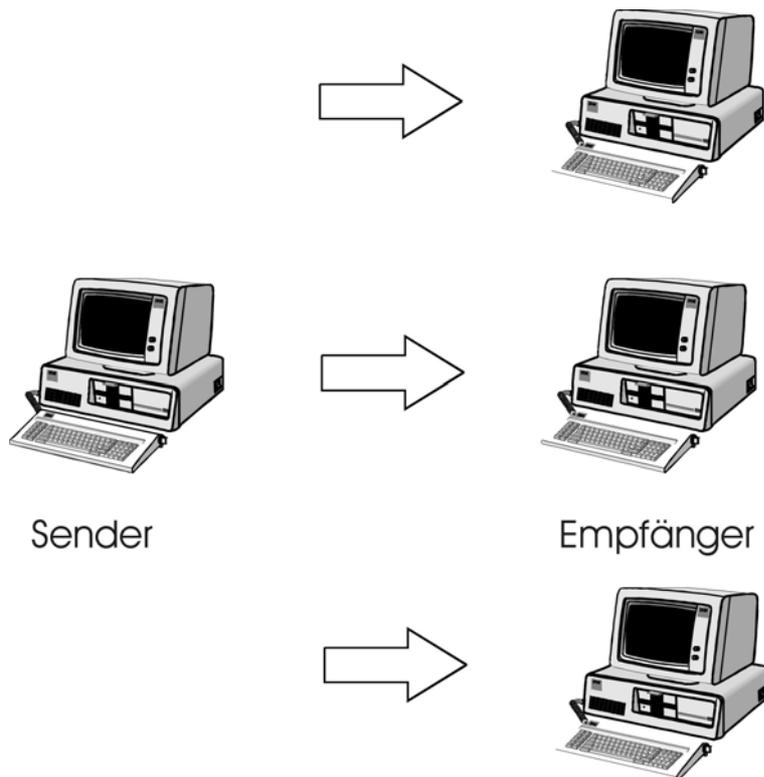
## 2. Multicast Routing Protokolle

### 2.1 Unicast vs. Multicast



**Abbildung 1: Unicast (unidirektional)**

Die Kommunikationsform Unicast [3] entspricht einer 1:1 Kommunikation, mit genau einem Sender und eine Empfänger. Ein Beispiel hierfür ist der klassische Briefverkehr. Dieser Austausch der Daten erfolgt somit unidirektional. Es gibt die erweiterte Form der bidirektionalen Kommunikation. Dieses setzt sich aus zwei Unicast Kommunikationsbeziehungen in entgegengesetzter Richtung zusammen, und wird über das gleiche Kommunikationsmedium geleitet, wie z.B. beim Telefonieren.



**Abbildung 2: Multicast**

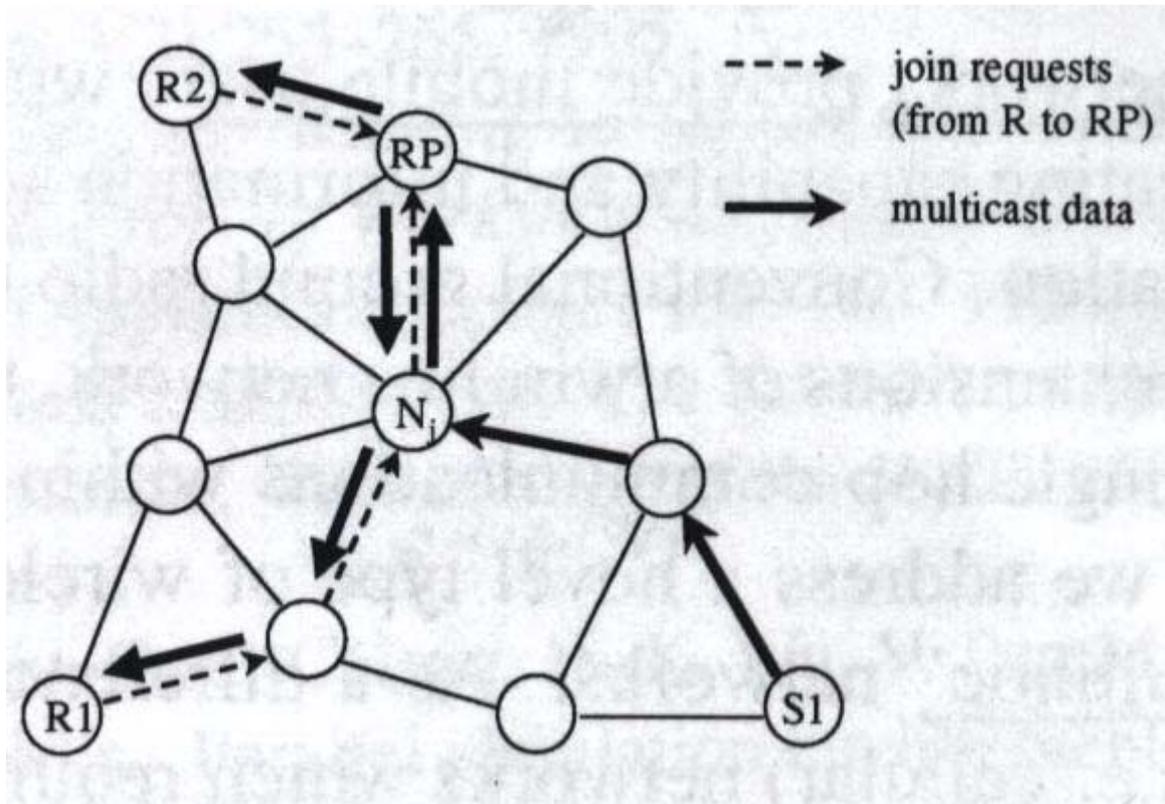
Bei der Multicast [3] Kommunikation sendet eine Datenquelle Nutzdaten an mehrere Empfänger. Hierbei spricht man von einer 1:n Kommunikation, wobei es einen Sender und n Empfänger gibt. Diese Kommunikationsform ist in diesem Sinne unidirektional. Sollen nun allerdings bidirektionale Gruppenkommunikationen stattfinden, so sind bei einer Gruppe von n Teilnehmern auch n Multicast Kommunikationsbeziehungen erforderlich, einer pro Teilnehmer. Pragmatisch gesehen, lässt sich eine Multicast Kommunikation also auch über Unicast Kommunikation emulieren. Das Problem hierbei ist allerdings, dass es dabei zu einer Verschwendung von Netzressourcen kommt, da die Datenpakete mehrmals empfangen und weiter versendet werden müssen, hinzu werden beim Sender mehrere Kommunikationsbeziehungen gleichzeitig unterhalten, die den Ressourcenverbrauch erhöhen. Lege man allerdings eine Multicast Kommunikation zu Grunde, so werden die Daten nur einmal in das Netz versendet. Die Zwischensysteme kopieren die Dateneinheiten jeweils auf solche Ausgangslinks, an denen Gruppenmitglieder angesiedelt sind. Dies führt zu einer Verringerung des Verkehrsaufwandes im Netz, sowie zu einem geringeren Aufwand in den Zwischensystemen. Bei einer Unicast Kommunikation werden darüber hinaus die Daten in unterschiedliche zeitlichen Abständen versandt, bedingt durch die n-fache hintereinander Übertragung. So ergeben sich wesentliche Vorteile des Multicast gegenüber dem Unicast auf Grund der geringeren Belastung der beteiligten Systeme bezüglich des Datenvolumens und Verarbeitungskapazität, welches sich vor allem in großen Gruppen bemerkbar macht.

