Im Zeichen der Fledermaus

Mobiles Routing in Ad-hoc-Netzen mithilfe von B.A.T.M.A.N.

Kai-Oliver Detken

Ad-hoc-Netze haben, obwohl immer noch relativ unbekannt, speziell bei Katastropheneinsätzen eine hohe Bedeutung. So lassen sich z.B. fehlende IT-Infrastruktur kompensieren und die Arbeiten verschiedener Rettungsorganisationen bündeln. Damit Ad-hoc-Netze automatisiert aufgesetzt werden können, müssen entsprechende Routing-Mechanismen greifen. Diese werden allerdings immer noch untersucht, da Ad-hoc-Umgebungen permanent Veränderungen ausgesetzt sind, wodurch sich die kürzesten Routing-Wege immer wieder aktualisieren. Anhand des Routing-Protokolls B.A.T.M.A.N. sollen der derzeitige Entwicklungsstand und neue Anwendungsszenarien aufgezeigt werden.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Ein Ad-hoc-Netz ist ein Funknetz, das diverse Funkknoten und Funkstrecken enthält, die zusammengenommen ein vermaschtes Netz bilden, und das sich selbstständig aufbaut und konfiguriert. Hier existiert quasi keine verwaltende Infrastruktur untereinander – auch nicht mit anderen Netzen. Die Daten werden somit über mehrere Stationen von Netzknoten zu Netzknoten weitergeleitet, bis sie den entsprechenden Empfänger erreicht haben. Die Datenlast verteilt sich dadurch vorteilhafter als in sternförmigen Netzen mit einem zentralen Knoten. Das bedeutet aber auch, dass keine Access Points (AP) verwendet werden, wie das normalerweise bei Wireless LANs (WLANs) der Fall ist. *Bild 1* verdeutlicht einen solchen Ad-hoc-Aufbau, der auch als Mesh Network bezeichnet wird. In diesem Fall ist ein Laptop mit einem Internetrouter fest verbunden, so dass auch alle anderen Teilnehmer diesen Internetzugang nutzen können.

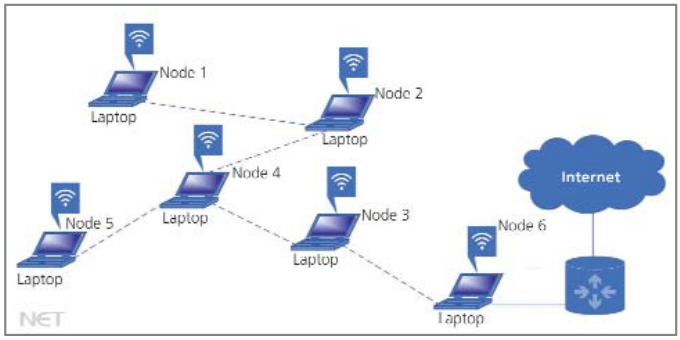

Bild 1: Ad-hoc- bzw. Mesh-Netz mit Internetanbindung

Die Vorteile eines solchen Netzes liegen auf der Hand. Bei Ausfall eines Endgeräts ist der Rest der Teilnehmer nicht betroffen, sondern es bildet sich einfach ein neues Ad-hoc-Netz mit den verbliebenen Knoten aus. Auch die Lastverteilung ist idealer, als bei Netzverbunden mit zentraler Verwaltung. Allerdings gibt es nicht nur Vorteile: So ist ein vergleichsweise komplexes Routing erforderlich, da die Netzkonstellation sich kontinuierlich ändern kann. Jedes Endgerät muss zudem Routing-Aufgaben übernehmen und dementsprechend eine Routing-Tabelle besitzen. Um das Ad-hoc-Netz stabil zu betreiben, sollten die Endgeräte auch eingeschaltet bleiben.

