

Selbstorganisierende Netze

Rene Schneider
Hochschule der Medien
Nobelstr. 10, 70569 Stuttgart
e-mail: rs034@hdm-stuttgart.de

Abstract

Technological advancement has provided us with microcontrollers and radio transceivers which get smaller and more powerful each year. These hardware components have paved the way for a new wireless network technology which differs considerably from the well-known model of a stationary transmitter with many mobile receivers. The new „Mesh Networks“ create their own, dynamic networking infrastructure without the need for stationary equipment. This technology opens up completely new fields of application and new savings potential in already-known scenarios. This survey paper is intended to provide you with an overview over the area of self-organizing networks, with a focus on the technological aspects.

Die fortschreitende technische Entwicklung hat durch immer kleinere und leistungsfähige Mikrocontrollerschaltkreise sowie Funksender und -empfänger den Weg für Funknetztechnologien geebnet, die sich vom althergebrachten Modell des stationären Sendemasts und der mobilen Endgeräte radikal unterscheiden. Diese neuen „Mesh-Netzwerke“ bilden ihre eigene, dynamische Netzinfrastruktur, ohne dass dazu stationäre Anlagen erforderlich wären, wodurch sich ganz neue Einsatzgebiete sowie Einsparpotentiale ergeben. Dieses Paper gibt einen Überblick über den derzeitigen technischen Stand im Bereich der selbstorganisierenden Mesh-Netze.

1 Einleitung

Seit der Erfindung des Rundfunks dominierte eine zweigeteilte Netztopologie die Funknetze, welche durch große, stationäre und starke Sendeanlagen sowie kleine und mobile Empfänger geprägt war. Auch die heute modernen Mobilfunknetze nach dem UMTS-Standard basieren im Kern immer noch auf diesem erprobten Konzept, wenngleich sie auf beiden Seiten eine Sende- und Empfangsfunktion realisieren sowie eine stationäre Netzinfrastruktur von erheblich höherer Komplexität erfordern.

Allerdings hat dieses Konzept neben klaren Vorteilen wie der Möglichkeit, schnelle stationäre Leitungstechnik zu nutzen, der garantierten Netzabdeckung und der praktisch erprobten Stabilität auch Nachteile: Aufbau und Wartung der stationären Netzinfrastruktur ist kostenintensiv - insbesondere dann, wenn ein ganzes Funknetz oder auch nur ein Netzbereich nur für begrenzte Zeit (etwa während einer Veranstaltung) benötigt wird. Darüberhinaus erlaubt es die Umgebung nicht immer, ein stabiles stationäres Netzwerk zu errichten, beispielsweise wenn die Stromversorgung der Sender/Empfänger problematisch ist.

Die neue Technologie der selbstorganisierenden Funknetze ist geradezu prädestiniert für Situationen, in denen diese Nachteile den Einsatz der klassischen stationären Funknetztechnik erschweren oder sogar unmöglich machen. Funknetze, die weitestgehend bis vollständig ohne stationäre Komponenten arbeiten, erfordern weder den Aufbau teurer Infrastruktur noch deren Unterhalt oder einen Abbau nach der Nutzung. Trotzdem bieten sie - unter gewissen Voraussetzungen - eine ähnlich großflächige Abdeckung wie die bewährten stationären Netze.

Selbstorganisierende Funknetze - oft auch als „Mesh-Netzwerke“ oder „mobile Ad-hoc-Netzwerke“ (kurz: MANETs) bezeichnet - können in vielen potenziellen Anwendungsbereichen eingesetzt werden. Dazu zählt beispielsweise die Car-to-Car-Communication: Ein Sende/Empfangsmodul in jedem Auto kommuniziert mit den Modulen der Autos in nächster Nähe und gibt Statusinformationen über die nähere Umgebung weiter. Heranfahrende Wagen könnten auf diese Weise etwa präzise und zeitnah vor einem Stau in einigen Kilometern Entfernung gewarnt werden, so dass die Fahrer rechtzeitig auf Alternativrouten ausweichen können. Ein weiterer interessanter Anwendungsbereich ist die kurzfristige und günstige Vernetzung von Standorten ohne feste Netzwerkinfrastruktur, beispielsweise Veranstaltungsorte für Messen oder Kongresse. Nicht zuletzt spielen Mesh-Netzwerke bei der Vernetzung von Entwicklungs- und Schwellenländern bereits heute eine Rolle: der bekannte OLPC-Laptop¹ nutzt ein Mesh-WLAN,

¹OLPC = One Laptop Per Child - Eine Initiative gestartet durch den MIT-Professor Nicholas Negroponte, die es sich zum Ziel gesetzt hat, einen günstigen, nur 100 Dollar teuren Spezial-Laptop für die Ausbildung

um den Datenaustausch zwischen zwei entfernten Laptops über mehrere Zwischenstationen hinweg zu erlauben.

In diesem Survey Paper wird ein Überblick über den momentanen technischen Stand im Bereich der selbstorganisierenden Funknetze gegeben. Es wird dabei auf zwei Kernpunkte eingegangen: das Routing in Mesh-Netzen (Anforderungen an Routing-Protokolle, Adressierung der Knoten, Betrachtung unterschiedlicher Routing-Ansätze sowie deren Vor- und Nachteile) und die Frage, wie in einem Netzwerk, dessen Teilnehmer fremde Daten weiterleiten, die Datenintegrität und Vertraulichkeit zu jeder Zeit gewährleistet werden kann. Dabei wird in erster Linie auf technische Aspekte eingegangen, während Anwendungsszenarien nur am Rande betrachtet werden.

2 Routing-Protokolle für mobile Ad-hoc-Netze

Eines der Kernprobleme in der Konzeption von Netzwerken ohne stets vorhandene, als stabil und verlässlich geltende stationäre Infrastruktur, ist das Routing bzw. die Frage, wie ein Datenpaket auf möglichst effiziente Weise seinen Weg vom Sender zum Empfänger findet. Die Routing-Problematik stellt sich natürlich auch bei kabelgebundenen Netzwerken, jedoch ergeben sich für selbstorganisierende mobile Netzwerke einige weitergehenden Anforderungen, die von den für kabelgebundene Netzwerke entworfenen Routing-Protokollen in der Regel nicht erfüllt werden können.

