Untersuchung von Wireless Mesh Network-Routing-Protokollen für den Einsatz in Netzen für Katastrophengebiete

A. Paguem Tchinda, Dr. A. Lehmann, Prof. Dr. -Ing. U. Trick, Forschungsgruppe für Telekommunikationsnetze, Frankfurt University of Applied Sciences, Frankfurt am Main, Deutschland, {paguem, lehmann, trick}@e-technik.org

Kurzfassung

Wireless Mesh Network (WMN) ist eine Netzwerkarchitektur, die im Lauf der letzten zehn Jahre das Interesse von vielen Wissenschaftlern geweckt hat. Aufgrund ihrer Eigenschaften werden für WMNs unterschiedliche Anwendungsfelder vorgesehen, insbesondere für den Aufbau eines Notnetzes nach einer Katastrophe. Im Gegensatz zu anderen Netzen unterliegt ein solches Netz einer Reihe von Einschränkungen wie z.B. Kosten, Energieverbrauch oder Topologie-Anpassungsfähigkeit. In diesem Paper wird versucht, aus diesen Einschränkungen die resultierenden Anforderungen für Routing-Protokolle herzuleiten, um einen Performance-Vergleich der Protokolle DSDV, OLSR, DSR, AODV, ZRP, BATMAN, HWMP und Babel zu realisieren. Das Protokoll HWMP zeigt in der Gesamtbetrachtung die besten Ergebnisse. Zusätzlich wird erstmalig das Konzept der Virtualisierung in WMN eingeführt sowie die Möglichkeiten zur Netzoptimierung, die sich daraus ergibt.

Abstract

Wireless Mesh Network is a network architecture, which has aroused the interest of many scientists over the past decade. Because of characteristics like easy deployment, low hardware cost, self-configuration and self-healing, WMN is tipped to be a suitable network architecture for network recovery after natural disaster. In contrast to other networks, a disaster network is submitted to many challenges like costs, energy consumption and adaptability. In this paper, network challenges are used to define requirements for routing protocols. Then this requirements are used to analyze the performance of protocols DSDV, OLSR, DSR, AODV, ZRP, BATMAN, HWMP and Babel. We conclude that the protocol HWMP has the average best performance. In addition, the concept of virtualization is introduced for the first time in WMN as well as the opportunities for network optimization.

1 Einführung

Katastrophen treffen aufgrund ihrer Vielfältigkeit (Feuer, Überschwemmungen, Erdbeben) nahezu alle Regionen der Welt und können schwere menschliche und wirtschaftliche Folgen haben. Die Kommunikation, unabhängig davon, ob sie zwischen den Mitgliedern eines Rettungsteams (z.B. Feuerwehr, Polizei oder Ärzte) oder zwischen den Katastrophenopfern und ihren Familien stattfindet, wurde in [1] als zentrales Element identifiziert, um Leben und Eigentum nach einer Naturkatastrophe zu schützen. Da die öffentlichen Kommunikationsinfrastrukturen nach Unglücken oft zerstört sind, muss unmittelbar nach der Katastrophe ein neues Netz etabliert werden. Dieses Notnetz unterliegt besonderen Herausforderungen bezüglich der benutzten Technologien wie z.B. Wireless Local Area Network (WLAN) oder Long Term Evolution (LTE), Anpassungsfähigkeit der Topologie, Unterstützung dienstorientierter Kommunikation, Sicherheit und Energieeffizienz.

Die zahlreichen technologischen Fortschritte der letzten fünfzig Jahre auf dem Gebiet der drahtlosen Kommunikation haben zur Entwicklung neuer Netzwerk-architekturen wie z.B. Wireless Mesh Network (WMN) geführt. Diese Netze finden heutzutage international Anwendung im Bereich des ländlichen breitbandigen Internetzugangs [2], der Firmen- und Gemeinschaftsnetzwerke [4, 5] sowie beim Wiederaufbau eines Kommunikationsnetzes nach Katastrophen [2, 3]. Aufgrund der Vorteile von WMN-Architekturen wie z.B. geringer Hardwarekosten, dezentralisierter Verwaltung und der selbständigen Aufbau- und Konfigurationsfähigkeit wurden sie von den Autoren in [3, 6] als eine mögliche Lösung genannt, die Kommunikation nach einer Katastrophe wiederherzustellen.

