UNIVERSITY OF APPLIED SCIENCES

Department of Computer Science

Seminar

IT-Sicherheit

Wireless Mesh Networks

Eingereicht am:

16. Dezember 2015

Eingereicht von:

Tim Pauls
inf101369@fh-wedel.de

Betreut von:

Prof. Dr. Gerd Beuster
gb@fh-wedel.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Ein Wireless Mesh Network (WMN) ist ein dezentrales, kabelloses Computernetzwerk, das der Verbindung mehrerer Endgeräte untereinander dient. WMNs liegt dabei die Idee zugrunde, dass Netze an Orten etabliert werden können, an denen eine kabelgebundene Infrastruktur bislang fehlt oder schlicht unmöglich ist.

Knoten im Netzwerk sind direkt miteinander vernetzt und nicht auf eine gemeinsame Anlaufstelle angewiesen. Die Netze sollen sich selbst organisieren und konfigurieren, wenn neue Teilnehmer in das Netz eintreten, und sich selbst heilen, wenn Netzknoten ausfallen. Sie können ihre Topologie also dynamisch den Gegebenheiten anpassen, was ihnen eine enorme Zuverlässigkeit und Vielseitigkeit beschert.

Durch ihre Eigenschaften eignen sich Wireless Mesh Networks hervorragend dazu zu geringen Kosten und über größere Gebiete hinweg eine flächendeckende Netzwerkanbindung zu ermöglichen. Allerdings birgt ihr Einsatz auch gewisse Herausforderungen und Risiken.

Diese Arbeit gibt einen breiten Überblick über unterschiedliche Aspekte von Wireless Mesh Networks. Zunächst wird auf die technischen Voraussetzungen eingegangen. Dabei werden die Gesichtspunkte Topologie, Eigenschaften und Bedingungen des Betriebs und Routing der Daten betrachtet. Anschließend werden Sicherheitsrisiken und mögliche Verteidigungen auf unterschiedlichen Netzwerkschichten analysiert. Abschließend werden verschiedene Motivationen zum Einsatz von WMNs vorgestellt.

2 Technik

2.1 Netztopologie

Bei Wireless Mesh Networks handelt es sich, wie der Name bereits verrät, um *vermaschte* Netze. In einem vermaschten Netz ist jeder Knoten mit einem oder mehreren Nachbarknoten verbunden und reicht an sie Daten durch das Netz weiter, bis sie beim Empfänger angelangt sind. Sind alle Knoten untereinander verknüpft, spricht man von einem *vollständig vermaschten Netz*. Durch die vielen Verbindugen zwischen den Knoten können auch bei Ausfällen einzelner Verbindungen oder Knoten die Daten über andere Teile des Netzwerks an ihr Ziel geleitet werden. Außerdem wird die Reichweite der Datenübertragung durch Zwischensprünge erhöht. In einem WMN kann jeder Knoten, der sich in der kabellosen Übertragungsreichweite eines anderen befindet, als sein Nachbarknoten betrachtet werden. Abbildung 2.1 zeigt die Struktur eines teil- und eines vollvermaschten Netzes.

(a) Teilvermaschtes Netz (b) Vollvermaschtes Netz

Abbildung 2.1: Struktur vermaschter Netze

Da sich die Anzahl der Verbindungen in einem vermaschten Netz mit steigender Teilnehmerzahl rapide erhöht, bieten sich zur Umsetzung kabellose Technologien besonders an. Durch sie entstehen weitaus geringere Kosten, als durch die Nutzung von Kabeln.

Wireless Mesh Networks bestehen im Wesentlichen aus zwei unterschiedlichen Komponenten: Mesh-Routern und Mesh-Clients [AWW05, S. 446].

Mesh-Router basieren oft auf der selben Hardware wie handelsübliche Wireless-Router, bieten jedoch zusätzliche Fähigkeiten zum Mesh-Routing und besitzen häufig mehrere kabellose Netzwerkinterfaces, unter Umständen für unterschiedliche Technologien (z.B. LTE, WiMAX).

Mesh-Clients können beliebige Endgeräte sein, die eine kabellose Datenverbindung unterstützen (Computer, Smartphones, Funksensoren). Sie können ebenfalls Daten weiterleiten, sind in ihren Routing-Fähigkeiten jedoch weitaus beschränkter als Mesh-Router.

WMNs lassen sich in drei unterschiedliche Architektur-Typen einteilen, die im Folgenden näher erläutert werden.

2.1.1 Infrastructure WMNs

Infrastructure WMNs, auch *Backbone WMNs* genannt, bestehen im Grundgerüst aus miteinander vernetzten Mesh-Routern, die Clients eine Infrastruktur bieten, mit der diese sich verbinden können. Die Verknüpfung, mit der die Mesh-Router ein selbstheilendes und selbskonfigurierendes Netz aufbauen, kann auf beliebigen kabellosen Technologien basieren, beispielsweise auch auf dem gewöhnlichen IEEE 802.11. Üblicherweise wird jedoch für die Backbone-Kommunikation eine getrennte Technologie verwendet, etwa Richtfunkantennen. Einige der Router können als Gateways an das Internet angebunden sein, was den Clients zusätzlich zur netzinternen Kommunikation eine Schnittstelle in andere Netze eröffnet [AWW05, S. 447 f.]. Abbildung 2.2 zeigt den Aufbau eines Infrastructure WMNs, wobei die durchgezogenen Linien eine Internetanbindung, die dickeren gestrichelten Linien das Mesh-Netz der Router und die dünnen gestrichelten Linien die kabellose Verbindung der Clients darstellen.

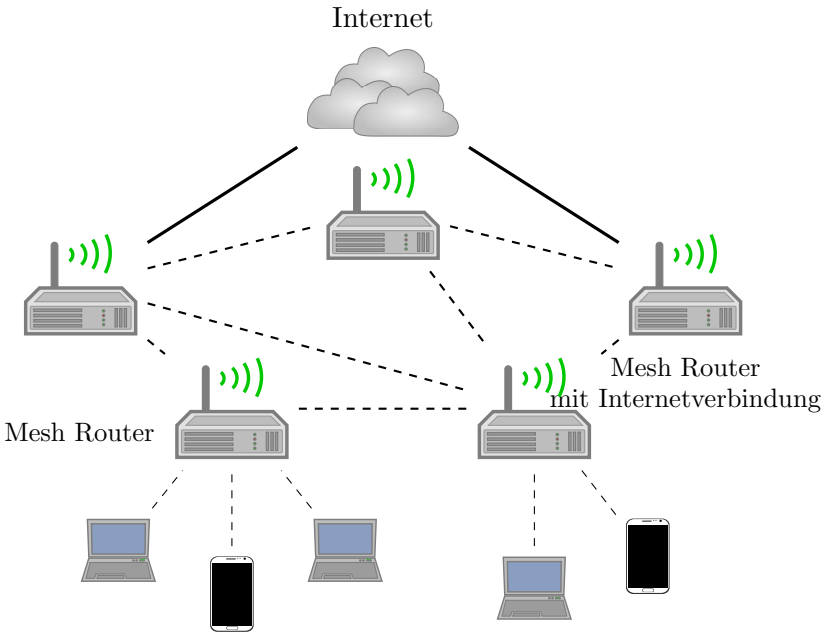


Abbildung 2.2: Struktur eines Infrastructure WMNs

2.1.2 Client WMNs

In *Client WMNs* bilden die Endgeräte selber das Netzwerk. Da es sich hierbei um ein reines Peer-to-Peer-Netz handelt, werden keine Mesh-Router benötigt. Die Daten werden zwischen den Clients weitergereicht, bis sie an ihrem Zielknoten ankommen. In Client WMNs wird meist nur auf eine einzige Übertragungstechnologie zurückgegriffen. Weiterhin werden gegenüber dem Infrastructure Meshing höhere technische Anforderungen an die Endgeräte gestellt, da diese neben ihren Anwendungsaufgaben nun auch die volle Verantwortung für das Routing und die Netzwerkkonfiguration tragen [AWW05, S. 448 f.]. Ein beispielhaftes Client WMN ist in Abbildung 2.3 dargestellt.

2.1.3 Hybrid WMNs

Hybid WMNs kombinieren die Technologien der beiden vorangegangenen Architekturen innerhalb eines Wireless Mesh Networks. Die grundlegende Struktur des Netzes wird, wie bei Infrastructure WMNs, von Mesh-Routern bereitgestellt, gegen die sich Mesh-Clients verbinden können. Zusätzlich

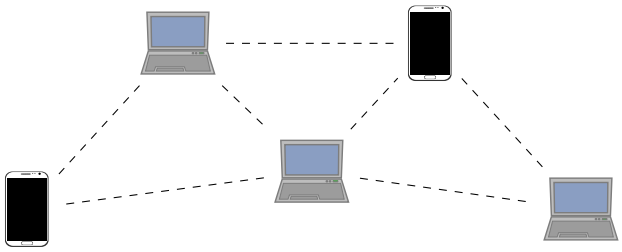


Abbildung 2.3: Struktur eines Client WMNs

bauen aber auch die Clients untereinander Verbindungen auf, mit denen das Netzwerk erweitert wird. Dieser hybride Ansatz führt zu einem enger gemaschten Netz, was eine bessere Abdeckung und besseres Routing zur Folge hat, während die Mesh-Router weiterhin externe Netze anbinden und die Clients im Routing entlasten [AWW05, S. 449]. Abbildung 2.4 zeigt den Aufbau eines Hybrid WMNs.