2.1 Anforderungen an das Routing

Effiziente Bandbreitennutzung: Da in Funknetzwerken meist weit geringere Bandbreiten als in kabelgebundenen Netzen zur Verfügung stehen, die darüberhinaus zwischen allen Teilnehmern einer Funkzelle geteilt werden müssen, ist eine effiziente Nutzung der verfügbaren Bandbreite erforderlich. Für Netze ohne „Basisstationen“, die Pakete oft über mehrere Funk-Zwischenstationen zu ihrem Ziel weiterleiten müssen, gilt dies in besonderem Maß, denn jedes Paket belegt das gemeinsame Medium während der Weiterleitung mehrfach.

Stabilität bei Topologieänderungen: In einem selbstorganisierenden Funknetz sind die Teilnehmer potenziell stets in Bewegung und verändern ihre Position. Darüberhinaus verlassen Teilnehmer den Abdeckungsbereich des Netzes, während andere hin-

zukommen. Dies führt zu einer sich laufend ändernden Netzwerktopologie.

Berücksichtigung von Umgebungseinflüssen:

Funknetze sind stets anfällig gegen Umwelteinflüsse, z.B. störende Einstrahlungen in den genutzten Frequenzbereich, Interferenzen, starken Dämpfungen et cetera. Darüber hinaus gibt es direkt auf die Netzknoten einwirkende Einflüsse wie z.B. die verfügbare Akkuleistung bei mobilen Knoten. Ein Routing-Protokoll sollte diese Einflüsse erkennen und bei der Erfüllung seiner Aufgabe miteinbeziehen können.

2.2 Adressierung der Knoten

Bevor überhaupt ein Routing von Paketen möglich ist, müssen die einzelnen Netzknoten eindeutig identifizierbar sein. Zu diesem Zweck teilt man - wie in kabelgebundenen Netzwerken auch - den teilnehmenden Geräten eindeutige Adressen zu. Diese Adressen können dabei auf unterschiedlichen Stufen „eindeutig“ sein [1]: **Global eindeutige Adressen** sind weltweit nur einem einzigen Knoten zugeordnet, während **netzwerkweit eindeutige Adressen** in einem Netzwerk eindeutig sind, aber durchaus in mehreren unabhängigen Netzwerken gleichzeitig existieren dürfen. **Lokal eindeutige Adressen** schließlich sind innerhalb einer „Nachbarschaft“ eindeutig. Diese Nachbarschaft ist eine auf irgendeine Weise definierte Untermenge eines Netzwerks und muss für die Verwendung lokal eindeutiger Adressen zuvor festgelegt werden.

Eine wichtige Größe bei der Wahl eines Adressierungsschemas ist die Anzahl Bits, die für die Repräsentation einer Adresse nötig sind - oder anders ausgedrückt: die Größe des Adressraumes. Da die Adresse Teil des Headers jedes Pakets im Netzwerk sein muss, um die Ankunft am richtigen Knoten zu gewährleisten, vergrößern große Adressräume automatisch den Protokoll-Overhead und damit die zu übertragende Gesamtdatenmenge. Zur möglichst effizienten Bandbreitennutzung sollte der Adressraum folglich möglichst klein sein.

Gegen einen sehr kleinen Adressraum sprechen allerdings gleich mehrere Gründe. Zum Einen möchte man in der Regel möglichst viele Teilnehmer innerhalb eines Netzwerks zulassen - die Masse der Knoten ist es ja, die einem ein größeres Gebiet abdeckenden selbstorganisierenden Netz zu seiner Stabilität verhilft. Da jeder Knoten eindeutig identifizierbar sein muss, muss der Adressraum folglich mindestens so viele Adressen wie die gewünschte Maximalknotenzahl aufnehmen können.

Die zweite Schwierigkeit ist gekoppelt mit der Problematik der Adressvergabe. Adressen können auf unterschiedliche Arten vergeben werden: bereits bei der Produktion der Geräte (vgl. Ethernet-MAC), von einer befug-

und Wissensvermittlung in Entwicklungs- und Schwellenländern in Serie zu produzieren. <http://laptop.org>

ten Instanz innerhalb eines Netzwerks (vgl. IP-Adressen per DHCP-Server) oder mittels eines Adressvergabe-Algorithmus unter den Netzwerkteilnehmern selbst. Die Version mit einer „befugten Instanz“, der die Adressvergabe obliegt, widerspricht dem Bestreben, ein selbstorganisierendes Netzwerk zu schaffen, weshalb diese für komplett selbstorganisierende MANETs ungeeignet ist (als Kompromiss wäre es allerdings durchaus denkbar, einen normalen Netzwerknoten temporär zur Adressvergabe-Instanz zu ernennen).

Im ersten Fall, d.h. bei während der Produktion vergebenen Adressen, kommen lediglich global eindeutige Adressen in Frage: es ist nicht vorhersehbar, in welchen Netzwerken ein gerade produzierter Knoten eingesetzt wird, daher muss die Adresse weltweit eindeutig sein, um Kollisionen zu vermeiden. Dementsprechend ist bei dieser Variante ein großer Adressbereich erforderlich, um genügend eindeutige Adressen für sämtliche Netzwerkteilnehmer auf der Welt bereitzuhalten.

Im Fall der Adressvergabe durch die Teilnehmer selbst kann je nach verwendetem Algorithmus ein kleinerer oder größerer Adressbereich erforderlich sein. Wird eine Adresse beispielsweise durch Koordination mit den anderen Knoten eines Netzwerks bei der Kontaktaufnahme mit dem Netz gewählt, kann der Adressraum klein sein, denn er muss lediglich die Geräte eines Netzwerks aufnehmen. Wird eine Adresse aber ohne Koordination zufällig von jedem Knoten selbst gewählt, muss der Adressraum erheblich größer sein - nicht etwa, weil tatsächlich so viele Adressen benötigt würden, sondern, weil die Kollisionswahrscheinlichkeit durch einen enorm großen Adressraum bis in die praktische Unmöglichkeit verkleinert werden muss.

2.3 Bekannte Routing-Verfahren

Für das Routing von Paketen in MANETs sind bereits viele Verfahren erdacht worden. Leider existieren zahlreiche dieser Verfahren lediglich auf dem Papier, da es bislang nur sehr wenige Mesh-Funknetze gibt, die praktisch im Einsatz sind. Nichtsdestotrotz zeigt die Vielzahl an möglichen und zumindest theoretisch funktionsfähigen Verfahren, dass eine praktische Umsetzung der Grundidee eines selbstorganisierenden Funknetzes möglich ist, und dass dabei das Routing-Protokoll auf vielfältige Weise an die konkreten Bedürfnisse einer Applikation angepasst werden kann.