Dieser Aufsatz stellt die innovative Idee sowie die ersten Ergebnisse eines in der Forschungsgruppe für Telekommunikationsnetze der Frankfurt University of Applied Sciences laufenden Forschungsprojektes dar. Ziel hierbei ist es, ein WMN basierend auf geeigneten Routing-Protokollen für den Einsatz in Katastrophengebieten zu optimieren, insbesondere auch durch die Integration von Network Functions Virtualisation (NFV). Der Aufsatz ist wie folgt strukturiert: Kapitel 2 führt die unterschiedlichen WMN-Architekturen ein sowie ihre Abgrenzungen zu anderen Wireless Netzen. In Kapitel 3 wird das NFV-Framework vorgestellt und die Vorteile seiner Integration in WMNs kurz dargestellt. Das Kapitel 4 erläutert die Anforderungen eines Kommunikations-netzes für Katastrophengebiete mit dem Fokus auf das zu verwendende Routing-Protokoll. Diese Anforderungen werden in Kapitel 5 angewandt, um die Einsetzbarkeit der WMN-Routing-Protokolle Optimized Link State Routing (OLSR), Better Approach to Mobile Ad-hoc Networking (BATMAN), Destination-Sequenced Distance Vector (DSDV), Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Zone Routing Protocol (ZRP), Hybrid Wireless Mesh Protocol (HWMP) und Babel in Katastrophenszenarien zu untersuchen. In Kapitel 6 werden die Ergebnisse zusammengefasst und die nächsten Schritte diskutiert.

2 Wireless Mesh Networks (WMN)

Ein WMN ist eine dezentralisierte Netzwerkarchitektur, in der Knoten mit Hilfe einer drahtlosen Technologie (z.B. 802.11, 802.15, 802.16, etc.) verbunden sind. Im Gegensatz zu einem Mobile Ad hoc Network (MANET) oder Vehicular Ad hoc Network (VANET), in denen die Mobilität eine wichtige Bedeutung hat, wird in einem WMN angenommen, dass die Networkknoten statisch sind oder nur eine geringe Mobilität aufweisen. WMNs haben neben ihrer unstrukturierten und dezentralisierten Verwaltungseigenschaft einige weitere Vorteile, die für ihren Einsatz zum Wiederaufbau der Kommunikation nach einer Katastrophe sprechen. Unter diese fallen unter anderem die kostengünstige Hardware und die schnelle Aufbaufähigkeit (ein paar Stunden nach dem Unglück). In der Literatur wird zwischen drei WMN-Kategorien unterschieden:

- **Client Mesh**: Client WMNs unterscheiden sich nur wenig von MANETs in der Hinsicht, dass das Netz mit User-Endgeräten aufgebaut wird. Dabei wird angenommen, dass einige dieser Geräte ortsfest sind und das Grundgerüst des Netzes bilden. Darüber hinaus können einige dieser Endgeräte Gateway-Funktionen anbieten.
- **Infrastructure Mesh**: Infrastructure WMNs werden mit Hilfe von Wireless-Routern und Gateways gebildet. Die User-Endgeräte sind hier nicht Teil des Netzes und müssen daher kein Routing-Protokoll implementieren.
- **Hybrid Mesh**: diese Architektur kombiniert Client- und Infrastructure Mesh-Eigenschaften. Das heißt, in einem hybriden WMN können Endgeräte Nachrichten entweder direkt miteinander oder über das WMN austauschen.

Die Abbildung 1 zeigt die schematische Darstellung eines WMN für den Einsatz in Katastrophengebieten. Das WMN kann genutzt werden, um z.B. Zugang zum Internet und dessen Diensten zu ermöglichen. Hierfür müssen Gateway-Funktionen in bestimmte WMN-Knoten (Edge Nodes) eingebunden werden, die es ermöglichen das Notnetz nach der Katastrophe mit noch bestehenden anderen Infrastrukturen wie z.B. einem Mobilfunknetz zu verbinden.

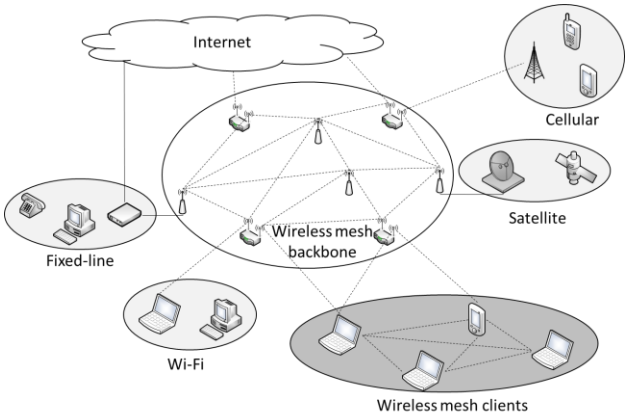

Bild 1 Netzwerkarchitektur im Katastrophengebiet [8]