Beispielhaftes Anwendungsszenario

Als beispielhaftes Anwendungsszenario kann man HiMoNN (Highly Mobile Network Node, **http://himonn.iabg.de/index.php/technik/mobiles-ad-hoc-netzwerk**) von der IABG, dem Forschungs- und Technologiezentrum in Ottobrunn bei München, heranziehen. Die Industrie-Anlagen-Betriebs-Gesellschaft mbH ist 1961 ursprünglich als zentrale Analyse- und Testeinrichtung für die Luftfahrtindustrie und das Verteidigungsministerium gegründet worden. Inzwischen werden aber auch andere Geschäftsfelder, wie mobiles Ad-hoc-Networking, adressiert.
Das HiMoNN-System besteht aus einer Anzahl von mobilen Kommunikationsknoten, die sich nach der Inbetriebnahme funkbasiert automatisch miteinander vernetzen. An diese Knoten (*Bild 2*) können dann über standardisierte Schnittstellen diverse Endgeräte (z.B. Laptops, Tablet-PCs, Smartphones) angeschlossen werden. Der HiMoNN-Knoten kann dabei auch als Gateway betrieben werden, um darüber externe Netze, wie das Internet, verbinden zu können. Zwischen den Knoten lässt sich eine Übertragungsrate von bis zu 28 Mbit/s ausnutzen. Die Knoten dürfen dabei bis zu 2 km voneinander entfernt stehen. Bei der Umsetzung hat man auch an die IT-Sicherheit gedacht und entsprechende Sicherheitsmerkmale inte-

Bild 2: HiMoNN-Basis für Ad-hoc-Netze in Krisensituationen

(Foto: IABG)

griert, die sich konform zu den BSI-Sicherheitsrichtlinien verhalten.

Als Anwendungen kommen speziell Notfallszenarien infrage, bei denen auf keine herkömmliche IT-Infrastruktur zurückgegriffen werden kann:

- Feuerwehr und Rettungskräfte: Vernetzung von Stabführungsstellen, Anbindung von Gebäudefunksystemen, Zusammenführung von Mess- und Sensordaten, Vernetzung von Behandlungsplätzen auf Großveranstaltungen;
- Polizei: Aufbau mobiler Befehlsstellen, Einsätze bei Schadenslagen, Überwachung von Personen, kritischen Infrastrukturen und Verkehrsabschnitten;
- Verteidigung: Vernetzung von Feldlagern, Anbindung von Checkpoints, Konvoi-Kommunikation, Anbindung von Begleitbooten an eine Fregatte;
- Industrie: Überwachung von Industrieanlagen, kritischen Infrastrukturen und logistischen Umschlagplätzen, Inbetriebnahme von Anlagen.

Es gibt also zahlreiche Anwendungen, bei denen ein solches Ad-hoc-Netz von Vorteil ist, vor allem dann, wenn bei Einsatzkräften der Kommunikationsbedarf unterstützt werden muss und dieser nicht über die vorhandene Infrastruktur vorgenommen werden kann. Im Katastrophenfall (z.B. Hochwasser oder Großbrände) kann zudem oft nicht auf eine bestehende IT-Infrastruktur zurückgegriffen werden, weshalb HiMoNN eine entsprechende Alternative darstellt.

B.A.T.M.A.N. – das „Fledermaus"-Protokoll

Es gibt eine Vielzahl von Routing-Vorschlägen, die für Ad-hoc-Netze eingesetzt werden können. Eine einheitliche Klassifikation solcher Protokolle existiert allerdings nicht. Man kann aber grundsätzlich zwischen reaktiven und proaktiven Protokollen unterscheiden, bei denen auf unterschiedliche Weise Pfade im Netz gefunden, gespeichert und ausgetauscht werden. Deren Hauptaufgabe ist es, den kürzesten Pfad von der Quelle zum Empfänger zu bestimmen, der bei einem Routing-Protokoll durch die Metrik festgelegt wird. Aufgrund des Aufbaus von Ad-hoc-Netzen können dabei keine üblichen Routing-Algorithmen aus dem Internet zum Einsatz kommen. Dies liegt hauptsächlich an folgenden Eigenschaften:

- Ad-hoc-Knoten besitzen kein Vorwissen über die Netztopologie.
- Es gibt keine zentrale Instanz zum Speichern von Routing-Informationen.
- Die Knoten sind ggf. mobil, wodurch sich in dem Fall ständig die Topologie ändert.
- Die Metriken wechseln durch Topologieänderungen kontinuierlich.
- Die Netzknoten haben ggf. limitierte Ressourcen (z.B. Systemleistung, Speicher).

Das Protokoll B.A.T.M.A.N. (Better Approach to Mobile Adhoc Networking, **www.open-mesh.org**) ist ein reaktives Routing-Protokoll für Ad-hoc-Netze und ist durch die Entwicklung und Nutzung in der Freifunk-Community relativ weit verbreitet. Es ist außerdem Open Source und untersteht der GNU General Public License (GPL). Dieses Protokoll berechnet nicht auf jedem Endknoten eine Routing-Tabelle für das komplette Netz. Aber jeder Router informiert regelmäßig seine Nachbar-Router über Broadcast-Nachrichten, ob er noch aktiv ist und an der Kommunikation teilnehmen kann. Dadurch reicht es aus, dass in der Routing-Tabelle nur enthalten ist, über welchen Nachbarn weitere Router erreicht werden können, ohne dass die gesamte Route jedes Mal überprüft werden muss. In den Broadcast-Mitteilungen ist damit eine Metrik enthalten, die die Qualität der Verbindung wiedergibt, wodurch die Router auch Informationen über den Verbindungszustand erhalten.