Im Folgenden wird eine grobe Klassifizierung von bekannten Routing-Verfahren vorgenommen. Zunächst teilen sich diese auf in zwei Gruppen:

Reaktive Verfahren: Diese Sorte von Routing-Verfahren ermittelt die nötigen Topologieinformationen für das Routing erst dann, wenn ein Paket mit einem konkreten Sender/Empfänger-Paar vorliegt, für welches eine Route benötigt wird.

Proaktive Verfahren: Diese Verfahren ermitteln bereits vor dem Versand echter Datenpakete die nötigen Informationen für das Routing (in der Regel einen Graph des kompletten Netzes).

Bei dieser Einordnung ist zu beachten, dass es auch Mischformen dieser grundlegend verschiedenen Gruppen gibt, etwa Protokolle, die nur im „Nahbereich“ proaktiv arbeiten, während sie für Verbindungen über sehr viele Hops eine reaktive Bestimmung möglicher Pfade umsetzen. Im Folgenden sollen jedoch exemplarisch zwei Protokolle vorgestellt werden, die sich auf je eines der Grundprinzipien beschränken - auf diese Weise wird das jeweilige Grundprinzip möglichst gut verständlich.

2.3.1 Reaktive Routing-Verfahren

Reaktive Verfahren stellen die einfachste Form der rein topologiebasierten Routingverfahren dar: sie ermitteln bei Bedarf einen Pfad zwischen einem Sender und einem Empfänger und nutzen diesen anschließend zur Datenübertragung. Die Bestimmung des Pfades ist mit der Ermittlung der Netz-Topologie gleichzusetzen, wenngleich im Falle nur eines Pfades lediglich ein Bruchteil der Netztopologie - nämlich der Teil, der für das Zustandekommen des gewünschten Pfades benötigt wird - tatsächlich ermittelt und verarbeitet wird.

Ein Routing-Verfahren, welches nach diesem einfachen Konzept funktioniert, ist das DSR²-Protokoll [2]. Entwickelt 1994 von David B. Johnson, stellt es die Grundlage für viele später entworfene Protokolle dar, die das grundlegende Prinzip übernehmen und auf unterschiedliche Weise optimierten. Das Protokoll wurde bereits mehrfach real implementiert und gilt daher als eines der ausgereifteren MANET-Routing-Protokolle. Es ist außer in Papers und Artikeln auch in Form eines RFC (wenngleich mit dem Status „Experimental“) spezifiziert [3].

2.3.2 Reaktives Routing: Das DSR-Grundprinzip

DSR routet Pakete, indem bei deren Erzeugung im Header eine komplette Route vom Sender bis zum Empfänger platziert und das Paket anschließend von allen Knoten an den jeweils nächsten Knotenpunkt weitergereicht wird. Die Route erhält der Sender idealerweise aus einem Cache, in welchem er bereits bekannte Routen speichert. Liegt dort noch keine Route vor, startet die sogenannte „Route Discovery“ ([2], Kapitel 3.2).

Ein einfaches Beispiel mit 4 Teilnehmern A, B, C und D: A möchte ein Paket an D versenden und sucht eine Route. Dazu sendet A ein Broadcast-Paket mit einem *Route Request* an alle Knoten in Reichweite, in welchem zunächst

²Dynamic Source Routing

nur Start und Ziel der gewünschten Route sowie eine von A gewählte Request-ID stehen. B empfängt diesen Request, fügt seine eigene Adresse dem Request hinzu und sendet ihn erneut als Broadcast an alle Knoten in seiner Reichweite. C empfängt den Request, setzt ebenfalls seine Adresse hinter die Adresse von B und leitet den Request per Broadcast weiter, woraufhin ihn D empfängt. D stellt fest, dass er das Ziel der Route darstellt, erstellt aus der Liste aller Knoten eine *Route Reply* und adressiert diese an A.

Zur Übermittlung der *Route Reply* an A kann D nun entweder eine eigene Route aus seinem Cache verwenden oder - falls eine solche nicht vorhanden ist - ebenfalls eine Route Discovery starten. Um dabei Endlosschleifen zu vermeiden, wird dem neuen *Route Request* von D zu A die *Route Reply* mit der Route von A zu D beigelegt, so dass nach Beendigung der zweiten Route Discovery beide Knoten bidirektional kommunizieren können. In Netzwerken, die bereits im MAC-Protokoll eine bidirektionale Kommunikation aller Teilnehmer voraussetzen, kann zur Optimierung auch die erste ermittelte Route umgedreht werden, wodurch die zweite Route Discovery vermieden werden kann.

Während der regulären Datenübertragung ist jeder Knoten für die korrekte Weiterleitung eines Pakets an den Folgeknoten verantwortlich. Die dazu nötigen Empfangsbestätigungen können entweder implizit durch das zugrundeliegende MAC-Protokoll generiert oder explizit über das DSR-Protokoll angefordert werden. Kann ein Paket auch nach mehreren Versuchen nicht weitergeleitet werden, sendet ein Knoten einen *Route Error* zum Absender des Pakets. Dieser entfernt die nicht mehr nutzbare Route aus seinem Cache und startet - sofern keine weitere Route zum Ziel im Cache vorhanden ist - eine neue Route Discovery.

Das DSR-Protokoll enthält eine Reihe von Optimierungen für diese Basisfunktionalität, auf die jedoch hier aus Platzgründen nicht näher eingegangen werden kann. Siehe dazu [2], Kapitel 3.4.

2.3.3 Proaktives Routing: Das OLSR-Protokoll

Das OLSR³-Protokoll [4] ist ein Beispiel für ein proaktives MANET-Routing-Protokoll. „Proaktiv“ bedeutet, dass das Protokoll die Netzwerktopologie und damit die möglichen Routen zwischen den Knoten nicht erst bei Bedarf, sondern bereits im Voraus ermittelt. Dieses Protokoll ist ähnlich ausgereift wie DSR und wurde bereits mehrfach implementiert sowie praktisch eingesetzt, z.B. im Freifunk-Projekt⁴. Auch OLSR ist in Form eines „Experimental“-RFC spezifiziert [5].