3 Network Functions Virtualisation (NFV)

Funktionen von Netzelementen oder Netzwerkdiensten, wie zum Beispiel Gateways, Firewalls oder Access Points, sind heutzutage mittels Software realisiert, allerdings läuft diese Software meist auf spezieller Hardware. Nachteilig hierbei sind z.B. die höheren Anschaffungskosten und darüber hinaus eine unflexible Netzstruktur mit festen Netzfunktionen [40]. Um diesen bestehenden Nachteil zu begegnen hat sich eine Gruppe von Netzbetreibern 2012, innerhalb des ETSI zur Industry Specification Group for NFV (ISG NFV), zusammengeschlossen. Bei den Standardisierungsarbeiten zu NFV, wird davon ausgegangen, dass eine Virtual Network Function (VNF) die gleiche Funktion erbringt wie eine Physical Network Function (PNF). Unter einer Network Function (NF) versteht man sowohl ein Netzelement mit spezifischer Funktion, wie zum Beispiel einen DHCP-, oder einen DNS-Server als auch Subnetze mit Switches und Routern für den Nachrichtentransport. Abbildung 2 gibt einen Überblick über eine NFV Framework nach ETSI. Dieses Framework besteht aus der Network Functions Virutalisation Infrastructure (NFVI), welche sich aus den Hardware Ressourcen, also Standard IT Hardware Servern und dem Virtualisation Layer zu Virtualisierung der VNFs zusammensetzt, den VNFs selbst und einer Komponente namens NFV Management and Orchestration [40]. Die folgenden genannten Vorteile können sich durch den Einsatz von NFV ergeben, wie z.B. geringere Gerätekosten, Bereitstellungskosten und Betriebskosten, schnellere Einführung neuer Netzeigenschaften, hohe Skalierbarkeit, Anpassung der Netzkonfiguration an aktuellen Verkehr und dessen Verteilung in nahezu Echtzeit und insbesondere im Hinblick auf den Einsatz in Katastrophengebieten die niedrigere elektrische Leistungsaufnahme.

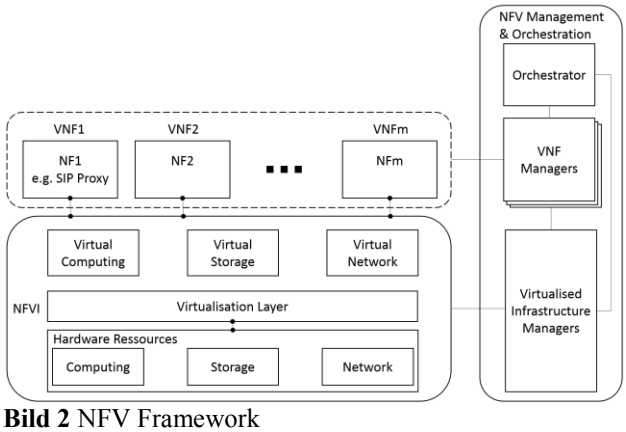

Bild 2 NFV Framework

Durch die bereits genannten Vorteile, die sich durch den Einsatz von NFV ergeben können, kann ein WMN speziell für Katastrophenfälle optimiert werden. Z.B. ermöglicht das NFV-Konzept die Verlagerung von Netzfunktionen. Hieraus resultiert ein weiteres Einsparpotential hinsichtlich des elektrischen Leistungsverbrauchs, da virtuelle Netzfunktionen in Abhängigkeit der Auslastung des jeweiligen WMN-Knotens oder dessen Energiereserven im Netz verschoben werden können.

Die Grundlage allerdings, damit der Einsatz des NFV-Konzepts innerhalb eines WMNs gelingen kann, bilden die zum Einsatz kommenden Protokolle, auf dem das WMN basiert.

4 Anforderungen an WMN-Protokolle

Die Anforderungen an WMN-Routing-Protokolle lassen sich aus den Anforderungen an Netze für Katastrophengebiete herleiten:

Energieeffizienz – Da die auf dem Katastrophengebiet zum Einsatz kommenden Geräte oft batteriebetrieben sind, ist die Lebensdauer des Notnetzes durch den Energieverbrauch der einzelnen WMN-Knoten abhängig. Dies kann verlängert werden, indem ein energie- oder lastberücksichtigendes Routing-Protokoll benutzt wird, das einerseits die Menge an Kontrollpaketen reduzieren kann und andererseits neue Parameter bei der Berechnung der Metriken hinzufügt, um die bestehende Last im Netz und die Knotenrestenergie zu berücksichtigen [9].

Verwendbarkeit – Das Katastrophennetz wird mit dem Ziel gebildet, bestimmte Dienste (z.B. Audio oder Videotelefonie) und deren entsprechende Quality of Service (QoS) bereitzustellen. Das heißt, das Protokoll muss geringe Latenzzeiten, Jitter und Paketverlustraten sowie maximalen Durchsatz anbieten.