Unterscheiden muss man inzwischen das konventionelle B.A.T.M.A.N.-Protokoll und die „Advanced"-Variante. Während Ersteres auf Schicht 3 des OSI-Referenzmodells arbeitet und IP-Pakete zum Austausch verwendet, nutzt die erweiterte Variante die Schicht 2, weshalb das vermaschte Netz als verteilter Switch für die darüberliegenden Schichten erscheint. Dadurch erkennen darüberliegende Schichten nicht mehr, über welches Netz sie ihre Datenpakete schicken. Hinzu kommt, dass die Performance verbessert wurde, indem das Protokoll der zweiten Generation seit 2011 fest als Modul im Linux-Kernel ab der Version 2.6.38 integriert ist. Dadurch bildet das Protokoll in Embedded-Linux-Routern einen integralen Bestandteil.

Als Basiseigenschaften von B.A.T.M.A.N. lassen sich nennen:

- Ein Knoten kann bereits an der Kommunikation teilnehmen, bevor er eine IP-Adresse bekommen hat.
- Es lassen sich beliebige Schicht-3-Protokolle nutzen, z.B. neben dem Internetprotokoll Version 4 (IPv4) auch Version 6 (IPv6).
- Mobile und stationäre Endgeräte lassen sich durch DHCP (automatische IP-Adressvergabe) in das Gesamtnetz integrieren,
- Mobile und stationäre Endgeräte sind in der Lage, zwischen vermasch-

ten Access Points Roaming durchzuführen.

Als alternatives Protokoll wird ebenfalls Optimized Link State Routing (OLSR) eingesetzt, das eine angepasste Variante des Link State Routings beinhaltet. Bei diesem Protokoll ist es notwendig, dass alle Router die Netztopologie kennen. Es gehört zu den proaktiven Routing-Protokollen, weshalb die Routing-Informationen jederzeit an den jeweiligen Knoten vorgehalten werden müssen. Die Topologieerkennung erfolgt über Hello- und Topologie-Control-Nachrichten. Hello-Nachrichten dienen dabei zur Nachbarentdeckung und zur Mitteilung der Multipoint-Relay-Wahl sowie zur Verbindungserfassung (Link Sensing). Die Topologie-Control-Nachrichten müssen anschließend die gesammelten Informationen im Netz verteilen. OLSR ist ebenfalls in der Freifunk-Community im Einsatz und in der RFC-Spezifikation 3626 beschrieben. Diese besitzt allerdings nur einen experimentellen Charakter. Aufgrund von Performance-Problemen wurde OLSR immer mehr gegen B.A.T.M.A.N. eingetauscht.

B.A.T.M.A.N. skaliert besser und ist daher, wie im Namen hinterlegt, der bessere bzw. effizientere Routing-Ansatz. Der Vorteil von B.A.T.M.A.N. gegenüber OLSR liegt hauptsächlich in der geringeren Information, die pro Knoten bereitgehalten werden muss. Bei einem Link-State-Routing-Protokoll wie OLSR muss jeder Router die gesamte Topologieinformation halten, um die optimalste Route durch das Netz zu finden. Um diese Information zu erfassen, müssen alle Knoten miteinander synchron sein. Dies ist, je größer das Netz ist, schwer zu realisieren. Zusätzlich kostet der Informationsaustausch über das gesamte Netz mehr Bandbreite, impliziert eine höhere Verzögerung und beinhaltet einen größeren CPU- und Speicheraufwand durch Schleifen und Paketverluste.

Einsatz im Freifunk-Netz

Entstanden ist die Freifunk-Community (**www.freifunk.net**) hauptsächlich aus Gründen der Störerhaftung in Deutschland, die bis 2017 vorsah, dass der Betreiber eines WLAN für die Handlung der Benutzer mit haftbar gemacht werden konnte. Dadurch waren Abmahnungen quasi an der Tagesordnung und viele Restaurants oder Hotels schafften den freien Internetzugang wieder ab oder ließen ihn über einen anderen Anbieter (z.B. Deutsche Telekom) realisieren, der die entsprechende Verantwortung mit übernahm.