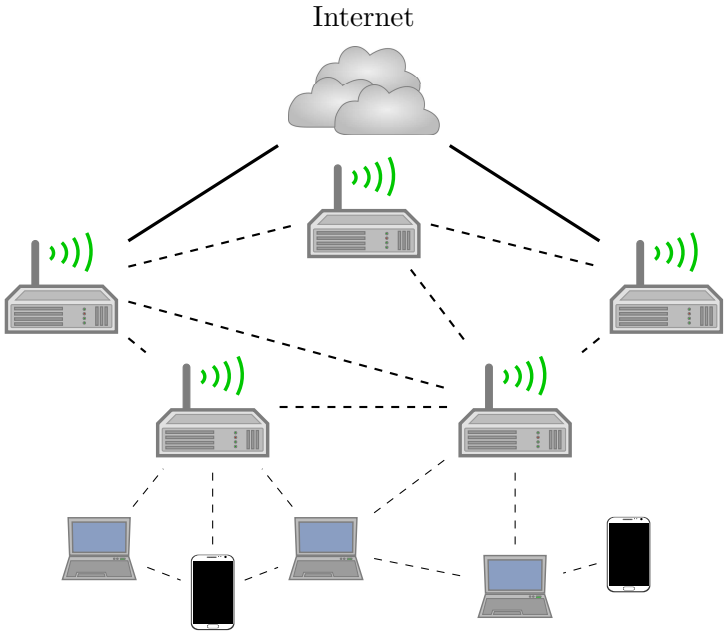


Abbildung 2.4: Struktur eines Hybrid WMNs

2.2 Eigenschaften von Wireless Mesh Networks

Eine zentrale Eigenschaft von Wireless Mesh Networks ist die Multi-Hop-Kommunikation zwischen den Teilnehmern. Sie ist erforderlich, um ein wichtiges Ziel bei der Verwendung von WMNs zu erreichen: eine im Vergleich zu gewöhnlichen kabellosen Netzen deutlich höhere Reichweite. Da die Übertragung von Daten über größere Distanzen durch mehrere relativ kurze Funkverbindungen erzielt wird, bleiben die Nachteile von Langstreckenfunkverbindungen (beispielsweise starke Gefahr von Interferenzen) aus.

Die zweite bedeutende Charakteristik ist die Fähigkeit zur Selbstorganisation und Selbstheilung der Netze, da sie dadurch eine besonders hohe Robustheit bei geringem Wartungsaufwand erhalten. Durch die Selbstkonfiguration kann ein WMN organisch mit dem Bedarf der Abdeckung wachsen.

Die initialen Kosten für die Einrichtung eines WMNs sind sehr gering, da neben den Netzwerkkomponenten (Mesh-Routern und -Clients) keine zusätzlichen Kosten für die Infrastruktur anfallen (es ist keine Verkabelung erforderlich). Dadurch, dass sich ein WMN selbst konfiguriert, ist eine flexible Erweiterung durch zusätzliche Router sehr leicht möglich, die die Abdeckung des Netzes ausbauen. Wenn z.B. ein weiteres Gebäude an einen Komplex angebaut wird, können einfach neue Mesh-Router dem Netz hinzugefügt werden, um es an das bestehende Netzwerk anzubinden. Auch bei vereinzelten Fehlern sorgt ein WMN dafür, dass der Datenverkehr nicht vollständig abreißt. Ausfälle im Netz können bemerkt und behandelt werden, indem Daten von nun an über andere Knoten an ihr Ziel geleitet werden.

In einem WMN haben die Komponenten typischerweise unterschiedliche Fähigkeiten in Bezug auf ihre Mobilität. Mesh-Router dienen als stationäre Ansprechpunkte, wohingegen die meisten Mesh-Clients in ihrer Beweglichkeit größtenteils uneingeschränkt agieren können.

Ähnlich wie bei der Mobilität unterscheiden sich auch die Ansprüche an die Energieeffizienz der unterschiedlichen Netzwerkgeräte. Da die fest angebrachten Mesh-Router üblicherweise auch über eine durchgehende Stromversorgung verfügen, ist es nicht zwingend erforderlich sie besonders sparsam zu betreiben. Ganz anders sieht das jedoch bei den Mesh-Clients aus. Hier kommen größtenteils mobile Endgeräte zum Einsatz, deren Energieversorgung unter umständen deutlich sparsamere Kommunikationsprotokolle erfordert. So können für Mesh-Clients nicht automatisch dieselben Routing-Protokolle verwendet werden, die für den Einsatz in Mesh-Routern optimiert wurden [AWW05, S. 449 f.].

2.3 Zentrale Bedingungen für die Leistungsfähigkeit von WMNs

Bei der Planung und dem Aufbau eines WMNs gilt es einige grundlegende Bedingungen zu beachten, von denen die Leistungsfähigkeit des Netzwerks bedeutend abhängig ist.

Im Vordergrung steht naheliegenderweise die zum Einsatz kommende Funktechnologie. Hier existieren viele unterschiedliche Ansätze, etwa gerichtete und intelligente Antennen oder Multiple-Input-Multiple-Output-Systeme (MIMO), die mehrere Antennen zum Senden und Empfangen von Daten gleichzeitig verwenden (eine Technik, die auch im WLAN-Standard IEEE 802.11n verwendet wird).

Die Skalierbarkeit eines WMNs bedeutet weitere Herausforderungen. Viele gängige Kommunikationsprotokolle bekommen innerhalb von größeren Multi-Hop-Umgebungen Probleme, was bedeutet, dass die Leistungsfähigkeit eines Netzes mit steigender Ausdehnung stark abnimmt. Routingprotokolle können eventuell keine zuverlässige Route für die Daten mehr ermitteln, Transportprotokolle verlieren unter Umständen die Verbindung und der Datendurchsatz von MAC-Protokollen verringert sich immens. Auch die Kollisionsvermeidung ist in WMNs nicht trivial.

Da WMNs ihre Stärken aus der Mesh-Topologie ziehen, können MAC- und Routingprotokolle, die gerade auf diese Netzstruktur eingehen, gegenüber unspezialisierten Protokollen massive Performanceverbesserungen bringen. Einige davon werden in 2.4 vorgestellt.

Damit potentielle Nutzer keine Bedenken haben WMNs zu nutzen, ist die Sicherheit innerhalb der Netze ein wichtiges Thema. Bereits existierende Sicherheitskonzepte lassen sich nicht unbedingt ohne weiteres auf WMNs übertragen. So existiert beispielsweise keine zentrale Authorität, die Zertifikate ausstellen könnte. Außerdem bietet der grundlegende technische Aufbau von WMNs eine große Angrifsfläche für potenzielle Angreifer. Kapitel 3 geht näher auf einige Sicherheitsbedenken ein.

So wie die Sicherheit ist auch eine einfache Benutzbarkeit von WMNs zentral für die Akzeptanz beim Nutzer. Wireless Mesh Networks sollten sich weitgehend automatisch verhalten, d.h. organisieren,

konfigurieren und Fehler behandeln. Gleichzeitig sollte ein manuelles Eingreifen durch Administratoren dennoch leicht möglich sein. Auch Clients, die selber keine Mesh-Routing-Fähigkeiten besitzen, sollten sich mit einem WMN verbinden können. Daher ist es sinnvoll Mesh-Router einzusetzen, die zwischen unterschiedlichen Wireless-Netzwerken vermitteln können [AWW05, S. 455 f.].

2.4 Routingprotokolle

Die Routenfindung in Mesh-Netzwerken lässt sich auf unterschiedliche Art und Weise umsetzen. Dabei kann zunächst zwischen zwei grundlegend unterschiedlichen Ansätzen unterschieden werden:

Topologiebasierte Routingverfahren funktionieren auf Basis von Wissen über den logischen Netzaufbau. Sie nutzen Informationen über Nachbarschaftsbeziehungen zwischen den Knoten um Daten an ihr Ziel zu leiten.

Positionsbasierte Routingverfahren nutzen Daten über die physische Position der Knoten im Netzwerk, die z.B. über GPS gewonnen werden. Verbindungen zwischen nahe beieinanderliegenden Knoten können bevorzugt werden.

Wir werden die topologiebasierten Routingverfahren im Folgenden näher betrachten und anhand einiger Beispiele ihre Funktionsweise erläutern.

2.4.1 Proaktive Verfahren

Proaktive Routingverfahren sammeln im Voraus Informationen über die Verbindungen der einzelnen Knoten untereinander. Auf diese Art und Weise liegt das zum Routing benötigte Wissen bereits vor, wenn tatsächlich Nutzdaten versendet werden sollen. Ein Nachteil dieses Verfahrens ist jedoch die Erzeugung zusätzlichen Verkehrs durch Kontrollpakete, da die Informationen über die Topologie periodisch aktualisiert werden müssen. Eine Verbindung oder ein Knoten könnte schließlich jederzeit ausfallen, oder es könnte ein neuer Knoten hinzukommen, der eine bessere Route ermöglicht [MS11, S. 404].