## 2.2 Shared Tree und Source Tree Verfahren

Die verschiedenen Multicast Routingprotokolle bauen auf einen Spannbaum auf. Dabei gibt es Protokolle, die für jede Gruppe nur einen Baum aufbauen. Diese werden Shared Tree Verfahren genannt. Ein bestimmter Router bildet hier die Wurzel des Routingbaumes [3]. Jeder Sender sendet seine Multicast Daten an die Gruppe über diesen Router (oft als Core

Router bezeichnet [1]). Die andere Möglichkeit ist, dass für jeden Sender einer Multicast Gruppe ein eigener Routingbaum aufgebaut wird. Diese Protokolle werden als Source Routed Tree Protokolle bezeichnet, das heißt jeder Sender bildet die Wurzel eines eigenen Multicast Baumes [3].

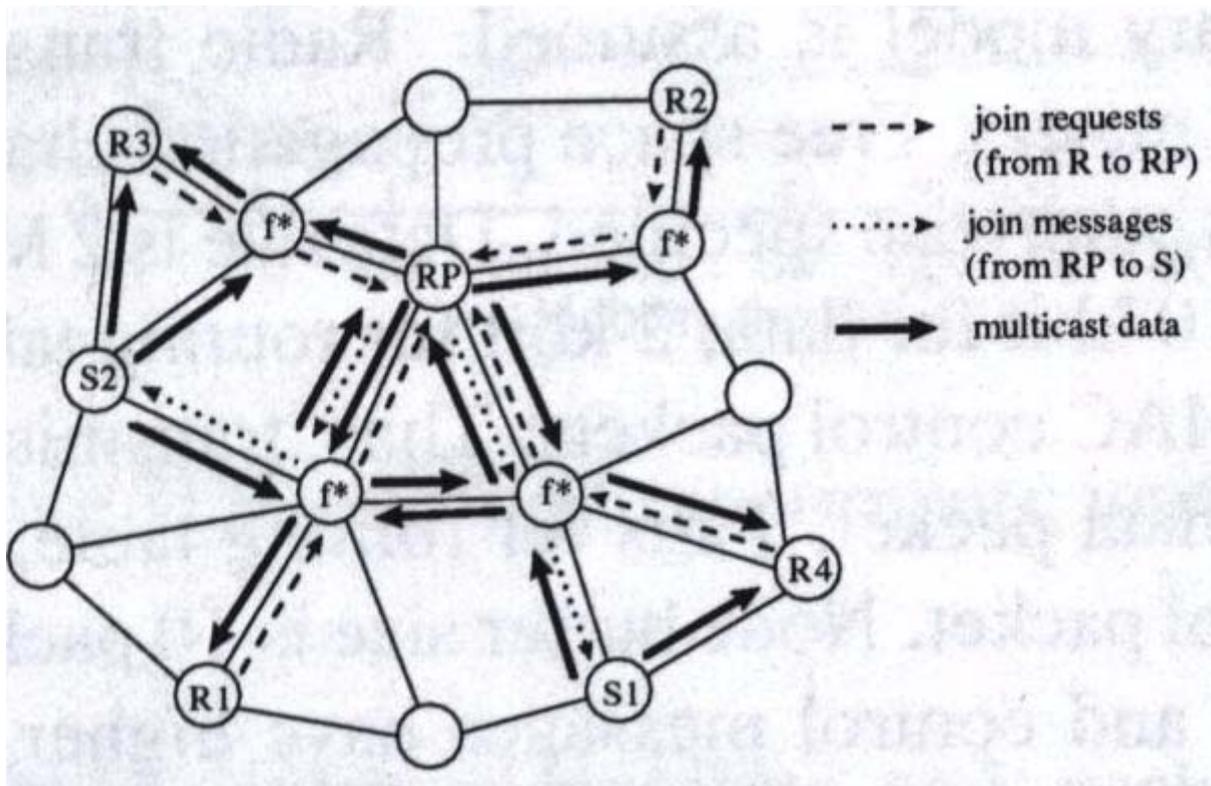
Das Shared Tree Verfahren unterstützt n:n Kommunikationen mit verschiedenen Sendern und Empfängern. In jeder Multicast Gruppe werden Datenpakete von den Sendern zu allen Empfängern verschickt. Das Shared Tree Verfahren basiert dabei auf Rendezvous Punkten.