OLSR basiert auf dem Link-State-Algorithmus, einem Prinzip zum Aufbau von Topologieinformationen. In seiner einfachsten Form arbeitet dieser Algorithmus folgen-

dermaßen: Zunächst stellt jeder Node fest, mit welchen Nodes er direkt verbunden ist. Dies erfolgt über den Austausch von sogenannten *Hello*-Nachrichten mit den direkten Nachbarn. Kennt ein Node seine Nachbarn, wird eine Nachricht mit allen bekannten Nachbarn und der eigenen Adresse als Broadcast an sämtliche erreichbaren Nodes gesendet (die sogenannte *Topology-Control*-Nachricht), welche diese wiederum weiterleiten, so dass letztendlich jeder Node im Netzwerk die Nachbarn jedes anderen Nodes kennt. Aus diesen Informationen lässt sich ein vollständiger Graph der gesamten Netzwerktopologie ableiten, der anschließend zur Auffindung der optimalen Route für jede beliebige Sender/Empfänger-Kombination genutzt werden kann.

Der größte Nachteil des Link-State-Mechanismus in seiner einfachsten Form ist, dass er mit zunehmender Anzahl Knoten schlecht skaliert, insbesondere dann, wenn die Knoten auf engem Raum liegen und sich somit viele Knoten gegenseitig erreichen können. Speziell in diesem Fall machen sich die OLSR-Optimierungen besonders deutlich bemerkbar. Diese umfassen eine zusätzliche Hierarchieebene, die Multipoint Relays (MPR). Ein MPR ist ein normaler Knoten, der zu dieser Funktion von seinen unmittelbaren Nachbarknoten gewählt wurde (Abb. 1). Bei dieser Wahl der MPRs, die jeder Knoten für sich durchführt, gibt es ein Kriterium, welches die gewählten MPRs erfüllen müssen: Über seine gewählten MPRs muss ein Knoten jeden anderen Knoten in einem Umkreis von maximal 2 Hops direkt erreichen können. Diese Bestimmung ist algorithmisch möglich; ein heuristischer Algorithmus zur Bestimmung des MPR-Sets kann in [5], Kapitel 8.3.1 nachgelesen werden.

Die MPRs dienen zur Verteilung der *Topology-Control*-Nachrichten, indem sie diese Nachrichten von allen Selectors (= Knoten, die den jeweiligen MPR gewählt haben) einsammeln, untereinander verteilen und schließlich an ihre Selectors weitergeben. Die MPRs dienen folglich der Reduktion von Broadcast-Nachrichten im Netz, was umso besser funktioniert, je kleiner das Verhältnis von MPRs zur Gesamtanzahl Knoten ist.

2.3.4 Weitere Optimierungsmöglichkeiten

Die große Zahl an Protokollvorschlägen für MANETs enthält viele weitere Ideen, um die grundlegenden Funktionsprinzipien eines reaktiven oder proaktiven Verfahren zu erweitern und in Bezug auf verschiedenste Kriterien zu verbessern.

Ein möglicher Ansatz ist - wie bereits in 2.3 auf Seite 3 erwähnt - eine Kombination beider Prinzipien in einem hybriden Protokoll. Ein beispielhaftes hybrides Routing-Protokoll ist das ZRP⁵, welches in einem durch eine gewisse Zahl Hops beschränkten Bereich um einen Knoten

³Optimized Link State Routing

⁴<http://www.freifunk.net>

⁵Zone Routing Protocol

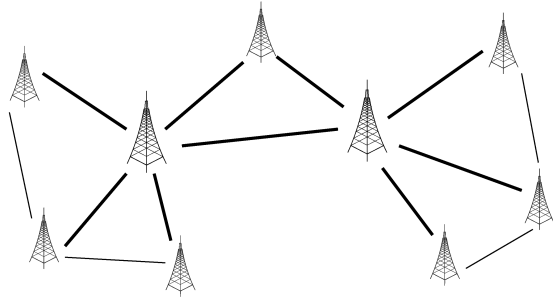


Abbildung 1: OLSR: Die beiden hervorgehobenen, zentralen Knoten würden hier die MPR-Funktion übernehmen

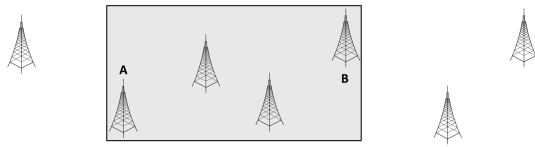


Abbildung 2: Ein LAR-Beispiel mit zwei kommunizierenden Knoten A und B

proaktiv arbeitet, darüber hinaus aber Routen erst bei Bedarf, also reaktiv, ermittelt. Das Protokoll basiert daher auf beiden vorgestellten Grundverfahren; eine genaue Beschreibung überschreitet aber den Umfang dieses Papers und kann bei Interesse in [6] nachgelesen werden.

Auch denkbar ist das Einbeziehen von geodätischen Positionsinformationen - also Daten über die physikalische Position eines Knoten - in das Routing. Die Idee dahinter ist, dass auf diese Weise die Broadcast-Nachrichten zur Routenbestimmung auf einen örtlich begrenzten Bereich beschränkt werden können (Abbildung. 2), was die Gesamtbelastung durch Protokoll-Overhead im Netzwerk drastisch senkt, insbesondere im Falle größerer Netzwerke. Ein Protokoll, welches auf diese Weise arbeitet, ist LAR⁶, beschrieben in [7].

Eine weitere interessante Optimierung geht davon aus, dass die meisten Teilnehmer eines MANETs nur eine begrenzte Menge elektrischer Energie zur Verfügung haben (etwa bei akkubetriebenen Funkknoten). Starker Funkverkehr benötigt mehr Energie, daher besteht die Gefahr, dass die Energiereserven von Knoten auf Pfaden, über die sehr viele Daten geroutet werden, schnell aufgebraucht sind, was im schlimmsten Fall zu einer Partitionierung des Netzes führen kann. Die Grundidee eines „Energy-Aware-Protokolls“ wie z.B. EADSR⁷ (siehe [8]) ist es, eine „Energie-Metrik“ zur Auswahl der für eine Übertragung genutzten Route einzusetzen. Diese Metrik basiert auf den

Energiereserven der einzelnen Knoten und führt dazu, dass auch topologietechnisch suboptimale Routen gewählt werden, wenn diese Routen über Knoten mit hohen Energiereserven führen.