Ein aktuelles Beispiel für ein proaktives Routingverfahren ist *Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N.)*. B.A.T.M.A.N. basiert auf der Idee, das Wissen über die Netztopologie zu dezentralisieren. Kein einzelner Knoten muss über die Lage aller anderen Knoten informiert sein um Nachrichten an sie zu versenden. Stattdessen reicht es aus, dass jeder Knoten weiß, in welche Richtung er Daten senden muss um ein bestimmtes Ziel zu erreichen.

Jeder Knoten sendet in regelmäßigen Abständen eine sogenannte *Originator Message (OGM)* als Broadcast an alle Nachbarn. Diese Nachricht hat den Zweck den Knoten im Netzwerk bekannt zu machen und die Qualität der Routen im Netz zu bestimmen. Die Nachbarn leiten die OGM wiederum an ihre Nachbarn weiter, usw. Dadurch erfährt jeder Knoten von der Existenz der anderen. Damit die OGMs nicht endlos hin und her geschickt werden, wird jede von ihrem Ursprungsknoten mit einer Sequenznummer versehen, die nur bei einer neu generierten Nachricht inkrementiert wird. Dadurch können Duplikate festgestellt und behandelt werden.

In den Knoten werden für jeden Nachbarn drei Metriken zur Verbindungsqualität berechnet (siehe Abbildung 2.5). Jeder Knoten A speichert die letzten N empfangenen OGMs ab. Die *Receive Quality (RQ)* für einen Nachbarn B ergibt sich aus dem Anteil an von B ausgehenden OGMs in den N Nachrichten. Aus der Tatsache, dass eine von A an B gesendete und von ihm per Broadcast weitergeleitete OGM im Normalfall auch wieder A erreicht, lässt sich die *Echo Quality (EQ)* ableiten. Auch sie wird wieder über die letzten empfangenen OGMs ermittelt. Aus beiden Metriken kann nun die *Transmit Quality (TQ)*, also die Qualität der Verbindung von A nach B, bestimmt werden.

Da die EQ die Wahrscheinlichkeit beschreibt, dass ein Paket erst von A nach B und dann von B nach A erfolgreich versendet wurde gilt $EQ = TQ \cdot RQ$. Daraus folgt $TQ = \frac{EQ}{RQ}$. Dieser Wert wird als 8-Bit-Zahl in den OGMs mitgesendet (anfänglich mit dem Maximum 255 initialisiert) und von jedem Knoten unter Einbeziehung der TQ zum vorherigen Knoten angepasst. Mit jedem Sprung wird zusätzlich ein *Hop Penalty* von der TQ abgezogen, sodass kürzere Routen längeren vorgezogen werden (vgl. Abbildung 2.6). Wenn ein Knoten die gleiche OGM über mehrere unterschiedliche Routen erhält, bestimmt er jeweils deren TQ und sendet anschließend die weiter, die den höheren Wert besitzt.

Am Ende kennt jeder Knoten zu jedem potentiellen Ziel im Netz den Nachbarn, der seine Daten am schnellsten und zuverlässigsten in die richtige Richtung weiterleiten wird [HLP11, S. 13 ff.].

Im Jahr 2007 wurde eine Weiterentwicklung namens *B.A.T.M.A.N. advanced (batman-adv)* begonnen, die anstelle des Network-Layers (OSI Layer 3) den Data-Link-Layer (Layer 2) für das Routing verwendet. Das Routing findet also direkt auf MAC-Ebene in einem Linux-Kernel-Modul statt, und die Routen werden in einem eigenen Netzwerk-Interface verborgen. Das erlaubt den flexiblen Einsatz unterschiedlicher Netzwerkprotokolle auf Schicht 3 (z.B. IPv4, IPv6), beschränkt allerdings den Einsatz zunächst auch auf Linux-Systeme [bat07].

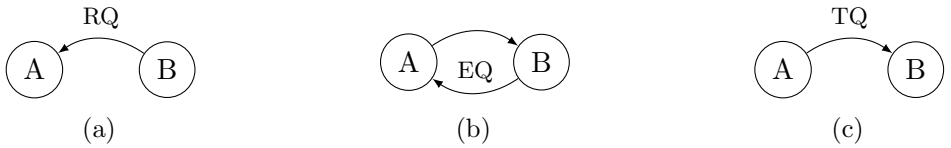


Abbildung 2.5: Verbindungsqualitäten in B.A.T.M.A.N. Netzen. RQ, EQ und TQ stehen jeweils für die Wahrscheinlichkeit, dass ein Paket empfangen wird.

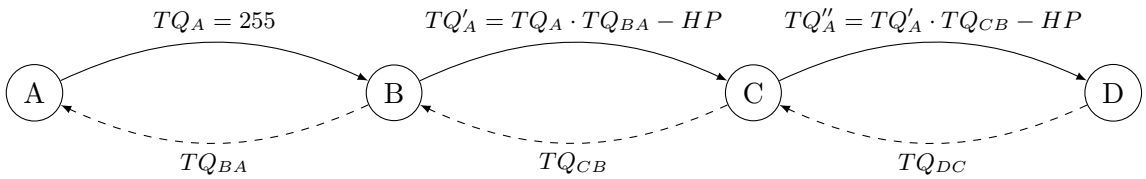


Abbildung 2.6: Weiterverbreitung der Transmit Quality in einem B.A.T.M.A.N.-Netz. In jedem Knoten wird die im Paket mitgesendete TQ mit der TQ zum vorherigen Knoten multipliziert und der Hop Penalty (HP) abgezogen.

2.4.2 Reaktive Verfahren

Reaktive Routingverfahren bestimmen im Gegensatz zu den proaktiven Verfahren die beste Route für zu sendenden Daten erst in dem Moment, in dem sie tatsächlich verschickt werden sollen. Dies führt unweigerlich zu einer Verzögerung im Versand des ersten Datenpakets, da zunächst die Routenbestimmung abgeschlossen werden muss. Der Vorteil von reaktiven gegenüber proaktiven Verfahren liegt ganz klar darin, dass weniger Overhead durch Kontrollpakete erzeugt wird, was die Auslastung der Datenverbindungen, sowie der einzelnen Clients, verringert [MS11, S. 404 f.].

Ein Beispiel für ein reaktives Routingverfahren ist der *Ad hoc On-Demand Distance Vector (AODV)*-Algorithmus. Jeder Knoten besitzt eine Routingtabelle, die alle ihm bekannten Routen zu anderen Knoten enthält. Solange Daten an ein Ziel gesendet werden sollen, für das dem Sender-Knoten bereits eine Route bekannt ist, kommt AODV nicht zum Einsatz. Soll eine Route zu einem neuen Ziel gesucht werden, sendet der Knoten eine *Route Request (RREQ)*-Nachricht per Broadcast in das Netz. Eine Route gilt als gefunden, wenn entweder der Zielknoten direkt gefunden wird, oder

ein anderer Knoten gefunden wird, der eine Route zum Ziel kennt. Ist dies der Fall, wird eine Unicast-Nachricht (*Route Reply, RREP*) an den Anfragesteller zurückgesendet, die über die gleiche Route zurückläuft, über die der Request ursprünglich gekommen ist. Jeder Knoten merkt sich also woher er einen an ihn weitergeleiteten Request bekommen hat. Alle Knoten beobachten die Verbindung zu Nachbarknoten auf ihnen bekannten Routen. Sobald ein Abbruch erkannt wird, wird eine *Route Error (RERR)*-Nachricht an andere Nachbarn des Knoten, der den Fehler bemerkt hat, versendet. Diese Nachricht gibt an, welche Ziele durch den Ausfall der Verbindung nun nicht mehr erreicht werden können, wodurch nun gegebenenfalls bekannte Routen invalidiert werden können [PBRD03].

2.4.3 Hybride Verfahren

Hybride Routingverfahren kombinieren sowohl proaktive als auch reaktive Ansätze. Ein Beispiel für einen solchen Algorithmus ist das *Zone Routing Protocol (ZRP)*. Im ZRP wird für jeden Knoten eine lokale Nachbarschaft festgelegt, die aus allen Knoten bestehen, die über höchstens k Sprünge erreichbar sind. Für alle Knoten innerhalb der Nachbarschaft wird über ein proaktives Verfahren eine Routingtabelle angelegt, sodass Daten direkt zu nahe gelegenen Zielen geleitet werden können. Liegt der Zielknoten nicht in der Nachbarschaft des Senders kommt ein reaktives Verfahren zum Einsatz. Allen Knoten, die am Rand der Zone liegen, wird eine *Route Request*-Nachricht gesendet, die daraufhin prüfen, ob das Ziel von ihnen aus innerhalb von k Sprüngen erreichbar ist. Ist dies nicht der Fall, fügen sie ihre Adresse zur Anfrage hinzu und leiten sie an ihre peripheren Knoten weiter. Andernfalls wird eine *Route Reply* den Pfad zurück an den ursprünglichen Sender geschickt, der diesen Pfad dann zum Versenden von Daten nutzen kann [HPS02].