**Abbildung 3: Unicast Sendermodus**

Beim Unicast Sendemodus, kennt der Sender (S1) die Adressen der Empfänger (R1), (R2) nicht, sondern nur die des Rendezvous Punktes (RP). Somit besteht die einfachste Möglichkeit des Senders (S1) ein Datenpakete in der Gruppe zu verteilen darin, eben dieses Datenpaket verkapselt per Unicast zum Rendezvous Punkt (RP) zu verschicken, welcher diese Pakete zu allen Empfängern (R1), (R2) weiterleitet.

Ein weitaus höhere Bandbreiteeffizienz würde sich dadurch ergeben, wenn es möglich wäre die Datenpakete direkt an die Empfänger (R1), (R2) weiterleiten zu können, ohne den Umweg über den Rendezvous Punkt (RP) gehen zu müssen.



**Abbildung 4: Multicast Sendemodus**

Um diesen Multicast Sendemodus zu ermöglichen, verschickt der Rendezvous Punkt (RP) nach Erhalt des ersten Datenpaketes vom Sender (S1) eine Join-Nachricht an diesen zurück. Das Ergebnis davon ist, dass alle Router (f\*), die diese Join-Nachricht durchläuft, die Senderadresse mit in ihre Multicast-Adressliste aufnehmen, wodurch diese jetzt in der Lage sind, Multicast-Pakete vom Sender (S1) direkt im Multicast weiterzuleiten. Ein aber weiter bestehendes Problem besteht darin, dass Datenpakete vom Sender einen weiteren Weg zum Empfänger zurücklegen, als es eigentlich nötig wäre. Beispiele für Shared Trees sind: der Core Based Tree (CBT) und Protocol Independent Multicast – Sparse Mode (PIM-SM).

Beim Source Routed Tree wird für jeden Senderknoten ein Baum aufgespannt. Dies wird durch den Reverse Path Forwarding Algorithmus (RPF) ermöglicht. Empfängt also ein Router ein Multicast-Datenpaket, so merkt er sich den Sender sowie die Schnittstelle des Routers, an der das Datenpaket empfangen wurde. Liegt nun die Schnittstelle auf dem kürzesten Pfad zum Sender, so wird das Datenpaket an alle anderen Schnittstellen des Routers weitergeleitet, mit Ausnahme dieser Schnittstelle. Somit werden die Pakete jeweils über die kürzestmögliche Verbindung weitergeleitet und auf verschiedene Pfade des Netzes, was zu einer besseren Netzwerkauslastung führt. Leider werden damit Daten auch unnötig in Teile des Netzes geleitet, in denen keine Empfänger aktiv sind. Eine Beschränkung dieser Weiterleitung zwischen Routern kann durch ein Pruning-Verfahren erreicht werden. Ein Teil des Baumes kann temporär von ihm abgeschnitten werden, wenn sich unterhalb des entsprechenden Knotens keine weiteren Gruppenmitglieder befinden. Dazu sendet dieser eine Prune-Nachricht in Richtung Quelle (Baumwurzel). Um Veränderungen der Netztopologie zu gewährleisten, werden diese Nachrichten periodisch verworfen. Beispiele für Source Based Tree-Protokolle sind: Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF) und Protocol Independent Multicast – Dense Mode (PIM-DM).