2.4 Vergleich der Protokollarten

Die vorgestellten Protokoll-Ansätze haben unterschiedliche Vor- und Nachteile, was sie für jeweils andere Einsatzzwecke prädestiniert. Generell existiert derzeit kein „perfektes“ MANET-Protokoll, weshalb das genutzte Protokoll für eine praktische Anwendung unter Berücksichtigung der konkreten Anforderungen gewählt werden sollte.

Reaktive Protokolle: Zu den Vorteilen der reaktiven Protokolle zählt in erster Linie der vergleichsweise geringe Protokoll-Overhead bei häufigen Topologieänderungen. Routen werden erst bestimmt, wenn sie tatsächlich gebraucht werden, was den Overhead auch dann in Grenzen hält, wenn häufig Teilnehmer das Netz verlassen oder betreten. Der Hauptnachteil ist die hohe Latenzzeit, die vergeht, bis eine neue Route durch das Netzwerk gefunden worden ist. Ein weiterer Nachteil kann sich in Situationen ergeben, in denen die Kommunikationspartner sehr häufig wechseln: in diesem Fall wären sehr viele Route-Requests erforderlich, was den Vorteil der bedarfsgesteuerten Routenermittlung in einen Nachteil verwandeln kann, der für viel Overhead im Netzwerk sorgt. Ein nicht ganz offensichtlicher Vorteil dieser Protokollgruppe ist ihre Einfachheit: ein reaktives Protokoll ist vergleichsweise simpel aufgebaut, auch erste Optimierungsmaßnahmen wie das „Mithören“ der Route-Requests anderer Stationen sind einfach zu implementieren.

Proaktive Protokolle: Die proaktiven Protokolle können ihre Stärken dort ausspielen, wo die reaktiven Protokolle versagen. Sie zeichnen sich durch sehr schnelle Ermittlung eines neuen Routing-Pfads sowie eine Resistenz gegenüber häufig wechselnden Kommunikationspartnern aus. Ihr gewichtigster Nachteil ist ein schlechtes Skalierungsverhalten, welches auch durch Optimierungsmaßnahmen nicht vollständig wettgemacht werden kann, und die langsame Reaktion auf Topologieänderungen. Um letzteren Nachteil zu beheben, ist eine sehr häufige Neuermittlung der Netzwerktopologie erforderlich, was aber wiederum den Overhead stark ansteigen lässt. Außerdem ist diese Art von Protokoll in der Regel komplexer als ein reaktives Protokoll; auch Optimierungsmaßnahmen wie die MPRs im OLSR-Protokoll sind vergleichsweise komplex umzusetzen.

Hybride Protokolle: Die hybriden Protokolle versuchen, die Vorteile der proaktiven und reaktiven Protokoll-

⁶Location Aided Routing

⁷Energy-Aware Dynamic Source Routing

le zu kombinieren. Dies gelingt zumindest teilweise; im Nahbereich stellen hybride Protokollansätze beispielsweise erheblich schneller neue Verbindungen her wie reaktive Protokolle, ohne dabei das tendenziell schlechtere Skalierungsverhalten der proaktiven Protokolle im vollständigen Umfang zu erben. Allerdings vereinen hybride Ansätze in gewisser Weise auch die Nachteile beider Verfahren: Verbindungen über viele Hops hinweg erfordern beispielsweise nach wie vor eine reaktive Ermittlung des Routing-Pfads. Trotzdem können sich hybride Verfahren in vielen Situationen als guter Kompromiss erweisen. Ein den hybriden Protokollen inhärenter Nachteil ist ihre extrem hohe Komplexität; da diese Protokolle eigentlich aus zwei Unterprotokollen zusammengesetzt sind (ein reaktives und ein proaktives) kombinieren sie auch deren Komplexität, während die nötige zusätzliche Logik zur Vereinigung der beiden Protokolltypen den Komplexitätsgrad weiter erhöht.

Spezielle Optimierungen wie das erwähnte Location Aided Routing oder die Energy Awareness können in manchen Einzelfällen sehr praktikabel sein, eignen sich aber selten für eine generelle Anwendung, da sie von gewissen Annahmen ausgehen, die nicht auf jeden Anwendungsfall zutreffen (dass etwa ein GPS-Modul vorhanden ist, um die Position eines Knotens zu bestimmen). Daher sind sie hier nicht im Einzelnen berücksichtigt.

3 Sicherheitsaspekte

Für eine sinnvolle Nutzung von MANETs werden besondere Anforderungen an die Sicherheit gestellt. Dies resultiert aus der Tatsache, dass sämtliche übertragenen Daten zum Einen die für jedermann frei einsehbare Luftschnittstelle passieren, zum Anderen über mehrere, potenziell bösartige Relais-Knoten weitergeleitet werden. Ohne Sicherheits-Features sind MANETs daher für die meisten Anwendungen untauglich. Die Routing-Protokolle klammern Sicherheitserwägungen aber in aller Regel aus und bieten von sich aus keinerlei Schutz. Sicherheit muss daher entweder durch eine Protokollmodifikation auf Ebene des Routings oder auf einer höheren Ebene durch zusätzliche Protokolle hergestellt werden.

Im Einzelnen können folgende Bereiche bzw. Sicherheitsaspekte unterschieden werden:

- Datenintegrität
- Vertraulichkeit
- Privatsphäre

Auf jeden einzelnen soll im Folgenden detaillierter eingegangen werden.

3.1 Datenintegrität

Unter „Datenintegrität“ wird die Garantie verstanden, dass versendete Daten in unveränderter Form beim Empfänger ankommen (bzw. dass Veränderungen auf dem Transportweg nicht unentdeckt bleiben) und dass der angegebene Absender einer Nachricht auch tatsächlich dem wahren Absender entspricht. Eine solche Garantie ist für viele Anwendungen zwingend erforderlich, beispielsweise die Car2Car-Communication (auf dem Transportweg verfälschte Warnungen können schnell die Verkehrssicherheit gefährden).

Aus den heutigen Netzwerken ist für die Gewährleistung der Datenintegrität das Prinzip der Digitalen Signatur bekannt und praktisch erprobt. Es spricht nichts dagegen, dieses Grundprinzip auch in MANETs einzusetzen. Allerdings ergeben sich bei Ad-Hoc-Netzen mit mobilen Endgeräten, von denen jedes seine eigenen Datenpakete signieren sowie empfangene Datenpakete von allen anderen Knoten auf Integrität prüfen können soll, erhebliche Schwierigkeiten im Bereich des Schlüsselmanagements.