2.5 IP-Adresszuweisung

Damit überhaupt Kommunikation in einem WMN stattfinden kann, benötigen alle beteiligten Geräte eine IP-Adresse. Dies betrifft sowohl Mesh Router, als auch Mesh Clients. Außerdem ist gegebenenfalls die Möglichkeit einer Verbindung nach außen notwendig.

Um die fehlerfreie Verteilung von IP-Adressen zu vereinfachen bietet es sich an, dass Router und Clients unterschiedliche private Adressbereiche zugewiesen bekommen. Ein Mesh Router kann jedem mit ihm verbundenen Client eine IP-Adresse zuweisen (z.B. per DHCP), was dem üblichen Vorgehen in Single-Hop-Umgebungen entspricht. Auf diese Weise besteht die Möglichkeit IP-Adressen für Clients innerhalb eines WMNs mehrfach einzusetzen, solange die entsprechenden Clients mit unterschiedlichen Routern verbunden sind. Die Verbindung zu anderen Mesh Routern und deren Clients, sowie zu anderen Netzwerken und dem Internet, wird durch *Network Address Translation (NAT)* ermöglicht [BCS+10, S. 7 f.].

Da ein zentraler DHCP-Server in einem WMN nicht praktikabel ist, muss die Vergabe der IP-Adressen für die Router durch ein anderes Verfahren erfolgen, das die dynamische Topologie eines WMNs in betracht zieht. Nicht nur einzelnen neuen Knoten muss eine eindeutige Adresse zugewiesen werden. Ein zusätzlicher Knoten kann auch ein Verbindungsglied zu einem weiteren WMN sein, womit plötzlich sehr viele neue Knoten dem Netzwerk beitreten, die zuvor bereits über IP-Adressen verfügten. Um sicherzustellen, dass es auch hierbei nicht zu Adresskonflikten kommt, muss kontinuierlich geprüft werden, ob es doppelte IP-Adressen im Netzwerk gibt (*In-service non-unique address detection*). Das kann prinzipiell durch zwei Vorgehensweisen realisiert werden: aktiv, indem periodisch Kontrollpakete versendet werden, durch die die Adressen der Knoten im Netz abgeglichen werden, oder passiv, indem Konflikte durch Fehler in den Routing-Vorgängen bemerkt

werden. Da der passive Ansatz durch einen geringeren Overhead die Ressourcen des Netzwerks schont, ist er dem aktiven im Allgemeinen vorzuziehen.

Ein solcher passiver Autokonfigurationsmechanismus ist *Passive Autoconfiguration For Mobile Ad-hoc Networks (PACMAN)*. Er basiert auf der Idee, dass sich jeder Mesh Router selbst eine IP-Adresse zuweist, von der er vermutet, dass sie noch nicht verwendet wird. Diese Vermutung beruht auf Beobachtungen des Routing-Traffics im Netz und auf Informationen zu bekannten IP-Adressen, die von benachbarten Routern bereitgestellt werden. Anschließend werden eventuelle Konflikte durch *Passive Duplicate Address Detection (PDAD)* festgestellt. PDAD besteht aus einigen Algorithmen, die aufgrund von Routingprotokollereignissen Rückschlüsse darauf ziehen, ob eine Adresse mehrfach zugewiesen wurde. Einige Ereignisse treten nur (oder häufiger) auf, wenn dies der Fall ist. Ein Beispiel hierfür ist ein Algorithmus, der Sequenznummern in Routingpaketen analysiert. Da jeder Knoten seine eigene Sequenznummer hochzählt, kann von einer doppelt vergebenen Adresse ausgegangen werden, wenn ein Router ein Paket mit seiner eigenen IP-Adresse, aber einer höheren Sequenznummer erhält. Wird durch PDAD ein Adresskonflikt beobachtet, wird der betreffende Router darüber informiert und kann seine eigene Adresse ändern [BCS+10, S. 10 ff.].

3
Sicherheit in WMNs

Wie bereits in Kapitel 2.3 angeführt, ist die Sicherheit ein bedeutendes Thema für den Betrieb eines Wireless Mesh Networks. Allerdings sorgt die Multi-Hop-Struktur mit ihrer Abhängigkeit von Zwischenknoten, sowie die kabellose Übertragung der Daten für ernstzunehmende Schwachstellen. Im Folgenden werden einige mögliche Angriffe auf WMNs auf unterschiedlichen Protokollschichten, sowie Gegenmaßnahmen zu ihnen vorgestellt.

3.1 Angriffe auf dem Physical Layer

Der Physical Layer dient dem Auf- und Abbau der Verbindung, sowie der Übetragung der Daten über das Medium Funk. An dieser Stelle sind WMNs, wie alle anderen kabellosen Netzwerke, besonders anfällig gegenüber Attacken durch Störsender. Störsender behindern die zum Datenaustausch genutzten Funkfrequenzen und können bei ausreichender Stärke gegebenenfalls die Übertragungen im gesamten Netz blockieren. Aber auch schwächere Störsender können, wenn sie an den richtigen Stellen eingesetzt werden, einen Großteil des Netzwerks lahmlegen [Sen13, S. 3].

Angriffe auf dem Physical Layer könen durch *Frequenzspreizung* verhindert werden. In der Variante *Frequency Hoppping Spread Spectrum (FHSS)* wird das zu sendende Signal auf mehrere Kanäle unterschiedlicher Frequenz aufgeteilt, die nacheinander in einer pseudozufälligen Reihenfolge verwendet werden. Der Empfänger muss die gleichen Frequenzkanäle wie der Sender verwenden, um die Nachricht zu erhalten. Dadurch, dass sich permanent die zur Datenübertragung genutzte Frequenz ändert, besteht für den Angreifer keine Möglichkeit das Signal zuverlässig zu stören.

Beim *Direct Sequence Spread Spectrum (DSSS)* wird jedes Bit des Nutzsignals mit einem längeren (pseudozufälligen) Spreizcode per XOR verknüpft, womit die gesamten Daten über eine größeres Spektrum verteilt werden und so im Hintergrundrauschen untergehen. Im Empfänger wird derselbe Spreizcode auf die empfangenen Daten angewandt, wodurch die Nutzdaten wieder entspreizt werden. Auftretende Störsignale werden dort jedoch zum ersten Mal mit mit dem Spreizcode verknüpft und dadurch geschwächt.

Damit ein Angreifer bei Verwendung einer dieser Techniken das Signal sicher stören kann, muss ihm entweder der genaue zeitliche Ablauf der Frequenzwechsel bekannt sein (FHSS) oder er muss den verwendeten Spreizcode kennen (DSSS) [Sen13, S. 12].

3.2 Angriffe auf dem Data Link Layer

Auf dem Data Link Layer sind eine ganze Reihe von Attacken denkbar. Die einfachste ist sicherlich das Abhören der gesendeten Nachrichten. Dies ist zum einen von außen möglich, wenn sich ein Angreifer in Reichweite der Übertragungspartner befindet. Zum anderen kann aber auch ein bösartiger Knoten

innerhalb des Netzes den über ihn weitergeleiteten Verkehr unbemerkt mitprotokollieren. Diese Daten können später auch für einen Replay-Angriff verwendet werden [Sen13, S. 3 ff.].

Um dem Abhören von Nachrichten entgegenzuwirken, können sie verschlüsselt übermittelt werden. Zwar kann man so nicht verhindern, dass ein Angreifer die Nachricht abfängt. Allerding kann er ohne Kenntnis des nötigen Schlüssels ihren Inhalt nicht auslesen. Replay-Attacken lassen sich verhindern, indem eine paketweise Authentifizierung durchgeführt wird, bei der für jedes Paket vom Sender und Empfänger ein neuer Schlüssel berechnet wird. Ein durch einen Replay-Angriff gesendetes Paket verwendet somit einen veralteten Schlüssel und kann vom Empfänger automatisch verworfen werden [Sen13, S. 12 f.].

Auch auf dem Data Link Layer kann das Netzwerk gestört werden. Ein Knoten könnte permanent MAC-Frames ohne Nutzdaten versenden, was dazu führen würde, dass andere Teilnehmer den Kanal immer als belegt ansehen und erst später versuchen ihre Daten zu senden (nach einer Backoff-Periode). Dies führt ultimativ zu einem *Denial of Service*. Zusätzlich kann der unnötige Datenverkehr dazu führen, dass mobilen Mesh-Clients durch dessen Verarbeitung die Energie schneller ausgeht, als eigentlich nötig wäre. Auch das wiederholte absichtliche Verursachen von Kollisionen führt dazu, dass Datenpakete immer wieder erneut gesendet werden müssen, wobei die Wartezeit zwischen zwei Versuchen möglicherweise exponentiell ansteigt. Intelligentere Störversuche nutzen Sensoren, die aufgrund von Annahmen über genutze Protokolle auf höheren Schichten eine Trafficanalyse durchführen und so ganz gezielt bestimmte Verbindungen stören können [Sen13, S. 3 ff.].