Kapazität – Aufgrund der großen Nachfrage an Informationen (z.B. für die Koordination von Helfern oder für Überlebende, die ihre Freunde und Familien kontaktieren wollen) nach der Katastrophe und in Abhängigkeit der Größe des betroffenen Gebietes muss das Netz eine erhebliche Anzahl von Nutzern unterstützen können. Das heißt, das Protokoll muss die Verbindung zwischen einer großen Anzahl von Endgeräten und Routing-Knoten ermöglichen.

Nachhaltigkeit – Das gebildete Notnetz muss die Kommunikation im Katastrophengebiet solange gewährleisten, bis das übliche Kommunikationsnetz wiederhergestellt ist. Es darf daher nicht ausfallen. Diese Anforderung ist durch eine dezentralisierte Verwaltung zu erreichen, bei der alle Knoten gleichberechtigt sind. Das heißt, das Protokoll muss auf einer flachen Topologie basieren.

Anpassungsfähigkeit – Das Katastrophennetzwerk muss auf Änderungen im Netz reagieren können. Das heißt, das Routing-Protokoll muss sowohl neue Verbindungen und Knoten wie auch Verbindungs- und Knotenausfälle erkennen.

Operabilität – Das Notnetz muss überwacht werden können und an die Kommunikationsanforderungen angepasst werden können. Verwaltungs- und Wartungsfunktionen sind dafür notwendig. Das Routing-Protokoll muss daher kontinuierlich die Metrik sämtlicher Verbindungen im Netz bestimmen.

Konnektivität – Das Netz muss die Kommunikation zwischen Mitgliedern einer Gruppe sowie zwischen Mitgliedern unterschiedlicher Gruppen garantieren. Diese Anforderung lässt sich durch hohe Verfügbarkeit und Routenstabilität umsetzen. D.h., das Routing-Protokoll muss in der Lage sein, eine dauerhafte Verbindung zwischen zwei beliebigen Endgeräten im Netz bereitzustellen.

Sicherheit – Die Sicherheit ist ein wichtiger Aspekt in WMNs. Aufgrund des Broadcast-Charakters der physikalischen Schicht, der Knotenmobilität sowie der automatischen Knotenanbindung sind WMNs hinsichtlich Sicherheitsattacken besonders anfällig. Diese Schwierigkeit wird auf der Routing-Protokollebene durch die Implementierung neuer, sicherer Routing-Protokolle wie dem Authenticated Routing for Ad hoc Networks (ARAN) oder die Erweiterung bestehender Protokolle wie dem Secure Routing Protocol (SRP) [12] gelöst.

Praktikabilität – Für Katastrophennetze stehen nur begrenzte Budgets zur Verfügung. Das heißt, das Routing-Protokoll soll im optimalen Fall frei lizenziert und implementierbar sein.

Diese Kriterien werden im nächsten Abschnitt hinsichtlich des Einsatzes verschiedener WMN-Protokolle in Katastrophenscenarios untersucht.

5 Ausgewählte WMN-Protokolle zur Netzoptimierung

Die Leistungsfähigkeit eines WMN hängt stark von dem verwendeten Protokoll ab. In der Literatur werden zahlreiche Algorithmen und Protokolle vorgeschlagen, um das Problem des Routings in WMNs zu lösen. Dieser Aufsatz beschränkt sich auf die meist verbreiteten und zum Einsatz kommenden Protokolle. Diese sind: DSDV, OLSR, DSR, AODV, BATMAN, Babel, HWMP und ZRP. Mit dem Ziel, einen Vergleich auf Basis der bereits genannten Kriterien darzustellen, die sich auf ein beliebiges Routing-Protokoll übertragen lassen, wird hier auf die Kerneigenschaften des Protokolls (Route-Discovery und Wartungsmechanismus, Metrik, Protokollschicht etc.) eingegangen.

5.1 Dynamic Source Routing (DSR)

DSR ist ein reaktives MANET Routing-Protokoll. Das heißt, die Route zwischen der Quelle und dem Ziel wird nur bei Bedarf generiert. Es wurde von der IETF in Form des RFC 4728 [13] spezifiziert und veröffentlicht. DSR gehört zu den Source Routing-Protokollen. Das heißt, die zu übertragenden Datenpakete bekommen beim Senderknoten eine vollständige Wegbeschreibung bezüglich des Zielknotens. Diese Beschreibung enthält die IP-Adresse aller zu durchlaufenden Knoten, was zu einer Vergrößerung des Paket-Headers führt. DSR lässt sich daher schlecht in Kombination mit IPv6 (128 Bit-Adressen) für große Netze (lange Pfade) einsetzen. Aufgrund der „on-demand“ Pfadbestimmung in DSR kann das Protokoll als besonders energieeffizient klassifiziert werden (Nachhaltigkeit). Darüber hinaus ermöglich die Route-Anfrage