Für eine funktionierende Integritätsprüfung mittels Digitaler Signatur ist es erforderlich, dass jeder Knoten über einen einzigartigen Private Key zur Signierung der eigenen Pakete sowie die Public Keys aller anderen Knoten zur Prüfung der Integrität eingehender Datenpakete verfügt. Das Problem besteht darin, dass eine große Zahl von Public Keys auf sichere Weise auf sämtliche Knoten eines Netzwerks gebracht werden müssen. Darüberhinaus muss der begrenzten Gültigkeitsdauer von Public/Private-Key-Paaren Rechnung getragen werden.

Für dieses Problem gibt es mehrere denkbare Lösungsansätze. Der Austausch der Public Keys könnte beispielsweise über ein unabhängiges, ausreichend sicheres Zweitnetzwerk (etwa das GSM-Netz) und einen externen Server abgewickelt werden. Alternativ wäre auch ein Verfahren denkbar, bei dem der Gerätehersteller einen Hersteller-Public-Key sowie ein mit dem Private Key des Herstellers signiertes, einzigartiges Public/Private-Key-Paar in jedes Gerät fest integriert. Seinen Public Key kann das Gerät später anderen Knoten, mit denen es Datenaustausch durchführen möchte, weitergeben; anhand der Herstellersignatur ist die Authentizität des übermittelten Public Keys und seine Zugehörigkeit zum absendenden Gerät eindeutig verifizierbar.

Ein großer Nachteil beider Lösungen ist offensichtlich: Die vollständige Selbstorganisation angesichts des Bedarfs nach einer Public/Private-Key-Infrastruktur aufrechtzuerhalten ist problematisch. In jedem Fall tritt der Gerätehersteller (oder alternativ der Netzbetreiber) in Aktion und erhält dadurch eine weitgehende Eingriffsmöglichkeit in den integritätsgeschützten Datenverkehr. In ersterem Szenario wäre darüberhinaus ein Zweitnetzwerk nötig, im zweiten Szenario ergäben sich auf längere Zeit Probleme beim Rückruf bzw. der Ersetzung von Keys.

Eine ganz andere Alternative bestünde in der Nutzung nur eines bzw. weniger fester Public/Private-Key-Paare im gesamten Netzwerk. Diese Methode erfordert eine hochgradig sichere Speicherung des Private Key in der Endgeräte-Hardware: jedwede mögliche Extraktion dieses Keys würde die Datenintegritätsgarantie nichtig machen. Außerdem wird es unmöglich, die Private Keys einzelner Geräte für ungültig zu erklären - eine Funktionalität, die etwa für Car2Car-Communication sowie für viele andere Anwendungsfälle auch unabdingbar ist.

3.2 Vertraulichkeit

„Vertraulichkeit“ meint, dass die übertragenen Daten lediglich von Sender und Empfänger, nicht aber von den Relais-Stationen auf dem Weg dazwischen entziffert werden können. Die Gewährleistung dieser Vertraulichkeit kann ebenfalls auf demselben Weg stattfinden wie die Sicherung der Vertraulichkeit bei Kommunikationen über bestehende, kabelgebundene Netzwerke: durch Verschlüsselung der Kommunikation.

Eine Verschlüsselung kann beispielsweise direkt mittels der Public/Private-Key-Paare, die bereits zur Sicherung der Datenintegrität erforderlich sind, stattfinden: Ein Knoten A verschlüsselt seine Nachrichten an B dabei mit dem Public Key von B, wodurch nur B in der Lage ist, diese Nachrichten mit seinem Private Key wieder lesbar zu machen. Der Nachteil dieser Lösung ist der hohe Rechenaufwand zur Ver- und Entschlüsselung: asymmetrische Kryptographie benötigt sehr viel CPU-Leistung im Vergleich zur einfacheren, symmetrischen Kryptographie.

Um diesen Nachteil wettzumachen, kann symmetrische Kryptographie genutzt werden. Diese erfordert zwar den Austausch eines Sitzungsschlüssels vor der Datenübertragung, allerdings funktionieren Schlüsselaustauschprotokolle wie das Diffie-Hellman-Protokoll auch im Kontext eines MANET einwandfrei und können damit diesen Zweck erfüllen. Die Anwendung eines solchen Protokolls macht die Gewährleistung der Vertraulichkeit letztendlich wieder zu einem Identitätsproblem: es muss zweifelsfrei feststellbar sein, dass eine Gegenstelle, mit der man gerade den Schlüssel für eine Verbindung aushandelt, tatsächlich die gewünschte Gegenstelle ist und sich nicht nur als diese ausgibt. Die Lösung des Problems ergibt sich folglich aus den Erwägungen in Kapitel 3.1.

3.3 Privatsphäre

Unter „Privatsphäre“ wird nicht die Vertraulichkeit der übertragenen Daten an sich verstanden, sondern die Vertraulichkeit der Verbindungsdaten - also der Informationen darüber, wer mit welchen Kommunikationspartnern Daten austauscht. In einem MANET sind diese Informationen zu-

nächst selbst dann, wenn die eigentlichen Daten verschlüsselt übertragen werden, ungeschützt: durch simples Mitleesen der Routing-Metainformationen können Kommunikationspfade rekonstruiert werden. Darüberhinaus besteht bei einigen Routing-Protokollen, die mit Flooding von Route Requests arbeiten (etwa DSR), die Möglichkeit, durch Mitleesen der Route Requests die Kommunikationspfade sämtlicher Netzwerkteilnehmer von jedem beliebigen Punkt des Netzwerks aus zu ermitteln.

Steht nun noch eine Methode zur Verfügung, einzelne Netzwerkteilnehmer dauerhaft zu identifizieren (etwa über eine feste Netzwerkadresse), so ist die Privatsphäre der Nutzer nicht mehr gewährleistet. Zur Verbesserung dieser Situation stehen mehrere Wege offen.