Durch den Einsatz eines Freifunk-Routers umging man dieses Problem, indem man die Kommunikation über einen schwedischen VPN-Anbieter (Virtual Private Network) ins Internet laufen ließ (*Bild 3*), da es dort keine Störerhaftung gab. Die Community selbst ist dezentral organisiert, da jeder Teilnehmer einen Freifunk-Router aufstellen und über die technische Ausgestaltung frei verfügen darf. Sie organisiert die Vernetzung der einzelnen Betreiber und schafft einen gemeinsamen Nenner bei der Verwendung kompatibler Software. Festlegen muss man sich beispielsweise bei der Router-Firmware, bei Richtfunkstrecken zur Überwindung größerer Hindernisse und beim Support bei der Konfiguration.

Durch die Organisation als Verein bietet sie zudem den Teilnehmern eine gewisse Rechtssicherheit.

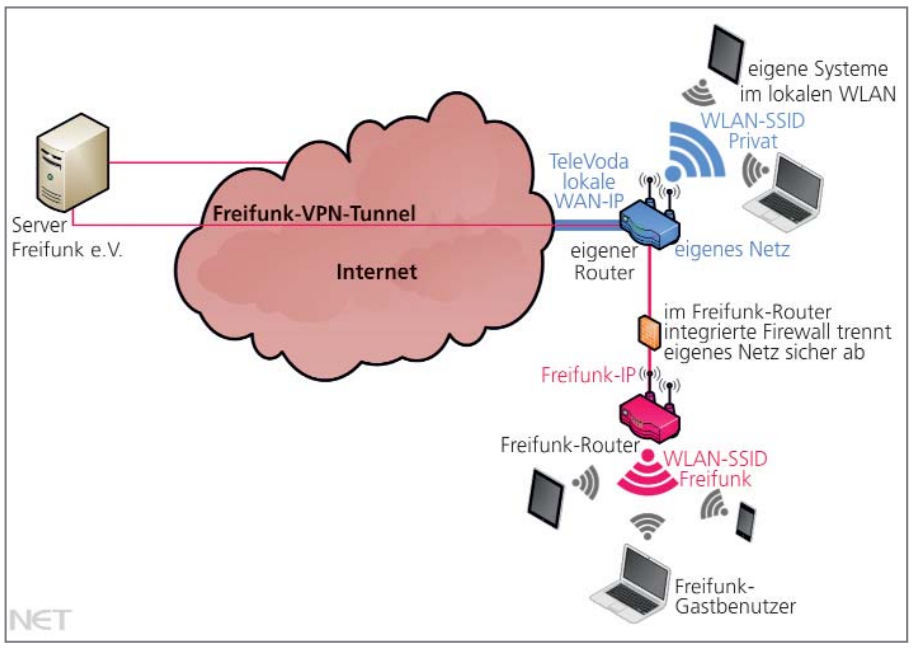

Bild 3: Freifunk-Szenario mit VPN-Verbindung zu einem Provider
(Quelle: Felix Bosseler, http://freifunk-aachen.de/freifunk-basiswissen/)

Fazit

Ad-hoc-Routing-Protokolle, wie z.B. B.A.T.M.A.N., werden nicht nur im WLAN-Umfeld verwendet. Auch in der IP-Telefonie gibt es Anwendungen, innerhalb derer Smartphones als Knoten angesehen werden, die sich über ein vermaschtes Netz ad-hoc verbinden können, um miteinander zu telefonieren. Dies funktioniert ohne einen Provider bzw. einen zentralen Server, auf dem ein VoIP-System gehostet wird. Die größte Innovation dieses Protokolls ist es daher, dass viele unterschiedliche Netzgeräte unterstützt werden können. Einmal verbunden, können so Daten über unterschiedliche Verbindungen ohne Verzögerung übertragen werden.

Zusätzlich ist B.A.T.M.A.N. bereits im Freifunk-Netz relativ weit verbreitet. Diese Initiative wird aber wahrscheinlich an Teilnehmern verlieren, wenn die Störerhaftung komplett abgeschafft und kein Thema mehr ist. B.A.T.M.A.N. selbst wird aber aller Wahrscheinlichkeit nach weiter beliebt bleiben, da es nicht auf Freifunk beschränkt ist und bereits in anderen Umfeldern (z.B. guifi.net) zum Einsatz kommt. Hinzu kommt, dass es Anwendungsszenarien gibt, die den Einsatz von mobilen Routing-Verfahren einfach voraussetzen. *(bk)*