Das permanente Senden von Stör-Frames kann durch *Rate Limiting* behandelt werden. Pakete, die über das festgelegte Limit hinaus gesendet werden, können vom Empfänger ignoriert werden, was ihm erlaubt auf die kostspielige Verarbeitung und Beantwortung der Nachrichten zu verzichten. Dabei kann das Limit allerdings nicht unter dem gewünschten Datendurchsatz des Netzwerks liegen. Ein zu niedrig gewähltes Limit beschränkt also die Leistungsfähigkeit des Netzwerks. Ein anderer Ansatz ist ein *Zeitmultiplexverfahren*, bei dem jedem Knoten ein festes Zeitfenster für Übertragungen eingeräumt wird. Knoten, die wiederholt gegen dieses Zeitfenster verstoßen, lassen sich leicht identifizieren und anschließend z.B. vom Netzwerk ausschließen.

Das erneute Senden von Daten nach Paketkollisionen lässt sich gegebenenfalls durch Fehlerkorrekturverfahren verhindern. Allerdings eignen sich diese Verfahren eher zur Behandlung sporadischer Fehler. Ein Angreifer wird immer mehr Daten beschädigen können, als ein fehlerbehandelnder Code korrigieren kann. Zudem steigt bei der Verwendung von Fehlerkorrekturen der Verarbeitungs- und Übertragungsaufwand [WS02, S. 51].

3.3 Angriffe auf dem Network Layer

Der Network Layer wird üblicherweise für das Routing der Daten im Netzwerk verwendet[1]. Angriffe auf die Kontrollpakete der Routingprotokolle können somit sehr schnell dafür sorgen, dass sich große Teile des Datenverkehrs in der Hand der Angreifer befinden.

Zwei eng verwandte Attacken auf WMNs, die reaktive Routingprotokolle nutzen, sind der *Rushing-* und der *Wormhole-Angriff*. Beide haben zum Ziel, dass sämtliche Daten zu einem (oder mehreren) bestimmten Zielknoten über einen Knoten geleitet werden, den der Angreifer kontrolliert. Im Rushing-Angriff leitet dazu der bösartige Knoten einen Route-Request schneller zum Ziel weiter, als alle anderen Knoten, was ihn mit hoher Wahrscheinlichkeit auf der besten Route liegen lässt. Dies kann in einigen Protokollen zum Beispiel durch absichtliches ignorieren von vorgegebenen Wartezeiten möglich sein. Der Wormhole-Angriff erfordert zwei oder mehr boshafte Knoten, zwischen

[1] Eine Ausnahme bildet z.B. das in 2.4.1 vorgestellte *batman-adv*.

denen über ein weiteres Übertragungsmedium ein schneller Tunnel besteht. Route-Requests werden nun zwischen diesen Knoten über den Tunnel übertragen, was ihnen enorme Geschwindigkeitsvorteile bei der Routenfindung verschafft. Sobald die betroffenen Knoten in etablierten Routen vorkommen, können sie den Verkehr protokollieren oder die Daten ganz oder teilweise zurückhalten, um einen Denial of Service zu verursachen. Ein weiterer Angriff, mit dem Ziel das Netzwerk zu blockieren, ist der *Blackhole-Angriff*. Ein Knoten, der den Blackhole-Angriff durchführen möchte, beantwortet einfach alle Route-Requests mit einer positiven Antwort. Da er keine echte Route finden muss, kann er immer sehr schnell antworten. Das hat zur Folge, dass ein Großteil der Datenpakete aus seiner Nachbarschaft über ihn geroutet werden, wo sie dann einfach verworfen werden.

Angriffe, die auf Basis kurzer Antwortzeiten auf Route-Requests funktionieren, können abgewehrt werden, indem nicht immer direkt der erste empfangene Request weitergeleitet wird. Stattdessen werden alle Route-Requests gesammelt und anschließend einer von ihnen zufällig ausgewählt und weitergesendet. Dabei muss festgelegt werden, wie viele Anfragen maximal angesammelt werden und wie viel Zeit maximal bis zur Weiterleitung vergehen darf. Je kleiner die Anzahl der gesammelten Route-Requests, desto höher ist die Wahrscheinlichkeit, dass einer von ihnen einen kompromittierten Knoten enthält. Bei einer hohen Anzahl an Requests hat die definierte Wartezeit einen großen Einfluss auf die Performanz des Netzwerks. Beide Variablen können auch pro Route-Request dynamisch vom Anfrageknoten festgelegt werden [HPJ03, S. 34].

Bei einer *Sybil-Attacke* täuscht ein Knoten mehrere Identitäten im Netzwerk vor, die von anderen Teilnehmern alle als getrennte Knoten wahrgenommen werden. Routing-Protokolle in WMNs nutzen die unterschiedlichen Pfade im Netz, um eine höhere Zuverlässigkeit und besseren Datendurchsatz zu erreichen. Durch das Vorgeben mehrerer Knoten, die in Wahrheit über dasselbe physische Gerät erreichbar sind, führen mehrere angeblich unterschiedliche Routen über denselben Punkt, was diese Vorteile zunichte macht. Zusätzlich besitzt der angreifende Knoten nun wieder die Kontrolle über den Datenfluss durch sämtliche gefälschten Knoten [Sen13, S. 5 ff.].

Sybil-Angriffe können auf unterschiedliche Art und Weise abgewehrt werden. Ein naheliegendes Verfahren ist die Verifizierung jedes Knotens durch eine zentrale Autorität, der eine Liste aller erlaubten Identitäten vorliegt und die ein Angreifer nicht manipulieren kann.

Eine weiteres Vorgehen basiert auf der Annahme, dass ein physischer Knoten nur in der Lage ist auf einem Kanal zur Zeit zu senden und zu empfangen. Um Sybil-Knoten in seiner Nachbarschaft zu entdecken, fordert ein Teilnehmer alle seine benachbarten Knoten auf auf einem jeweils anderen Kanal eine Nachricht zu versenden. Anschließend lauscht er auf einem zufällig gewählten Kanal. Ein Knoten, der mehrere Identitäten vortäuscht, kann nur auf einem einzigen der geforderten Kanäle antworten. Somit besteht eine gewisse Wahrscheinlichkeit, dass er nicht den Kanal auswählt, auf dem der Initiator nun lauscht und dadurch eine gefälschte Identität als solche identifiziert werden kann. Durch mehrfache Wiederholung dieses Verfahrens sinkt die Wahrscheinlichkeit, dass ein Sybil-Knoten unentdeckt bleibt rapide [NSSP04].

3.4 Angriffe auf dem Transport Layer

Auf dem Transport Layer können Schwächen der verwendeten Transportprotokolle ausgenutzt werden, um die Funktionalität eines WMNs zu stören. Ein häufig verwendetes Protokoll ist TCP, dessen *Three-Way-Handshake* für eine *SYN-Flooding-Attacke* ausgenutzt werden kann. Normalerweise wird beim Aufbau einer TCP-Verbindung vom initiierenden Knoten eine *SYN-Nachricht* an den Verbindungspartner geschickt, der diese mit einer *SYN/ACK-Nachricht* beantwortet. Darauf antwortet der erste Knoten noch einmal mit einer *ACK-Nachricht*, die eine im Vergleich zur SYN/ACK-Nachricht um eins erhöhte Sequenznummer enthält. Damit ist die Verbindung hergestellt. Beim SYN-Flooding

erzeugt der angreifende Knoten sehr viele SYN-Nachrichten (gegebenenfalls mit einer gefälschten Absenderadresse), die alle vom Ziel verarbeitet und beantwortet werden. Allerdings sendet der Angreifer nie die finale ACK-Nachricht, womit sämtliche Verbindungen halb geöffnet bleiben und (zumindest für einige Zeit) im Speicher des Zielknotens gehalten werden. Bei einer ausreichend großen Anzahl an SYN-Nachrichten kommt es dann dazu, dass der Knoten keine legitimen Anfragen mehr bearbeiten kann. Je nach Rolle dieses Zielknotens im Netzwerk werden somit weite Teile des Datenverkehrs unterbunden.