## 2.3 Flooding

Ein Verfahren, welches von einigen Multicast Protokollen verwendet wird, ist das Flooding. Hierbei werden die Daten von einem Router nach dem Empfang an alle Schnittstellen verteilt, mit der Ausnahme der Schnittstellen über die diese Daten empfangen wurden. Für die Weiterleitung müssen keine Routingtabellen unterhalten werden und es ist somit einfach zu realisieren. Darüber hinaus wird gewährleistet, dass alle Gruppenmitglieder erreicht werden. Die Ineffizienz zeigt sich allerdings darin, dass es eine hohe Netzlast nach sich zieht, da viele Systeme Daten empfangen, die gar nicht an sie adressiert sind oder, dass verschiedene Daten Schleifen durchlaufen und somit ewig im Netz bleiben. Das Flooding kann allerdings noch optimiert werden. Zum einen besteht die Möglichkeit, den Datenpaketen eine begrenzte Lebenszeit einzuräumen. Eine weitere mögliche Optimierung ist, dass sich der Router merkt, welche Pakete er schon empfangen hat. Pakete, die der Router zum zweiten Mal empfängt, werden verworfen. Des weiteren stellt Reverse Path Broadcasting eine Optimierung des Flooding dar. Ein Datenpaket wird nur dann weitergeleitet, wenn es über die Netzschnittstelle empfangen wurde, über die Unicast Pakete zum Sender gesendet wurden (also die Schnittstelle), die dem kürzesten Pfad zum Sender entspricht. Ein alternatives Verfahren hierzu verwendet Spannbäume. Hierbei wird ein Overlay Netz [3] etabliert, das einige vorhandene Übertragungsabschnitte und Zwischenspeichersysteme aus dem Netz eliminiert, um die Schleifen zu vermeiden. Die so selektierten Übertragungsabschnitte und Brücken bilden einen Spannbaum, der alle Systeme im Netz erreicht, wobei nicht maßgebend ist, ob es sich hierbei um einen optimalen Spannbaum handelt, bedingt dadurch, dass beim Aufbau des Baumes keine Informationen über Gruppenzugehörigkeiten ausgewertet werden, ganz im Gegenteil zu einem Multicast Baum, in dem die Gruppenmitgliedschaft explizit berücksichtigt wird. Eine Möglichkeit hierfür bieten Bäume mit Rendezvous Punkten. Diese repräsentieren eine neue Entwicklung im Zusammenhang mit Multicast bzw. Multipeer Kommunikation. Es werden mehrere Sender und mehrere Empfänger berücksichtigt. Rendezvous Punkte kennen die Zusammensetzung der Gruppe. Diese erhalten die entsprechende Information. Bei der Weitergabe dieser Information werden alle Router, die zwischen dem neuen Mitglied und des Rendezvous Punktes liegen durchlaufen und diese können sich die Information der Gruppenzugehörigkeit des neuen Mitglieds extrahieren und speichern. Um dieses Verfahren zu etablieren muss zunächst ein solcher Rendezvous Punkt eingerichtet werden. Die Gruppenmitglieder melden sich dann an diesem an. Ein Vorteil hiervon ist die begrenzte Datenvergabe direkt an eine bestimmte Gruppe, auch in den Routern ist der Aufwand gering, da sie nur die Gruppe und nicht die Paare von Kommunikationspartnern identifizieren müssen. Die Nachteile liegen allerdings in der Verkehrskonzentrierung in den Rendezvous Punkten.

## 2.4 Dense Mode und Sparse Mode

Beim Multicast werden je nach der erwarteten Verteilung der Gruppenmitglieder im Netzwerk noch zwei Ansätze bei den Routingprotokollen unterschieden. Liegen die Gruppenmitglieder dicht beieinander, so verwendet man so genannte Dense Mode Protokolle. Dieses setzen in der Regel Flooding ein, um Routinginformationen zu den beteiligten Routern zu verteilen. Der andere Ansatz geht davon aus, dass Gruppenmitglieder im Netzwerk weit voneinander entfernt sind. Verfahren für diesen Ansatz werden als Sparse Mode Protokolle bezeichnet und verwenden den Shared Tree.

Das Distance Vector Multicast Protocol (DVMRP) [3],[4] basiert auf dem Distanz Vektor Algorithmus [3], der den kürzesten Weg zur Datenquelle ermittelt. Die Grundlage bildet das Reverse Path Flooding [3] Verfahren, bei dem der Router Datenpakete in periodischen Abständen über alle ihm bekannten Pfade versendet um die Nachbar Router kennen zu lernen.

Die Weiterleitung von Multicast Paketen erfolgt mit dem Reverse Path Forwarding Algorithmus, der auch Pruning Nachrichten benutzt. Knoten, die keine Router zu weiteren Multicast Gruppenmitglieder haben, senden eine Prune Nachricht an die Gruppe. Die Zwischenknoten, die eine solche Nachricht erhalten, markieren den Link zu diesem Knoten als abgeschnitten und senden keine Multicast Pakete mehr dorthin. Wenn der Pruning Prozess im ganzen Netz abgeschlossen ist, ist der optimale Source Based Tree aufgespannt. Das Flooding muss regelmäßig stattfinden, um abhängig vom Versenden von Prune Nachrichten Join bzw. Leave Operationen von neuen bzw. Endknoten zu ermöglichen. Bei Multicast Open Shortest Path First (MOSPF) [3] handelt es sich um ein so genanntes Link State Protokoll. Es setzt auf dem Unicast Routingprotokoll Open Shortest Path First (OSPF) [3] auf. Jeder Router sammelt Informationen über seine Verbindungen zum Netzwerk und über Gruppenmitglieder. Diese Information (Link State Pakete) werden durch Flooding an alle Router verteilt. Jeder Router kennt die ganze Netzwerktopologie und kann so für jeden Sender einer Gruppe den optimalen Verteilungsbaum berechnen. Das PIM (Protocol Independent Multicast) [3], wurde auf Multicast Kommunikationen in räumlich verstreuten Gruppen mit geringer Dichte entworfen. PIM arbeitet dabei mit einer Minimierung der Zustandshaltung in den Routern, Minimierung des Verarbeitungsaufwandes von Kontroll- und Nutzdaten in den Routern sowie einer Minimierung der beanspruchten Bandbreite im Netz. PIM gliedert Netze in sog. PIM Domänen und nicht-PIM-fähige Domänen. Alle Router in einer PIM Domäne implementieren PIM für das Multicast Routing. Sie arbeiten innerhalb eines gemeinsamen Bereiches, der durch Multicast Grenz-Router begrenzt wird, welche für die Anbindung an den Rest des Internets verantwortlich sind. Innerhalb einer PIM Domäne existieren weiterhin noch Bootstrap-Router, die Informationen über Rendezvous Punkte verteilen [3].