beim Route-Discovery-Mechanismus das Erlernen unterschiedlicher Routen zu einem Ziel. Dies hat zwei Vorteile. Es ermöglicht einerseits die Implementierung des Load-Balancing auf der Routing-Protokoll-Ebene. Das heißt, aufeinander folgende Pakete können über verschiedene Wege gesendet werden, um den Energieverbrauch über das Netz besser zu verteilen und die Netzlebensdauer somit zu verlängern. Dieser Vorteil hat zur Entwicklung von zahlreichen energie- und lastberücksichtigenden Protokollen auf Basis von DSR geführt [16-20]. Andererseits kann DSR genutzt werden, um die Ausfallsicherheit im Notnetz zu steigern, indem Pakete gleichzeitig über zwei unterschiedliche Wege geschickt werden (z.B. Pakete mit einer hohen Priorität, wie bei der Echtzeit-Video-Unterstützung für einen Chirurgen im Katastrophengebiet). Das Link Quality Source Routing (LQSR) -Protokoll und das SrcRR -Protokoll sind zwei Erweiterungen von DSR für die WMN-Architektur. Beide Protokolle benutzen die Expected Tansmission Count (ETX) -Metrik.

5.2 Ad hoc On-Demand Distance Vector (AODV)

AODV ist analog zu DSR ein reaktives Routing-Protokoll. Hier wird jedoch beim Sender des Pakets keine komplette Wegbeschreibung für das Ziel hinzugefügt. Stattdessen entscheidet jeder Knoten nach dem Empfang, welcher Knoten sich am besten eignet, um das Ziel zu erreichen. Neben seinem reaktiven Charakter werden in der Literatur [21, 22] zusätzliche Mechanismen beschrieben, um Energie beim Einsatz von AODV zu sparen. Auch wenn AODV in seiner ursprünglichen Version kein Load-Balancing ermöglicht, wurden mehrere Erweiterungen des Protokolls vorgeschlagen, wie das Ad hoc On-demand Multipath Distance Vector (AOMDV), das die gleichzeitige Bestimmung von mehreren Pfaden zwischen zwei Knoten erlaubt. Außerdem unterstützt AODV Multicast.

5.3 Destination-Sequenced Distance Vector (DSDV)

DSDV ist ein proaktives Protokoll. Das heißt, jeder Knoten bestimmt permanent seine Route zu allen möglichen Zielen im Netz. Auf diesem Weg kann die Zeitverzögerung beim Aufbau neuer Verbindungen verringert werden. DSDV ist ein älteres Protokoll und kommt heutzutage nicht mehr zum Einsatz. Zahlreiche Untersuchen in den letzten Jahren haben die schlechte Leistungsfähigkeit von DSDV in Vergleich zu aktuelleren Protokollen wie AODV oder Babel [37, 38] aufgezeigt.

5.4 Optimized Link State Routing (OLSR)

OLSR ist ein proaktives Link-State-Routing-Protokoll für ein MANET. OLSR wurde im RFC 3626 standardisiert [33]. In 2014 wurde eine neue Version dieses Protokolls veröffentlicht, die dem Protokoll eine Metrik hinzufügt, um die Link-Qualität zu berücksichtigen. OLSR wird oft in WMNs (z.B. Freifunk [41]) eingesetzt. In der Literatur werden zahlreiche Mechanismen beschrieben, um Energie in Netzen beim Einsatz von OLSR einzusparen [34, 35]. Auch Sicherheitsmechanismen werden in [36] genannt. Mit OLSR verfügt jeder Knoten über die Kenntnis der kompletten Topologie und kann somit die effektivste Route zum Ziel mittels des Dijkstra-Algorithmus berechnen. Dafür benötigt der Knoten zusätzliche Speicher- und Rechenkapazität.

5.5 Better Approach to Mobile Ad-hoc Networking (BATMAN)

BATMAN [23] ist analog zu OLSR ein proaktives Routing-Protokoll. Eine neue Version wurde entwickelt, um in Schicht 2 des OSI-Modells arbeiten zu können. Dies hat hinsichtlich eines Katastrophenszenarios folgende Vorteile: Beliebige OSI-Layer-3-Protokolle können im Netz verwendet werden. Die Vergabe von IP-Adressen kann zentral verwaltet und damit Endgeräte leichter in das Gesamtnetz integriert werden, sodass Network Address Translation (NAT)-Funktionalitäten an Edge-Routern überflüssig werden. Zusätzlich gibt es hier die Möglichkeit des Roamings von Endgeräten zwischen Access Points. Diese Eigenschaft kann in manchen Szenarien vorteilhaft sein, z.B. im Fall eines Rettungswagens, der durch die Stadt fährt und dabei eine kontinuierliche Verbindung mit dem Krankenhaus behalten soll. Obwohl BATMAN selbst keinen Sicherheitsmechanismus implementiert, wurde in [24] eine Erweiterung des Protokolls (BatCave) vorgeschlagen, mit dessen Hilfe das WMN durch Schlüsselaustausch abgesichert werden kann.