SYN-Flooding lässt sich durch mehrere Vorgehensweisen entgegenwirken. Wenn die IP-Adresse des Angreifers eingegrenzt werden kann, können entsprechende Nachrichten einfach herausgefiltert werden. Eine weitere Möglichkeit wäre es den verfügbaren Speicher für halb geöffnete Verbindungen zu erhöhen, beziehungsweise die Zeitspanne, bis diese verworfen werden, zu verringern. Bei einem Überlauf kann alternativ die älteste Verbindung recyclet werden. *SYN-Caches* und *SYN-Cookies* verringern den benötigten Speicher. Bei der Nutzung eines SYN-Caches werden pseudozufällige Bits aus der SYN-Nachricht in Kombination mit der Absender-IP und dem Port gehasht und Teile der Verbindungsanfrage über diesen Hash in einer Hashtabelle abgelegt. Sowohl jeder Hash-Bucket, als auch die gesamte Tabelle, besitzen eine maximale Anzahl an Einträgen, bei deren Überschreitung der älteste verworfen wird. Durch das Hashing unter Einbeziehung des Zufalls kann ein Angreifer nicht gezielt Hash-Buckets überfüllen. Bei SYN-Cookies werden überhaupt keine Daten über eine halb geöffnete Verbindung gespeichert. Stattdessen werden die über die Verbindung bekannten Daten (IP-Adressen, Ports, SYN-Sequenznummer) zusammen mit einem Geheimnis gehasht. Dieser Hash wird dann auf die benötigte Länge gekürzt und als Sequenznummer der SYN/ACK-Nachricht verwendet. Bei Eintreffen einer Bestätigung wird deren Sequenznummer um eins dekrementiert und der Hash für das neue Paket berechnet. Nur wenn der neue Hash mit der dekrementierten Sequenznummer übereinstimmt wird die Verbindung im Speicher des Knotens angelegt [Edd07, S. 6 ff.].

Eine weitere Möglichkeit des Angriffs auf dem Transport Layer ist das *Session-Hijacking*. Dabei gibt sich der angreifende Knoten gegenüber dem Ziel als einer der Knoten aus, mit dem dieser zuvor eine TCP-Verbindung aufgebaut hatte. Gelingt es dem Angreifer, die zur Kommunikation benötigte *Sequenznummer* des Verbindungspartners zu ermitteln, kann er die TCP-Sitzung kapern [Sen13, S. 8 f.].

Zur Sicherung des Transport Layers kommen *Secure Socket Layer (SSL)* und die Weiterentwicklung *Transport Layer Security (TLS)* zum Einsatz, die übertragene Daten symmetrisch verschlüsseln, wobei die Schlüsselerzeugung sicher über asymmetrische Verfahren ausgehandelt wird [Sen13, S. 32].

3.5 Angriffe auf dem Application Layer

Angriffe auf Anwendungsebene werden beispielsweise mithilfe von Viren und Würmern durchgeführt. Dabei bieten WMNs den Schadprogrammen gute Möglichkeiten sich weiterzuverbreiten, da Knoten oft mehrere direkte Nachbarn besitzen und Daten für andere Knoten weiterleiten.

Weiterhin besteht die Möglichkeit von *Repudiation-Attacks*, in denen ein Angreifer innerhalb des Netzwerks bestimmte Daten manipuliert um entweder nicht-existierenden Verkehr zwischen Knoten vorzutäuschen, oder Datenaustausch zu vertuschen [Sen13, S. 9 f.].

Zur Verteidigung dienen nach außen hin Firewalls und *Intrusion Detection Systeme*, wie etwa Virenscanner. Interne Datenmanipulationen können zum Beispiel durch digitale Signaturen festegestellt und verhindert werden [Sen13, S. 32].

4

Anwendungen und Initiativen

Wireless Mesh Networks kommen in vielen unterschiedlichen Bereichen zum Einsatz. Ihr Eigenschaften werden sowohl von Privatpersonen und Vereinen, als auch von Unternehmen und Regierungsorganisationen, aus verschiedensten Gründen geschätzt. Im Folgenden werden drei unterschiedliche Motivationen zur Verwendung von WMNs erläutert und Einsatzbeispiele angeführt.

4.1 Freie Netze

Seit einigen Jahren schließen sich weltweit Gemeinschaften zusammen, die es sich zum Ziel gesetzt haben für jedermann *freie Netze* zu errichten und zu betreiben. Dabei steht der Gedanke im Vordergrund, dass die Bürger sich selber für den Ausbau der Vernetzung einsetzen, frei von staatlichen oder wirtschaftlichen Interessen. Der Begriff der *freien Netze* ist dabei ähnlich dem Begriff der *freien Software* zu interpretieren, und zwar nicht als *gratis*, sondern vielmehr so, dass die Freiheit der Nutzer der zentrale Gedanke ist.

Beim Aufbau von diesen Community-Netzen, die teilweise ganze Stadtteile abdecken können, haben sich kabellose Technologien etabliert. Sie sind allgemein zugänglich, unabhängig von bestehender Infrastruktur und eignen sich gut für verteilte Netzwerke.

Mit dem Aufkommen des Funkstandards IEEE 802.11b entwickelten sich zu Beginn der 2000er Jahre mehrere unabhängige Gruppierungen, die mit freien kabellosen Netzwerken experimentierten. Zwei einflussreiche Initiativen waren *Consume the Net* und *free2air* aus London, die unter anderem auch Workshops zum Thema anboten. Gründer dieser Gruppen waren wesentlich an der Entstehung des *Pico Peering Agreement (PPA)* mitbeteiligt, das bis heute eine zentrale Rolle in der Ideologie vieler Community-Netze darstellt.

Community-Netzwerke basieren darauf, dass jeder Betreiber eines Netzes im Rahmen seiner eigenen Möglichkeiten freiwillig Netzwerkressourcen zur Verfügung stellt, die von jedem genutzt werden können. Das im Jahr 2003 verfasste PPA ist ein Versuch unterschiedliche freie Netze unter diesem Gesichtspunkt miteinander zu verbinden. Anfang der 2000er Jahre kam das Problem auf, dass zwar immer mehr Gemeinschaftsnetze entstanden, diese jedoch größtenteils getrennt voneinander existierten und kein Datenaustausch zwischen ihnen möglich war. Aus den Workshops „BerLon“ Ende 2002 in Berlin, sowie „Copenhagen Interpolation“ 2003 in Kopenhagen ging ein Dokument hervor, welches eine formale Beschreibung der Leistungen bietet, die der Betreiber eines freies Netzes erbringt und aufgrund derer andere sein Netz nutzen können [Med04, S. 190 ff.]. Zentrale Punkte des PPA sind:

Freier Transit: Der Betreiber erklärt, dass Daten frei und ohne von ihm gestört oder manipuliert zu werden, seine Netzwerkinfrastruktur passieren dürfen.

Offene Kommunikation: Der Betreiber veröffentlicht alle zur Nutzung des Netzes benötigten Informationen unter einer freien Lizenz und erklärt zumindest über Email erreichbar zu sein.

Keine Garantie: Es besteht keine Garantie für die Leistung oder Verfügbarkeit des Netzes. Der Betrieb kann jederzeit eingestellt werden.

Nutzungsbestimmungen: Der Betreiber darf Nutzungsbestimmungen definieren, die zusätzliche angebotene Dienste betreffen, jedoch nicht dem sonstigen PPA wiedersprechen.

Das PPA stellt lediglich eine Vorlage für eine Peering-Abmachung dar. Es kann von jedem Betreiber um zusätzliche Punkte erweitert werden [pic].

Ebenfalls auf der „BerLon“ kamen Pläne auf, in Berlin ein freies Funknetz aufzubauen. Es wurden regelmäßige Treffen veranstaltet und das Webportal *freifunk.net* entstand. Im September 2003 wurde der gemeinnützige *Förderverein Freie Netzwerke e.V.* gegründet, der seitdem Projekte im Bereich freier Netzinfrastrukturen finanziell und rechtlich unterstützt und Hauptträger von freifunk.net ist [frea].

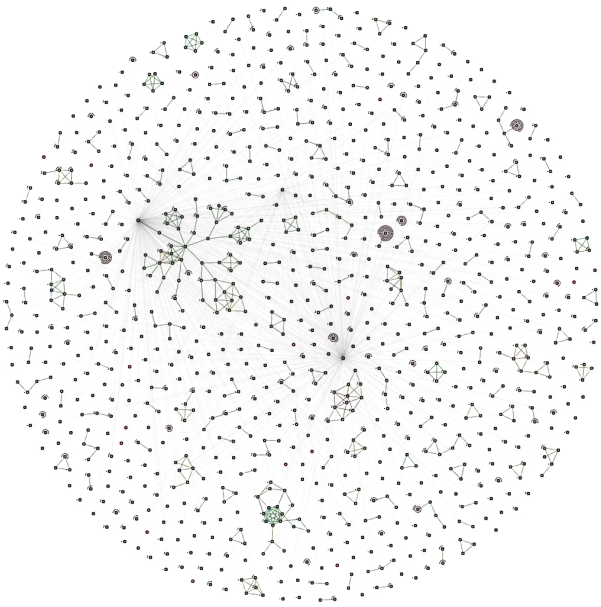
Freifunk ist der größte Zusammenschluss von freien Funknetzwerken in Deutschland. Die Gemeinschaft ist dezentral in einzelnen Communities organisiert, die in ihren Netzen eine lokale Alternative zu großen Kommunikationsprovidern sehen. Unter anderem wird über Freifunk-Netze ein kostenloser Internetzugang geboten. Teilweise geschieht dies dadurch, dass Mitglieder freiwillig einen Teil ihrer privaten Bandbreite zur Verfügung stellen. Einige Communities besitzen jedoch auch zentrale Gateways oder sind sogar selber als Internet-Provider registriert. Der Internetanschluss ist jedoch nicht das Hauptziel der Freifunk-Initiative. Es geht vielmehr darum unabhängige Netze zu schaffen, die nicht von wirtschaftlichen oder politischen Interessen beeinflusst werden. Erklärte Ziele sind die Aufklärung über Kommunikations- und Informationsfreiheit, die Verminderung der digitalen Spaltung in Deutschland, die Verbreitung von Wissen, die Aufklärung über Netztechnologien und nicht zuletzt auch die Förderung von sozialen Strukturen. Die freien Netze, deren Betrieb sich explizit auf das Pico-Peering Agreement beruft, sollen öffentlich, anonym, nicht kommerziell und unzensiert sein und sich dezentral im Besitz der Gemeinschaft befinden. Jeder kann sich einer lokalen Community anschließen oder selber eine gründen. In den Netzen werden auch lokale Dienste angeboten, an denen sich jeder beteiligen kann, wie zum Beispiel regionale Nachrichten, Chaträume, Spieleserver, Kollaborationstools oder Audio- und Videoangebote [fred].