Beim Sparse Mode Verfahren wird zwischen dem Core Based Tree (CBT) [1],[3] und Protocol Independent Multicast – Sparse Mode (PIM-SM) [3] unterschieden. Beim Core Based Tree (CBT) Verfahren wird für jede Multicast Gruppe nur ein Routingbaum aufgebaut. Unabhängig vom Sender werden Multicast Daten immer über diesen Baum verteilt. Der Baum enthält einen oder mehrere bestimmte, so genannte Core Router. Multicast Pakete werden über einen CBT Baum verteilt. Die Pakete werden auf allen Netzschnittstellen des Spannbaums außer der, auf welcher das Paket eingetroffen ist, weitergeleitet. Ein neues Gruppenmitglied hängt sich an den Baum an, indem es eine join Nachricht per Unicast an einen Core Router schickt. Alle zwischen Sender der join Nachricht und Core Router liegenden Router ergänzen entsprechend ihre Routingtabellen. Bei CBT ist es auch möglich, dass Nichtmitglieder Multicast Nachrichten an die Gruppe schicken. Der Sender schickt das Multicast Paket per Unicast in die Richtung eines Core Routers. Trifft das Paket auf einen Router des Multicast Baums, so wird es über Multicast verteilt. Probleme beim CBT Ansatz sind die Konzentration von Daten in der Nähe der Core Router und die Tatsache, dass es natürlich durch die Verwendung eines einzigen Baums für alle Sender suboptimale Pfade und größere Verzögerungen gibt. Die zuletzt geschilderten Probleme versucht Protocol Independent Multicasting – Sparse Mode (PIM-SM) zu umgehen, indem es die Wahl zwischen einem gemeinsamen Baum pro Gruppe (wie bei CBT) und senderspezifischen Bäumen (wie bei den Dense Mode Verfahren) zulässt. Bei der Erzeugung einer Multicast Gruppe wird von PIM-SM zunächst immer ein gemeinsamer Baum wie bei CBT erzeugt. Core Router werden bei PIM-SM mit Rendezvous Punkte bezeichnet, haben aber im Grunde die gleiche Funktion. Die Besonderheit bei PIM-SM ist, dass ein Empfänger an einen Sender (nachdem er schon Daten über den gemeinsamen Baum empfängt) eine join Nachricht senden kann und so den Aufbau eines (optimalen) senderbasierten Baums veranlassen kann.