5.6 Hybrid Wireless Mesh Protocol (HWMP)

Das HWMP-Routing-Protokoll ist ein hybrides Protokoll, das in IEEE 802.11s standardisiert wurde [29]. HWMP gehört zu den Traffic-aware Routing Protocols [25]. Das heißt, es wird davon ausgegangen, dass die meisten Pakete von oder zu den Gateways gerichtet sind (z.B. im Fall der Zurverfügungstellung einer funktionsfähigen Internet-Verbindung im Katastrophengebiet). HWMP kombiniert ein proaktives Routing-Protokoll, um die Wege zu den Gateways zu bestimmen, mit einem reaktiven Routing-Protokoll, um den Weg zu anderen Knoten im Netz zu berechnen. HWMP arbeitet auf in Schicht 2 des OSI-Modells und benutzt die Air Time Metrik, um die Qualität der Links zu bestimmen. Diese Metrik berechnet den Ressourcen-Verbrauch, wenn ein Paket über einen Link versendet wird. Das Protokoll HWMP steht im Fokus von vielen wissenschaftlichen Publikationen. In [26] wird ein Verschlüsselungsmechanismus angewandt, um die Manipulation von Routing-Paketen zu verhindern. In [27] und [28], schlagen die Autoren Erweiterungen der Metrik vor, um die verbleibende Energie der Knoten zu berücksichtigen.

5.7 Babel

Babel ist ein proaktives Distance-Vector-Routing-Protokoll, das sowohl in leitungsgebunden als auch drahtlosen Netzen eingesetzt werden kann [30]. Es nutzt im WMN eine Variante der ETX-Metrik. Im Spezifikations-Update von 2013 [31] wurde ein Authentifikationsmecha-

nismus für Babel definiert. Das Protokoll Babel ist für kleine Netze geeignet [30]. Die Analyse nach [32] zeigt, dass Babel eine höhere Leistungsfähigkeit als OLSR und BATMAN aufweist.

5.8 Zone Routing Protocol (ZRP)

ZRP [39] ist ein hybrides Routing-Protokoll. Das heißt, es kombiniert sowohl proaktive als auch reaktive Eigenschaften. ZRP definiert einen Umkreis (Zone) um jeden Knoten im Netz. Innerhalb dieser Zone werden die Routen proaktiv bestimmen. Diese Zone umschließt Knoten mit einer Entfernung kleiner als eine Hop-Anzahl k von der Quelle. Für die Knoten außerhalb dieser Zone werden die Routen reaktiv bestimmt, indem der Source-Knoten eine Route-Anfrage an seinen Edge-Knoten sendet. Da ZRP weder das proaktive Intra-Zone Routing-Protokoll (IARP) noch das reaktive Inter-Zone Routing-Protokoll (IERP) festlegt, ist eine Performanceanalyse schwer zu realisieren. Die hybride Eigenschaft von ZRP ermöglicht es, das Protokoll in großen Netzen einzusetzen. Dabei bleibt jedoch die Anpassungsfähigkeit der Topologie durch die Frequenz der Updates des IARP-Protokolls begrenzt.

6 Zusammenfassung und Ausblick

In Tabelle 1 sind die Ergebnisse der WMN-Routing-Protokoll-Untersuchung zusammengefasst. Aufgrund der Unterschiede in ihren Funktionsprinzipien wie z.B. bei der Verwaltung der Routing-Tabelle (proaktive, reaktive oder hybrid) oder bei der Erkennung der Topologie (Traffic-aware Routing Protocol) lässt sich immer ein Szenario definieren, bei dem eines dieser Protokolle eine bessere Leistungsfähigkeit als alle anderen besitzt. Ziel dieses Aufsatzes ist eine ganzheitliche Sicht auf das Routing-Protokoll, d.h., die Optimierung berücksichtigt möglichst alle der im Kapitel 4 genannten Anforderungen.