Eine Möglichkeit bestünde in dynamischen Netzwerkadressen, die in regelmäßigen Abständen geändert werden. Das Verfahren gliche in etwa dem, welches die meisten DSL-Provider in Deutschland derzeit einsetzen: bei jeder Einbuchung in das Netzwerk erhält der Teilnehmer zufällig eine Adresse aus einem Pool zugewiesen, die er anschließend für eine gewisse Zeit (z.B. 24 Stunden) nutzen kann. Nach Ablauf dieser Zeitspanne erhielte ein Teilnehmer automatisch eine neue Adresse, ebenso bei jeder Neueinbuchung in das Netz. Durch die häufigen Adresswechsel und die zufällige Neuzuweisung wird ein dauerhaftes Tracking eines Knotens erheblich erschwert: eine Verfolgung ist nur noch für den beschränkten Gültigkeitszeitraum einer Adresse möglich.

Eine weitere Möglichkeit wäre durch eine vollständige Anonymisierung sämtlicher Netzwerkkommunikation gegeben. Für diesen Zweck geeignet wäre das Prinzip des Onion Routing, welches im folgenden Kapitel näher erläutert wird.

3.4 Onion Routing als Sicherheitsgarant

Die Technik des Onion Routing hat primär eine Anonymisierung der Kommunikationspartner gegenüber beteiligten Zwischenstationen zum Ziel. Da dies über mehrfache Verschlüsselung der Nachricht erreicht wird, bietet Onion Routing aber gleichzeitig Vertraulichkeit und eine Sicherung der Datenintegrität. Onion Routing wäre folglich denkbar als Garant für alle drei möglichen Sicherheitsmerkmale.

Der Name „Onion Routing“ leitet sich von den Schalen der Zwiebel ab: wie bei einer Zwiebel werden die eigentlichen Nutzdaten in mehrere „Schalen“ eingehüllt, jede davon repräsentiert einen Verschlüsselungsschritt. Diese Schritte werden beim Sender einer Nachricht in umgekehrter Reihenfolge der bis zum Ziel zu durchlaufenden Hops durchgeführt - dem ersten Hop zugehörig ist folglich die äußerste Verschlüsselungsschicht, dem zweiten Hop die darauffolgende, ..., bis zur innersten Verschlüsselungsschicht, die dem Zielknoten zugeordnet ist (siehe Abb. 3).

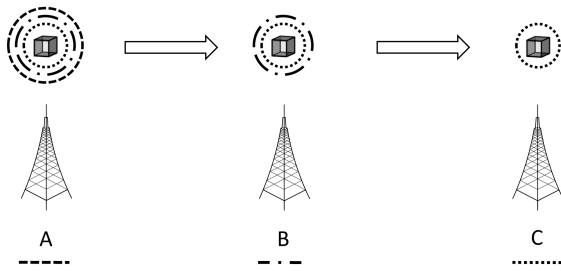


Abbildung 3: Der Aufbau der Mehrfach-Verschlüsselung beim Onion Routing

Zur Verschlüsselung werden Schlüssel der jeweiligen Hops verwendet. Dabei kann es sich entweder um rein asymmetrische Kryptographie unter Nutzung der Public Keys der Hops handeln, oder - um den Rechenzeit-Overhead so gering wie möglich zu halten - um einen zufällig bestimmten symmetrischen Schlüssel für jeden Hop, welcher vor dem eigentlichen Datenaustausch vom Sender an den Hop vergeben wird. Wichtig ist, dass nur der jeweilige Hop die ihm zugedachte Verschlüsselungsschicht entfernen kann, und dass er dies nur tun kann, wenn die vorhergehenden Hops jeweils ihre Schichten bereits entfernt haben.

Die Anonymität ergibt sich daraus, dass beim Onion Routing jeder Knoten nur den vorigen Knoten (von diesem Knoten kam die Nachricht) sowie den Folgeknoten (an diesen leitet er die Nachricht weiter; seine Adresse muss demzufolge zur Verfügung stehen) kennt, darüberhinaus aber keine Informationen besitzt, die eine vollständige Rekonstruktion der Route sowie eine eindeutige Bestimmung des Senders und des Empfängers erlauben würden. Voraussetzung für das Funktionieren dieses Verfahrens ist eine minimale Anzahl von 2 Hops zwischen Start- und Zielknoten (ein Hop könnte zwar je nach Implementation grundsätzlich schon genügen, falls es dem Hop unmöglich ist, zu erkennen, dass seine Nachbarknoten die Start- und Zielknoten und nicht nur Relais-Knoten sind, aber im Falle von nur einem Hop besäße dieser selbst in diesem positiven Fall sowohl die Adresse des Start- als auch des Zielknotens; ein Zustand, den es zu vermeiden gilt).

Onion Routing als grundsätzliches Verfahren funktioniert in der Praxis, wie das TOR-Netzwerk⁸ - ein Anonymisierungsnetzwerk, welches auf IP aufsetzt und das Anonymisieren jeglicher TCP-Verbindung erlaubt - seit Jahren beweist, und es würde sich ideal auf das Szenario „MANET“ übertragen lassen. Allerdings traten speziell bei TOR, welches zum wohl weltweit größten praktisch angewandten Onion-Routing-Netz gewachsen ist, auch Nachteile des Verfahrens zutage, die zum Großteil auch bei einer eventu-

⁸<http://www.torproject.org>

ellen Anwendung in einem MANET zum Tragen kommen.

- Onion Routing erhöht die Latenzzeit beträchtlich durch mehrfache (rechenaufwendige) Verschlüsselung sowie die Weiterleitung über viele Knoten. Letzteres ist in einem MANET im Gegensatz zum TOR-Netzwerk auch ohne Onion Routing erforderlich, die zusätzliche Rechenzeit, die für mehrfache Ver- und Entschlüsselung der Daten benötigt wird, wirkt sich dafür in einem mobilen Umfeld mit beschränkter CPU-Leistung und dem Gebot zur Energieeffizienz umso stärker aus.
- Onion Routing erfordert eine Mindestanzahl von Hops, welche größer als die physikalisch zur Übermittlung der Nachricht benötigte Anzahl Hops sein kann. In diesem Fall verursacht Onion Routing eine unnötige Belegung der Luftschnittstelle und dadurch eine Vergeudung von Bandbreite.
- Onion Routing schützt Daten nur innerhalb des Netzwerks, **nicht** am Start- oder Endpunkt.