## 2.5 Adaptive Shared Tree Multicast in mobilen, leitungslosen Netzwerken

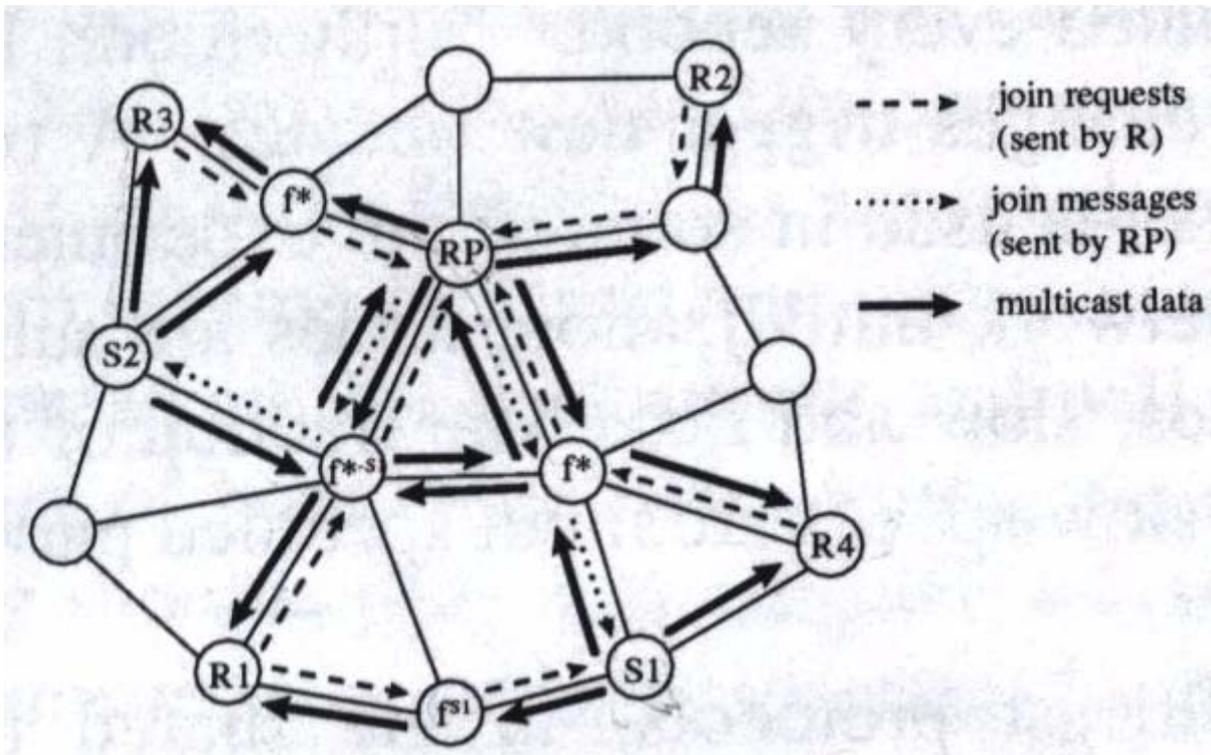


Abbildung 5: Adaptive Multicast

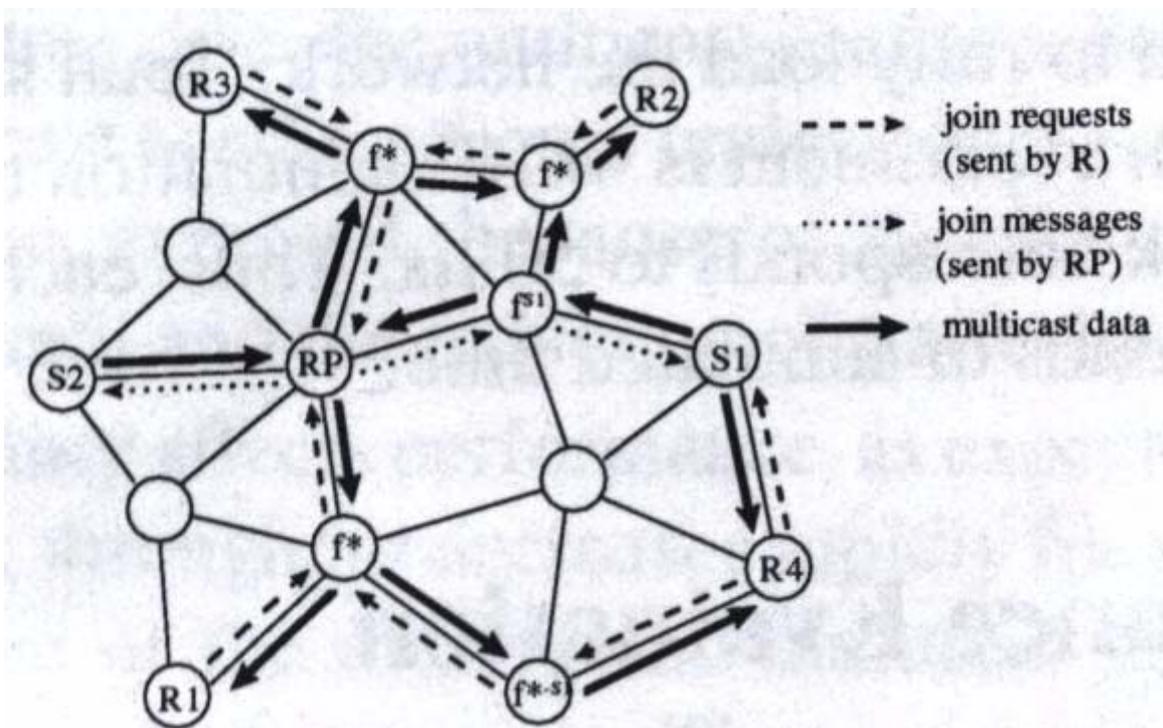


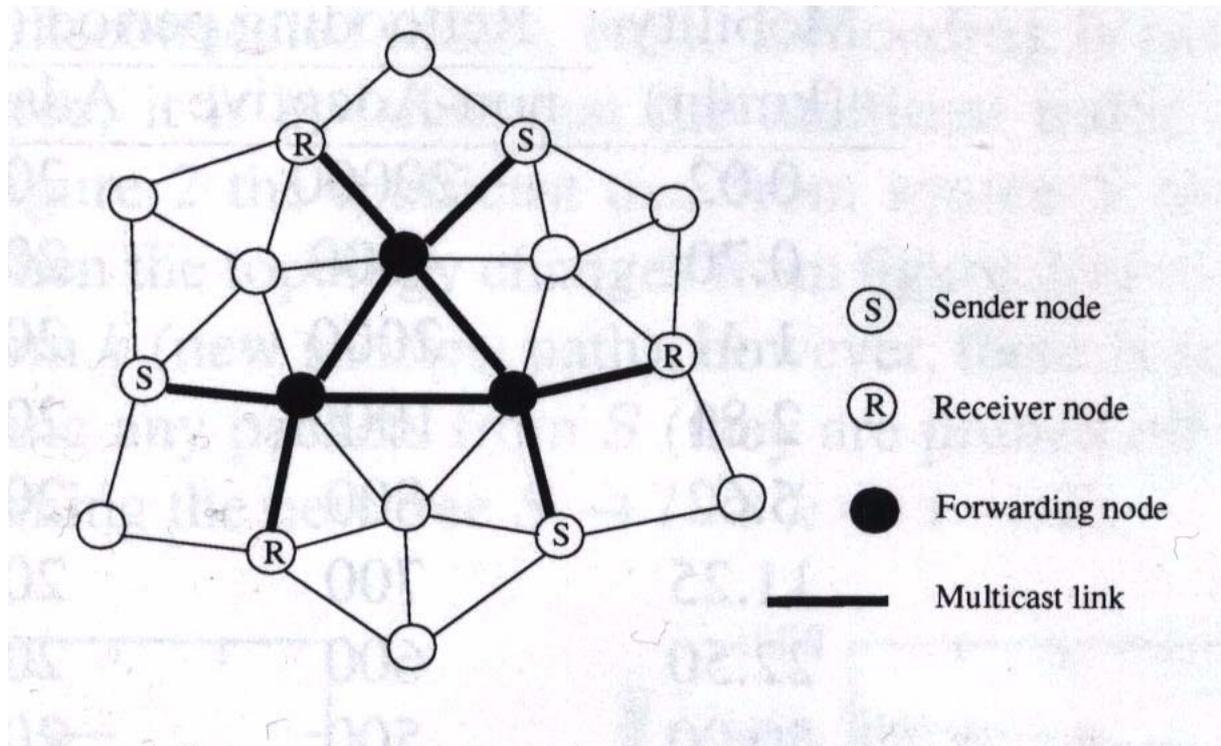
Abbildung 6: Adaptive Multicast (nach Verschiebung der Knoten)