Energieeffizienz: Reaktives Routing-Protokoll (R), Energy-Aware (E), Load-Balancing (L), Sonstige (o)
Verwendbarkeit Subjektiv (-/o/+)
Kapazität: Skalierbarkeit-ja (+)-nein (-)
Nachhaltigkeit: hierarchische Topologie (ja/nein)
Anpassungsfähig: proaktive Routing-Protokolle langsamer (-), Babel (o), reaktive Protokolle schneller (+)
Operabilität: Erweiterte Metrik (ja/nein)
Konnektivität: Subjektiv (-/o/+)
Sicherheit: ja/nein
Praktikabilität: Lizenzfrei (ja/nein)

	Energieeffizienz	Verwendbarkeit	Kapazität	Nachhaltigkeit	Anpassungsfähigkeit	Operabilität	Konnektivität	Sicherheit	Praktikabilität
DSR	REL	o	-	ja	+	ja	o	ja	ja
AODV	REL	-	+	ja	+	ja	o	ja	ja
OLSR	EL	o	-	ja	-	ja	o	ja	ja
DSDV	E	-	-	ja	-	ja	-	ja	ja
ZRP	RE	-	+	ja	-	nein	-	ja	ja
BATMAN	o	+	-	ja	-	ja	+	ja	ja
HWMP	RE	+	+	ja/nein	+	ja	+	ja	ja
Babel	o	-	-	ja	+	ja	o	ja	ja

Tabelle 1 WMN-Routing-Protokollvergleich

Besonders viel versprechend ist hier das Protokoll HWMP. Es hat im Vergleich zu BATMAN eine höhere Anpassungsfähigkeit, das heißt, es reagiert schneller auf Knotenausfälle. Ferner kann das Protokoll angepasst werden, um nicht mehr proaktiv die Route zu den Gateways zu bestimmen, sondern zu den Knoten, die nach der NFV-Integration Funktionalitäten wie Web-Server anbieten. Im nächsten Schritt in diesem Projekt soll HWMP mit anderen Protokollen wie BATMAN oder Babel, die auch gute Ergebnisse liefern, für einige Szenarien in Katastrophensituationen experimentell verglichen werden.

7 Literatur

[1] International Telecommunication Union (ITU), “Technical Report on Telecommunications und Disaster Mitigation”, Technischer Bericht, Version 1.0, Juni 2013

[2] A. Yarali, B. Ahsant und S. Rahman, “Wireless Mesh Networking: A Key Solution for Emergency & Rural Applications”, Advances in Mesh Networks, MESH, Juni 2009

[3] M. Portman und A. A. Pirzada, “Wireless-Mesh-Networks for Public safety and Crisis Management Applications”, IEEE Computer Society, Januar /Februar 2008.

[4] C. J. Bernardos, M. Calderon, I. Soto, A. Beatriz Solana und K. Weniger, “Building an IP-based community wireless mesh network: Assessment of PACMAN as an IP address autoconfiguration protocol”, Computer Networks 54, pp.291–303, 2010.

[5] F. Licandro und G. Schembra, “Wireless Mesh Networks to Support Video Surveillance: Architecture, Protocol, and Implementation Issues”, EURASIP Journal on Wireless Communications and Networking Hindawi Publishing Corporation, 2007

[6] D. G. Reina, M. Askalani, S. L. Toral, F. Barrero, E. Asimakopoulou, und N. Bessis, “A survey on multihop ad hoc networks for disaster response scenarios”, International Journal of Distributed Sensor Networks (in press), Mai 2015.

[7] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten und F. D. Turck, “Network function virtualization: State of-the-art and research challenges”, IEEE Communications Surveys and Tutorials, 2016.

[8] A. Lehmann, A. Paguem Tchinda, und U. Trick, “Optimization of Wireless Disaster Network throughNetwork Virtualisation”, in process, International Network Conference, 2016

[9] S. Mamechaoui, F. Didi und G. Pujolle, “A Survey on Energy Efficiency for Wireless Mesh Network”, International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, März 2013

[10] J.-S. Huang und Y.-N. Lien, “Challenges of emergency communication network for disaster response”, IEEE International conference on Communication System (ICCS), Singapore, pp.528-532, November 2012

[11] K. Ali, H. X. Nguyen, Q.-T. Vien, und P. Shah, “Disaster Management Communication Networks: Challenges and Architecture Design”, The Fifth International Workshop on Pervasive Networks for Emergency Management, St. Louis MO., pp.537-542, ISBN: 978-1-4799-8425-1, März 2015.

[12] Thillaikarasi und M. S. Bhanu, “A Survey of Secure Routing Protocols for Wireless Mesh Networks”, International Journal of Computer Applications (0975 – 8887) Volume 97–No.6, Juli 2014

[13] D. Johnson, Y. Hu, und D. Maltz, “The Dynamic Source Routing Protocol (DSR) for Mobile”, RFC 4728, Februar 2007.

[14] F. Dc Rango, P. Lonctti und S. Marano, "MEA-DSR: A Multipath Energy-awarc Routing Protocol for Wireless Ad Hoc Networks", Procecdings of the Seventh Annual Mediterranean Ad Hoc Networking Workshop, Palma de Mallorca, Spain, Juni 2008.

[15] M. Tarique, K. Tepe, und M. Naserian, “Energy Saving Dynamic Source Routing for Ad-hoc Wireless Networks “, In WIOPT, 2005.