Speziell der letzte Punkt bedarf einiger weiterer Erläuterungen. So lange Onion Routing lediglich zur Kommunikation zwischen zwei echten Endpunkten (welche die Nachrichten nicht selbst weiterleiten) genutzt wird, bietet es umfassenden Schutz. Sobald der Endpunkt des Onion-Routing aber gar nicht der eigentliche Empfänger der Klartext-Nachricht ist, sondern lediglich ein Gateway, welches die Nachricht aus welchem Grund auch immer im Klartext besitzen muss (beispielsweise, weil es als Gateway zum unverschlüsselten Internet dient), erlangt ein an der Kommunikation Unbeteiligter Kenntnis über den Inhalt der Nachricht sowie die Identität von Sender und Empfänger. Vermieden werden kann dies z.B. im Falle des Internet-Gateways dadurch, dass eine zusätzliche Verschlüsselung auf einer höheren Ebene (etwa durch Anwendung von SSL) eingesetzt wird.

4 Fazit

In die Forschung zu praxistauglichen Protokollen für selbstorganisierende Ad-Hoc-Funknetze ist bereits einiges an Aufwand geflossen. Es steht eine fast unüberschaubar große Zahl von Protokollen zur Verfügung, die sich jedoch auf wenige Grundprinzipien zurückführen lässt, welche jeweils unterschiedlich und mit teilweise äußerst kreativen Optimierungsansätzen abgewandelt werden. Dadurch ergibt sich für den praktischen Aufbau eines MANETs der Bedarf nach gründlicher Recherche vor der Entscheidung für ein Protokoll, um eine für den jeweiligen Anwendungsfall optimale Lösung zu finden.

Einen Vorteil durch weitgehende Unterstützung hat bislang mangels verbreiteter Standards keines der Protokolle. Zwar gibt es erste Ansätze, Protokolle in RFCs zu gießen und auf diese Weise zu einem „Internet-Standard“ zu erheben, doch sind auch diese „Standards“ nur so gut wie ihr Verbreitungsgrad, welcher derzeit noch zu wünschen übrig lässt. Dasselbe gilt für den im Entwurf befindlichen Standard IEEE 802.11s. In diesem Zusammenhang gilt es auch zu beachten, dass von vielen der vorgeschlagenen Protokolle bislang nur eine Spezifikation in Form eines Papers o.ä. existiert; eine funktionierende, praxistaugliche Implementierung ist die Ausnahme.

Einige wenige Protokolle sind jedoch bereits in praktischer Anwendung, etwa das OLSR-Protokoll im Freifunk-Netzwerk (welches allerdings längerfristig von einer Freifunk-Eigenentwicklung namens B.A.T.M.A.N. abgelöst werden soll) oder das hybride HWMP-Protokoll im noch im Entwurfsstadium befindlichen Industriestandard IEEE 802.11s für Mesh-Netzwerke. Dieser Standard ist zwar noch weit von seiner Verabschiedung entfernt, allerdings gibt es mit den OLPC-Laptops immerhin bereits eine nennenswerte, auf einem Draft von 802.11s aufbauende Anwendung. Dies lässt hoffen, dass mit 802.11s schlussendlich ein praxistauglicher Standard verabschiedet wird, der in den anvisierten Anwendungsfeldern (Vernetzung von unwirtlichem Gebiet, Kurzzeit-Vernetzung von Event-Gelände, Car2Car-Communication) genutzt werden kann. Ein Standard, der die Verbreitung entsprechender Endgeräte durch universelle Nutzungsmöglichkeiten und niedrige Hardware-Preise ankurbeln könnte, ist einer der wichtigsten Bausteine, die für eine effektive Nutzung von MANETs heute noch fehlen.

Allerdings sind auch auf Seiten der Protokolle und Infrastruktur noch lange nicht alle offenen Fragen geklärt. Wie die Vielzahl an möglichen, oftmals in ihrer Wirkung stark situationsabhängigen Optimierungsansätze überhaupt in einen einheitlichen Standard gefasst werden könnten, ohne zu viel an Flexibilität und Effektivität einzubüßen, ist eine solche Frage; auch besteht auf Seiten der Sicherheit noch Handlungsbedarf, denn für viele Anwendungsfälle sind sehr spezifische Sicherheitsbedingungen zu erfüllen, die in den bestehenden Routing-Protokollen üblicherweise keine Berücksichtigung fanden. Aber die Grundidee funktioniert und wird in spezifischen Einzelanwendungen, die auch wirtschaftlich gesehen Sinn ergeben, bereits eingesetzt - eine durchaus brauchbare Basis für weitere Entwicklungen, wenngleich der Technologie wohl keine so schlagartige Ausbreitung wie etwa der WiFi-Technik vergönnt sein wird.

Literatur

- [1] Holger Karl, Andreas Willig, *Protocols and Architectures for Wireless Sensor Networks*, Wiley, 2007.
- [2] David B. Johnson, David A. Maltz, Josh Broch, *DSR: The Dynamic Source Routing Protocol für Multi-Hop Wireless Ad Hoc Networks*, Computer Science Department, Carnegie Mellon University, Pittsburgh, 2001. <http://www.monarch.cs.rice.edu/monarch-papers/dsr-chapter00.pdf>
- [3] D. Johnson (Rice University), Y. Hu (UIUC), D. Maltz (Microsoft Research), *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4*, RFC 4728, Februar 2007
- [4] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, *Optimized Link State Routing Protocol for Ad Hoc Networks*, Hipercom Project, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France <http://hipercom.inria.fr/olsr/inmic2001.ps>
- [5] T. Clausen, P. Jacquet, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4*, RFC 3626, Oktober 2003
- [6] Nicklas Beijar, *Zone Routing Protocol*, Networking Laboratory, Helsinki University of Technology, Finland, 1998 <http://www.netlab.hut.fi/opetus/s38030/k02/Papers/08-Nicklas.pdf>
- [7] Young-Bae Ko, Nitin H. Vaidya, *Location-Aided Routing (LAR) in mobile ad hoc networks*, Department of Computer Science, Texas A&M University, 2000 http://www.cs.huji.ac.il/labs/danss/sensor/adhoc/routing/ko_1998locationaidedrouting.pdf
- [8] Rahul C. Shah, Jan M. Rabaey *Energy Aware Routing for Low Energy Ad Hoc Sensor Networks*, Berkeley Wireless Research Center, University of California, Berkeley, 2002 <http://bwrc.eecs.berkeley.edu/Publications/2002/presentations/WCNC2002/wcnc.rahul.pdf>