Aufbauend auf den Prinzipien der Shared Tree und Source Based Tree Verfahren, kann der Empfänger entscheiden, welches Verfahren er nehmen will, um effizient zu arbeiten [4].

Hiefür ist es notwendig den Vorteil des einen gegenüber dem anderen Verfahren herauszustellen. Als erstes überprüft der Empfänger, ob die Distanz vom Sender zu ihm, die durch die Routingtabellen gegeben ist, länger ist, als die Distanz, die ihm der hop Zähler aufweist. Als nächstes wird geprüft, ob die Distanz von ihm zum Sender kürzer ist, als die Distanz von ihm zum Rendezvous Punkt. So kann der Empfänger einen ungefähren Vergleich anstellen bezüglich der Verbindungslänge. Ist also die Distanz zum Sender viel größer als die Distanz zum Rendezvous Punkt behält der Empfänger diesen Shared Tree mit dem Rendezvous Punkt bei. Ansonsten besteht die Möglichkeit auf das Source Based Tree Verfahren zu wechseln. Dies geschieht dann dadurch, dass der Empfänger join Nachrichten in der Forwarding Liste zum Sender schickt, um somit eine direkte Verbindung mit ihm zu unterhalten. Es werden also keine weiteren Datenpakete mehr über den Rendezvous Punkt verschickt. Sollte sich nun durch die dynamische Netzwerktopologie die Distanz wieder vergrößern und wieder das Shared Tree Verfahren von Vorteil sein, so beendet der Empfänger das Versenden von join Nachrichten zum Sender und fügt diesen wieder in die Forwarding Liste, beinhaltet in der join Nachricht zum Rendezvous Punkt, mit ein.

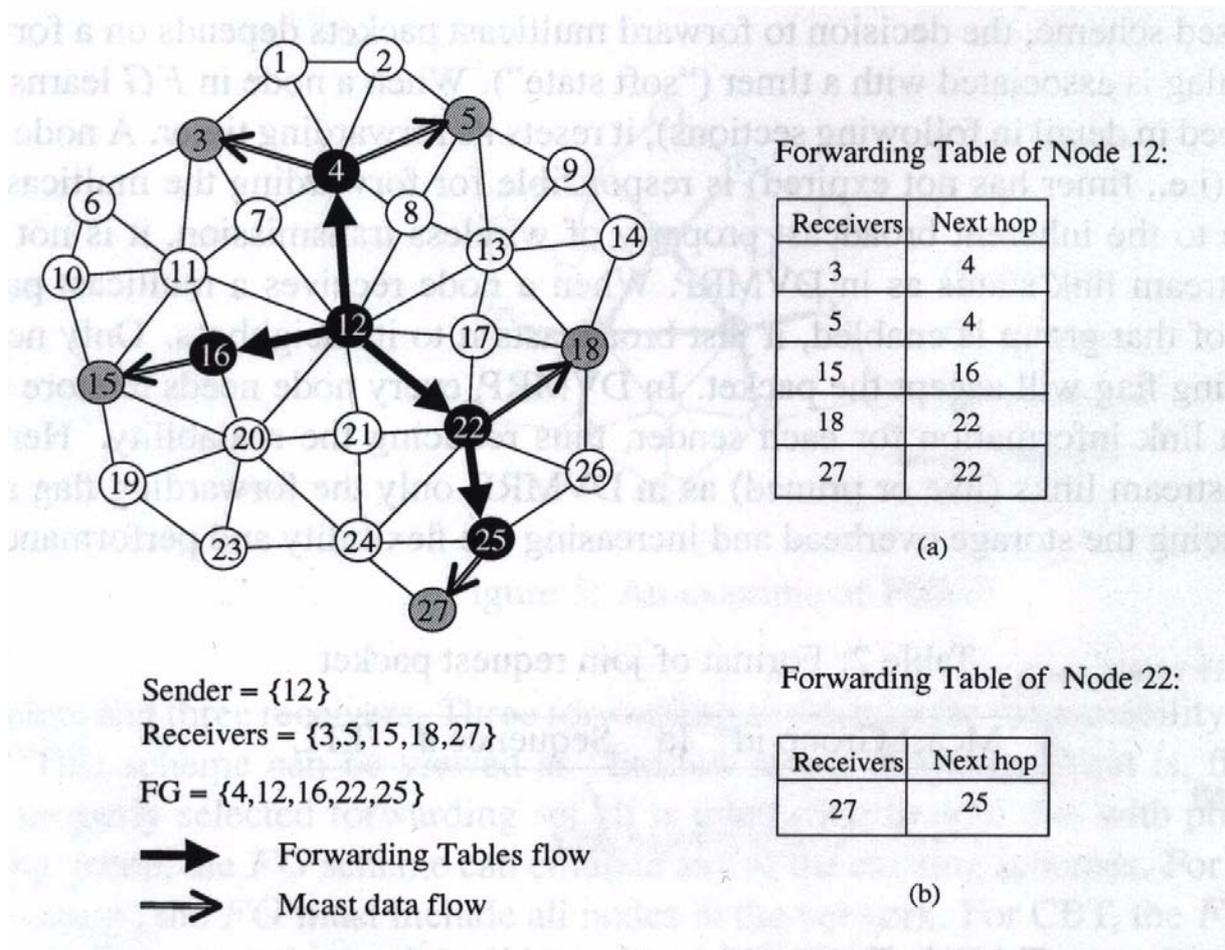
### **3.5 Das Forwarding Group Multicast Protocol (FGMP)**