[16] I. Stojmenovic und X. Lin, “Power-Aware Localized Routing in Wireless Networks”, IEEE Trans. Parallel and Distributed Systems, 2001.

[17] J.-E. Garcia, A. K. Kyamakya und K. Jobmann, “A Novel DSR-based Energy-efficient Routing Algorithm for Mobile Ad Hoc Netowrks”, IEEE Trans., 2003.

[18] V. N. Talooki, H. Marques, J. Rodrigue und H. Agua, “An Energy Efficient Flat Routing for Mobile Ad-hoc Networks,” Proc. INFSO-ICT-22564, 2010.

[19] X. Li, W. Zi-we und Z. Bao-yu,”A New DSR based Energy Saving Routing in MANET”, Proc. ICCNM, 2003.

[20] M. Timlarasi, S. Chandramithi und T. G. Palanivelu, “Overhead Reduction and Energy Management in DSR for MANET”, Proc. Of COMSWARE, pp. 762-766, Januar 2008.

[21] N. Gupta und S. R. Das, “Energy-aware on-demand routing for mobile ad hoc networks”, In IWDC, Volume 2571, pp.164–173, Januar 2002.

[22] J.-M. Kim, J.-W. Jang, “AODV based Energy Efficient Routing Protocol for Maximum Lifetime in MANET”, Proc. AICT-ICIW, Februar 2006

[23] A. Neumann, C. Aichele, M. Lindner, und S. Wunderlich, “Better approach to mobile ad-hoc networking (B.A.T.M.A.N.)”, Internet Draft (2008), Internet-Draft Intended status: Experimental, http://tools.ietf.org/id/draft-openmesh-b-a-t-m-a-n-00.txt.

[24] A. G. Bowitz, E. G. Graarud, L. Brown und M. G. Jaatun, “BatCave: Adding security to the BATMAN protocol”, Proc. 6th Int. Conf. Digit. Inf. Manage., pp.199-204, 2011

[25] M. E. M. Campista und M. G. Rubinstein, “Advanced routing protocols for wireless networks”, London, Wiley, 2014

[26] D. Bansal, S. Sofat und G. Singh, “Secure Routing Protocol for Hybrid Wireless Mesh Network (HWMN)”, In: International Conference on Computer and Communication Technology (ICCCT), vol. 25, pp.837–843, 2010

[27] A. N. Ming und K-L.A. Yau, “An Energy Efficient Hybrid Wireless Mesh Protocol (HWMP) for IEEE 802.11s Mesh Networks”, pp.17-21, ICCSCE, Dezember 2013.

[28] D. Yuranov und A. Rudakova, “Power Aware Metrics for HWMP in 802.11s”, 7th Conference of Finnish-Russian University Cooperation in Telecommunications, 2010

[29] Institute of Electrical and Electronics Engineers, “HWMP Protocol specification”, Mai 2009

[30] J. Chroboczek, “The Babel Routing Protocol”, RFC 6126, April 2011

[31] D. Ovsienko, “Babel HMAC Cryptographic Authentication”, Juli 2013

[32] D. Murray, M. Dixon und T. Koziniec, “An experimental comparison of routing protocols in multi hop ad hoc networks”, Proc. Australasian Telecommun. Netw. Appl. Conf., pp.159-164, 2010

[33] T. Clausen und P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, RFC 3626, Oktober 2003

[34] A. Benslimane, R. E. Khoury, R. E. Azouzi und S. Pierre, “Energy Power-Aware Routing in OLSR Protocol”, Proc. First Int. Mobile Comp. and Wireless Communication Conf., September 2006

[35] T. Kunz, “Energy-efficient variations of OLSR”, In Wireless Communications and Mobile Computing Conference, 2008 IWCMC '08 International, August 2008.

[36] A. Hafslund, A. Tønnesen, R. B. Rotvik, J. Andersson und Ø. Kure “Securing the OLSR protocol”, Proc. IFIP Med-Hoc-Net. 2003, pp.25-35, 2003

[37] M. Morshed, F. Ko, D. Lim, H. Rahman, R. Mazumder und J. Ghosh, “Performance evaluation of DSDV and AODV routing protocols in Mobile Ad hoc Networks”, Proceedings of International Conference on NISS, pp.399-403, Mai 2010

[38] S. Barakovic und J. Barakovic, “Comparative performance evaluation of Mobile Ad Hoc routing protocols”, Proceedings of International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp.518-523, Mai 2010.

[39] Z. J. Haas, M. R. Pearlman und P.Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks”, Internet Draft, https://tools.ietf.org/html/draft-ietf-manet-zone-zrp-04, 2003.

[40] U. Trick, F. Weber, “SIP und Telekommunikationsnetze”, De Gruyter, 2015

[41] Förderverein Freie Netzwerke e. V. online: https://freifunk.net/, 2016