In Deutschland besteht die sogenannte *Störerhaftung*, nach der ein Betreiber eines Netzwerks dafür haftet, wenn ein Dritter über seinen Anschluss Rechtsverletzungen begeht. Um dem zu entgehen, kommen in vielen Communities VPN-Tunnel zum Einsatz, entweder ins Ausland (zum Beispiel nach Schweden oder die Niederlande, wo es keine entsprechenden Gesetze gibt), oder zu anderen Freifunk-Vereinen, die das *Providerprivileg* besitzen und daher nicht haftbar gemacht werden können [free].

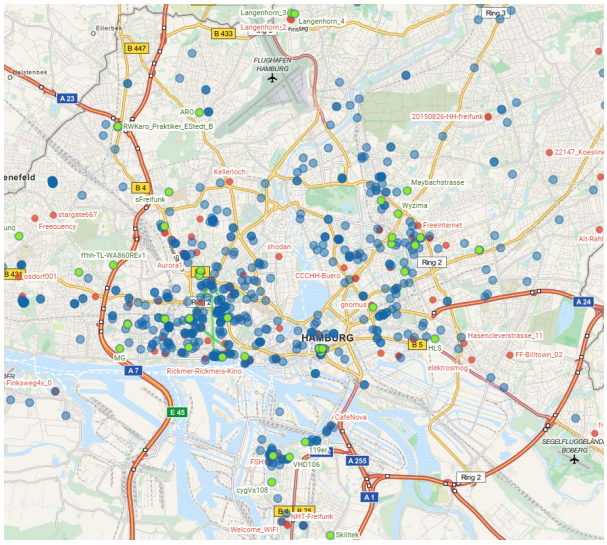
Das Freifunk Netzwerk besteht aktuell aus 228 Communities[2] (zwei davon unter dem Namen der österreichischen Initiative *FunkFeuer*) mit insgesamt über 26 000 Knoten. Die größten Communities sind *Freifunk Moehne* in Südwestfalen mit ca. 1400 Zugängen, *Freifunk Nordwest* um den Raum Oldenburg, *Freifunk München* (jeweils ca. 1100 Zugänge), *Freifunk Münster* und *Freifunk Hamburg* (jeweils ca. 1000 Zugänge). Aufgrund der Größen dieser Gemeinschaften werden diese jedoch inzwischen teilweise weiter in Ortsgruppen unterteilt, damit ein stabiler Betrieb der Mesh-Netze gewährleistet werden kann. Abbildung 4.1 zeigt den Aufbau des Hamburger Freifunk-Netzes [freb].

Das aktuell weltweit wohl größte Community-Netzwerk ist das spanische *guifi.net*. Es umfasst über 30 000 aktive Knoten, die zu einem großen Teil an der spanischen Ostküste liegen, jedoch vereinzelt auch bis Asien, Afrika und Südamerika reichen [gui]. Weitere (deutlich kleinere) Projekte sind das griechische *Athens Wireless Metropolitan Network* (ca. 2400 Knoten [awm]), *Ninux.org* aus Italien (ca. 350 Knoten [nin]), *Île Sans Fil* in Montreal (ca. 260 Knoten [ile]) und *Personal Telco* in Portland, Oregon (ca. 100 Knoten [per]).

[2] Stand: 07.12.2015



(a) Topologische Ansicht. Viele Knoten sind nicht direkt miteinander vernetzt, sondern lediglich per VPN an eines der drei Gateways angebunden.



(b) Geographische Ansicht. Blaue Knoten sind gerade online, grüne Knoten sind neu hinzugekommen und rote Knoten sind offline.

Abbildung 4.1: Das Netzwerk von Freifunk Hamburg. Quelle: [frec]

4.2 Erschließung schlecht ausgebauter Gebiete

Neben ideologischen gibt es für viele Menschen auch rein praktische Gründe sich mit Wireless Mesh Networks auseinanderzusetzen. In ländlichen Gebieten ist es oft schwer überhaupt eine Breitbandverbindung zu bekommen, geschweige denn eine relativ preisgünstige. Telekommunikationsprovider bauen ihr Netz hier häufig nicht aus, da die damit verbundenen Kosten die zu erzielenden Einnahmen um ein Vielfaches übersteigen würden. Hier kommen wieder von der Gemeinschaft selber organisierte Netze zum Einsatz.

Ein Beispiel ist die dünn besiedelte Halbinsel Djursland in Dänemark auf der 25% der Haushalte keinen Breitbandanschluss über existierende Provider bekamen. In der Folge gründeten sie lokale Selbsthilfegruppen, um das Problem anzugehen. Acht Dörfer waren bereits per Glasfaser an den dänischen Internetbackbone angebunden. Innerhalb der Dörfer wurden die Haushalte über WMNs versorgt. Gleichzeitig wurde der Anschluss per Richtfunk an benachbarte Dörfer weitergeleitet, die ihrerseits über WMNs und Richtfunkverbindungen zu weiteren Orten verfügten. Dadurch konnte ein Großteil der Bevölkerung zu sehr geringen Kosten (einmalige Anschaffung der Hardware und niedrige Instandhaltungskosten) an das Internet angebunden werden [dju]. Auch die bereits erwähnte Initiative guifi.net setzt sich stark für den Ausbau der Infrastruktur auf dem Land ein.

Es sollte beachtet werden, dass die Anbindung über Funk unter Betrachtung der Zukunftsperspektiven jedoch der direkten Anbindung über Kupfer- bzw. Glasfaserleitungen immer noch um einiges nachsteht. Zwar sind die Anschaffungskosten deutlich geringer, da keine neue Infrastruktur benötigt wird. Allerdings teilen sich so viele Haushalte die Kapazität der einen Funkverbindung, was schnell zu Engpässen führen kann [Man10].

Die Non-Profit-Organisation *One Laptop Per Child* setzt ebenfalls auf Wireless Mesh Networks zur Erschließung schlecht ausgebauter Gebiete. Die Initiative hat sich der Verbreitung von Computerhardware zu Bildungszwecken in Entwicklungsländern verschrieben. Das Gerät *OLPC XO* (auch als *$100 Laptop* bekannt) besitzt eingebaute Mesh-Routing-Fähigkeiten. Laptops können über den

Standard IEEE 802.11s (der auf einem hybriden MAC-Layer-Routingprotokoll basiert) Verbindung zu anderen Geräten in der Nähe aufnehmen. Die Reichweite der ausklappbaren Antennen des Geräts beträgt dabei bis zu 200 Meter. Da die Energieeffizienz der Hardware in den Einsatzgebieten eine sehr hohe Priorität hat, beschränkt sich die Bandbreite der Übertragung auf maximal 2 Mbit. Durch die Implementierung des Routings direkt im Netzwerkchip können selbst ausgeschaltete Laptops noch als Mesh-Router agieren [olpb]. Für die Verbindung zu externen Computersystemen, beispielsweise Schul-Servern, befindet sich derzeit eine *Active Antenna* in der Entwicklung, die eine als USB-Netzwerkinterface angeschlossene Standalone-Variante der verbauten WMN-Chips ist [olpa].

Im Internet sind mehrere Leitfäden zur Errichtung von Wireless Mesh Networks in Entwicklungsländern zu finden, in denen von der Planung, über den Aufbau, bis zur Instandhaltung der Netze, alle relevanten Informationen enthalten sind. Beispiele sind *Building a Rural Wireless Mesh Network* des Projekts *Wireless Africa* [rur] und das Buch *Wireless Networking in the Developing World* [wnd].

4.3 Kommerzielle Anwendungen

Auch im kommerziellen Bereich werden an vielen Stellen Wireless Mesh Networks, gerade für ihre Fähigkeiten zur Kommunikation in schwer erreichbaren Gebieten, eingesetzt. Im Bergbau wird mithilfe von WMNs eine Echtzeit-Kommunikation (sowohl Audio, als auch Video) zwischen Bergarbeitern und der Oberfläche ermöglicht. Dies erhöht zum einen die Sicherheit der Arbeiter und spart zum anderen viel Zeit bei der Verständigung. Eine Kabelverbindung ist in Minen nicht praktikabel, da die Verlegung recht zeitaufwändig ist und Kabel schnell beschädigt werden können. WMNs können hingegen schnell errichtet und erweitert werden, um mit den sich ständig ändernden Begebenheiten einer Mine mitzuhalten [Hen08].