Beim Multicast Routing in leitungsgebundenen Netzwerken, wird bei den angesprochenen Protokollen ein Spannbaum etabliert. Dabei wurde zwischen dem Shared Tree und dem Source Based Tree Verfahren unterschieden. Es ist jedoch in beiden Verfahren der Fall, dass dem Spannbaum eine Wurzel sowie zahlreiche Blätter zugeordnet werden müssen. Dabei entstehen sog. Up- und Downstream Verbindungen. Als schwierig stellt es sich nun heraus, diesen Baum auf ein mobiles leitungsloses Netzwerk abbilden zu wollen, da dieses einer sehr dynamischen Topologie unterliegt [4]. Aus diesem Grunde spielt das FGMP [4] eine große Rolle. Dieses beinhaltet Gruppen von Knoten, die an der Weiterleitung von Datenpaketen beteiligt sind. In jeder Multicast Gruppe  $G$  gibt es eine Weiterleitungsgruppe  $FG$ , wobei jeder Knoten in der Lage ist, Nachrichten von  $G$  weiterzuleiten, wenn es sich dabei nicht um ein Duplikat handelt. Im Beispiel übernehmen drei Knoten die Verantwortung Multicast Datenpakete weiterzuleiten. Ein großes Problem im FGMP, ist die Festlegung der Knoten, die an der  $FG$  beteiligt sind, wobei die Anzahl der Knoten gering gehalten werden soll, um eine hohe Effizienz zu gewährleisten, bezüglich kurzer Distanzen.



**Abbildung 7: Beispiel eines FGMP**

Das FGMP-RA (Receiver Advertising) beruht darauf, dass die Empfänger in periodischen Abständen join Nachrichten ins Netzwerk verschicken, um die Mitgliedschaft einer Gruppe zu bestätigen. Erhält ein Sender diese Nachricht, so aktualisiert er seine Liste, wobei die Empfänger, die keine join Nachricht gesendet haben, aus dieser entfernt werden. Der Sender verschickt nun nur Datenpakete, wenn mindestens ein Eintrag in seiner Liste vorliegt. Hierzu erstellt er eine Forwarding Liste, die die next hop Information, die ihm durch die Routingtabellen gegeben ist, enthält. Diese Liste wird nun an alle Nachbarn weitergeleitet, wobei nur die Nachbarn, die in der next hop Liste verzeichnet sind, diese Forwarding Liste weiter verarbeiten können. Diese erzeugen nun selbst eine Forwarding Liste, die wiederum die next hop Information enthält, welche nun weiterverschickt wird. Dieses Verfahren wird schließlich so oft wiederholt, bis alle Empfänger erreicht werden. Im Beispiel bildet der Knoten 12 den Sender. Fünf Knoten bilden insgesamt die  $FG = \{4, 12, 16, 22, 25\}$ , weil diese in der next hop Liste vorhanden sind. Es ist nur notwendig dass innere Knoten, wie 12 und 22 eine Forwarding Liste bilden, da bei den Blättern 4, 16, 25 automatisch bereits die Nachbarn die Empfänger darstellen.



**Abbildung 8: Beispiel für Forwarding Listen**

Im Gegensatz dazu beruht das FGMP-SA (Sender Advertising) darauf, dass die Sender ein Flooding durchführen, was allerdings nur von Bedeutung ist, wenn es weniger Sender als Empfänger gibt. Die Empfänger sammeln diese Informationen der Sender und verschicken periodisch joining Listen zum Sender, um eine FG zu etablieren, wobei die joining Listen das selbe Format wie die Forwarding Listen besitzen.

## 4. References

- [1] Chai-Keong Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems“, Prentice Hall PTR, 2002
- [2] Charles Perkins, “Ad Hoc Networking”, Addison Wesley Publishing Company, 2002
- [3] Ralph Wittmann, Martina Zitterbart, “Multicast: Protokolle und Anwendungen”, dpunkt Verlag 1999
- [4] Ching-Chuan Chiang, Mario Gerla and Lixia Zhang, Paper: “Forwarding Group Multicast Protocol (FGMP) for Multihop, Mobile Wireless Networks”, Computer Science Department, University of California, Los Angeles
- [5] Ching-Chuan Chiang, Mario Gerla and Lixia Zhang, Paper: “Adaptive shared tree multicast in mobile wireless networks”, Computer Science Department, University of California, Los Angeles