Die dynamische Anpassungsfähigkeit ist auch für das Militär von großer Bedeutung. Traditionelle, auf einer Sichtverbindung basierende, Kommunikationsmittel stoßen in Einsatzgebieten schnell an ihre Grenzen. Durch WMNs kann die Kommunikation auch um Hindernisse, wie Berge oder Wälder, herum aufrechterhalten werden. Netzwerke werden beispielsweise zwischen den einzelnen Fahrzeugen eines Konvois errichtet, um zwischen dem ersten und dem letzten Fahrzeug eine Videoübertragung zu ermöglichen. Dabei kann ein Fahrzeug über eine Satellitenverbindung Kontakt zum Internet herstellen und an die anderen weiterleiten. Gerade die Ausfallsicherheit durch die dezentrale Architektur und redundante Verbindungen zwischen einzelnen Netzwerkknoten machen WMNs für militärische Zwecke interessant [raj].

Ein Wireless Mesh Network der etwas anderen Art kommt im Satellitensystem *Iridium* zum Einsatz. Iridium stellt über 66 Satelliten im Erdorbit flächendeckend Kommunikationsdienstleistungen auf der ganzen Welt zur Verfügung. Die Satelliten kommunizieren über Intersatellitenlinks mit je vier benachbarten Satelliten, um Daten so im Netz zu verteilen, dass sie möglichst schnell an eine Verbindungsstelle auf der Erde weitergeleitet werden können. Dabei nutzen sie Mikrowellen im Frequenzbereich zwischen 26,5 und 40 GHz. Das Vermitteln der Daten zwischen den Satelliten ermöglicht im Vergleich zu anderen Systemen deutlich geringere Latenzen und eine geringere Anzahl an Stationen auf der Erde [Gup].

5 Zusammenfassung

In dieser Arbeit wurde ein grundlegender Überblick über verschiedene Aspekte von Wireless Mesh Networks vermittelt. Es wurden unterschiedliche Architekturtypen vorgestellt, zentrale Eigenschaften der Netze aufgeführt und die bedeutende Faktoren für die Leistungsfähigkeit von WMNs erläutert. Außerdem wurden gängige Routingprotokolle erklärt, die in Wireless Mesh Networks Anwendung finden.

Es wurden mögliche Sicherheitsrisiken in WMNs hervorgebracht und entsprechende Abwehrmechanismen diskutiert.

Abschließend wurden unterschiedliche Anwendungsgebiete vorgestellt, in denen Wireless Mesh Networks heutzutage zum Einsatz kommen. Ein sehr großer Anteil der Menschen, die WMNs nutzen, tut dies aus ideologischen und netzpolizischen Gründen. Es sollen freie und unabhängige Netze für jeden zur Verfügung stehen. Das bereitstellen eines kostenlosen Internetzugangs nimmt dabei eine untergeordnete Rolle ein. WMNs werden aber auch aus rein praktischen Gründen, nämlich in schlecht ausgebauten, oder schwer zugänglichen Gebieten, eingesetzt, und zwar sowohl für das Gemeinwohl, als auch für kommerzielle und militärische Zwecke.

Wireless Mesh Networks sind weiter auf dem Vormarsch, sowohl im Bereich der Community-Netze, als auch auf dem kommerziellen Markt. Ihre positiven Eigenschaften der Selbstkonfiguration und -heilung, verbunden mit der Fähigkeit entfernte Gebiete zu relativ geringen Kosten in ein Netzwerk zu integrieren, machen sie zu einer gefragten Technologie. Für die aus ihrer Natur erwachsenden potenziellen Sicherheitsrisiken wurden im Allgemeinen gute Lösungen gefunden, was auch ihren Einsatz in sicherheitskritischen Bereichen gestattet. Als Grundstein für freie Netze erlauben sie diesen sich weiter in einem hohen Tempo auszubreiten, um so vielleicht tatsächlich irgendwann eine echte Alternative zu großen Kommunikationsprovidern darzustellen. Mit der stetigen Weiterentwicklung der zugrundeliegenden Funktechnologien wird sich die Leistungsfähigkeit der Netze in Zukunft immer weiter verbessern.

Literaturverzeichnis

[awm] Athens wireless metropolitan network. http://wind.awmn.net/?page=nodes. Stand: 07.12.2015.

[AWW05] Ian F. Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks: a survey. *COMPUTER NETWORKS*, 47(4):445–487, 2005.

[bat07] Wireless kernel tweaking: or how B.A.T.M.A.N learned to fly. Video. http://downloads.open-mesh.org/batman/misc/24c3-2292-en-wireless_kernel_tweaking.webm, 2007. Stand: 24.11.2015.

[BCS+10] Carlos J. Bernardos, Maria Calderon, Ignacio Soto, Ana Beatriz Solana, and Kilian Weniger. Building an IP-based community wireless mesh network: Assessment of PACMAN as an IP address autoconfiguration protocol. *Computer Networks*, 54(2):291–303, 2010.

[dju] Djurslands.net. http://freifunk.net/sc2004/DJURSLANDSNET.html. Stand: 07.12.2015.

[Edd07] W. Eddy. TCP SYN flooding attacks and common mitigations. RFC 4987, RFC Editor, August 2007.

[frea] Förderverein Freie Netzwerke e.V. http://foerderverein.freie-netzwerke.de/organisation/. Stand: 07.12.2015.

[freb] Freifunk Community finden. http://freifunk.net/wie-mache-ich-mit/community-finden/. Stand: 07.12.2015.

[frec] Freifunk Hamburg Karte. https://map.hamburg.freifunk.net/. Stand: 07.12.2015.

[fred] Freifunk Vision. http://freifunk.net/worum-geht-es/vision/. Stand: 07.12.2015.

[free] Technik der Community Netzwerke. https://freifunk.net/worum-geht-es/technik-der-community-netzwerke/. Stand: 07.12.2015.

[gui] guifi.net World. https://guifi.net/en/guifi_zones. Stand: 07.12.2015.

[Gup] Om Gupta. Iridium - a global communication network. http://web.stanford.edu/class/aa247/Iridium_Innovations.pdf. Stand: 10.12.2015.

[Hen08] Byron Henderson. Miners give a nod to nodes. *Mission Critical Magazine*, July 2008.

[HLP11] Martin Hundebøll and Jeppe Ledet-Pedersen. Inter-flow network coding for wireless mesh networks. Master thesis, Aalborg University, Denmark, June 2011.

[HPJ03] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *ACM Workshop on Wireless Security (WiSe)*, pages 30–40, 2003.

[HPS02] Zygmunt J. Haas, Marc R. Pearlman, and Prince Samar. The Zone Routing Protocol (ZRP) for ad hoc networks. https://tools.ietf.org/html/draft-ietf-manet-zone-zrp-04, 2002.

[ile] Île sans fil - À propos. http://www.ilesansfil.org/a-propos/. Stand: 07.12.2015.

[Man10] Urs Mansmann. Alle schnell ans Netz: Breitband-Internet in ländlichen Gebieten. *c't*, (10):152, 2010.

[Med04] Armin Medosch. *Freie Netze - Geschichte, Politik und Kultur offener WLAN-Netze*. Heise Zeitschriften Verlag, 2004.

[MS11] C. Meinel and H. Sack. *Internetworking: Technische Grundlagen und Anwendungen*. X.media.press. Springer Berlin Heidelberg, 2011.

[nin] Ninux.org. `http://map.ninux.org/`. Stand: 07.12.2015.

[NSSP04] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis defenses. In *Third International Symposium on Information Processing in Sensor Networks*, pages 259–268, April 2004.

[olpa] The OLPC Wiki: Active Antenna. `http://wiki.laptop.org/go/Active_Antenna`. Stand: 09.12.2015.

[olpb] The OLPC Wiki: Networking. `http://wiki.laptop.org/go/Networking`. Stand: 09.12.2015.

[PBRD03] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (aodv) routing. RFC 3561, RFC Editor, July 2003.

[per] Personal Telco Project - node map. `http://map.personaltelco.net/`. Stand: 07.12.2015.

[pic] Pico peering agreement v1.0. `http://www.picopeer.net/PPA-de.shtml`. Stand: 07.12.2015.

[raj] Battle-tested broadband for mission-critical applications. `http://www.rajant.com/applications/federal-military-civilian/`. Stand: 10.12.2015.

[rur] Building a rural wireless mesh network. `http://wirelessafrica.meraka.org.za/wiki/index.php/DIY_Mesh_Guide`. Stand: 09.12.2015.

[Sen13] Jaydip Sen. Security and privacy issues in wireless mesh networks: A survey. *CoRR*, abs/1302.0939, 2013.

[wnd] Wireless networking in the developing world. `http://www.wndw.net/`. Stand: 09.12.2015.

[WS02] A. Wood and J.A. Stankovic. Denial of service in sensor networks. *Computer*, 35(10):54–62, Oct 2002.